

Configuración de la condición de VPN de Linux con ISE 3.3

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuraciones en FMC/FTD](#)

[Configuraciones en ISE](#)

[Configuraciones en Ubuntu](#)

[Verificación](#)

[Troubleshoot](#)

[Información Relacionada](#)

Introducción

Este documento describe cómo configurar el estado de la VPN Linux con Identity Services Engine (ISE) y Firepower Threat Defence (FTD).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Cliente seguro de Cisco
- VPN de acceso remoto en Firepower Threat Defence (FTD)
- Identity Services Engine (ISE)

Componentes Utilizados

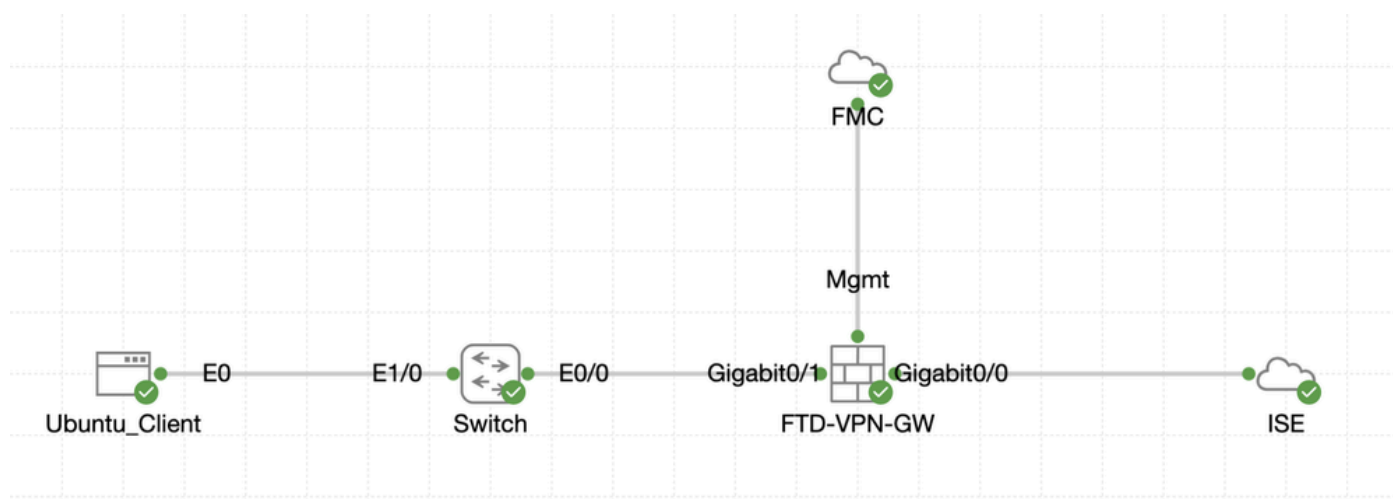
La información que contiene este documento se basa en estas versiones de software:

- Ubuntu 22,04
- Cisco Secure Client 5.1.3.62
- Cisco Firepower Threat Defense (FTD) 7.4.1
- Cisco Firepower Management Center (FMC) 7.4.1
- Cisco Identity Services Engine (ISE) 3.3

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Configurar

Diagrama de la red



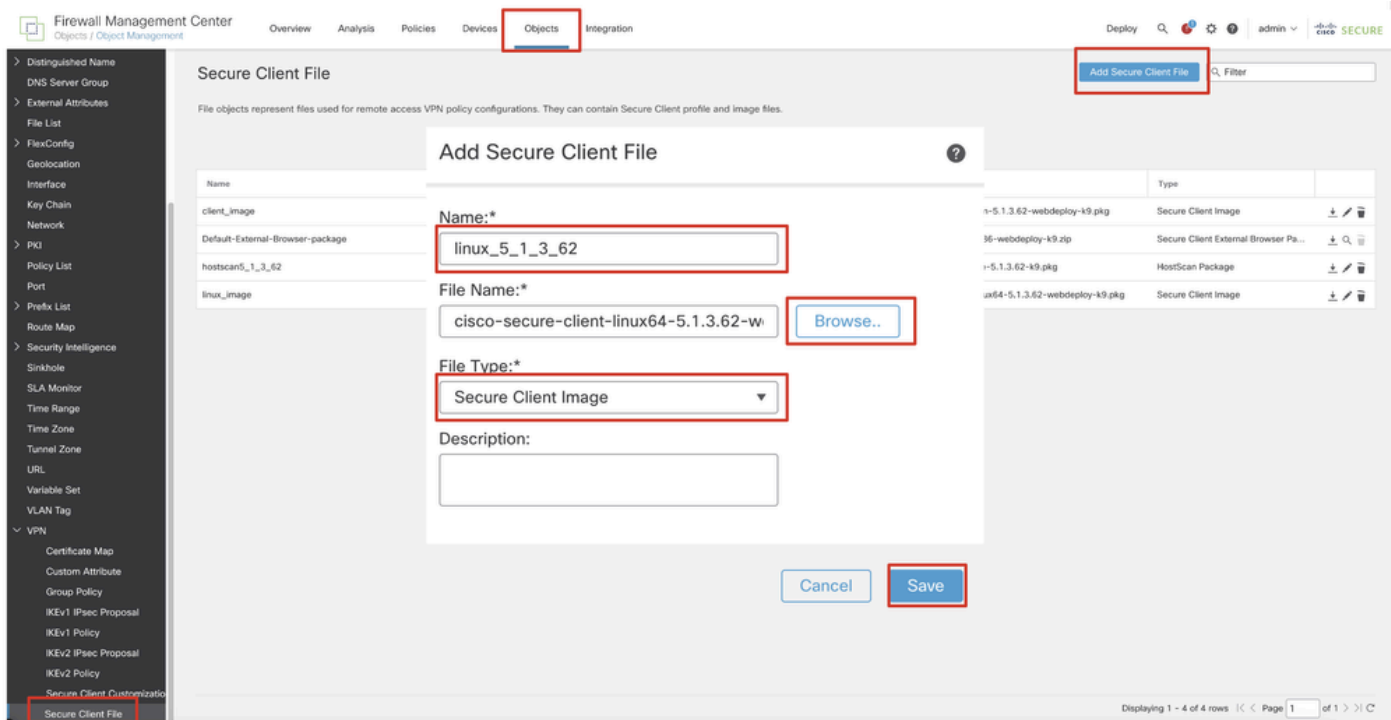
Topología

Configuraciones en FMC/FTD

Paso 1. La conectividad entre el cliente, FTD, FMC e ISE se ha configurado correctamente. Como enroll.cisco.com se utiliza para los terminales que hacen sondeos para redirección (consulte los [documentos de CCO](#) sobre el flujo de postura [Comparación del estilo de postura ISE para versiones anteriores y posteriores a la 2.2](#) para obtener más información). Asegúrese de que la ruta para el tráfico a enroll.cisco.com en FTD esté configurada correctamente.

Paso 2. Descargue el nombre del paquete `cisco-secure-client-linux64-5.1.3.62-webdeploy-k9.pkg` de [Descarga de Software de Cisco](#) y asegúrese de que el archivo sea bueno después de la descarga confirmando que la suma de comprobación md5 del archivo descargado es la misma que la página de Descarga de Software de Cisco.

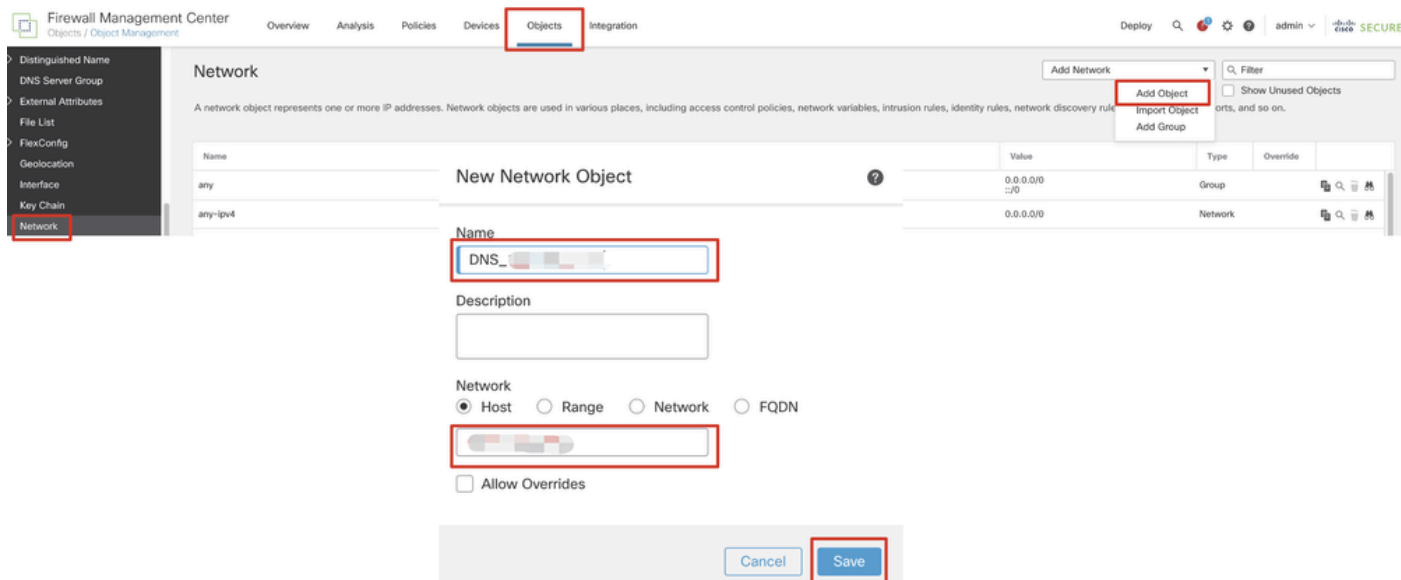
Paso 3. Desplácese hasta **Objects > Object Management > VPN > Secure Client File**. Haga clic en **Add Secure Client File**, proporcione el nombre, navegue **File Name** para seleccionar `cisco-secure-client-linux64-5.1.3.62-webdeploy-k9.pkg`, seleccione **Secure Client Image** en la lista desplegable **File Type**. A continuación, haga clic en **Save**.



FMC_Upload_Secure_Client_Image

Paso 4. Desplácese hasta Objects > Object Management > Network.

Paso 4.1. Cree un objeto para el servidor DNS. Haga clic en Add Object, indique el nombre y la dirección IP de DNS disponible. Haga clic en Save.

