De Linux VPN-houding configureren met ISE 3.3

Inhoud

Inleiding

Dit document beschrijft hoe u de Linux VPN-postuur kunt configureren met Identity Services Engine (ISE) en Firepower Threat Defense (FTD).

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco Secure-client
- Remote Access VPN bij Firepower Threat Defence (FTD)
- Identity Services Engine (ISE)

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende softwareversies:

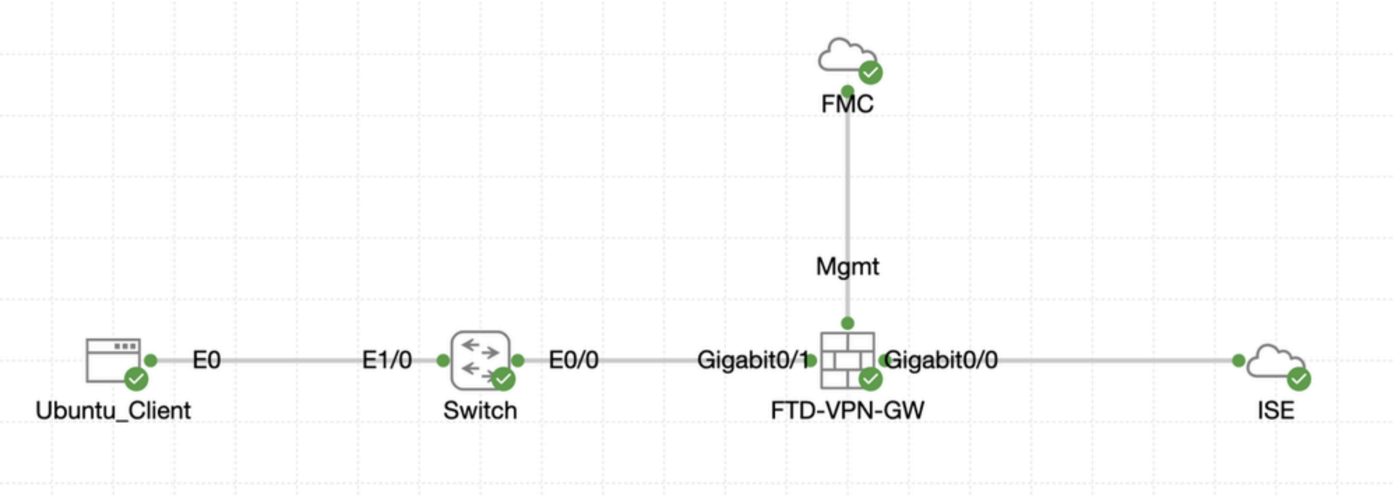
- Ubuntu 22.04
- Cisco Secure-client 5.1.3.62

- Cisco Firepower Threat Defence (FTD) 7.4.1
- Cisco Firepower Management Center (FMC) 7.4.1
- Cisco Identity Services Engine (ISE) 3.3

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Configureren

Netwerkdiagram



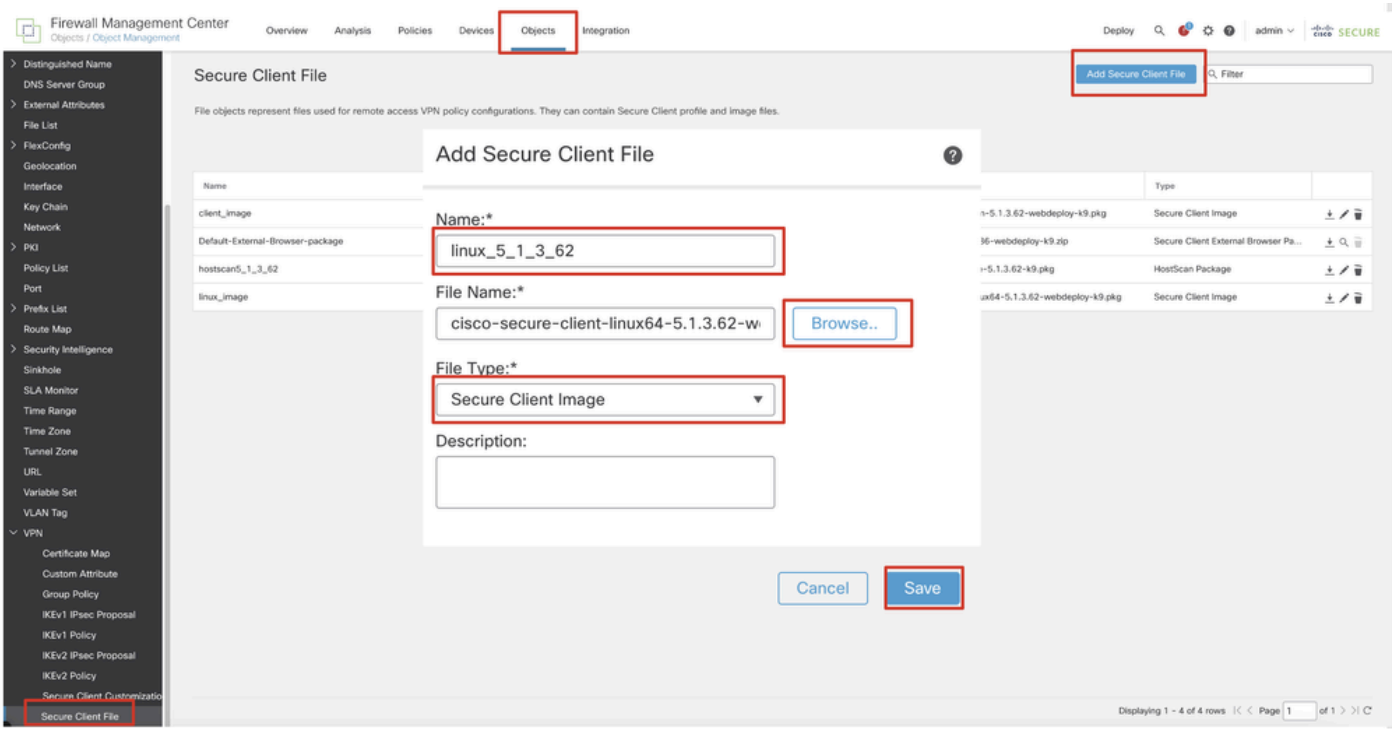
Topologie

Configuraties op FMC/FTD

Stap 1. De connectiviteit tussen de client, FTD, FMC en ISE is met succes geconfigureerd. Als enroll.cisco.com wordt gebruikt voor endpoints die probe voor omleiding doen (verwijs naar postuur CCO documentenISE postuur stijl vergelijking voor Pre en Post 2.2 voor details). Zorg ervoor dat de route voor verkeer naar enroll.cisco.com op FTD correct is geconfigureerd.

Stap 2. Download de pakketnaam cisco-secure-client-linux64-5.1.3.62-webdeploy-k9.pkg van Cisco Software Download en zorg ervoor dat het bestand na het downloaden goed is door te bevestigen dat de MD5-checksum van het gedownloade bestand hetzelfde is als de Cisco Software Download-pagina.

Stap 3. Navigeer naar Objects > Object Management > VPN > Secure Client File. Klik op Add Secure Client File, geef de naam op, blader File Name om te selecteren cisco-secure-client-linux64-5.1.3.62-webdeploy-k9.pkg en selecteer Secure Client Image in File Type de vervolgkeuzelijst. Klik vervolgens op Save.



Secure Client File

File objects represent files used for remote access VPN policy configurations. They can contain Secure Client profile and image files.

Name		Type
client_image	n-5.1.3.62-webdeploy-k9.pkg	Secure Client Image
Default-External-Browser-package	36-webdeploy-k9.zip	Secure Client External Browser Pa...
hostscan5_1_3_62	-5.1.3.62-k9.pkg	HostScan Package
linux_image	ux64-5.1.3.62-webdeploy-k9.pkg	Secure Client Image

Add Secure Client File

Name:* linux_5_1_3_62

File Name:* cisco-secure-client-linux64-5.1.3.62-w

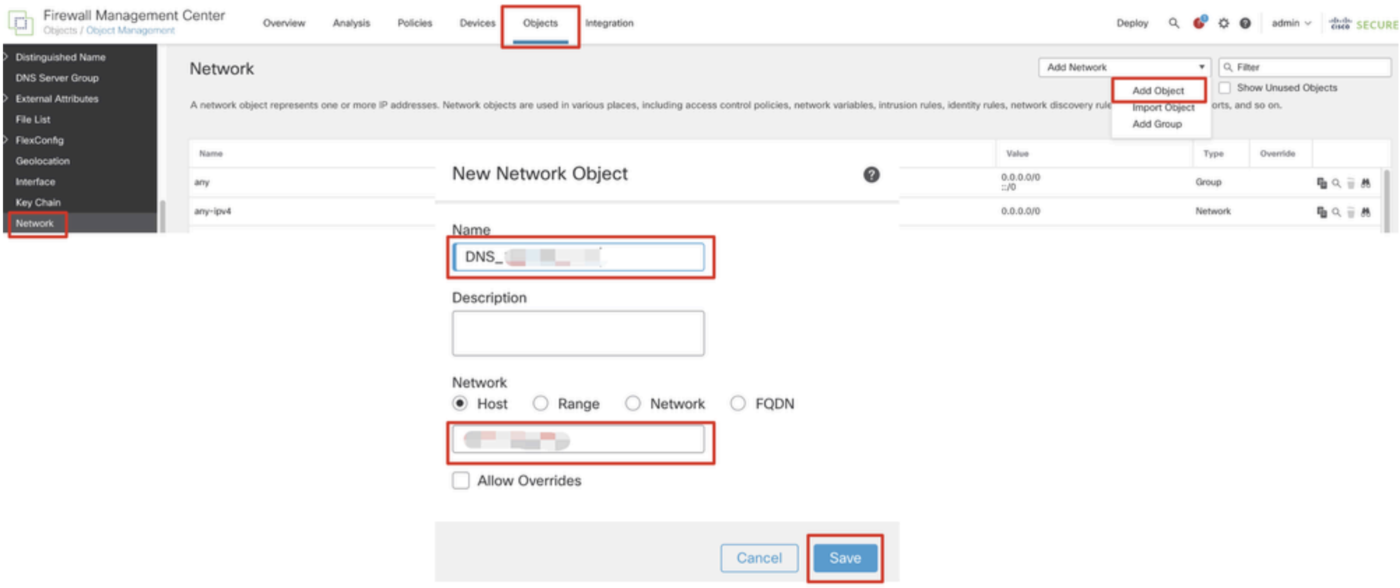
File Type:* Secure Client Image

Description:

FMC_Upload_Secure_Client_Image

Stap 4. Navigeer naar Objects > Object Management > Network.

Stap 4.1. Maak een object voor de DNS-server. Klik op Add Object, geef de naam en het beschikbare DNS-IP-adres op. Klik op de knop .Save



Network

☐ Show Unused Objects

A network object represents one or more IP addresses. Network objects are used in various places, including access control policies, network variables, intrusion rules, identity rules, network discovery rule... orts, and so on.

Name	Value	Type	Override
any	0.0.0.0/0 ::/0	Group	
any-ipv4	0.0.0.0/0	Network	

New Network Object

Name: DNS_[redacted]

Description:

Network: ● Host ○ Range ○ Network ○ FQDN

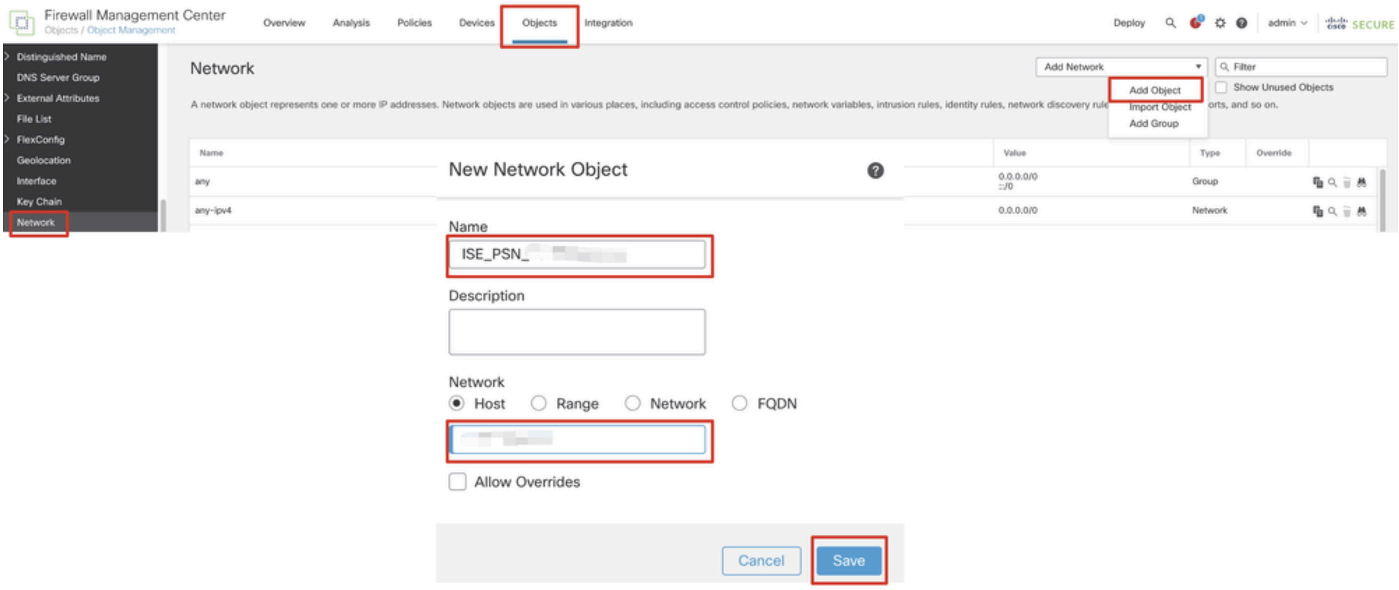
[redacted]

☐ Allow Overrides

FMC_Add_Object_DNS

Opmerking: DNS-server die hier is geconfigureerd moet worden gebruikt voor VPN-gebruikers.

Stap 4.2. Maak een object voor ISE-PSN. Klik op Add Object, geef de naam en het beschikbare IP-adres van ISE-PSN op. Klik op de knop .Save



Firewall Management Center
Objects / Object Management

Overview Analysis Policies Devices Objects Integration

Deploy admin SECURE

Distinguished Name
DNS Server Group
External Attributes
File List
FlexConfig
Geolocation
Interface
Key Chain
Network

Network

Add Network ▾ Filter
Add Object
Import Object
Add Group
☐ Show Unused Objects

A network object represents one or more IP addresses. Network objects are used in various places, including access control policies, network variables, intrusion rules, identity rules, network discovery rul… …orts, and so on.

Name	Value	Type	Override
any	0.0.0.0/0 ::/0	Group	
any-ipv4	0.0.0.0/0	Network	

New Network Object

Name
ISE_PSN_[redacted]

Description

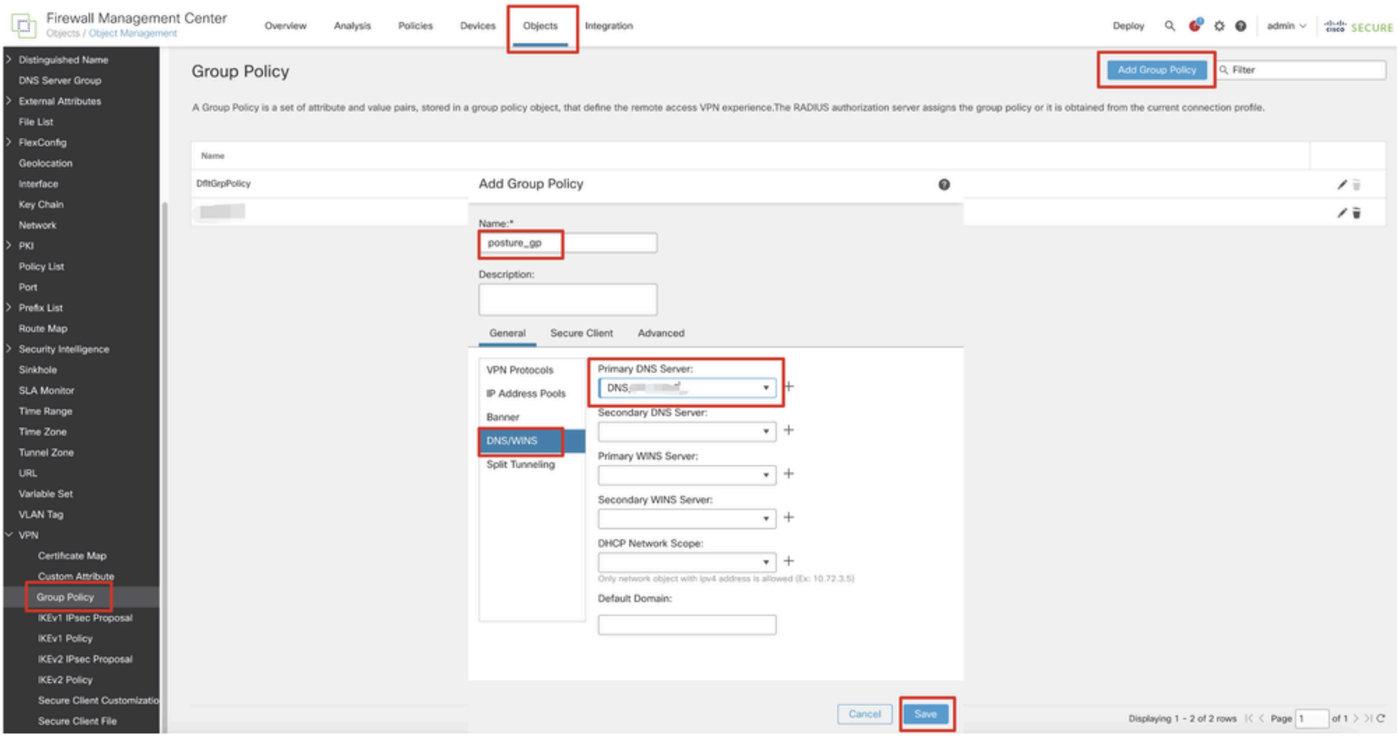
Network
● Host ○ Range ○ Network ○ FQDN
[redacted]

☐ Allow Overrides

Cancel Save

FMC_Add_Object_ISE

Stap 5. Navigeer naar Objects > Object Management > VPN > Group Policy. Klik op de knop .Add Group Policy Klik op DNS/WINS, selecteer het object van de DNS-server in Primary DNS Server. Klik vervolgens op Save.



Firewall Management Center
Objects / Object Management

Overview Analysis Policies Devices Objects Integration

Deploy admin SECURE

Distinguished Name
DNS Server Group
External Attributes
File List
FlexConfig
Geolocation
Interface
Key Chain
Network
PKI
Policy List
Port
Prefix List
Route Map
Security Intelligence
Sinkhole
SLA Monitor
Time Range
Time Zone
Tunnel Zone
URL
Variable Set
VLAN Tag
VPN
Certificate Map
Custom Attribute
Group Policy
IKEv1 IPsec Proposal
IKEv1 Policy
IKEv2 IPsec Proposal
IKEv2 Policy
Secure Client Customizatio
Secure Client File

Group Policy

Add Group Policy Filter

A Group Policy is a set of attribute and value pairs, stored in a group policy object, that define the remote access VPN experience.The RADIUS authorization server assigns the group policy or it is obtained from the current connection profile.

Name
DfltGrpPolicy
[redacted]

Add Group Policy

Name:*
posture_gp

Description:

General Secure Client Advanced

VPN Protocols
IP Address Pools
Banner
DNS/WINS
Split Tunneling

Primary DNS Server:
DNS[redacted] ▾ +
Secondary DNS Server:
▾ +
Primary WINS Server:
▾ +
Secondary WINS Server:
▾ +
DHCP Network Scope:
▾ +
Only network object with ipv4 address is allowed (Ex: 10.72.3.5)
Default Domain:

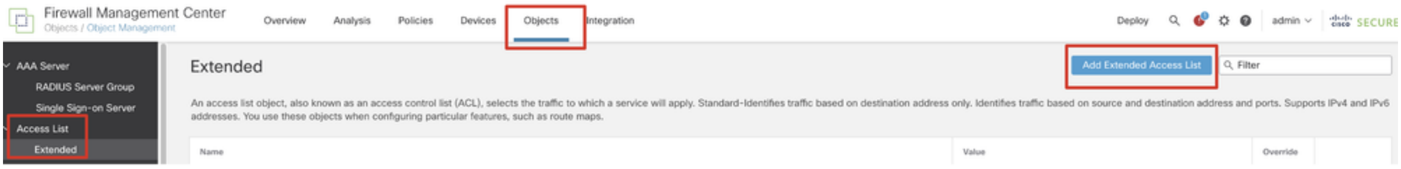
Cancel Save

Displaying 1 - 2 of 2 rows Page 1 of 1

FMC_Add_Group_Policy

Opmerking: zorg ervoor dat de DNS-server die wordt gebruikt in het VPN-groepsbeleid een oplossing kan bieden voor het ISE-client provisioningportal FQDN en enroll.cisco.com.

Stap 6. Navigeer naar Objects > Object Management > Access List > Extended. Klik op de knop .Add Extended Access List

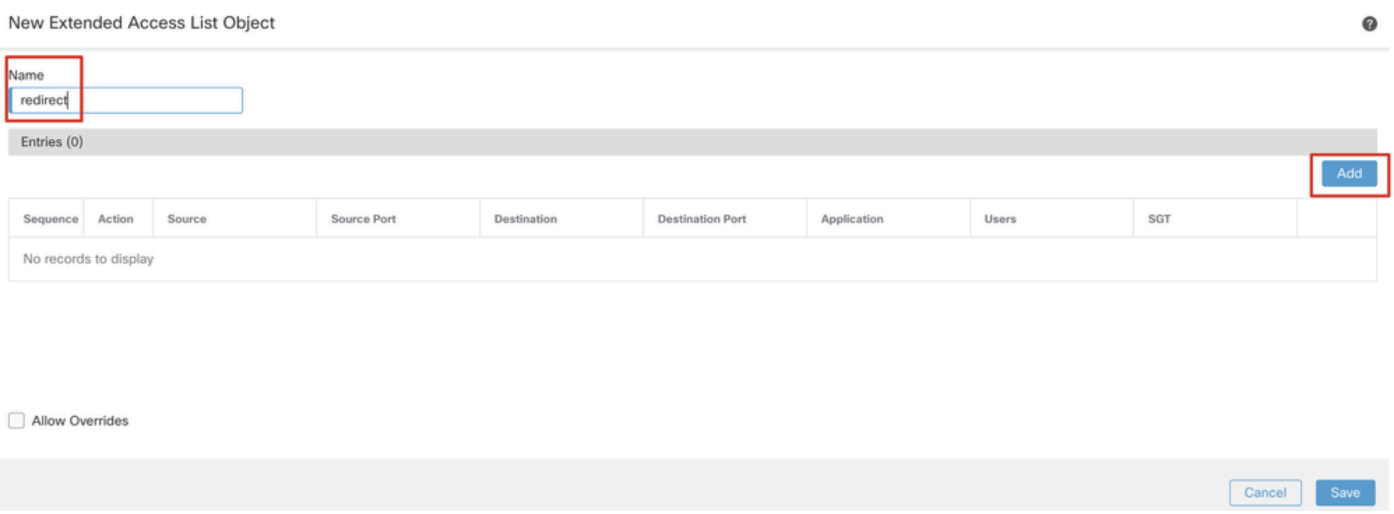


Extended

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.

