

Configurar a postura da VPN Linux com o ISE

3.3

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configurações no FMC/FTD](#)

[Configurações no ISE](#)

[Configurações no Ubuntu](#)

[Verificar](#)

[Troubleshooting](#)

[Informações Relacionadas](#)

Introdução

Este documento descreve como configurar a postura da VPN Linux com o Identity Services Engine (ISE) e o Firepower Threat Defense (FTD).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Cisco Secure Client
- VPN de acesso remoto no Firepower Threat Defense (FTD)
- Identity services engine (ISE)

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software:

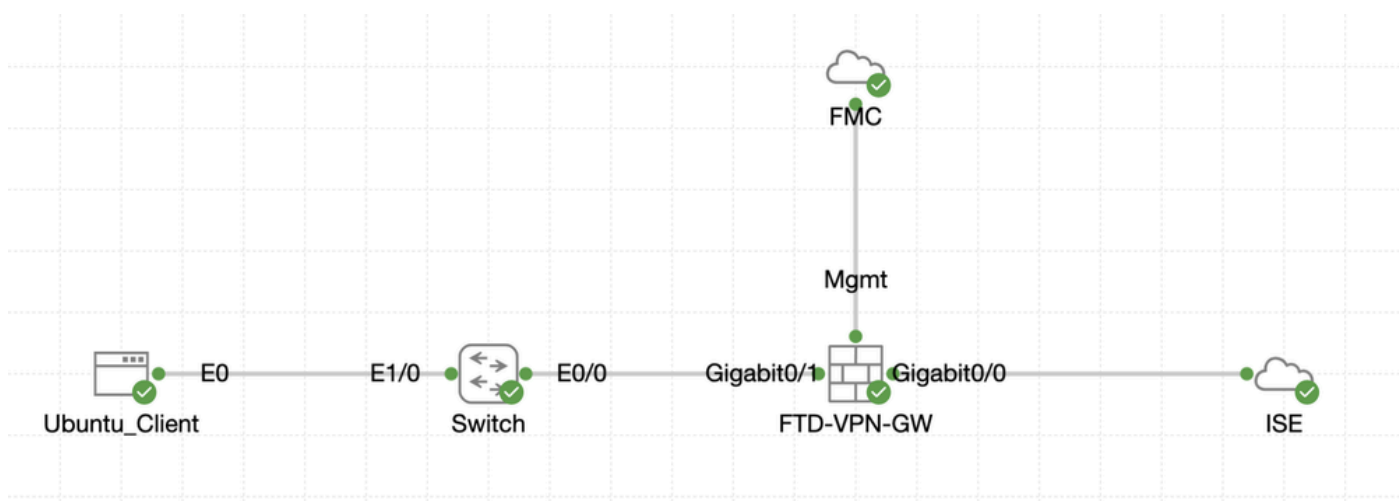
- Ubuntu 22,04
- Cisco Secure Client 5.1.3.62

- Defesa contra ameaças do Cisco Firepower (FTD) 7.4.1
- Cisco Firepower Management Center (FMC) 7.4.1
- Cisco Identity Services Engine (ISE) 3.3

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

Diagrama de Rede



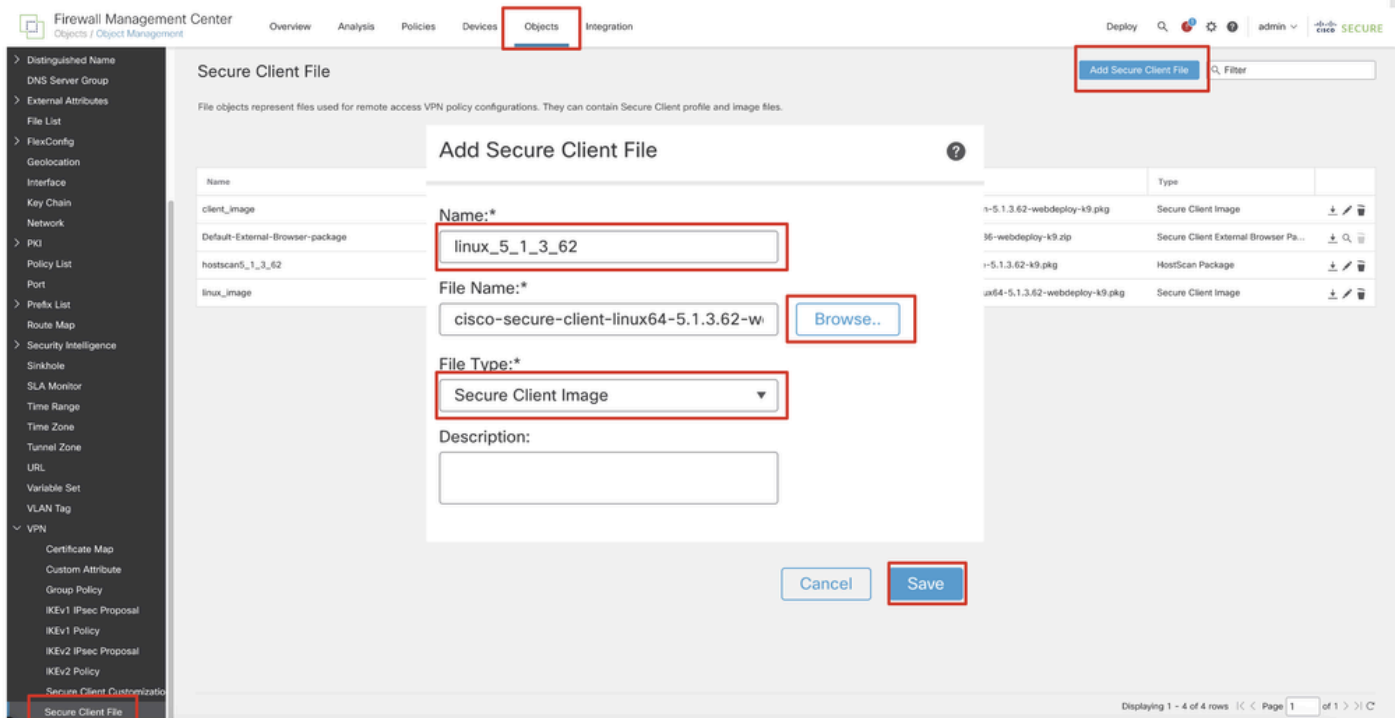
Topologia

Configurações no FMC/FTD

Etapa 1. A conectividade entre o cliente, o FTD, o FMC e o ISE foi configurada com êxito. Como enroll.cisco.com é usado para endpoints que realizam sondagem para redirecionamento (consulte fluxo de postura CCO documentsISE Posture Style Comparison for Pre and Post 2.2 para obter detalhes). Verifique se a rota para o tráfego para enroll.cisco.com no FTD está configurada corretamente.

Etapa 2. Faça o download do nome `cisco-secure-client-linux64-5.1.3.62-webdeploy-k9.pkg` do pacote a partir de [Download do Software Cisco](#) e certifique-se de que o arquivo esteja bom após o download confirmando que o checksum md5 do arquivo baixado é o mesmo que a página Download do Software Cisco.

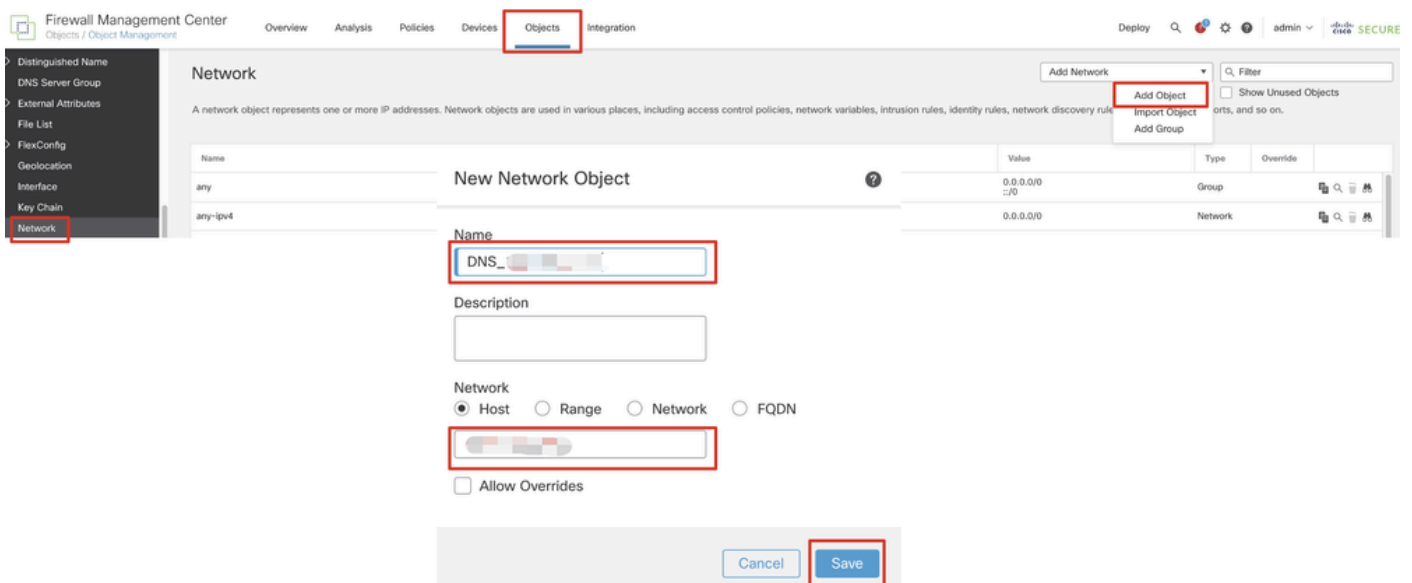
Etapa 3. Navegue até `Objects > Object Management > VPN > Secure Client File`. Clique em `Add Secure Client File`, forneça o nome, procure `File Name` para selecionar `cisco-secure-client-linux64-5.1.3.62-webdeploy-k9.pkg`, selecione `Secure Client Image` na lista suspensa `File Type`. Em seguida, clique em `Save`.



FMC_Upload_Secure_Client_Image

Etapa 4. Navegue até Objects > Object Management > Network.

Etapa 4.1. Crie um objeto para o servidor DNS. Clique em Add Object, forneça o nome e o endereço IP DNS disponível. Clique em Save.

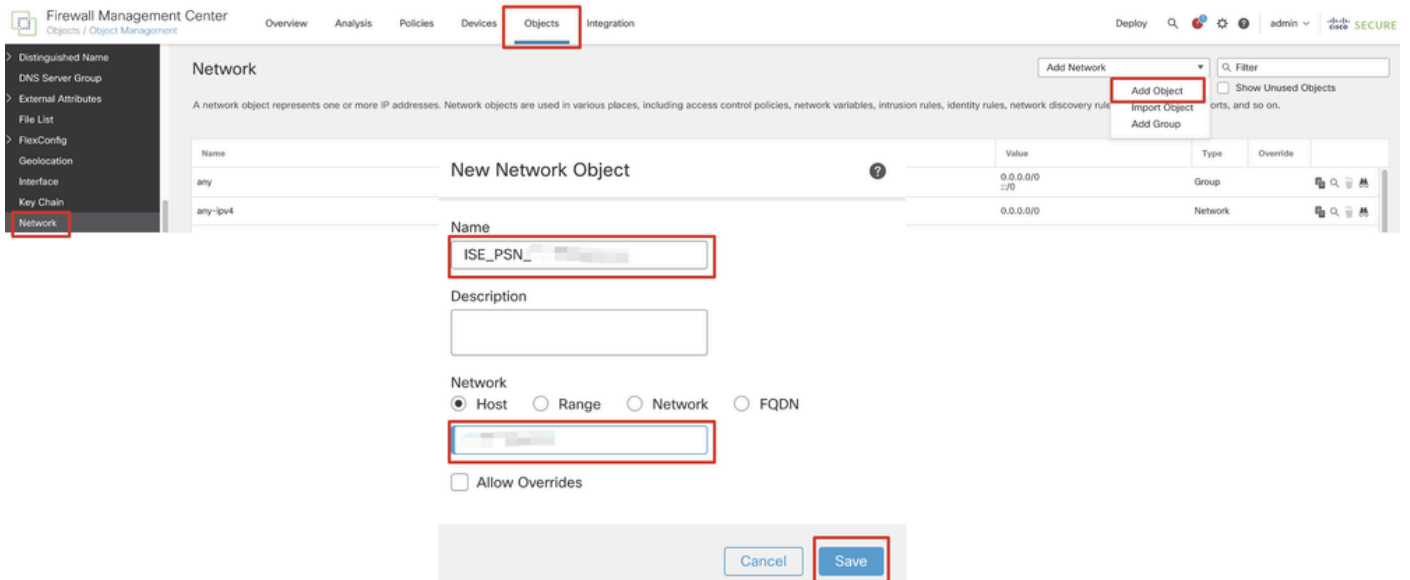


FMC_Add_Object_DNS



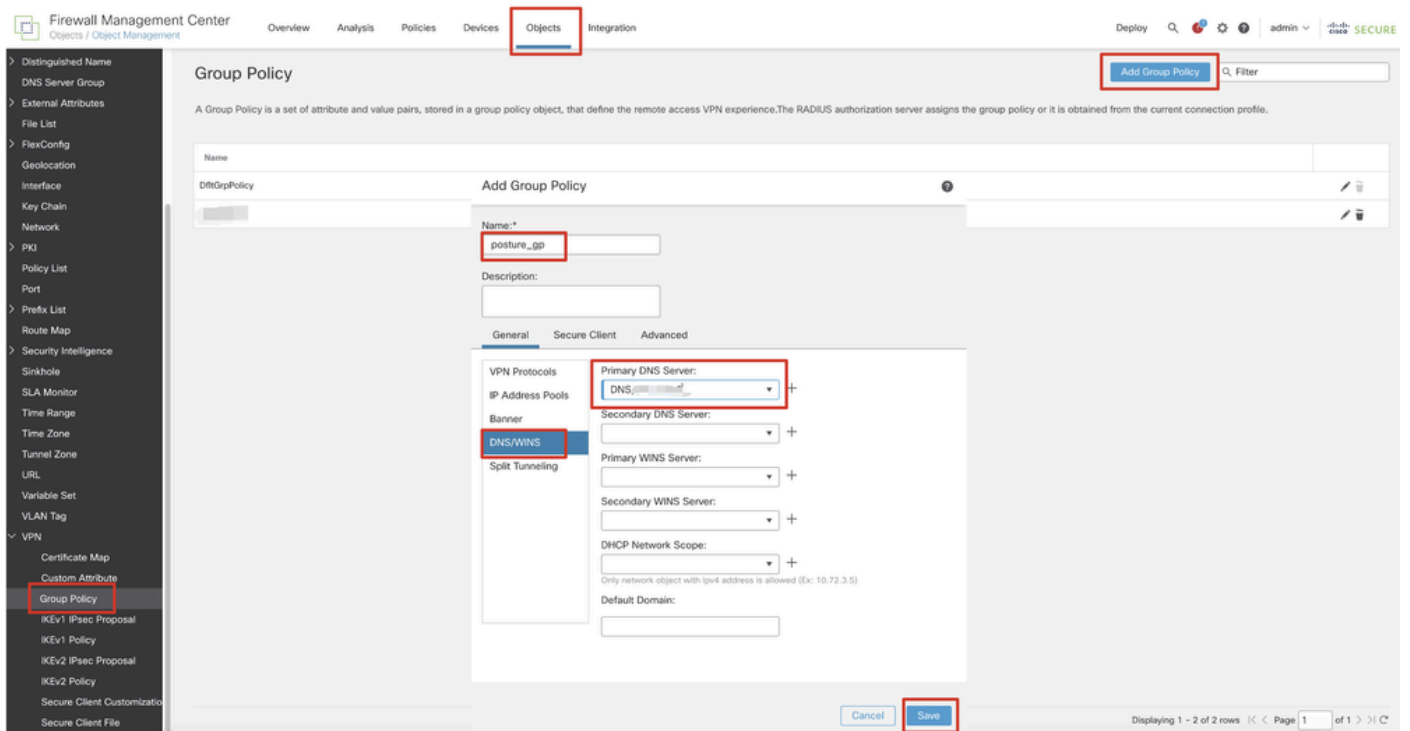
Observação: o servidor DNS configurado aqui deve ser usado para usuários VPN.

Etapa 4.2. Crie um objeto para ISE PSN. Clique em Add Object, forneça o nome e o endereço IP PSN do ISE disponível. Clique em Save.



FMC_Add_Object_ISE

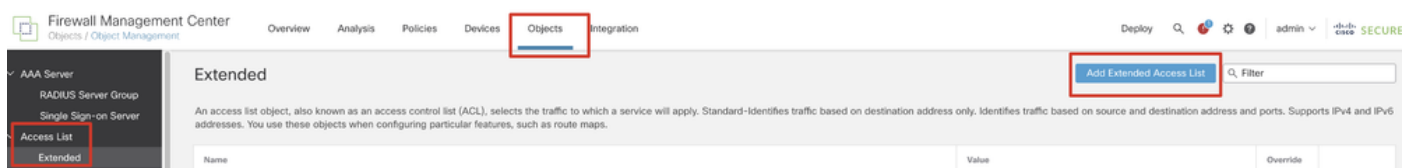
Etapa 5. Navegue até Objects > Object Management > VPN > Group Policy. Clique em Add Group Policy. Clique em DNS/WINS e selecione o objeto do servidor DNS no Primary DNS Server. Em seguida, clique em Save.



FMC_Add_Group_Policy

Observação: verifique se o servidor DNS usado na política de grupo VPN pode resolver o FQDN e o enroll.cisco.com do portal de provisionamento do cliente ISE.

Etapa 6. Navegue até Objects > Object Management > Access List > Extended. Clique em Add Extended Access List.



The screenshot shows the Firewall Management Center (FMC) interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', and 'Integration'. The 'Objects' menu item is highlighted with a red box. The main content area is titled 'Extended' and contains a description: 'An access list object, also known as an access control list (ACL), selects the traffic to which a service will apply. Standard-Identifies traffic based on destination address only. Identifies traffic based on source and destination address and ports. Supports IPv4 and IPv6 addresses. You use these objects when configuring particular features, such as route maps.' Below this description is a table with columns for 'Name', 'Value', and 'Override'. In the top right corner, there is a button labeled 'Add Extended Access List' and a search filter box. The left sidebar shows a tree view with 'AAA Server', 'RADIUS Server Group', 'Single Sign-on Server', 'Access List', and 'Extended' (highlighted).

FMC_Add_Redirect_ACL

Etapa 6.1. Forneça o nome da ACL de redirecionamento. Esse nome deve ser o mesmo do perfil de autorização do ISE. Clique em Add.

