Configure Linux VPN Posture with ISE 3.3

Contents

Introduction

This document describes how to configure Linux VPN posture with Identity Services Engine (ISE) and Firepower Threat Defense (FTD).

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Secure Client
- Remote Access VPN on Firepower Threat Defense (FTD)
- Identity Services Engine (ISE)

Components Used

The information in this document is based on these software versions:

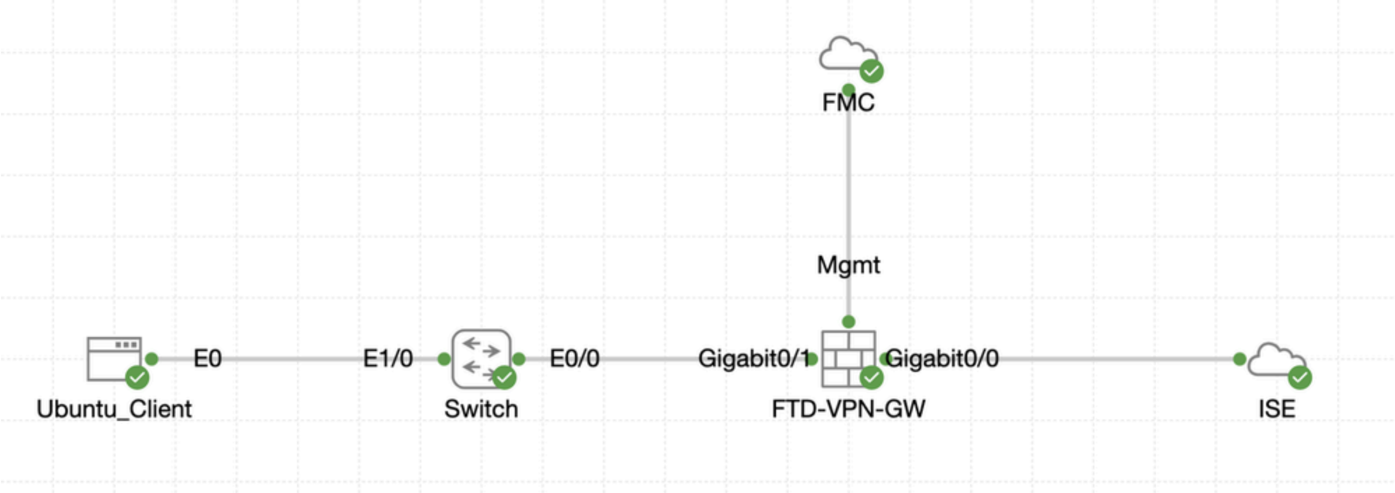
- Ubuntu 22.04
- Cisco Secure Client 5.1.3.62

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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Configure

Network Diagram



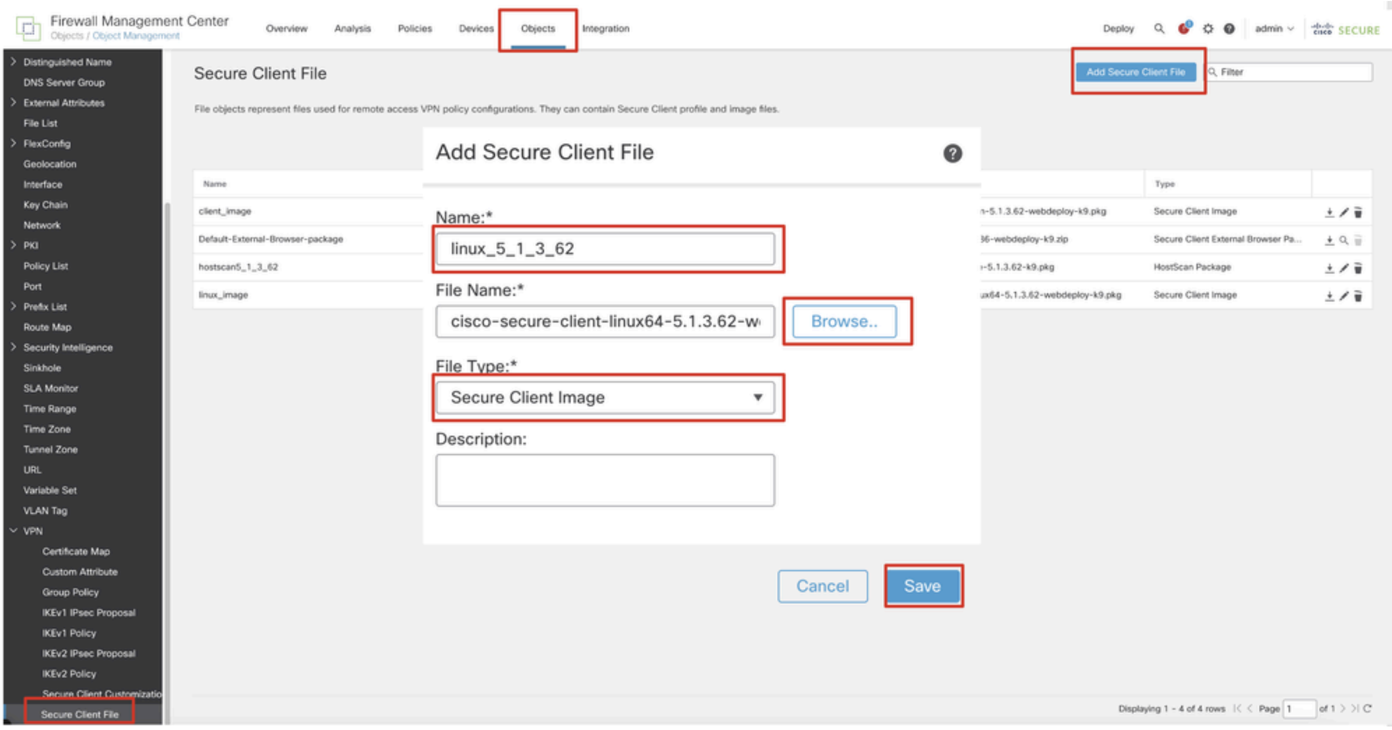
Topology

Configurations on FMC/FTD

Step 1. Connectivity among the client, FTD, FMC, and ISE has been successfully configured. As enroll.cisco.com is used for endpoints doing probe for redirection (refer to posture flow CCO documentsISE Posture Style Comparison for Pre and Post 2.2 for details). Ensure the route for traffic to enroll.cisco.com on FTD is configured correctly.

Step 2. Download the package name cisco-secure-client-linux64-5.1.3.62-webdeploy-k9.pkg from Cisco Software Download and ensure the file is good after download by confirming md5 checksum of the downloaded file is the same as the Cisco Software Download page.

Step 3. Navigate to Objects > Object Management > VPN > Secure Client File. Click Add Secure Client File, provide the name, browse File Name to select cisco-secure-client-linux64-5.1.3.62-webdeploy-k9.pkg, select Secure Client Image in File Type drop-down list. Then click Save.



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

Add Secure Client File

Name:* linux_5_1_3_62

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

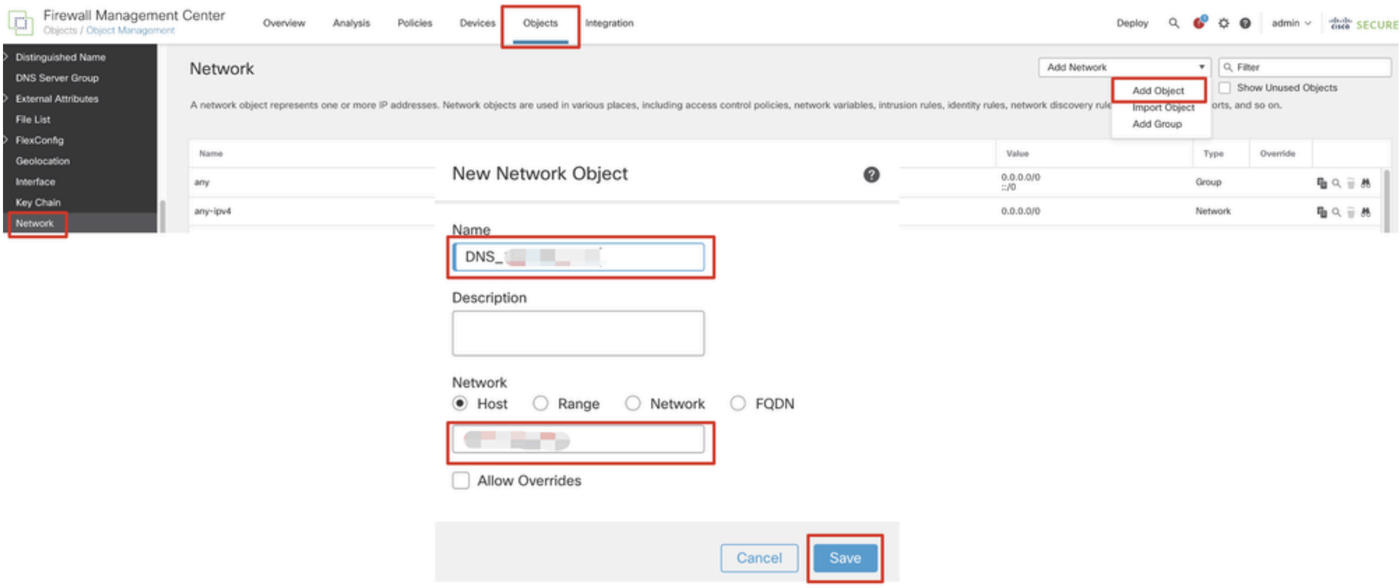
File Type:* Secure Client Image

Description:

FMC_Upload_Secure_Client_Image

Step 4. Navigate to Objects > Object Management > Network.

Step 4.1. Create an object for the DNS server. Click Add Object, provide the name and available DNS IP address. Click Save.



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

New Network Object

Name DNS_[redacted]

Description

Network
● Host ○ Range ○ Network ○ FQDN

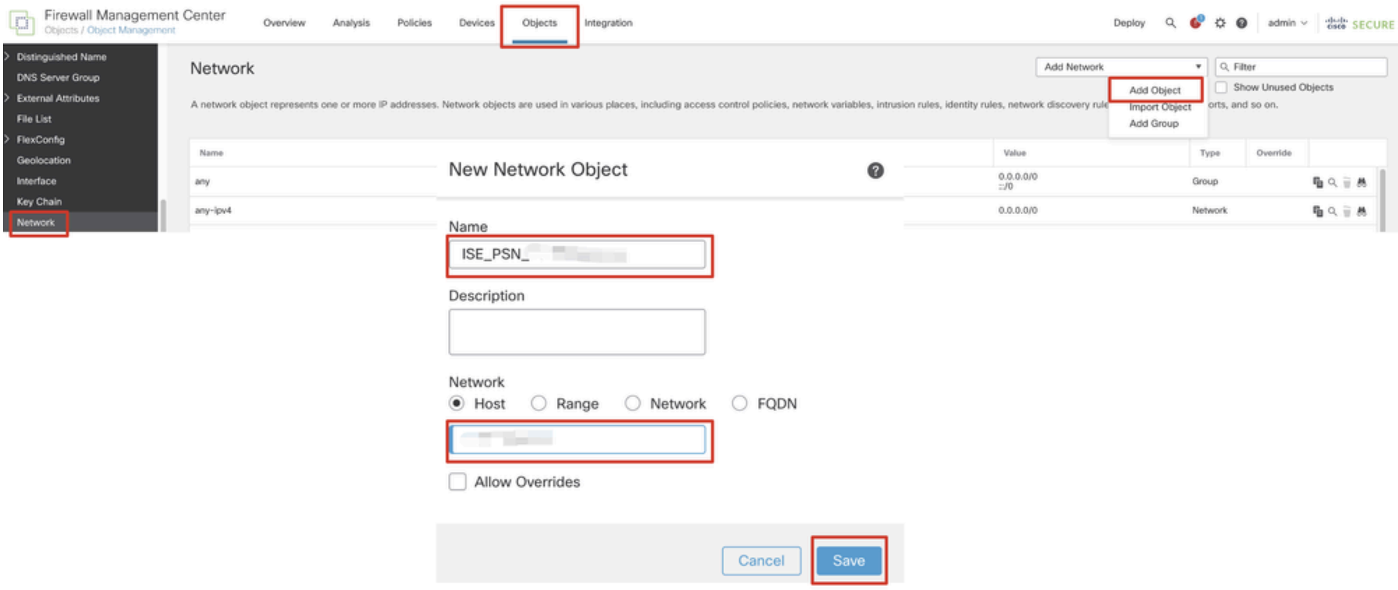
[redacted]

□ Allow Overrides

FMC_Add_Object_DNS

Note: DNS server configured here is to be used for VPN users.

Step 4.2. Create an object for ISE PSN. Click Add Object, provide the name and available ISE PSN IP address. Click Save.



New Network Object

Name: ISE_PSN_[redacted]

Description:

Network: ● Host ○ Range ○ Network ○ FQDN

[redacted]

□ Allow Overrides

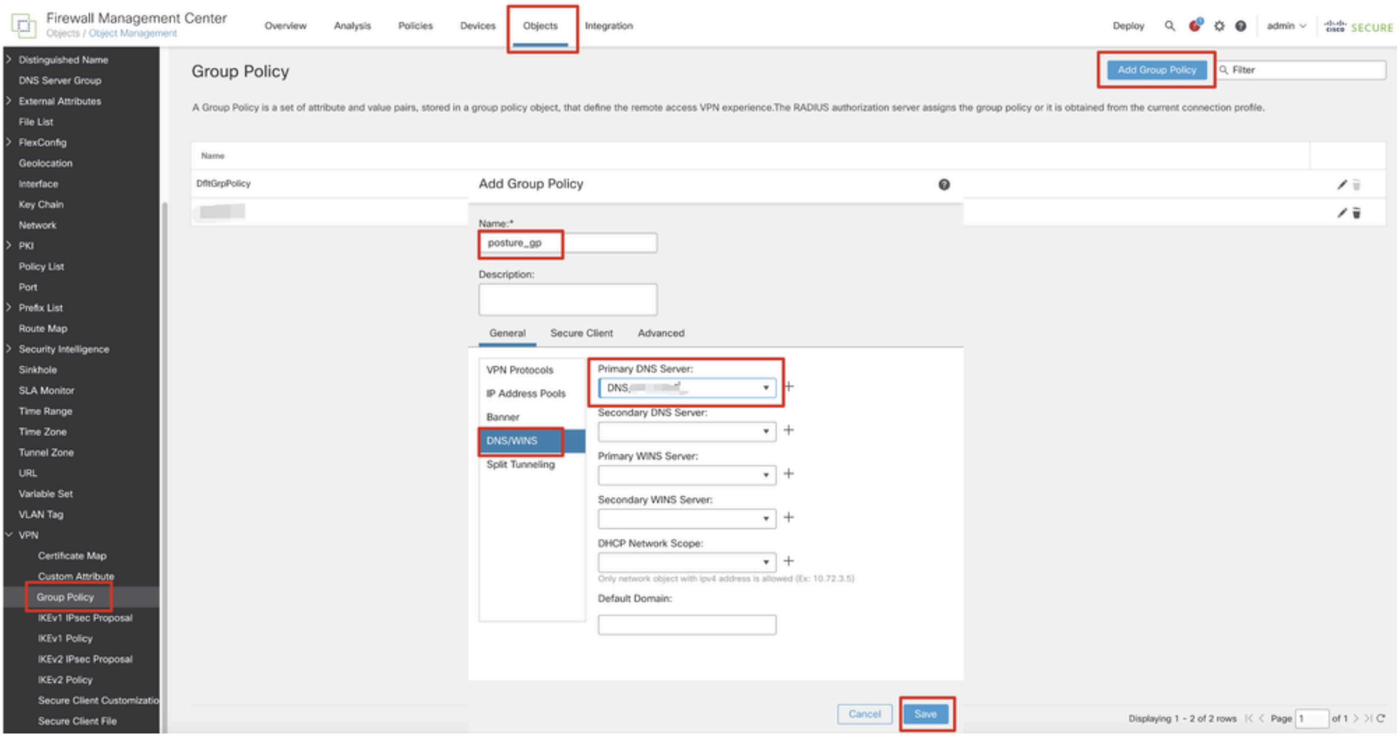
Network

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	

FMC_Add_Object_ISE

Step 5. Navigate to Objects > Object Management > VPN > Group Policy. Click Add Group Policy. Click DNS/WINS, select the object of the DNS server in Primary DNS Server. Then click 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:

General | Secure Client | Advanced

DNS/WINS

Primary DNS Server: DNS_[redacted]

Secondary DNS Server:

Primary WINS Server:

Secondary WINS Server:

DHCP Network Scope:

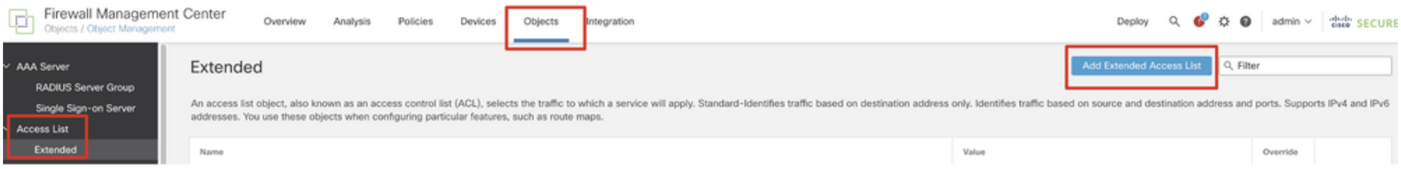
Only network object with ipv4 address is allowed (Ex: 10.72.3.5)

Default Domain:

FMC_Add_Group_Policy

Note: Ensure the DNS server used in the VPN group policy can resolve ISE client provisioning portal FQDN and enroll.cisco.com.

Step 6. Navigate to Objects > Object Management > Access List > Extended. Click Add Extended Access List.

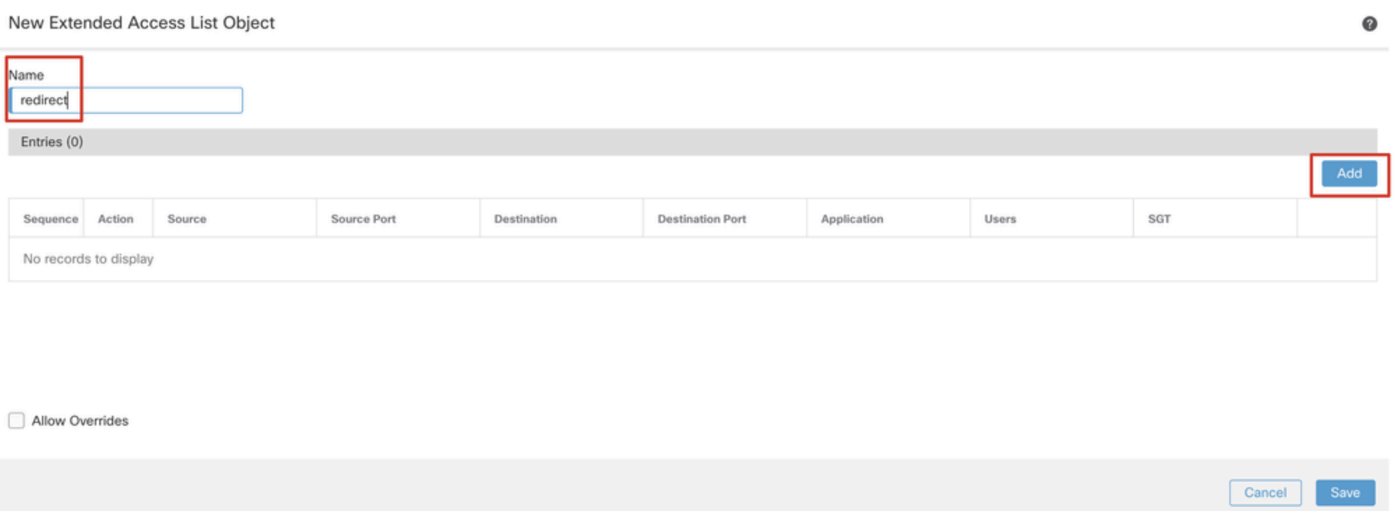


Extended

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

Step 6.1. Provide the name of the redirect ACL. This name must be the same as in the ISE authorization profile. Click Add.



New Extended Access List Object

Name: redirect

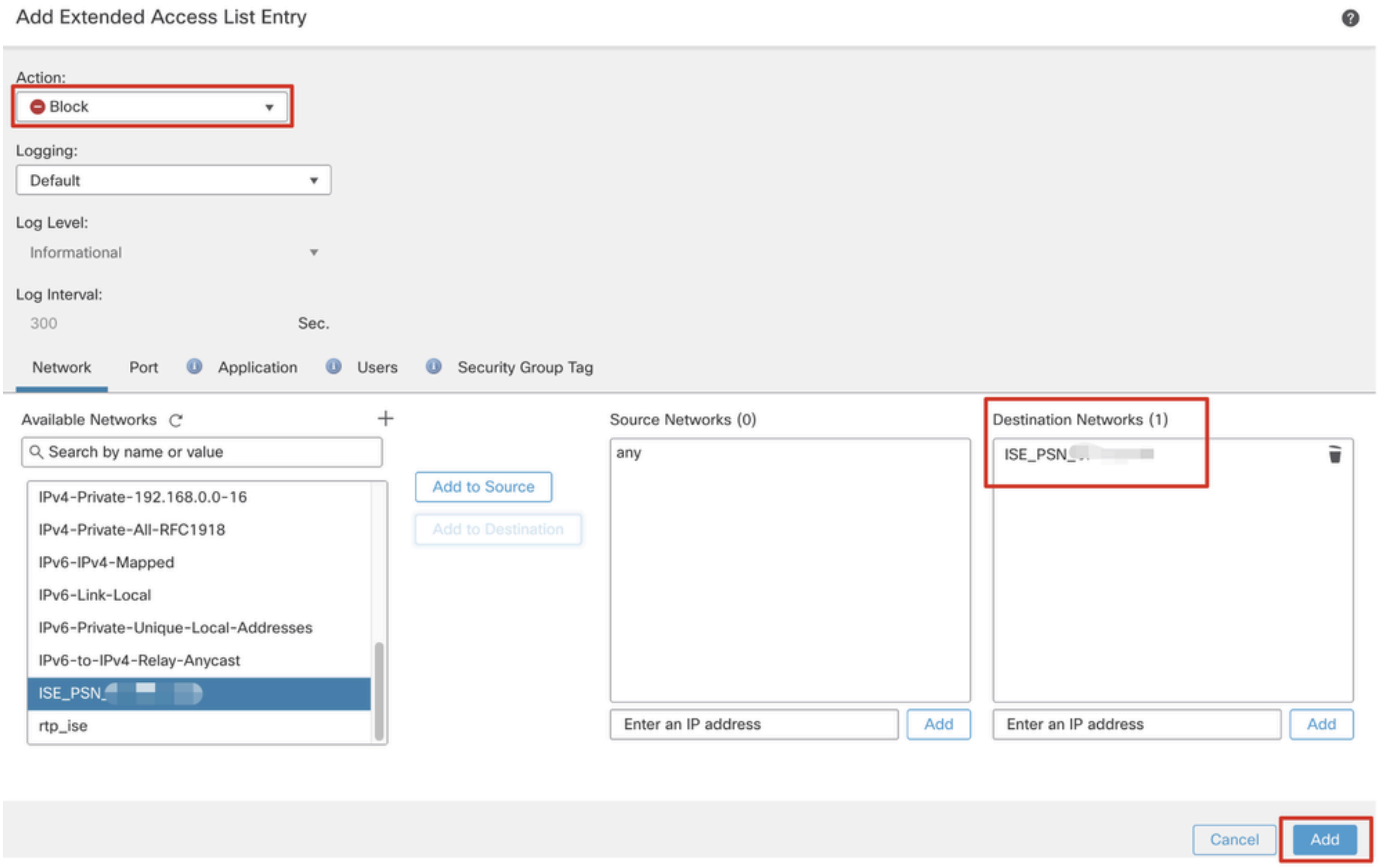
Entries (0)

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

□ Allow Overrides

FMC_Add_Redirect_ACL_Part_1

Step 6.2. Block DNS traffic, traffic to ISE PSN IP address, and the remediation servers to exclude them from redirection. Allow the rest of the traffic. This triggers redirection. Click `Save`.



