ISE 3.3에서 Linux VPN Posture 구성

목차

소개

이 문서에서는 ISE(Identity Services Engine) 및 FTD(Firepower Threat Defense)를 사용하여 Linux VPN Posture를 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco 보안 클라이언트
- FTD(Firepower 위협 방어)의 원격 액세스 VPN
- Identity Services Engine(ISE)

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 버전을 기반으로 합니다.

- Ubuntu 22.04
- Cisco Secure Client 5.1.3.62

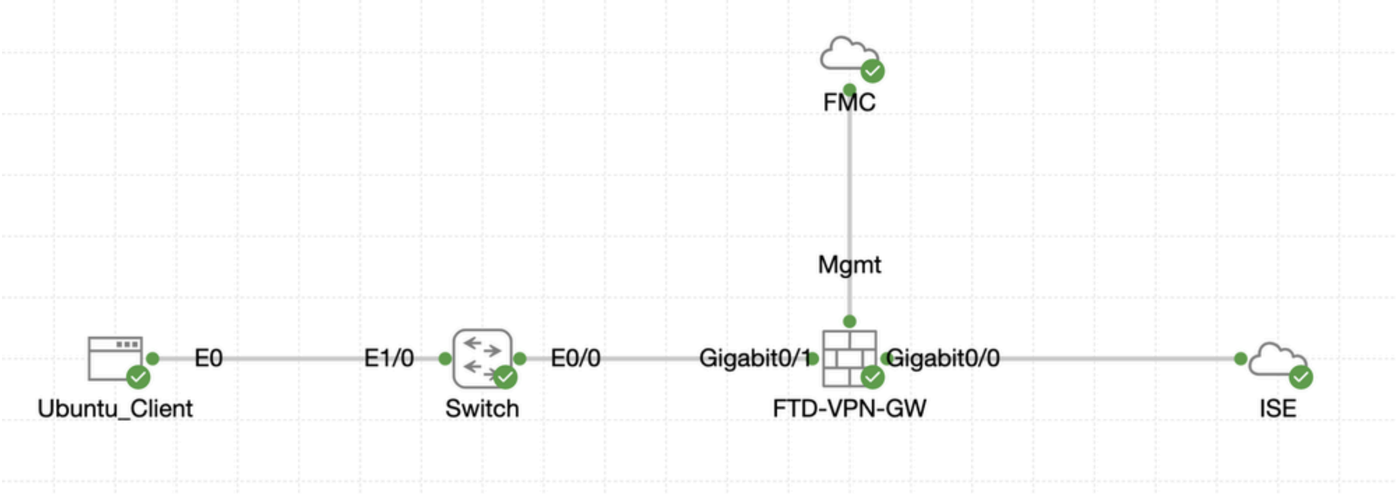
- Cisco FTD(Firepower Threat Defense) 7.4.1
- Cisco FMC(Firepower Management Center) 7.4.1
- Cisco ISE(Identity Services Engine) 3.3

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바

이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

구성

네트워크 다이어그램



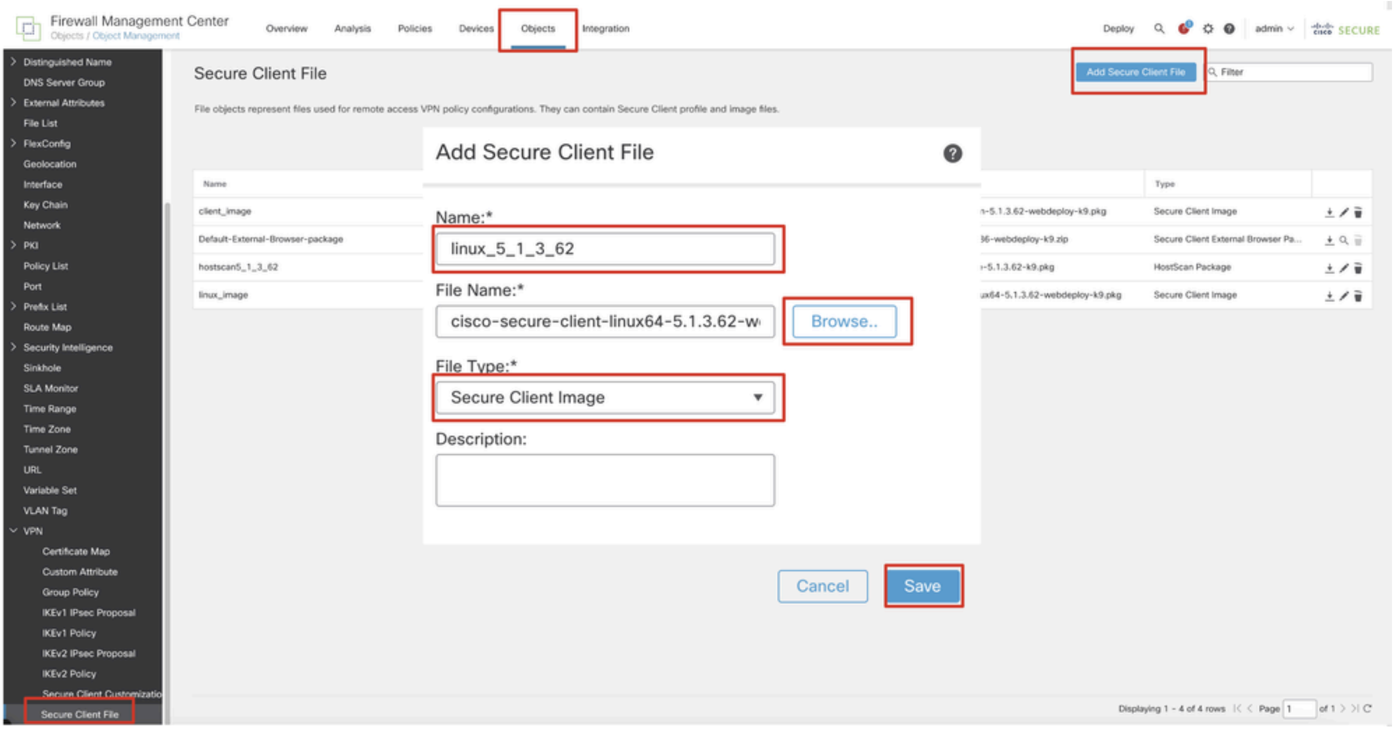
토폴로지

FMC/FTD의 컨피그레이션

1단계. 클라이언트, FTD, FMC 및 ISE 간의 연결이 성공적으로 구성되었습니다. enroll.cisco.com는 리디렉션을 위해 프로브를 수행하는 엔드포인트에 사용됩니다(자세한 내용은 포스처 플로우 CCO 문서ISE Posture Style Comparison for Pre and Post 2.2 참조). FTD에서 enroll.cisco.com으로 이동하는 트래픽에 대한 경로가 올바르게 구성되었는지 확인합니다.

2단계. Cisco Software Downloadcisco-secure-client-linux64-5.1.3.62-webdeploy-k9.pkg에서 패키지 이름을 다운로드하고 다운로드한 파일의 md5 체크섬이 Cisco Software Download 페이지와 동일한지 확인하여 다운로드 후 파일이 정상인지 확인합니다.

3단계. 로 Objects > Object Management > VPN > Secure Client File 이동합니다. 클릭Add Secure Client File, 이름 입력, 선택File Name, cisco-secure-client-linux64-5.1.3.62-webdeploy-k9.pkg드롭다운 목록에서 선택Secure Client Image File Type. 그런 다음 을 클릭합니다 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	…-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

Browse..

File Type:* Secure Client Image

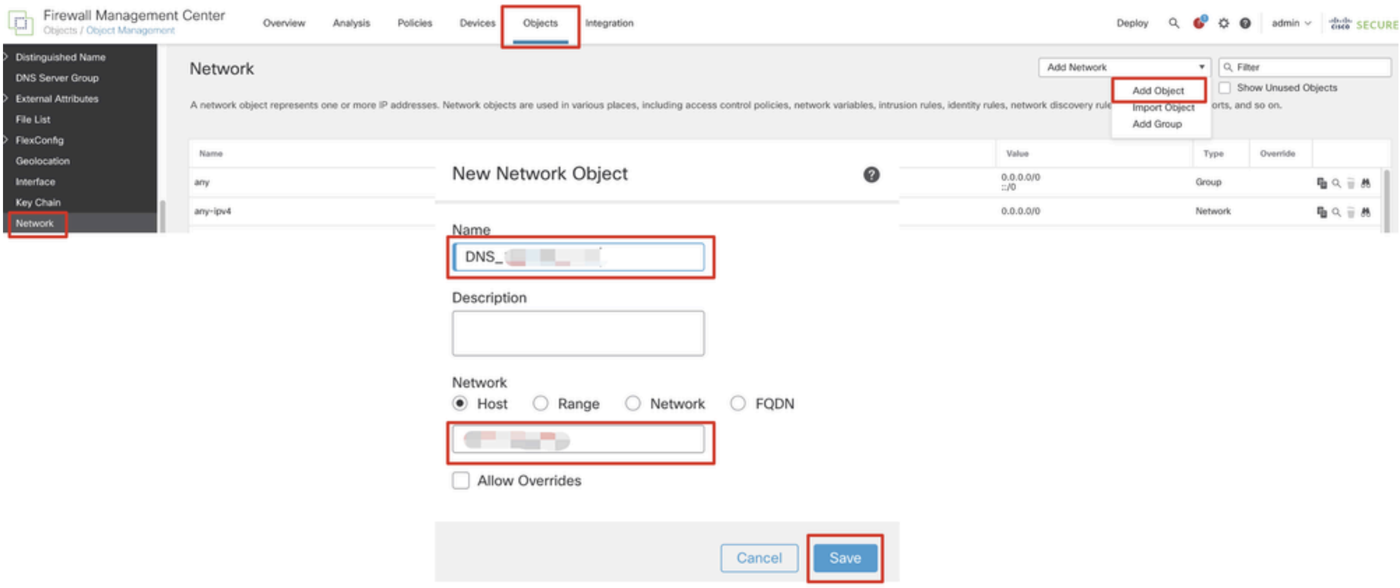
Description:

Cancel Save

FMC_Upload_Secure_Client_Image

4단계. 로 Objects > Object Management > Network 이동합니다.

4.1단계. DNS 서버용 개체를 만듭니다. 을 Add Object 클릭하고 이름과 사용 가능한 DNS IP 주소를 입력합니다. 를 Save 클릭합니다.



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]

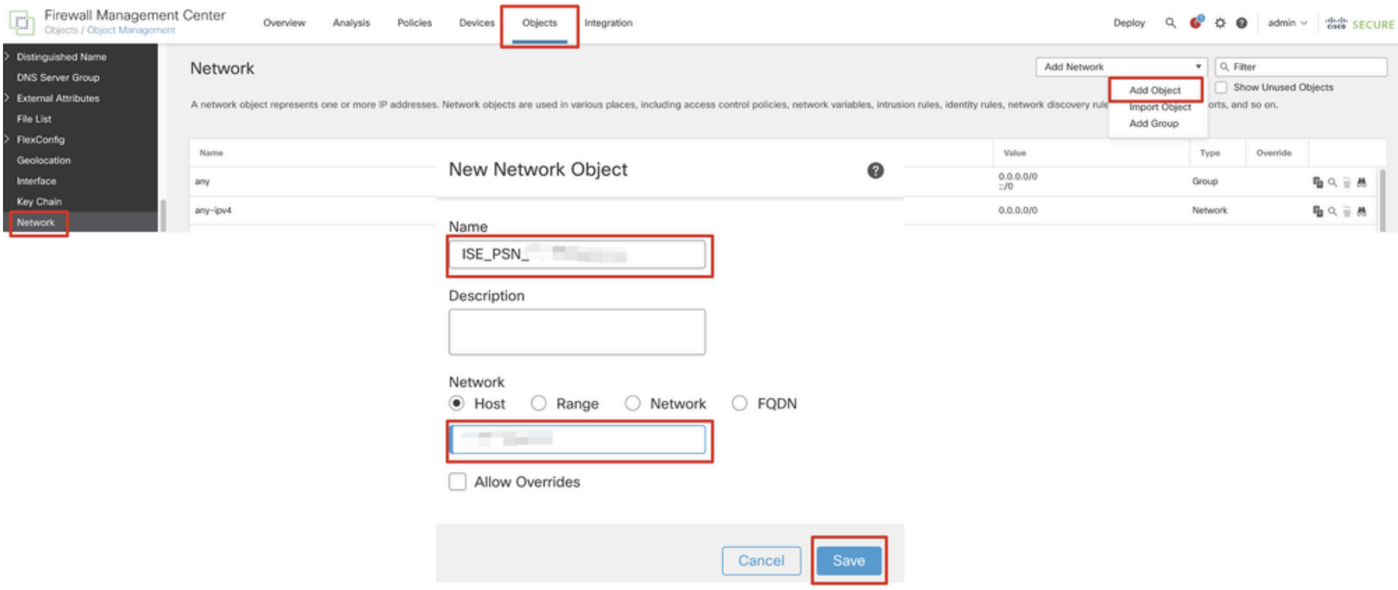
□ Allow Overrides

Cancel Save

FMC_Add_Object_DNS

참고: 여기에 구성된 DNS 서버는 VPN 사용자를 위해 사용됩니다.

4.2단계. ISE PSN에 대한 개체를 만듭니다. 을 Add Object 클릭하고 이름 및 사용 가능한 ISE PSN IP 주소를 입력합니다. 를 Save 클릭합니다.



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:

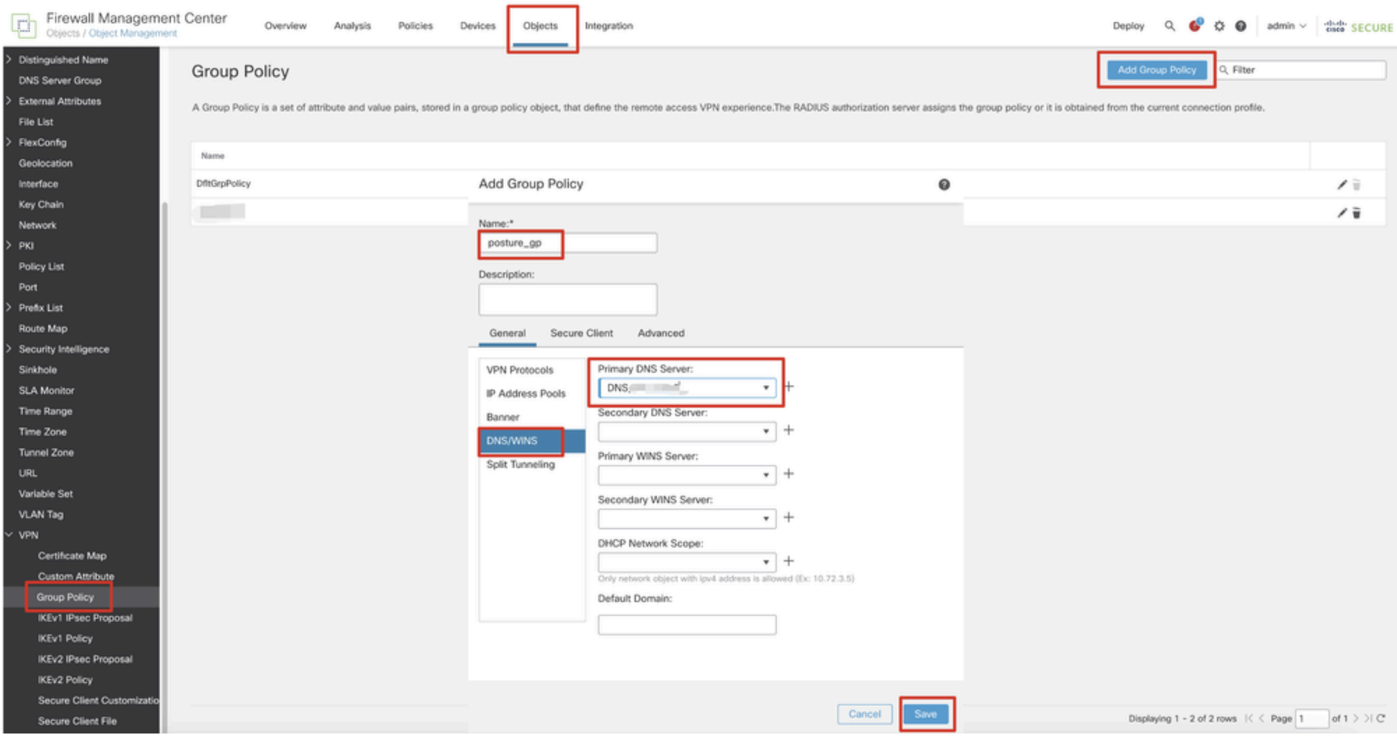
Network: ● Host ○ Range ○ Network ○ FQDN

[redacted]

□ Allow Overrides

FMC_Add_Object_ISE

5단계. 로 Objects > Object Management > VPN > Group Policy 이동합니다. 를 Add Group Policy 클릭합니다. 를 DNS/WINS 클릭하고 의 DNS 서버 개체를 선택합니다Primary DNS Server. 그런 다음 을 클릭합니다Save.



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:

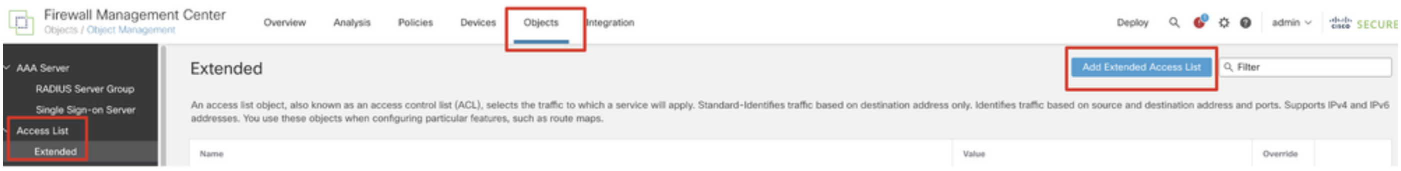
Only network object with ipv4 address is allowed (Ex: 10.72.3.5)

Default Domain:

FMC_Add_Group_Policy

참고: VPN 그룹 정책에 사용된 DNS 서버가 ISE 클라이언트 프로비저닝 포털 FQDN 및 enroll.cisco.com을 확인할 수 있는지 확인하십시오.

6단계. 로 Objects > Object Management > Access List > Extended 이동합니다. 를 Add Extended Access List 클릭합니다.



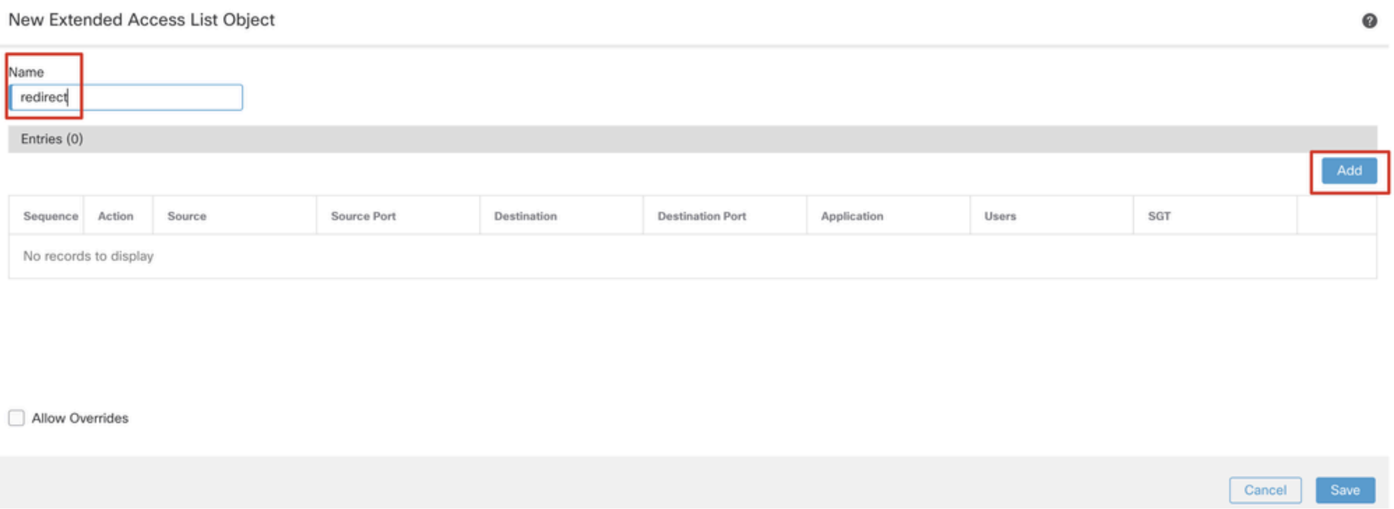
Extended

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

6.1

단계. 리디렉션 ACL의 이름을 제공합니다. 이 이름은 ISE 권한 부여 프로파일과 동일해야 합니다. 를 Add 클릭합니다.



New Extended Access List Object

Name: redirect

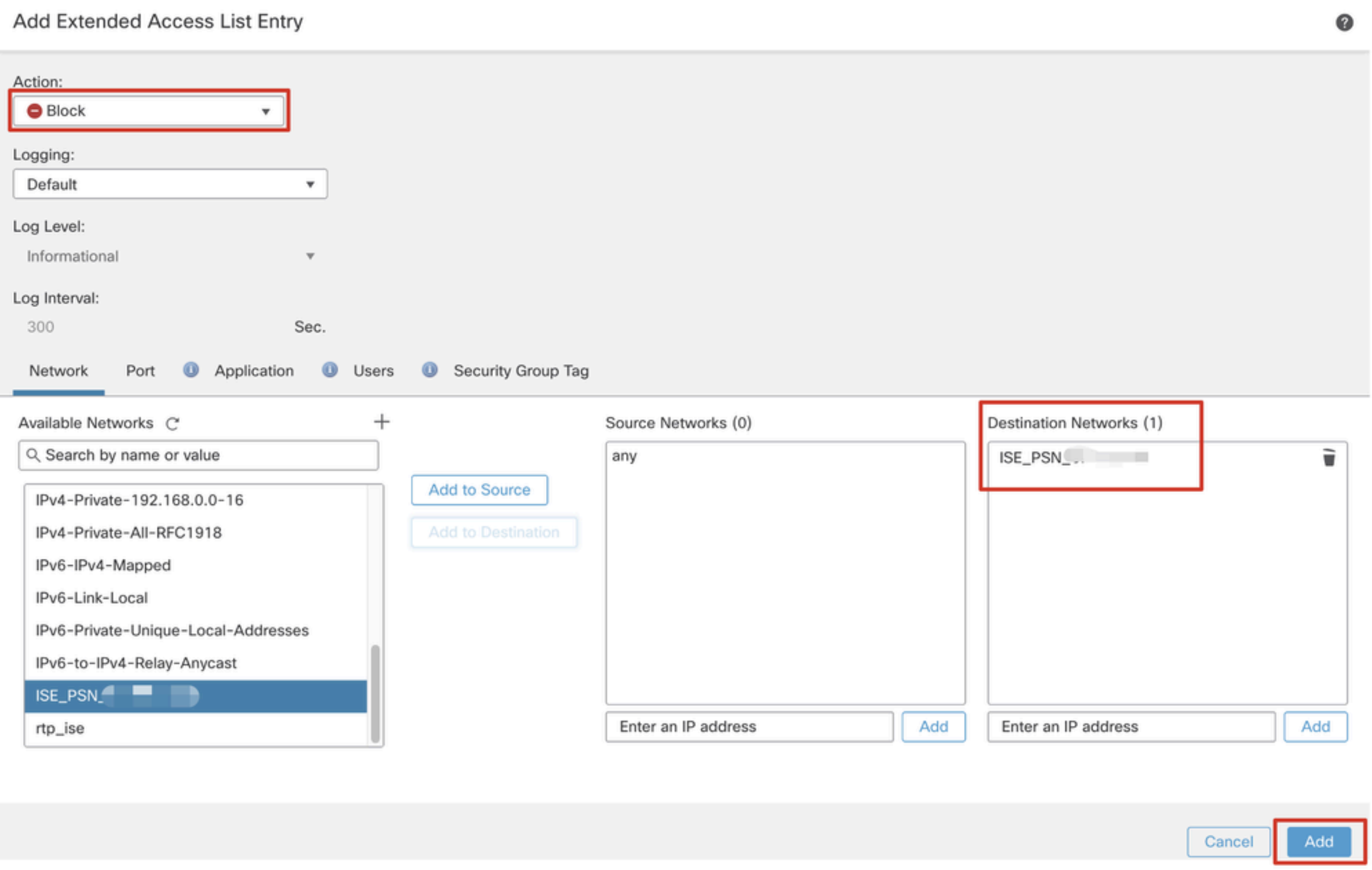
Entries (0)

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

□ Allow Overrides

FMC_Add_Redirect_ACL_Part_1

6.2단계. 리디렉션에서 제외할 DNS 트래픽, ISE PSN IP 주소에 대한 트래픽 및 리미디에이션 서버를 차단합니다. 나머지 트래픽을 허용합니다. 리디렉션이 트리거됩니다. 를 Save 클릭합니다.



