Configurare la postura della VPN Linux con ISE 3.3

Sommario

Introduzione

Questo documento descrive come configurare la postura della VPN Linux con Identity Services Engine (ISE) e Firepower Threat Defense (FTD).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco Secure Client
- VPN ad accesso remoto su Firepower Threat Defense (FTD)
- Identity Services Engine (ISE)

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software:

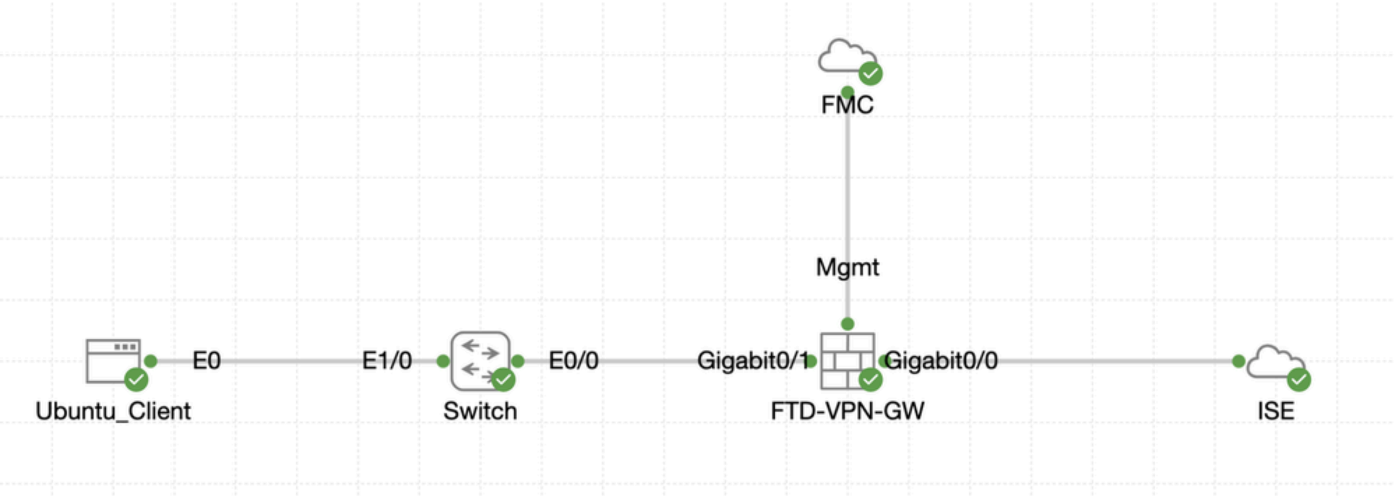
- Ubuntu 22,04
- Cisco Secure Client 5.1.3.62

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

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

Esempio di rete



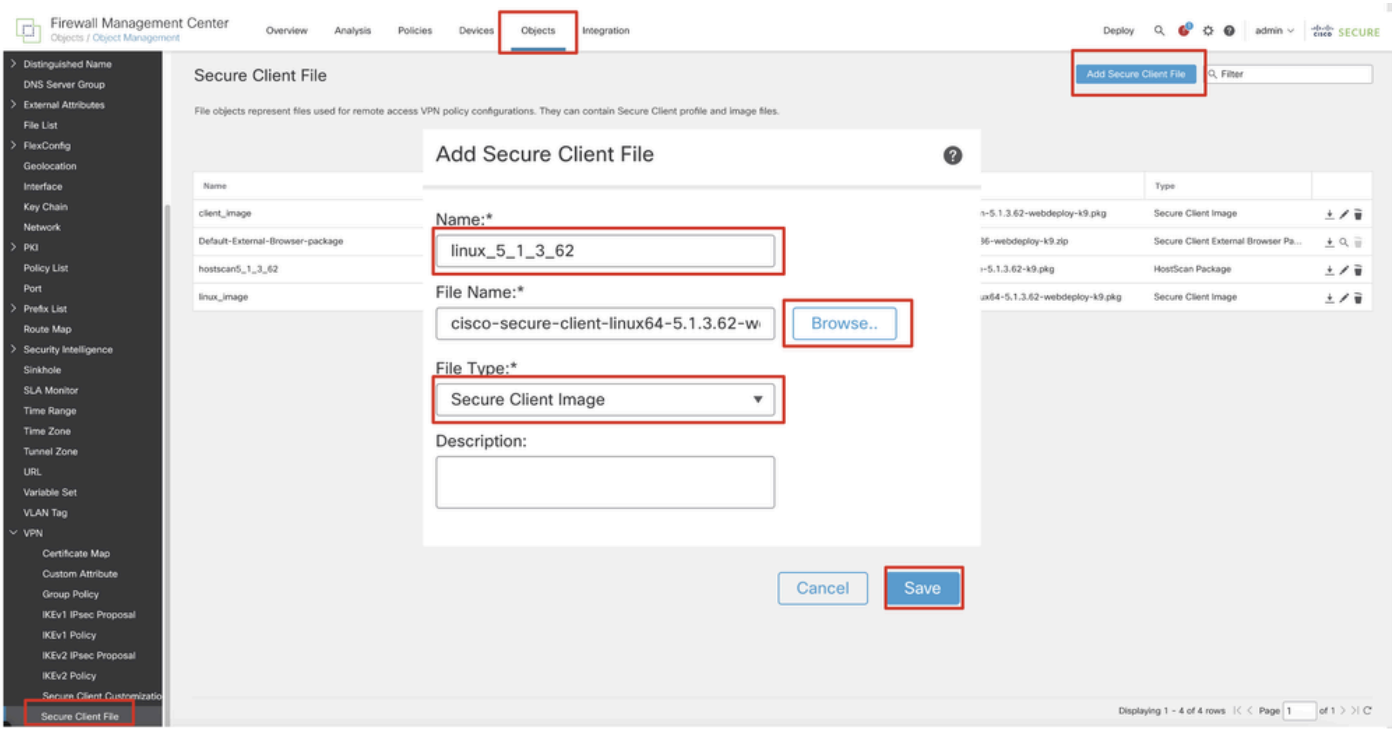
Topologia

Configurazioni su FMC/FTD

Passaggio 1. Configurazione della connettività tra client, FTD, FMC e ISE completata. Come enroll.cisco.com si usa per gli endpoint che eseguono la sonda per il reindirizzamento (per i dettagli, fare riferimento ai documenti CCO del flusso di postura e al confronto degli stili di postura ISE per le versioni precedenti e successive alla 2.2). Verificare che il percorso del traffico verso enroll.cisco.com su FTD sia configurato correttamente.

Passaggio 2. Scaricare il nome del pacchetto cisco-secure-client-linux64-5.1.3.62-webdeploy-k9.pkg da Cisco Software Download e assicurarsi che il file sia valido dopo il download confermando che il checksum md5 del file scaricato è lo stesso della pagina di download del software Cisco.

Passaggio 3. Passare a Objects > Object Management > VPN > Secure Client File. Fare clic suAdd Secure Client File, fornire il nome, sfogliare File Name per selezionare cisco-secure-client-linux64-5.1.3.62-webdeploy-k9.pkg, selezionare Secure Client Image in elenco a discesaFile Type. Quindi fate clic su 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	ı-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	ı-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

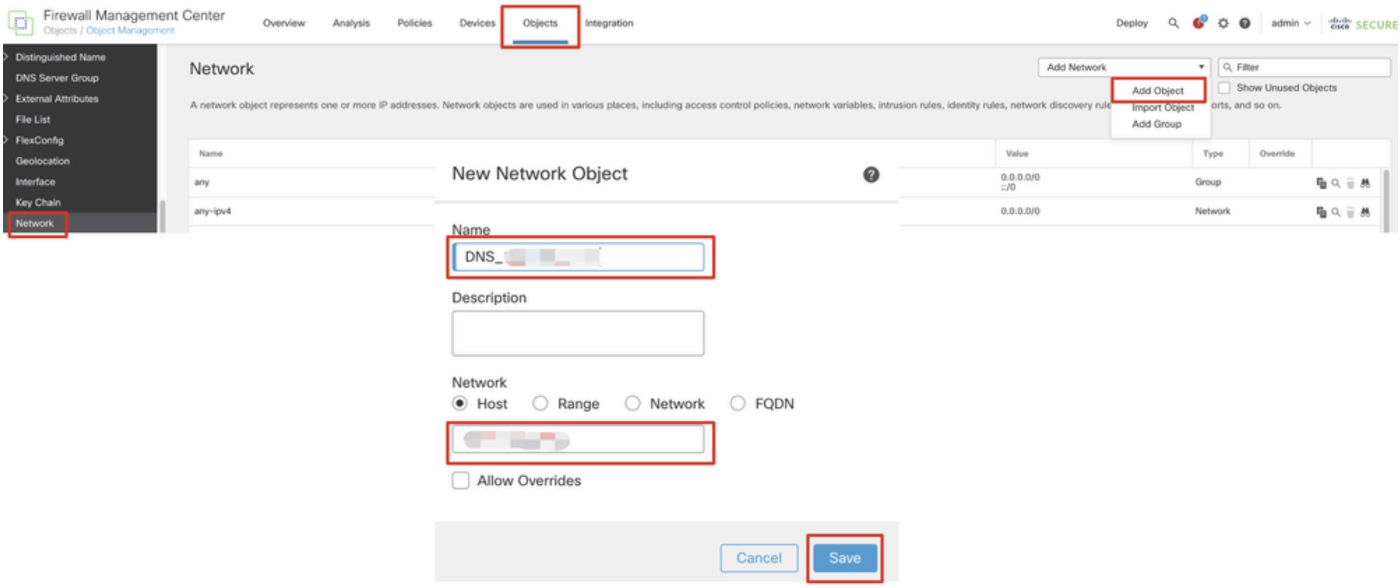
File Type:* Secure Client Image

Description:

Immagine_client_caricamento_protetto_FMC

Passaggio 4. Passare a Objects > Object Management > Network.

Passaggio 4.1. Creare un oggetto per il server DNS. Fare clic su Add Object, specificare il nome e l'indirizzo IP DNS disponibile. Fare clic su .Save



Network

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

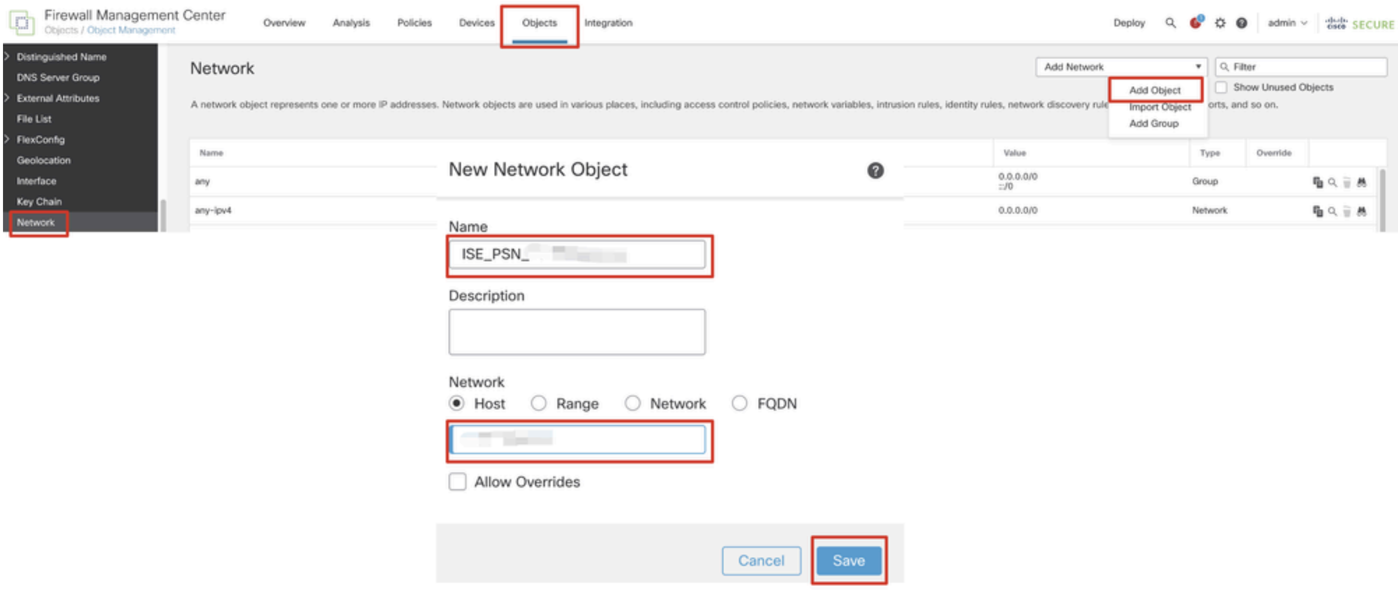
[redacted]

☐ Allow Overrides

FMC_Aggiungi_Oggetto_DNS

Nota: il server DNS configurato qui deve essere utilizzato per gli utenti VPN.

Passaggio 4.2. Crea un oggetto per ISE PSN. Fare clic su Add Object, fornire il nome e l'indirizzo IP PSN ISE disponibile. Fare clic su .Save



Network

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.

New Network Object

Name: ISE_PSN_[redacted]

Description:

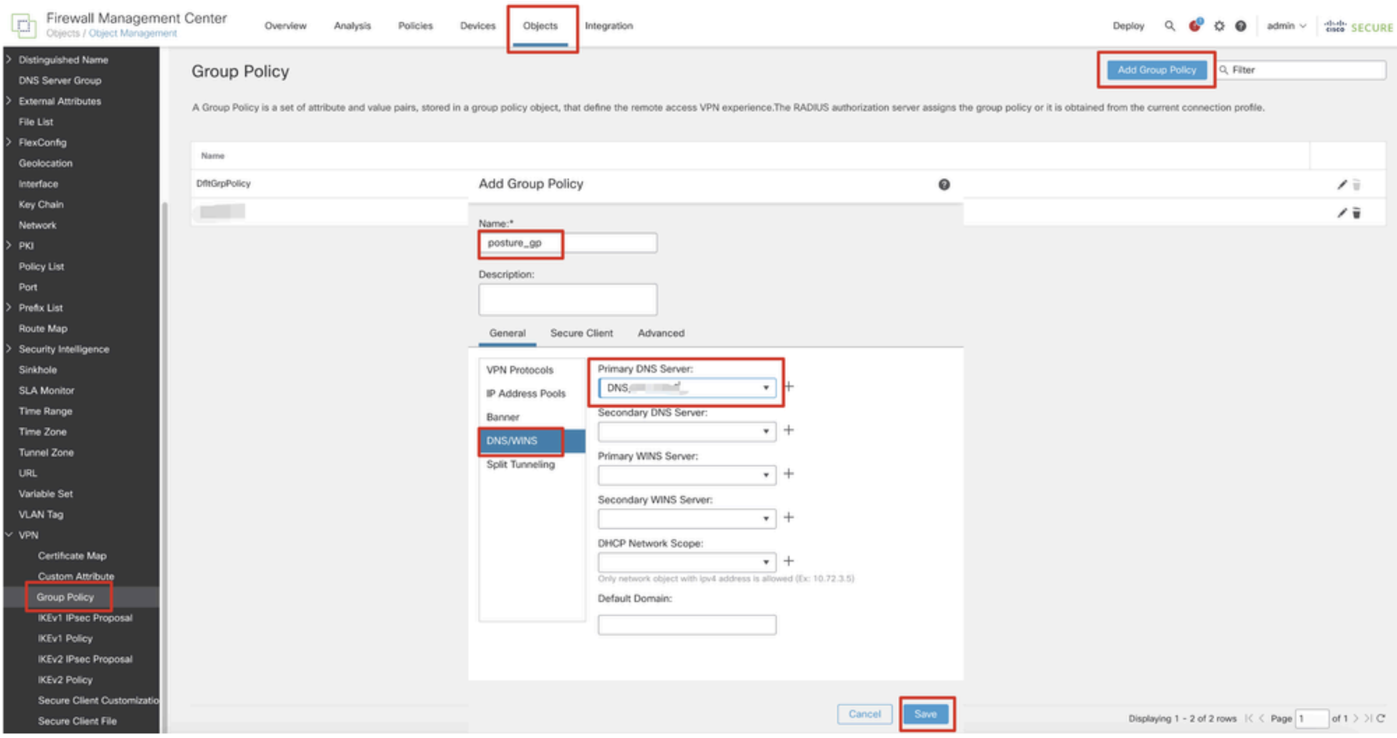
Network: ● Host ○ Range ○ Network ○ FQDN

[redacted]

□ Allow Overrides

FMC_Add_Object_ISE

Passaggio 5. Passare a Objects > Object Management > VPN > Group Policy. Fare clic su .Add Group Policy Fare clic su DNS/WINS, selezionare l'oggetto del server DNS in Primary DNS Server. Quindi fate clic su Save.



Group Policy

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.

Add Group Policy

Name:* posture_gp

Description:

Primary DNS Server: DNS_[redacted]

Secondary DNS Server:

Primary WINS Server:

Secondary WINS Server:

DHCP Network Scope:

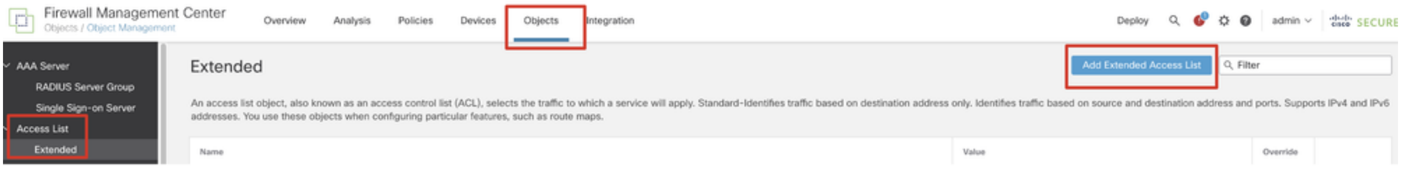
Only network object with ipv4 address is allowed (Ex: 10.72.3.5)

Default Domain:

FMC_Add_Group_Policy

Nota: verificare che il server DNS utilizzato in Criteri di gruppo VPN sia in grado di risolvere il nome di dominio completo del portale di provisioning dei client ISE e enroll.cisco.com.

Passaggio 6. Passare a Objects > Object Management > Access List > Extended. Fare clic su .Add Extended Access List

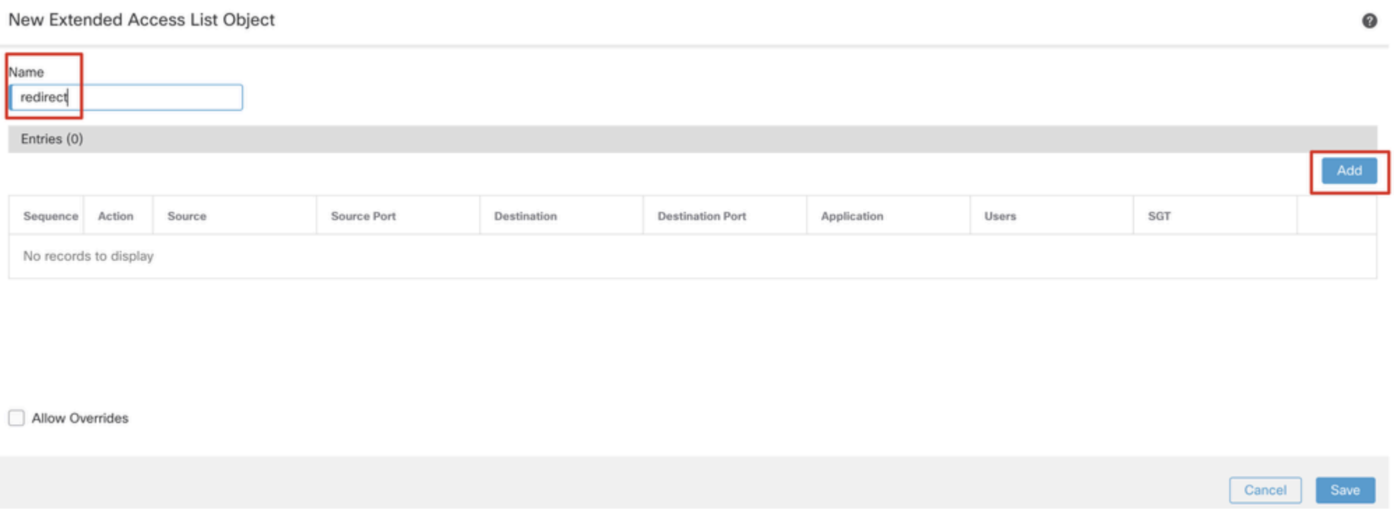


Extended

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.

FMC_Add_Redirect_ACL

Passaggio 6.1. Specificare il nome dell'ACL di reindirizzamento. Questo nome deve essere uguale a quello specificato nel profilo di autorizzazione ISE. Fare clic su .Add



New Extended Access List Object

Name: redirect

Entries (0)

Add

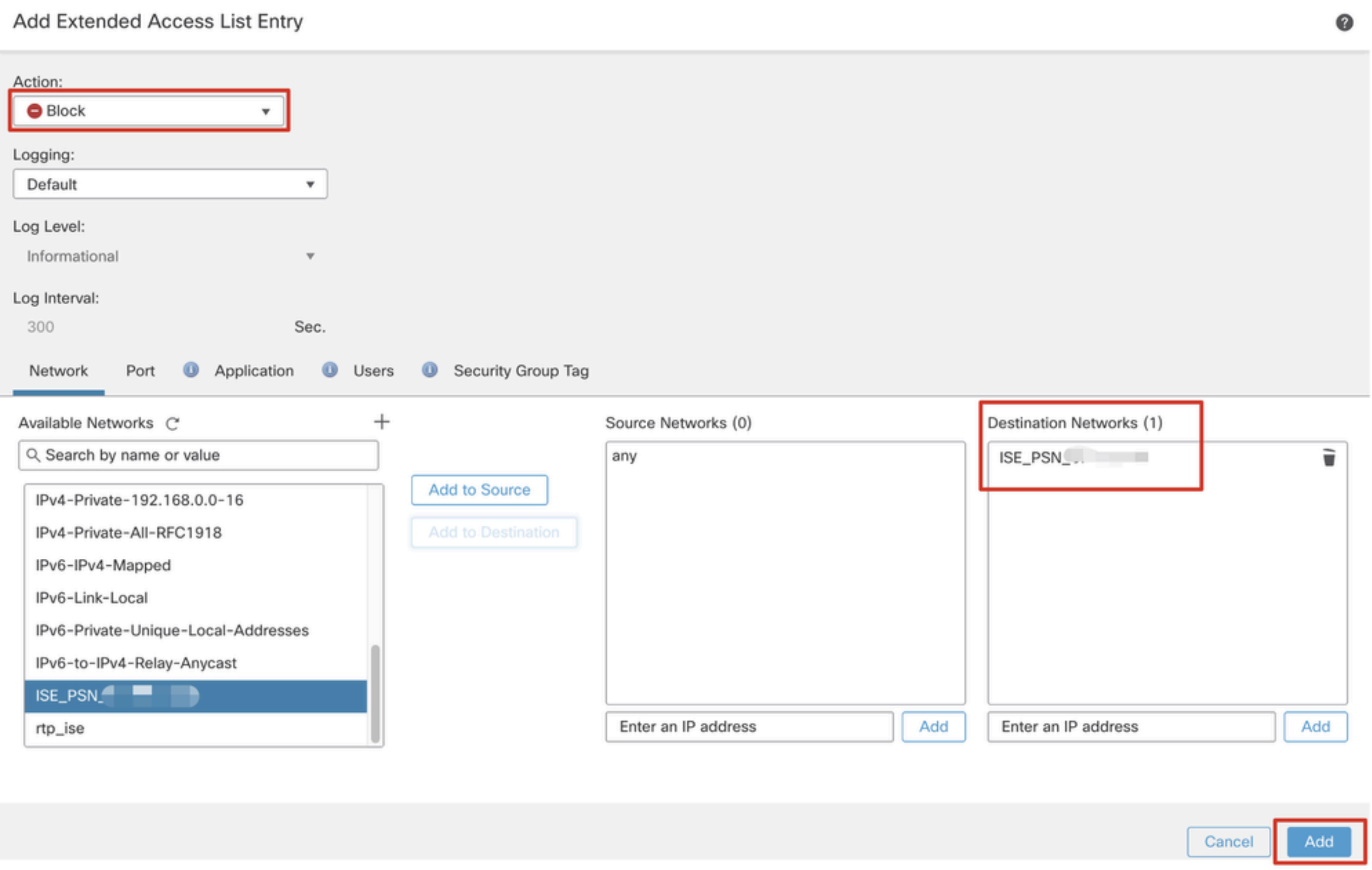
Sequence	Action	Source	Source Port	Destination	Destination Port	Application	Users	SGT
No records to display								

□ Allow Overrides

Cancel Save

FMC_Add_Redirect_ACL_Part_1

Passaggio 6.2. Blocca il traffico DNS, il traffico verso l'indirizzo IP PSN ISE e i server di correzione per escluderli dal reindirizzamento. Consentire il resto del traffico. Questo attiva il reindirizzamento. Fare clic su .Save



Add Extended Access List Entry

Action: Block

Logging: Default

Log Level: Informational

Log Interval: 300 Sec.

