ISE 3.3を使用したLinux VPNポスチャの設定

内容

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

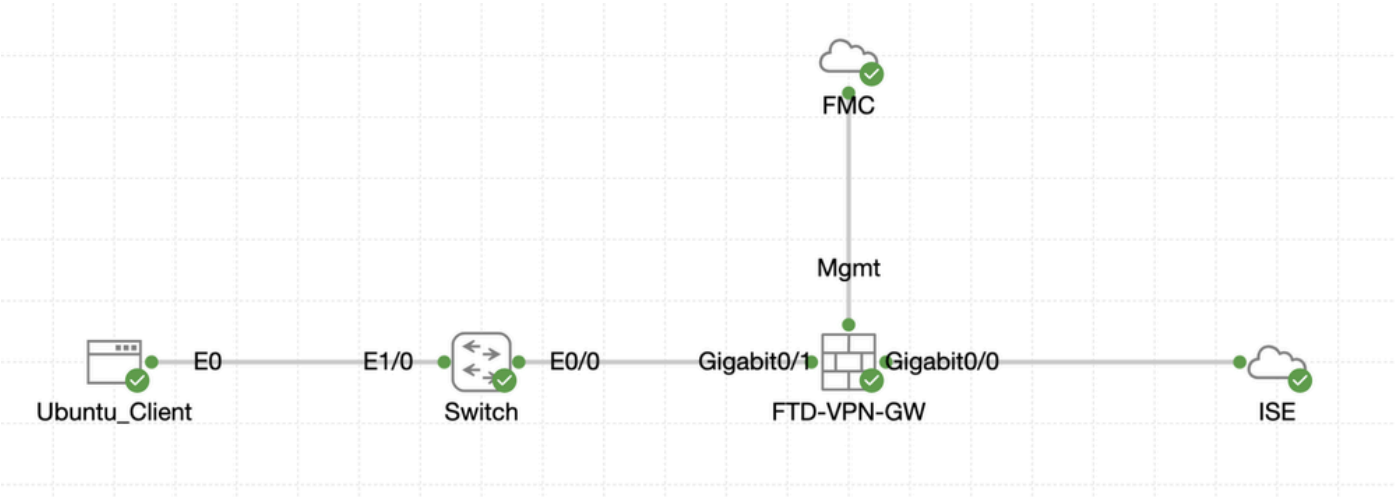
- Cisco Firepower Threat Defense(FTD)7.4.1
- Cisco Firepower Management Center(FMC)7.4.1
- Cisco Identity Services Engine(ISE)3.3

