

# ISE 3.3を使用したLinux VPNポスチャの設定

## 内容

---

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[ネットワーク図](#)

[FMC/FTDでの設定](#)

[ISEでの設定](#)

[Ubuntuでの設定](#)

[確認](#)

[トラブルシューティング](#)

[関連情報](#)

---

## はじめに

このドキュメントでは、Identity Services Engine(ISE)およびFirepower Threat Defense(FTD)でLinux VPNポスチャを設定する方法について説明します。

## 前提条件

### 要件

次の項目に関する知識があることが推奨されます。

- Cisco Secureクライアント
- Firepower Threat Defense(FTD)のリモートアクセスVPN
- Identity Services Engine ( ISE )

### 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアのバージョンに基づいています。

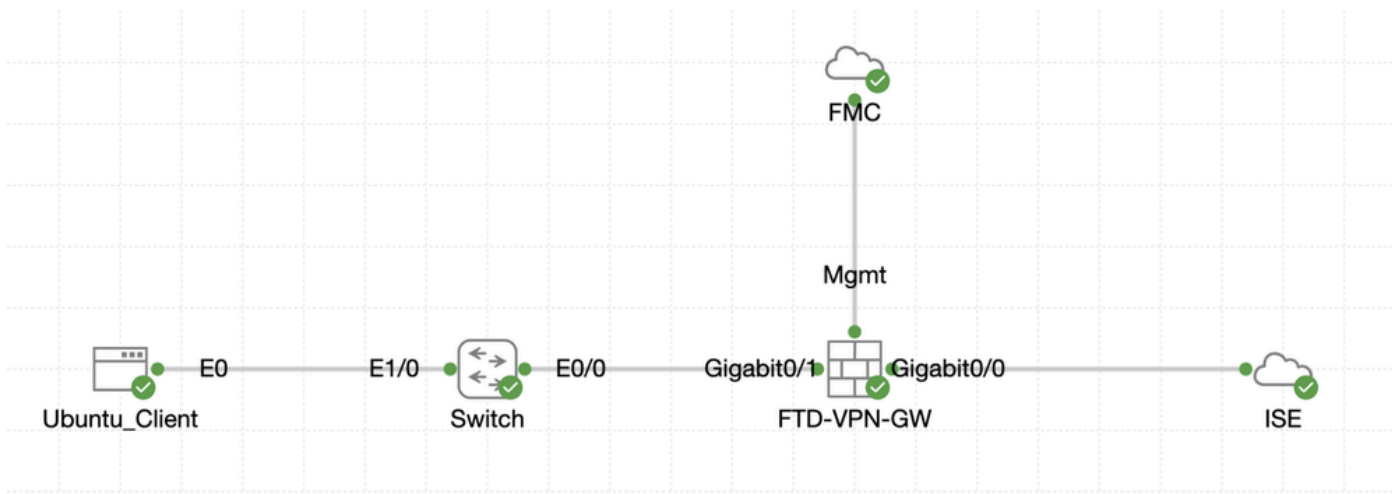
- Ubuntu 22.04
- Cisco Secureクライアント5.1.3.62
- Cisco Firepower Threat Defense(FTD)7.4.1
- Cisco Firepower Management Center(FMC)7.4.1
- Cisco Identity Services Engine(ISE)3.3

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド

キュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

## 設定

### ネットワーク図



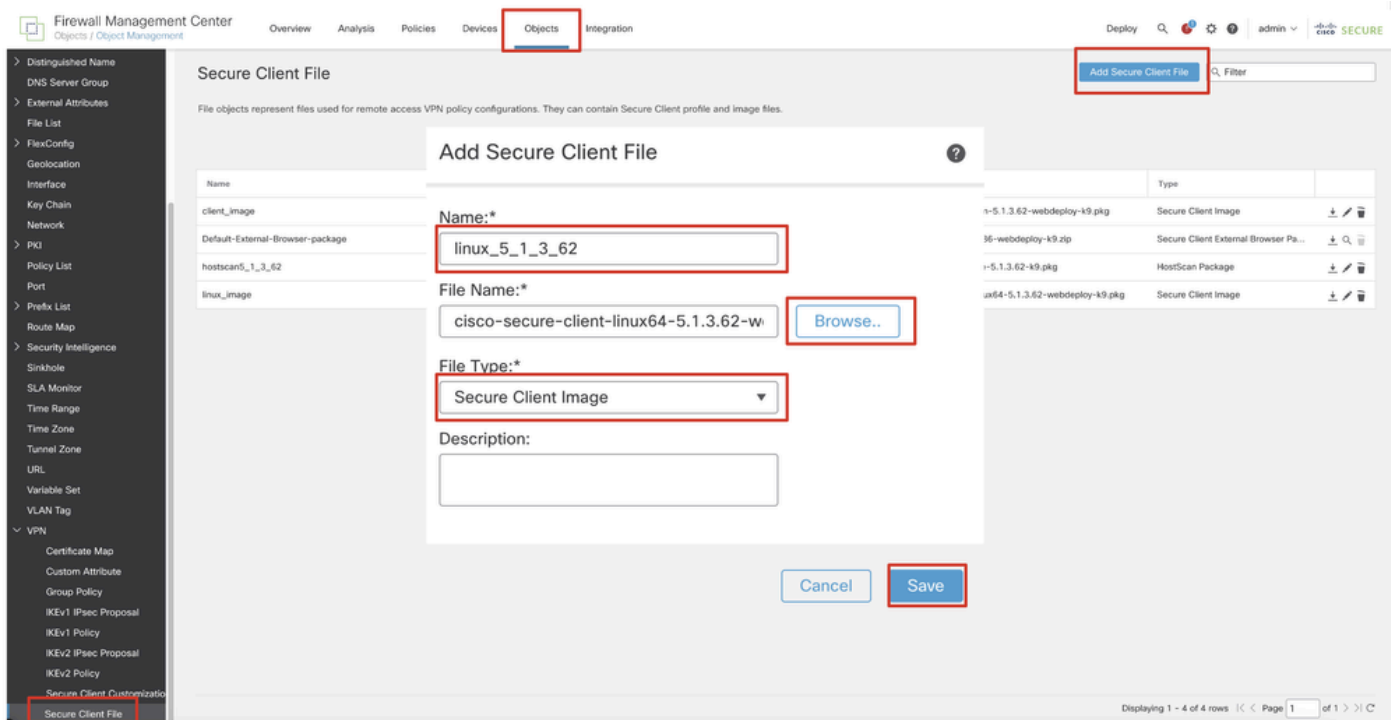
トポロジ

### FMC/FTDでの設定

ステップ 1：クライアント、FTD、FMC、およびISE間の接続が正常に設定されました。as enroll.cisco.comは、リダイレクトのプローブを行うエンドポイントに使用されます(詳細については、『ポスチャフロ-CCOドキュメント:2.2前後のISEポスチャスタイル比較』を参照してください)。FTDでenroll.cisco.comへのトラフィックのルートが正しく設定されていることを確認します。

ステップ 2： [Cisco Software Download](#)からパッケージ名cisco-secure-client-linux64-5.1.3.62-webdeploy-k9.pkgをダウンロードし、ダウンロードしたファイルのmd5チェックサムがCisco Software Downloadページと同じであることを確認して、ダウンロード後にファイルの状態が良好であることを確認します。

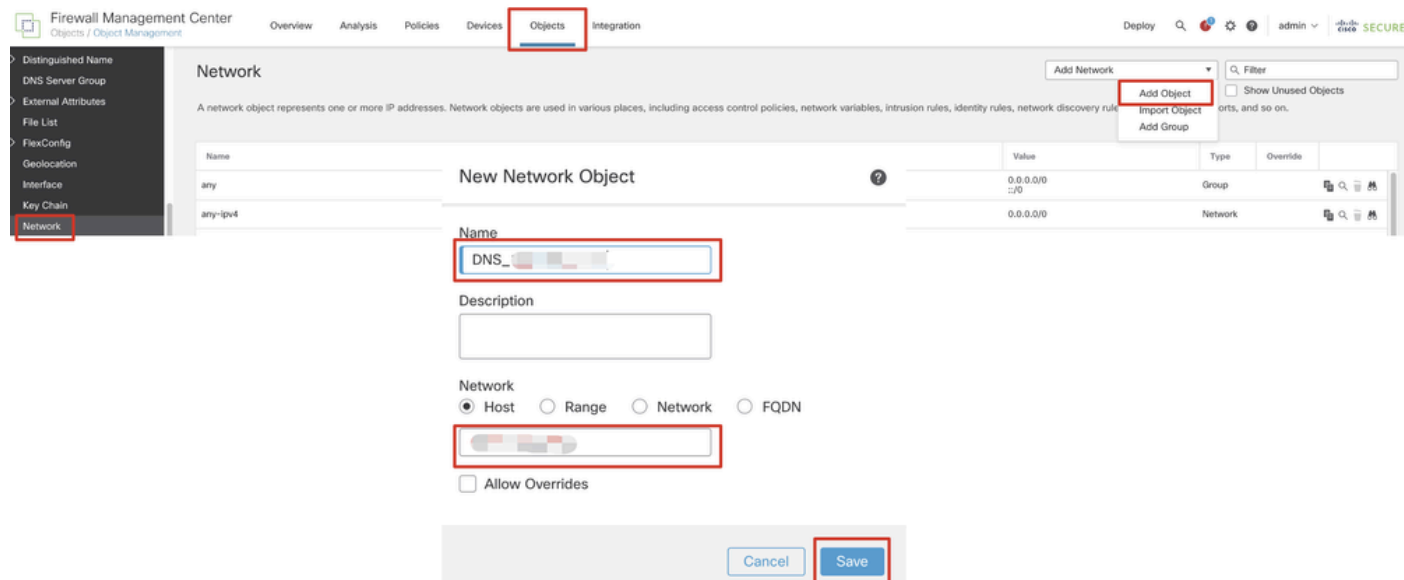
ステップ 3： Objects > Object Management > VPN > Secure Client Fileに移動します。Add Secure Client Fileをクリックし、名前を入力し、File Nameを参照して選択します。cisco-secure-client-linux64-5.1.3.62-webdeploy-k9.pkg、Secure Client Image inFile Typeドロップダウンリストを選択します。次にSaveをクリックします。



FMC\_Upload\_Secure\_Client\_イメージ

ステップ 4 : Objects > Object Management > Networkに移動します。

ステップ 4.1 : DNSサーバのオブジェクトを作成します。Add Objectをクリックし、名前と使用可能なDNS IPアドレスを入力します。をクリックします。Save



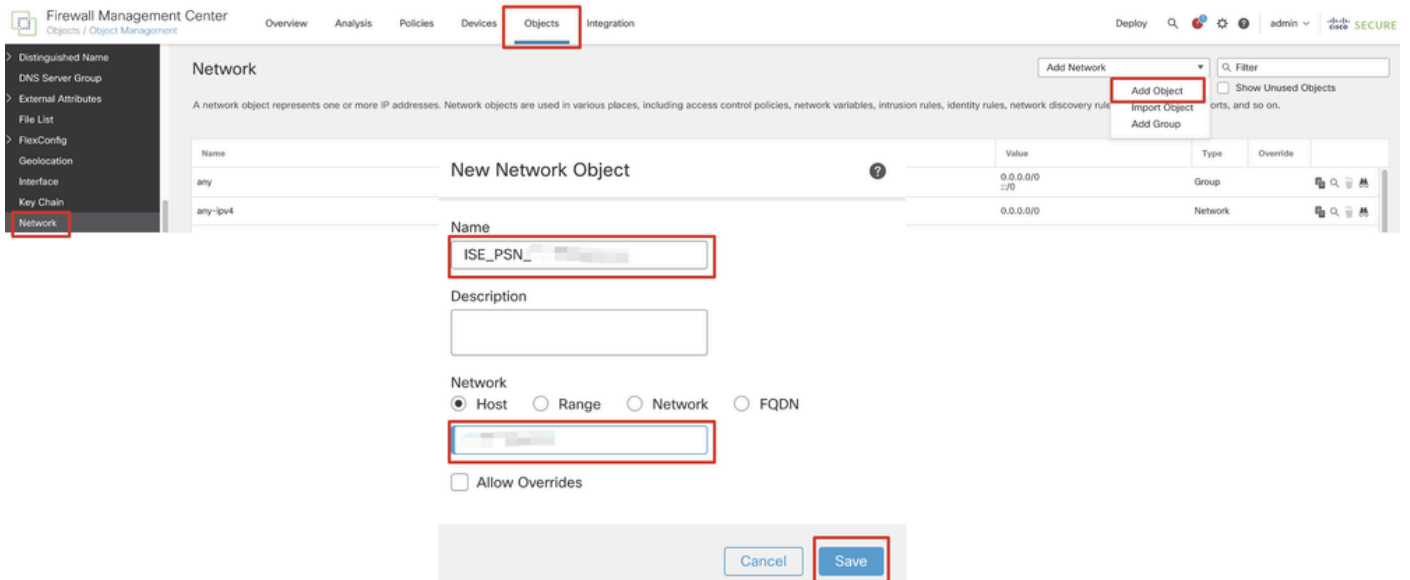
FMC\_Add\_Object\_DNS ( オプション )



注：ここで設定するDNSサーバは、VPNユーザ用です。

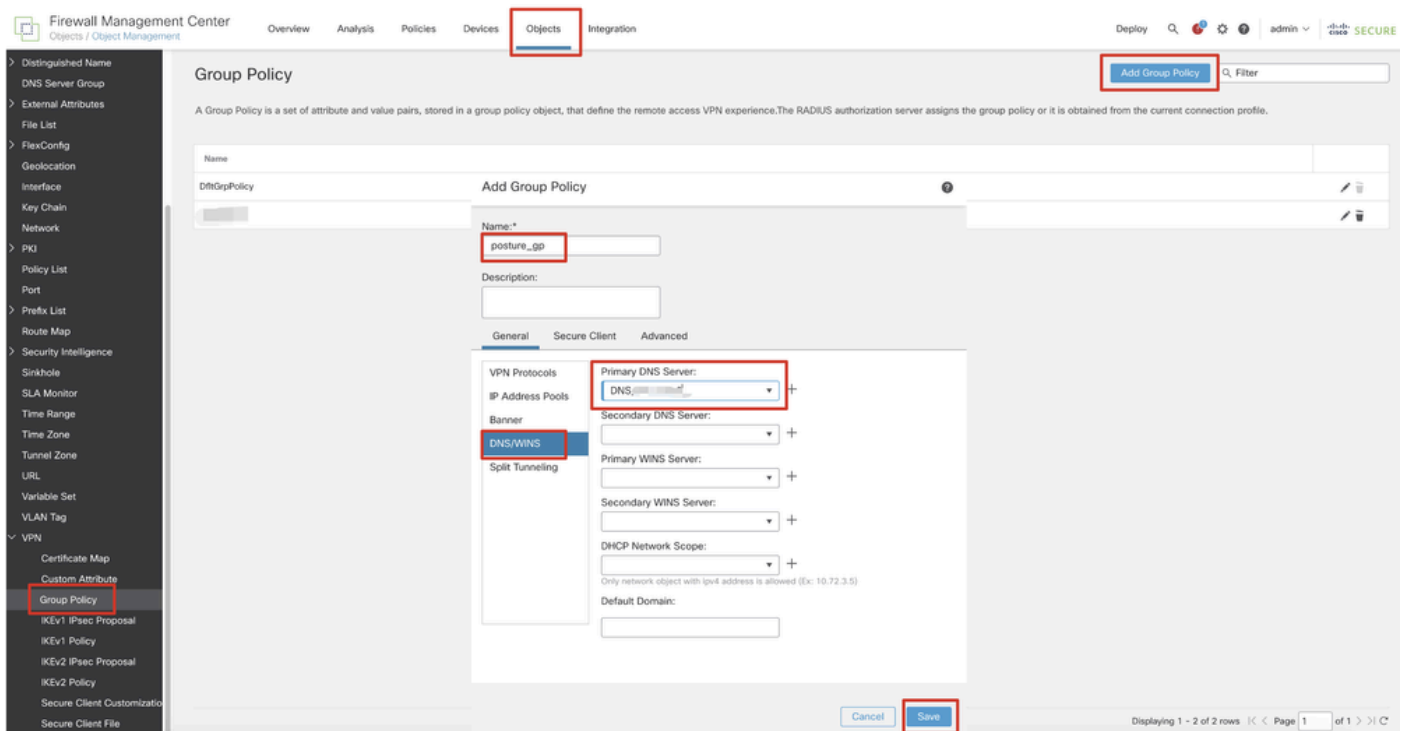
---

ステップ 4.2 : ISE PSNのオブジェクトを作成します。Add Objectをクリックし、名前と使用可能なISE PSN IPアドレスを入力します。をクリックします。Save



FMC\_Add\_Object\_ISE ( オプション )

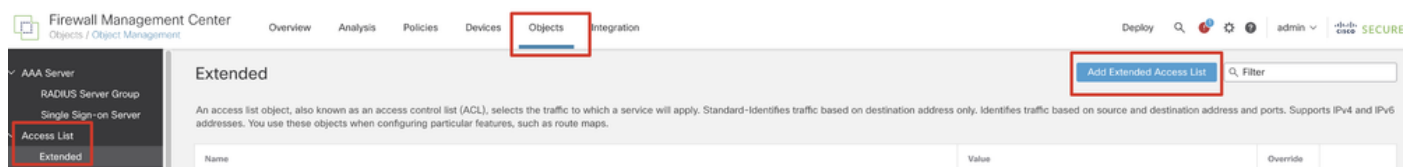
ステップ 5 : Objects > Object Management > VPN > Group Policyに移動します。をクリックします。Add Group PolicyDNS/WINSをクリックし、Primary DNS ServerでDNSサーバのオブジェクトを選択します。次にSaveをクリックします。



FMC\_Add\_Group\_ポリシー

注：VPNグループポリシーで使用されるDNSサーバがISEクライアントプロビジョニングポータル(FQDNとenroll.cisco.com)を解決できることを確認します。

手順 6： Objects > Object Management > Access List > Extendedに移動します。をクリックします。Add Extended Access List



The screenshot shows the Firewall Management Center (FMC) interface. The top navigation bar includes 'Overview', 'Analysis', 'Policies', 'Devices', 'Objects', and 'Integration'. The 'Objects' tab is selected. On the left sidebar, the 'Access List' menu item is highlighted, and the 'Extended' sub-item is selected. The main content area displays the 'Extended' configuration page, which includes a description of access list objects and a table with columns for 'Name', 'Value', and 'Override'. A blue button labeled 'Add Extended Access List' is visible in the top right corner of the main content area.

