使用ISE 3.3配置Linux VPN终端安全评估

目录

简介

本文档介绍如何使用身份服务引擎(ISE)和Firepower威胁防御(FTD)配置Linux VPN状态。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科安全客户端
- 基于Firepower威胁防御(FTD)的远程访问VPN
- 身份服务引擎 (ISE)

使用的组件

本文档中的信息基于以下软件版本：

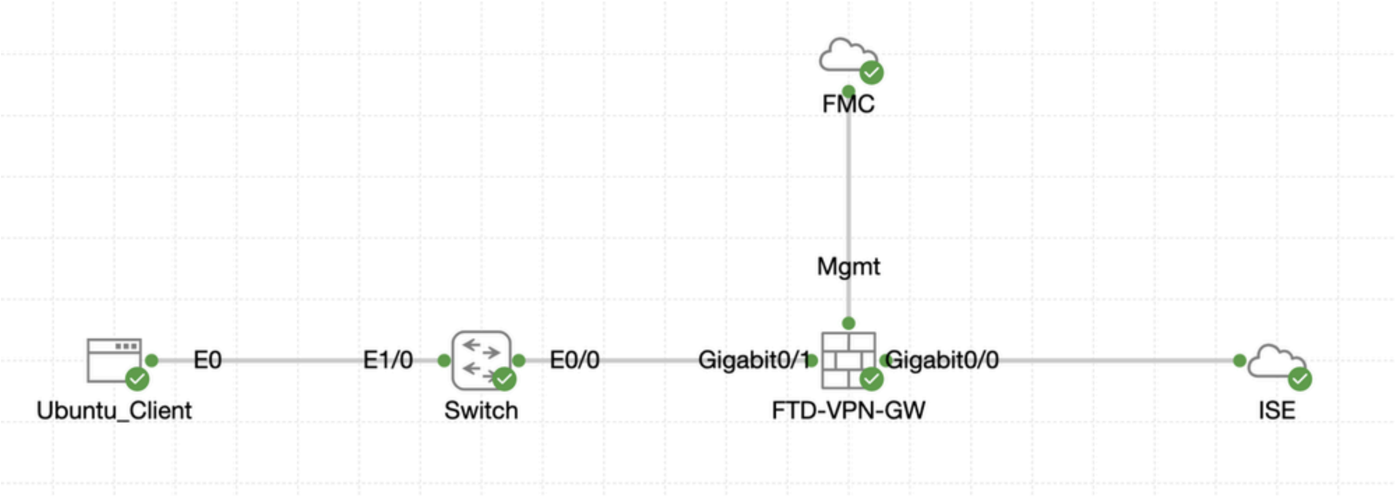
- Ubuntu 22.04
- 思科安全客户端5.1.3.62

- 思科Firepower威胁防御(FTD) 7.4.1
- 思科Firepower管理中心(FMC) 7.4.1
- 思科身份服务引擎(ISE) 3.3

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

配置

网络图



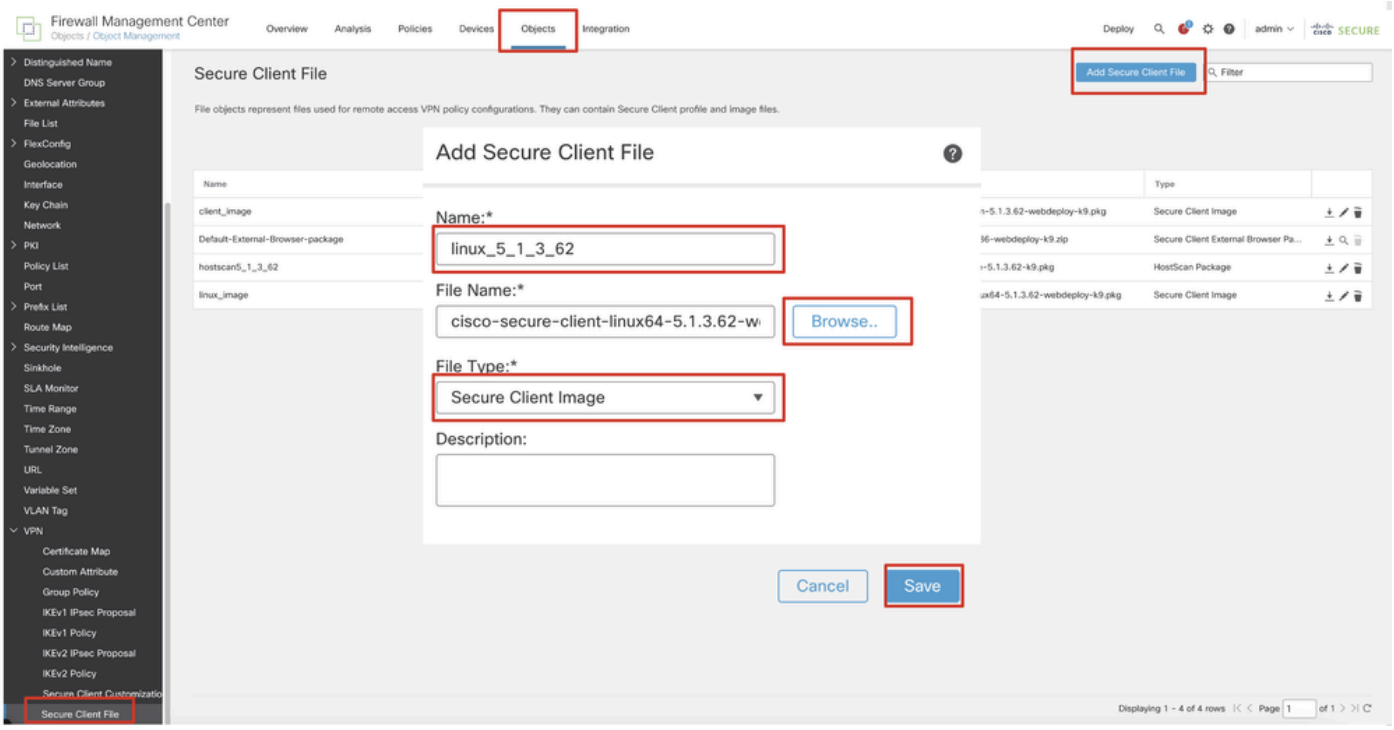
拓扑

FMC/FTD上的配置

步骤1:客户端、FTD、FMC和ISE之间的连接已成功配置。因为enroll.cisco.com用于执行重定向探测的终端(有关详细信息，请参阅终端安全评估流量CCO 文档ISE终端安全评估样式比较以前版本和之后2.2)。确保正确配置了FTD上通往enroll.cisco.com的流量的路由。

第二步：从Cisco软件下载下载软件包名称cisco-secure-client-linux64-5.1.3.62-webdeploy-k9.pkg，通过确认下载文件的md5校验和与Cisco软件下载页相同，确保文件在下载后一切正常。

第三步： 导航到Objects > Object Management > VPN > Secure Client File。单击Add Secure Client File、提供名称、浏览File Name以选择cisco-secure-client-linux64-5.1.3.62-webdeploy-k9.pkg、在File Type下拉列表中选择Secure Client Image。？？然后单击.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

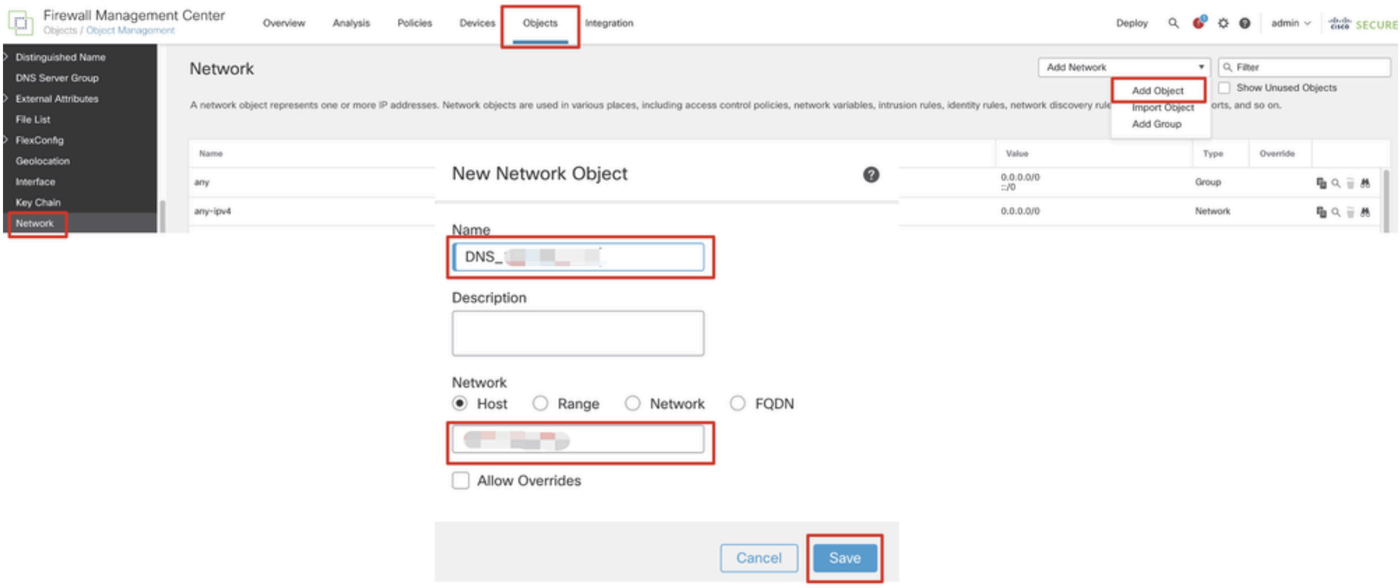
File Type:* Secure Client Image

Description:

FMC_Upload_Secure_Client_Image

第四步： 导航到Objects > Object Management > Network。

步骤 4.1为DNS服务器创建对象。单击Add Object，提供名称和可用的DNS IP地址。单击。Save



Network

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

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

New Network Object

Name: DNS_[redacted]

Description

Network ● Host ○ Range ○ Network ○ FQDN

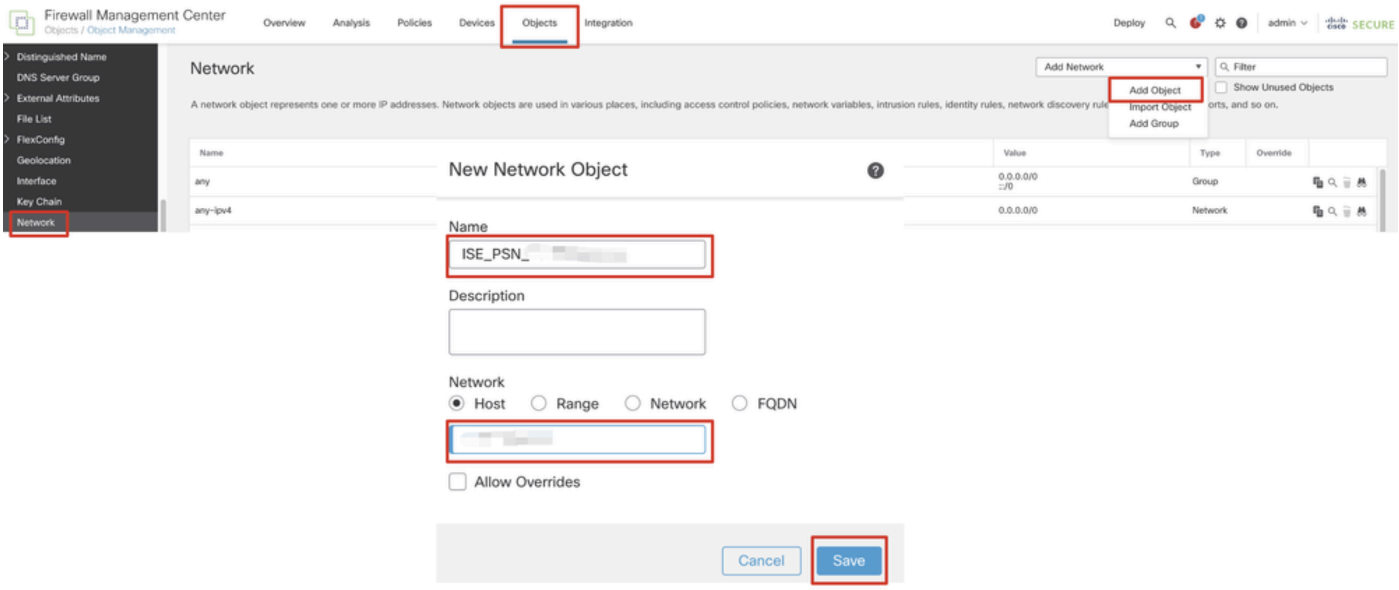
[redacted]

□ Allow Overrides

FMC_Add_Object_DNS

注意：此处配置的DNS服务器将用于VPN用户。

步骤 4.2为ISE PSN创建对象。单击Add Object，提供名称和可用的ISE PSN IP地址。单击。Save



Network

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

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

New Network Object

Name: ISE_PSN_[redacted]

Description:

Network: ● Host ○ Range ○ Network ○ FQDN

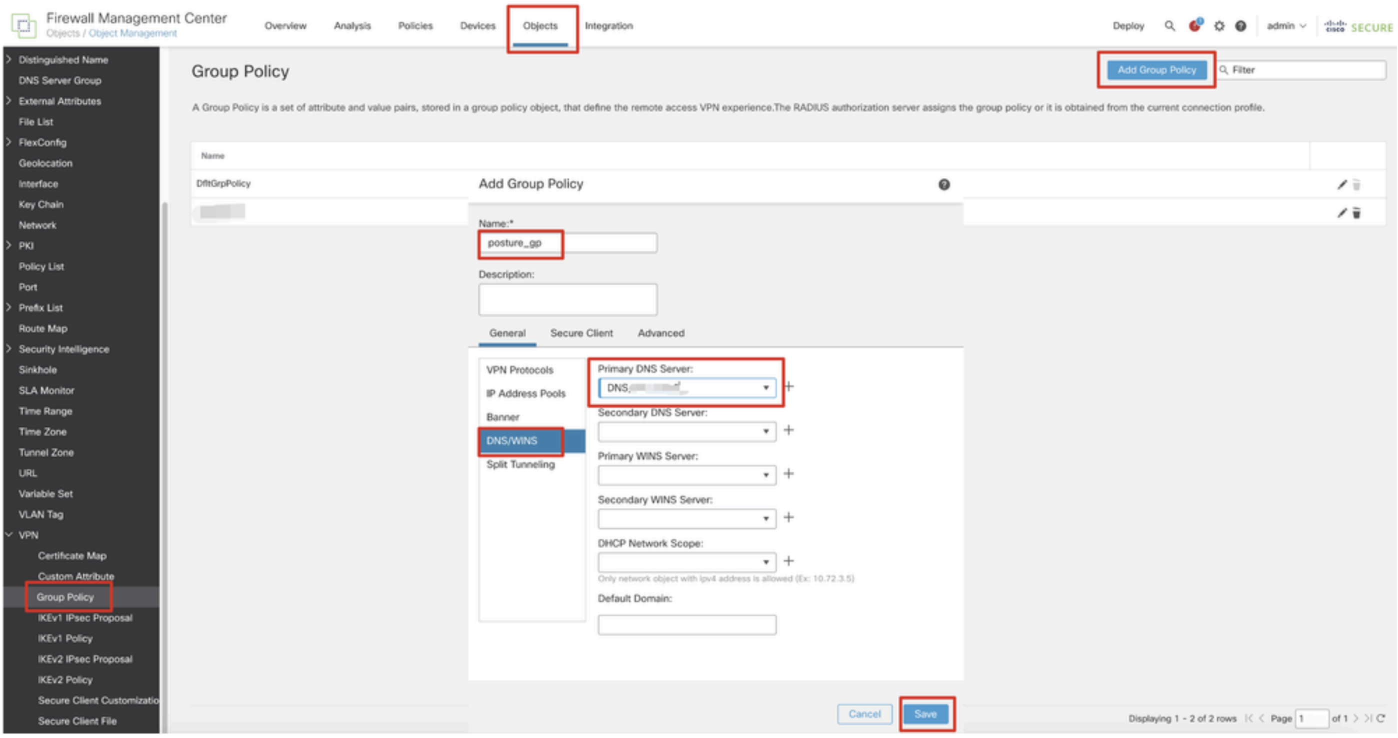
[redacted]

□ Allow Overrides

Cancel Save

FMC_Add_Object_ISE

第五步：导航到Objects > Object Management > VPN > Group Policy。单击。Add Group Policy单击DNS/WINS，然后在Primary DNS Server中选择DNS服务器的对象。？？然后单击.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.

Name
DfltGrpPolicy
[redacted]

Add Group Policy

Name:* posture_gp

Description:

Primary DNS Server: DNS_[redacted]

Secondary DNS Server:

Primary WINS Server:

Secondary WINS Server:

DHCP Network Scope:

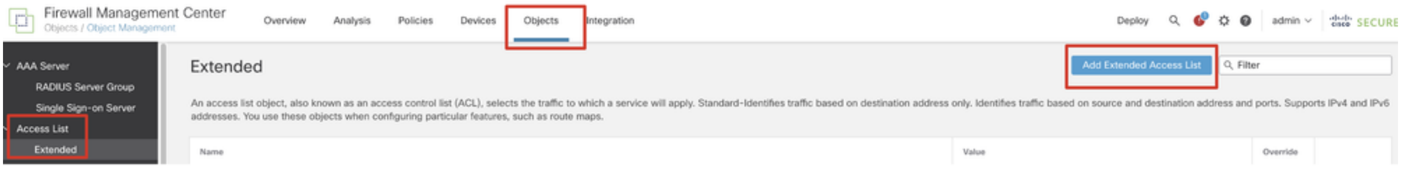
Only network object with ipv4 address is allowed (Ex: 10.72.3.5)

Default Domain:

FMC_Add_Group_Policy

注意：确保VPN组策略中使用的DNS服务器可以解析ISE客户端调配门户FQDN和enroll.cisco.com。

第六步： 导航到Objects > Object Management > Access List > Extended。单击。Add Extended Access List

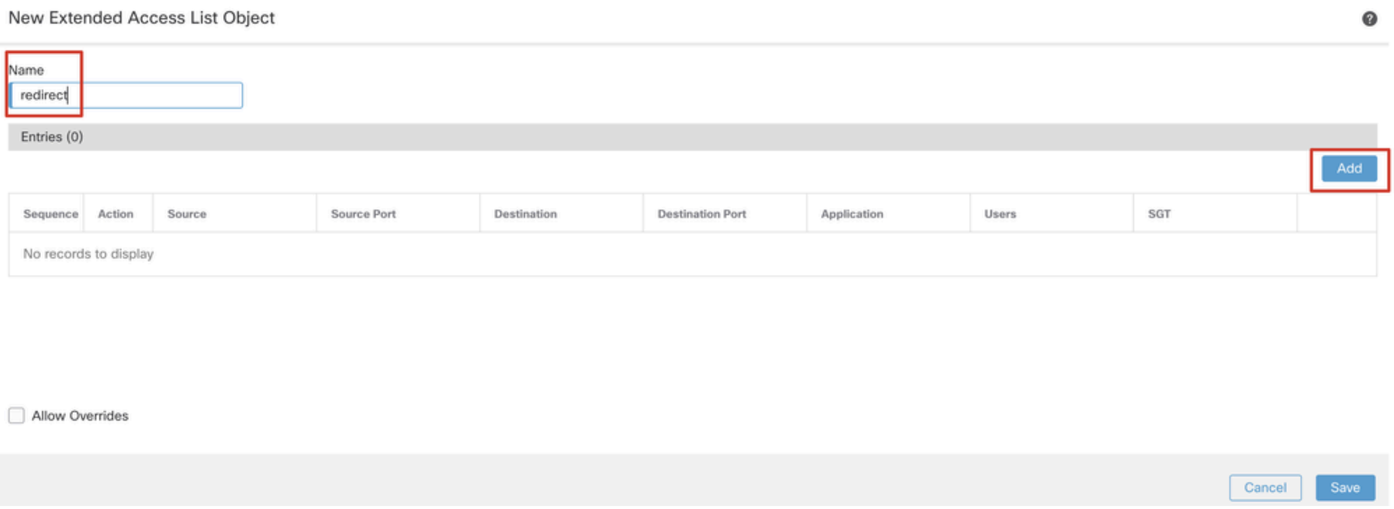


Extended

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

步骤 6.1提供重定向ACL的名称。此名称必须与ISE授权配置文件中的名称相同。单击。Add



New Extended Access List Object

Name: redirect

Entries (0)

Add

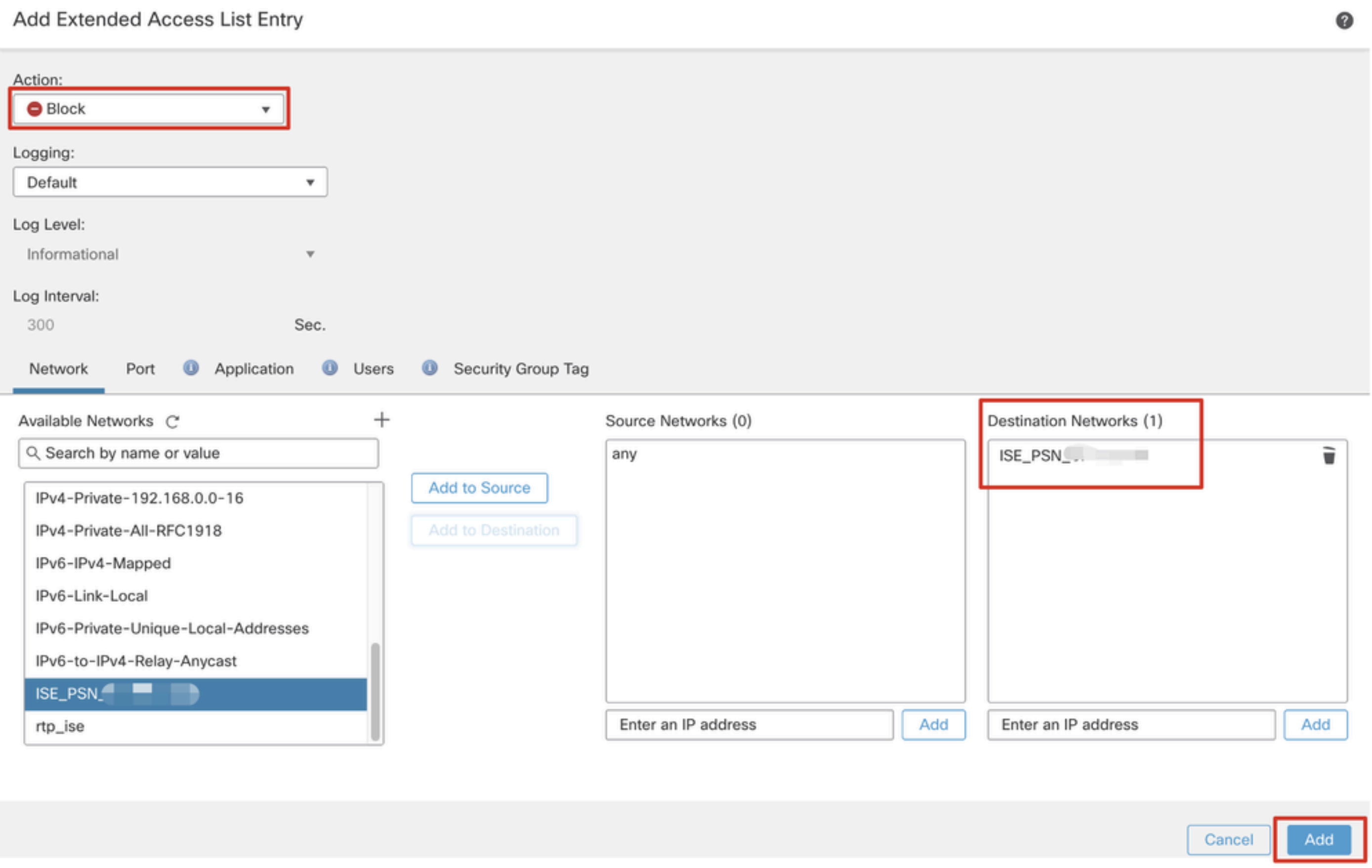
Sequence	Action	Source	Source Port	Destination	Destination Port	Application	Users	SGT
No records to display								

□ Allow Overrides

Cancel Save

FMC_Add_Redirect_ACL_Part_1

步骤 6.2 阻止DNS流量、发往ISE PSN IP地址的流量以及补救服务器，以将其排除在重定向范围之外。允许其余流量。这将触发重定向。单击。Save



Add Extended Access List Entry

Action: Block

Logging: Default

Log Level: Informational

Log Interval: 300 Sec.