Network | Port | Application | Users | Security Group Tag

Available Networks

Search by name or value

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

Add to Source

Add to Destination

Source Networks (0): any

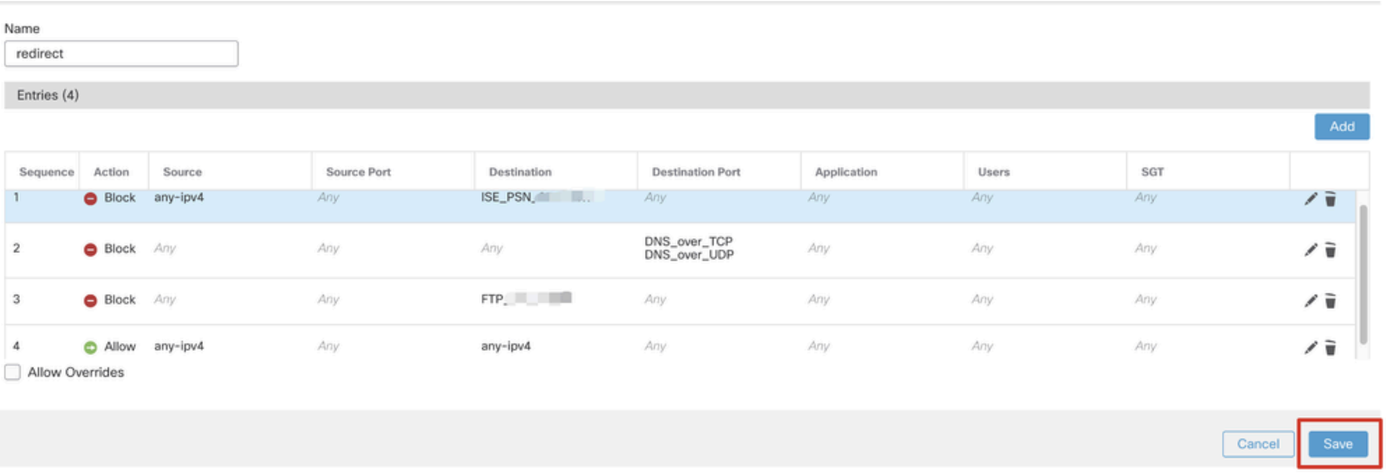
Enter an IP address Add

Destination Networks (1): ISE_PSN_[redacted]

Enter an IP address Add

Cancel Add

FMC_Add_Redirect_ACL_Part_2



Name

redirect

Entries (4)

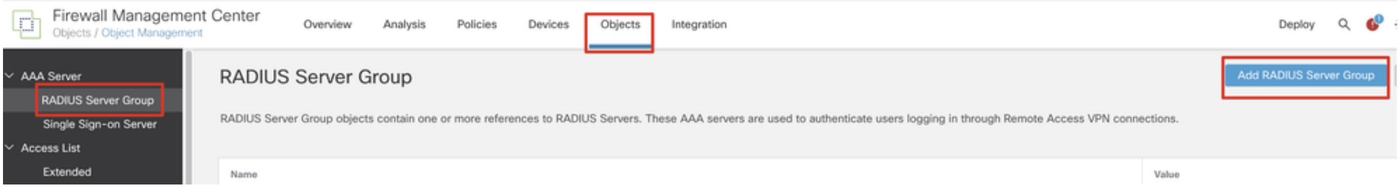
Sequence	Action	Source	Source Port	Destination	Destination Port	Application	Users	SGT
1	Block	any-ipv4	Any	ISE_PSN_[redacted]	Any	Any	Any	Any
2	Block	Any	Any	Any	DNS_over_TCP DNS_over_UDP	Any	Any	Any
3	Block	Any	Any	FTP_[redacted]	Any	Any	Any	Any
4	Allow	any-ipv4	Any	any-ipv4	Any	Any	Any	Any

□ Allow Overrides

FMC_Add_Redirect_ACL_Part_3

Nota: come esempio del server di monitoraggio e aggiornamento viene utilizzato l'FTP di destinazione in questo esempio di ACL di reindirizzamento.

Passaggio 7. Passare a Objects > Object Management > RADIUS Server Group. Fare clic su .Add RADIUS Server Group

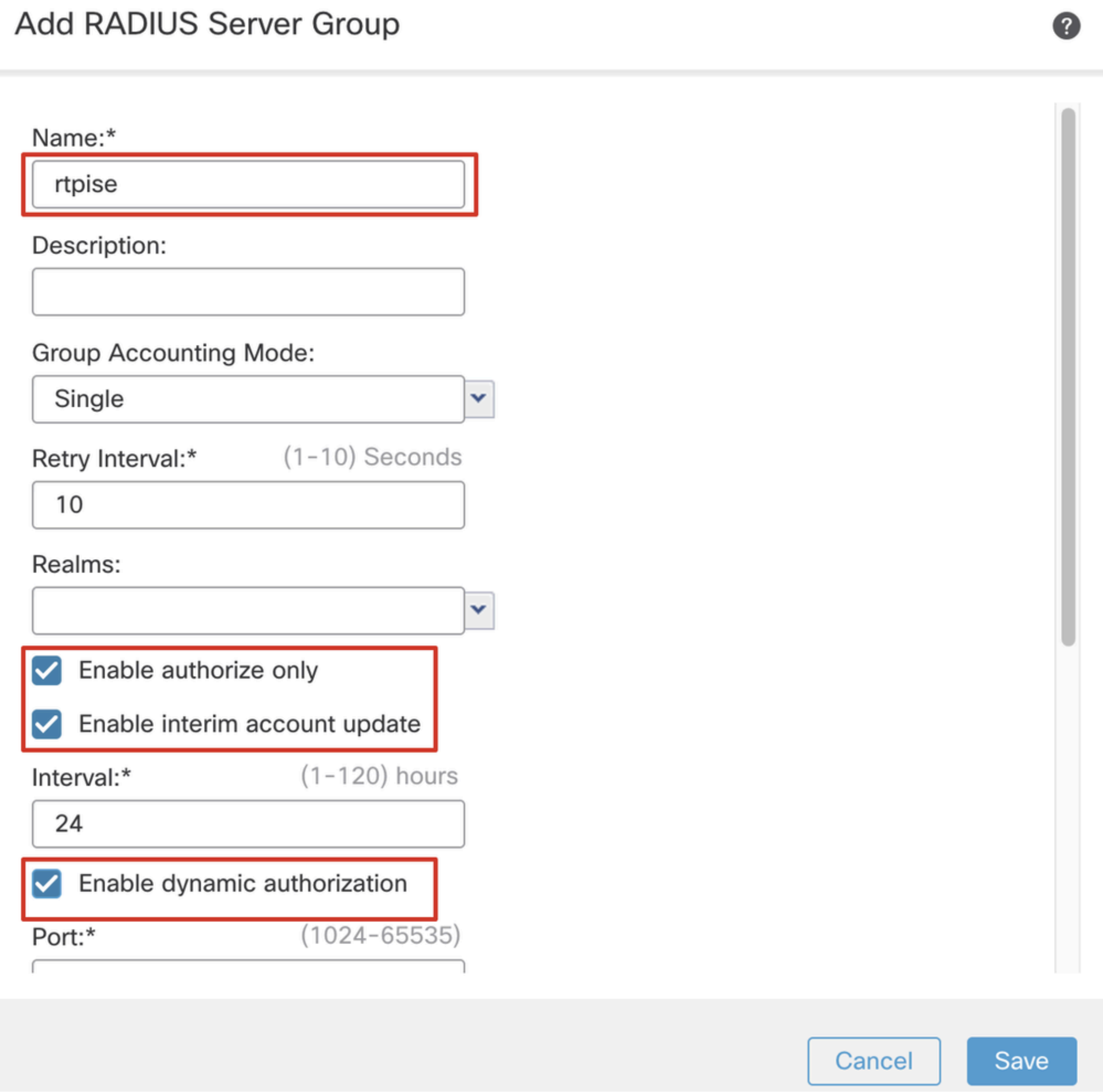


RADIUS Server Group

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

Passaggio 7.1. Fornire nome, controlloEnable authorize only, controllo Enable interim account update, controllo 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

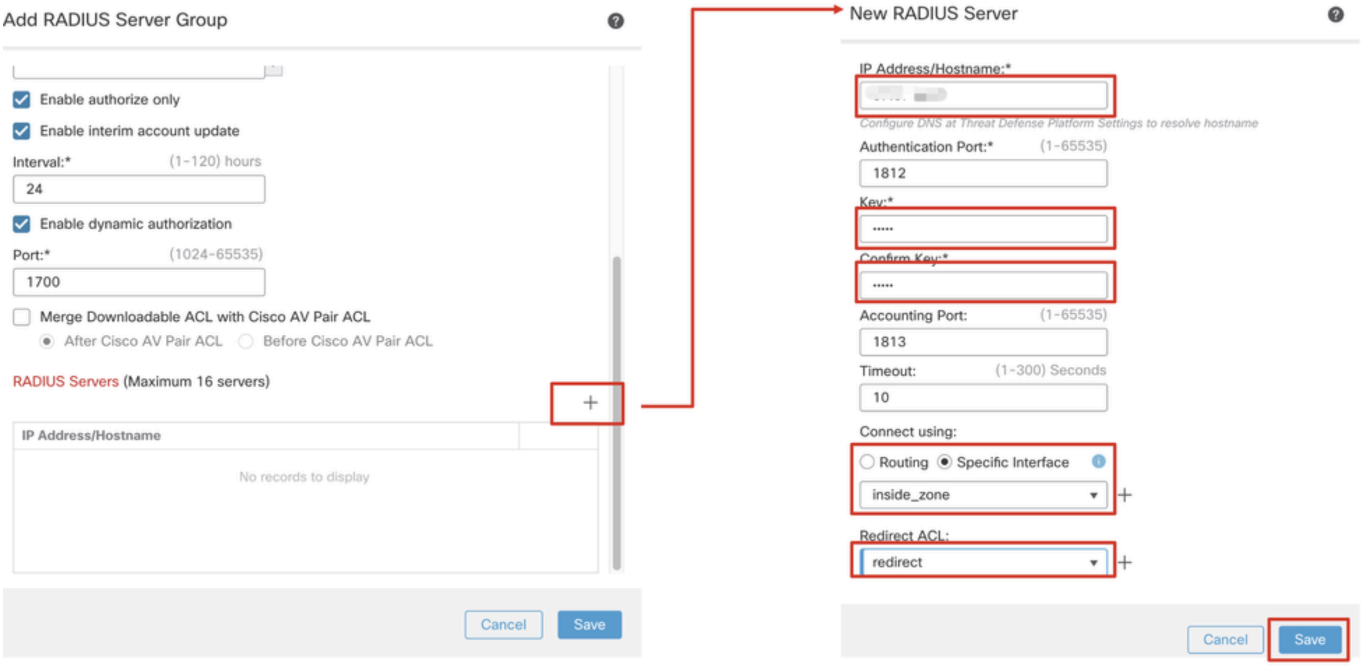
Interval:* (1-120) hours 24

☑ Enable dynamic authorization

Port:* (1024-65535)

FMC_Add_New_Radius_Server_Group_Part

Passaggio 7.2. Fare clic sull'Plus icona per aggiungere un nuovo server RADIUS. Fornire il numero di serie del servizio (PSN)IP Address/Hostname, Key per l'ISE. Selezionare il nome per la specific interface connessione. Selezionare la Redirect ACLvoce. Quindi fare clic su Saveper salvare il nuovo server radius. Quindi fare nuovamente clicSave su per salvare il nuovo gruppo di server radius.



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)

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

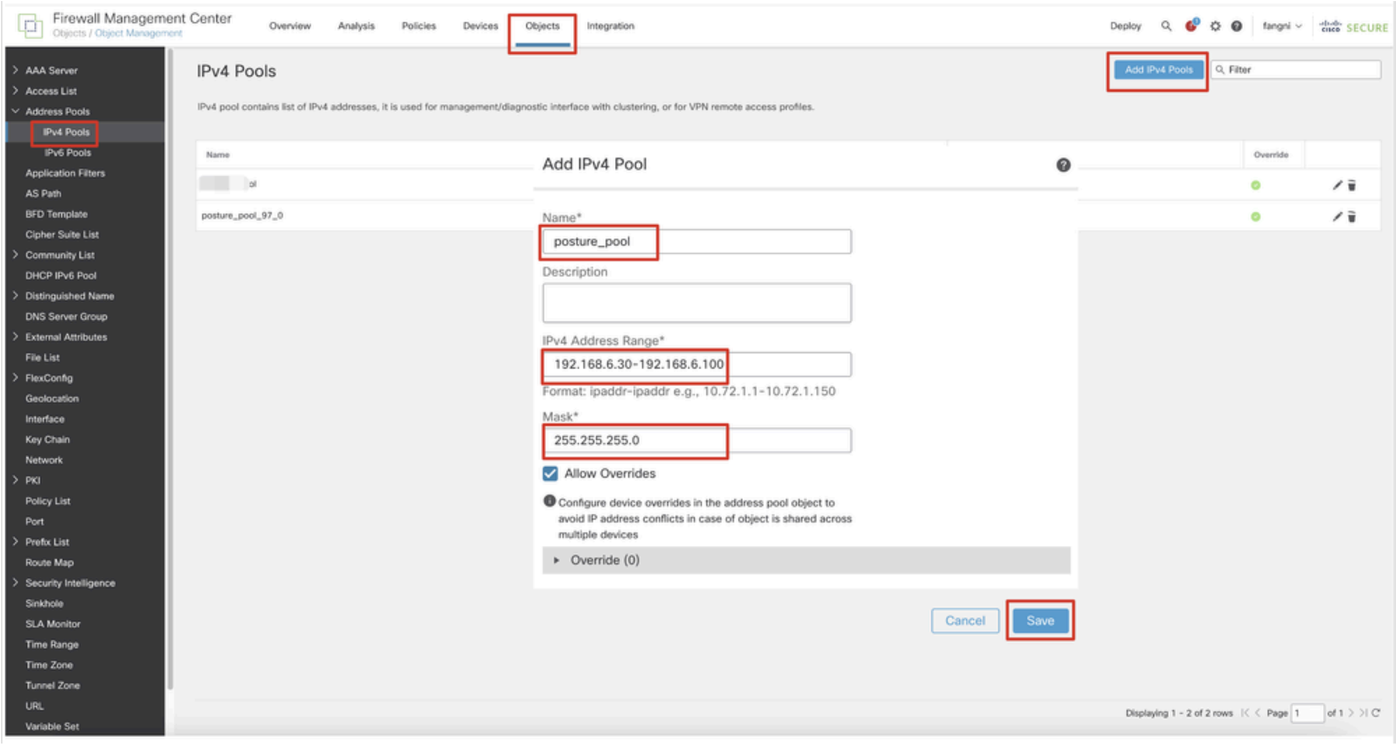
inside_zone

Redirect ACL:

redirect

FMC_Add_New_Radius_Server_Group_Part

Passaggio 8. Passare a Objects > Object Management > Address Pools > IPv4 Pools. Fare clic su Add IPv4 Pools e specificare **Name, IPv4 Address Range**e Mask. Quindi fate clic su 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]ol	●
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

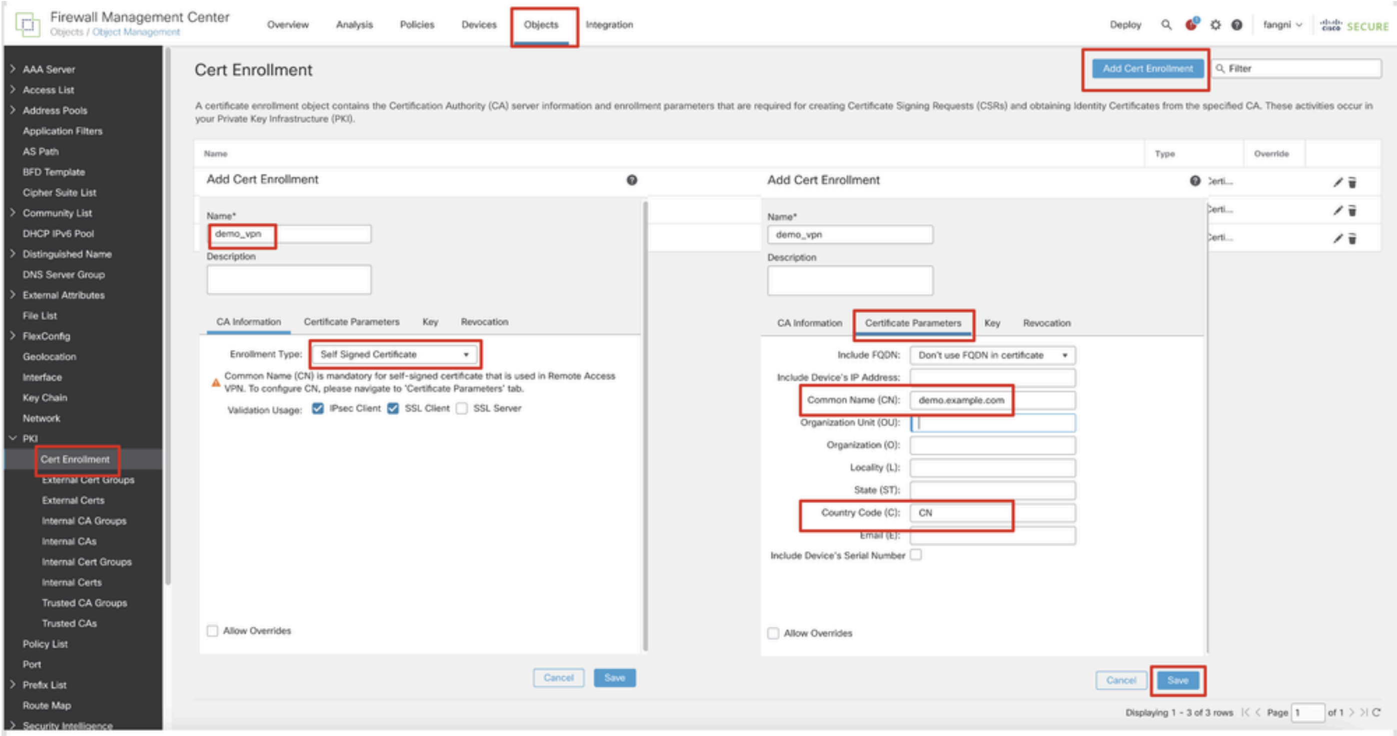
☑ Allow Overrides

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

Passaggio 9. Passare a Certificate Objects > Object Management > PKI > Cert Enrollment. Fare clic suAdd Cert Enrollment, fornire un nome e selezionare Self Signed Certificatein Enrollment Type. Fare clic sulla Certificate Parameters scheda e specificare Common Name e Country Code. Quindi fate clic su 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

□ Allow Overrides

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):

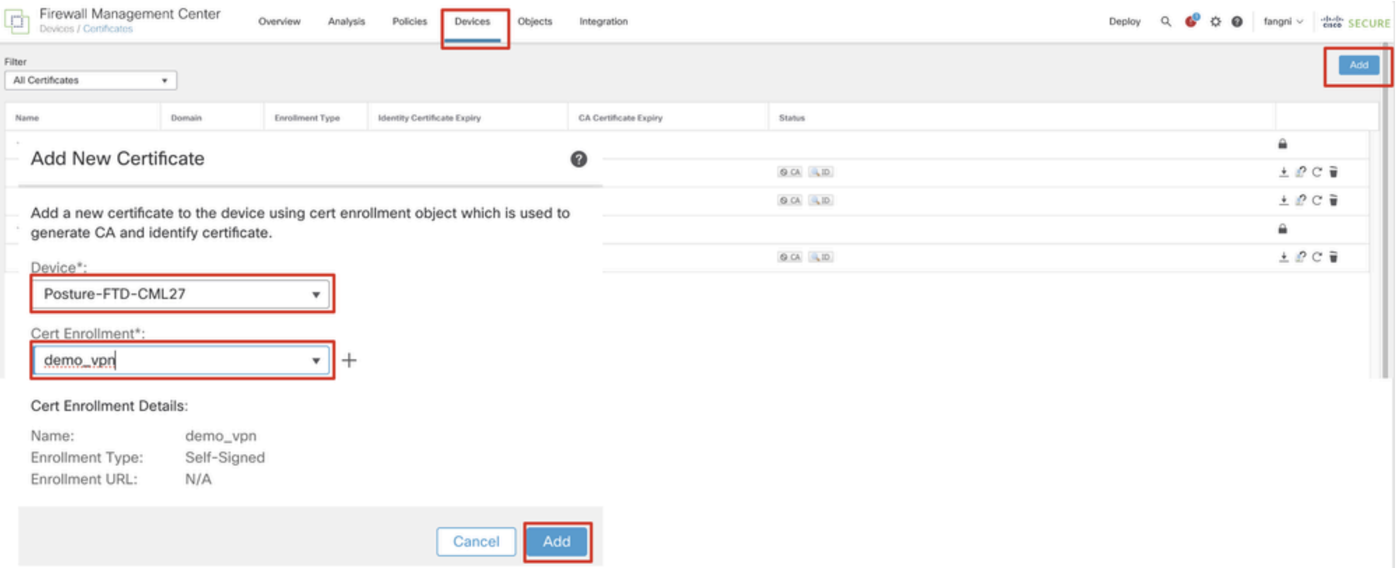
Include Device's Serial Number □

□ Allow Overrides

Displaying 1 - 3 of 3 rows

FMC_Add_New_Cert_Enroll

Passaggio 10. Passare a Devices > Certificates. Fare clic suAdd, selezionare il nome FTD in Device, selezionare l'iscrizione configurata in precedenza in Cert Enrollment. Fare clic su .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