Add Extended Access List Entry

Action: Block

Logging: Default

Log Level: Informational

Log Interval: 300 Sec.

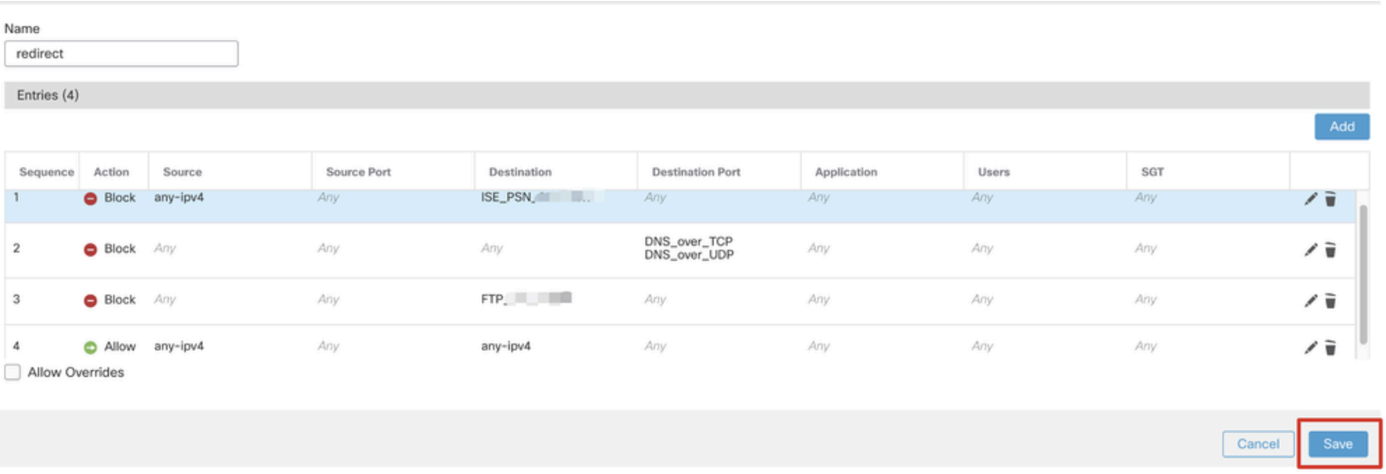
Available Networks

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

Source Networks (0): any

Destination Networks (1): ISE_PSN_[redacted]

FMC_Add_Redirect_ACL_Part_2



Name

redirect

Entries (4)

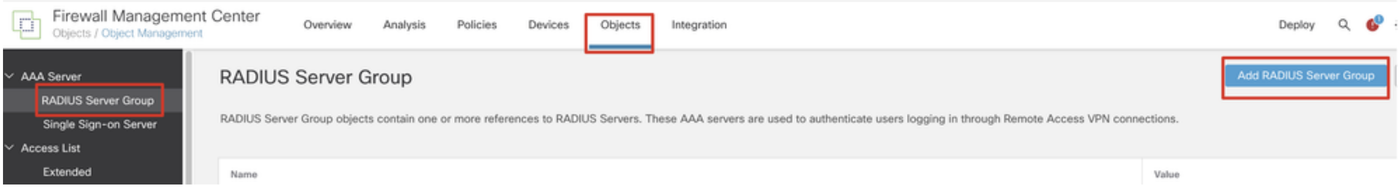
Sequence	Action	Source	Source Port	Destination	Destination Port	Application	Users	SGT
1	● Block	any-ipv4	Any	ISE_PSN_[redacted]	Any	Any	Any	Any
2	● Block	Any	Any	Any	DNS_over_TCP DNS_over_UDP	Any	Any	Any
3	● Block	Any	Any	FTP_[redacted]	Any	Any	Any	Any
4	● Allow	any-ipv4	Any	any-ipv4	Any	Any	Any	Any

□ Allow Overrides

FMC_Add_Redirect_ACL_Part_3

참고: 이 리디렉션 ACL 예의 대상 FTP는 리미디에이션 서버 예제로 사용됩니다.

7단계. 로 Objects > Object Management > RADIUS Server Group 이동합니다. 를 Add RADIUS Server Group 클릭합니다.

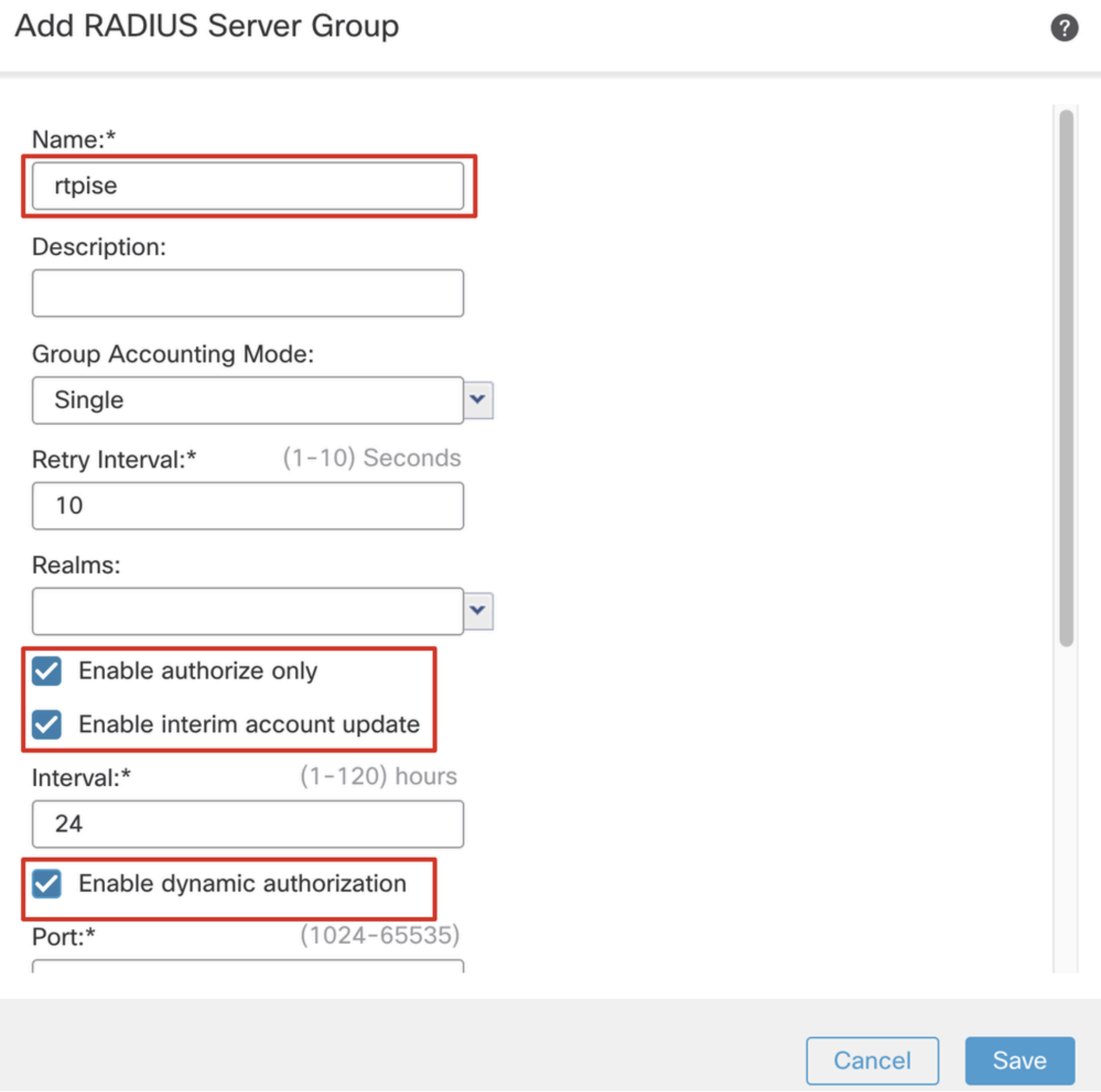


RADIUS Server Group

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

7.1단계. 이름, 확인Enable authorize only, 확인Enable interim account update, 확인Enable dynamic authorization을 입력합니다.



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

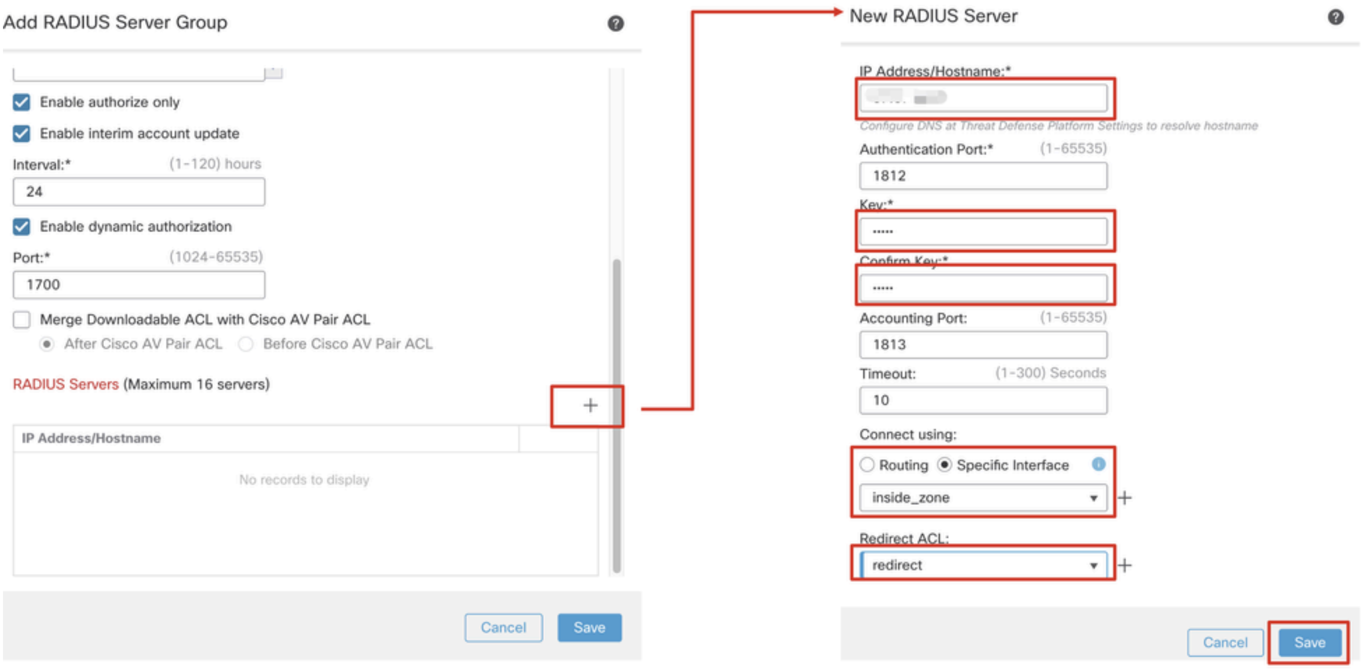
Interval:* (1-120) hours
24

☑ Enable dynamic authorization

Port:* (1024-65535)

FMC_Add_New_Radius_Server_Group_Part_1

7.2단계. 아이콘을 Plus 클릭하여 새 RADIUS 서버를 추가합니다. ISE PSN을 제공합니다. IP Address/Hostname, Key연결할 를 specific interface 선택합니다. 을 Redirect ACL선택합니다. 그런 다음 새 SaveRADIUS 서버를 저장하려면 클릭합니다. 그런 다음 다시 클릭하여Save 새 RADIUS 서버 그룹을 저장합니다.



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)

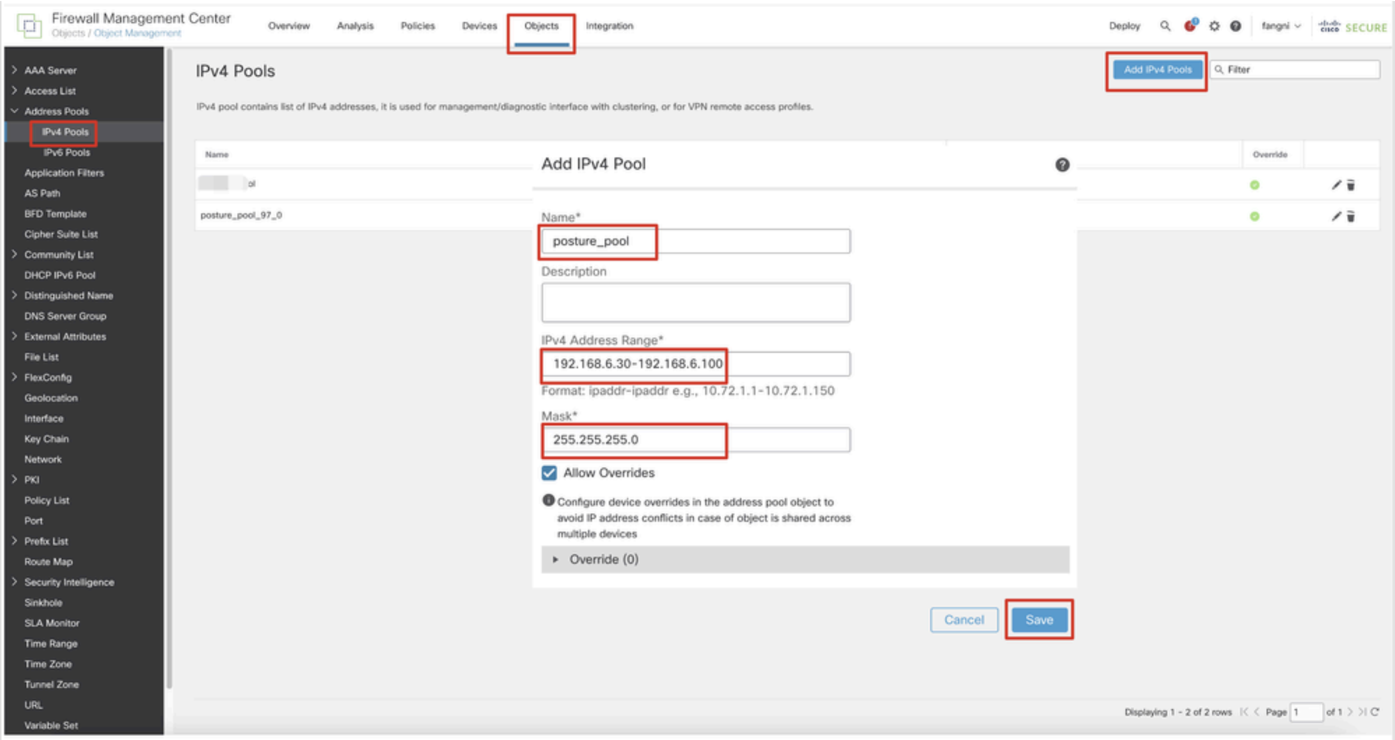
IP Address/Hostname
No records to display

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

8단계. 로 Objects > Object Management > Address Pools > IPv4 Pools 이동합니다. 을 Add IPv4 Pools 클릭하고 및 을 **Name, IPv4 Address Range**제공합니다Mask. 그런 다음 을 클릭합니다Save.



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	●

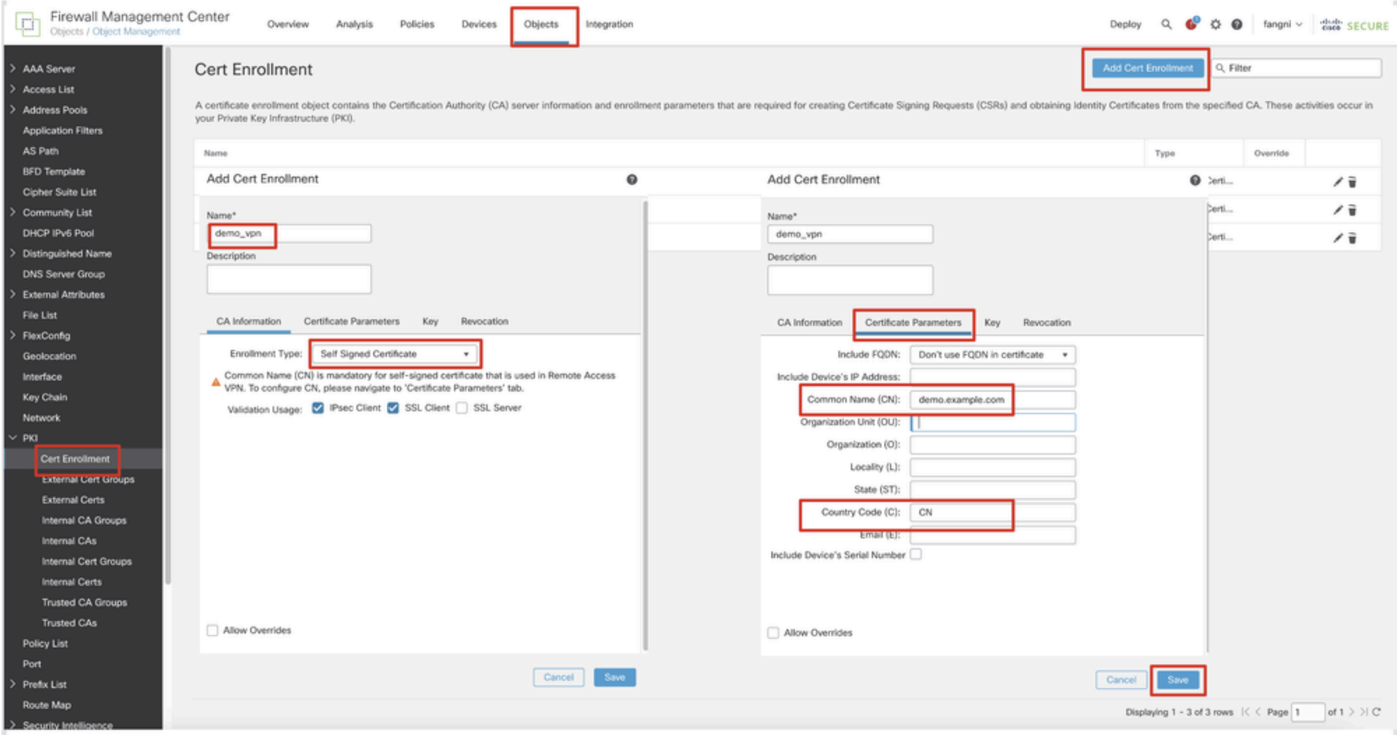
Add IPv4 Pool

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

9단계. 로 Certificate Objects > Object Management > PKI > Cert Enrollment 이동합니다. 을 Add Cert Enrollment 클릭하고 이름을 입력한 다음 Self Signed Certificatein을 Enrollment Type 선택합니다. 탭을 Certificate Parameters 클릭하고 및 를Common Name 제공합니다 Country Code. 그런 다음 을 클릭합니다Save.



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:

CA Information | Certificate Parameters | Key | Revocation

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

Description:

CA Information | Certificate Parameters | Key | Revocation

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):

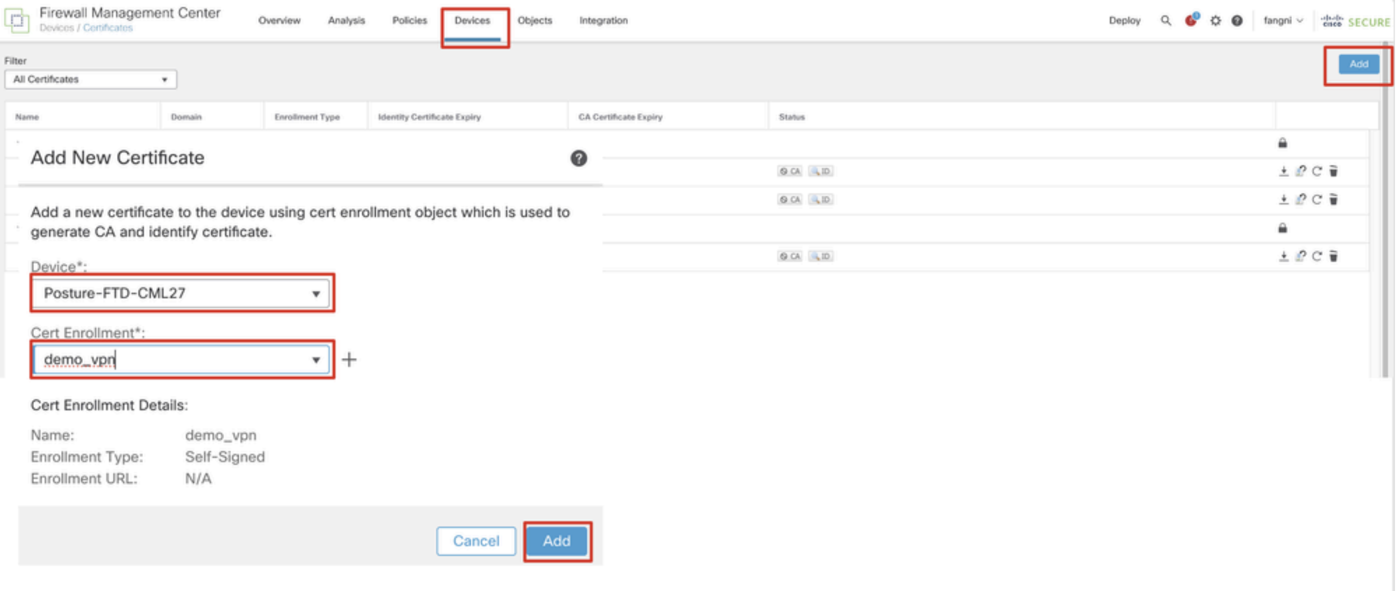
Include Device's Serial Number □

□ Allow Overrides

Displaying 1 - 3 of 3 rows

FMC_Add_New_Cert_Enroll

10단계. 로 Devices > Certificates 이동합니다. 을 Add 클릭하고 아래에서 FTD 이름을 Device 선택한 다음 아래에서 이전 구성된 등록을 선택합니다Cert Enrollment. 를 Add 클릭합니다.