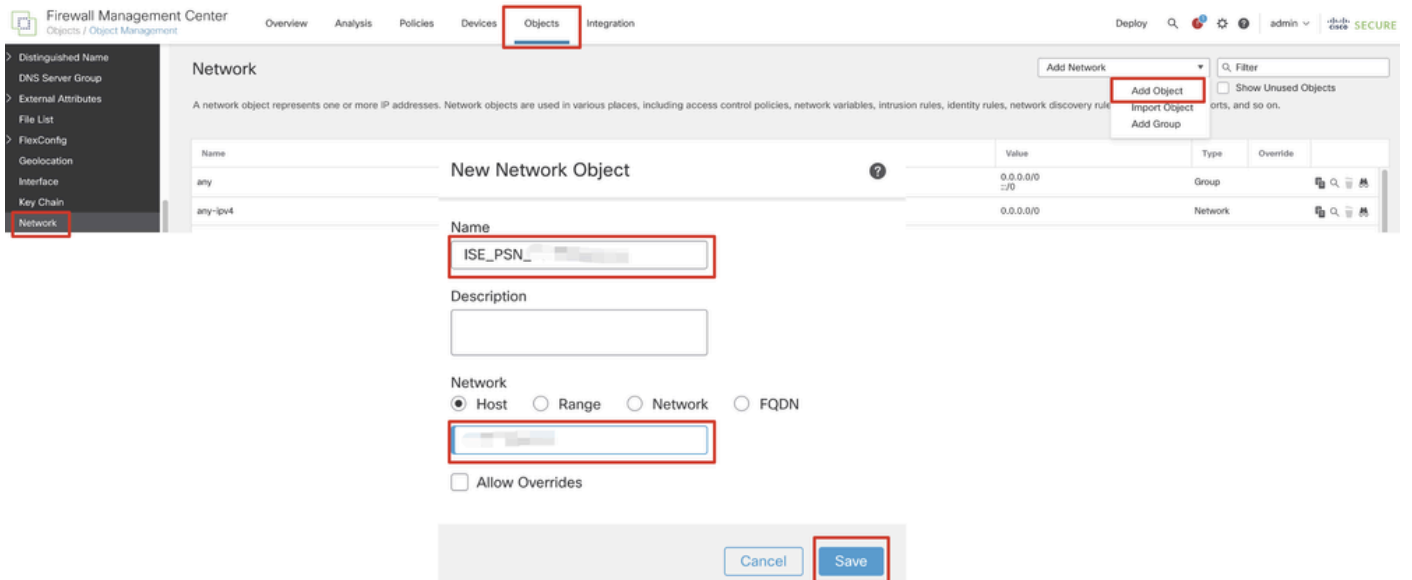


FMC_Add_Object_DNS



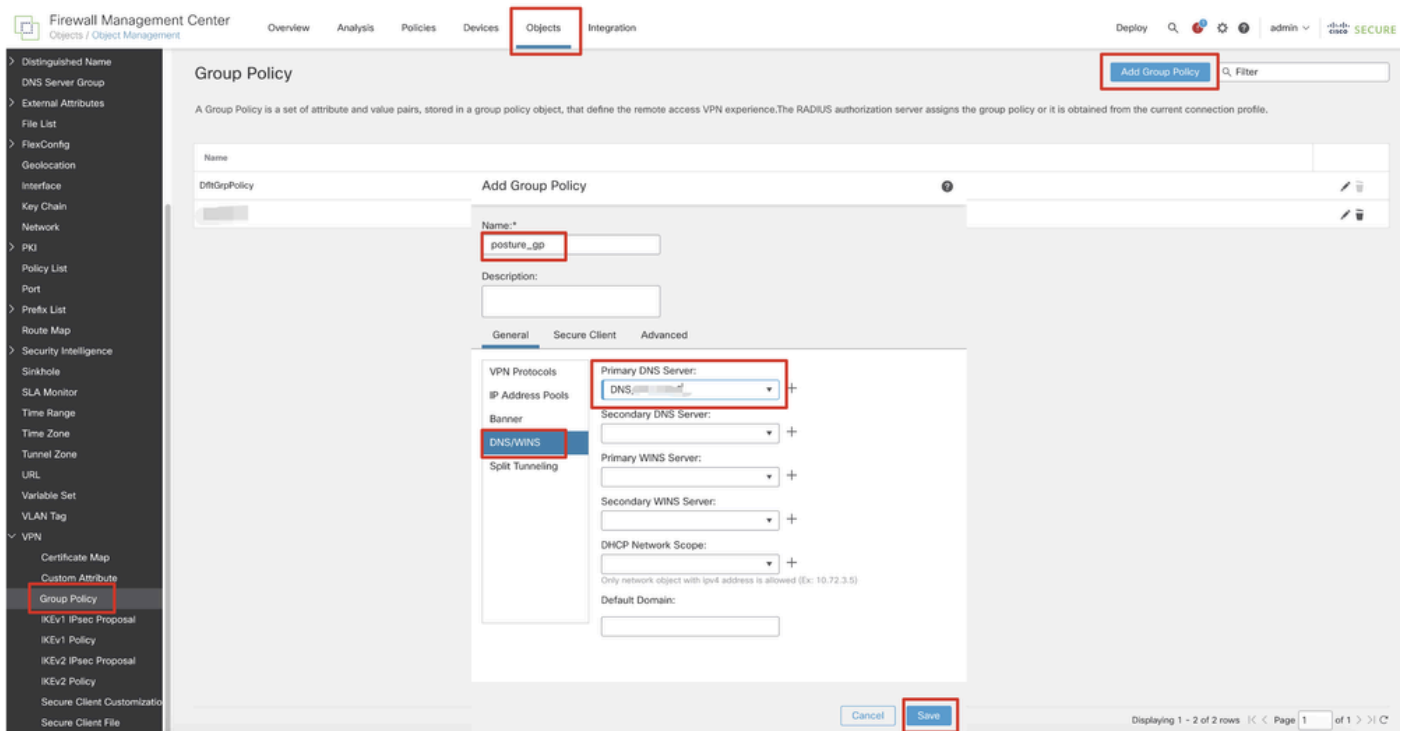
Nota: El servidor DNS configurado aquí se debe utilizar para los usuarios de VPN.

Paso 4.2. Cree un objeto para ISE PSN. Haga clic en Add Object, introduzca el nombre y la dirección IP PSN de ISE disponible. Haga clic en Save.



FMC_Add_Object_ISE

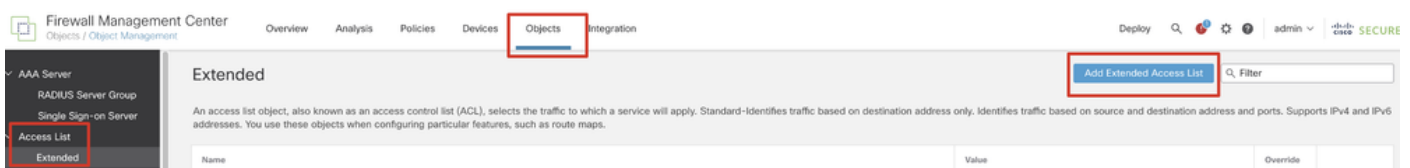
Paso 5. Desplácese hasta Objects > Object Management > VPN > Group Policy. Haga clic en Add Group Policy. Haga clic en DNS/WINS, seleccione el objeto del servidor DNS en Primary DNS Server. A continuación, haga clic en Save.



FMC_Add_Group_Policy

Nota: asegúrese de que el servidor DNS utilizado en la política de grupo VPN puede resolver el FQDN y enroll.cisco.com del portal de aprovisionamiento de clientes de ISE.

Paso 6. Desplácese hasta Objects > Object Management > Access List > Extended. Haga clic en Add Extended Access List.



FMC_Add_Redirect_ACL

Paso 6.1. Proporcione el nombre de la ACL de redirección. Este nombre debe ser el mismo que en el perfil de autorización de ISE. Haga clic en

Add.

New Extended Access List Object

Name

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

Paso 6.2. Bloquee el tráfico DNS, el tráfico a la dirección IP PSN de ISE y los servidores de corrección para excluirlos de la redirección. Permitir el resto del tráfico. Esto activa la redirección. Haga clic en Save.

Add Extended Access List Entry

Action:

Logging:

Log Level:

Log Interval: Sec.

Network Port Application Users Security Group Tag

Available Networks

- 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

Source Networks (0)

Destination Networks (1)

Enter an IP address Add

Enter an IP address Add

Cancel Add

FMC_Add_Redirect_ACL_Part_2

Name
redirect

Entries (4)

Add

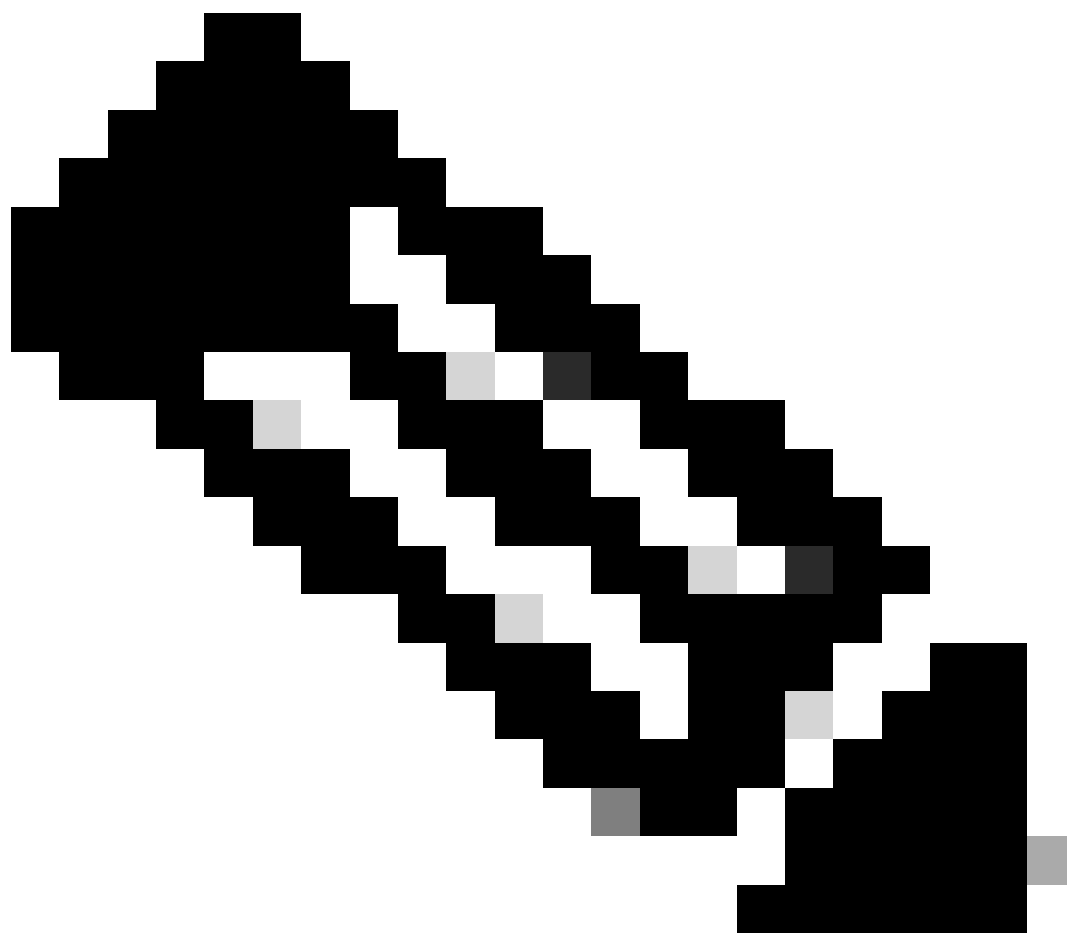
Sequence	Action	Source	Source Port	Destination	Destination Port	Application	Users	SGT	
1	Block	any-ipv4	Any	ISE_PSN	Any	Any	Any	Any	
2	Block	Any	Any	Any	DNS_over_TCP DNS_over_UDP	Any	Any	Any	
3	Block	Any	Any	FTP	Any	Any	Any	Any	
4	Allow	any-ipv4	Any	any-ipv4	Any	Any	Any	Any	

Allow Overrides

Cancel

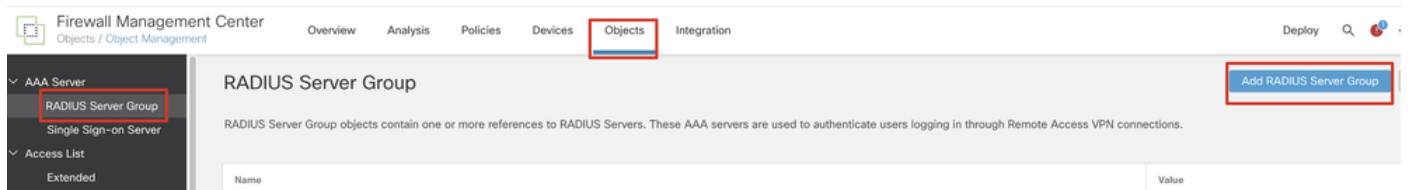
Save

FMC_Add_Redirect_ACL_Part_3



Nota: El FTP de destino en este ejemplo de ACL de redirección se utiliza como ejemplo de servidor de corrección.

Paso 7. Desplácese hasta Objects > Object Management > RADIUS Server Group. Haga clic en Add RADIUS Server Group.



FMC_Add_New_Radius_Server_Group

Paso 7.1. Proporcione el nombre, la comprobación Enable authorize only, la comprobación Enable interim account update, la comprobación 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

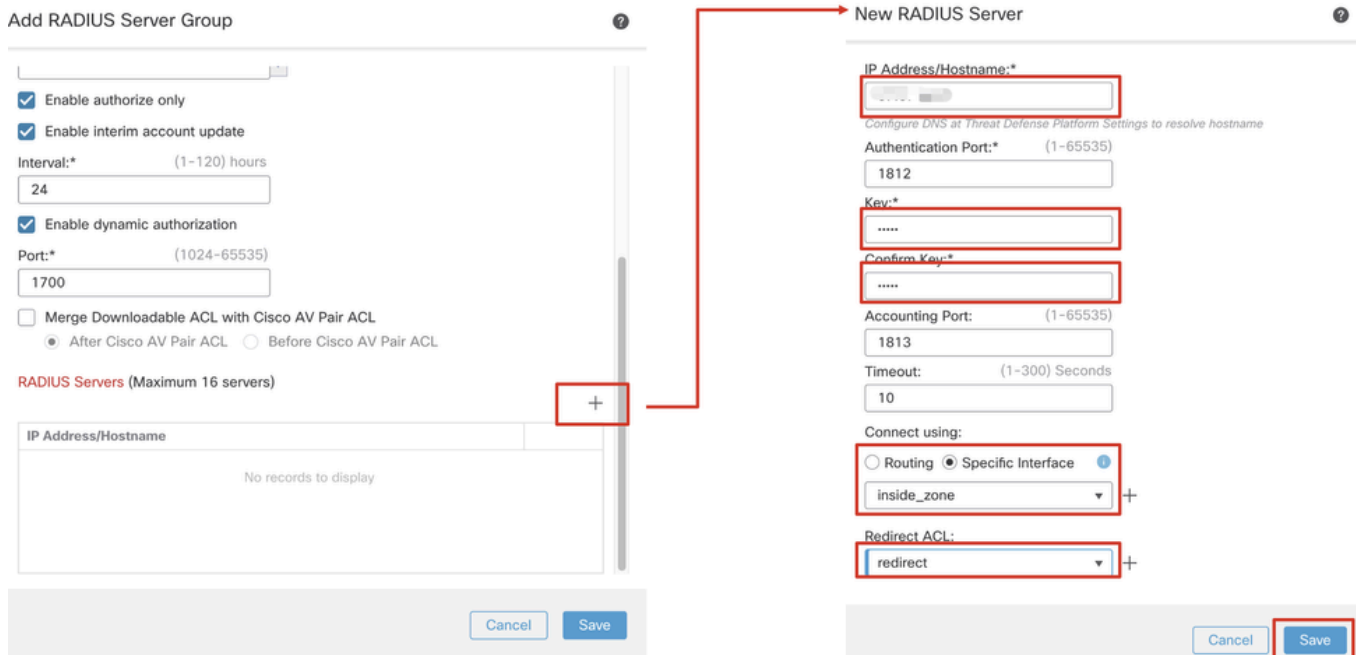
Port:* (1024-65535)