Network | Port | Application | Users | Security Group Tag

Available Networks

Search by name or value

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

Add to Source

Add to Destination

Source Networks (0)

any

Enter an IP address Add

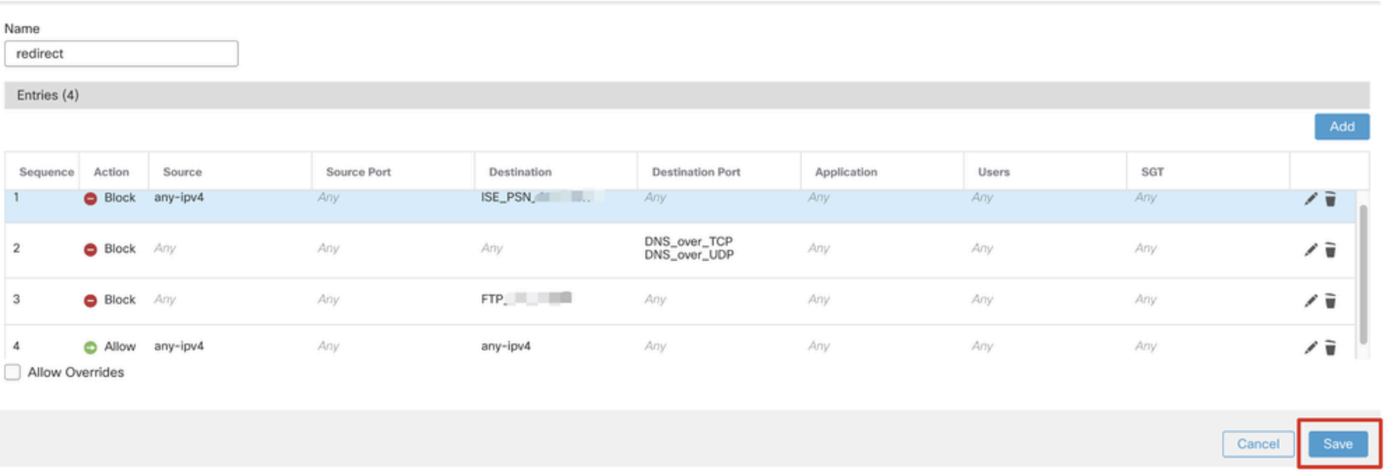
Destination Networks (1)

ISE_PSN_[redacted]

Enter an IP address Add

Cancel Add

FMC_Add_Redirect_ACL_Part_2



Name

redirect

Entries (4)

Add

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

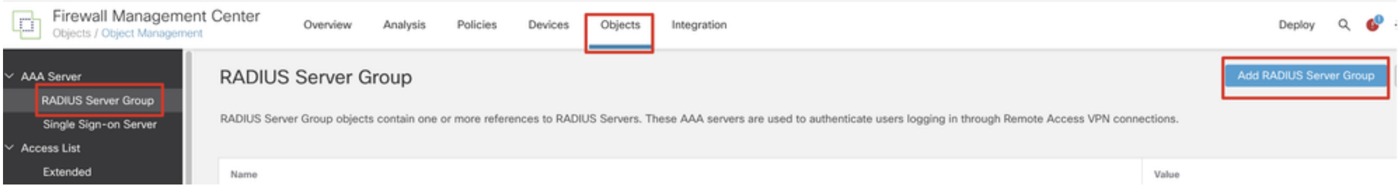
□ Allow Overrides

Cancel Save

FMC_Add_Redirect_ACL_Part_3

注意：此重定向ACL示例中的目标FTP用作补救服务器示例。

步骤 7. 导航到Objects > Object Management > RADIUS Server Group。单击。Add RADIUS Server Group

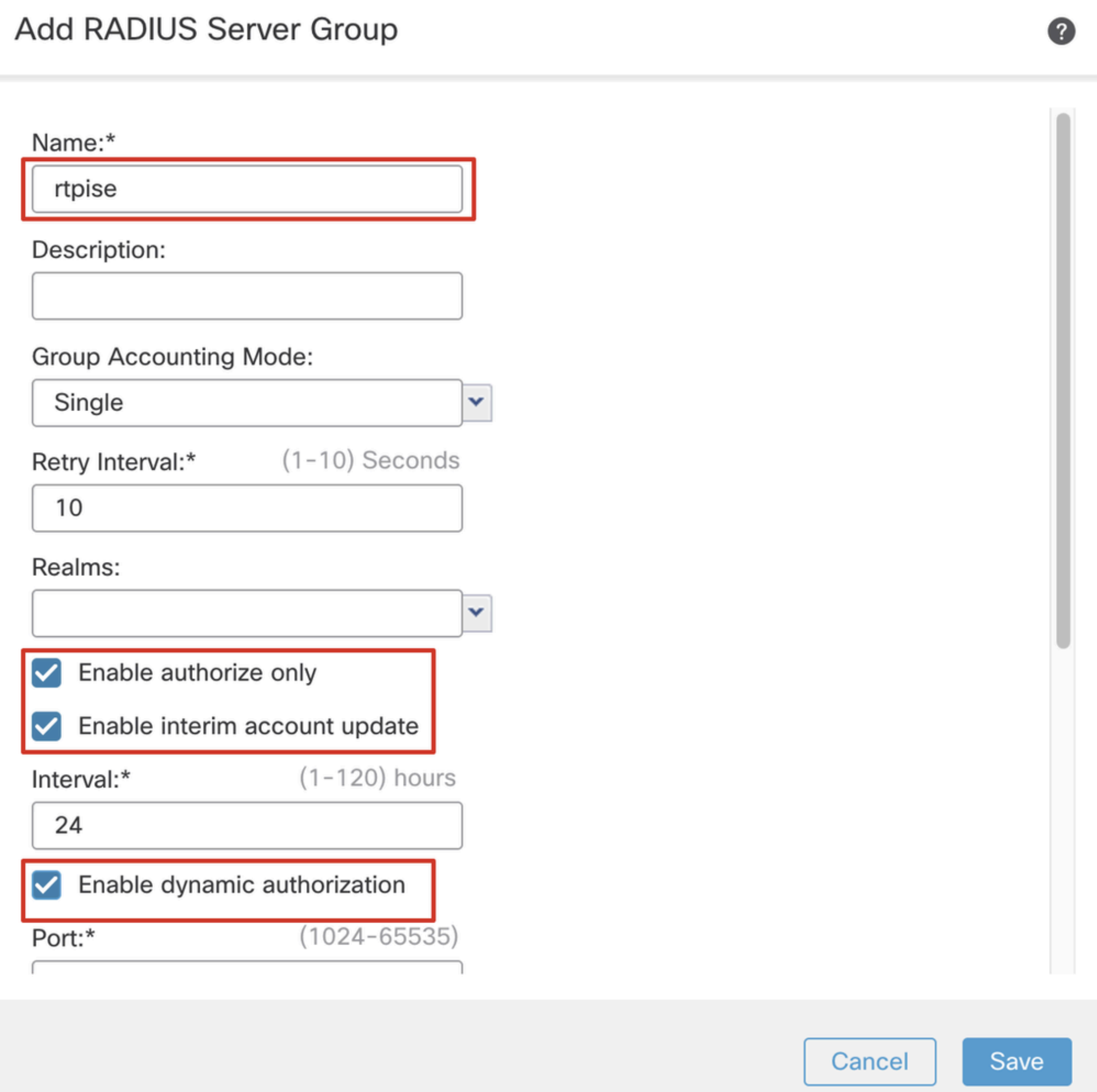


RADIUS Server Group

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

FMC_Add_New_Radius_Server_Group

步骤 7.1提供名称、检查Enable authorize only、检查Enable interim account update、检查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

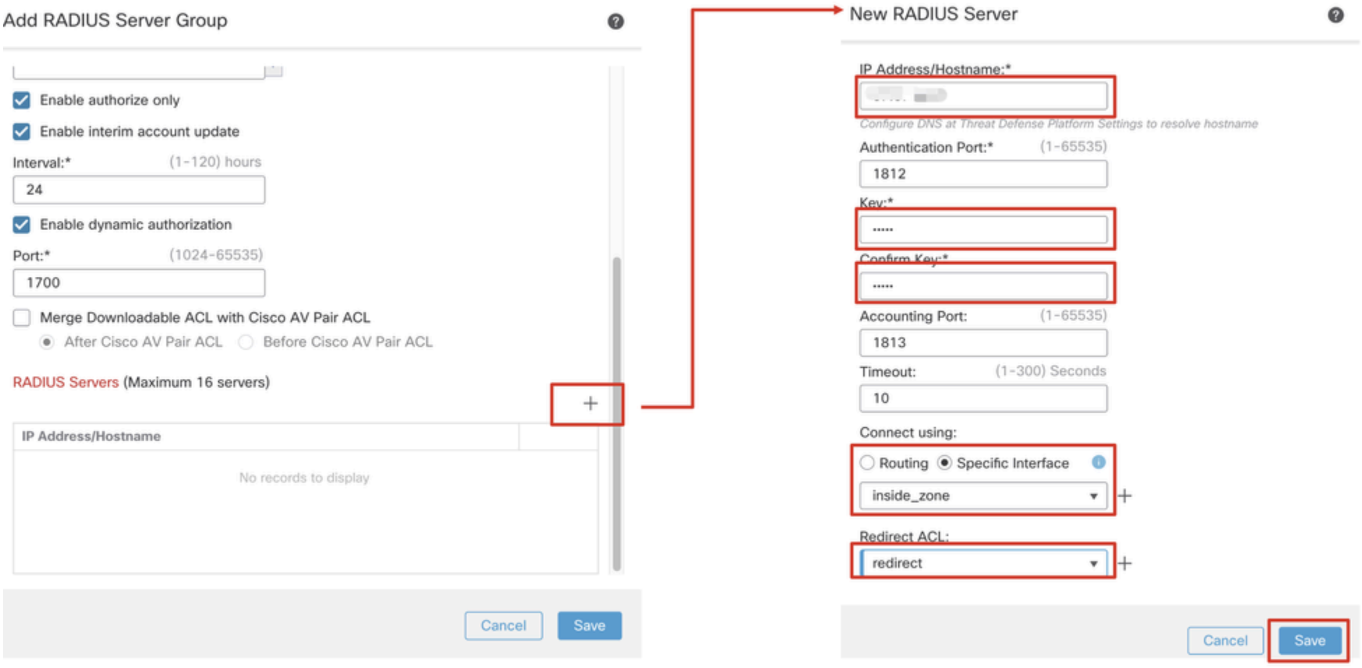
Interval:* (1-120) hours 24

☑ Enable dynamic authorization

Port:* (1024-65535)

FMC_Add_New_Radius_Server_Group_Part_1

步骤 7.2单击Plus 图标添加新的radius服务器。提供ISE PSNIP Address/Hostname, Key。选择specific interface进行连接。选择Redirect ACL。然后，单击Save保存新的radius服务器。然后，再次单击Save，保存新的RADIUS服务器组。



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

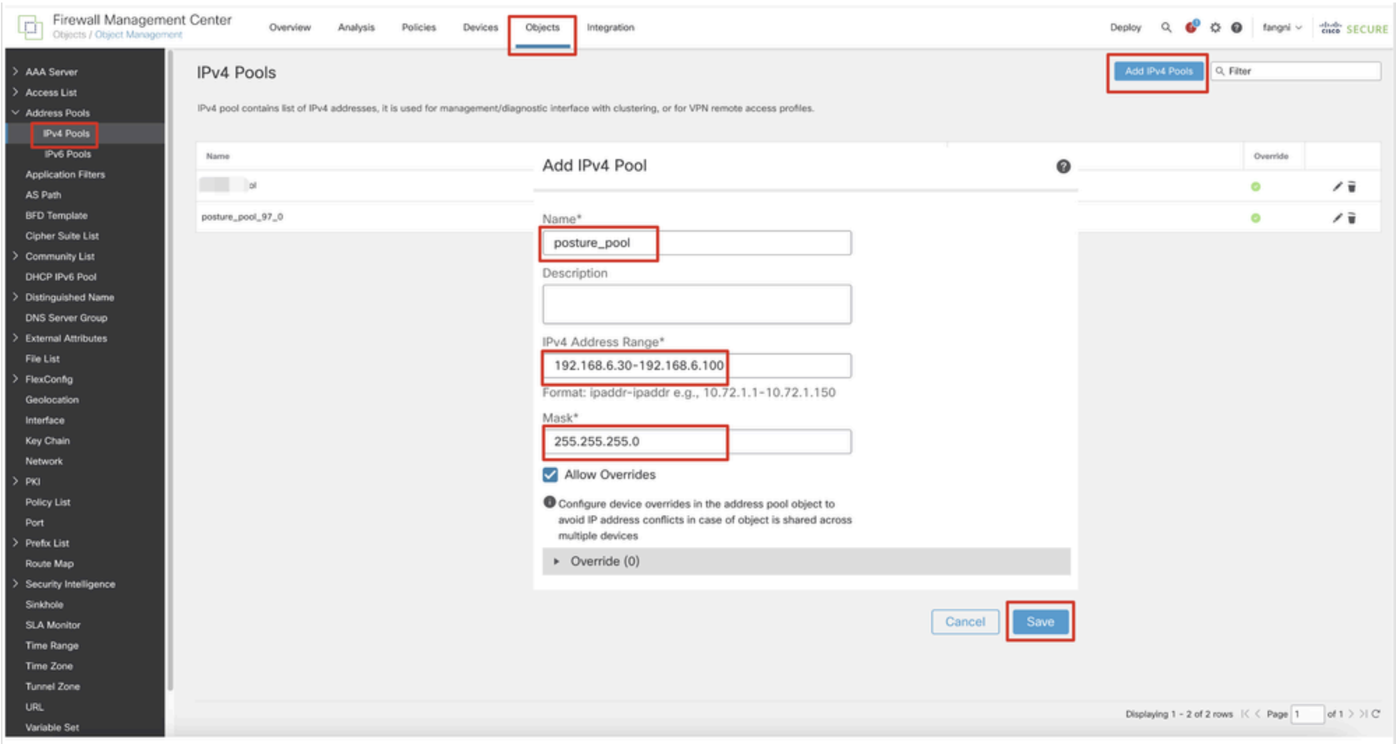
Connect using: ○ Routing ● Specific Interface

inside_zone

Redirect ACL: redirect

FMC_Add_New_Radius_Server_Group_Part_2

步骤 8 导航到Objects > Object Management > Address Pools > IPv4 Pools。单击Add IPv4 Pools并提供**Name, IPv4 Address Range**和Mask。？？然后单击.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

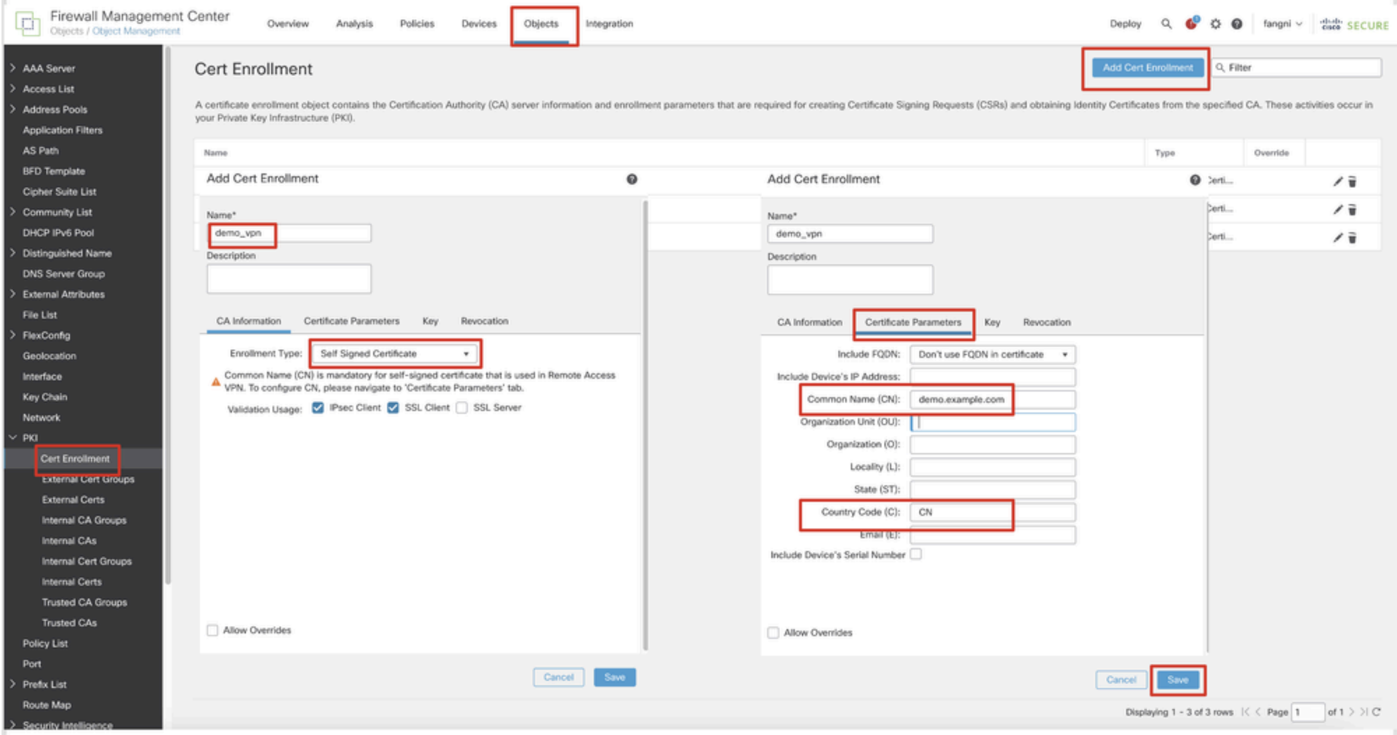
▸ Override (0)

Displaying 1 - 2 of 2 rows Page 1 of 1

FMC_Add_Newpool

步骤 9 导航到Certificate Objects > Object Management > PKI > Cert Enrollment。单击Add Cert Enrollment、提供一个名称，然后在

Enrollment Type中选择Self Signed Certificate。单击Certificate Parameters选项卡并提供Common Name和Country Code。？？然后单击.Save



Cert Enrollment

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

Add Cert Enrollment

Name*: demo_vpn

Description:

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

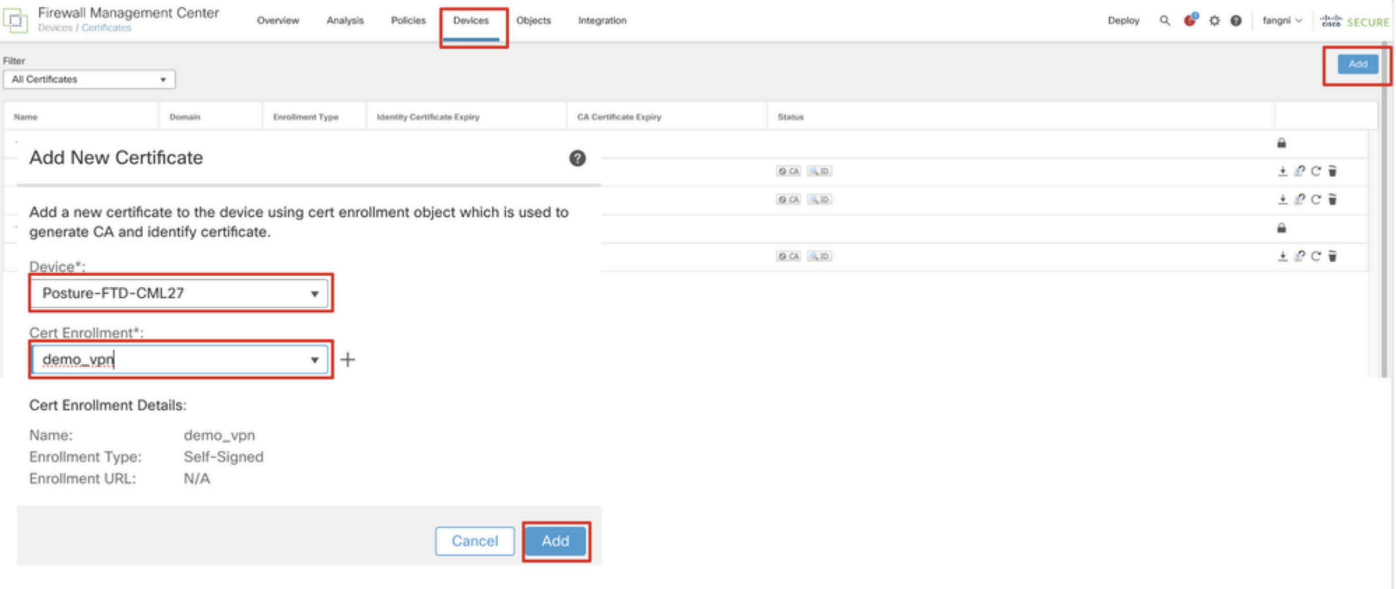
Email (E):

Include Device's Serial Number □

□ Allow Overrides

FMC_Add_New_Cert_Enroll

步骤 10 导航到Devices > Certificates。点击Add，在Device下选择FTD名称，在Cert Enrollment下选择以前配置的注册。单击。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:

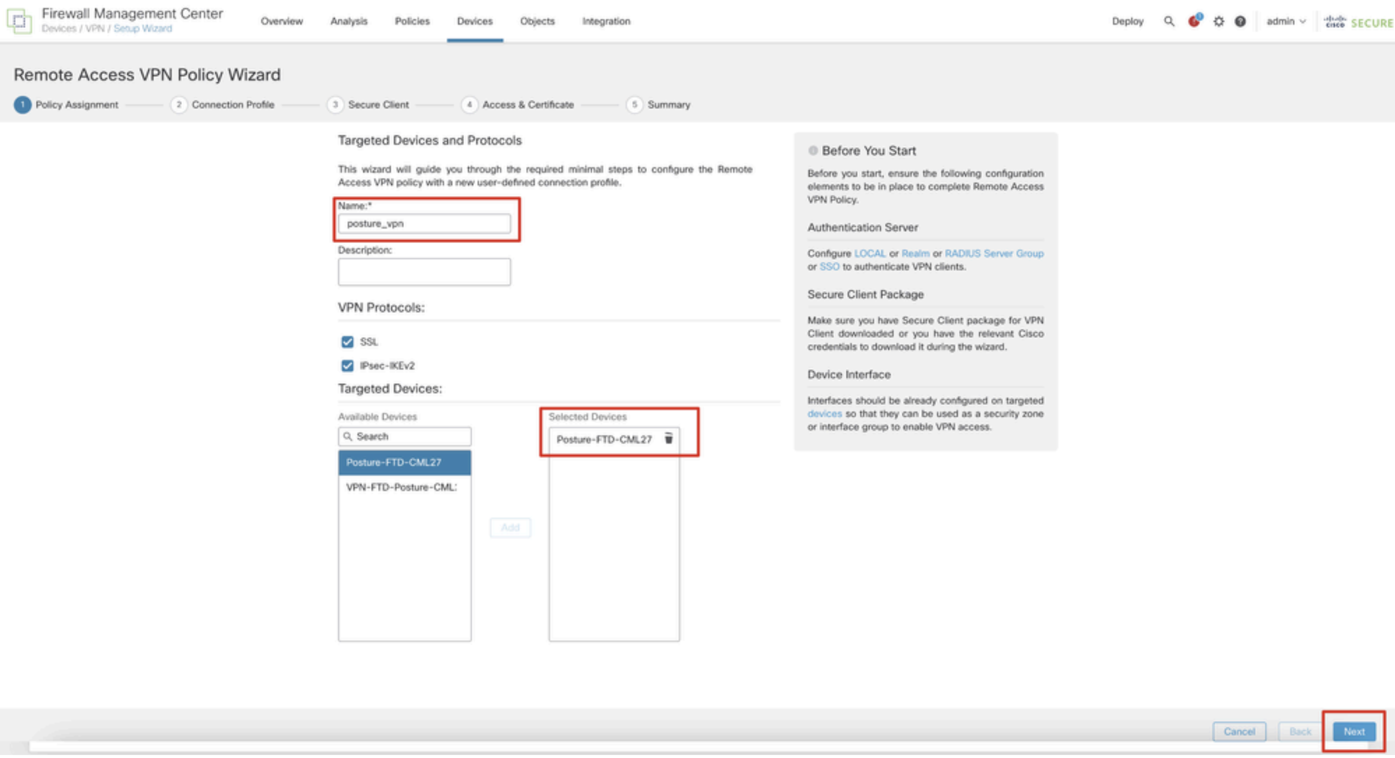
Name: demo_vpn
Enrollment Type: Self-Signed
Enrollment URL: N/A

Cancel Add

FMC_Add_New_Cert_To_FTD

步骤 11 导航到Devices > VPN > Remote Access。单击。Add

步骤 11.1提供名称，并将FTD添加到Selected Devices。单击。Next



Remote Access VPN Policy Wizard

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

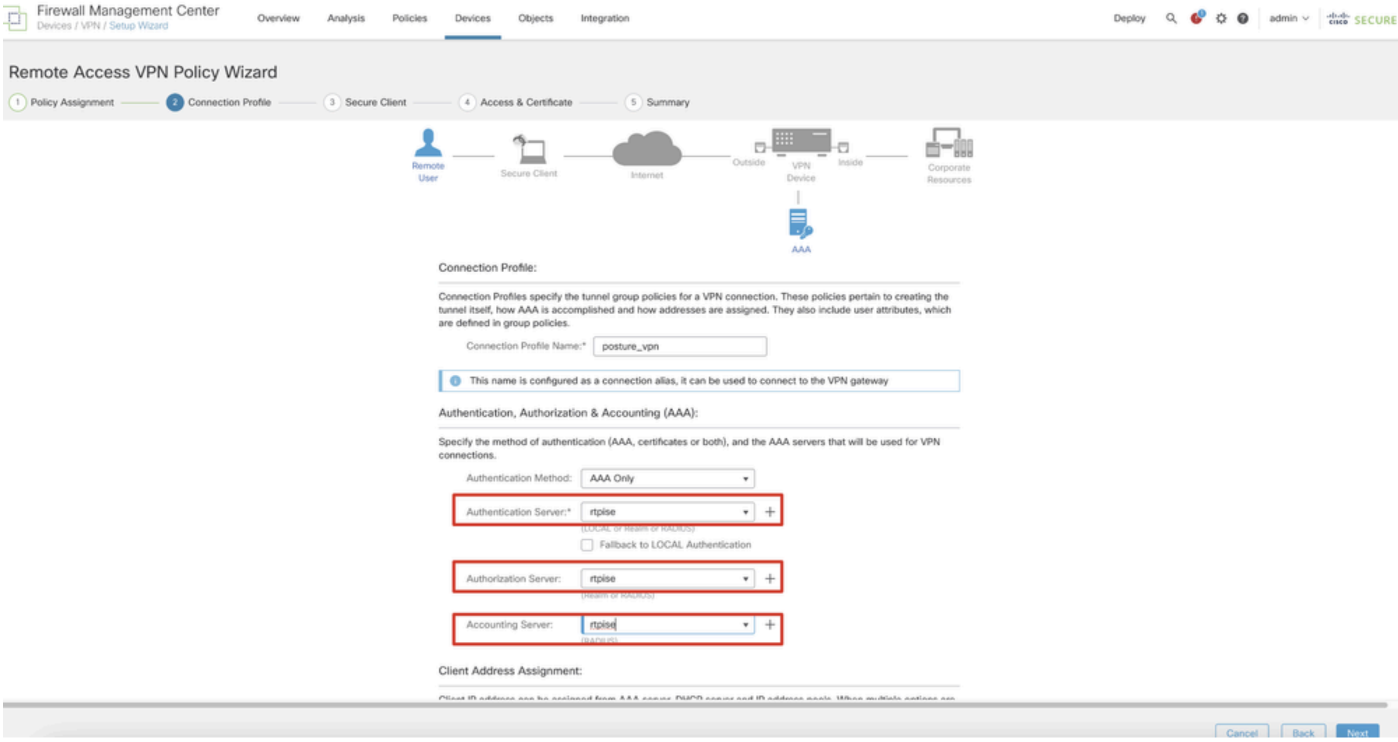
Make sure you have Secure Client package for VPN Client downloaded or you have the relevant Cisco credentials to download it during the wizard.

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

步骤 11.2在Authentication Server, Authorization Server, Accounting Server中选择以前配置的radius服务器组。向下滚动页面。



Remote Access VPN Policy Wizard

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

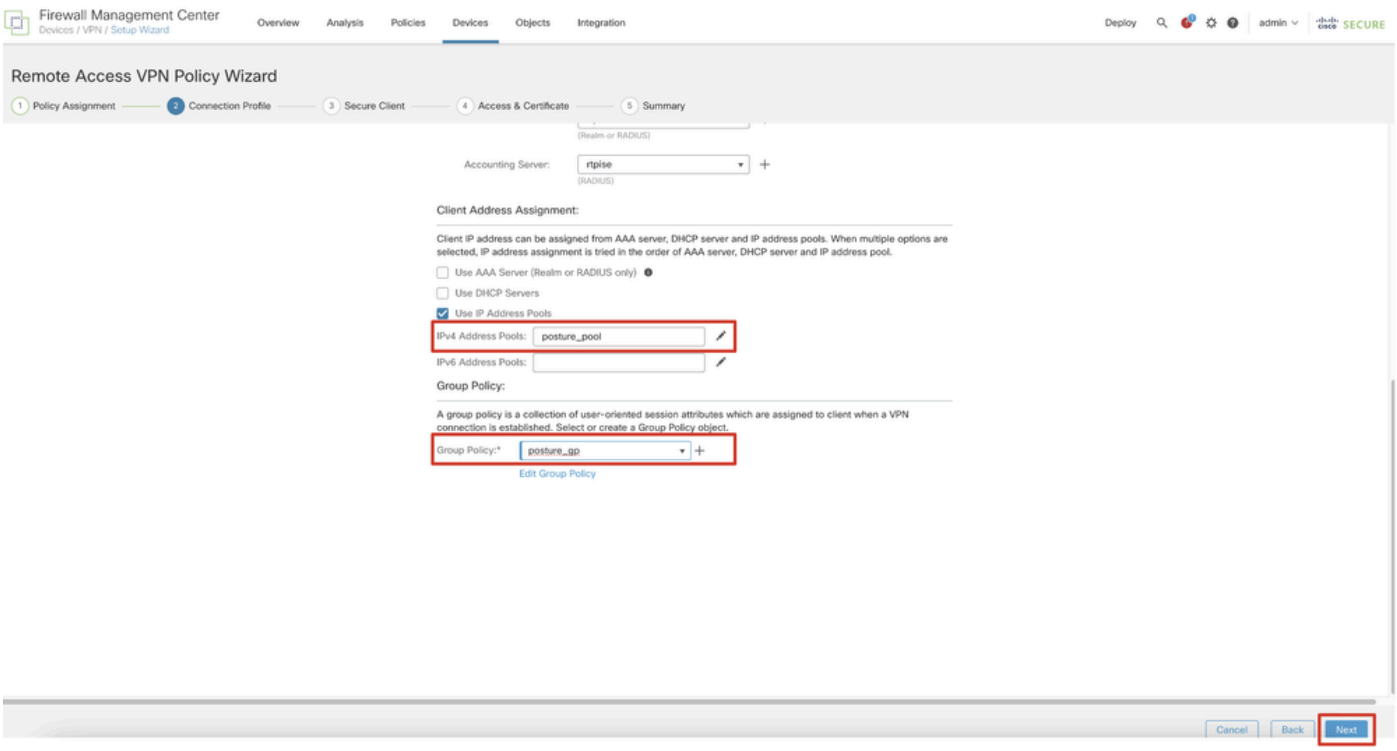
Authorization Server: rtpise (Realm or RADIUS)

Accounting Server: rtpise (RADIUS)

Client Address Assignment:

FMC_New_RAVPN_Wizard_2

步骤 11.3在IPv4 Address Pools中选择以前配置的池名称。在Group Policy中选择以前配置的组策略。单击Next。



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:

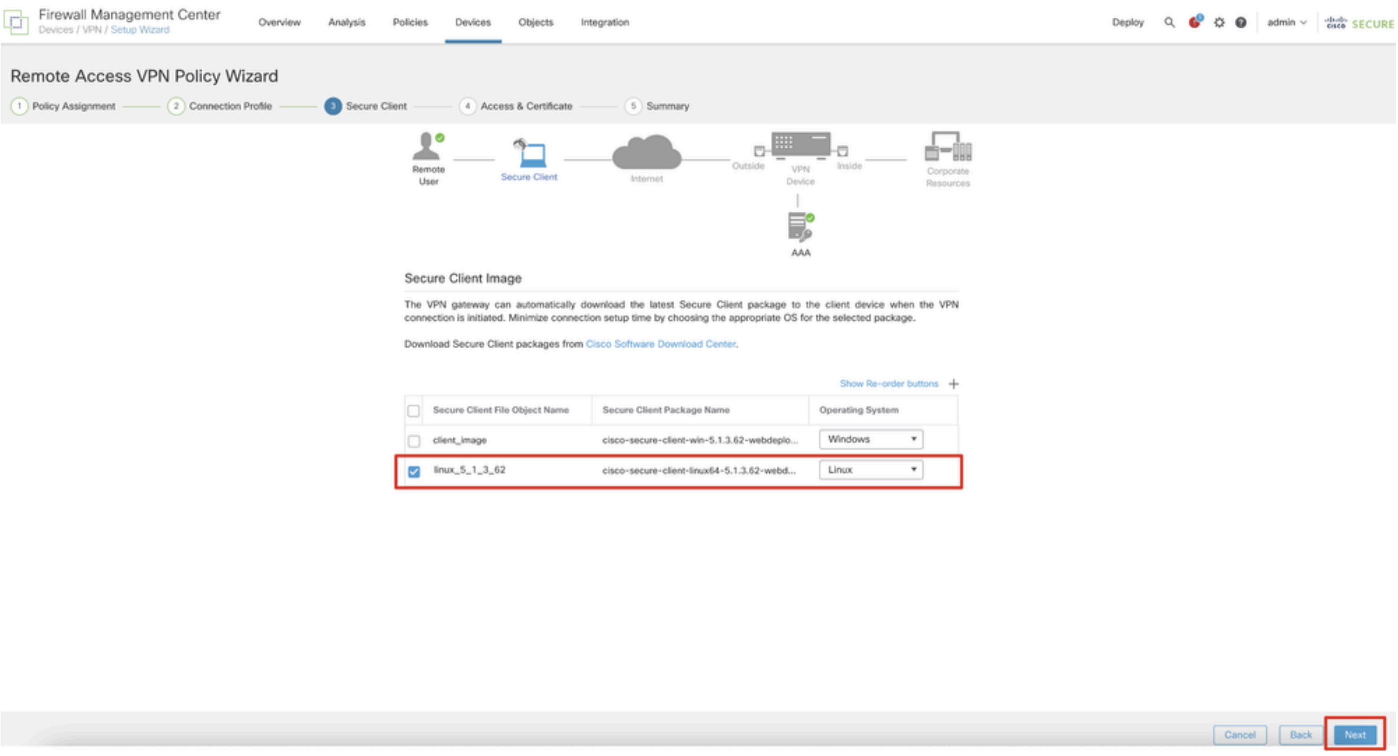
A group policy is a collection of user-oriented session attributes which are assigned to client when a VPN connection is established. Select or create a Group Policy object.

Group Policy:* posture_gp

Edit Group Policy

FMC_New_RAVPN_Wizard_3

步骤 11.4选中Linux映像的复选框。单击。Next



Remote Access VPN Policy Wizard

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

Secure Client Image

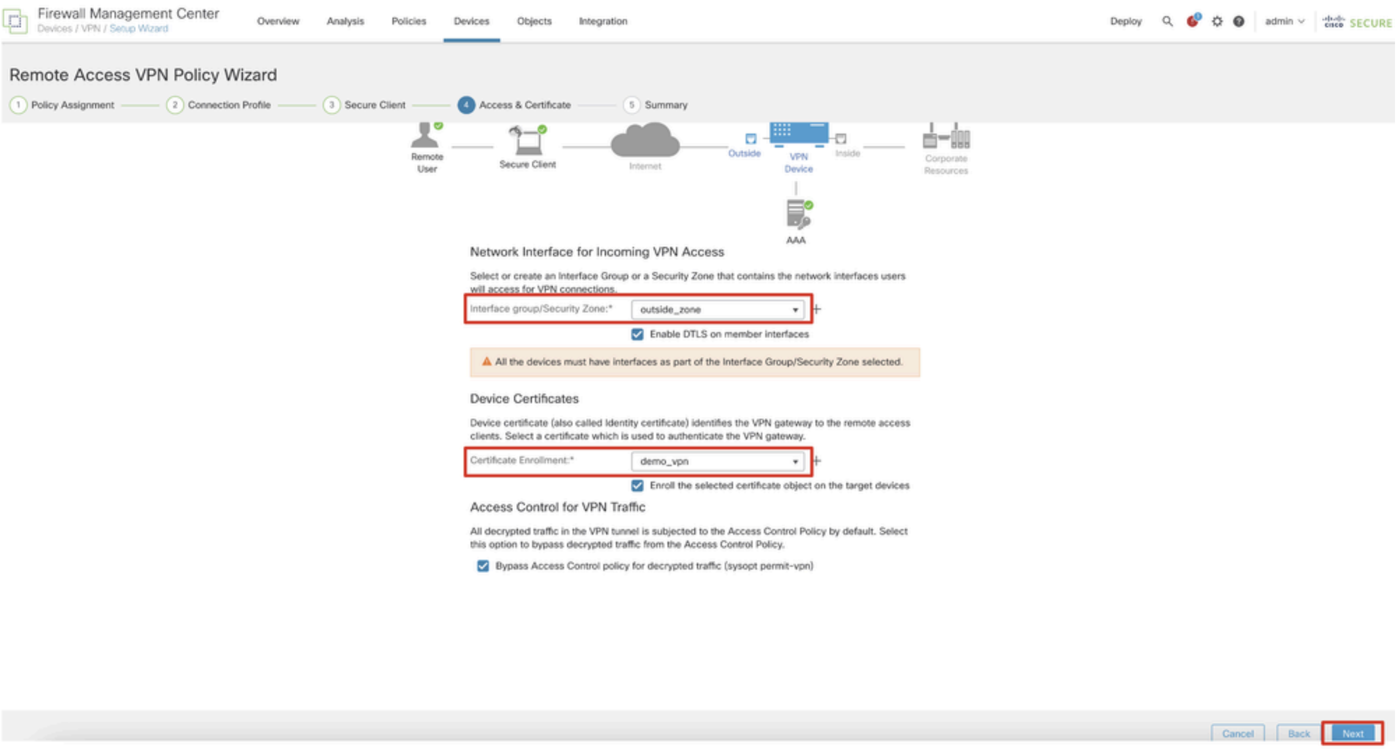
The VPN gateway can automatically download the latest Secure Client package to the client device when the VPN connection is initiated. Minimize connection setup time by choosing the appropriate OS for the selected package.

Download Secure Client packages from Cisco Software Download Center.

□	Secure Client File Object Name	Secure Client Package Name	Operating System
□	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

步骤 11.5选择VPN接口的接口。选择在第9步中在FTD上注册的证书注册。单击。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

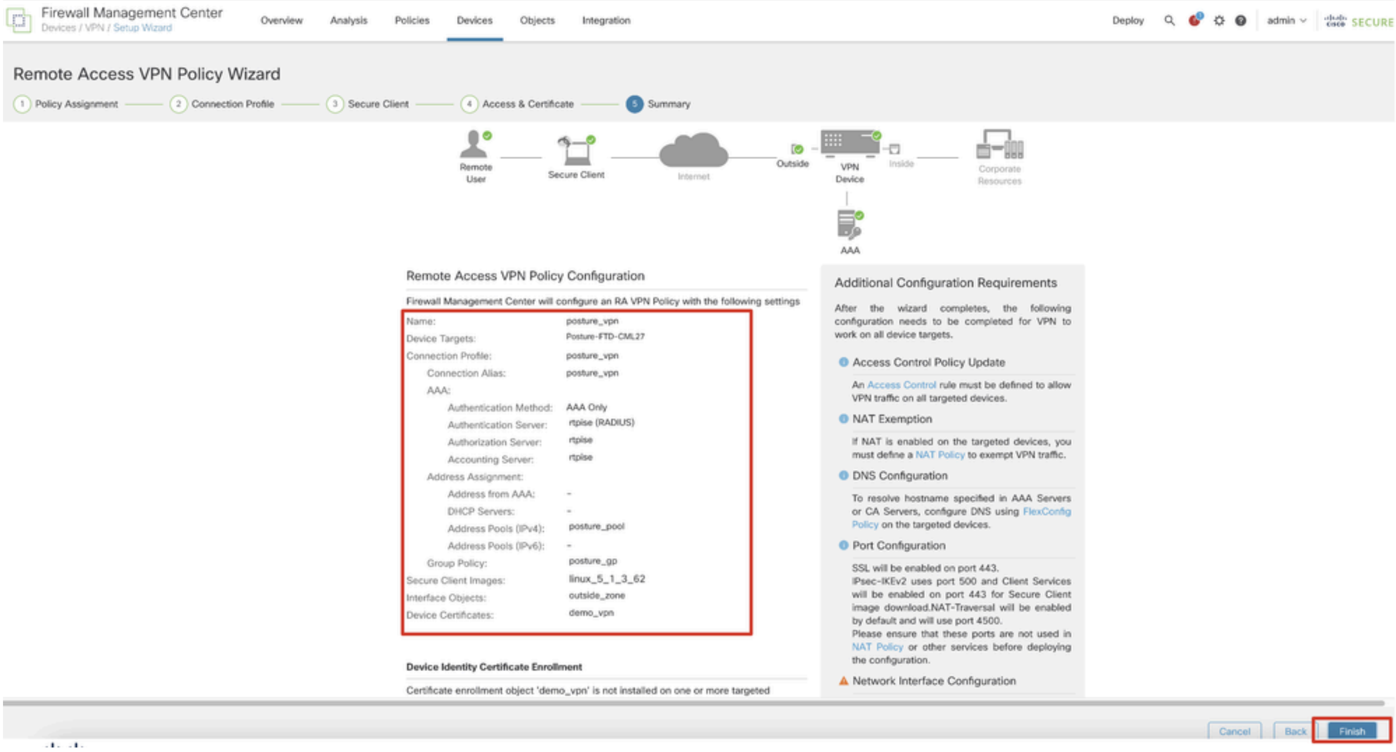
Access Control for VPN Traffic

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

步骤 11.6在摘要页面上再次确认相关信息。如果一切正常，请单击Finish。如果需要修改任何内容，请单击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.