VCC_Add_Redirect_ACL

Stap 6.1. Geef de naam op van de doorverwijzing ACL. Deze naam moet dezelfde zijn als in het ISE-autorisatieprofiel. Klik op de knop .Add



New Extended Access List Object

Name: redirect

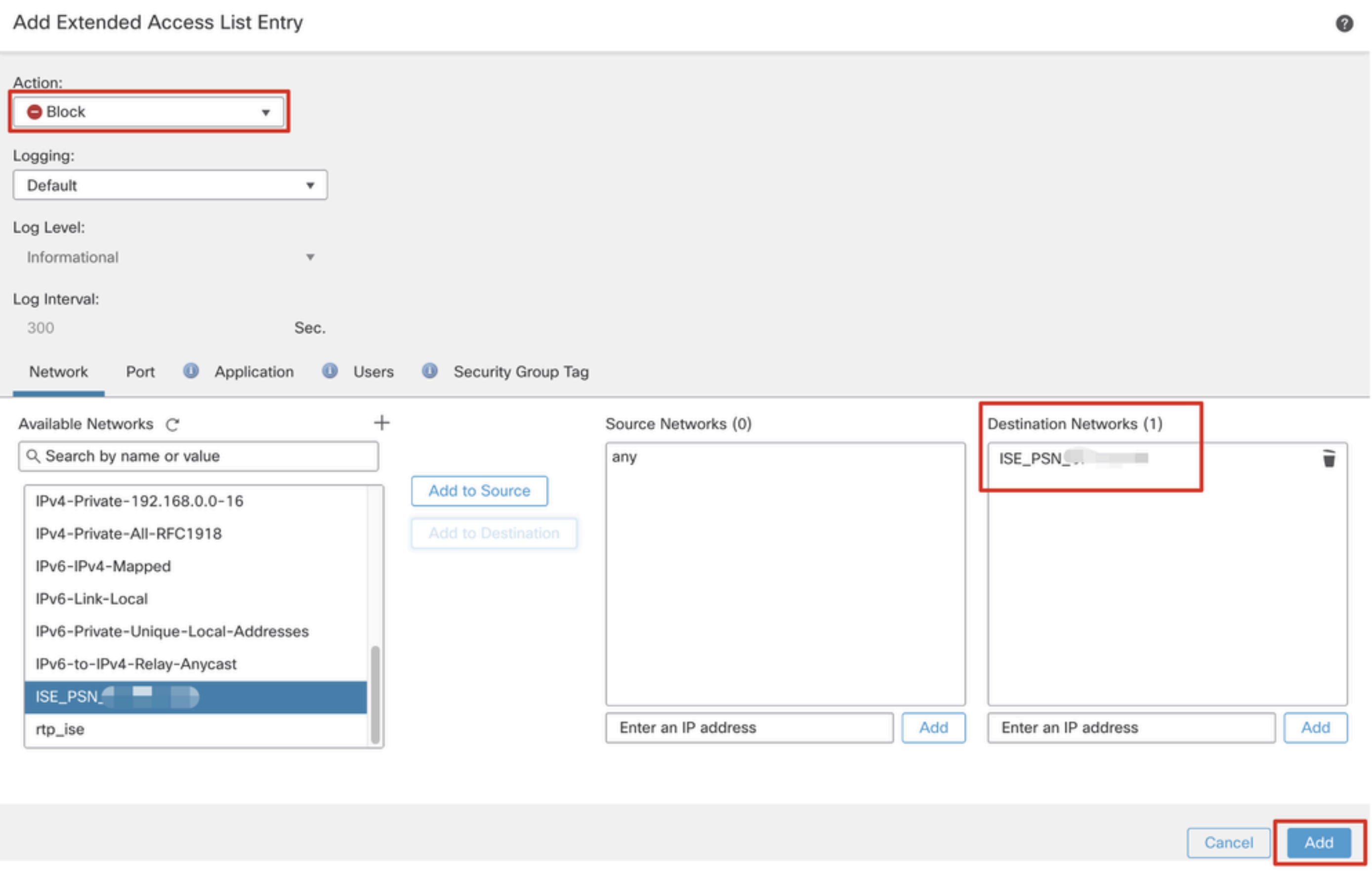
Entries (0)

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

□ Allow Overrides

FMC_Add_Redirect_ACL_Part_1

Stap 6.2. Blokkeer DNS-verkeer, verkeer naar ISE-PSN-IP-adres en de herstelservers om deze uit te sluiten van omleiding. Laat de rest van het verkeer toe. Dit activeert een omleiding. Klik op de knop .Save



Add Extended Access List Entry

Action: Block

Logging: Default

Log Level: Informational

Log Interval: 300 Sec.

Available Networks

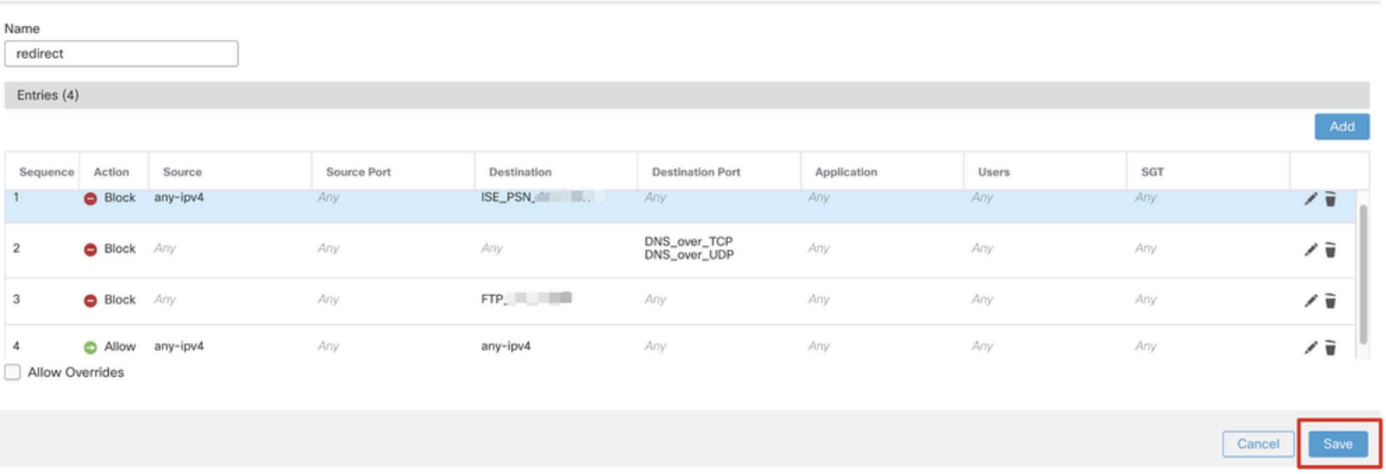
Search by name or value

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

Source Networks (0): any

Destination Networks (1): ISE_PSN_[redacted]

FMC_Add_Redirect_ACL_Part_2



Name

redirect

Entries (4)

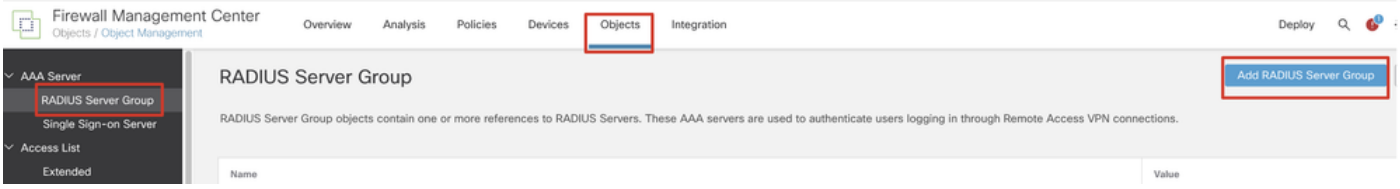
Sequence	Action	Source	Source Port	Destination	Destination Port	Application	Users	SGT
1	Block	any-ipv4	Any	ISE_PSN_[redacted]	Any	Any	Any	Any
2	Block	Any	Any	Any	DNS_over_TCP DNS_over_UDP	Any	Any	Any
3	Block	Any	Any	FTP_[redacted]	Any	Any	Any	Any
4	Allow	any-ipv4	Any	any-ipv4	Any	Any	Any	Any

□ Allow Overrides

FMC_Add_Redirect_ACL_Part_3

Opmerking: Bestemmings-FTP wordt in dit voorbeeld van omleiding van ACL gebruikt als voorbeeld van de herstelserver.

Stap 7. Navigeer naar Objects > Object Management > RADIUS Server Group. Klik op de knop .Add RADIUS Server Group

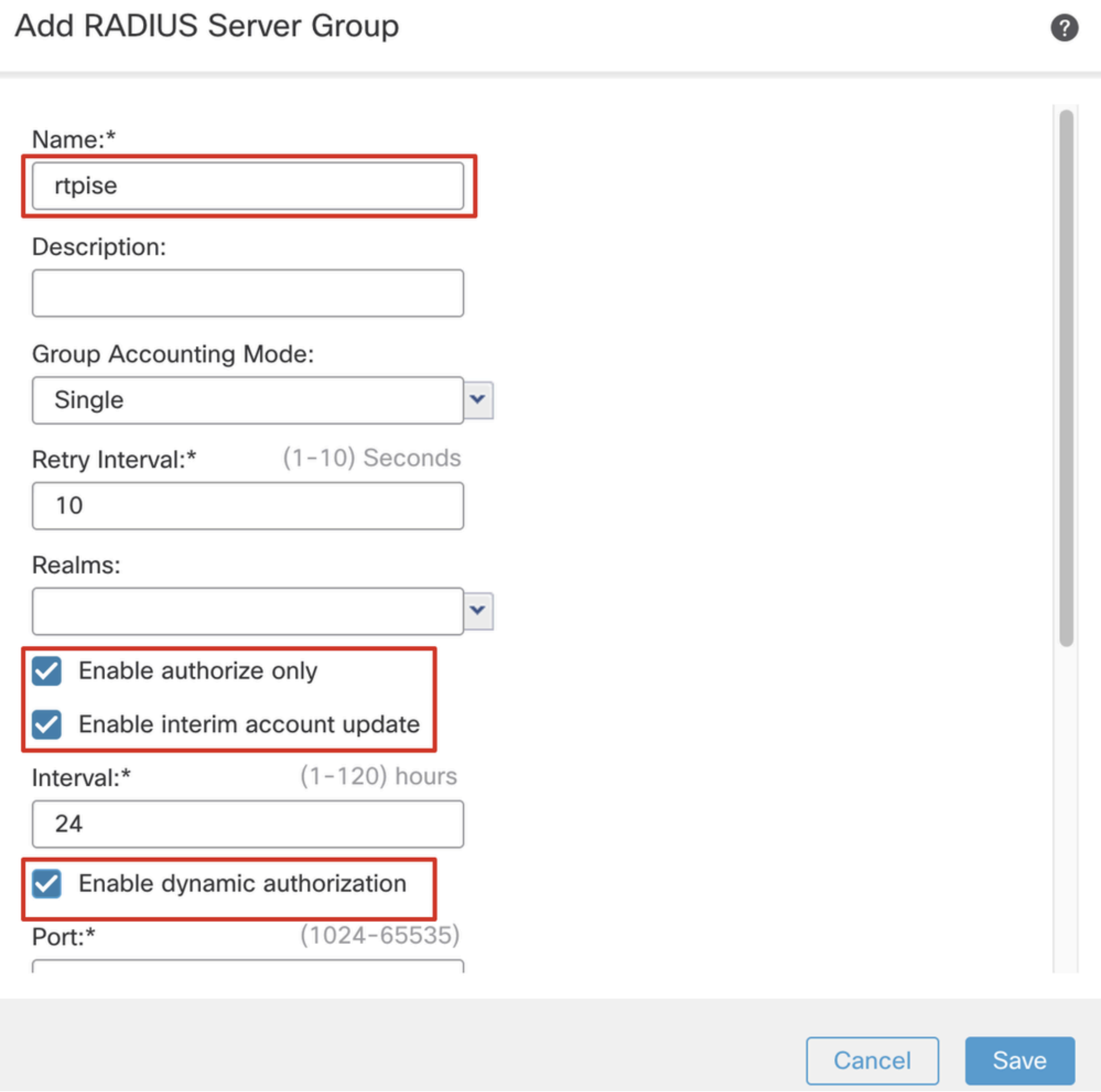


RADIUS Server Group

RADIUS Server Group objects contain one or more references to RADIUS Servers. These AAA servers are used to authenticate users logging in through Remote Access VPN connections.

FMC_Add_New_Radius_Server_Group

Stap 7.1. Geef naam, check Enable authorize only, check Enable interim account update, check 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

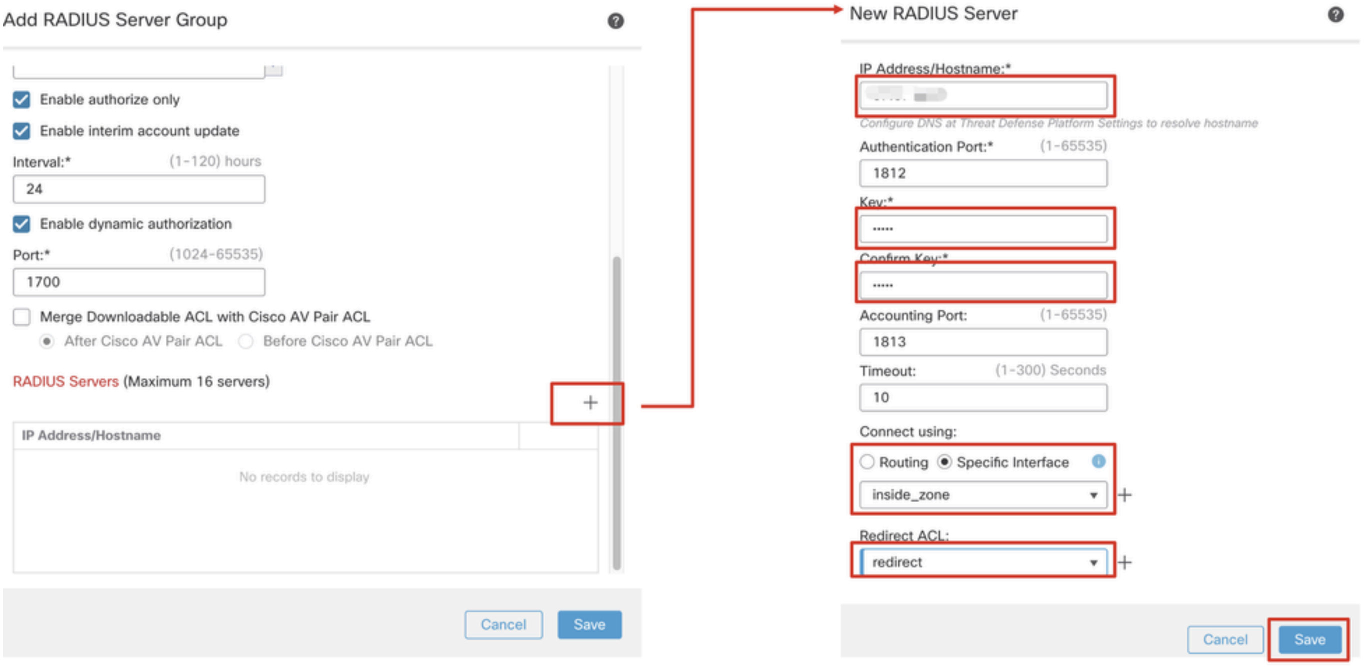
Interval:* (1-120) hours 24

☑ Enable dynamic authorization

Port:* (1024-65535)

FMC_Add_New_Radius_Server_Group_Part_1

Stap 7.2. Klik op het Plus pictogram om een nieuwe radiusserver toe te voegen. Verstrek ISE-PSN IP Address/Hostname, Key. Selecteer de modusspecific interface voor verbinding. Selecteer het Redirect ACL. Klik vervolgens op Saveom de nieuwe radiusserver op te slaan. Klik vervolgens nogmaals opSave om de nieuwe servergroep met de straal op te slaan.



Add RADIUS Server Group

☑ Enable authorize only

☑ Enable interim account update

Interval:* (1-120) hours: 24

☑ Enable dynamic authorization

Port:* (1024-65535): 1700

□ Merge Downloadable ACL with Cisco AV Pair ACL

● After Cisco AV Pair ACL ○ Before Cisco AV Pair ACL

RADIUS Servers (Maximum 16 servers)

IP Address/Hostname
No records to display

New RADIUS Server

IP Address/Hostname:*: [redacted]

Configure DNS at Threat Defense Platform Settings to resolve hostname

Authentication Port:* (1-65535): 1812

Key:*: •••••

Confirm Key:*: •••••

Accounting Port: (1-65535): 1813

Timeout: (1-300) Seconds: 10

Connect using:

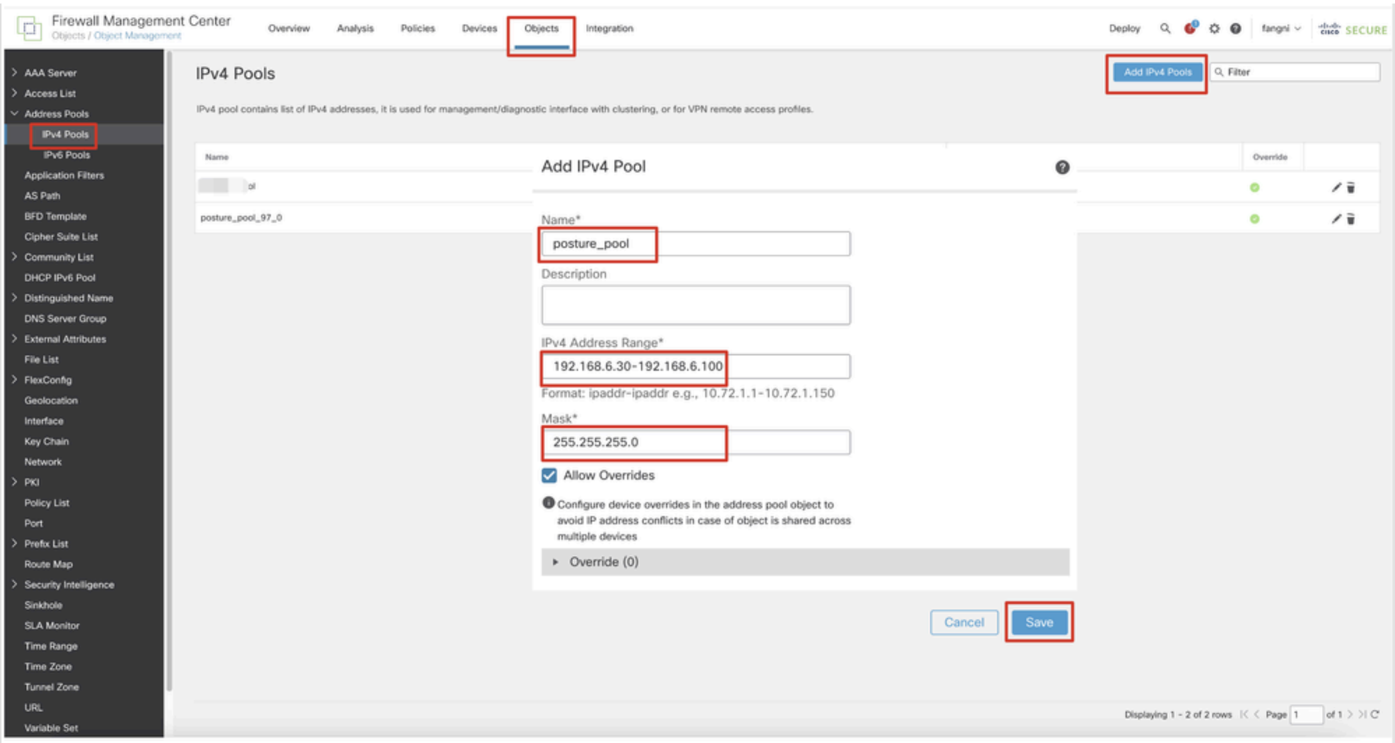
○ Routing ● Specific Interface

inside_zone

Redirect ACL: redirect

FMC_Add_New_Radius_Server_Group_Part_2

Stap 8. Navigeer naar Objects > Object Management > Address Pools > IPv4 Pools. Klik op Add IPv4 Pools de afbeelding **Name, IPv4 Address Range**en geef deze op Mask. Klik vervolgens op Save.



IPv4 Pools

IPv4 pool contains list of IPv4 addresses, it is used for management/diagnostic interface with clustering, or for VPN remote access profiles.

Name	Override
[redacted]	●
posture_pool_97_0	●

Add IPv4 Pool

Name*: posture_pool

Description:

IPv4 Address Range*: 192.168.6.30-192.168.6.100

Format: ipaddr-ipaddr e.g., 10.72.1.1-10.72.1.150

Mask*: 255.255.255.0

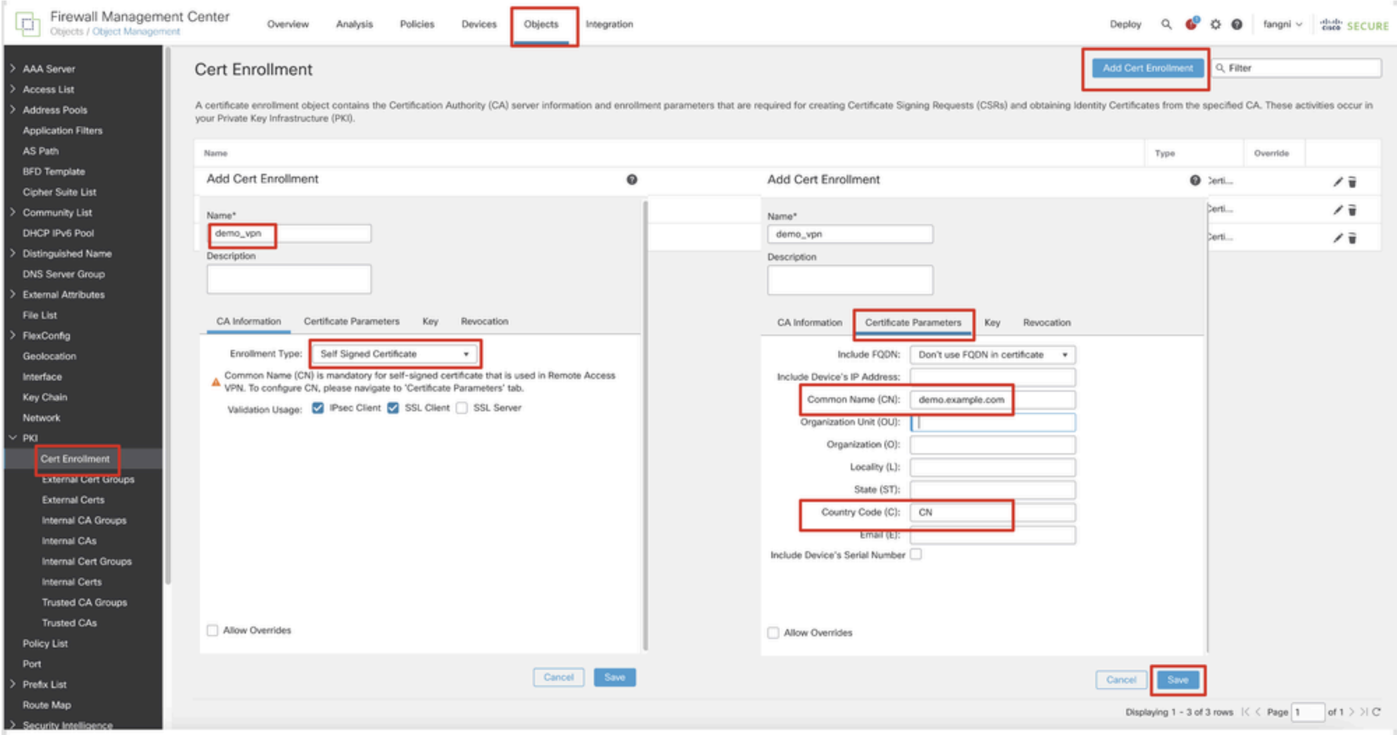
☑ Allow Overrides

Configure device overrides in the address pool object to avoid IP address conflicts in case of object is shared across multiple devices

▸ Override (0)

FMC_Add_New_Pool

Stap 9. Navigeer naar Certificate Objects > Object Management > PKI > Cert Enrollment. Klik op Add Cert Enrollment, geef een naam op en selecteer Self Signed Certificatein Enrollment Type. Klik op het Certificate Parameters tabblad en specificeer Common Name en Country Code. Klik vervolgens op Save.



Cert Enrollment

A certificate enrollment object contains the Certification Authority (CA) server information and enrollment parameters that are required for creating Certificate Signing Requests (CSRs) and obtaining Identity Certificates from the specified CA. These activities occur in your Private Key Infrastructure (PKI).

Add Cert Enrollment

Name*: demo_vpn

Description:

Enrollment Type: Self Signed Certificate

Common Name (CN) is mandatory for self-signed certificate that is used in Remote Access VPN. To configure CN, please navigate to 'Certificate Parameters' tab.

Validation Usage: ☑ IPsec Client ☑ SSL Client □ SSL Server

Add Cert Enrollment

Name*: demo_vpn

Include FQDN: Don't use FQDN in certificate

Include Device's IP Address:

Common Name (CN): demo.example.com

Organization Unit (OU):

Organization (O):

Locality (L):

State (ST):

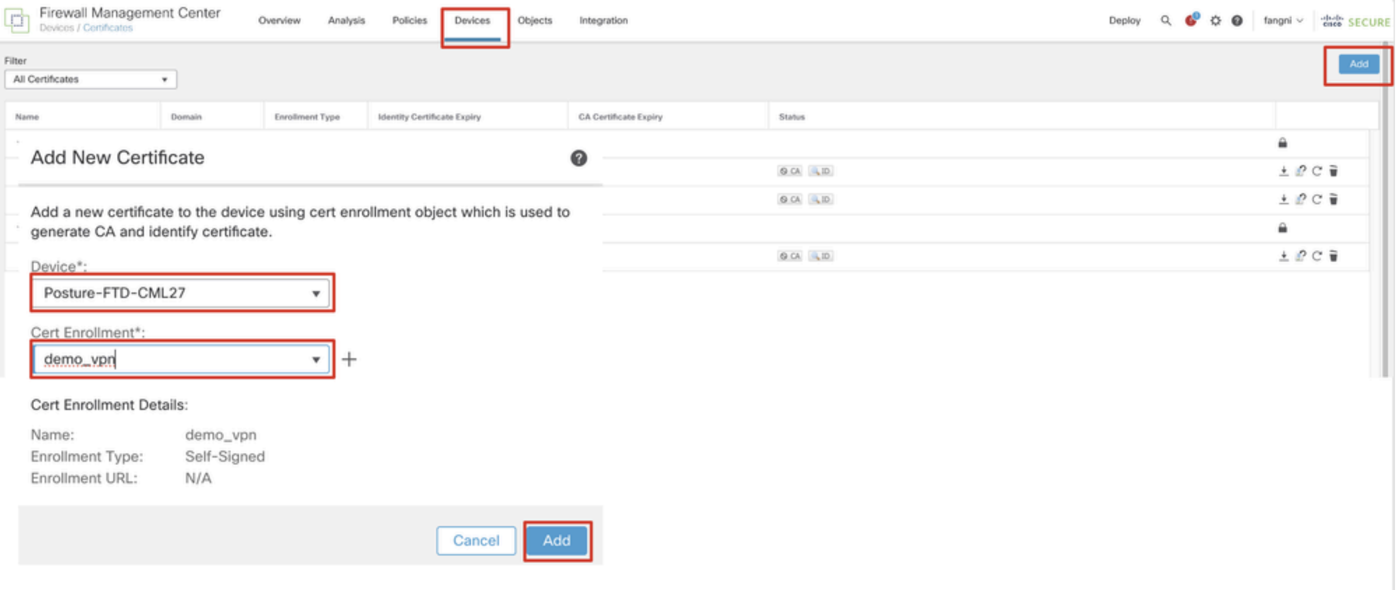
Country Code (C): CN

Email (E):

Include Device's Serial Number □

VCC_Add_New_Cert_Enroll

Stap 10. Navigeer naar Devices > Certificates. Klik op Add, selecteer de FTD-naam onder Device, selecteer de vorige geconfigureerde inschrijving onder Cert Enrollment. Klik op de knop .Add



Add New Certificate

Add a new certificate to the device using cert enrollment object which is used to generate CA and identify certificate.

