

# Configuration de la position VPN Linux avec ISE

## 3.3

### Table des matières

---

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Configurer](#)

[Diagramme du réseau](#)

[Configurations sur FMC/FTD](#)

[Configurations sur ISE](#)

[Configurations sur Ubuntu](#)

[Vérifier](#)

[Dépannage](#)

[Informations connexes](#)

---

## Introduction

Ce document décrit comment configurer la position VPN Linux avec Identity Services Engine (ISE) et Firepower Threat Defense (FTD).

## Conditions préalables

### Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Client sécurisé Cisco
- VPN d'accès à distance sur Firepower Threat Defense (FTD)
- Identity Services Engine (ISE)

### Composants utilisés

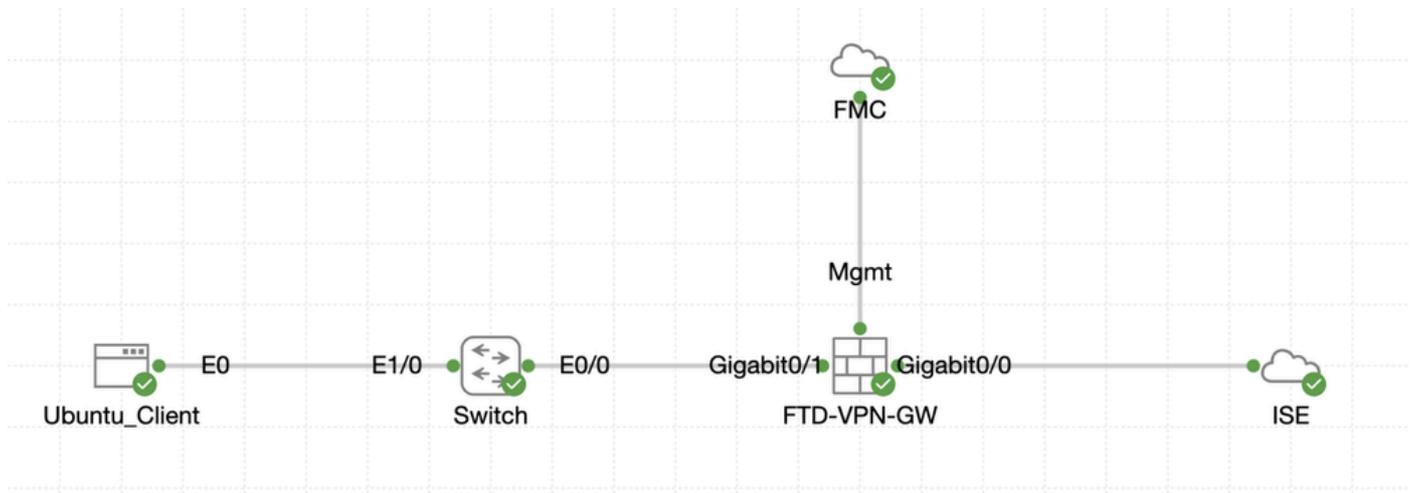
Les informations contenues dans ce document sont basées sur les versions de logiciel suivantes :

- 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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

## Configurer

### Diagramme du réseau



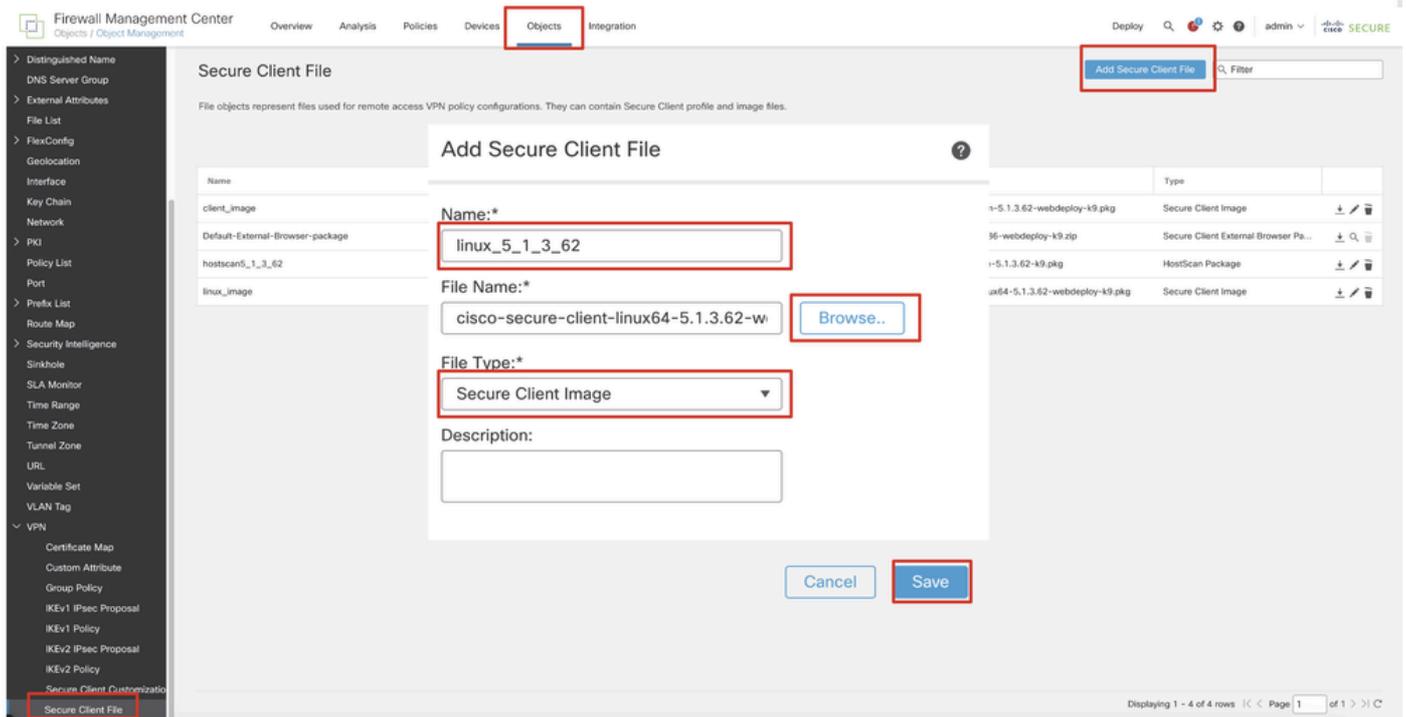
Topologie

### Configurations sur FMC/FTD

Étape 1. La connectivité entre le client, FTD, FMC et ISE a été correctement configurée. Comme [enroll.cisco.com](https://enroll.cisco.com) est utilisé pour les terminaux qui effectuent des tests de redirection (référez-vous aux [documents](#) CCO de flux de posture [Comparaison de style de posture ISE pour Pre et Post 2.2](#) pour plus de détails). Assurez-vous que la route du trafic vers [enroll.cisco.com](https://enroll.cisco.com) sur FTD est correctement configurée.

Étape 2. Téléchargez le nom `cisco-secure-client-linux64-5.1.3.62-webdeploy-k9.pkg` du package à partir de [Cisco Software Download](#) et assurez-vous que le fichier est correct après le téléchargement en confirmant que la somme de contrôle md5 du fichier téléchargé est identique à celle de la page Cisco Software Download.

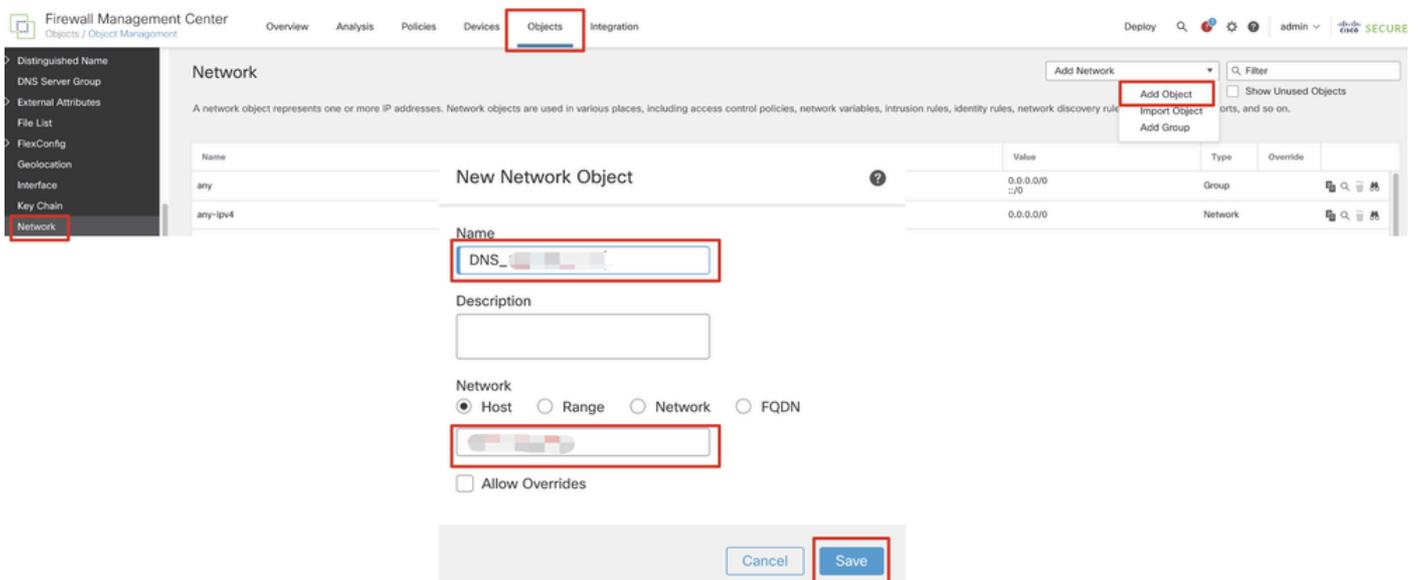
Étape 3. Accédez à **Objects > Object Management > VPN > Secure Client File**. Cliquez sur **Add Secure Client File**, indiquez le nom, recherchez **File Name** pour sélectionner `cisco-secure-client-linux64-5.1.3.62-webdeploy-k9.pkg`, sélectionnez **Secure Client Image** dans la liste déroulante **File Type**. Cliquez ensuite sur **Save**.



Image\_Client\_Sécurisé\_Téléchargement\_FMC

Étape 4. Accédez à Objects > Object Management > Network.

Étape 4.1. Créez un objet pour le serveur DNS. Cliquez sur Add Object, indiquez le nom et l'adresse IP DNS disponible. Cliquez sur Save.



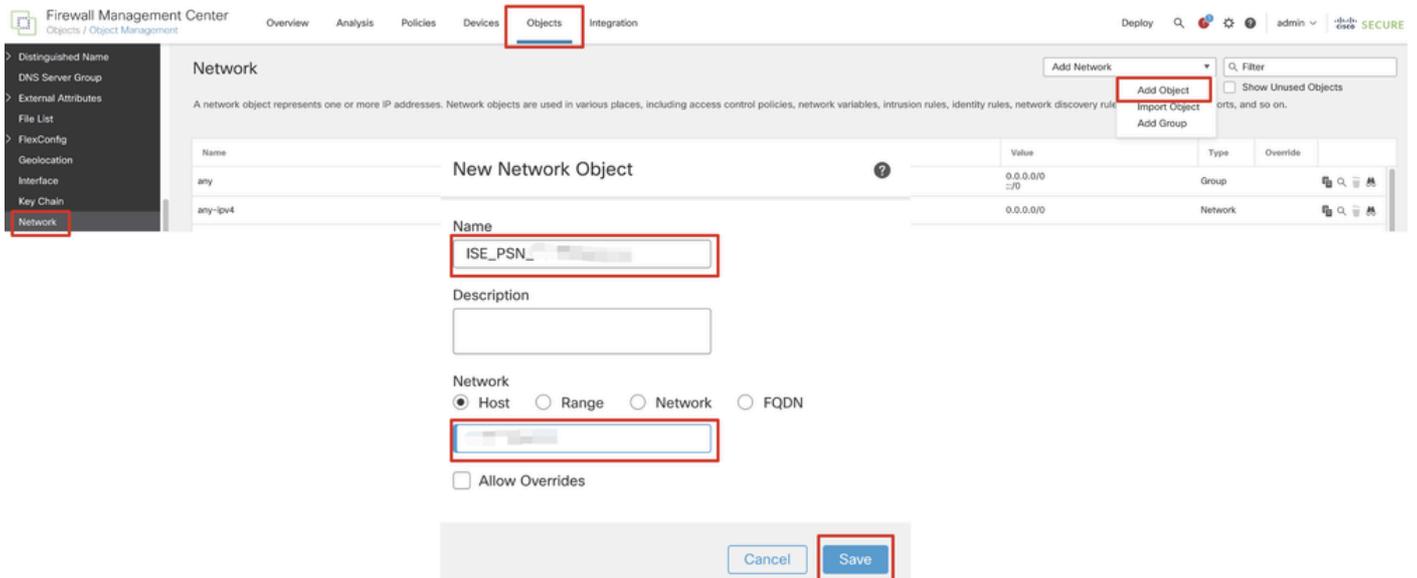
FMC\_Add\_Object\_DNS



**Remarque :** le serveur DNS configuré ici doit être utilisé pour les utilisateurs VPN.

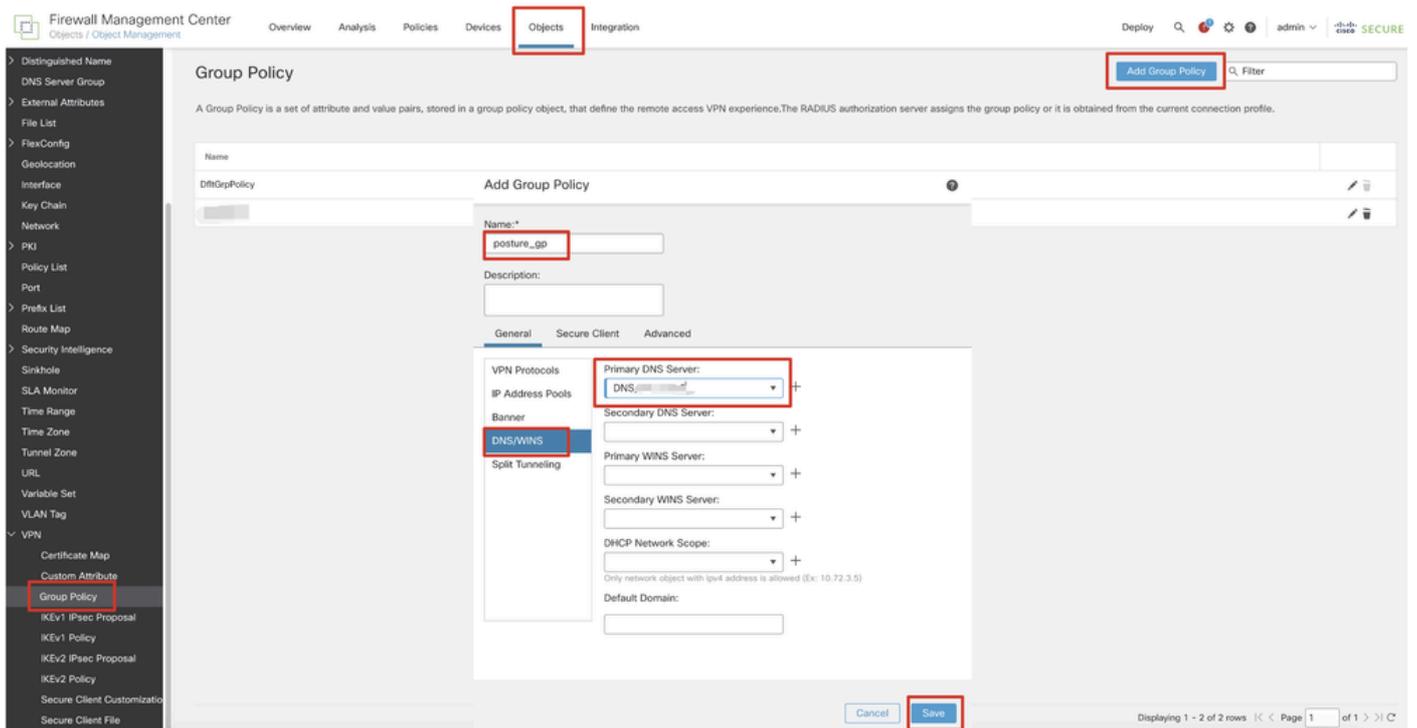
---

Étape 4.2. Créez un objet pour ISE PSN. Cliquez sur Add Object, indiquez le nom et l'adresse IP PSN ISE disponible. Cliquez sur Save.