Add Extended Access List Entry

Action: Block

Logging: Default

Log Level: Informational

Log Interval: 300 Sec.

Available Networks

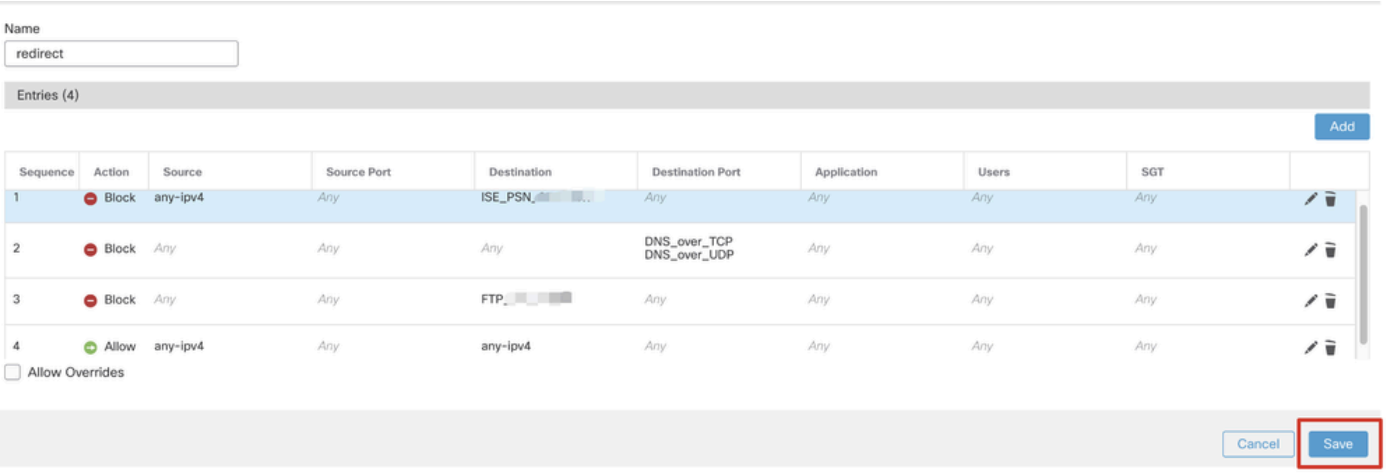
Search by name or value

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

Source Networks (0): any

Destination Networks (1): ISE_PSN_[redacted]

FMC_Add_Redirect_ACL_Part_2


Name

redirect

Entries (4)

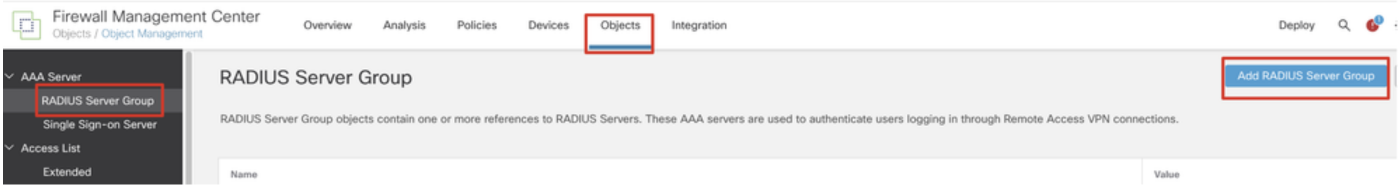
Sequence	Action	Source	Source Port	Destination	Destination Port	Application	Users	SGT
1	● Block	any-ipv4	Any	ISE_PSN_[redacted]	Any	Any	Any	Any
2	● Block	Any	Any	Any	DNS_over_TCP DNS_over_UDP	Any	Any	Any
3	● Block	Any	Any	FTP_[redacted]	Any	Any	Any	Any
4	● Allow	any-ipv4	Any	any-ipv4	Any	Any	Any	Any

□ Allow Overrides

FMC_Add_Redirect_ACL_Part_3

Note: Destination FTP in this redirect ACL example is used as the remediation server example.

Step 7. Navigate to Objects > Object Management > RADIUS Server Group. Click Add RADIUS Server Group.



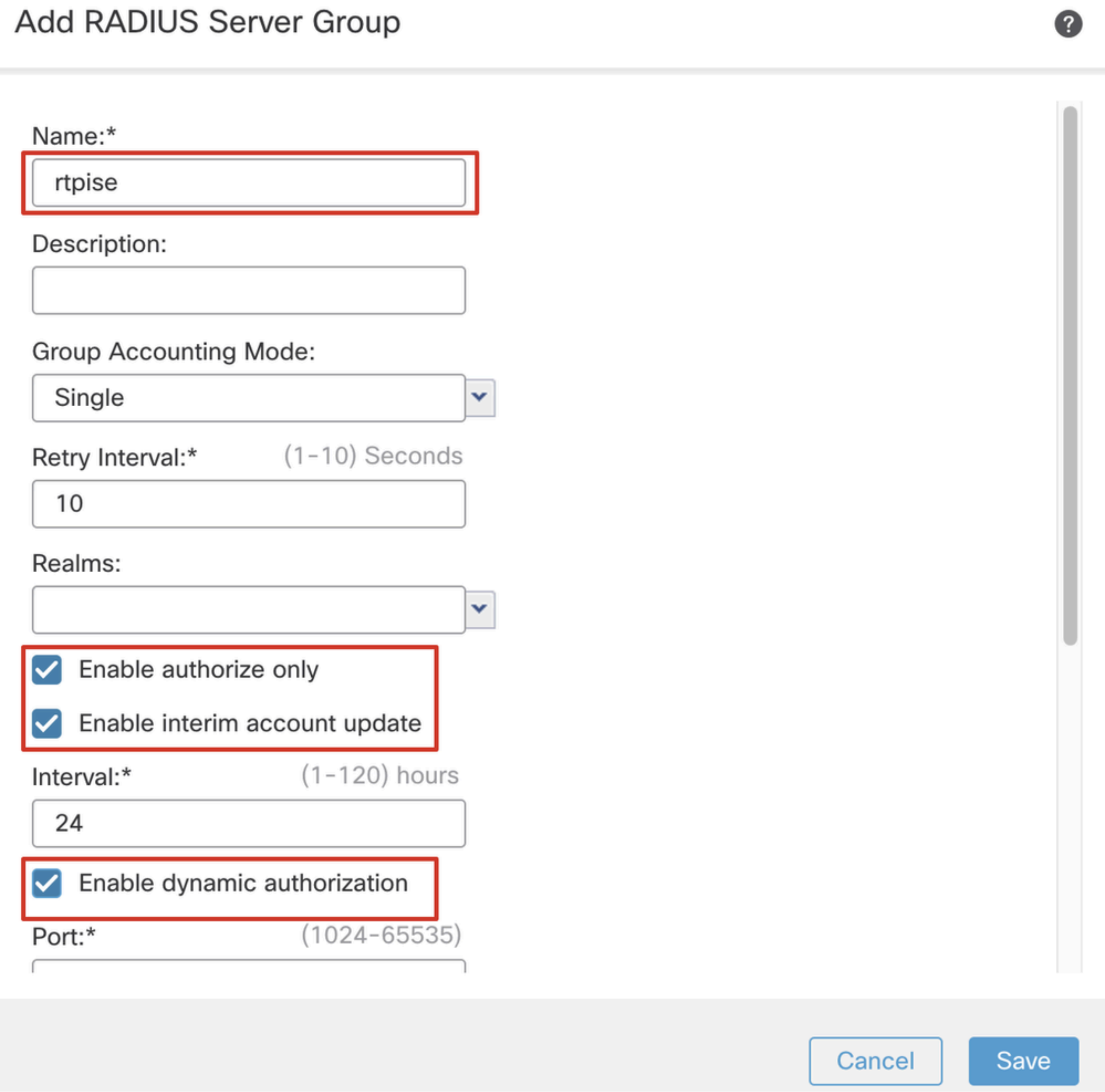
RADIUS Server Group

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.

Name	Value

FMC_Add_New_Radius_Server_Group

Step 7.1. Provide name, check Enable authorize only, check Enable interim account update, check Enable dynamic authorization.



Add RADIUS Server Group

Name:* rtpise

Description:

Group Accounting Mode: Single

Retry Interval:* (1-10) Seconds 10

Realms:

☑ Enable authorize only

☑ Enable interim account update

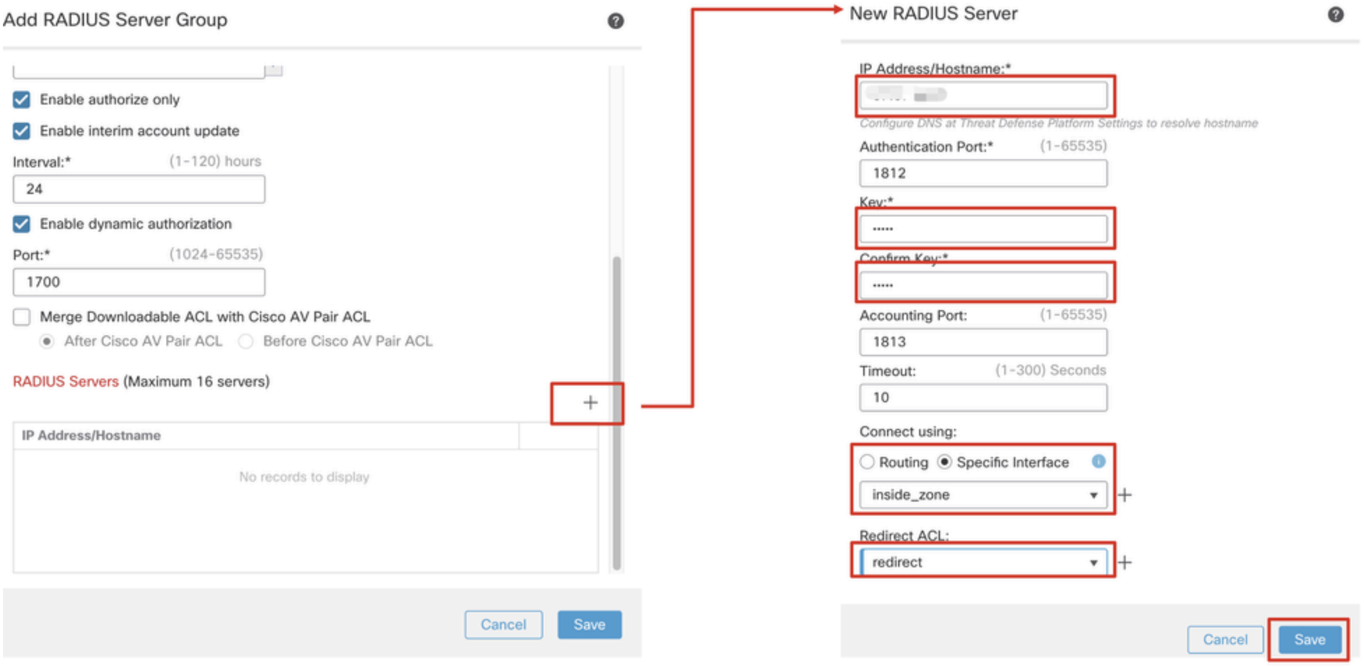
Interval:* (1-120) hours 24

☑ Enable dynamic authorization

Port:* (1024-65535)

FMC_Add_New_Radius_Server_Group_Part_1

Step 7.2. Click the iconPlus to add a new radius server. Provide the ISE PSN IP Address/Hostname, Key. Select the specific interface for connecting. Select the Redirect ACL. Then click Saveto save the new radius server. Then click Save again to save the new radius server group.



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

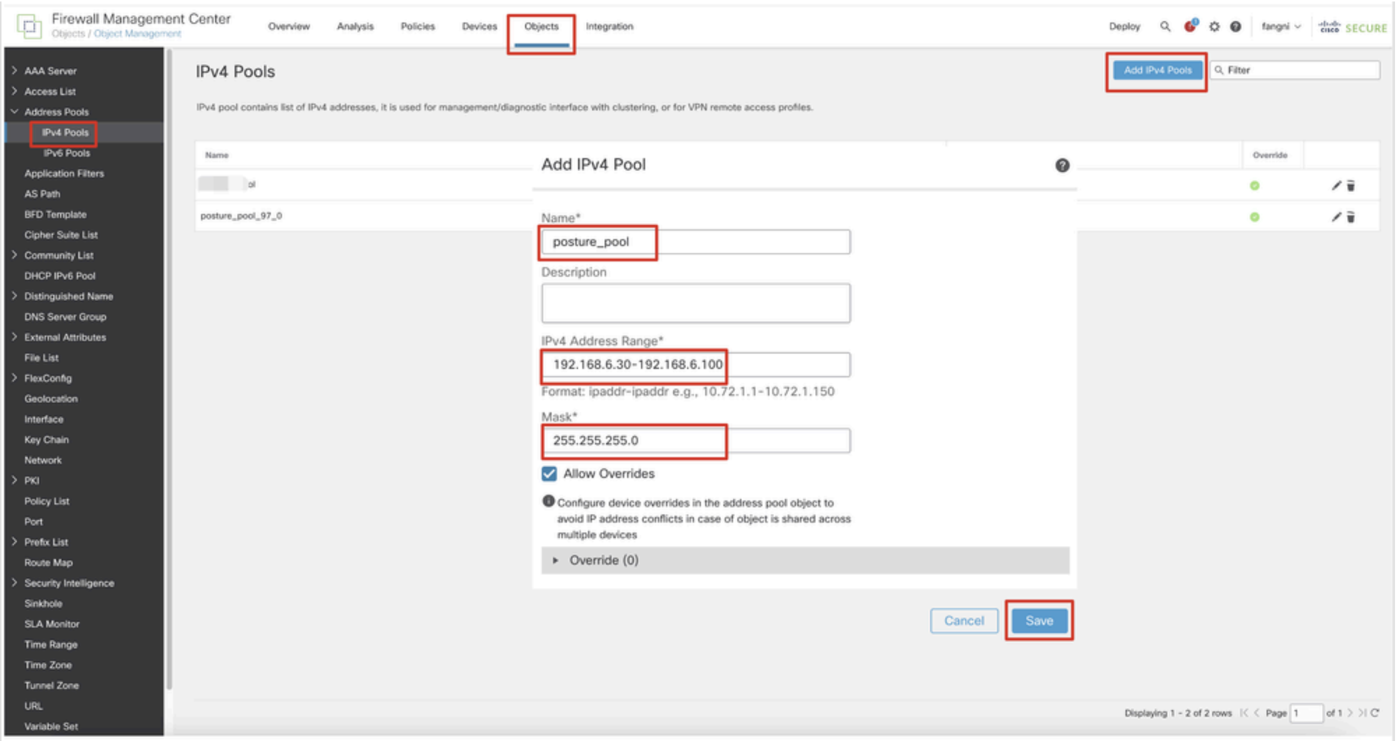
Connect using: ○ Routing ● Specific Interface

inside_zone

Redirect ACL: redirect

FMC_Add_New_Radius_Server_Group_Part_2

Step 8. Navigate to Objects > Object Management > Address Pools > IPv4 Pools. Click Add IPv4 Pools and provide the **Name, IPv4 Address Range**and Mask. Then click 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

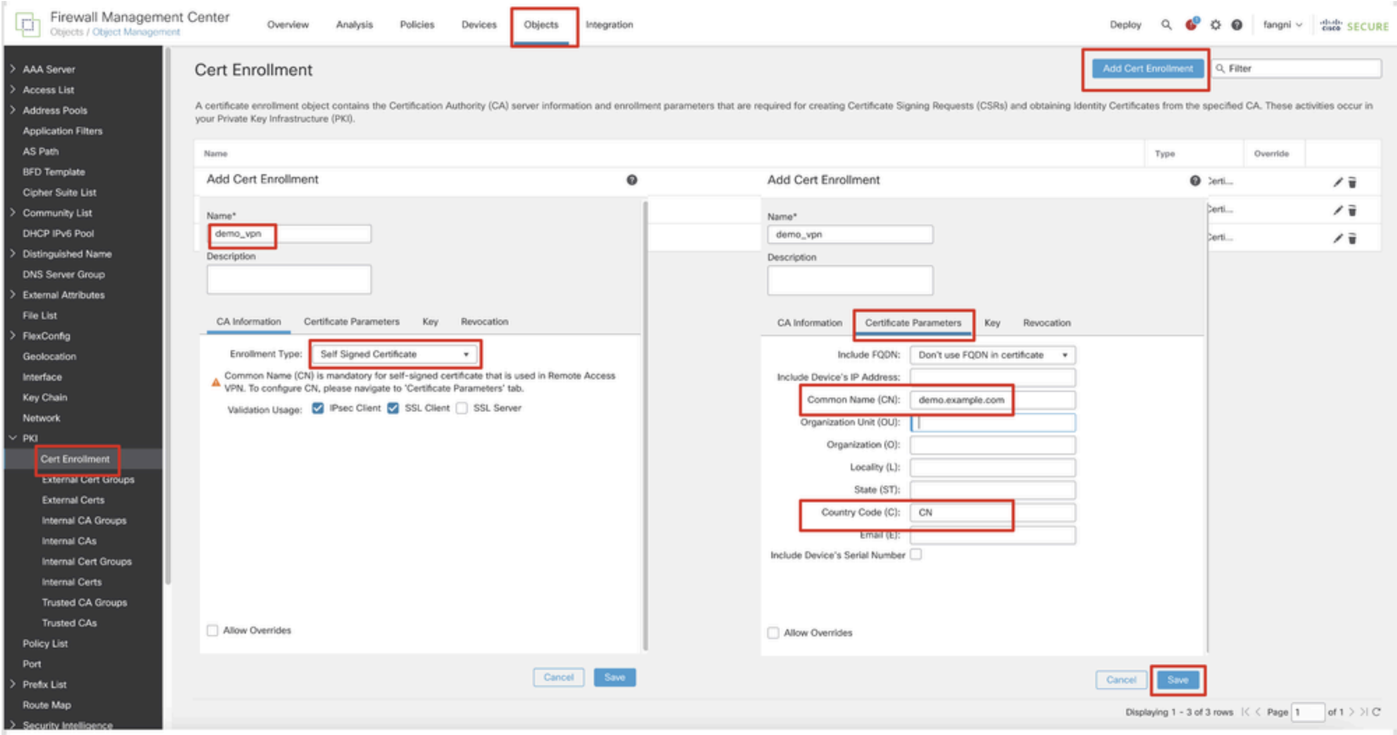
☑ Allow Overrides

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

Step 9. Navigate to Certificate Objects > Object Management > PKI > Cert Enrollment. Click Add Cert Enrollment, provide a name, and select Self Signed Certificatein Enrollment Type. Click the Certificate Parameters tab and provide Common Name and Country Code. Then click Save.



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

Add Cert Enrollment

Name*: demo_vpn

Description:

Enrollment Type: Self Signed Certificate

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

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

Add Cert Enrollment

Name*: demo_vpn

Description:

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):

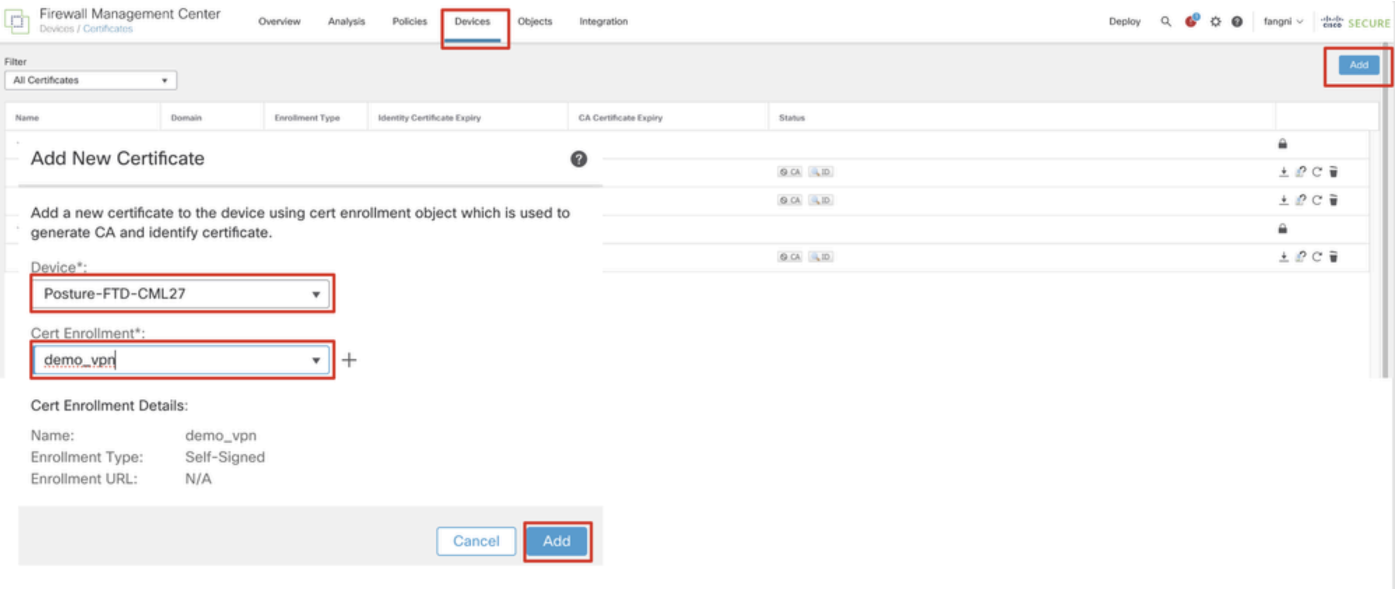
Country Code (C): CN

Email (E):

Include Device's Serial Number □

FMC_Add_New_Cert_Enroll

Step 10. Navigate to Devices > Certificates. Click Add, select the FTD name under Device, select previous configured enrollment under Cert Enrollment. Click 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

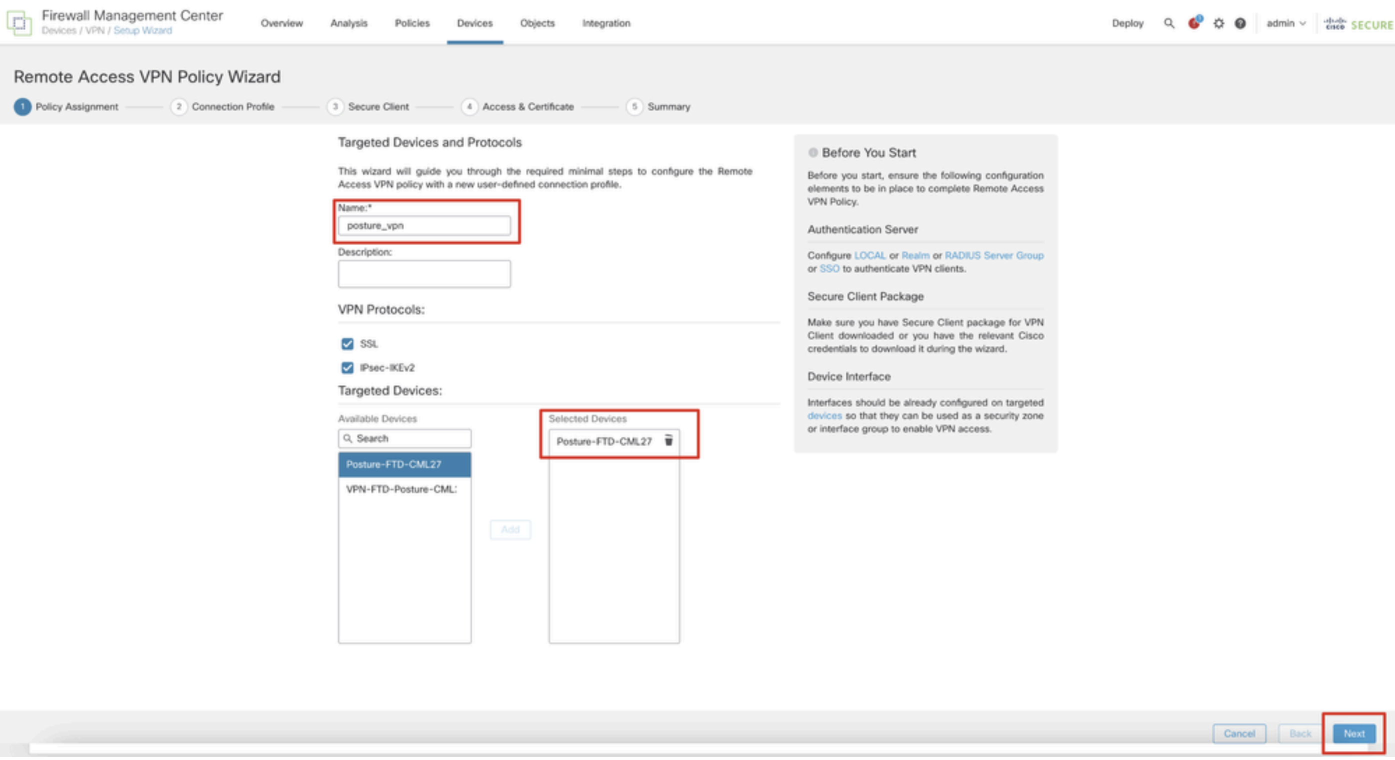
Cert Enrollment Details:

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

FMC_Add_New_Cert_To_FTD

Step 11. Navigate to Devices > VPN > Remote Access. Click Add.