Cancel

Save

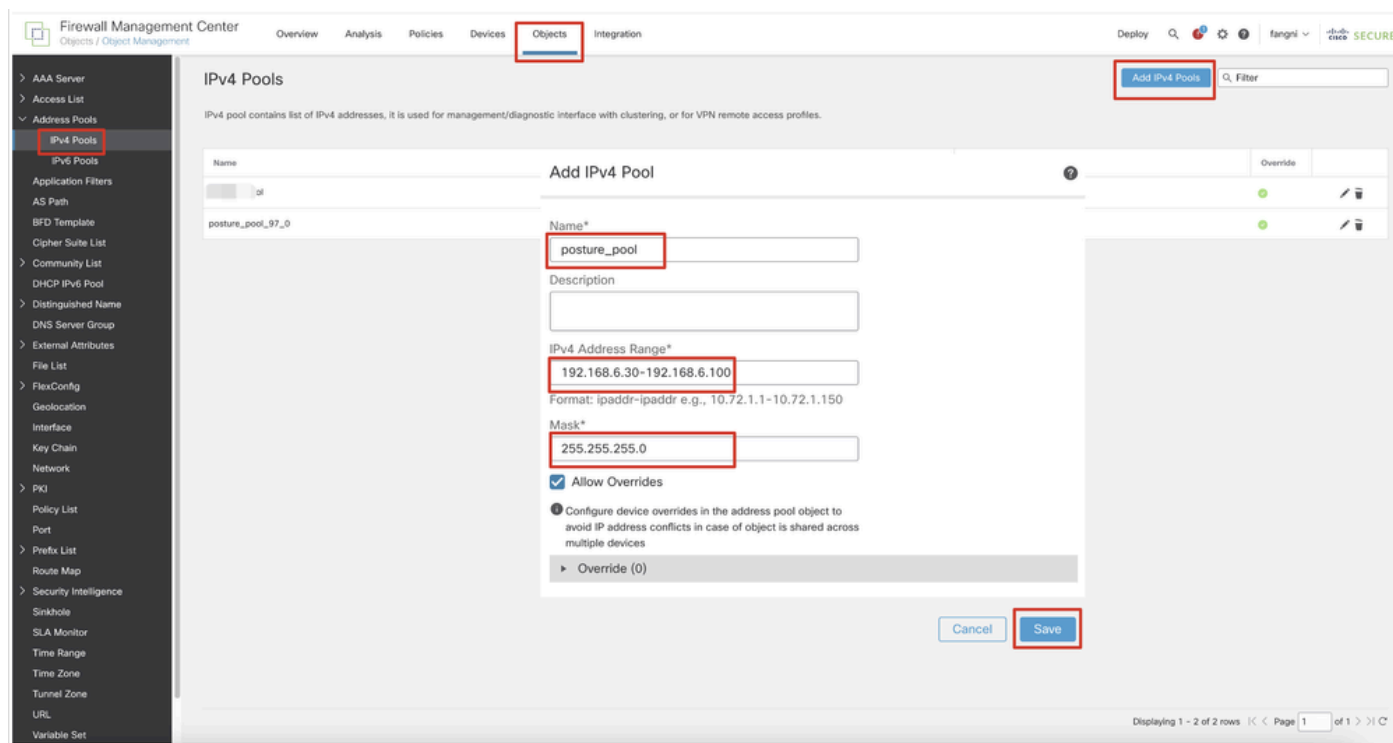
FMC_Add_New_Radius_Server_Group_Part_1

Paso 7.2. Haga clic en el Plus icono para agregar un nuevo servidor RADIUS. Proporcione el ISE PSN IP Address/Hostname, Key. Seleccione el specific interface para conectarse. Seleccione el Redirect ACL. A continuación, haga clic Save para guardar el nuevo servidor RADIUS. A continuación, haga clic Save de nuevo para guardar el nuevo grupo de servidores RADIUS.



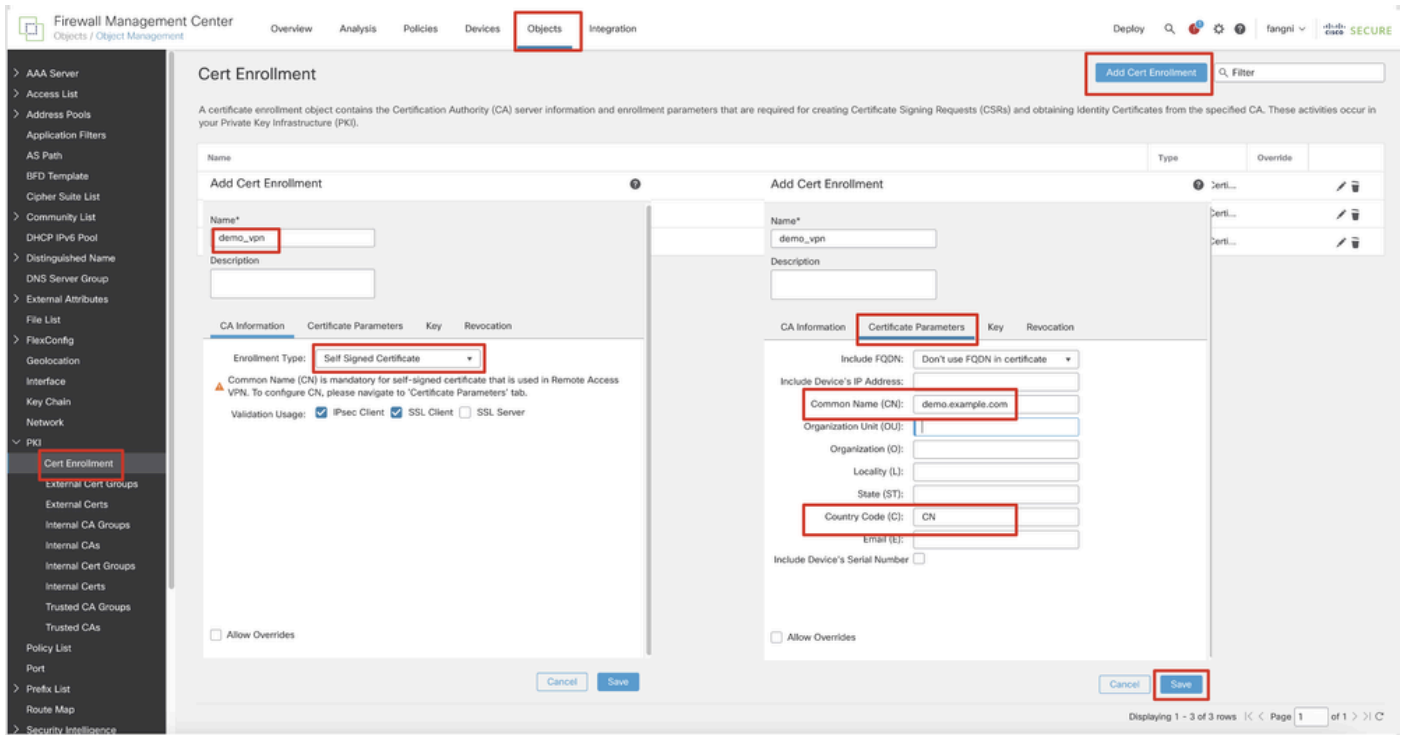
FMC_Add_New_Radius_Server_Group_Part_2

Paso 8. Desplácese hasta Objects > Object Management > Address Pools > IPv4 Pools. Haga clic en Add IPv4 Pools y proporcione el **Name**, **IPv4 Address Range** y **Mask**. A continuación, haga clic en Save.



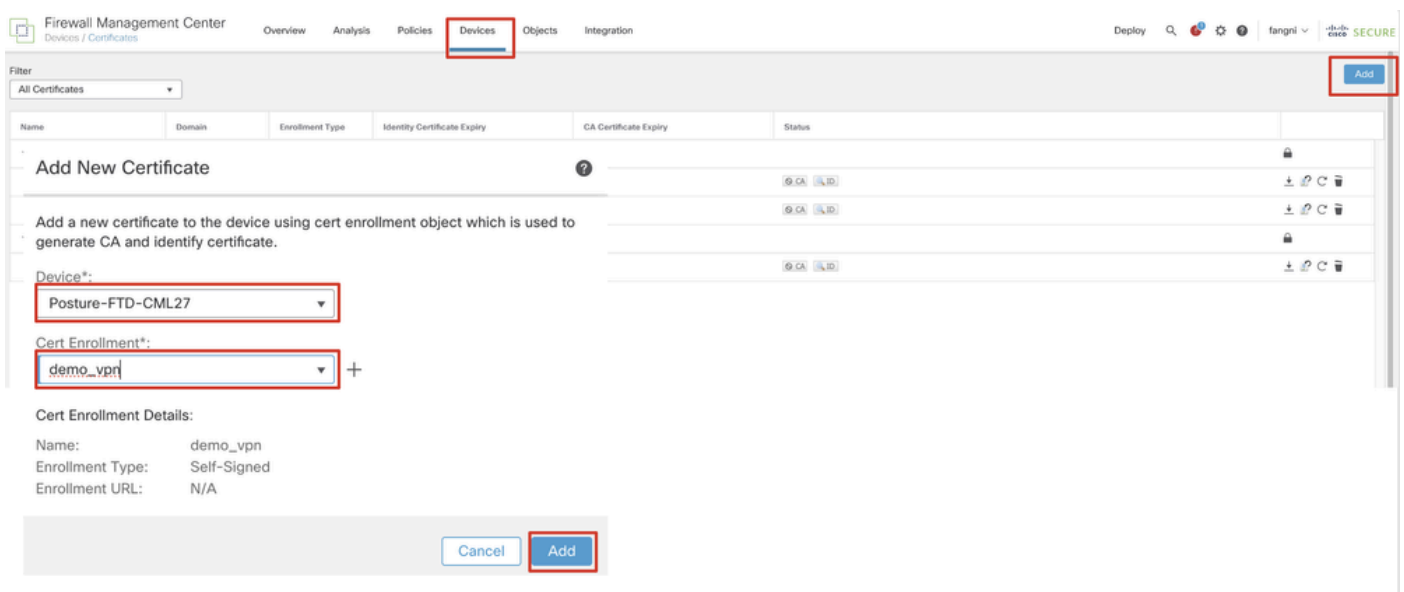
FMC_Add_New_Pool

Paso 9. Desplácese hasta Certificate Objects > Object Management > PKI > Cert Enrollment. Haga clic en Add Cert Enrollment, proporcione un nombre y seleccione Self Signed Certificateen Enrollment Type. Haga clic en la Certificate Parameters ficha y proporcione Common Name y Country Code. A continuación, haga clic en Save.



FMC_Add_New_Cert_Enroll

Paso 10. Desplácese hasta Devices > Certificates. Haga clic en Add, seleccione el nombre de FTD en Device, seleccione la inscripción configurada anterior en Cert Enrollment. Haga clic en Add.



FMC_Add_New_Cert_To_FTD

Paso 11. Desplácese hasta Devices > VPN > Remote Access. Haga clic en Add.

Paso 11.1. Proporcione el nombre y añada el FTD a Selected Devices. Haga clic en 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

Paso 11.2. Seleccione el grupo de servidores RADIUS configurado anteriormente en la Authentication Server, Authorization Server, Accounting Server. Desplácese hacia abajo en la página.

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:* rpise

(LOCAL or Realm or RADIUS)

Fallback to LOCAL Authentication

Authorization Server: rpise

(Realm or RADIUS)

Accounting Server: rpise

(Account)

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

Paso 11.3. Seleccione el nombre de conjunto configurado anteriormente en IPv4 Address Pools. Seleccione la política de grupo configurada anteriormente en Group Policy. Haga clic en 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

Paso 11.4. Marque la casilla de la imagen de Linux. Haga clic en 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

Paso 11.5. Seleccione la interfaz de la interfaz VPN. Seleccione la inscripción de certificados que se inscribió en el FTD en el paso 9. Haga clic en Next.

Firewall Management Center
Devices / VPN / Setup Wizard

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 ⚙️ 👤 admin v **SECURE**

Remote Access VPN Policy Wizard

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

Network Interface for Incoming VPN Access
Select or create an Interface Group or a Security Zone that contains the network interfaces users will access for VPN connections.

Interface group/Security Zone:

Enable DTLS on member interfaces

⚠️ All the devices must have interfaces as part of the Interface Group/Security Zone selected.

Device Certificates
Device certificate (also called identity certificate) identifies the VPN gateway to the remote access clients. Select a certificate which is used to authenticate the VPN gateway.

Certificate Enrollment:

Enroll the selected 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)

Cancel Back **Next**

FMC_New_RAVPN_Wizard_5

Paso 11.6. Confirme la información relacionada en la página de resumen. Si todo está bien, haga clic en Finish. Si necesita modificar algo, haga clic en Back.