FMC\_Add\_Object\_ISE

Étape 5. Accédez à Objects > Object Management > VPN > Group Policy. Cliquez sur Add Group Policy. Cliquez sur DNS/WINS, sélectionnez l'objet du serveur DNS dans Primary DNS Server. Cliquez ensuite sur Save.



FMC\_Add\_Group\_Policy

**Remarque :** assurez-vous que le serveur DNS utilisé dans la stratégie de groupe VPN peut résoudre le FQDN et le enroll.cisco.com du portail d'approvisionnement du client ISE.

Étape 6. Accédez à Objects > Object Management > Access List > Extended. Cliquez sur Add Extended Access List.

Firewall Management Center  
Objects / Object Management

Overview Analysis Policies Devices **Objects** Integration

Deploy 🔍 ⚙️ 👤 admin 🔒 **SECURE**

AAA Server  
RADIUS Server Group  
Single Sign-on Server  
**Access List**  
Extended

### Extended

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.

[Add Extended Access List](#) 🔍 Filter

Name	Value	Override
------	-------	----------

*FMC\_Add\_Redirect\_ACL*

Étape 6.1. Indiquez le nom de la liste de contrôle d'accès de redirection. Ce nom doit être le même que dans le profil d'autorisation ISE. Cliquez

sur 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

Étape 6.2. Bloquez le trafic DNS, le trafic vers l'adresse IP PSN ISE et les serveurs de conversion pour les exclure de la redirection. Autorisez le reste de la circulation. Cela déclenche la redirection. Cliquez sur 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

- 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) 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

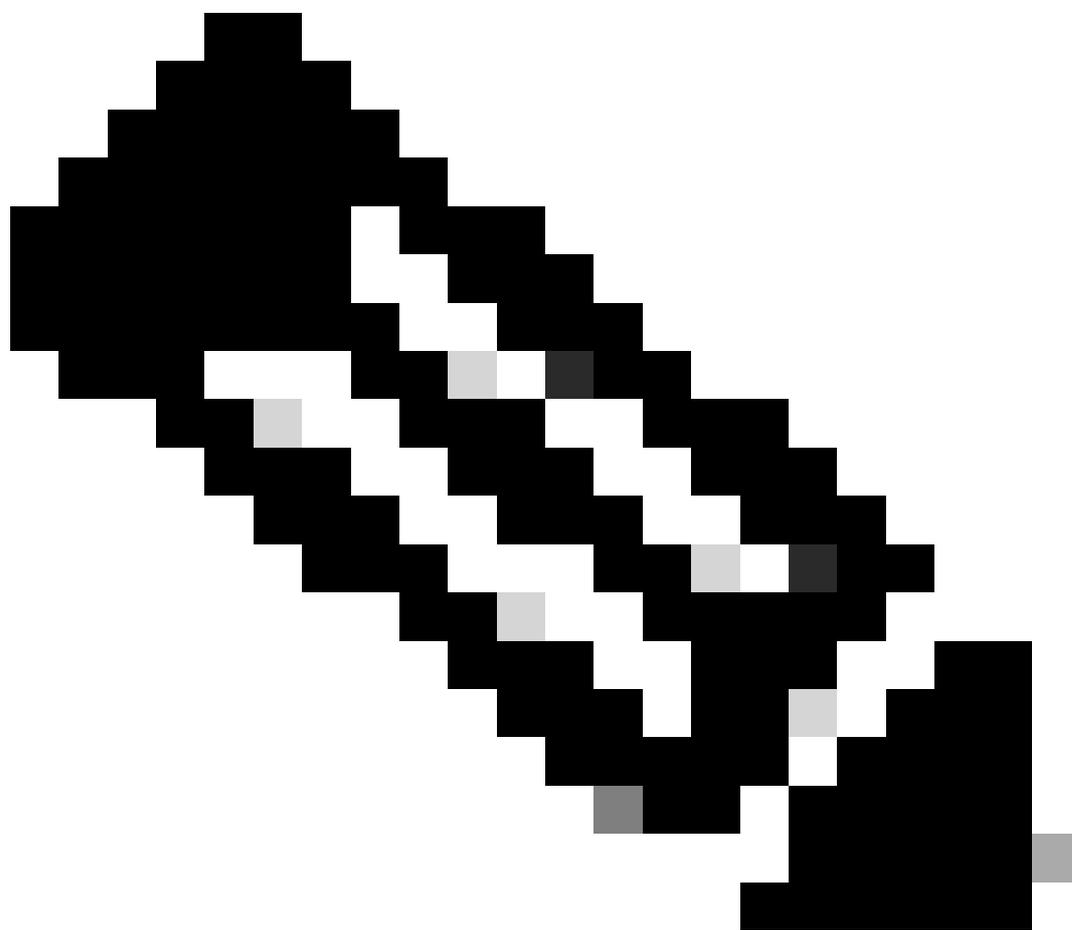
Sequence	Action	Source	Source Port	Destination	Destination Port	Application	Users	SGT	
1	Block	any-ipv4	Any	ISE_PSN_	Any	Any	Any	Any	
2	Block	Any	Any	Any	DNS_over_TCP DNS_over_UDP	Any	Any	Any	
3	Block	Any	Any	FTP_	Any	Any	Any	Any	
4	Allow	any-ipv4	Any	any-ipv4	Any	Any	Any	Any	

Allow Overrides

Cancel

Save

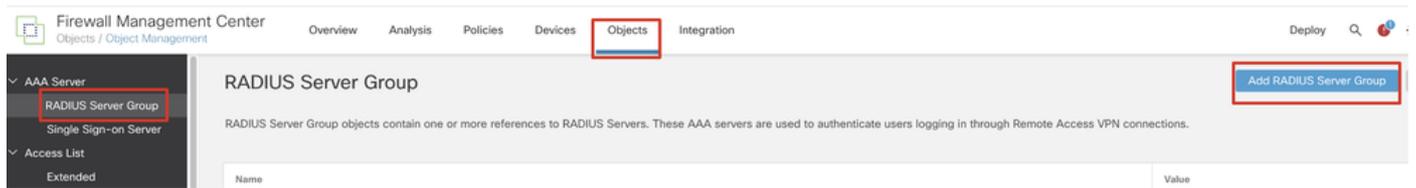
FMC\_Add\_Redirect\_ACL\_Part\_3



**Remarque :** le FTP de destination dans cet exemple de liste de contrôle d'accès de redirection est utilisé comme exemple de serveur

de conversion.

Étape 7. Accédez à Objects > Object Management > RADIUS Server Group. Cliquez sur Add RADIUS Server Group.



*FMC\_Add\_New\_Radius\_Server\_Group*

Étape 7.1. Indiquez le nom, la vérification Enable authorize only, la vérification Enable interim account update, la vérification 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

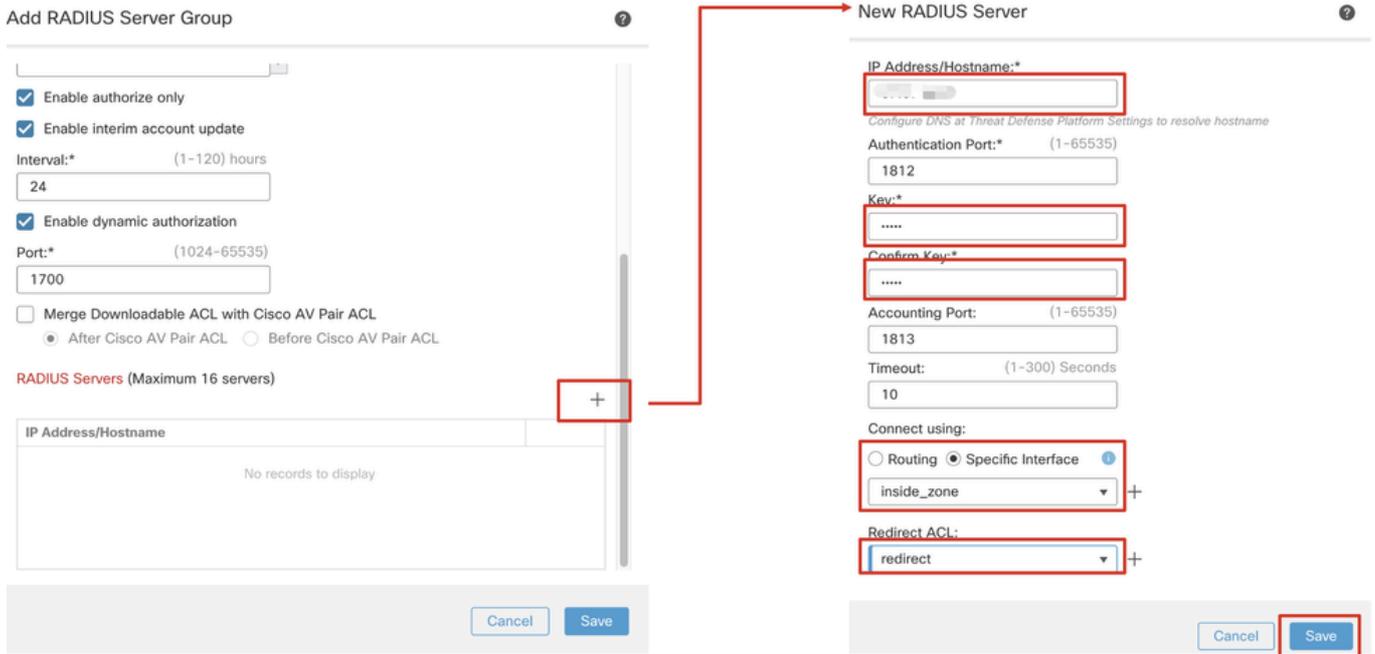
Port:\* (1024-65535)

Cancel

Save

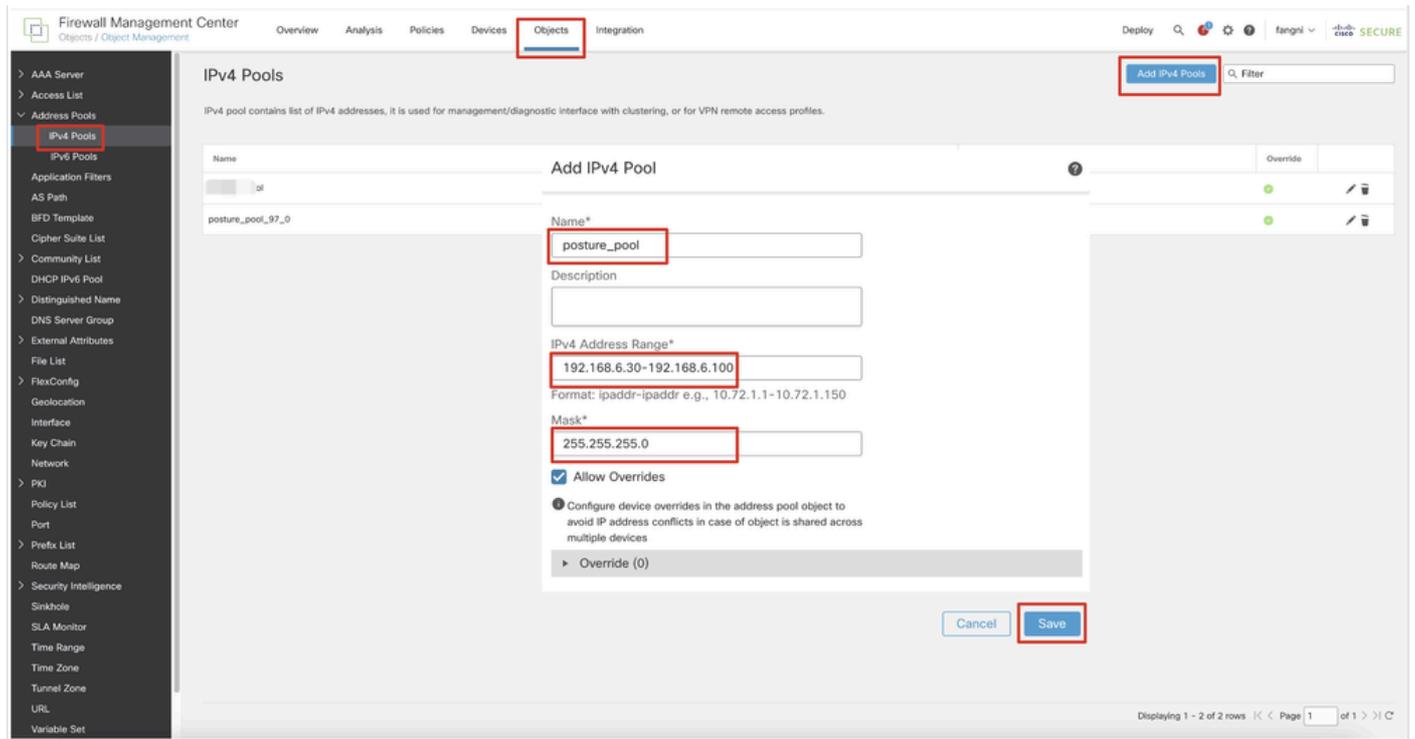
*FMC\_Add\_New\_Radius\_Server\_Group\_Part\_1*

Étape 7.2. Cliquez sur l'Plus icône pour ajouter un nouveau serveur RADIUS. Fournissez le PSN ISE IP Address/Hostname, Key. Sélectionnez le specific interface pour la connexion. Sélectionnez la Redirect ACL. Cliquez ensuite sur Save pour enregistrer le nouveau serveur RADIUS. Cliquez ensuite Save à nouveau sur pour enregistrer le nouveau groupe de serveurs RADIUS.