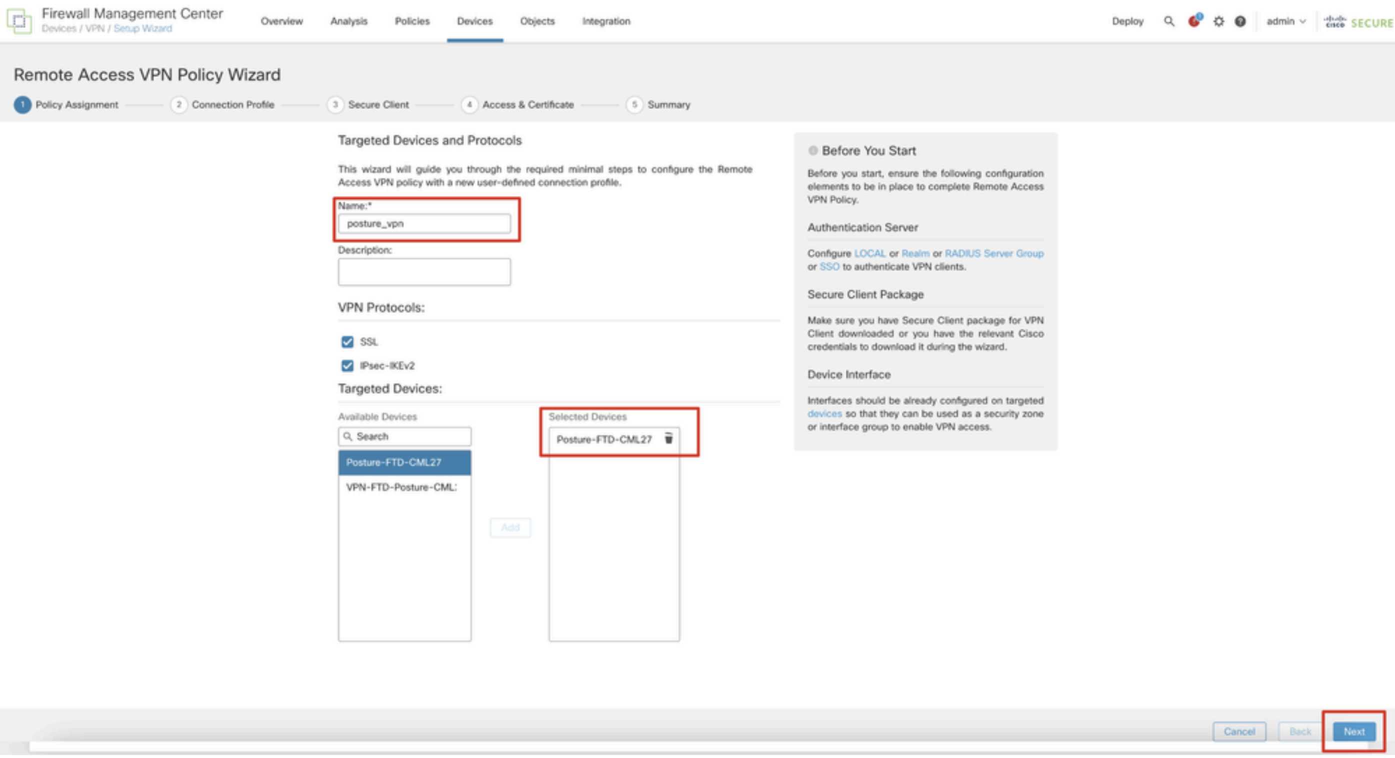
Cert Enrollment Details:

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

FMC_Add_New_Cert_To_FTD

Passaggio 11. Passare a Devices > VPN > Remote Access. Fare clic su .Add

Passaggio 11.1. Fornire il nome e aggiungere l'FTD a Selected Devices. Fare clic su .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

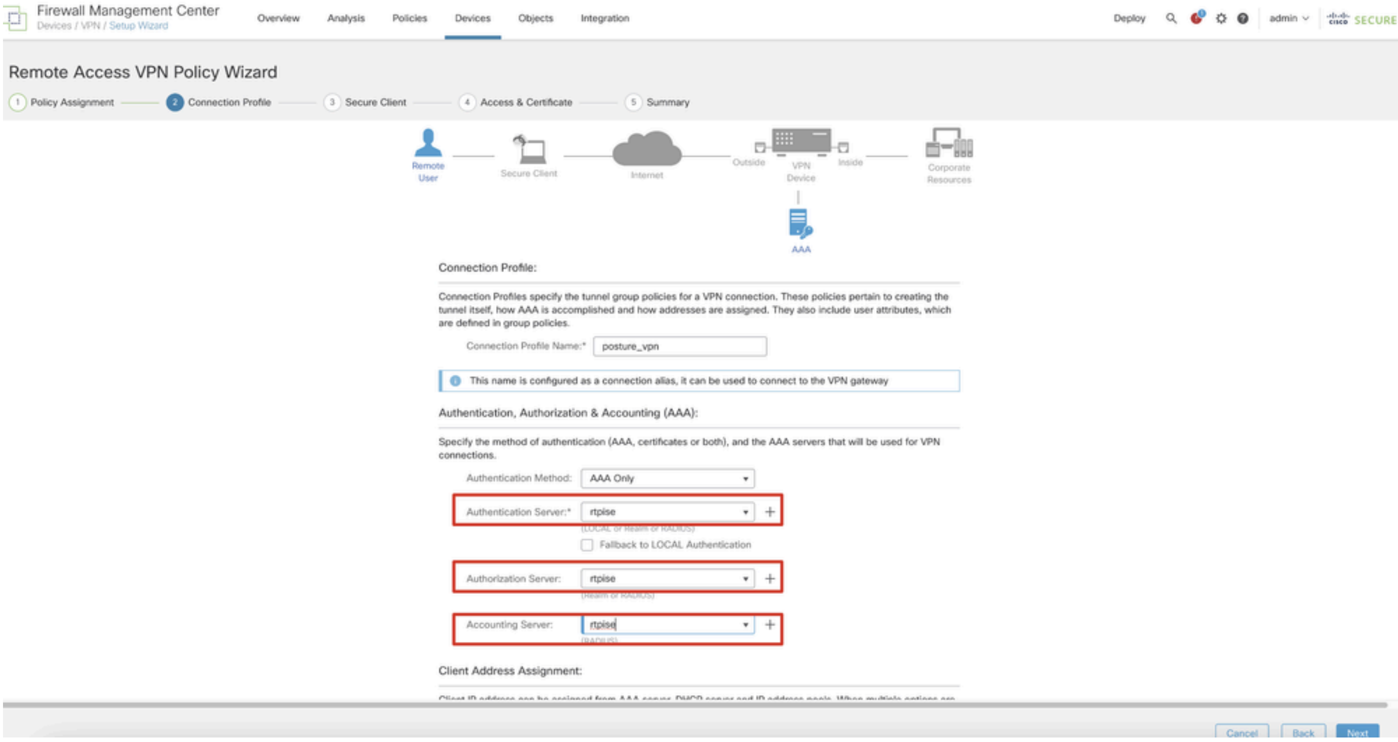
Make sure you have Secure Client package for VPN Client downloaded or you have the relevant Cisco credentials to download it during the wizard.

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

Passaggio 11.2. Selezionare il gruppo di server radius configurato in precedenza in Authentication Server, Authorization Server, Accounting Server. Scorrere la pagina verso il basso.



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

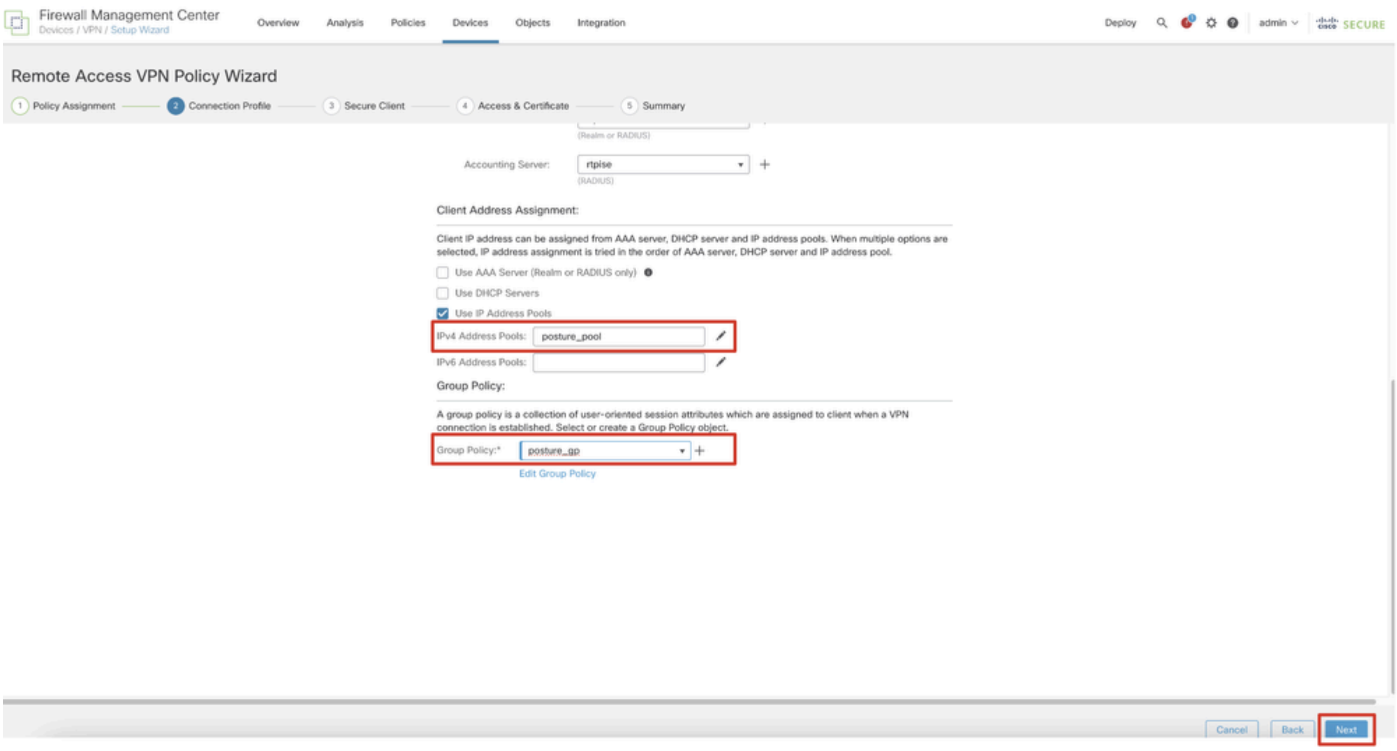
Authorization Server: rtpise (Realm or RADIUS)

Accounting Server: rtpise (RADIUS)

Client Address Assignment:

FMC_New_RAVPN_Wizard_2

Passaggio 11.3. Selezionare il nome del pool configurato in precedenza in IPv4 Address Pools. Selezionare Criteri di gruppo configurati in precedenza in Group Policy. Fare clic su 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:

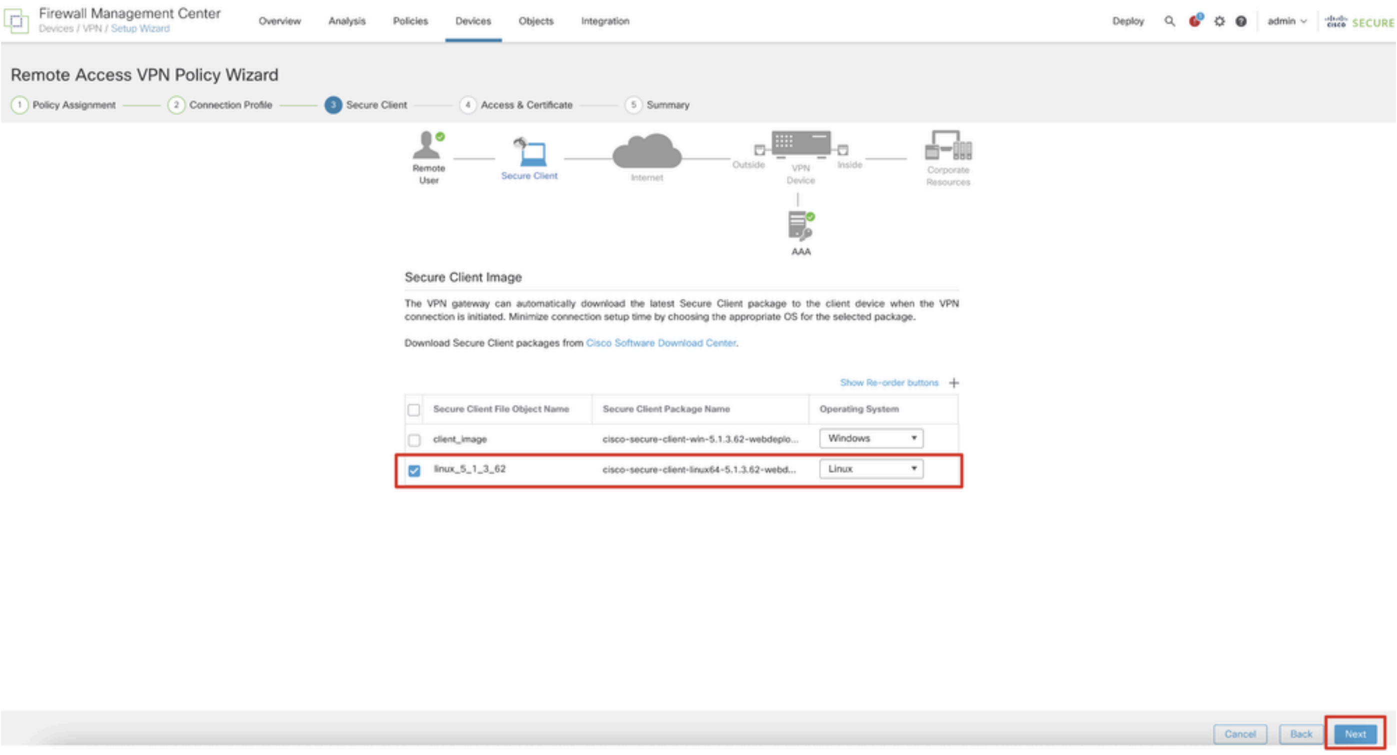
A group policy is a collection of user-oriented session attributes which are assigned to client when a VPN connection is established. Select or create a Group Policy object.

Group Policy:* posture_gp

Edit Group Policy

FMC_New_RAVPN_Wizard_3

Passaggio 11.4. Selezionare la casella di controllo dell'immagine Linux. Fare clic su .Next



Secure Client Image

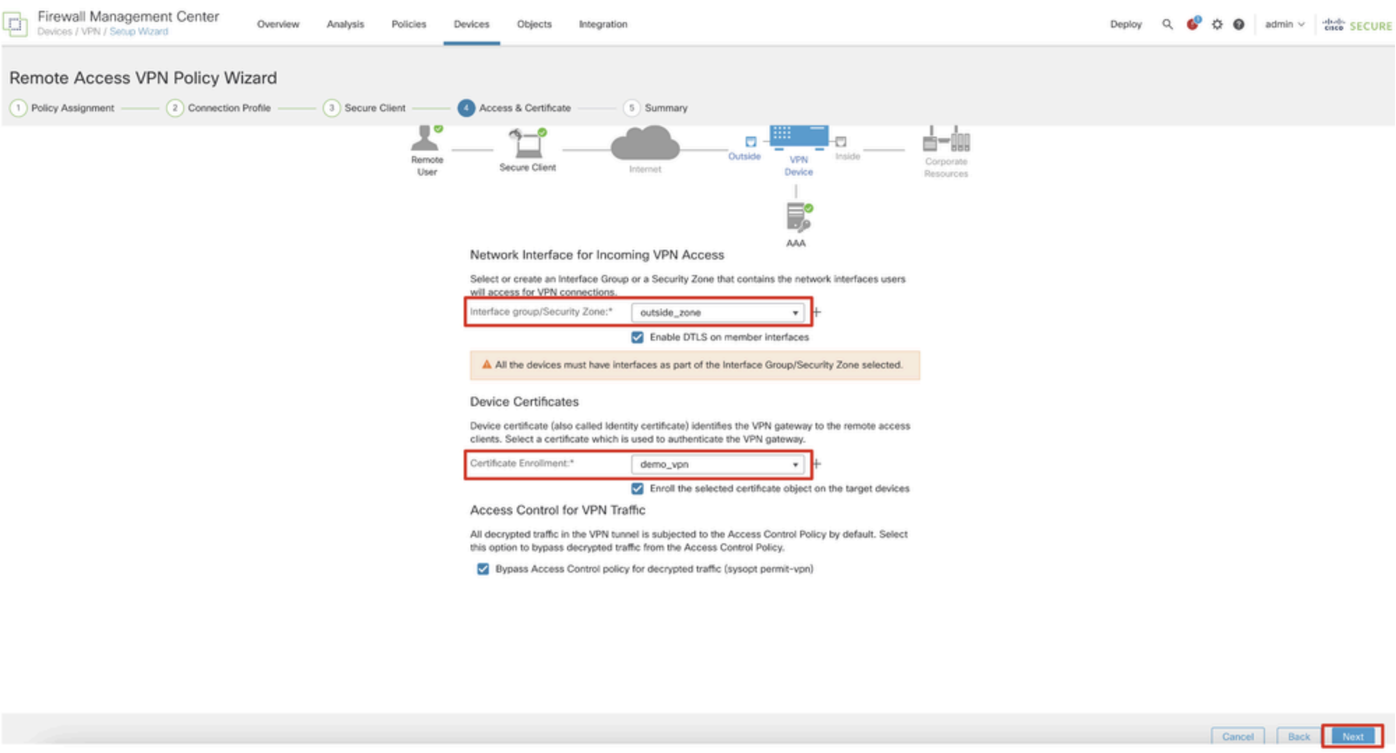
The VPN gateway can automatically download the latest Secure Client package to the client device when the VPN connection is initiated. Minimize connection setup time by choosing the appropriate OS for the selected package.

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

Passaggio 11.5. Selezionare l'interfaccia dell'interfaccia VPN. Selezionare l'iscrizione certificato registrata in FTD nel passaggio 9. Fare clic su .Next



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:* 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

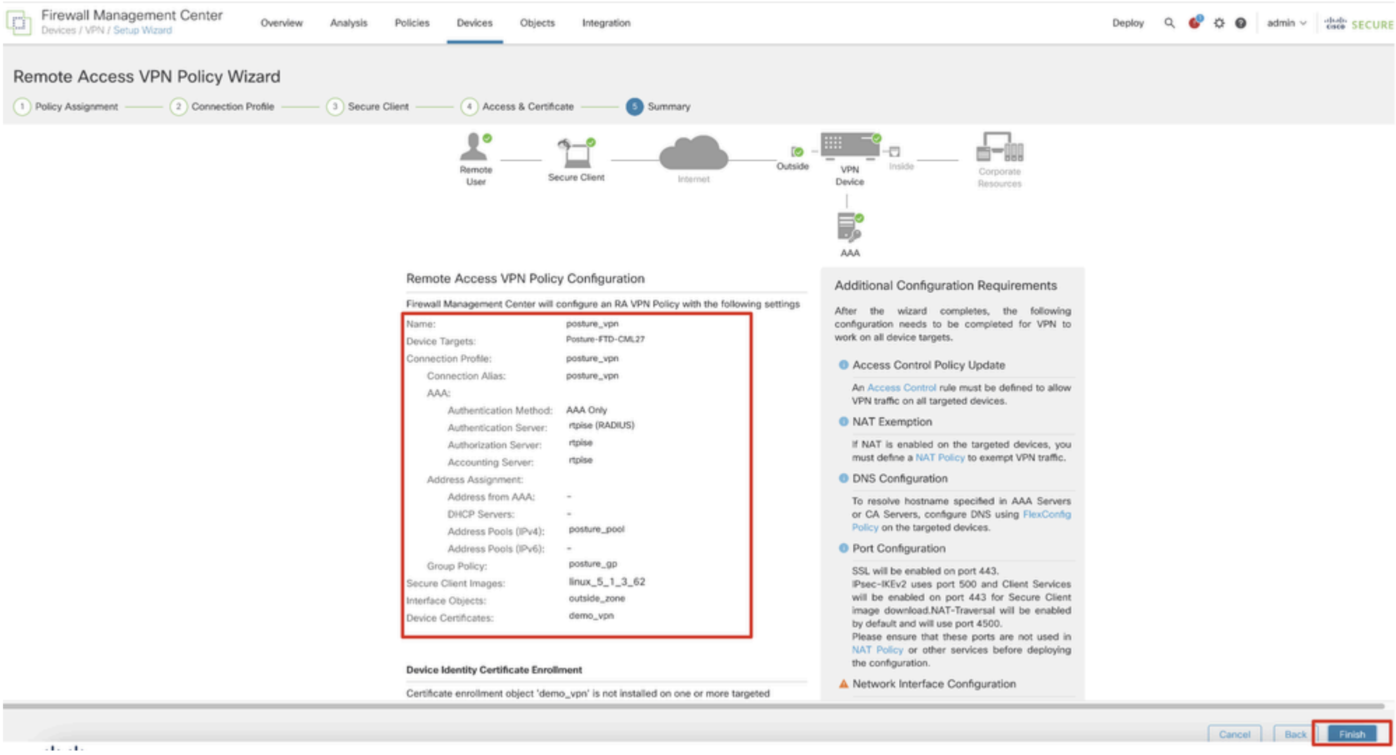
Access Control for VPN Traffic

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

Passaggio 11.6. Confermare le informazioni correlate nella pagina di riepilogo. Se tutto funziona, fare clic su Finish. Se è necessario apportare modifiche, fare clic su Back.



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-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.

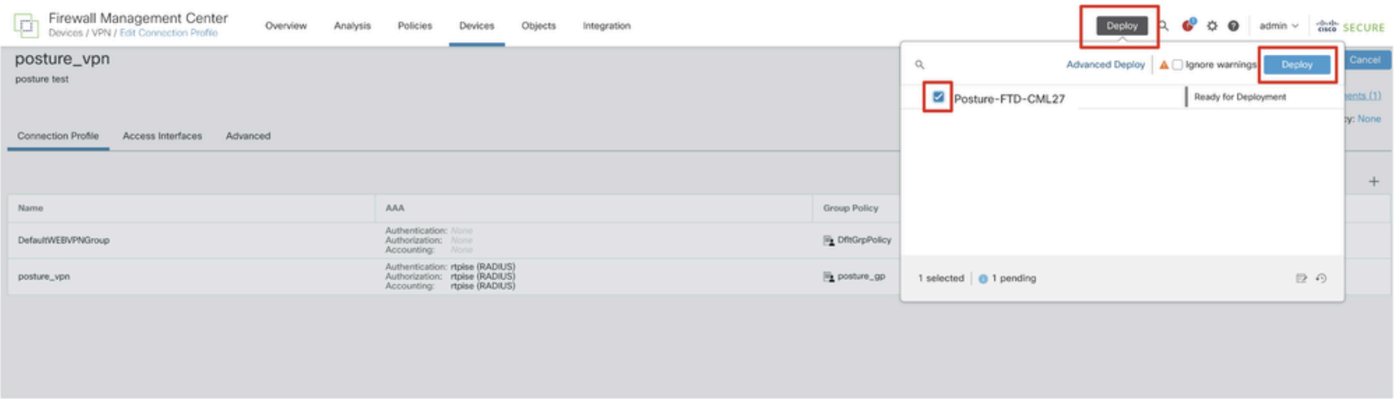
Port Configuration

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

Passaggio 12. Distribuire la nuova configurazione in FTD per completare la configurazione della VPN di accesso remoto.