FMC\_追加\_リダイレクト\_ACL

ステップ 6.1 : リダイレクトACLの名前を指定します。この名前は、ISE認可プロファイルと同じである必要があります。をクリックします。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

Cancel Save

#### FMC\_追加\_リダイレクト\_ACL\_パート\_1

ステップ 6.2 : DNSトラフィック、ISE PSN IPアドレスへのトラフィック、および修復サーバをブロックして、リダイレクトから除外します。残りのトラフィックを許可します。これにより、リダイレクトがトリガーされます。をクリックします。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 C +  
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\_
- rtp\_ise

Add to Source  
Add to Destination

Source Networks (0)  
any  
Enter an IP address Add

Destination Networks (1)  
ISE\_PSN\_  
Enter an IP address Add

Cancel Add

#### FMC\_追加\_リダイレクト\_ACL\_パート\_2

Name  
redirect

Entries (4)

Add

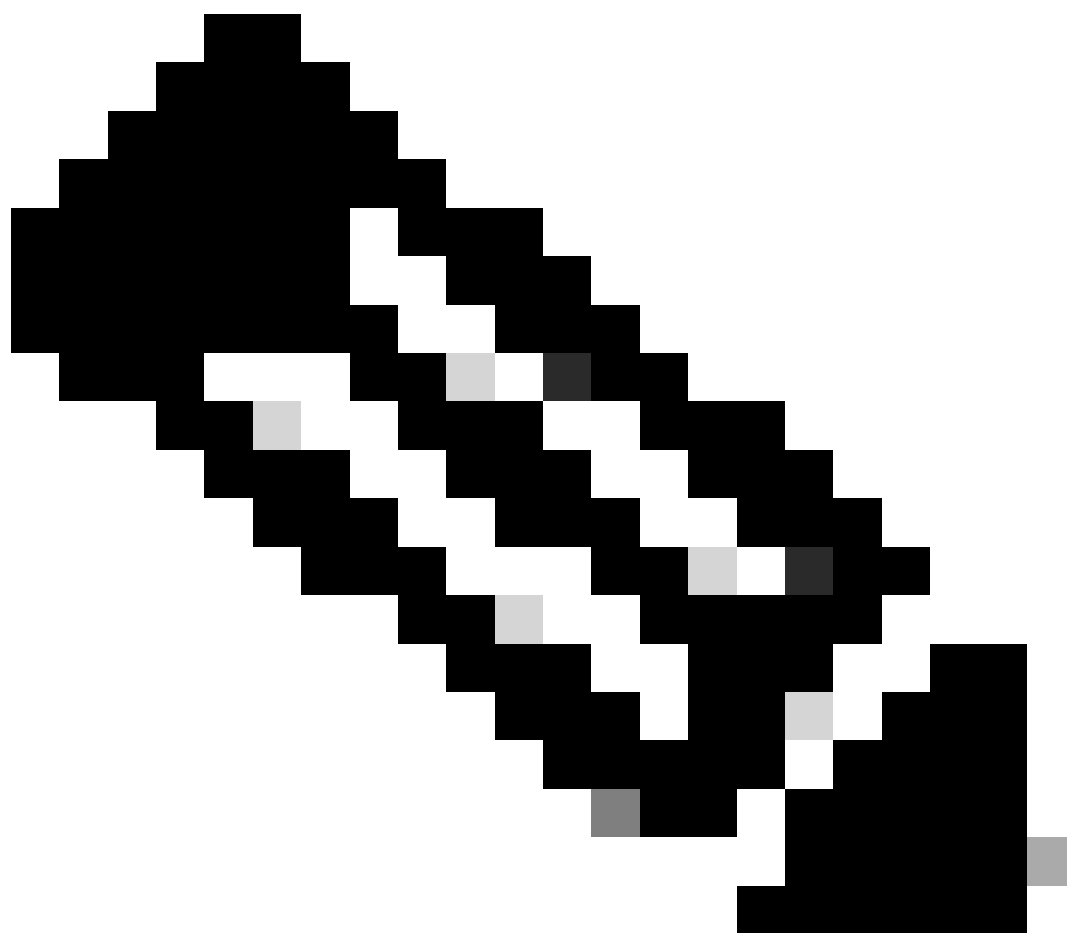
Sequence	Action	Source	Source Port	Destination	Destination Port	Application	Users	SGT	
1	Block	any-ipv4	Any	ISE_PSN_	Any	Any	Any	Any	
2	Block	Any	Any	Any	DNS_over_TCP DNS_over_UDP	Any	Any	Any	
3	Block	Any	Any	FTP_	Any	Any	Any	Any	
4	Allow	any-ipv4	Any	any-ipv4	Any	Any	Any	Any	

Allow Overrides

Cancel

Save

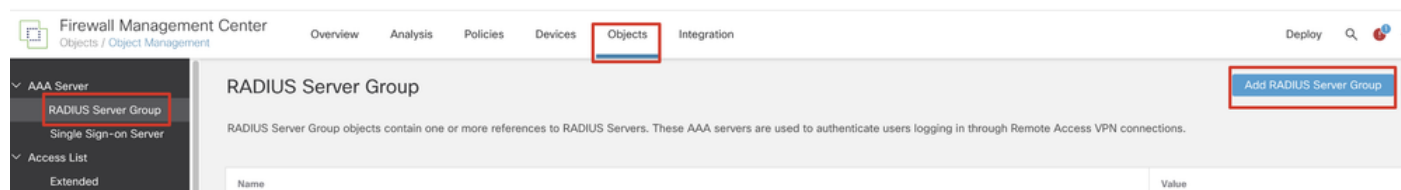
FMC\_追加\_リダイレクト\_ACL\_パート\_3



注：このリダイレクトACLの例では、宛先FTPが修復サーバの例として使用されています。



手順 7 : Objects > Object Management > RADIUS Server Groupに移動します。をクリックします。Add RADIUS Server Group



*FMC\_Add\_New\_Radius\_サーバグループ*

ステップ 7.1 : 名前、チェック、チェック、チェック Enable authorize only、チェック Enable interim account update、チェック Enable dynamic authorizationを指定します。

## 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

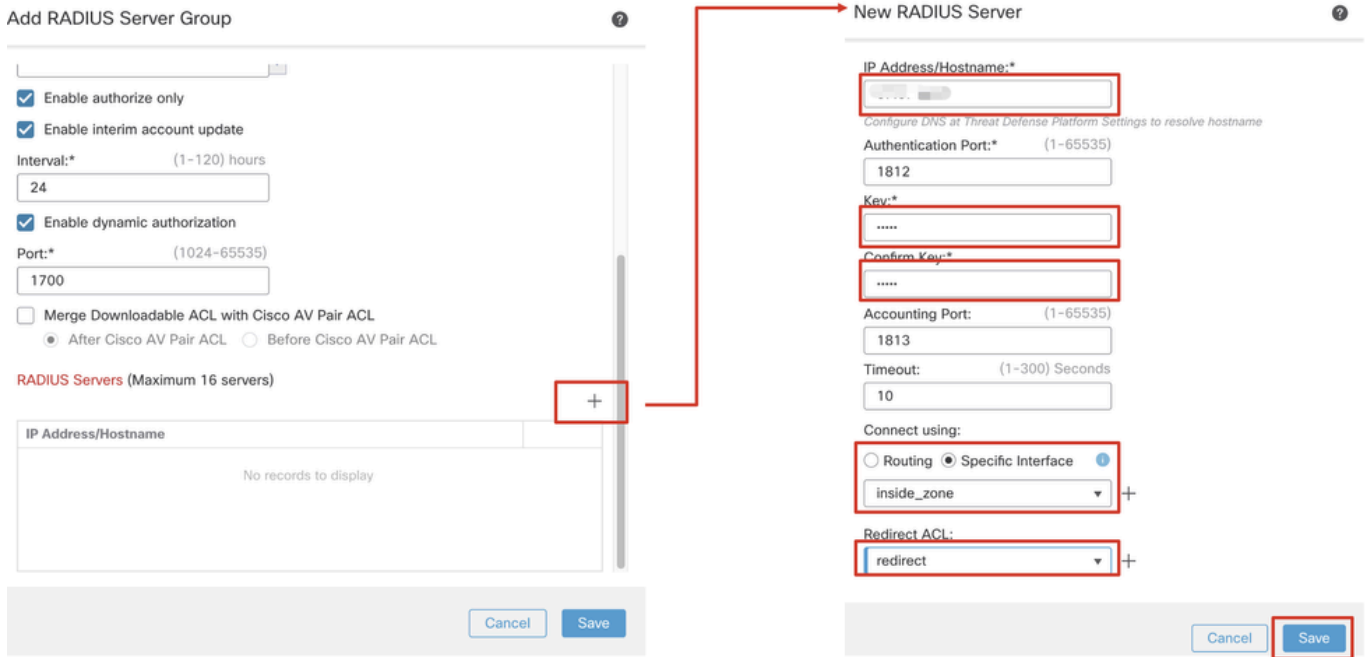
Port:\* (1024-65535)

Cancel

Save

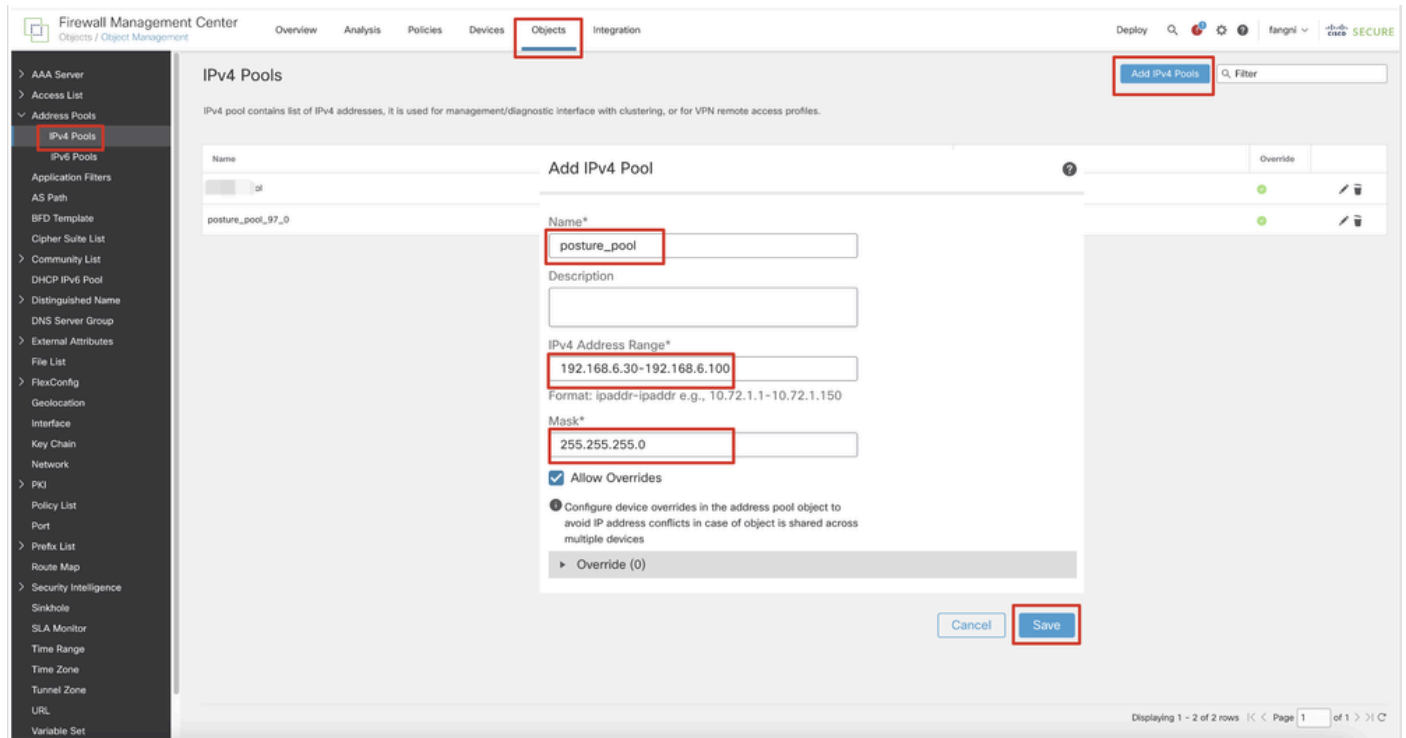
FMC\_追加\_新規\_Radius\_サーバ\_グループ\_パート\_1

ステップ 7.2 : 新しいradiusサーバを追加するPlus アイコンをクリックします。ISE PSNを入力しIP Address/Hostname, Keyます。接続するspecific interfaceを選択します。Redirect ACLを選択します。次に、をクリックSaveして新しいRADIUSサーバを保存します。次にSaveを再度クリックして、新しいRADIUSサーバグループを保存します。