Step 11.1. Provide the name, and add the FTD to Selected Devices. Click Next.



Firewall Management Center
Devices / VPN / Setup Wizard

Overview Analysis Policies Devices Objects Integration

Deploy admin SECURE

Remote Access VPN Policy Wizard

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

Targeted Devices and Protocols

This wizard will guide you through the required minimal steps to configure the Remote Access VPN policy with a new user-defined connection profile.

Name:* posture_vpn

Description:

VPN Protocols:

☑ SSL

☑ IPsec-IKEv2

Targeted Devices:

Available Devices: 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

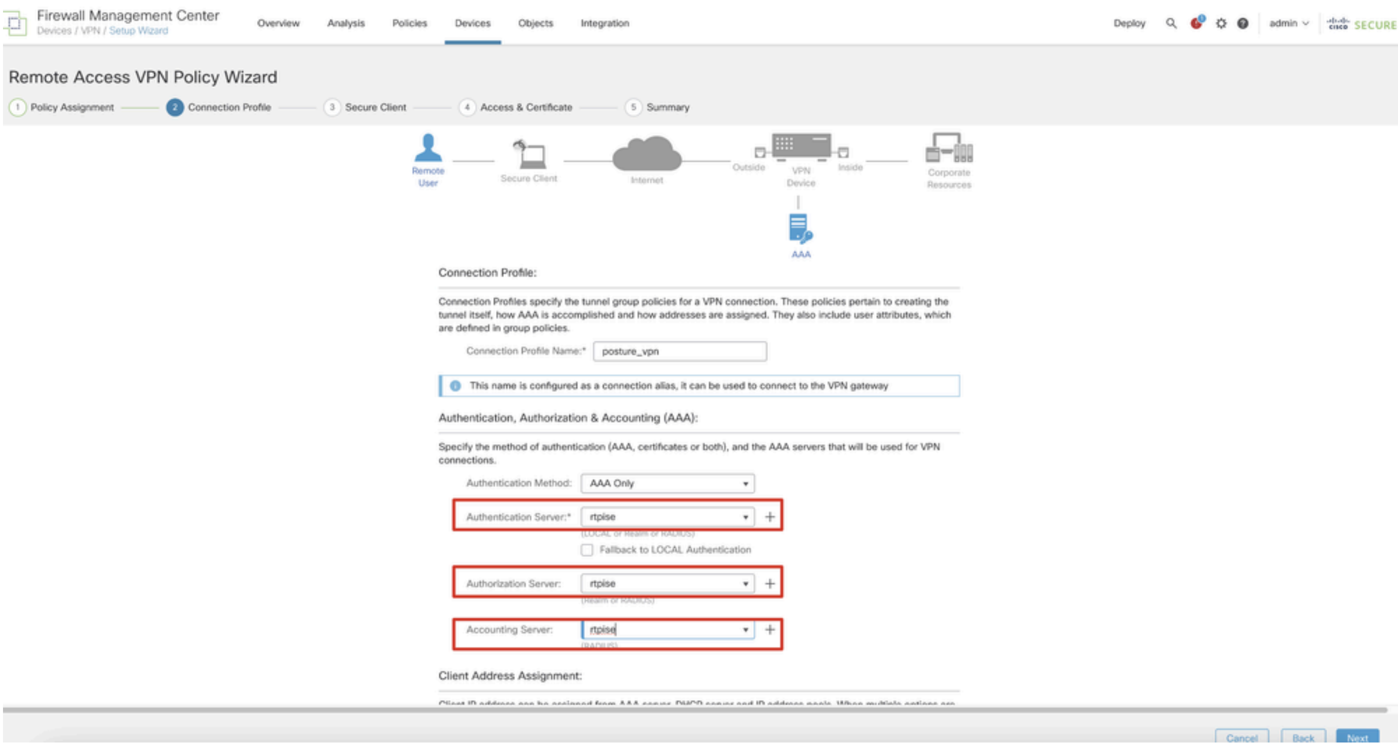
Make sure you have Secure Client package for VPN Client downloaded or you have the relevant Cisco credentials to download it during the wizard.

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

Step 11.2. Select previously configured radius server group in the Authentication Server, Authorization Server, Accounting Server. Scroll down the page.



Firewall Management Center
Devices / VPN / Setup Wizard

Overview Analysis Policies Devices Objects Integration

Deploy admin SECURE

Remote Access VPN Policy Wizard

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

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

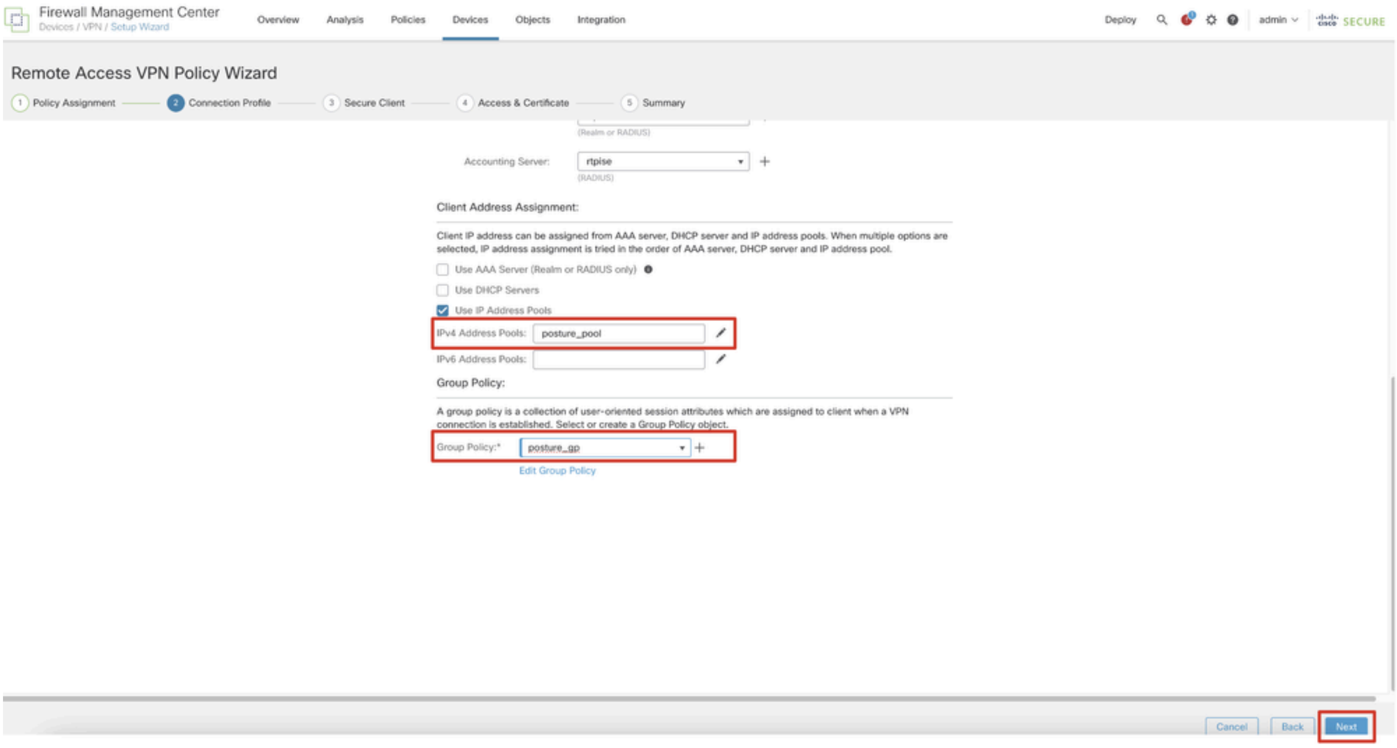
Authorization Server: rtpise (Realm or RADIUS)

Accounting Server: rtpise (RADIUS)

Client Address Assignment:

FMC_New_RAVPN_Wizard_2

Step 11.3. Select the previously configured pool name in IPv4 Address Pools. Select previously configured group policy in Group Policy. Click Next.



Remote Access VPN Policy Wizard

(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:

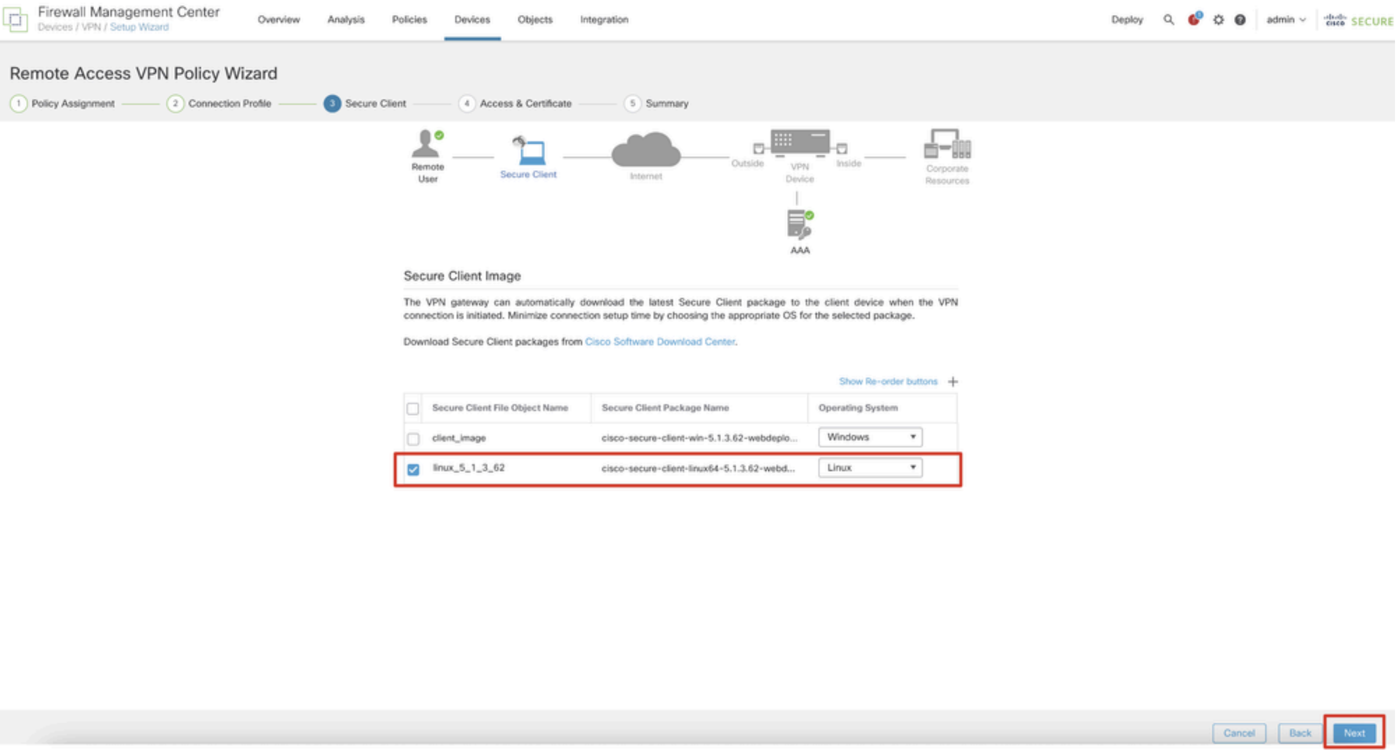
Group Policy:

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

FMC_New_RAVPN_Wizard_3

Step 11.4. Check the checkbox of Linux image. Click Next.



Remote Access VPN Policy Wizard

Secure Client Image

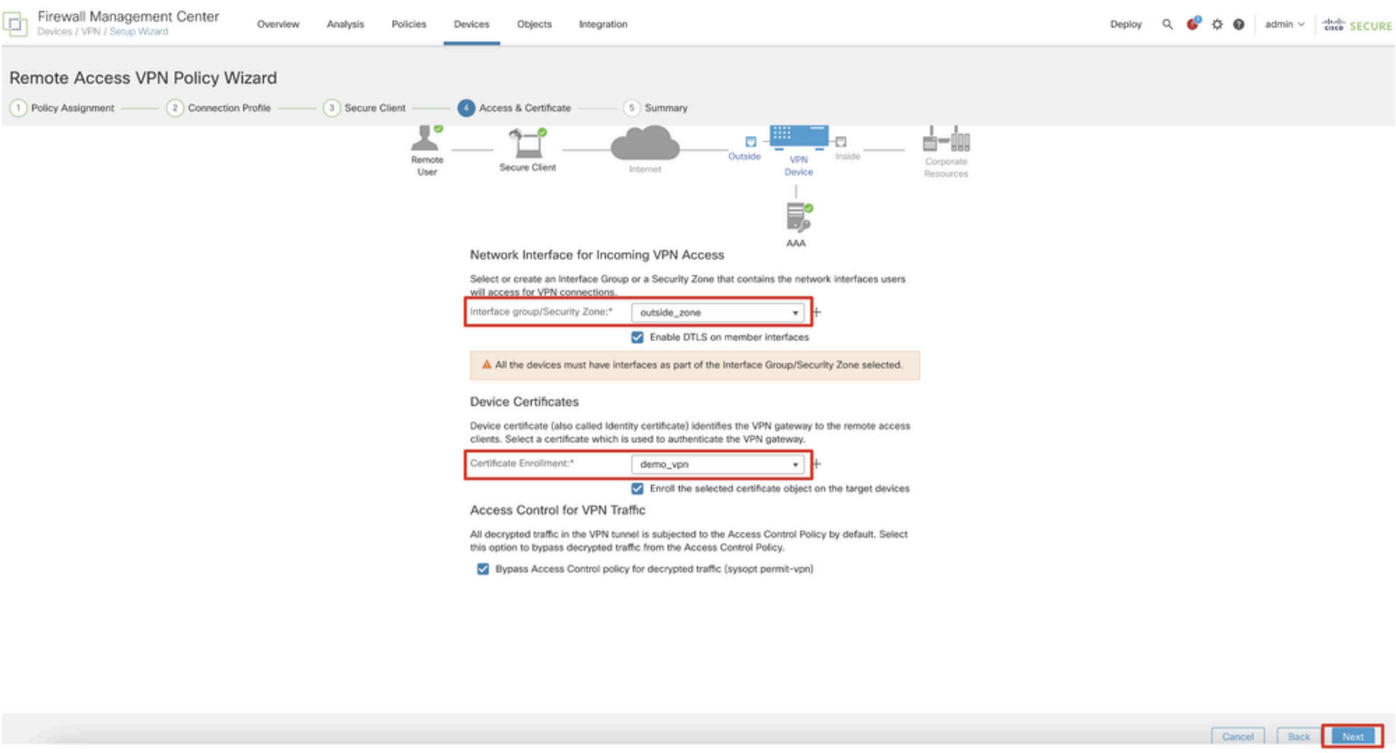
The VPN gateway can automatically download the latest Secure Client package to the client device when the VPN connection is initiated. Minimize connection setup time by choosing the appropriate OS for the selected package.

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

Step 11.5. Select the interface of VPN interface. Select the cert enrollment that enrolled on FTD in step 9. Click Next.



Network Interface for Incoming VPN Access

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

Interface group/Security Zone:* outside_zone

☑ Enable DTLS on member interfaces

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

Device Certificates

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

Certificate Enrollment:* demo_vpn

☑ Enroll the selected certificate object on the target devices

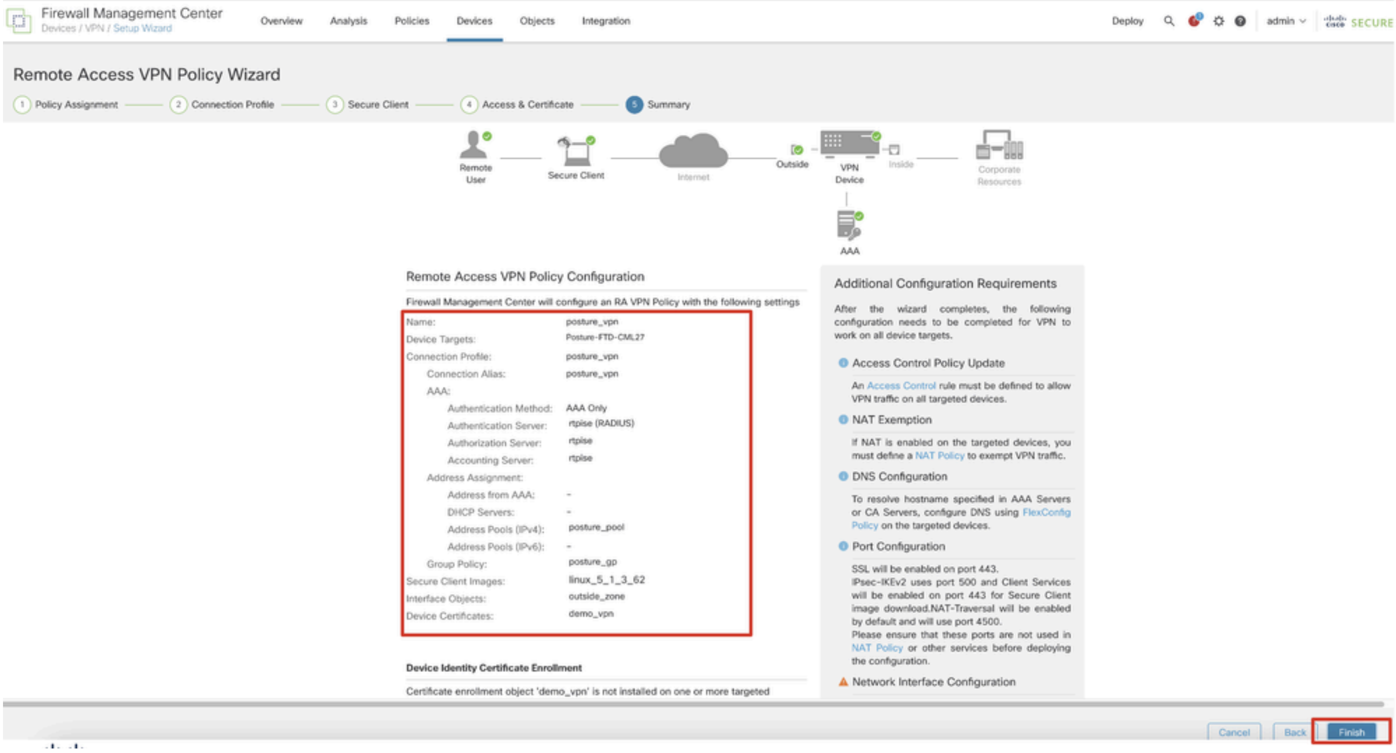
Access Control for VPN Traffic

All decrypted traffic in the VPN tunnel is subjected to the Access Control Policy by default. Select this option to bypass decrypted traffic from the Access Control Policy.

☑ Bypass Access Control policy for decrypted traffic (sysopt permit-vpn)

FMC_New_RAVPN_Wizard_5

Step 11.6. Double confirm the related information on summary page. If everything is good, click Finish. If anything needs to be modified, click Back.



Remote Access VPN Policy Configuration

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

Name:	posture_vpn
Device Targets:	Posture-FTD-CML27
Connection Profile:	posture_vpn
Connection Alias:	posture_vpn
AAA:	
Authentication Method:	AAA Only
Authentication Server:	rtpise (RADIUS)
Authorization Server:	rtpise
Accounting Server:	rtpise
Address Assignment:	
Address from AAA:	-
DHCP Servers:	-
Address Pools (IPv4):	posture_pool
Address Pools (IPv6):	-
Group Policy:	posture_gp
Secure Client Images:	linux_5_1_3_62
Interface Objects:	outside_zone
Device Certificates:	demo_vpn

Device Identity Certificate Enrollment

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

Additional Configuration Requirements

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

Access Control Policy Update

An Access Control rule must be defined to allow VPN traffic on all targeted devices.

NAT Exemption

If NAT is enabled on the targeted devices, you must define a NAT Policy to exempt VPN traffic.

DNS Configuration

To resolve hostname specified in AAA Servers or CA Servers, configure DNS using FlexConfig Policy on the targeted devices.

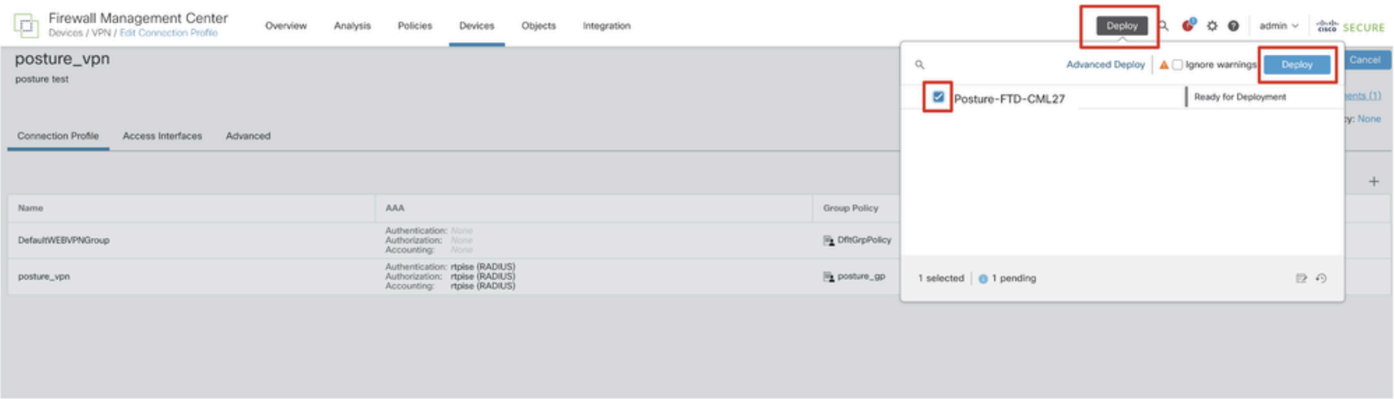
Port Configuration

SSL will be enabled on port 443.
IPsec-IKEv2 uses port 500 and Client Services will be enabled on port 443 for Secure Client image download.NAT-Traversal will be enabled by default and will use port 4500.
Please ensure that these ports are not used in NAT Policy or other services before deploying the configuration.