Device*: Posture-FTD-CML27

Cert Enrollment*: demo_vpn

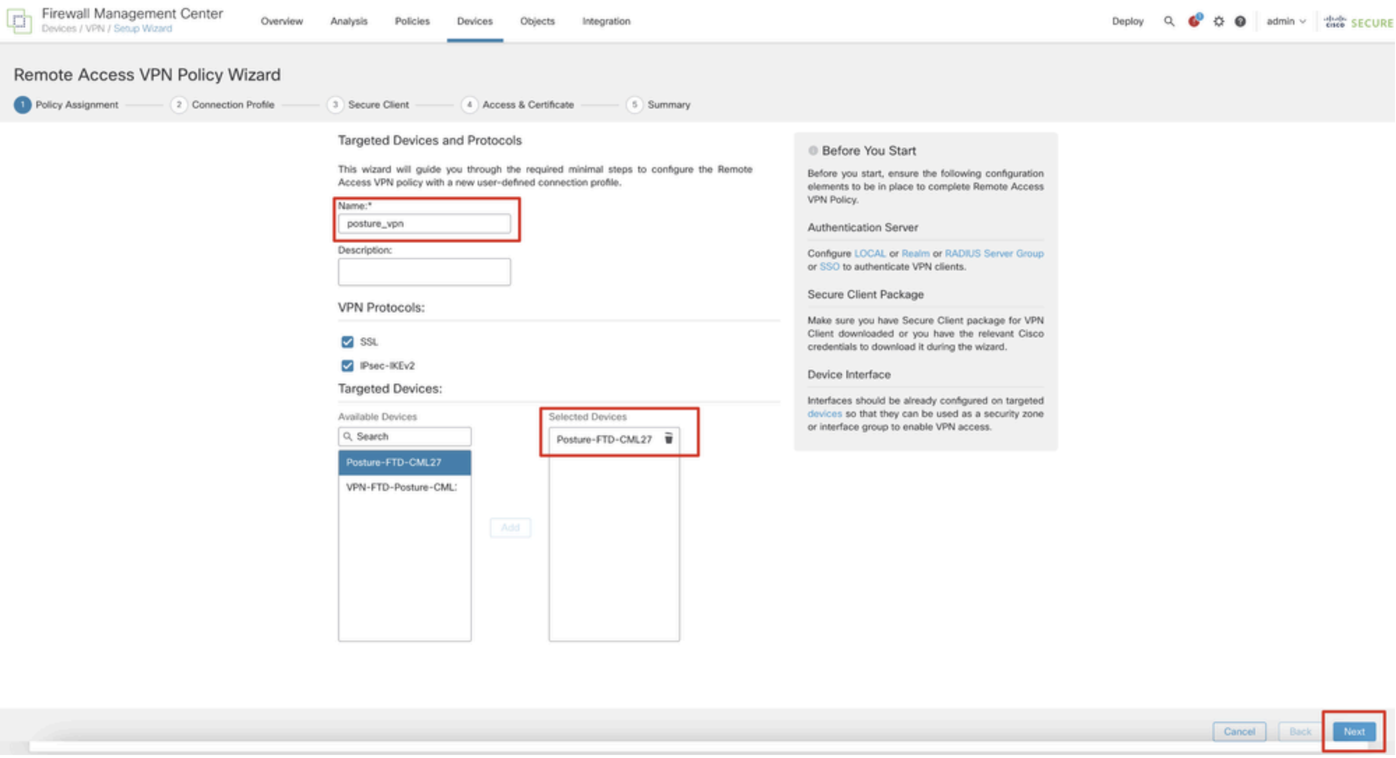
Cert Enrollment Details:

Name: demo_vpn
Enrollment Type: Self-Signed
Enrollment URL: N/A

FMC_Add_New_Cert_To_FTD

Stap 11. Navigeer naar Devices > VPN > Remote Access. Klik op de knop .Add

Stap 11.1. Geef de naam op en voeg het FTD toe aan Selected Devices. Klik op de knop .Next



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: Posture-FTD-CML27, VPN-FTD-Posture-CML

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

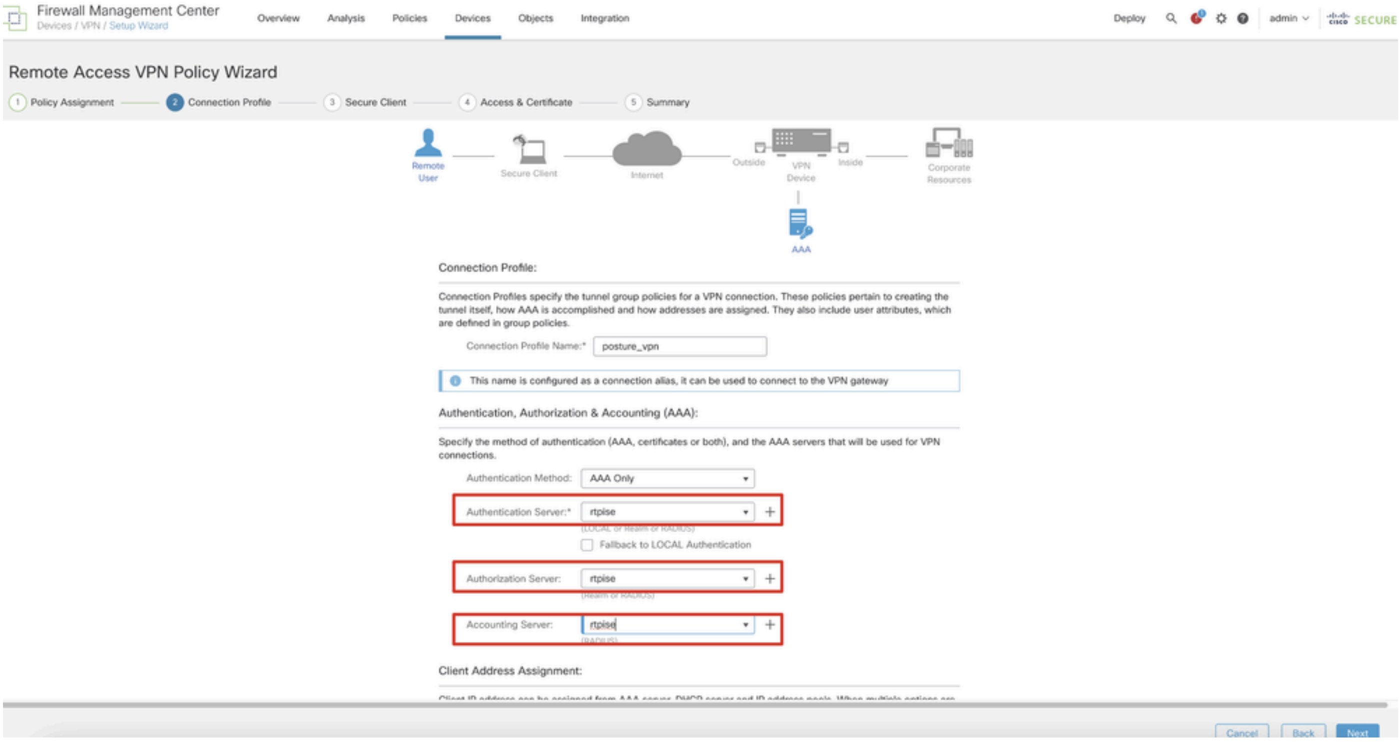
Make sure you have Secure Client package for VPN Client downloaded or you have the relevant Cisco credentials to download it during the wizard.

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.

FMC_New_RAVPN_Wizard_1

Stap 11.2. Selecteer een servergroep met een straal die eerder is geconfigureerd in de Authentication Server, Authorization Server, Accounting Server. Blader naar beneden op de pagina.



Remote Access VPN Policy Wizard

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

Connection Profile:

Connection Profiles specify the tunnel group policies for a VPN connection. These policies pertain to creating the tunnel itself, how 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 (LOCAL or Realm or RADIUS)

□ Fallback to LOCAL Authentication

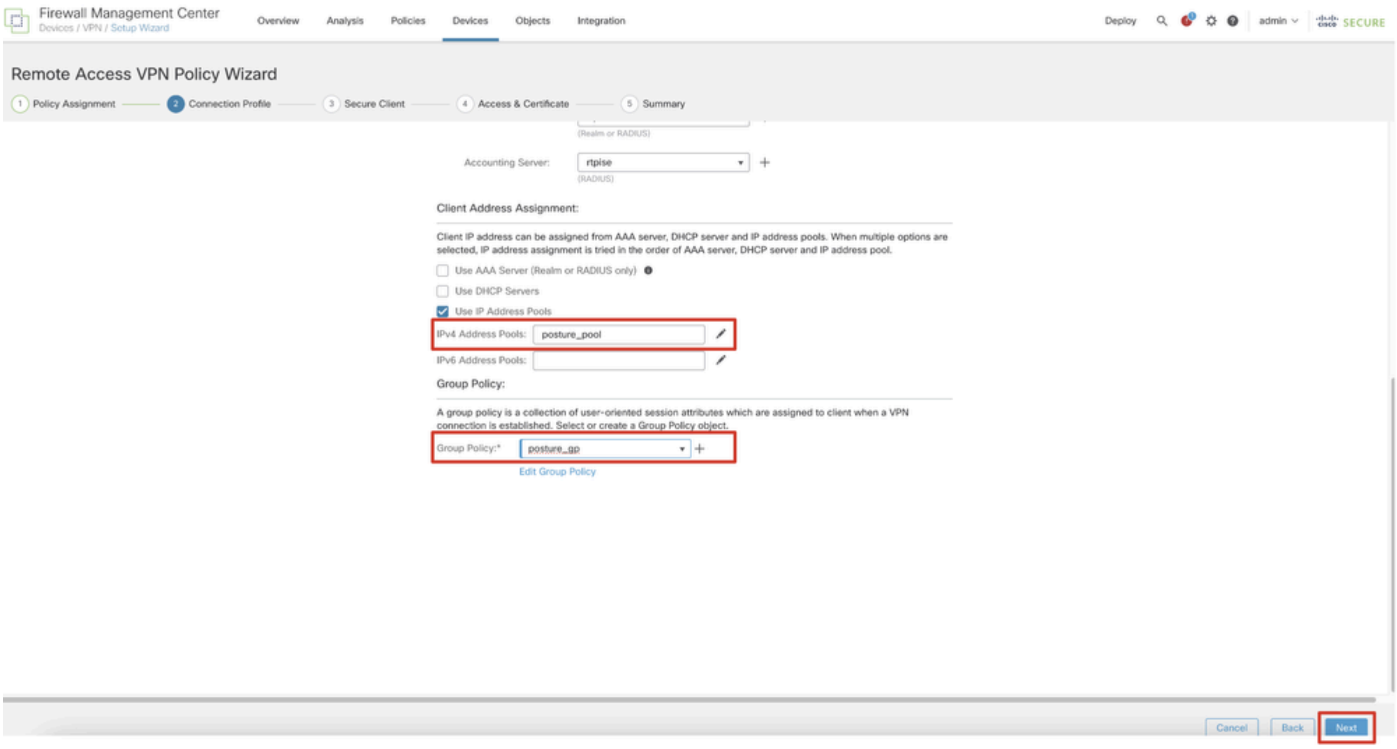
Authorization Server: rtpise (Realm or RADIUS)

Accounting Server: rtpise (RADIUS)

Client Address Assignment:

FMC_New_RAVPN_Wizard_2

Stap 11.3. Selecteer de eerder ingestelde poolnaam in IPv4 Address Pools. Selecteer eerder geconfigureerd groepsbeleid in Group Policy. Klik Next.



(Realm or RADIUS)

Accounting Server: rtpise ▾ +
(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: posture_pool

IPv6 Address Pools:

Group Policy:

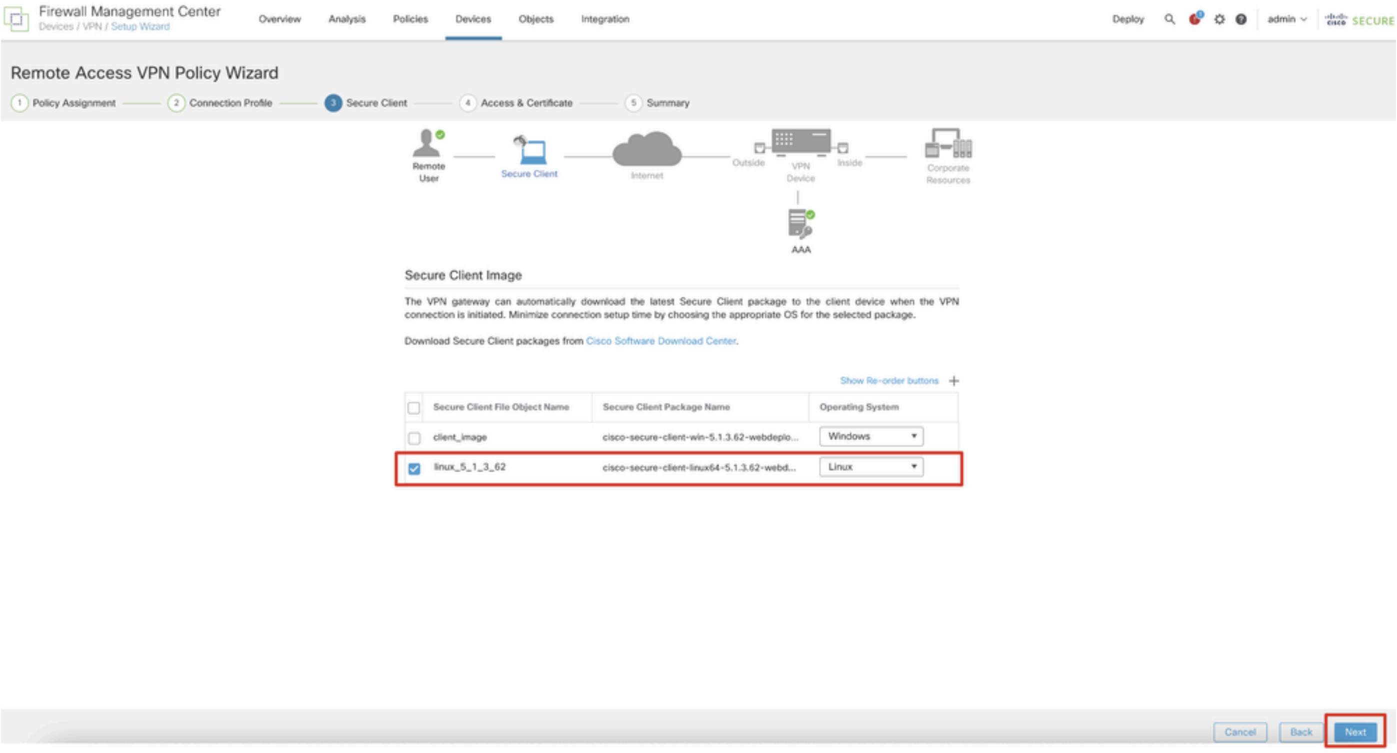
A group policy is a collection of user-oriented session attributes which are assigned to client when a VPN connection is established. Select or create a Group Policy object.

Group Policy:* posture_gp ▾ +

Edit Group Policy

FMC_New_RAVPN_Wizard_3

Stap 11.4. Schakel het selectievakje van de Linux-afbeelding in. Klik op de knop .Next



Secure Client Image

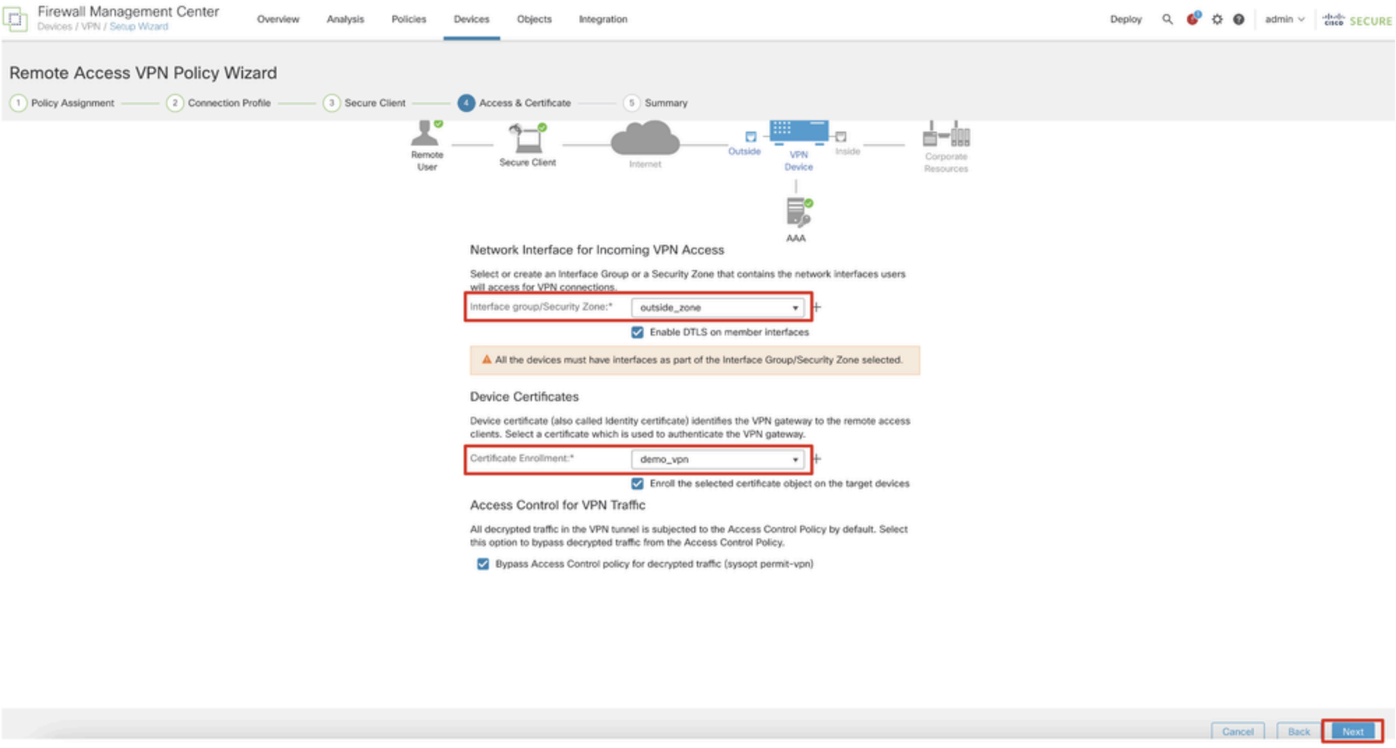
The VPN gateway can automatically download the latest Secure Client package to the client device when the VPN connection is initiated. Minimize connection setup time by choosing the appropriate OS for the selected package.

Download Secure Client packages from Cisco Software Download Center.

□	Secure Client File Object Name	Secure Client Package Name	Operating System
□	client_image	cisco-secure-client-win-5.1.3.62-webdeplo...	Windows ▾
☑	linux_5_1_3_62	cisco-secure-client-linux64-5.1.3.62-webd...	Linux ▾

FMC_New_RAVPN_Wizard_4

Stap 11.5. Selecteer de interface van VPN-interface. Selecteer de cert-inschrijving die is aangemeld voor FTD in stap 9. Klik op de knop .Next



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:* outside_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:* demo_vpn

☑ Enroll the selected certificate object on the target devices

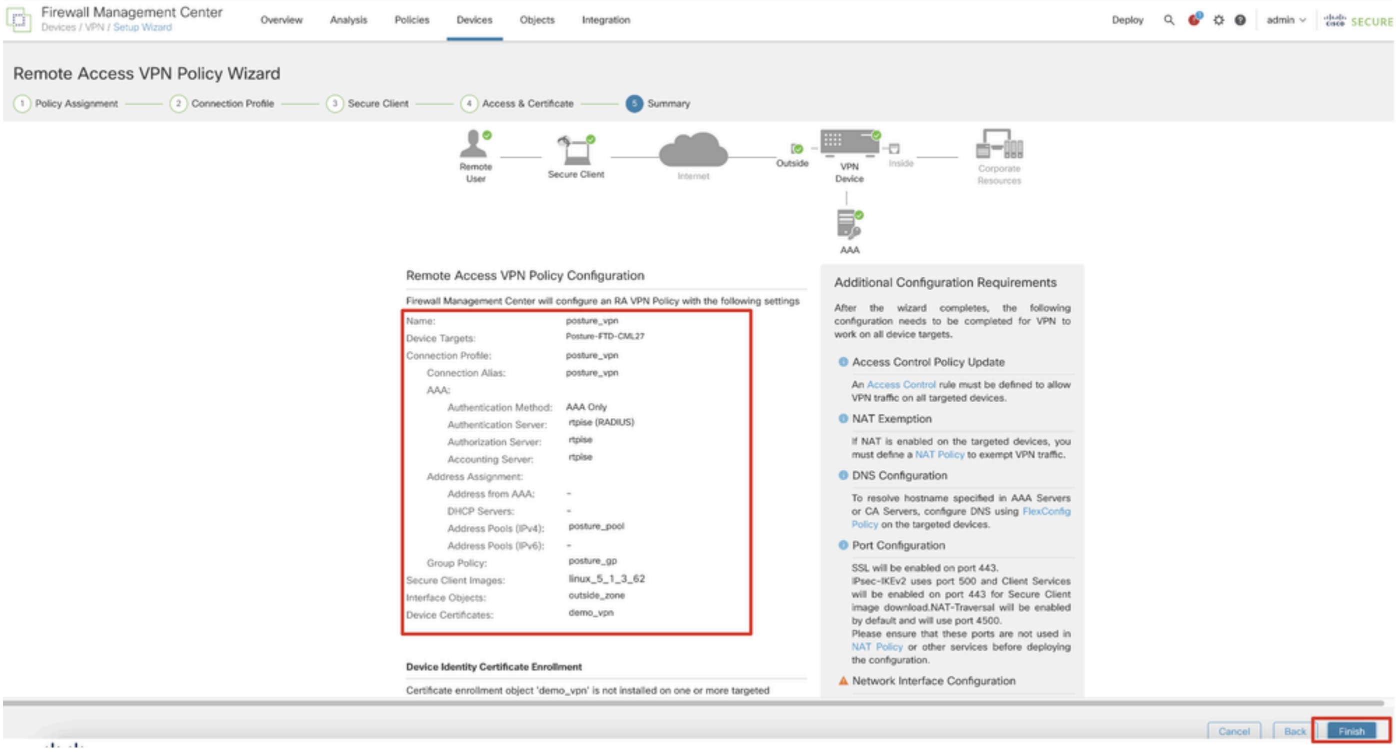
Access Control for VPN Traffic

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)

FMC_New_RAVPN_Wizard_5

Stap 11.6. Bevestig de gerelateerde informatie op de overzichtspagina. Als alles goed is, klikt u op Finish. Als u iets moet wijzigen, klikt u op Back.



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-CML27
Connection Profile:	posture_vpn
Connection Alias:	posture_vpn
AAA:	
Authentication Method:	AAA Only
Authentication Server:	rtpise (RADIUS)
Authorization Server:	rtpise
Accounting Server:	rtpise
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.

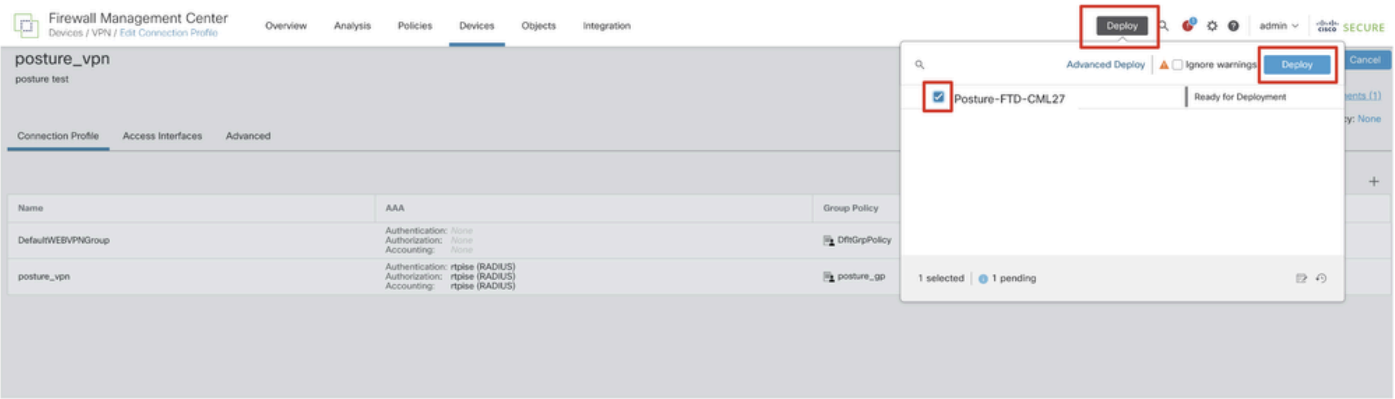
Port Configuration

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

FMC_New_RAVPN_Wizard_6

Stap 12. Implementeer de nieuwe configuratie in FTD om de configuratie van VPN voor externe toegang te voltooien.