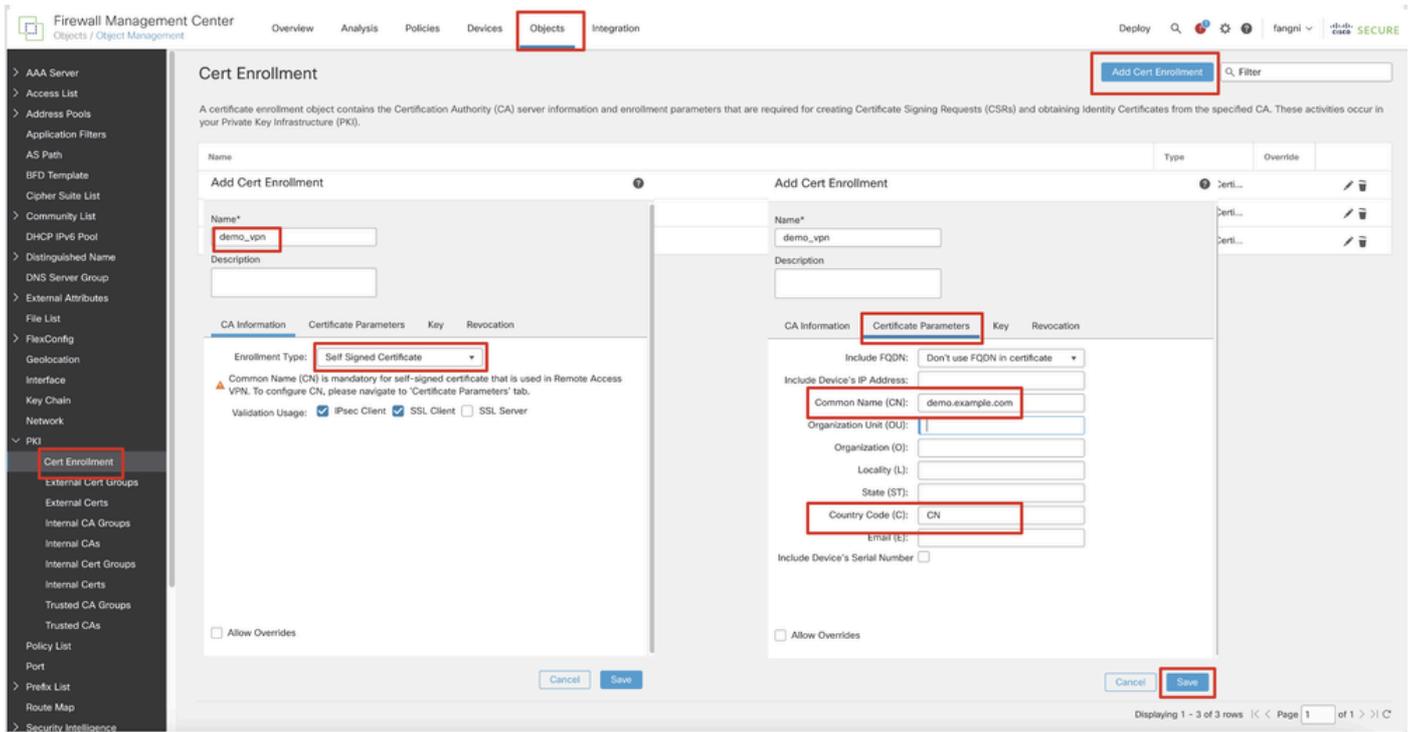
FMC\_Add\_New\_Radius\_Server\_Group\_Part\_2

Étape 8. Accédez à **Objects > Object Management > Address Pools > IPv4 Pools**. Cliquez sur **Add IPv4 Pools** et indiquez les **Name, IPv4 Address Rangeet Mask**. Cliquez ensuite sur **Save**.



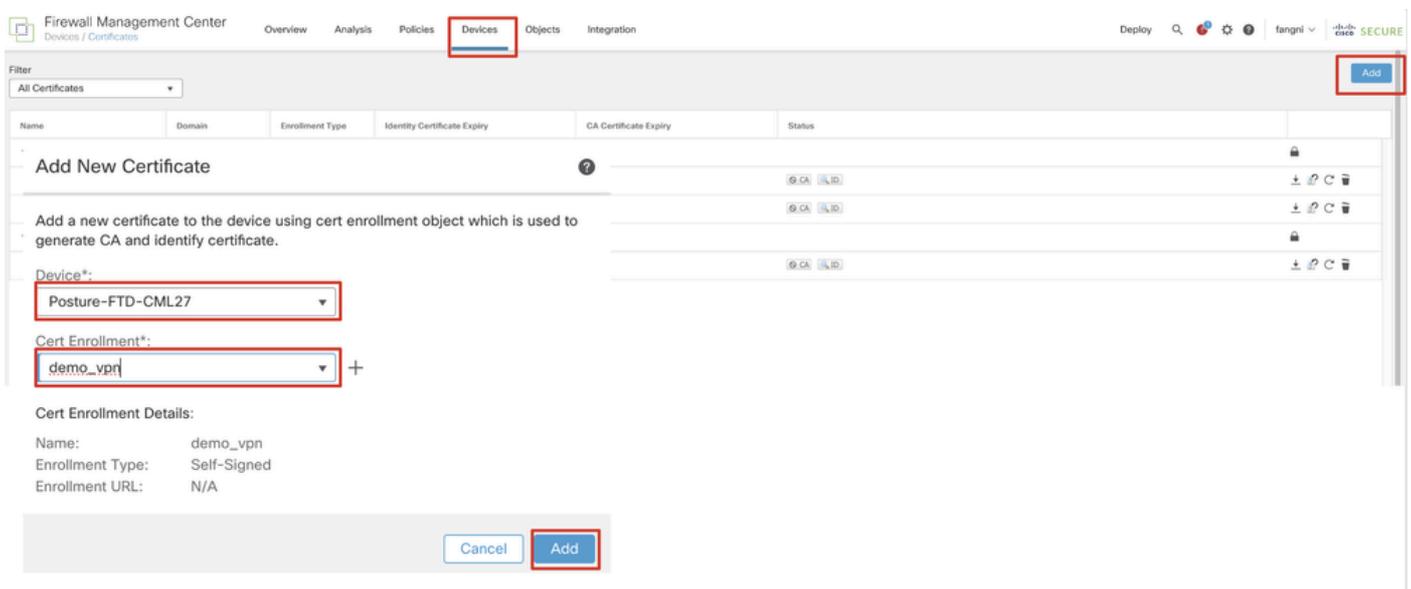
FMC\_Add\_New\_Pool

Étape 9. Accédez à **Certificate Objects > Object Management > PKI > Cert Enrollment**. Cliquez sur **Add Cert Enrollment**, indiquez un nom, puis sélectionnez **Self Signed Certificate** dans **Enrollment Type**. Cliquez sur l'**Certificate Parameters** onglet et indiquez **Common Name** et **Country Code**. Cliquez ensuite sur **Save**.



### FMC\_Add\_New\_Cert\_Enroll

Étape 10. Accédez à Devices > Certificates. Cliquez sur Add, sélectionnez le nom FTD sous Device, sélectionnez l'inscription configurée précédente sous Cert Enrollment. Cliquez sur Add.



### FMC\_Add\_New\_Cert\_To\_FTD

Étape 11. Accédez à Devices > VPN > Remote Access. Cliquez sur Add.

Étape 11.1. Saisissez le nom et ajoutez le FTD à Selected Devices. Cliquez sur 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

Étape 11.2. Sélectionnez le groupe de serveurs RADIUS précédemment configuré dans la Authentication Server, Authorization Server, Accounting Server. Faites défiler la page.

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: rtpise

Authorization Server: rtpise

Accounting Server: rtpise

**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

Étape 11.3. Sélectionnez le nom du pool précédemment configuré dans IPv4 Address Pools. Sélectionnez la stratégie de groupe précédemment configurée dans Group Policy. Cliquez sur 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

Étape 11.4. Cochez la case de l'image Linux. Cliquez sur 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-win-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

Étape 11.5. Sélectionnez l'interface de l'interface VPN. Sélectionnez l'inscription de certificat qui s'est inscrite sur FTD à l'étape 9. Cliquez sur 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

**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

Étape 11.6. Double-confirmez les informations associées sur la page de résumé. Si tout va bien, cliquez sur Finish. Si vous devez modifier quelque chose, cliquez sur Back.

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 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

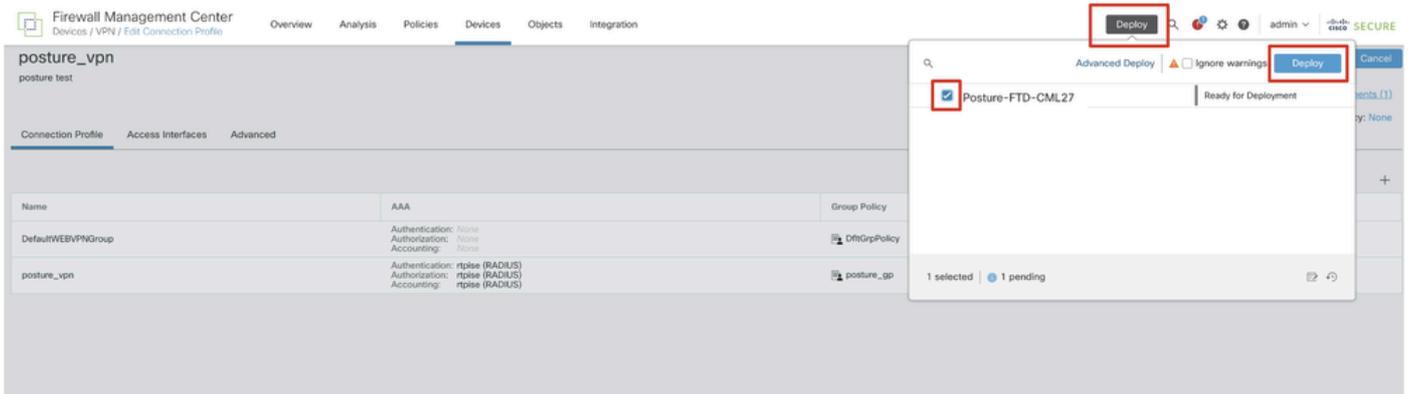
**Additional Configuration Requirements**  
After the wizard completes, the following configuration needs to be completed for VPN to work on all device targets.

- 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

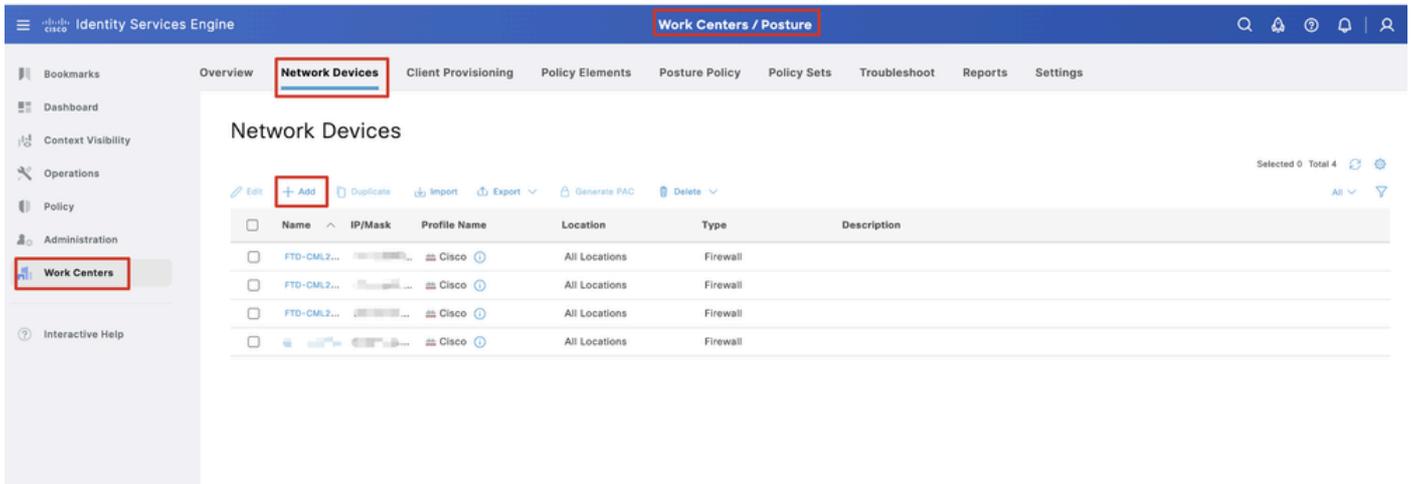
Étape 12. Déployez la nouvelle configuration sur FTD pour terminer la configuration VPN d'accès à distance.



*FMC\_Deploy\_FTD*

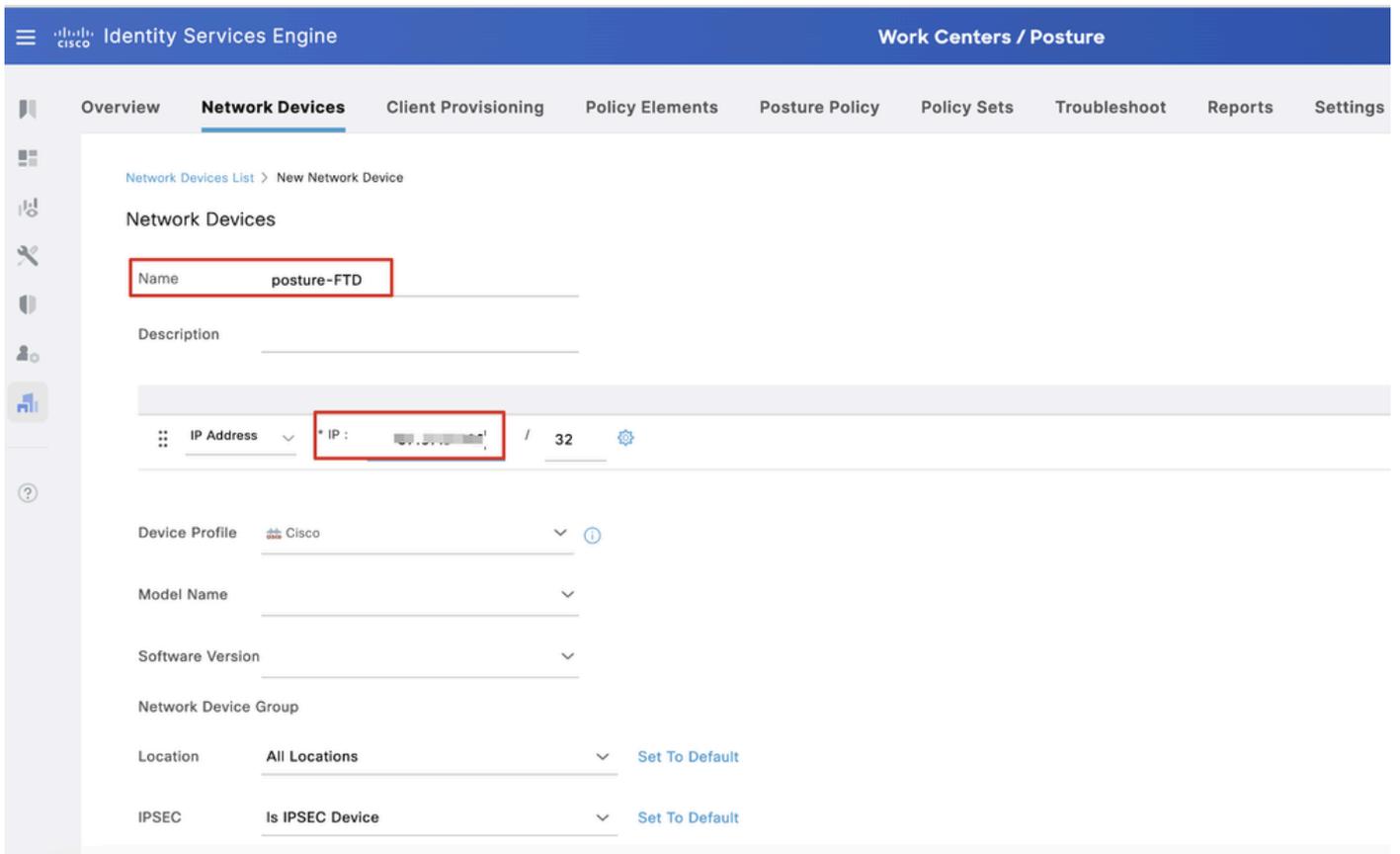
## Configurations sur ISE

Étape 13. Accédez à Work Centers > Posture > Network Devices. Cliquez sur Add.