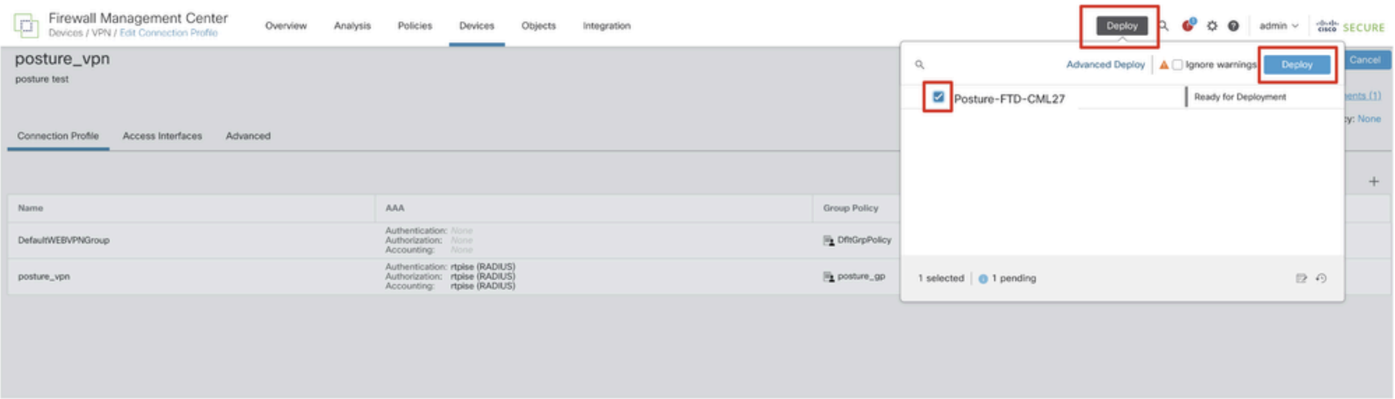
Port Configuration

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

步骤 12将新配置部署到FTD以完成远程访问VPN配置。

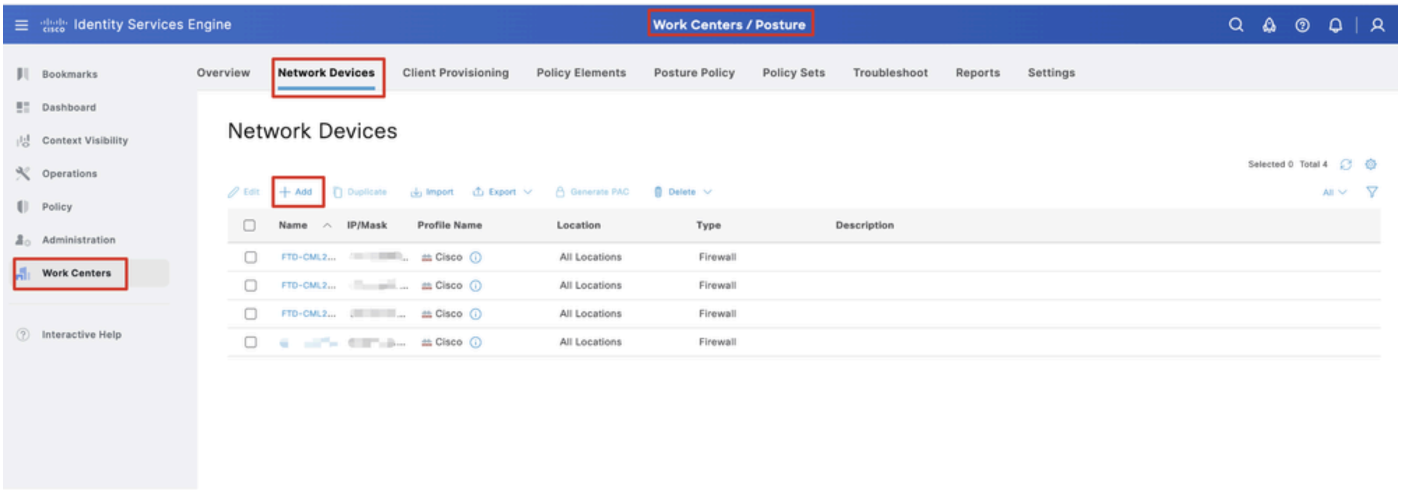


Name	AAA	Group Policy
DefaultWEBVPNGroup	Authentication: None Authorization: None Accounting: None	DfltGrpPolicy
posture_vpn	Authentication: rtpise (RADIUS) Authorization: rtpise (RADIUS) Accounting: rtpise (RADIUS)	posture_gp

FMC_Deploy_FTD

ISE上的配置

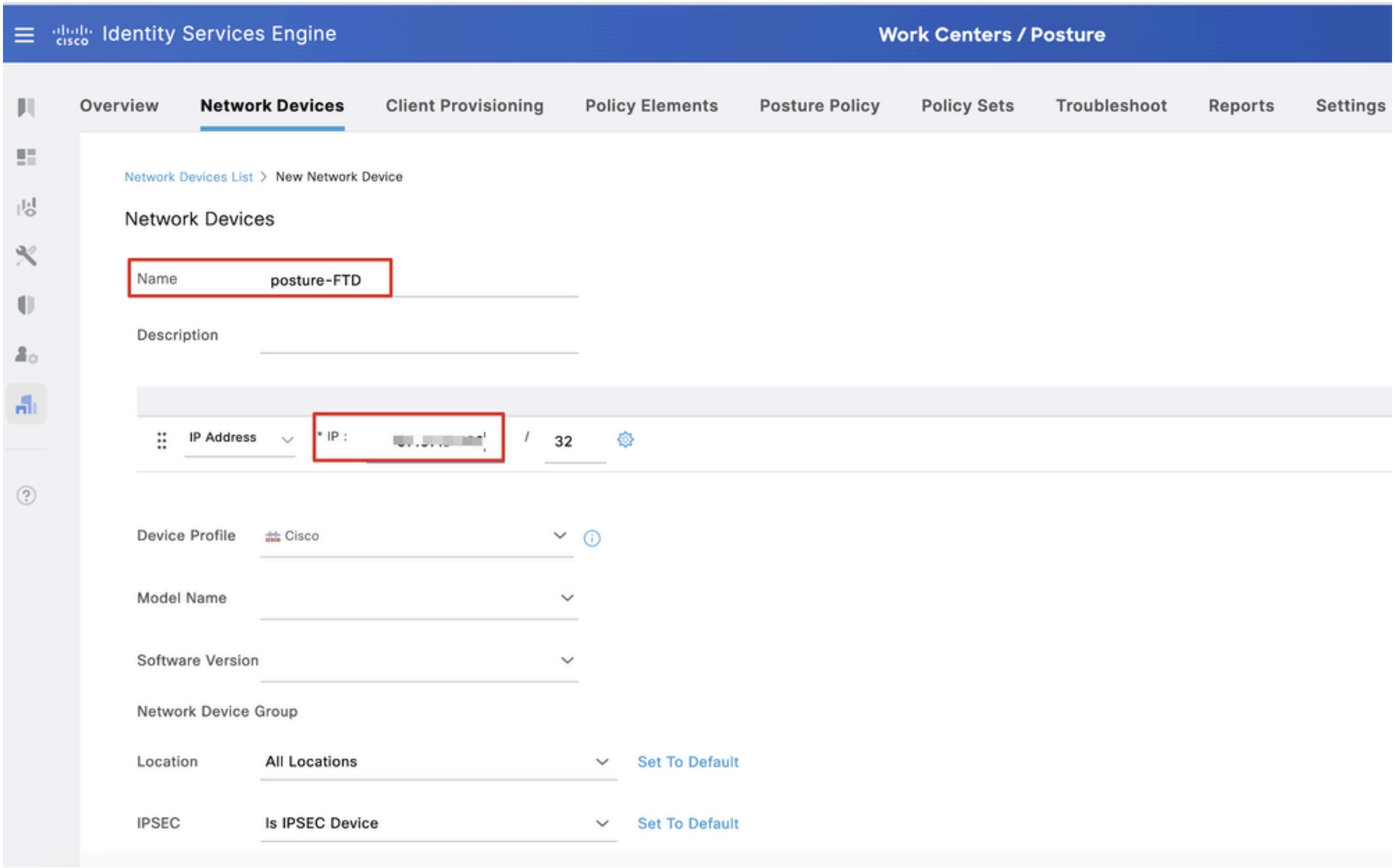
步骤 13 导航到Work Centers > Posture > Network Devices。单击。Add



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

ISE_Add_New_Device

步骤 13.1提供Name, IP Address并向下滚动页面。



Network Devices

Name posture-FTD

Description

IP Address * IP : [redacted] / 32

Device Profile Cisco

Model Name

Software Version

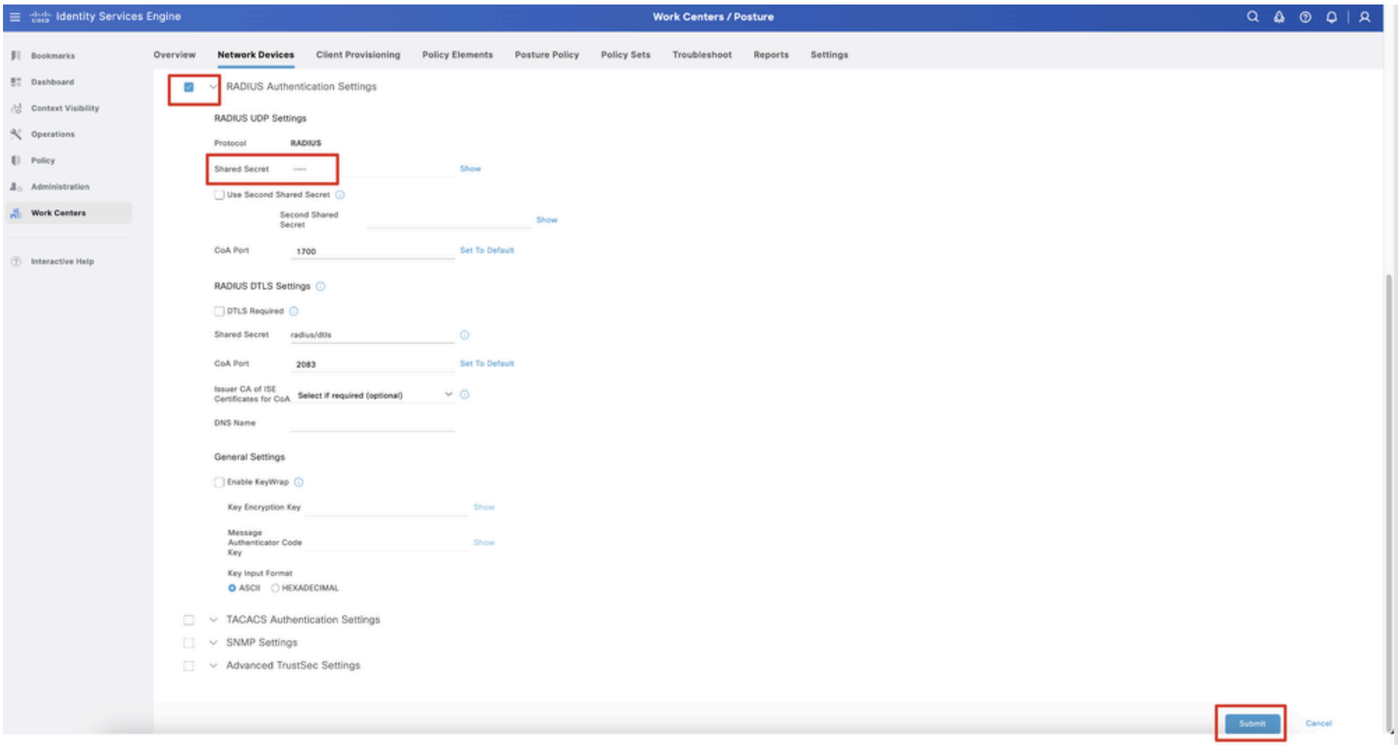
Network Device Group

Location All Locations

IPSEC Is IPSEC Device

ISE_Add_New_Device_1

步骤 13.2选中RADIUS Authentication Settings复选框。提供Shared Secret。单击。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

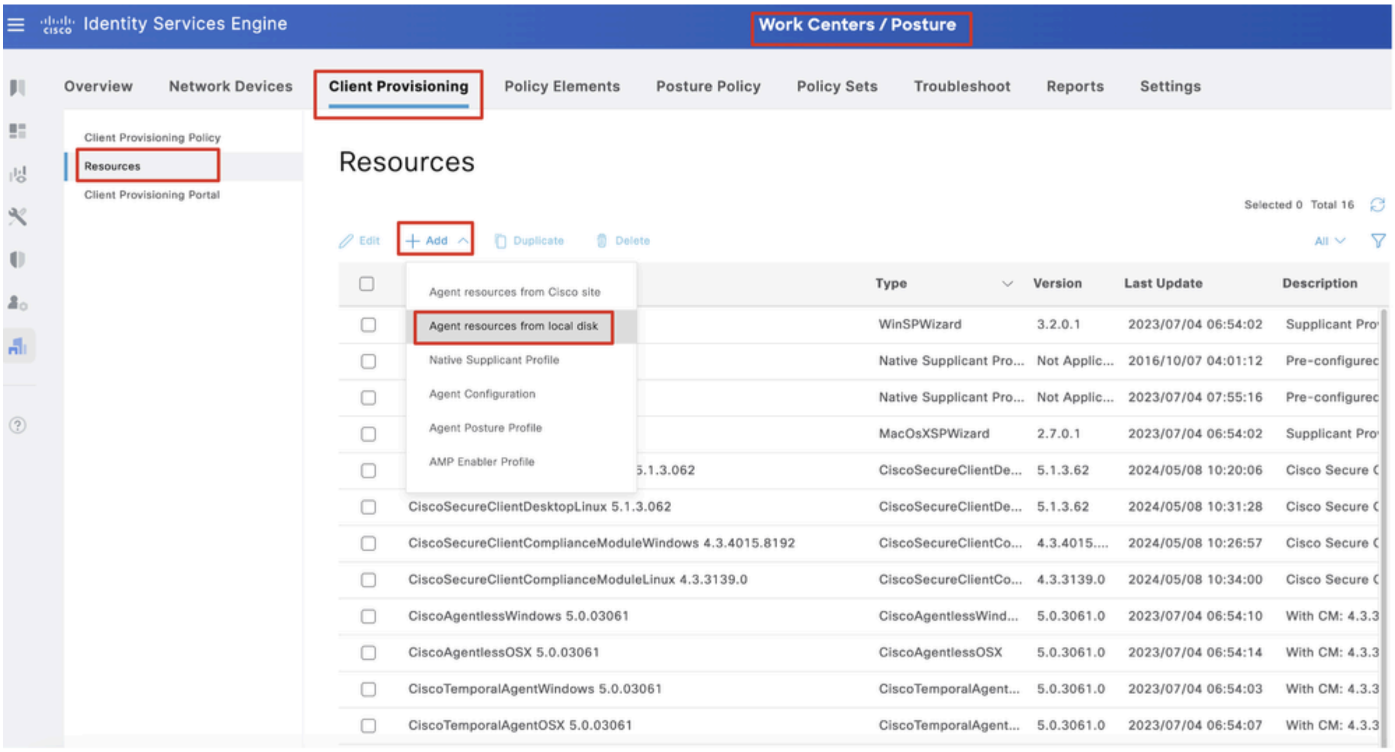
□ Advanced TrustSec Settings

ISE_Add_New_Device_2

步骤 14 从Cisco软件下载下载软件包名称cisco-secure-client-linux64-4.3.3139.0-isecompliance-webdeploy-k9.pkg，通过确认下载文件的md5校验和与Cisco软件下载页相同，来确保文件完好。 已在步骤1中成功下载软件包名称cisco-secure-client-linux64-5.1.3.62-

webdeploy-k9.pkg。

步骤 15 导航到Work Centers > Posture > Client Provisioning > Resources。单击。Add选择.Agent resources from local disk



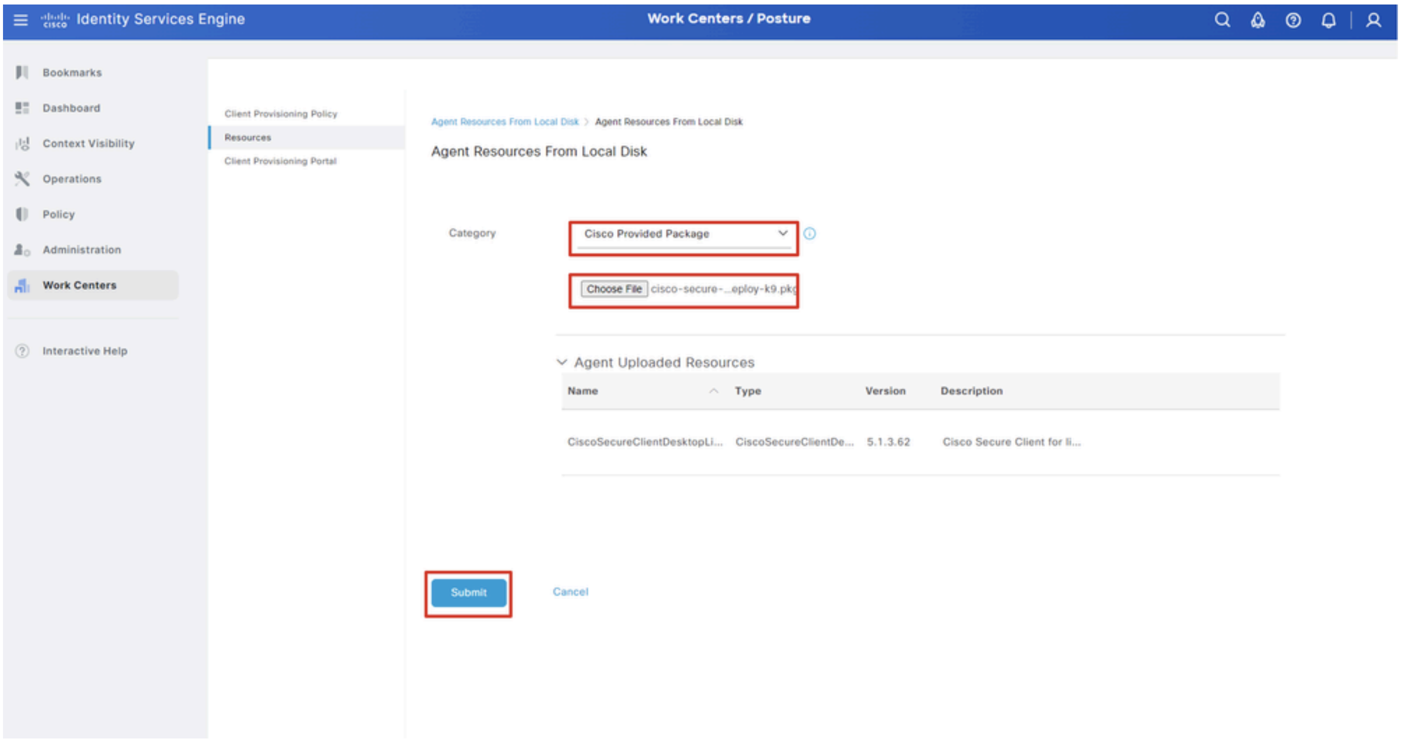
Resources

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

步骤 15.1选择.Cisco Provided Package点击Choose File上传cisco-secure-client-linux64-5.1.3.62-webdeploy-k9.pkg。单击。Submit



Agent Resources From Local Disk

Category: Cisco Provided Package

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

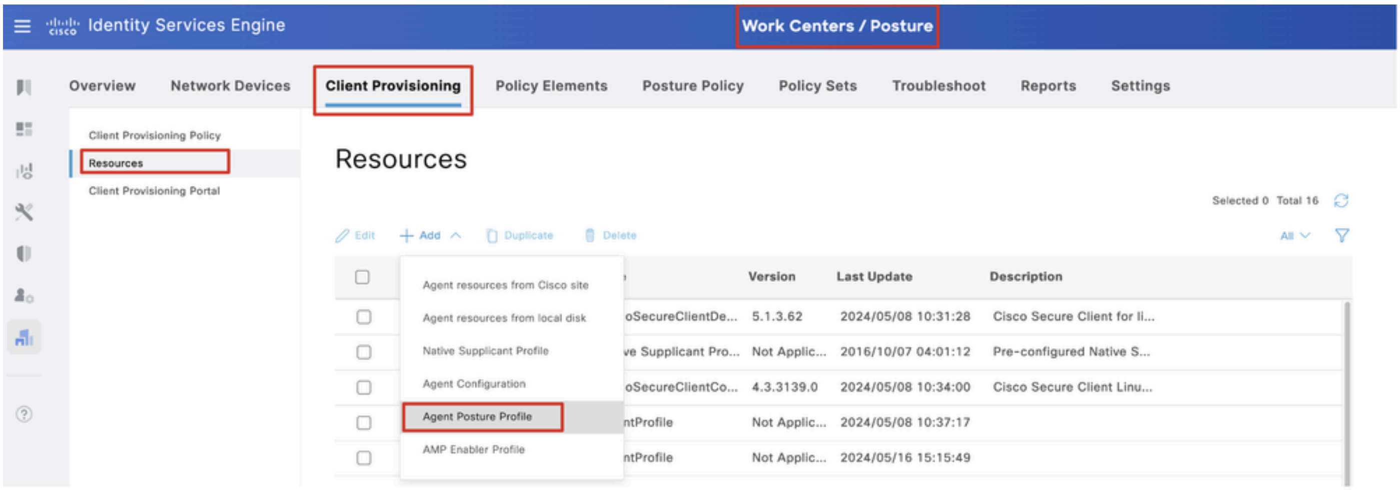
Agent Uploaded Resources

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

ISE_Upload_Resources_1

注意：重复步骤14.上传cisco-secure-client-linux64-4.3.3139.0-isecompliance-webdeploy-k9.pkg。

步骤 16 导航到Work Centers > Posture > Client Provisioning > Resources。单击。Add选择.Agent Posture Profile



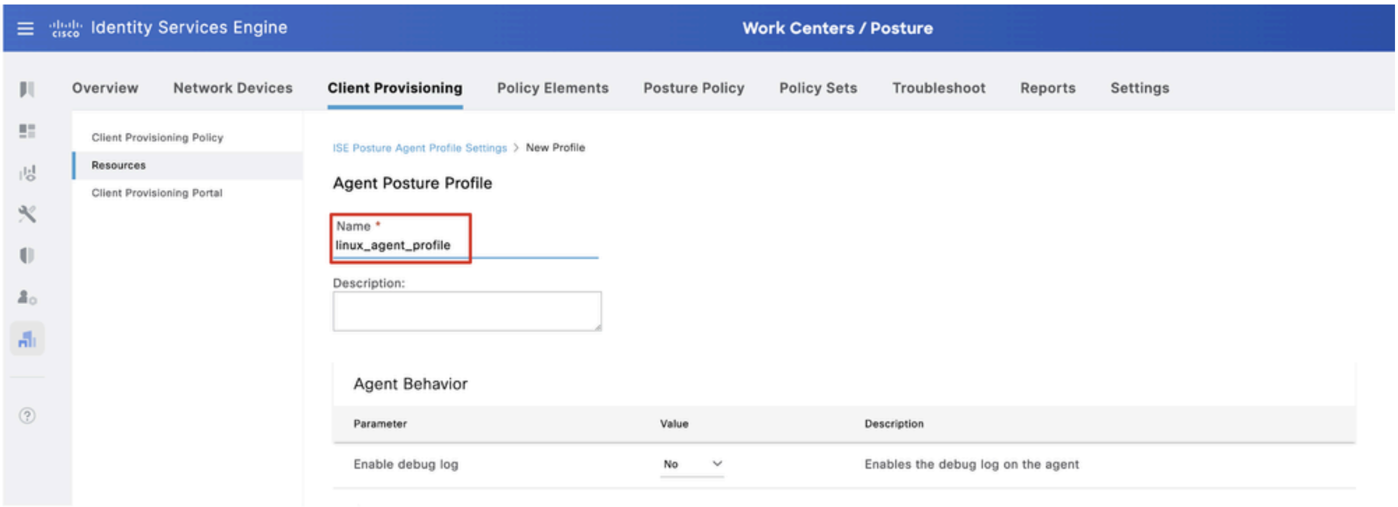
	Version	Last Update	Description
oSecureClientDe...	5.1.3.62	2024/05/08 10:31:28	Cisco Secure Client for li...
ve Supplicant Pro...	Not Applic...	2016/10/07 04:01:12	Pre-configured Native S...
oSecureClientCo...	4.3.3139.0	2024/05/08 10:34:00	Cisco Secure Client Linu...
ntProfile	Not Applic...	2024/05/08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