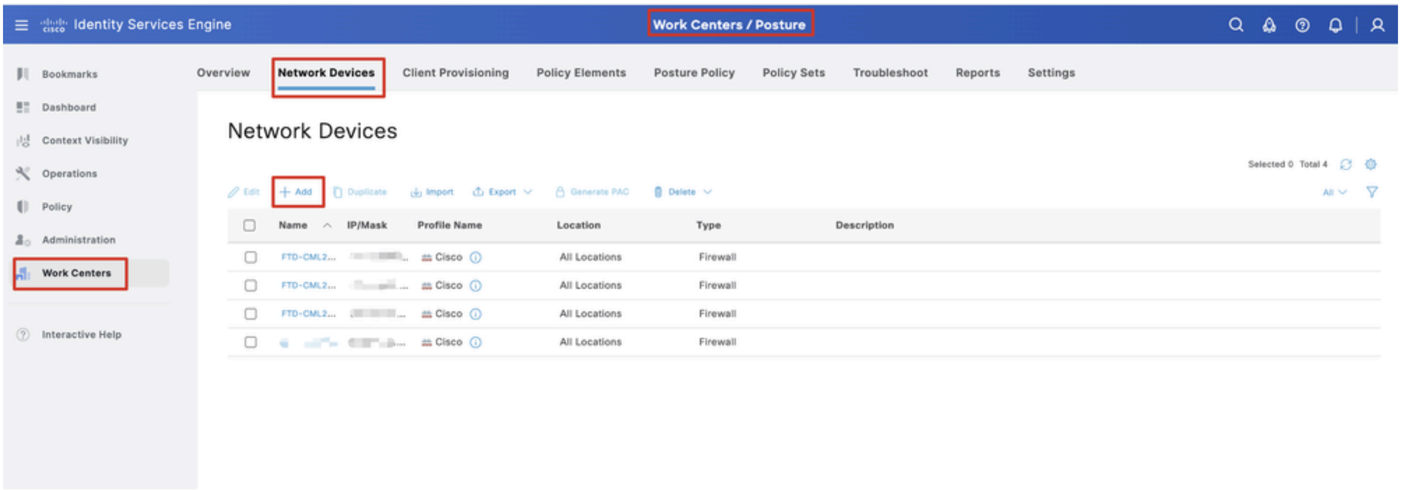
Name	AAA	Group Policy
DefaultWEBVPNGroup	Authentication: None Authorization: None Accounting: None	DfltGrpPolicy
posture_vpn	Authentication: rtpise (RADIUS) Authorization: rtpise (RADIUS) Accounting: rtpise (RADIUS)	posture_gp

☑ Posture-FTD-CML27 — Ready for Deployment

VCC_Implementatie_FTD

Configuraties op ISE

Stap 13. Navigeer naar Work Centers > Posture > Network Devices. Klik op de knop .Add

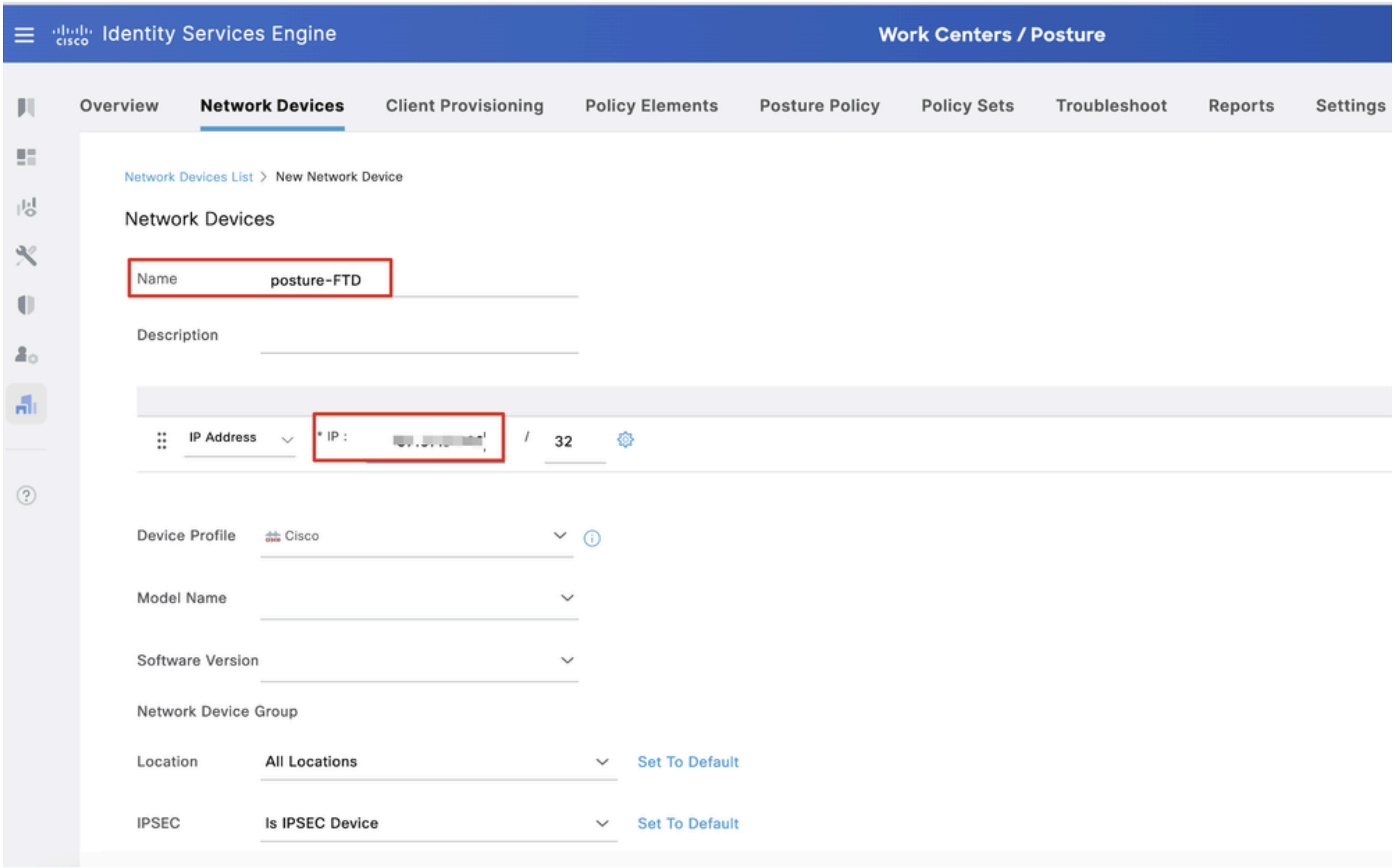


Network Devices

☐	Name	IP/Mask	Profile Name	Location	Type	Description
☐	FTD-CML2...	[redacted]	Cisco	All Locations	Firewall	
☐	FTD-CML2...	[redacted]	Cisco	All Locations	Firewall	
☐	FTD-CML2...	[redacted]	Cisco	All Locations	Firewall	
☐	[redacted]	[redacted]	Cisco	All Locations	Firewall	

ISE_Add_New_Devices

Stap 13.1. Verstrek de pagina Name, IP Addressen scrol de pagina omlaag.



Network Devices

Name posture-FTD

Description

IP Address * IP : [redacted] / 32

Device Profile Cisco

Model Name

Software Version

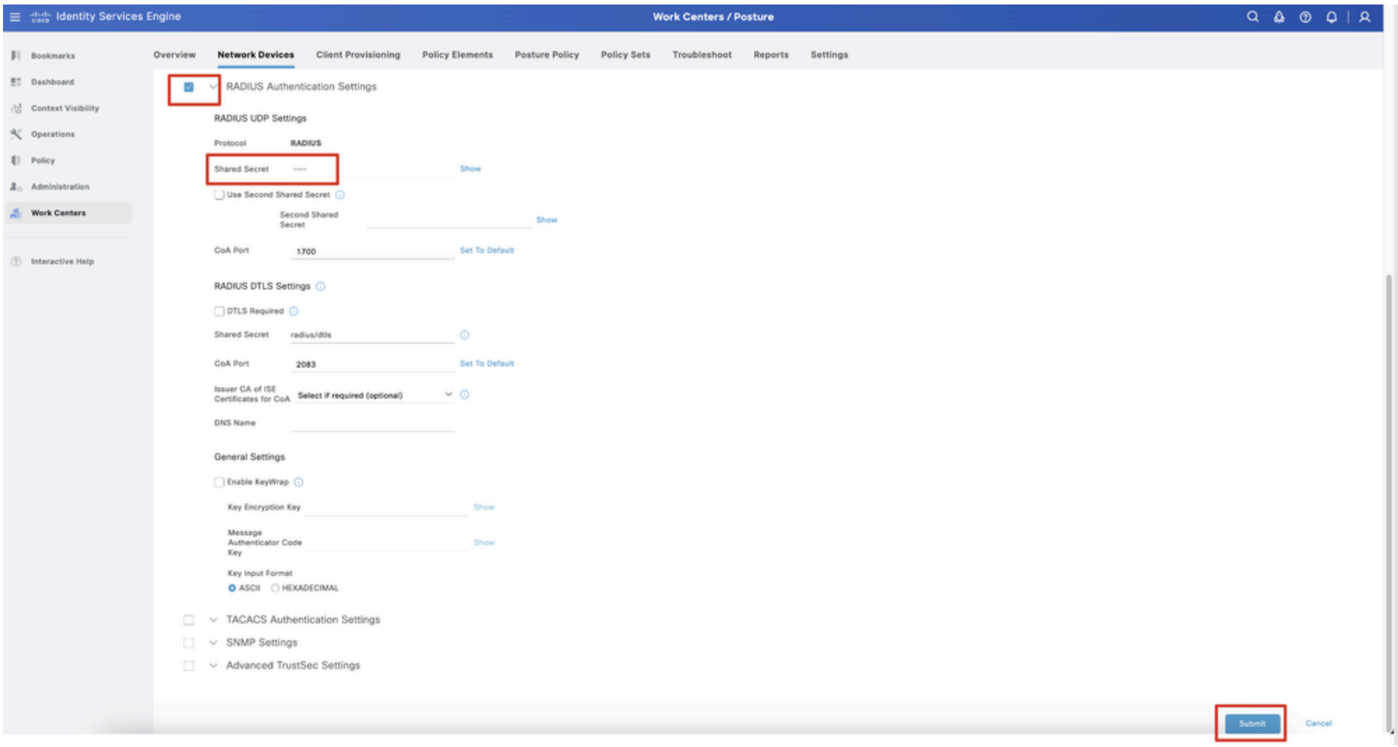
Network Device Group

Location All Locations

IPSEC Is IPSEC Device

ISE_add_new_devices_1

Stap 13.2. Schakel het selectievakje RADIUS Authentication Settings in. Geef het Shared Secret aan. Klik op de knop .Submit



☑ RADIUS Authentication Settings

RADIUS UDP Settings

Protocol RADIUS

Shared Secret •••••

□ Use Second Shared Secret

Second Shared Secret

CoA Port 1700

RADIUS DTLS Settings

□ DTLS Required

Shared Secret radius/dtls

CoA Port 2083

Issuer CA of ISE Certificates for CoA Select if required (optional)

DNS Name

General Settings

□ Enable KeyWrap

Key Encryption Key

Message Authenticator Code Key

Key Input Format

● ASCII ○ HEXADECIMAL

□ TACACS Authentication Settings

□ SNMP Settings

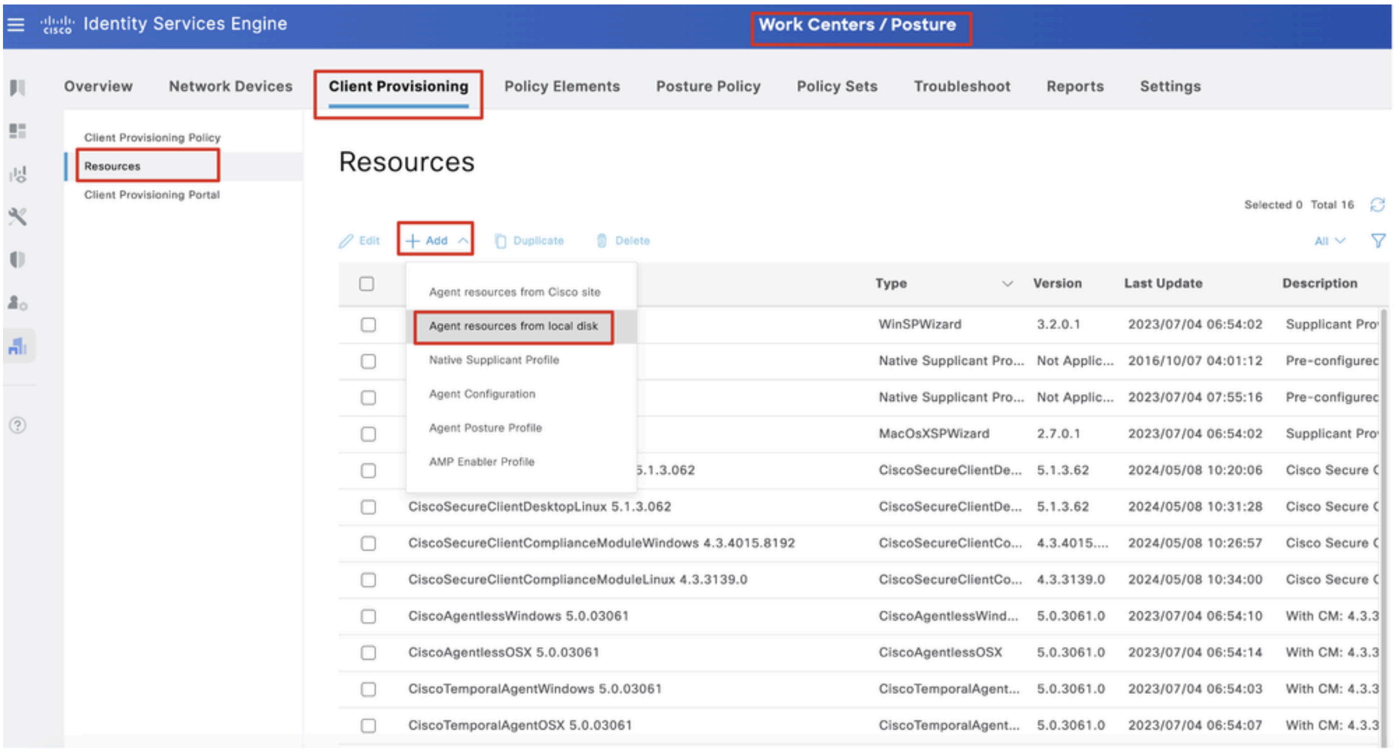
□ Advanced TrustSec Settings

ISE_add_new_devices_2

Stap 14. Download de pakketnaam cisco-secure-client-linux64-4.3.3139.0-isecompliance-webdeploy-k9.pkg van Cisco Software Download en zorg ervoor dat het bestand goed is door te bevestigen dat de MD5-checksum van het gedownloade bestand hetzelfde is als de pagina Cisco

Software Download. De pakketnaam cisco-secure-client-linux64-5.1.3.62-webdeploy-k9.pkg is gedownload in Stap 1.

Stap 15. Navigeer naar Work Centers > Posture > Client Provisioning > Resources. Klik op de knop .Add Selecteer Agent resources from local disk.

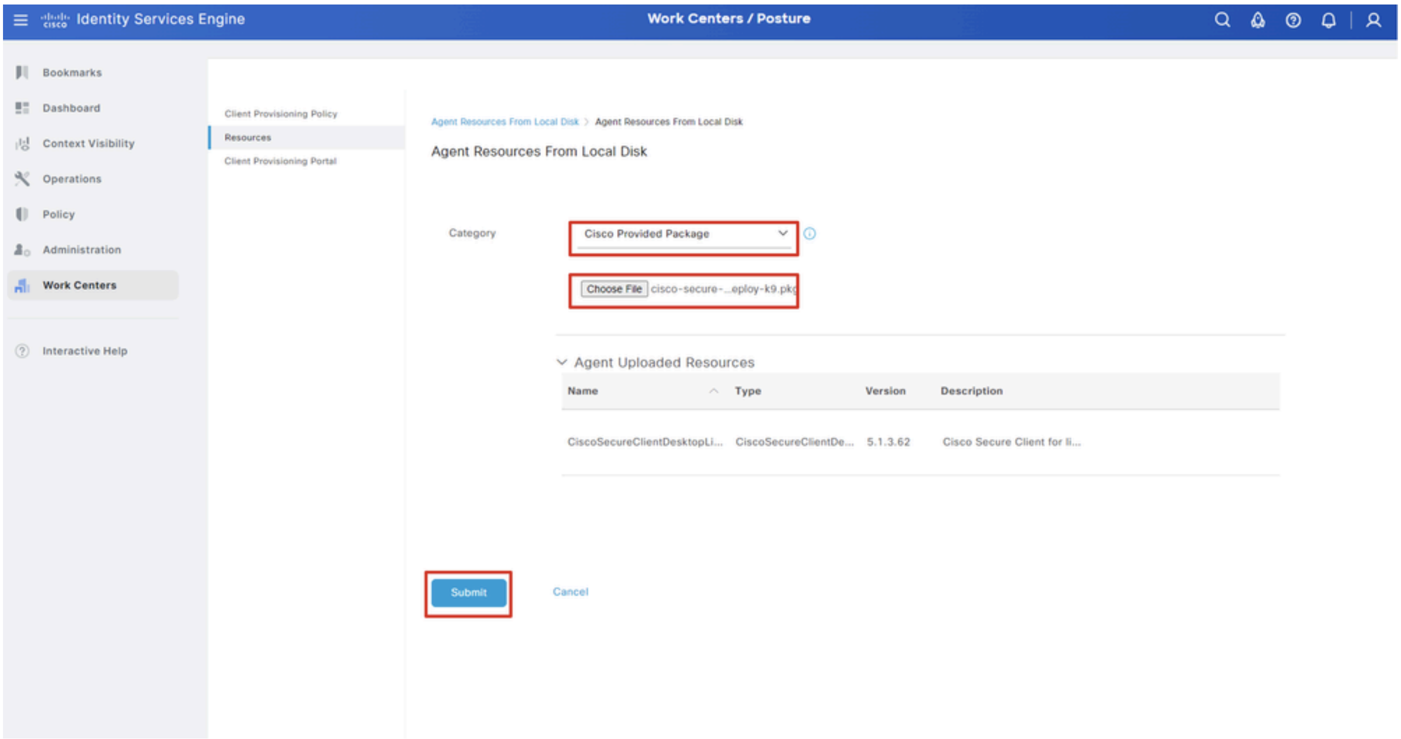


Resources

☐	Name	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-configurec
☐		Native Supplicant Pro...	Not Applic...	2023/07/04 07:55:16	Pre-configurec
☐		MacOsXSPWizard	2.7.0.1	2023/07/04 06:54:02	Supplicant Pro
☐	5.1.3.062	CiscoSecureClientDe...	5.1.3.62	2024/05/08 10:20:06	Cisco Secure C
☐	CiscoSecureClientDesktopLinux 5.1.3.062	CiscoSecureClientDe...	5.1.3.62	2024/05/08 10:31:28	Cisco Secure C
☐	CiscoSecureClientComplianceModuleWindows 4.3.4015.8192	CiscoSecureClientCo...	4.3.4015....	2024/05/08 10:26:57	Cisco Secure C
☐	CiscoSecureClientComplianceModuleLinux 4.3.3139.0	CiscoSecureClientCo...	4.3.3139.0	2024/05/08 10:34:00	Cisco Secure C
☐	CiscoAgentlessWindows 5.0.03061	CiscoAgentlessWind...	5.0.3061.0	2023/07/04 06:54:10	With CM: 4.3.3
☐	CiscoAgentlessOSX 5.0.03061	CiscoAgentlessOSX	5.0.3061.0	2023/07/04 06:54:14	With CM: 4.3.3
☐	CiscoTemporalAgentWindows 5.0.03061	CiscoTemporalAgent...	5.0.3061.0	2023/07/04 06:54:03	With CM: 4.3.3
☐	CiscoTemporalAgentOSX 5.0.03061	CiscoTemporalAgent...	5.0.3061.0	2023/07/04 06:54:07	With CM: 4.3.3

ISE_Upload_Resource

Stap 15.1. Selecteer Cisco Provided Package. Choose File Klik om cisco-secure-client-linux64-5.1.3.62-webimplementation-k9.pkg te uploaden. Klik op de knop .Submit



Agent Resources From Local Disk

Category: Cisco Provided Package

Choose File cisco-secure-...eploy-k9.pkg

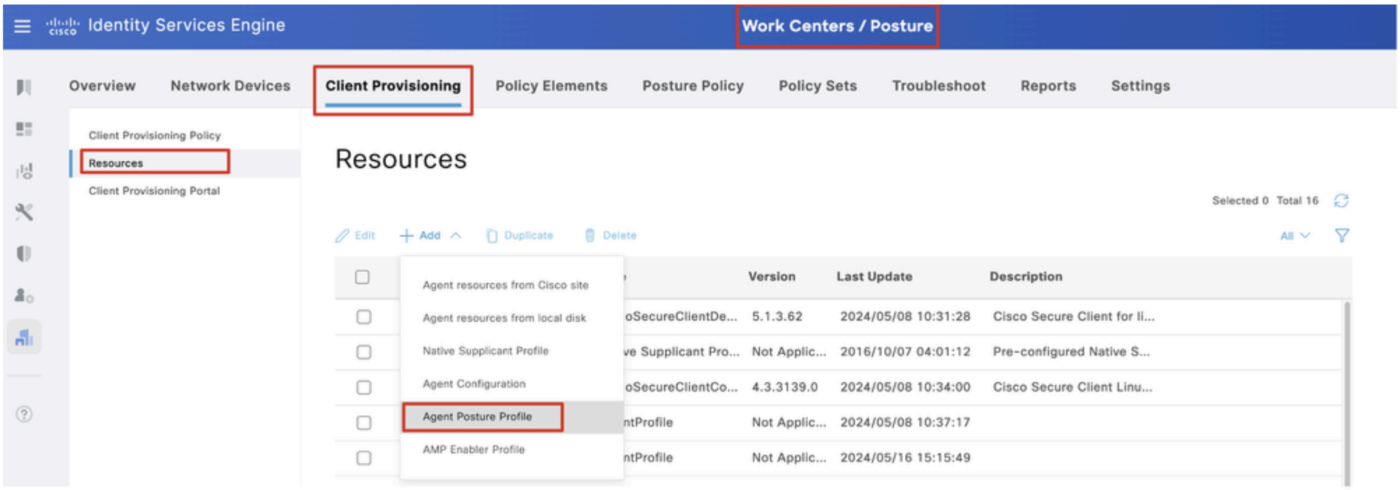
Agent Uploaded Resources

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

ISE_Upload_Resources_1

Opmerking: Herhaal stap 14. om te uploaden cisco-secure-client-linux64-4.3.3139.0-isecompliance-webdeploy-k9.pkg .

Stap 16. Navigeer naar Work Centers > Posture > Client Provisioning > Resources. Klik op de knop .Add Selecteer Agent Posture Profile.