Network Interface Configuration

FMC_New_RAVPN_Wizard_6

Step 12. Deploy the new configuration to FTD to complete the remote access VPN configuration.



posture_vpn

posture test

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

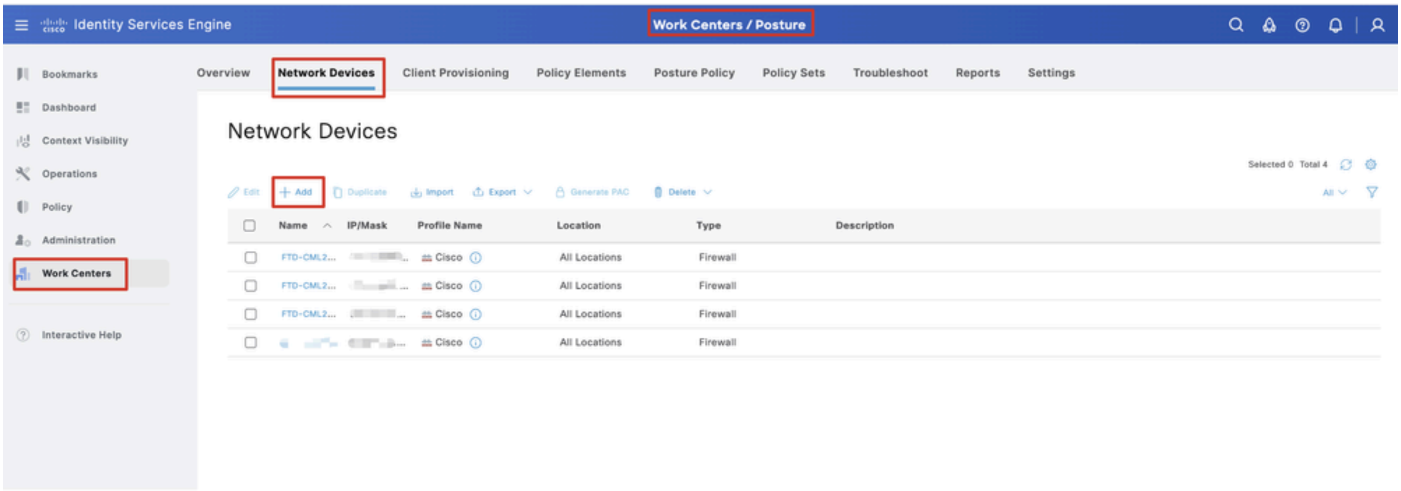
☑ Posture-FTD-CML27 — Ready for Deployment

1 selected | 1 pending

FMC_Deploy_FTD

Configurations on ISE

Step 13. Navigate to Work Centers > Posture > Network Devices. Click Add.



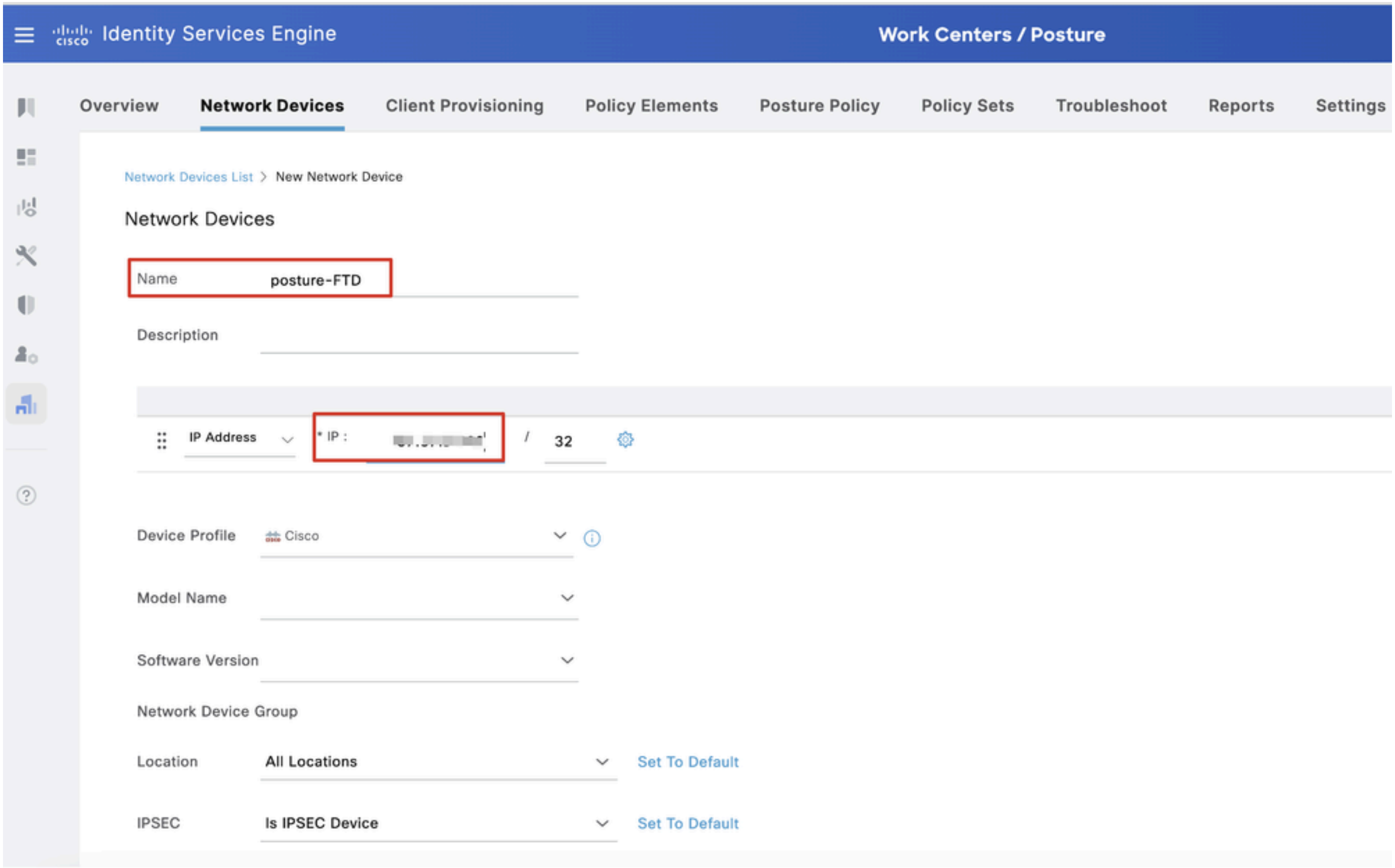
Network Devices

Selected 0 Total 4

☐	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

Step 13.1. Provide the Name, IP Addressand scroll down the page.



Network Devices

Name posture-FTD

Description

IP Address * IP : [redacted] / 32

Device Profile Cisco

Model Name

Software Version

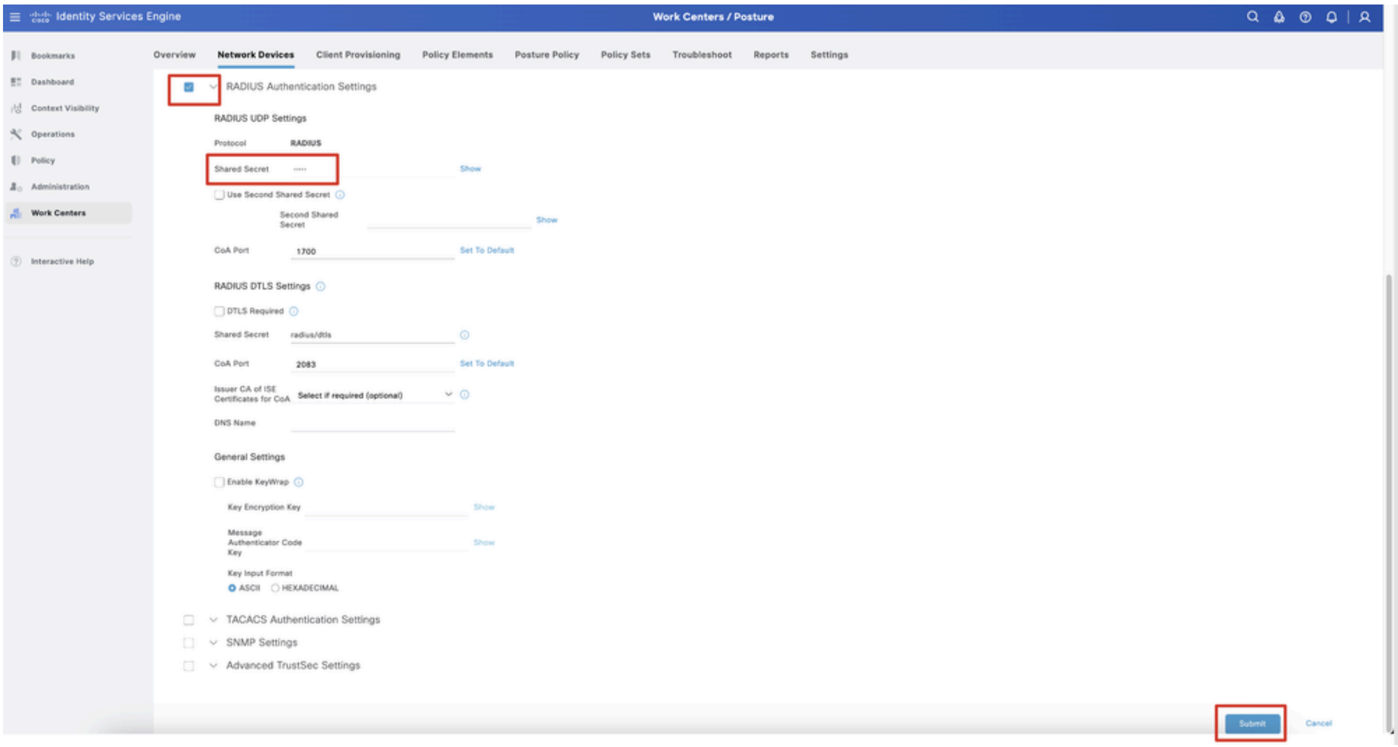
Network Device Group

Location All Locations

IPSEC Is IPSEC Device

ISE_Add_New_Devices_1

Step 13.2. Check the checkbox of RADIUS Authentication Settings. Provide the Shared Secret. Click Submit.



☑ RADIUS Authentication Settings

RADIUS UDP Settings

Protocol RADIUS

Shared Secret •••••

□ Use Second Shared Secret

Second Shared Secret

CoA Port 1700

RADIUS DTLS Settings

□ DTLS Required

Shared Secret radius/dtls

CoA Port 2083

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

DNS Name

General Settings

□ Enable KeyWrap

Key Encryption Key

Message Authenticator Code Key

Key Input Format

● ASCII ○ HEXADECIMAL

□ TACACS Authentication Settings

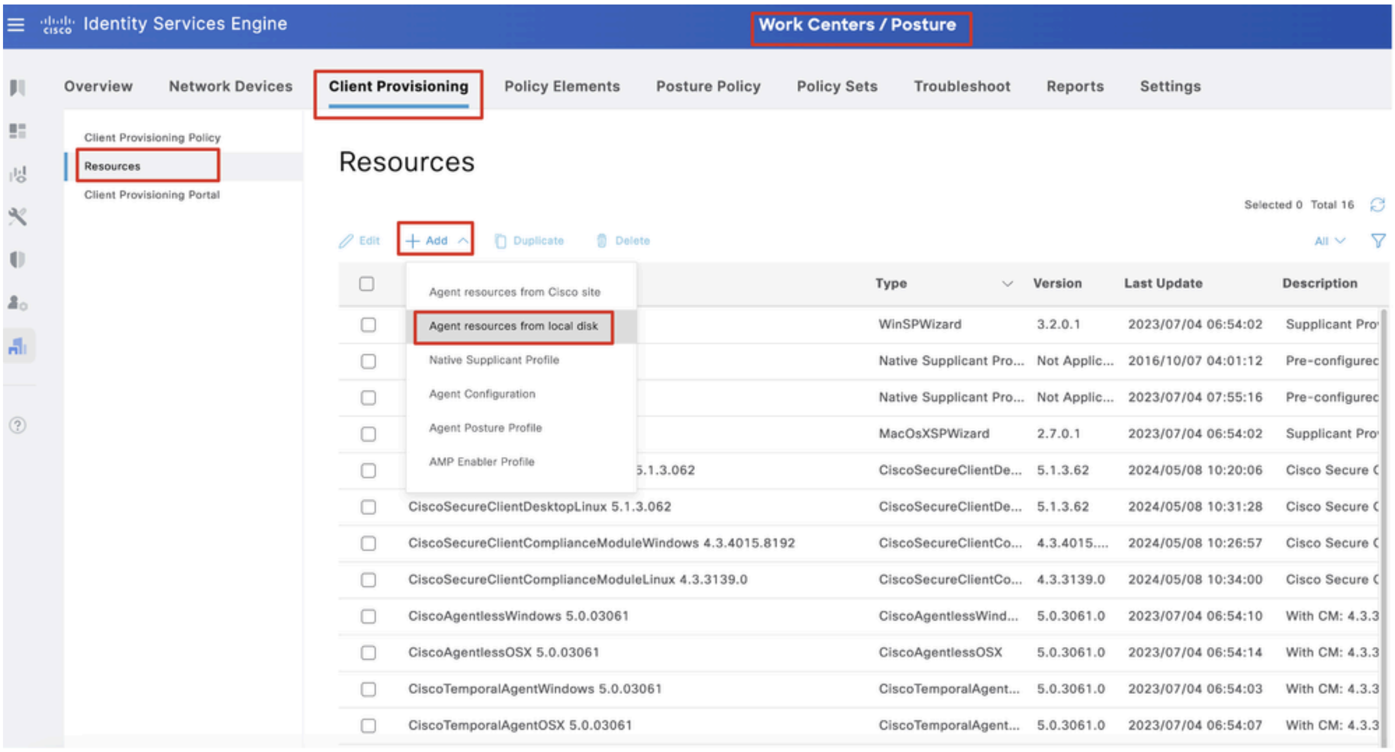
□ SNMP Settings

□ Advanced TrustSec Settings

ISE_Add_New_Devices_2

Step 14. Download the package name cisco-secure-client-linux64-4.3.3139.0-isecompliance-webdeploy-k9.pkg from [Cisco Software Download] and ensure the file is good by confirming md5 checksum of downloaded file is the same as Cisco Software Download page. Package name cisco-secure-client-linux64-5.1.3.62-webdeploy-k9.pkg has been downloaded successfully in Step 1.

Step 15. Navigate to Work Centers > Posture > Client Provisioning > Resources. Click Add. Select Agent resources from local disk.



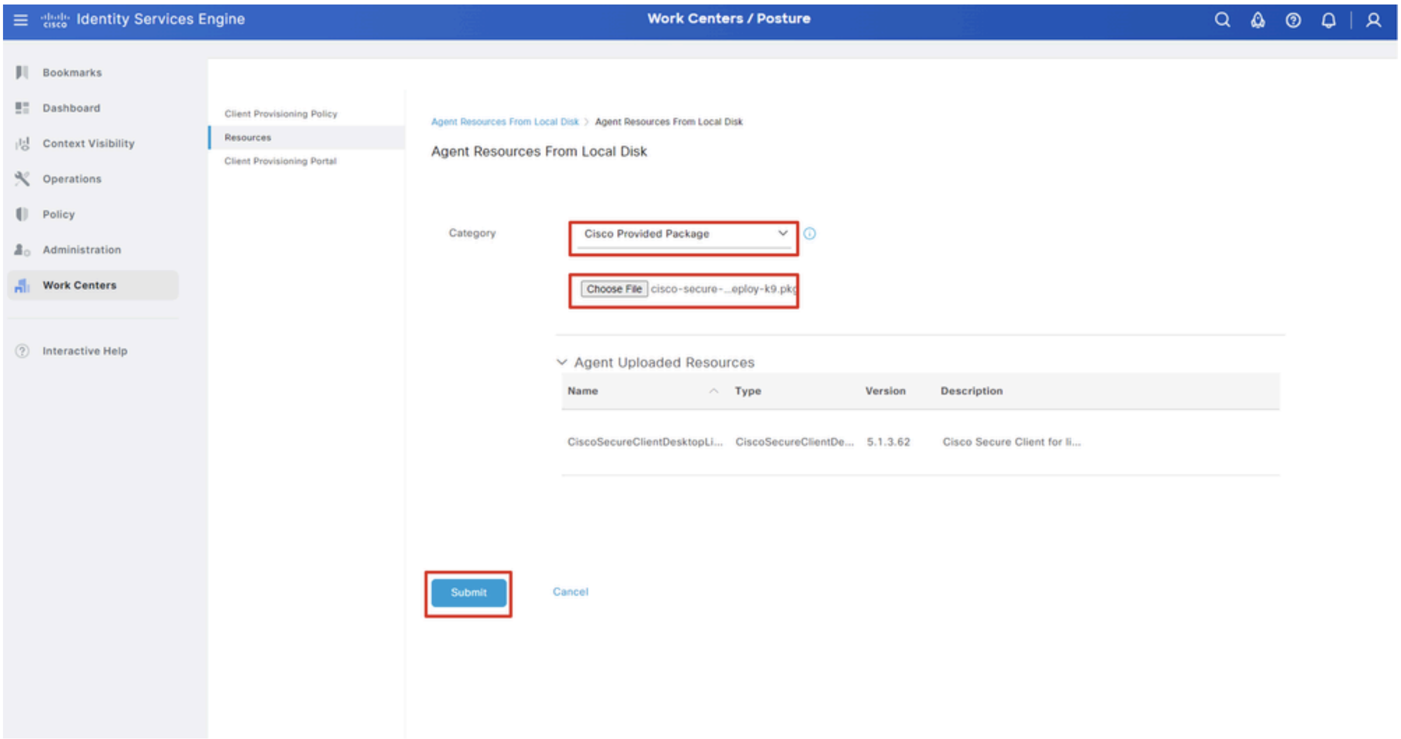
Resources

Selected 0 Total 16

□		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

Step 15.1. Select Cisco Provided Package. Click Choose File to upload cisco-secure-client-linux64-5.1.3.62-webdeploy-k9.pkg. Click Submit.



Agent Resources From Local Disk

Category: Cisco Provided Package

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

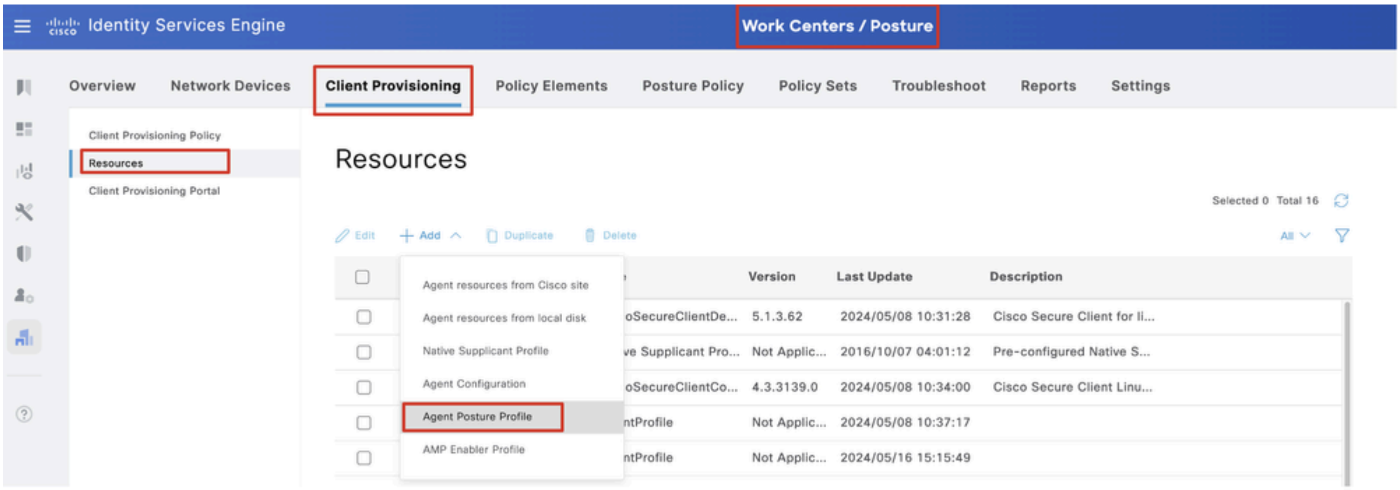
Agent Uploaded Resources

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

ISE_Upload_Resources_1

Note: Repeat the Step 14. to upload cisco-secure-client-linux64-4.3.3139.0-isecompliance-webdeploy-k9.pkg .

Step 16. Navigate to Work Centers > Posture > Client Provisioning > Resources. Click Add. Select Agent Posture Profile.



Resources

Selected 0 Total 16

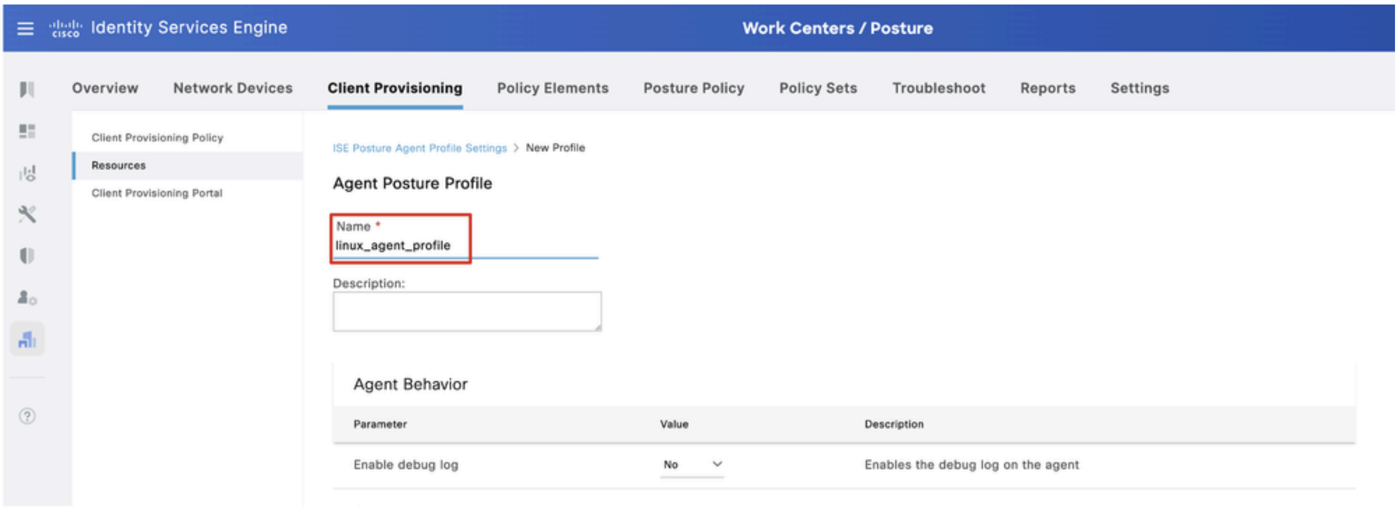
		Version	Last Update	Description
□	oSecureClientDe...	5.1.3.62	2024/05/08 10:31:28	Cisco Secure Client for li...
□	ve Supplicant Pro...	Not Applic...	2016/10/07 04:01:12	Pre-configured Native S...
□	oSecureClientCo...	4.3.3139.0	2024/05/08 10:34:00	Cisco Secure Client Linu...
□	ntProfile	Not Applic...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

ISE_Add_Agent_Posture_Profile

Step 16.1. Provide the Name, Server name rules and keep the rest as default. Click Save.