Firewall Management Center
Devices / VPN / Setup Wizard

Overview Analysis Policies **Devices** Objects Integration

Deploy 🔍 ⚙️ 👤 admin v **SECURE**

Remote Access VPN Policy Wizard

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

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

Name:	posture_vpn
Device Targets:	Posture-FTD-CM127
Connection Profile:	posture_vpn
Connection Alias:	posture_vpn
AAA:	
Authentication Method:	AAA Only
Authentication Server:	rtplse (RADIUS)
Authorization Server:	rtplse
Accounting Server:	rtplse
Address Assignment:	
Address from AAA:	-
DHCP Servers:	-
Address Pools (IPv4):	posture_pool
Address Pools (IPv6):	-
Group Policy:	posture_gp
Secure Client Images:	linux_5_1_3_62
Interface Objects:	outside_zone
Device Certificates:	demo_vpn

Device Identity Certificate Enrollment
Certificate enrollment object 'demo_vpn' is not installed on one or more targeted

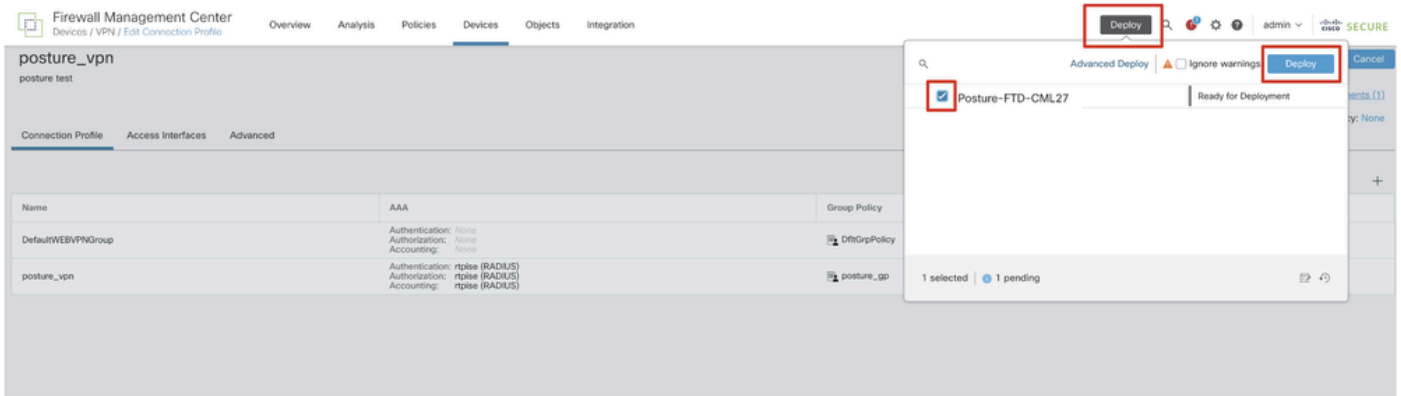
Additional Configuration Requirements
After the wizard completes, the following configuration needs to be completed for VPN to work on all device targets.

- Access Control Policy Update**
An Access Control rule must be defined to allow VPN traffic on all targeted devices.
- NAT Exemption**
If NAT is enabled on the targeted devices, you must define a NAT Policy to exempt VPN traffic.
- DNS Configuration**
To resolve hostname specified in AAA Servers or CA Servers, configure DNS using FlexConfig Policy on the targeted devices.
- Port Configuration**
SSL will be enabled on port 443. IPsec-IKEv2 uses port 500 and Client Services will be enabled on port 443 for Secure Client image download. NAT-Traversal will be enabled by default and will use port 4500. Please ensure that these ports are not used in NAT Policy or other services before deploying the configuration.
- Network Interface Configuration**

Cancel Back **Finish**

FMC_New_RAVPN_Wizard_6

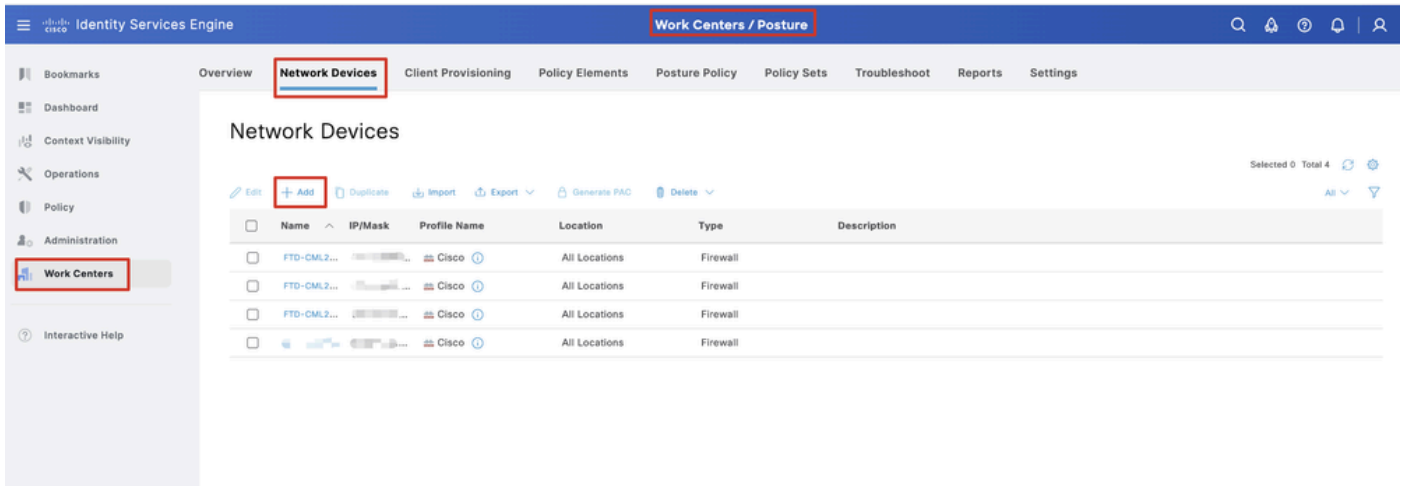
Paso 12. Implemente la nueva configuración en FTD para completar la configuración de VPN de acceso remoto.



FMC_Deploy_FTD

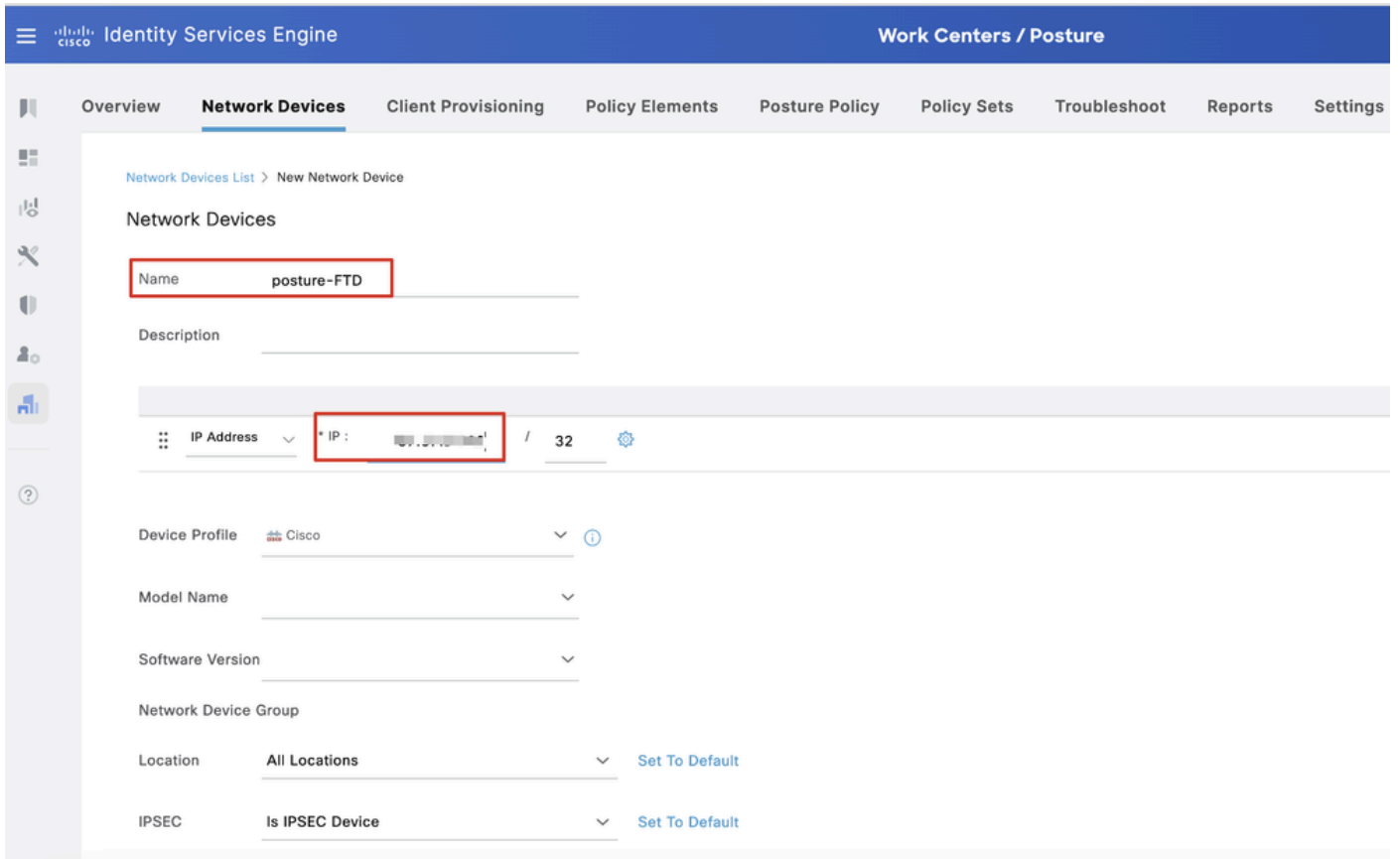
Configuraciones en ISE

Paso 13. Desplácese hasta Work Centers > Posture > Network Devices. Haga clic en Add.



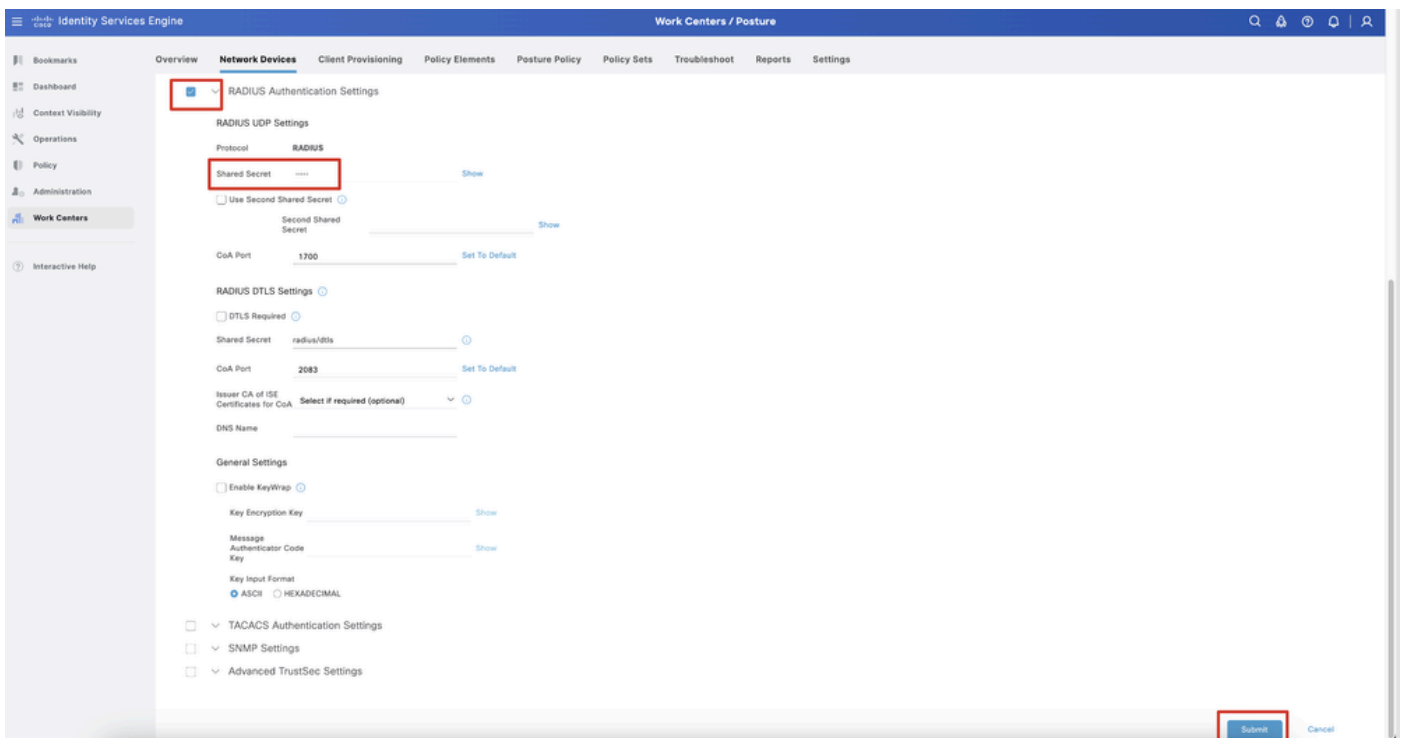
ISE_Add_New_Devices

Paso 13.1. Proporcione el Name, IP Addressy desplácese hacia abajo por la página.