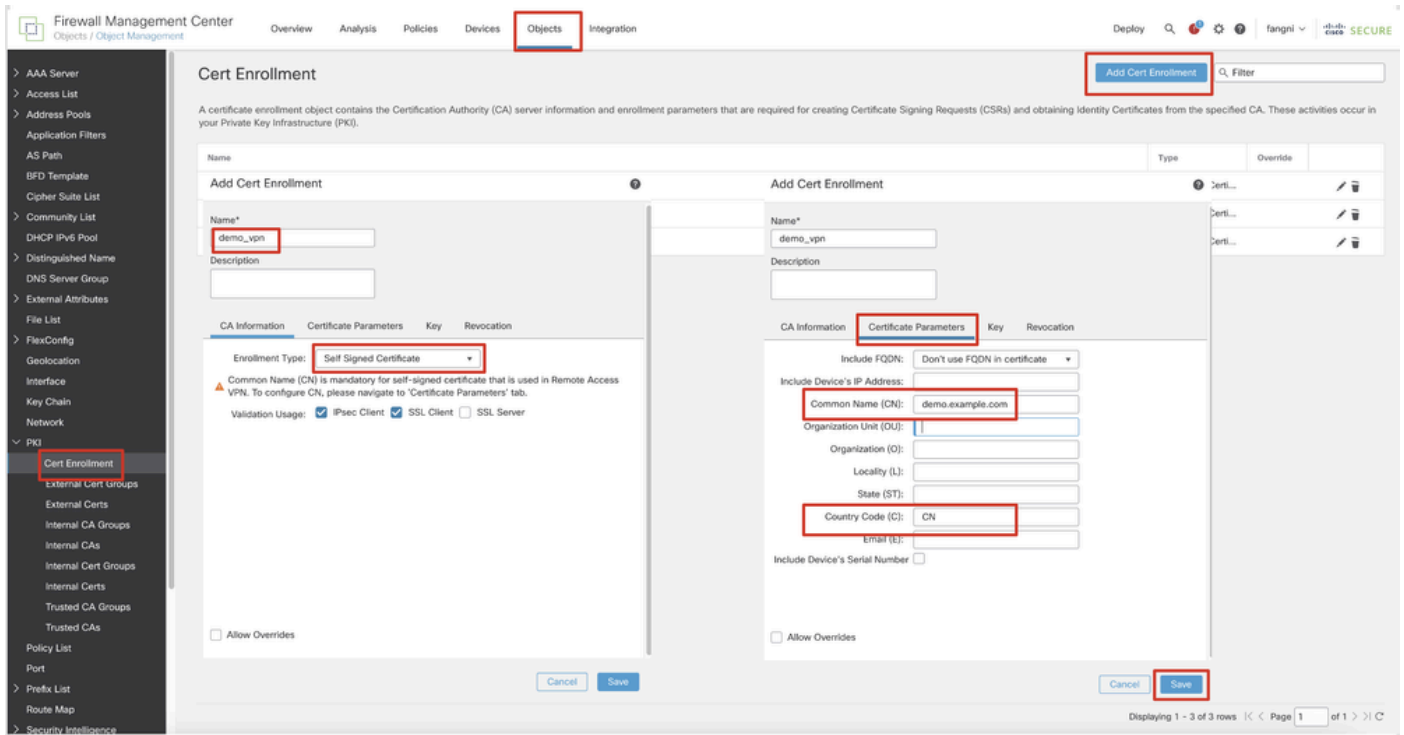
FMC\_追加\_新規\_Radius\_サーバ\_グループ\_パート\_2

ステップ 8 : Objects > Object Management > Address Pools > IPv4 Poolsに移動します。Add IPv4 Poolsをクリックし、Name, IPv4 Address RangeおよびMaskを入力します。次にSaveをクリックします。



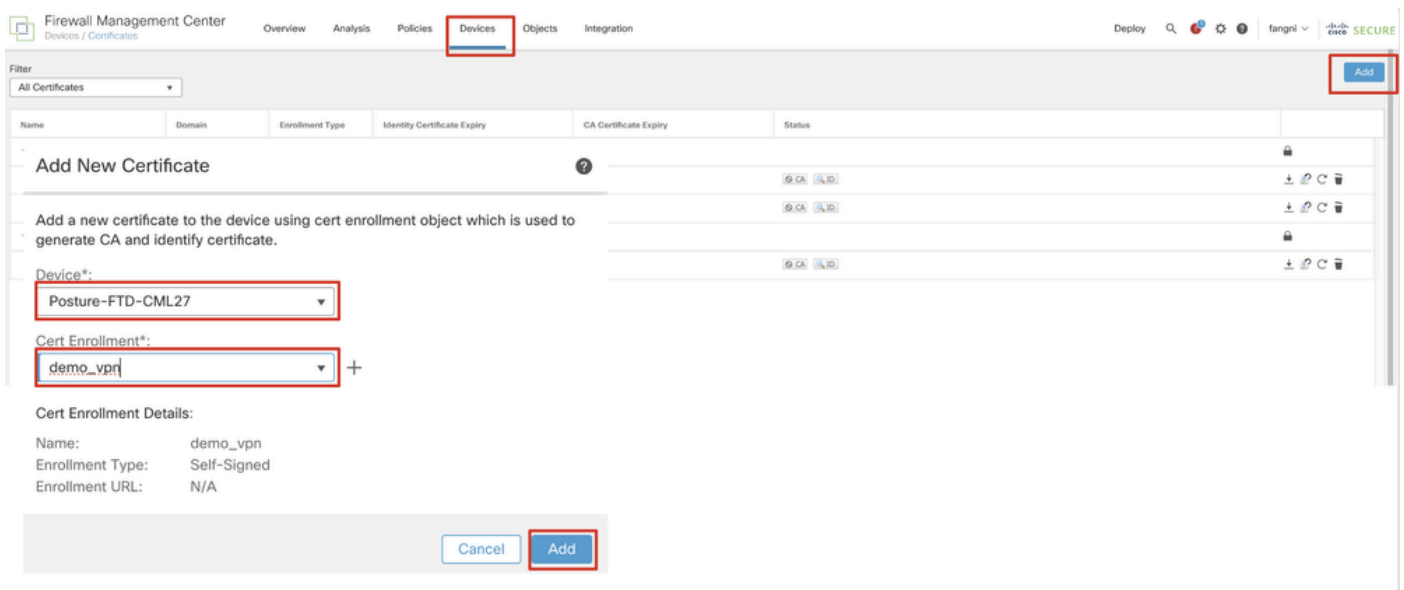
FMC\_Add\_New\_プール

ステップ 9 : Certificate Objects > Object Management > PKI > Cert Enrollmentに移動します。Add Cert Enrollmentをクリックし、名前を指定してSelf Signed Certificate in Enrollment Typeを選択します。Certificate Parametersタブをクリックし、Common NameおよびCountry Codeを入力します。次にSaveをクリックします。



### FMC\_Add\_New\_Cert\_Enroll (登録ユーザのみ)

ステップ 10 : Devices > Certificatesに移動します。Addをクリックし、DeviceでFTD名を選択し、Cert Enrollmentで以前に設定した登録を選択します。をクリックします。Add



### FMC\_Add\_New\_Cert\_To\_FTD (オプション)

ステップ 11 Devices > VPN > Remote Accessに移動します。をクリックします。Add

ステップ 11.1 : 名前を入力し、FTDをSelected Devicesに追加します。をクリックします。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

Search

Posture-FTD-CML27  
VPN-FTD-Posture-CML

Add

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.

Cancel Back **Next**

FMC\_New\_RAVPN\_Wizard\_1

ステップ 11.2 : Authentication Server, Authorization Server, Accounting Serverで事前に設定したRADIUSサーバグループを選択します。ページを下にスクロールします。

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

Remote User — Secure Client — Internet — Outside — VPN Device — Inside — Corporate Resources

AAA

**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)

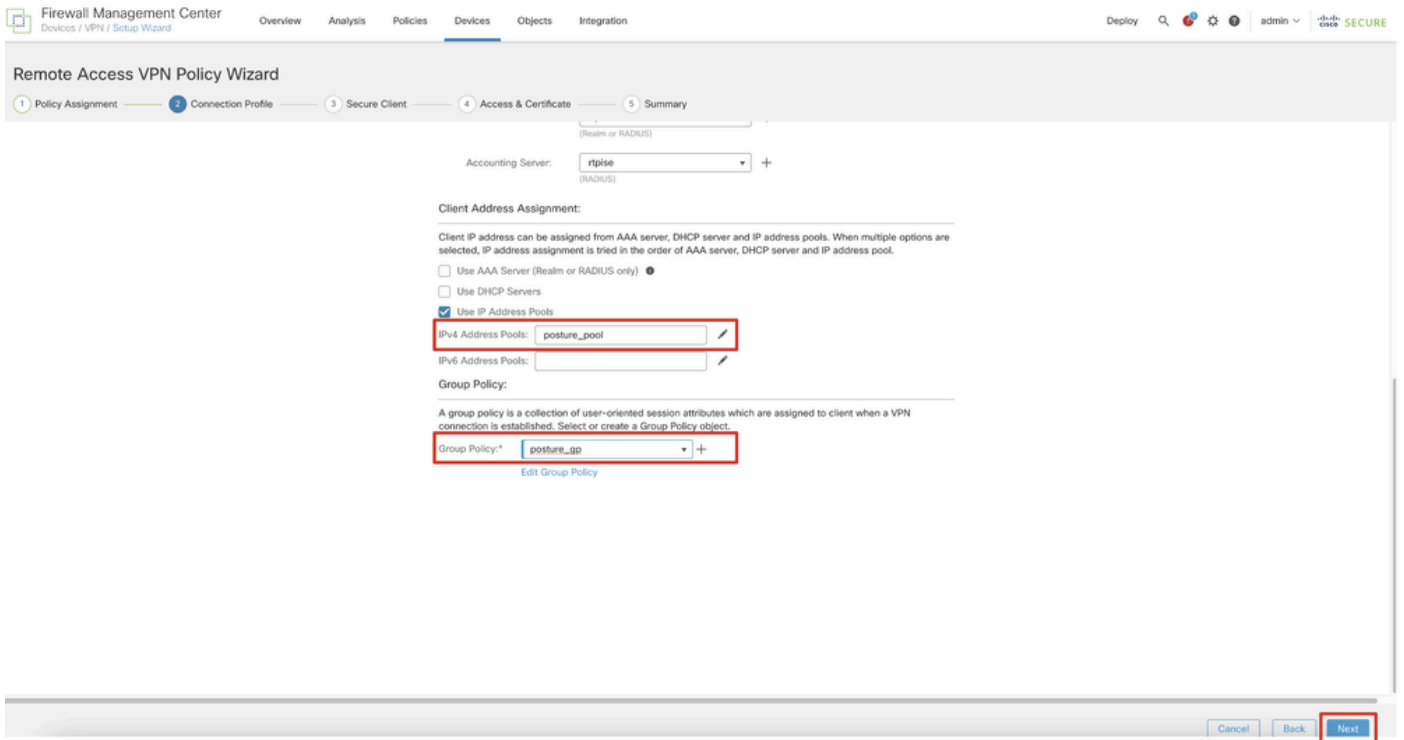
**Client Address Assignment:**

Client IP address can be assigned from AAA server, FQDN server and IP address pool. When multiple servers are...

Cancel Back **Next**

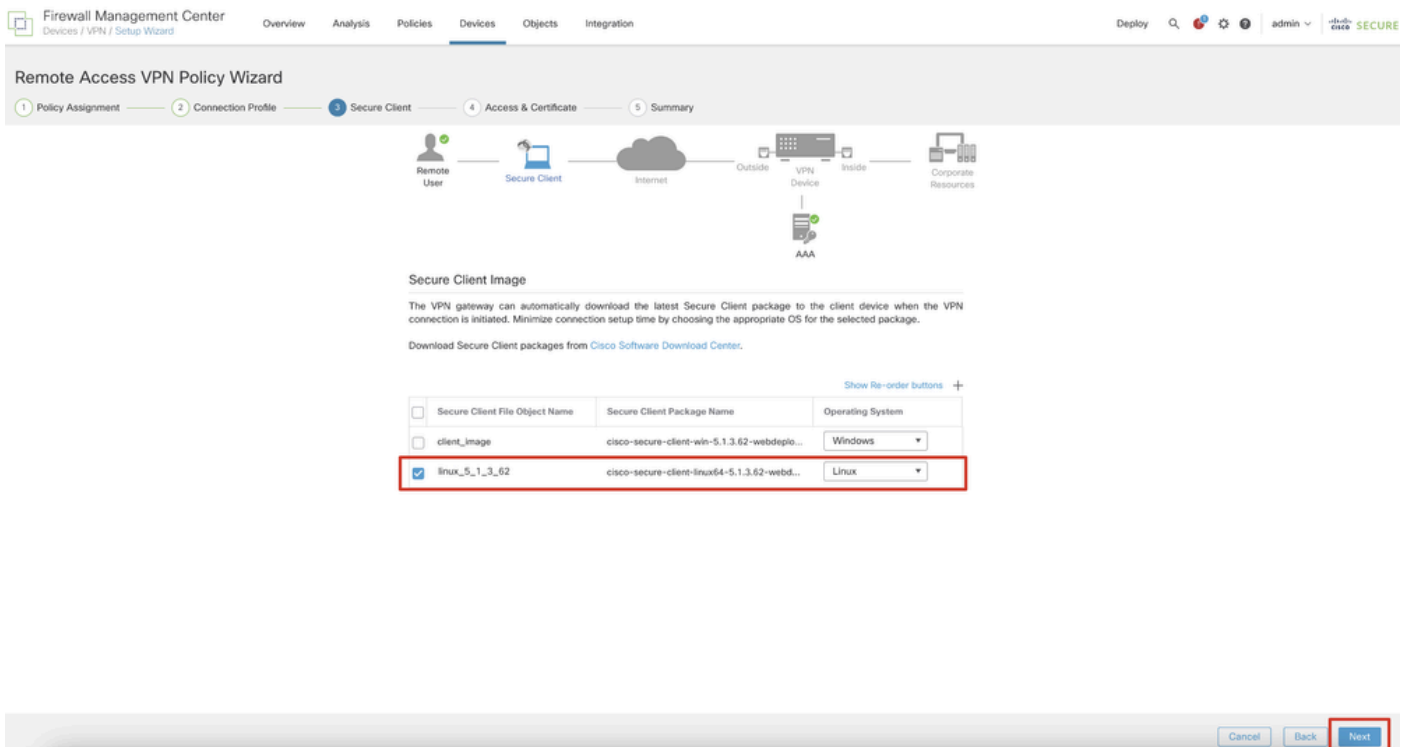
FMC\_New\_RAVPN\_Wizard\_2

ステップ 11.3 : IPv4 Address Poolsで以前に設定したプール名を選択し、Group Policyで以前に設定したグループポリシーを選択します。Nextをクリックします。



FMC\_New\_RAVPN\_Wizard\_3 ( 推奨 )

ステップ 11.4 : Linuxイメージのチェックボックスをオンにします。をクリックします。Next



FMC\_New\_RAVPN\_Wizard\_4 ( 推奨 )

ステップ 11.5 : VPNインターフェイスのインターフェイスを選択します。ステップ9でFTDに登録した証明書の登録を選択します。をクリックします。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

**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:

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:

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)

Cancel Back **Next**

#### FMC\_New\_RAVPN\_Wizard\_5

ステップ 11.6 : サマリーページで関連情報を再度確認します。問題がなければ、Finishをクリックします。変更する必要がある場合は、Backをクリックします。

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**

**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-CM127
Connection Profile:	posture_vpn
Connection Alias:	posture_vpn
AAA:	
Authentication Method:	AAA Only
Authentication Server:	rtpile (RADIUS)
Authorization Server:	rtpile
Accounting Server:	rtpile
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

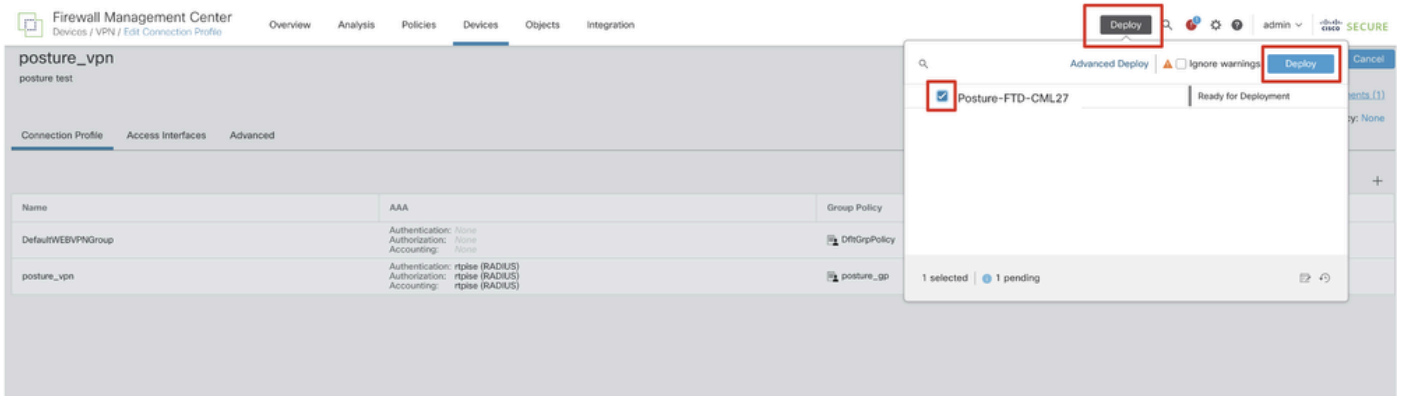
**Additional Configuration Requirements**  
After the wizard completes, the following configuration needs to be completed for VPN to work on all device targets.