Name: linux_agent_profile

Server name rules: *.example.com



Agent Posture Profile

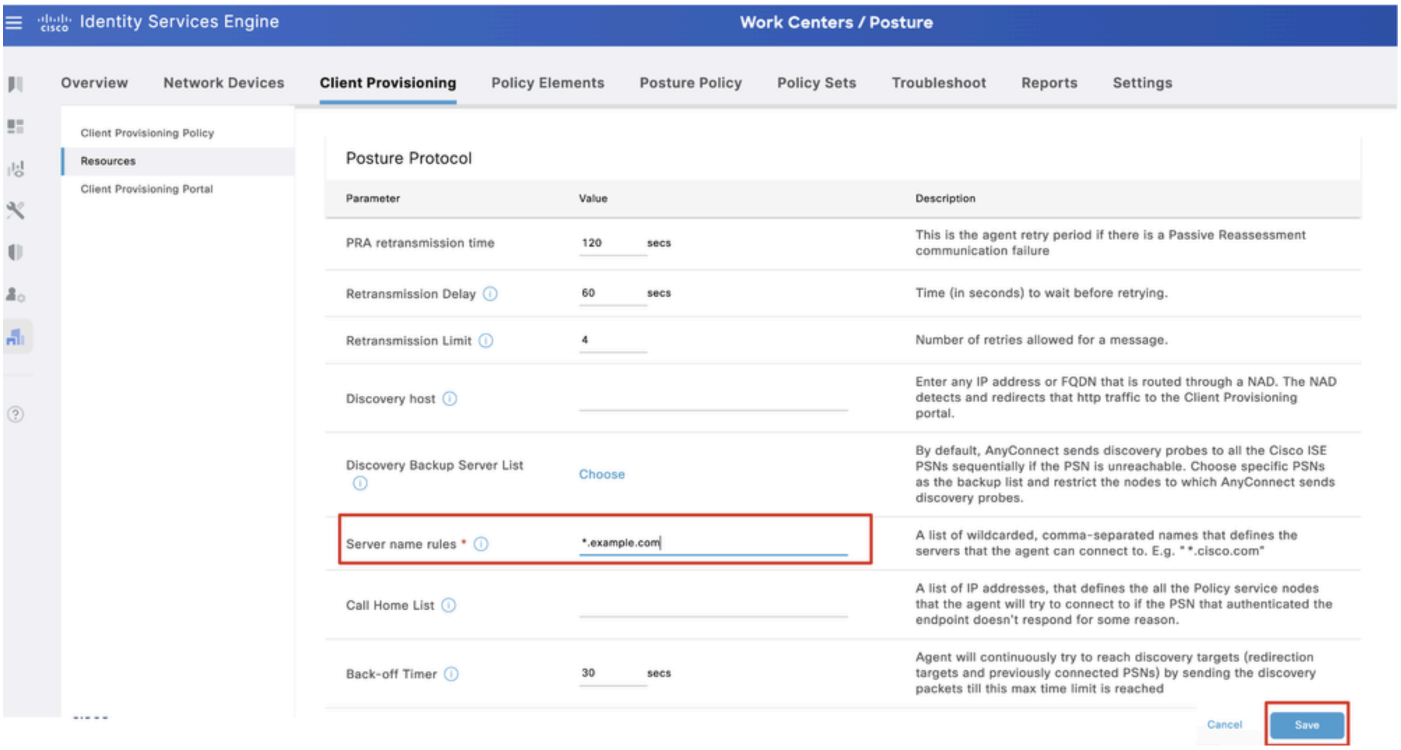
Name * linux_agent_profile

Description:

Agent Behavior

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

ISE_Add_Agent_Posture_Profile_1

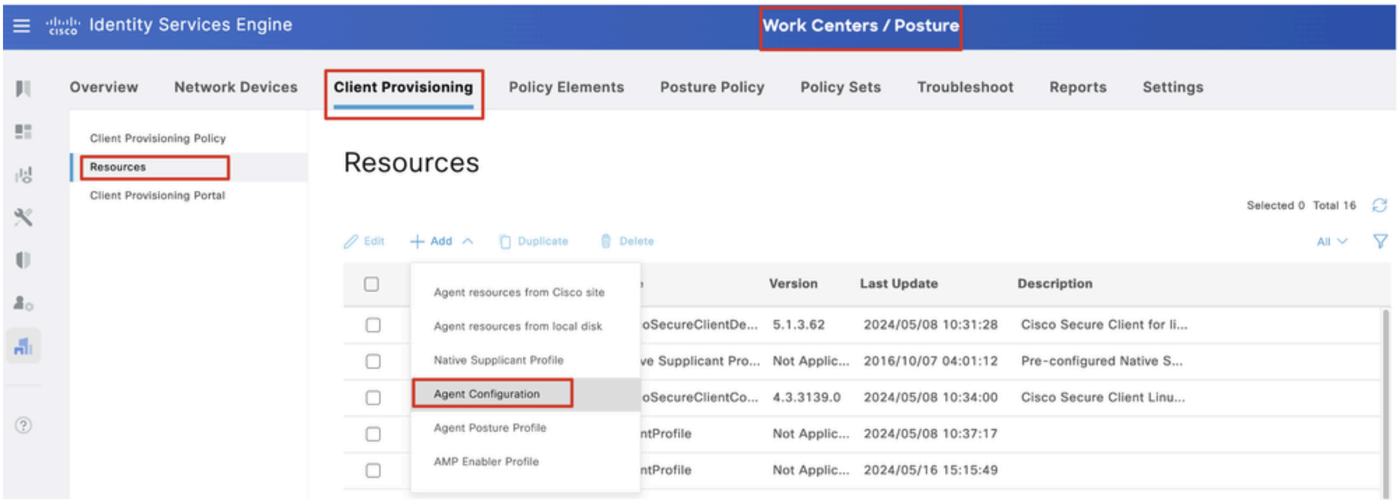


Posture Protocol

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

Step 17. Navigate to Work Centers > Posture > Client Provisioning > Resources. Click Add. Select Agent Configuration.



	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

Step 17.2. Configure the details:

Select Agent Package: CiscoSecureClientDesktopLinux 5.1.3.062

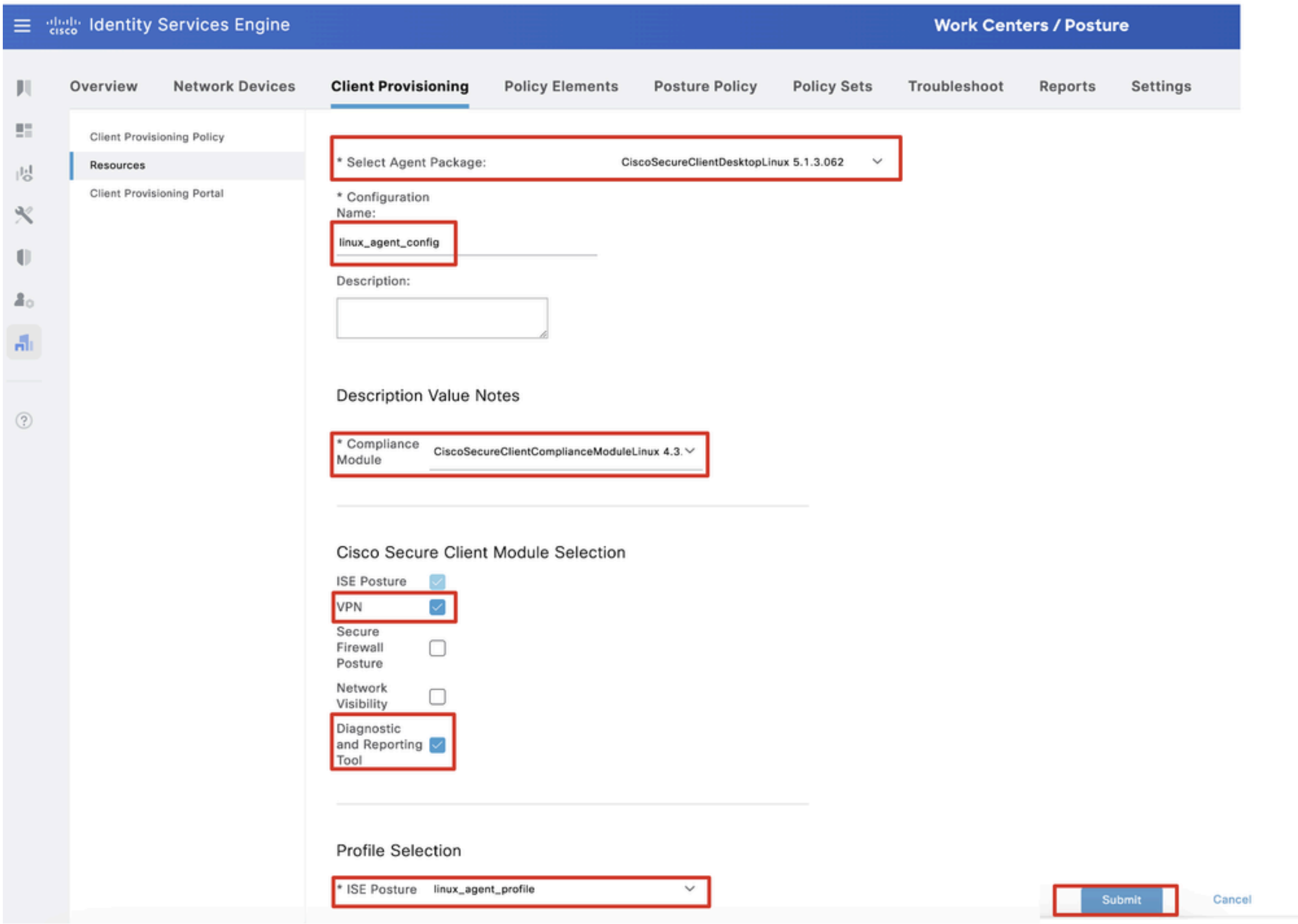
Name: linux_agent_config

Compliance module: CiscoSecureClientComplianceModuleLinux 4.3.3139.0

Check the checkbox of VPN, Diagnostic and Reporting Tool

Profile Selection ISE Posture: linux_agent_profile

Click 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 □

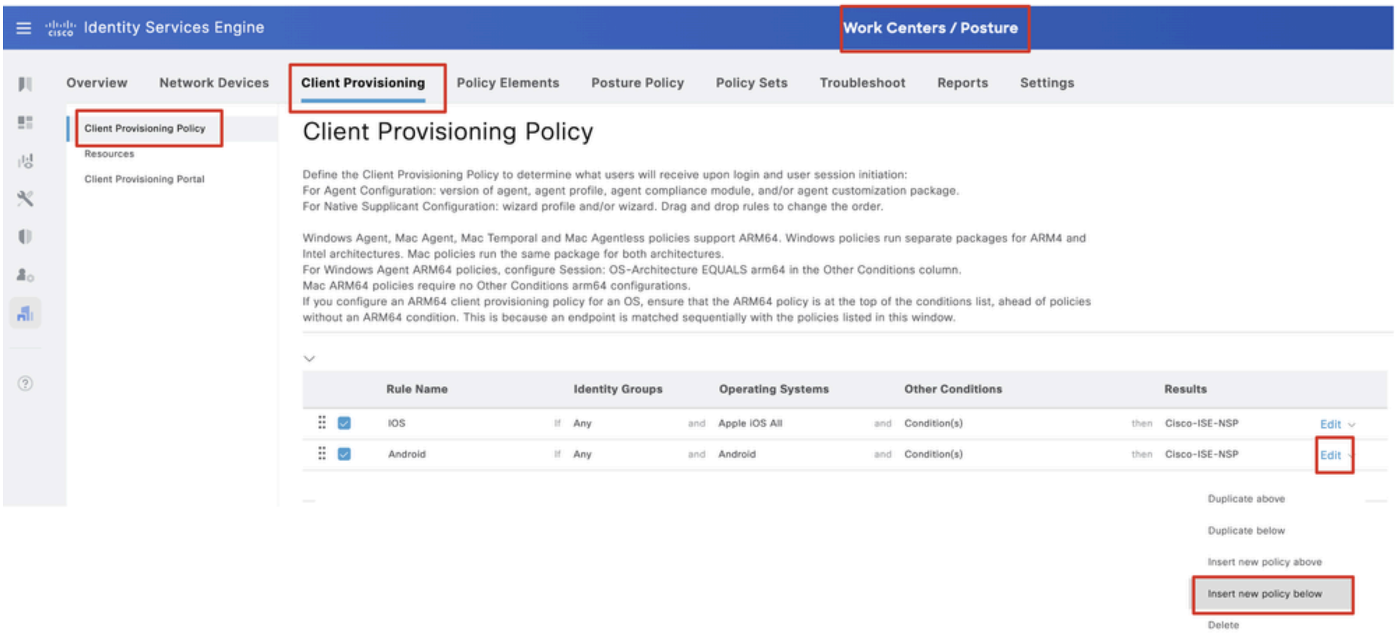
Diagnostic and Reporting Tool ☑

Profile Selection

* ISE Posture linux_agent_profile

ISE_Add_Agent_Configuration_1

Step 18. Navigate to Work Centers > Posture > Client Provisioning > Client Provisioning Policy. Click Edit at the end of any rule name. Select 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

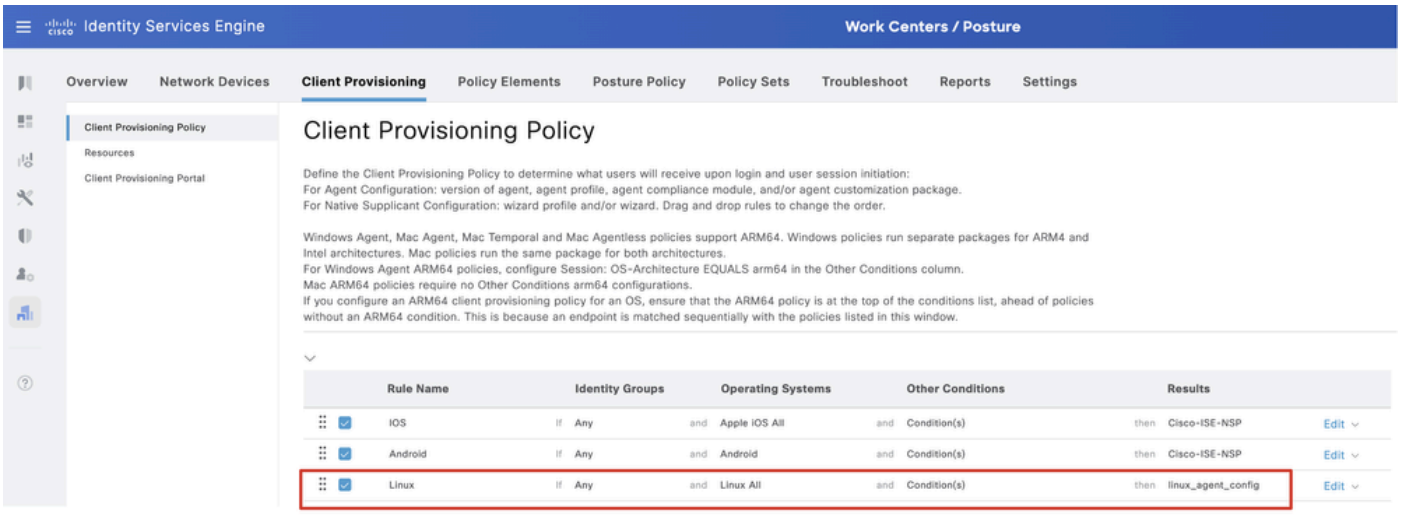
Step 18.1. Configure the details:

Rule Name: Linux

Operating Systems: Linux All

Results: linux_agent_config

Click Done and Save.



Client Provisioning Policy

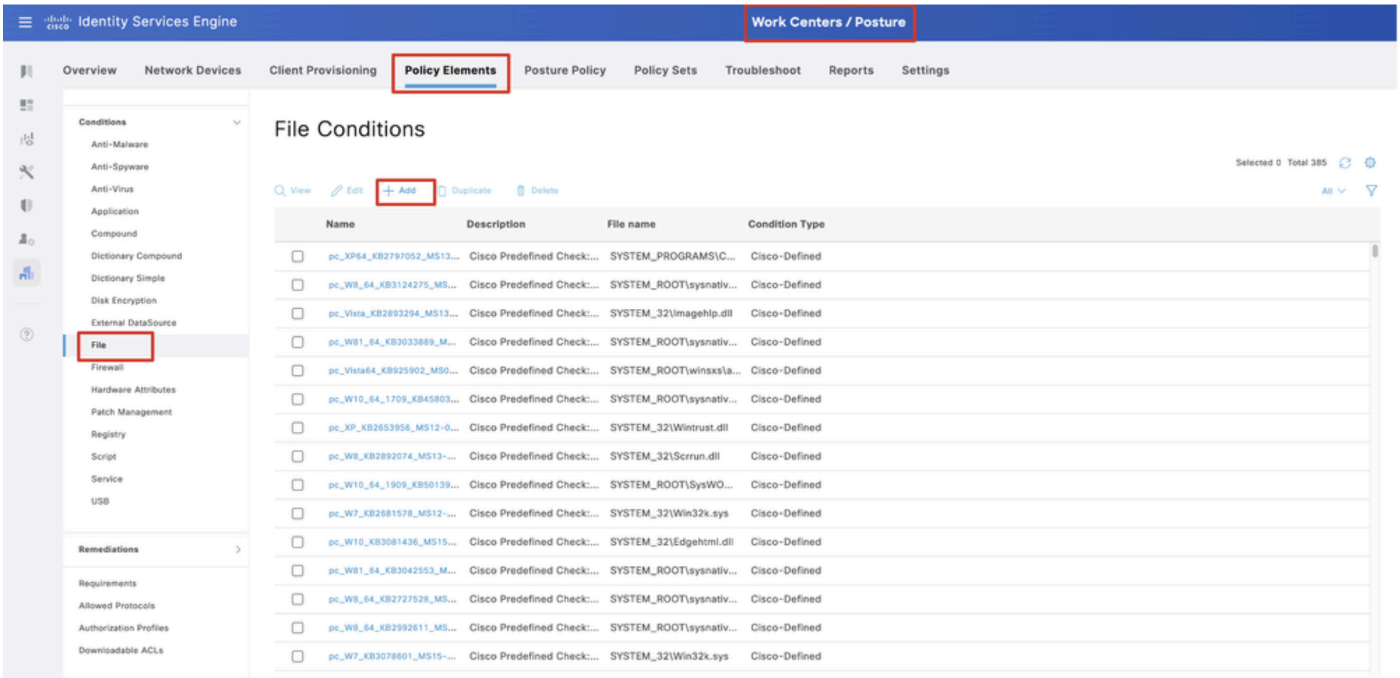
Define the Client Provisioning Policy to determine what users will receive upon login and user session initiation:
For Agent Configuration: version of agent, agent profile, agent compliance module, and/or agent customization package.
For Native Supplicant Configuration: wizard profile and/or wizard.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

Step 19. Navigate to Work Centers > Posture > Policy Elements > Conditions > File. Click 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

Step 19.1. Configure the details:

Name: linux_demo_file_exist

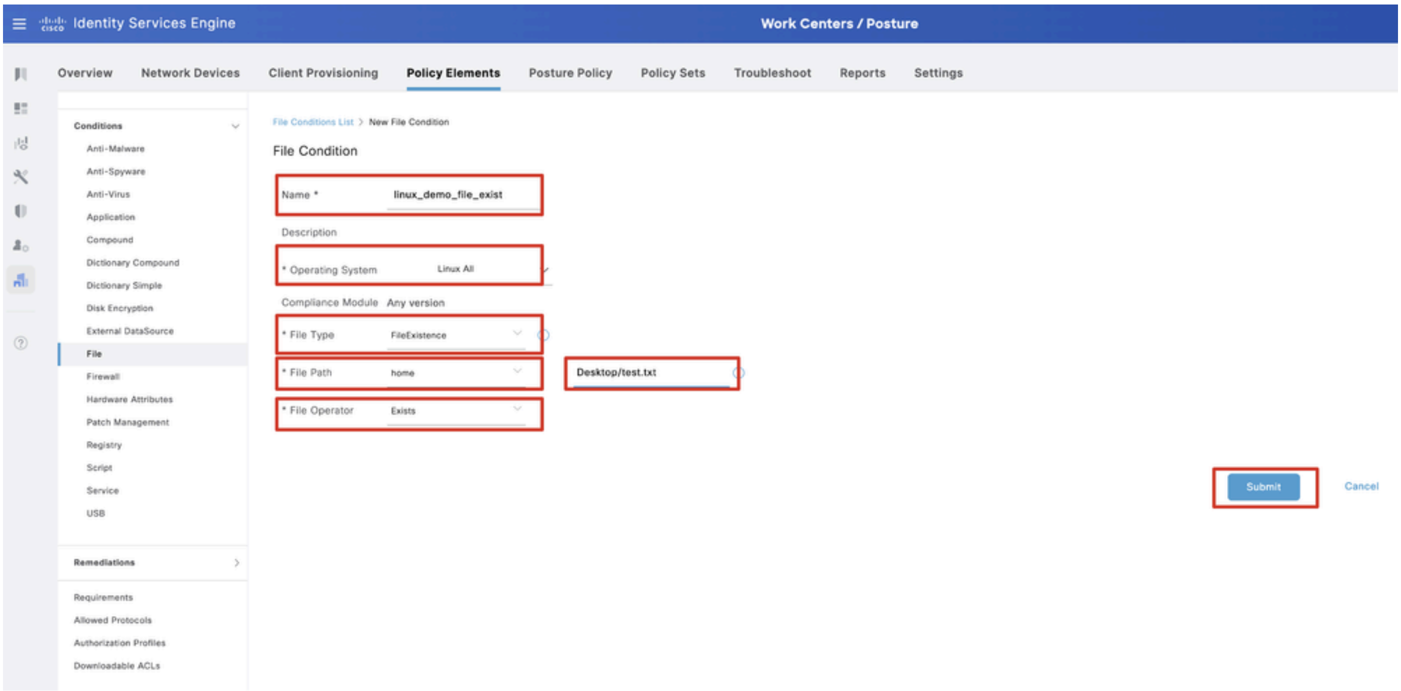
Operating Systems: Linux All

File Type: FileExistence

File Path: home, Desktop/test.txt

File Operator: Exists

Click Submit.