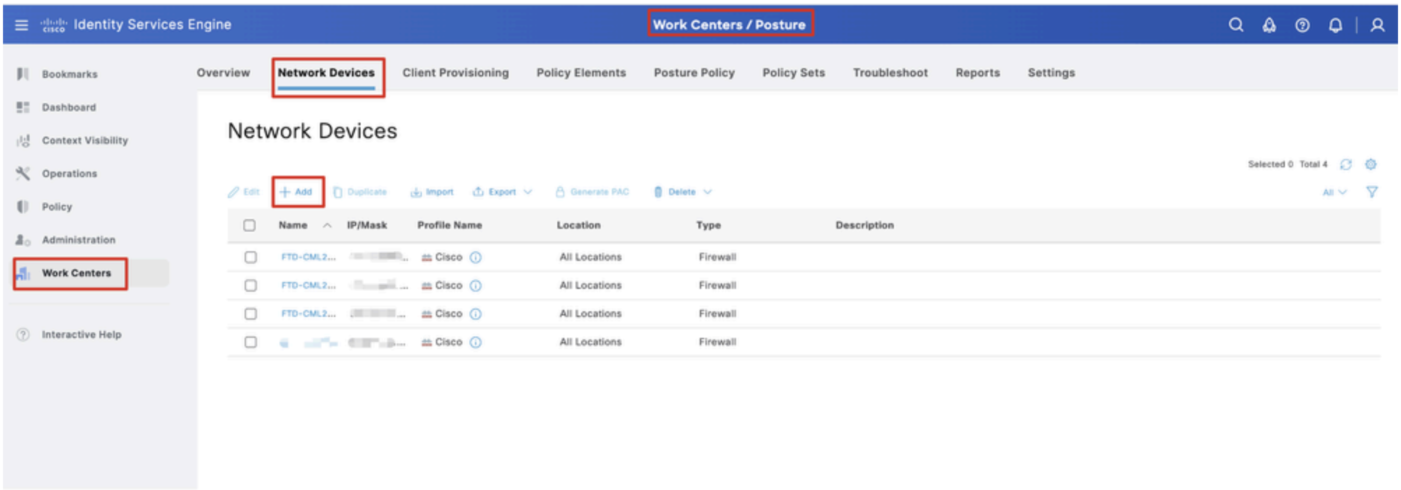


Name	AAA	Group Policy
DefaultWEBVPNGroup	Authentication: None Authorization: None Accounting: None	DfltGrpPolicy
posture_vpn	Authentication: rtpise (RADIUS) Authorization: rtpise (RADIUS) Accounting: rtpise (RADIUS)	posture_gp

FMC_Deploy_FTD

Configurazioni su ISE

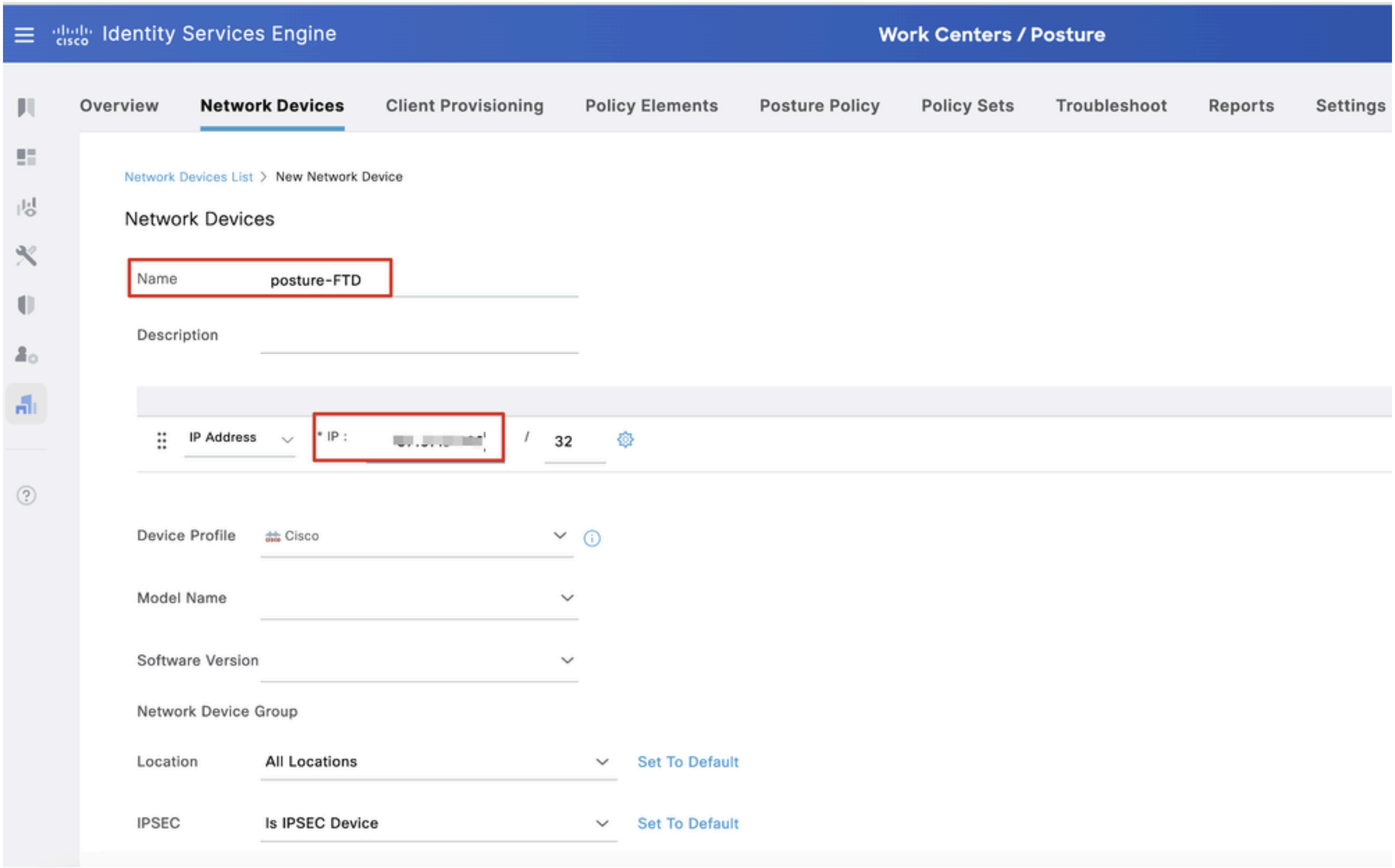
Passaggio 13. Passare a Work Centers > Posture > Network Devices. Fare clic su .Add



☐	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

Passaggio 13.1. Fornire le informazioni Name, IP Addresse scorrere la pagina verso il basso.



Network Devices List > New Network Device

Network Devices

Name posture-FTD

Description

IP Address * IP : [redacted] / 32

Device Profile Cisco

Model Name

Software Version

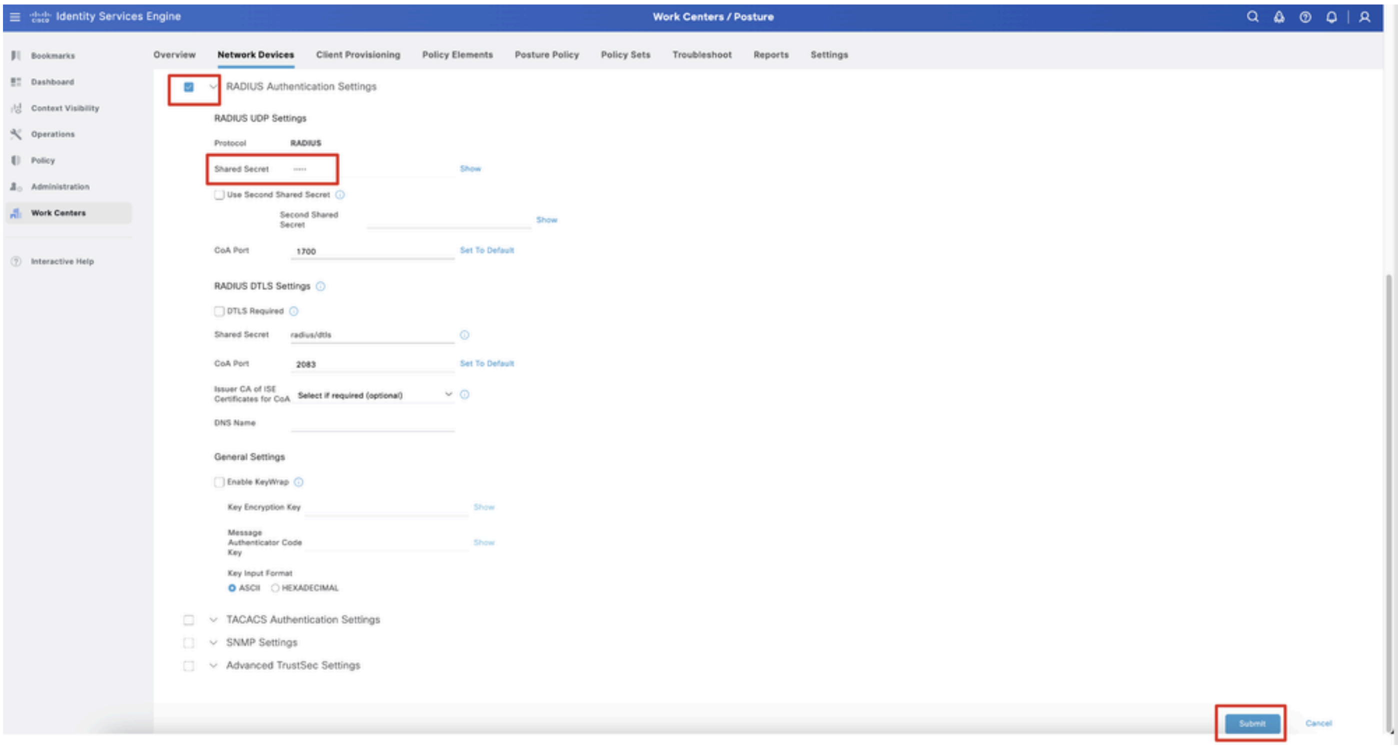
Network Device Group

Location All Locations Set To Default

IPSEC Is IPSEC Device Set To Default

ISE_Add_New_Devices_1

Passaggio 13.2. Selezionare la casella di spunta di RADIUS Authentication Settings. Fornire il Shared Secret. Fare clic su .Submit



☑ RADIUS Authentication Settings

RADIUS UDP Settings

Protocol RADIUS

Shared Secret ····· Show

□ Use Second Shared Secret

Second Shared Secret Show

CoA Port 1700 Set To Default

RADIUS DTLS Settings

□ DTLS Required

Shared Secret radius/dtls

CoA Port 2083 Set To Default

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

DNS Name

General Settings

□ Enable KeyWrap

Key Encryption Key Show

Message Authenticator Code Key Show

Key Input Format

● ASCII ○ HEXADECIMAL

□ TACACS Authentication Settings

□ SNMP Settings

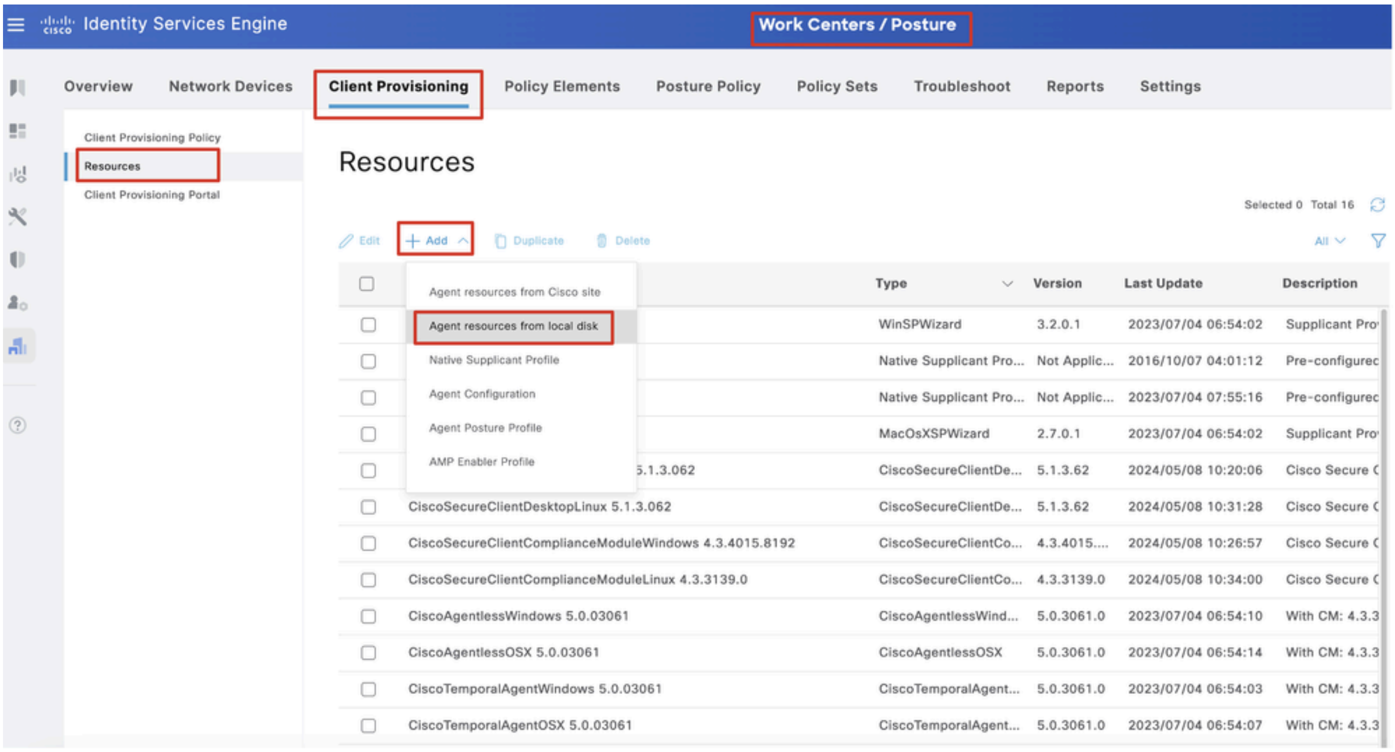
□ Advanced TrustSec Settings

ISE_Add_New_Devices_2

Passaggio 14. Scaricare il nome del pacchetto cisco-secure-client-linux64-4.3.3139.0-isecompliance-webdeploy-k9.pkg da Cisco Software Download e accertarsi che il file sia valido confermando che il checksum md5 del file scaricato è lo stesso della pagina di download del software

Cisco. Download del nomecisco-secure-client-linux64-5.1.3.62-webdeploy-k9.pkg del pacchetto completato nel passaggio 1.

Passaggio 15. Passare a Work Centers > Posture > Client Provisioning > Resources. Fare clic su .Add Selezionare Agent resources from local disk.

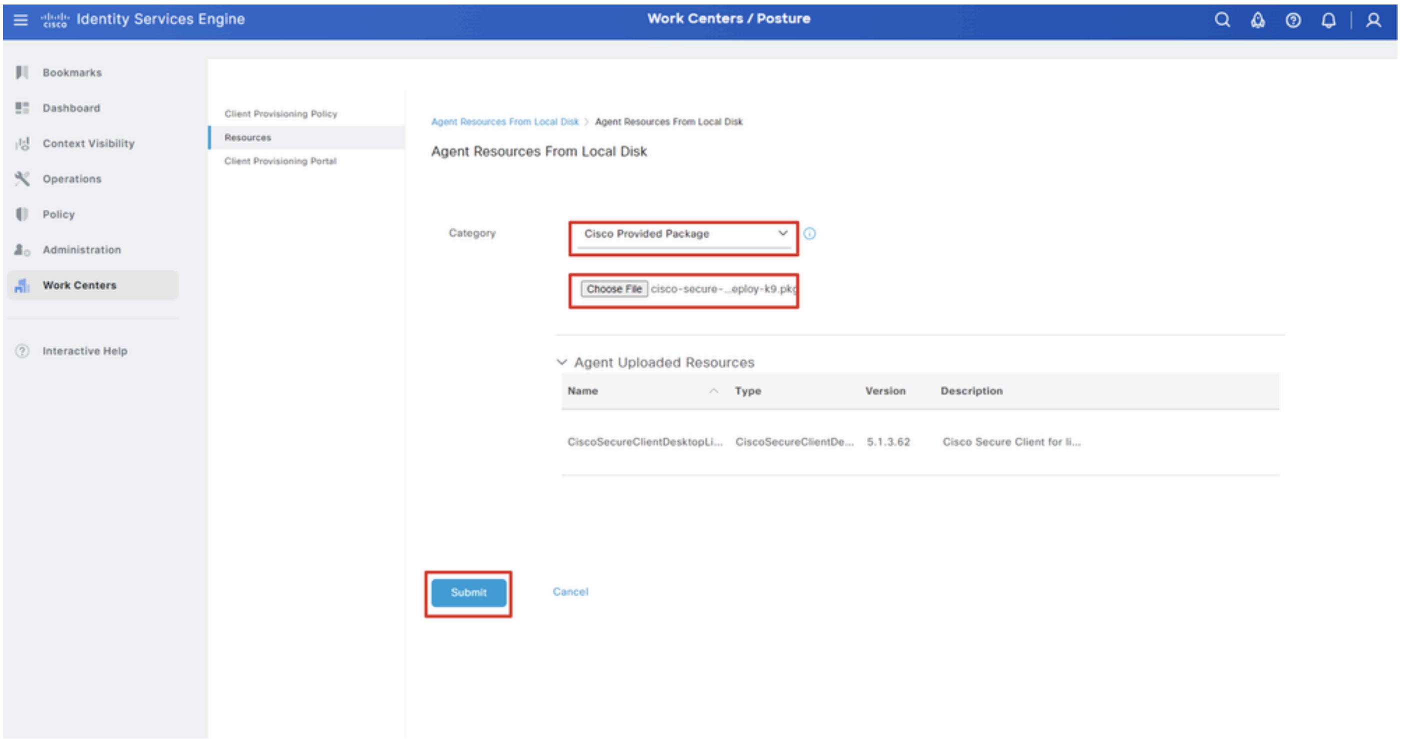


Resources

□		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

Passaggio 15.1. Selezionare Cisco Provided Package. Fare clicChoose File per caricare cisco-secure-client-linux64-5.1.3.62-webdeploy-k9.pkg. Fare clic su .Submit



Agent Resources From Local Disk

Category: Cisco Provided Package

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

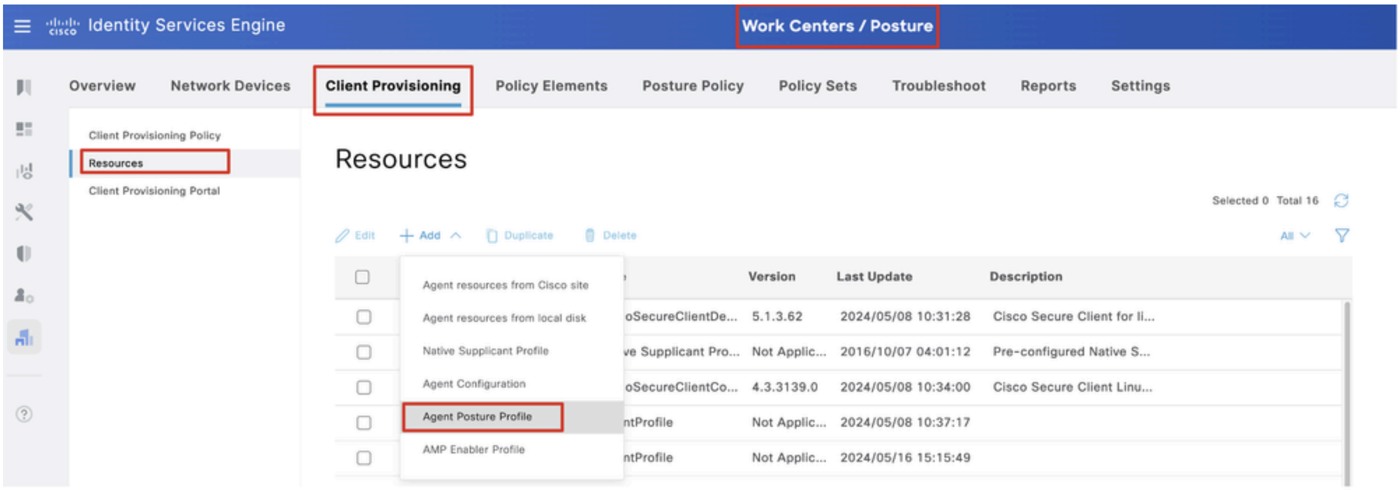
Agent Uploaded Resources

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

ISE_Upload_Resources_1

Nota: ripetere il passo 14. per caricare cisco-secure-client-linux64-4.3.3139.0-isecompliance-webdeploy-k9.pkg.

Passaggio 16. Passare a Work Centers > Posture > Client Provisioning > Resources. Fare clic su .Add Selezionare Agent Posture Profile.