ISE_Add_Agent_Posture_Profile

步骤 16.1提供Name, Server name rules，并将剩余部分保留为默认值。单击。Save

名称：linux_agent_profile

服务器名称规则：*.example.com



Agent Posture Profile

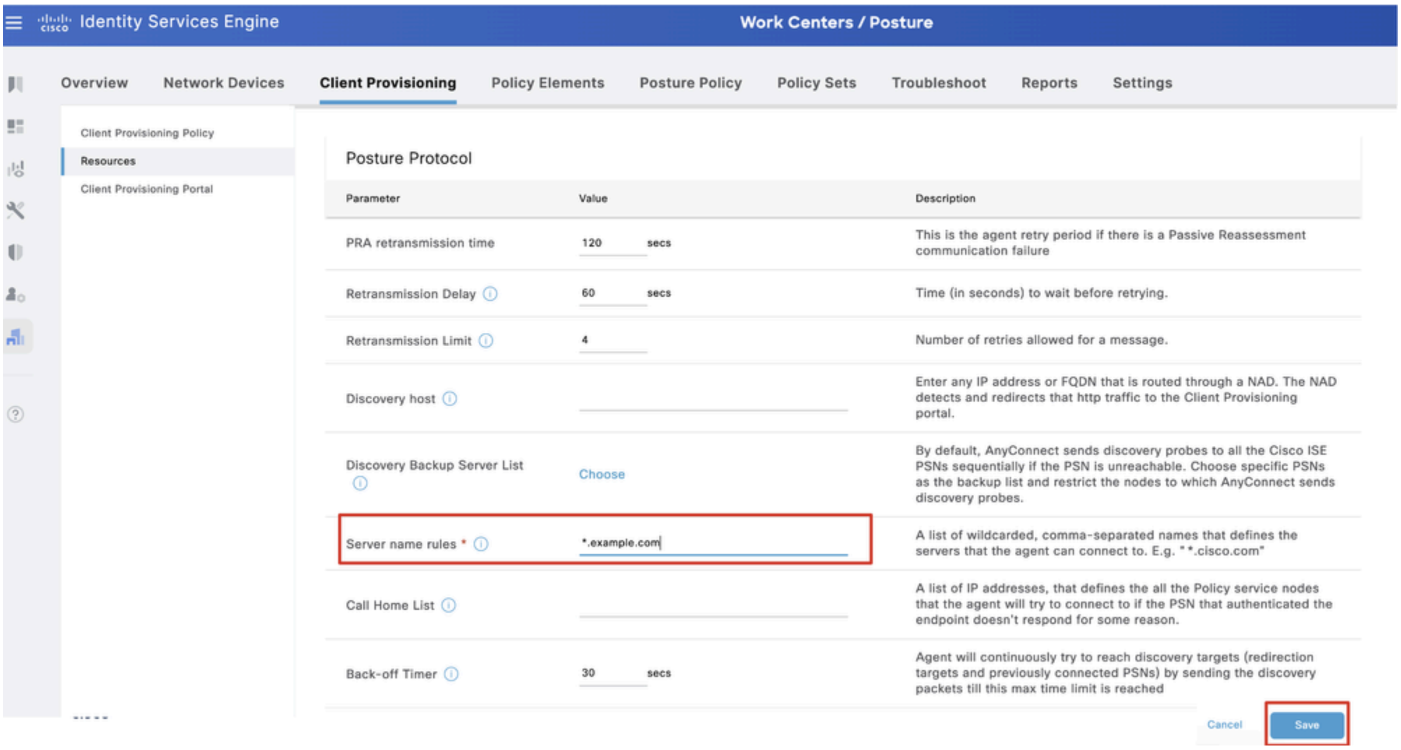
Name * linux_agent_profile

Description:

Agent Behavior

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

ISE_Add_Agent_Posture_Profile_1

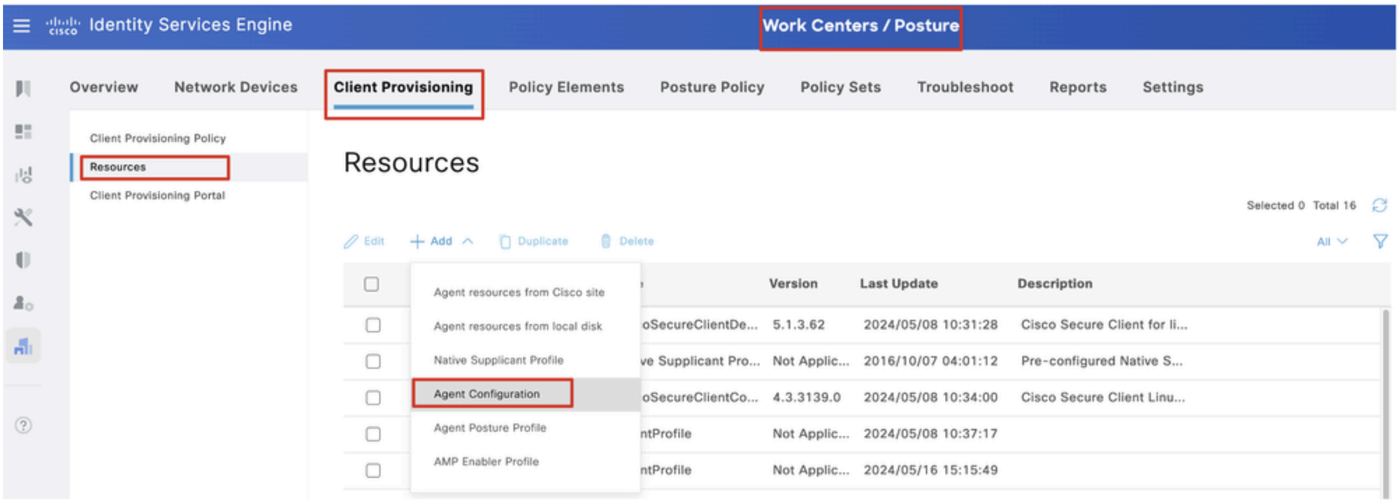


Posture Protocol

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

步骤 17 导航到Work Centers > Posture > Client Provisioning > Resources。单击。Add选择.Agent Configuration



Resources

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

ISE_Add_Agent_Configuration

步骤 17.2配置详细信息：

选择代理包：CiscoSecureClientDesktopLinux 5.1.3.062

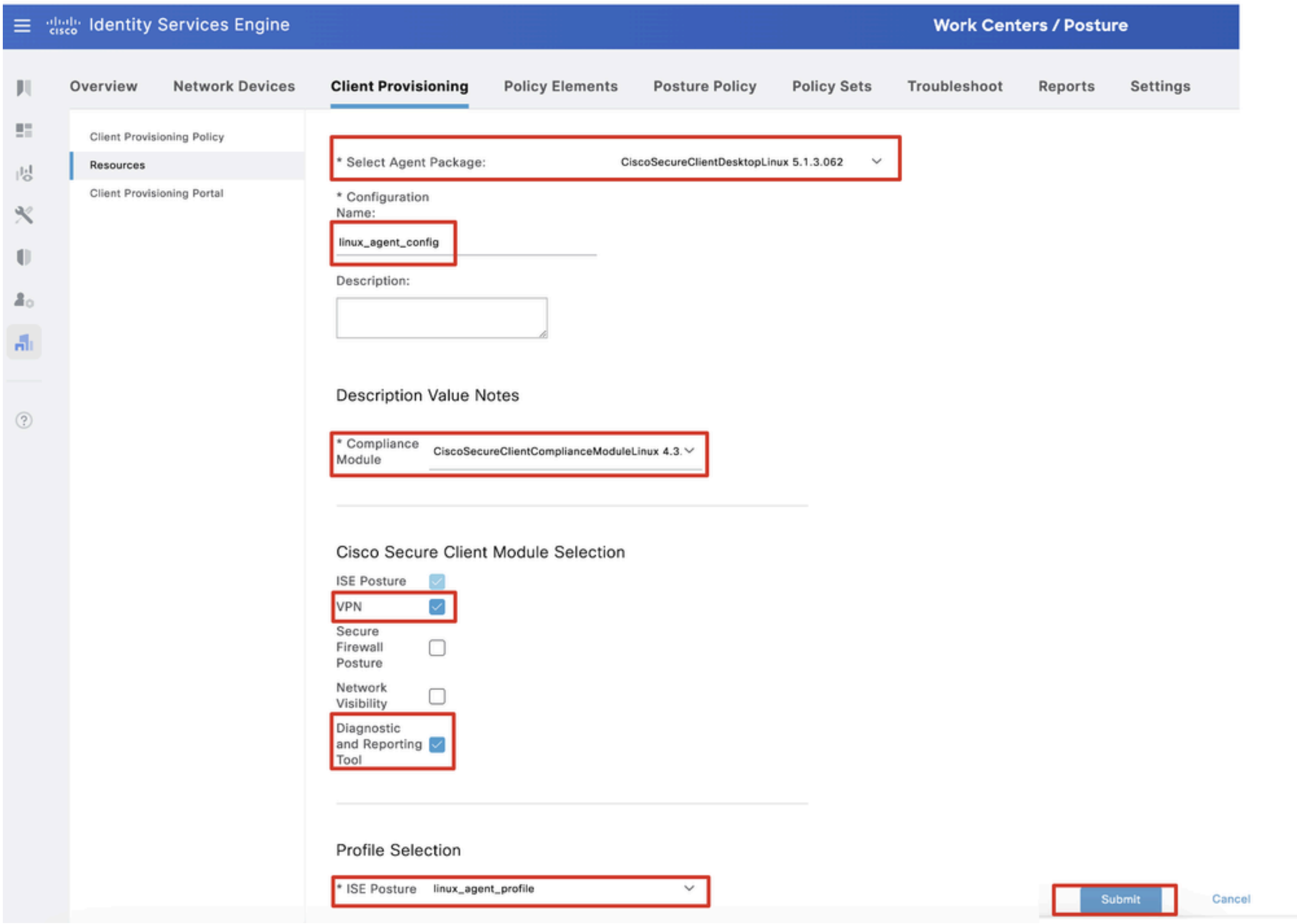
名称：linux_agent_config

合规性模块：CiscoSecureClientComplianceModuleLinux 4.3.3139.0

选中复选框 VPN, Diagnostic and Reporting Tool

配置文件选择ISE终端安全评估：linux_agent_profile

单击。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 □

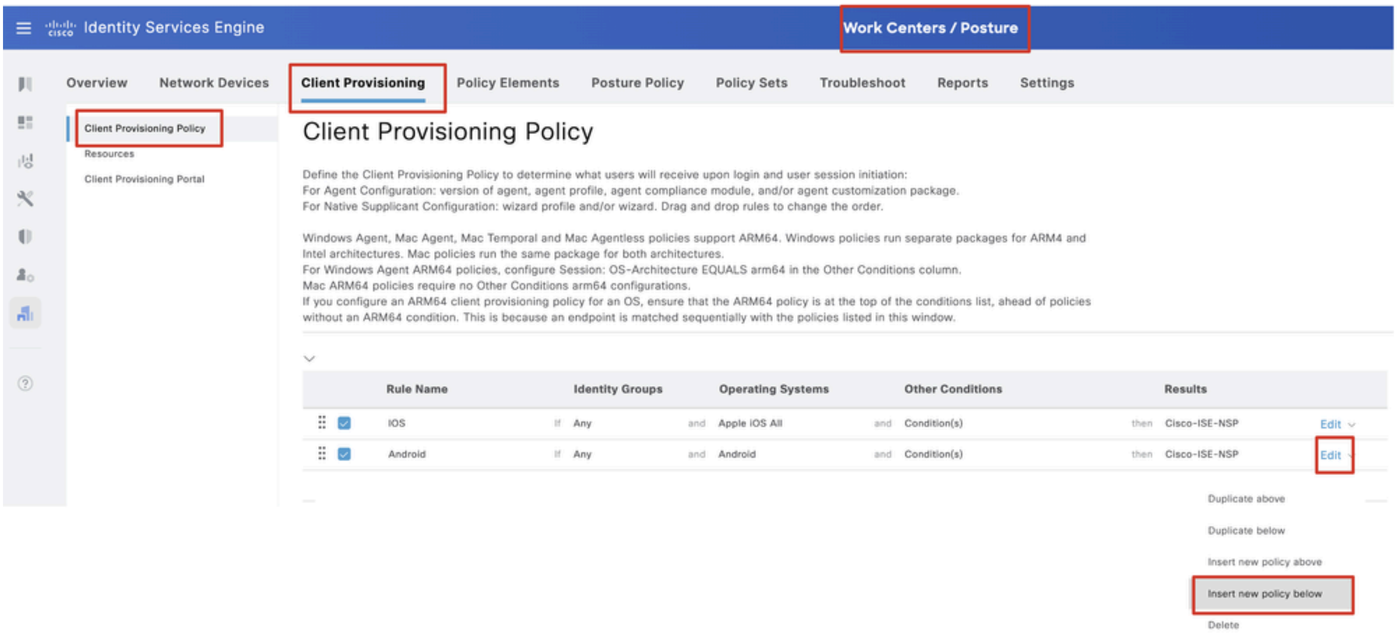
Diagnostic and Reporting Tool ☑

Profile Selection

* ISE Posture linux_agent_profile

ISE_Add_Agent_Configuration_1

步骤 18. 导航到Work Centers > Posture > Client Provisioning > Client Provisioning Policy。在任何规则名称末尾点击Edit 。选择.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

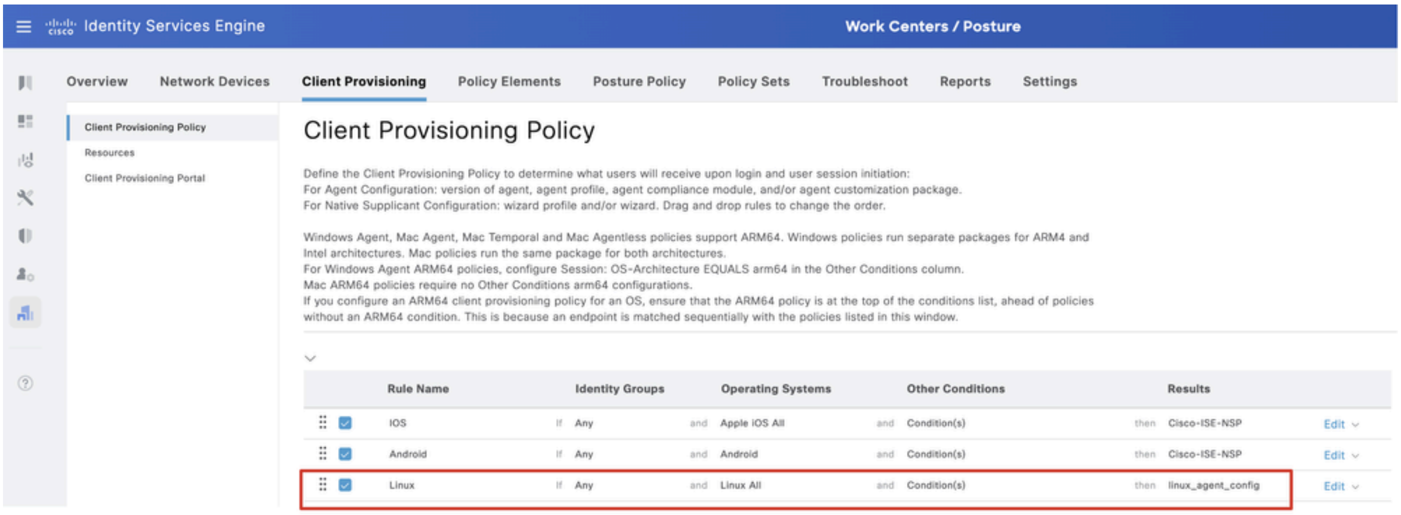
步骤 18.1 配置详细信息：

规则名称：Linux

操作系统：Linux All

结果：linux_agent_config

单击Done 和Save。



Client Provisioning Policy

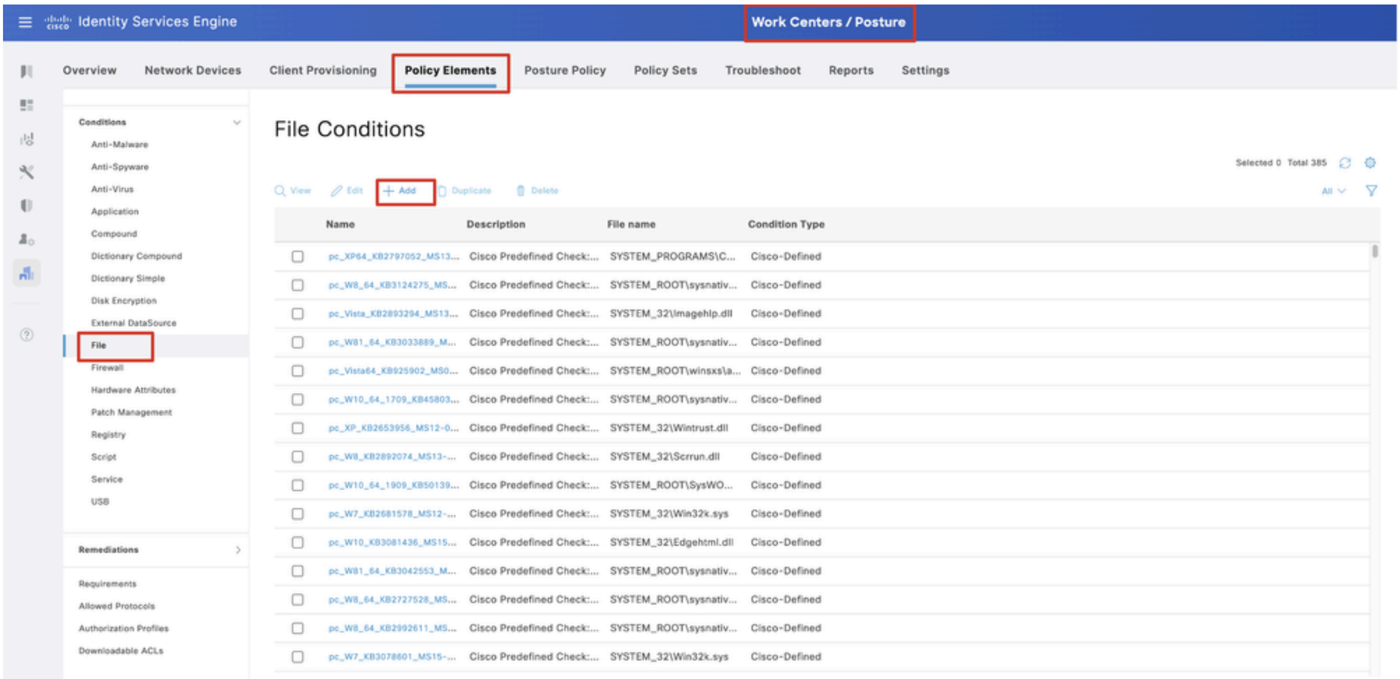
Define the Client Provisioning Policy to determine what users will receive upon login and user session initiation:
For Agent Configuration: version of agent, agent profile, agent compliance module, and/or agent customization package.
For Native Supplicant Configuration: wizard profile and/or wizard.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

步骤 19. 导航到Work Centers > Posture > Policy Elements > Conditions > File。单击。Add



File Conditions

Selected 0 Total 385

	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

步骤 19.1 配置详细信息：

名称：linux_demo_file_exist

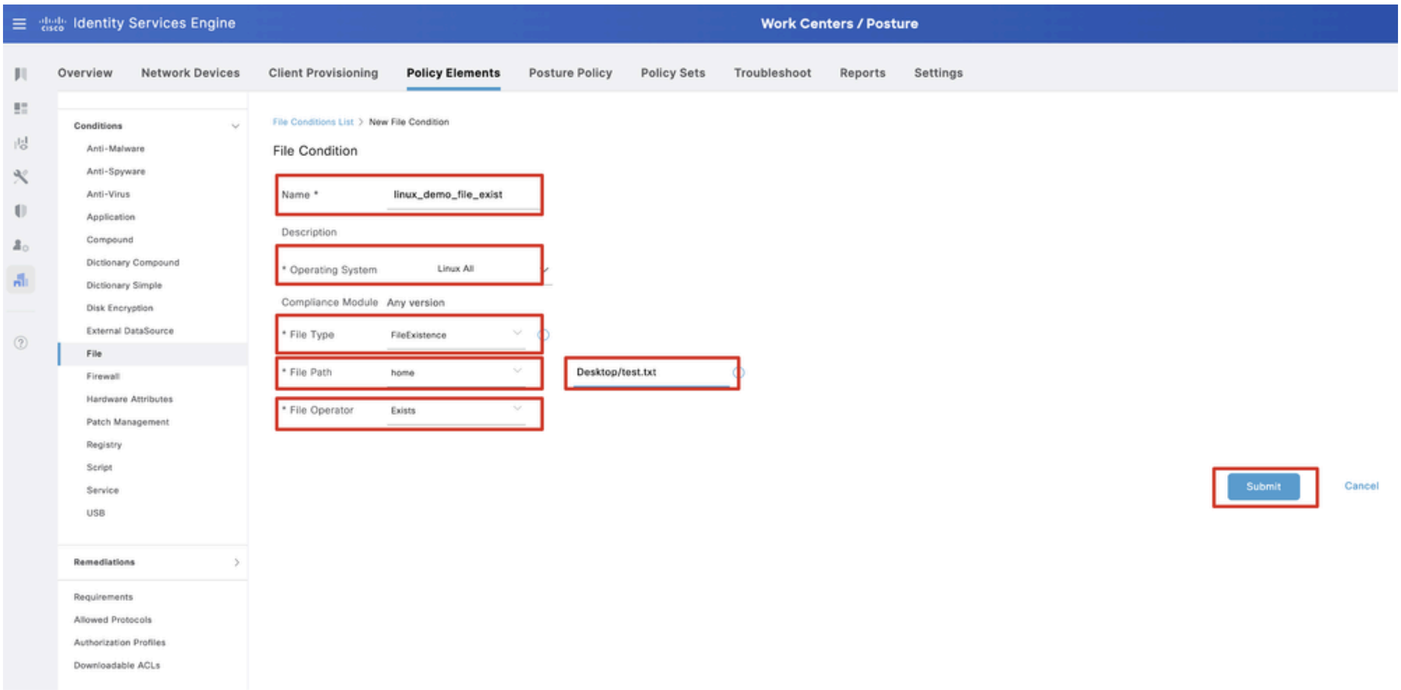
操作系统：Linux All

文件类型：FileExist

文件路径：home、Desktop/test.txt

文件运算符：存在

单击。Submit



File Condition

Name * linux_demo_file_exist

Description

* Operating System Linux All

Compliance Module Any version

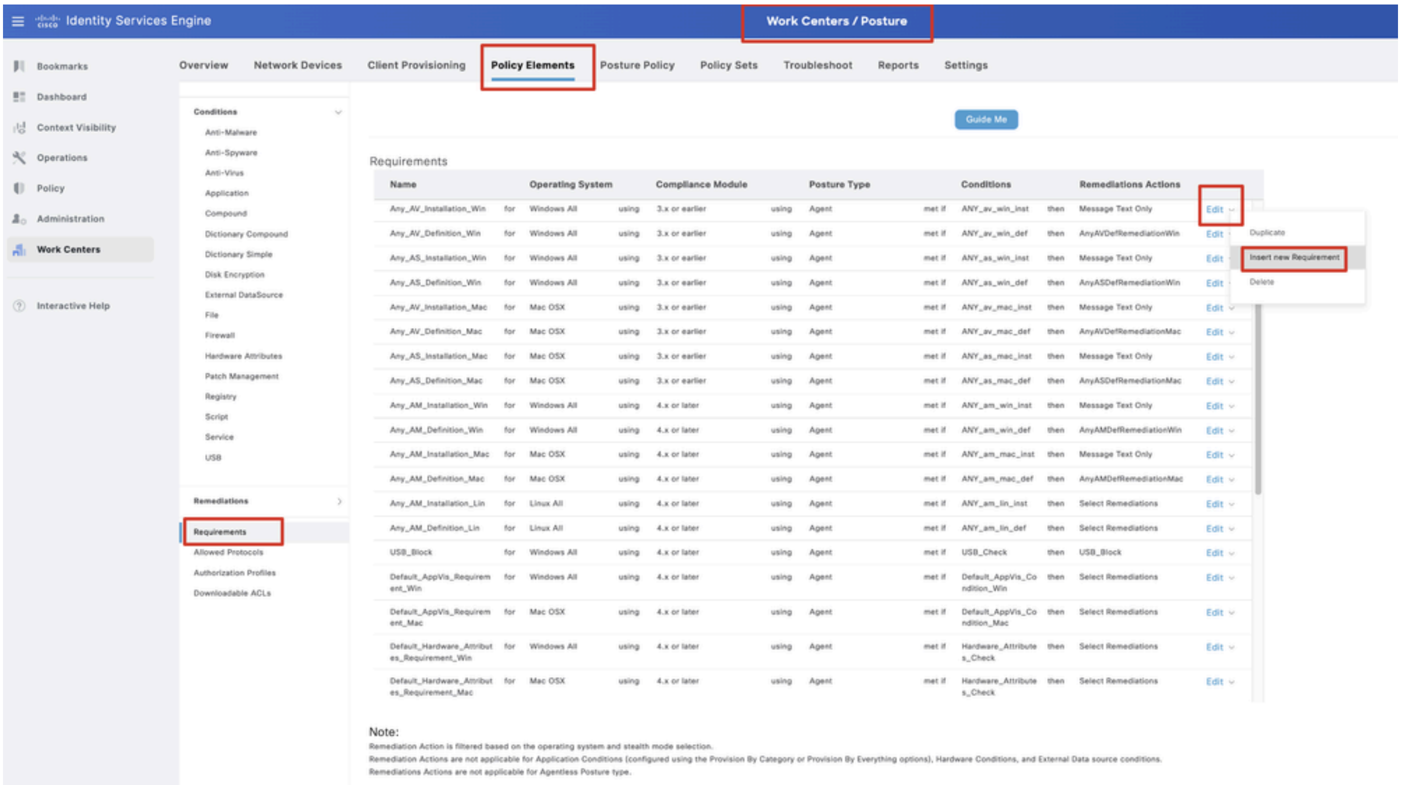
* File Type FileExistence

* File Path home Desktop/test.txt

* File Operator Exists

ISE_Add_New_File_Condition_1

步骤 20. 导航到Work Centers > Posture > Policy Elements > Requirements。在任何规则名称末尾点击Edit 。选择.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