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

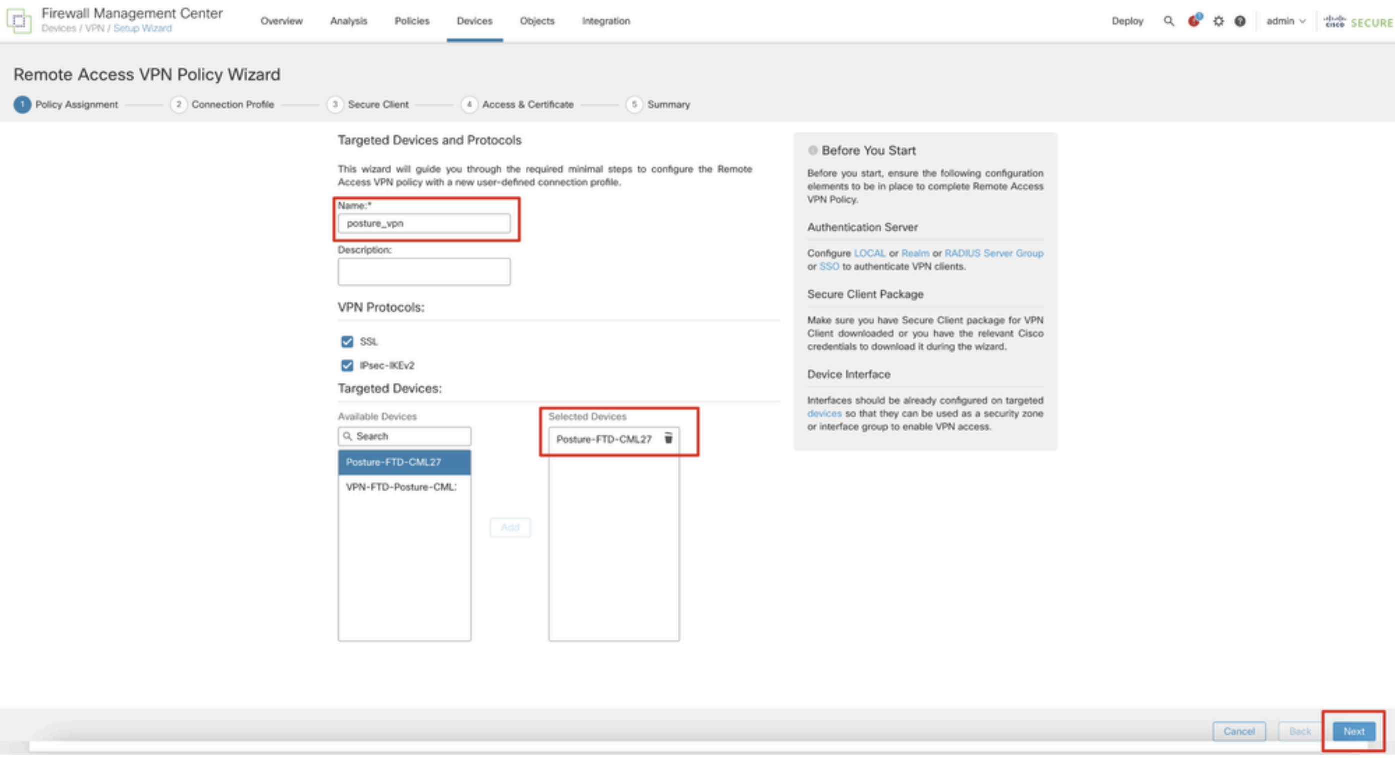
Cert Enrollment Details:

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

FMC_Add_New_Cert_To_FTD

11단계. 로 Devices > VPN > Remote Access 이동합니다. 를 Add 클릭합니다.

11.1단계. 이름을 입력하고 FTD를 추가합니다Selected Devices. 를 Next 클릭합니다.



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

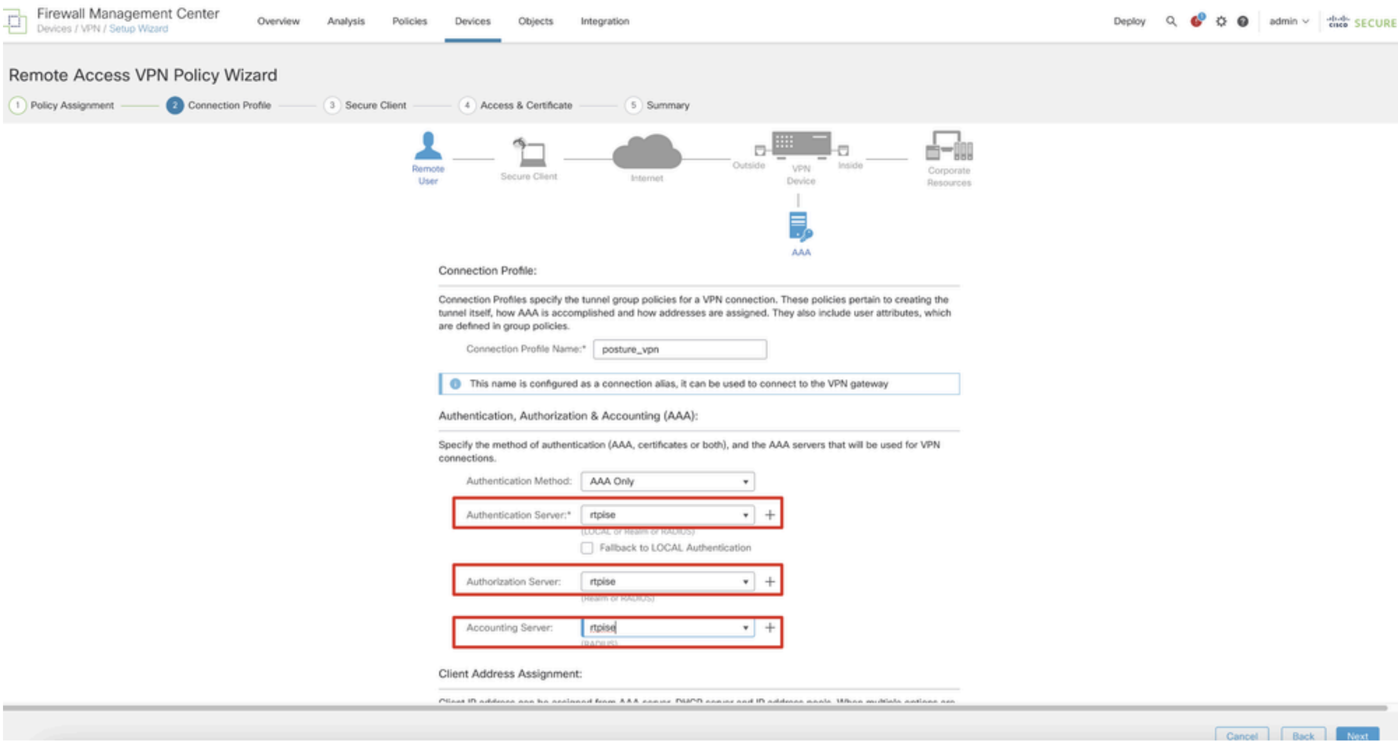
Make sure you have Secure Client package for VPN Client downloaded or you have the relevant Cisco credentials to download it during the wizard.

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

11.2단계. 에서 이전에 구성한 RADIUS 서버 그룹을 Authentication Server, Authorization Server, Accounting Server 선택합니다. 페이지를 아래로 스크롤합니다.



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

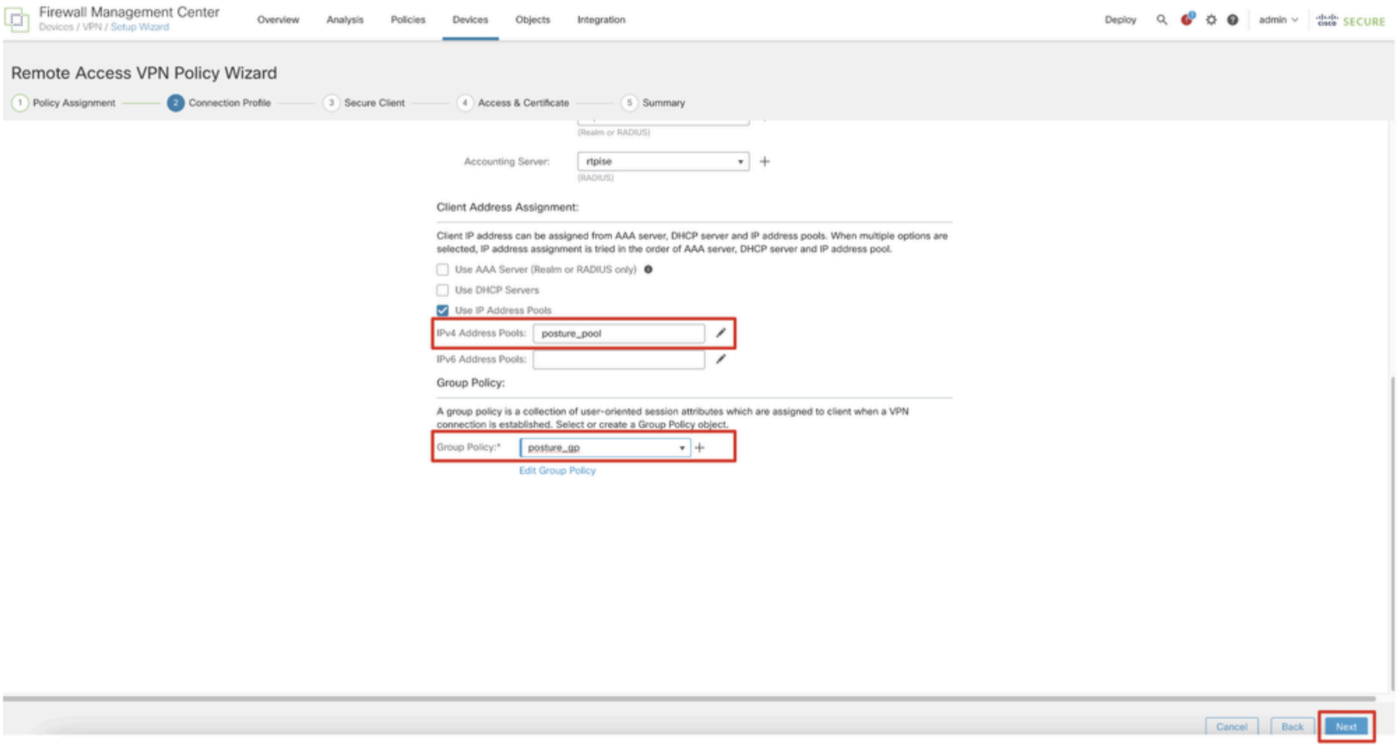
Authorization Server: rtpise (Realm or RADIUS)

Accounting Server: rtpise (RADIUS)

Client Address Assignment:

FMC_New_RAVPN_Wizard_2

11.3단계. 에서 이전에 구성된 풀 이름을 IPv4 Address Pools 선택합니다. 에서 이전에 구성된 그룹 정책을 Group Policy 선택합니다. 을 Next 누릅니다.



Remote Access VPN Policy Wizard

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

(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:

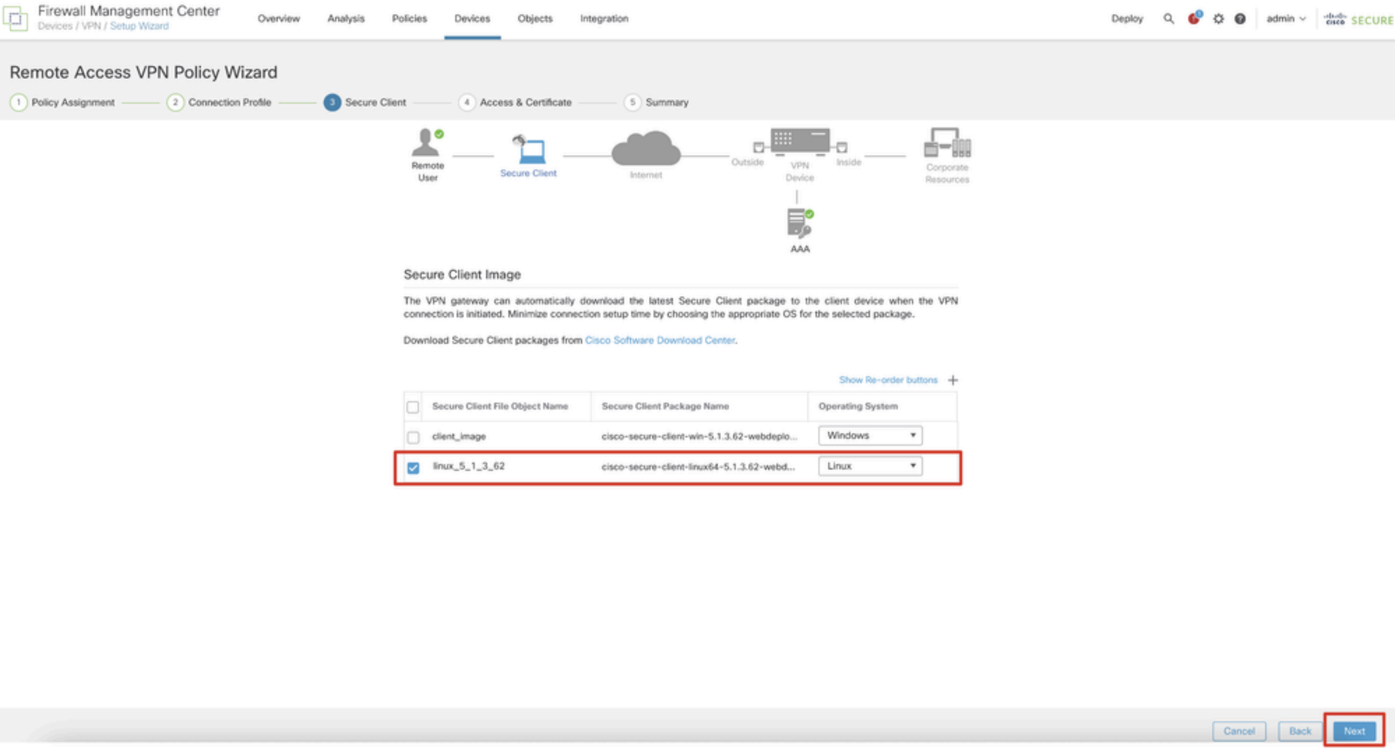
A group policy is a collection of user-oriented session attributes which are assigned to client when a VPN connection is established. Select or create a Group Policy object.

Group Policy:* posture_gp

Edit Group Policy

FMC_New_RAVPN_Wizard_3

11.4단계. Linux 이미지의 확인란을 선택합니다. 를 Next 클릭합니다.



Remote Access VPN Policy Wizard

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

Secure Client Image

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

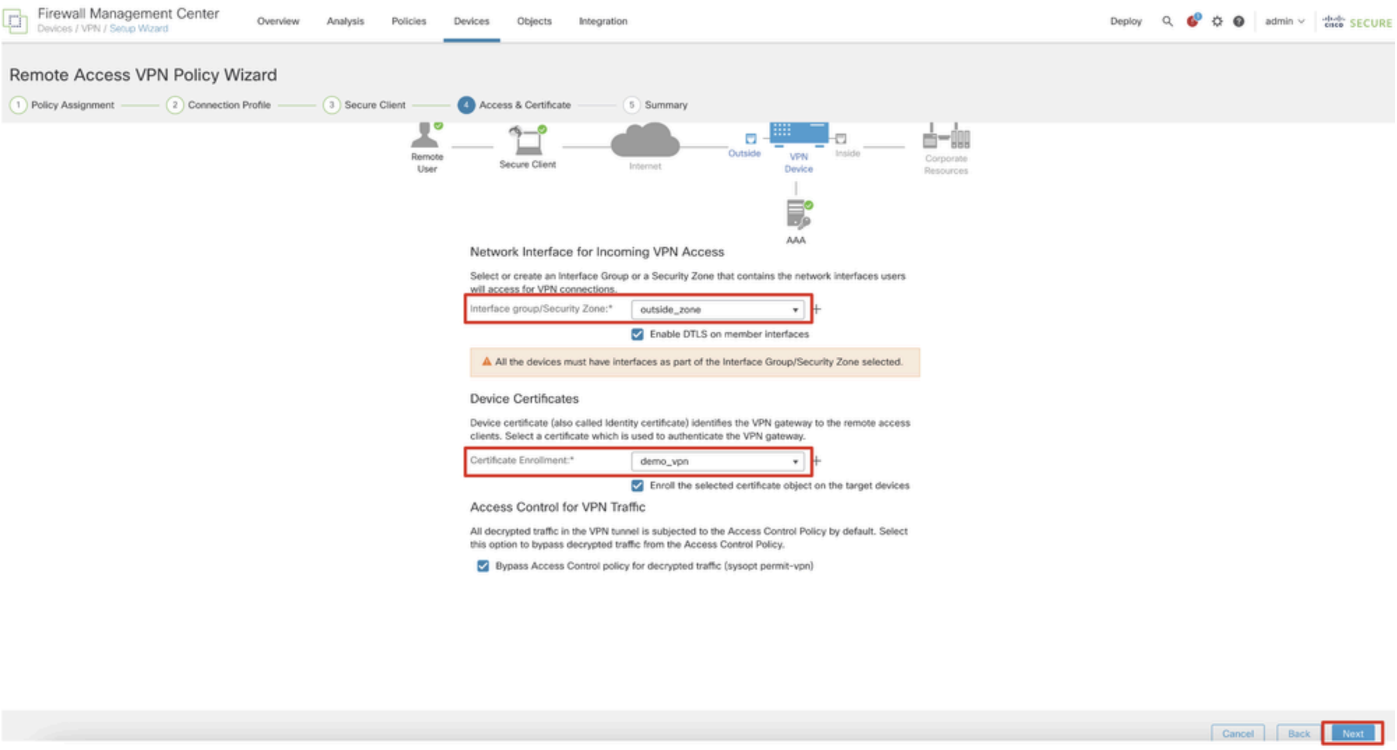
Download Secure Client packages from Cisco Software Download Center.

Show Re-order buttons +

□	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

11.5단계. VPN 인터페이스의 인터페이스를 선택합니다. 9단계에서 FTD에 등록한 인증서 등록을 선택합니다. 를 Next 클릭합니다.



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

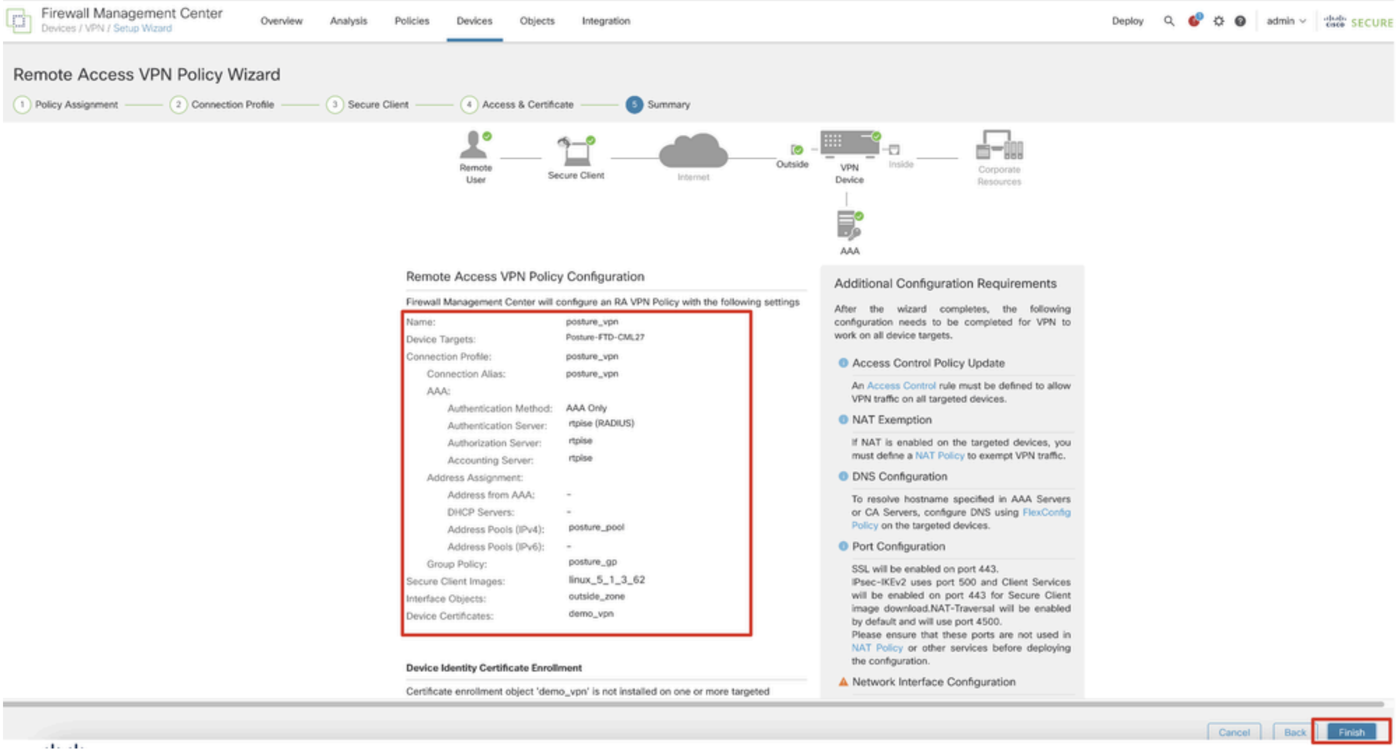
Access Control for VPN Traffic

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

11.6단계. 요약 페이지에서 관련 정보를 다시 확인합니다. 모든 것이 좋으면 클릭하십시오Finish. 수정해야 할 사항이 있으면 을 클릭합니다Back.



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.

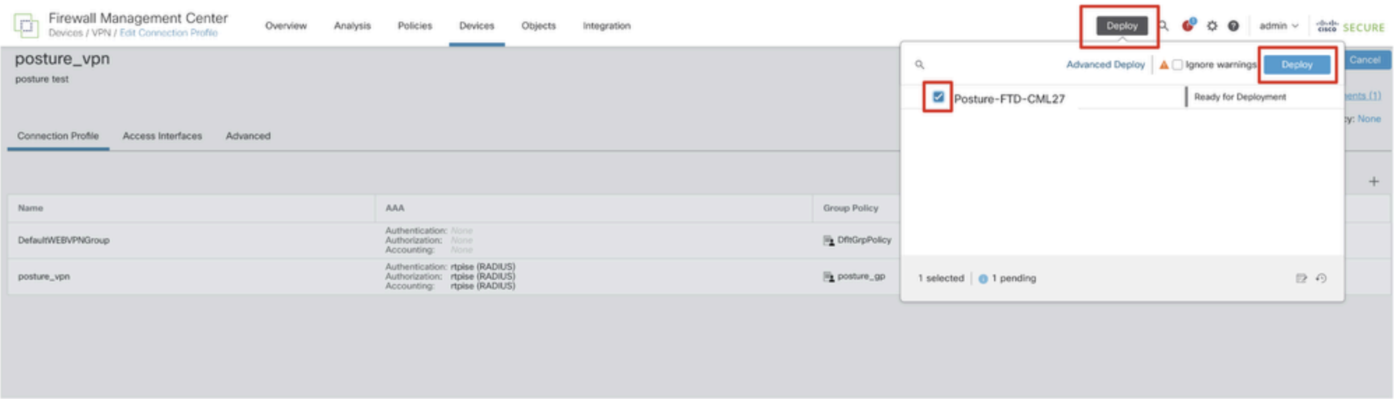
Port Configuration

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

12단계. FTD에 새 컨피그레이션을 구축하여 원격 액세스 VPN 컨피그레이션을 완료합니다.