New Extended Access List Object

Name
redirect

Entries (0)

Add

Sequence	Action	Source	Source Port	Destination	Destination Port	Application	Users	SGT
No records to display								

Allow Overrides

Cancel Save

FMC_Add_Redirect_ACL_Part_1

Etapa 6.2. Bloqueie o tráfego DNS, o tráfego para o endereço IP PSN do ISE e os servidores de remediação para excluí-los do redirecionamento. Permita o restante do tráfego. Isso aciona o redirecionamento. Clique em Save.

Add Extended Access List Entry

Action:
Block

Logging:
Default

Log Level:
Informational

Log Interval:
300 Sec.

Network Port Application Users Security Group Tag

Available Networks

Search by name or value

- IPv4-Private-192.168.0.0-16
- IPv4-Private-All-RFC1918
- IPv6-IPv4-Mapped
- IPv6-Link-Local
- IPv6-Private-Unique-Local-Addresses
- IPv6-to-IPv4-Relay-Anycast
- ISE_PSN_...
- rtp_ise

Add to Source
Add to Destination

Source Networks (0)
any

Destination Networks (1)
ISE_PSN_...

Enter an IP address Add

Enter an IP address Add

Cancel Add

FMC_Add_Redirect_ACL_Part_2

Name
redirect

Entries (4)

Add

Sequence	Action	Source	Source Port	Destination	Destination Port	Application	Users	SGT	
1	Block	any-ipv4	Any	ISE_PSN_...	Any	Any	Any	Any	
2	Block	Any	Any	Any	DNS_over_TCP DNS_over_UDP	Any	Any	Any	
3	Block	Any	Any	FTP_...	Any	Any	Any	Any	
4	Allow	any-ipv4	Any	any-ipv4	Any	Any	Any	Any	

Allow Overrides

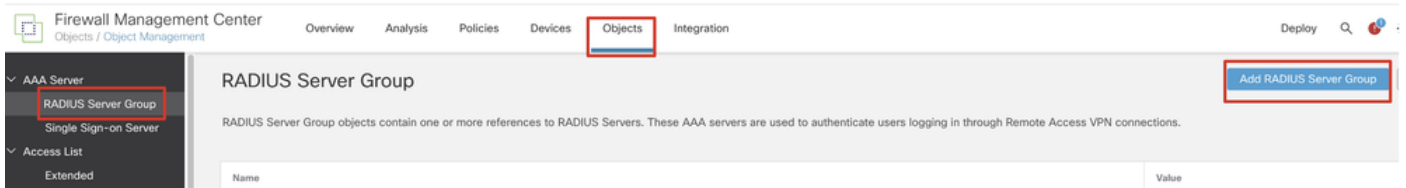
Cancel

Save

FMC_Add_Redirect_ACL_Part_3

Observação: o FTP de destino neste exemplo de ACL de redirecionamento é usado como o exemplo de servidor de correção.

Passo 7. Navegue até Objects > Object Management > RADIUS Server Group. Clique em Add RADIUS Server Group.



FMC_Add_New_Radius_Server_Group

Etapa 7.1. Forneça o nome, cheque Enable authorize only, cheque Enable interim account update, cheque Enable dynamic authorization.

Add RADIUS Server Group



Name:*

rtpise

Description:

Group Accounting Mode:

Single



Retry Interval:* (1-10) Seconds

10

Realms:

Enable authorize only

Enable interim account update

Interval:* (1-120) hours

24

Enable dynamic authorization

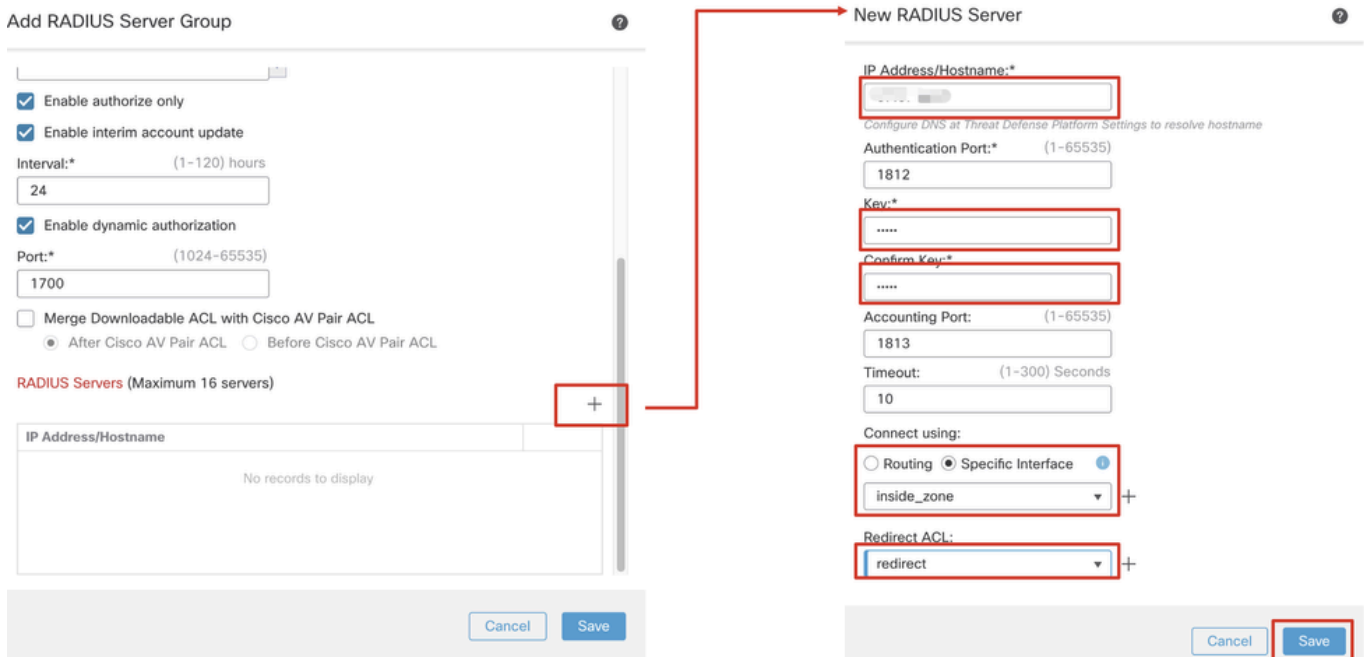
Port:* (1024-65535)

Cancel

Save

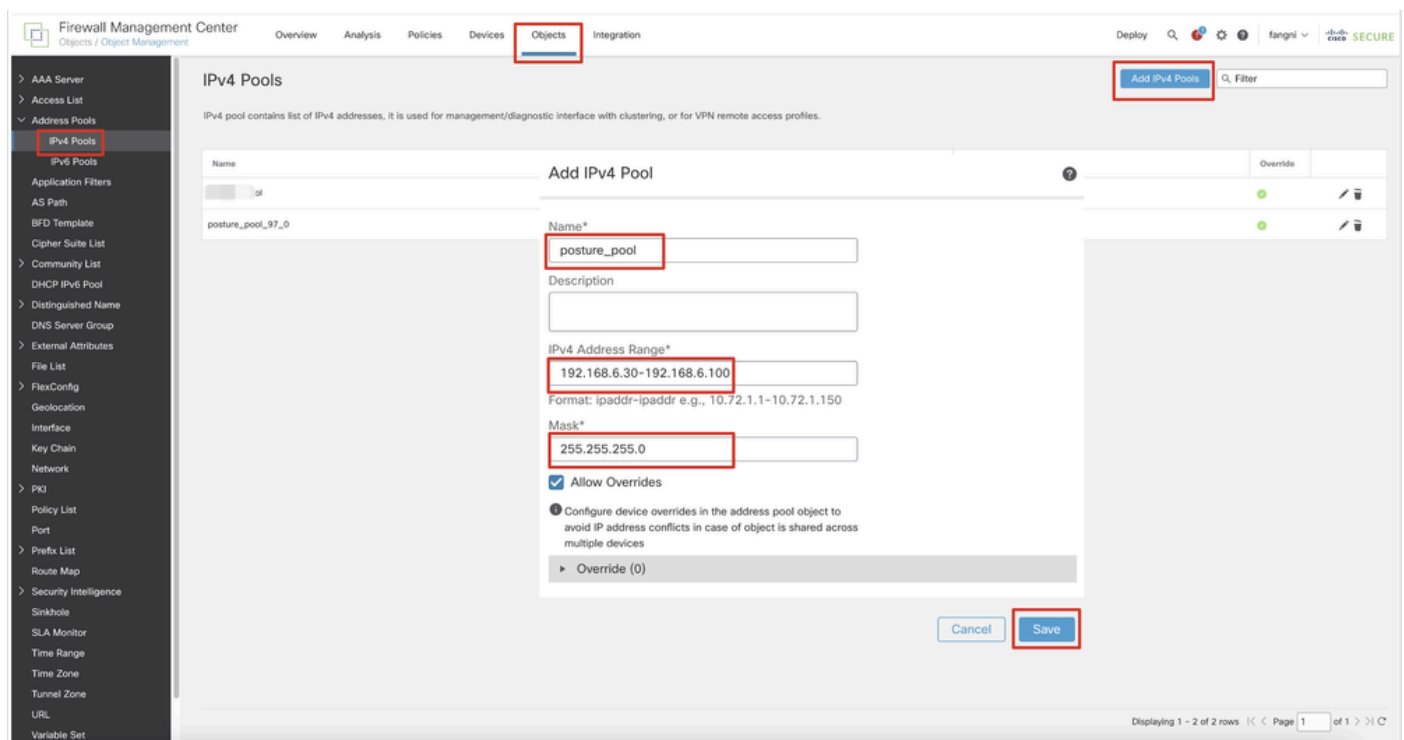
FMC_Add_New_Radius_Server_Group_Part_1

Etapa 7.2. Clique no Plus ícone para adicionar um novo servidor radius. Forneça o PSNIP Address/Hostname, Key do ISE. Selecione o específico interface para conexão. Selecione o Redirect ACL. Em seguida, clique Save para salvar o novo servidor radius. Em seguida, clique Save novamente para salvar o novo grupo de servidores radius.



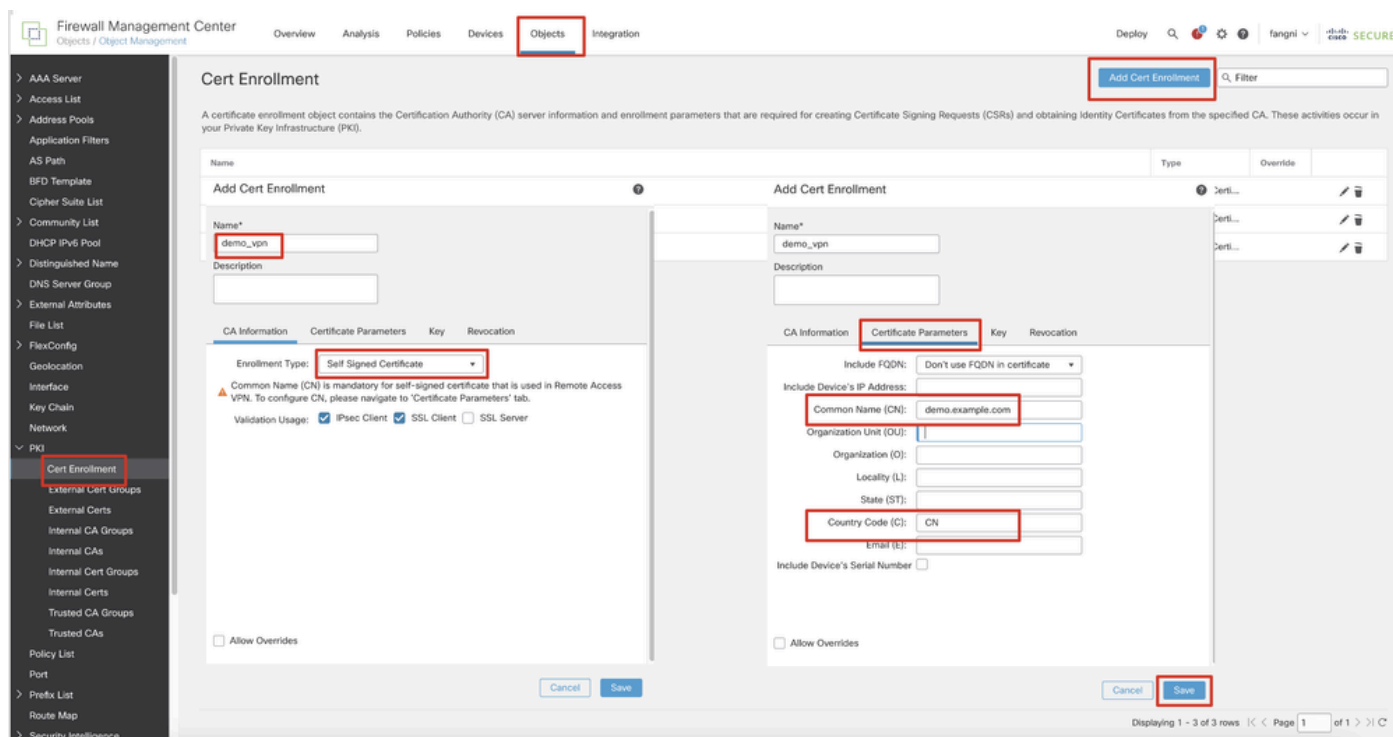
FMC_Add_New_Radius_Server_Group_Part_2

Etapa 8. Navegue até Objects > Object Management > Address Pools > IPv4 Pools. Clique em Add IPv4 Pools e forneça o Name, IPv4 Address Range Mask. Em seguida, clique em Save.



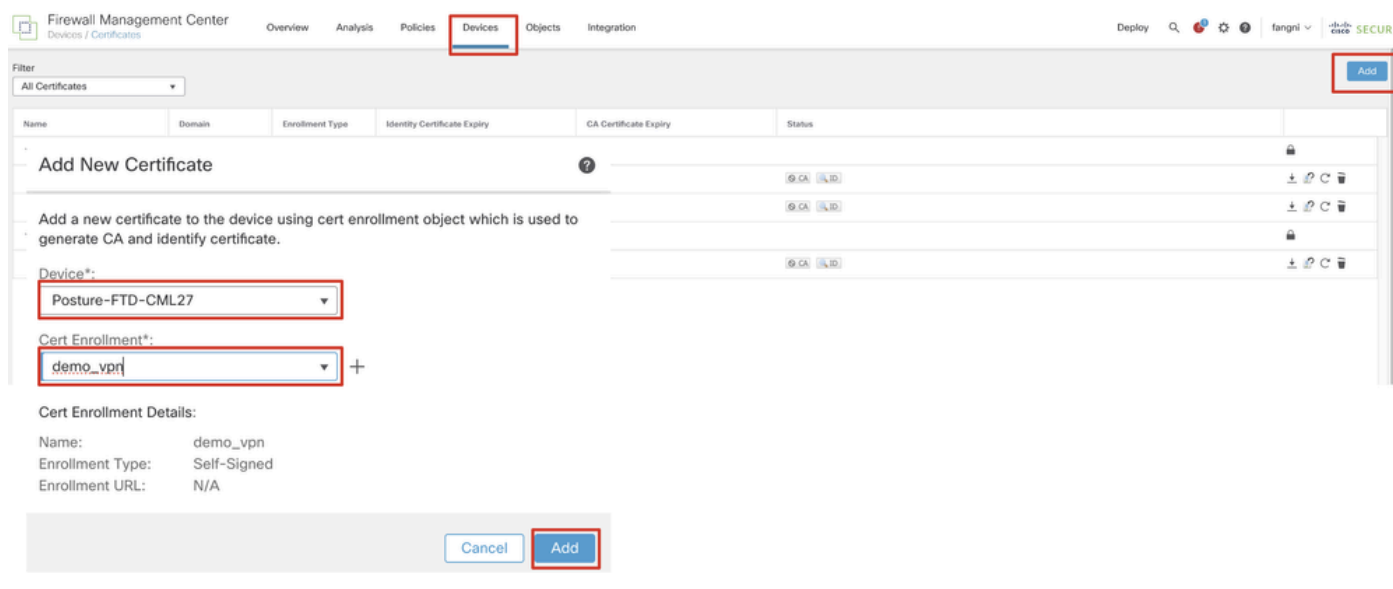
FMC_Add_New_Pool

Etapa 9. Navegue até Certificate Objects > Object Management > PKI > Cert Enrollment. Clique em Add Cert Enrollment, forneça um nome e selecione Self Signed Certificate em Enrollment Type. Clique na guia Certificate Parameters e forneça Common Name e Country Code. Em seguida, clique em Save.



FMC_Add_New_Cert_Enroll

Etapa 10. Navegue até Devices > Certificates. Clique em Add, selecione o nome do FTD em Device, selecione inscrição configurada anteriormente em Cert Enrollment. Clique em Add.



FMC_Add_New_Cert_To_FTD

Etapa 11. Navegue até Devices > VPN > Remote Access. Clique em Add.

Etapa 11.1. Forneça o nome e adicione o FTD ao Selected Devices. Clique em Next.

Firewall Management Center
Devices / VPN / Setup Wizard

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 ⚙️ 👤 admin 🔒 **SECURE**

Remote Access VPN Policy Wizard

1 Policy Assignment — 2 Connection Profile — 3 Secure Client — 4 Access & Certificate — 5 Summary

Targeted Devices and Protocols

This wizard will guide you through the required minimal steps to configure the Remote Access VPN policy with a new user-defined connection profile.

Name: posture_vpn

Description:

VPN Protocols:

- SSL
- IPsec-IKEv2

Targeted Devices:

Available Devices

Search

Posture-FTD-CML27

VPN-FTD-Posture-CML

Add

Selected Devices

Posture-FTD-CML27

Before You Start

Before you start, ensure the following configuration elements to be in place to complete Remote Access VPN Policy.

Authentication Server

Configure LOCAL or Realm or RADIUS Server Group or SSO to authenticate VPN clients.

Secure Client Package

Make sure you have Secure Client package for VPN Client downloaded or you have the relevant Cisco credentials to download it during the wizard.

Device Interface

Interfaces should be already configured on targeted devices so that they can be used as a security zone or interface group to enable VPN access.

Cancel Back **Next**

FMC_New_RAVPN_Wizard_1

Etapa 11.2. Selecione o grupo de servidores radius configurado anteriormente no Authentication Server, Authorization Server, Accounting Server. Role a página para baixo.

Firewall Management Center
Devices / VPN / Setup Wizard

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 ⚙️ 👤 admin 🔒 **SECURE**

Remote Access VPN Policy Wizard

1 Policy Assignment — 2 **Connection Profile** — 3 Secure Client — 4 Access & Certificate — 5 Summary

Remote User — Secure Client — Internet — Outside — VPN Device — Inside — Corporate Resources

AAA

Connection Profile:

Connection Profiles specify the tunnel group policies for a VPN connection. These policies pertain to creating the tunnel itself, how AAA is accomplished and how addresses are assigned. They also include user attributes, which are defined in group policies.