步骤 20.1 配置详细信息：

名称：Test_exist_linux

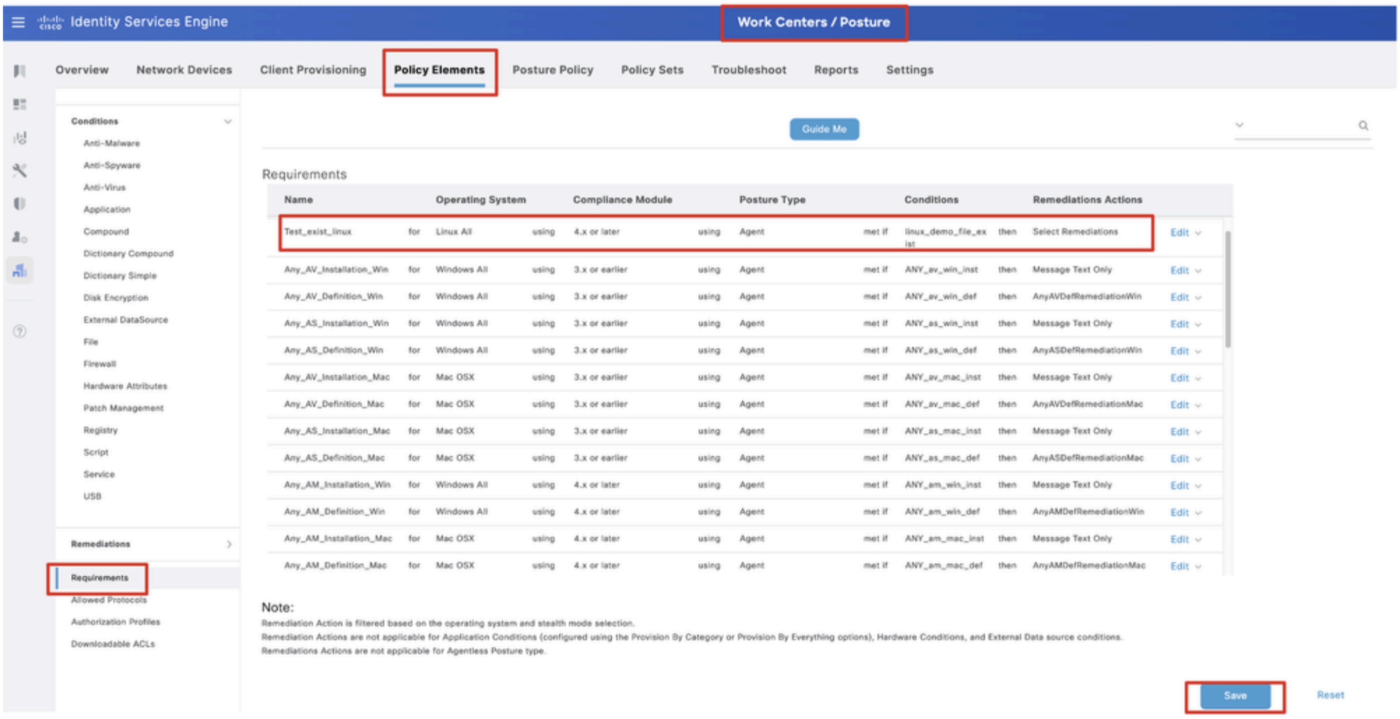
操作系统：Linux All

合规性模块：4.x或更高版本

状态类型：代理

条件：linux_demo_file_exist

单击Done 和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

注意：到目前为止，Linux代理仅支持shell脚本作为补救。

步骤 21. 导航到Work Centers > Posture > Policy Elements > Authorization Profiles。单击。Add

步骤 21.1 配置详细信息：

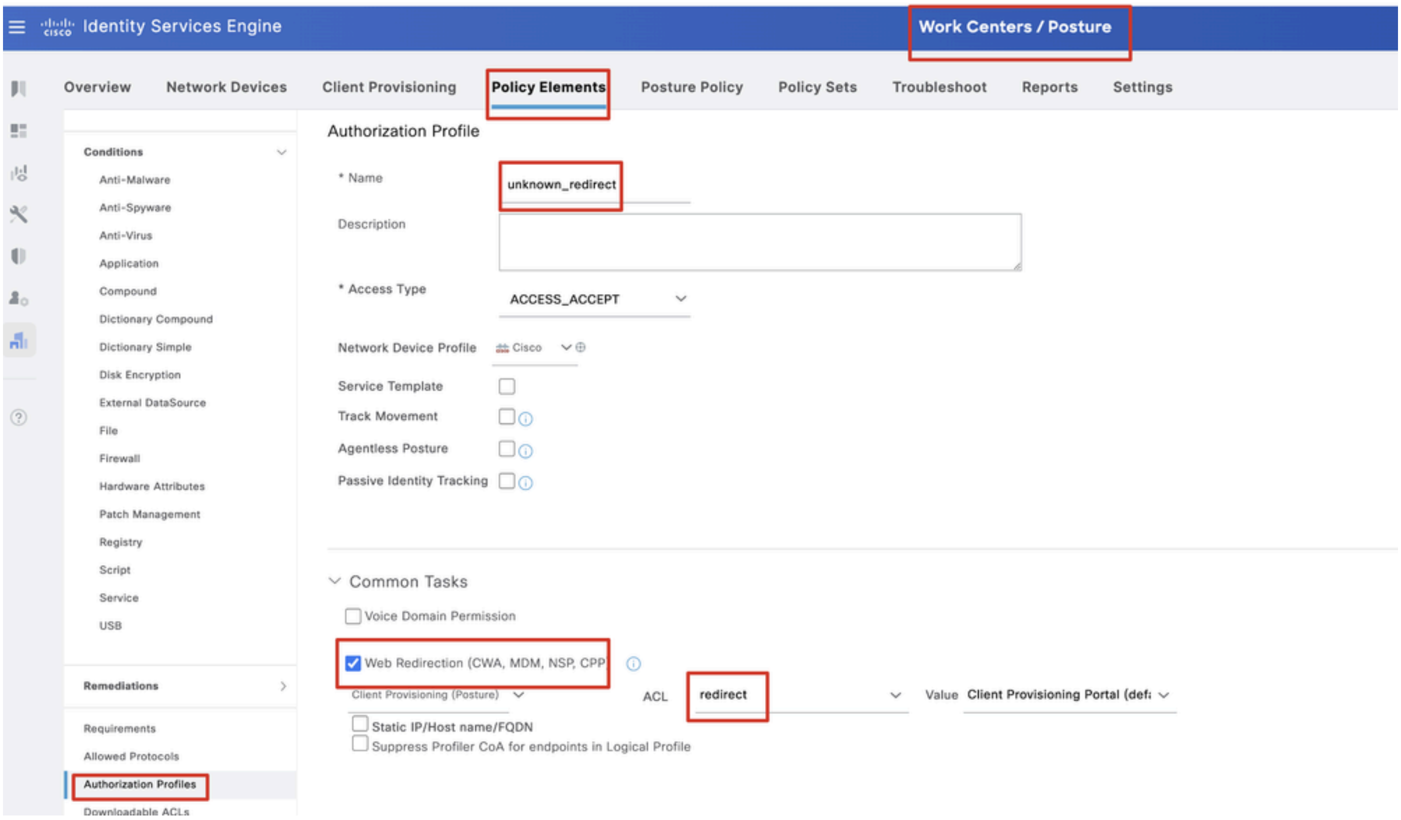
名称：unknown_redirect

选中复选框 Web Redirection(CWA,MDM,NSP,CPP)

选择 Client Provisioning(Posture)

ACL：重定向

值：客户端调配门户（默认）



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

注意：此ACL名称重定向必须与FTD上配置的相应ACL名称匹配。

步骤 21.2重复Add 以为不兼容和兼容的终端创建另外两个授权配置文件及详细信息。

名称：non_compliant_profile

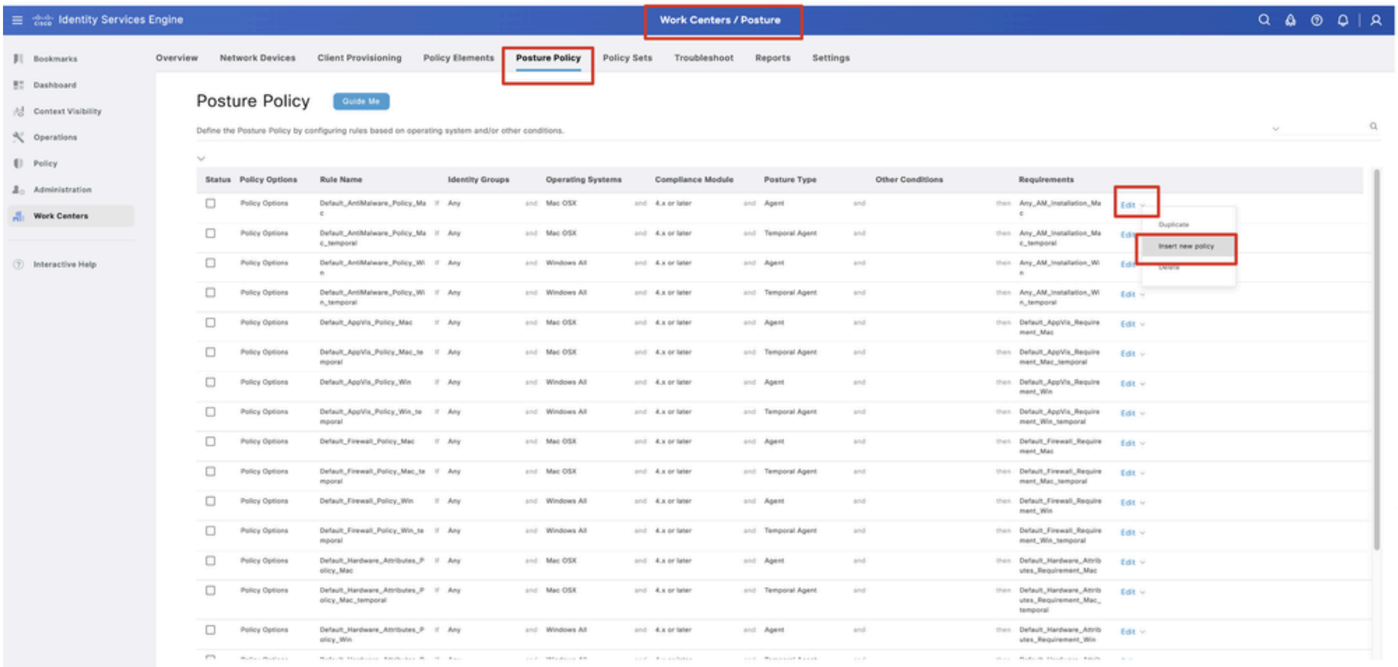
DACL名称：DENY_ALL_IPv4_TRAFFIC

名称：compliant_profile

DACL名称：PERMIT_ALL_IPv4_TRAFFIC

注意：需要根据实际要求配置合规或不合规终端的DACL。

步骤 22. 导航到Work Centers > Posture > Posture Policy。在任何规则末尾单击Edit 。选择.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

步骤 22.1 配置详细信息：

规则名称：Demo_test_exist_linux

身份组：任意

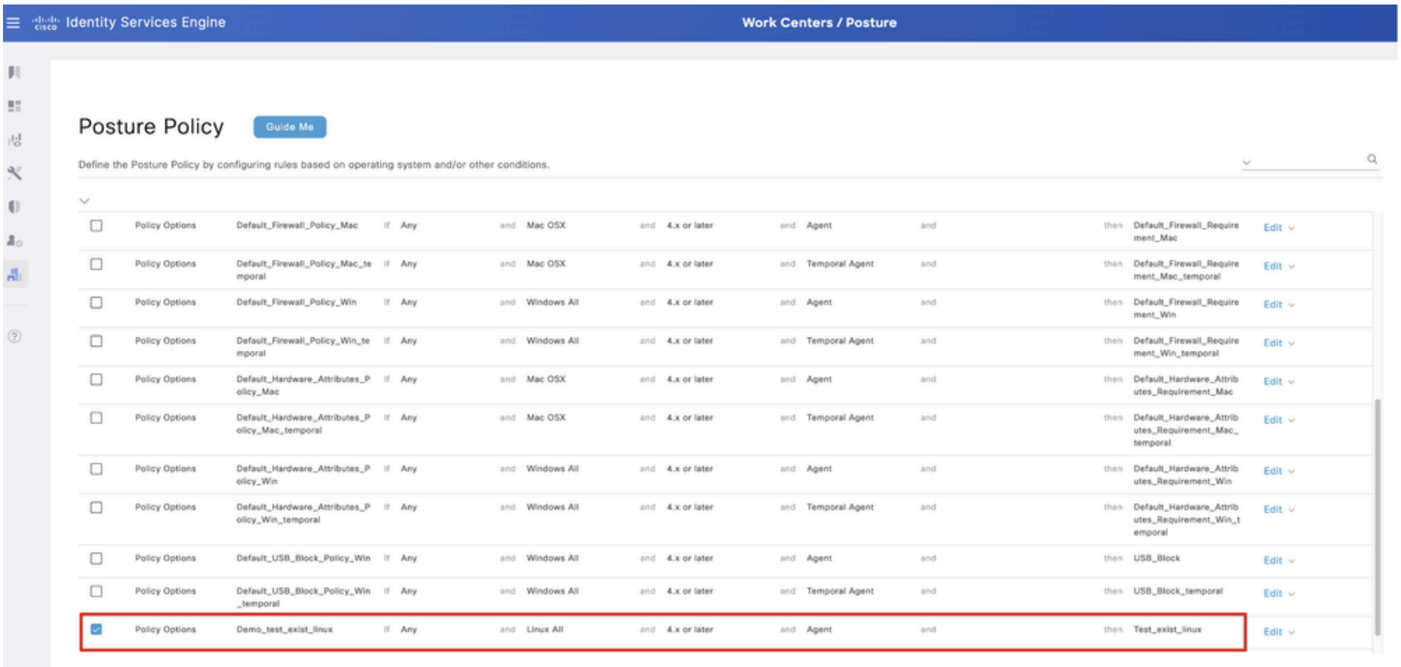
操作系统：Linux All

合规性模块：4.x或更高版本

状态类型：代理

要求：Test_exist_linux

单击Done 和Save。



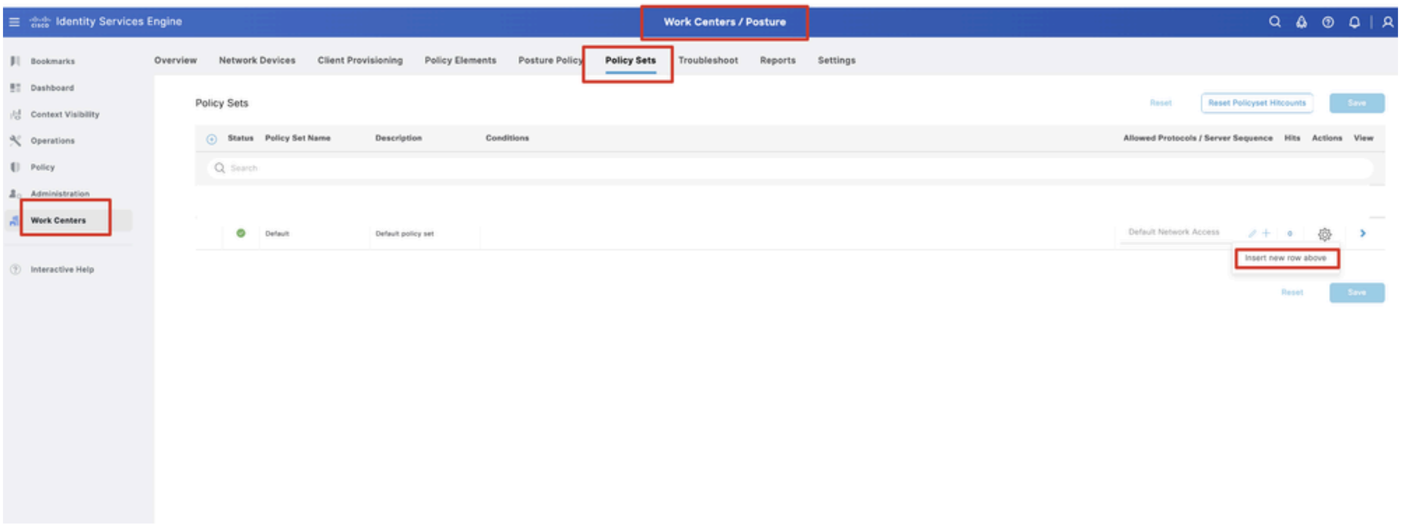
Posture Policy

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

步骤 23. 导航到Work Centers > Posture > Policy Sets。单击以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		›

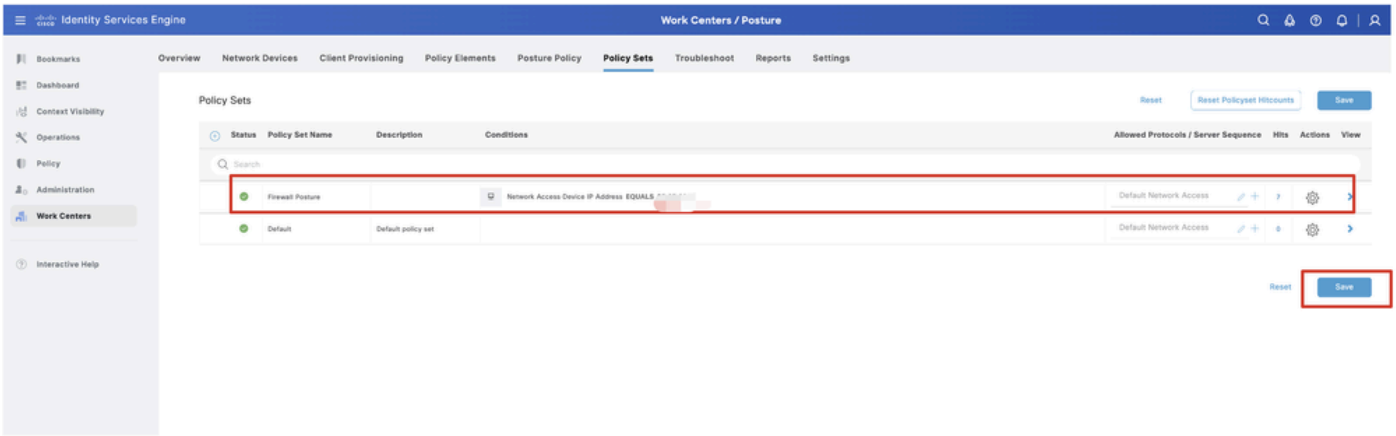
ISE_Add_New_Policy_Set

步骤 23.1 配置详细信息：

策略集名称：Firewall Posture

条件：网络接入设备IP地址等于[FTD IP地址]

单击。 Save



Policy Sets

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

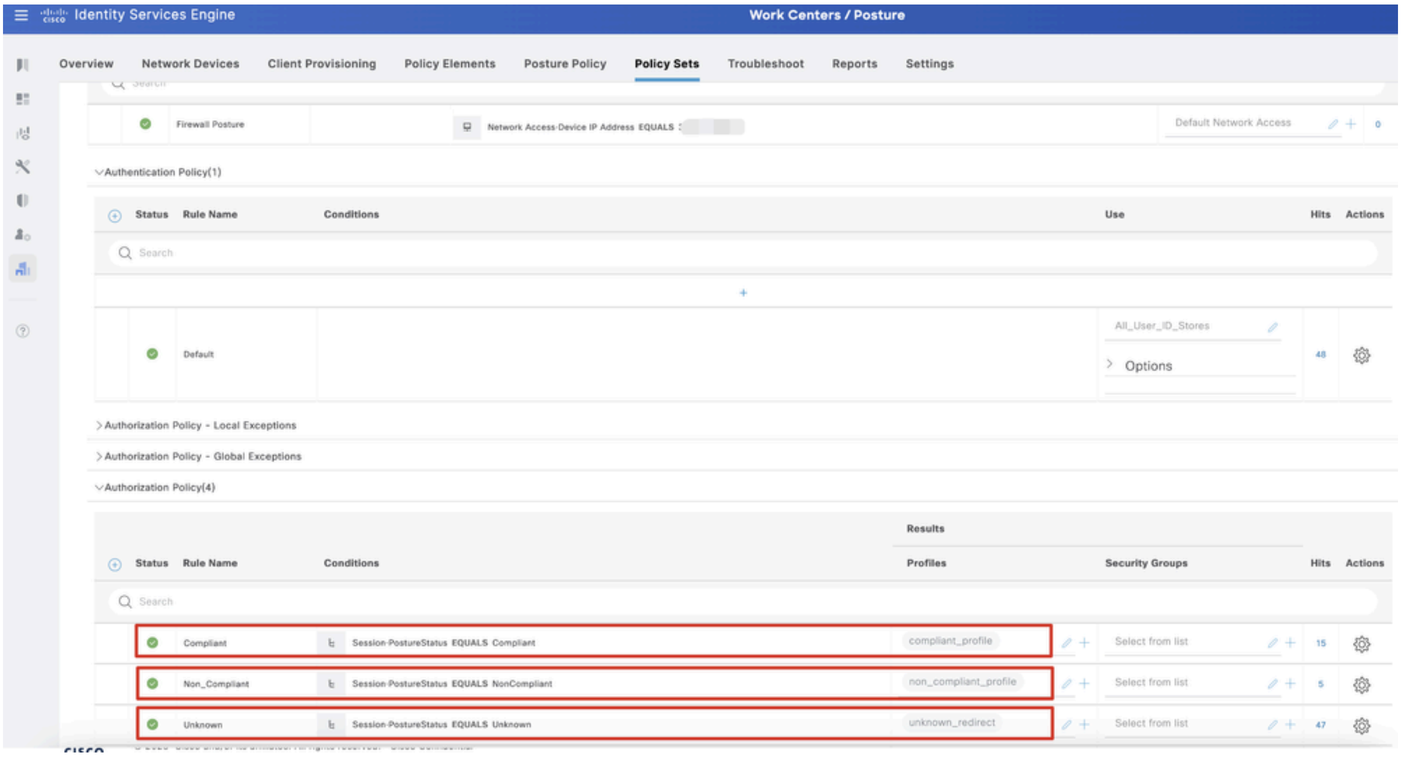
ISE_Add_New_Policy_Set_1

步骤 23.2单击>以输入策略集。 为状态兼容、不兼容和未知状态创建新的授权规则。单击。Save

与compliant_profile兼容

与non_compliant_profile不兼容

Unknown_redirect未知



Status	Policy Set Name	Description	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