Resources

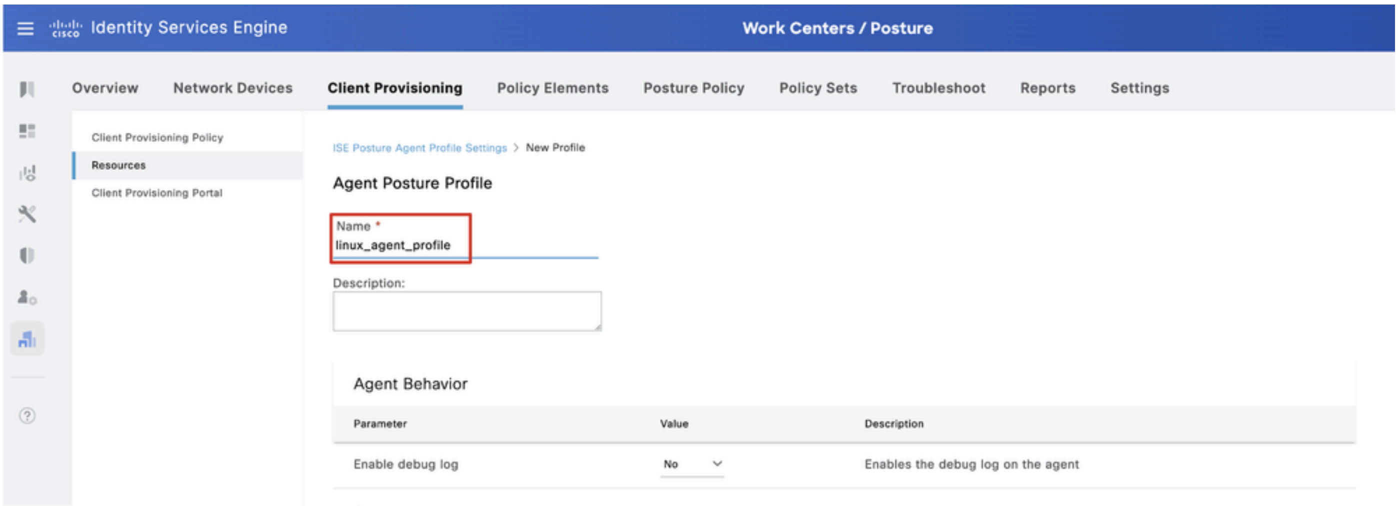
	Version	Last Update	Description
oSecureClientDe...	5.1.3.62	2024/05/08 10:31:28	Cisco Secure Client for li...
ve Supplicant Pro...	Not Applic...	2016/10/07 04:01:12	Pre-configured Native S...
oSecureClientCo...	4.3.3139.0	2024/05/08 10:34:00	Cisco Secure Client Linu...
ntProfile	Not Applic...	2024/05/08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

ISE_Add_Agent_Posture_Profile

Passaggio 16.1. Fornire il Name, Server name rules e mantenere il resto come valore predefinito. Fare clic su .Save

Nome: linux_agent_profile

Regole nome server: *.example.com



Agent Posture Profile

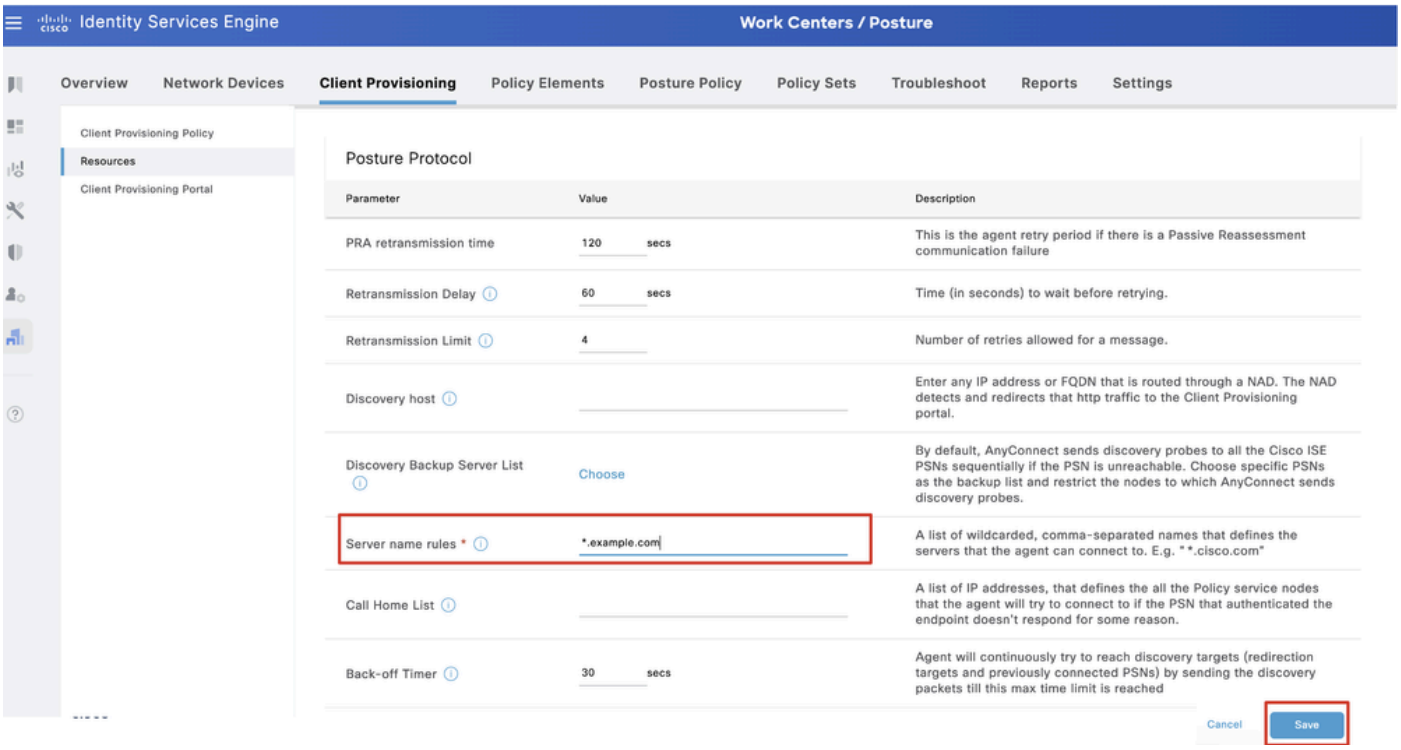
Name *
linux_agent_profile

Description:

Agent Behavior

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

ISE_Add_Agent_Posture_Profile_1

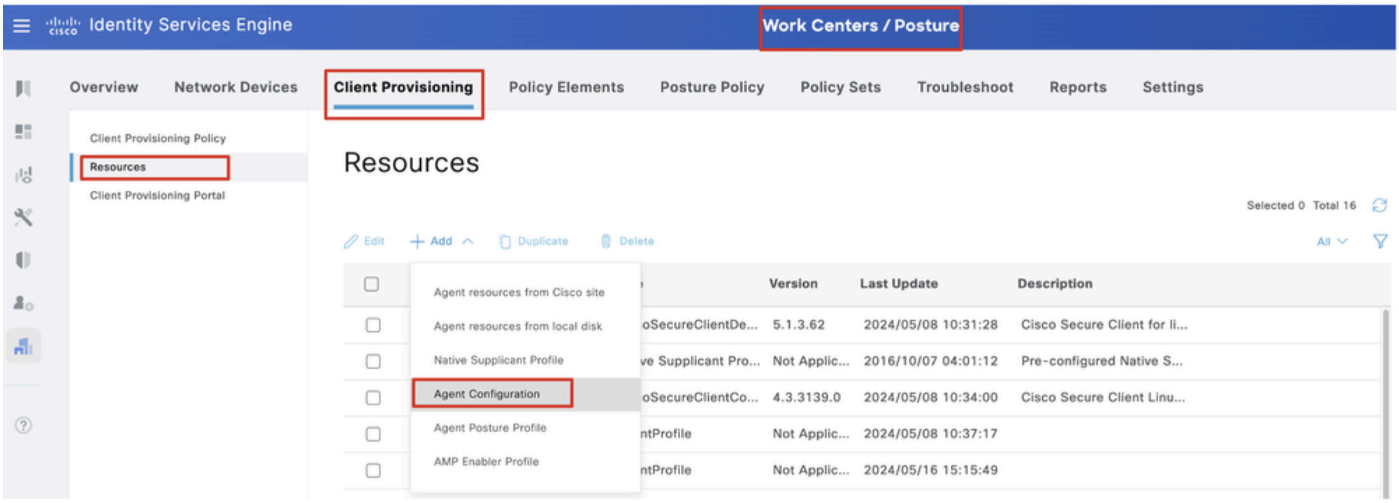


Posture Protocol

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

ISE_Add_Agent_Posture_Profile_2

Passaggio 17. Passare a Work Centers > Posture > Client Provisioning > Resources. Fare clic su .Add Selezionare Agent Configuration.



Resources

Selected 0 Total 16

	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

Passaggio 17.2. Configurare i dettagli:

Seleziona pacchetto agente: CiscoSecureClientDesktopLinux 5.1.3.062

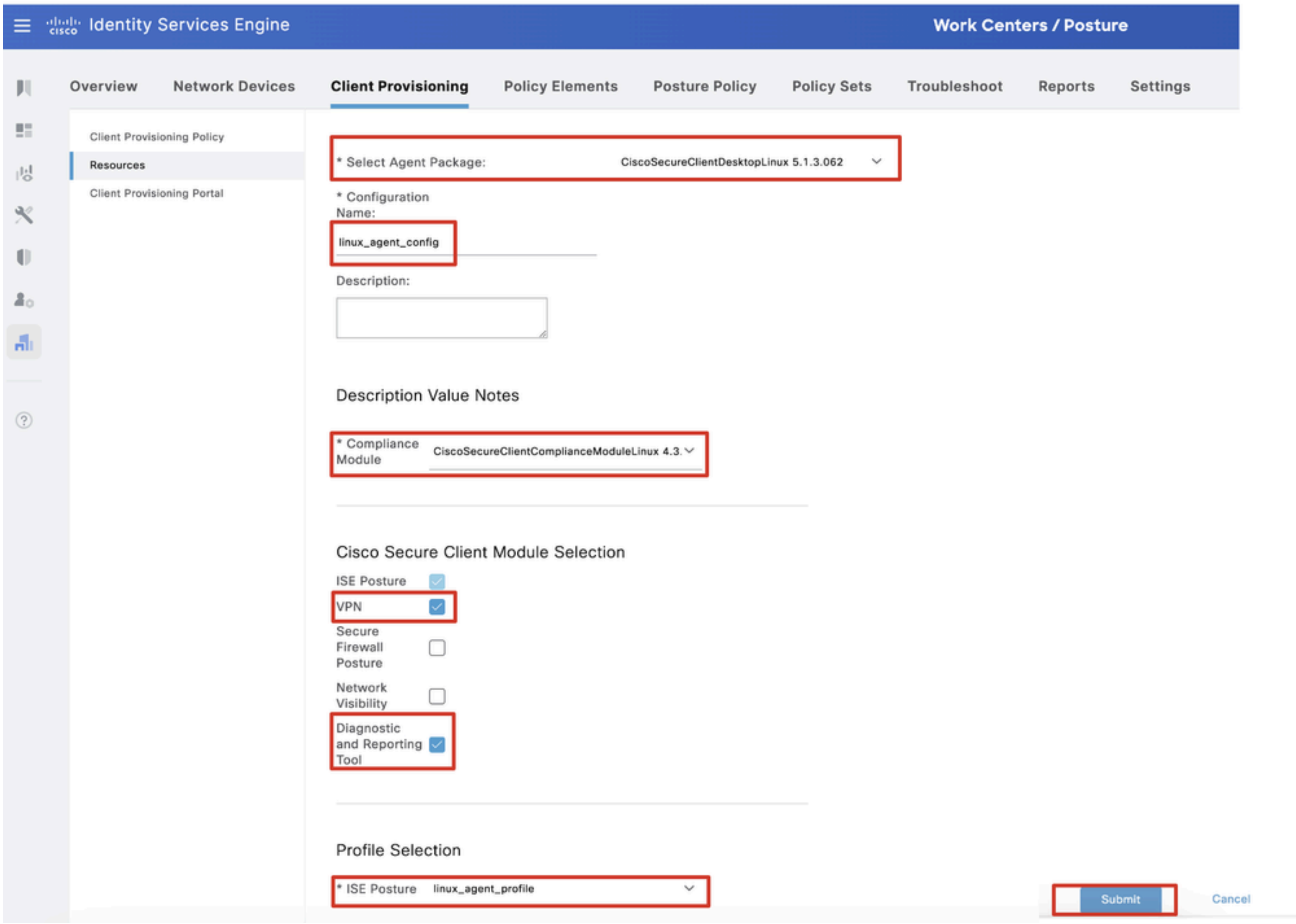
Nome: linux_agent_config

Modulo conformità: Cisco Secure Client Compliance Module Linux 4.3.3139.0

Selezionare la casella di controllo VPN, Diagnostic and Reporting Tool

Selezione profilo ISE Posture: linux_agent_profile

Fare clic su .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 □

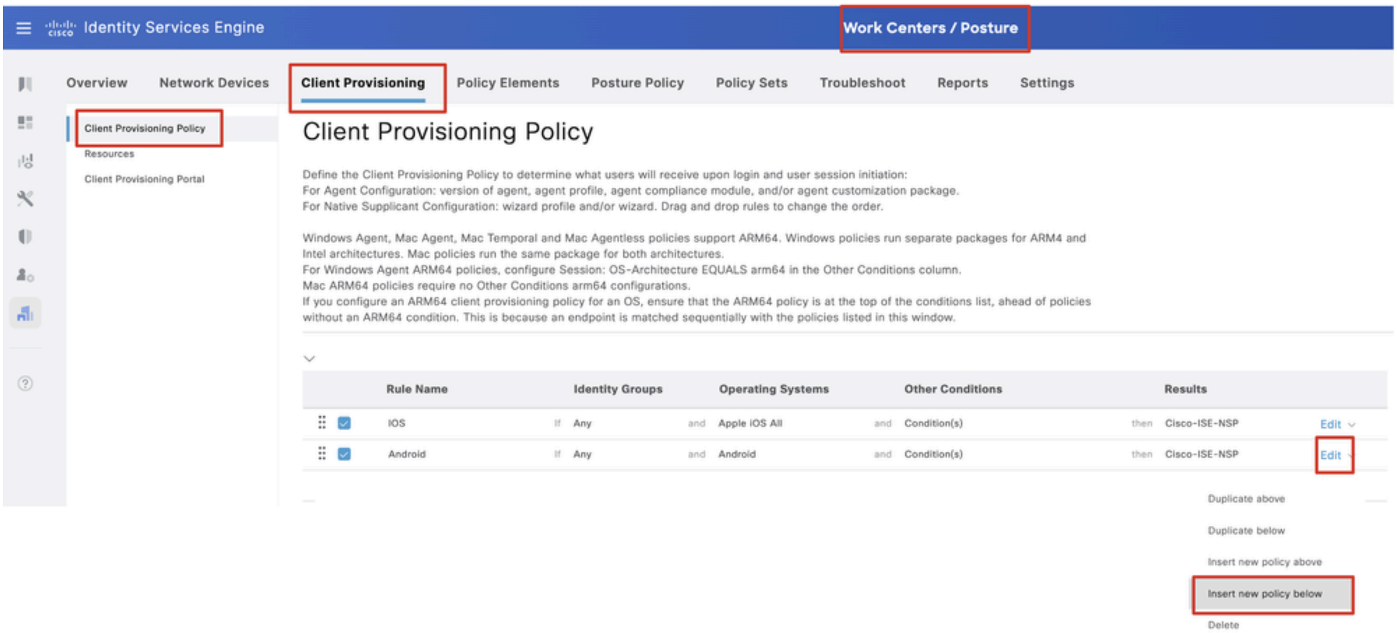
Diagnostic and Reporting Tool ☑

Profile Selection

* ISE Posture linux_agent_profile

ISE_Add_Agent_Configuration_1

Passaggio 18. Passare a Work Centers > Posture > Client Provisioning > Client Provisioning Policy. Fare clic Edit alla fine del nome di una regola. Selezionare 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

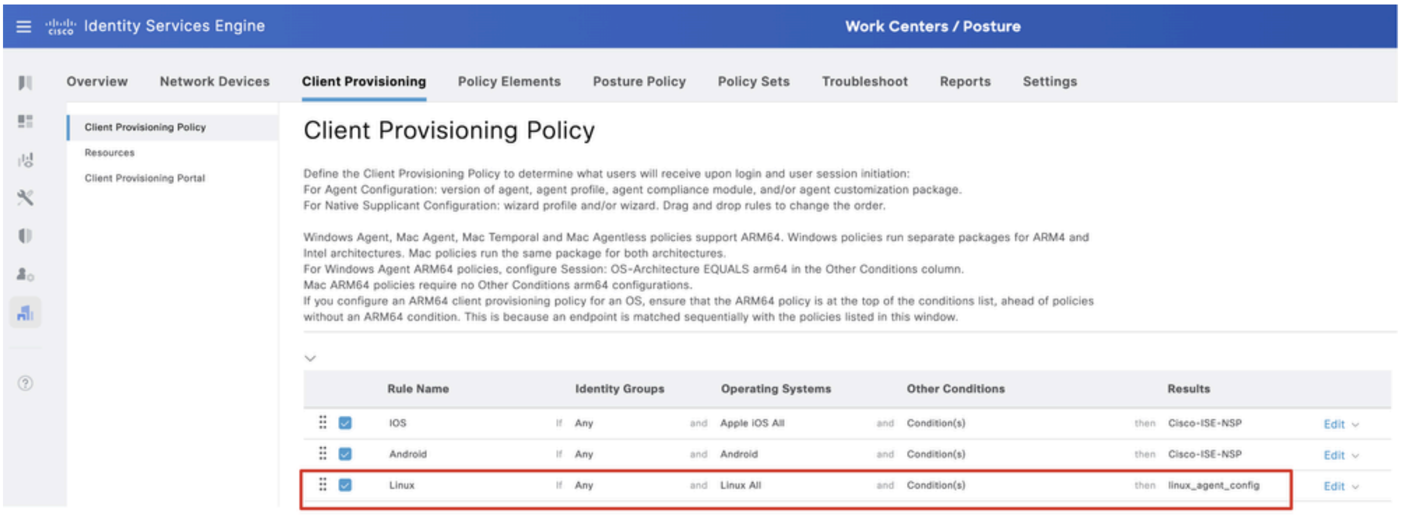
Passaggio 18.1. Configurare i dettagli:

Nome regola: Linux

Sistemi operativi: Linux All

Risultati: linux_agent_config

Fare clic su Done e su Save.



Client Provisioning Policy

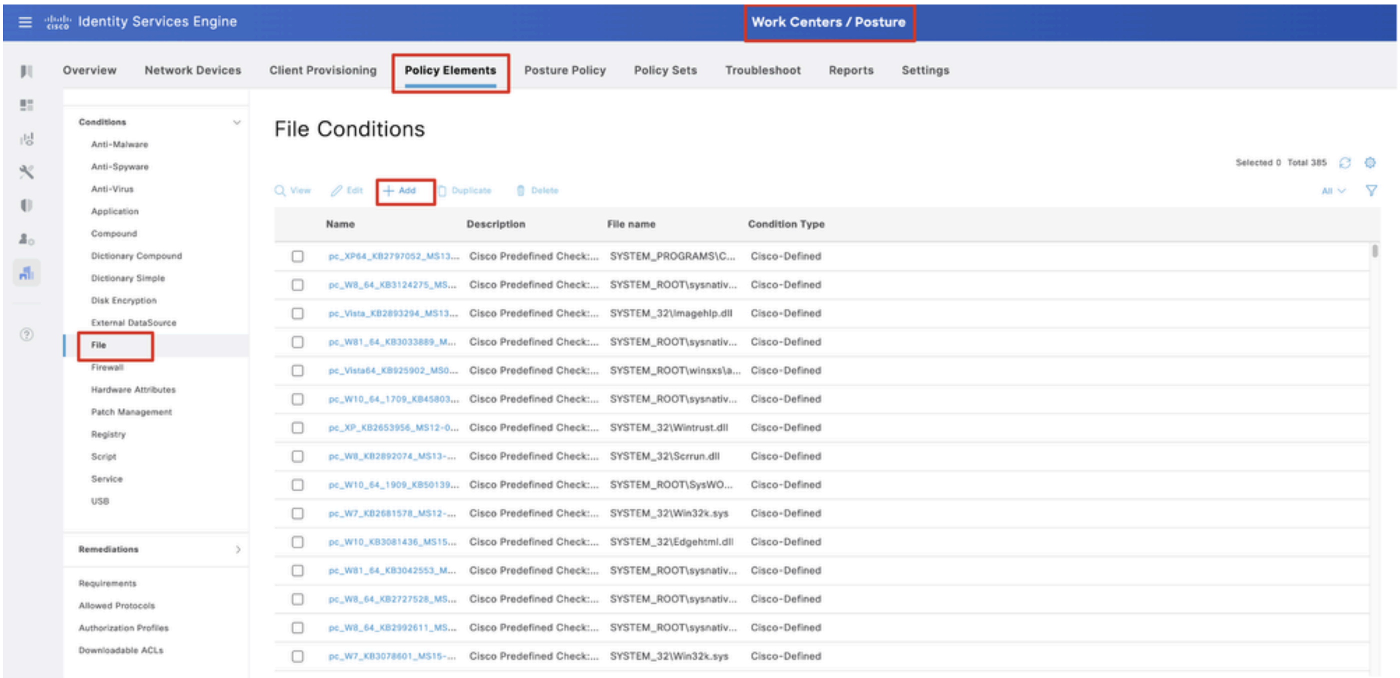
Define the Client Provisioning Policy to determine what users will receive upon login and user session initiation:
For Agent Configuration: version of agent, agent profile, agent compliance module, and/or agent customization package.
For Native Supplicant Configuration: wizard profile and/or wizard.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

Passaggio 19. Passare a Work Centers > Posture > Policy Elements > Conditions > File. Fare clic su .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

Passaggio 19.1. Configurare i dettagli:

Nome: linux_demo_file_exist

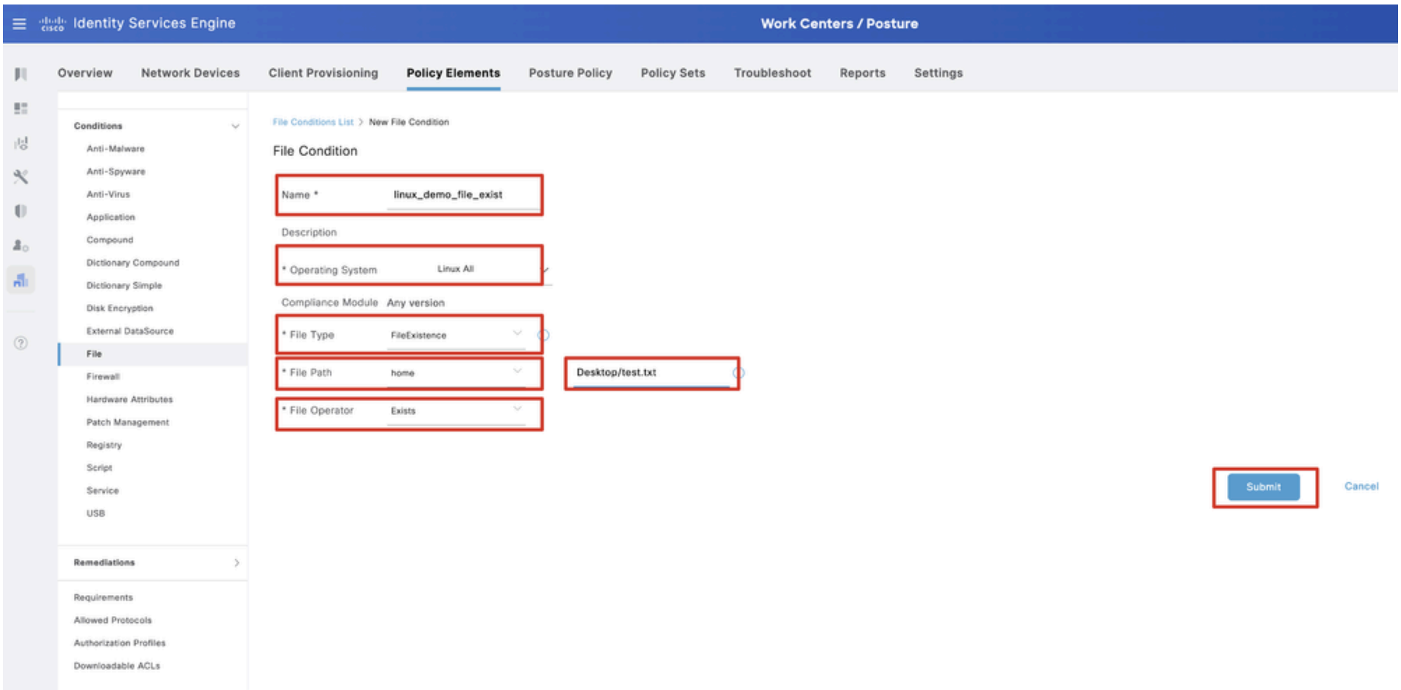
Sistemi operativi: Linux All

Tipo di file: FileExistence

Percorso file: home, Desktop/test.txt

Operatore file: esistente

Fare clic su .Submit



File Condition

Name * linux_demo_file_exist

Description

* Operating System Linux All

Compliance Module Any version

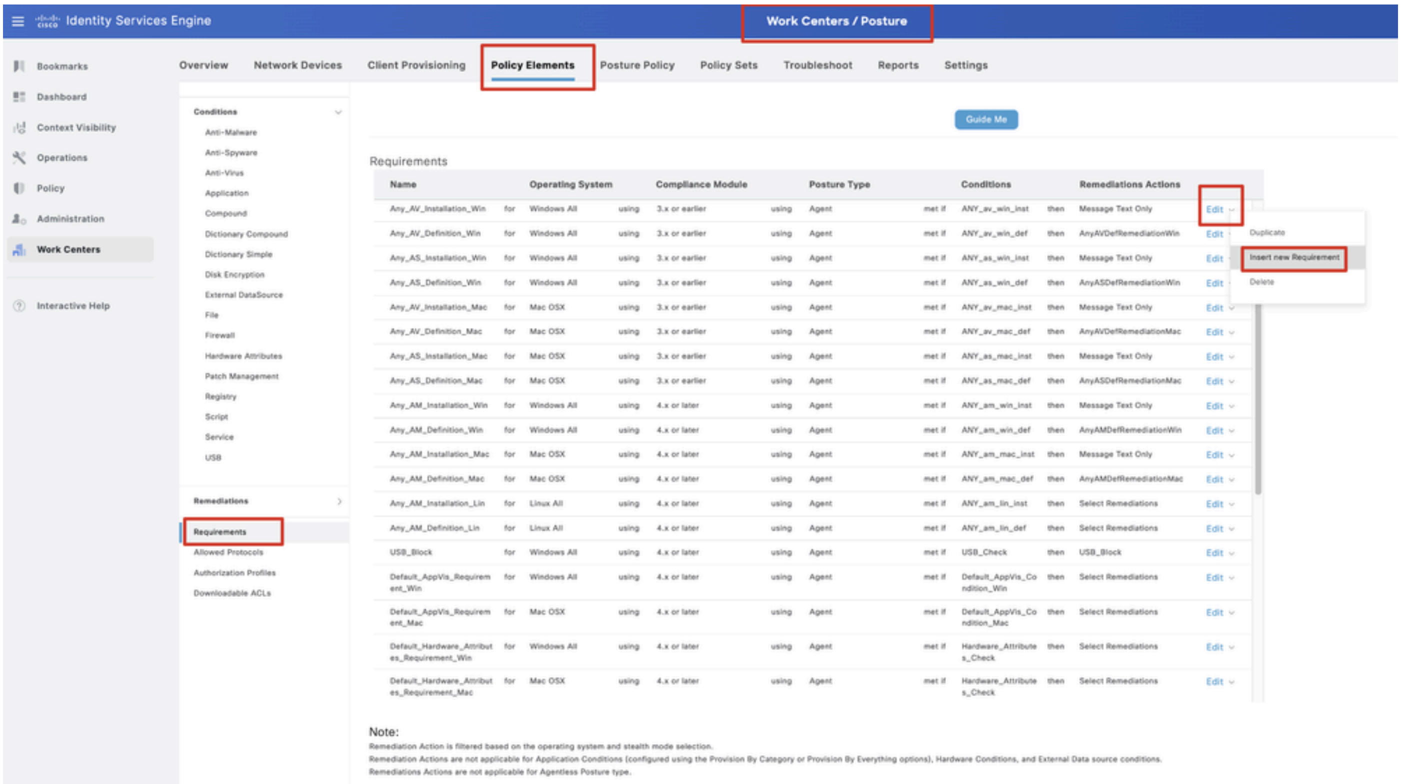
* File Type FileExistence

* File Path home Desktop/test.txt

* File Operator Exists

ISE_Add_New_File_Condition_1

Passaggio 20. Passare a Work Centers > Posture > Policy Elements > Requirements. Fare clic Edit alla fine del nome di una regola. Selezionare 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