File Conditions List > New File Condition

File Condition

Name * linux_demo_file_exist

Description

* Operating System Linux All

Compliance Module Any version

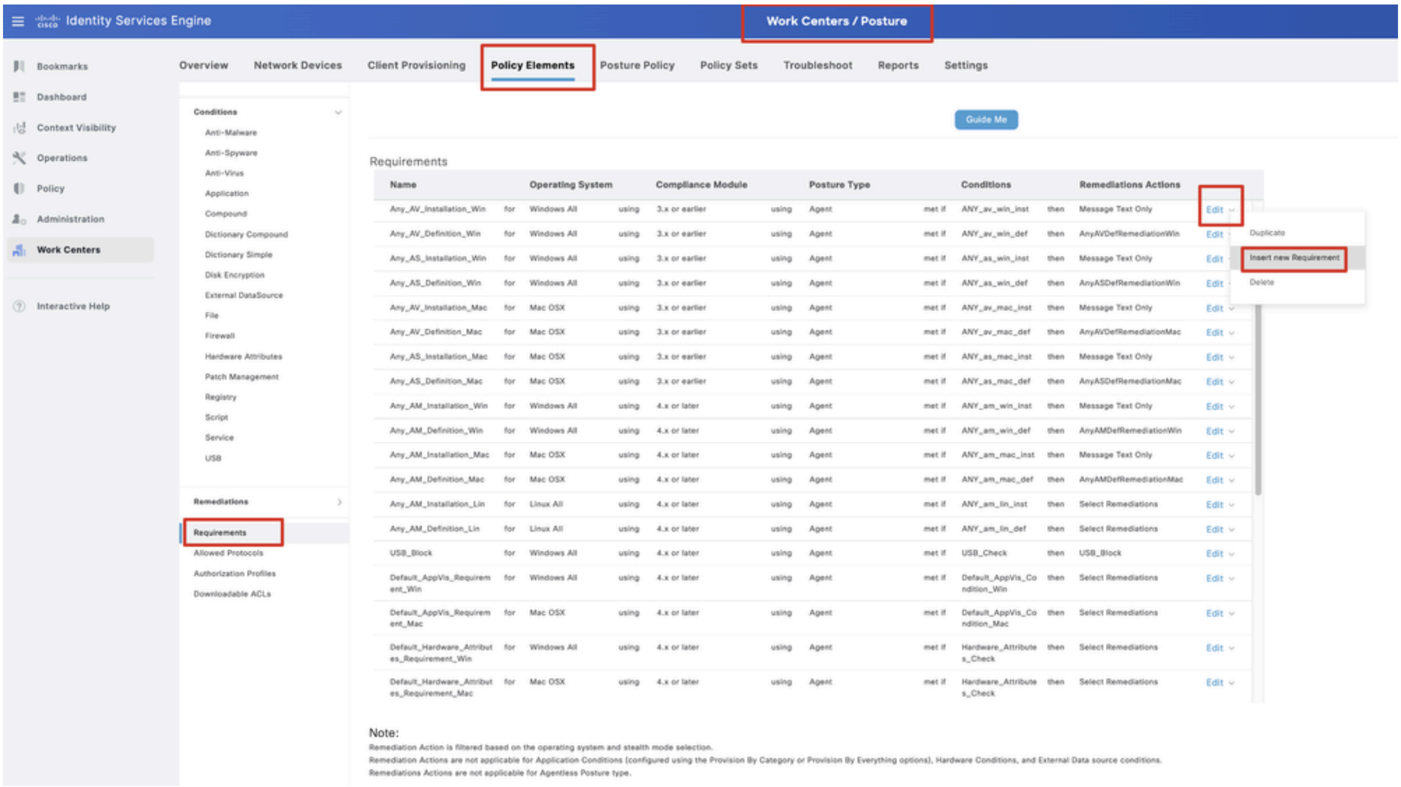
* File Type FileExistence

* File Path home Desktop/test.txt

* File Operator Exists

ISE_Add_New_File_Condition_1

Step 20. Navigate to Work Centers > Posture > Policy Elements > Requirements. Click Edit at the end of any rule name. Select 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

Step 20.1. Configure the details:

Name: Test_exist_linux

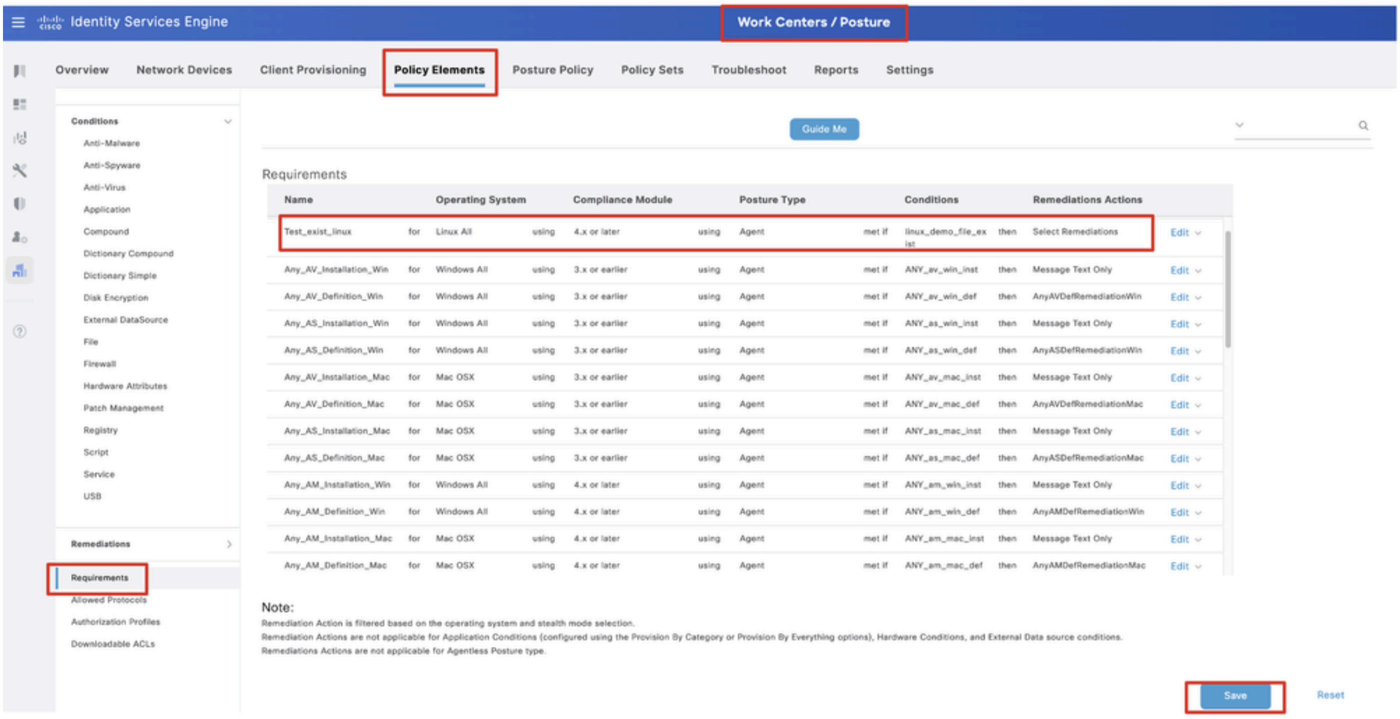
Operating Systems: Linux All

Compliance Module: 4.x or later

Posture Type: Agent

Conditions: linux_demo_file_exist

Click Done and 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

Note: As of now, only shell scripts are supported for Linux agents as remediation.

Step 21. Navigate to Work Centers > Posture > Policy Elements > Authorization Profiles. Click Add.

Step 21.1. Configure the details:

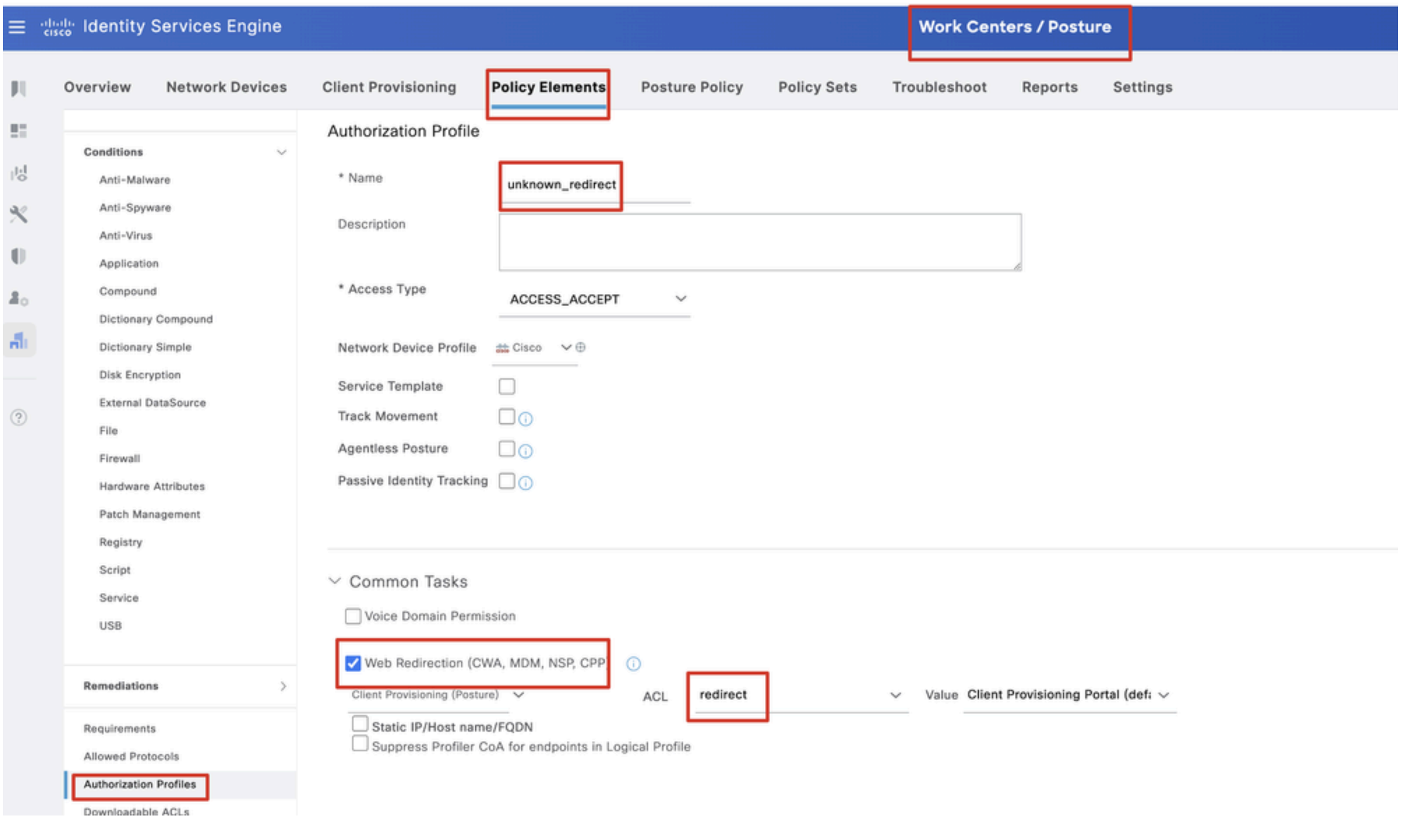
Name: unknown_redirect

Check the checkbox of Web Redirection(CWA,MDM,NSP,CPP)

Select Client Provisioning(Posture)

ACL: redirect

Value: Client Provisioning Portal(default)



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

Note: This ACL name redirect must match the corresponding ACL name configured on FTD.

Step 21.2. Repeat the Add to create another two authorization profiles for non-compliant and compliant endpoints with the details.

Name: non_compliant_profile

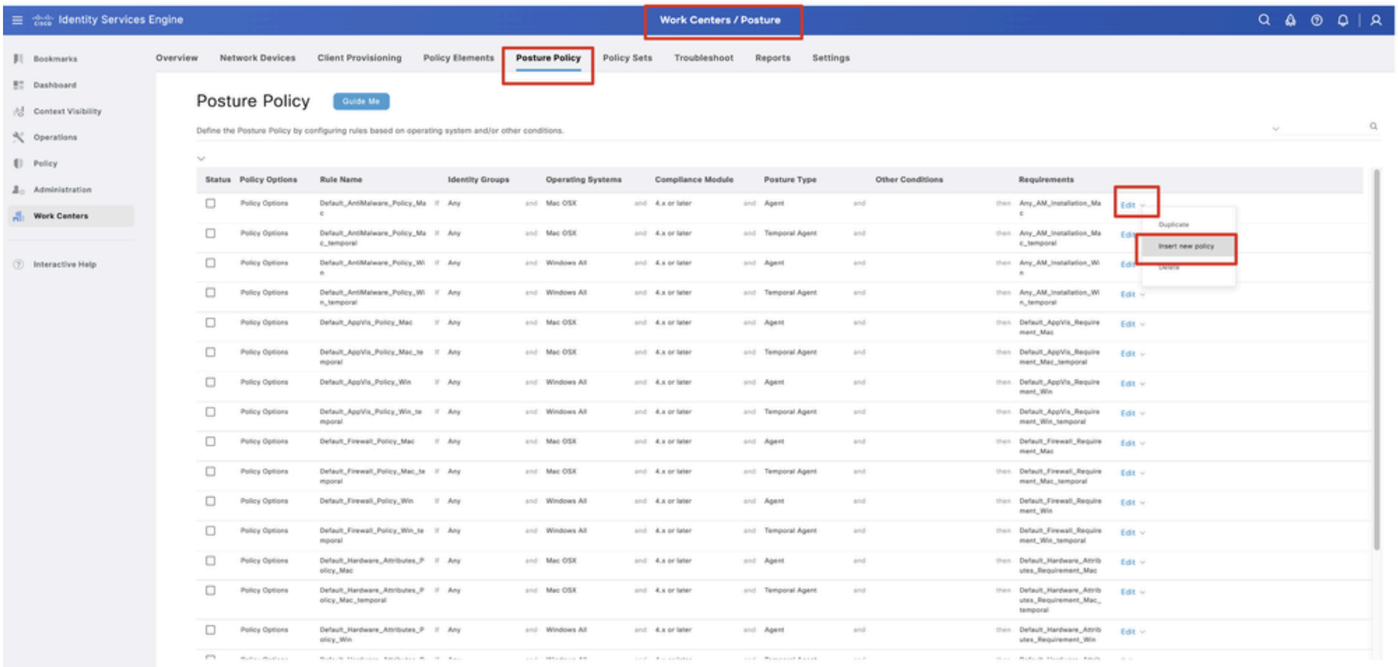
DACL Name: DENY_ALL_IPv4_TRAFFIC

Name: compliant_profile

DACL Name: PERMIT_ALL_IPv4_TRAFFIC

Note: The DACL for compliant or non-compliant endpoints needs to be configured according to the actual requirements.

Step 22. Navigate to Work Centers > Posture > Posture Policy. Click Edit at the end of any rules. Select 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

Step 22.1. Configure the details:

Rule Name: Demo_test_exist_linux

Identity Groups: Any

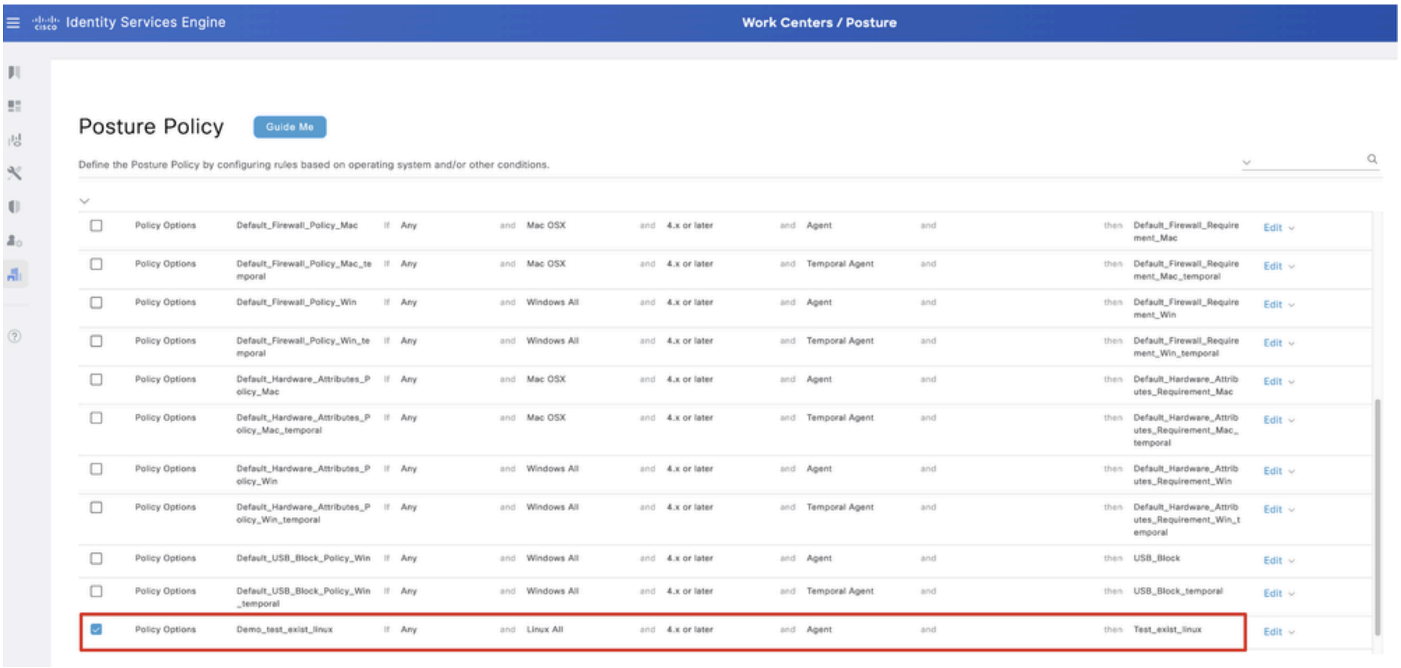
Operating Systems: Linux All

Compliance Module: 4.x or later

Posture Type: Agent

Requirements: Test_exist_linux

Click Done and Save.



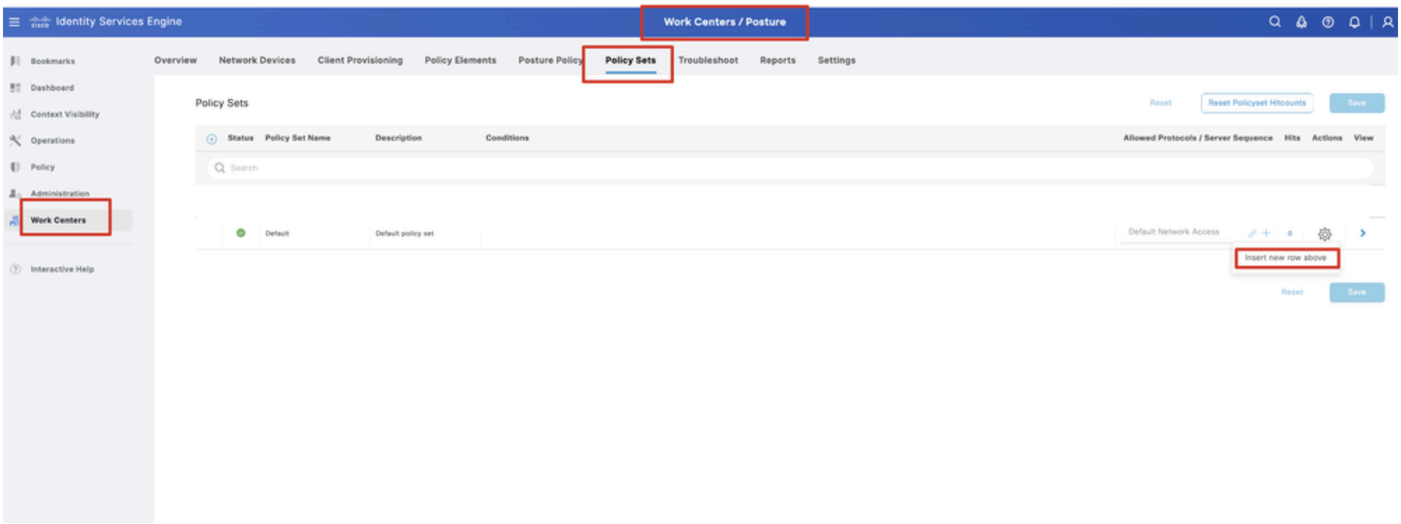
Posture Policy

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

Step 23. Navigate to Work Centers > Posture > Policy Sets. Click to 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	⚙	>

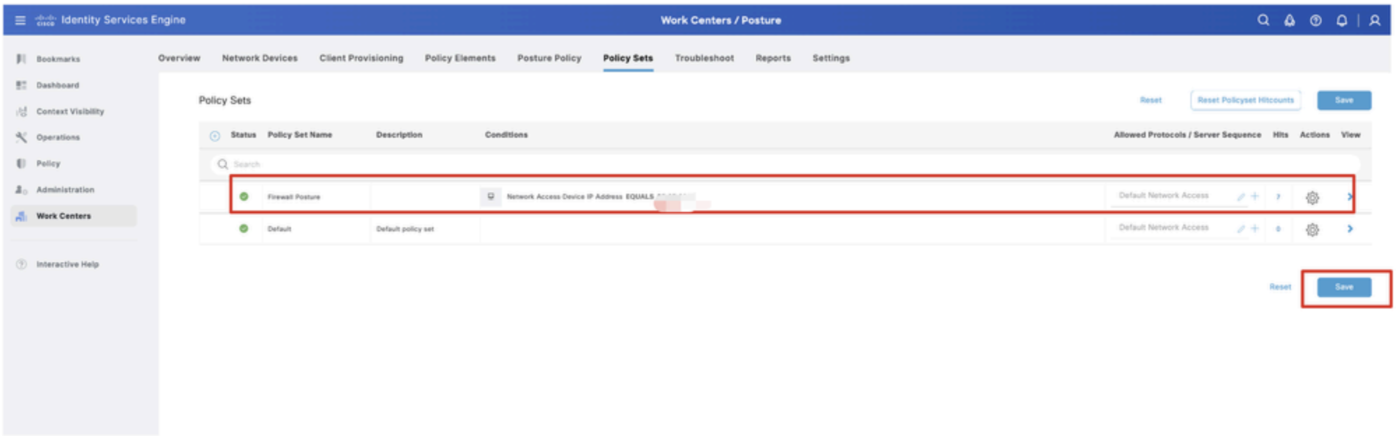
ISE_Add_New_Policy_Set

Step 23.1. Configure the details:

Policy Set Name: Firewall Posture

Conditions: Network Access Device IP Address EQUALs [FTD IP Address]

Click 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		⚙	>
●	Default	Default policy set		Default Network Access	0	⚙	>

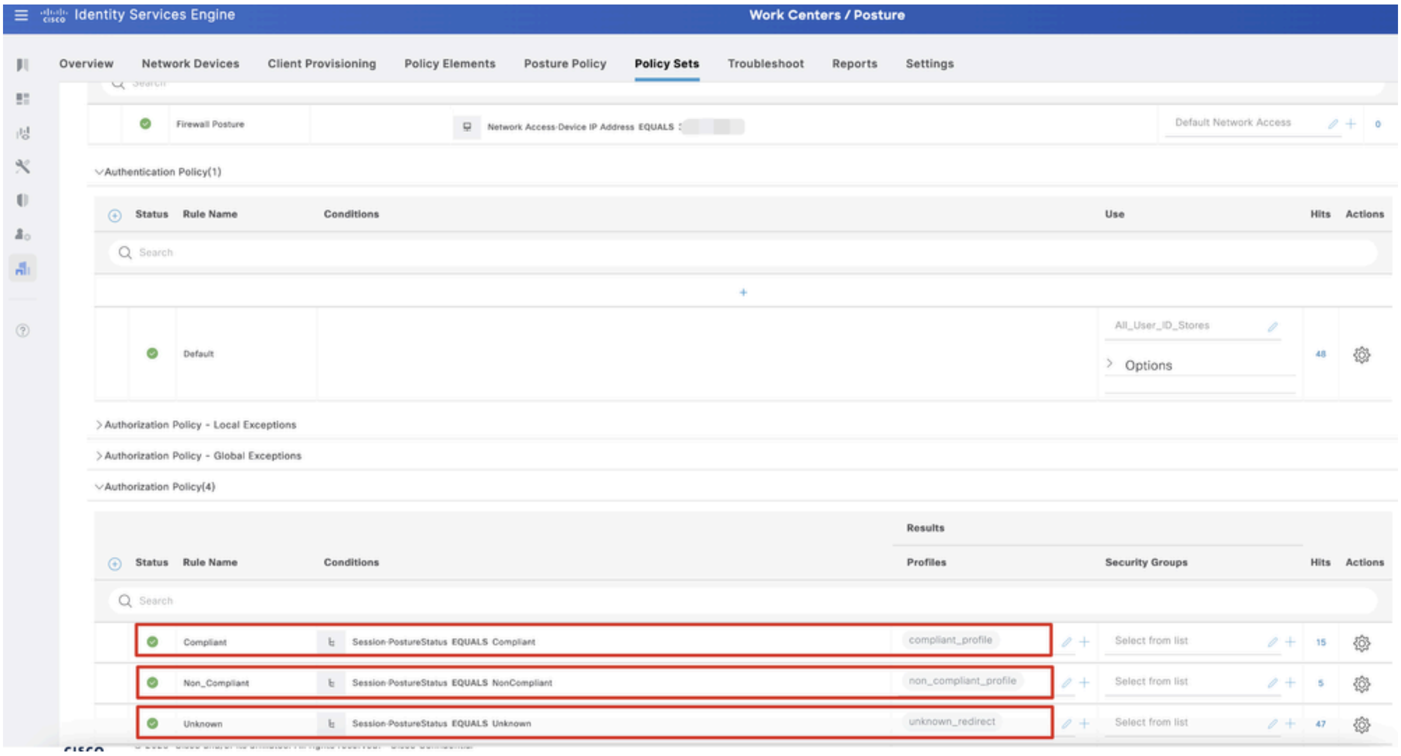
ISE_Add_New_Policy_Set_1

Step 23.2. Click > to enter the policy set. Create new authorization rules for posture compliant, non-compliant, and unknown status. Click Save.