Resources

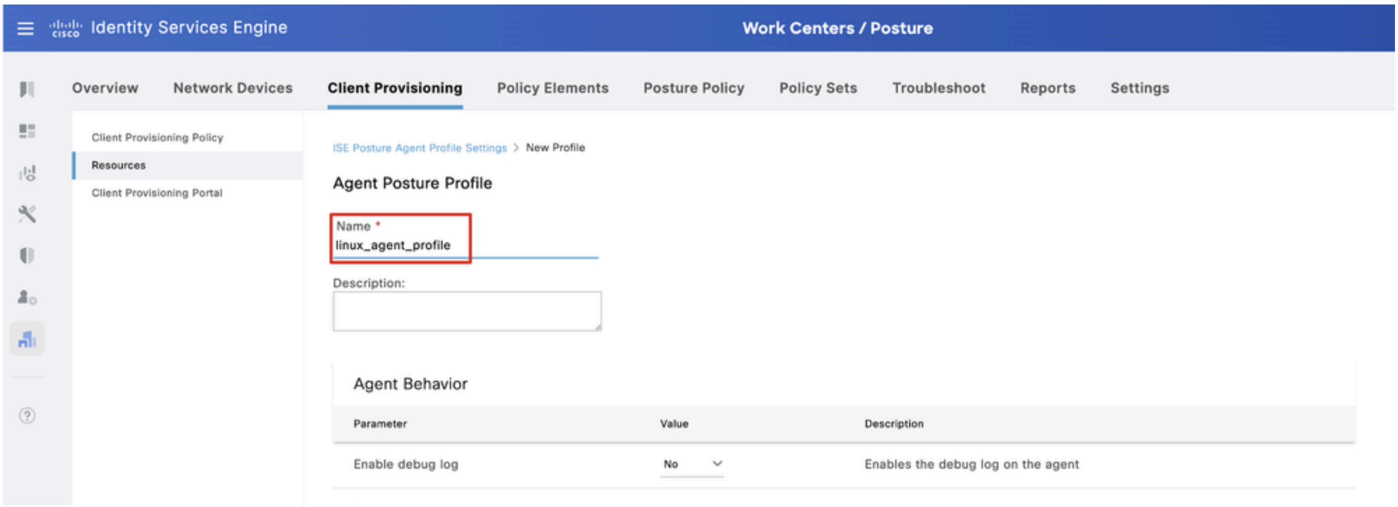
		Version	Last Update	Description
□	oSecureClientDe...	5.1.3.62	2024/05/08 10:31:28	Cisco Secure Client for li...
□	ve Supplicant Pro...	Not Applic...	2016/10/07 04:01:12	Pre-configured Native S...
□	oSecureClientCo...	4.3.3139.0	2024/05/08 10:34:00	Cisco Secure Client Linu...
□	ntProfile	Not Applic...	2024/05/08 10:37:17	
□	ntProfile	Not Applic...	2024/05/16 15:15:49	

ISE_Add_Agent_Posture_Profile

Stap 16.1. Verstrek het Name, Server name rules en bewaar de rest als standaard. Klik op de knop .Save

Naam: linux_agent_profile

Regels voor servernamen: *.example.com



Agent Posture Profile

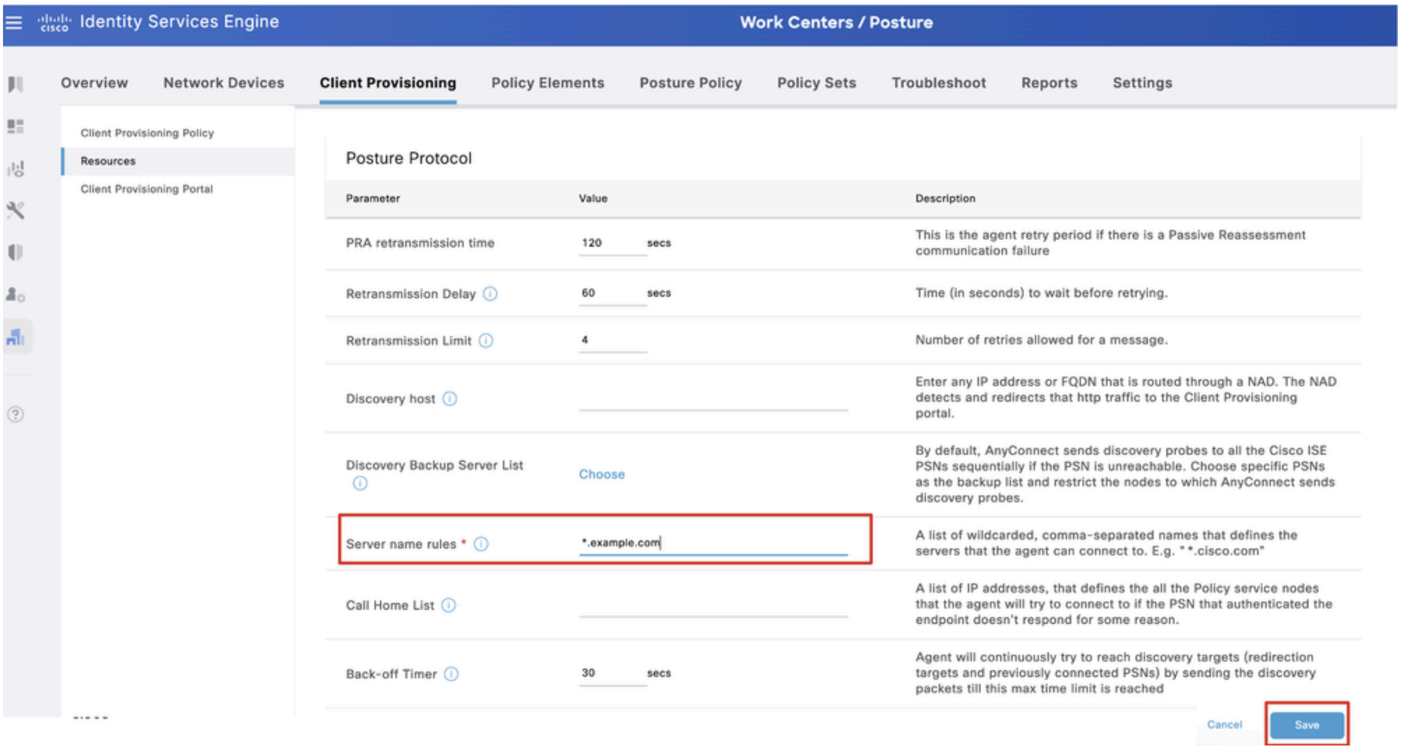
Name * linux_agent_profile

Description:

Agent Behavior

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

ISE_Add_Agent_Posture_Profile_1



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

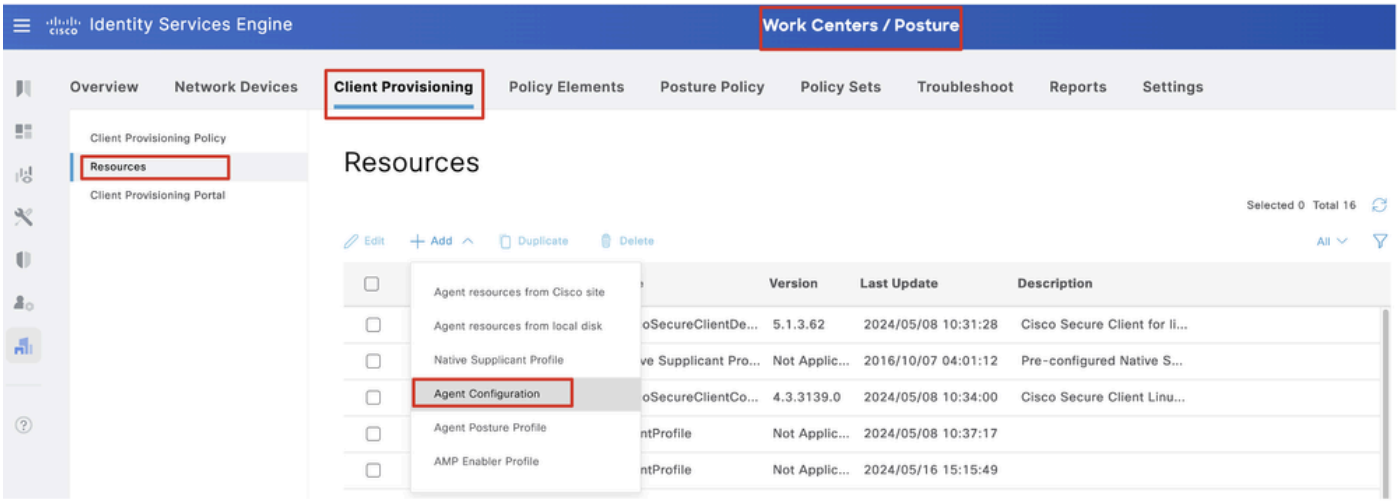
Posture Protocol

Parameter	Value	Description
PRA retransmission time	120 secs	This is the agent retry period if there is a Passive Reassessment communication failure
Retransmission Delay	60 secs	Time (in seconds) to wait before retrying.
Retransmission Limit	4	Number of retries allowed for a message.
Discovery host		Enter any IP address or FQDN that is routed through a NAD. The NAD detects and redirects that http traffic to the Client Provisioning portal.
Discovery Backup Server List	Choose	By default, AnyConnect sends discovery probes to all the Cisco ISE PSNs sequentially if the PSN is unreachable. Choose specific PSNs as the backup list and restrict the nodes to which AnyConnect sends discovery probes.
Server name rules *	*.example.com	A list of wildcarded, comma-separated names that defines the servers that the agent can connect to. E.g. "*.cisco.com"
Call Home List		A list of IP addresses, that defines the all the Policy service nodes that the agent will try to connect to if the PSN that authenticated the endpoint doesn't respond for some reason.
Back-off Timer	30 secs	Agent will continuously try to reach discovery targets (redirection targets and previously connected PSNs) by sending the discovery packets till this max time limit is reached

Cancel | Save

ISE_Add_Agent_Posture_Profile_2

Stap 17. Navigeer naar Work Centers > Posture > Client Provisioning > Resources. Klik op de knop .Add Selecteer Agent Configuration.



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

Resources

Selected 0 Total 16

Edit | + Add | Duplicate | Delete | All

Agent resources from Cisco site
Agent resources from local disk
Native Supplicant Profile
Agent Configuration
Agent Posture Profile
AMP Enabler Profile

		Version	Last Update	Description
□	oSecureClientDe...	5.1.3.62	2024/05/08 10:31:28	Cisco Secure Client for li...
□	ve Supplicant Pro...	Not Applic...	2016/10/07 04:01:12	Pre-configured Native S...
□	oSecureClientCo...	4.3.3139.0	2024/05/08 10:34:00	Cisco Secure Client Linu...
□	ntProfile	Not Applic...	2024/05/08 10:37:17	
□	ntProfile	Not Applic...	2024/05/16 15:15:49	

ISE_Add_Agent_Configuration

Stap 17.2. Configureer de details:

Select Agent-pakket: Cisco SecureClientDesktopLinux 5.1.3.062

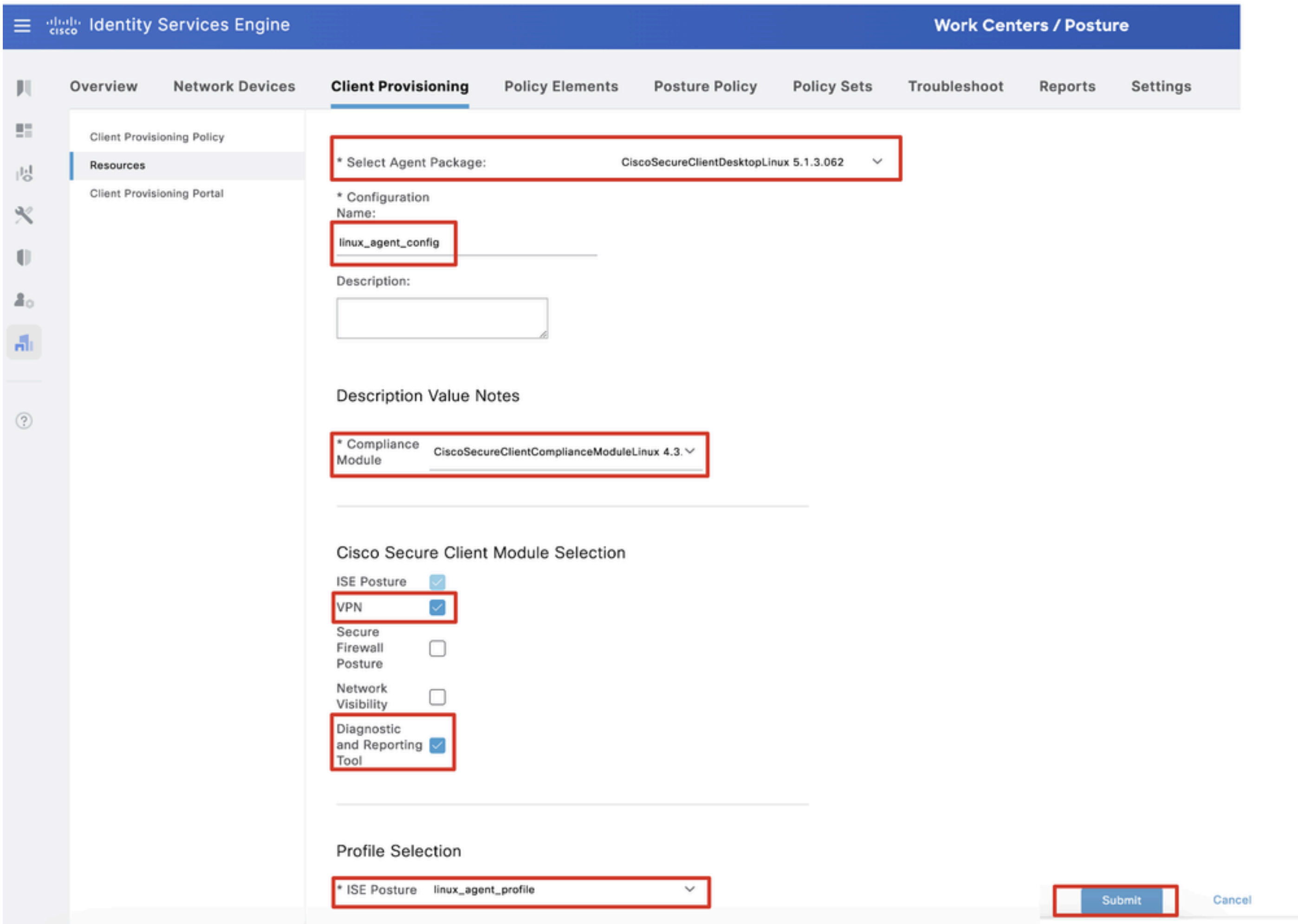
Naam: linux_agent_config

Nalevingsmodule: Cisco Secure ClientCompliance-moduleLinux 4.3.313.0

Schakel het selectievakje in van VPN, Diagnostic and Reporting Tool

Profiel Selectie ISE Positie: linux_agent_profile

Klik op de knop .Submit



* 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 □

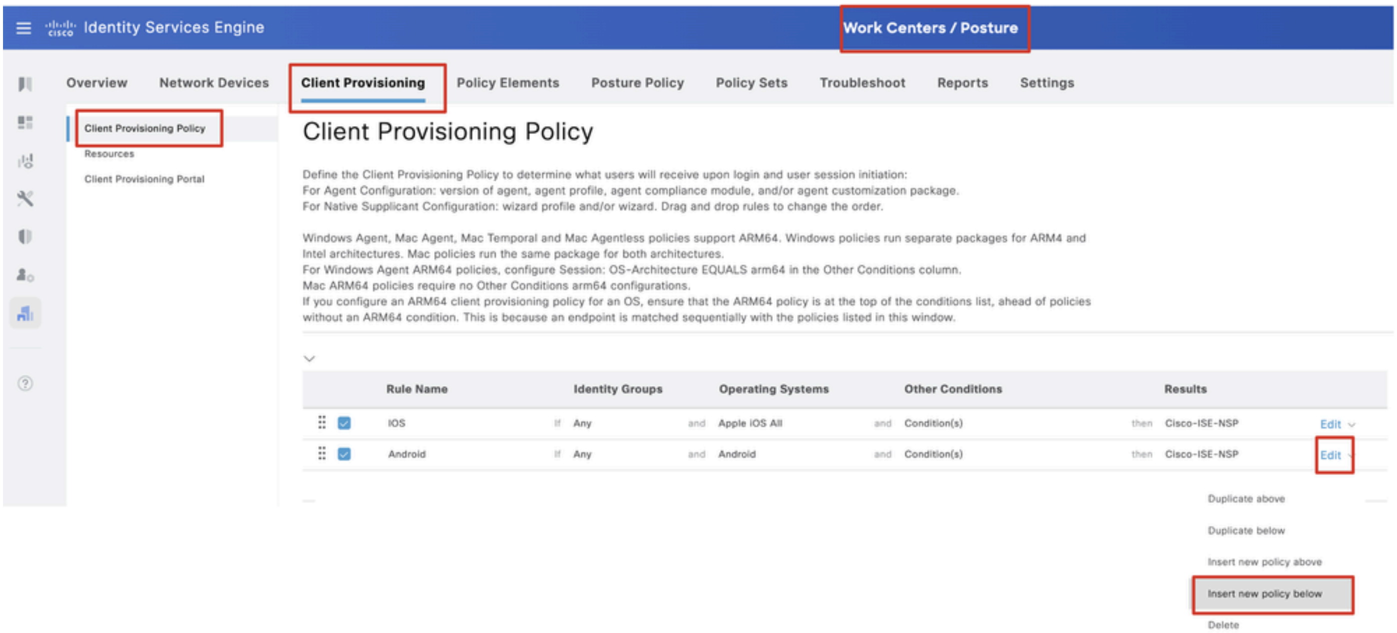
Diagnostic and Reporting Tool ☑

Profile Selection

* ISE Posture: linux_agent_profile

ISE_Add_Agent_Configuration_1

Stap 18. Navigeer naar Work Centers > Posture > Client Provisioning > Client Provisioning Policy. Klik Edit aan het eind van een regelnaam. Selecteer Insert new policy below.



Client Provisioning Policy

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	Edit
☑	Android	If	Any	and	Android	and	Condition(s)	then	Cisco-ISE-NSP	Edit

ISE_Add_New_Provisioning_Policy

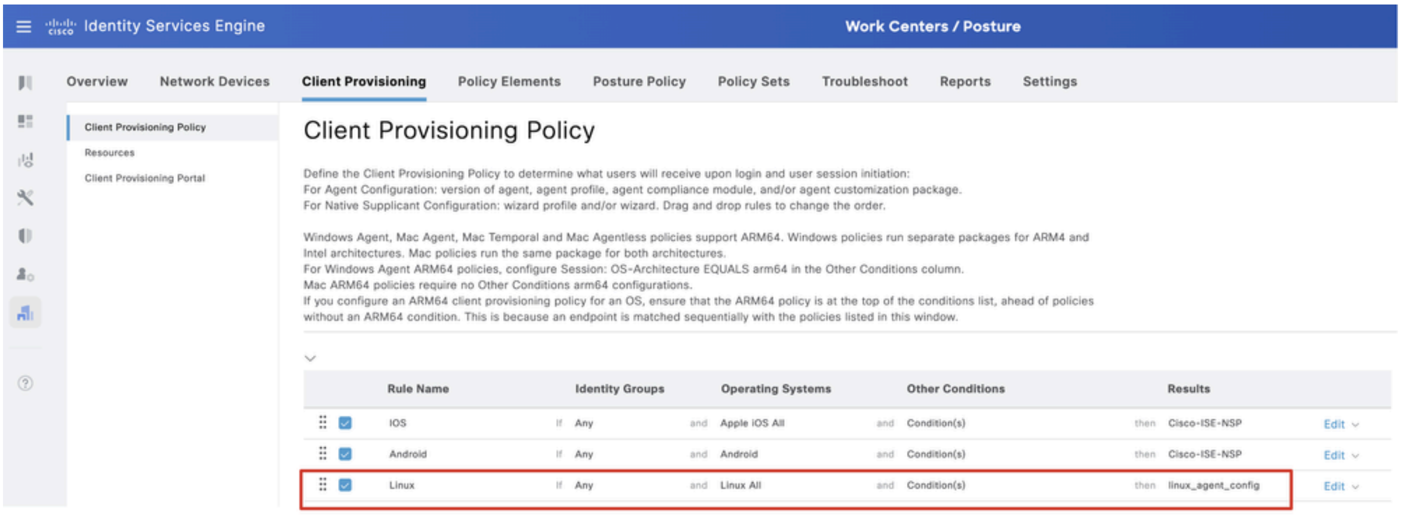
Stap 18.1. Configureer de details:

Regelnaam: Linux

Besturingssystemen: Linux All

Resultaten: linux_agent_config

Klik Done en Saveklik.



Client Provisioning Policy

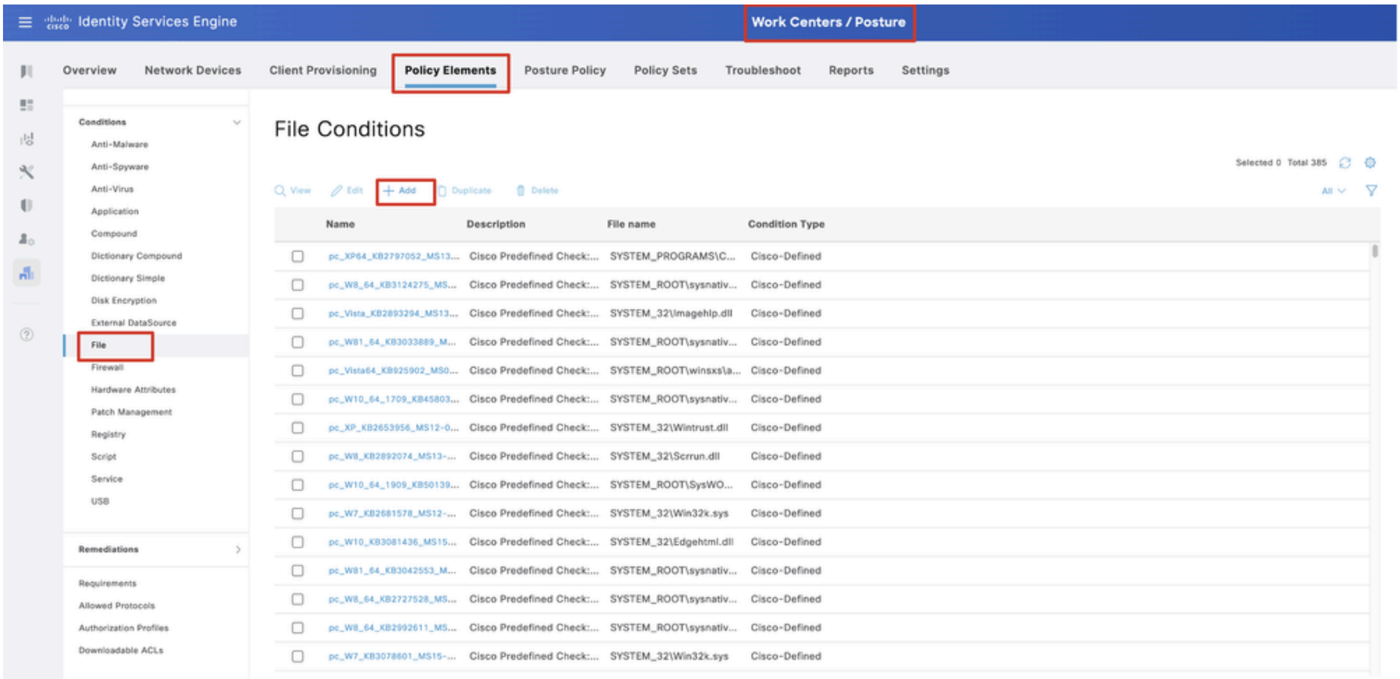
Define the Client Provisioning Policy to determine what users will receive upon login and user session initiation:
For Agent Configuration: version of agent, agent profile, agent compliance module, and/or agent customization package.
For Native Supplicant Configuration: wizard profile and/or wizard. 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	Edit ⌄
☑	Android	If	Any	and	Android	and	Condition(s)	then	Cisco-ISE-NSP	Edit ⌄
☑	Linux	If	Any	and	Linux All	and	Condition(s)	then	linux_agent_config	Edit ⌄

ISE_Add_New_Provisioning_Policy_1

Stap 19. Navigeer naar Work Centers > Posture > Policy Elements > Conditions > File. Klik op de knop .Add



File Conditions

	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\a...	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_KB2727528_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

Stap 19.1. Configureer de details:

Naam: linux_demo_file_existent

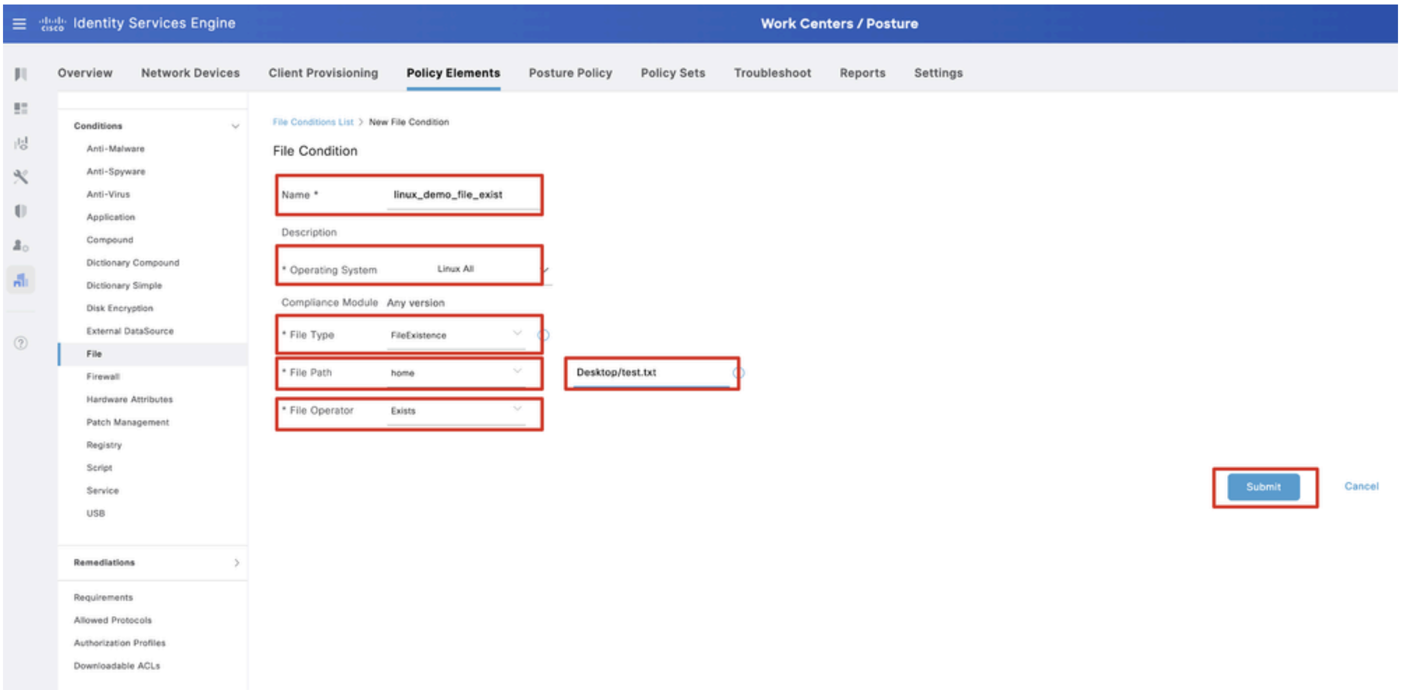
Besturingssystemen: Linux All

Bestandstype: FileExistence

File Path: startpunt, Desktop/test.txt

Bestandsbeheerder: bestaat

Klik op de knop .Submit



File Condition

Name * linux_demo_file_exist

Description

* Operating System Linux All

Compliance Module Any version

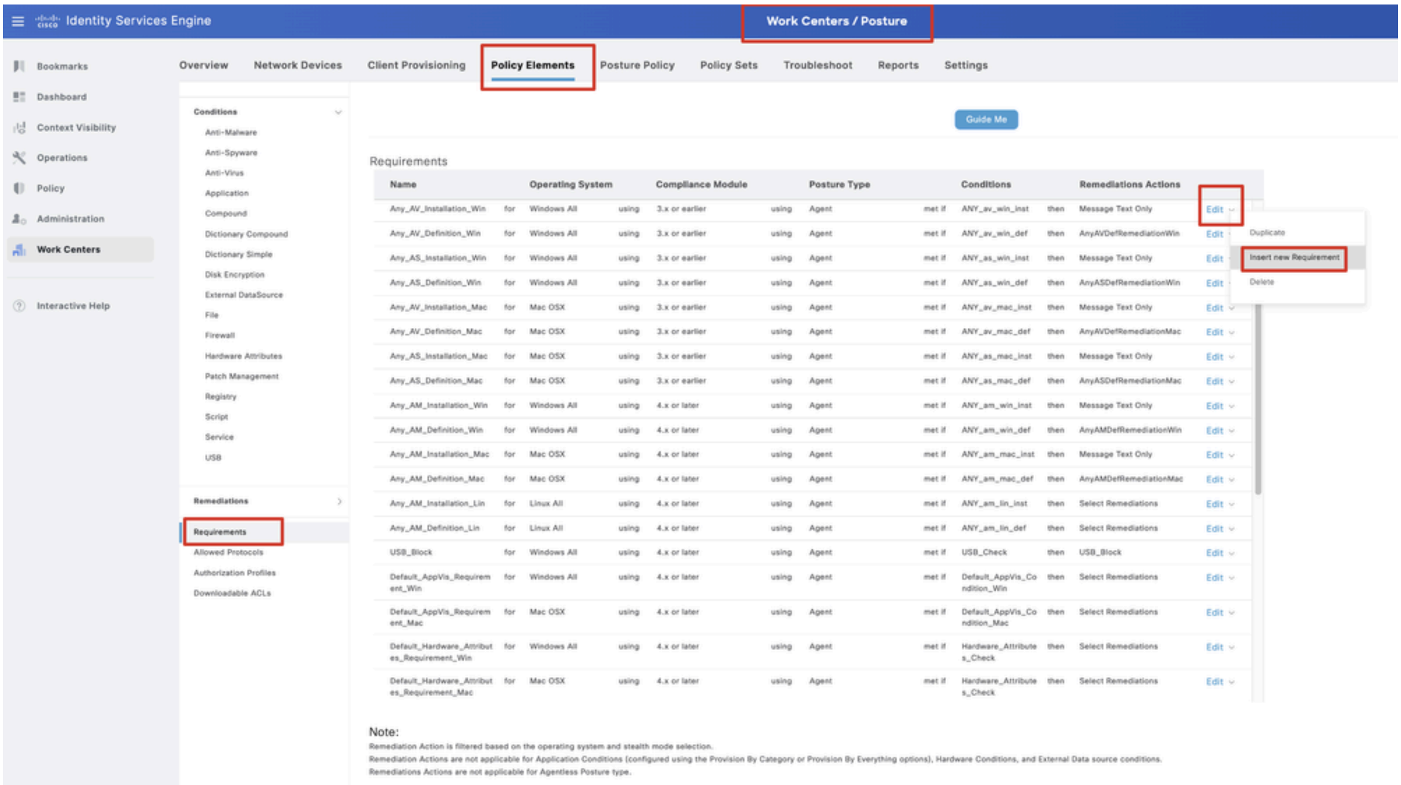
* File Type FileExistence

* File Path home Desktop/test.txt

* File Operator Exists

ISE_Add_New_File_Condition_1

Stap 20. Navigeer naar Work Centers > Posture > Policy Elements > Requirements. Klik Edit aan het eind van een regelnaam. Selecteer Insert new Requirement.