ISE_Add_New_Devices_1

Paso 13.2. Marque la casilla de verificación de RADIUS Authentication Settings. Proporcione el Shared Secret. Haga clic en Submit.



ISE_Add_New_Devices_2

Paso 14. Descargue el nombre del paquete `cisco-secure-client-linux64-4.3.3139.0-isecompliance-webdeploy-k9.pkg` de [Descarga de Software de Cisco](#) y asegúrese de que el archivo sea bueno confirmando que la suma de comprobación md5 del archivo descargado es la misma que la página

de Descarga de Software de Cisco. El nombre del paquete cisco-secure-client-linux64-5.1.3.62-webdeploy-k9.pkg se ha descargado correctamente en el paso 1.

Paso 15. Desplácese hasta Work Centers > Posture > Client Provisioning > Resources. Haga clic en Add. Seleccione Agent resources from local disk.

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 'Resources' under 'Client Provisioning Policy'. The main content area is titled 'Resources' and shows a table of resources. A dropdown menu is open under the '+ Add' button, with 'Agent resources from local disk' selected. The table lists various resources with columns for Type, Version, Last Update, and Description.

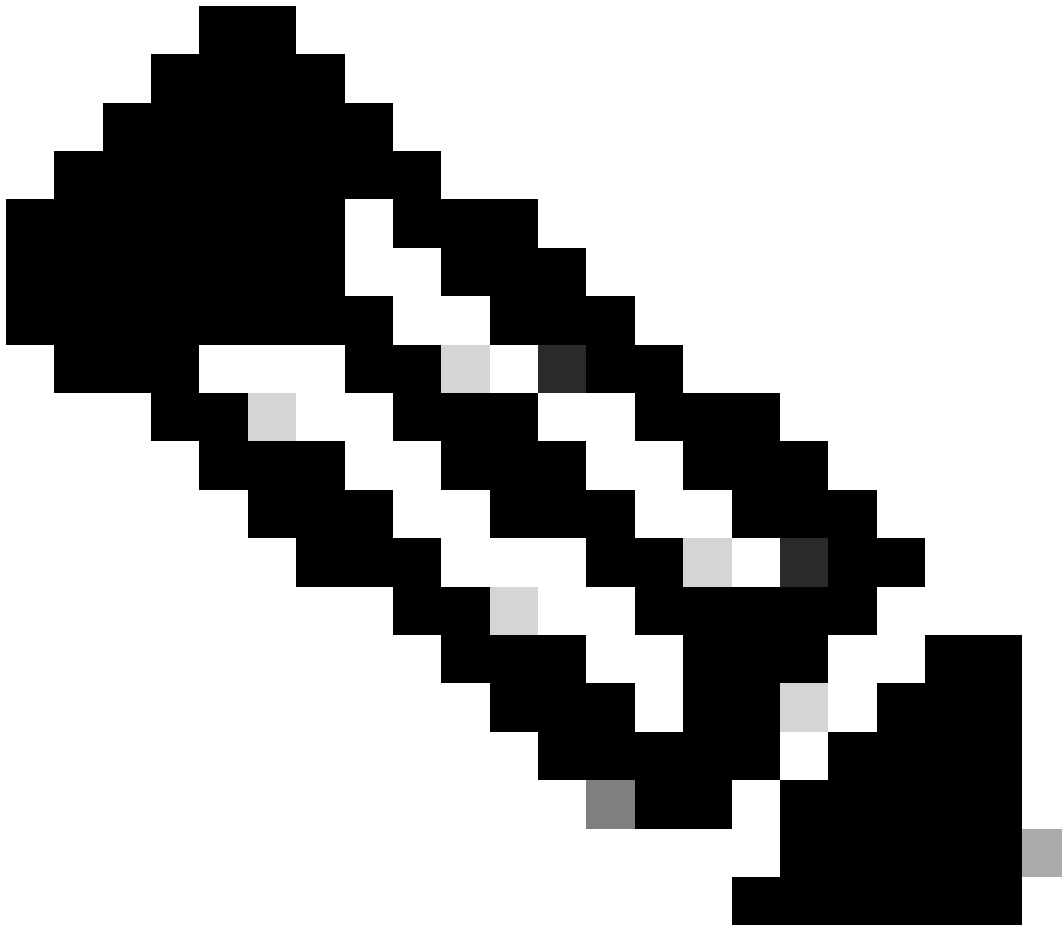
Type	Version	Last Update	Description
WinSPWizard	3.2.0.1	2023/07/04 06:54:02	Supplicant Pro...
Native Supplicant Pro...	Not Applic...	2016/10/07 04:01:12	Pre-configur...
Native Supplicant Pro...	Not Applic...	2023/07/04 07:55:16	Pre-configur...
MacOsXSPWizard	2.7.0.1	2023/07/04 06:54:02	Supplicant Pro...
CiscoSecureClientDe...	5.1.3.62	2024/05/08 10:20:06	Cisco Secure C...
CiscoSecureClientDe...	5.1.3.62	2024/05/08 10:31:28	Cisco Secure C...
CiscoSecureClientCo...	4.3.4015...	2024/05/08 10:26:57	Cisco Secure C...
CiscoSecureClientCo...	4.3.3139.0	2024/05/08 10:34:00	Cisco Secure C...
CiscoAgentlessWind...	5.0.3061.0	2023/07/04 06:54:10	With CM: 4.3.3
CiscoAgentlessOSX	5.0.3061.0	2023/07/04 06:54:14	With CM: 4.3.3
CiscoTemporalAgent...	5.0.3061.0	2023/07/04 06:54:03	With CM: 4.3.3
CiscoTemporalAgent...	5.0.3061.0	2023/07/04 06:54:07	With CM: 4.3.3

ISE_Upload_Resource

Paso 15.1. Seleccione Cisco Provided Package. Haga clic Choose File para cargar cisco-secure-client-linux64-5.1.3.62-webdeploy-k9.pkg. Haga clic en Submit.

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 'Work Centers' selected. The left sidebar shows 'Work Centers' under 'Administration'. The main content area is titled 'Agent Resources From Local Disk' and shows a form for adding resources. The 'Category' dropdown is set to 'Cisco Provided Package'. The 'Choose File' button is highlighted, and the file name 'cisco-secure-...eploy-k9.pkg' is visible. Below the form, there is a table for 'Agent Uploaded Resources' with columns for Name, Type, Version, and Description. The 'Submit' button is highlighted.

Name	Type	Version	Description
CiscoSecureClientDeskto...	CiscoSecureClientDe...	5.1.3.62	Cisco Secure Client for li...



Nota: Repita el paso 14 para cargar cisco-secure-client-linux64-4.3.3139.0-isecompliance-webdeploy-k9.pkg .

Paso 16. Desplácese hasta Work Centers > Posture > Client Provisioning > Resources. Haga clic en Add. Seleccione Agent Posture Profile.

Work Centers / Posture

Client Provisioning

Resources

Selected 0 Total 16

	Version	Last Update	Description
Agent resources from Cisco site			
Agent resources from local disk	oSecureClientDe...	5.1.3.62 2024/05/08 10:31:28	Cisco Secure Client for li...
Native Supplicant Profile	ve Supplicant Pro...	Not Applic... 2016/10/07 04:01:12	Pre-configured Native S...
Agent Configuration	oSecureClientCo...	4.3.3139.0 2024/05/08 10:34:00	Cisco Secure Client Linu...
Agent Posture Profile	ntProfile	Not Applic... 2024/05/08 10:37:17	
AMP Enabler Profile	ntProfile	Not Applic... 2024/05/16 15:15:49	

ISE_Add_Agent_Posture_Profile

Paso 16.1. Proporcione el Name, Server name rules y mantenga el resto como predeterminado. Haga clic en Save.

Nombre: linux_agent_profile

Reglas de nombre de servidor: *.example.com

Work Centers / Posture

Client Provisioning

ISE Posture Agent Profile Settings > New Profile

Agent Posture Profile

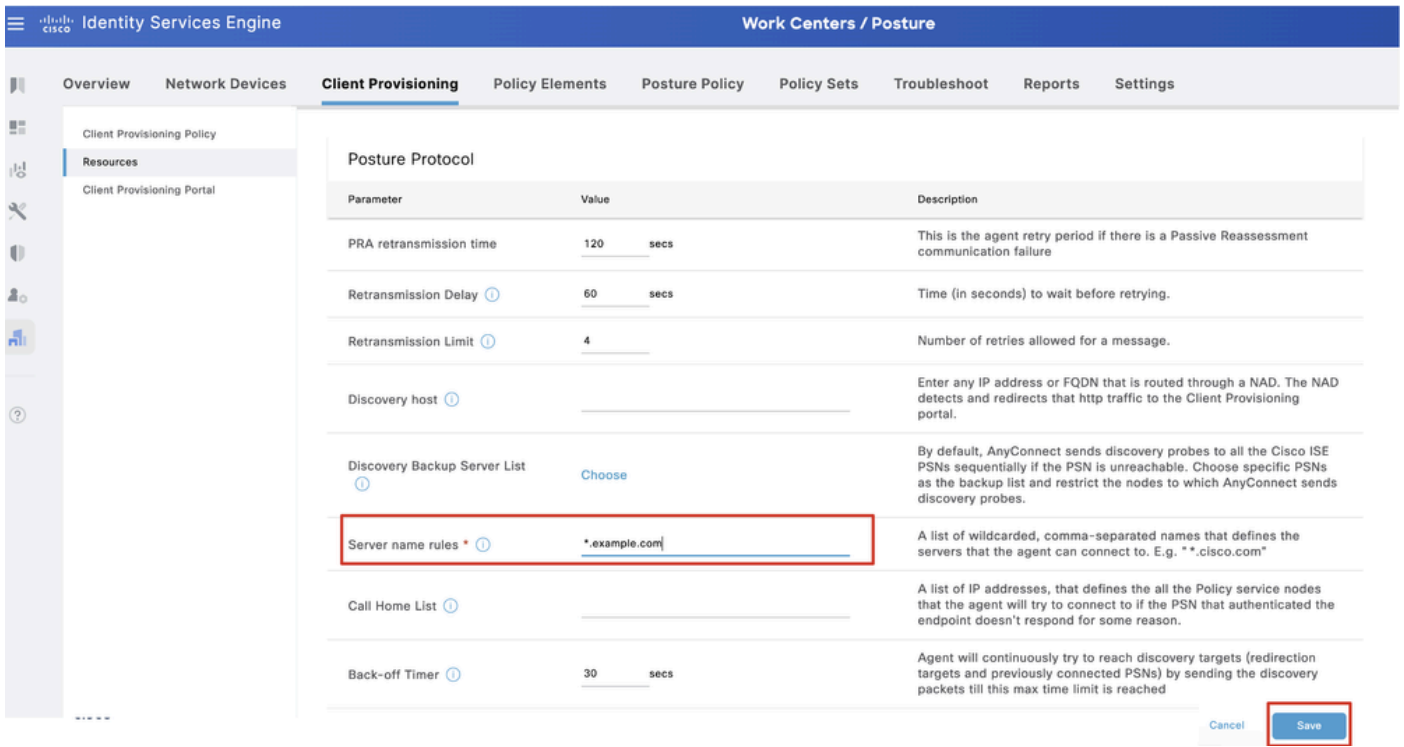
Name *
linux_agent_profile

Description:

Agent Behavior

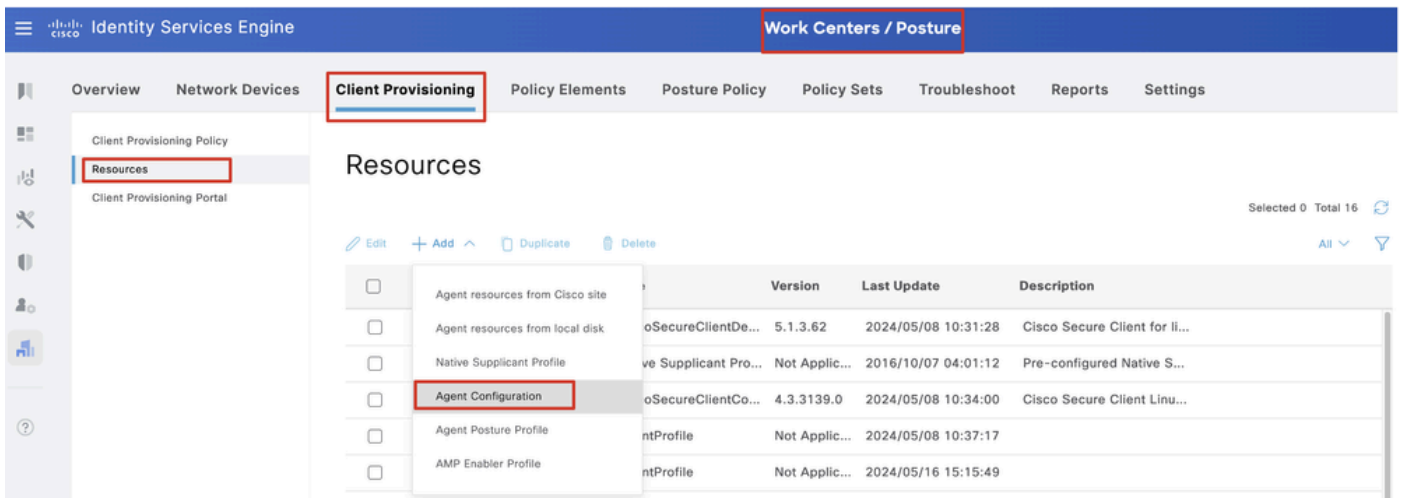
Parameter	Value	Description
Enable debug log	No	Enables the debug log on the agent

ISE_Add_Agent_Posture_Profile_1



ISE_Add_Agent_Posture_Profile_2

Paso 17. Desplácese hasta Work Centers > Posture > Client Provisioning > Resources. Haga clic en Add. Seleccione Agent Configuration.