Connection Profile Name: posture_vpn

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: AAA Only

Authentication Server: rtplse

Authorization Server: rtplse

Accounting Server: rtplse

Client Address Assignment:

Client IP address can be assigned from AAA server, FQDN server and IP address pool. When multiple servers are...

Cancel Back **Next**

FMC_New_RAVPN_Wizard_2

Etapa 11.3. Selecione o nome do pool configurado anteriormente em IPv4 Address Pools. Selecione a política de grupo configurada anteriormente em Group Policy. Clique em Next.

Firewall Management Center
Devices / VPN / Setup Wizard

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 ⚙️ 👤 admin 🔒 **SECURE**

Remote Access VPN Policy Wizard

1 Policy Assignment — 2 Connection Profile — 3 Secure Client — 4 Access & Certificate — 5 Summary

(Realm or RADIUS)

Accounting Server: +
(RADIUS)

Client Address Assignment:

Client IP address can be assigned from AAA server, DHCP server and IP address pools. When multiple options are selected, IP address assignment is tried in the order of AAA server, DHCP server and IP address pool.

Use AAA Server (Realm or RADIUS only) ●
 Use DHCP Servers
 Use IP Address Pools

IPv4 Address Pools: ↗
 IPv6 Address Pools: ↗

Group Policy:

A group policy is a collection of user-oriented session attributes which are assigned to client when a VPN connection is established. Select or create a Group Policy object.

Group Policy*: +
 Edit Group Policy

Cancel Back **Next**

FMC_New_RAVPN_Wizard_3

Etapa 11.4. Marque a caixa de seleção da imagem do Linux. Clique em Next.

Firewall Management Center
Devices / VPN / Setup Wizard

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 ⚙️ 👤 admin 🔒 **SECURE**

Remote Access VPN Policy Wizard

1 Policy Assignment — 2 Connection Profile — 3 Secure Client — 4 Access & Certificate — 5 Summary

Secure Client Image

The VPN gateway can automatically download the latest Secure Client package to the client device when the VPN connection is initiated. Minimize connection setup time by choosing the appropriate OS for the selected package.

Download Secure Client packages from [Cisco Software Download Center](#).

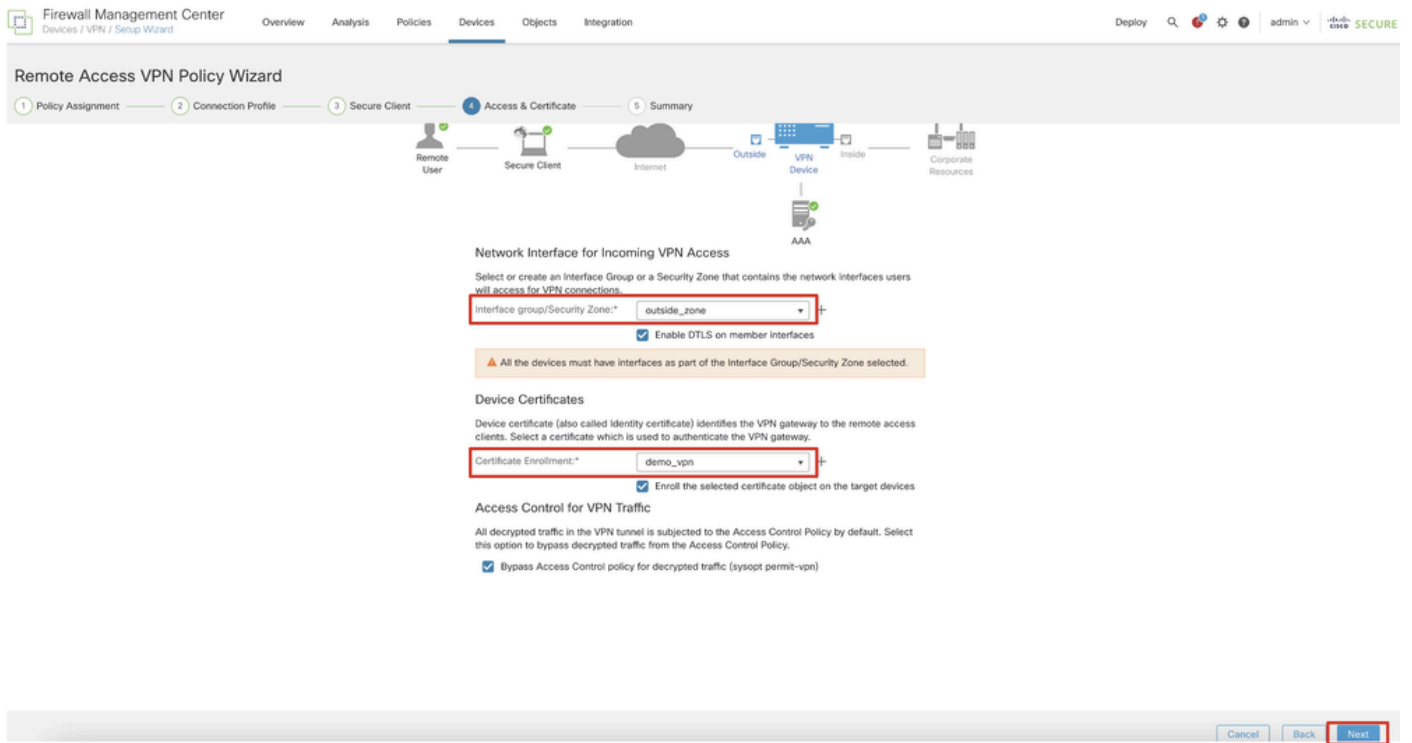
Secure Client File Object Name	Secure Client Package Name	Operating System
<input type="checkbox"/> client_image	cisco-secure-client-wln-5.1.3.62-webdepl...	Windows
<input checked="" type="checkbox"/> linux_5_1_3_62	cisco-secure-client-linux64-5.1.3.62-webd...	Linux

Show Re-order buttons +

Cancel Back **Next**

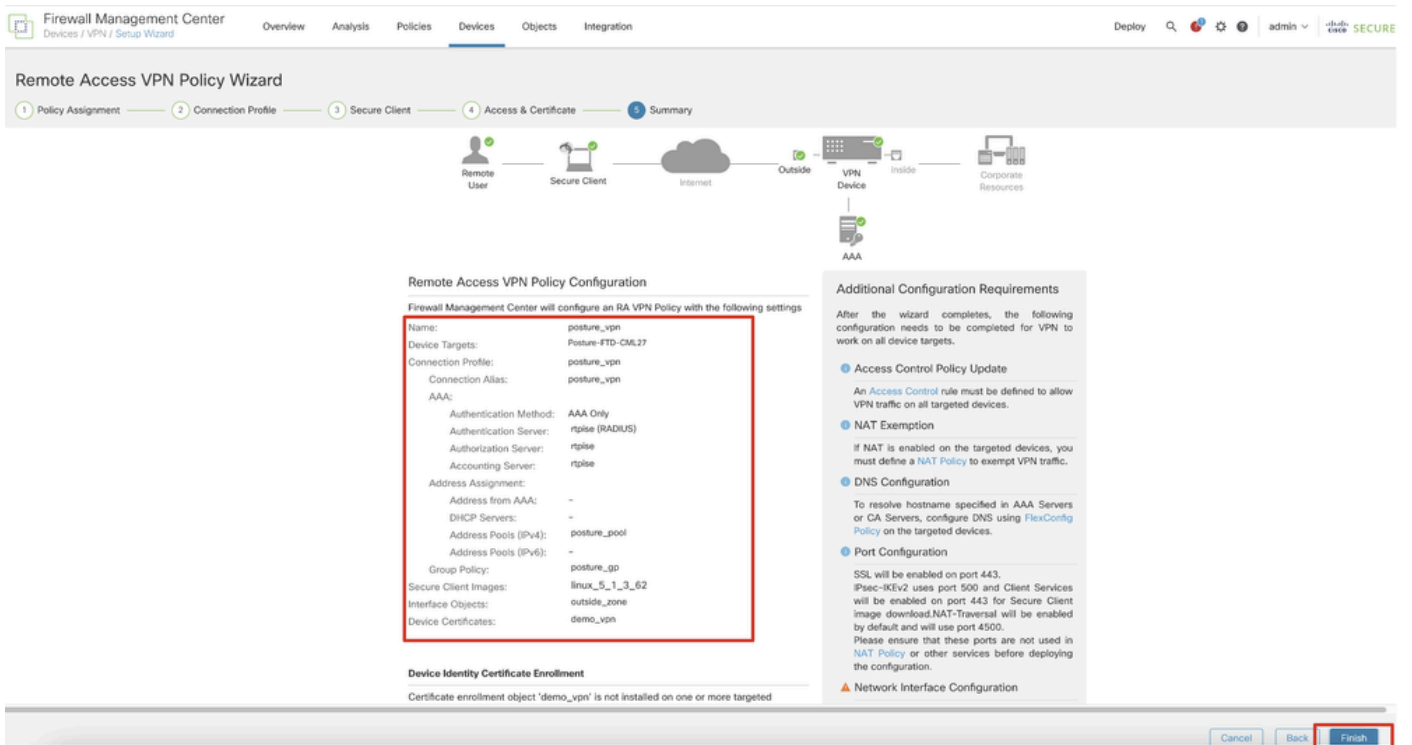
FMC_New_RAVPN_Wizard_4

Etapa 11.5. Selecione a interface da interface VPN. Selecione a inscrição de certificado inscrita no FTD na etapa 9. Clique em Next.



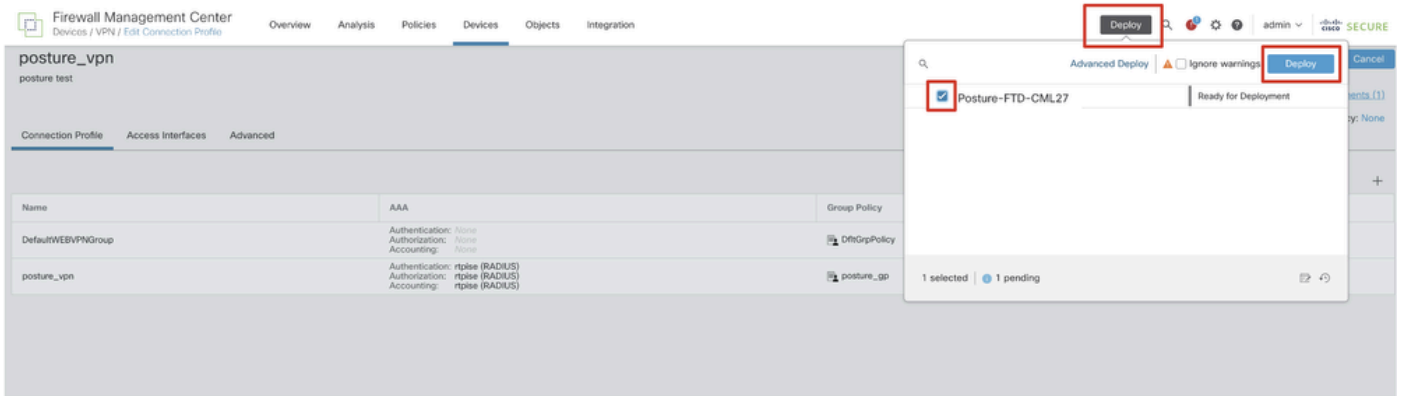
FMC_New_RAVPN_Wizard_5

Etapa 11.6. Confirme duas vezes as informações relacionadas na página de resumo. Se tudo estiver bem, clique em Finish. Se algo precisar ser modificado, clique em Back.



FMC_New_RAVPN_Wizard_6

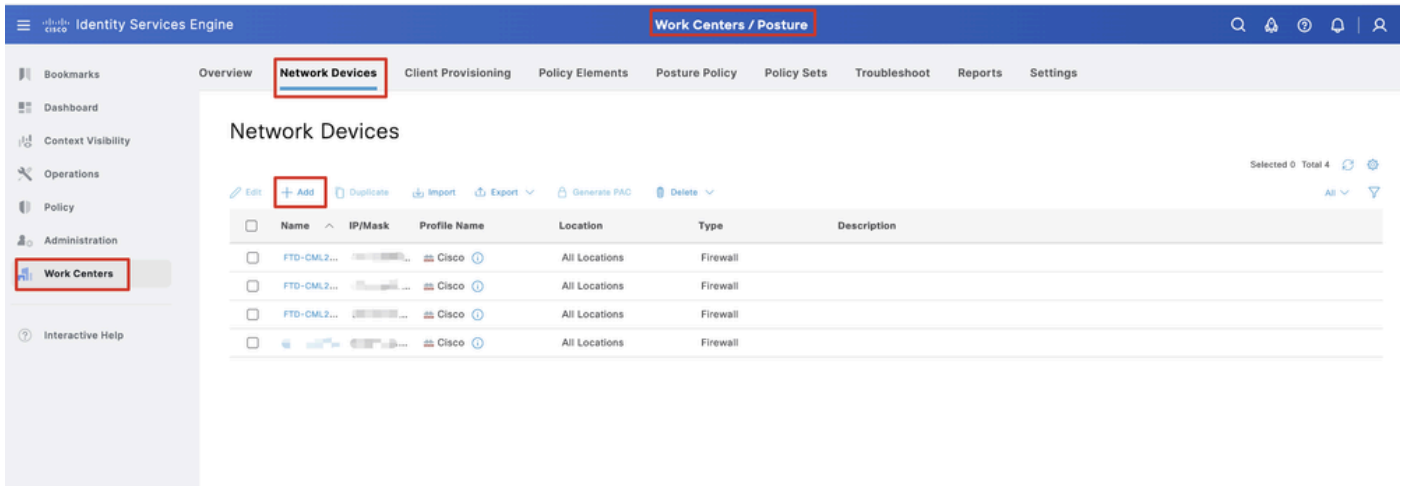
Etapa 12. Implante a nova configuração no FTD para concluir a configuração da VPN de acesso remoto.



FMC_Deploy_FTD

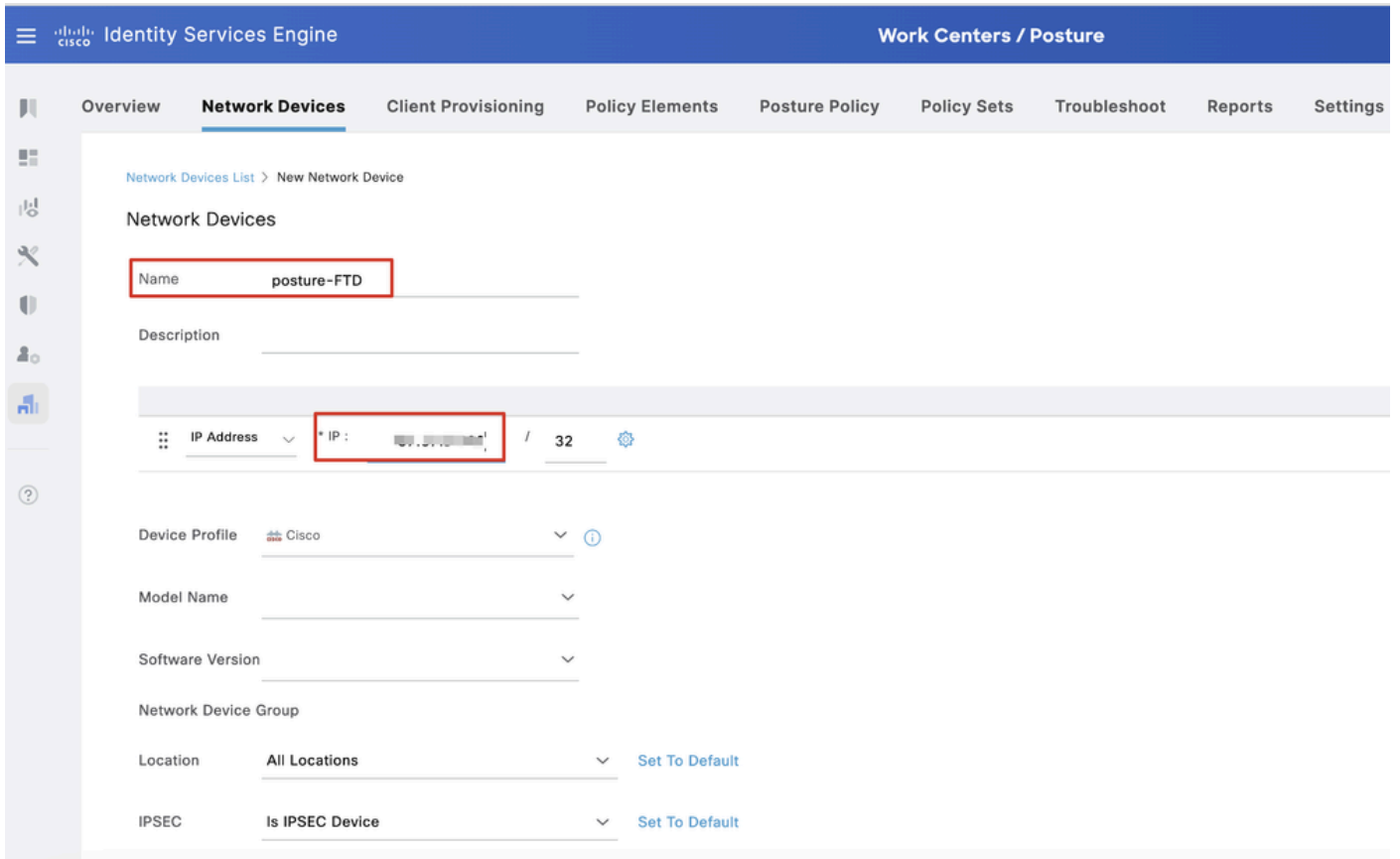
Configurações no ISE

Etapa 13. Navegue até Work Centers > Posture > Network Devices. Clique em Add.