- **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**

Cancel Back **Finish**

#### FMC\_New\_RAVPN\_Wizard\_6 ( 推奨 )

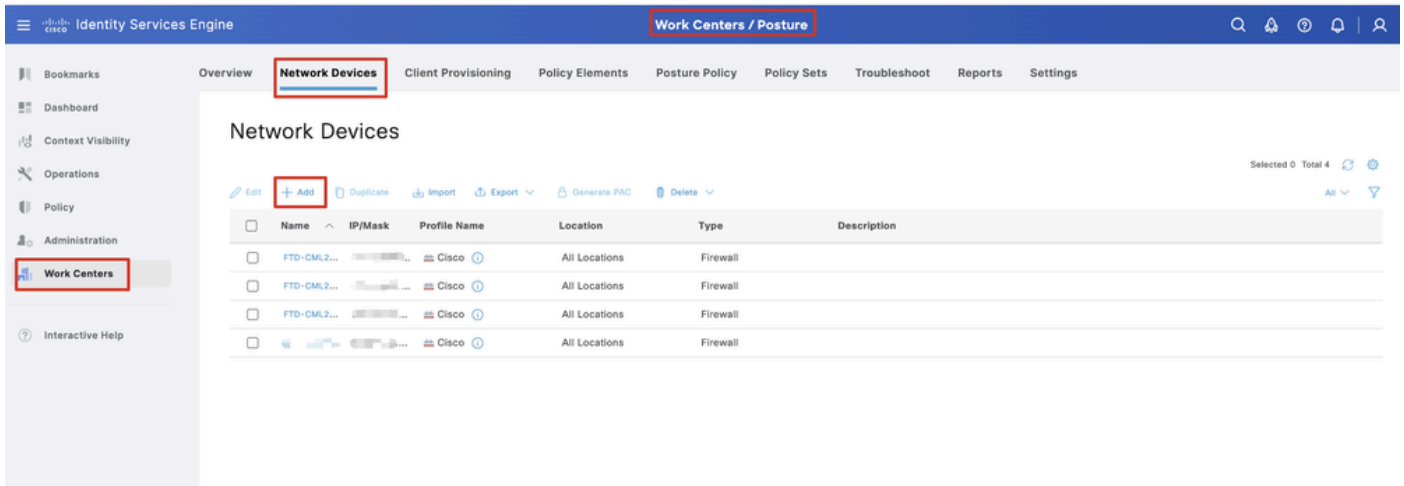
ステップ 12新しい設定をFTDに展開して、リモートアクセスVPNの設定を完了します。



FMC\_Deploy\_FTD

## ISEでの設定

ステップ 13 Work Centers > Posture > Network Devicesに移動します。をクリックします。Add



ISE\_Add\_New\_デバイス

ステップ 13.1 : Name, IP Addressコマンドを入力し、ページを下にスクロールします。



Identity Services Engine Work Centers / Posture

Overview **Network Devices** Client Provisioning Policy Elements Posture Policy Policy Sets Troubleshoot Reports Settings

Network Devices List > New Network Device

### Network Devices

Name **posture-FTD**

Description

IP Address \* IP : [redacted] / 32

Device Profile Cisco

Model Name

Software Version

Network Device Group

Location All Locations [Set To Default](#)

IPSEC Is IPSEC Device [Set To Default](#)

ISE\_Add\_New\_Devices\_1

ステップ 13.2 : RADIUS Authentication Settingsのチェックボックスをオンにします。Shared Secretを入力します。をクリックします。Submit

Identity Services Engine Work Centers / Posture

Overview **Network Devices** Client Provisioning Policy Elements Posture Policy Policy Sets Troubleshoot Reports Settings

RADIUS Authentication Settings

RADIUS UDP Settings

Protocol RADIUS

Shared Secret [redacted] [Show](#)

Use Second Shared Secret

Second Shared Secret [Show](#)

CoA Port 1700 [Set To Default](#)

RADIUS DTLS Settings

DTLS Required

Shared Secret radius/dtls [Show](#)

CoA Port 2083 [Set To Default](#)

Issuer CA of ISE Certificates for CoA Select if required (optional) [Show](#)

DNS Name

General Settings

Enable KeyWrap

Key Encryption Key [Show](#)

Message Authenticator Code Key [Show](#)

Key Input Format  ASCII  HEXADECIMAL

TACACS Authentication Settings

SNMP Settings

Advanced TrustSec Settings

[Submit](#) [Cancel](#)

ISE\_Add\_New\_Devices\_2

ステップ 14 : [Cisco Software Download](#)からパッケージ名cisco-secure-client-linux64-4.3.3139.0-isecompliance-webdeploy-k9.pkgをダウ

ダウンロードし、ダウンロードしたファイルのmd5チェックサムが [Cisco Software Download page](#)と同じであることを確認して、ファイルの状態が良好であることを確認します。パッケージ名cisco-secure-client-linux64-5.1.3.62-webdeploy-k9.pkgは手順1で正常にダウンロードされました。

ステップ 15 : Work Centers > Posture > Client Provisioning > Resourcesに移動します。をクリックします。AddAgent resources from local diskを選択します。

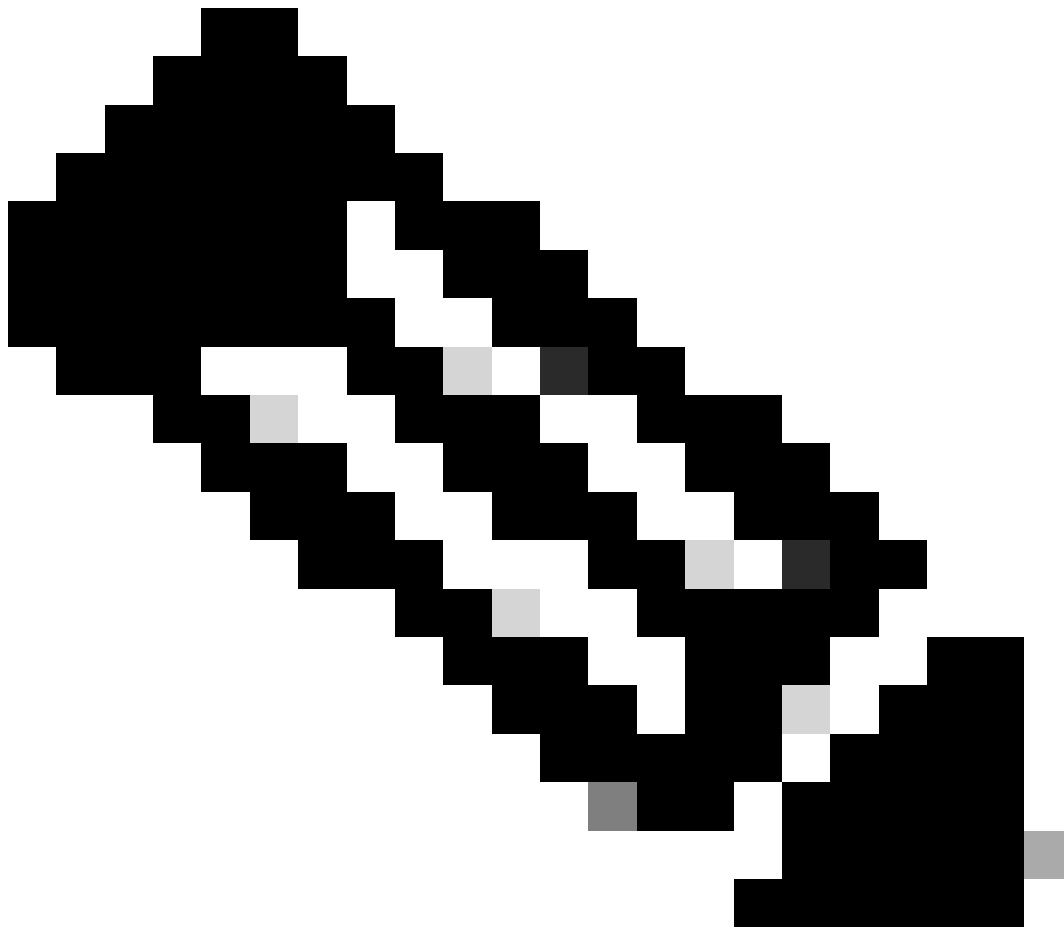
The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes 'Identity Services Engine' and 'Work Centers / Posture'. The main navigation menu has 'Client Provisioning' selected. The left sidebar shows 'Client Provisioning Policy' and 'Resources' (highlighted with a red box). The main content area is titled 'Resources' and shows a table of agent resources. A dropdown menu is open under the '+ Add' button, with 'Agent resources from local disk' selected (highlighted with a red box). The table below lists various resources with columns for Type, Version, Last Update, and Description.

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

### ISE\_Upload\_Resource

ステップ 15.1 : Cisco Provided Packageを選択します。Choose Fileをクリックして、cisco-secure-client-linux64-5.1.3.62-webdeploy-k9.pkgをアップロードします。をクリックします。Submit

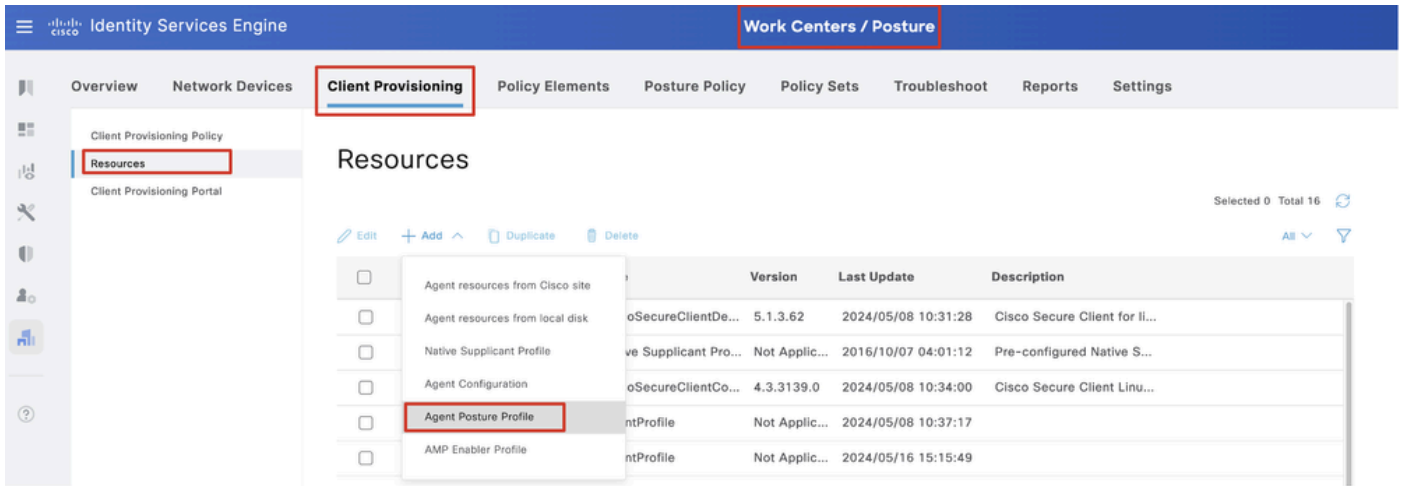
The screenshot shows the Cisco Identity Services Engine (ISE) interface for configuring 'Agent Resources From Local Disk'. The top navigation bar includes 'Identity Services Engine' and 'Work Centers / Posture'. The left sidebar shows 'Work Centers' selected. The main content area is titled 'Agent Resources From Local Disk' and shows a form with a 'Category' dropdown set to 'Cisco Provided Package' (highlighted with a red box) and a 'Choose File' button next to the filename 'cisco-secure-...eploy-k9.pkg' (highlighted with a red box). Below the form is a table of 'Agent Uploaded Resources' with columns for Name, Type, Version, and Description. The table shows one resource: 'CiscoSecureClientDesktoLinux...'. At the bottom, there is a 'Submit' button (highlighted with a red box) and a 'Cancel' button.



注：ステップ14を繰り返して、cisco-secure-client-linux64-4.3.3139.0-isecompliance-webdeploy-k9.pkgをアップロードします。

---

ステップ 16： Work Centers > Posture > Client Provisioning > Resourcesに移動します。をクリックします。AddAgent Posture Profileを選択します。

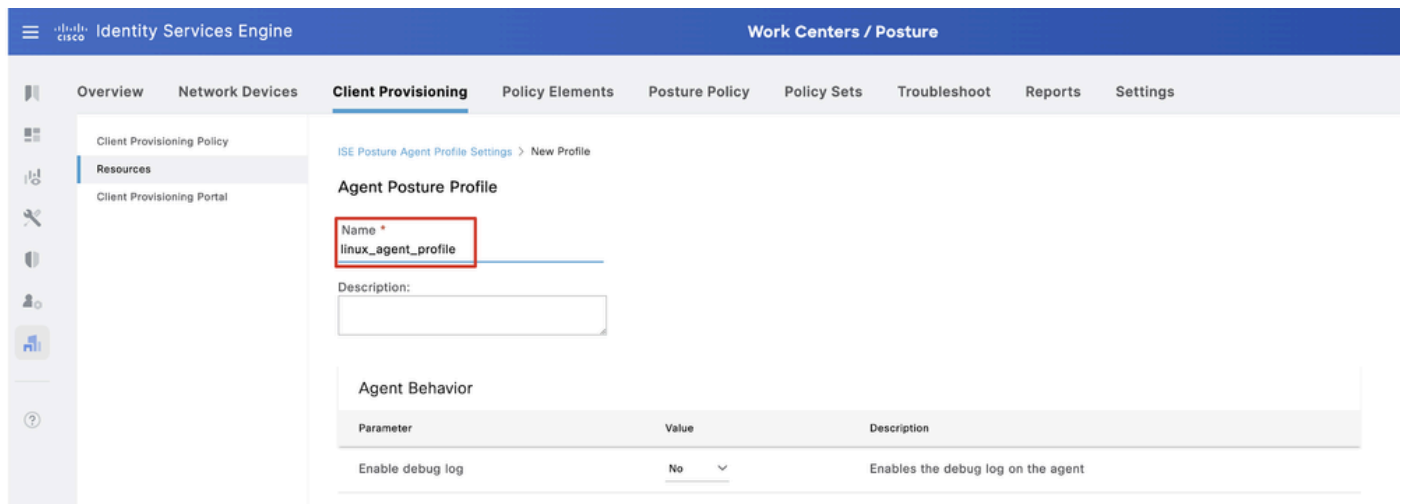


ISE\_Add\_Agent\_Posture\_プロファイル

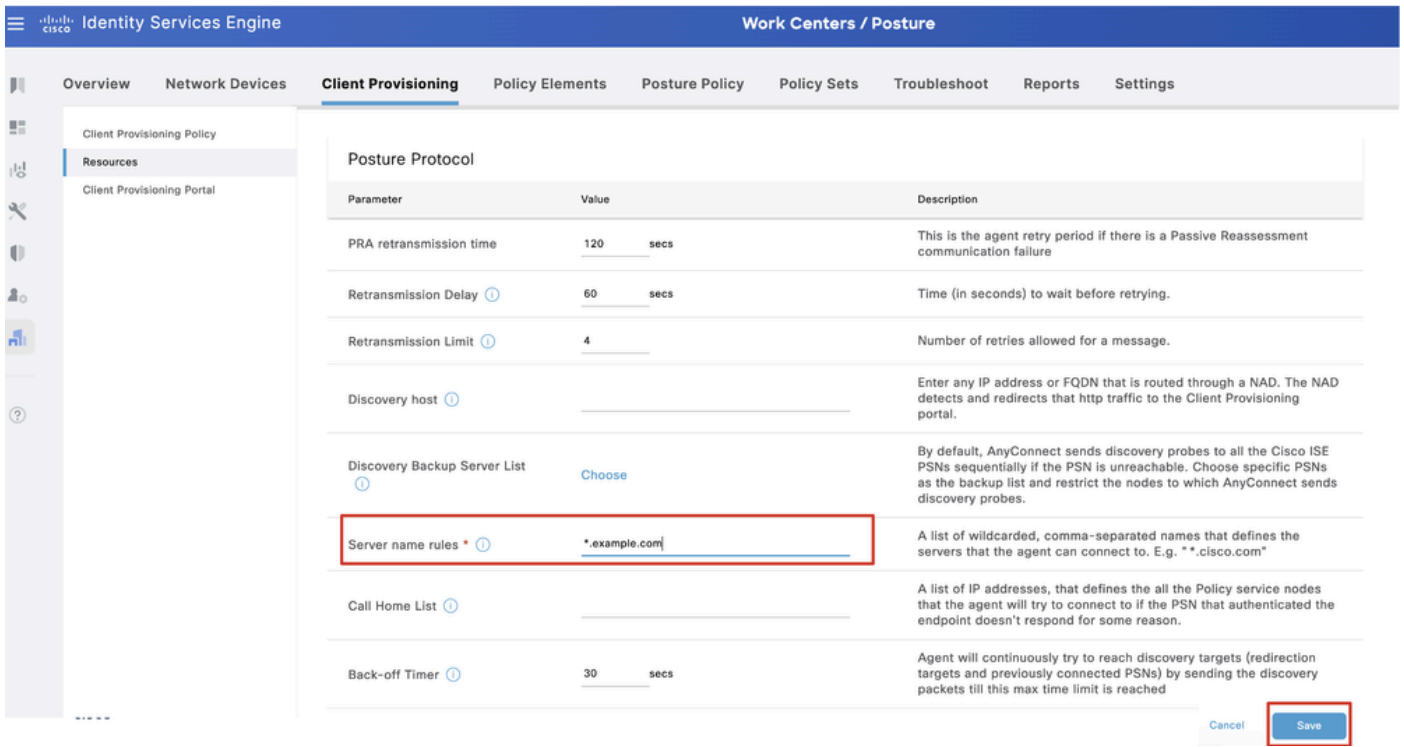
ステップ 16.1 : Name, Server name rulesを指定し、その他はデフォルトのままにします。をクリックします。Save