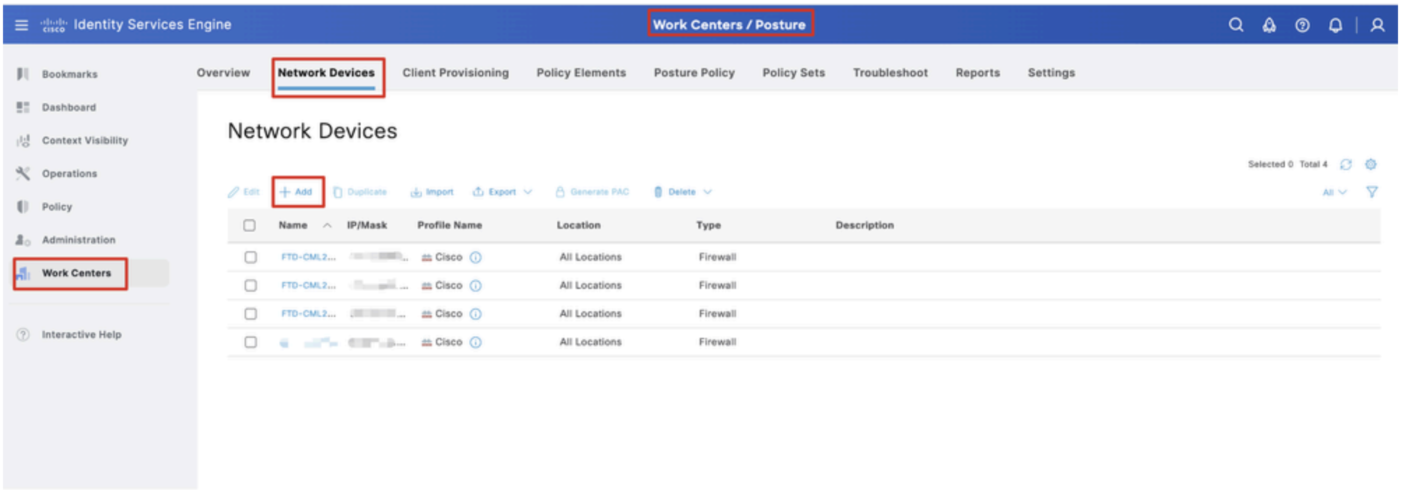


Name	AAA	Group Policy
DefaultWEBVPNGroup	Authentication: None Authorization: None Accounting: None	DfltGrpPolicy
posture_vpn	Authentication: rtpise (RADIUS) Authorization: rtpise (RADIUS) Accounting: rtpise (RADIUS)	posture_gp

FMC_Deploy_FTD

ISE의 컨피그레이션

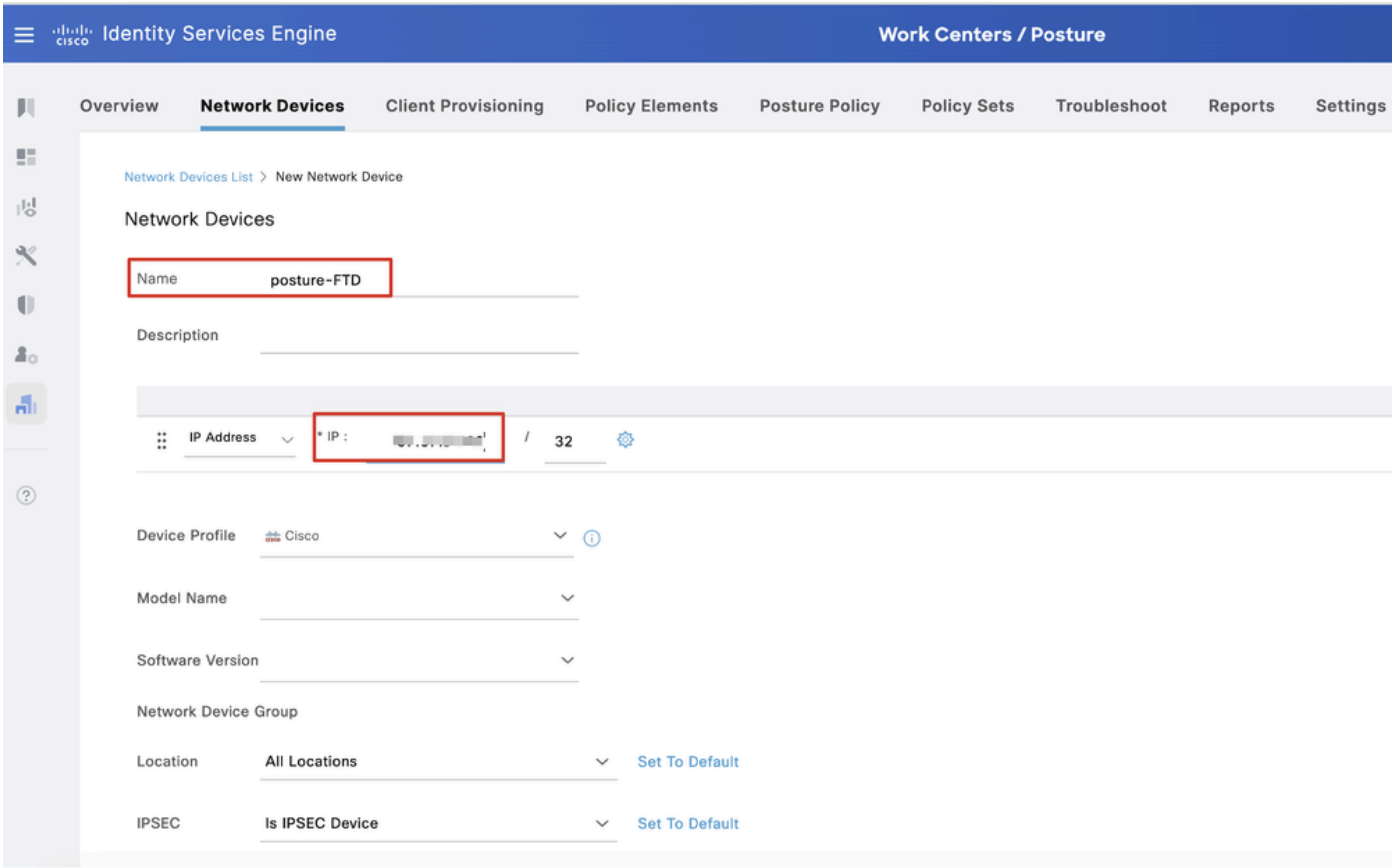
13단계. 로 Work Centers > Posture > Network Devices 이동합니다. 를 Add 클릭합니다.



□	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_Device

13.1단계. 를 Name, IP Address입력하고 페이지를 아래로 스크롤합니다.



Network Devices

Name: posture-FTD

Description:

IP Address | * IP : [redacted] / 32

Device Profile: Cisco

Model Name:

Software Version:

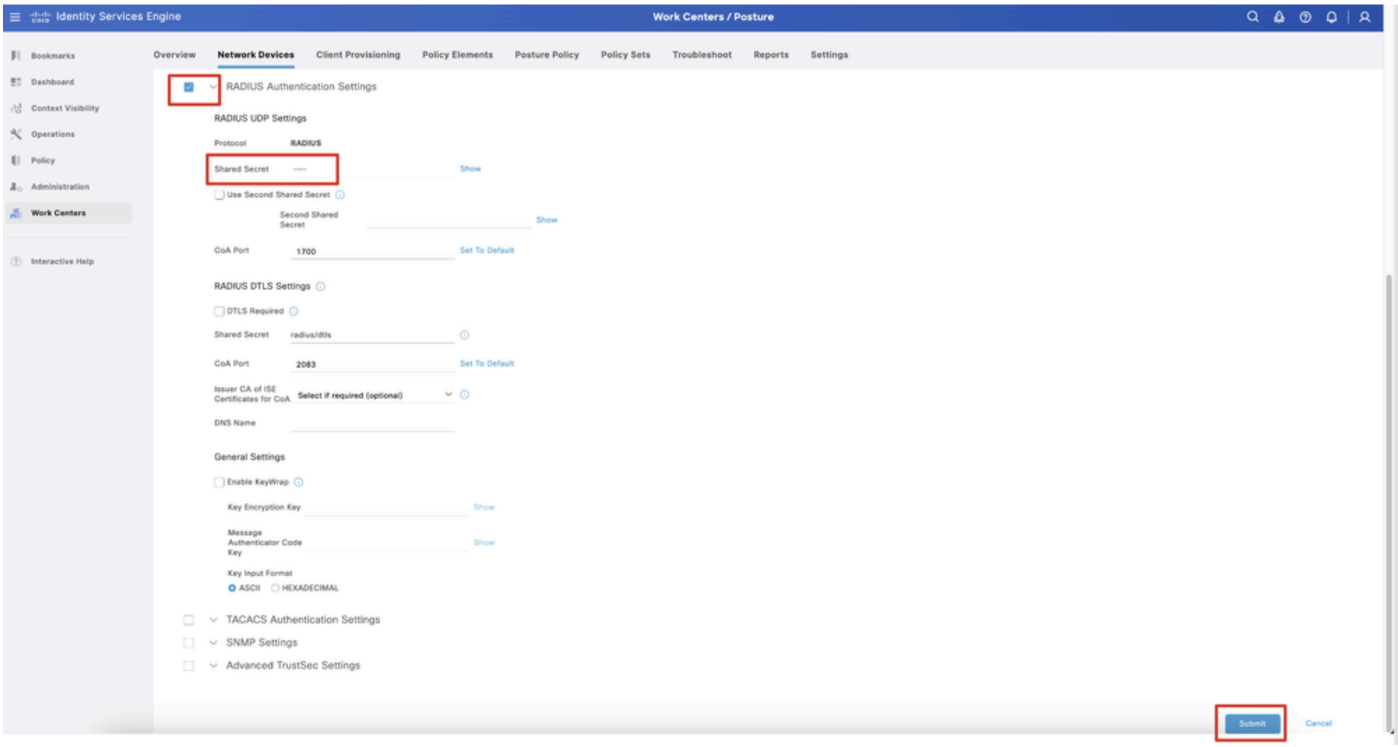
Network Device Group

Location: All Locations — Set To Default

IPSEC: Is IPSEC Device — Set To Default

ISE_Add_New_Devices_1

13.2단계. 의 확인란을 RADIUS Authentication Settings 선택합니다. 를 Shared Secret 제공합니다. 를 Submit 클릭합니다.



☑ 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

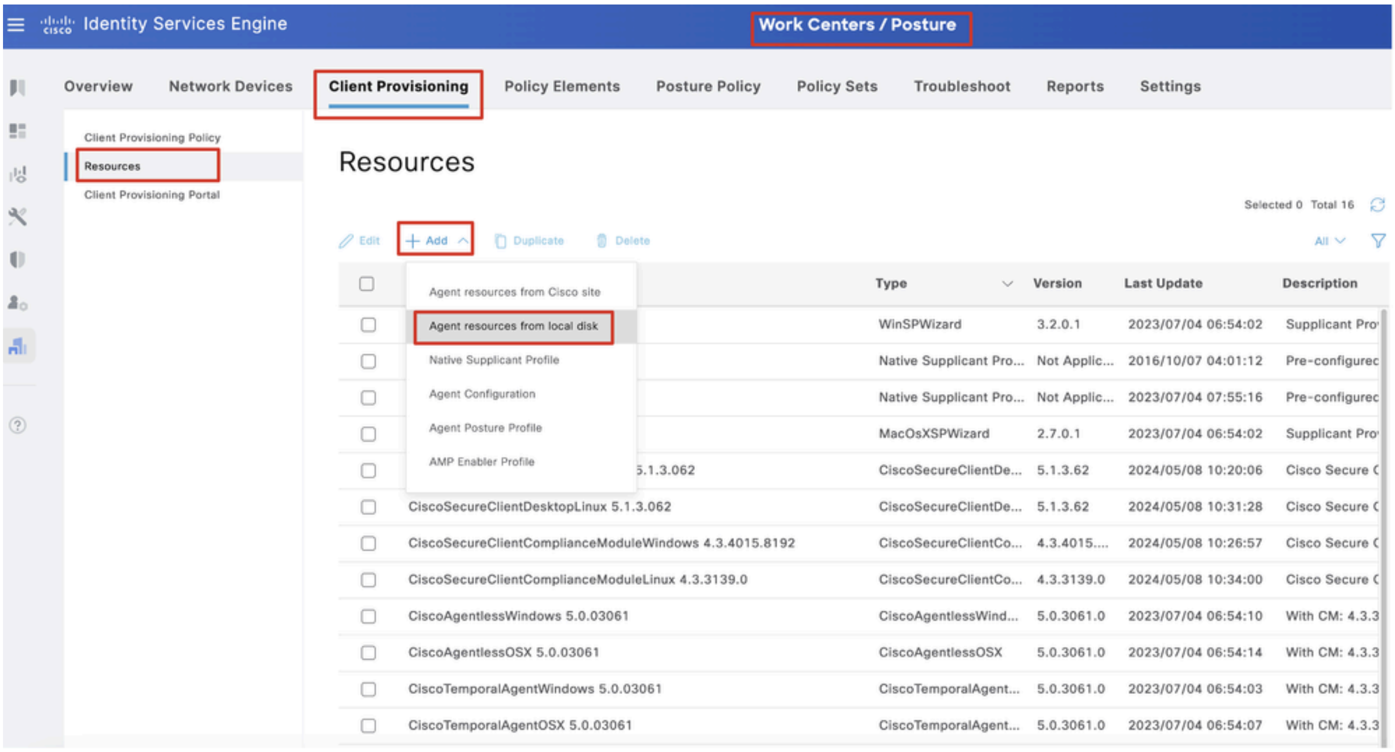
□ Advanced TrustSec Settings

ISE_Add_New_Devices_2

14단계. Cisco Software Downloadcisco-secure-client-linux64-4.3.3139.0-isecompliance-webdeploy-k9.pkg에서 패키지 이름을 다운로드하고 다운로드한 파일의 md5 체크섬이 Cisco Software Download 페이지와 동일한지 확인하여 파일이 정상인지 확인합니다. 패키지 이름

cisco-secure-client-linux64-5.1.3.62-webdeploy-k9.pkg이 1단계에서 성공적으로 다운로드되었습니다.

15단계. 로 Work Centers > Posture > Client Provisioning > Resources 이동합니다. 를 Add 클릭합니다. 를 Agent resources from local disk선택합니다.

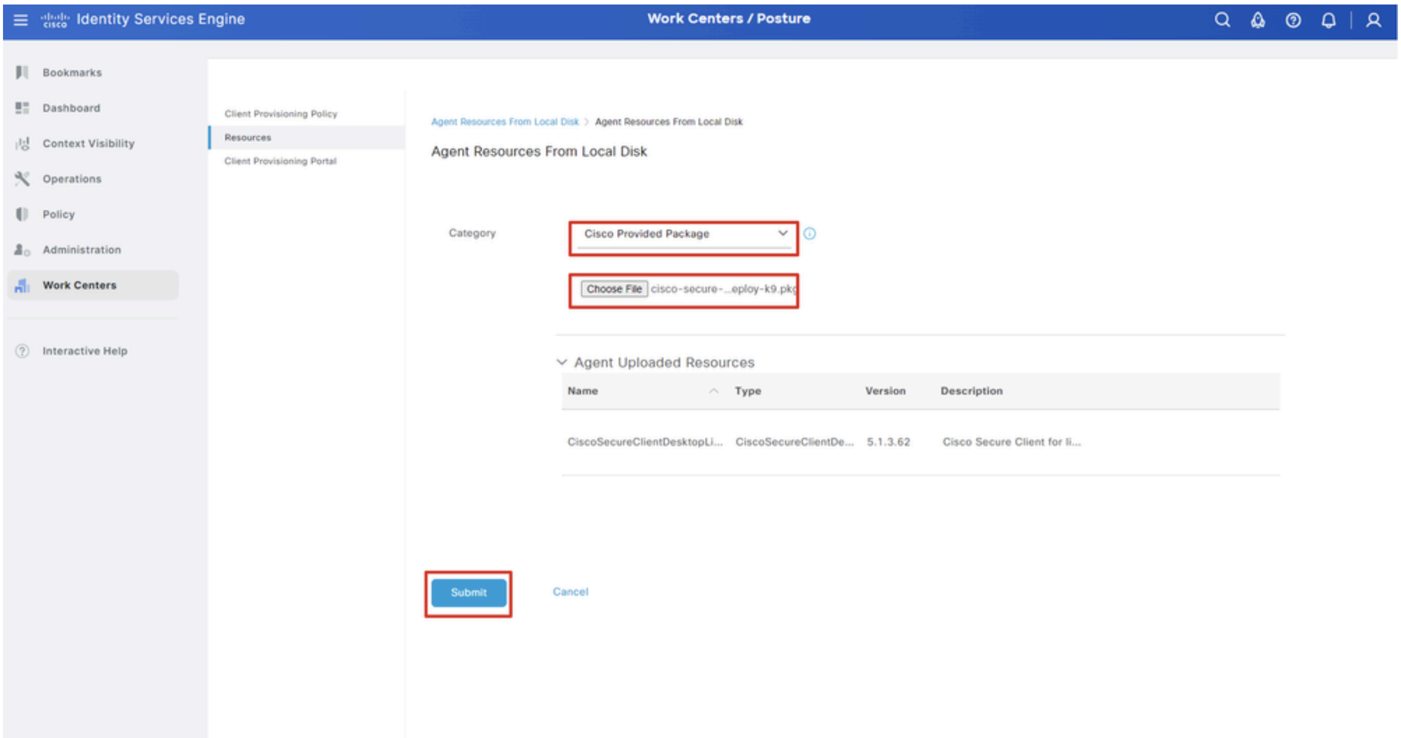


Resources

	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

15.1단계. 를 Cisco Provided Package선택합니다. cisco-secure-client-linux64-5.1.3.62-webdeploy-k9.pkg를 업로드하려면 클릭합니다 Choose File. 를 Submit 클릭합니다.



Agent Resources From Local Disk

Category: Cisco Provided Package

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

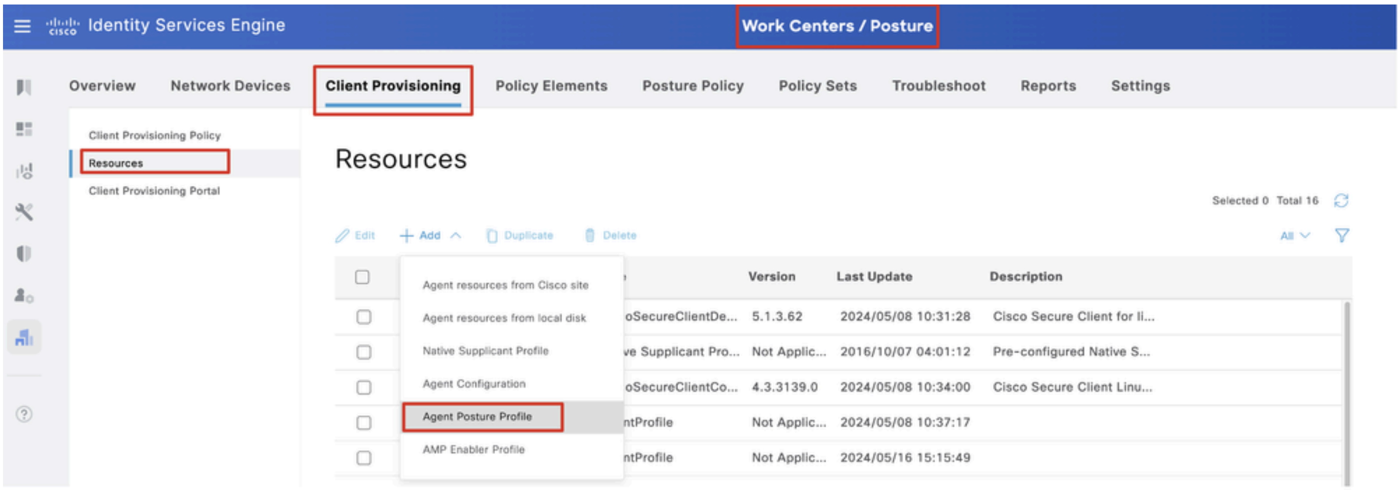
Agent Uploaded Resources

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

ISE_Upload_Resources_1

참고: 14단계를 반복하여 를 업로드합니다cisco-secure-client-linux64-4.3.3139.0-isecompliance-webdeploy-k9.pkg.

16단계. 로 Work Centers > Posture > Client Provisioning > Resources 이동합니다. 를 Add 클릭합니다. 를 Agent Posture Profile선택합니다
.



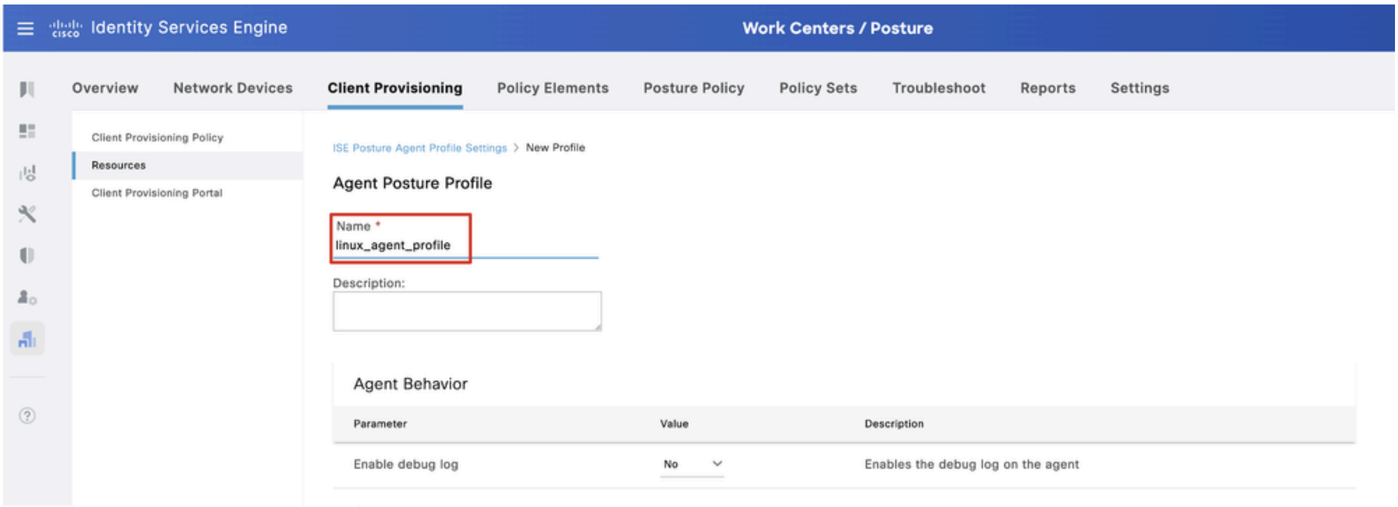
	Version	Last Update	Description
oSecureClientDe...	5.1.3.62	2024/05/08 10:31:28	Cisco Secure Client for li...
ve Supplicant Pro...	Not Applic...	2016/10/07 04:01:12	Pre-configured Native S...
oSecureClientCo...	4.3.3139.0	2024/05/08 10:34:00	Cisco Secure Client Linu...
ntProfile	Not Applic...	2024/05/08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

ISE_Add_Agent_Posture_Profile

16.1단계. 를 Name, Server name rules 제공하고 나머지는 기본값으로 유지합니다. 를 Save 클릭합니다.