Compliant with compliant_profile

NonCompliant with non_compliant_profile

Unknown with unknown_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

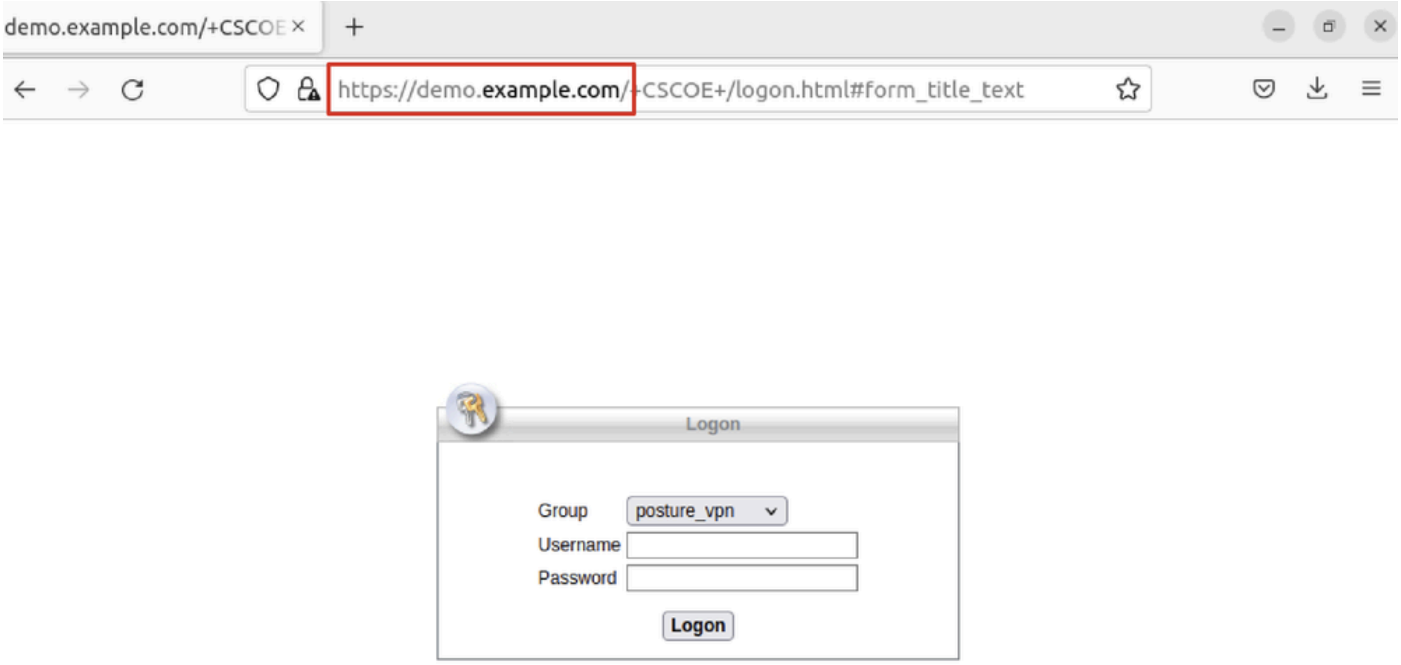
Authorization Policy(4)

			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

Configurations on Ubuntu

Step 24. Login to Ubuntu client via GUI. Open the browser to login the VPN portal. In this example, it is demo.example.com.



Group posture_vpn

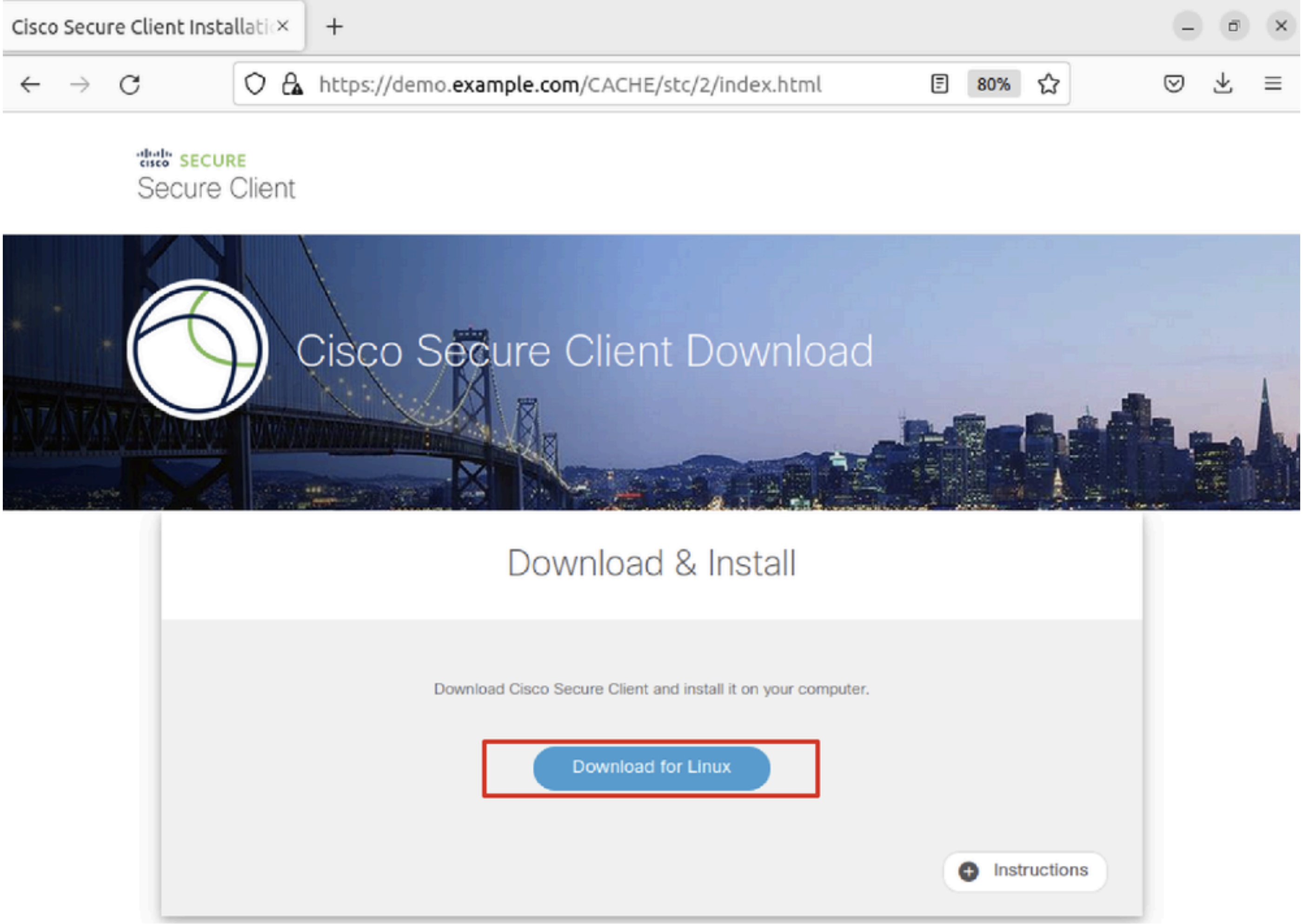
Username

Password

Logon

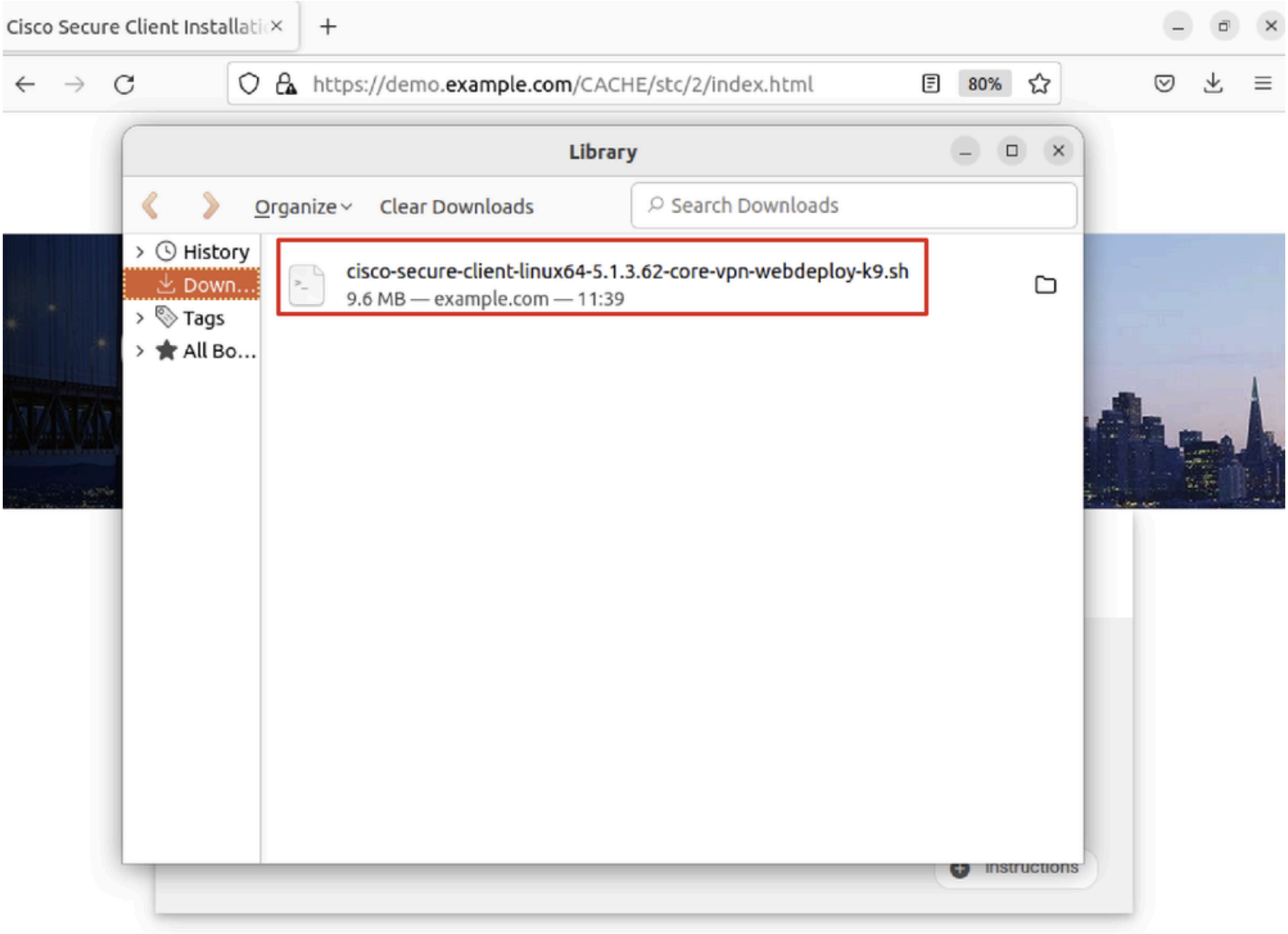
Ubuntu_Browser_VPN_Login

Step 25. Click 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 Cisco Secure Client and install it on your computer.
Download for Linux
Instructions

Ubuntu_Browser_VPN_Download_1

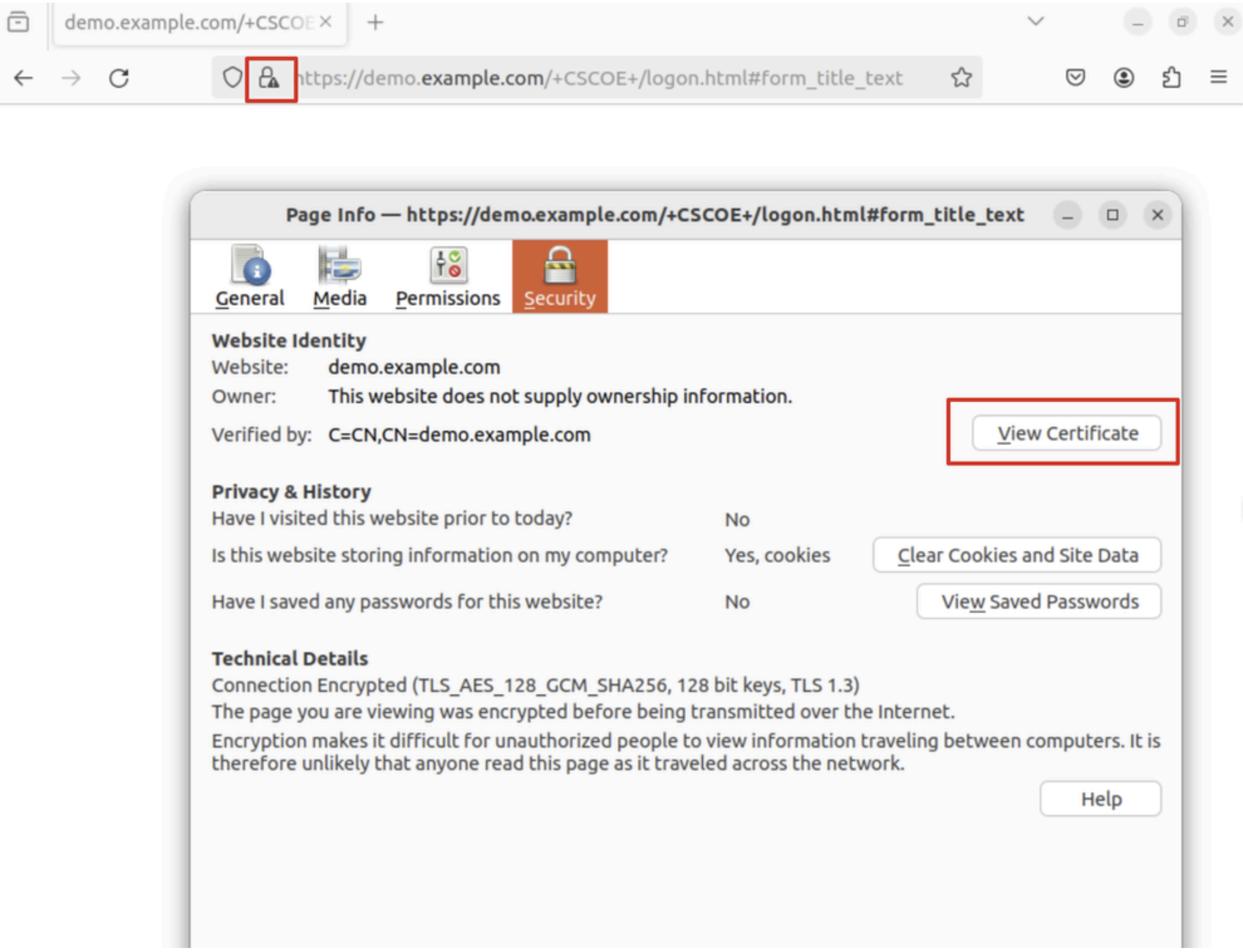
The downloaded file name is cisco-secure-client-linux64-5.1.3.62-core-vpn-webdeploy-k9.sh.



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

Ubuntu_Browser_VPN_Download_2

Step 26. Download VPN certificate through the browser and rename the file to <certificate>.crt. This is the example of using firefox to download the certificate.



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

Step 27. Open the terminal on the Ubuntu client. Navigate to path home/user/Downloads/ to install 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$
```

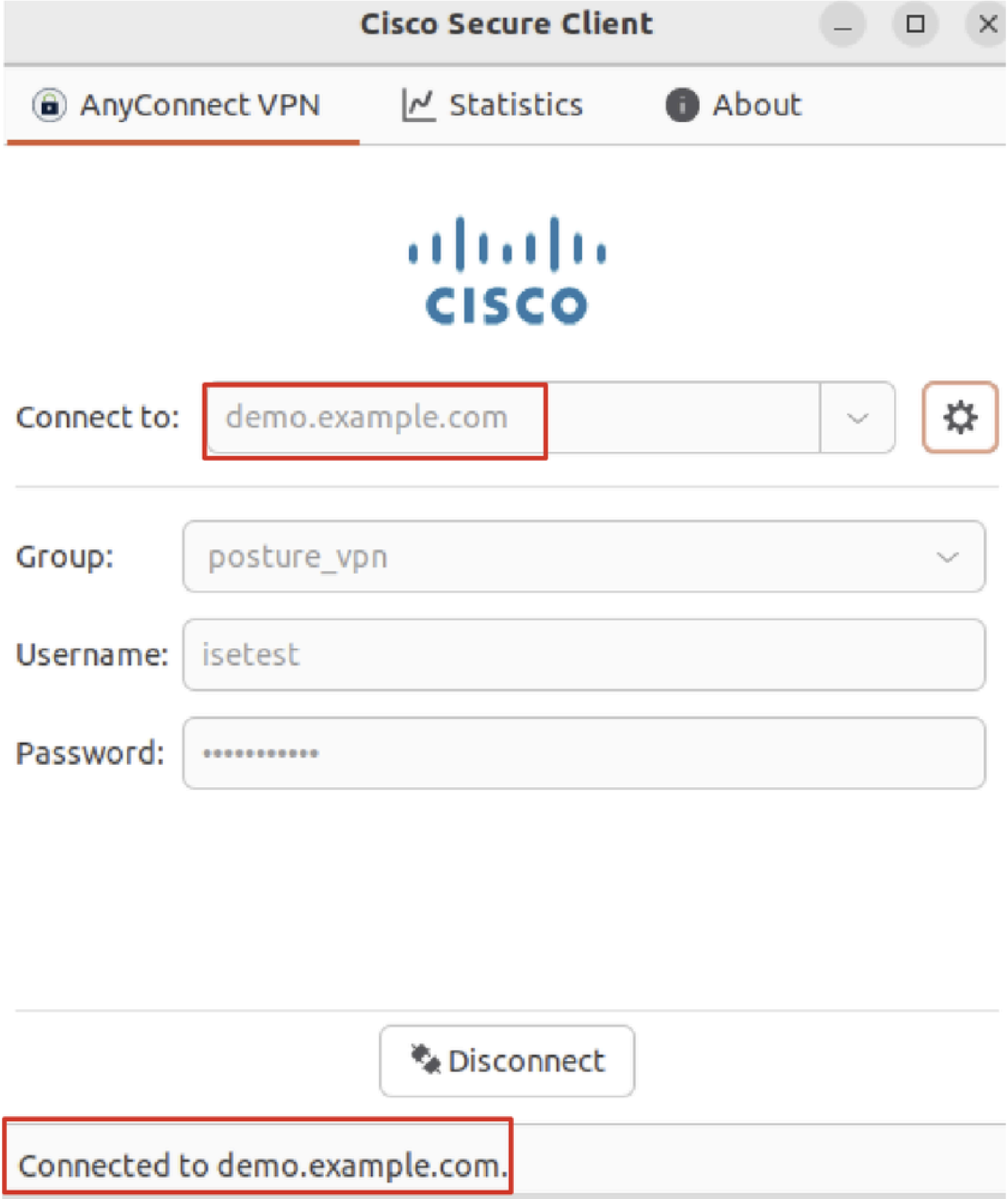
Step 28. Trust the VPN portal certificate on the Ubuntu client.

<#root>

```
user@ubuntu22-desktop:~$

cd Downloads/


user@ubuntu22-desktop:~/Downloads$

ls


cisco-secure-client-linux64-5.1.3.62-core-vpn-webdeploy-k9.sh

demo-example-com.crt


user@ubuntu22-desktop:~/Downloads$

 openssl verify demo-example-com.crt

CN = demo.example.com, C = CN
error 18 at 0 depth lookup: self-signed certificate
Error demo-example-com.crt:

verification failed



user@ubuntu22-desktop:~/Downloads$

sudo cp demo-example-com.crt /usr/local/share/ca-certificates/


user@ubuntu22-desktop:~/Downloads$

sudo update-ca-certificates


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

1 added

, 0 removed; done.
Running hooks in /etc/ca-certificates/update.d...
done.
```

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

openssl verify demo-example-com.crt


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

Step 29. Open Cisco Secure Client on Ubuntu client, and connect VPN to demo.example.com successfully.



Connect to: demo.example.com

Group: posture_vpn

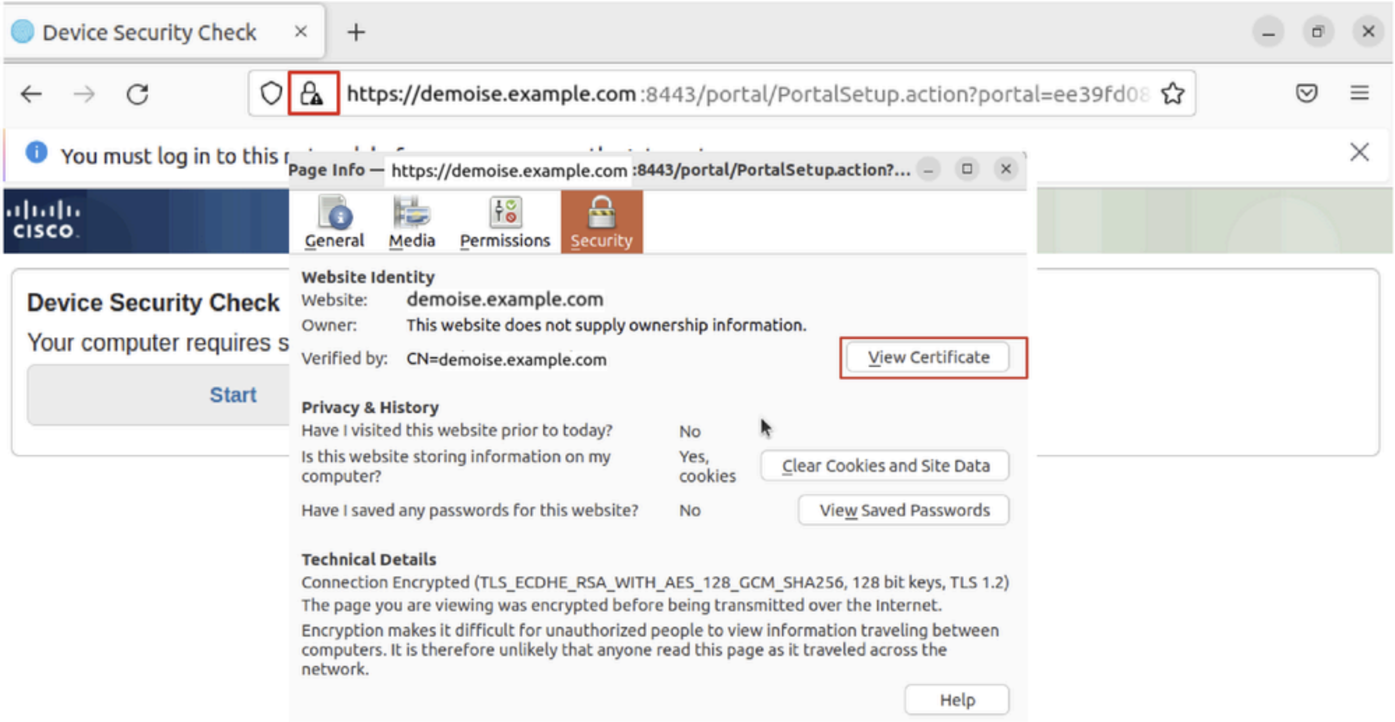
Username: isetest

Password: ••••••••••••

Connected to demo.example.com.

Ubuntu_Secure_Client_Connected

Step 30. Open the browser to access any website triggering the redirection to the ISE CPP portal. Download the certificate from the ISE CPP portal and rename the file to <certificate>.crt. This is an example of using Firefox for downloading.



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

Step 30.1. Trust the ISE CPP portal certificate on the Ubuntu client.

<#root>

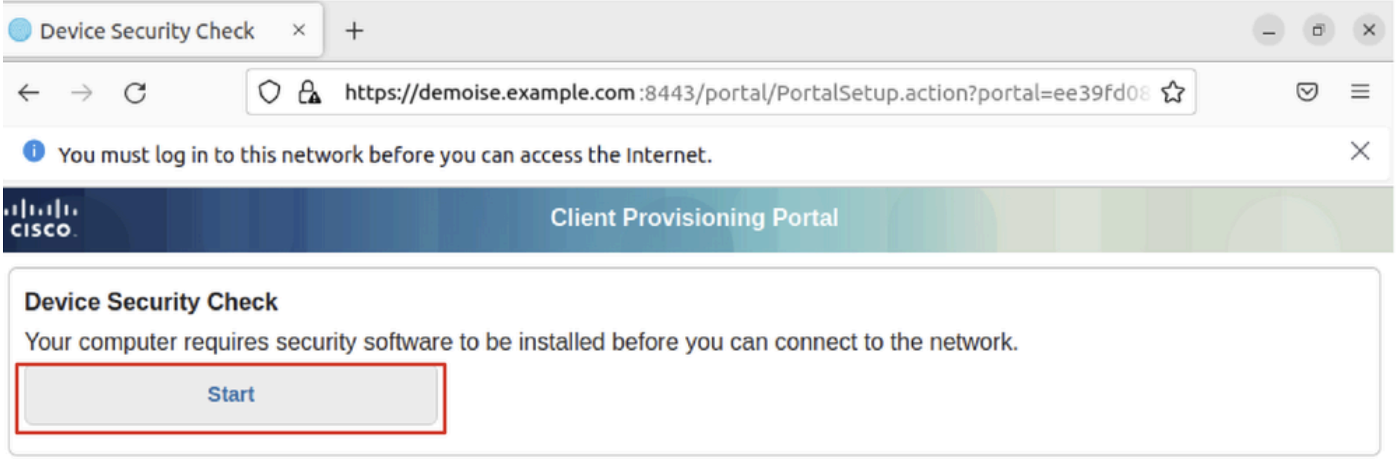
```
user@ubuntu22-desktop:~/Downloads$ ls
cisco-secure-client-linux64-5.1.3.62-core-vpn-webdeploy-k9.sh
demo-example-com.crt

ise-cert.crt
```

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

sudo cp ise-cert.crt /usr/local/share/ca-certificates/
```

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

sudo update-ca-certificates
```

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

1 added

, 0 removed; done.
Running hooks in /etc/ca-certificates/update.d...
done.
```

Step 31. Click Start on the ISE CPP portal.