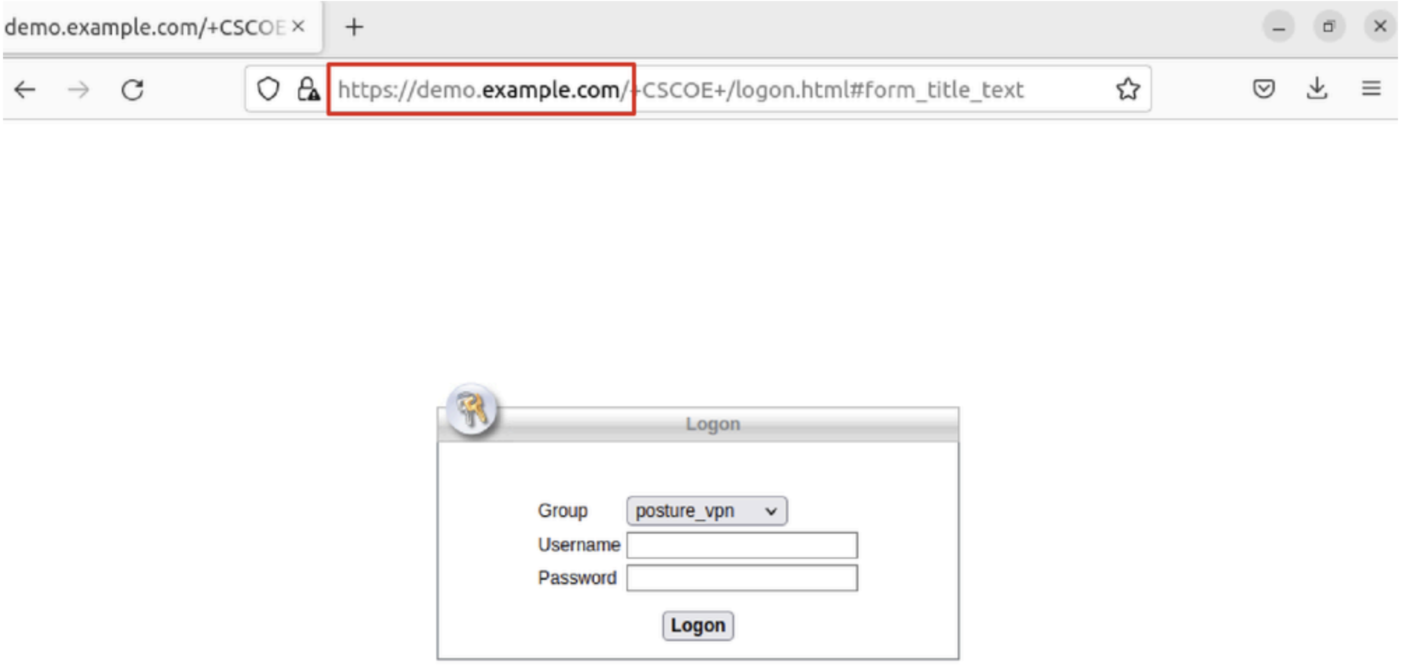
Authorization Policy(4)

			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

Ubuntu上的配置

步骤 24通过GUI登录到Ubuntu客户端。打开浏览器以登录VPN门户。在本例中为demo.example.com。



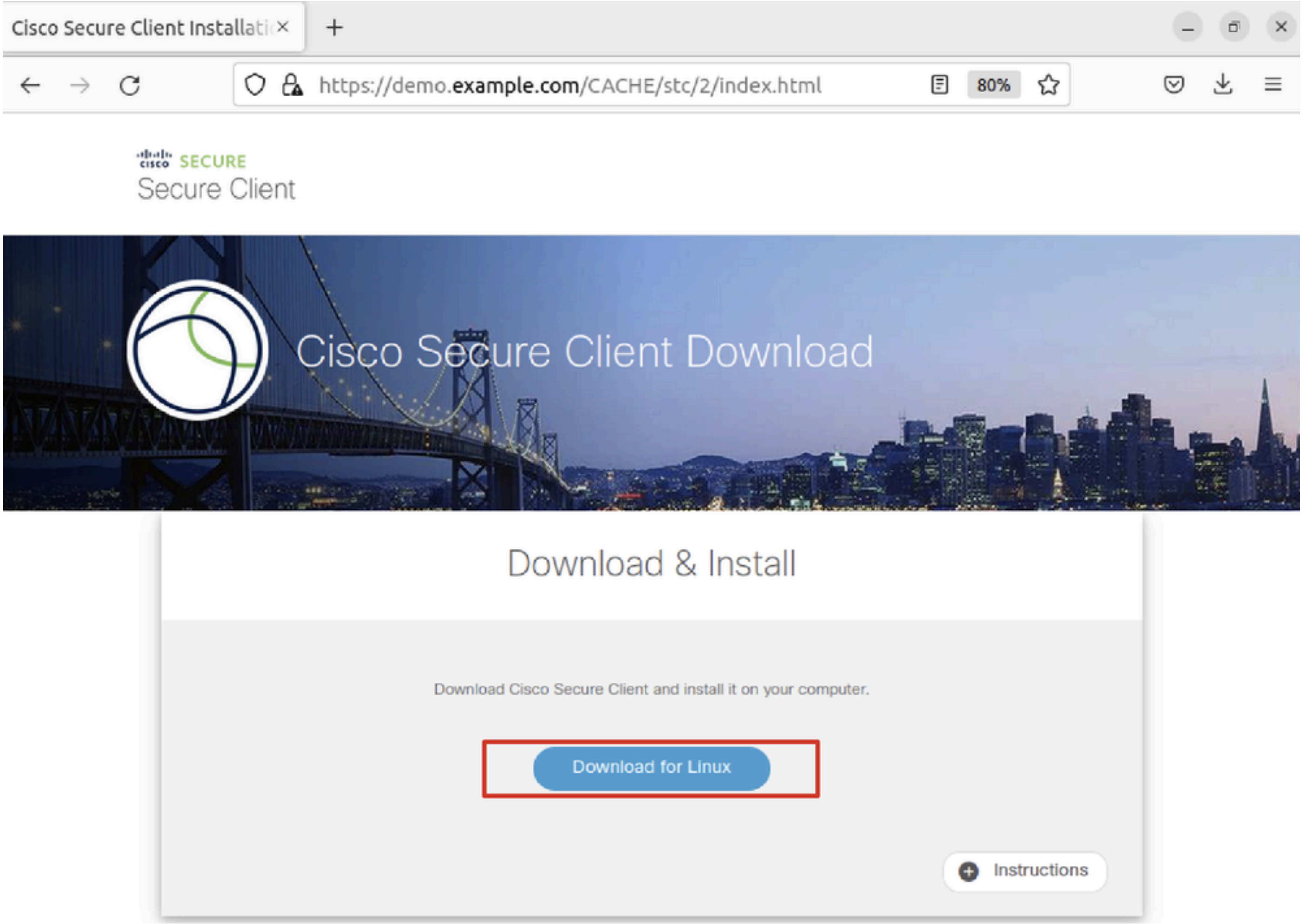
Group posture_vpn

Username

Password

Ubuntu_Browser_VPN_Login

步骤 25单击。Download for Linux

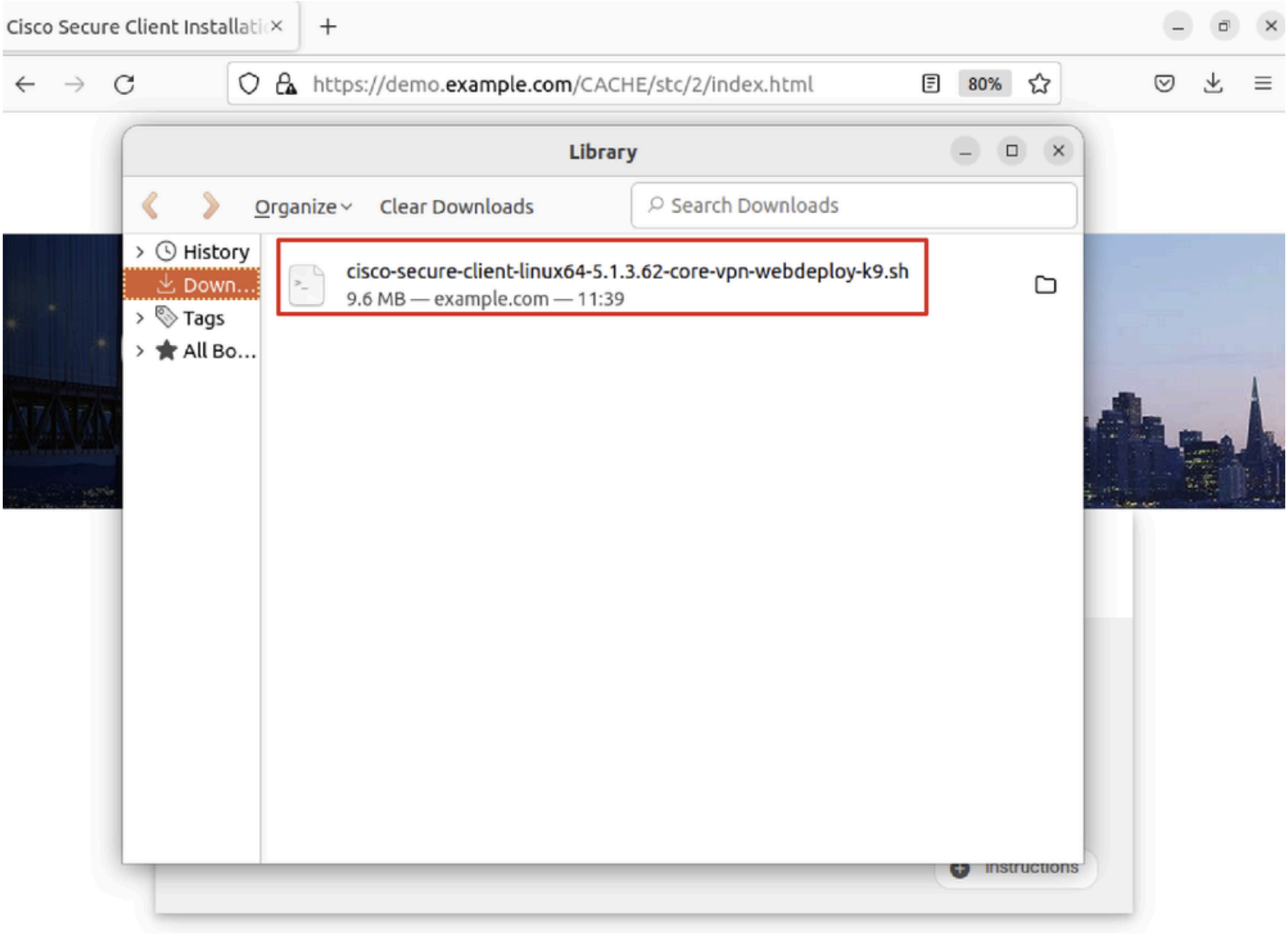


Cisco Secure Client Installati
https://demo.example.com/CACHE/stc/2/index.html
80%
SECURE
Secure Client
Cisco Secure Client Download
Download & Install
Download for Linux
Instructions

Download Cisco Secure Client and install it on your computer.

Ubuntu_Browser_VPN_Download_1

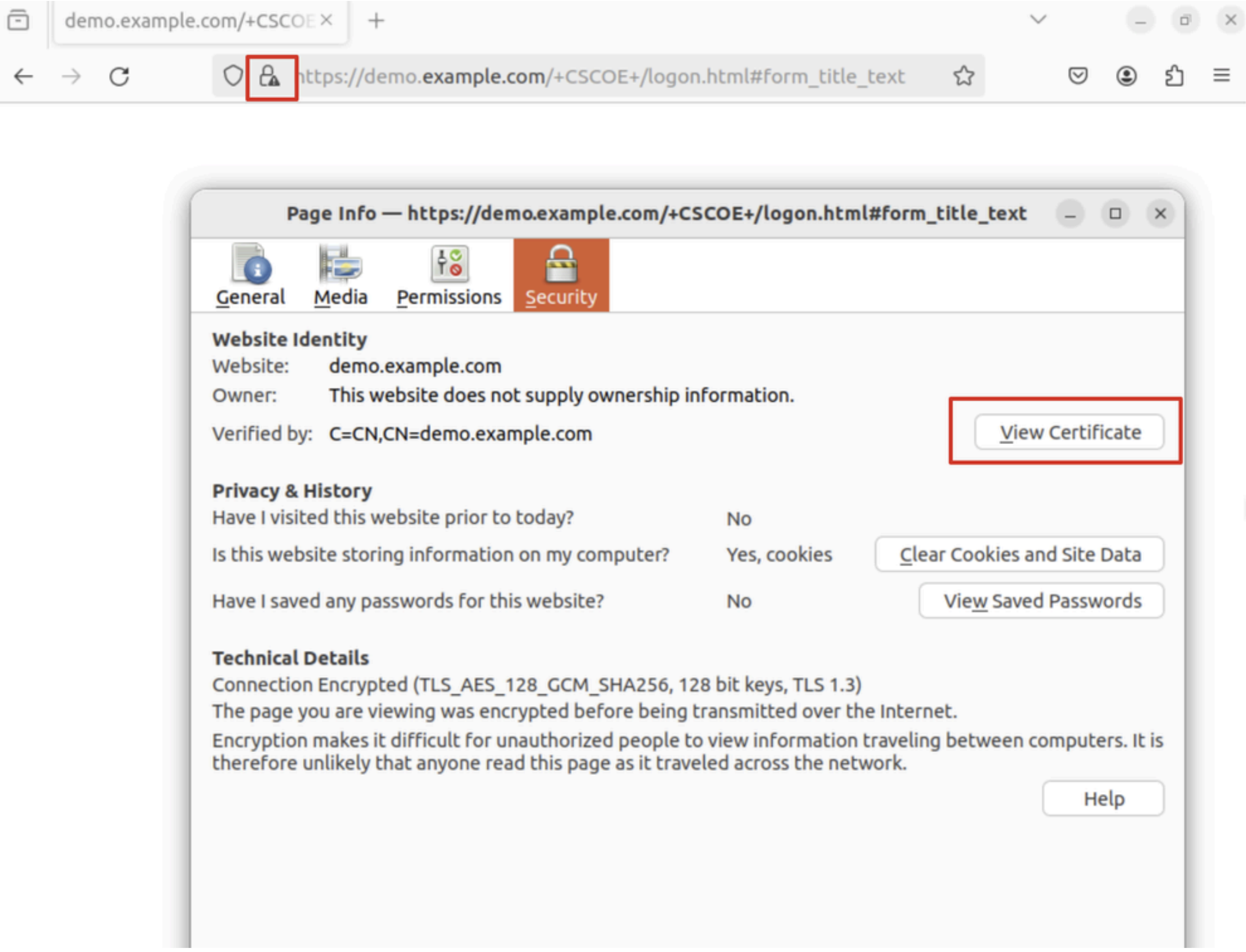
下载的文件名为cisco-secure-client-linux64-5.1.3.62-core-vpn-webdeploy-k9.sh。



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

步骤 26通过浏览器下载VPN证书并将文件重命名为<certificate>.crt。这是使用firefox下载证书的示例。



demo.example.com/+CSCOE

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

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

步骤 27在Ubuntu客户端上打开终端。导航到path home/user/Downloads/安装Cisco安全客户端。

<#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$
```

步骤 28信任Ubuntu客户端上的VPN门户证书。

<#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
```

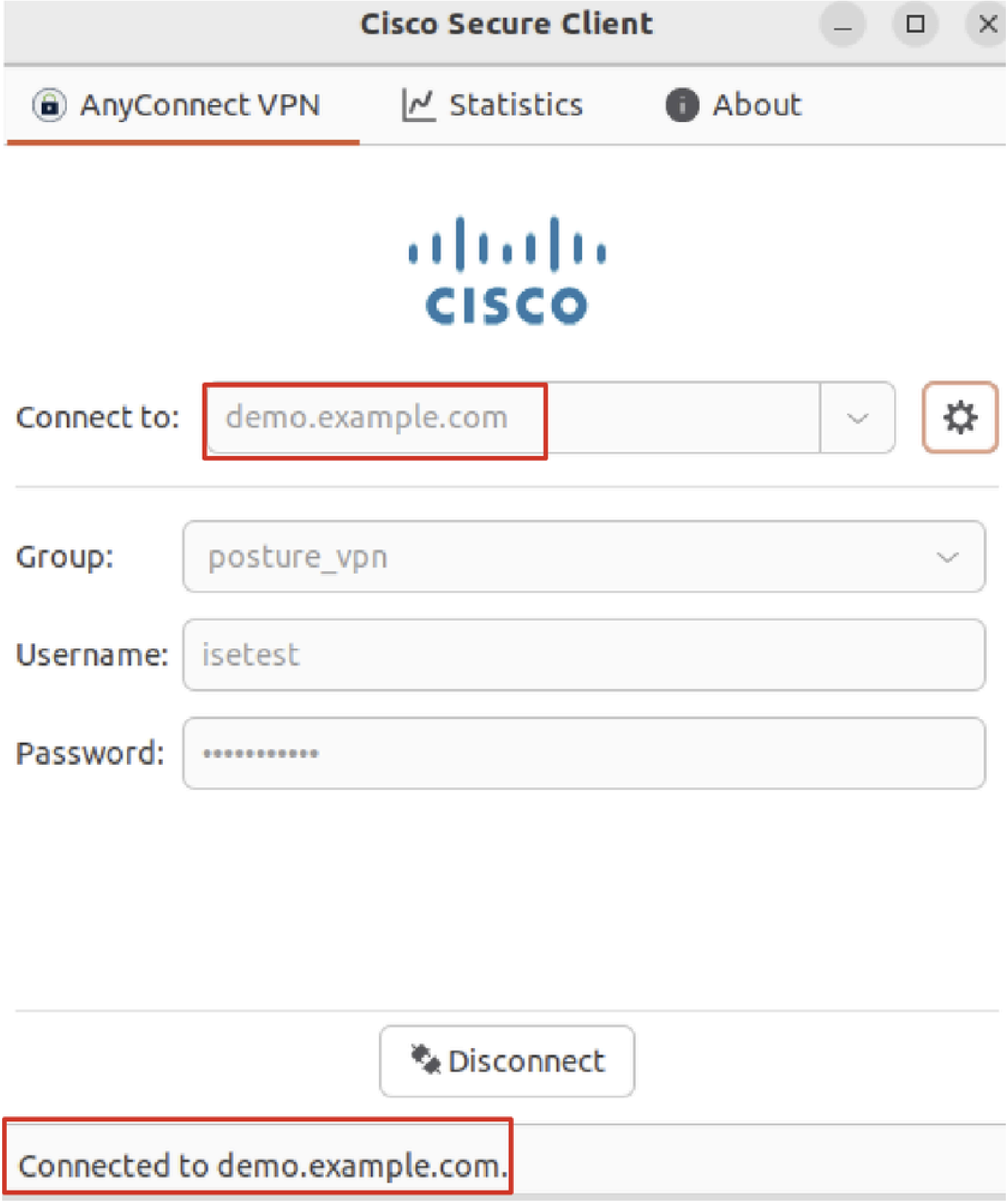
```
Updating certificates in /etc/ssl/certs...
rehash: warning: skipping ca-certificates.crt,it does not contain exactly one certificate or CRL
```

```
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
```

步骤 29在Ubuntu客户端上打开Cisco Secure Client，然后将VPN成功连接到demo.example.com。



Connect to: demo.example.com

Group: posture_vpn

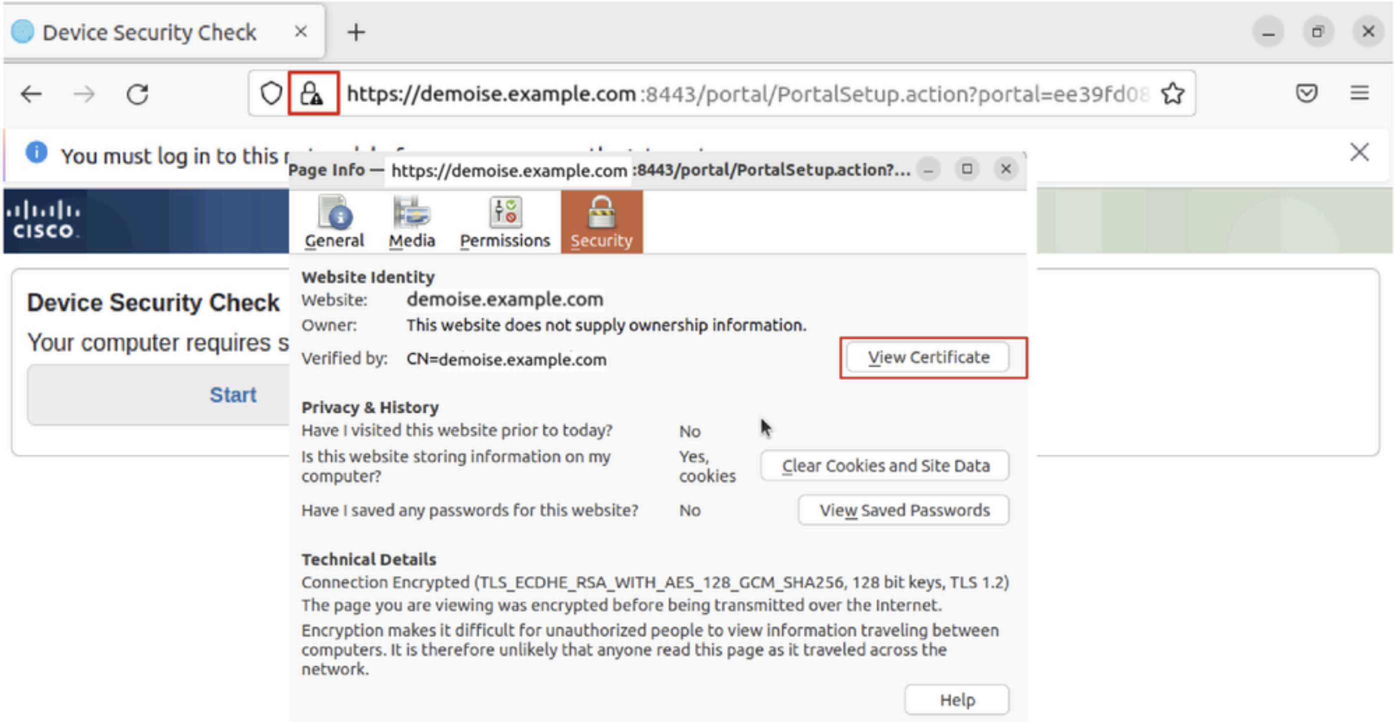
Username: isetest

Password: ••••••••••••

Connected to demo.example.com.