이름: linux_agent_profile

서버 이름 규칙: *.example.com



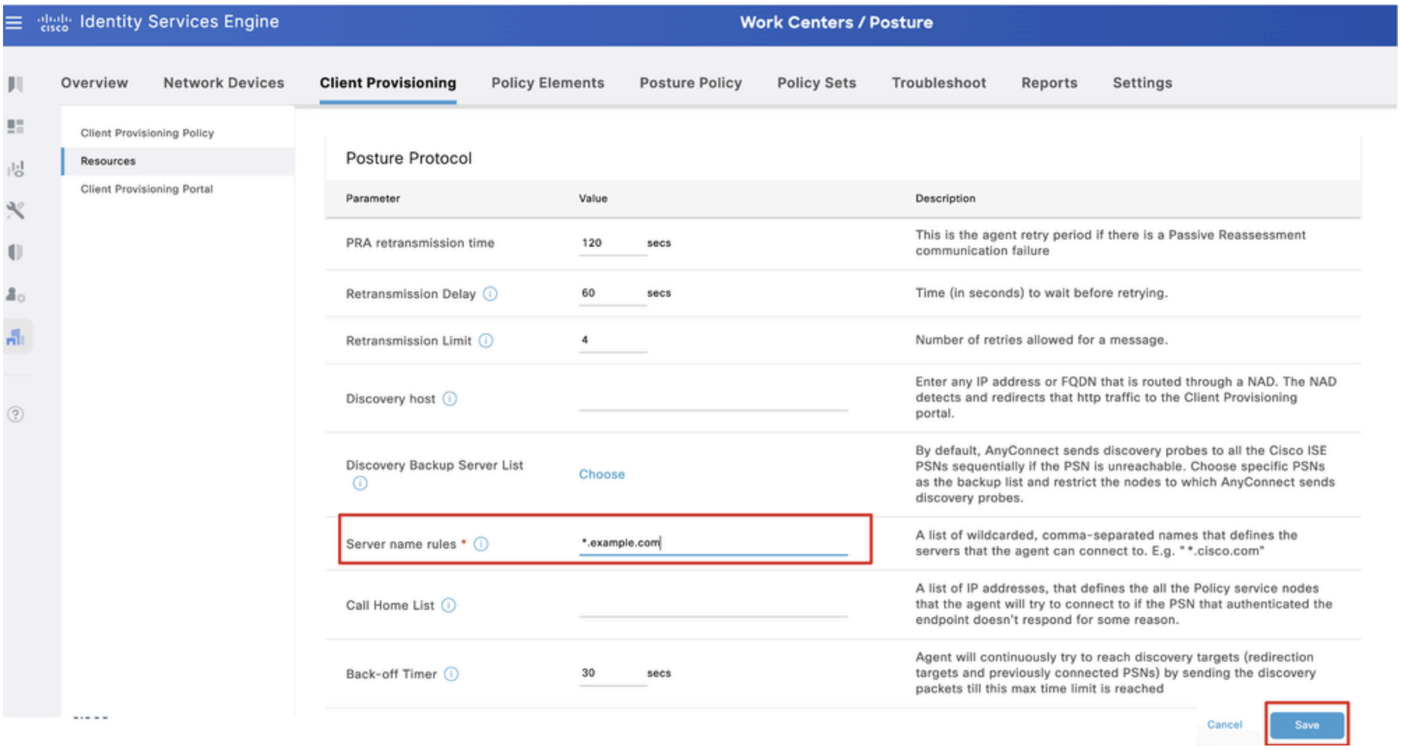
Name * linux_agent_profile

Description:

Agent Behavior

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

ISE_Add_Agent_Posture_Profile_1

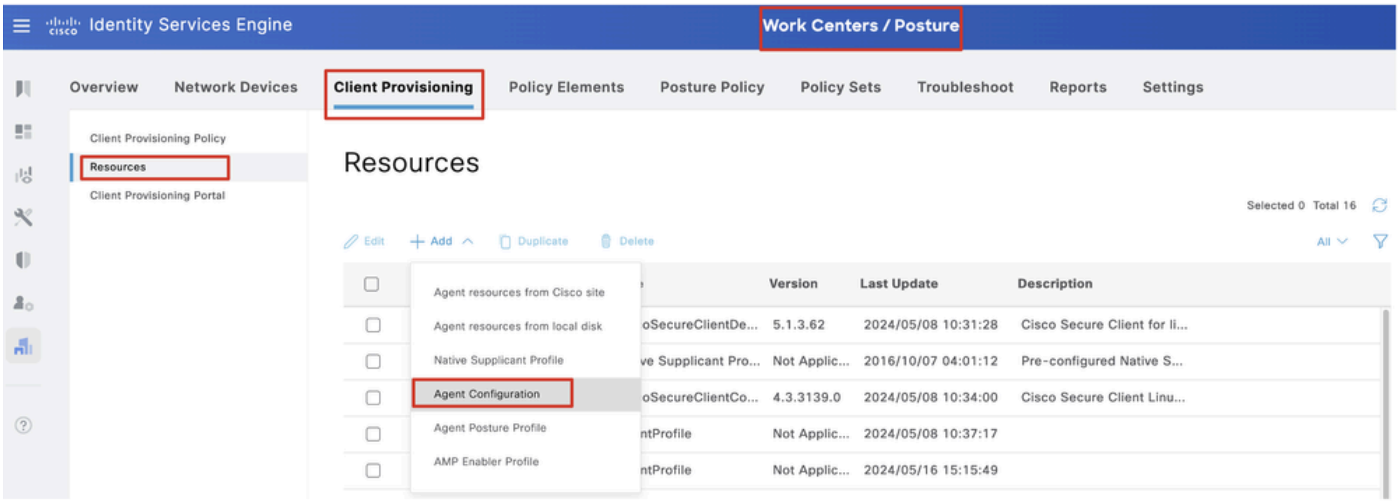


Posture Protocol

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

17단계. 로 Work Centers > Posture > Client Provisioning > Resources 이동합니다. 를 Add 클릭합니다. 를 Agent Configuration선택합니다.



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

17.2단계. 세부 정보를 구성합니다.

에이전트 패키지 선택: CiscoSecureClientDesktopLinux 5.1.3.062

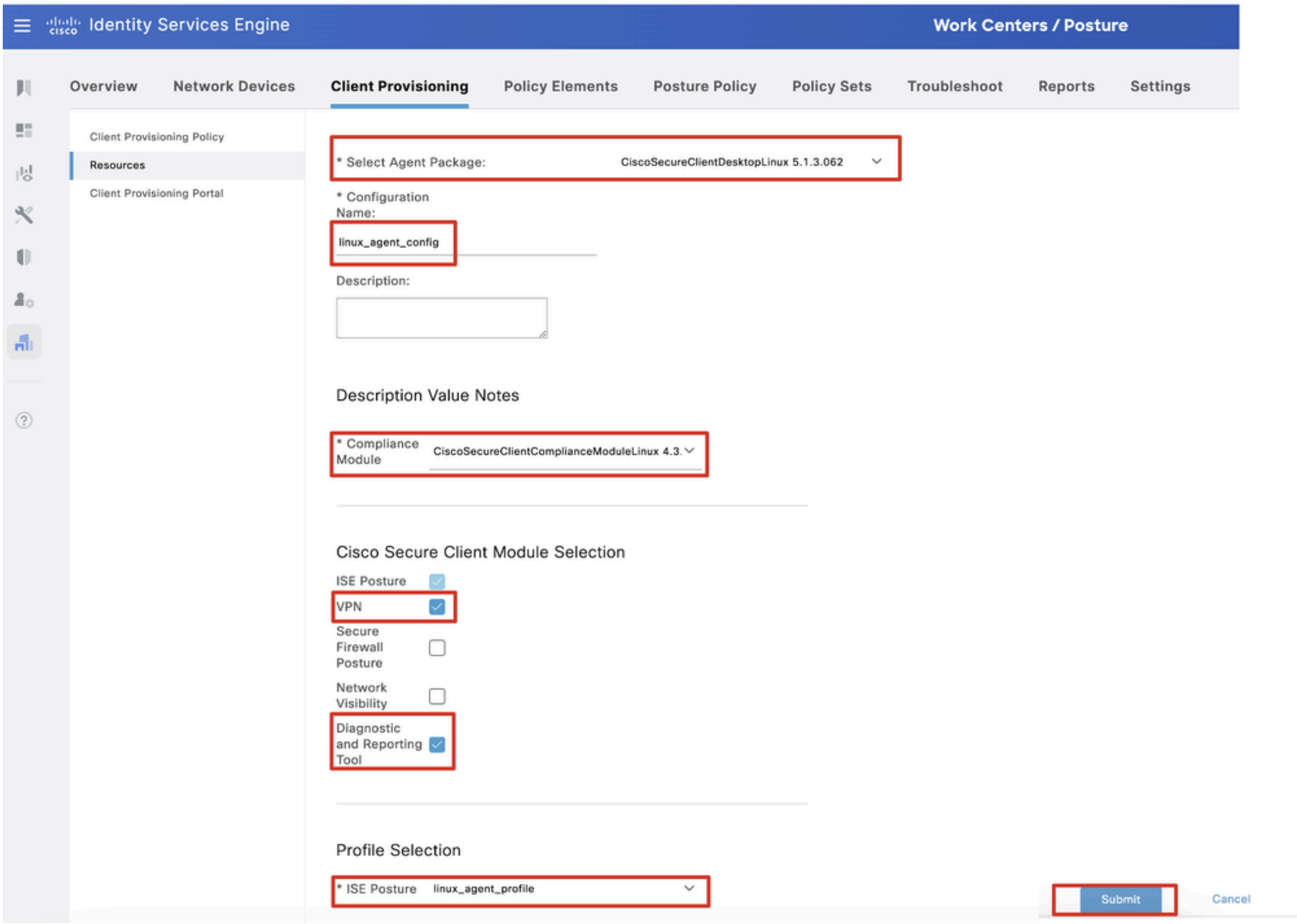
이름: linux_agent_config

규정 준수 모듈: CiscoSecureClientComplianceModuleLinux 4.3.3139.0

의 확인란을 선택합니다. VPN, Diagnostic and Reporting Tool

프로파일 선택 ISE 상태: linux_agent_profile

를 Submit 클릭합니다.



* 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

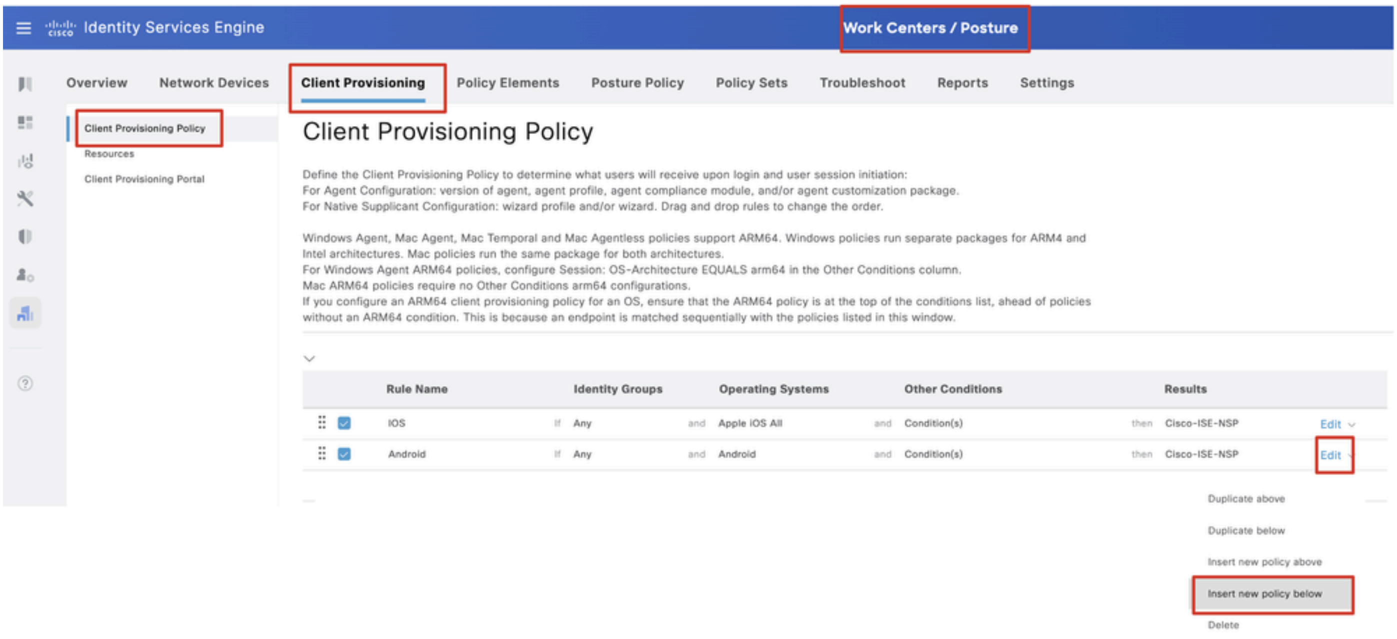
ISE Posture ☑
VPN ☑
Secure Firewall Posture □
Network Visibility □
Diagnostic and Reporting Tool ☑

Profile Selection

* ISE Posture linux_agent_profile

ISE_Add_Agent_Configuration_1

18단계. 로 Work Centers > Posture > Client Provisioning > Client Provisioning Policy 이동합니다. 규칙 이름Edit 의 끝에서 을 클릭합니다 . 를 Insert new policy below선택합니다.



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

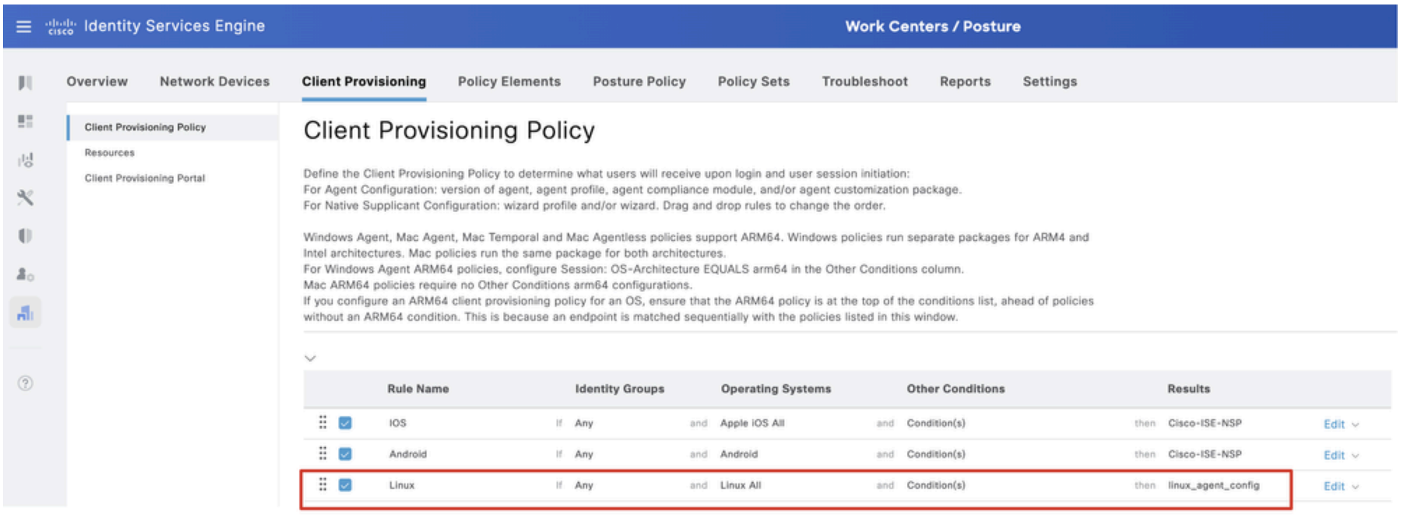
18.1단계. 세부 정보를 구성합니다.

규칙 이름: Linux

운영 체제: Linux All

결과: linux_agent_config

andDone 를 Save클릭합니다.



Client Provisioning Policy

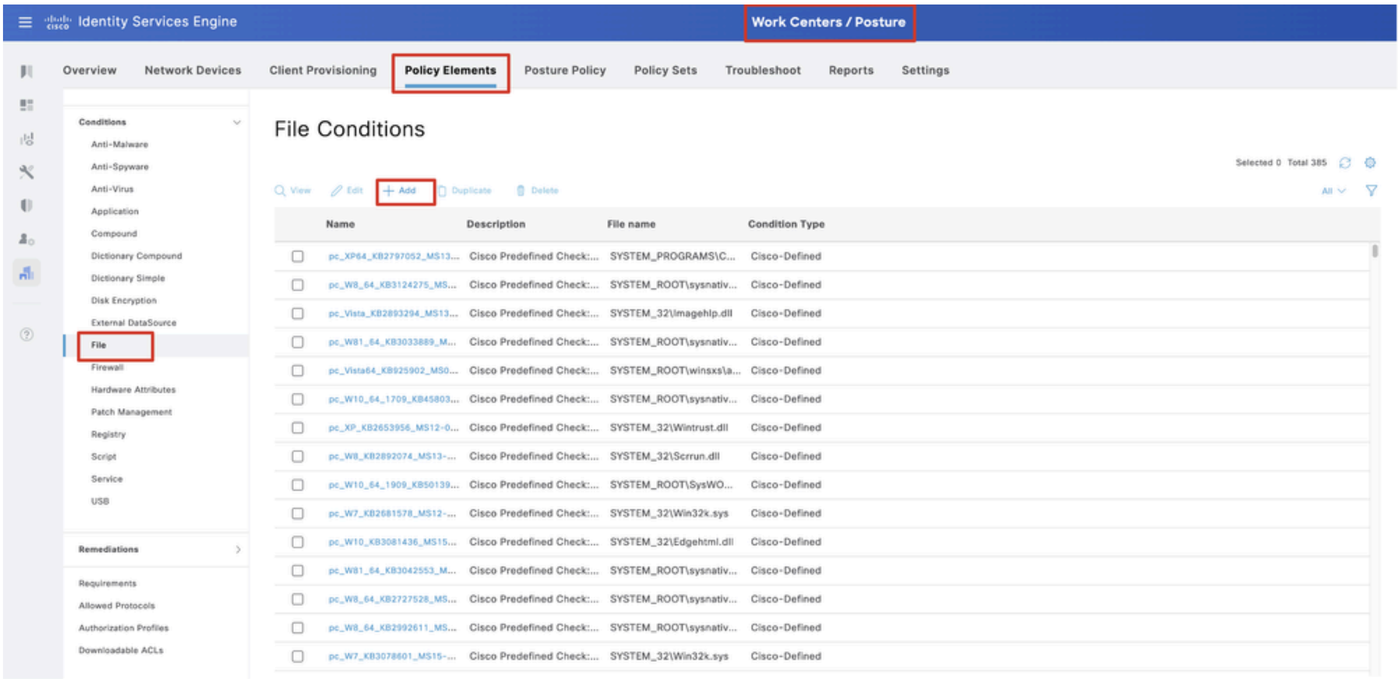
Define the Client Provisioning Policy to determine what users will receive upon login and user session initiation:
For Agent Configuration: version of agent, agent profile, agent compliance module, and/or agent customization package.
For Native Supplicant Configuration: wizard profile and/or wizard.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

19단계. 로 Work Centers > Posture > Policy Elements > Conditions > File 이동합니다. 를 Add 클릭합니다.



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

19.1단계. 세부 정보를 구성합니다.

이름: linux_demo_file_exist

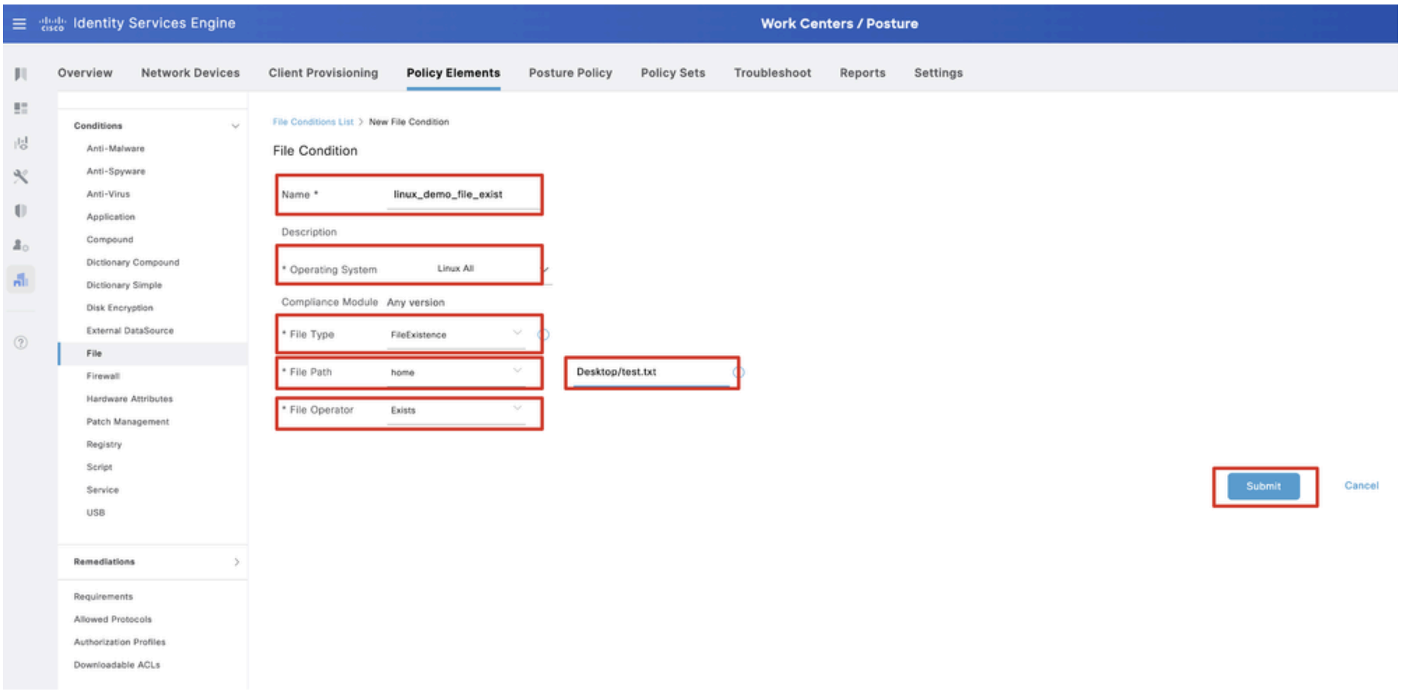
운영 체제: Linux All

파일 유형: FileExistence

파일 경로: 홈, Desktop/test.txt

파일 연산자: 있음

를 Submit 클릭합니다.



File Condition

Name * linux_demo_file_exist

Description

* Operating System Linux All

Compliance Module Any version

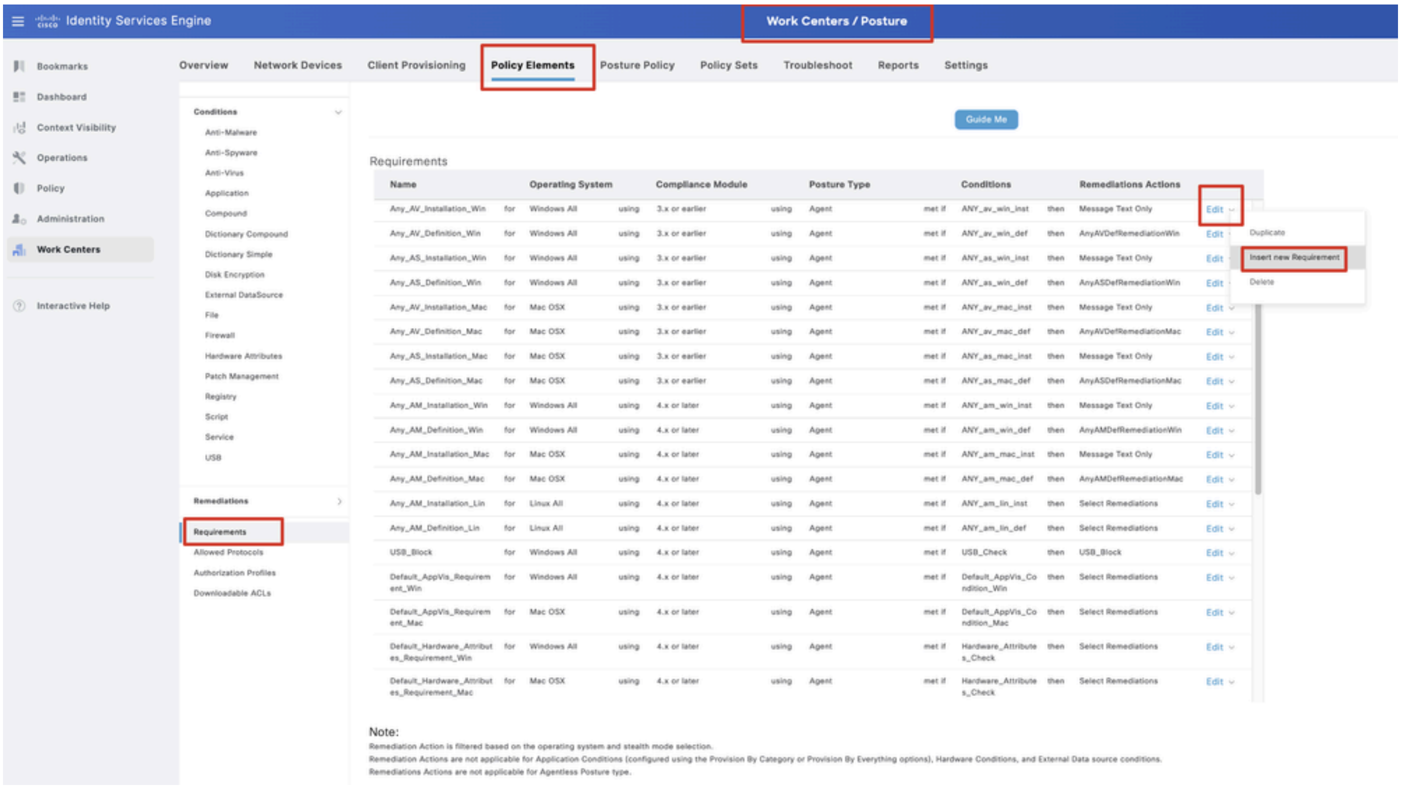
* File Type FileExistence

* File Path home Desktop/test.txt

* File Operator Exists

ISE_Add_New_File_Condition_1

20단계. 로 Work Centers > Posture > Policy Elements > Requirements 이동합니다. 규칙 이름Edit 의 끝에서 을 클릭합니다. 를 Insert new Requirement선택합니다.