名前 : linux\_agent\_profile

サーバー名の規則 : \*.example.com

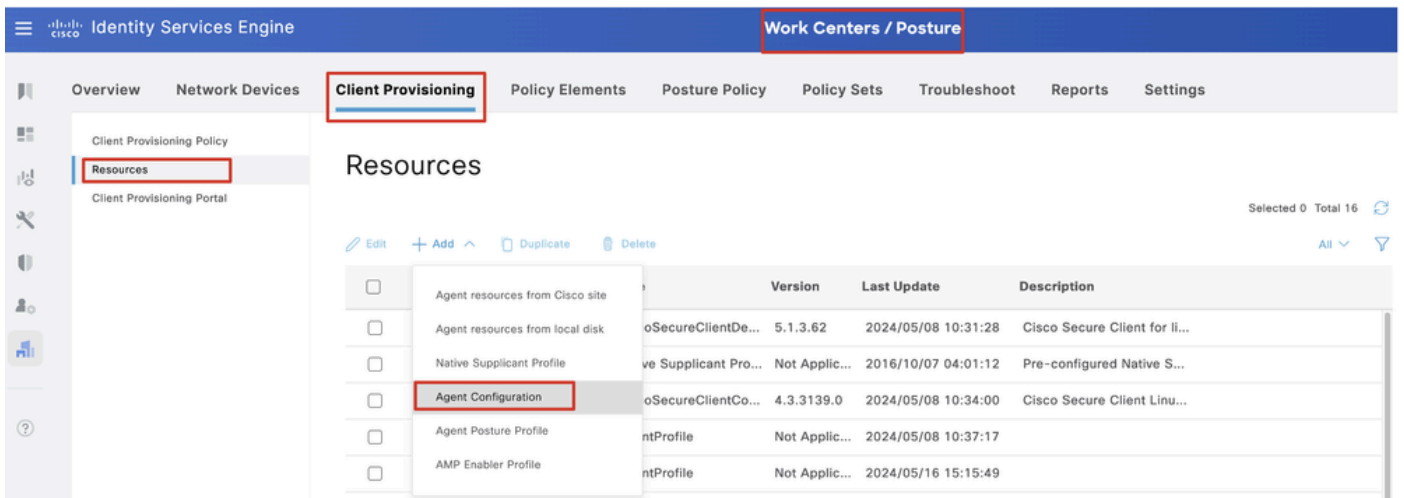


ISE\_追加\_エージェント\_ポスチャ\_プロファイル\_1



ISE\_追加\_エージェント\_ポスチャ\_プロフィール\_2

ステップ 17 : Work Centers > Posture > Client Provisioning > Resourcesに移動します。をクリックします。AddAgent Configurationを選択します。



ISE\_Add\_Agent\_設定

ステップ 17.2 : 詳細を設定します。

エージェントパッケージの選択 : CiscoSecureClientDesktopLinux 5.1.3.062

名前 : linux\_agent\_config

コンプライアンスモジュール : CiscoSecureClientComplianceModuleLinux 4.3.3139.0

チェックボックスをオンにする VPN, Diagnostic and Reporting Tool

プロフィール選択ISEポスチャ : linux\_agent\_profile

をクリックします。Submit

Identity Services Engine Work Centers / Posture

Overview Network Devices **Client Provisioning** Policy Elements Posture Policy Policy Sets Troubleshoot Reports Settings

Client Provisioning Policy

Resources

Client Provisioning Portal

\* 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

Submit Cancel

ISE\_Add\_Agent\_Configuration\_1

ステップ 18 : Work Centers > Posture > Client Provisioning > Client Provisioning Policyに移動します。ルール名の最後にあるEdit をクリックします。Insert new policy belowを選択します。

Identity Services Engine Work Centers / Posture

Overview Network Devices **Client Provisioning** Policy Elements Posture Policy Policy Sets Troubleshoot Reports Settings

Client Provisioning Policy

Resources

Client Provisioning Portal

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

Duplicate above

Duplicate below

Insert new policy above

Insert new policy below

Delete

ISE\_Add\_New\_Provisioning\_

ポリシー

ステップ 18.1 : 詳細を設定します。

ルール名 : Linux

オペレーティングシステム : すべてLinux

結果 : linux\_agent\_config

Done およびSaveをクリックします。

The screenshot shows the 'Client Provisioning Policy' configuration page in Cisco ISE. The 'Linux' rule is highlighted with a red box. The table below shows the rules configuration:

Rule Name	Identity Groups	Operating Systems	Other Conditions	Results
IOS	if Any	and Apple IOS All	and Condition(s)	then Cisco-ISE-NSP
Android	if Any	and Android	and Condition(s)	then Cisco-ISE-NSP
Linux	if Any	and Linux All	and Condition(s)	then linux_agent_config

ISE\_Add\_New\_Provisioning\_Policy\_1

ステップ 19 : Work Centers > Posture > Policy Elements > Conditions > Fileに移動します。をクリックします。Add

The screenshot shows the 'File Conditions' page in Cisco ISE. The 'Add' button is highlighted with a red box. The table below shows the file conditions:

Name	Description	File name	Condition Type
pc_XP64_KB2797052_MS13...	Cisco Predefined Check...	SYSTEM_PROGRAMSIC...	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\winsxsla...	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\Win32x.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\Win32x.sys	Cisco-Defined

ISE\_Add\_New\_File\_条件

ステップ 19.1 : 詳細を設定します。

名前 : linux\_demo\_file\_exist

オペレーティングシステム : すべてLinux

ファイルの種類 : FileExistence

ファイルパス : home、Desktop/test.txt

ファイル演算子 : 存在します

をクリックします。Submit

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes 'Identity Services Engine' and 'Work Centers / Posture'. The main navigation menu has 'Policy Elements' selected. The left sidebar lists various conditions, with 'File' selected. The main content area is titled 'File Condition' and contains the following fields:

- Name \*: linux\_demo\_file\_exist
- Description: (empty)
- \* Operating System: Linux All
- Compliance Module: Any version
- \* File Type: FileExistence
- \* File Path: home (with a dropdown menu open showing 'Desktop/test.txt')
- \* File Operator: Exists

The 'Submit' button is highlighted with a red box.

ISE\_Add\_New\_File\_Condition\_1

ステップ 20 : Work Centers > Posture > Policy Elements > Requirementsに移動します。ルール名の最後にあるEdit をクリックします。Insert new Requirementを選択します。



Identity Services Engine Work Centers / Posture

Overview Network Devices Client Provisioning **Policy Elements** Posture Policy Policy Sets Troubleshoot Reports Settings

Bookmarks Dashboard Context Visibility Operations Policy Administration **Work Centers** Interactive Help

Conditions

- Anti-Malware
- Anti-Spyware
- Anti-Virus
- Application
- Compound
- Dictionary Compound
- Dictionary Simple
- Disk Encryption
- External DataSource
- File
- Firewall
- Hardware Attributes
- Patch Management
- Registry
- Script
- Service
- USB

Remediations

- Allowed Protocols
- Authorization Profiles
- Downloadable ACLs
- Requirements**

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 Duplicate
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 Insert new Requirement
Any_AS_Definition_Win	for Windows All	using 3.x or earlier	using Agent	met if ANY_as_win_def then	AnyASDefRemediationWin	Edit Delete
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

ステップ 20.1 : 詳細を設定します。

名前 : Test\_exist\_linux

オペレーティングシステム : すべてLinux

コンプライアンスモジュール : 4.x以降

ポスチャタイプ : Agent

条件 : linux\_demo\_file\_exist

Done およびSaveをクリックします。

Identity Services Engine Work Centers / Posture

Overview Network Devices Client Provisioning **Policy Elements** Posture Policy Policy Sets Troubleshoot Reports Settings

Conditions

- Anti-Malware
- Anti-Spyware
- Anti-Virus
- Application
- Compound
- Dictionary Compound
- Dictionary Simple
- Disk Encryption
- External DataSource
- File
- Firewall
- Hardware Attributes
- Patch Management
- Registry
- Script
- Service
- USB

Remediations

- Required Protocols
- Allowed Protocols
- Authorization Profiles
- Downloadable ACLs

Guide Me

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
Any_AV_Installation_Win	for Windows All	using 3.x or earlier	using Agent	met if ANY_av_win_inst	then Message Text Only
Any_AV_Definition_Win	for Windows All	using 3.x or earlier	using Agent	met if ANY_av_win_def	then AnyAVDefRemediationWin
Any_AS_Installation_Win	for Windows All	using 3.x or earlier	using Agent	met if ANY_as_win_inst	then Message Text Only
Any_AS_Definition_Win	for Windows All	using 3.x or earlier	using Agent	met if ANY_as_win_def	then AnyASDefRemediationWin
Any_AV_Installation_Mac	for Mac OSX	using 3.x or earlier	using Agent	met if ANY_av_mac_inst	then Message Text Only
Any_AV_Definition_Mac	for Mac OSX	using 3.x or earlier	using Agent	met if ANY_av_mac_def	then AnyAVDefRemediationMac
Any_AS_Installation_Mac	for Mac OSX	using 3.x or earlier	using Agent	met if ANY_as_mac_inst	then Message Text Only
Any_AS_Definition_Mac	for Mac OSX	using 3.x or earlier	using Agent	met if ANY_as_mac_def	then AnyASDefRemediationMac
Any_AM_Installation_Win	for Windows All	using 4.x or later	using Agent	met if ANY_am_win_inst	then Message Text Only
Any_AM_Definition_Win	for Windows All	using 4.x or later	using Agent	met if ANY_am_win_def	then AnyAMDefRemediationWin
Any_AM_Installation_Mac	for Mac OSX	using 4.x or later	using Agent	met if ANY_am_mac_inst	then Message Text Only
Any_AM_Definition_Mac	for Mac OSX	using 4.x or later	using Agent	met if ANY_am_mac_def	then AnyAMDefRemediationMac

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.

Save Reset

ISE\_Add\_New\_Posture\_Requirement\_1

---

注：現時点では、修復機能としてLinuxエージェント用のシェルスクリプトのみがサポートされています。

---

ステップ 21： Work Centers > Posture > Policy Elements > Authorization Profilesに移動します。をクリックします。Add

ステップ 21.1： 詳細を設定します。

名前： unknown\_redirect

チェックボックスをオンにする Web Redirection(CWA,MDM,NSP,CPP)

選択 Client Provisioning(Posture)

ACL：リダイレクト

値 : クライアントプロビジョニングポータル ( デフォルト )

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes 'Work Centers / Posture'. The main navigation tabs are 'Overview', 'Network Devices', 'Client Provisioning', 'Policy Elements', 'Posture Policy', 'Policy Sets', 'Troubleshoot', 'Reports', and 'Settings'. The left sidebar lists various configuration categories, with 'Authorization Profiles' highlighted. The main content area is titled 'Authorization Profile' and shows the configuration for a profile named 'unknown\_redirect'. The 'Name' field is 'unknown\_redirect'. The 'Access Type' is 'ACCESS\_ACCEPT'. The 'Network Device Profile' is 'Cisco'. Under 'Common Tasks', the 'Web Redirection (CWA, MDM, NSP, CPP)' checkbox is checked. The 'ACL' dropdown is set to 'redirect' and the 'Value' dropdown is set to 'Client Provisioning Portal (def. ...)'. Other options like 'Voice Domain Permission', 'Static IP/Host name/FQDN', and 'Suppress Profiler CoA for endpoints in Logical Profile' are unchecked.

ISE\_Add\_New\_Authorization\_プロフィール\_リダイレクト\_1

---

注：このACL名リダイレクトは、FTDで設定された対応するACL名と一致する必要があります。

---

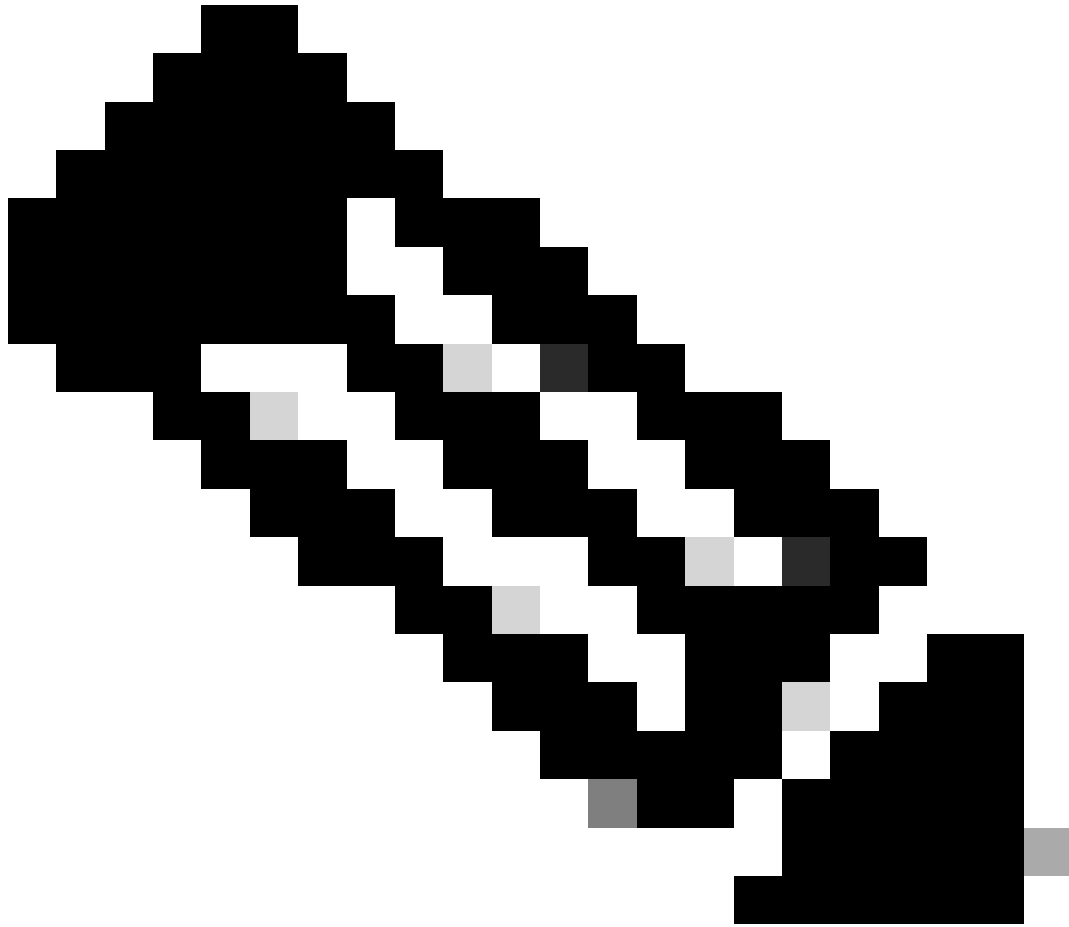
ステップ 21.2 : Add を繰り返し、詳細を含む、準拠していないエンドポイントと準拠しているエンドポイント用に別の2つの認可プロファイルを作成します。