ISE_Add_Agent_Configuration

Paso 17.2. Configure los detalles:

Seleccionar paquete de agente: CiscoSecureClientDesktopLinux 5.1.3.062

Nombre: linux_agent_config

Módulo de cumplimiento: CiscoSecureClientComplianceModuleLinux 4.3.3139.0

Marque la casilla de verificación de VPN, Diagnostic and Reporting Tool

Posición de ISE para la selección de perfiles: linux_agent_profile

Haga clic en 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

Paso 18. Desplácese hasta Work Centers > Posture > Client Provisioning > Client Provisioning Policy. Haga clic Edit al final de cualquier número de regla. Seleccione 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
<input checked="" type="checkbox"/> IOS	If Any	and Apple iOS All	and Condition(s)	then Cisco-ISE-NSP Edit
<input checked="" type="checkbox"/> Android	If Any	and Android	and Condition(s)	then Cisco-ISE-NSP Edit

Duplicate above

Duplicate below

Insert new policy above

[Insert new policy below](#)

Delete

ISE_Add_New_Provisioning_Policy

Paso 18.1. Configure los detalles:

Nombre de regla: Linux

Sistemas operativos: Linux All

Resultados: linux_agent_config

Haga clic en Done y Save.

The screenshot shows the Cisco Identity Services Engine (ISE) interface for configuring a Client Provisioning Policy. The page title is "Client Provisioning Policy". Below the title, there is a description: "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." Below this, there is a table with columns: Rule Name, Identity Groups, Operating Systems, Other Conditions, and Results. The table contains three rows: IOS, Android, and Linux. The Linux row is highlighted with a red box. The Linux row details are: Rule Name: Linux, Identity Groups: If Any, Operating Systems: and Linux All, Other Conditions: and Condition(s), Results: then linux_agent_config, and an Edit button.

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

Paso 19. Desplácese hasta Work Centers > Posture > Policy Elements > Conditions > File. Haga clic en Add.

The screenshot shows the Cisco Identity Services Engine (ISE) interface for configuring File Conditions. The page title is "File Conditions". Below the title, there is a table with columns: Name, Description, File name, and Condition Type. The table contains 18 rows of predefined checks. The "Add" button is highlighted with a red box. The "Add" button is located in the top right corner of the table area, next to the "View", "Edit", "Duplicate", and "Delete" buttons.

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\winsxsl...	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\Scrren.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

Paso 19.1. Configure los detalles:

Nombre: linux_demo_file_exist

Sistemas operativos: Linux All

Tipo de archivo: FileExistence

Ruta del archivo: inicio, Desktop/test.txt

Operador de archivos: existe

Haga clic en 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 is located at the bottom right of the form.

ISE_Add_New_File_Condition_1

Paso 20. Desplácese hasta Work Centers > Posture > Policy Elements > Requirements. Haga clic Edit al final de cualquier nombre de regla. Seleccione 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

Paso 20.1. Configurar los detalles:

Nombre: Test_exist_linux

Sistemas operativos: Linux All

Módulo de cumplimiento: 4.x o posterior

Tipo de postura: Agente

Condiciones: linux_demo_file_exist

Haga clic en Done y 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



Nota: A partir de ahora, sólo se admiten scripts de shell para los agentes Linux como solución.

Paso 21. Desplácese hasta Work Centers > Posture > Policy Elements > Authorization Profiles. Haga clic en Add.

Paso 21.1. Configure los detalles:

Nombre: unknown_redirect

Marque la casilla de verificación de Web Redirection(CWA,MDM,NSP,CPP)

Seleccionar Client Provisioning(Posture)

ACL: redirección

Valor: Client Provisioning Portal (predeterminado)

The screenshot shows the Cisco Identity Services Engine (ISE) configuration interface. The top navigation bar includes 'Work Centers / Posture'. The main navigation tabs are 'Overview', 'Network Devices', 'Client Provisioning', 'Policy Elements', 'Posture Policy', 'Policy Sets', 'Troubleshoot', 'Reports', and 'Settings'. The 'Policy Elements' tab is selected, and the 'Authorization Profile' configuration page is displayed. The profile name is 'unknown_redirect'. The 'Access Type' is set to 'ACCESS_ACCEPT'. The 'Network Device Profile' is 'Cisco'. Under 'Common Tasks', 'Web Redirection (CWA, MDM, NSP, CPP)' is checked, and the ACL is set to 'redirect'. The 'Value' is 'Client Provisioning Portal (defi...'. The left sidebar shows various configuration categories, with 'Authorization Profiles' highlighted.

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

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

Authorization Profile

* Name **unknown_redirect**

Description

* Access Type **ACCESS_ACCEPT**

Network Device Profile Cisco

Service Template

Track Movement

Agentless Posture

Passive Identity Tracking

Common Tasks

- Voice Domain Permission
- Web Redirection (CWA, MDM, NSP, CPP)**
- Static IP/Host name/FQDN
- Suppress Profiler CoA for endpoints in Logical Profile

Client Provisioning (Posture) ACL **redirect** Value Client Provisioning Portal (defi...)

ISE_Add_New_Authorization_Profile_Redirect_1



Nota: Esta redirección de nombre de ACL debe coincidir con el nombre de ACL correspondiente configurado en FTD.

Paso 21.2. Repita el Add para crear otros dos perfiles de autorización para terminales no conformes y conformes con los detalles.

Nombre: non_compliance_profile

Nombre de DACL: DENY_ALL_IPv4_TRAFFIC

Nombre: compliance_profile

Nombre de DACL: PERMIT_ALL_IPv4_TRAFFIC



Nota: La DACL para terminales conformes o no conformes debe configurarse según los requisitos reales.

Paso 22. Desplácese hasta Work Centers > Posture > Posture Policy. Haga clic Edit al final de las reglas. Seleccione Insert new policy.

Identity Services Engine Work Centers / Posture

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

Posture Policy Guide Me

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

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 - Duplicate
<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_AppViz_Policy_Mac	If Any	and Mac OSX	and 4.x or later	and Agent	and	then Default_AppViz_Requirement_Mac	Edit - Duplicate
<input type="checkbox"/>	Policy Options	Default_AppViz_Policy_Mac_temporal	If Any	and Mac OSX	and 4.x or later	and Temporal Agent	and	then Default_AppViz_Requirement_Mac_temporal	Edit - Duplicate
<input type="checkbox"/>	Policy Options	Default_AppViz_Policy_Win	If Any	and Windows All	and 4.x or later	and Agent	and	then Default_AppViz_Requirement_Win	Edit - Duplicate
<input type="checkbox"/>	Policy Options	Default_AppViz_Policy_Win_temporal	If Any	and Windows All	and 4.x or later	and Temporal Agent	and	then Default_AppViz_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

Paso 22.1. Configure los detalles:

Nombre de regla: Demo_test_exist_linux

Grupos de identidades: Cualquiera

Sistemas operativos: Linux All

Módulo de cumplimiento: 4.x o posterior

Tipo de postura: Agente

Requisitos: Test_exist_linux

Haga clic en Done y 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

Paso 23. Desplácese hasta Work Centers > Posture > Policy Sets. Haga clic para Insert new row above.

Identity Services Engine Work Centers / Posture

Work Centers / Posture

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](#)

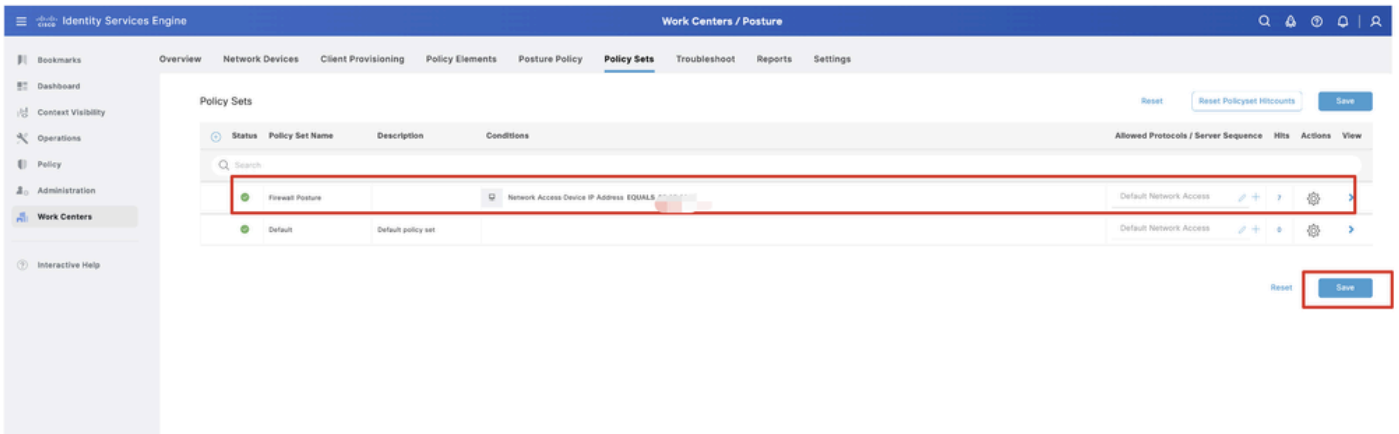
ISE_Add_New_Policy_Set

Paso 23.1. Configure los detalles:

Nombre del conjunto de políticas: Estado del firewall

Condiciones: Dispositivo de acceso a la red Dirección IP EQUALs [Dirección IP FTD]

Haga clic Save .



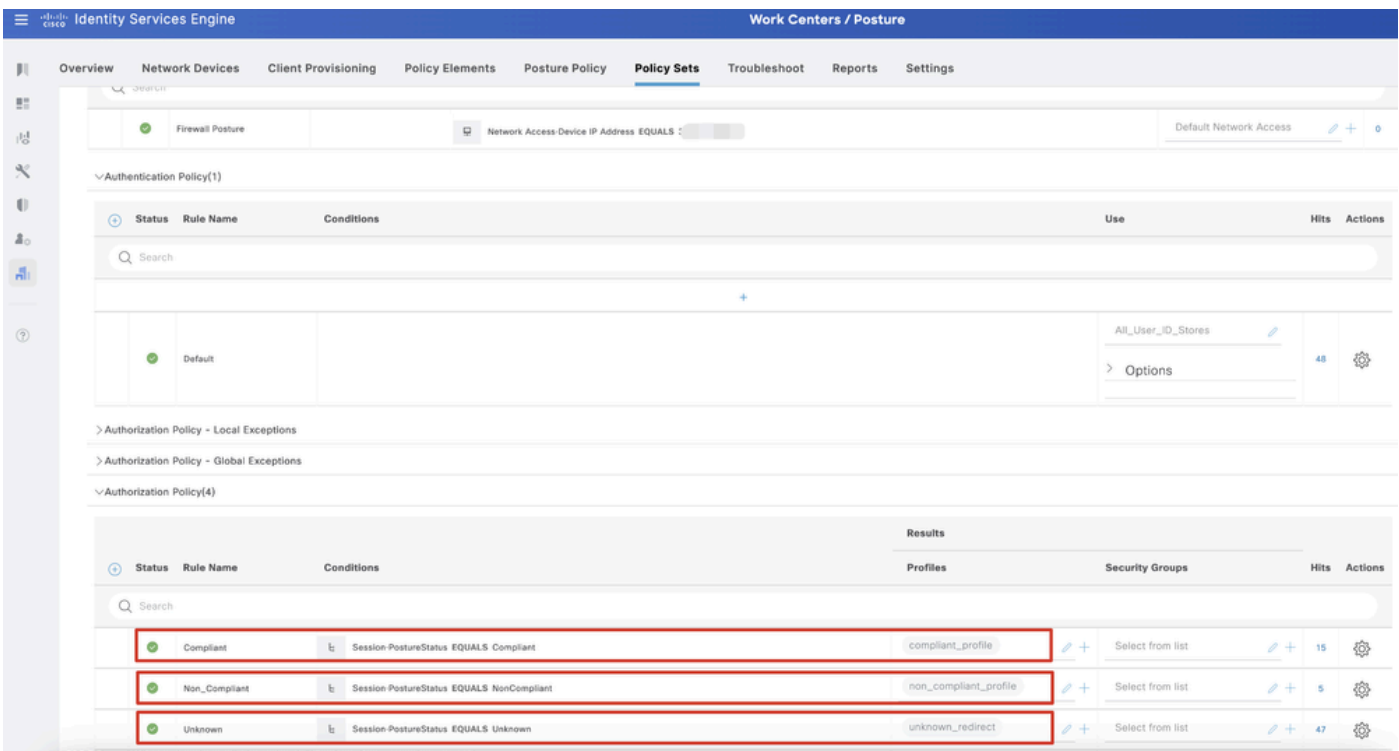
ISE_Add_New_Policy_Set_1

Paso 23.2. Haga clic > para introducir el conjunto de políticas. Crear nuevas reglas de autorización para estados conformes al estado, no conformes y desconocidos. Haga clic en Save.