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

20.1단계. 세부 정보를 구성합니다.

이름: Test_exist_linux

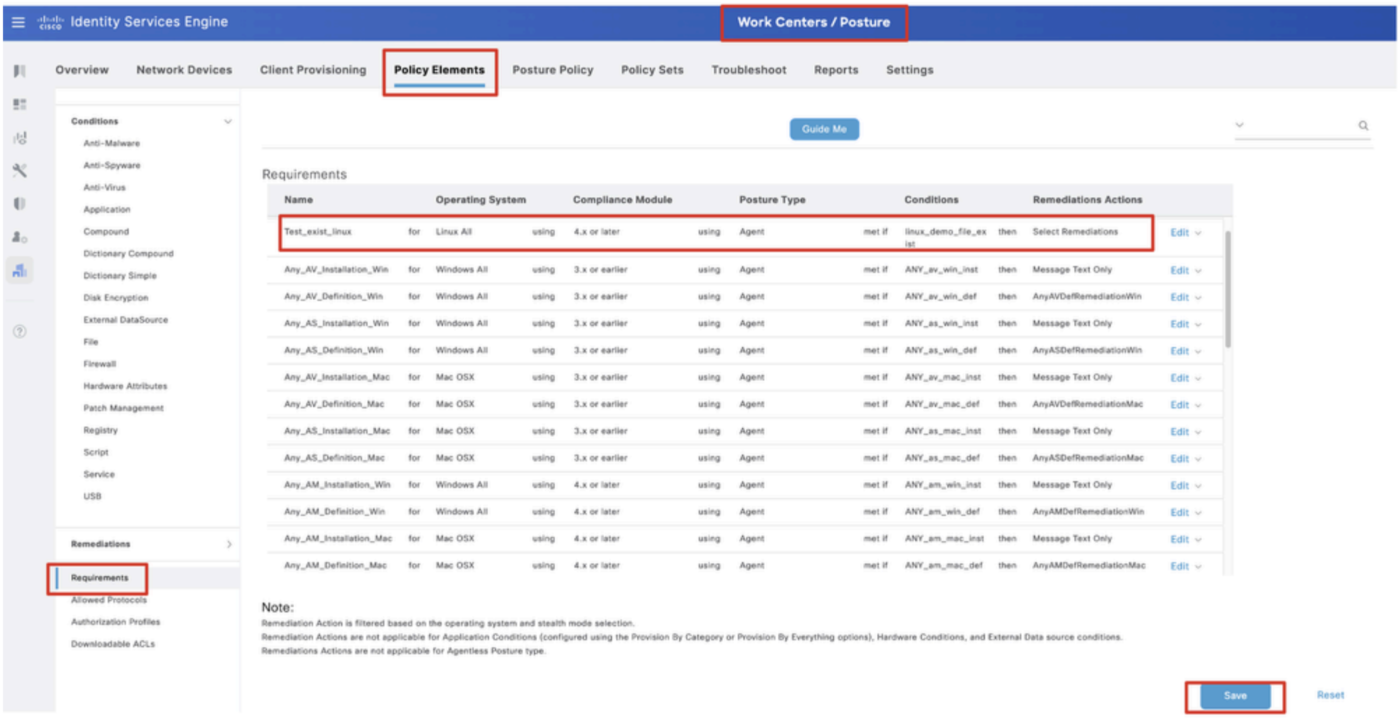
운영 체제: Linux All

Compliance Module: 4.x 이상

포스처 유형: 에이전트

조건: linux_demo_file_exist

andDone 를 Save클릭합니다.



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

참고: 현재로서는 Linux 에이전트에 대한 셸 스크립트만 교정으로 지원됩니다.

21단계. 로 Work Centers > Posture > Policy Elements > Authorization Profiles 이동합니다. 를 Add 클릭합니다.

21.1단계. 세부 정보를 구성합니다.

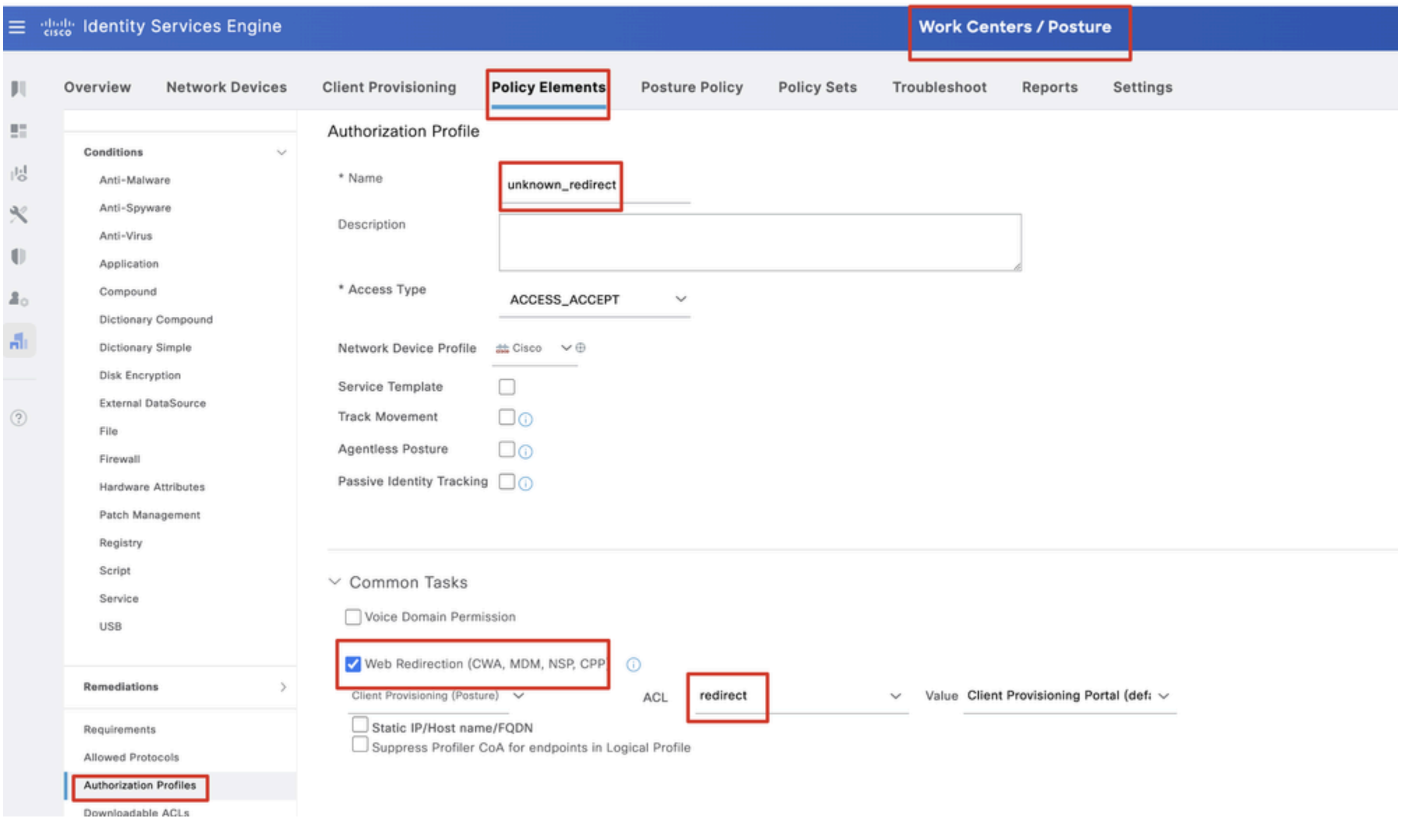
이름: unknown_redirect

의 확인란을 선택합니다. Web Redirection(CWA,MDM,NSP,CPP)

선택 Client Provisioning(Posture)

ACL: 리디렉션

값: Client Provisioning Portal(기본값)



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_Authorization_Profile_Redirect_1

참고: 이 ACL 이름 리디렉션은 FTD에 구성된 해당 ACL 이름과 일치해야 합니다.

21.2단계. 를 반복하여 Add 세부사항과 함께 규정준수 위반 및 규정준수 엔드포인트에 대한 또 다른 두 개의 권한 부여 프로파일을 생성합니다.

이름: non_compliant_profile

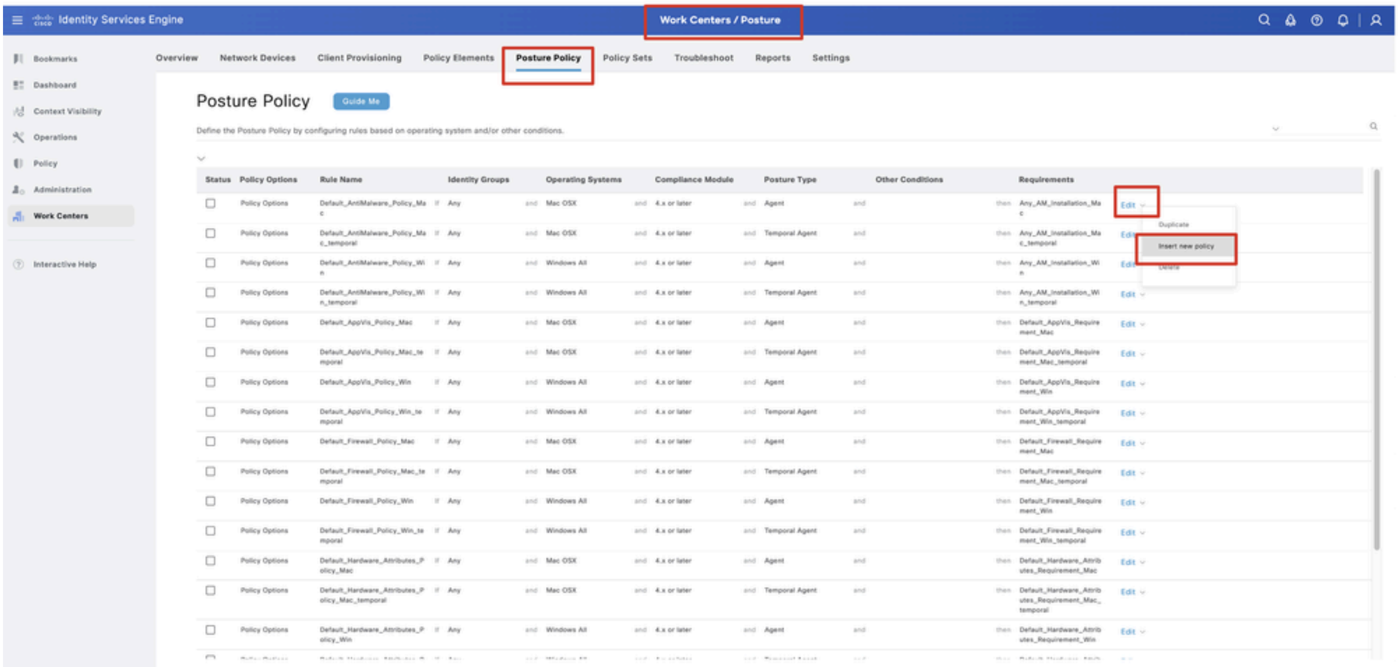
DACL 이름: DENY_ALL_IPv4_TRAFFIC

이름: compliant_profile

DACL 이름: PERMIT_ALL_IPv4_TRAFFIC

참고: 규정 준수 또는 비준수 엔드포인트에 대한 DACL은 실제 요구 사항에 따라 구성해야 합니다.

22단계. 로 Work Centers > Posture > Posture Policy 이동합니다. 규칙Edit 의 끝에 있는 을 클릭합니다. 를 Insert new policy선택합니다.



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

22.1단계. 세부 정보를 구성합니다.

규칙 이름: Demo_test_exist_linux

ID 그룹: 모두

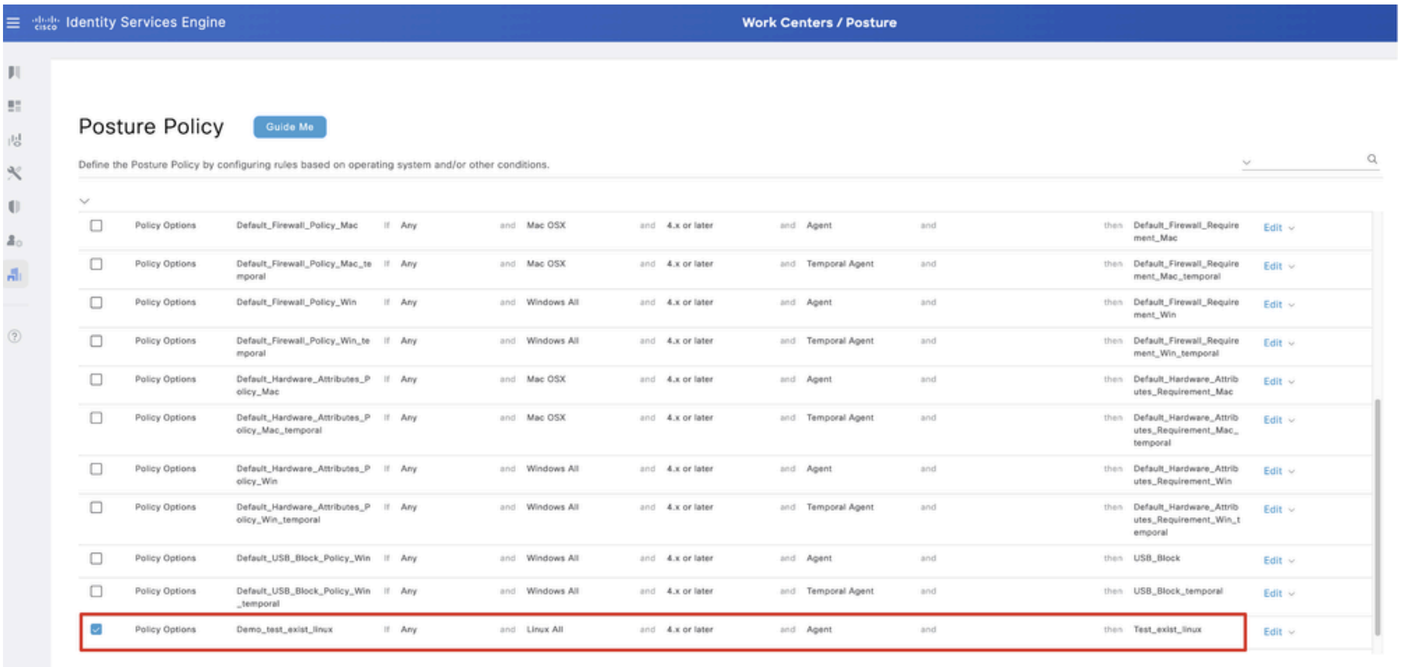
운영 체제: Linux All

Compliance Module: 4.x 이상

포스처 유형: 에이전트

요구 사항: Test_exist_linux

andDone 를 Save클릭합니다.



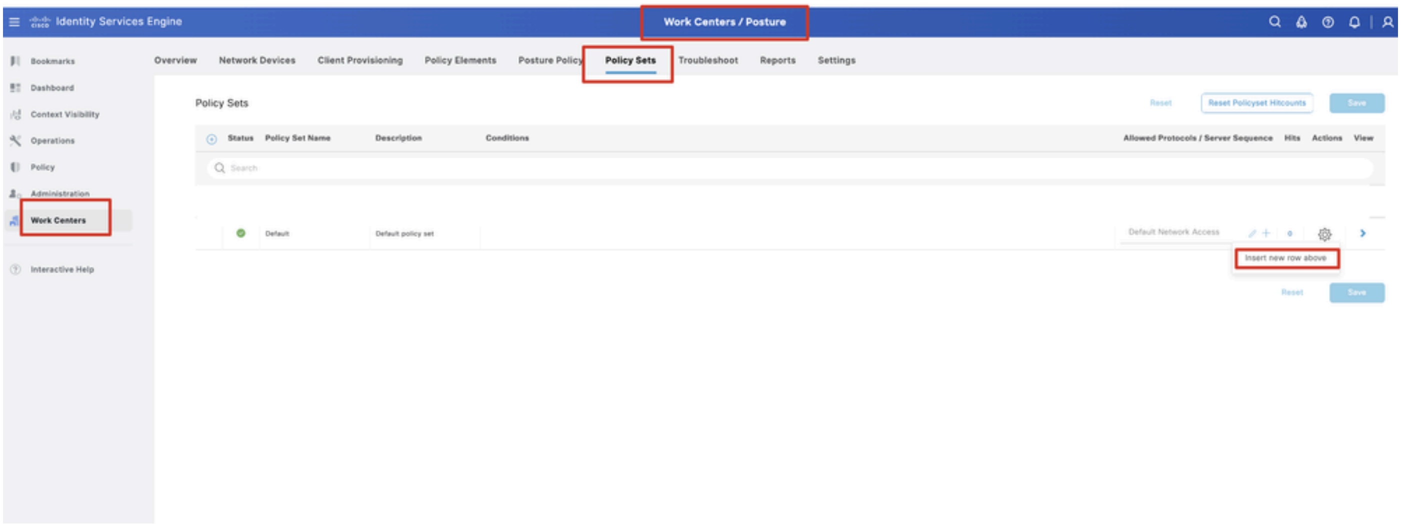
Posture Policy

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

23단계. 로 Work Centers > Posture > Policy Sets 이동합니다. 클릭하여 다음을 Insert new row above 수행합니다.



Policy Sets

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

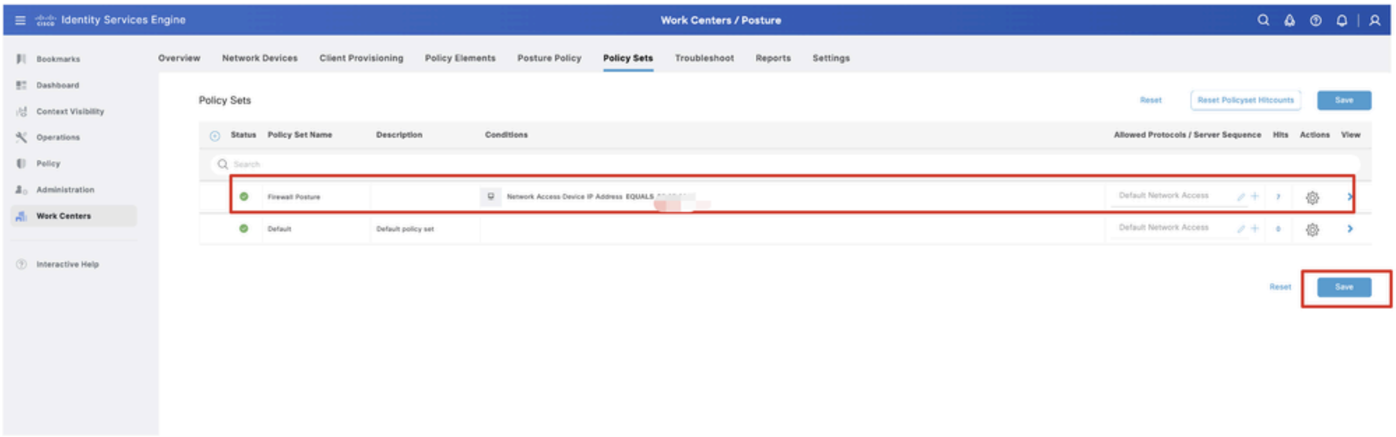
ISE_Add_New_Policy_Set

23.1단계. 세부 정보를 구성합니다.

정책 집합 이름: 방화벽 상태

조건: 네트워크 액세스 장치 IP 주소 EQUALs [FTD IP 주소]

를 클릭합니다 Save .