Passaggio 20.1. Configurare i dettagli:

Nome: Test_exist_linux

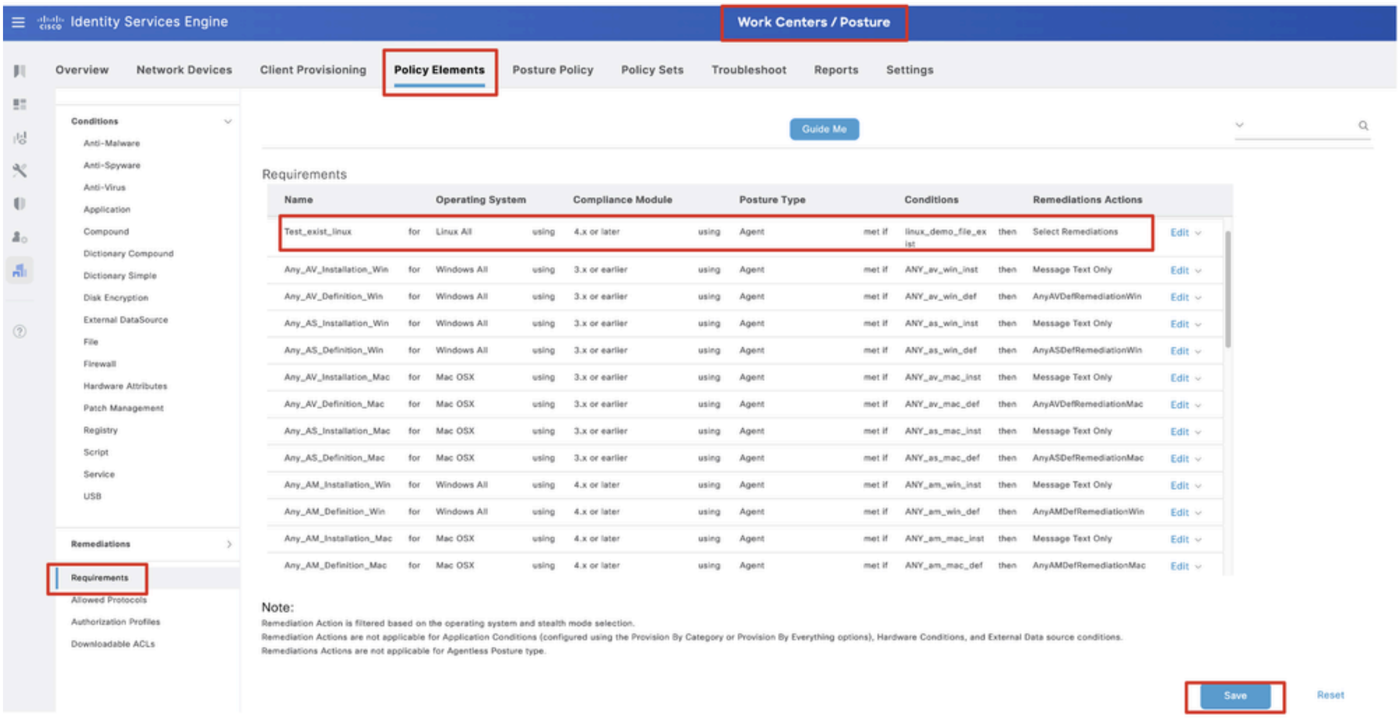
Sistemi operativi: Linux All

Modulo conformità: 4.x o versioni successive

Tipo di postura: agente

Condizioni: linux_demo_file_exist

Fare clic su Done e su Save.



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

Nota: al momento, solo gli script shell sono supportati per gli agenti Linux come correzione.

Passaggio 21. Passare a Work Centers > Posture > Policy Elements > Authorization Profiles. Fare clic su .Add

Passaggio 21.1. Configurare i dettagli:

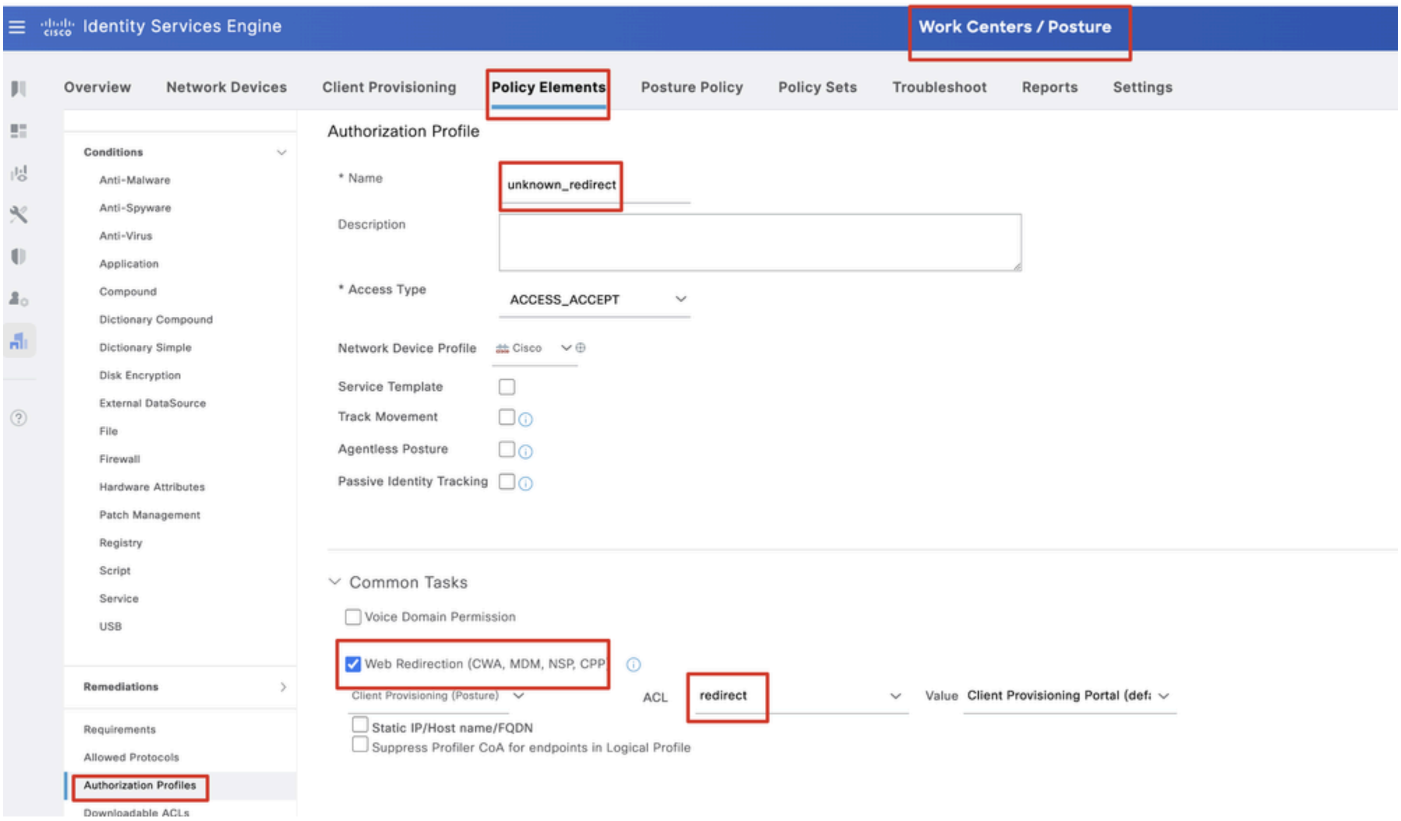
Nome: known_redirect

Selezionare la casella di controllo Web Redirection(CWA,MDM,NSP,CPP)

Seleziona Client Provisioning(Posture)

ACL: reindirizzamento

Valore: Portale di provisioning client (predefinito)



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 (def:

□ Static IP/Host name/FQDN

□ Suppress Profiler CoA for endpoints in Logical Profile

ISE_Add_New_Authorization_Profile_Redirect_1

Nota: questo reindirizzamento del nome ACL deve corrispondere al nome ACL corrispondente configurato su FTD.

Passaggio 21.2. Ripetere l'operazione Add per creare altri due profili di autorizzazione per gli endpoint non conformi e conformi con i dettagli.

Nome: non_compliant_profile

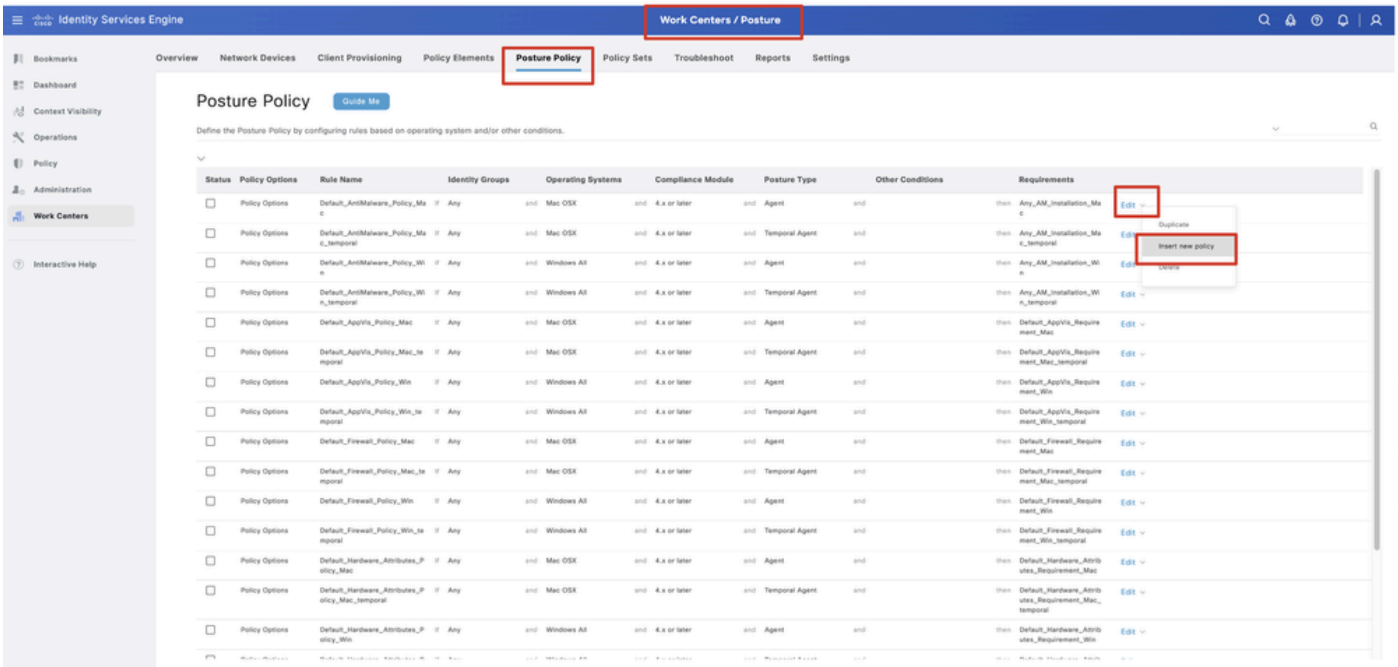
Nome DACL: DENY_ALL_IPv4_TRAFFIC

Nome: compliant_profile

Nome DACL: PERMIT_ALL_IPv4_TRAFFIC

Nota: il DACL per gli endpoint conformi o non conformi deve essere configurato in base ai requisiti effettivi.

Passaggio 22. Passare a Work Centers > Posture > Posture Policy. Fare clic Edit alla fine di qualsiasi regola. Selezionare 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

Passaggio 22.1. Configurare i dettagli:

Nome regola: Demo_test_exist_linux

Gruppi di identità: qualsiasi

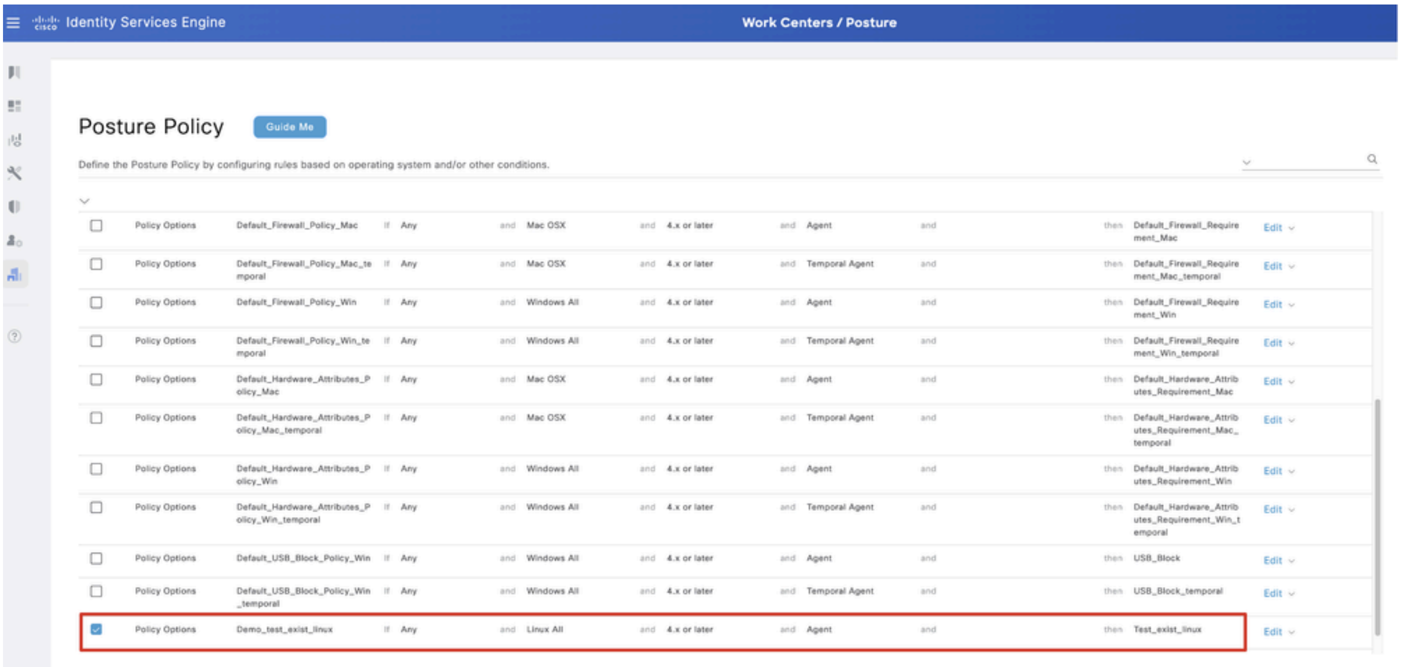
Sistemi operativi: Linux All

Modulo conformità: 4.x o versioni successive

Tipo di postura: agente

Requisiti: Test_exist_linux

Fare clic su Done e su Save.



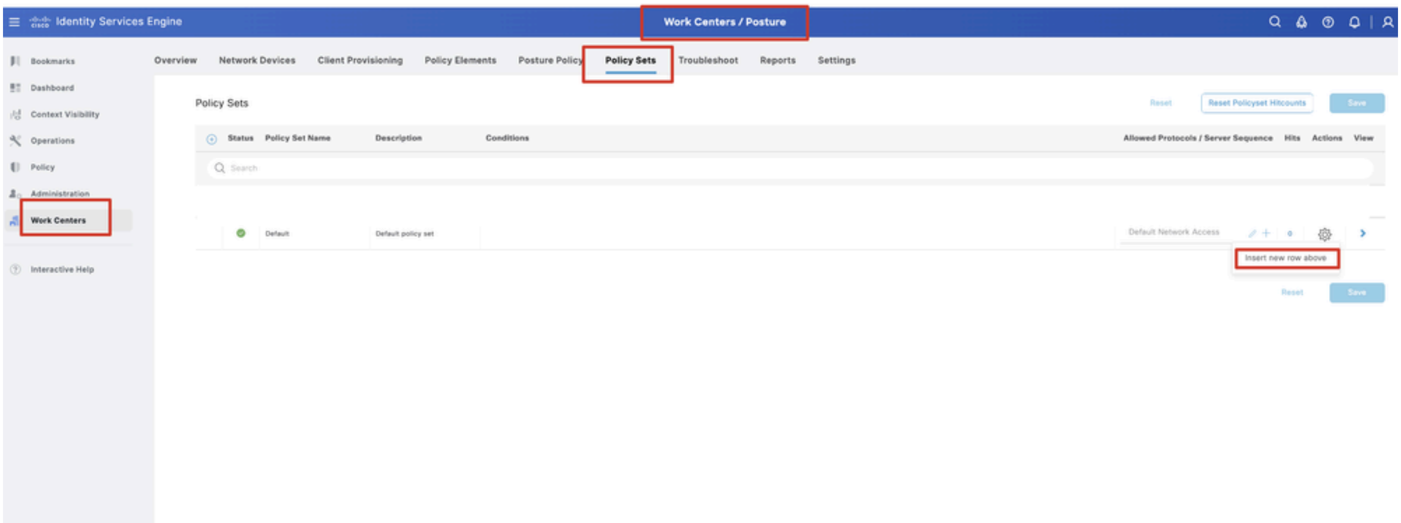
Posture Policy

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

Passaggio 23. Passare a Work Centers > Posture > Policy Sets. Fare clic per Insert new row above.



Policy Sets

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

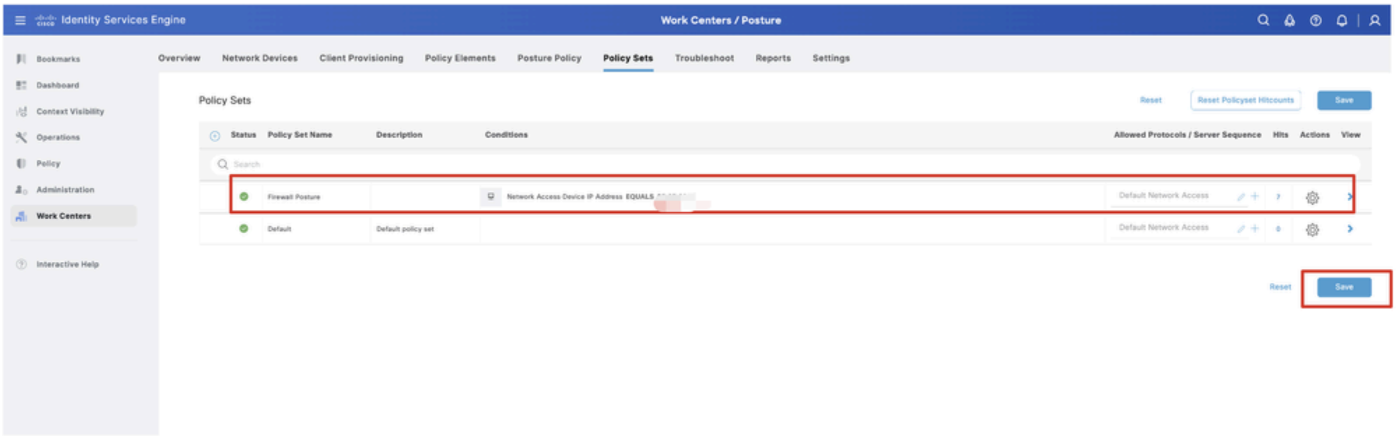
ISE_Add_New_Policy_Set

Passaggio 23.1. Configurare i dettagli:

Nome set di criteri: postura firewall

Condizioni: Indirizzo IP del dispositivo di accesso alla rete EQUALs [Indirizzo IP FTD]

Fare clic su . 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	⚙	>

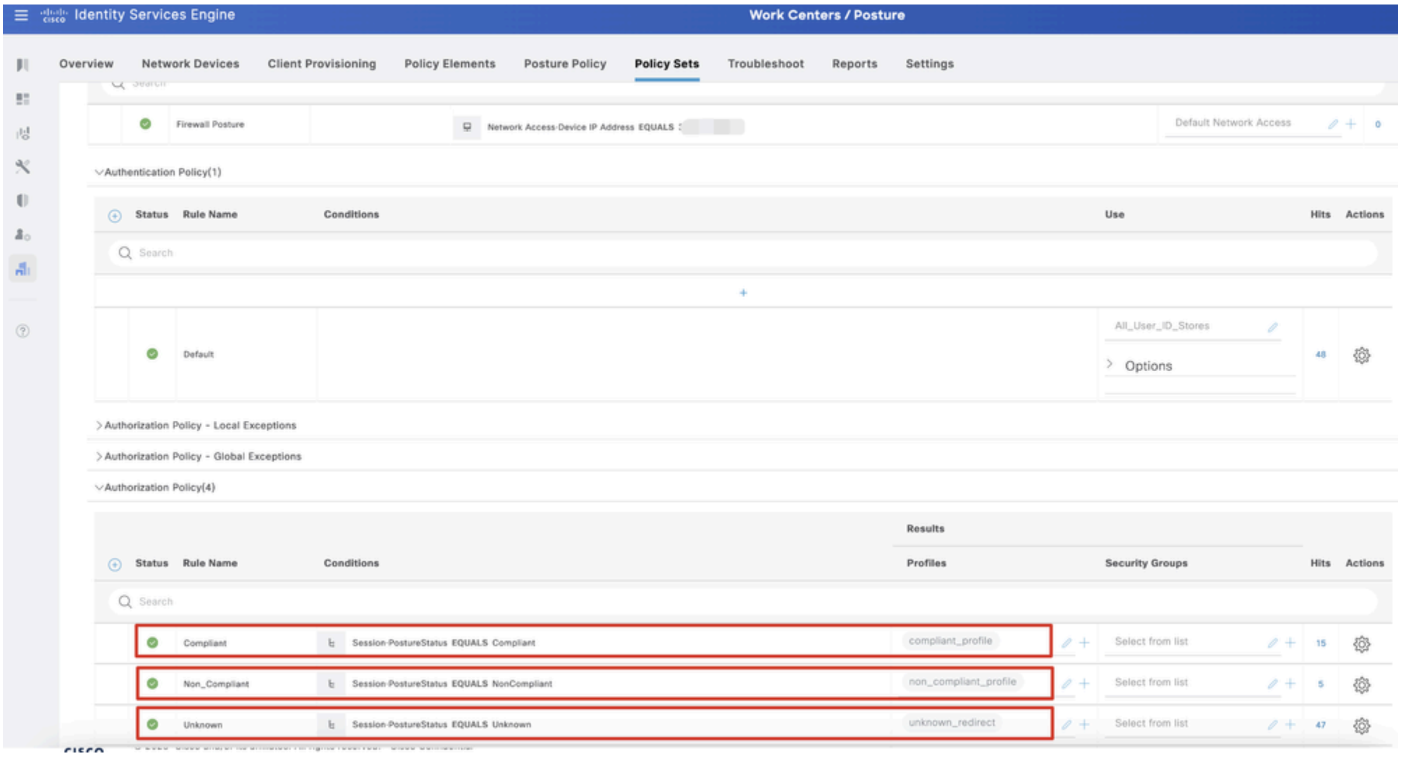
ISE_Add_New_Policy_Set_1

Passaggio 23.2. Fare clic> per immettere il set di criteri. Creare nuove regole di autorizzazione per lo stato conforme alla postura, non conforme e sconosciuto. Fare clic su .Save