名前 : non\_compliant\_profile

DAACL名 : DENY\_ALL\_IPv4\_TRAFFIC

名前 : compliant\_profile

DAACL名 : PERMIT\_ALL\_IPv4\_TRAFFIC



注：準拠または非準拠エンドポイントのDACLは、実際の要件に従って設定する必要があります。

---

ステップ 22： Work Centers > Posture > Posture Policyに移動します。ルールの最後にあるEdit をクリックします。Insert new policyを選択します。

Identity Services Engine Work Centers / Posture

Overview Network Devices Client Provisioning Policy Elements **Posture Policy** Policy Sets Troubleshoot Reports Settings

**Posture Policy** [Guide Me](#)

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	
<input type="checkbox"/>	Policy Options	Default_AntiMalware_Policy_Mac	Any	Mac OS X	4.x or later	Agent		Any_AM_Installation_Mac	<a href="#">Edit</a>
<input type="checkbox"/>	Policy Options	Default_AntiMalware_Policy_Mac_temporal	Any	Mac OS X	4.x or later	Temporal Agent		Any_AM_Installation_Mac_temporal	<a href="#">Edit</a>
<input type="checkbox"/>	Policy Options	Default_AntiMalware_Policy_Win	Any	Windows All	4.x or later	Agent		Any_AM_Installation_Win	<a href="#">Edit</a>
<input type="checkbox"/>	Policy Options	Default_AntiMalware_Policy_Win_temporal	Any	Windows All	4.x or later	Temporal Agent		Any_AM_Installation_Win_temporal	<a href="#">Edit</a>
<input type="checkbox"/>	Policy Options	Default_AppViz_Policy_Mac	Any	Mac OS X	4.x or later	Agent		Default_AppViz_Requirement_Mac	<a href="#">Edit</a>
<input type="checkbox"/>	Policy Options	Default_AppViz_Policy_Mac_temporal	Any	Mac OS X	4.x or later	Temporal Agent		Default_AppViz_Requirement_Mac_temporal	<a href="#">Edit</a>
<input type="checkbox"/>	Policy Options	Default_AppViz_Policy_Win	Any	Windows All	4.x or later	Agent		Default_AppViz_Requirement_Win	<a href="#">Edit</a>
<input type="checkbox"/>	Policy Options	Default_AppViz_Policy_Win_temporal	Any	Windows All	4.x or later	Temporal Agent		Default_AppViz_Requirement_Win_temporal	<a href="#">Edit</a>
<input type="checkbox"/>	Policy Options	Default_Firewall_Policy_Mac	Any	Mac OS X	4.x or later	Agent		Default_Firewall_Requirement_Mac	<a href="#">Edit</a>
<input type="checkbox"/>	Policy Options	Default_Firewall_Policy_Mac_temporal	Any	Mac OS X	4.x or later	Temporal Agent		Default_Firewall_Requirement_Mac_temporal	<a href="#">Edit</a>
<input type="checkbox"/>	Policy Options	Default_Firewall_Policy_Win	Any	Windows All	4.x or later	Agent		Default_Firewall_Requirement_Win	<a href="#">Edit</a>
<input type="checkbox"/>	Policy Options	Default_Firewall_Policy_Win_temporal	Any	Windows All	4.x or later	Temporal Agent		Default_Firewall_Requirement_Win_temporal	<a href="#">Edit</a>
<input type="checkbox"/>	Policy Options	Default_Hardware_Attributes_Policy_Mac	Any	Mac OS X	4.x or later	Agent		Default_Hardware_Attributes_Requirement_Mac	<a href="#">Edit</a>
<input type="checkbox"/>	Policy Options	Default_Hardware_Attributes_Policy_Mac_temporal	Any	Mac OS X	4.x or later	Temporal Agent		Default_Hardware_Attributes_Requirement_Mac_temporal	<a href="#">Edit</a>
<input type="checkbox"/>	Policy Options	Default_Hardware_Attributes_Policy_Win	Any	Windows All	4.x or later	Agent		Default_Hardware_Attributes_Requirement_Win	<a href="#">Edit</a>

## ISE\_Add\_New\_Posture\_ポリシー

ステップ 22.1 : 詳細を設定します。

ルール名 : Demo\_test\_exist\_linux

IDグループ : 任意

オペレーティングシステム : すべてLinux

コンプライアンスモジュール : 4.x以降

ポストチャタイプ : Agent

要件 : Test\_exist\_linux

Done およびSaveをクリックします。

Identity Services Engine Work Centers / Posture

## Posture Policy [Guide Me](#)

Define the Posture Policy by configuring rules based on operating system and/or other conditions.

Policy Options	Default_Firewall_Policy_Mac	If Any	and Mac OSX	and 4.x or later	and Agent	and	then Default_Firewall_Requirement_Mac	Edit
<input type="checkbox"/>	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
<input type="checkbox"/>	Default_Firewall_Policy_Win	If Any	and Windows All	and 4.x or later	and Agent	and	then Default_Firewall_Requirement_Win	Edit
<input type="checkbox"/>	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
<input type="checkbox"/>	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
<input type="checkbox"/>	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
<input type="checkbox"/>	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
<input type="checkbox"/>	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
<input type="checkbox"/>	Default_USB_Block_Policy_Win	If Any	and Windows All	and 4.x or later	and Agent	and	then USB_Block	Edit
<input type="checkbox"/>	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
<input checked="" type="checkbox"/>	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

ステップ 23 : Work Centers > Posture > Policy Setsに移動します。クリックしてInsert new row aboveします。

Identity Services Engine Work Centers / Posture

Work Centers / Posture

Policy Sets

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
<span style="color: green;">●</span>	Default	Default policy set		Default Network Access			

[Insert new row above](#)

### ISE\_Add\_New\_ポリシー\_セット

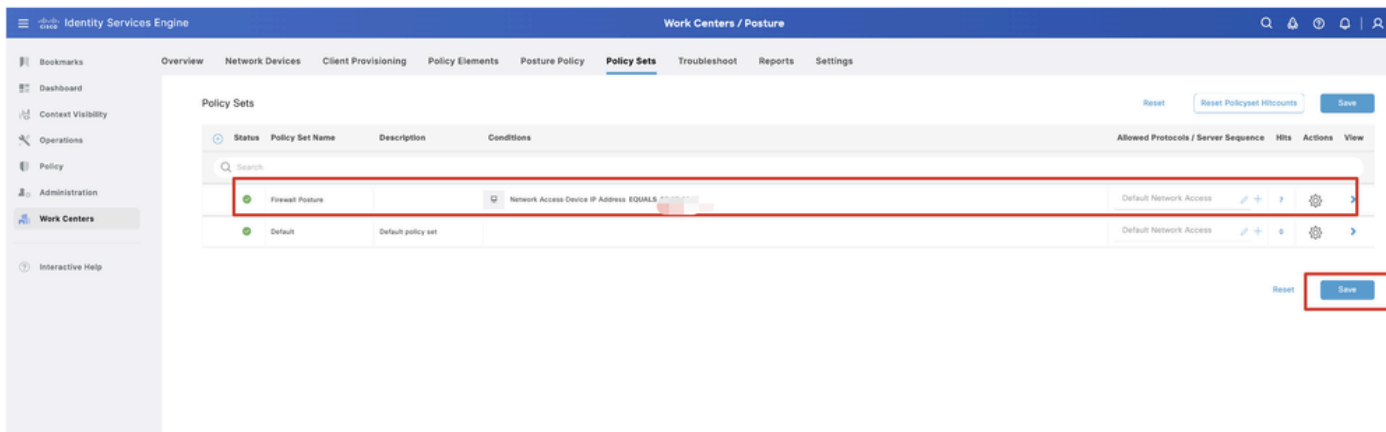
ステップ 23.1 : 詳細を設定します。

ポリシーセット名 : ファイアウォールポスチャ

条件 : ネットワークアクセスデバイスのIPアドレスが等しい[FTD IPアドレス]

をクリックします。 Save





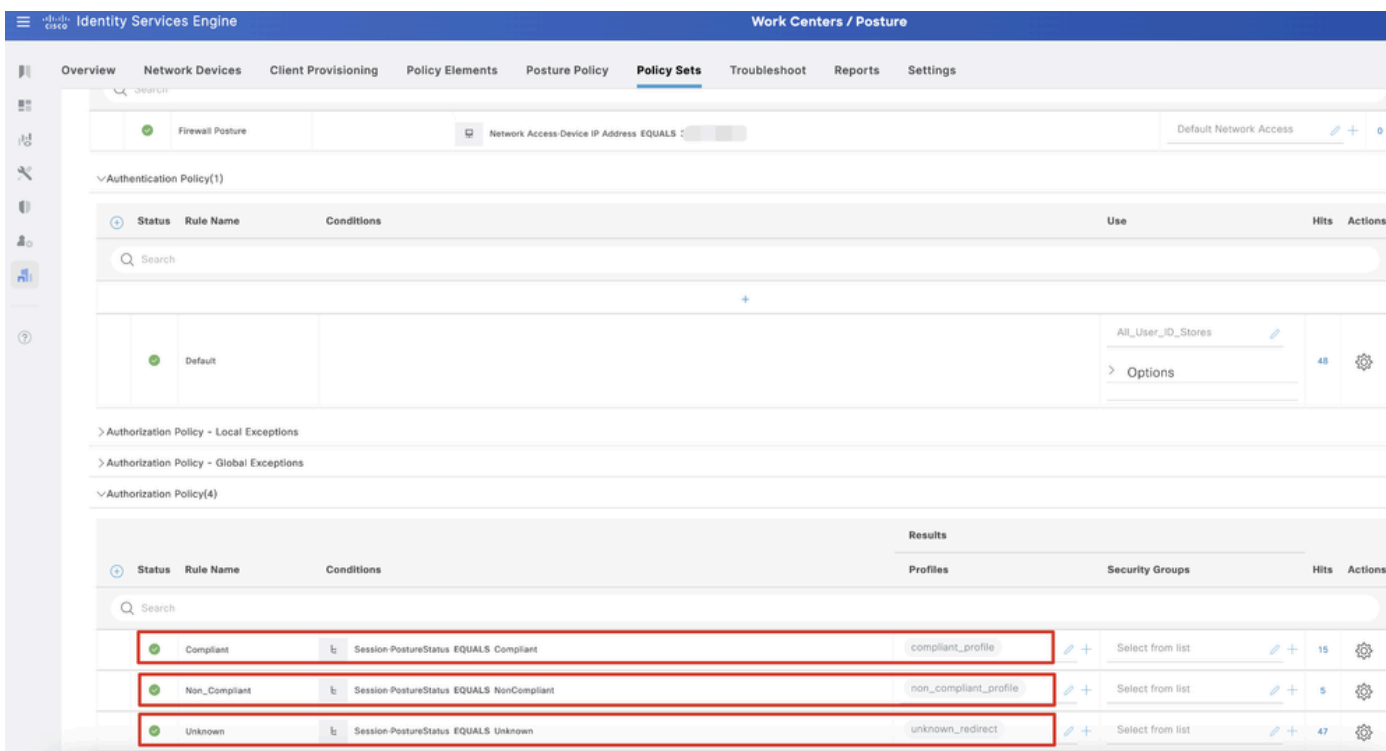
### ISE\_Add\_New\_Policy\_Set\_1

ステップ 23.2 : >をクリックして、ポリシーセットを入力します。 ポスチャ準拠、非準拠、および不明ステータスの新しい認可ルールを作成します。をクリックします。 Save

compliant\_profile準拠

non\_compliant\_profileによる非準拠

unknown\_redirectによる不明



### ISE\_Add\_New\_Policy\_Set\_2

Ubuntuでの設定

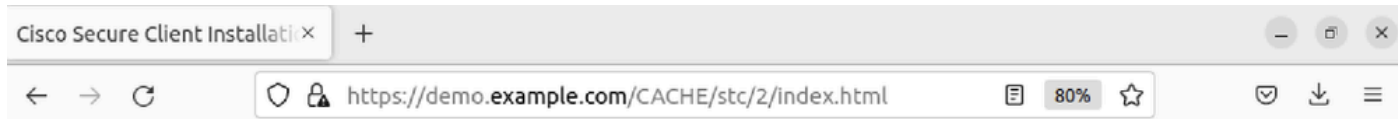
ステップ 24 : GUIを使用してUbuntuクライアントにログインします。ブラウザを開いてVPNポータルにログインします。この例では、demo.example.comです。

A screenshot of a web form titled "Logon". The form contains the following elements:

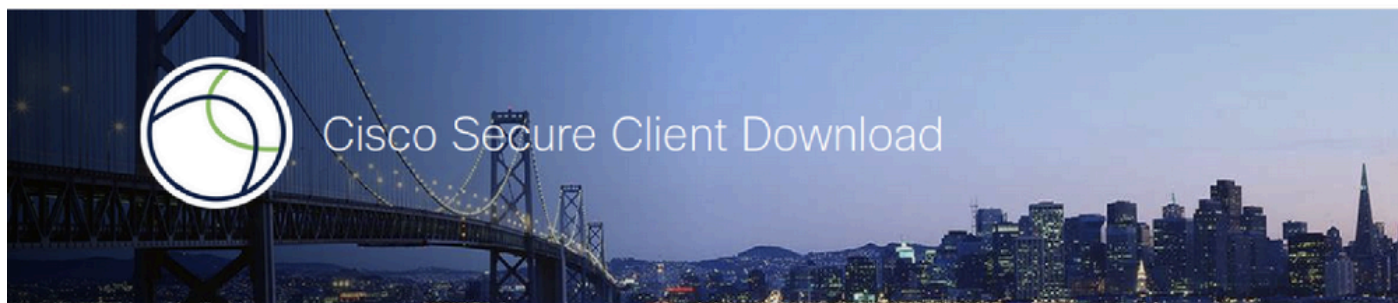
- A "Group" dropdown menu with the value "posture\_vpn" selected.
- A "Username" text input field.
- A "Password" text input field.
- A "Logon" button located below the input fields.