Ubuntu_Secure_Client_Connected

步骤 30打开浏览器以访问触发重定向至ISE CPP门户的任何网站。从ISE CPP门户下载证书并将文件重命名为<certificate>.crt。 这是使用Firefox进行下载的示例。



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?...
General
Media
Permissions
Security
View Certificate
Clear Cookies and Site Data
View Saved Passwords
Help

Website Identity

Website: demoise.example.com

Owner: This website does not supply ownership information.

Verified by: CN=demoise.example.com

Privacy & History

Have I visited this website prior to today? No

Is this website storing information on my computer? Yes, cookies

Have I saved any passwords for this website? No

Technical Details

Connection Encrypted (TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, 128 bit keys, TLS 1.2)

The page you are viewing was encrypted before being transmitted over the Internet.

Encryption makes it difficult for unauthorized people to view information traveling between computers. It is therefore unlikely that anyone read this page as it traveled across the network.

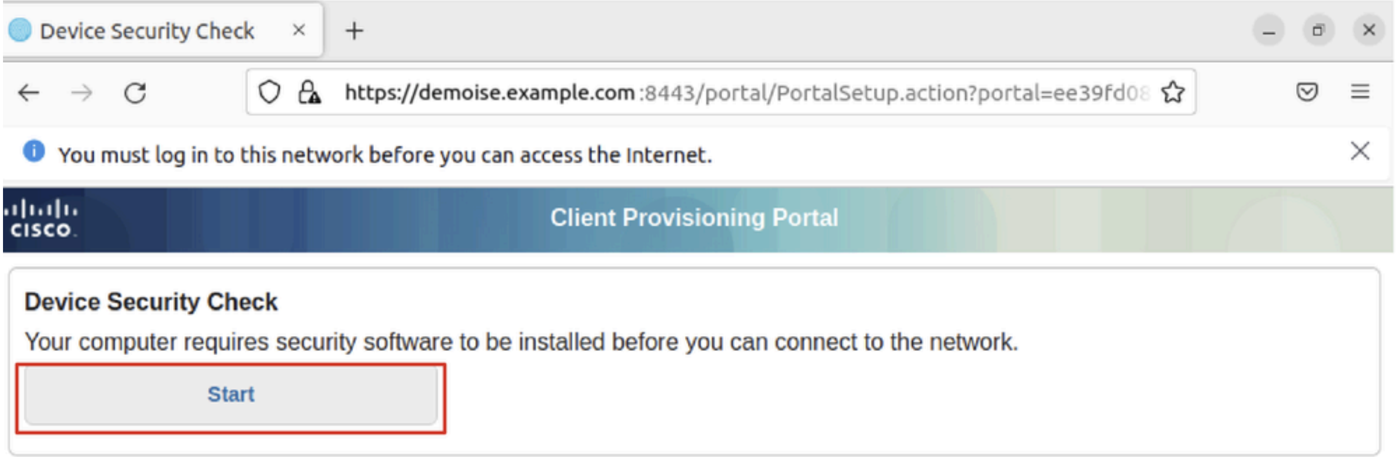
Ubuntu_Browser_CPP_Cert_Download

步骤 30.1信任Ubuntu客户端上的ISE CPP门户证书。

<#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.
```

步骤 31在ISE CPP门户上点击Start 。


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

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

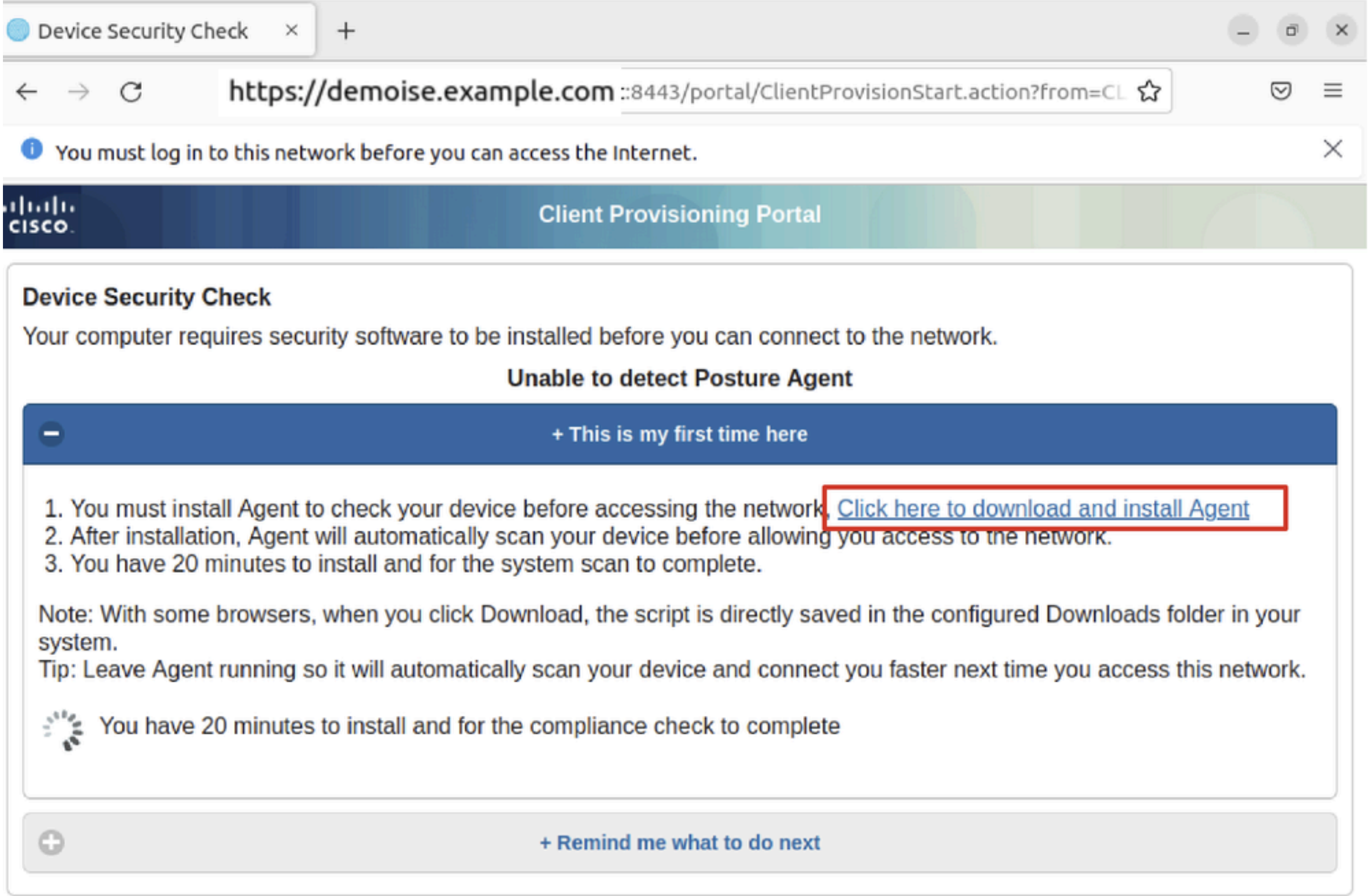
Client Provisioning Portal

Device Security Check

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

Ubuntu_Browser_CPP_Start

步骤32.Click here to download and install Agent.


Device Security Check
https://demoise.example.com:8443/portal/ClientProvisionStart.action?from=CL
+ 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.

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

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

步骤 33在Ubuntu客户端上打开终端。导航到路径home/user/Downloads/，安装状态模块。

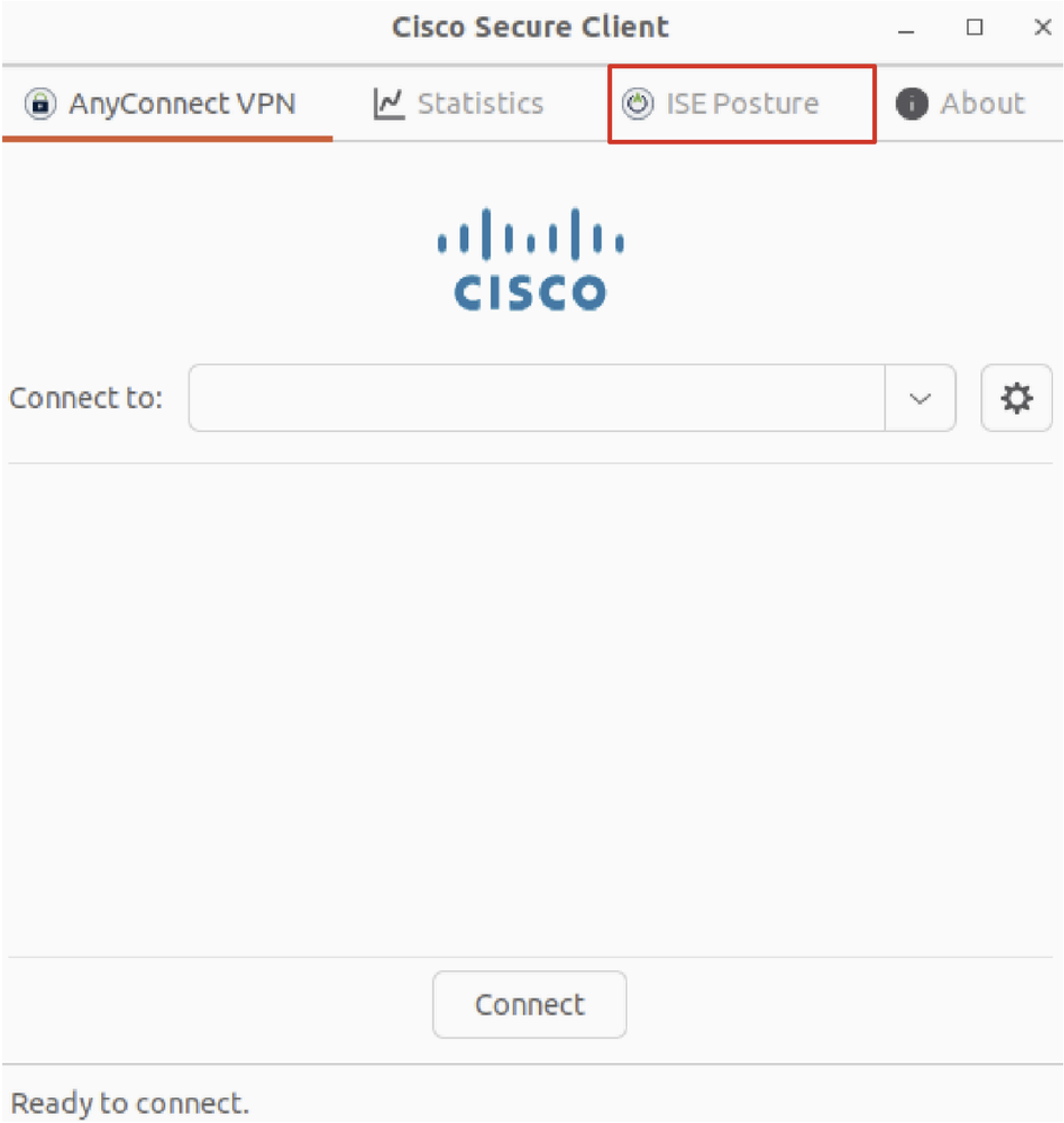
<#root>

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.
```

步骤 34在Ubuntu客户端UI上，退出Cisco安全客户端并重新打开它。ISE终端安全评估模块安装成功并运行。



Ubuntu_Secure_Client_ISE_Posture_Installed

步骤 35在Ubuntu客户端上打开终端。导航到路径home/user/Desktop，创建test.txt一个文件以满足ISE上配置的文件条件。

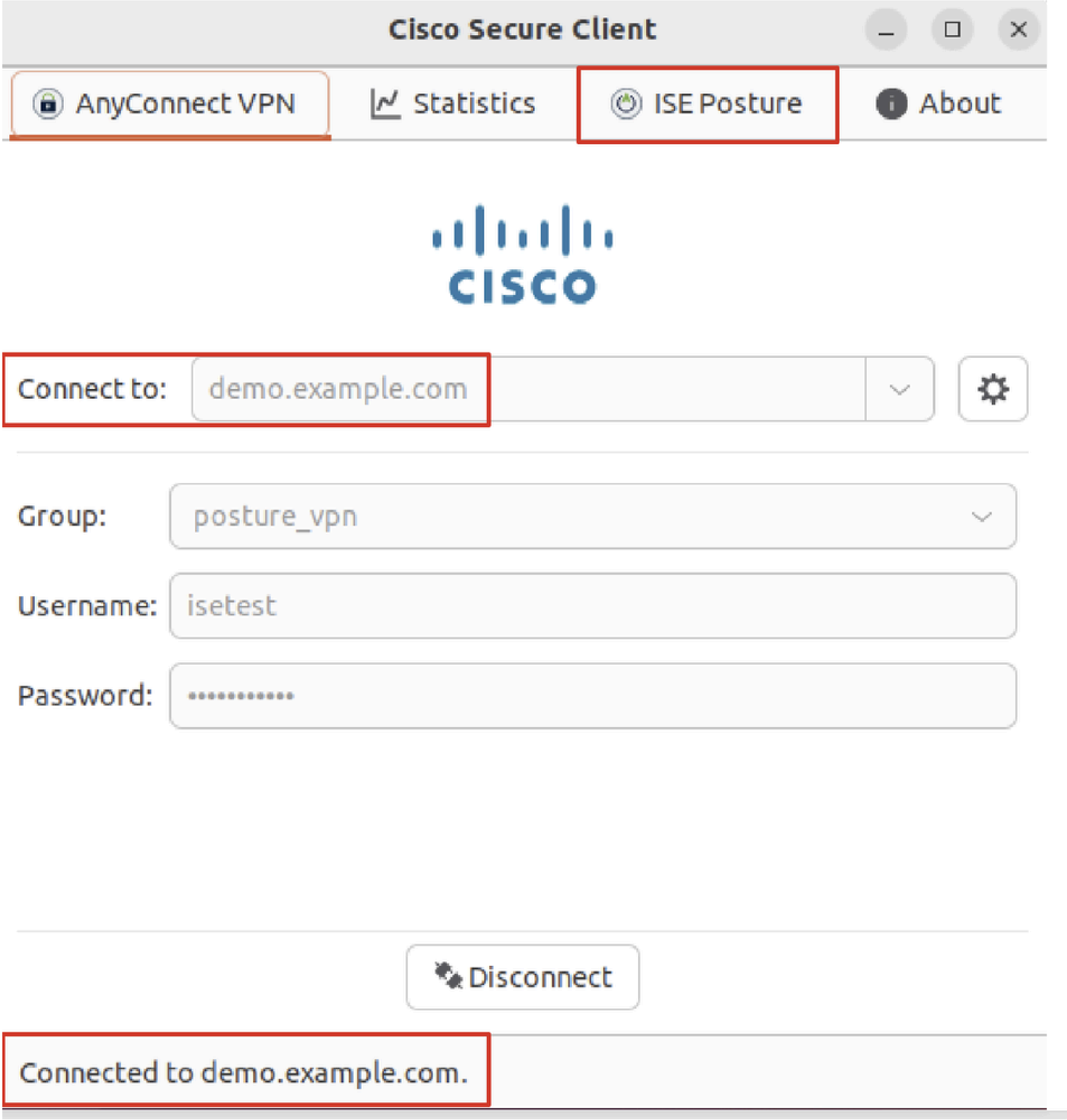
<#root>

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

user@ubuntu22-desktop:~/Desktop$
echo test > test.txt
```

验证

使用本部分可确认配置能否正常运行。

步骤1:在Ubuntu客户端上将VPN连接到demo.example.com。



Connect to: demo.example.com

Group: posture_vpn

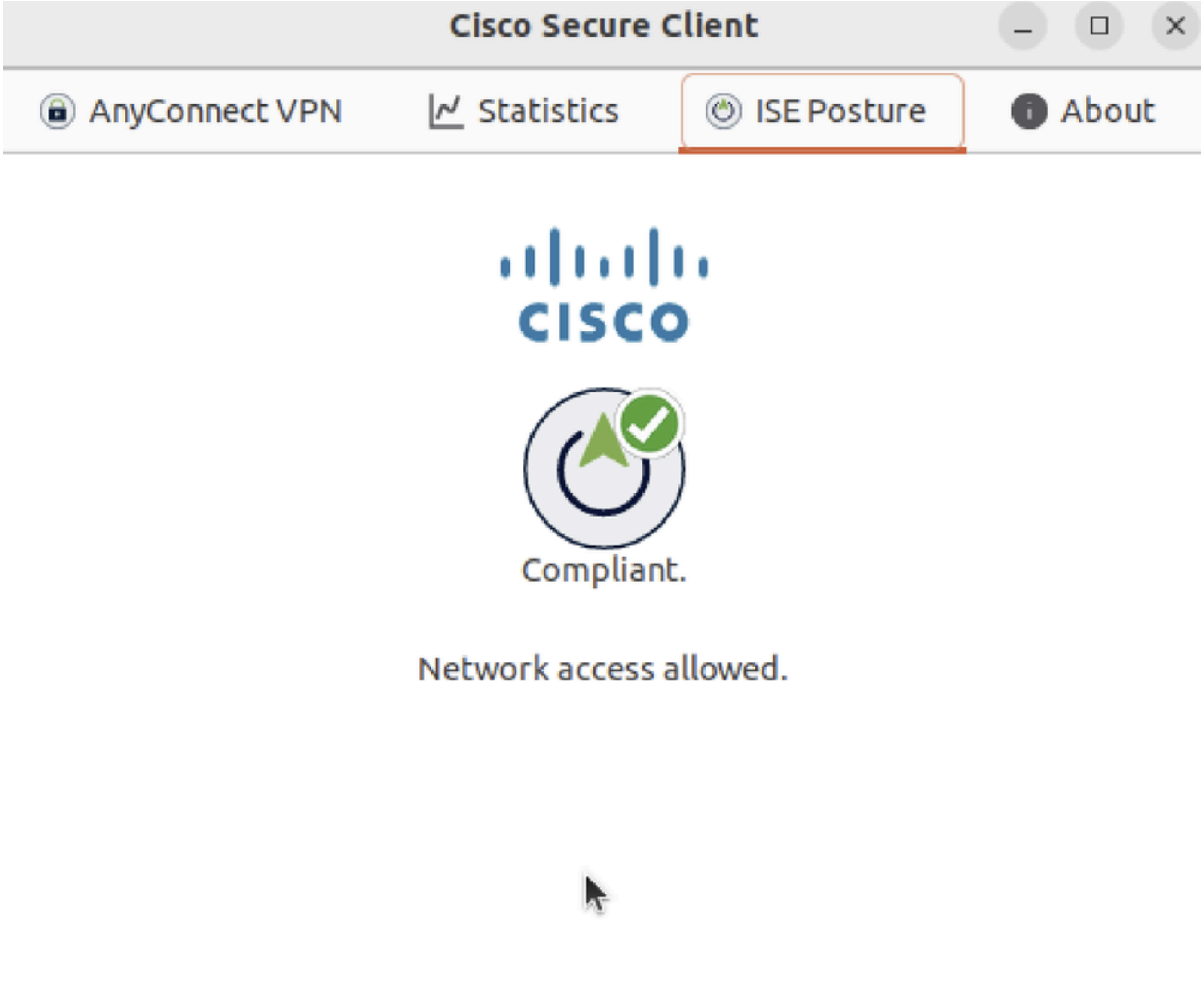
Username: isetest

Password: ••••••••••••

Connected to demo.example.com.

Verify_Ubuntu_Secure_Client_Connected

第二步：检查Ubuntu客户端上的ISE终端安全评估状态。

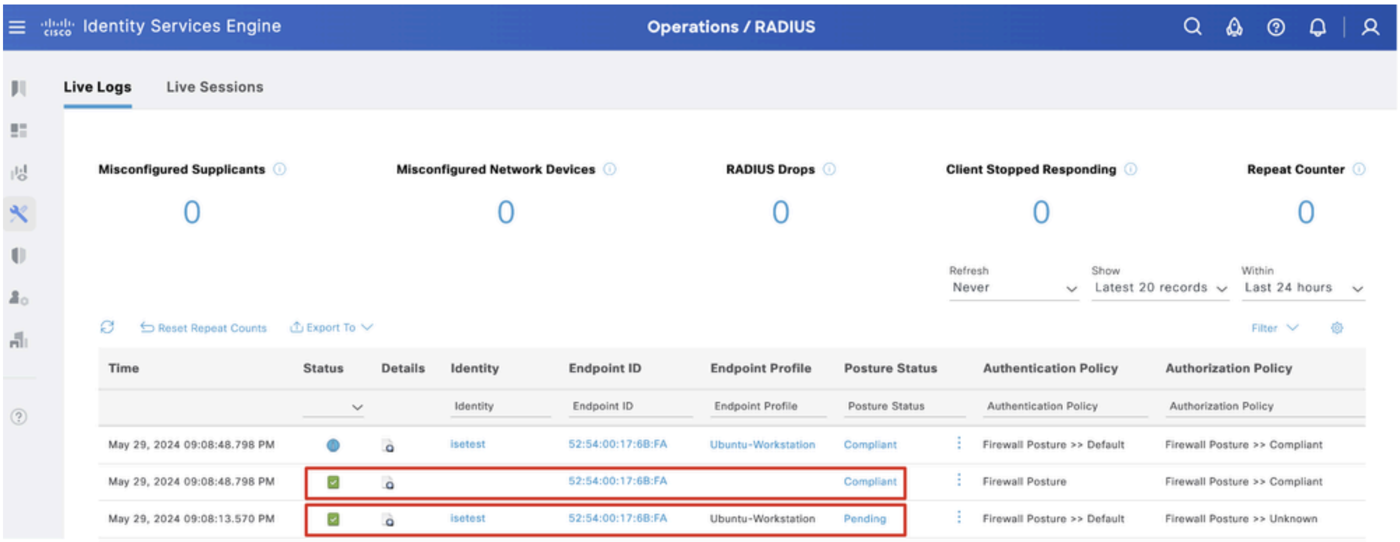


Compliant.

Network access allowed.

Verify_Ubuntu_Secure_Client_Compliance

第三步：检查ISE上的Radius实时日志。导航到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
			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

第四步：通过SSH或控制台导航至FTD CLI。

<#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
```

故障排除

本部分提供了可用于对配置进行故障排除的信息。

对于终端安全评估流程和思科安全客户端和ISE故障排除，请检查CCO文档ISE终端安全评估样式比较高级版和2.2后版本以及ISE会话管理和终端安全评估故障排除。

相关信息

- 思科身份服务引擎网络组件兼容性，版本3.3

- 思科身份服务引擎管理员指南，版本3.3

- **思科技**术支持和下载

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。