Device Security Check

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

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

Client Provisioning Portal

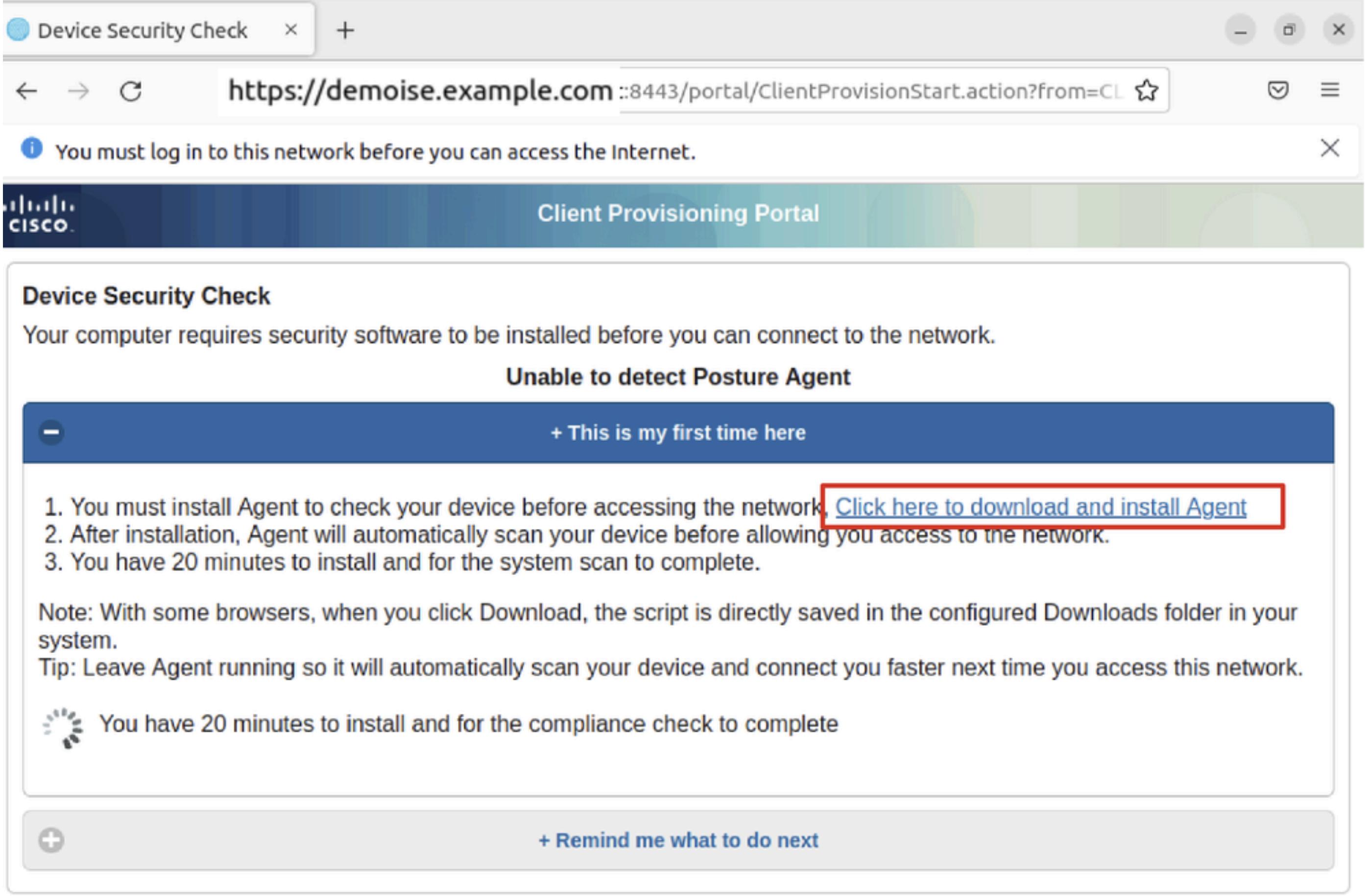
Device Security Check

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

Start

Ubuntu_Browser_CPP_Start

Step 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

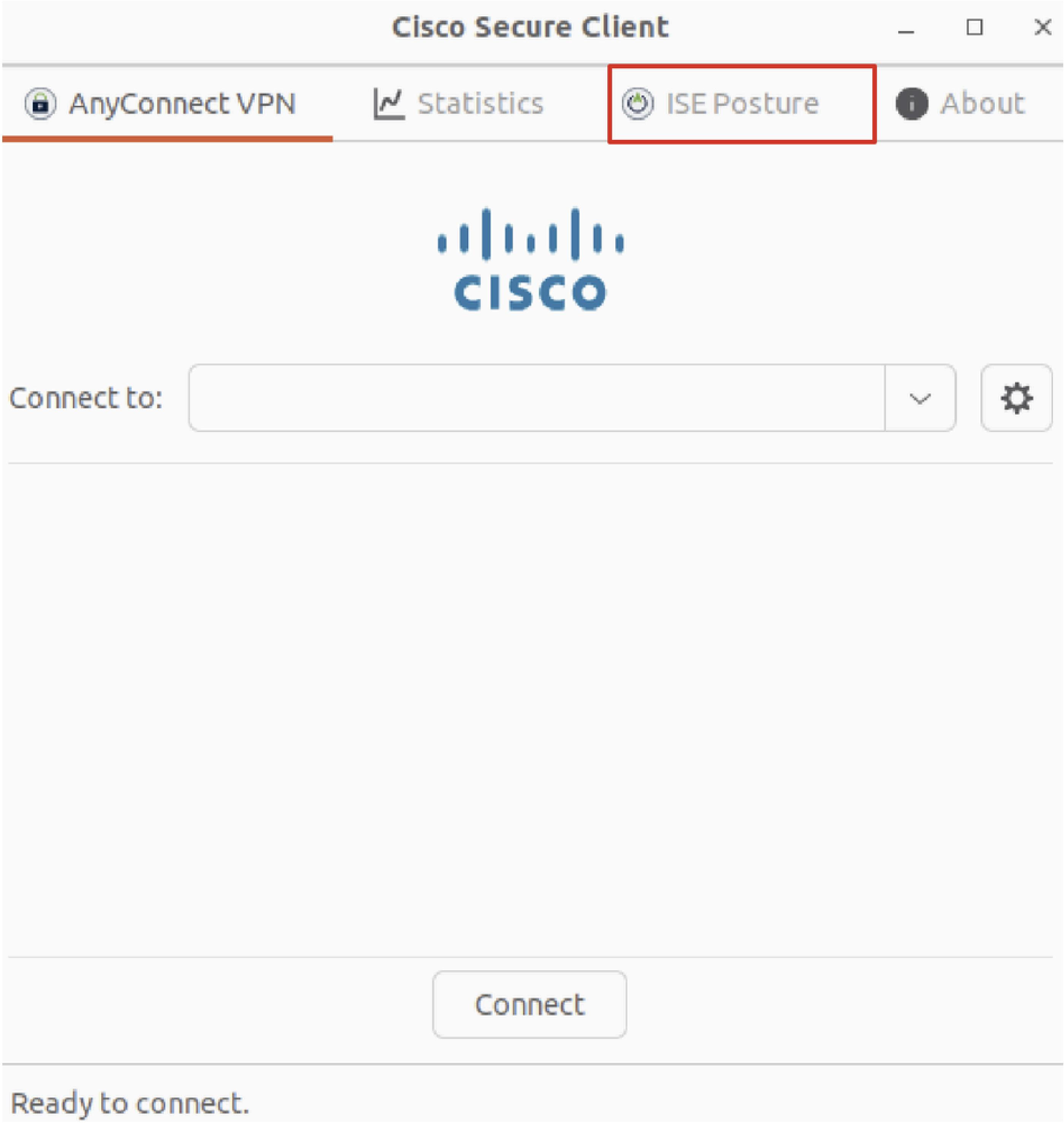
Step 33. Open the terminal on the Ubuntu client. Navigate to path home/user/Downloads/ to install the posture module.

<#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.
```

Step 34. On Ubuntu client UI, quit the Cisco Secure Client and reopen it. The ISE Posture module is installed and run successfully.



Ubuntu_Secure_Client_ISE_Posture_Installed

Step 35. Open the terminal on the Ubuntu client. Navigate to path home/user/Desktop , create a test.txt file to meet the file condition configured on ISE.

<#root>

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

cd Desktop/

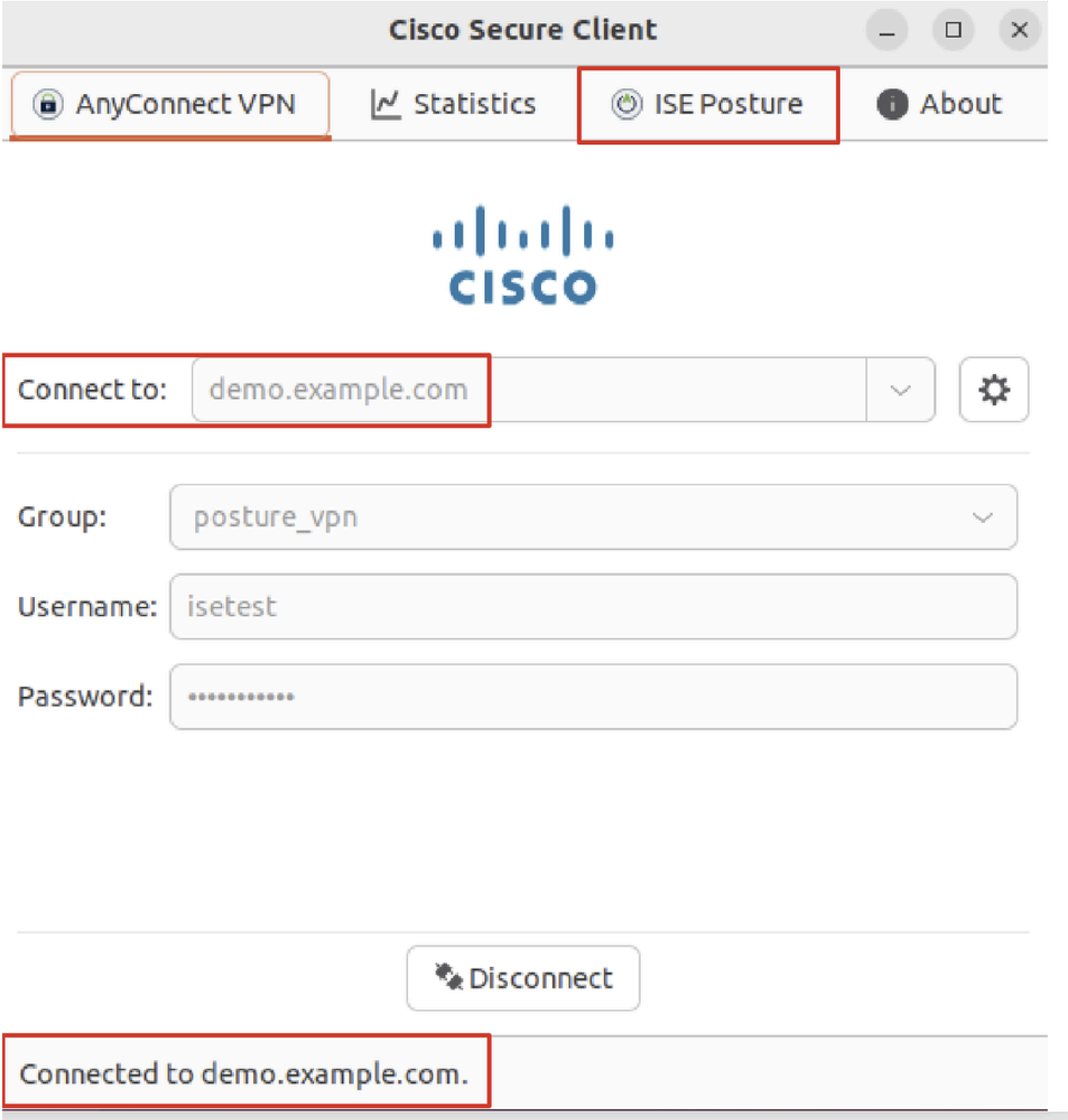
```
user@ubuntu22-desktop:~/Desktop$
```

echo test > test.txt

Verify

Use this section in order to confirm that your configuration works properly.

Step 1. Connect VPN to demo.example.com on Ubuntu client.



Connect to: demo.example.com

Group: posture_vpn

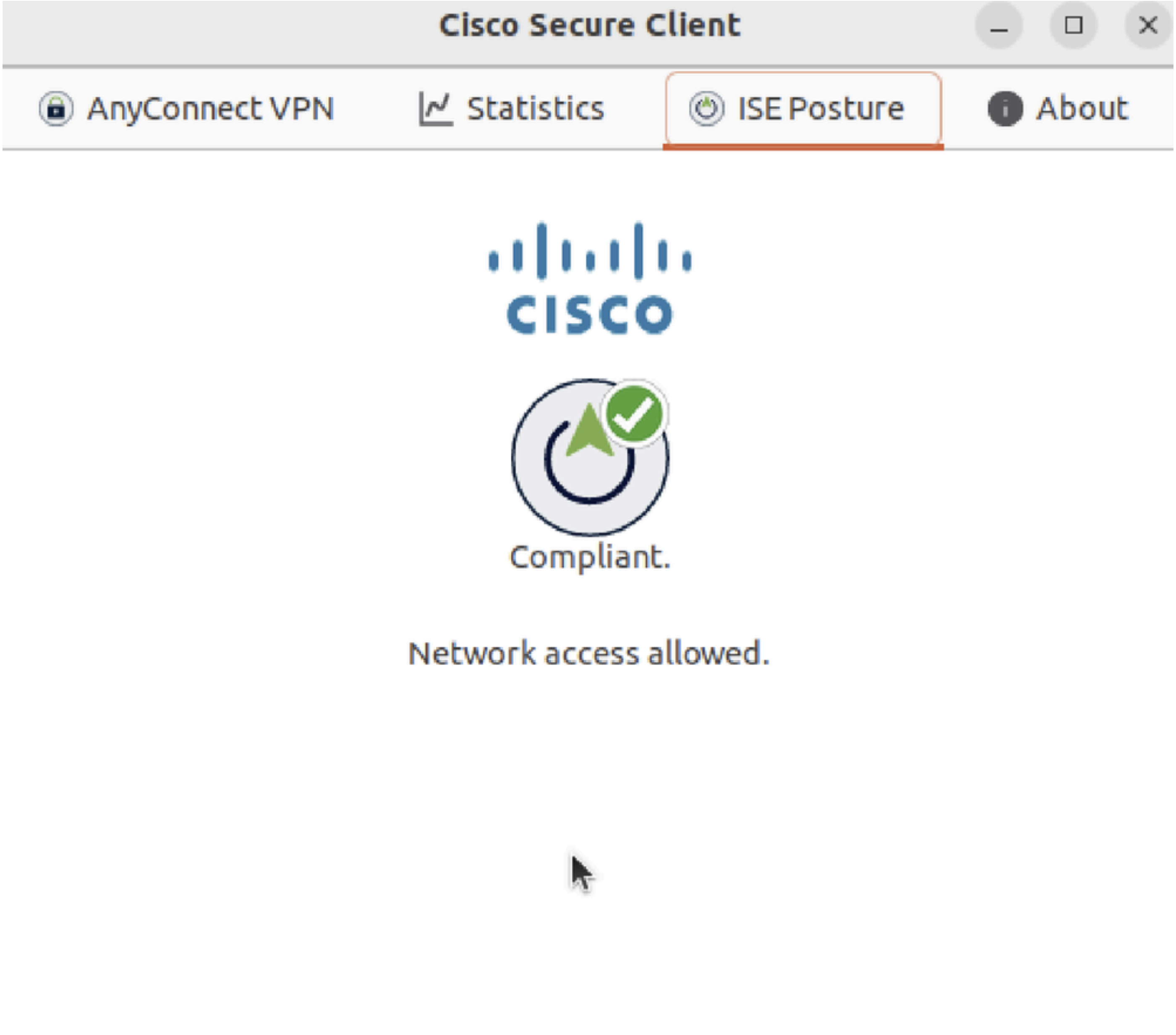
Username: isetest

Password: ••••••••••••

Connected to demo.example.com.

Verify_Ubuntu_Secure_Client_Connected

Step 2. Check the ISE Posture status on the Ubuntu client.

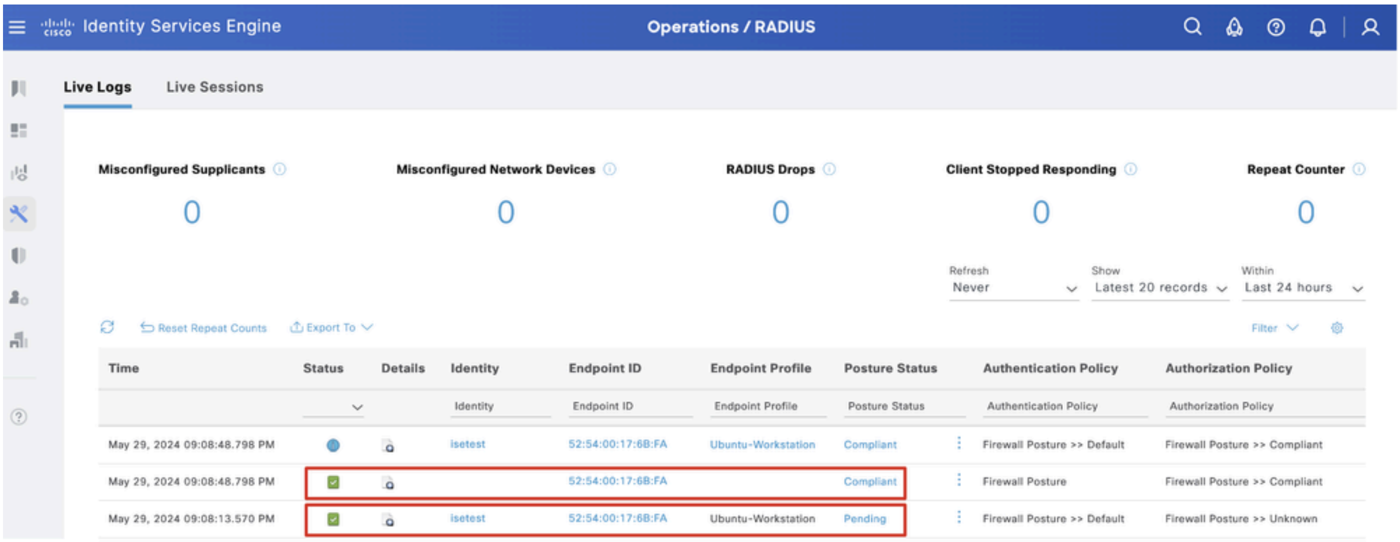


Compliant.

Network access allowed.

Verify_Ubuntu_Secure_Client_Compliant

Step 3. Check Radius Live Log on ISE. Navigate to Operations > RADIUS Live Log.



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

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

Time	Status	Details	Identity	Endpoint ID	Endpoint Profile	Posture Status	Authentication Policy	Authorization Policy
May 29, 2024 09:08:48.798 PM	●		isetest	52:54:00:17:6B:FA	Ubuntu-Workstation	Compliant	Firewall Posture >> Default	Firewall Posture >> Compliant
May 29, 2024 09:08:48.798 PM	✓			52:54:00:17:6B:FA		Compliant	Firewall Posture	Firewall Posture >> Compliant
May 29, 2024 09:08:13.570 PM	✓		isetest	52:54:00:17:6B:FA	Ubuntu-Workstation	Pending	Firewall Posture >> Default	Firewall Posture >> Unknown

Verify_ISE_LiveLog

Step 4. Navigate to FTD CLI via SSH or console.

<#root>

```
>
>
```

`system support diagnostic-cli`

```
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.

ftdv741>
```

`enable`

```
Password:
ftdv741#
ftdv741#
```

`show vpn-sessiondb detail anyconnect`

```
Session Type: AnyConnect Detailed

Username : isetest Index : 33
Assigned IP : 192.168.6.30 Public IP : 192.168.10.13
Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License : AnyConnect Premium
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES-GCM-128 DTLS-Tunnel: (1)AES-GCM-256
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA256 DTLS-Tunnel: (1)SHA384
Bytes Tx : 51596 Bytes Rx : 17606
Pkts Tx : 107 Pkts Rx : 136
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Group Policy : posture_gp Tunnel Group : posture_vpn
Login Time : 14:02:25 UTC Fri May 31 2024
Duration : 0h:00m:55s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A VLAN : none
Audt Sess ID : cb007182000210006659d871
Security Grp : none Tunnel Zone : 0

AnyConnect-Parent Tunnels: 1
SSL-Tunnel Tunnels: 1
DTLS-Tunnel Tunnels: 1

AnyConnect-Parent:
Tunnel ID : 33.1
Public IP : 192.168.10.13
Encryption : none Hashing : none
TCP Src Port : 59180 TCP Dst Port : 443
Auth Mode : userPassword
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Client OS : linux-64
```

`Client OS Ver: Ubuntu 22.04 LTS 22.04 (Jammy Jellyfish)`

```
Client Type : AnyConnect

Client Ver : Cisco AnyConnect VPN Agent for Linux 5.1.3.62


Bytes Tx : 6364 Bytes Rx : 0
Pkts Tx : 1 Pkts Rx : 0
Pkts Tx Drop : 0 Pkts Rx Drop : 0

SSL-Tunnel:
Tunnel ID : 33.2
Assigned IP :192.168.6.30 Public IP : 192.168.10.13
Encryption : AES-GCM-128 Hashing : SHA256
Ciphersuite : TLS_AES_128_GCM_SHA256
Encapsulation: TLSv1.3 TCP Src Port : 59182
TCP Dst Port : 443 Auth Mode : userPassword
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Client OS : Linux_64
Client Type : SSL VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Linux 5.1.3.62
Bytes Tx : 6364 Bytes Rx : 498
Pkts Tx : 1 Pkts Rx : 6
Pkts Tx Drop : 0 Pkts Rx Drop : 0

Filter Name : #ACSACL#-IP-PERMIT_ALL_IPV4_TRAFFIC-57f6b0d3



DTLS-Tunnel:
Tunnel ID : 33.3
Assigned IP :192.168.6.30 Public IP : 192.168.10.13
Encryption : AES-GCM-256 Hashing : SHA384
Ciphersuite : ECDHE-ECDSA-AES256-GCM-SHA384
Encapsulation: DTLSv1.2 UDP Src Port : 56078
UDP Dst Port : 443 Auth Mode : userPassword
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Client OS : Linux_64
Client Type : DTLS VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Linux 5.1.3.62
Bytes Tx : 38868 Bytes Rx : 17108
Pkts Tx : 105 Pkts Rx : 130
Pkts Tx Drop : 0 Pkts Rx Drop : 0

Filter Name : #ACSACL#-IP-PERMIT_ALL_IPV4_TRAFFIC-57f6b0d3
```

Troubleshoot

This section provides information you can use in order to troubleshoot your configuration.

For posture flow and troubleshooting Cisco Secure Client and ISE, check the CCO documents**ISE Posture Style Comparison for Pre and Post 2.2** and **Troubleshoot ISE Session Management and Posture.**

Related Information

- Cisco Identity Services Engine Network Component Compatibility, Release 3.3
- Cisco Identity Services Engine Administrator Guide, Release 3.3
- **Cisco Technical Support & Downloads**