De conformidad con compliance_profile

No conforme con non_compliance_profile

Desconocido con unknown_redirect



ISE_Add_New_Policy_Set_2

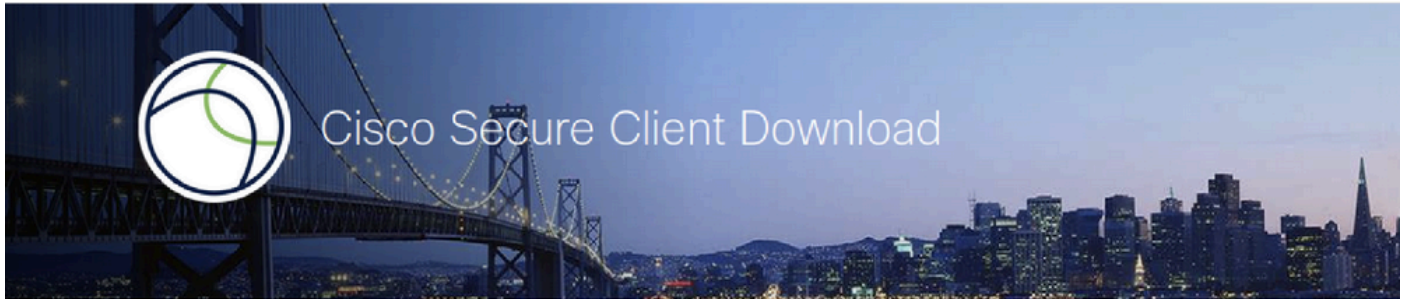
Configuraciones en Ubuntu

Paso 24. Inicie sesión en el cliente Ubuntu mediante la GUI. Abra el explorador para iniciar sesión en el portal VPN. En este ejemplo, es demo.example.com.

A screenshot of a "Logon" dialog box. The dialog box 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

Paso 25. Haga clic en Download for Linux.



Download & Install

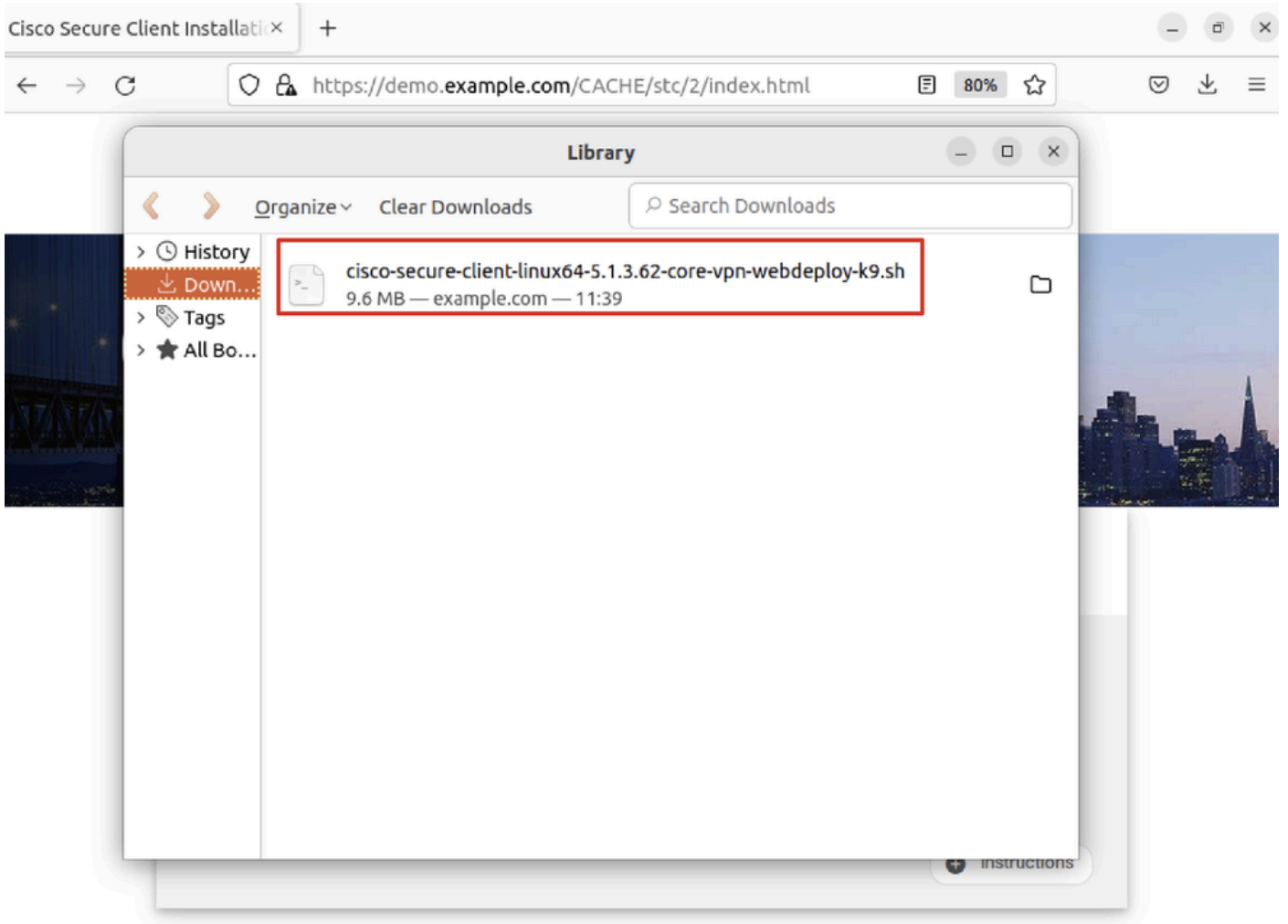
Download Cisco Secure Client and install it on your computer.

[Download for Linux](#)

[+ Instructions](#)

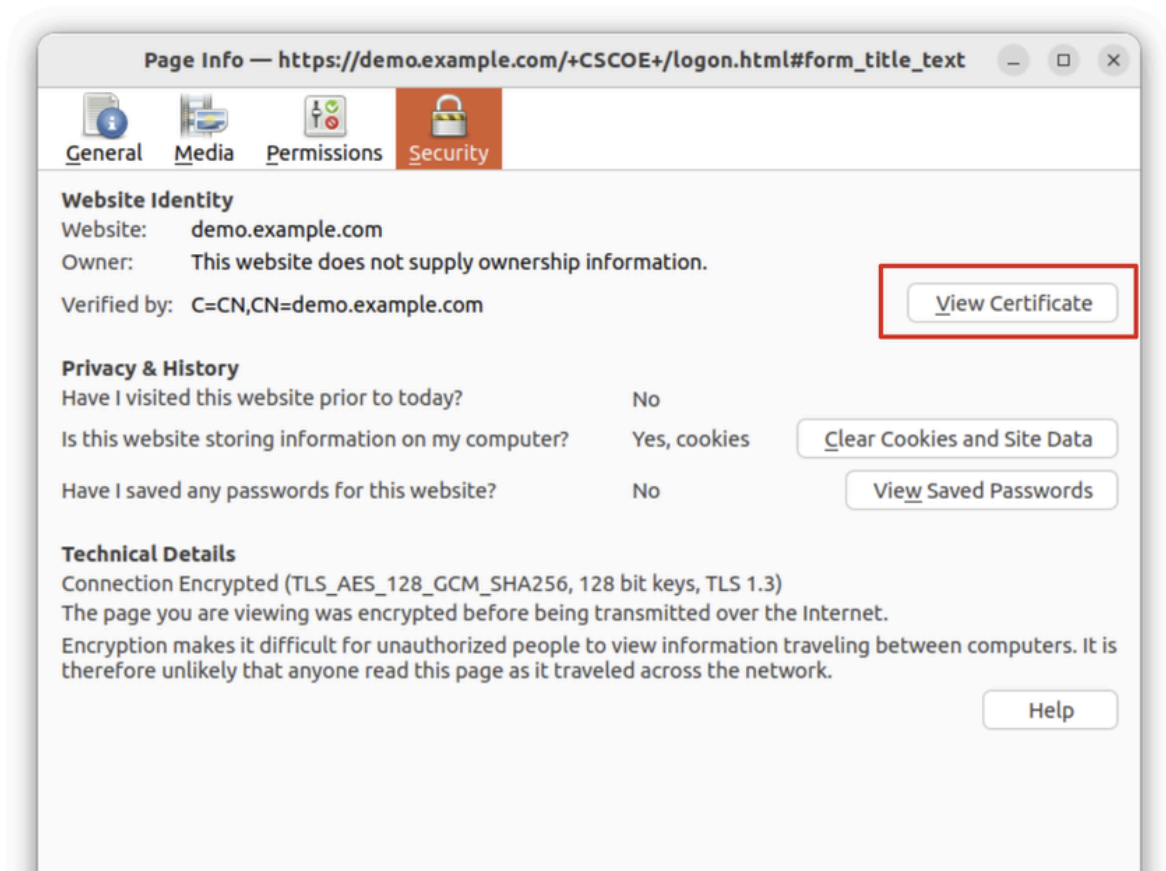
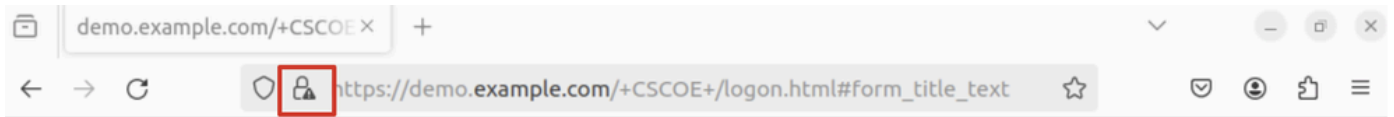
Ubuntu_Browser_VPN_Download_1

El nombre del archivo descargado es cisco-secure-client-linux64-5.1.3.62-core-vpn-webdeploy-k9.sh.



Ubuntu_Browser_VPN_Download_2

Paso 26. Descargue el certificado VPN a través del navegador y cambie el nombre del archivo a <certificate>.crt. Este es el ejemplo de cómo usar firefox para descargar el certificado.



Ubuntu_Browser_VPN_Cert_Download

Paso 27. Abra el terminal en el cliente Ubuntu. Desplácese hasta path `home/user/Downloads/` para instalar 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$
```

Paso 28. Confíe en el certificado del portal VPN en el 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...
```