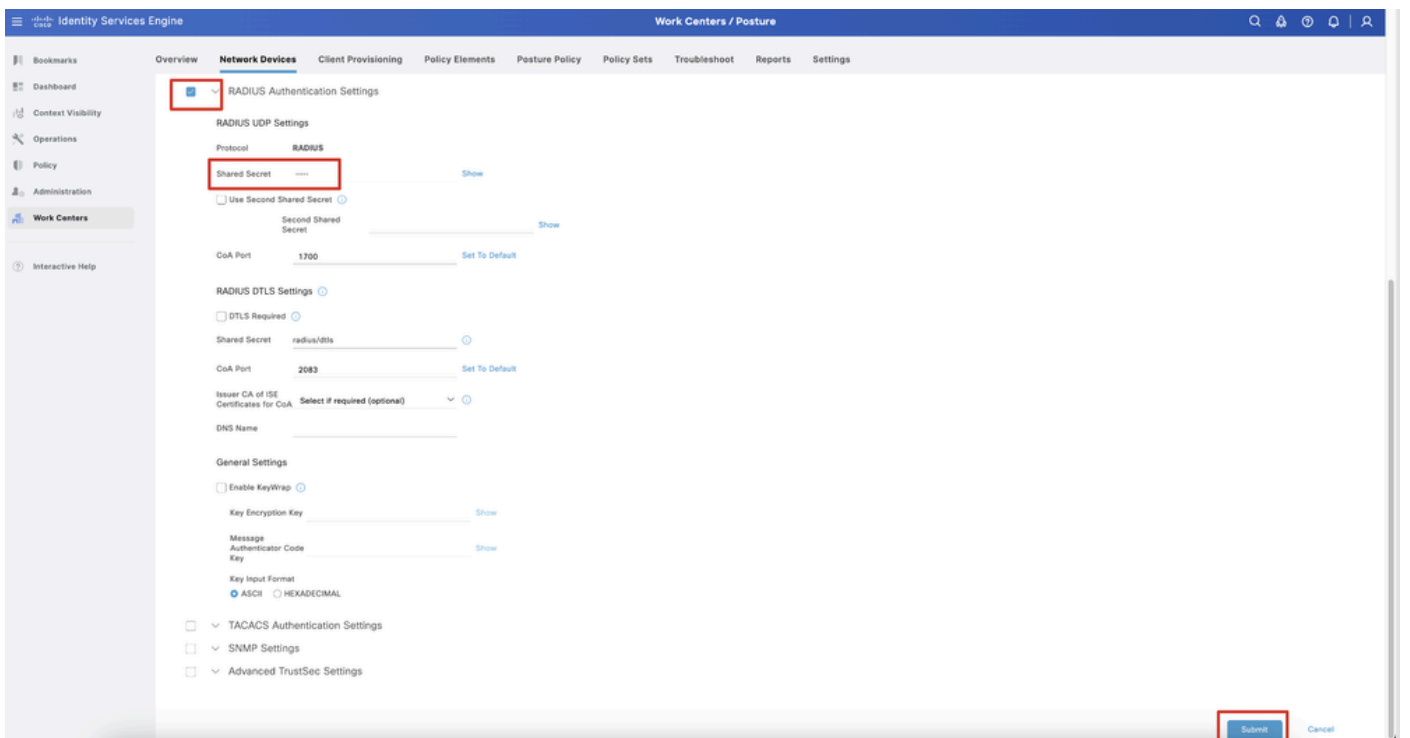
ISE_Add_New_Devices

Etapa 13.1. Forneça o Name, IP Adresse role a página para baixo.



ISE_Add_New_Devices_1

Etapa 13.2. Marque a caixa de seleção de RADIUS Authentication Settings. Forneça o Shared Secret. Clique em Submit.

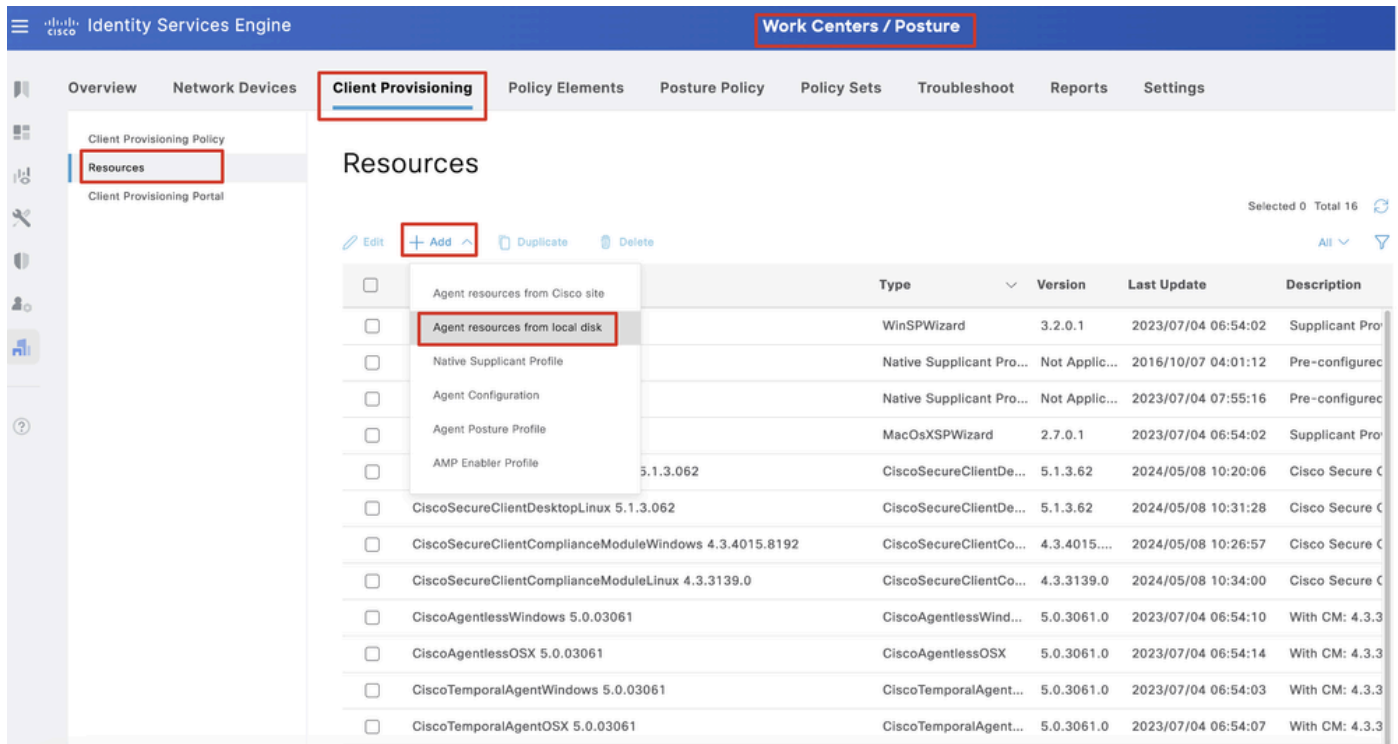


ISE_Add_New_Devices_2

Etapa 14. Baixe o nomecisco-secure-client-linux64-4.3.139.0-isecompliance-webdeploy-k9.pkg do pacote em [Download do software Cisco](#) e verifique se o arquivo está bom confirmando se a soma de verificação md5 do arquivo baixado é a mesma que a página de Download do

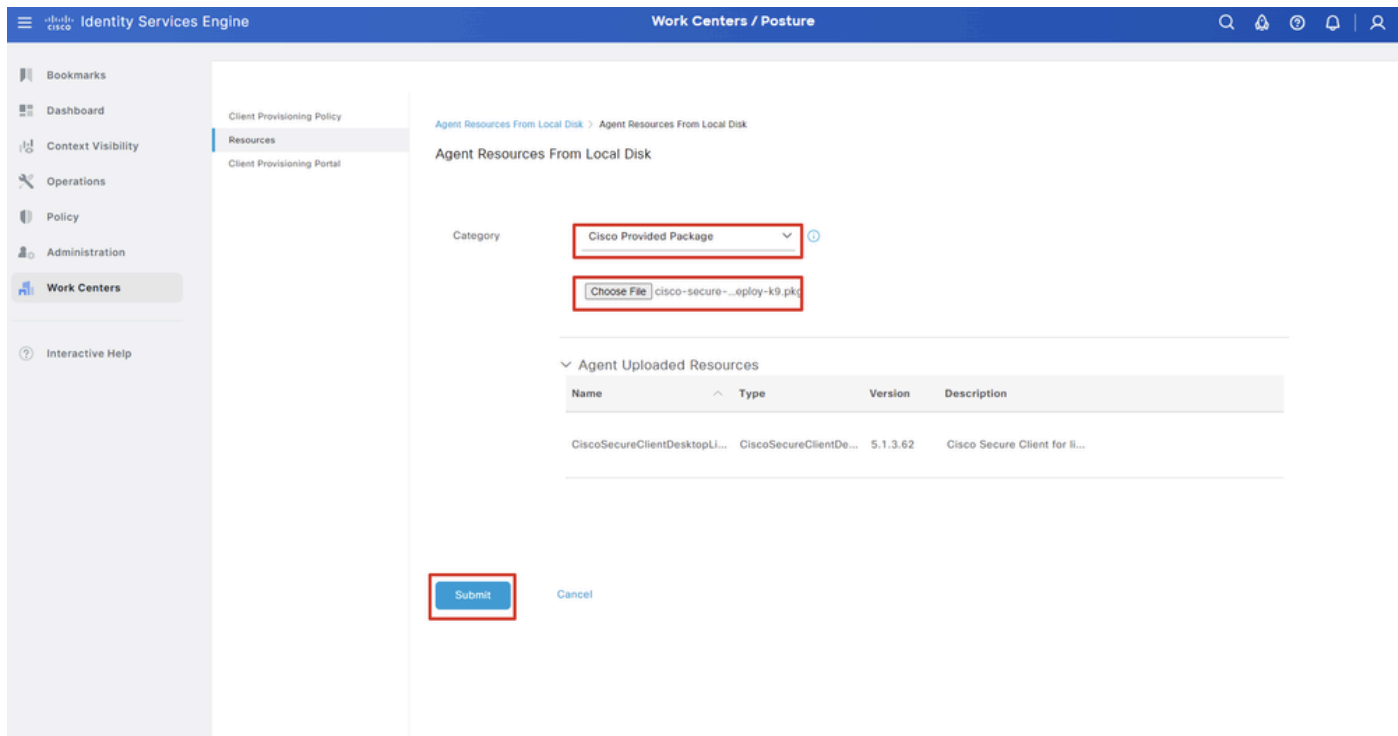
software Cisco. O download do nomecisco-secure-client-linux64-5.1.3.62-webdeploy-k9.pkg do pacote foi concluído com êxito na Etapa 1.

Etapa 15. Navegue até Work Centers > Posture > Client Provisioning > Resources. Clique em Add. Selecione Agent resources from local disk.

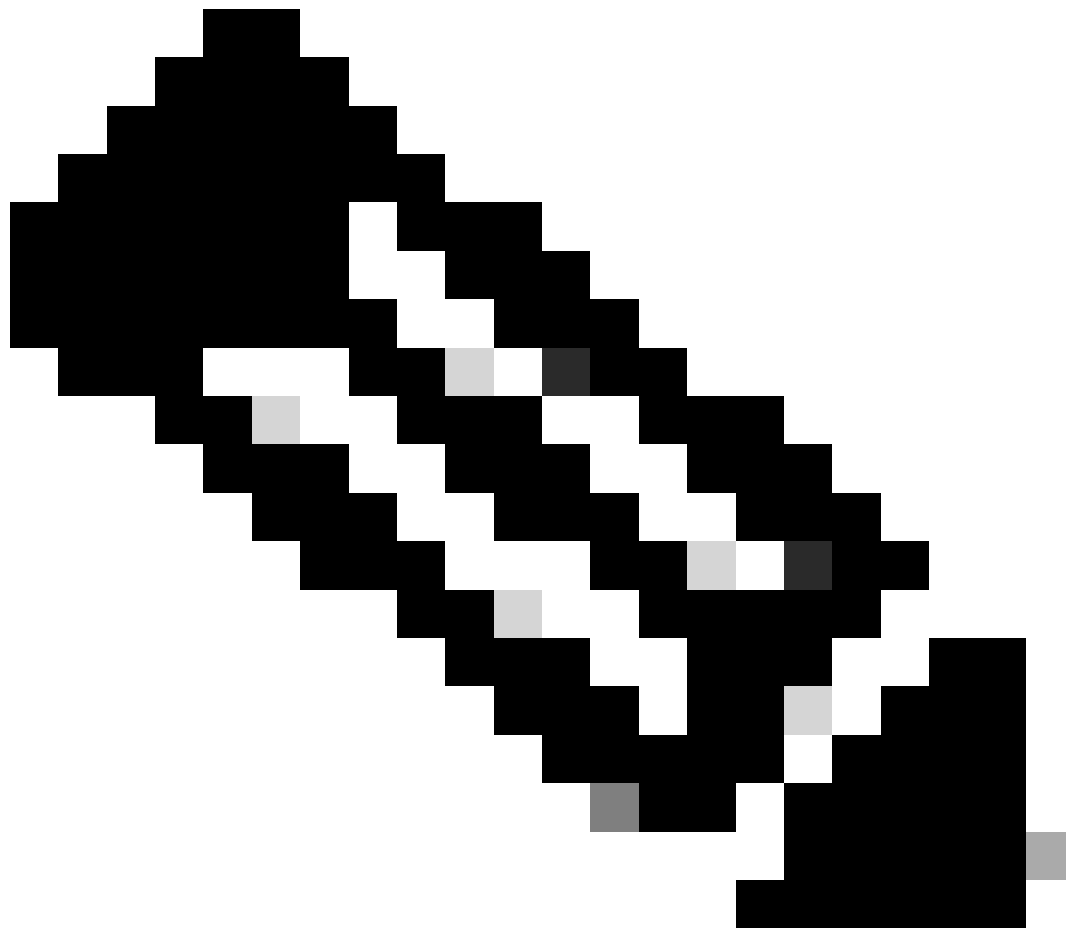


ISE_Upload_Resource

Etapa 15.1. Selecione Cisco Provided Package. Clique Choose File para carregar cisco-secure-client-linux64-5.1.3.62-webdeploy-k9.pkg. Clique em Submit.

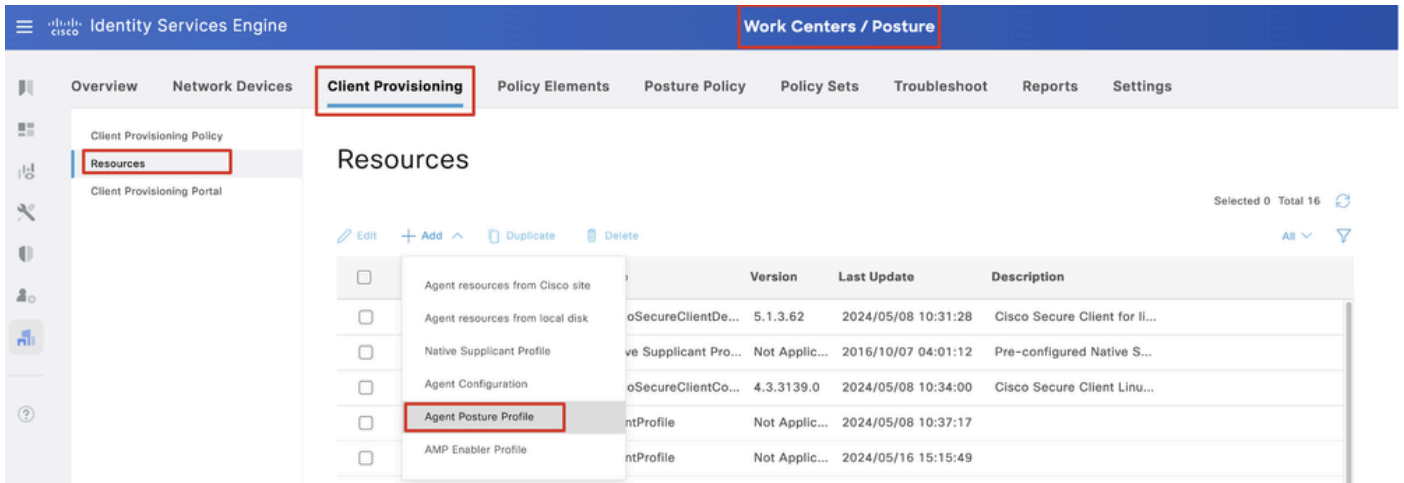


ISE_Upload_Resources_1



Observação: repita a Etapa 14. para carregar cisco-secure-client-linux64-4.3.3139.0-isecompliance-webdeploy-k9.pkg .

Etapa 16. Navegue até Work Centers > Posture > Client Provisioning > Resources. Clique em Add. Selecione Agent Posture Profile.

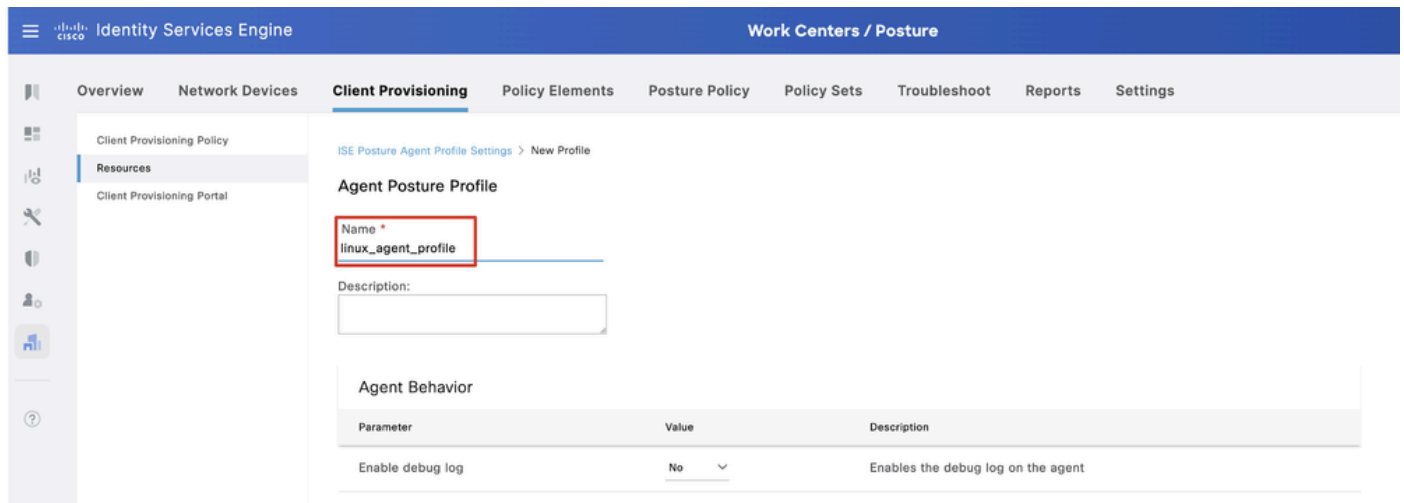


ISE_Add_Agent_Posture_Profile

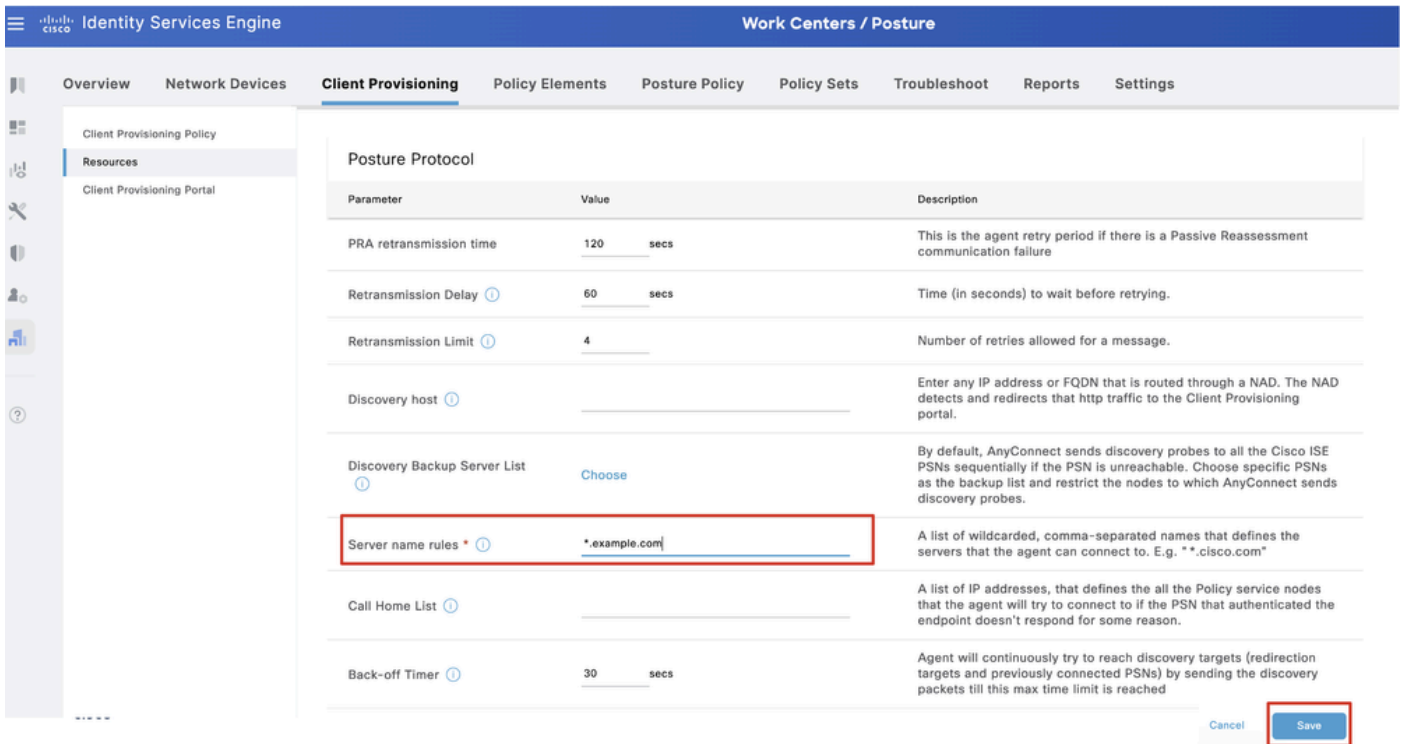
Etapa 16.1. Forneça o Nome, Server name rules e mantenha o restante como padrão. Clique em Save.