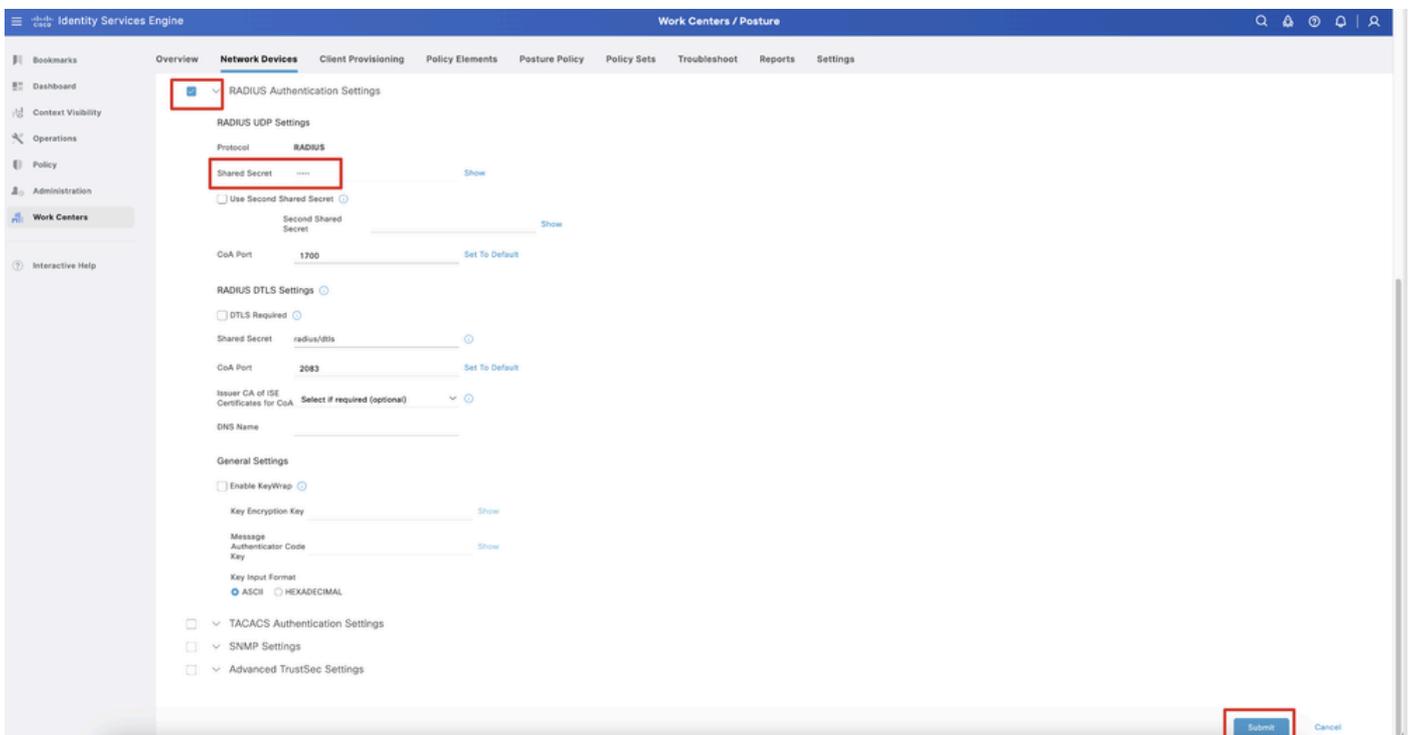
*ISE\_Add\_New\_Devices*

Étape 13.1. Fournissez le Name, IP Address et faites défiler la page vers le bas.



ISE\_Add\_New\_Devices\_1

Étape 13.2. Cochez la case de RADIUS Authentication Settings. Fournissez le Shared Secret. Cliquez sur Submit.

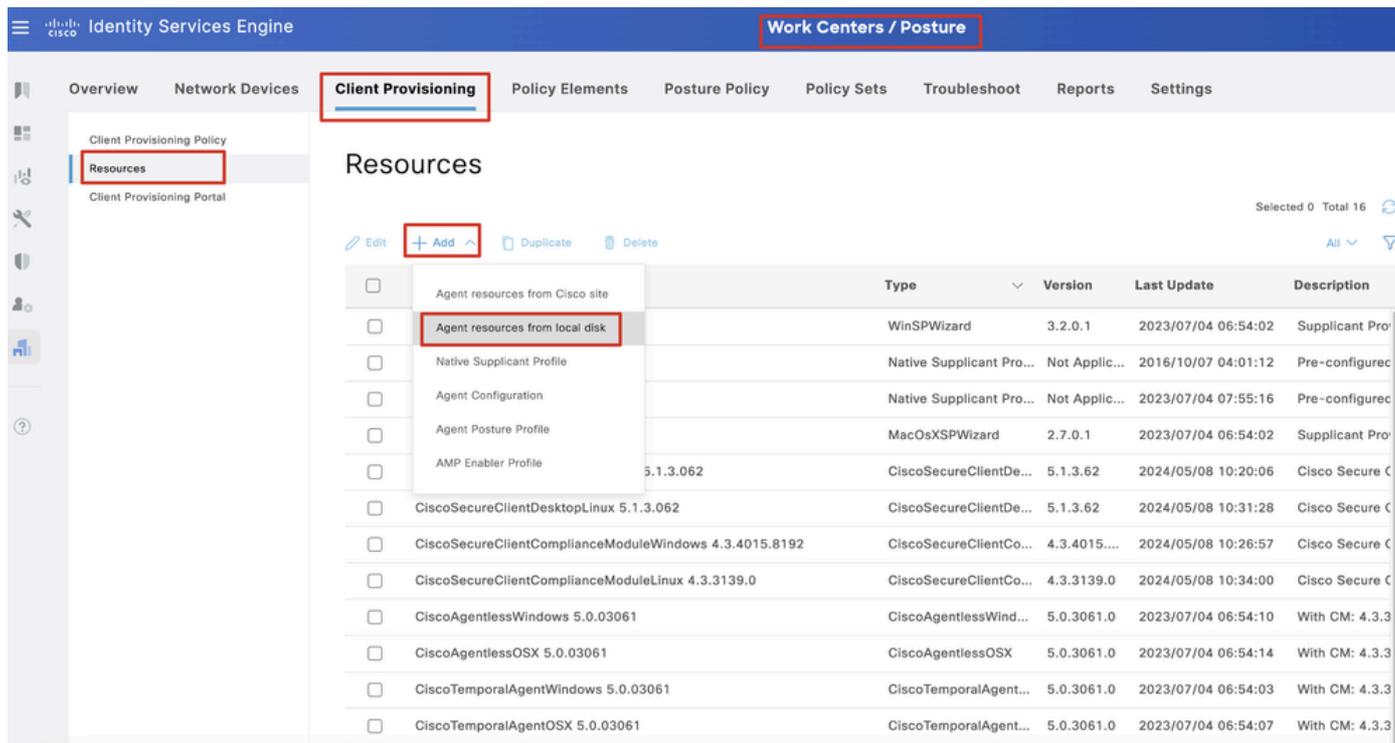


ISE\_Add\_New\_Devices\_2

Étape 14. Téléchargez le nom `cisco-secure-client-linux64-4.3.3139.0-isecompliance-webdeploy-k9.pkg` du package à partir de [Téléchargement de logiciel Cisco](#) et assurez-vous que le fichier est correct en confirmant que la somme de contrôle md5 du fichier téléchargé est identique à la

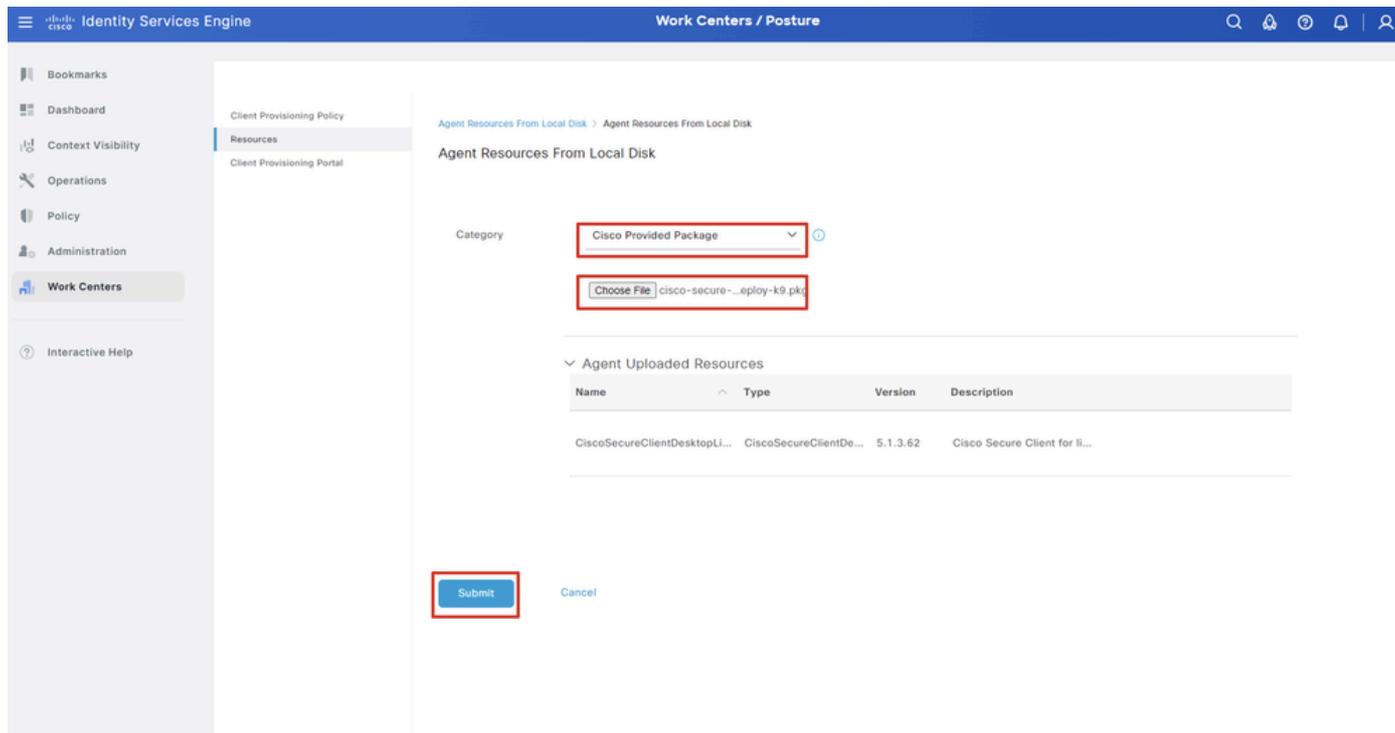
page Téléchargement de logiciel Cisco. Le nom du package cisco-secure-client-linux64-5.1.3.62-webdeploy-k9.pkg a été téléchargé à l'étape 1.

Étape 15. Accédez à Work Centers > Posture > Client Provisioning > Resources. Cliquez sur Add. Sélectionnez Agent resources from local disk.

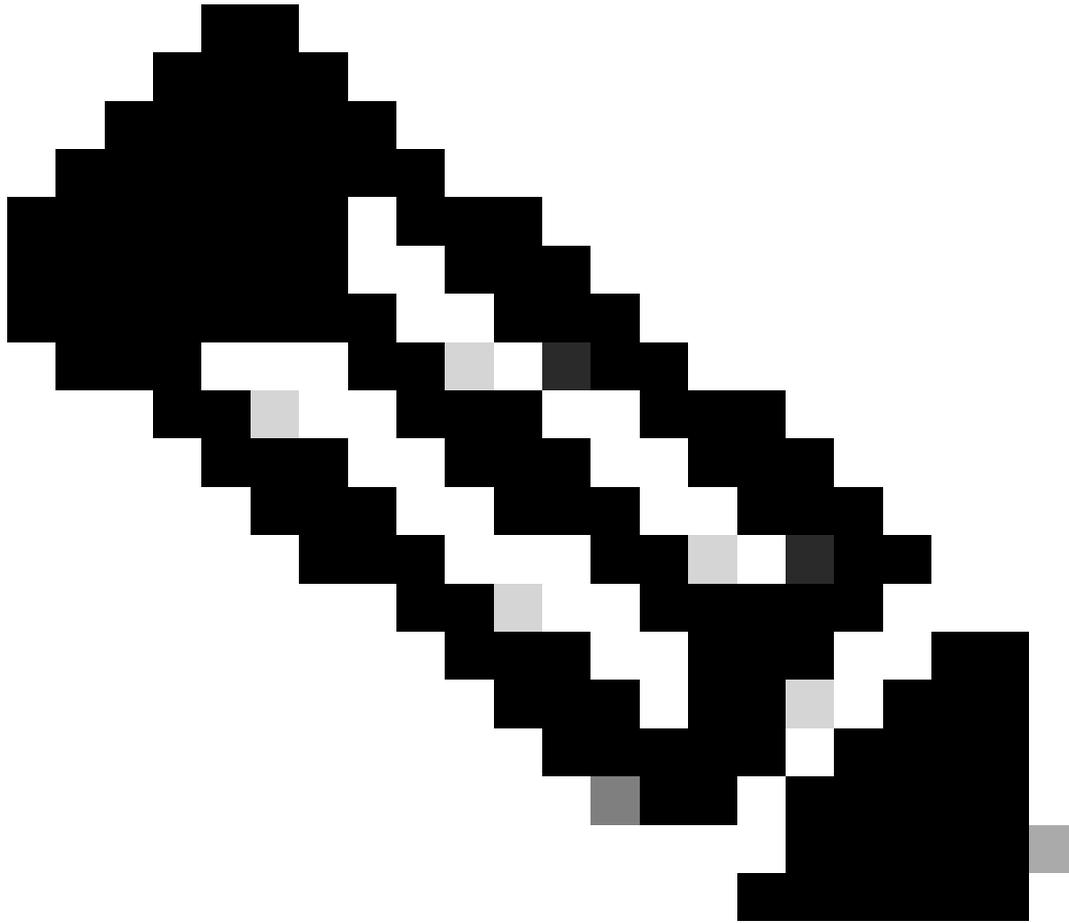


Ressource\_Téléchargement\_ISE

Étape 15.1. Sélectionnez Cisco Provided Package. Cliquez sur Choose File cette option pour télécharger cisco-secure-client-linux64-5.1.3.62-webdeploy-k9.pkg. Cliquez sur Submit.



ISE\_Upload\_Resources\_1



**Remarque** : répétez l'étape 14. pour télécharger `cisco-secure-client-linux64-4.3.3139.0-isecompliance-webdeploy-k9.pkg` .

---

Étape 16. Accédez à `Work Centers > Posture > Client Provisioning > Resources`. Cliquez sur `Add`. Sélectionnez `Agent Posture Profile`.