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		›

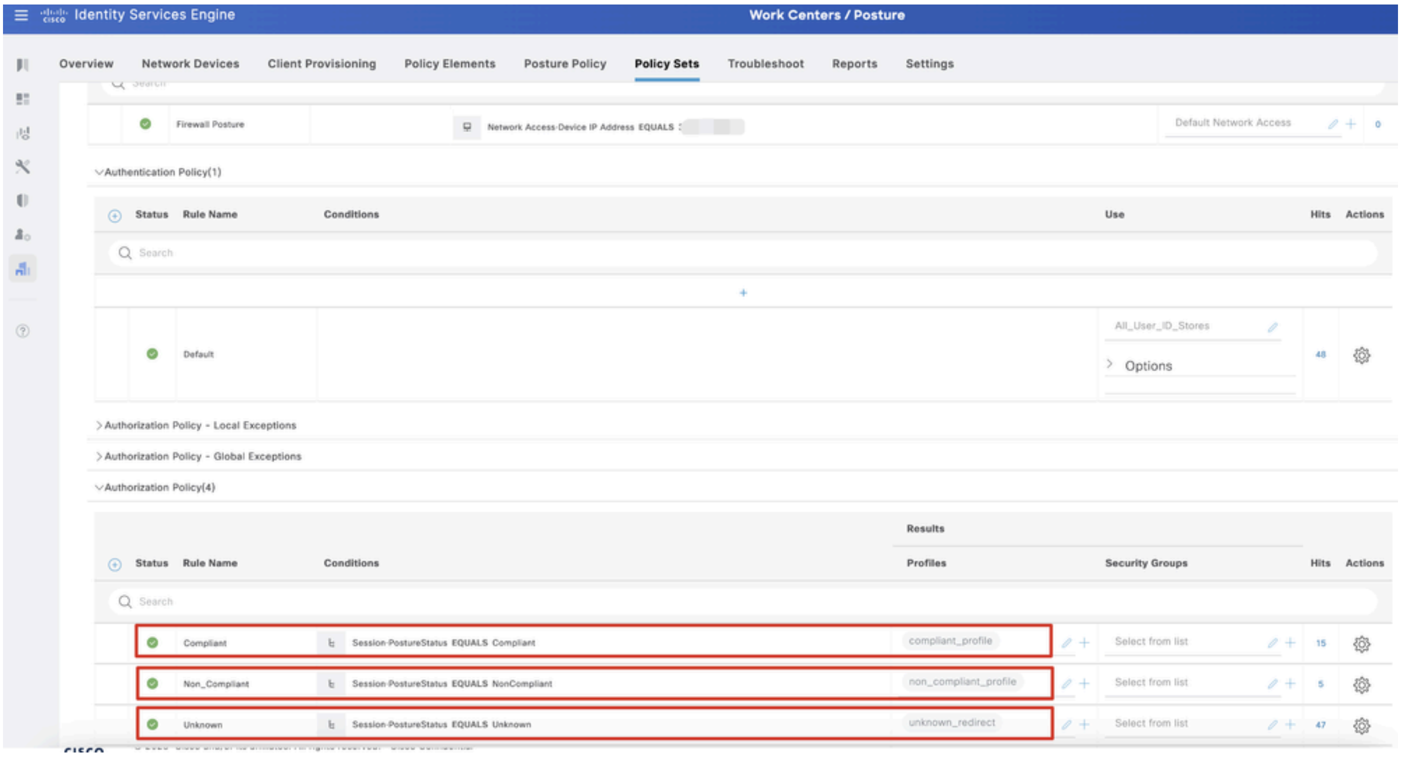
ISE_Add_New_Policy_Set_1

23.2단계. 정책 집합을 입력하려면 클릭하십시오>. 포스처 호환, 비호환, 알 수 없음 상태에 대한 새 권한 부여 규칙을 생성합니다. 를 Save 클릭합니다.

compliant_profile 준수

Non_compliant_profile 준수 안 됨

알 수 없음(unknown_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	48	

Authorization Policy - Local Exceptions

Authorization Policy - Global Exceptions

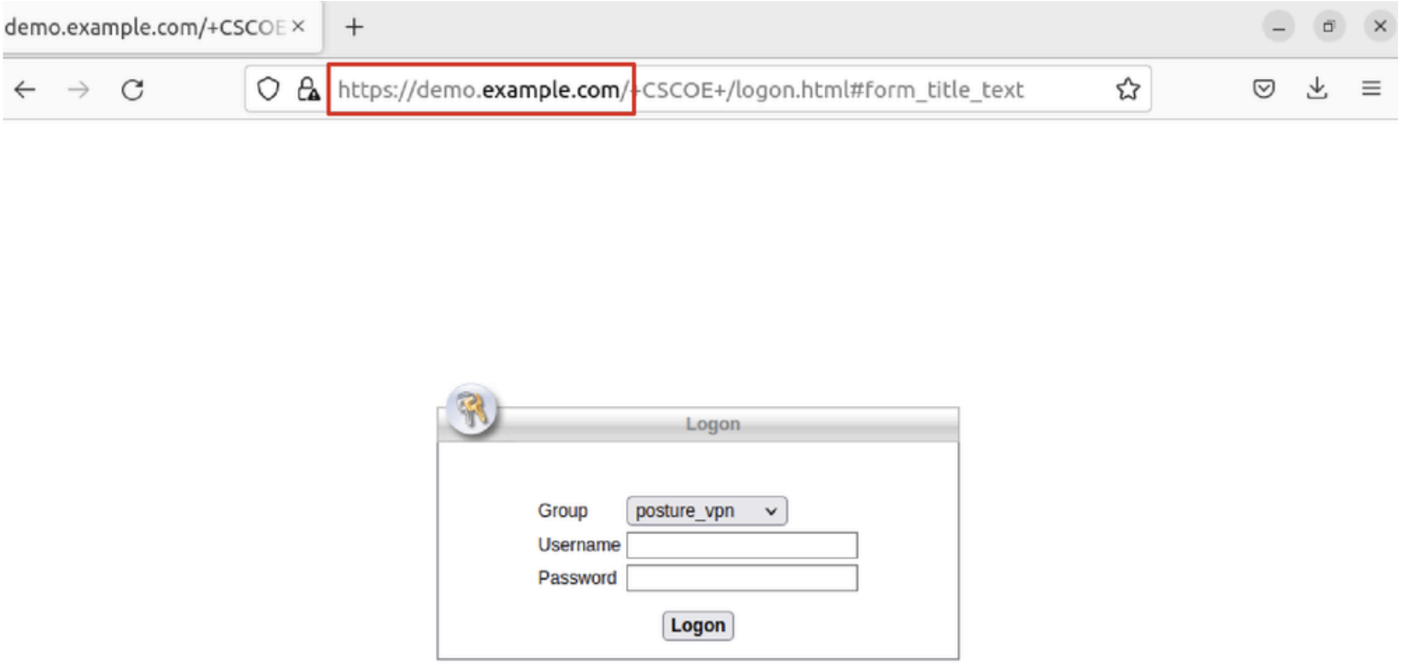
Authorization Policy(4)

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

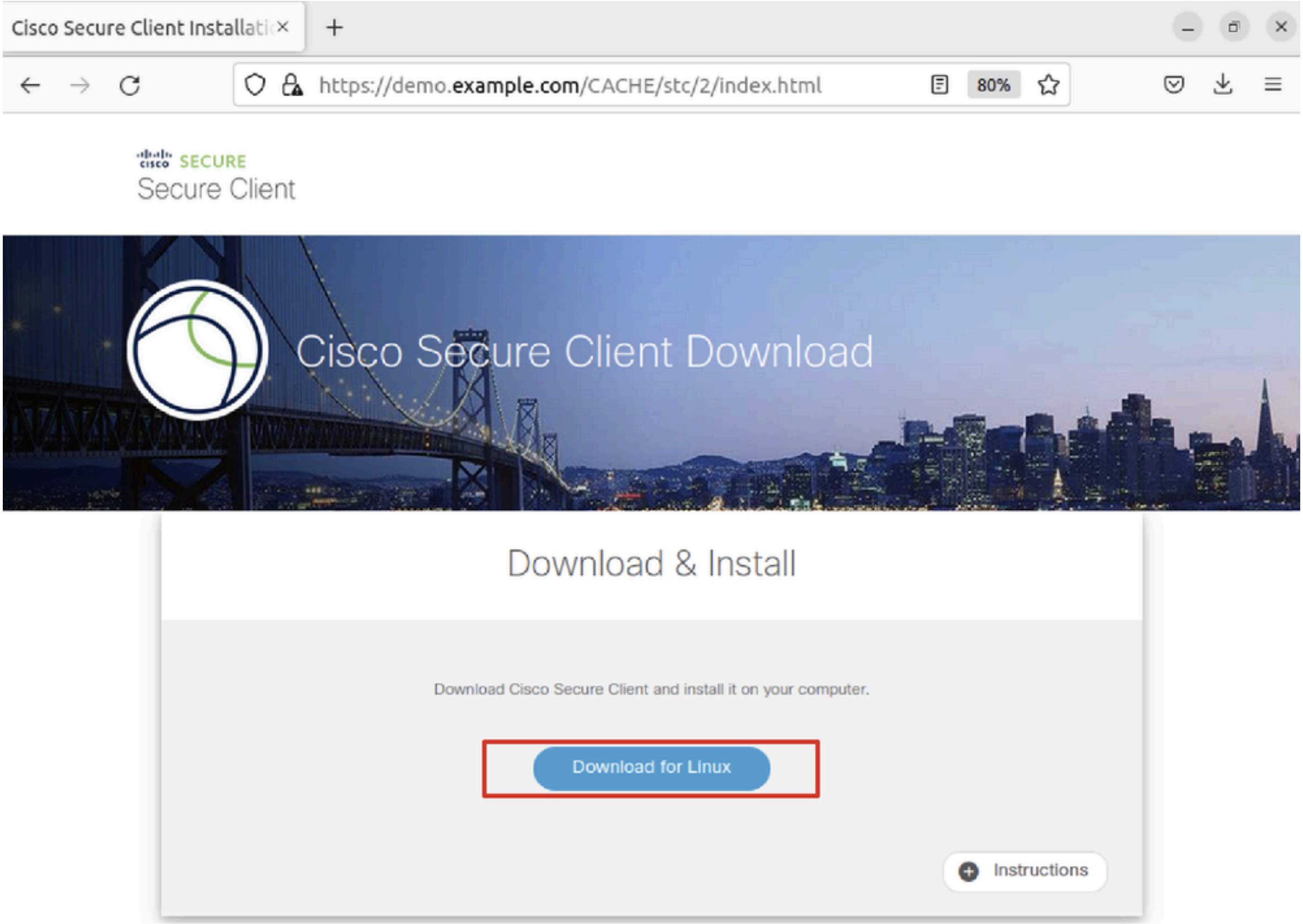
Ubuntu 구성

24단계. GUI를 통해 Ubuntu 클라이언트에 로그인합니다. VPN 포털에 로그인하려면 브라우저를 엽니다. 이 예에서는 demo.example.com입니다.



Ubuntu_Browser_VPN_Log

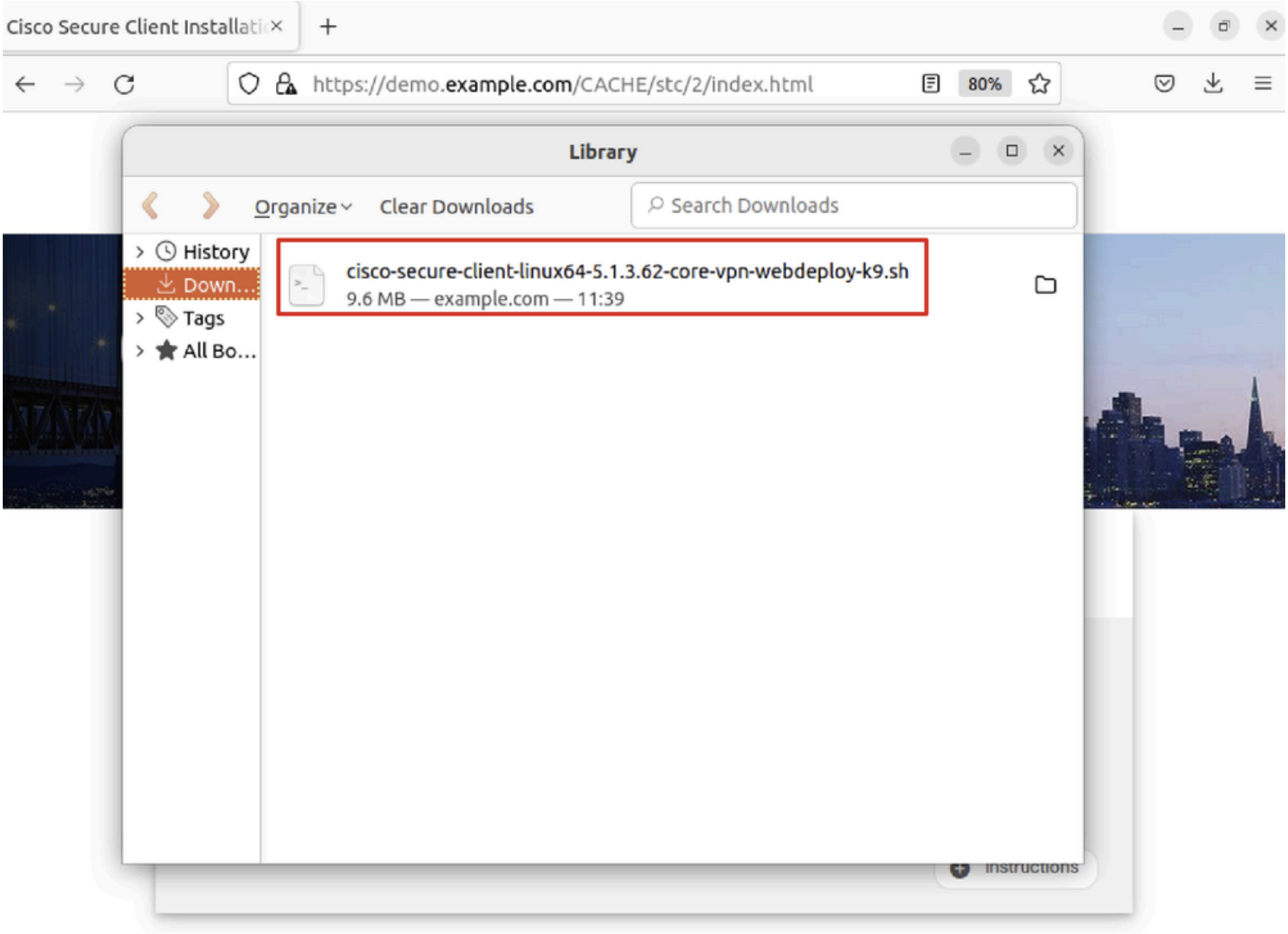
25단계. 를 Download for Linux 클릭합니다.



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

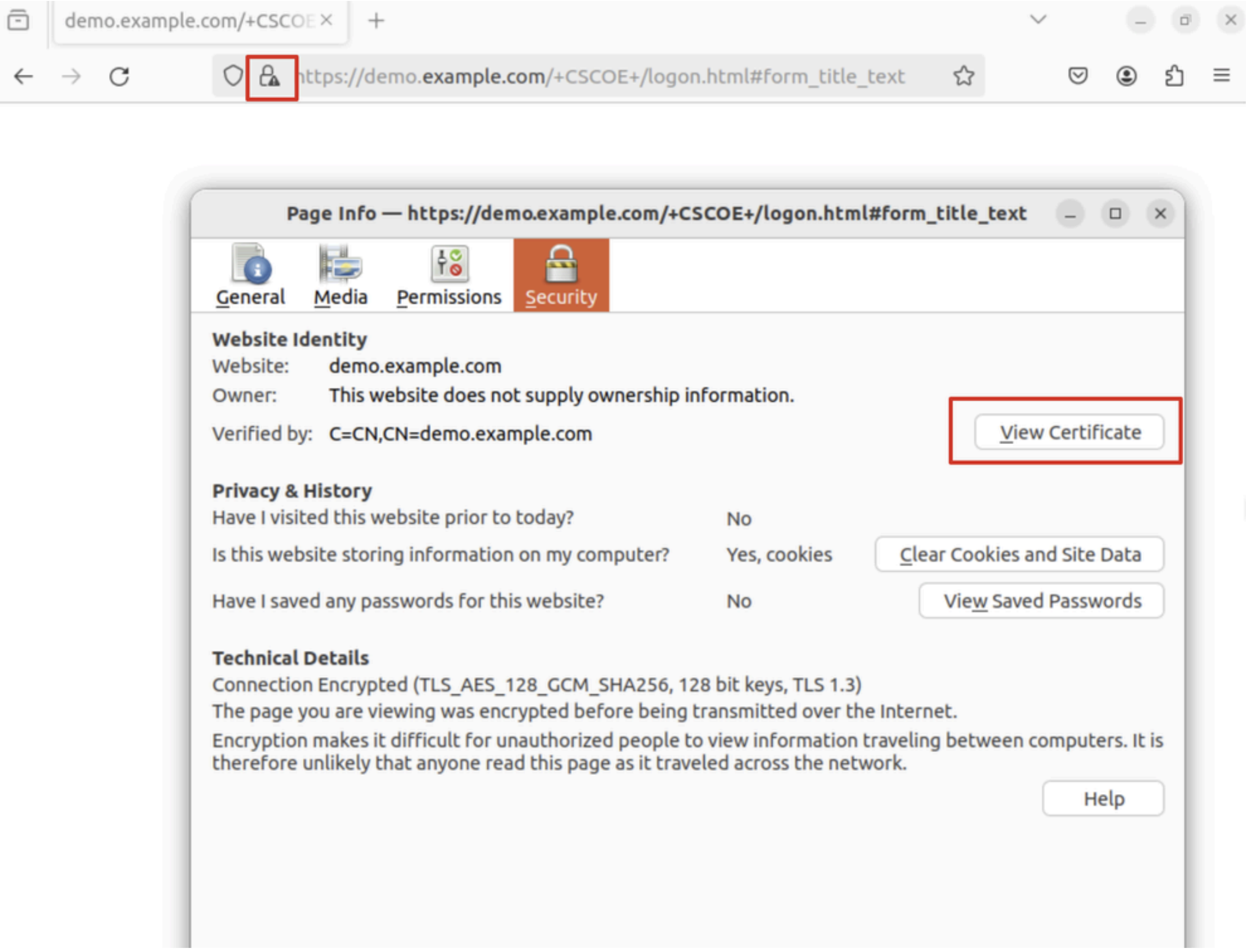
Ubuntu_Browser_VPN_Download_1

다운로드한 파일 이름은 입니다cisco-secure-client-linux64-5.1.3.62-core-vpn-webdeploy-k9.sh.


Cisco Secure Client Installati ×
https://demo.example.com/CACHE/stc/2/index.html
80%
Library
Organize
Clear Downloads
Search Downloads
History
Down…
Tags
All Bo…
cisco-secure-client-linux64-5.1.3.62-core-vpn-webdeploy-k9.sh
9.6 MB — example.com — 11:39
Instructions

Ubuntu_Browser_VPN_Download_2

26단계. 브라우저를 통해 VPN 인증서를 다운로드하고 파일 이름을 <certificate>로 변경합니다.crt. Firefox를 사용하여 인증서를 다운로드하는 예입니다.



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.

Untu_Browser_VPN_Cert_Download

27단계. Ubuntu 클라이언트에서 터미널을 엽니다. Cisco Secure Clientpath home/user/Downloads/를 설치하려면 로 이동합니다.

<#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$
```

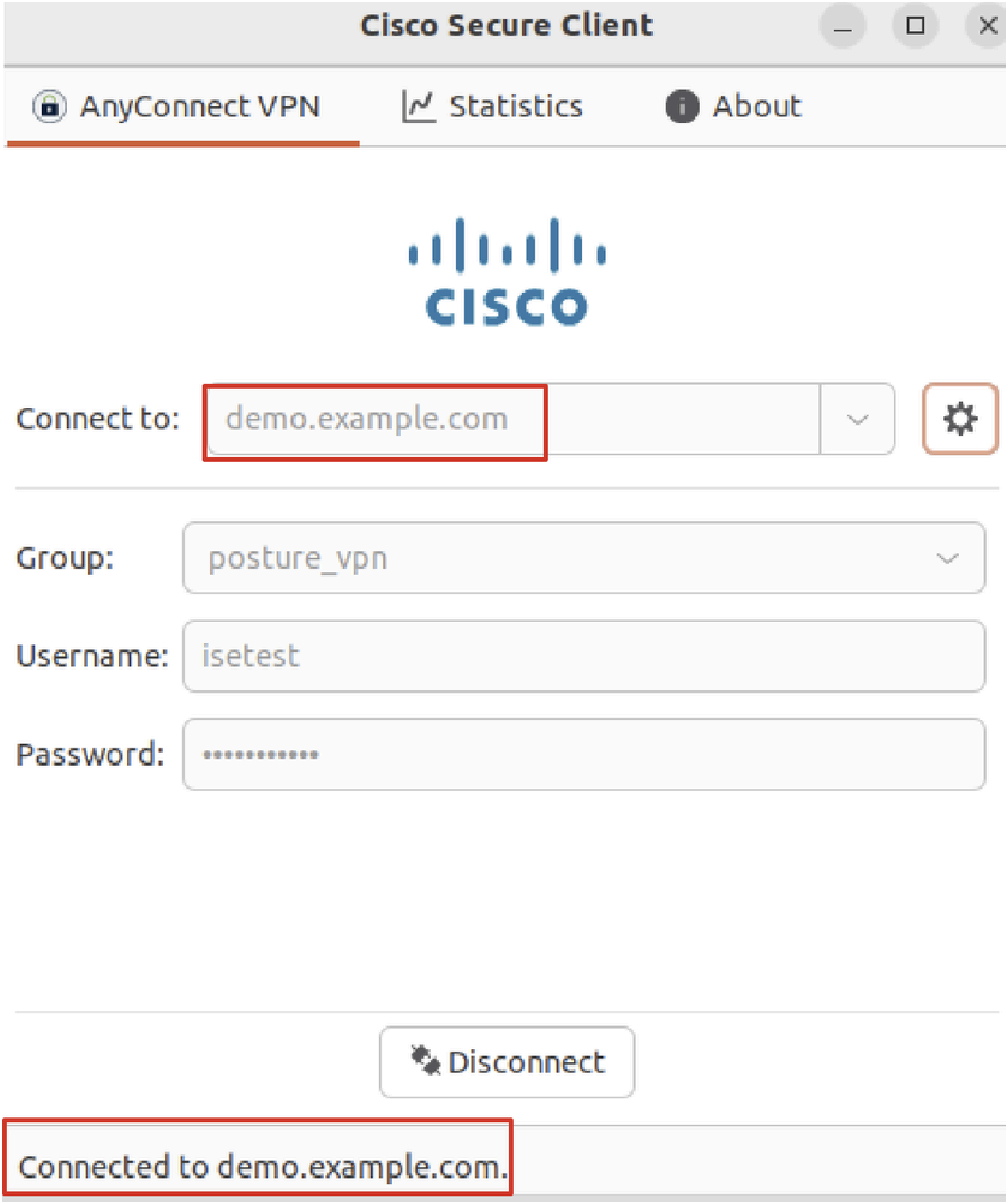
28단계. Ubuntu 클라이언트에서 VPN 포털 인증서를 신뢰합니다.

<#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
```

29단계. Ubuntu 클라이언트에서 Cisco Secure Client를 열고 VPN을 demo.example.com에 연결했습니다.



Cisco Secure Client

Connect to: demo.example.com

Group: posture_vpn

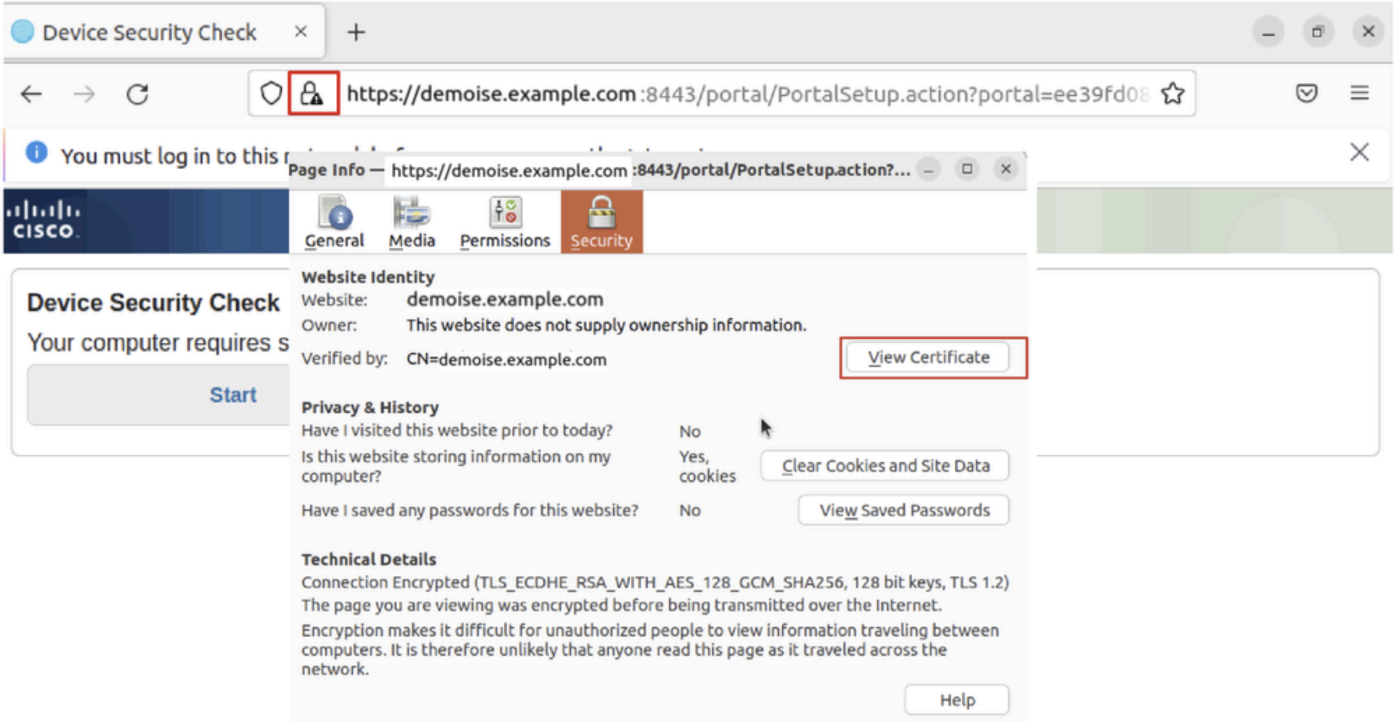
Username: isetest

Password: ••••••••••••

Connected to demo.example.com.