Nome: linux_agent_profile

Regras de nome de servidor: *.example.com

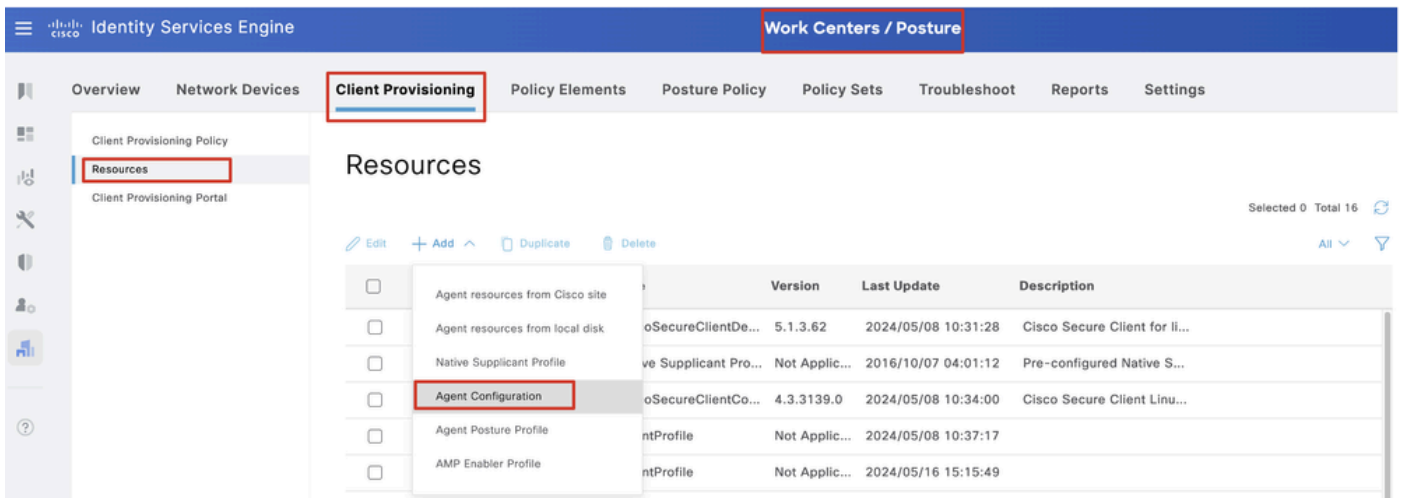


ISE_Add_Agent_Posture_Profile_1



ISE_Add_Agent_Posture_Profile_2

Etapa 17. Navegue até Work Centers > Posture > Client Provisioning > Resources. Clique em Add. Selecione Agent Configuration.



ISE_Add_Agent_Configuration

Etapa 17.2. Configure os detalhes:

Selecione Pacote de agentes: CiscoSecureClientDesktopLinux 5.1.3.062

Nome: linux_agent_config

Módulo de conformidade: CiscoSecureClientComplianceModuleLinux 4.3.3139.0

Marque a caixa de seleção de VPN, Diagnostic and Reporting Tool

Postura ISE de seleção de perfil: linux_agent_profile

Clique em Submit.

Identity Services Engine Work Centers / Posture

Overview Network Devices **Client Provisioning** Policy Elements Posture Policy Policy Sets Troubleshoot Reports Settings

Client Provisioning Policy

Resources

Client Provisioning Portal

* Select Agent Package: CiscoSecureClientDesktopLinux 5.1.3.062

* Configuration Name: linux_agent_config

Description:

Description Value Notes

* Compliance Module: CiscoSecureClientComplianceModuleLinux 4.3

Cisco Secure Client Module Selection

ISE Posture

VPN

Secure Firewall Posture

Network Visibility

Diagnostic and Reporting Tool

Profile Selection

* ISE Posture: linux_agent_profile

Submit Cancel

ISE_Add_Agent_Configuration_1

Etapa 18. Navegue até Work Centers > Posture > Client Provisioning > Client Provisioning Policy. Clique Edit no final de qualquer nome de regra. Selecione Insert new policy below.

Identity Services Engine Work Centers / Posture

Overview Network Devices **Client Provisioning** Policy Elements Posture Policy Policy Sets Troubleshoot Reports Settings

Client Provisioning Policy

Resources

Client Provisioning Portal

Define the Client Provisioning Policy to determine what users will receive upon login and user session initiation:
For Agent Configuration: version of agent, agent profile, agent compliance module, and/or agent customization package.
For Native Supplicant Configuration: wizard profile and/or wizard. Drag and drop rules to change the order.

Windows Agent, Mac Agent, Mac Temporal and Mac Agentless policies support ARM64. Windows policies run separate packages for ARM4 and Intel architectures. Mac policies run the same package for both architectures.
For Windows Agent ARM64 policies, configure Session: OS-Architecture EQUALS arm64 in the Other Conditions column.
Mac ARM64 policies require no Other Conditions arm64 configurations.
If you configure an ARM64 client provisioning policy for an OS, ensure that the ARM64 policy is at the top of the conditions list, ahead of policies without an ARM64 condition. This is because an endpoint is matched sequentially with the policies listed in this window.

Rule Name	Identity Groups	Operating Systems	Other Conditions	Results
IOS	If Any	and Apple iOS All	and Condition(s)	then Cisco-ISE-NSP
Android	If Any	and Android	and Condition(s)	then Cisco-ISE-NSP

Duplicate above

Duplicate below

Insert new policy above

Insert new policy below

Delete

ISE_Add_New_Provisioning_Policy

Etapa 18.1. Configure os detalhes:

Nome da regra: Linux

Sistemas Operacionais: Linux All

Resultados: linux_agent_config

Clique em Done e Save.

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes 'Identity Services Engine' and 'Work Centers / Posture'. The main navigation menu has 'Client Provisioning' selected. The left sidebar shows 'Client Provisioning Policy' and 'Resources'. The main content area is titled 'Client Provisioning Policy' and contains a table of rules. The 'Linux' rule is highlighted with a red box.

Rule Name	Identity Groups	Operating Systems	Other Conditions	Results
IOS	If Any	and Apple IOS All	and Condition(s)	then Cisco-ISE-NSP
Android	If Any	and Android	and Condition(s)	then Cisco-ISE-NSP
Linux	If Any	and Linux All	and Condition(s)	then linux_agent_config

ISE_Add_New_Provisioning_Policy_1

Etapa 19. Navegue até Work Centers > Posture > Policy Elements > Conditions > File. Clique em Add.

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes 'Identity Services Engine' and 'Work Centers / Posture'. The main navigation menu has 'Policy Elements' selected. The left sidebar shows 'Conditions' and 'File' selected. The main content area is titled 'File Conditions' and contains a table of file conditions. The 'Add' button is highlighted with a red box.

Name	Description	File name	Condition Type
pc_XP64_KB2797052_MS13...	Cisco Predefined Check...	SYSTEM_PROGRAMS\C...	Cisco-Defined
pc_W8_64_KB3124275_MS...	Cisco Predefined Check...	SYSTEM_ROOT\sysnativ...	Cisco-Defined
pc_Vista_KB2893294_MS13...	Cisco Predefined Check...	SYSTEM_32\imagehlp.dll	Cisco-Defined
pc_W81_64_KB3033889_M...	Cisco Predefined Check...	SYSTEM_ROOT\sysnativ...	Cisco-Defined
pc_Vista64_KB925902_MS0...	Cisco Predefined Check...	SYSTEM_ROOT\winsxs\l...	Cisco-Defined
pc_W10_64_1709_KB45803...	Cisco Predefined Check...	SYSTEM_ROOT\sysnativ...	Cisco-Defined
pc_XP_KB2653956_MS12-0...	Cisco Predefined Check...	SYSTEM_32\Wintrust.dll	Cisco-Defined
pc_W8_KB2892074_MS13-...	Cisco Predefined Check...	SYSTEM_32\Scrrun.dll	Cisco-Defined
pc_W10_64_1909_KB50139...	Cisco Predefined Check...	SYSTEM_ROOT\SysWO...	Cisco-Defined
pc_W7_KB2681578_MS12-...	Cisco Predefined Check...	SYSTEM_32\Win32k.sys	Cisco-Defined
pc_W10_KB3081436_MS15...	Cisco Predefined Check...	SYSTEM_32\Edgehtml.dll	Cisco-Defined
pc_W81_64_KB3042553_M...	Cisco Predefined Check...	SYSTEM_ROOT\sysnativ...	Cisco-Defined
pc_W8_64_KB2727526_MS...	Cisco Predefined Check...	SYSTEM_ROOT\sysnativ...	Cisco-Defined
pc_W8_64_KB2992611_MS...	Cisco Predefined Check...	SYSTEM_ROOT\sysnativ...	Cisco-Defined
pc_W7_KB3078601_MS15-...	Cisco Predefined Check...	SYSTEM_32\Win32k.sys	Cisco-Defined

ISE_Add_New_File_Condition

Etapa 19.1. Configure os detalhes:

Nome: linux_demo_file_exist

Sistemas Operacionais: Linux All

Tipo de arquivo: FileExistence

Caminho do arquivo: home, Desktop/test.txt

Operador de Arquivo: Existe

Clique em Submit.

The screenshot shows the Cisco Identity Services Engine (ISE) interface for configuring a new File Condition. The interface is divided into a left-hand navigation menu and a main configuration area. The navigation menu includes categories such as Conditions, File, and Remediations. The main configuration area is titled "File Condition" and contains several fields: "Name *" with the value "linux_demo_file_exist", "Description", "* Operating System" with the value "Linux All", "Compliance Module" with the value "Any version", "* File Type" with the value "FileExistence", "* File Path" with the value "home" and a text input field containing "Desktop/test.txt", and "* File Operator" with the value "Exists". A "Submit" button and a "Cancel" link are located at the bottom right of the form.

ISE_Add_New_File_Condition_1

Etapa 20. Navegue até Work Centers > Posture > Policy Elements > Requirements. Clique Edit no final de qualquer nome de regra. Selecione Insert new Requirement.

Identity Services Engine Work Centers / Posture

Overview Network Devices Client Provisioning **Policy Elements** Posture Policy Policy Sets Troubleshoot Reports Settings

Bookmarks Dashboard Context Visibility Operations Policy Administration **Work Centers** Interactive Help

Conditions

- Anti-Malware
- Anti-Spyware
- Anti-Virus
- Application
- Compound
- Dictionary Compound
- Dictionary Simple
- Disk Encryption
- External DataSource
- File
- Firewall
- Hardware Attributes
- Patch Management
- Registry
- Script
- Service
- USB

Remediations

- Allowed Protocols
- Authorization Profiles
- Downloadable ACLs
- Requirements**

Requirements

Name	Operating System	Compliance Module	Posture Type	Conditions	Remediations Actions	
Any_AV_Installation_Win	for Windows All	using 3.x or earlier	using Agent	met if ANY_av_win_inst then	Message Text Only	Edit
Any_AV_Definition_Win	for Windows All	using 3.x or earlier	using Agent	met if ANY_av_win_def then	AnyAVDefRemediationWin	Edit Duplicate
Any_AS_Installation_Win	for Windows All	using 3.x or earlier	using Agent	met if ANY_as_win_inst then	Message Text Only	Edit Insert new Requirement
Any_AS_Definition_Win	for Windows All	using 3.x or earlier	using Agent	met if ANY_as_win_def then	AnyASDefRemediationWin	Edit Delete
Any_AV_Installation_Mac	for Mac OSX	using 3.x or earlier	using Agent	met if ANY_av_mac_inst then	Message Text Only	Edit
Any_AV_Definition_Mac	for Mac OSX	using 3.x or earlier	using Agent	met if ANY_av_mac_def then	AnyAVDefRemediationMac	Edit
Any_AS_Installation_Mac	for Mac OSX	using 3.x or earlier	using Agent	met if ANY_as_mac_inst then	Message Text Only	Edit
Any_AS_Definition_Mac	for Mac OSX	using 3.x or earlier	using Agent	met if ANY_as_mac_def then	AnyASDefRemediationMac	Edit
Any_AM_Installation_Win	for Windows All	using 4.x or later	using Agent	met if ANY_am_win_inst then	Message Text Only	Edit
Any_AM_Definition_Win	for Windows All	using 4.x or later	using Agent	met if ANY_am_win_def then	AnyAMDefRemediationWin	Edit
Any_AM_Installation_Mac	for Mac OSX	using 4.x or later	using Agent	met if ANY_am_mac_inst then	Message Text Only	Edit
Any_AM_Definition_Mac	for Mac OSX	using 4.x or later	using Agent	met if ANY_am_mac_def then	AnyAMDefRemediationMac	Edit
Any_AM_Installation_Lin	for Linux All	using 4.x or later	using Agent	met if ANY_am_lin_inst then	Select Remediations	Edit
Any_AM_Definition_Lin	for Linux All	using 4.x or later	using Agent	met if ANY_am_lin_def then	Select Remediations	Edit
USB_Block	for Windows All	using 4.x or later	using Agent	met if USB_Check then	USB_Block	Edit
Default_AppVia_Requirement_Win	for Windows All	using 4.x or later	using Agent	met if Default_AppVia_Condition_Win then	Select Remediations	Edit
Default_AppVia_Requirement_Mac	for Mac OSX	using 4.x or later	using Agent	met if Default_AppVia_Condition_Mac then	Select Remediations	Edit
Default_Hardware_Attributes_Requirement_Win	for Windows All	using 4.x or later	using Agent	met if Hardware_Attributes_Check then	Select Remediations	Edit
Default_Hardware_Attributes_Requirement_Mac	for Mac OSX	using 4.x or later	using Agent	met if Hardware_Attributes_Check then	Select Remediations	Edit

Note:
Remediation Action is filtered based on the operating system and stealth mode selection.
Remediation Actions are not applicable for Application Conditions (configured using the Provision By Category or Provision By Everything options), Hardware Conditions, and External Data source conditions.
Remediations Actions are not applicable for Agentless Posture type.

ISE_Add_New_Posture_Requirement

Etapa 20.1. Configure os detalhes:

Nome: Test_exist_linux

Sistemas Operacionais: Linux All

Módulo de conformidade: 4.x ou posterior

Tipo de postura: Agente

Condições: linux_demo_file_exist

Clique em Done e Save.

Identity Services Engine Work Centers / Posture

Overview Network Devices Client Provisioning **Policy Elements** Posture Policy Policy Sets Troubleshoot Reports Settings

Conditions

- Anti-Malware
- Anti-Spyware
- Anti-Virus
- Application
- Compound
- Dictionary Compound
- Dictionary Simple
- Disk Encryption
- External DataSource
- File
- Firewall
- Hardware Attributes
- Patch Management
- Registry
- Script
- Service
- USB

Remediations

- Required Protocols
- Allowed Protocols
- Authorization Profiles
- Downloadable ACLs

Guide Me

Requirements

Name	Operating System	Compliance Module	Posture Type	Conditions	Remediations Actions
Test_exist_linux	for Linux All	using 4.x or later	using Agent	met if linux_demo_file_exist	then Select Remediations
Any_AV_Installation_Win	for Windows All	using 3.x or earlier	using Agent	met if ANY_av_win_inst	then Message Text Only
Any_AV_Definition_Win	for Windows All	using 3.x or earlier	using Agent	met if ANY_av_win_def	then AnyAVDefRemediationWin
Any_AS_Installation_Win	for Windows All	using 3.x or earlier	using Agent	met if ANY_as_win_inst	then Message Text Only
Any_AS_Definition_Win	for Windows All	using 3.x or earlier	using Agent	met if ANY_as_win_def	then AnyASDefRemediationWin
Any_AV_Installation_Mac	for Mac OSX	using 3.x or earlier	using Agent	met if ANY_av_mac_inst	then Message Text Only
Any_AV_Definition_Mac	for Mac OSX	using 3.x or earlier	using Agent	met if ANY_av_mac_def	then AnyAVDefRemediationMac
Any_AS_Installation_Mac	for Mac OSX	using 3.x or earlier	using Agent	met if ANY_as_mac_inst	then Message Text Only
Any_AS_Definition_Mac	for Mac OSX	using 3.x or earlier	using Agent	met if ANY_as_mac_def	then AnyASDefRemediationMac
Any_AM_Installation_Win	for Windows All	using 4.x or later	using Agent	met if ANY_am_win_inst	then Message Text Only
Any_AM_Definition_Win	for Windows All	using 4.x or later	using Agent	met if ANY_am_win_def	then AnyAMDefRemediationWin
Any_AM_Installation_Mac	for Mac OSX	using 4.x or later	using Agent	met if ANY_am_mac_inst	then Message Text Only
Any_AM_Definition_Mac	for Mac OSX	using 4.x or later	using Agent	met if ANY_am_mac_def	then AnyAMDefRemediationMac

Note:
Remediation Action is filtered based on the operating system and stealth mode selection.
Remediation Actions are not applicable for Application Conditions (configured using the Provision By Category or Provision By Everything options), Hardware Conditions, and External Data source conditions.
Remediations Actions are not applicable for Agentless Posture type.