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes 'Identity Services Engine' and 'Work Centers / Posture'. The left sidebar has 'Client Provisioning' selected, with a sub-menu 'Resources' highlighted. The main content area is titled 'Resources' and contains a table of resources. A dropdown menu is open over the 'Agent Posture Profile' resource, showing options like 'Agent resources from Cisco site', 'Agent resources from local disk', 'Native Supplicant Profile', 'Agent Configuration', 'Agent Posture Profile' (highlighted), and 'AMP Enabler Profile'.

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

*Profil\_Posture\_Agent\_Ajout\_ISE*

Étape 16.1. Fournissez le Name, Server name rules et conservez le reste par défaut. Cliquez sur Save.

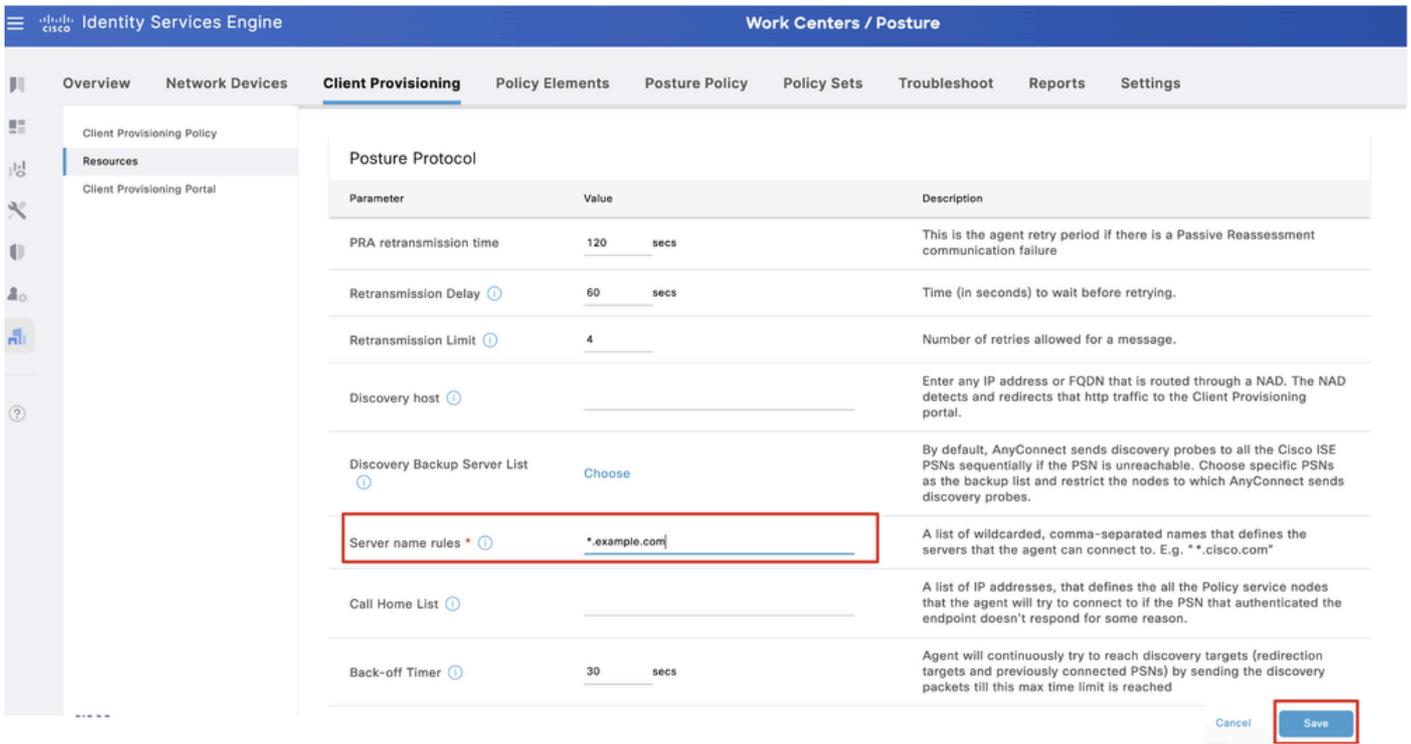
Nom : linux\_agent\_profile

Règles de nom de serveur : \*.example.com

The screenshot shows the Cisco Identity Services Engine (ISE) interface for configuring an Agent Posture Profile. The top navigation bar includes 'Identity Services Engine' and 'Work Centers / Posture'. The left sidebar has 'Client Provisioning' selected, with a sub-menu 'Resources' highlighted. The main content area is titled 'Agent Posture Profile' and contains a form for configuration. The 'Name' field is filled with 'linux\_agent\_profile' and is highlighted with a red box. The 'Description' field is empty. Below the form is a table for 'Agent Behavior'.

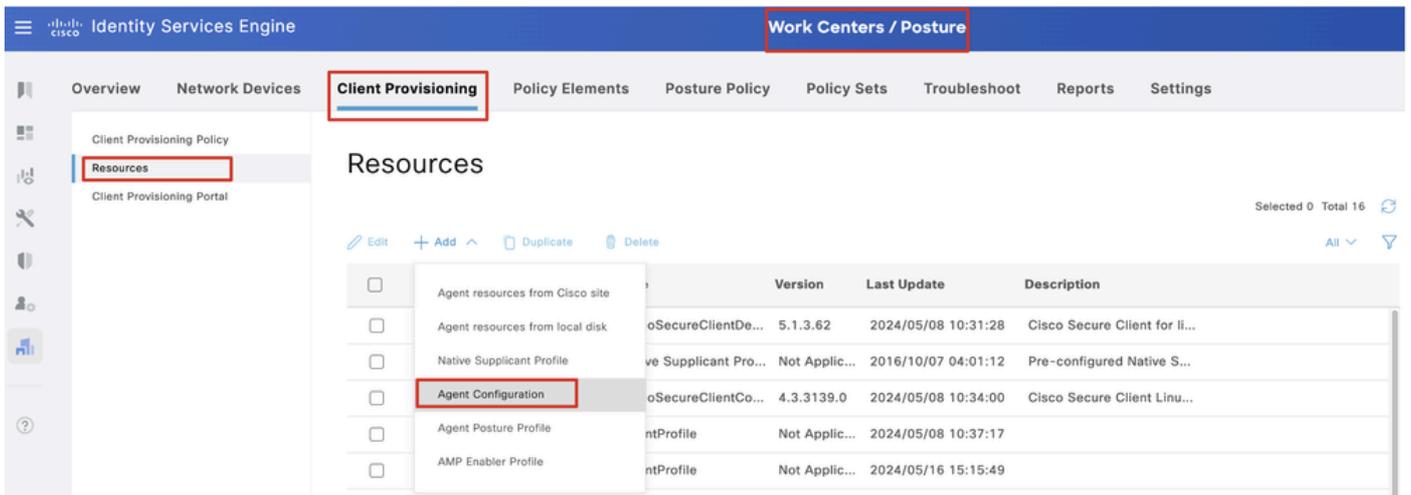
Parameter	Value	Description
Enable debug log	No	Enables the debug log on the agent

*ISE\_Add\_Agent\_Posture\_Profile\_1*



ISE\_Add\_Agent\_Posture\_Profile\_2

Étape 17. Accédez à Work Centers > Posture > Client Provisioning > Resources. Cliquez sur Add. Sélectionnez Agent Configuration.



ISE\_Add\_Agent\_Configuration

Étape 17.2. Configurez les détails :

Package Select Agent : CiscoSecureClientDesktopLinux 5.1.3.062

Nom : linux\_agent\_config

Module de conformité : CiscoSecureClientComplianceModuleLinux 4.3.3139.0

Cochez la case de VPN, Diagnostic and Reporting Tool

Position ISE de sélection de profil : linux\_agent\_profile

Cliquez sur 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

Étape 18. Accédez à Work Centers > Posture > Client Provisioning > Client Provisioning Policy. Cliquez Edit à la fin du nom d'une règle. Sélectionnez 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

Étape 18.1. Configurez les détails :

Nom de la règle : Linux

Systèmes d'exploitation : Linux All

Résultats : linux\_agent\_config

Cliquez sur Done et Save.

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The main heading is "Client Provisioning Policy". Below the heading, there is a description of the policy and a table of rules. The table has columns for Rule Name, Identity Groups, Operating Systems, Other Conditions, and Results. 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

Étape 19. Accédez à Work Centers > Posture > Policy Elements > Conditions > File. Cliquez sur Add.

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The main heading is "File Conditions". Below the heading, there is a table of 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

Étape 19.1. Configurez les détails :

Nom : linux\_demo\_file\_existing

Systèmes d'exploitation : Linux All

Type de fichier : FileExistence

Chemin d'accès au fichier : home, Desktop/test.txt

Opérateur de fichier : existe

Cliquez sur Submit.

The screenshot shows the Cisco Identity Services Engine (ISE) interface for configuring a new File Condition. The navigation menu on the left includes 'Conditions', 'File', and 'Remediations'. The main area is titled 'File Condition' and contains the following fields:

- Name \*: linux\_demo\_file\_exist
- Description:
- \* Operating System: Linux All
- Compliance Module: Any version
- \* File Type: FileExistence
- \* File Path: home (with a text input field containing Desktop/test.txt)
- \* File Operator: Exists

A 'Submit' button is located at the bottom right of the form area.

*ISE\_Add\_New\_File\_Condition\_1*

Étape 20. Accédez à Work Centers > Posture > Policy Elements > Requirements. Cliquez Edit à la fin du nom d'une règle. Sélectionnez 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

Étape 20.1. Configurez les détails :

Nom : Test\_existing\_linux

Systèmes d'exploitation : Linux All

Module de conformité : version 4.x ou ultérieure

Type de posture : Agent

Conditions : linux\_demo\_file\_existing

Cliquez sur Done et 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

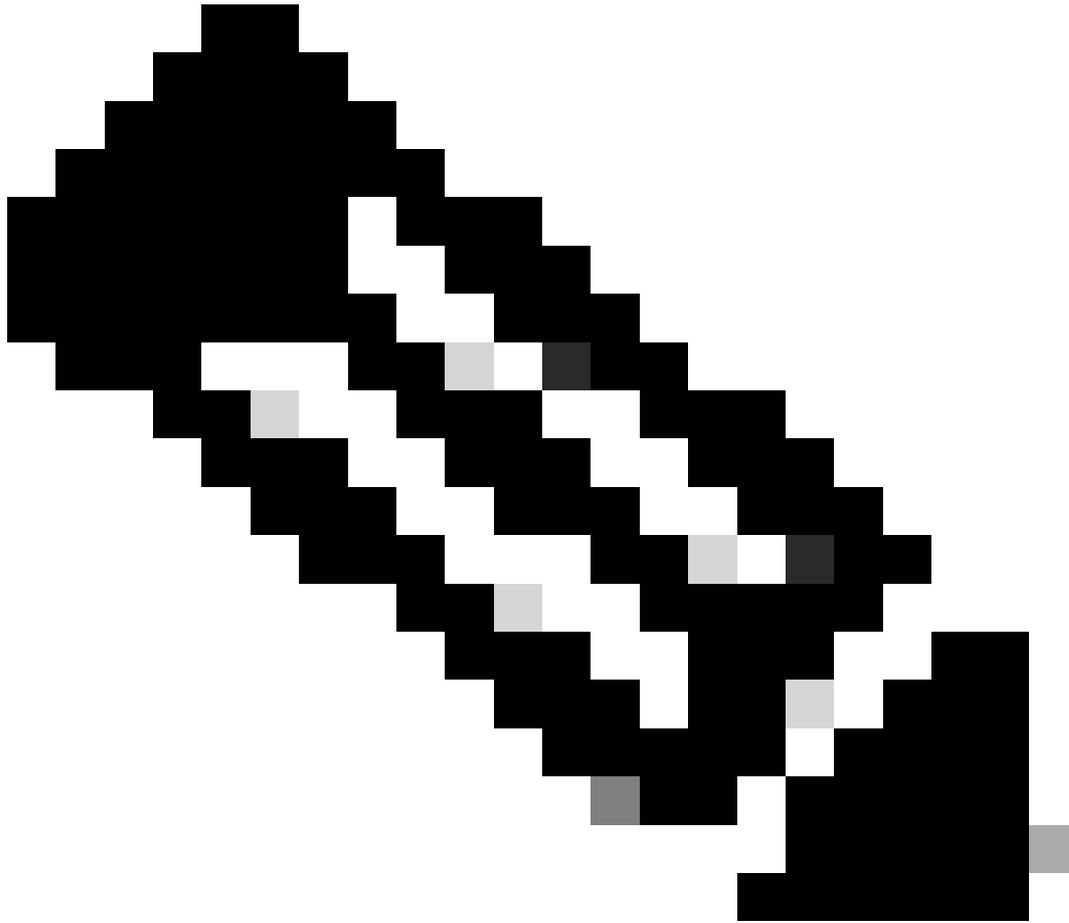
Requirements

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



**Remarque** : actuellement, seuls les scripts shell sont pris en charge pour les agents Linux en tant que correction.

---

Étape 21. Accédez à Work Centers > Posture > Policy Elements > Authorization Profiles. Cliquez sur Add.

Étape 21.1. Configurez les détails :

Nom : unknown\_redirect

Cochez la case de Web Redirection(CWA,MDM,NSP,CPP)

Sélectionner Client Provisioning(Posture)

ACL : redirection

Valeur : Client Provisioning Portal (par défaut)

The screenshot displays the Cisco Identity Services Engine (ISE) configuration interface. The top navigation bar includes 'Work Centers / Posture'. The main navigation menu has 'Policy Elements' selected. The left sidebar lists various configuration categories, with 'Authorization Profiles' highlighted. The main content area is titled 'Authorization Profile' and contains the following fields and options:

- Name:** unknown\_redirect
- Description:** (empty text area)
- Access Type:** ACCESS\_ACCEPT
- Network Device Profile:** Cisco
- Service Template:**
- Track Movement:**  ⓘ
- Agentless Posture:**  ⓘ
- Passive Identity Tracking:**  ⓘ

Under the 'Common Tasks' section, the following options are visible:

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

The 'Web Redirection' task is configured with the following settings:

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

ISE\_Add\_New\_Authorization\_Profile\_Redirect\_1

---

**Remarque** : cette redirection de nom de liste de contrôle d'accès doit correspondre au nom de liste de contrôle d'accès correspondant configuré sur FTD.