Conforme con compliant_profile

Non conforme con non_compliant_profile

Sconosciuto con known_redirect



Status	Policy Set Name	Conditions	Allowed Protocols / Server Sequence	Hits
●	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

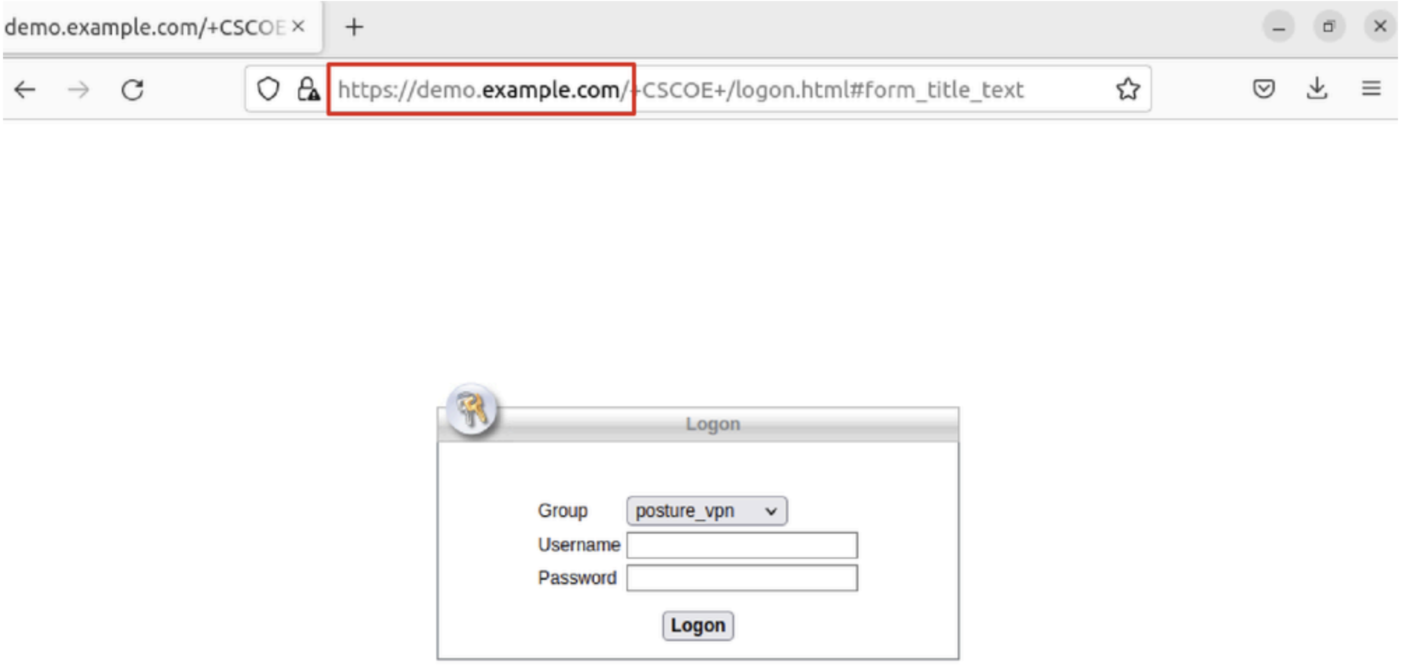
Authorization Policy(4)

			Results			
Status	Rule Name	Conditions	Profiles	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

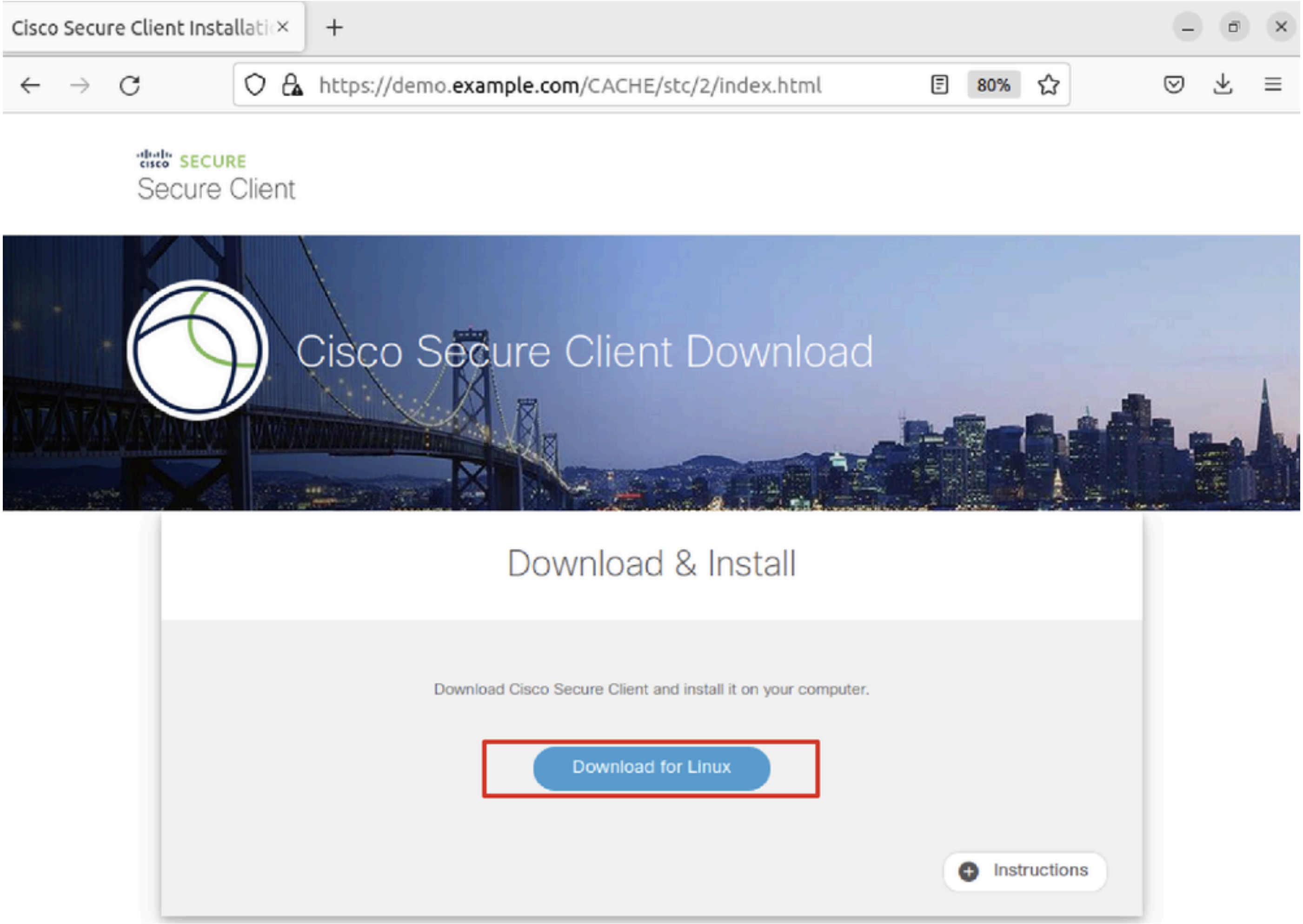
Configurazioni su Ubuntu

Passaggio 24. Accedere al client Ubuntu tramite la GUI. Aprire il browser per accedere al portale VPN. Nell'esempio, questo valore è demo.example.com.



Accesso Ubuntu_Browser_VPN

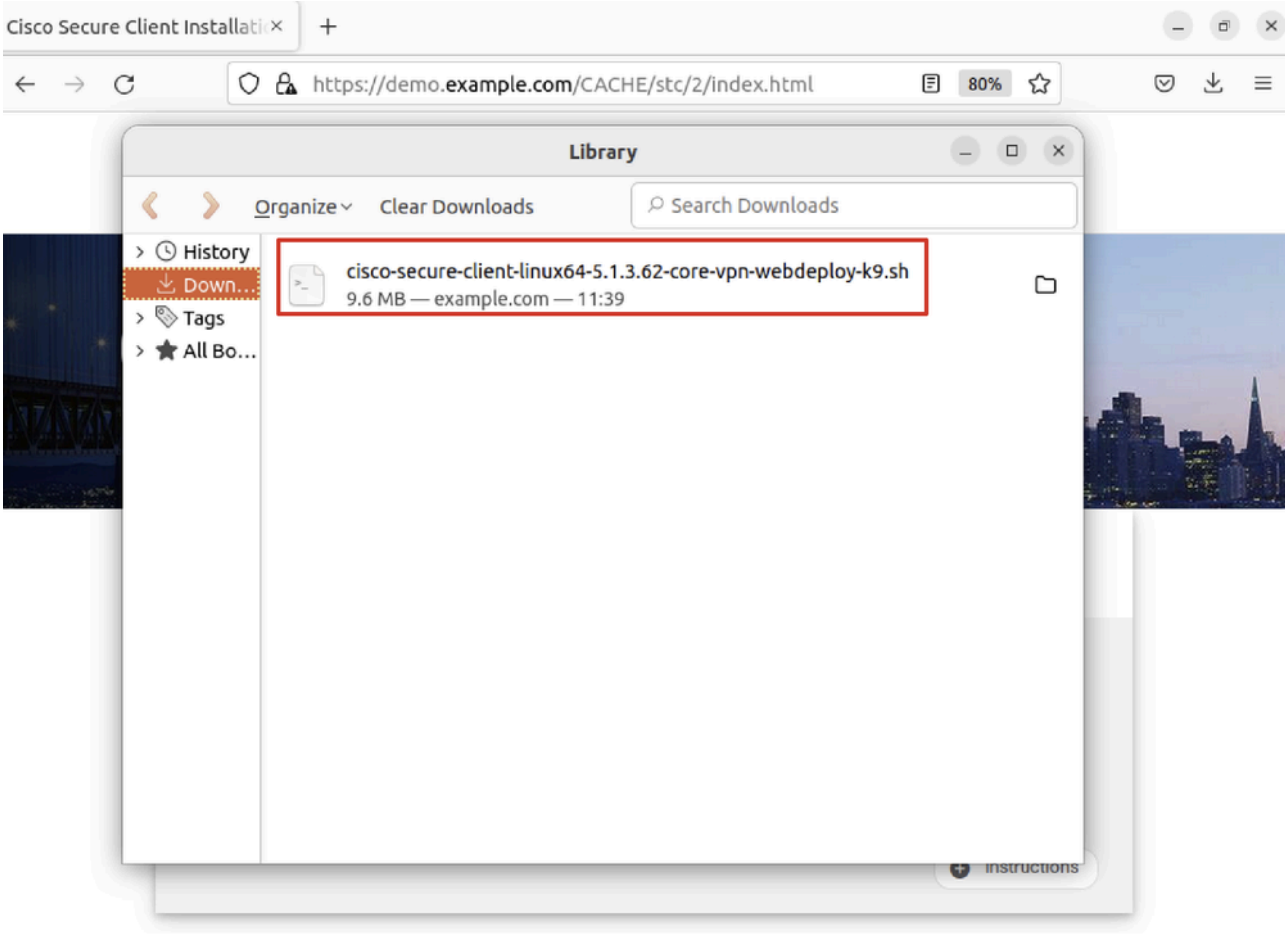
Passaggio 25. Fare clic su .Download for Linux


Cisco Secure Client Installati
https://demo.example.com/CACHE/stc/2/index.html
80%
SECURE
Secure Client
Cisco Secure Client Download
Download & Install
Download for Linux
Instructions

Download Cisco Secure Client and install it on your computer.

Ubuntu_Browser_VPN_Download_1

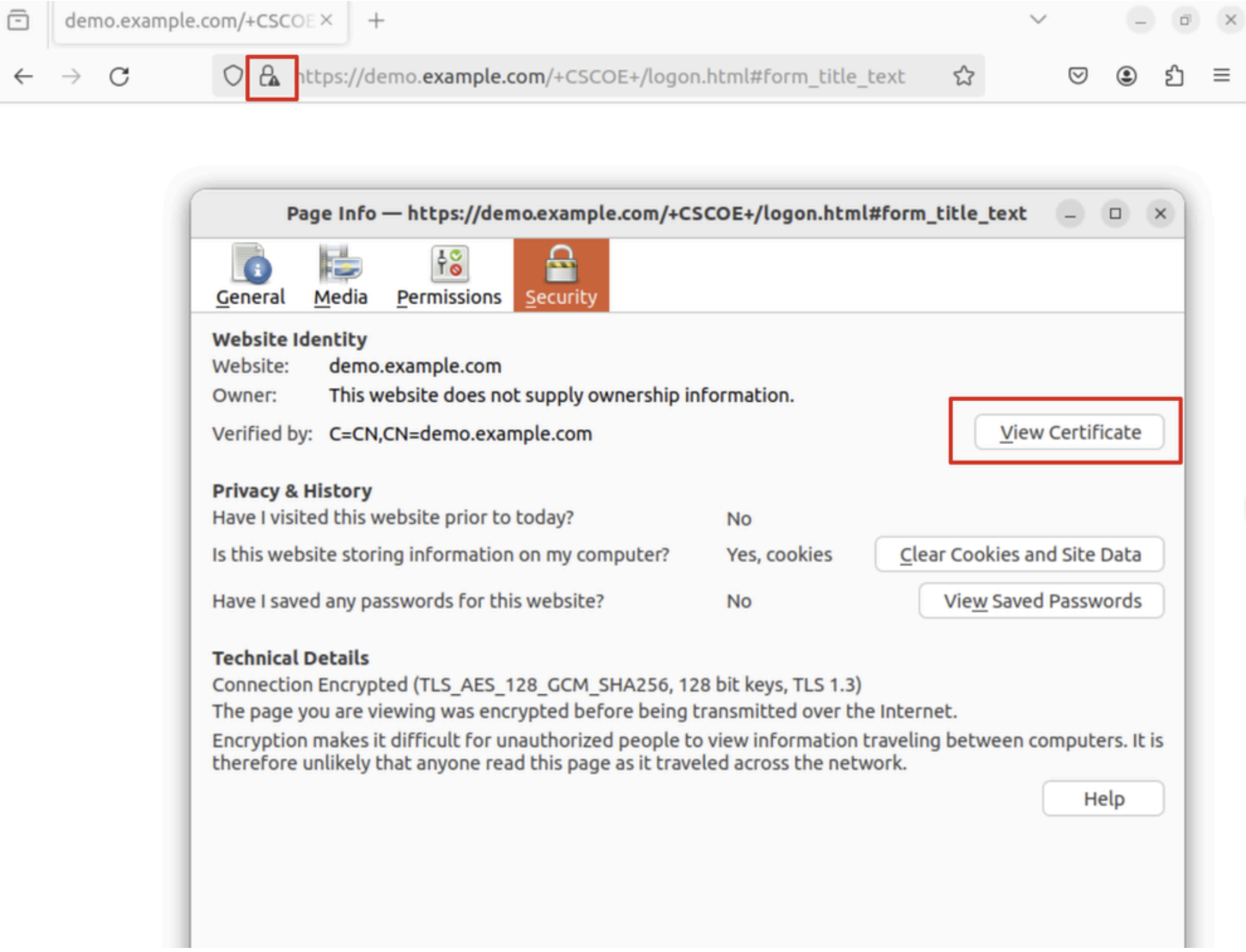
Il nome del file scaricato è cisco-secure-client-linux64-5.1.3.62-core-vpn-webdeploy-k9.sh.



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

Passaggio 26. Scaricare il certificato VPN tramite il browser e rinominare il file in <certificato>.crt. Questo è l'esempio di come utilizzare firefox per scaricare il certificato.



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

Passaggio 27. Aprire il terminale sul client Ubuntu. Passarepath home/user/Downloads/ a per installare 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$
```

Passaggio 28. Considera attendibile il certificato del portale VPN nel client Ubuntu.

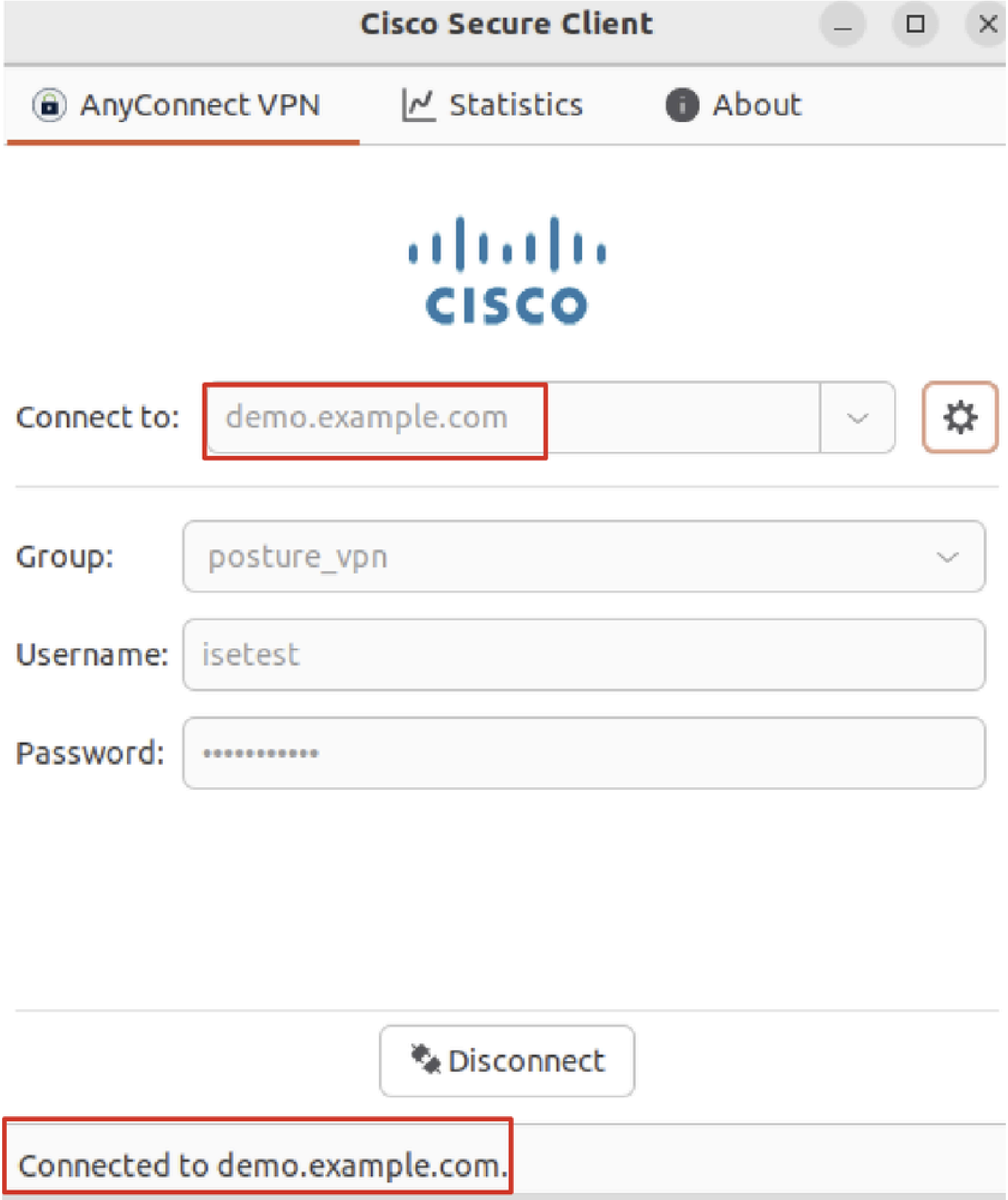
<#root>

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
```

Passaggio 29. Aprire Cisco Secure Client sul client Ubuntu e connettere la VPN a demo.example.com.



Cisco Secure Client

Connect to: demo.example.com

Group: posture_vpn

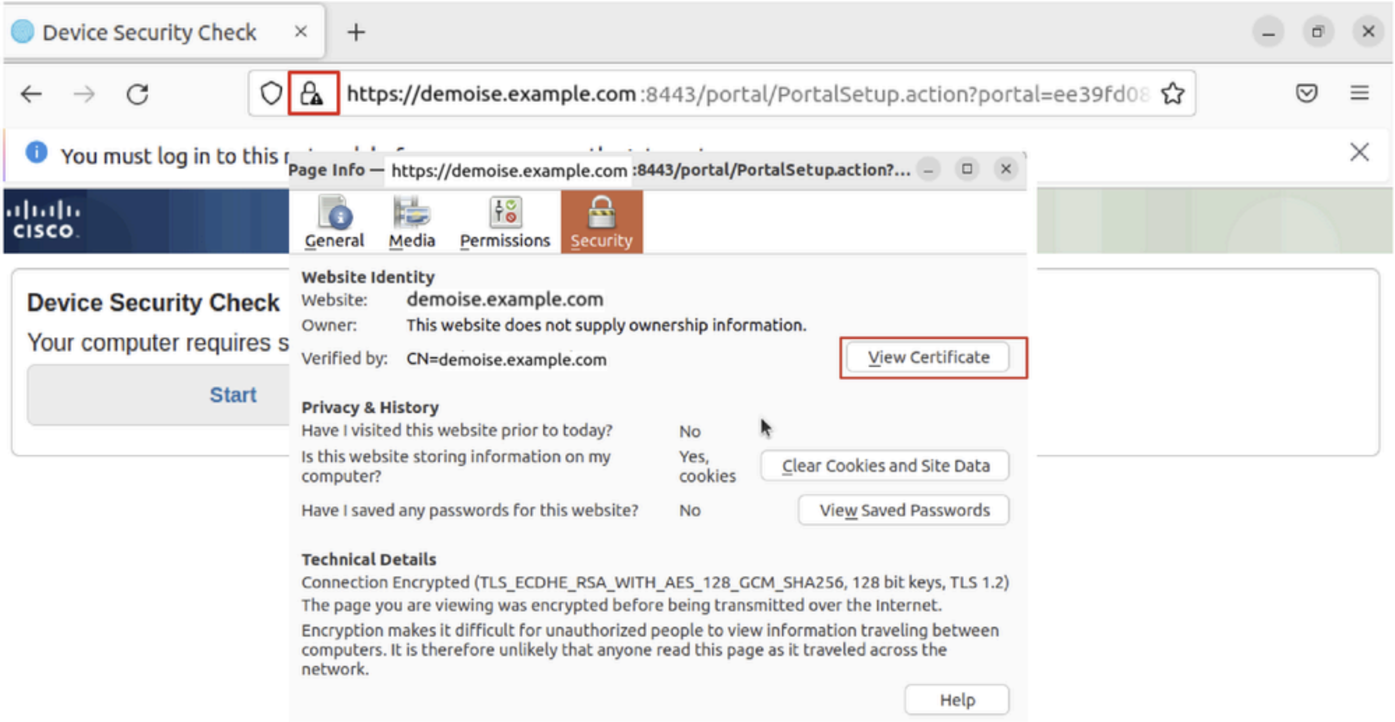
Username: isetest

Password: ••••••••••••

Connected to demo.example.com.