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
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
Any_AS_Definition_Win	for	Windows All	using	3.x or earlier	using	Agent	met if	ANY_as_win_def	then	AnyASDefRemediationWin	Edit
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_AppVis_Requirement_Win	for	Windows All	using	4.x or later	using	Agent	met if	Default_AppVis_Condition_Win	then	Select Remediations	Edit
Default_AppVis_Requirement_Mac	for	Mac OSX	using	4.x or later	using	Agent	met if	Default_AppVis_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

Stap 20.1. Configureer de details:

Naam: Test_existent_linux

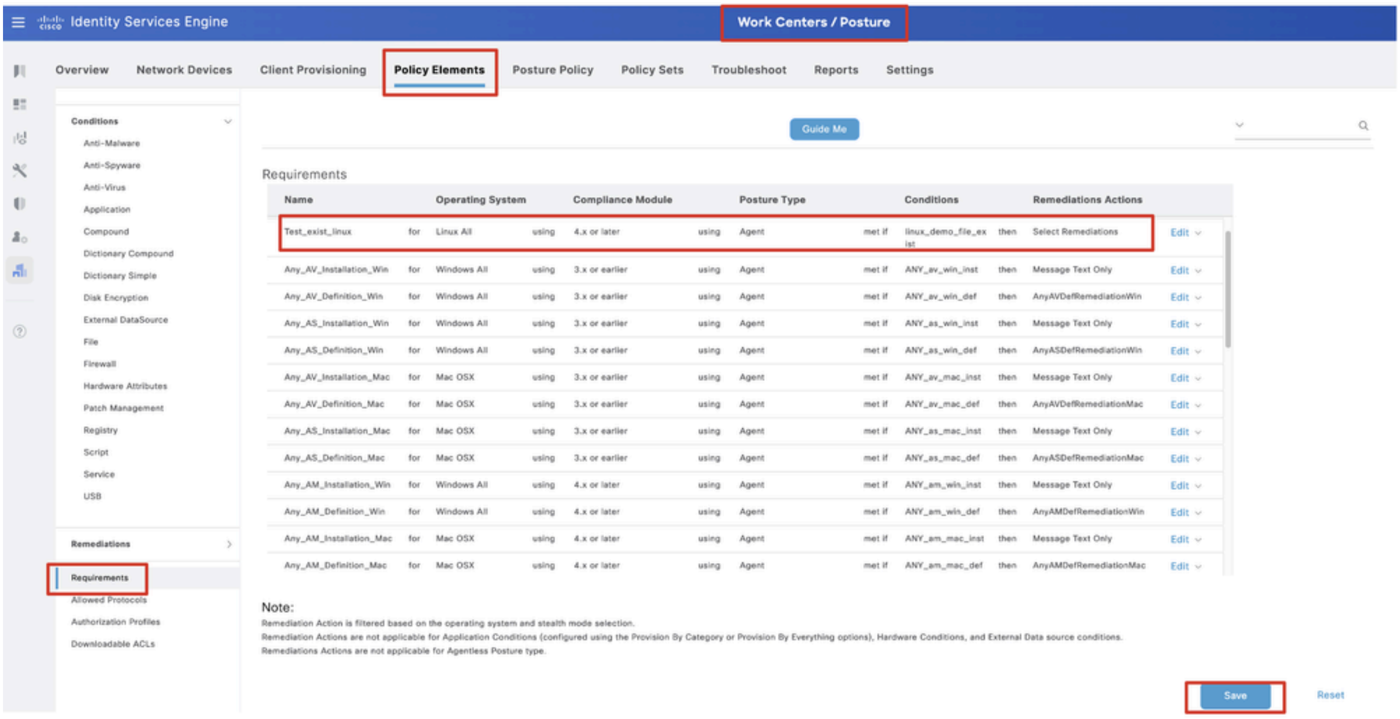
Besturingssystemen: Linux All

Nalevingsmodule: 4.x of hoger

Houdingstype: agent

Voorwaarden: linux_demo_file_existent

Klik Done en Saveklik.



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	Edit
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
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
Any_AS_Definition_Win	for	Windows All	using	3.x or earlier	using	Agent	met if	ANY_as_win_def	then	AnyASDefRemediationWin	Edit
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

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_1

Opmerking: Vanaf nu worden alleen shell scripts ondersteund voor Linux agents als herstel.

Stap 21. Navigeer naar Work Centers > Posture > Policy Elements > Authorization Profiles. Klik op de knop .Add

Stap 21.1. Configureer de details:

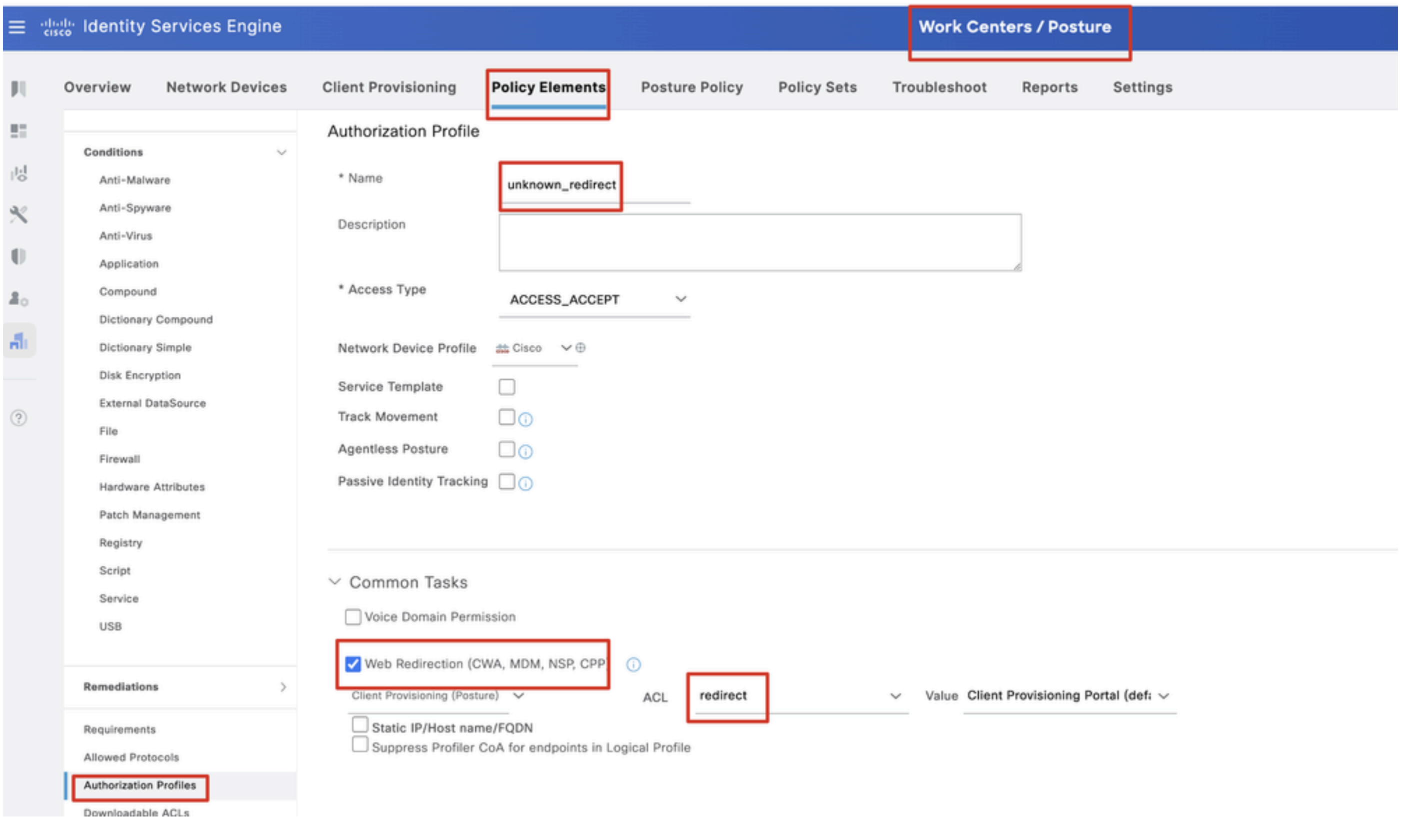
Naam: known_redirect

Schakel het selectievakje in van Web Redirection(CWA,MDM,NSP,CPP)

Kiezen Client Provisioning(Posture)

ACL: doorsturen

Waarde: client provisioningportal (standaard)



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

Client Provisioning (Posture) ACL: redirect Value: Client Provisioning Portal (defa

□ Static IP/Host name/FQDN

□ Suppress Profiler CoA for endpoints in Logical Profile

ISE_Add_New_Authorisation_Profile_Redirect_1

Opmerking: deze ACL-naam moet overeenkomen met de overeenkomstige ACL-naam die op FTD is geconfigureerd.

Stap 21.2. Herhaal het Add om nog twee autorisatieprofielen te maken voor niet-conforme en conforme endpoints met de details.

Naam: non_conforme_profile

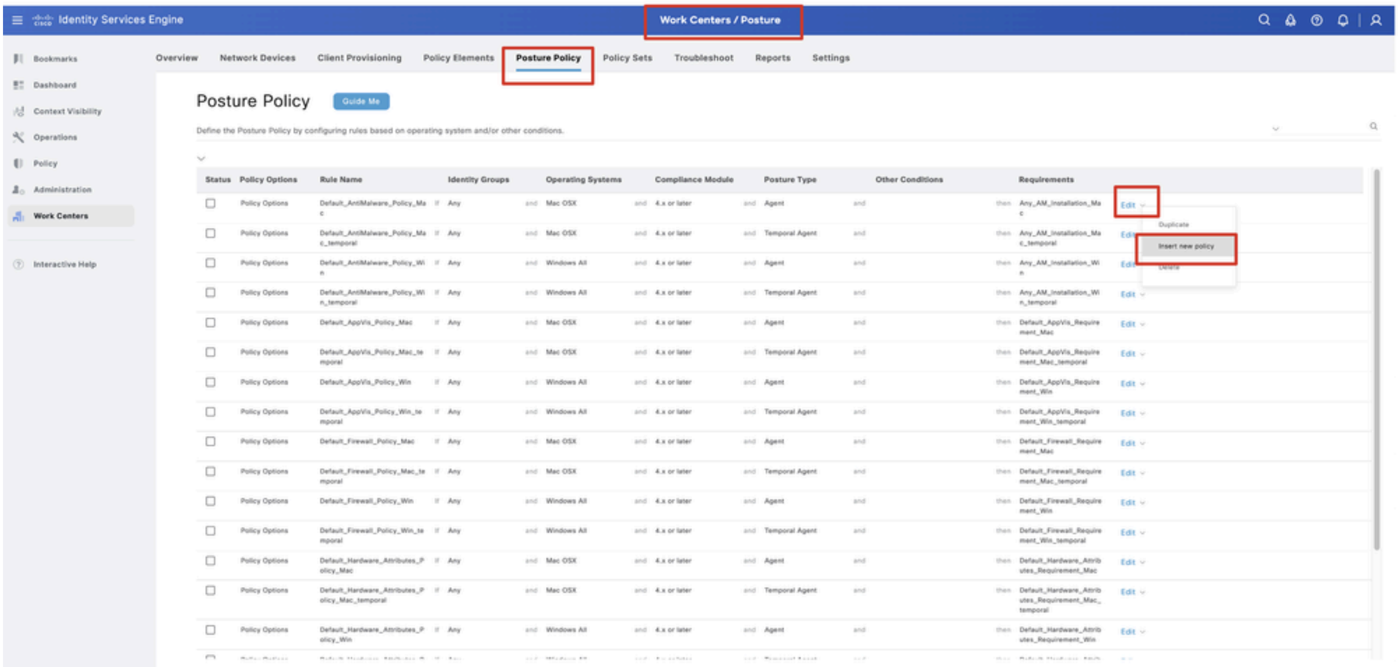
DACL-naam: DENY_ALL_IPv4_TRAFFIC

Naam: compatibel_profiel

DACL-naam: PERMIT_ALL_IPv4_TRAFFIC

Opmerking: de DACL voor compatibele of niet-conforme eindpunten moet worden geconfigureerd volgens de feitelijke vereisten.

Stap 22. Navigeer naar Work Centers > Posture > Posture Policy. Klik Edit aan het eind van regels. Selecteer Insert new policy.



Posture Policy

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	
□	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
□	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
□	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
□	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
□	Policy Options	Default_AppVis_Policy_Mac	If	Any	and	Mac OSX	and	4.x or later	and	Agent	and		then	Default_AppVis_Requirement_Mac	Edit
□	Policy Options	Default_AppVis_Policy_Mac_temporal	If	Any	and	Mac OSX	and	4.x or later	and	Temporal Agent	and		then	Default_AppVis_Requirement_Mac_temporal	Edit
□	Policy Options	Default_AppVis_Policy_Win	If	Any	and	Windows All	and	4.x or later	and	Agent	and		then	Default_AppVis_Requirement_Win	Edit
□	Policy Options	Default_AppVis_Policy_Win_temporal	If	Any	and	Windows All	and	4.x or later	and	Temporal Agent	and		then	Default_AppVis_Requirement_Win_temporal	Edit
□	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
□	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
□	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
□	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
□	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
□	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
□	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

ISE_Add_New_Posture_Policy

Stap 22.1. Configureer de details:

Regel Naam: Demo_test_existent_linux

Identiteitsgroepen: alle

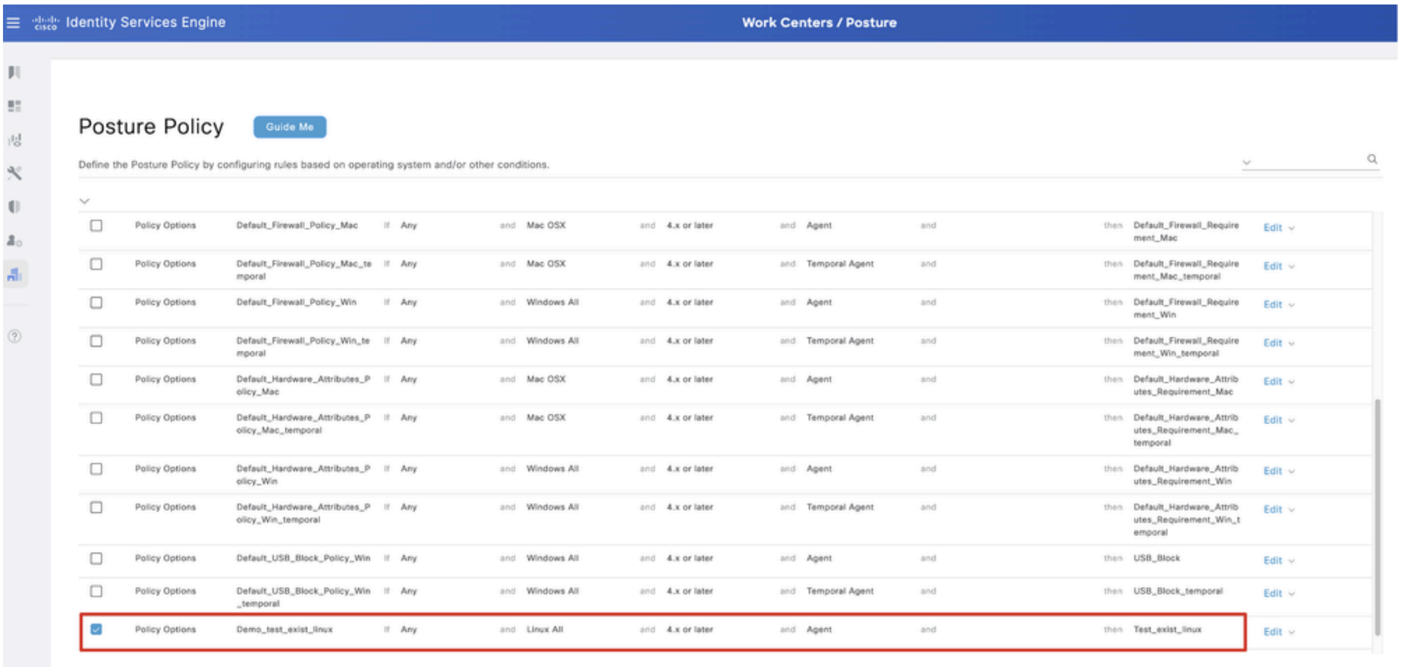
Besturingssystemen: Linux All

Nalevingsmodule: 4.x of hoger

Houdingstype: agent

Vereisten: Test_existent_linux

Klik Done en Saveklik.



Identity Services Engine — Work Centers / Posture

Posture Policy

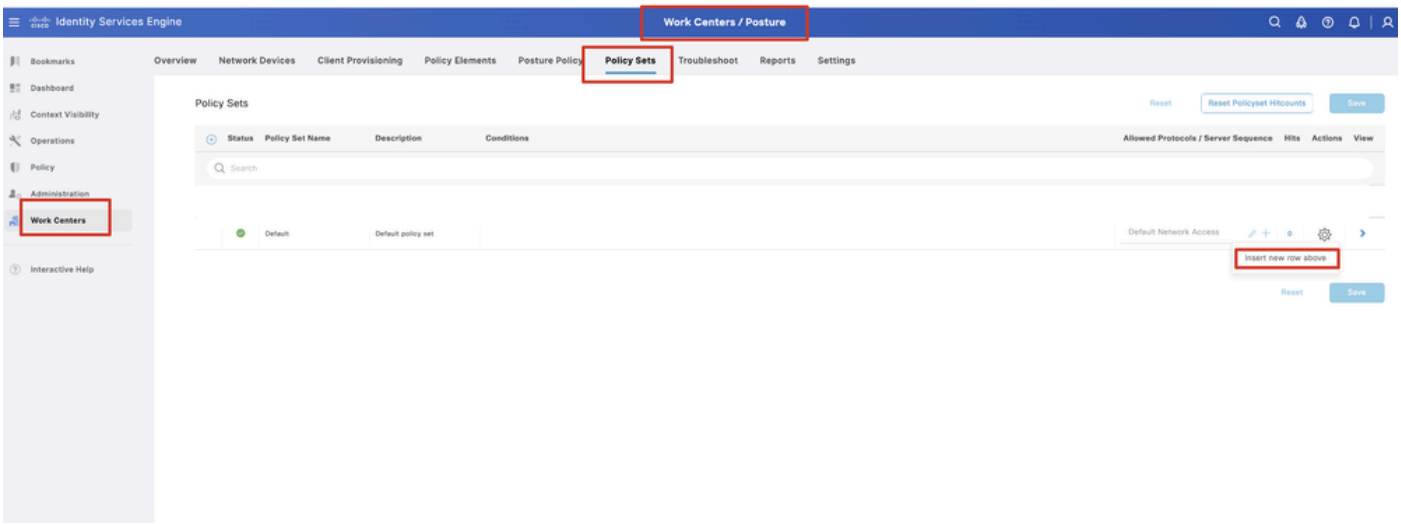
Guide Me

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
☐	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
☐	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
☐	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
☐	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
☐	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
☐	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
☐	Policy Options	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
☐	Policy Options	Default_USB_Block_Policy_Win	If	Any	and	Windows All	and	4.x or later	and	Agent	and	then	USB_Block	Edit
☐	Policy Options	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
☑	Policy Options	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

Stap 23. Navigeer naar Work Centers > Posture > Policy Sets. Klik om te Insert new row aboveklikken.