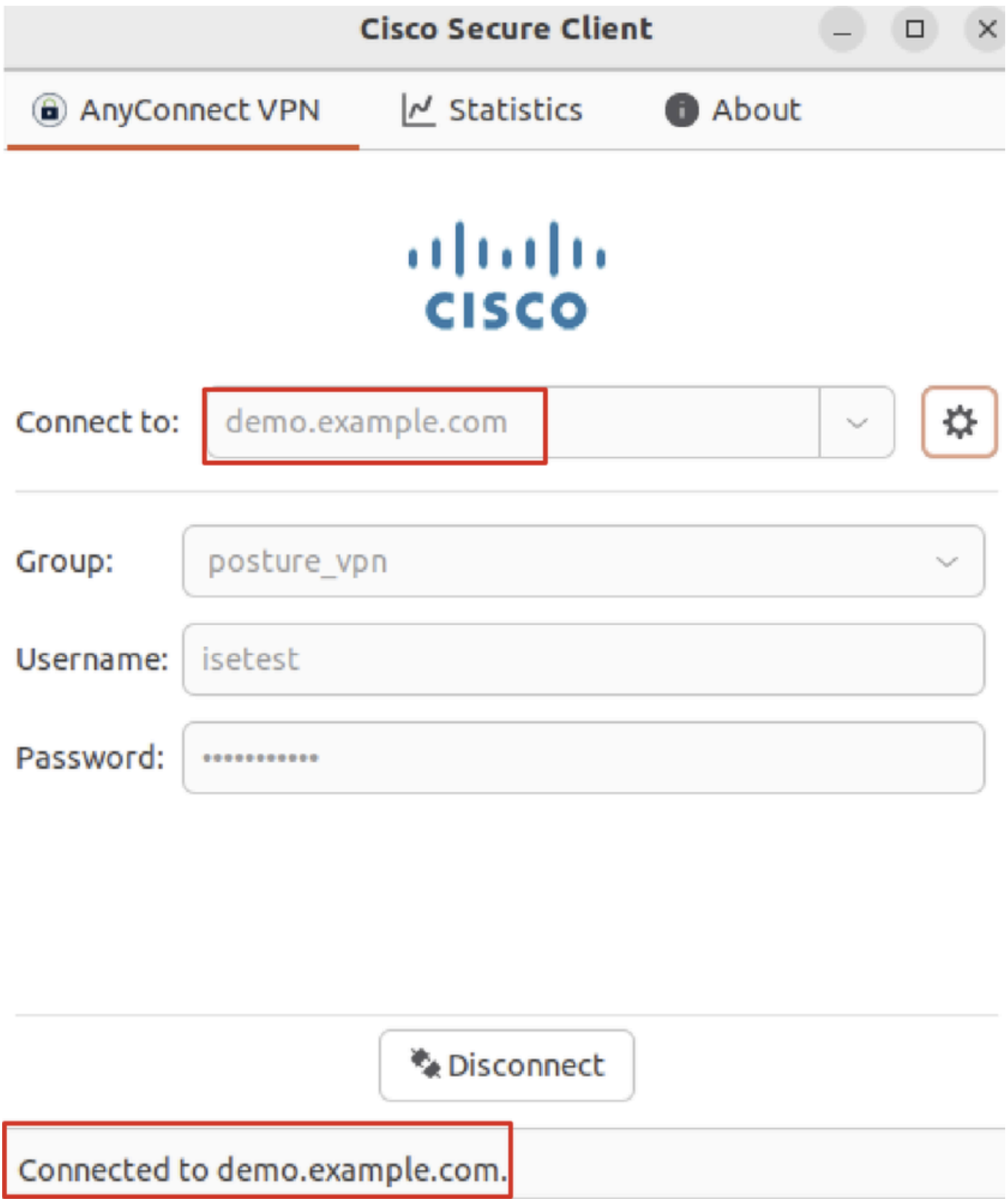
```
done.
```

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

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

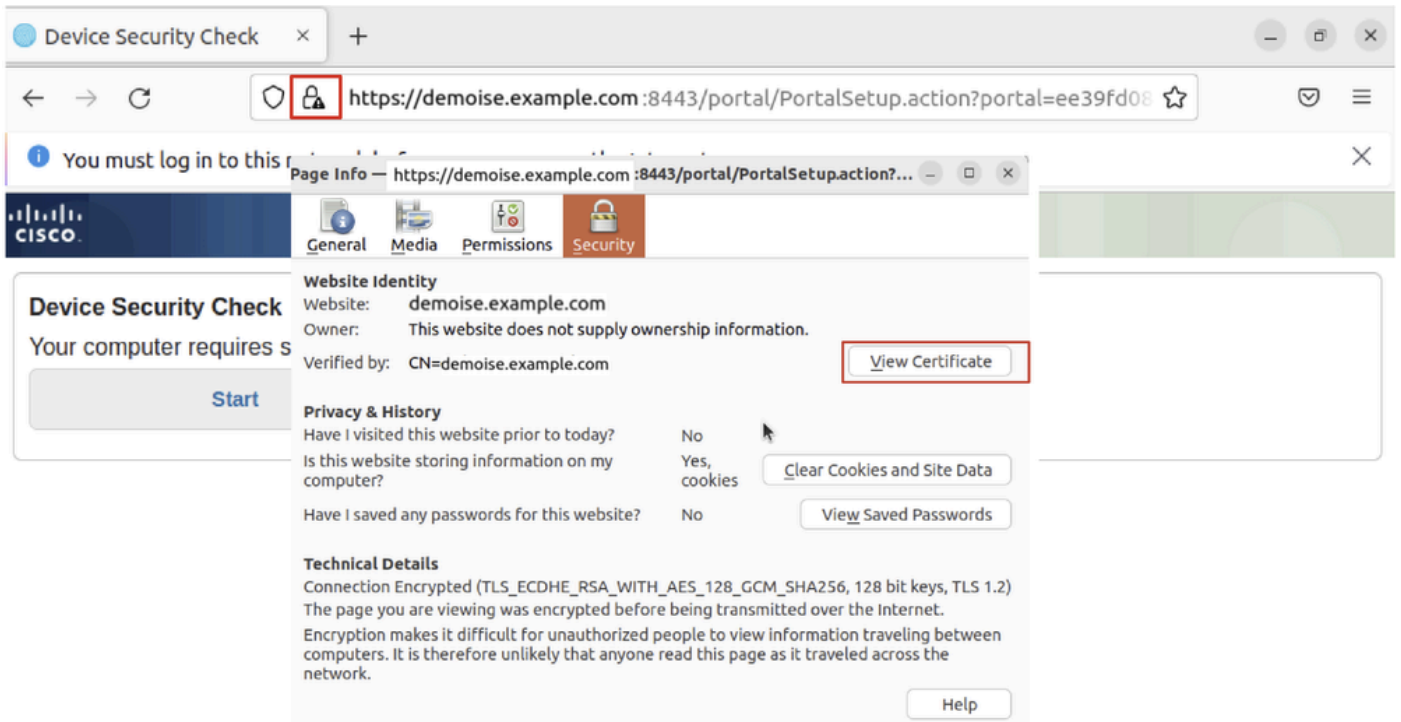
```
demo-example-com.crt: OK
```

Paso 29. Abra Cisco Secure Client en el cliente Ubuntu y conecte VPN a demo.example.com correctamente.



Ubuntu_Secure_Client_Connected

Paso 30. Abra el navegador para acceder a cualquier sitio web que active la redirección al portal ISE CPP. Descargue el certificado del portal ISE CPP y cambie el nombre del archivo a <certificate>.crt. Este es un ejemplo del uso de Firefox para la descarga.



Ubuntu_Browser_CPP_Cert_Download

Paso 30.1. Confíe en el certificado del portal CPP de ISE en el 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
```

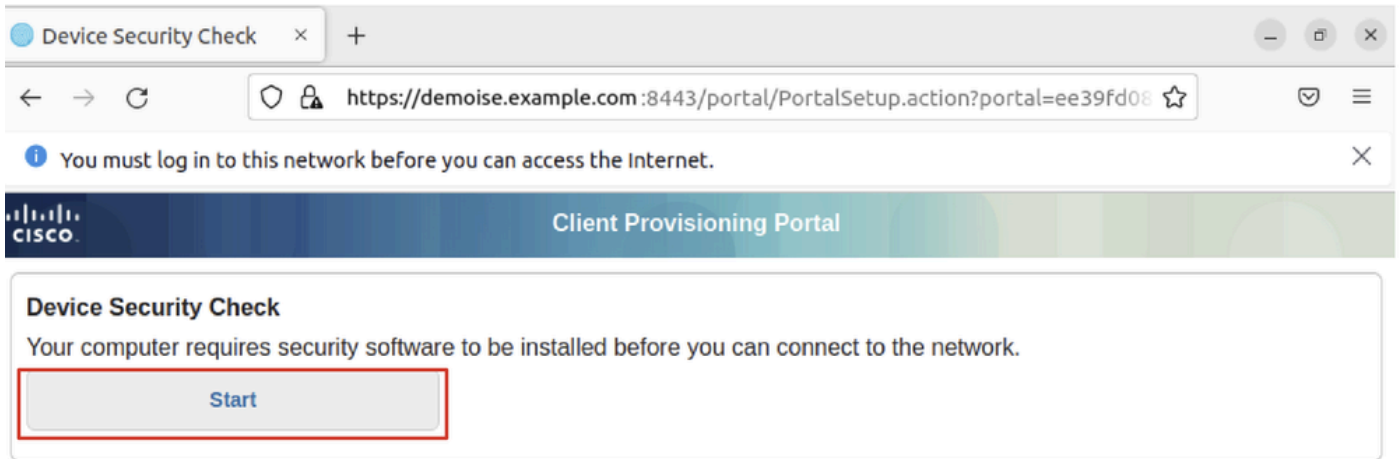
```
1 added
```

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

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

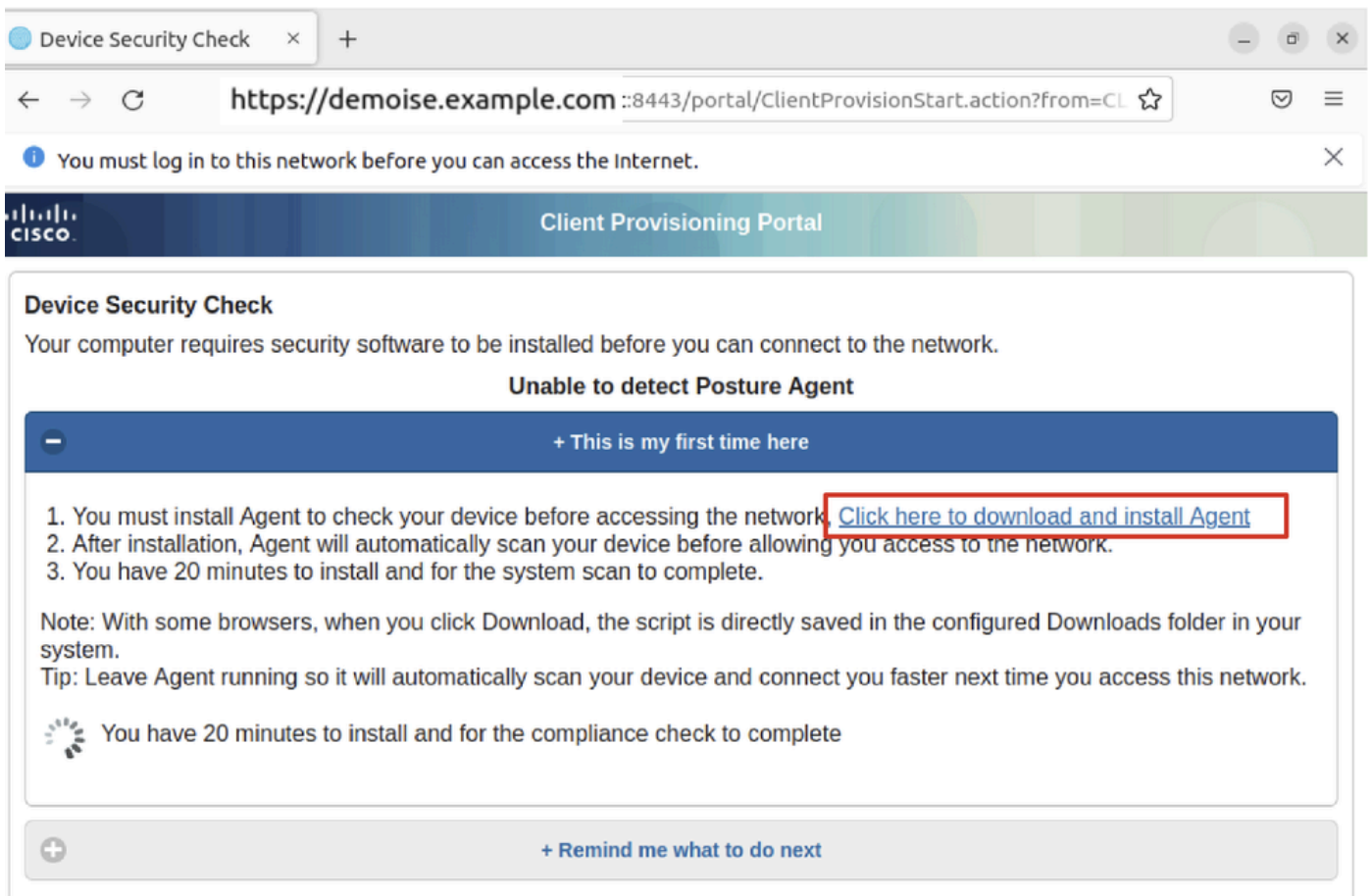
```
done.
```

Paso 31. Haga clic Start en el portal de ISE CPP.



Ubuntu_Browser_CPP_Start

Paso 32. Click here to download and install Agent.



Ubuntu_Browser_CPP_Download_Posture

Paso 33. Abra el terminal en el cliente Ubuntu. Vaya a la ruta home/user/Downloads/ para instalar el módulo de estado.

<#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.

Paso 34. En la interfaz de usuario del cliente de Ubuntu, salga de Cisco Secure Client y vuelva a abrirlo. El módulo de estado de ISE se ha instalado y se ha ejecutado correctamente.



Ubuntu_Secure_Client_ISE_Posture_Installed

Paso 35. Abra el terminal en el cliente Ubuntu. Navegue hasta `rutahome/user/Desktop` , cree un `test.txt` archivo para cumplir con la condición de archivo configurada en ISE.

```
<#root>
```

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

```
cd Desktop/
```

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

echo test > test.txt

Verificación

Utilice esta sección para confirmar que su configuración funcione correctamente.

Paso 1. Conecte VPN a demo.example.com en el 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 bottom of the window displays "Connected to demo.example.com."

Verify_Ubuntu_Secure_Client_Connected

Paso 2. Compruebe el estado de ISE en el cliente Ubuntu.



Network access allowed.



Verify_Ubuntu_Secure_Client_Compliant

Paso 3. Marque Radius Live Log en ISE. Desplácese hasta 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

Paso 4. Vaya a FTD CLI mediante SSH o la consola.

```
<#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

Troubleshoot

En esta sección se brinda información que puede utilizar para resolver problemas en su configuración.

Para ver el flujo de estado y la resolución de problemas de Cisco Secure Client e ISE, consulte los [documentos de CCOISE Posture Style Comparison for Pre and Post 2.2](#) y [Troubleshooting de ISE Session Management and Posture](#).

Información Relacionada

- [Compatibilidad de componentes de red de Cisco Identity Services Engine, versión 3.3](#)

- [Guía del administrador de Cisco Identity Services Engine, versión 3.3](#)
- [Soporte técnico y descargas de Cisco](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).