Ubuntu_Secure_Client_Connected

Passaggio 30. Aprire il browser per accedere a tutti i siti Web da cui viene attivato il reindirizzamento al portale CCP ISE. Scaricare il certificato dal portale ISE CPP e rinominare il file in <certificato>.crt. Questo è un esempio di come usare Firefox per scaricare.


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

Website Identity

Website: demoise.example.com

Owner: This website does not supply ownership information.

Verified by: CN=demoise.example.com

View Certificate

Privacy & History

Have I visited this website prior to today? No

Is this website storing information on my computer? Yes, cookies — Clear Cookies and Site Data

Have I saved any passwords for this website? No — 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.

Help

Ubuntu_Browser_CPP_Cert_Download

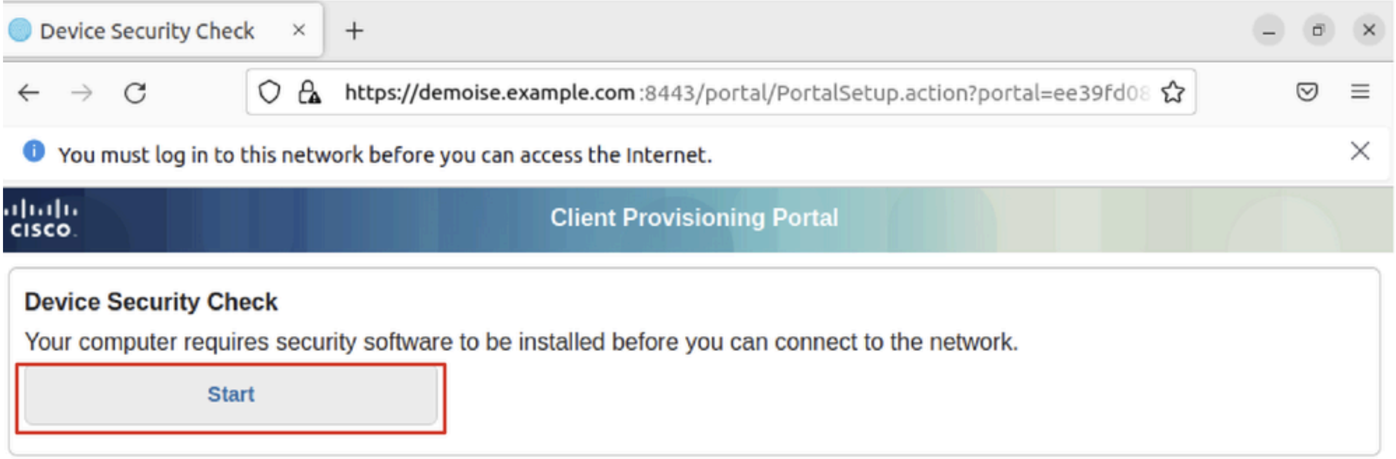
Passaggio 30.1. Considerare attendibile il certificato del portale CPP ISE sul client Ubuntu.

<#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.
```

Passaggio 31. Fare clic su Start sul portale ISE CPP.



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.

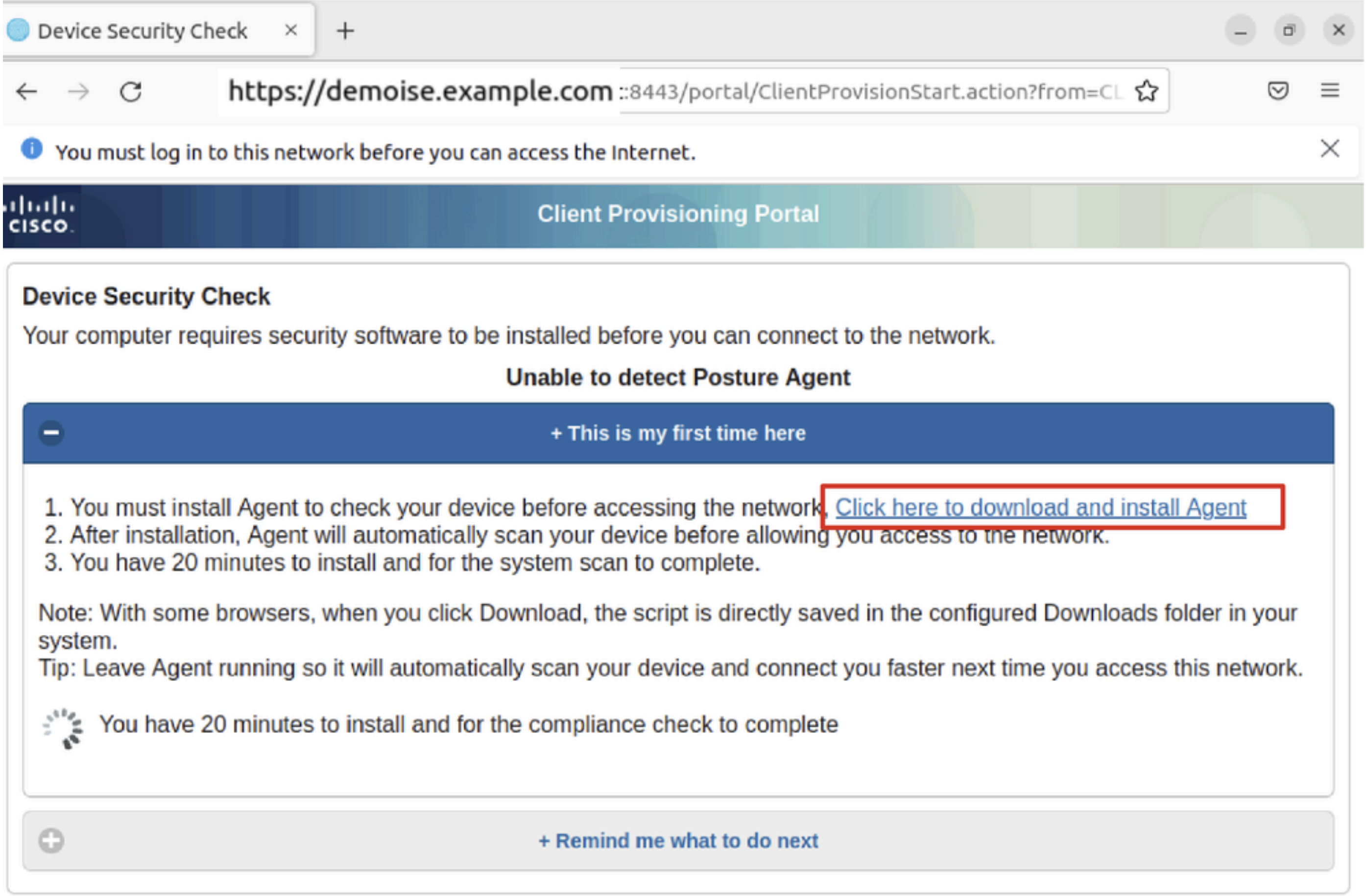
Client Provisioning Portal

Device Security Check

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

Ubuntu_Browser_CPP_Start

Passaggio 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_Posture

Passaggio 33. Aprire il terminale sul client Ubuntu. Passare al percorso home/user/Downloads/ per installare il modulo di postura.

<#root>

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

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

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

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

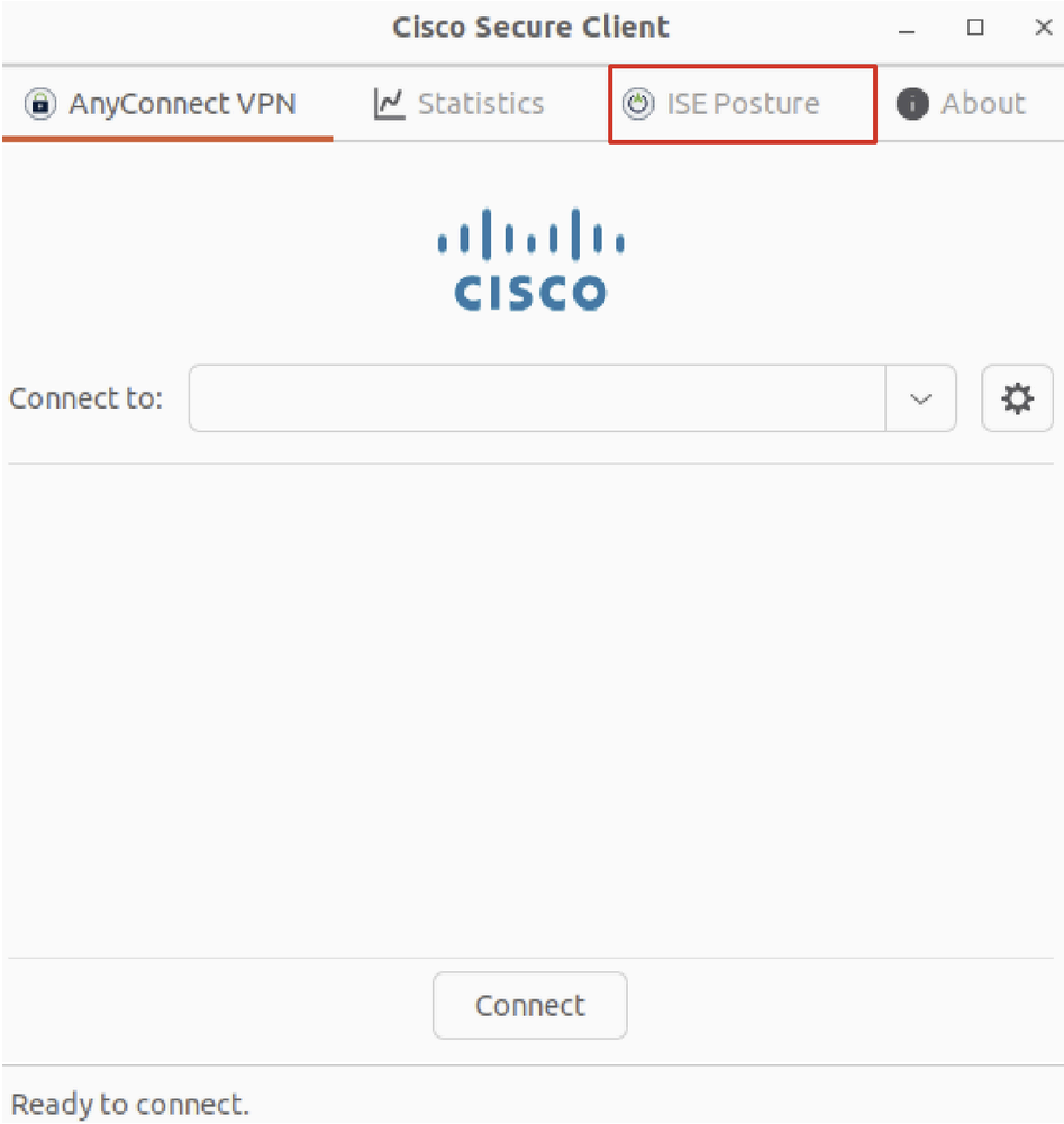
```
chmod +x cisco-secure-client-ise-network-assistant-linux64-5.1.3.62_demoise.example.com_8443_0NcLgcMURfy
```

```
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.
```

Passaggio 34. Nell'interfaccia utente del client Ubuntu, uscire da Cisco Secure Client e riaprirlo. Il modulo ISE Posture è stato installato ed eseguito correttamente.



Ubuntu_Secure_Client_ISE_Posture_Installed

Passaggio 35. Aprire il terminale sul client Ubuntu. Passare a pathhome/user/Desktop , creare un test.txt file che soddisfi la condizione configurata in ISE.

<#root>

user@ubuntu22-desktop:~$

```
cd Desktop/
```

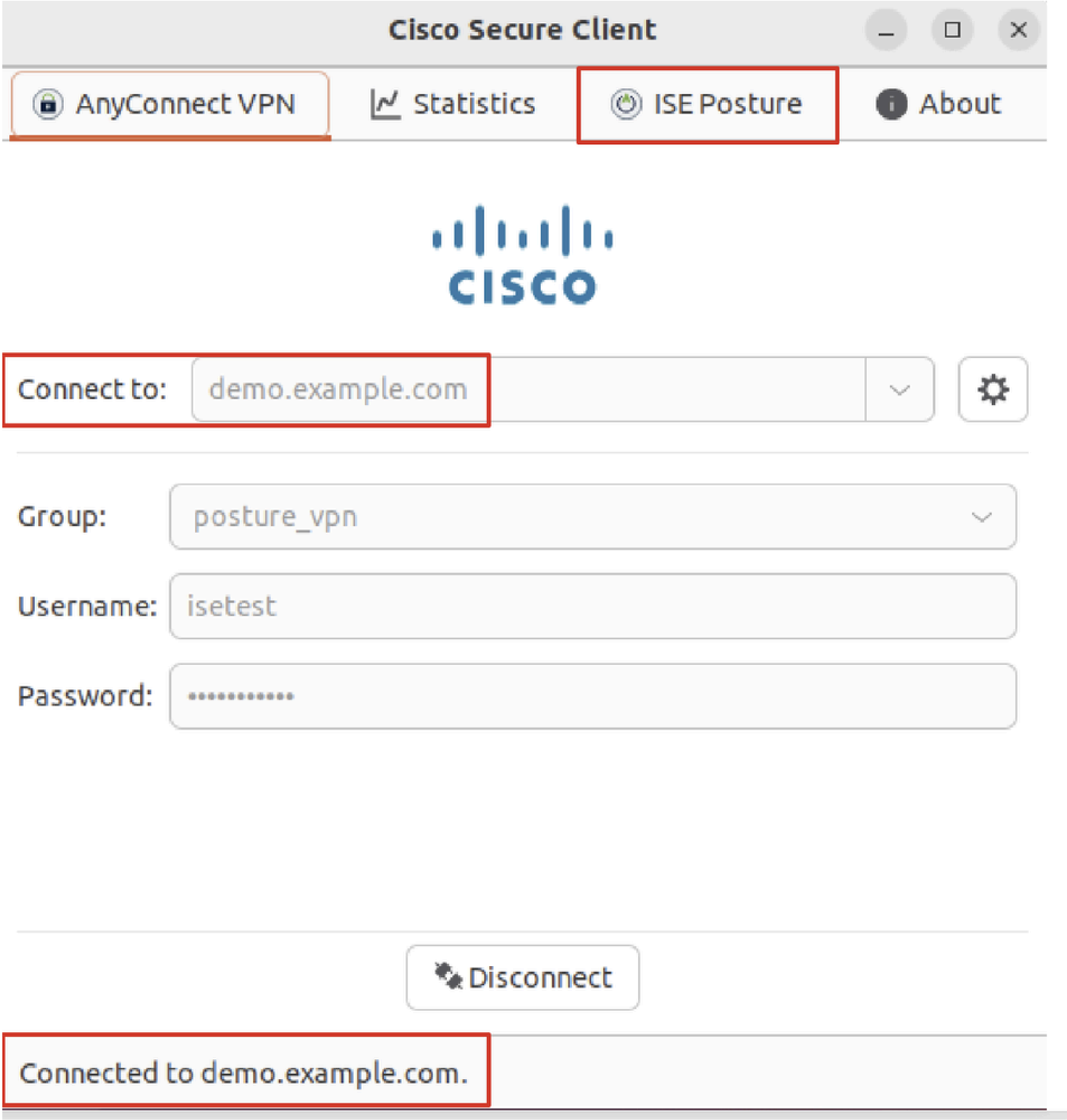
```
user@ubuntu22-desktop:~/Desktop$
```

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

Verifica

Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.

Passaggio 1. Connettere la VPN a demo.example.com sul client Ubuntu.



Connect to: demo.example.com

Group: posture_vpn

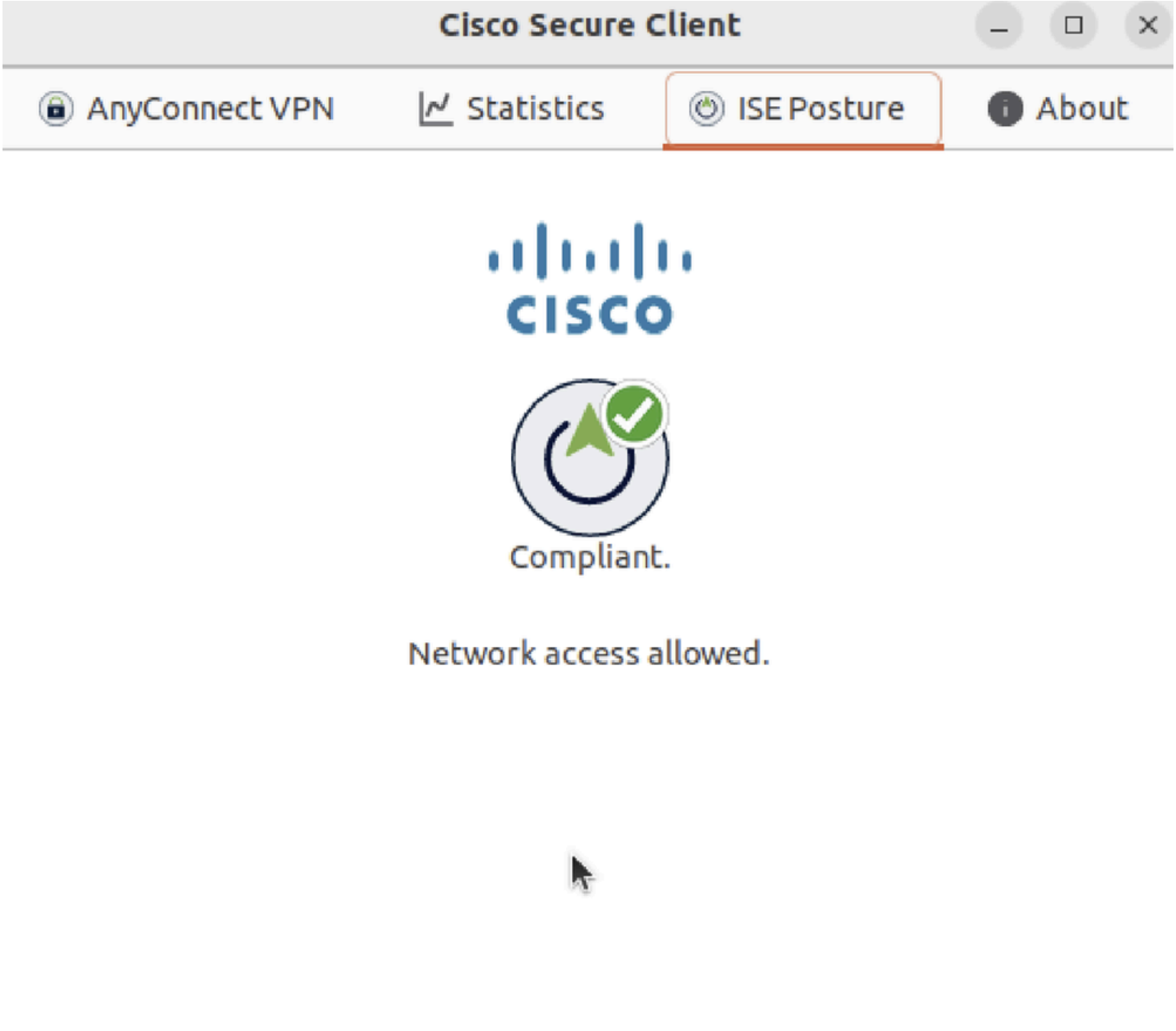
Username: isetest

Password: ••••••••••••

Connected to demo.example.com.

Verify_Ubuntu_Secure_Client_Connected

Passaggio 2. Controllare lo stato di ISE Posture sul client Ubuntu.

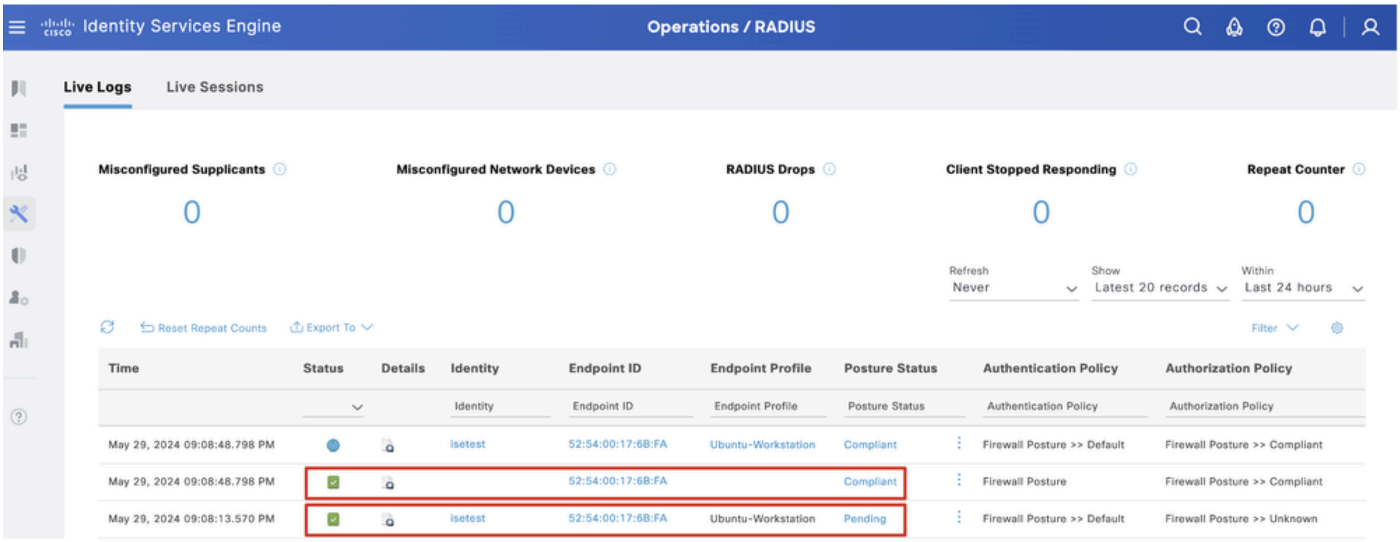


Compliant.

Network access allowed.

Verify_Ubuntu_Secure_Client_Compliant

Passaggio 3. Controllare Radius Live Log su ISE. Passare a 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

Verifica_ISE_LiveLog

Passaggio 4. Passare alla CLI FTD tramite SSH o 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 : cb00718200021000665 9d871
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
```

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Per il flusso della postura e la risoluzione dei problemi di Cisco Secure Client e ISE, consultare i **documenti** CCO **Confronto tra stili di postura ISE per versioni precedenti e successive alla 2.2** e **Risoluzione dei problemi di gestione e postura delle sessioni ISE.**

Informazioni correlate

- Compatibilità dei componenti di rete Cisco Identity Services Engine, versione 3.3

- Guida dell'amministratore di Cisco Identity Services Engine, versione 3.3
- **Supporto tecnico Cisco e download**