Policy Sets

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
●	Default	Default policy set		Default Network Access	0		›

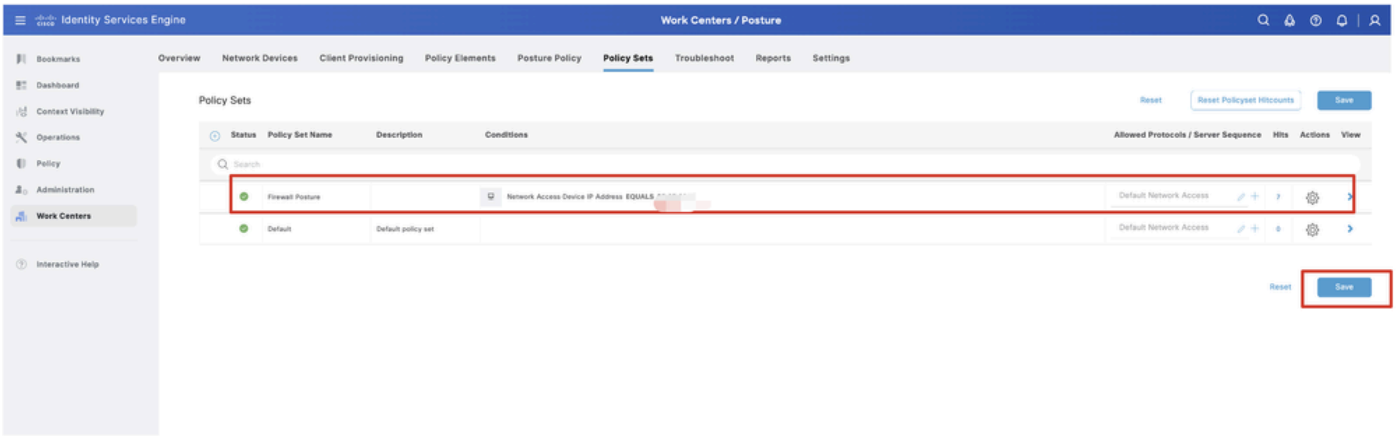
ISE_add_new_policy_set

Stap 23.1. Configureer de details:

Policy Set-naam: Firewallhouding

Voorwaarden: IP-adres voor netwerktoegangsapparaat gelijk aan [FTD IP-adres]

Klik op de knop . Save



Policy Sets

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
●	Firewall Posture		Network Access Device IP Address EQUALS [redacted]	Default Network Access	7	⚙	>
●	Default	Default policy set		Default Network Access	0	⚙	>

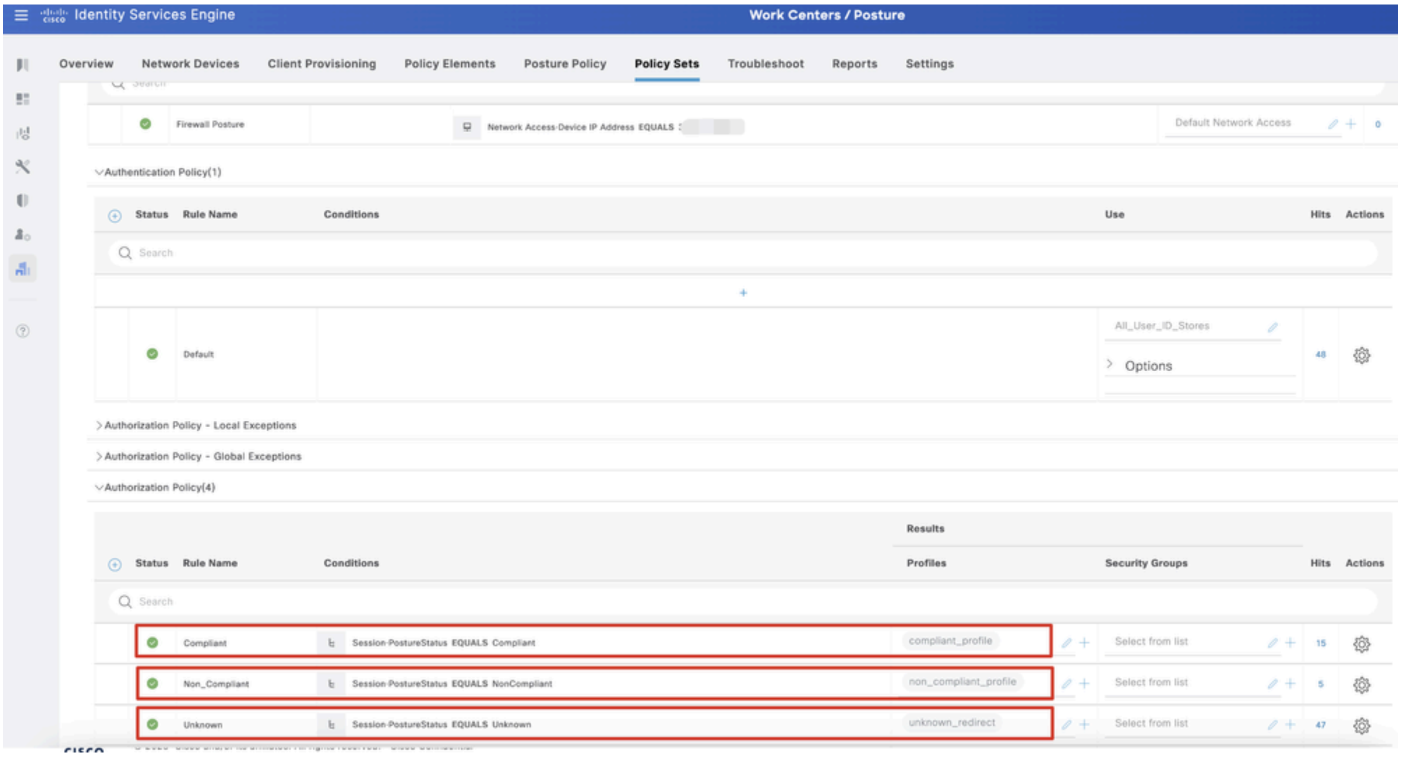
ISE_add_new_policy_set_1

Stap 23.2. Klik op > om de beleidsset in te voeren. Creëer nieuwe autorisatieregels voor status die compatibel, niet-conform en onbekende status is. Klik op de knop .Save

Voldoet aan compatibel_profiel

Niet conform niet-conform_conform_profiel

Onbekend met known_redirect



	Firewall Posture	Network Access Device IP Address EQUALS [redacted]	Default Network Access	0

Authentication Policy(1)

Status	Rule Name	Conditions	Use	Hits	Actions
●	Default		All_User_ID_Stores Options	48	⚙

Authorization Policy - Local Exceptions

Authorization Policy - Global Exceptions

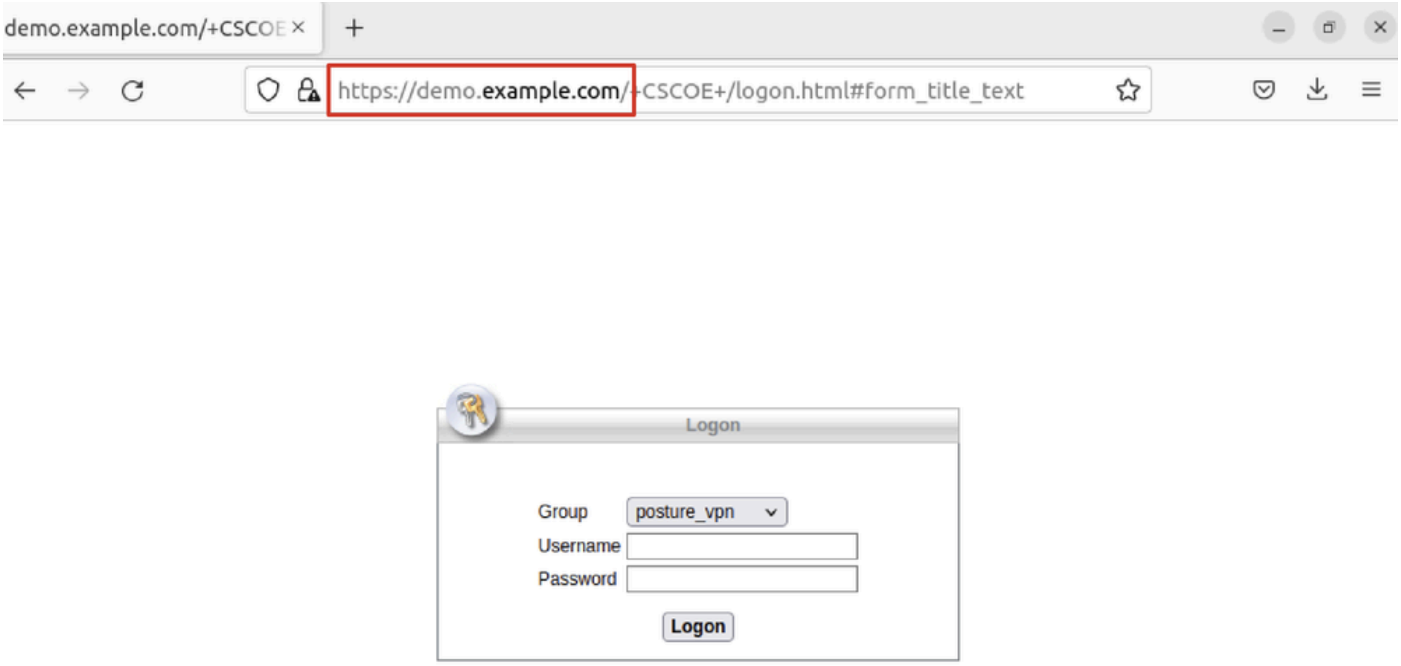
Authorization Policy(4)

Status	Rule Name	Conditions	Results: Profiles	Results: Security Groups	Hits	Actions
●	Compliant	Session·PostureStatus EQUALS Compliant	compliant_profile	Select from list	15	⚙
●	Non_Compliant	Session·PostureStatus EQUALS NonCompliant	non_compliant_profile	Select from list	5	⚙
●	Unknown	Session·PostureStatus EQUALS Unknown	unknown_redirect	Select from list	47	⚙

ISE_add_new_policy_set_2

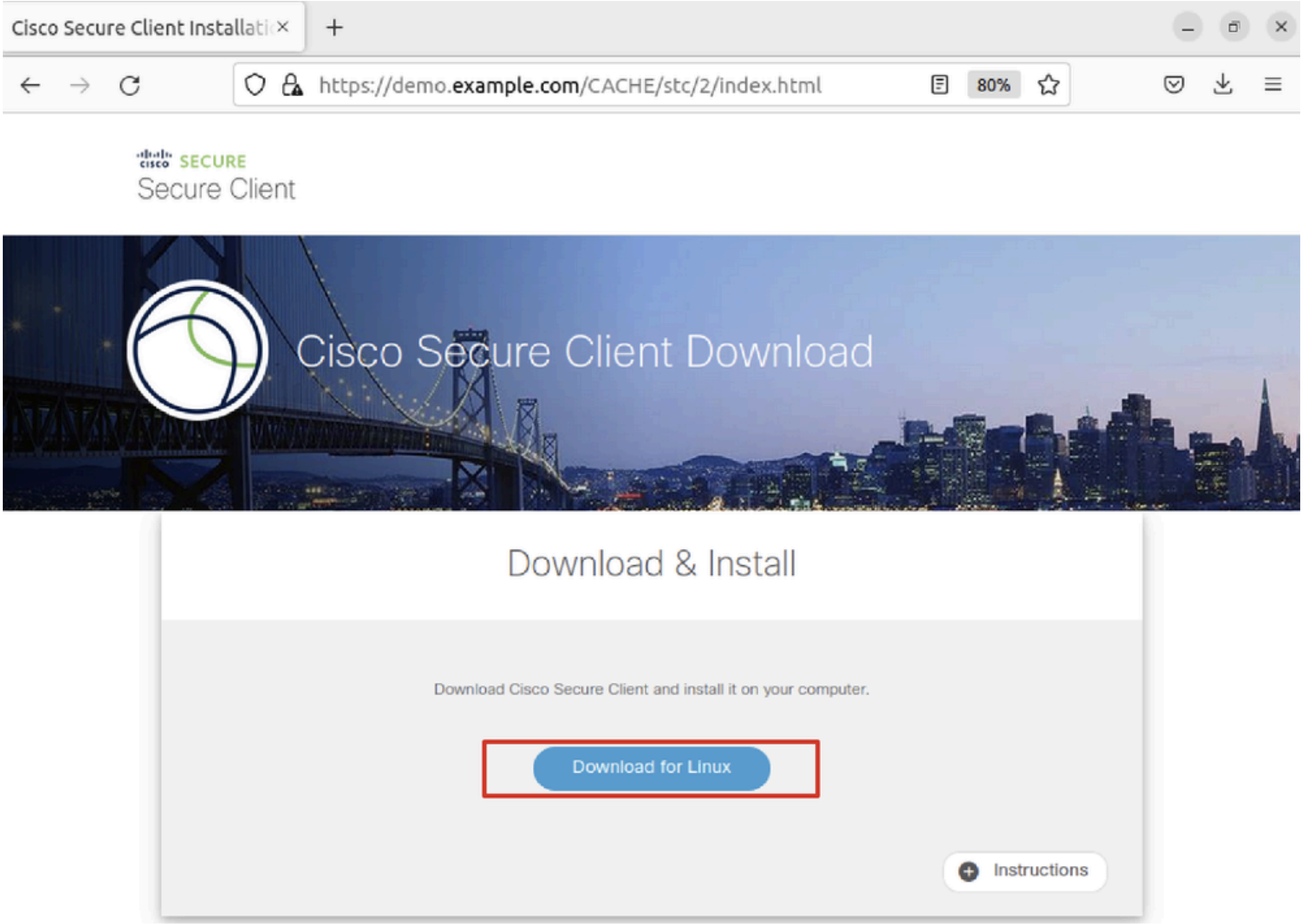
Configuraties op Ubuntu

Stap 24. Login bij Ubuntu client via GUI. Open de browser om in te loggen op het VPN-portal. In dit voorbeeld is het demo.example.com.



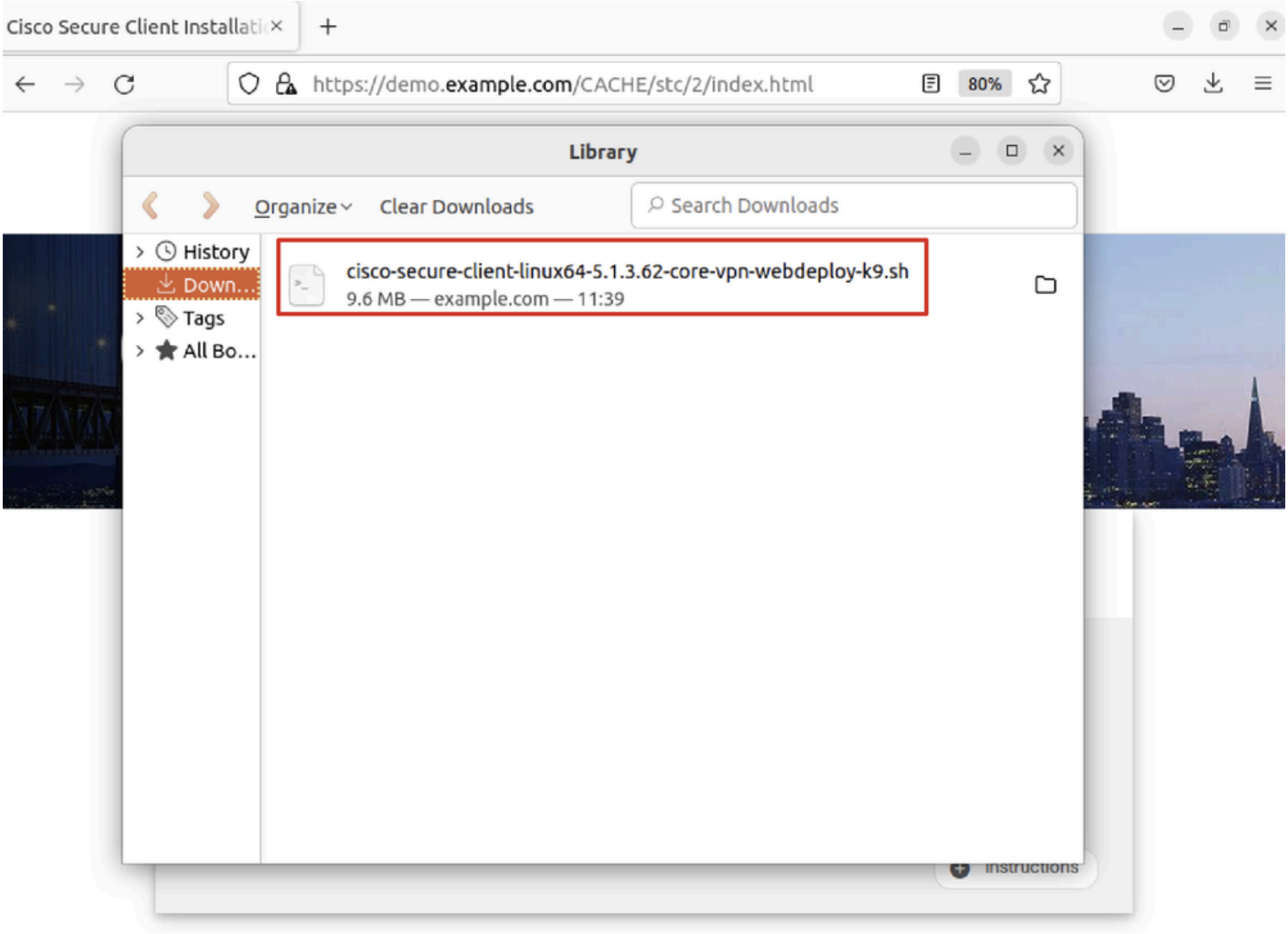
Ubuntu_browser_VPN_login

Stap 25. Klik op de knop .Download for Linux


Cisco Secure Client Installati
https://demo.example.com/CACHE/stc/2/index.html
80%
cisco SECURE
Secure Client
Cisco Secure Client Download
Download & Install
Download Cisco Secure Client and install it on your computer.
Download for Linux
Instructions

Ubuntu_browser_VPN_download_1

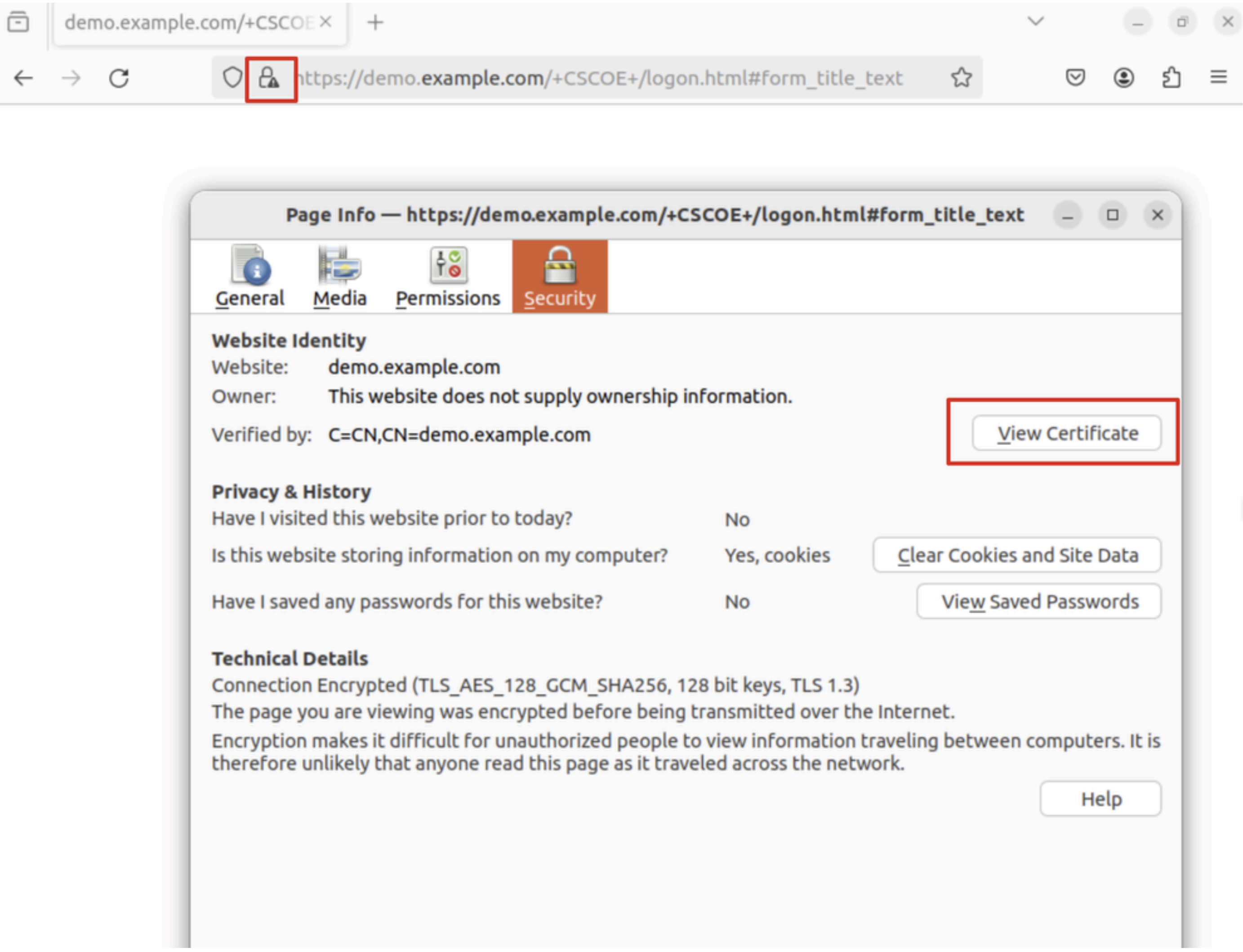
De gedownloade bestandsnaam is cisco-secure-client-linux64-5.1.3.62-core-vpn-webdeploy-k9.sh.



cisco-secure-client-linux64-5.1.3.62-core-vpn-webdeploy-k9.sh
9.6 MB — example.com — 11:39

Ubuntu_browser_VPN_download_2

Stap 26. VPN-certificaat downloaden via de browser en de naam van het bestand wijzigen in <certificaat>.crt. Dit is het voorbeeld van het gebruik van firefox om het certificaat te downloaden.



Page Info — https://demo.example.com/+CSCOE+/logon.html#form_title_text

Website Identity
Website: demo.example.com
Owner: This website does not supply ownership information.
Verified by: C=CN,CN=demo.example.com

Privacy & History
Have I visited this website prior to today? No
Is this website storing information on my computer? Yes, cookies
Have I saved any passwords for this website? No

Technical Details
Connection Encrypted (TLS_AES_128_GCM_SHA256, 128 bit keys, TLS 1.3)
The page you are viewing was encrypted before being transmitted over the Internet.
Encryption makes it difficult for unauthorized people to view information traveling between computers. It is therefore unlikely that anyone read this page as it traveled across the network.

Ubuntu_browser_VPN_cert_download

Stap 27. Open de terminal op de Ubuntu-client. Blader naar path home/user/Downloads/ om Cisco Secure-client te installeren.

<#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$
```

Stap 28. Vertrouw op het VPN portal certificaat op de Ubuntu 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$
```

```
 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
```

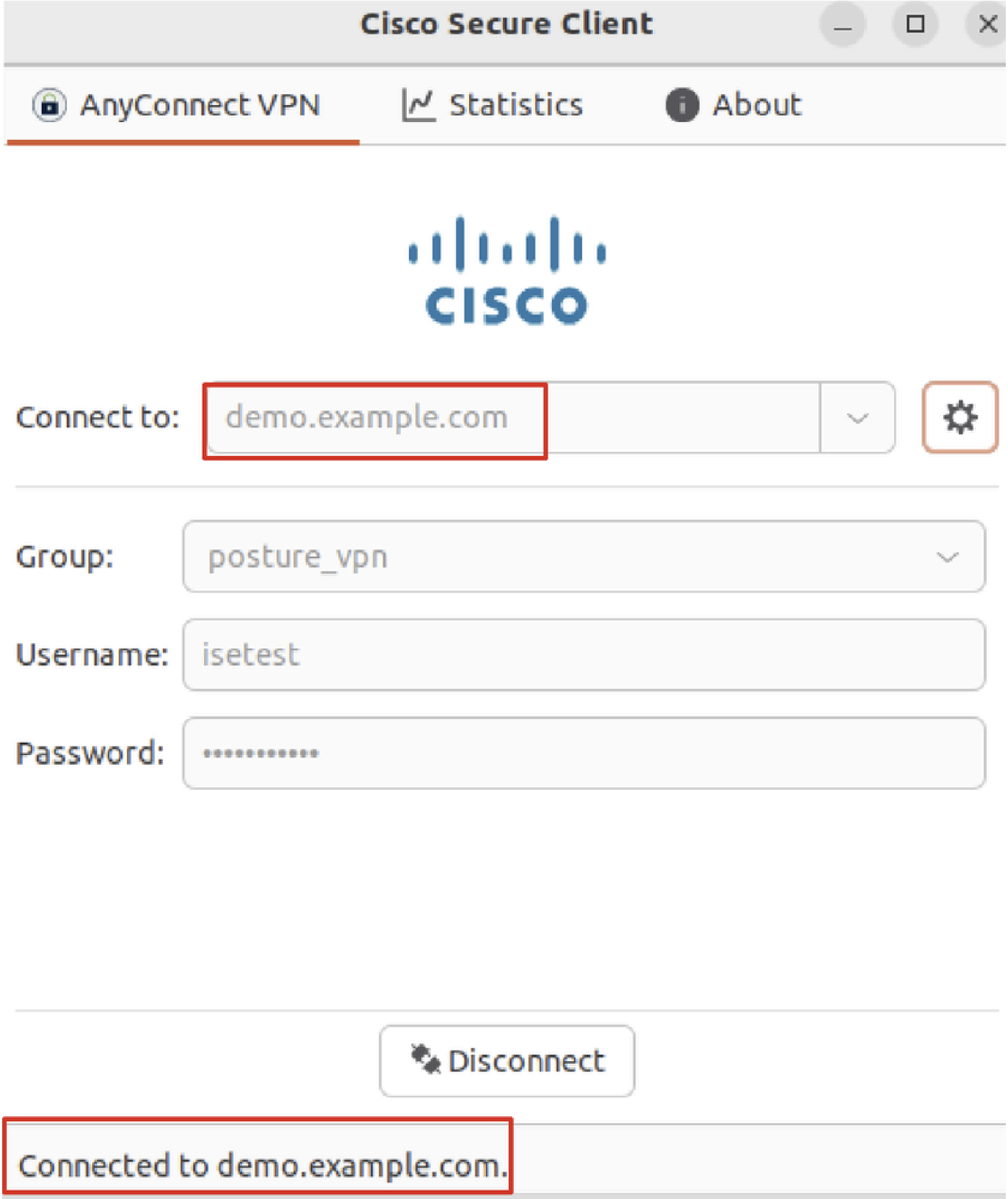
```
Updating certificates in /etc/ssl/certs...
rehash: warning: skipping ca-certificates.crt,it does not contain exactly one certificate or CRL
```

```
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
```

Stap 29. Open Cisco Secure-client op Ubuntu-client en sluit VPN met succes aan op demo.example.com.



Cisco Secure Client

Connect to: demo.example.com

Group: posture_vpn

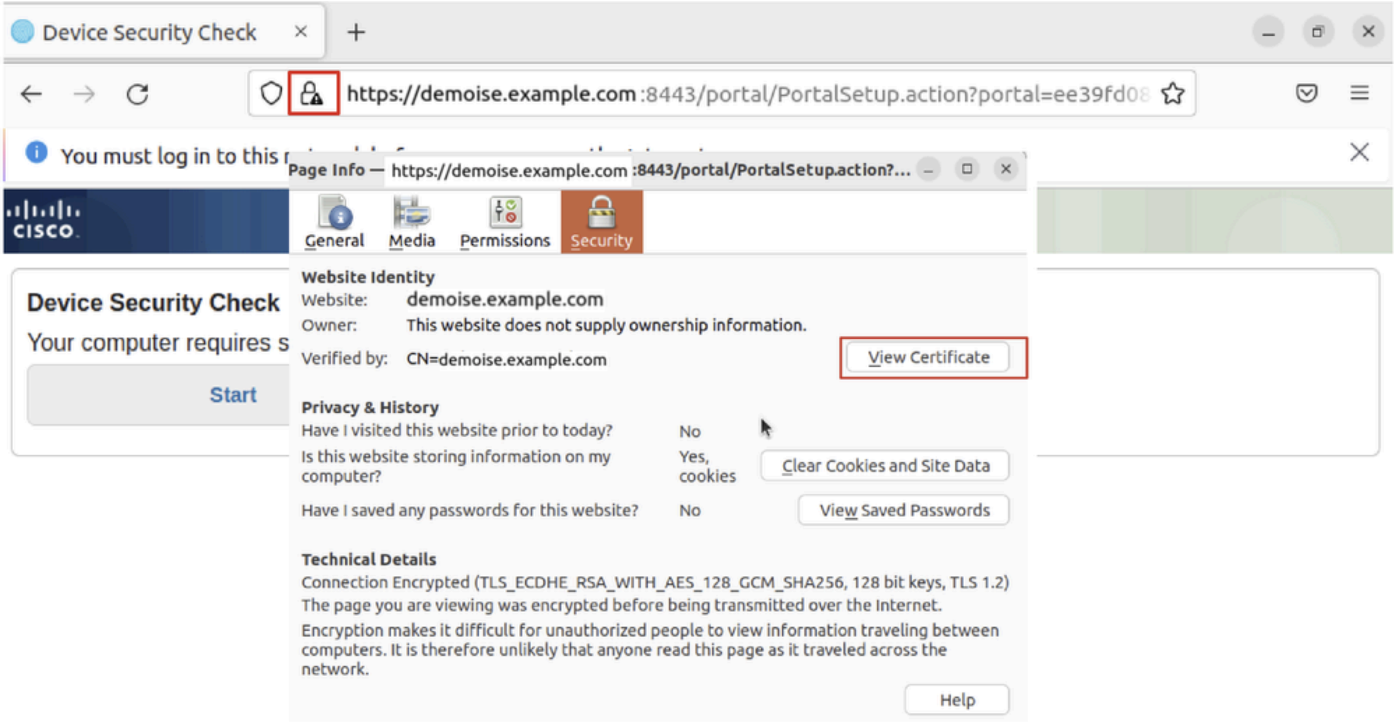
Username: isetest

Password: ••••••••••••

Connected to demo.example.com.