Save Reset

ISE_Add_New_Posture_Requirement_1



Observação: até agora, somente scripts de shell são suportados para agentes Linux como correção.

Etapa 21. Navegue até Work Centers > Posture > Policy Elements > Authorization Profiles. Clique em Add.

Etapa 21.1. Configure os detalhes:

Nome: unknown_redirect

Marque a caixa de seleção de Web Redirection(CWA,MDM,NSP,CPP)

Selecionar Client Provisioning(Posture)

ACL: redirecionar

Valor: Portal de provisionamento do cliente (padrão)

The screenshot displays the Cisco Identity Services Engine (ISE) configuration interface. The top navigation bar includes the Cisco logo and the text "Identity Services Engine". On the right side of the top bar, the text "Work Centers / Posture" is highlighted with a red box. Below the top bar, a horizontal menu contains several tabs: "Overview", "Network Devices", "Client Provisioning", "Policy Elements" (highlighted with a red box), "Posture Policy", "Policy Sets", "Troubleshoot", "Reports", and "Settings".

The main content area is divided into two sections. The left section is a sidebar menu with categories: "Conditions" (with a dropdown arrow) and "Remediations" (with a right-pointing arrow). Under "Conditions", there is a list of items: Anti-Malware, Anti-Spyware, Anti-Virus, Application, Compound, Dictionary Compound, Dictionary Simple, Disk Encryption, External DataSource, File, Firewall, Hardware Attributes, Patch Management, Registry, Script, Service, and USB. Under "Remediations", there is a list: Requirements, Allowed Protocols, and "Authorization Profiles" (highlighted with a red box). Below "Authorization Profiles" is the text "Downloadable ACLs".

The right section is titled "Authorization Profile". It contains the following fields and options:

- * Name: unknown_redirect (highlighted with a red box)
- Description: (empty text area)
- * Access Type: ACCESS_ACCEPT (dropdown menu)
- Network Device Profile: Cisco (dropdown menu)
- Service Template:
- Track Movement: ⓘ
- Agentless Posture: ⓘ
- Passive Identity Tracking: ⓘ

Below these fields is a section titled "Common Tasks" with a dropdown arrow. It contains the following tasks:

- Voice Domain Permission
- Web Redirection (CWA, MDM, NSP, CPP) ⓘ (highlighted with a red box)
- Static IP/Host name/FQDN
- Suppress Profiler CoA for endpoints in Logical Profile

At the bottom of the "Common Tasks" section, there is a configuration row:

Client Provisioning (Posture) ↓ ACL redirect (highlighted with a red box) Value Client Provisioning Portal (defi ↓

ISE_Add_New_Authorization_Profile_Redirect_1



Observação: esse redirecionamento de nome de ACL deve corresponder ao nome de ACL correspondente configurado no FTD.

Etapa 21.2. Repita o Add para criar outros dois perfis de autorização para endpoints não compatíveis e compatíveis com os detalhes.

Nome: non_compliance_profile

Nome DACL: DENY_ALL_IPv4_TRAFFIC

Nome: compliance_profile

Nome DACL: PERMIT_ALL_IPv4_TRAFFIC



Observação: a DACL para endpoints compatíveis ou não compatíveis precisa ser configurada de acordo com os requisitos reais.

Etapa 22. Navegue até Work Centers > Posture > Posture Policy. Clique Edit no final de qualquer regra. Selecione Insert new policy.

ISE Add New Posture Policy

Status	Policy Options	Rule Name	Identity Groups	Operating Systems	Compliance Module	Posture Type	Other Conditions	Requirements	
<input type="checkbox"/>	Policy Options	Default_AntiMalware_Policy_Mac	If Any	and Mac OSX	and 4.x or later	and Agent	and	then Any_AM_Installation_Mac	Edit - Duplicate
<input type="checkbox"/>	Policy Options	Default_AntiMalware_Policy_Mac_temporal	If Any	and Mac OSX	and 4.x or later	and Temporal Agent	and	then Any_AM_Installation_Mac_temporal	Edit - Insert new policy
<input type="checkbox"/>	Policy Options	Default_AntiMalware_Policy_Win	If Any	and Windows All	and 4.x or later	and Agent	and	then Any_AM_Installation_Win	Edit - Duplicate
<input type="checkbox"/>	Policy Options	Default_AntiMalware_Policy_Win_temporal	If Any	and Windows All	and 4.x or later	and Temporal Agent	and	then Any_AM_Installation_Win_temporal	Edit - Duplicate
<input type="checkbox"/>	Policy Options	Default_AppVn_Policy_Mac	If Any	and Mac OSX	and 4.x or later	and Agent	and	then Default_AppVn_Requirement_Mac	Edit - Duplicate
<input type="checkbox"/>	Policy Options	Default_AppVn_Policy_Mac_temporal	If Any	and Mac OSX	and 4.x or later	and Temporal Agent	and	then Default_AppVn_Requirement_Mac_temporal	Edit - Duplicate
<input type="checkbox"/>	Policy Options	Default_AppVn_Policy_Win	If Any	and Windows All	and 4.x or later	and Agent	and	then Default_AppVn_Requirement_Win	Edit - Duplicate
<input type="checkbox"/>	Policy Options	Default_AppVn_Policy_Win_temporal	If Any	and Windows All	and 4.x or later	and Temporal Agent	and	then Default_AppVn_Requirement_Win_temporal	Edit - Duplicate
<input type="checkbox"/>	Policy Options	Default_Firewall_Policy_Mac	If Any	and Mac OSX	and 4.x or later	and Agent	and	then Default_Firewall_Requirement_Mac	Edit - Duplicate
<input type="checkbox"/>	Policy Options	Default_Firewall_Policy_Mac_temporal	If Any	and Mac OSX	and 4.x or later	and Temporal Agent	and	then Default_Firewall_Requirement_Mac_temporal	Edit - Duplicate
<input type="checkbox"/>	Policy Options	Default_Firewall_Policy_Win	If Any	and Windows All	and 4.x or later	and Agent	and	then Default_Firewall_Requirement_Win	Edit - Duplicate
<input type="checkbox"/>	Policy Options	Default_Firewall_Policy_Win_temporal	If Any	and Windows All	and 4.x or later	and Temporal Agent	and	then Default_Firewall_Requirement_Win_temporal	Edit - Duplicate
<input type="checkbox"/>	Policy Options	Default_Hardware_Attributes_Policy_Mac	If Any	and Mac OSX	and 4.x or later	and Agent	and	then Default_Hardware_Attributes_Requirement_Mac	Edit - Duplicate
<input type="checkbox"/>	Policy Options	Default_Hardware_Attributes_Policy_Mac_temporal	If Any	and Mac OSX	and 4.x or later	and Temporal Agent	and	then Default_Hardware_Attributes_Requirement_Mac_temporal	Edit - Duplicate
<input type="checkbox"/>	Policy Options	Default_Hardware_Attributes_Policy_Win	If Any	and Windows All	and 4.x or later	and Agent	and	then Default_Hardware_Attributes_Requirement_Win	Edit - Duplicate

ISE Add New Posture Policy

Etapa 22.1. Configure os detalhes:

Nome da regra: Demo_test_exist_linux

Grupos de Identidade: Qualquer

Sistemas Operacionais: Linux All

Módulo de conformidade: 4.x ou posterior

Tipo de postura: Agente

Requisitos: Test_exist_linux

Clique em Done e Save.

Identity Services Engine Work Centers / Posture

Posture Policy [Guide Me](#)

Define the Posture Policy by configuring rules based on operating system and/or other conditions.

Policy Options	Default_Firewall_Policy_Mac	If Any	and Mac OSX	and 4.x or later	and Agent	and	then Default_Firewall_Requirement_Mac	Edit
<input type="checkbox"/>	Default_Firewall_Policy_Mac_temporal	If Any	and Mac OSX	and 4.x or later	and Temporal Agent	and	then Default_Firewall_Requirement_Mac_temporal	Edit
<input type="checkbox"/>	Default_Firewall_Policy_Win	If Any	and Windows All	and 4.x or later	and Agent	and	then Default_Firewall_Requirement_Win	Edit
<input type="checkbox"/>	Default_Firewall_Policy_Win_temporal	If Any	and Windows All	and 4.x or later	and Temporal Agent	and	then Default_Firewall_Requirement_Win_temporal	Edit
<input type="checkbox"/>	Default_Hardware_Attributes_Policy_Mac	If Any	and Mac OSX	and 4.x or later	and Agent	and	then Default_Hardware_Attributes_Requirement_Mac	Edit
<input type="checkbox"/>	Default_Hardware_Attributes_Policy_Mac_temporal	If Any	and Mac OSX	and 4.x or later	and Temporal Agent	and	then Default_Hardware_Attributes_Requirement_Mac_temporal	Edit
<input type="checkbox"/>	Default_Hardware_Attributes_Policy_Win	If Any	and Windows All	and 4.x or later	and Agent	and	then Default_Hardware_Attributes_Requirement_Win	Edit
<input type="checkbox"/>	Default_Hardware_Attributes_Policy_Win_temporal	If Any	and Windows All	and 4.x or later	and Temporal Agent	and	then Default_Hardware_Attributes_Requirement_Win_temporal	Edit
<input type="checkbox"/>	Default_USB_Block_Policy_Win	If Any	and Windows All	and 4.x or later	and Agent	and	then USB_Block	Edit
<input type="checkbox"/>	Default_USB_Block_Policy_Win_temporal	If Any	and Windows All	and 4.x or later	and Temporal Agent	and	then USB_Block_temporal	Edit
<input checked="" type="checkbox"/>	Demo_test_exist_linux	If Any	and Linux All	and 4.x or later	and Agent	and	then Test_exist_linux	Edit

ISE_Add_New_Posture_Policy_1

Etapa 23. Navegue até Work Centers > Posture > Policy Sets. Clique para Insert new row above.

Identity Services Engine Work Centers / Posture

Overview Network Devices Client Provisioning Policy Elements Posture Policy **Policy Sets** Troubleshoot Reports Settings

Policy Sets

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
●	Default	Default policy set		Default Network Access			

[Insert new row above](#)

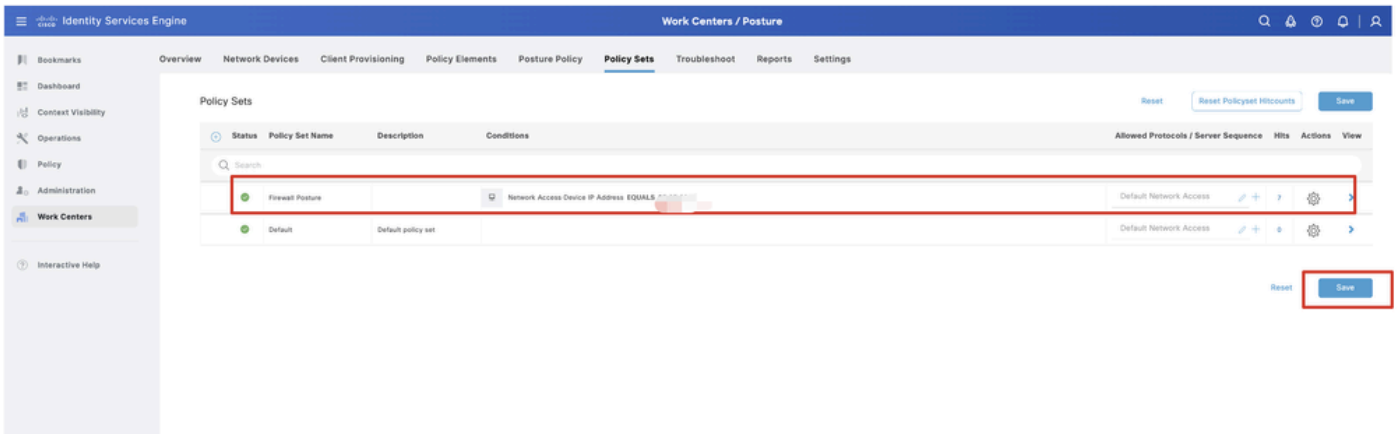
ISE_Add_New_Policy_Set

Etapa 23.1. Configure os detalhes:

Nome do Conjunto de Políticas: Postura de Firewall

Condições: Endereço IP do dispositivo de acesso à rede IGUALs [Endereço IP FTD]

Clique Save .



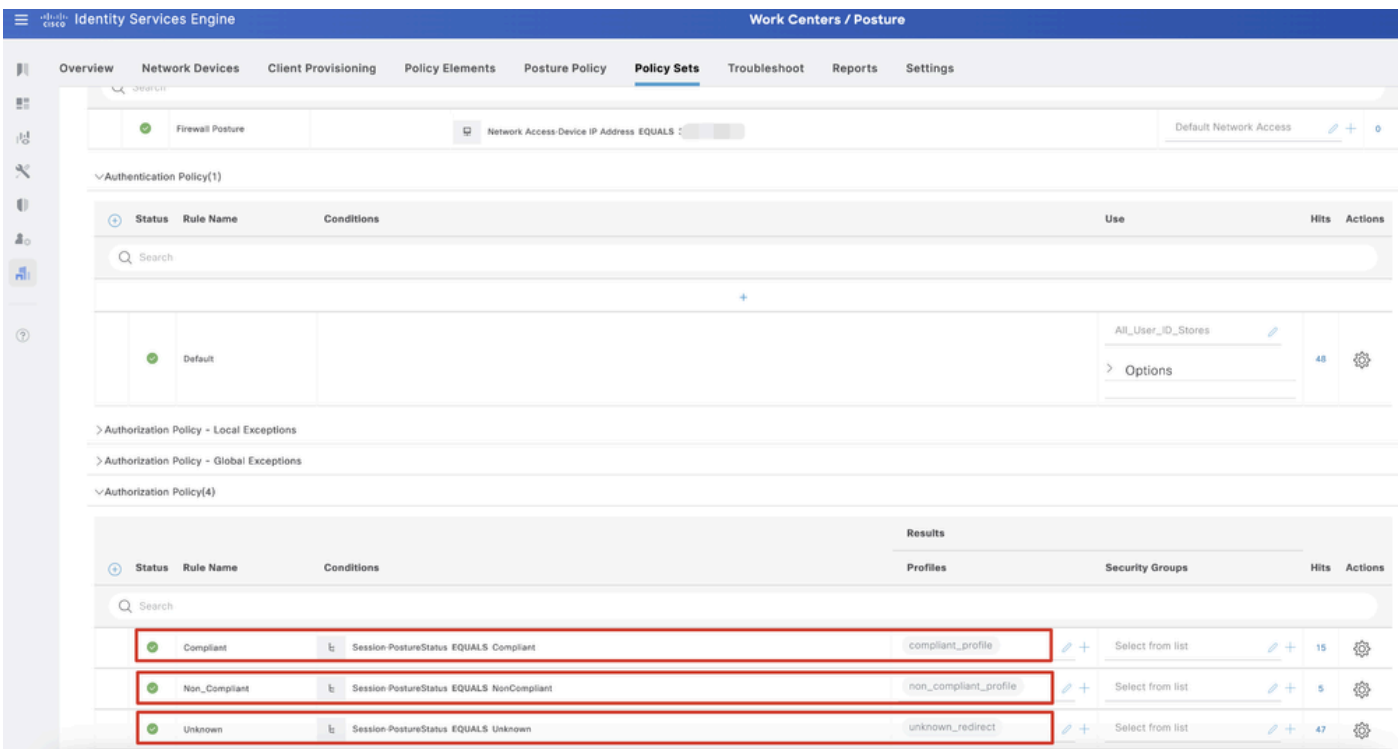
ISE_Add_New_Policy_Set_1

Etapa 23.2. Clique > para inserir o conjunto de políticas. Crie novas regras de autorização para status compatível, não compatível e desconhecido de postura. Clique em Save.

Compatível com compliance_profile

Não Compatível com non_compliance_profile

Desconhecido com unknown_redirect



ISE_Add_New_Policy_Set_2

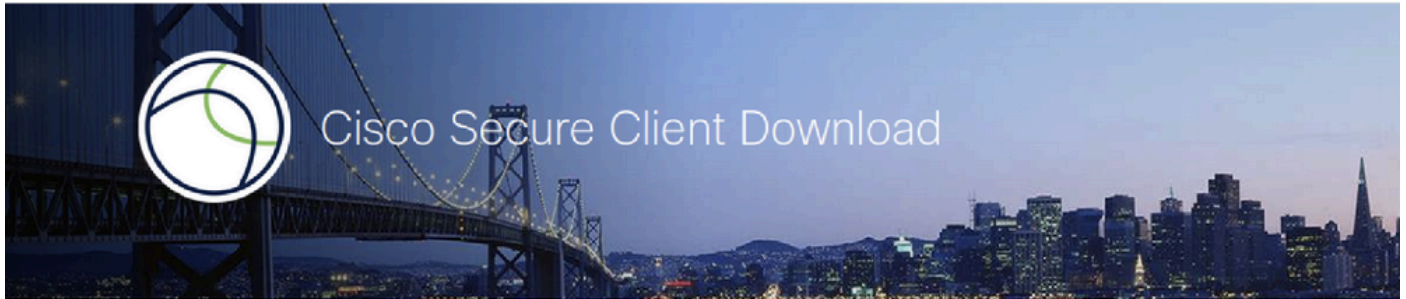
Configurações no Ubuntu

Etapa 24. Faça login no cliente Ubuntu via GUI. Abra o navegador para fazer login no portal VPN. Neste exemplo, é demo.example.com.

A screenshot of a "Logon" dialog box. The dialog has a title bar with a key icon and the text "Logon". Inside the dialog, there are three input fields: "Group" with a dropdown menu showing "posture_vpn", "Username" with a text input field, and "Password" with a text input field. Below the input fields is a button labeled "Logon".

Ubuntu_Browser_VPN_Login

Etapa 25. Clique em Download for Linux.