---

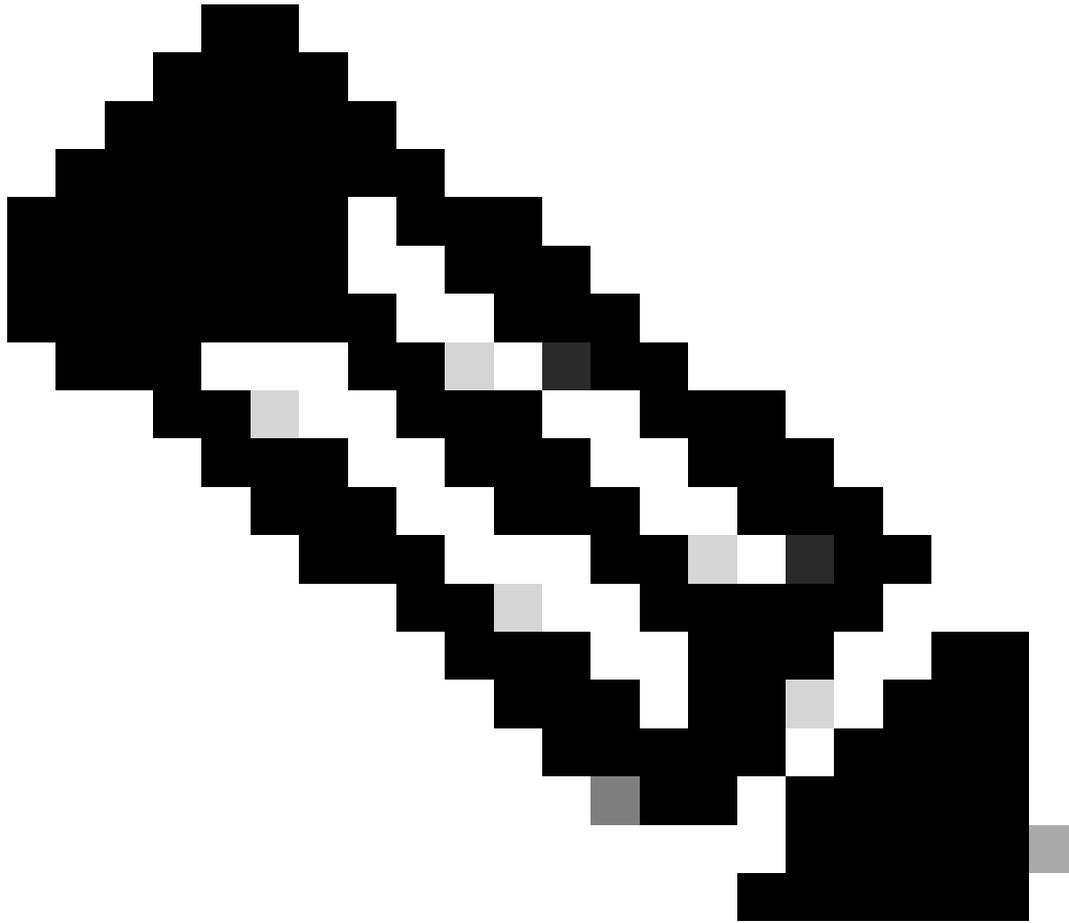
Étape 21.2. Répétez l' Add pour créer deux autres profils d'autorisation pour les terminaux non conformes et conformes avec les détails.

Nom : non\_compliance\_profile

Nom DACL : DENY\_ALL\_IPv4\_TRAFFIC

Nom : compliance\_profile

Nom DACL : PERMIT\_ALL\_IPv4\_TRAFFIC



**Remarque :** la liste de contrôle d'accès pour les terminaux conformes ou non conformes doit être configurée en fonction des exigences réelles.

---

Étape 22. Accédez à Work Centers > Posture > Posture Policy. Cliquez sur Edit à la fin des règles. Sélectionnez 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	Any	Mac OSX	4.x or later	Agent		Any_AM_Installation_Mac	Edit - Duplicate
<input type="checkbox"/>	Policy Options	Default_AntiMalware_Policy_Mac_temporal	Any	Mac OSX	4.x or later	Temporal Agent		Any_AM_Installation_Mac_temporal	Edit - Duplicate
<input type="checkbox"/>	Policy Options	Default_AntiMalware_Policy_Win	Any	Windows All	4.x or later	Agent		Any_AM_Installation_Win	Edit - Duplicate
<input type="checkbox"/>	Policy Options	Default_AntiMalware_Policy_Win_temporal	Any	Windows All	4.x or later	Temporal Agent		Any_AM_Installation_Win_temporal	Edit - Duplicate
<input type="checkbox"/>	Policy Options	Default_AppViz_Policy_Mac	Any	Mac OSX	4.x or later	Agent		Default_AppViz_Requirement_Mac	Edit - Duplicate
<input type="checkbox"/>	Policy Options	Default_AppViz_Policy_Mac_temporal	Any	Mac OSX	4.x or later	Temporal Agent		Default_AppViz_Requirement_Mac_temporal	Edit - Duplicate
<input type="checkbox"/>	Policy Options	Default_AppViz_Policy_Win	Any	Windows All	4.x or later	Agent		Default_AppViz_Requirement_Win	Edit - Duplicate
<input type="checkbox"/>	Policy Options	Default_AppViz_Policy_Win_temporal	Any	Windows All	4.x or later	Temporal Agent		Default_AppViz_Requirement_Win_temporal	Edit - Duplicate
<input type="checkbox"/>	Policy Options	Default_Firewall_Policy_Mac	Any	Mac OSX	4.x or later	Agent		Default_Firewall_Requirement_Mac	Edit - Duplicate
<input type="checkbox"/>	Policy Options	Default_Firewall_Policy_Mac_temporal	Any	Mac OSX	4.x or later	Temporal Agent		Default_Firewall_Requirement_Mac_temporal	Edit - Duplicate
<input type="checkbox"/>	Policy Options	Default_Firewall_Policy_Win	Any	Windows All	4.x or later	Agent		Default_Firewall_Requirement_Win	Edit - Duplicate
<input type="checkbox"/>	Policy Options	Default_Firewall_Policy_Win_temporal	Any	Windows All	4.x or later	Temporal Agent		Default_Firewall_Requirement_Win_temporal	Edit - Duplicate
<input type="checkbox"/>	Policy Options	Default_Hardware_Attributes_Policy_Mac	Any	Mac OSX	4.x or later	Agent		Default_Hardware_Attributes_Requirement_Mac	Edit - Duplicate
<input type="checkbox"/>	Policy Options	Default_Hardware_Attributes_Policy_Mac_temporal	Any	Mac OSX	4.x or later	Temporal Agent		Default_Hardware_Attributes_Requirement_Mac_temporal	Edit - Duplicate
<input type="checkbox"/>	Policy Options	Default_Hardware_Attributes_Policy_Win	Any	Windows All	4.x or later	Agent		Default_Hardware_Attributes_Requirement_Win	Edit - Duplicate

*Politique\_Nouvelle\_Posture\_Ajout\_ISE*

Étape 22.1. Configurez les détails :

Nom de la règle : Demo\_test\_existing\_linux

Groupes d'identités : Tous

Systèmes d'exploitation : Linux All

Module de conformité : version 4.x ou ultérieure

Type de posture : Agent

Configuration requise : Test\_existing\_linux

Cliquez sur Done et 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	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

Étape 23. Accédez à Work Centers > Posture > Policy Sets. Cliquez pour 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

Reset [Reset Policyset Hitcounts](#) [Save](#)

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
<span style="color: green;">●</span>	Default	Default policy set		Default Network Access		<a href="#">+</a> <a href="#">-</a> <a href="#">⚙️</a>	<a href="#">▶</a>

[Insert new row above](#) [Reset](#) [Save](#)

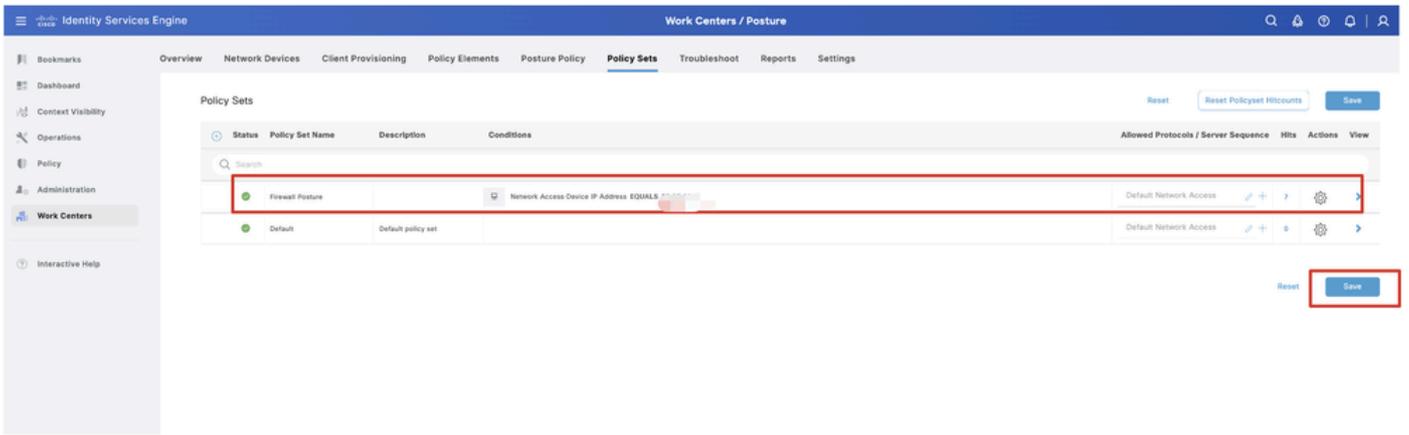
ISE\_Add\_New\_Policy\_Set

Étape 23.1. Configurez les détails :

Nom du jeu de stratégies : Position du pare-feu

Conditions : ÉGAL à l'adresse IP du périphérique d'accès réseau [FTD IP Address]

Cliquez sur Save .



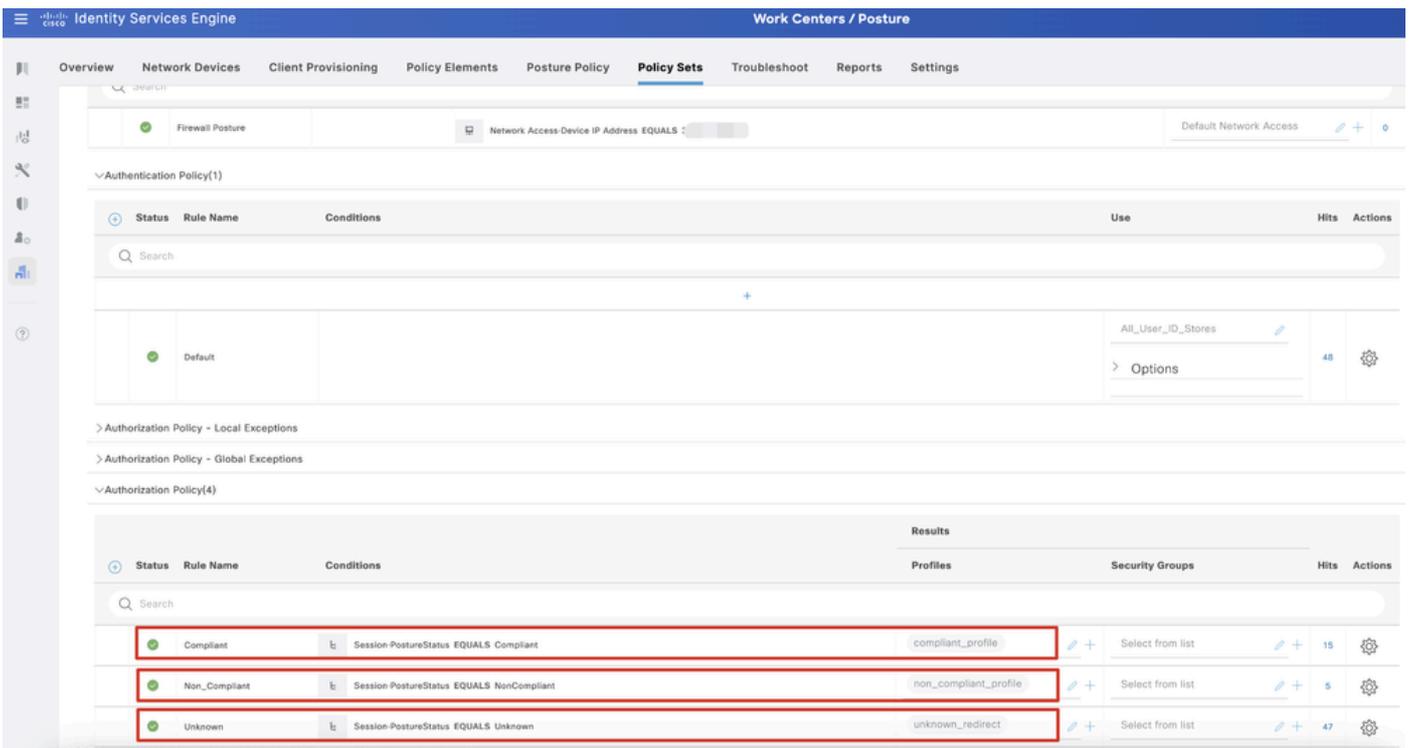
### ISE\_Add\_New\_Policy\_Set\_1

Étape 23.2. Cliquez sur > pour entrer le jeu de stratégies. Créez de nouvelles règles d'autorisation pour l'état conforme à la position, non conforme et inconnu. Cliquez sur Save.

Conforme à `compliance_profile`

Non conforme avec `non_compliance_profile`

Inconnu avec `unknown_redirect`



### ISE\_Add\_New\_Policy\_Set\_2

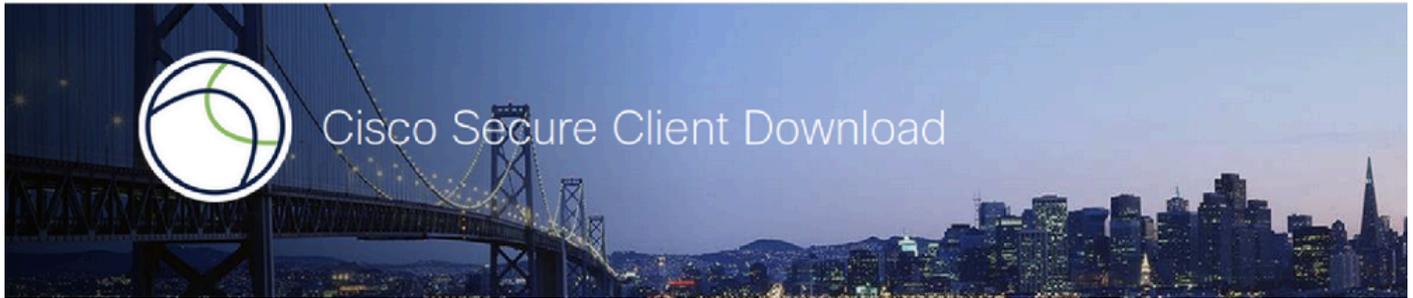
Configurations sur Ubuntu

Étape 24. Connectez-vous au client Ubuntu via l'interface utilisateur graphique. Ouvrez le navigateur pour vous connecter au portail VPN. Dans cet exemple, il s'agit de `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*

Étape 25. Cliquez sur Download for Linux.