Ubuntu_Secure_Client_Connected

Stap 30. Open de browser om toegang te krijgen tot elke website die de omleiding naar de ISE CPP portal veroorzaakt. Download het certificaat van het ISE CPP-portal en hernoem het bestand naar <certificaat>.crt. Dit is een voorbeeld van het gebruik van Firefox voor het downloaden.



Device Security Check
https://demoise.example.com:8443/portal/PortalSetup.action?portal=ee39fd08
You must log in to this
Page Info — https://demoise.example.com:8443/portal/PortalSetup.action?...
General
Media
Permissions
Security
Device Security Check
Your computer requires s
Start

Website Identity
Website: demoise.example.com
Owner: This website does not supply ownership information.
Verified by: CN=demoise.example.com

Privacy & History
Have I visited this website prior to today? No
Is this website storing information on my computer? Yes, cookies
Have I saved any passwords for this website? No

Clear Cookies and Site Data
View Saved Passwords

Technical Details
Connection Encrypted (TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, 128 bit keys, TLS 1.2)
The page you are viewing was encrypted before being transmitted over the Internet.
Encryption makes it difficult for unauthorized people to view information traveling between computers. It is therefore unlikely that anyone read this page as it traveled across the network.

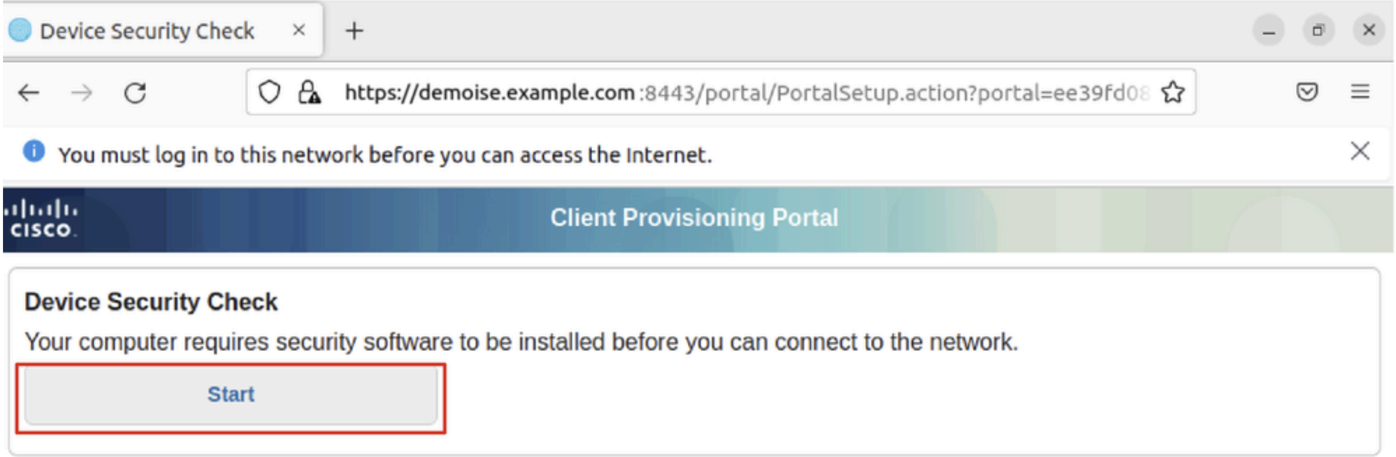
Ubuntu_browser_CPP_cert_download

Stap 30.1. Vertrouw het ISE CPP portal certificaat op de Ubuntu client.

<#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.
```

Stap 31. Klik Start op de ISE CPP portal.



Device Security Check

https://demoise.example.com:8443/portal/PortalSetup.action?portal=ee39fd08

You must log in to this network before you can access the Internet.

Client Provisioning Portal

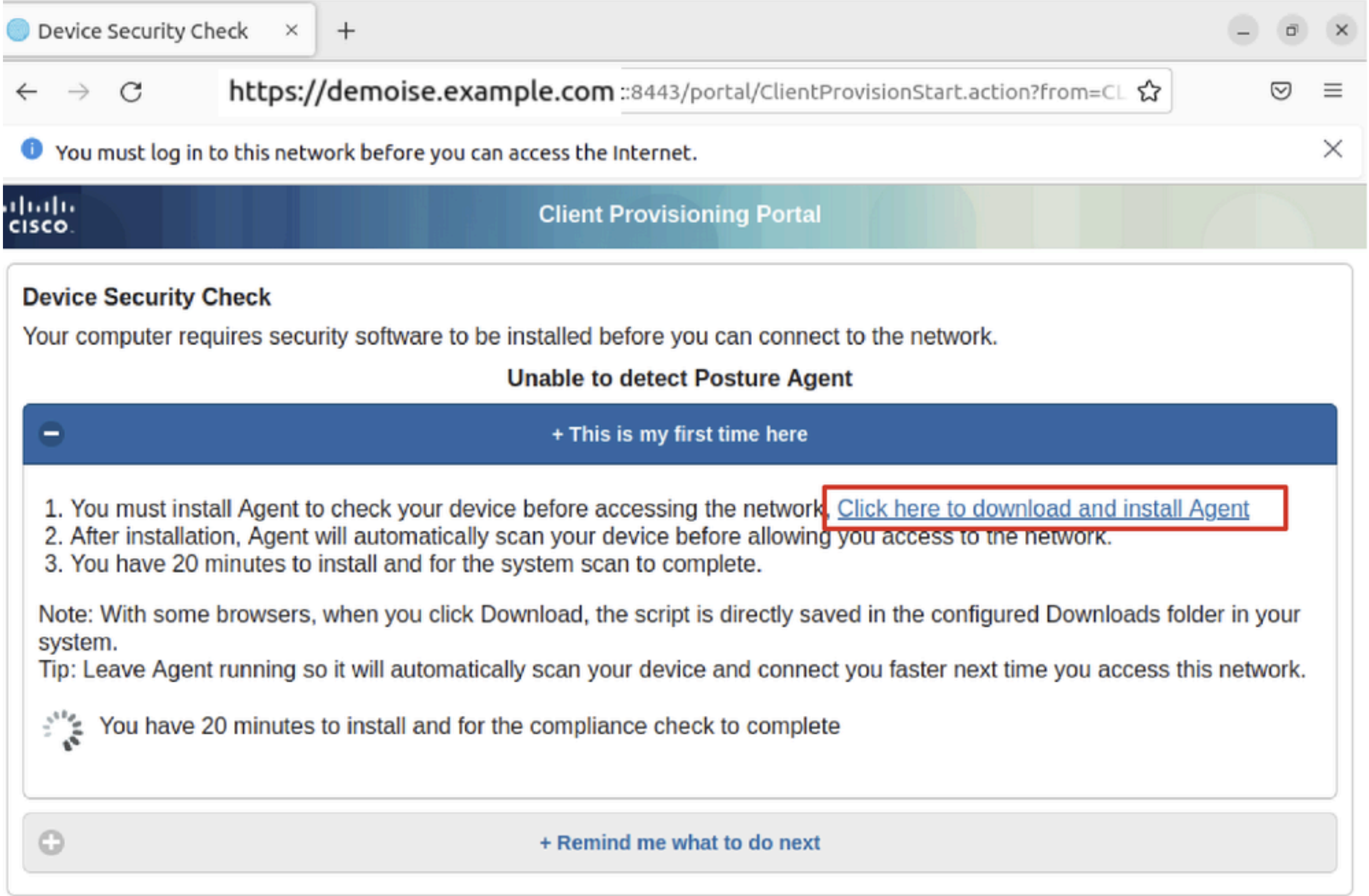
Device Security Check

Your computer requires security software to be installed before you can connect to the network.

Start

Ubuntu_browser_cpp_start

Stap 32. Click here to download and install Agent.



Device Security Check

https://demoise.example.com:8443/portal/ClientProvisionStart.action?from=CL

You must log in to this network before you can access the Internet.

Client Provisioning Portal

Device Security Check

Your computer requires security software to be installed before you can connect to the network.

Unable to detect Posture Agent

+ This is my first time here

1. You must install Agent to check your device before accessing the network. Click here to download and install Agent
2. After installation, Agent will automatically scan your device before allowing you access to the network.
3. You have 20 minutes to install and for the system scan to complete.

Note: With some browsers, when you click Download, the script is directly saved in the configured Downloads folder in your system.
Tip: Leave Agent running so it will automatically scan your device and connect you faster next time you access this network.

You have 20 minutes to install and for the compliance check to complete

+ Remind me what to do next

Ubuntu_browser_cpp_download_houding

Stap 33. Open de terminal op de Ubuntu-client. Navigeer naar pad home/user/Downloads/ om de postuur module te installeren.

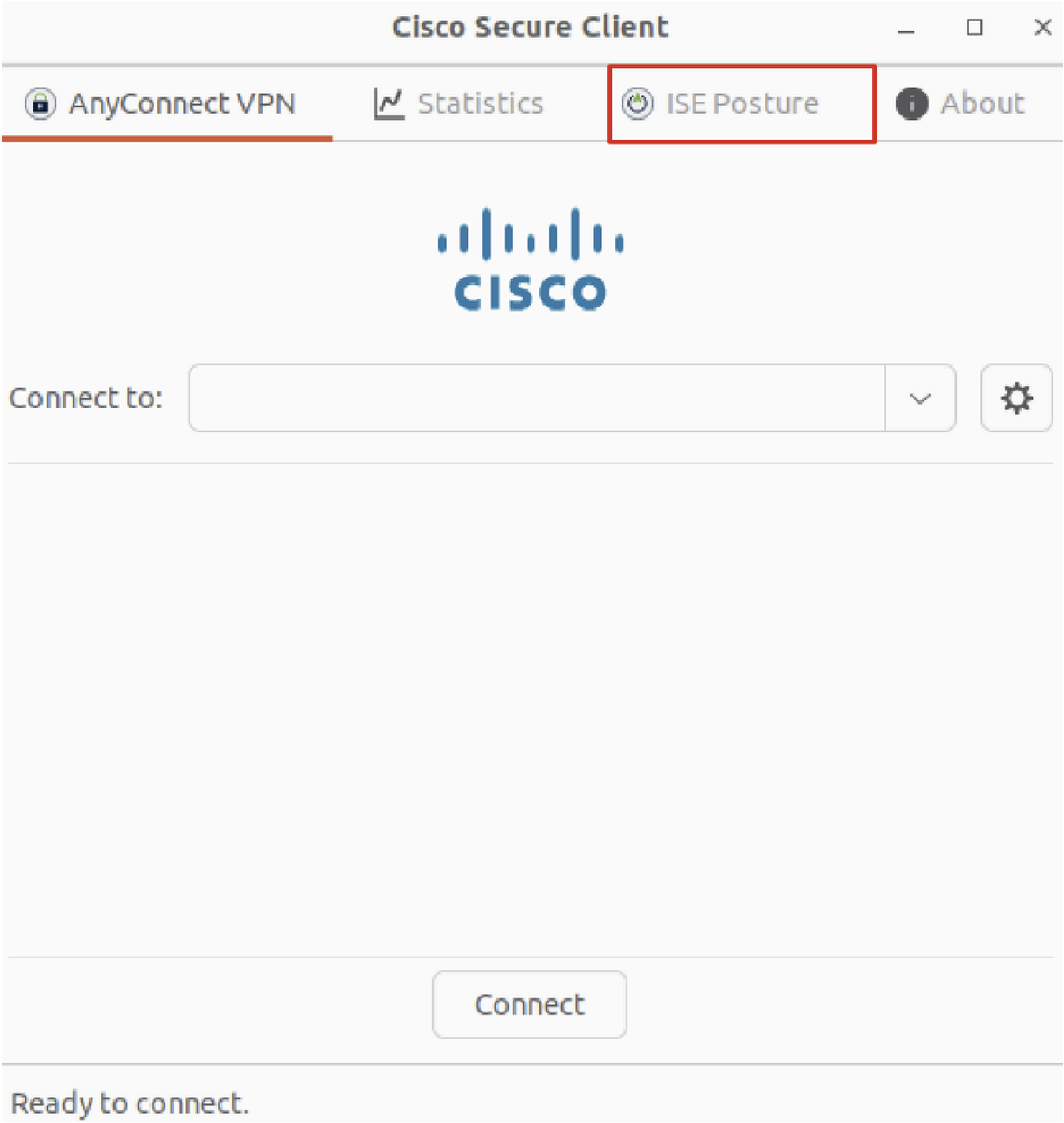
<#root>

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_0NcLgcMURfy


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_0NcLgcMURfyZmR6HoL


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.
```

Stap 34. Sluit op Ubuntu client UI de Cisco Secure-client af en open deze opnieuw. De ISE-postermodule is geïnstalleerd en kan met succes worden uitgevoerd.



Ubuntu_Secure_Client_ISE_posture_geïnstalleerd

Stap 35. Open de terminal op de Ubuntu-client. Navigeer naar pad home/user/Desktop , maak een test.txt bestand om te voldoen aan de bestandsvoorwaarde die op ISE is geconfigureerd.

<#root>

user@ubuntu22-desktop:~$

```
cd Desktop/
```

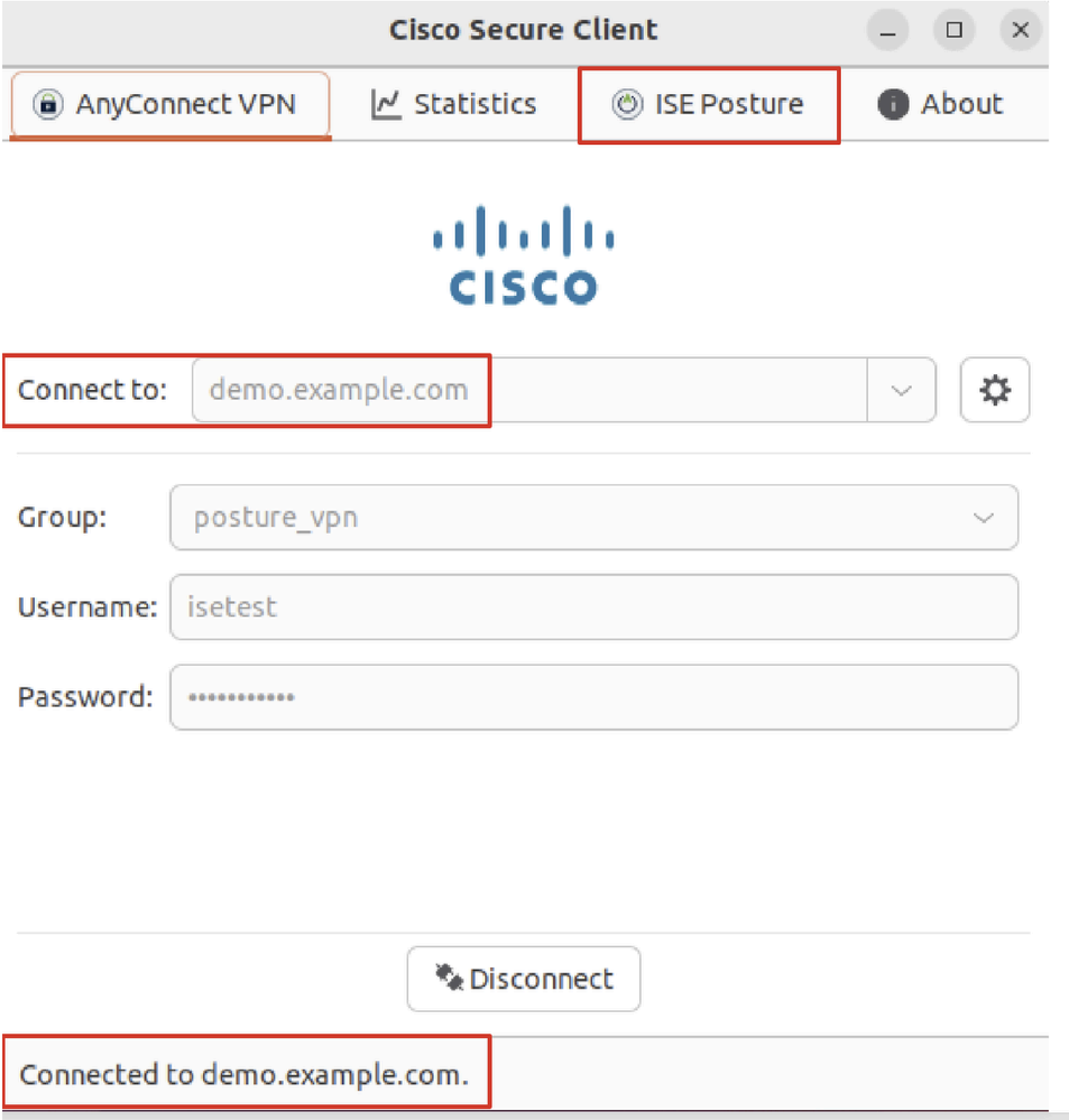
```
user@ubuntu22-desktop:~/Desktop$
```

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

Verifiëren

Gebruik deze sectie om te controleren of uw configuratie goed werkt.

Stap 1. Sluit VPN aan op demo.example.com op Ubuntu-client.



Connect to: demo.example.com

Group: posture_vpn

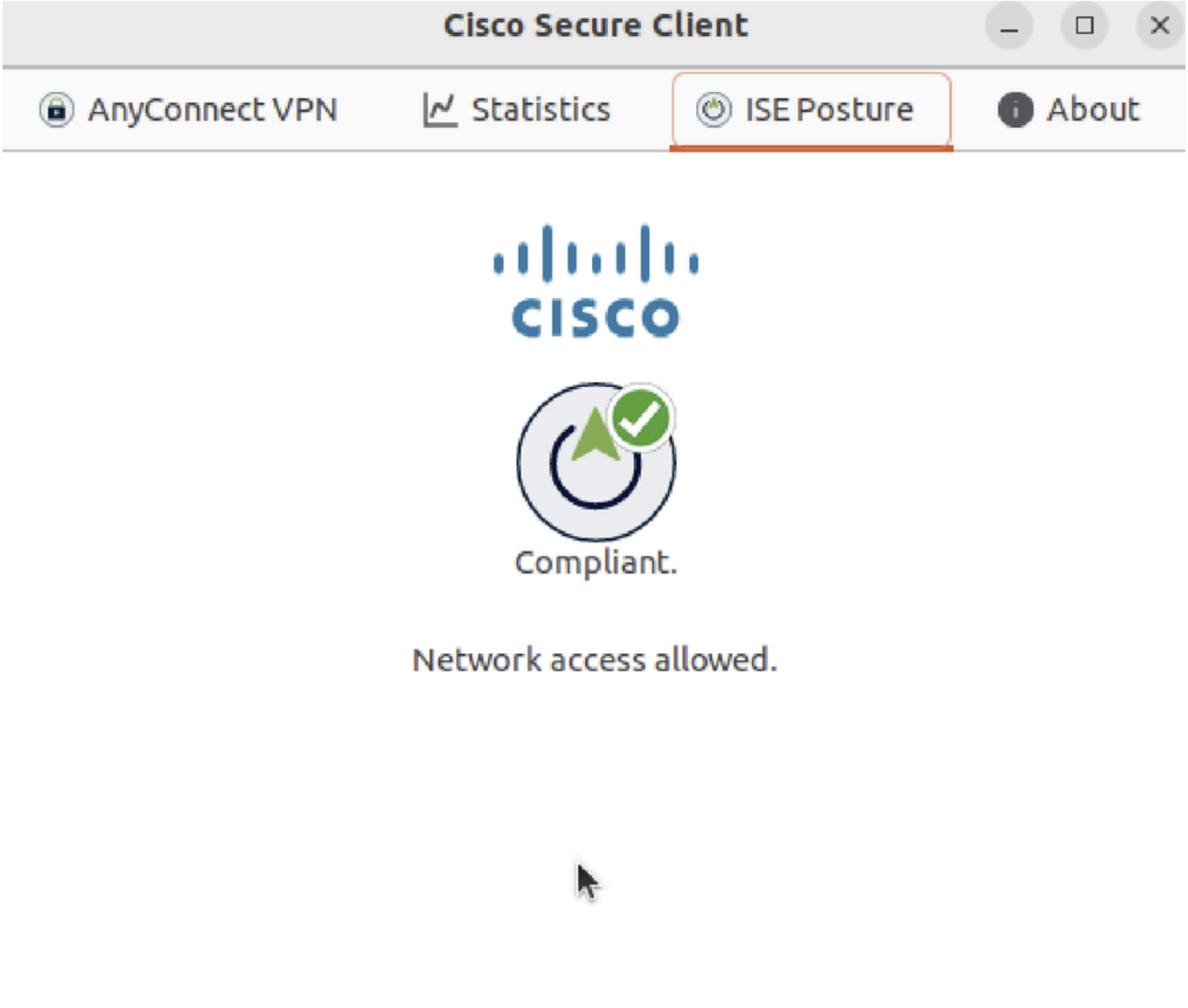
Username: isetest

Password: ••••••••••••

Connected to demo.example.com.

verify_ubuntu_beveiligde_client_verbinding

Stap 2. Controleer de status van de ISE-houding op de Ubuntu-client.

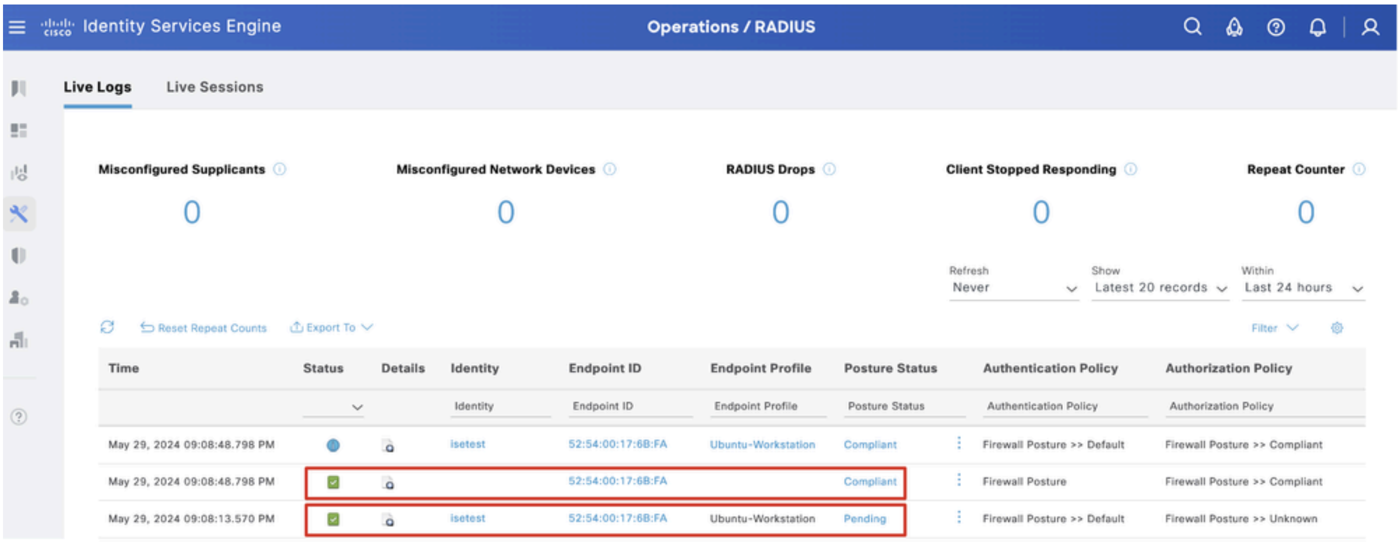


Compliant.

Network access allowed.

verify_ubuntu_Secure_client_conform

Stap 3. Controleer Radius Live Log in ISE. Navigeer naar Operations > RADIUS Live Log.



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

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

Time	Status	Details	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

verify_ise_livelog

Stap 4. Navigeer naar FTD CLI via SSH of 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
```

Problemen oplossen

Deze sectie bevat informatie die u kunt gebruiken om problemen met de configuratie te troubleshooten.

Voor een postenstroom en probleemoplossing bij Cisco Secure Client en ISE controleert u de **Vergelijking** van Cisco**-documentenISE-poortstijlen voor Pre en Post 2.2** en **probleemoplossing voor ISE-sessiebeheer en -houding.**

Gerelateerde informatie

- Compatibiliteit van netwerkcomponenten voor Cisco Identity Services Engine, release 3.3

- Beheerdershandleiding voor Cisco Identity Services Engine, release 3.3

- **Cisco Technical Support en downloads**