Download & Install

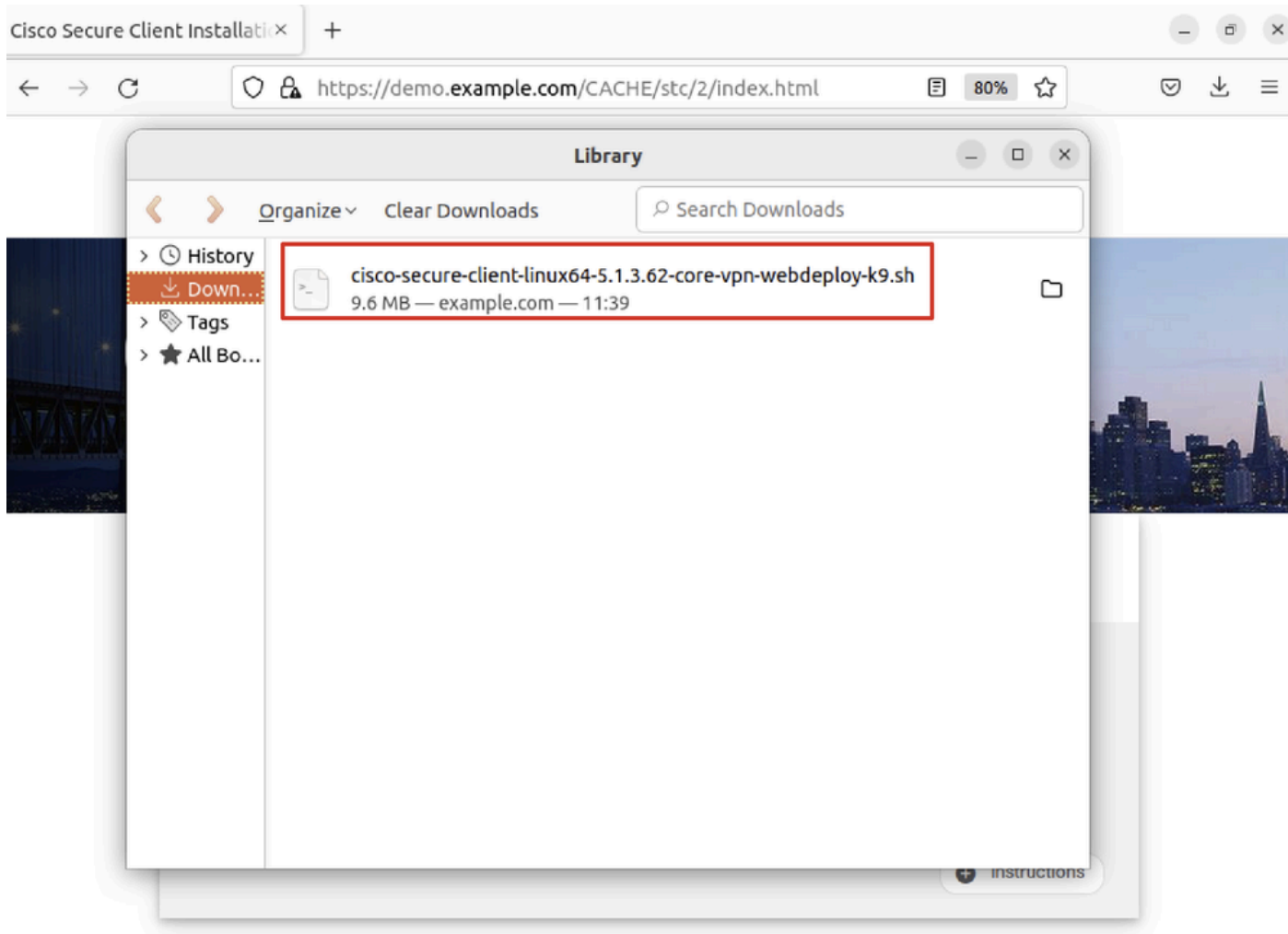
Download Cisco Secure Client and install it on your computer.

[Download for Linux](#)

[+ Instructions](#)

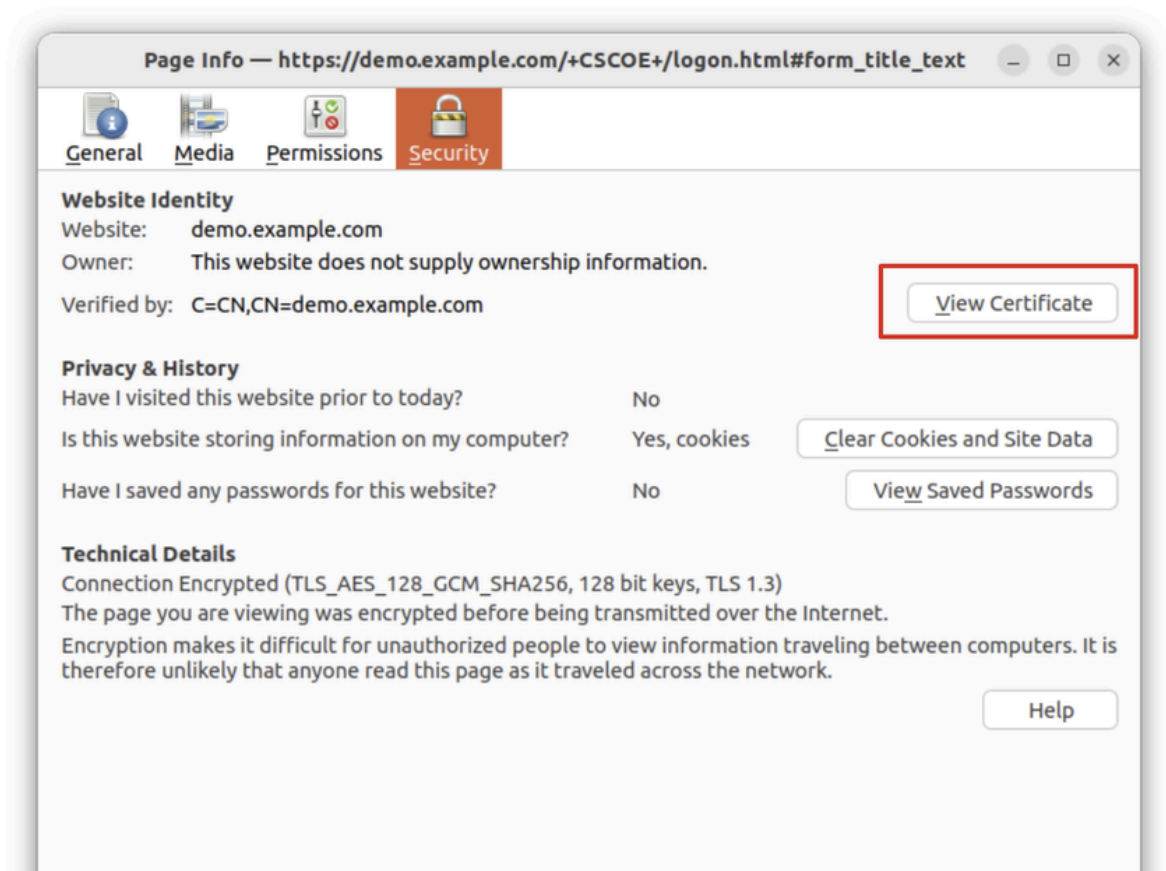
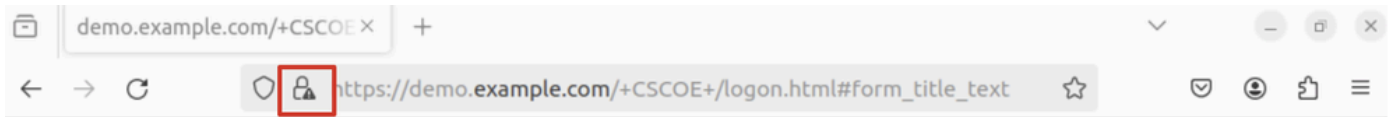
Ubuntu_Browser_VPN_Download_1

O nome do arquivo baixado é cisco-secure-client-linux64-5.1.3.62-core-vpn-webdeploy-k9.sh.



Ubuntu_Browser_VPN_Download_2

Etapa 26. Baixe o certificado VPN pelo navegador e renomeie o arquivo como <certificate>.crt. Este é o exemplo do uso do firefox para baixar o certificado.



Ubuntu_Browser_VPN_Cert_Download

Etapa 27. Abra o terminal no cliente Ubuntu. Navegue até path home/user/Downloads/ para instalar o Cisco Secure Client.

```
<#root>
```

```
user@ubuntu22-desktop:~$
```

```
cd Downloads/
```

```
user@ubuntu22-desktop:~/Downloads$
```

```
ls
```

```
cisco-secure-client-linux64-5.1.3.62-core-vpn-webdeploy-k9.sh
```

```
demo-example-com.crt
```

```
user@ubuntu22-desktop:~/Downloads$
```

```
chmod +x cisco-secure-client-linux64-5.1.3.62-core-vpn-webdeploy-k9.sh
```

```
user@ubuntu22-desktop:~/Downloads$
```

```
sudo ./cisco-secure-client-linux64-5.1.3.62-core-vpn-webdeploy-k9.sh
```

```
[sudo] password for user:  
Installing Cisco Secure Client...  
Migrating /opt/cisco/anyconnect directory to /opt/cisco/secureclient directory  
Extracting installation files to /tmp/vpn.zaeAZd/vpninst959732303.tgz...  
Unarchiving installation files to /tmp/vpn.zaeAZd...  
Starting Cisco Secure Client Agent...  
Done!  
Exiting now.  
user@ubuntu22-desktop:~/Downloads$
```

Etapa 28. Confiar no certificado do portal VPN no cliente Ubuntu.

```
<#root>
```

```
user@ubuntu22-desktop:~$
```

```
cd Downloads/
```

```
user@ubuntu22-desktop:~/Downloads$
```

```
ls
```

```
cisco-secure-client-linux64-5.1.3.62-core-vpn-webdeploy-k9.sh
```

```
demo-example-com.crt
```

```
user@ubuntu22-desktop:~/Downloads$
```

```
openssl verify demo-example-com.crt
```

```
CN = demo.example.com, C = CN  
error 18 at 0 depth lookup: self-signed certificate  
Error demo-example-com.crt:
```

```
verification failed
```

```
user@ubuntu22-desktop:~/Downloads$
```

```
sudo cp demo-example-com.crt /usr/local/share/ca-certificates/
```

```
user@ubuntu22-desktop:~/Downloads$
```

```
sudo update-ca-certificates
```

```
Updating certificates in /etc/ssl/certs...
```

```
rehash: warning: skipping ca-certificates.crt, it does not contain exactly one certificate or CRL
```

```
1 added
```

```
, 0 removed; done.
```

```
Running hooks in /etc/ca-certificates/update.d...
```

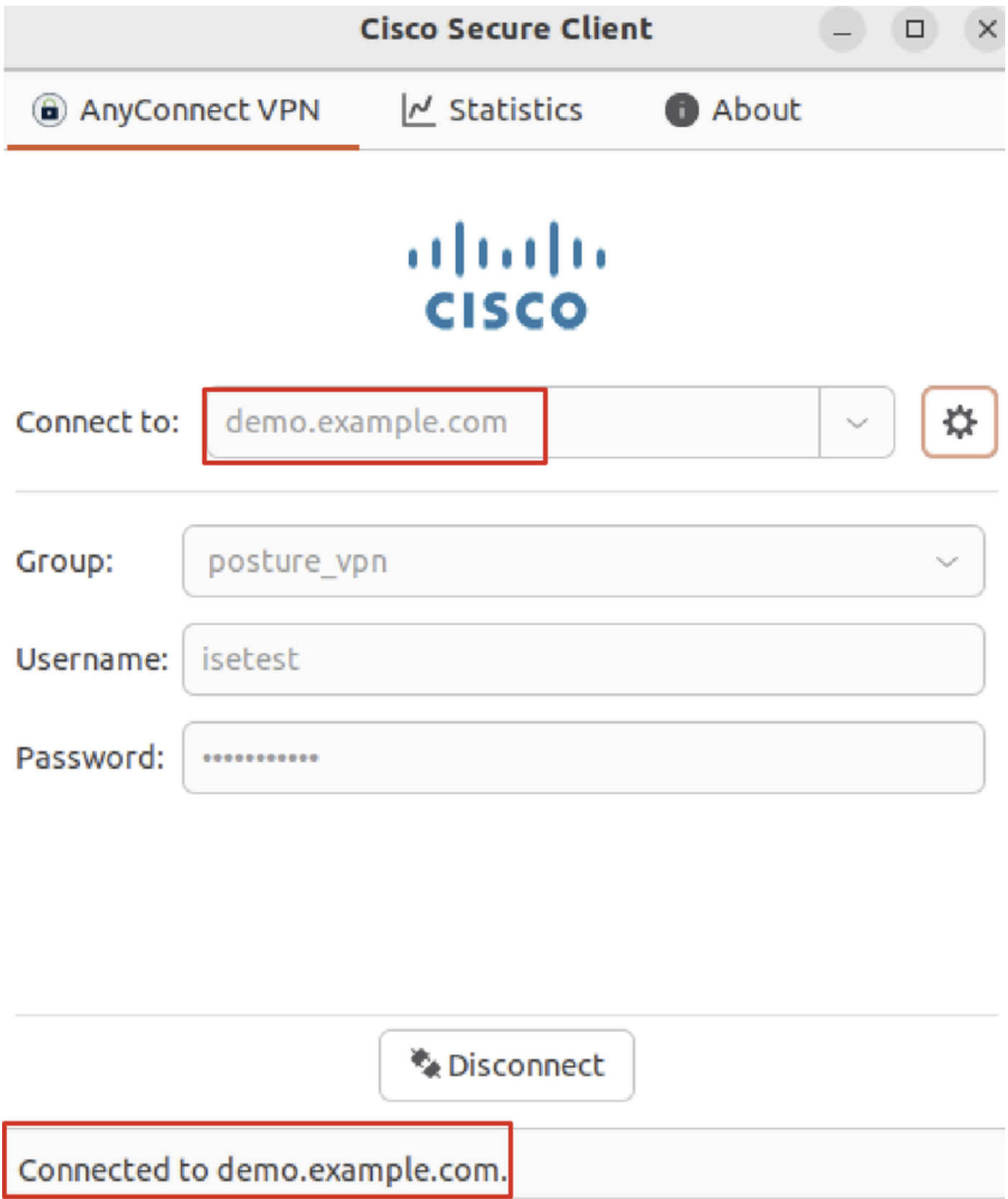
```
done.
```

```
user@ubuntu22-desktop:~/Downloads$
```

```
openssl verify demo-example-com.crt
```

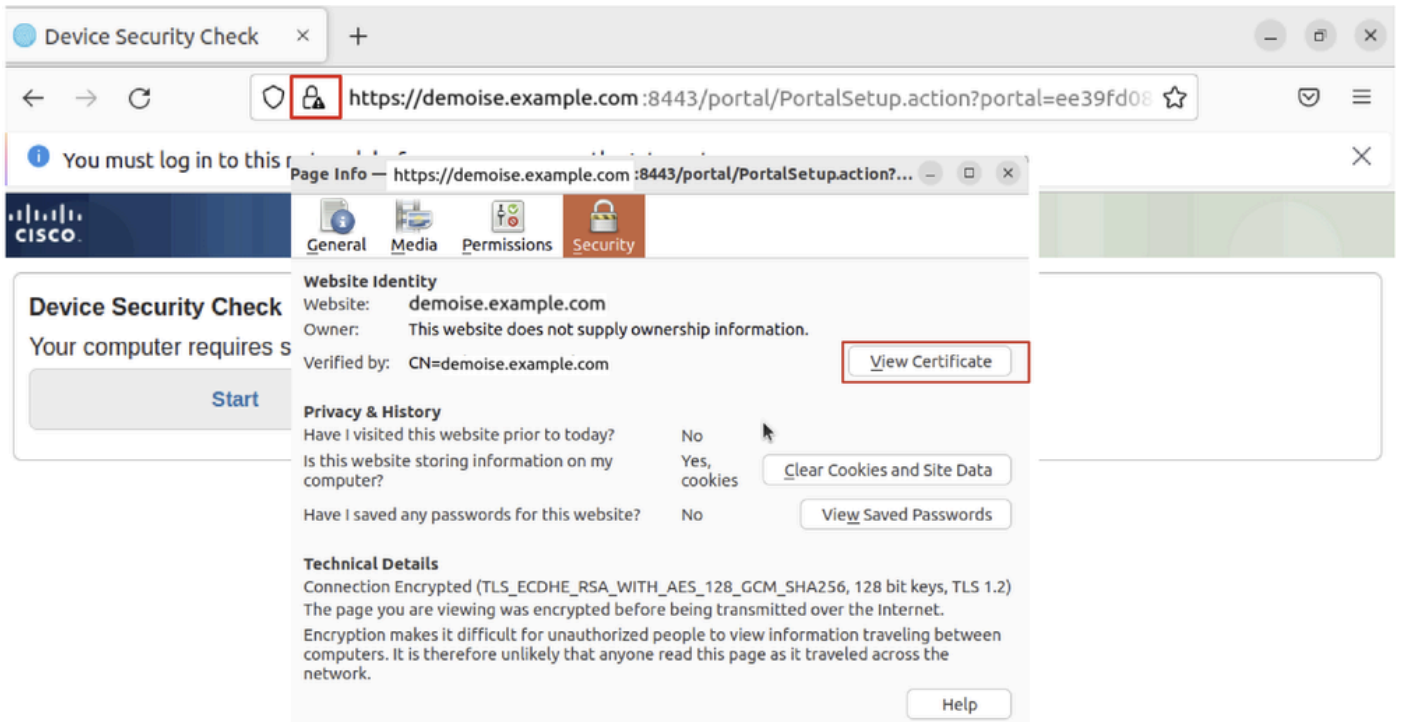
```
demo-example-com.crt: OK
```

Etapa 29. Abra o Cisco Secure Client no cliente Ubuntu e conecte a VPN ao demo.example.com com êxito.



Ubuntu_Secure_Client_Connected

Etapa 30. Abra o navegador para acessar qualquer site que dispare o redirecionamento para o portal CPP do ISE. Baixe o certificado do portal CPP do ISE e renomeie o arquivo como <certificate>.crt. Este é um exemplo do uso do Firefox para download.



Ubuntu_Browser_CPP_Cert_Download

Etapa 30.1. Confie no certificado do portal ISE CPP no cliente Ubuntu.