## Download & Install

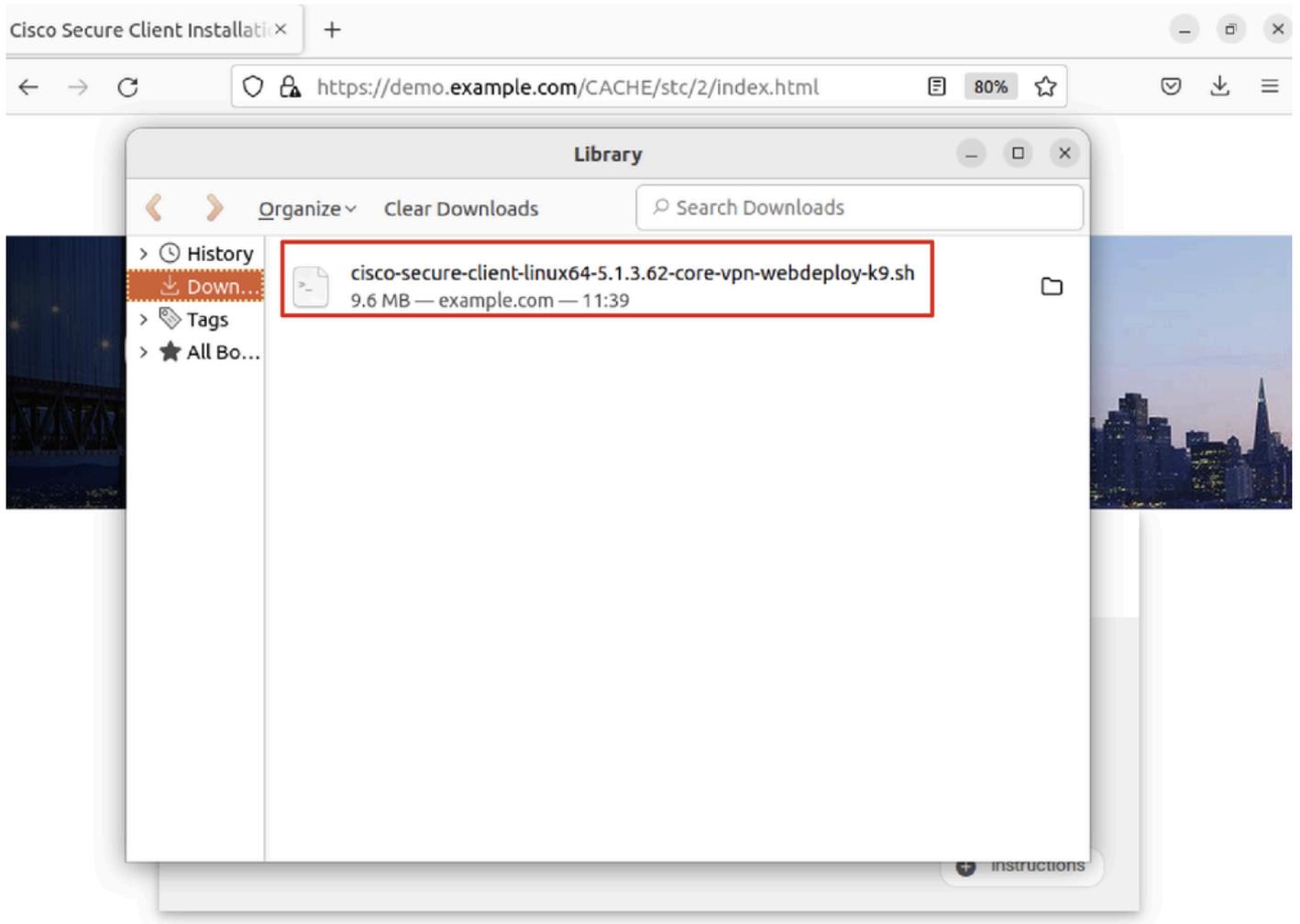
Download Cisco Secure Client and install it on your computer.

[Download for Linux](#)

[+ Instructions](#)

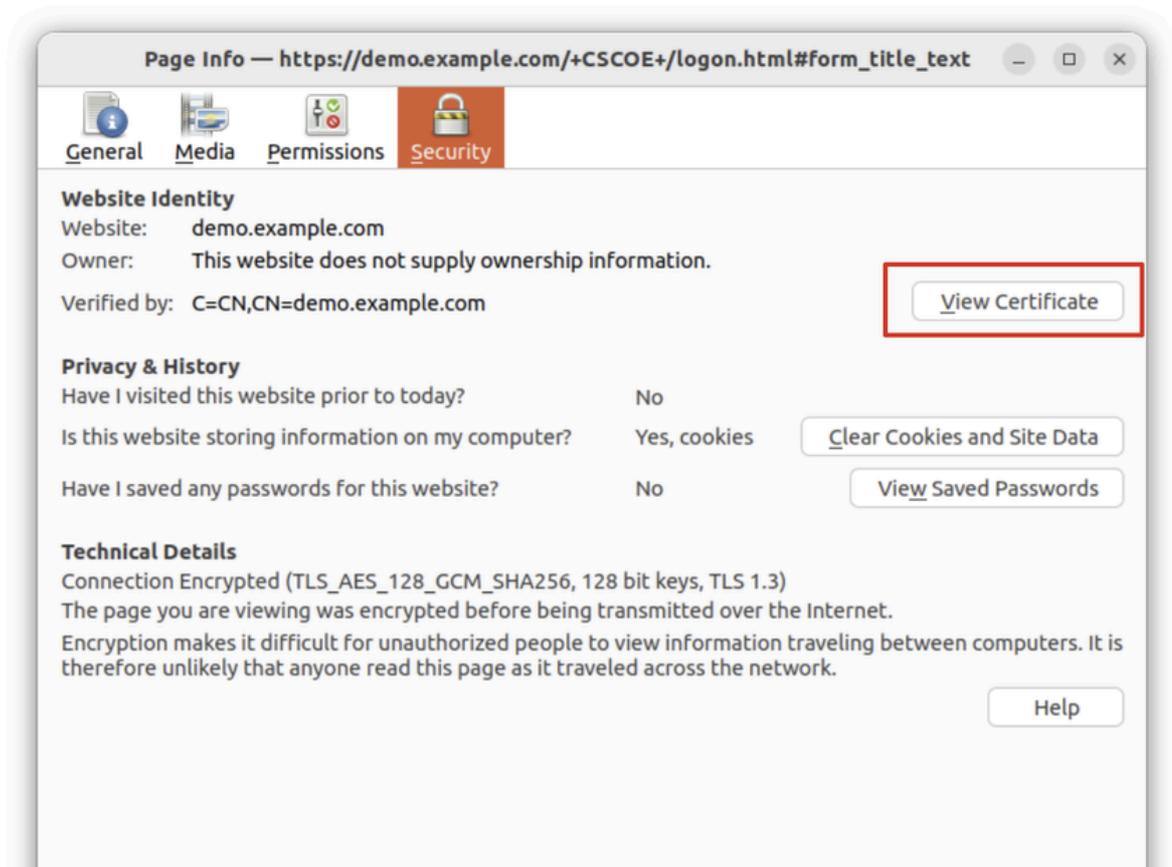
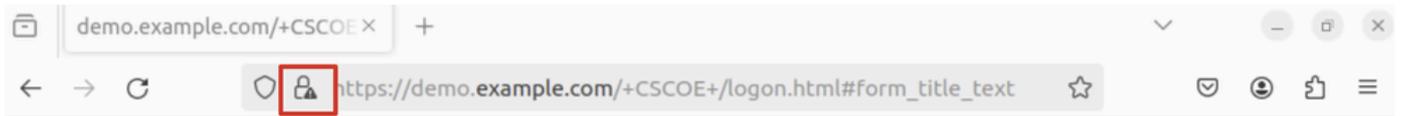
*Ubuntu\_Browser\_VPN\_Download\_1*

Le nom du fichier téléchargé est cisco-secure-client-linux64-5.1.3.62-core-vpn-webdeploy-k9.sh.



*Ubuntu\_Browser\_VPN\_Download\_2*

Étape 26. Téléchargez le certificat VPN via le navigateur et renommez le fichier en <certificate>.crt. Voici l'exemple d'utilisation de firefox pour télécharger le certificat.



*Ubuntu\_Browser\_VPN\_Cert\_Download*

Étape 27. Ouvrez le terminal sur le client Ubuntu. Accédez à pourpath home/user/Downloads/ installer 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$
```

Étape 28. Faites confiance au certificat du portail VPN sur le client 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...
```

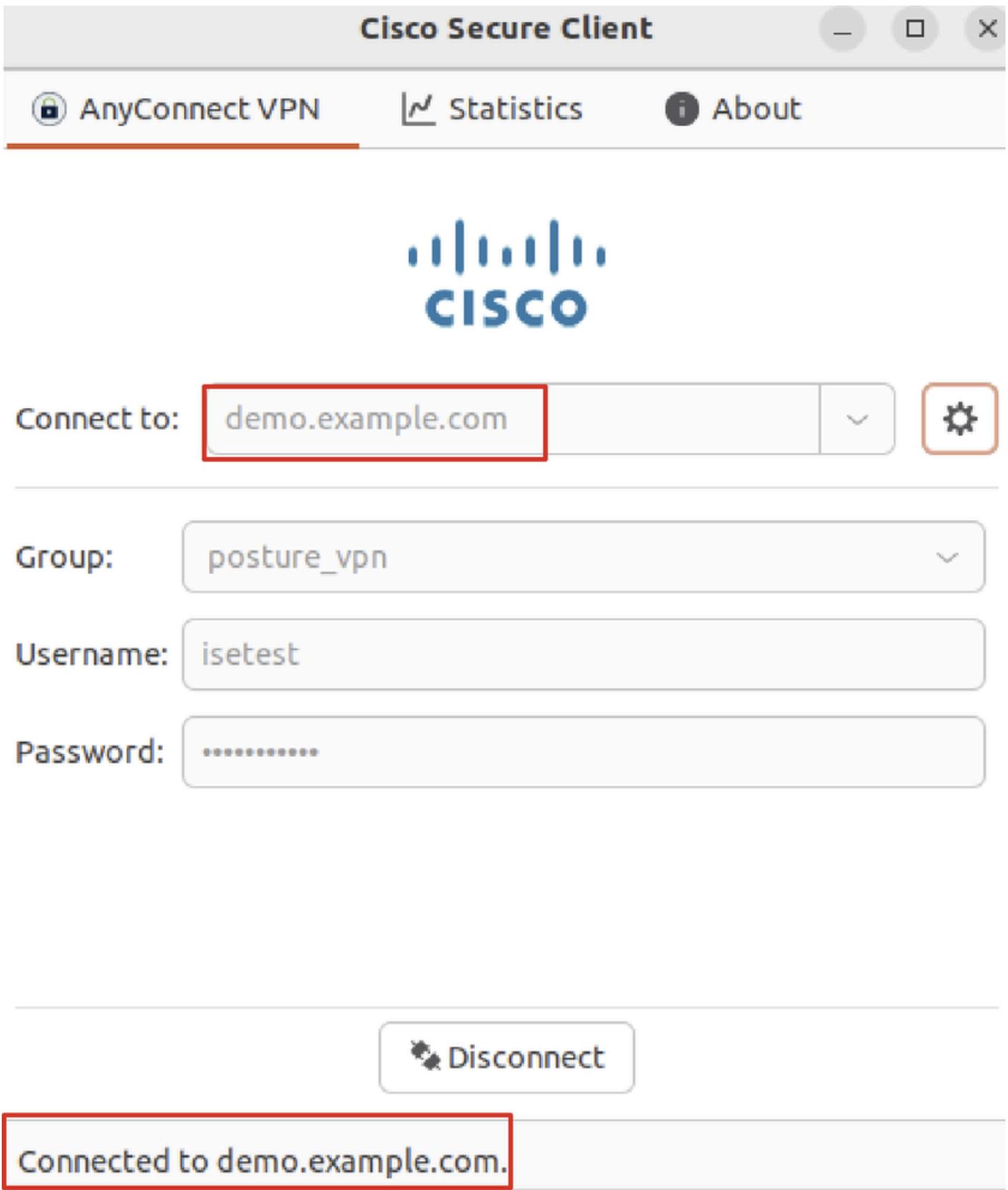
```
done.
```

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

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

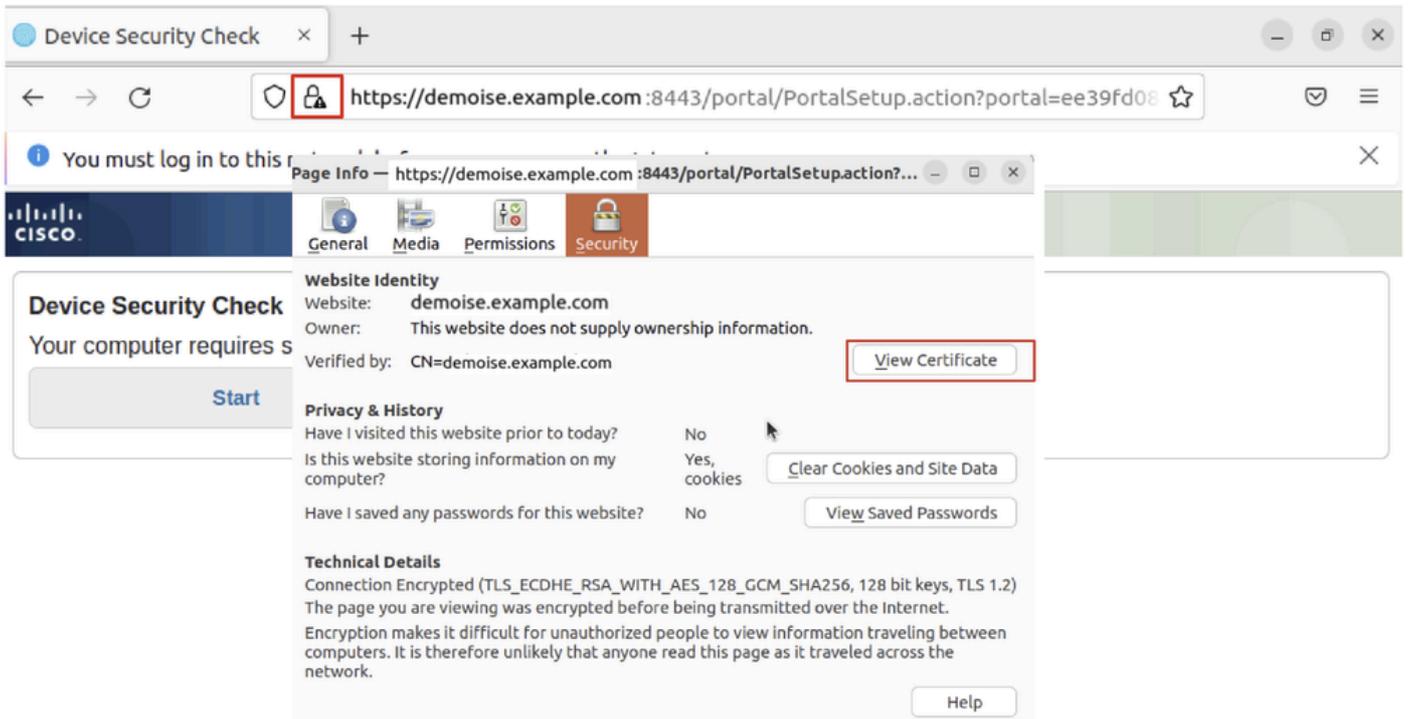
```
demo-example-com.crt: OK
```

Étape 29. Ouvrez Cisco Secure Client sur le client Ubuntu et connectez le VPN à [demo.example.com](https://demo.example.com) avec succès.



*Ubuntu\_Secure\_Client\_Connected*

Étape 30. Ouvrez le navigateur pour accéder à tout site Web déclenchant la redirection vers le portail CPP ISE. Téléchargez le certificat à partir du portail CPP ISE et renommez le fichier <certificate>.crt. Voici un exemple d'utilisation de Firefox pour le téléchargement.