*Ubuntu\_Browser\_VPN\_ログイン*

ステップ 25 : をクリックします。Download for Linux



 **SECURE**  
Secure Client



## Download & Install

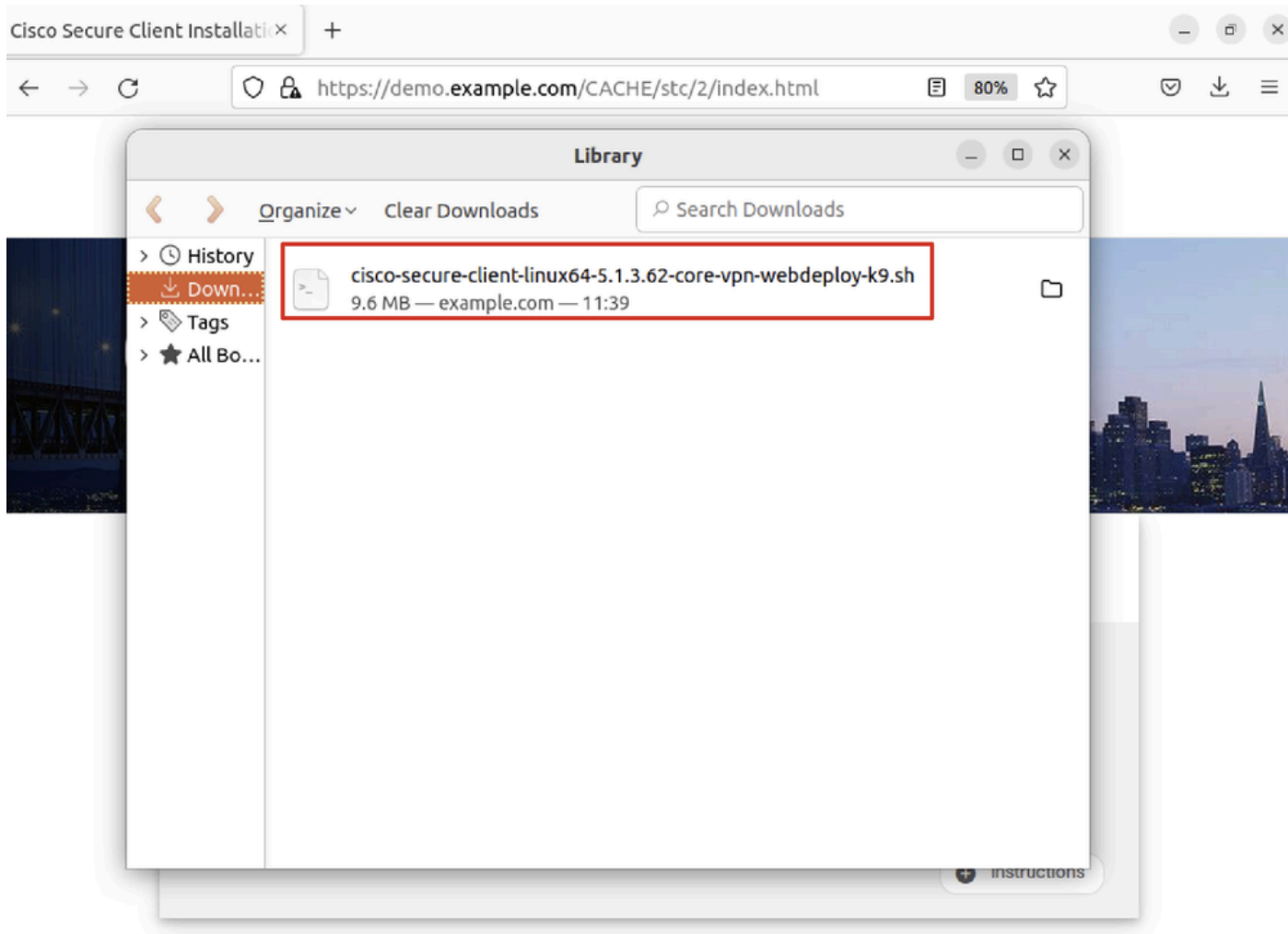
Download Cisco Secure Client and install it on your computer.

[Download for Linux](#)

[+ Instructions](#)

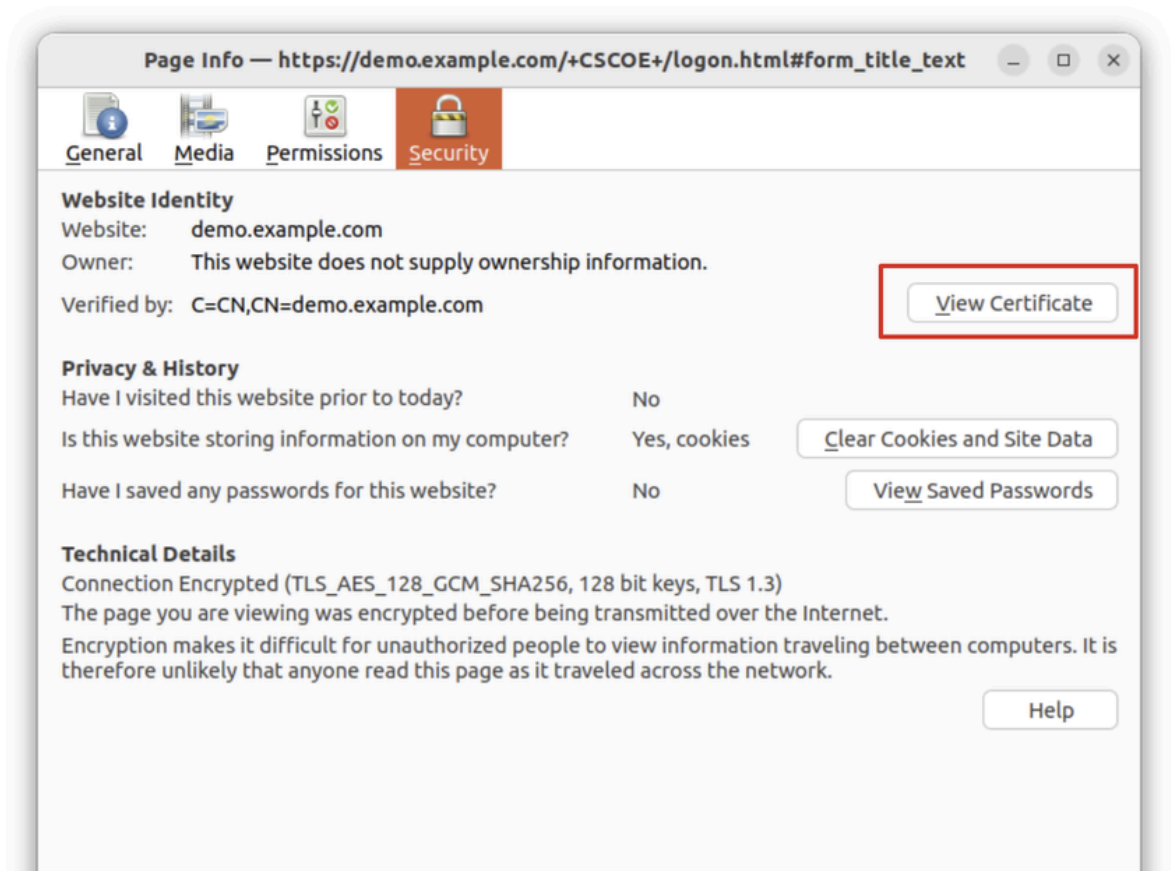
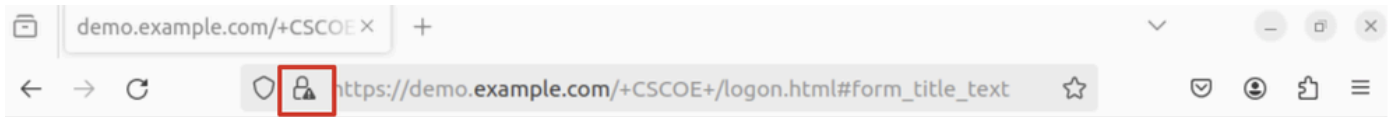
*Ubuntu\_Browser\_VPN\_ダウンロード\_1*

ダウンロードしたファイルの名前はcisco-secure-client-linux64-5.1.3.62-core-vpn-webdeploy-k9.shです。



Ubuntu\_Browser\_VPN\_ダウンロード\_2

ステップ 26 : ブラウザを使用してVPN証明書をダウンロードし、ファイル名を<certificate>に変更します。crt。これは、Firefoxを使用して証明書をダウンロードする例です。



*Ubuntu\_Browser\_VPN\_Cert\_Download (ダウンロード)*

ステップ 27 : Ubuntuクライアントで端末を開きます。path home/user/Downloads/に移動して、Cisco Secure Clientをインストールします。

```
<#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$
```

ステップ 28 : UbuntuクライアントのVPNポータル証明書を信頼します。

```
<#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...
```

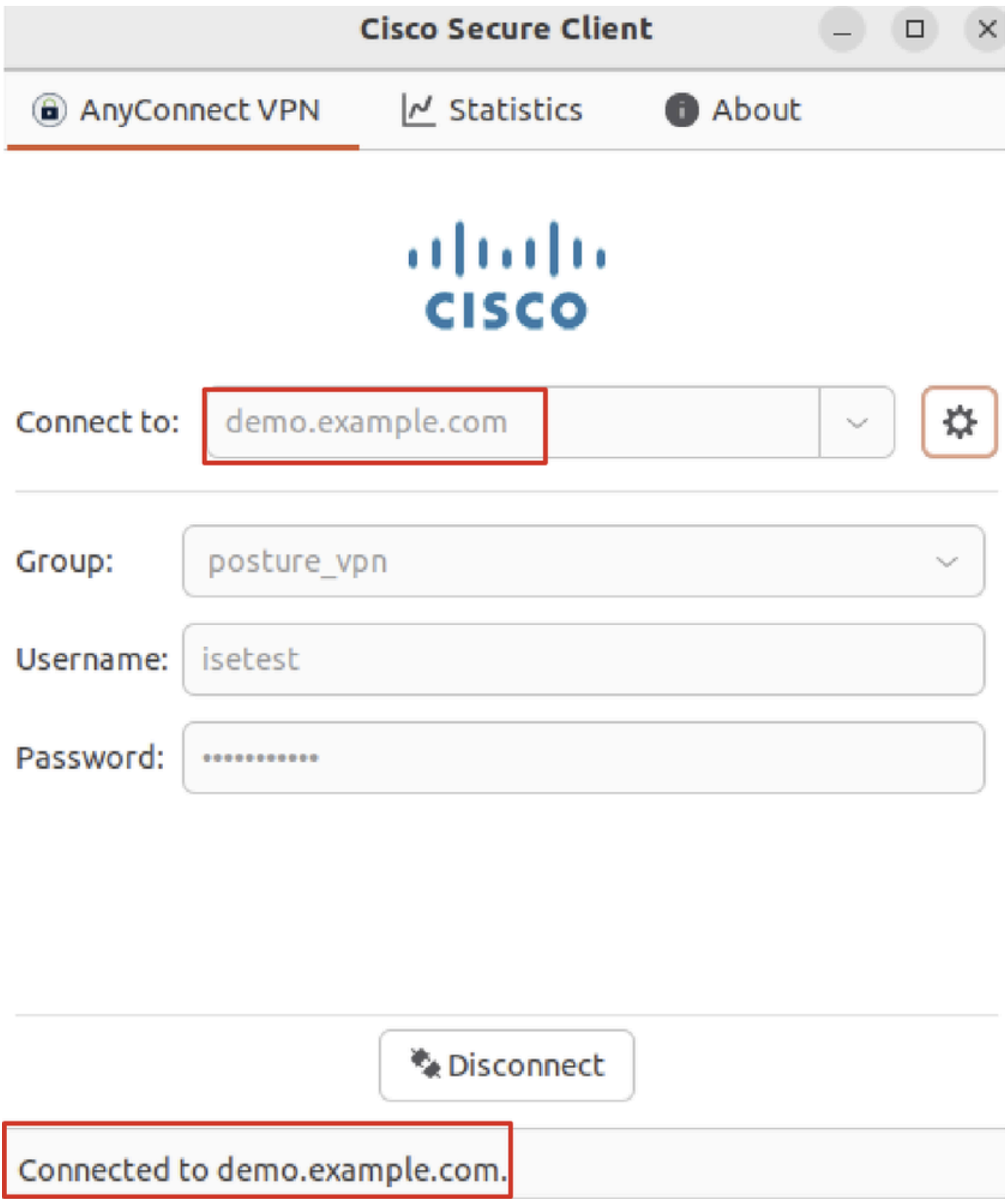
done.

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

```
openssl verify demo-example-com.crt
```

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

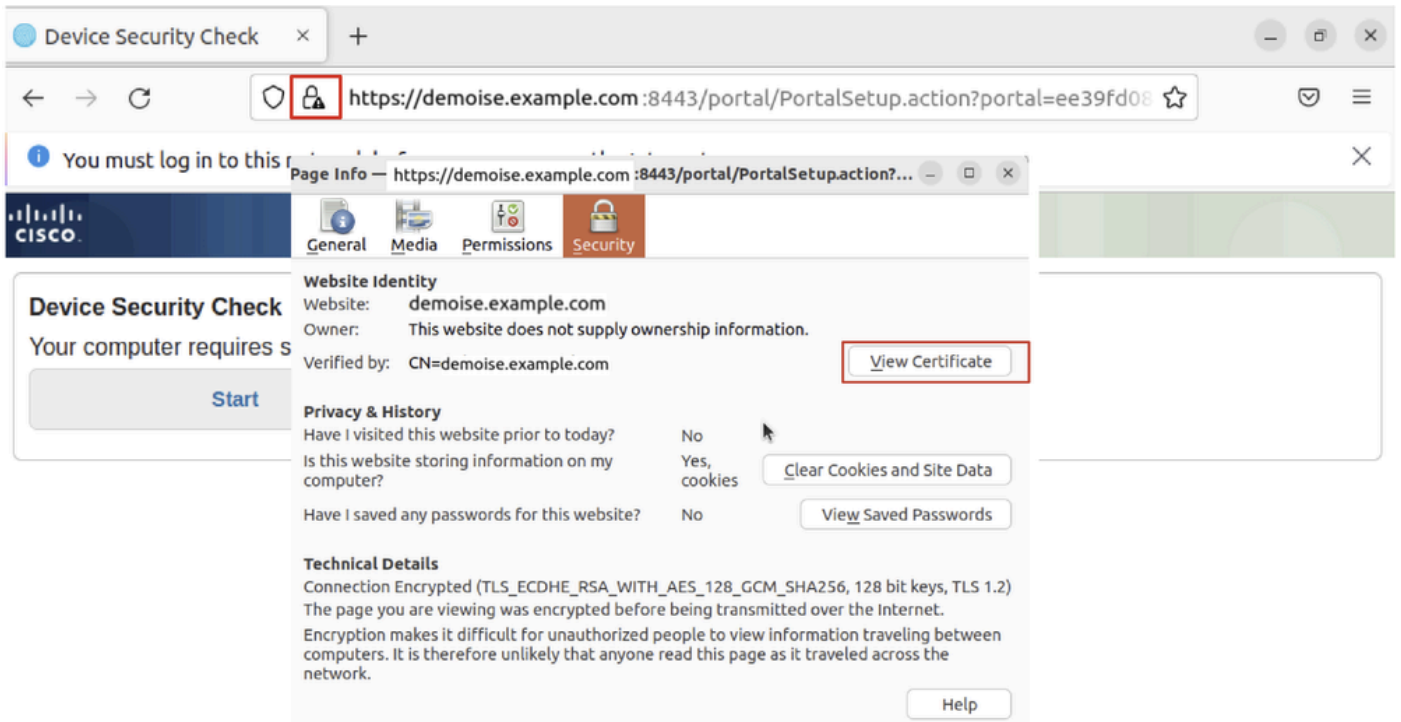
ステップ 29 : UbuntuクライアントでCisco Secure Clientを開き、VPNをdemo.example.comに正常に接続します。



Ubuntu\_Secure\_Client\_接続

ステップ 30 : ブラウザを開き、ISE CPPポータルへのリダイレクトをトリガーするWebサイトにアクセスします。ISE CPPポータルから証明書をダウンロードし、ファイル名を<certificate>に変更します。crt。次に、ダウンロードにFirefoxを使用する例を示します。





Ubuntu\_Browser\_CPP\_Cert\_ダウンロード

ステップ 30.1 : Ubuntuクライアント上のISE CPPポータル証明書を信頼します。

<#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
```

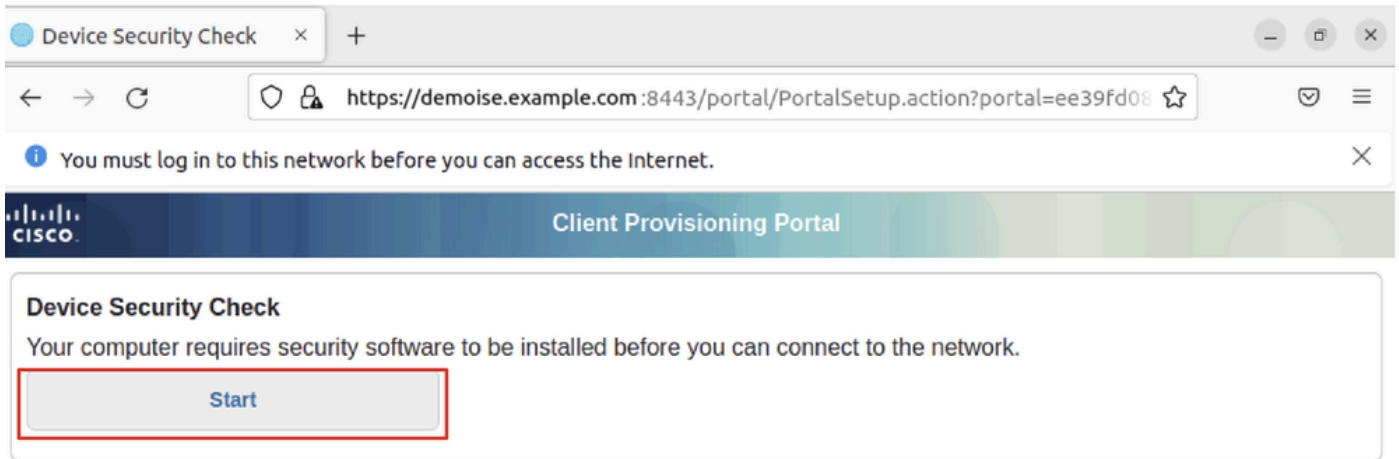
```
1 added
```