*Ubuntu_Secure_Client_*연결됨

30단계. 브라우저를 열어 ISE CPP 포털로의 리디렉션을 트리거하는 웹 사이트에 액세스합니다. ISE CPP 포털에서 인증서를 다운로드하고 파일 이름을 <certificate>.crt로 바꿉니다. 이는 Firefox를 사용하여 다운로드하는 예입니다.


Device Security Check

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

You must log in to this n

Device Security Check

Your computer requires s

Start

Page Info — https://demoise.example.com:8443/portal/PortalSetup.action?...

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_다운로드

30.1단계. Ubuntu 클라이언트에서 ISE CPP 포털 인증서를 신뢰합니다.

<#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$
```

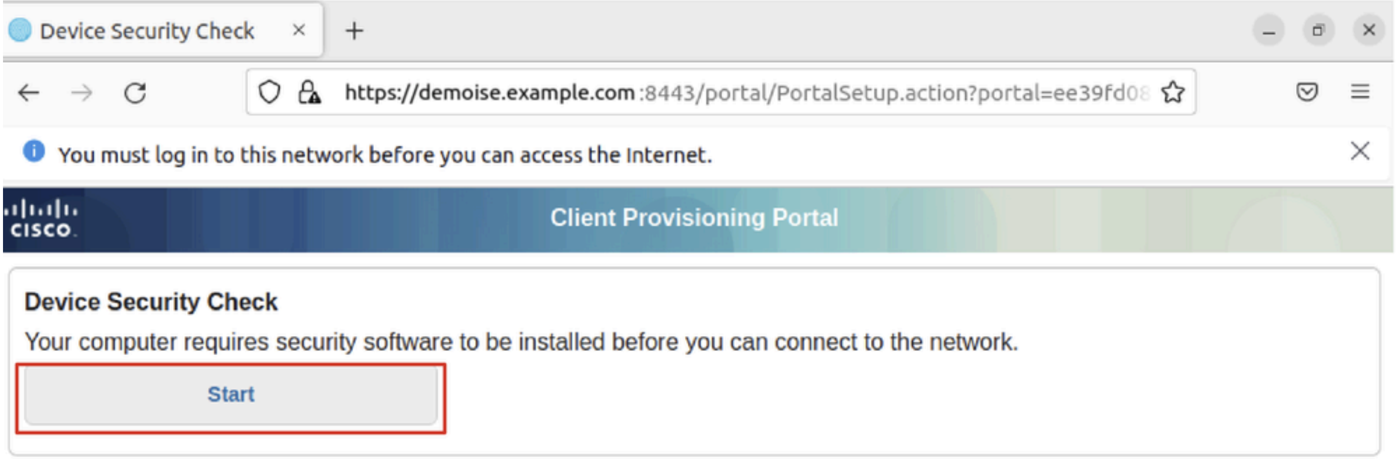
```
sudo update-ca-certificates
```

```
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.
```

31단계. ISE Start CPP 포털을 클릭합니다.


Device Security Check
https://demoise.example.com:8443/portal/PortalSetup.action?portal=ee39fd08
cisco
Client Provisioning Portal
Start

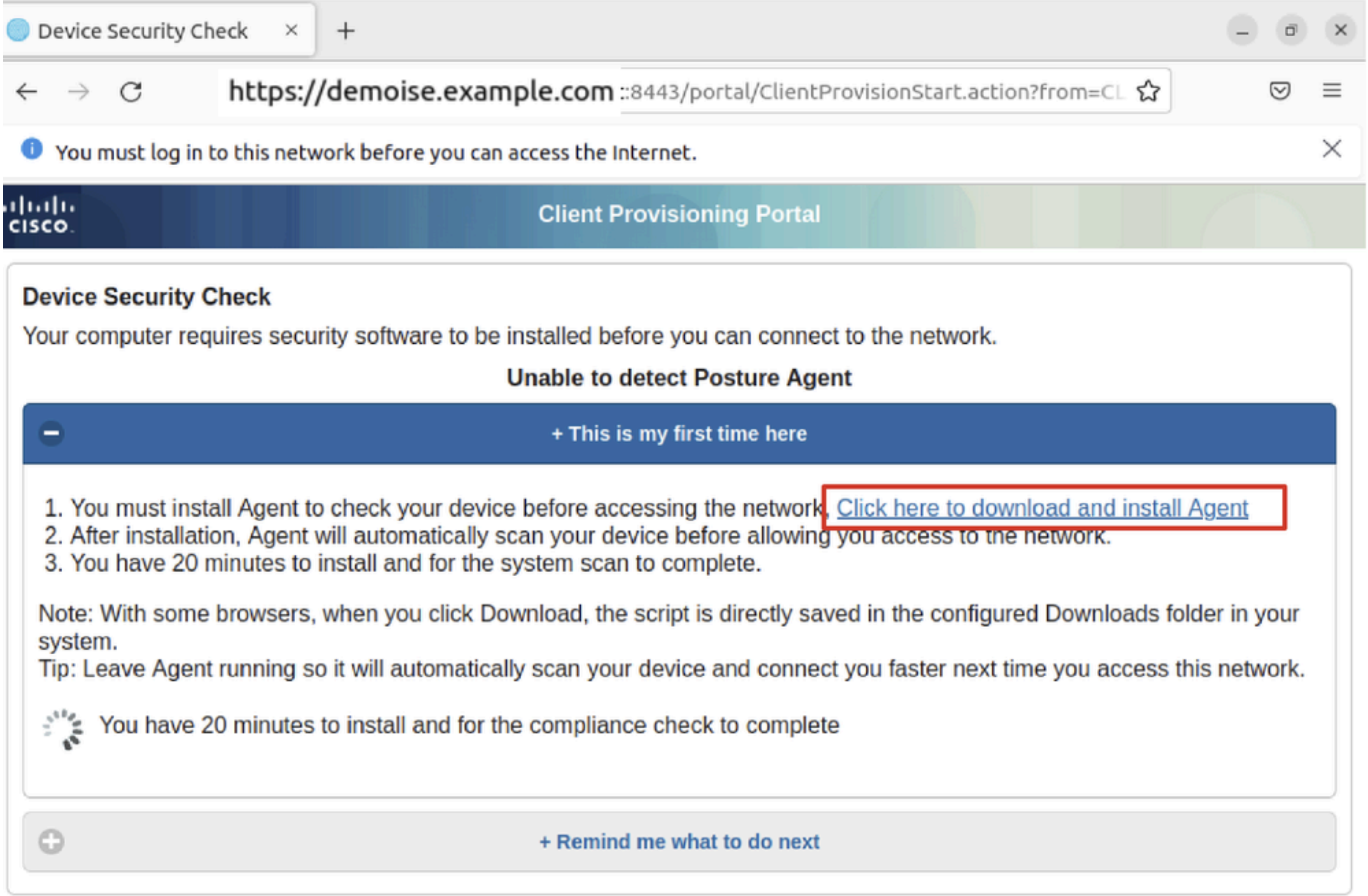
You must log in to this network before you can access the Internet.

Device Security Check

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

Ubuntu_Browser_CPP_시작

32단계. Click here to download and install Agent.


Device Security Check
https://demoise.example.com:8443/portal/ClientProvisionStart.action?from=CL
cisco
Client Provisioning Portal
+ This is my first time here
+ Remind me what to do next

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

Device Security Check

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

Unable to detect Posture Agent

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

Ubuntu_Browser_CPP_Download_Posture

33단계. Ubuntu 클라이언트에서 터미널을 엽니다. Posture 모듈을 home/user/Downloads/ 설치하기 위한 경로로 이동합니다.

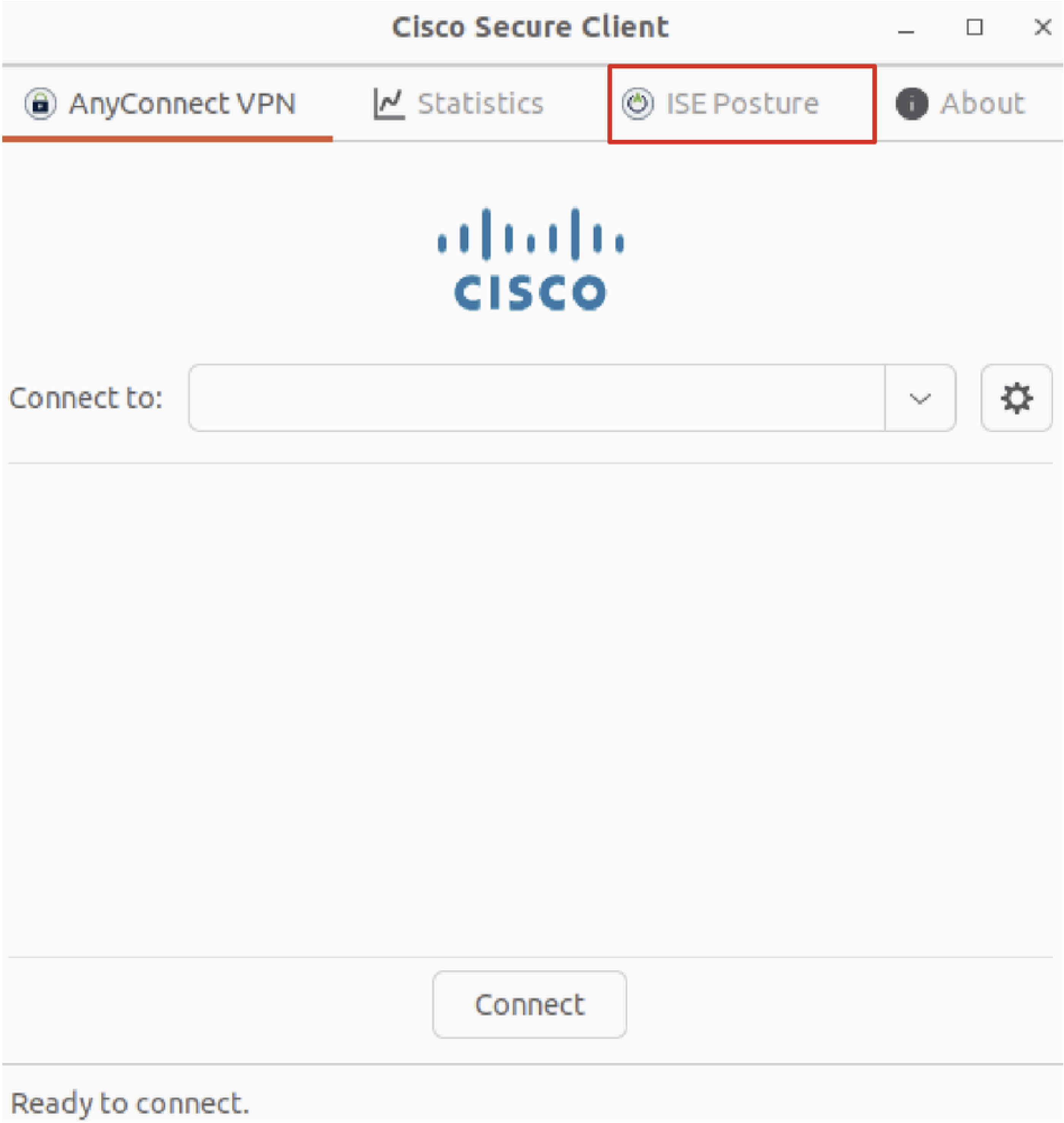
<#root>

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.
```

34단계. Ubuntu 클라이언트 UI에서 Cisco Secure Client를 종료하고 다시 엽니다. ISE Posture 모듈이 설치되고 성공적으로 실행됩니다.



Ubuntu_Secure_Client_ISE_Posture_Installed

35단계. Ubuntu 클라이언트에서 터미널을 엽니다. 경로home/user/Desktop로 이동하여 ISE에test.txt 구성된 파일 조건을 충족하도록 파일을 생성합니다.

<#root>

user@ubuntu22-desktop:~$

```
cd Desktop/
```

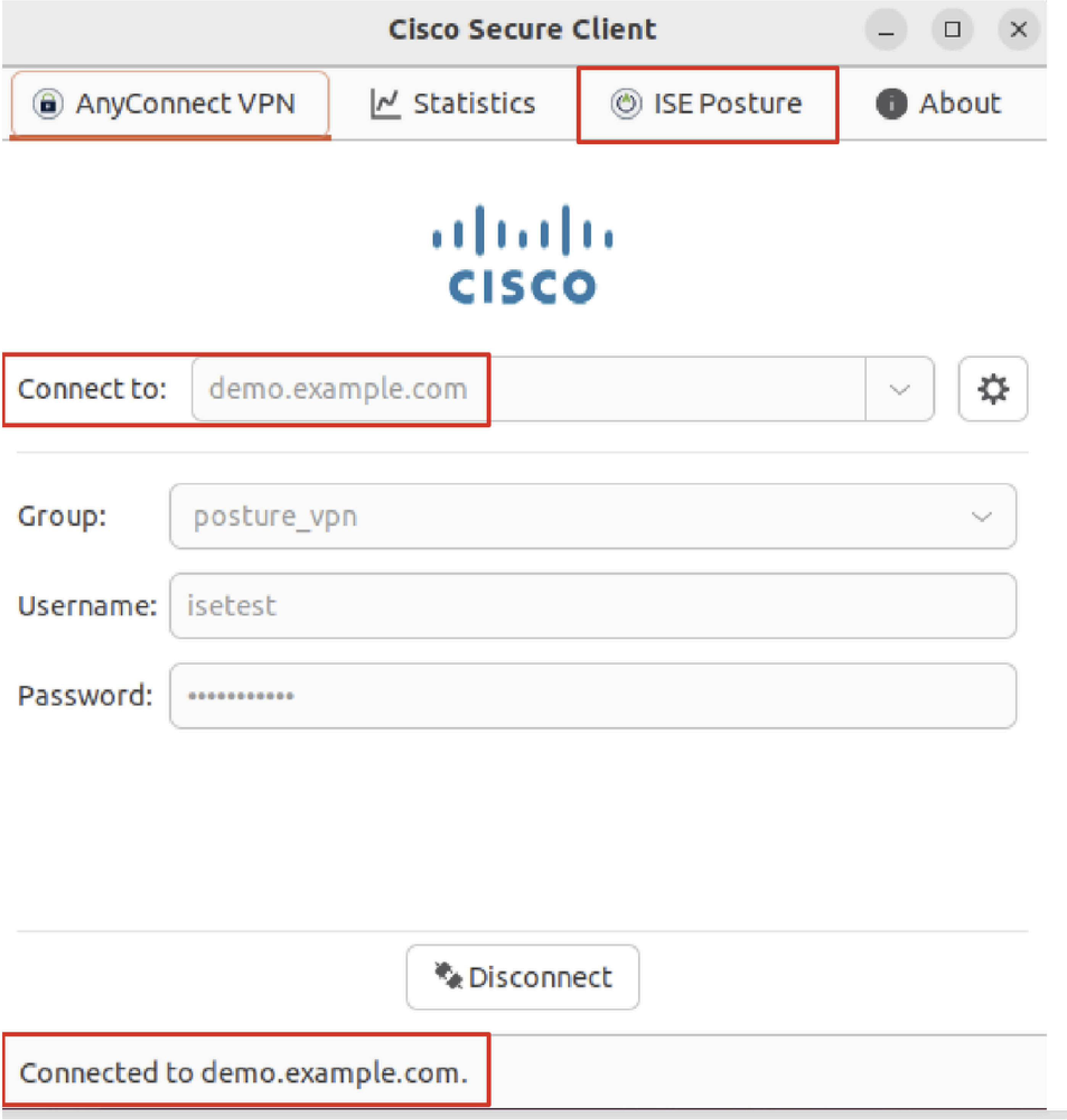
```
user@ubuntu22-desktop:~/Desktop$
```

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

다음을 확인합니다.

구성이 올바르게 작동하는지 확인하려면 이 섹션을 활용하십시오.

1단계. Ubuntu 클라이언트에서 VPN을 demo.example.com에 연결합니다.



Connect to: demo.example.com

Group: posture_vpn

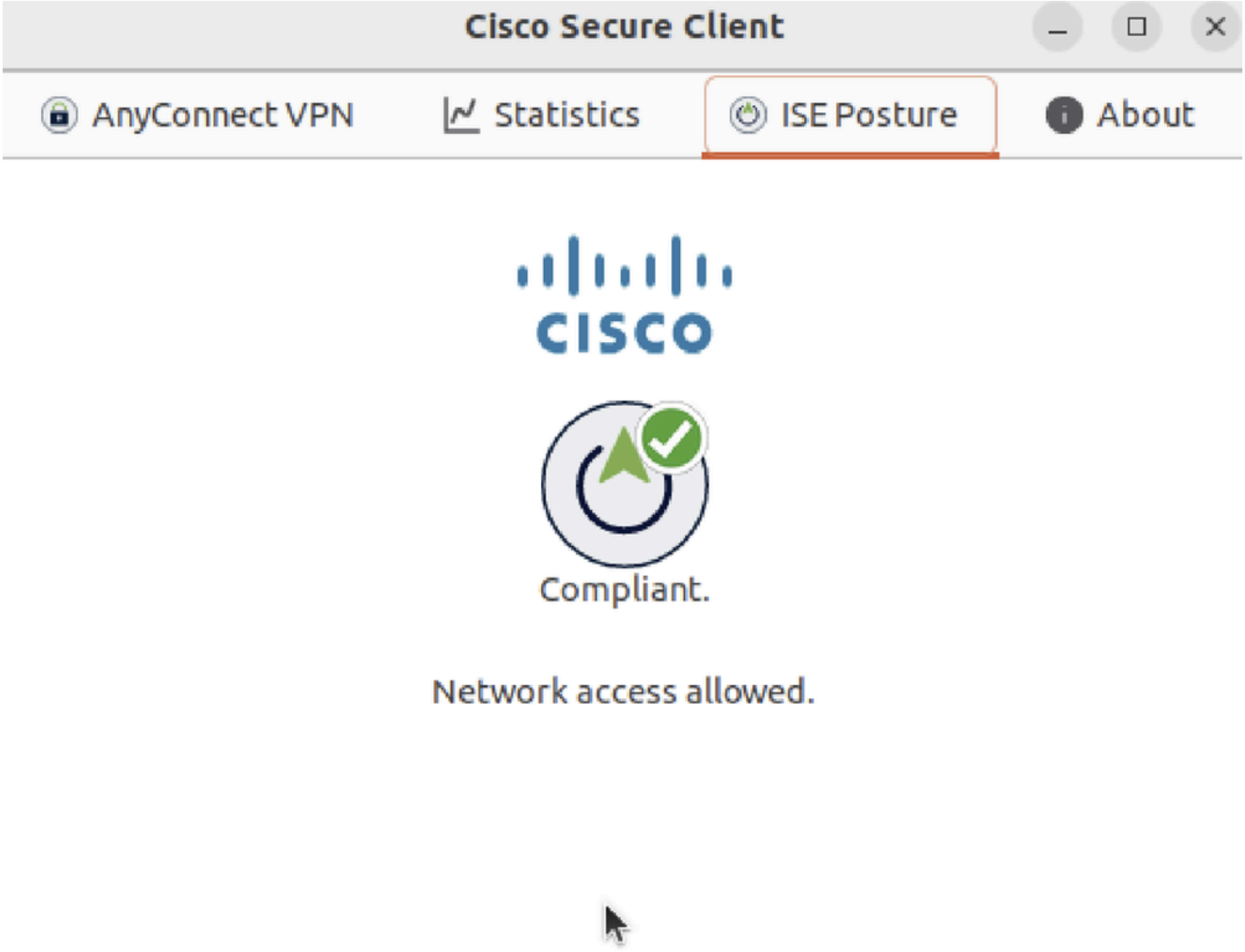
Username: isetest

Password: ••••••••••••

Connected to demo.example.com.

Verify_Ubuntu_Secure_Client_Connected

2단계. Ubuntu 클라이언트에서 ISE Posture 상태를 확인합니다.

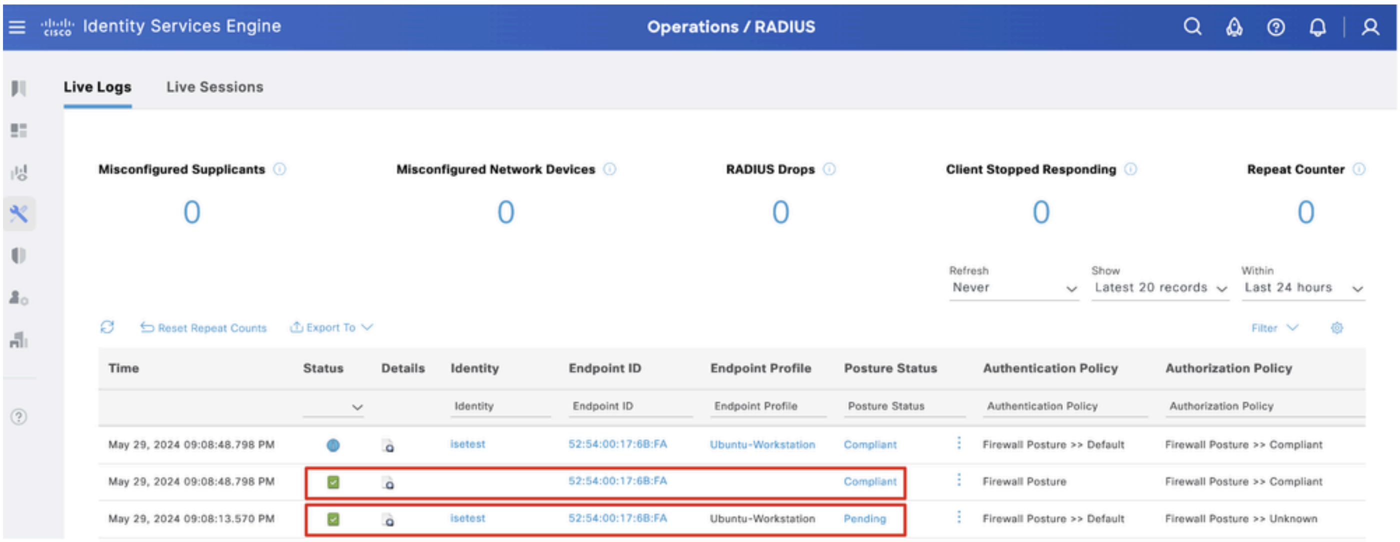


Compliant.

Network access allowed.

Verify_Ubuntu_Secure_Client_Compliance

3단계. ISE에서 Radius Live Log(RADIUS 라이브 로그)를 선택합니다. 로 Operations > RADIUS Live Log 이동합니다.



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

4단계. SSH 또는 콘솔을 통해 FTD CLI로 이동합니다.

<#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 : cb0071820002100066659d871
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
```

문제 해결

이 섹션에서는 설정 문제 해결을 위해 사용할 수 있는 정보를 제공합니다.

Cisco Secure Client 및 ISE의 상태 흐름 및 문제 해결에 대해서는 CCO **문서ISE Posture Style Comparison for Pre and Post 2.2** and Troubleshoot **ISE Session Management and Posture를 참조하십시오.**

관련 정보

- Cisco Identity Services Engine 네트워크 구성 요소 호환성, 릴리스 3.3

- Cisco Identity Services Engine 관리자 가이드, 릴리스 3.3
- **Cisco 기술 지원 및 다운로드**

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.