<#root>

```
user@ubuntu22-desktop:~/Downloads$ ls
cisco-secure-client-linux64-5.1.3.62-core-vpn-webdeploy-k9.sh
demo-example-com.crt
```

```
ise-cert.crt
```

```
user@ubuntu22-desktop:~/Downloads$
```

```
sudo cp ise-cert.crt /usr/local/share/ca-certificates/
```

```
user@ubuntu22-desktop:~/Downloads$
```

```
sudo update-ca-certificates
```

```
Updating certificates in /etc/ssl/certs...
```

```
rehash: warning: skipping ca-certificates.crt,it does not contain exactly one certificate or CRL
```

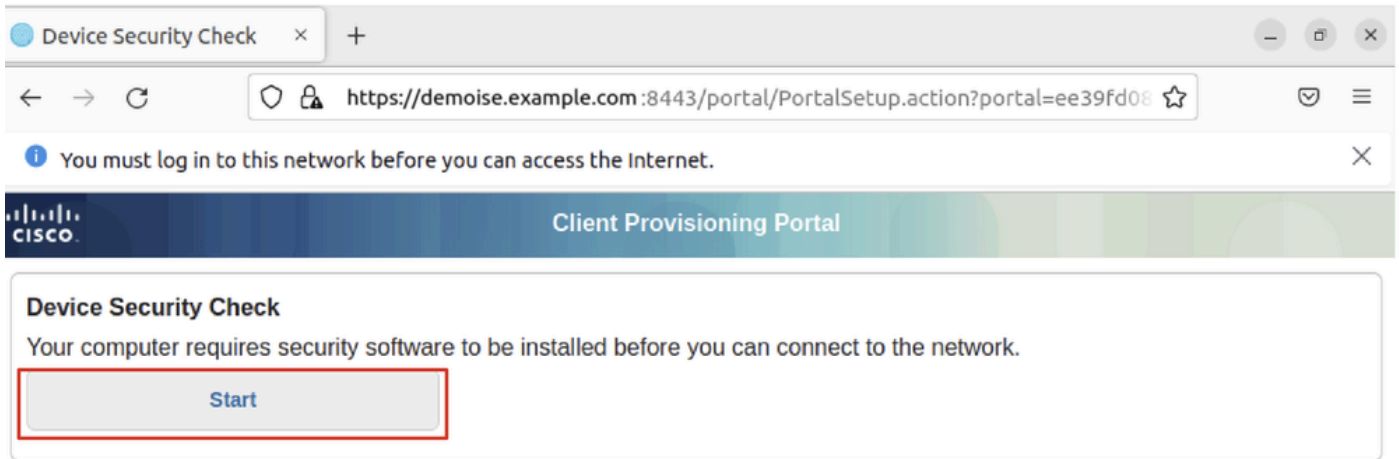
```
1 added
```

```
, 0 removed; done.
```

```
Running hooks in /etc/ca-certificates/update.d...
```

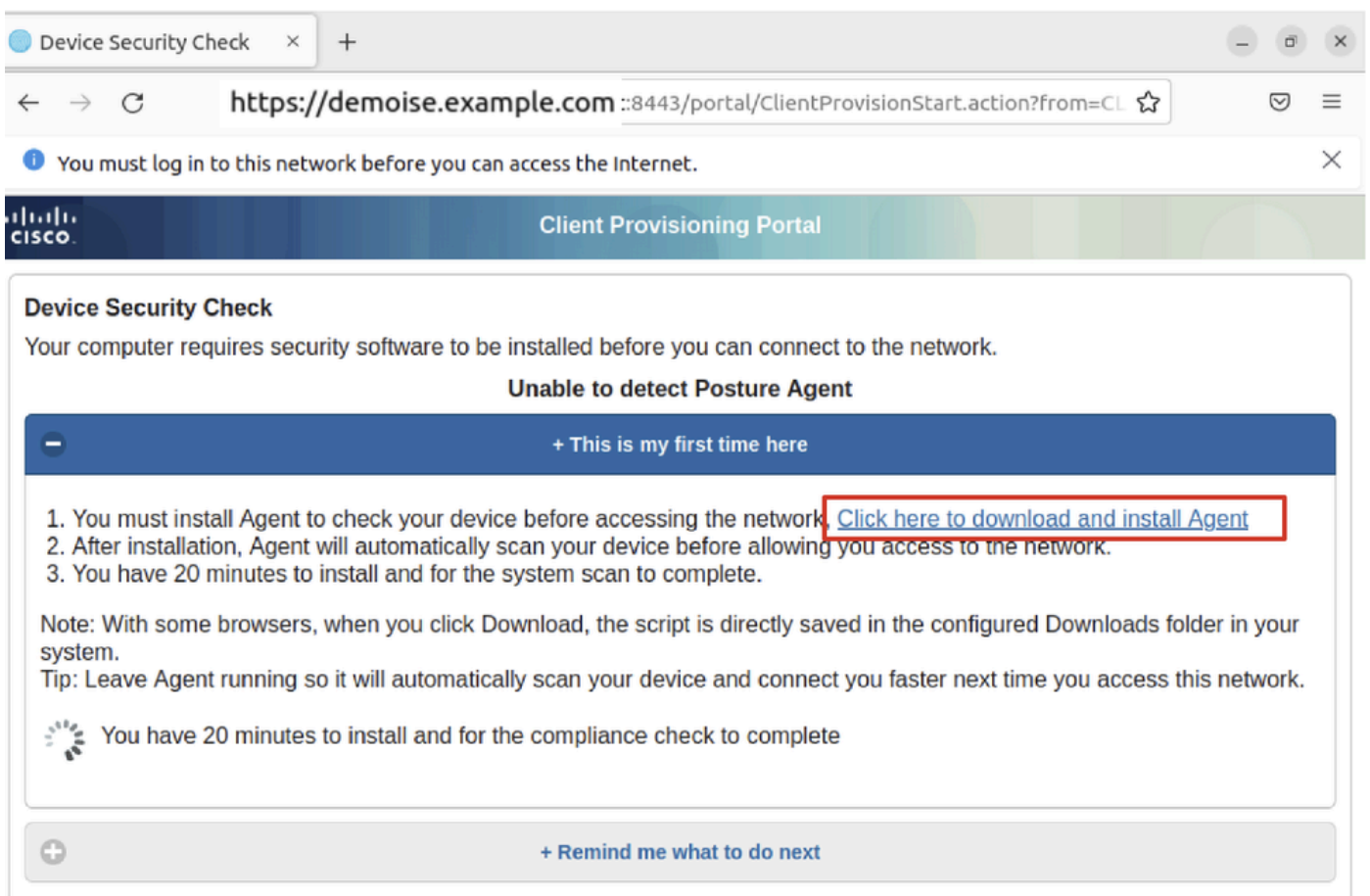
```
done.
```

Etapa 31. Clique Start no portal CPP do ISE.



Ubuntu_Browser_CPP_Start

Etapa 32. Click here to download and install Agent.



Ubuntu_Browser_CPP_Download_Posture

Etapa 33. Abra o terminal no cliente Ubuntu. Navegue até o caminho `home/user/Downloads/` para instalar o módulo de postura.

<#root>

```
user@ubuntu22-desktop:~/Downloads$ ls
```

```
cisco-secure-client-ise-network-assistant-linux64-5.1.3.62_demoise.example.com_8443_0NcLgcMURfyZmR6HoLmL
```

```
cisco-secure-client-linux64-5.1.3.62-core-vpn-webdeploy-k9.sh
demo-example-com.crt
ise-cert.crt
```

```
user@ubuntu22-desktop:~/Downloads$
```

```
chmod +x cisco-secure-client-ise-network-assistant-linux64-5.1.3.62_demoise.example.com_8443_0NcLgcMURfyZmR6Ho
```

```
user@ubuntu22-desktop:~/Downloads$
```

```
user@ubuntu22-desktop:~/Downloads$
```

```
user@ubuntu22-desktop:~/Downloads$
```

```
./cisco-secure-client-ise-network-assistant-linux64-5.1.3.62_demoise.example.com_8443_0NcLgcMURfyZmR6Ho
```

Cisco Network Setup Assistant

(c) 2022-2024 Cisco Systems, Inc. Cisco, Cisco Systems and Cisco Systems logo are registered trademarks

Cisco ISE Network Setup Assistant started. Version - 5.1.3.62

Trusted and Secure Connection

You are connected to

demoise.example.com

whose identity has been certified. Your connection to this website is encrypted.

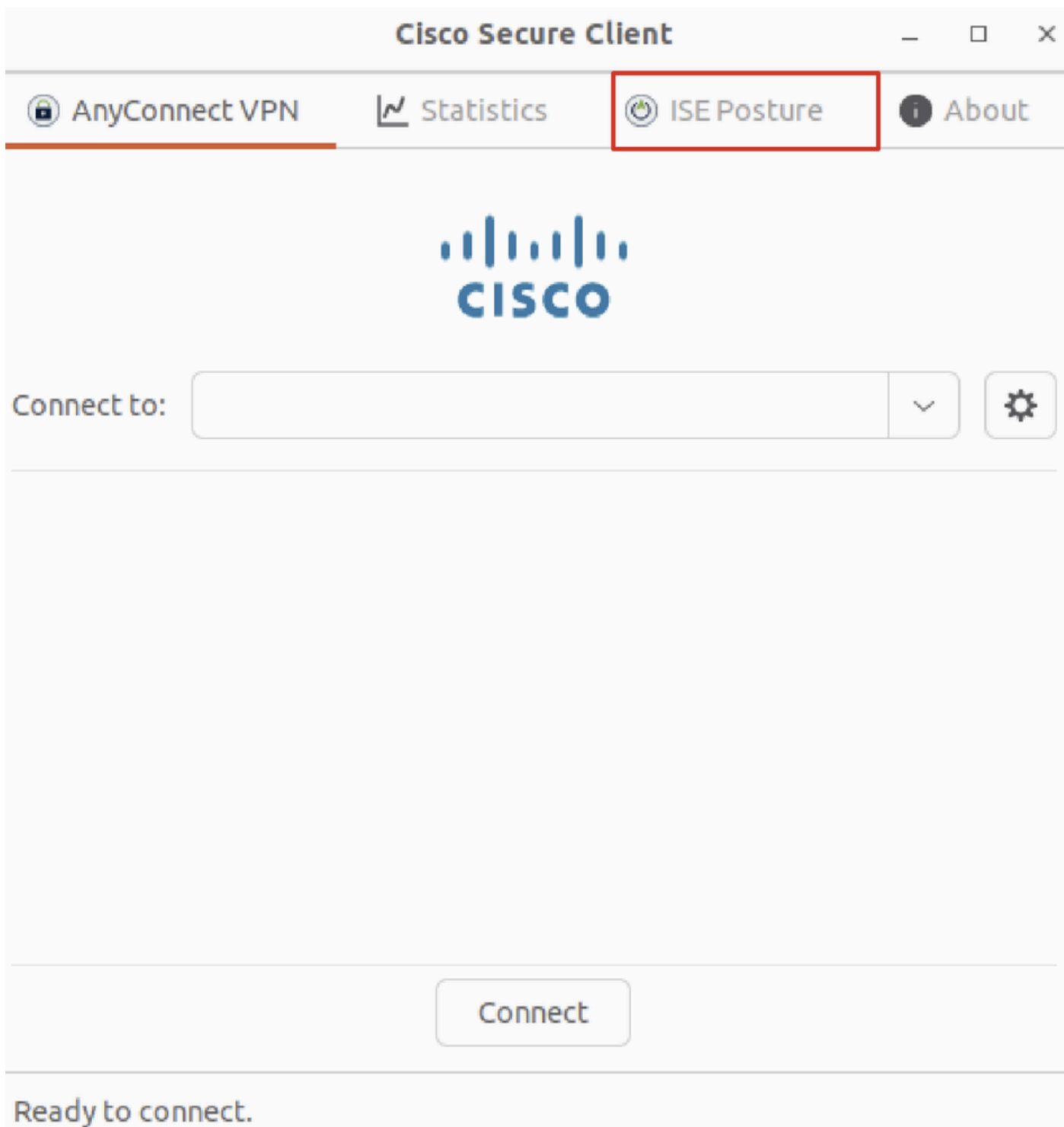
Downloading Cisco Secure Client...

Downloading remote package...

Running Cisco Secure Client - Downloader...

Installation is completed.

Etapa 34. Na interface do usuário do cliente Ubuntu, saia do Cisco Secure Client e abra-o novamente. O módulo de postura do ISE foi instalado e executado com êxito.



Ubuntu_Secure_Client_ISE_Posture_Installed

Etapa 35. Abra o terminal no cliente Ubuntu. Navegue até o caminho `home/user/Desktop` , crie um `test.txt` arquivo para atender à condição de arquivo configurada no ISE.

```
<#root>
```

```
user@ubuntu22-desktop:~$
```

```
cd Desktop/
```

```
user@ubuntu22-desktop:~/Desktop$
```

```
echo test > test.txt
```

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

Etapa 1. Conecte a VPN a demo.example.com no cliente Ubuntu.

The screenshot shows the Cisco Secure Client application window. The title bar reads "Cisco Secure Client". The main menu includes "AnyConnect VPN", "Statistics", "ISE Posture", and "About". The "ISE Posture" section is active, displaying the Cisco logo and a "Connect to:" field with the value "demo.example.com". Below this are fields for "Group:" (posture_vpn), "Username:" (isetest), and "Password:" (masked with dots). A "Disconnect" button is visible at the bottom. A status bar at the very bottom indicates "Connected to demo.example.com."

Verify_Ubuntu_Secure_Client_Connected

Etapa 2. Verifique o status da postura do ISE no cliente Ubuntu.



Network access allowed.



Verify_Ubuntu_Secure_Client_Compliant

Etapa 3. Verifique o registro em tempo real do Radius no ISE. Navegue até Operations > RADIUS Live Log.

Identity Services Engine | Operations / RADIUS

Live Logs | Live Sessions

Misconfigured Supplicants: 0 | Misconfigured Network Devices: 0 | RADIUS Drops: 0 | Client Stopped Responding: 0 | Repeat Counter: 0

Refresh: Never | Show: Latest 20 records | Within: Last 24 hours

Reset Repeat Counts | Export To

Time	Status	Details	Identity	Endpoint ID	Endpoint Profile	Posture Status	Authentication Policy	Authorization Policy
			Identity	Endpoint ID	Endpoint Profile	Posture Status	Authentication Policy	Authorization Policy
May 29, 2024 09:08:48.798 PM	●	🔒	isetest	52:54:00:17:6B:FA	Ubuntu-Workstation	Compliant	Firewall Posture >> Default	Firewall Posture >> Compliant
May 29, 2024 09:08:48.798 PM	✔	🔒		52:54:00:17:6B:FA		Compliant	Firewall Posture	Firewall Posture >> Compliant
May 29, 2024 09:08:13.570 PM	✔	🔒	isetest	52:54:00:17:6B:FA	Ubuntu-Workstation	Pending	Firewall Posture >> Default	Firewall Posture >> Unknown

Etapa 4. Navegue até a CLI do FTD via SSH ou console.

```
<#root>
```

```
>  
>
```

```
system support diagnostic-cli
```

```
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.  
Type help or '?' for a list of available commands.
```

```
ftdv741>
```

```
enable
```

```
Password:
```

```
ftdv741#
```

```
ftdv741#
```

```
show vpn-sessiondb detail anyconnect
```

```
Session Type: AnyConnect Detailed
```

```
Username : isetest Index : 33
```

```
Assigned IP : 192.168.6.30 Public IP : 192.168.10.13
```

```
Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
```

```
License : AnyConnect Premium
```

```
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-128 DTLS-Tunnel: (1)AES-GCM-256
```

```
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA256 DTLS-Tunnel: (1)SHA384
```

```
Bytes Tx : 51596 Bytes Rx : 17606
```

```
Pkts Tx : 107 Pkts Rx : 136
```

```
Pkts Tx Drop : 0 Pkts Rx Drop : 0
```

```
Group Policy : posture_gp Tunnel Group : posture_vpn
```

```
Login Time : 14:02:25 UTC Fri May 31 2024
```

```
Duration : 0h:00m:55s
```

```
Inactivity : 0h:00m:00s
```

```
VLAN Mapping : N/A VLAN : none
```

```
Audt Sess ID : cb007182000210006659d871
```

```
Security Grp : none Tunnel Zone : 0
```

```
AnyConnect-Parent Tunnels: 1
```

```
SSL-Tunnel Tunnels: 1
```

```
DTLS-Tunnel Tunnels: 1
```

```
AnyConnect-Parent:
```

```
Tunnel ID : 33.1
```

```
Public IP : 192.168.10.13
```

```
Encryption : none Hashing : none
```

```
TCP Src Port : 59180 TCP Dst Port : 443
```

```
Auth Mode : userPassword
```

```
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
```

```
Client OS : linux-64
```

```
Client OS Ver: Ubuntu 22.04 LTS 22.04 (Jammy Jellyfish)
```

Client Type : AnyConnect

Client Ver : Cisco AnyConnect VPN Agent for Linux 5.1.3.62

Bytes Tx : 6364 Bytes Rx : 0
Pkts Tx : 1 Pkts Rx : 0
Pkts Tx Drop : 0 Pkts Rx Drop : 0

SSL-Tunnel:

Tunnel ID : 33.2
Assigned IP :192.168.6.30 Public IP : 192.168.10.13
Encryption : AES-GCM-128 Hashing : SHA256
Ciphersuite : TLS_AES_128_GCM_SHA256
Encapsulation: TLSv1.3 TCP Src Port : 59182
TCP Dst Port : 443 Auth Mode : userPassword
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Client OS : Linux_64
Client Type : SSL VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Linux 5.1.3.62
Bytes Tx : 6364 Bytes Rx : 498
Pkts Tx : 1 Pkts Rx : 6
Pkts Tx Drop : 0 Pkts Rx Drop : 0

Filter Name : #ACSACL#-IP-PERMIT_ALL_IPV4_TRAFFIC-57f6b0d3

DTLS-Tunnel:

Tunnel ID : 33.3
Assigned IP :192.168.6.30 Public IP : 192.168.10.13
Encryption : AES-GCM-256 Hashing : SHA384
Ciphersuite : ECDHE-ECDSA-AES256-GCM-SHA384
Encapsulation: DTLSv1.2 UDP Src Port : 56078
UDP Dst Port : 443 Auth Mode : userPassword
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Client OS : Linux_64
Client Type : DTLS VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Linux 5.1.3.62
Bytes Tx : 38868 Bytes Rx : 17108
Pkts Tx : 105 Pkts Rx : 130
Pkts Tx Drop : 0 Pkts Rx Drop : 0

Filter Name : #ACSACL#-IP-PERMIT_ALL_IPV4_TRAFFIC-57f6b0d3

Troubleshooting

Esta seção disponibiliza informações para a solução de problemas de configuração.

Para fluxo de postura e solução de problemas do Cisco Secure Client e ISE, consulte os [documentos](#) do CCO [Comparação de estilo de postura do ISE para pré e pós-2.2](#) e [Solução de problemas de gerenciamento de sessão e postura do ISE](#).

Informações Relacionadas

- [Compatibilidade do componente de rede do Cisco Identity Services Engine, versão 3.3](#)

- [Guia do Administrador do Cisco Identity Services Engine, Versão 3.3](#)
- [Suporte técnico e downloads da Cisco](#)

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.