```
, 0 removed; done.
```

```
Running hooks in /etc/ca-certificates/update.d...
```

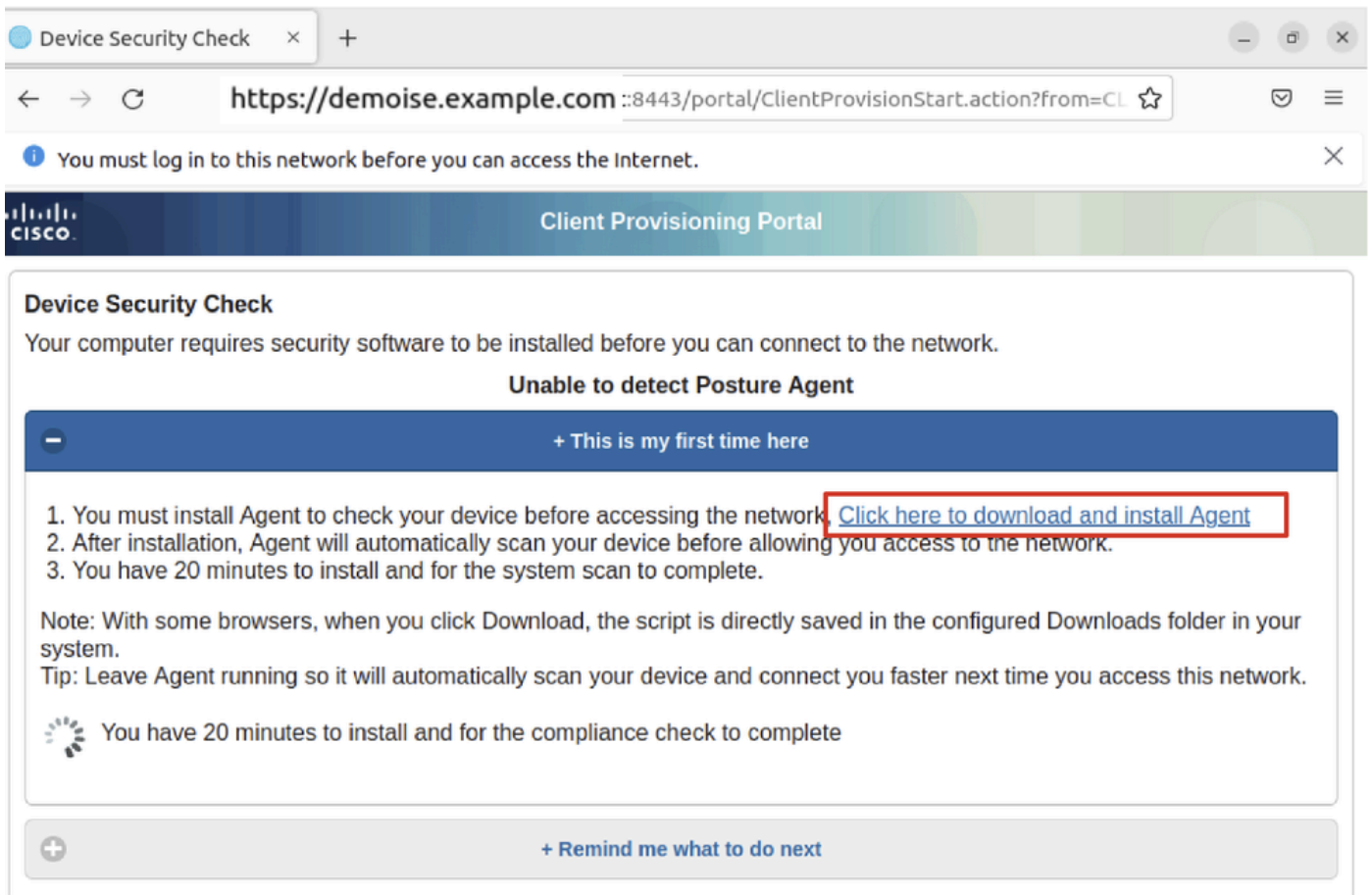
```
done.
```

ステップ 31 : ISE CPPポータルStart でクリックします。



Ubuntu\_Browser\_CPP\_開始

ステップ 32 : Click here to download and install Agent



Ubuntu\_Browser\_CPP\_Download\_ポスチャ

ステップ 33 : Ubuntuクライアントで端末を開きます。パスhome/user/Downloads/に移動して、ポスチャモジュールをインストールします。

<#root>

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

```
cisco-secure-client-ise-network-assistant-linux64-5.1.3.62_demoise.example.com_8443_0NcLgcMURfyZmR6HoLm
```

```
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_0NcLgcMURfyZmR6Ho
```

```
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_0NcLgcMURfyZmR6Ho
```

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.

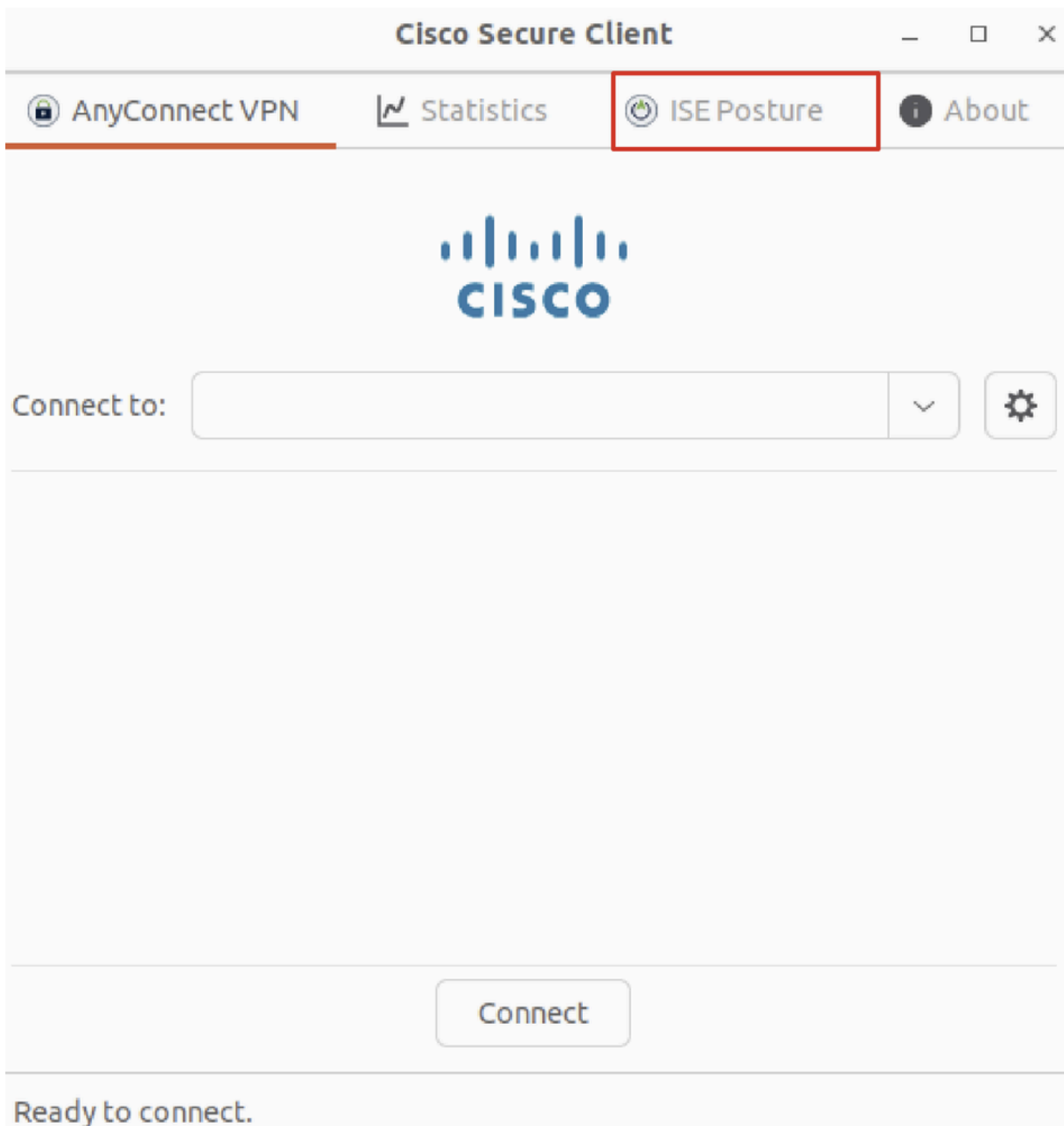
Downloading Cisco Secure Client...

Downloading remote package...

Running Cisco Secure Client - Downloader...

Installation is completed.

ステップ 34 : UbuntuクライアントのUIで、Cisco Secure Clientを終了し、再度開きます。ISEポスチャモジュールがインストールされ、正常に実行されます。



*Ubuntu\_Secure\_Client\_ISE\_Posture\_Installed* (インストール済み)

ステップ 35 : Ubuntuクライアントで端末を開きます。pathに移動home/user/Desktoptest.txt し、ISEで設定されたファイル条件を満たすファイルを作成します。

<#root>

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

```
cd Desktop/
```

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

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

## 確認

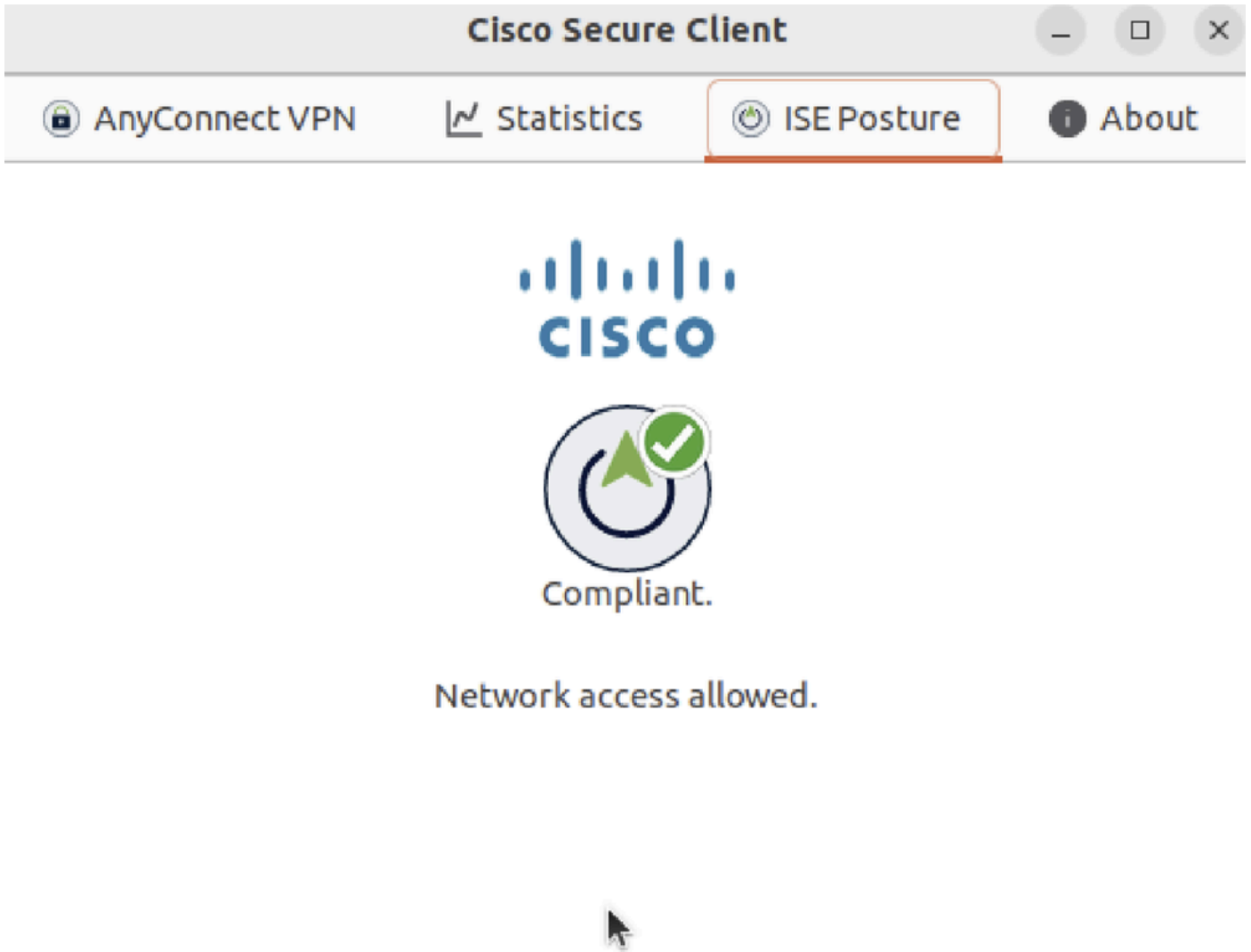
ここでは、設定が正常に機能しているかどうかを確認します。

ステップ 1 : UbuntuクライアントでVPNをdemo.example.comに接続します。

The screenshot shows the Cisco Secure Client application window. The title bar reads "Cisco Secure Client". The main menu includes "AnyConnect VPN", "Statistics", "ISE Posture", and "About". The "ISE Posture" menu item is highlighted with a red box. Below the menu is the Cisco logo. The main interface features a "Connect to:" field with "demo.example.com" entered, highlighted by a red box. Below this are fields for "Group:" (set to "posture\_vpn"), "Username:" (set to "isetest"), and "Password:" (masked with dots). A "Disconnect" button is located at the bottom. At the very bottom, a status bar shows "Connected to demo.example.com.", which is also highlighted with a red box.

確認\_Ubuntu\_セキュア\_クライアント\_接続

ステップ 2 : UbuntuクライアントでISEポスチャステータスを確認します。



確認\_Ubuntu\_Secure\_Client\_Compliant

ステップ 3 : ISEのRADIUSライブログを確認します。Operations > RADIUS Live Logに移動します。

The screenshot displays the Cisco Identity Services Engine (ISE) interface, specifically the "Operations / RADIUS" section. The "Live Logs" tab is active. The page shows several summary cards for "Misconfigured Supplicants", "Misconfigured Network Devices", "RADIUS Drops", "Client Stopped Responding", and "Repeat Counter", all with a value of 0. Below these cards is a table of live logs. The table has columns for Time, Status, Details, Identity, Endpoint ID, Endpoint Profile, Posture Status, Authentication Policy, and Authorization Policy. Two rows are highlighted with a red box, showing a "Compliant" status for the first two entries and a "Pending" status for the third entry.

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	●	🔒	isetest	52:54:00:17:6B:FA	Ubuntu-Workstation	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

確認ISE\_ライブログ

ステップ 4 : SSHまたはコンソールを使用してFTD CLIに移動します。

```
<#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

## トラブルシューティング

ここでは、設定のトラブルシューティングに使用できる情報を示します。

Cisco Secure ClientとISEのポスチャフローとトラブルシューティングについては、CCOの『[2.2前後のISEポスチャスタイルの比較](#)』および『[ISEセッション管理とポスチャのトラブルシューティング](#)』を参照してください。

## 関連情報

- [Cisco Identity Services Engineネットワークコンポーネントの互換性、リリース3.3](#)



- [Cisco Identity Services Engine 管理者ガイド リリース 3.3](#)
- [シスコのテクニカルサポートとダウンロード](#)

## 翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。