*Ubuntu\_Browser\_CPP\_Cert\_Download*

Étape 30.1. Faites confiance au certificat du portail CPP ISE sur le client 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
```

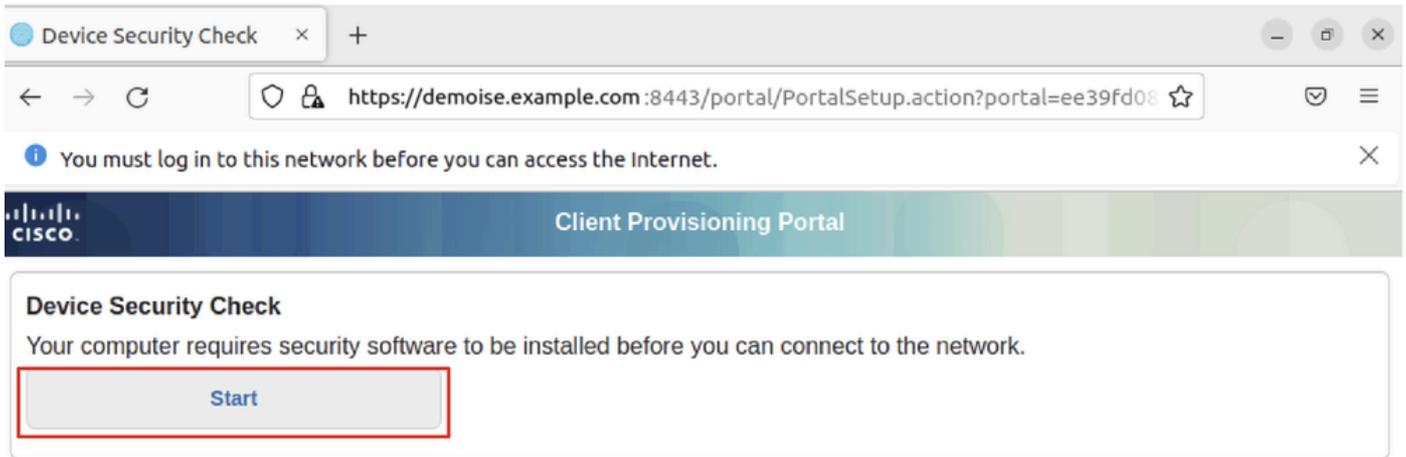
```
1 added
```

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

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

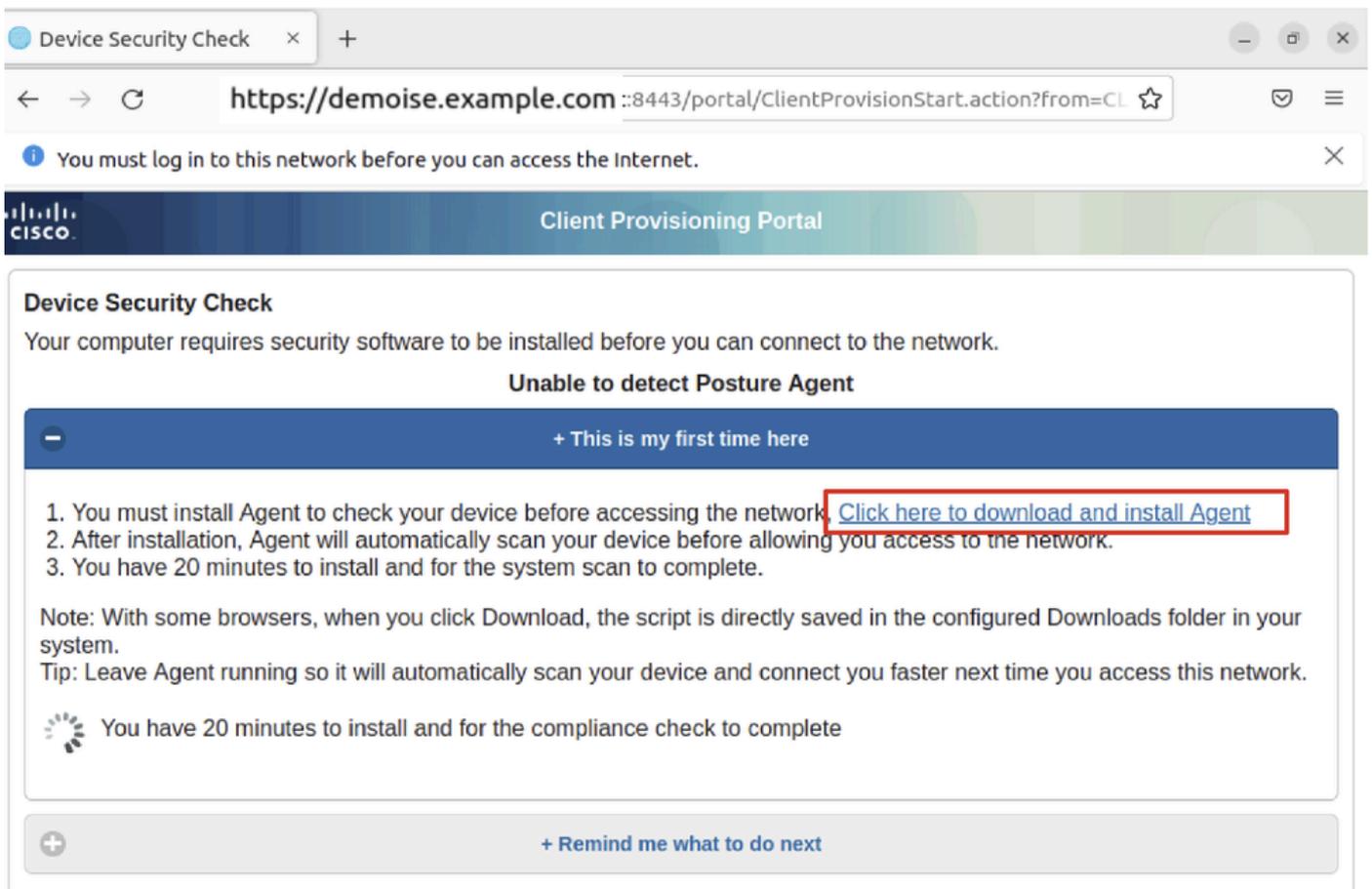
```
done.
```

Étape 31. Cliquez Start sur le portail CPP ISE.



*Ubuntu\_Browser\_CPP\_Start*

Étape 32. Cliquez ici pour télécharger et installer l'Agent.



*Ubuntu\_Browser\_CPP\_Download\_Posture*

Étape 33. Ouvrez le terminal sur le client Ubuntu. Accédez au chemin `home/user/Downloads/` d'installation du module de posture.

<#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.

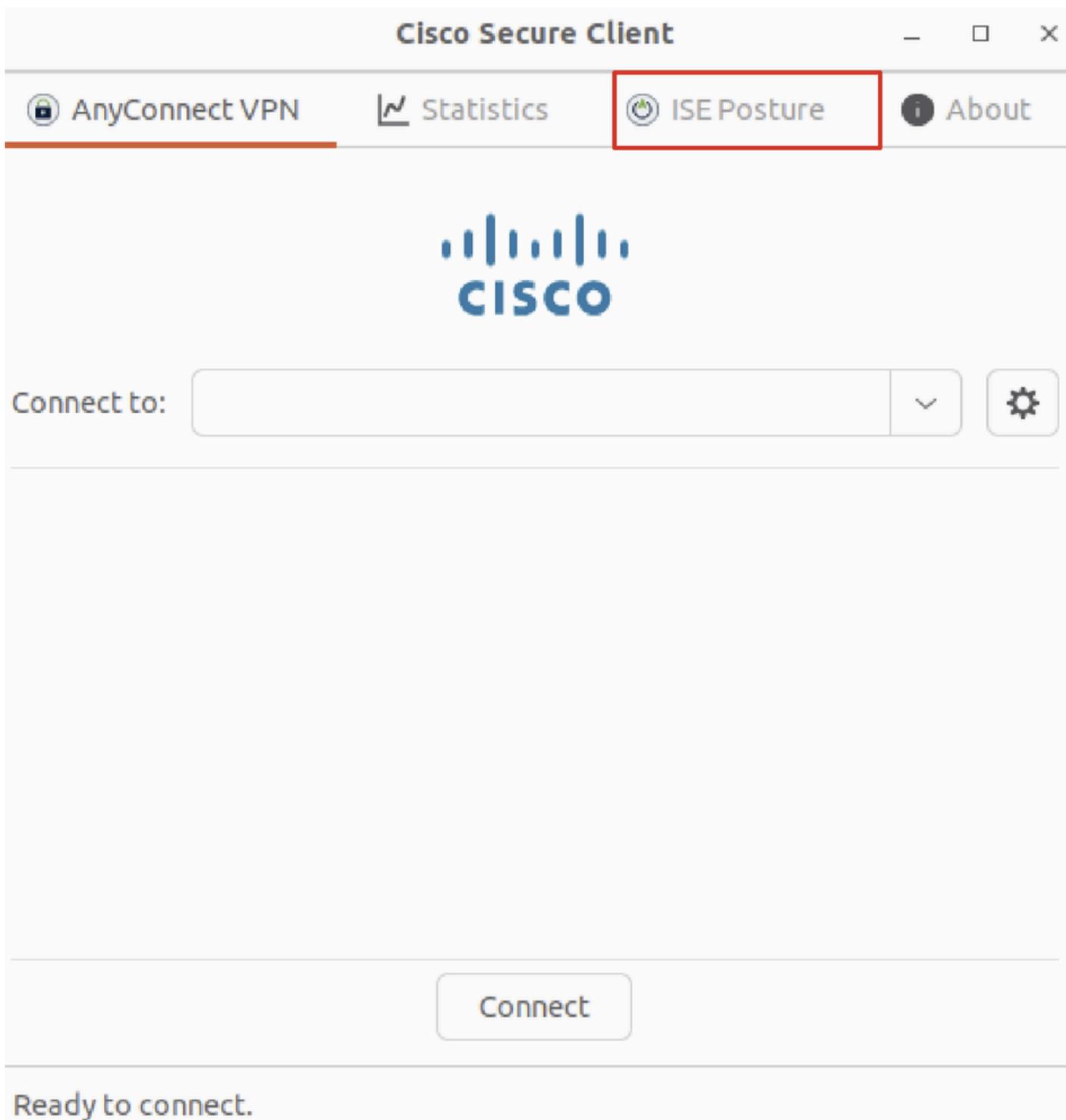
Downloading Cisco Secure Client...

Downloading remote package...

Running Cisco Secure Client - Downloader...

Installation is completed.

Étape 34. Sur l'interface utilisateur du client Ubuntu, quittez le client sécurisé Cisco et rouvrez-le. Le module de posture ISE est installé et s'exécute correctement.



*Ubuntu\_Secure\_Client\_ISE\_Posture\_Installed*

Étape 35. Ouvrez le terminal sur le client Ubuntu. Accédez à path home/user/Desktop , créez un fichier test.txt pour répondre à la condition de fichier configurée sur ISE.

```
<#root>
```

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

```
cd Desktop/
```

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

echo test > test.txt

Vérifier

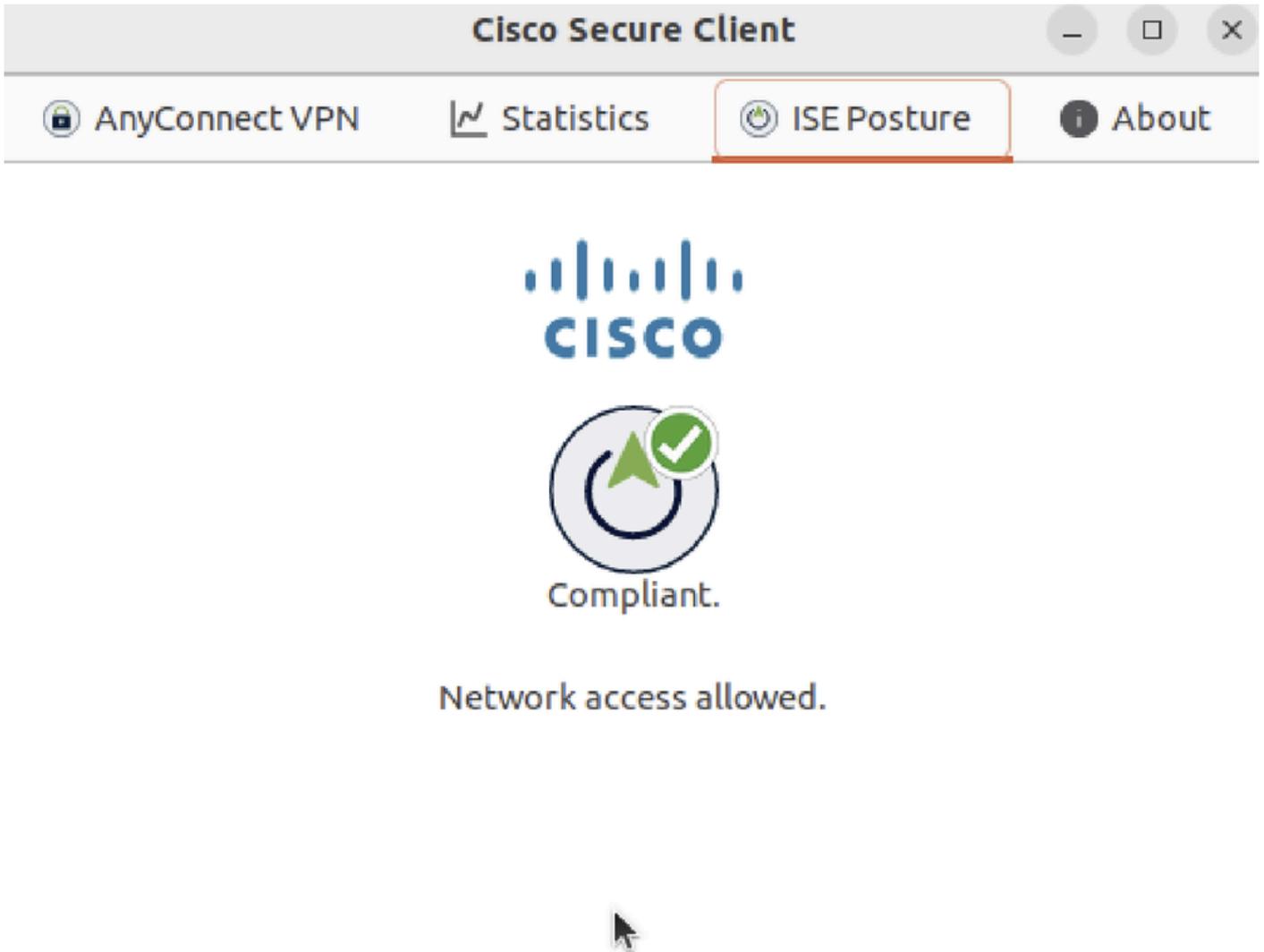
Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

Étape 1. Connectez le VPN à demo.example.com sur le client Ubuntu.



Vérifier\_Ubuntu\_Secure\_Client\_Connected

Étape 2. Vérifiez l'état de la position ISE sur le client Ubuntu.



Vérifier\_Ubuntu\_Secure\_Client\_Compliant

Étape 3. Cochez Radius Live Log sur ISE. Accédez à 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 Filter

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			isetest	52:54:00:17:6B:FA	Ubuntu-Workstation	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

Étape 4. Accédez à FTD CLI via SSH ou la 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

## Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Pour le flux de posture et le dépannage de Cisco Secure Client et ISE, consultez les [documents](#) [CCO](#) [Comparaison des styles de posture ISE pour les versions antérieures et postérieures à 2.2](#) et [Dépannage de la gestion et de la posture des sessions ISE](#).

Informations connexes

- [Compatibilité des composants réseau de Cisco Identity Services Engine, version 3.3](#)

- [Guide de l'administrateur de Cisco Identity Services Engine, version 3.3](#)
- [Assistance technique de Cisco et téléchargements](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.