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



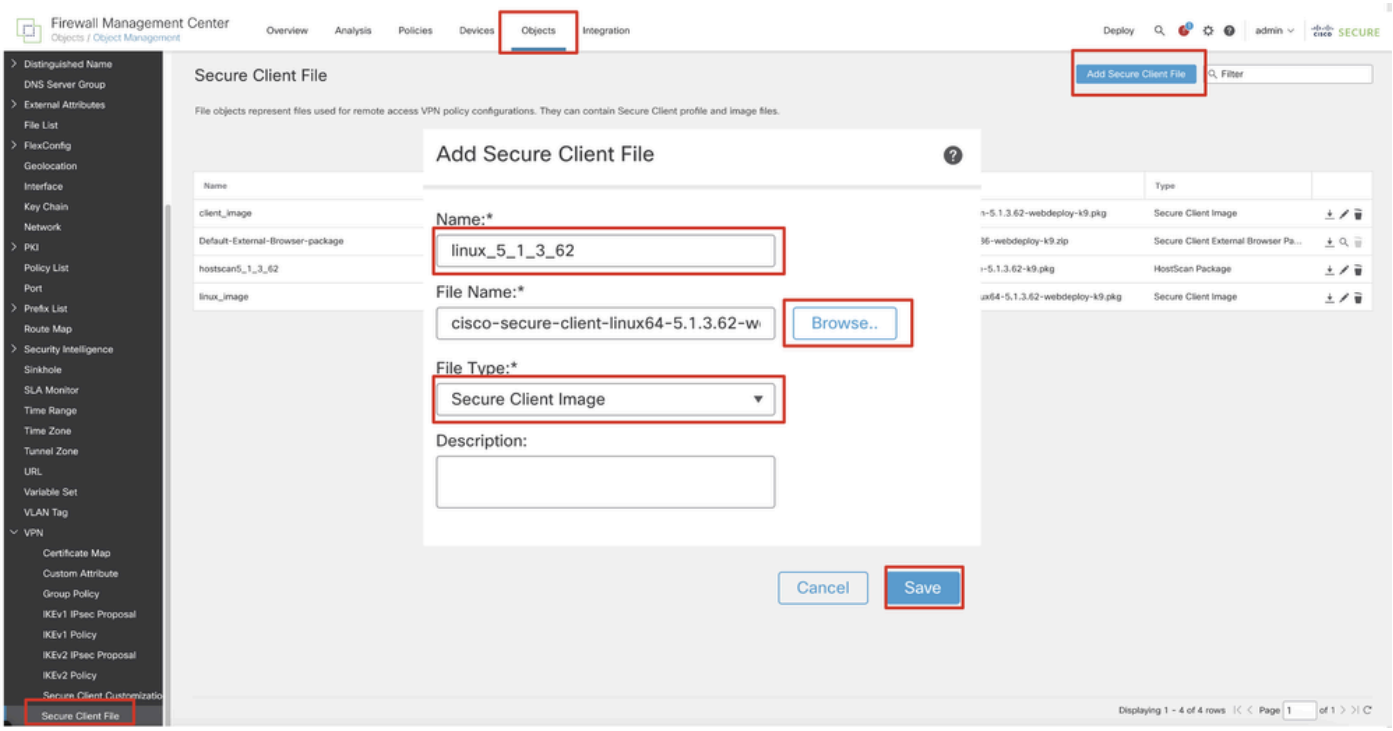
トポロジ

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、『ポスチャフロー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。

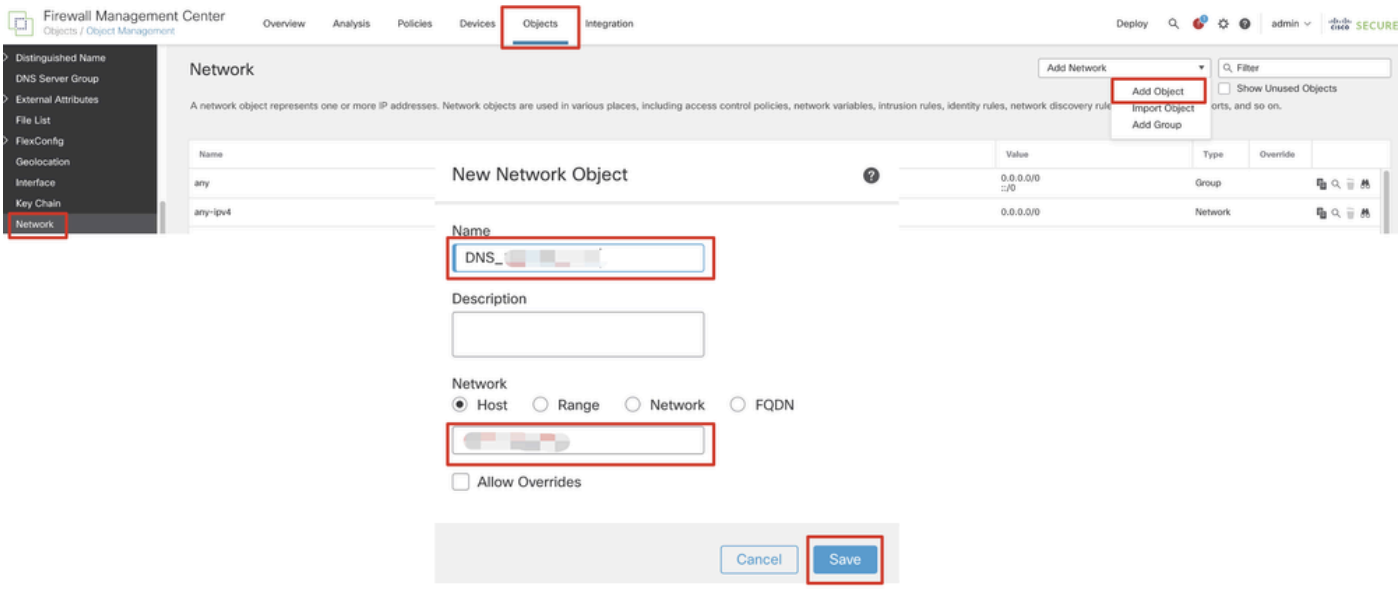
ステップ 3： Objects > Object Management > VPN > Secure Client Fileに移動します。Add Secure Client Fileをクリックし、名前を入力し、File Nameを参照して選択します。cisco-secure-client-linux64-5.1.3.62-webdeploy-k9.pkg、Secure Client Image inFile Typeドロップダウンリストを選択します。次にSaveをクリックします。



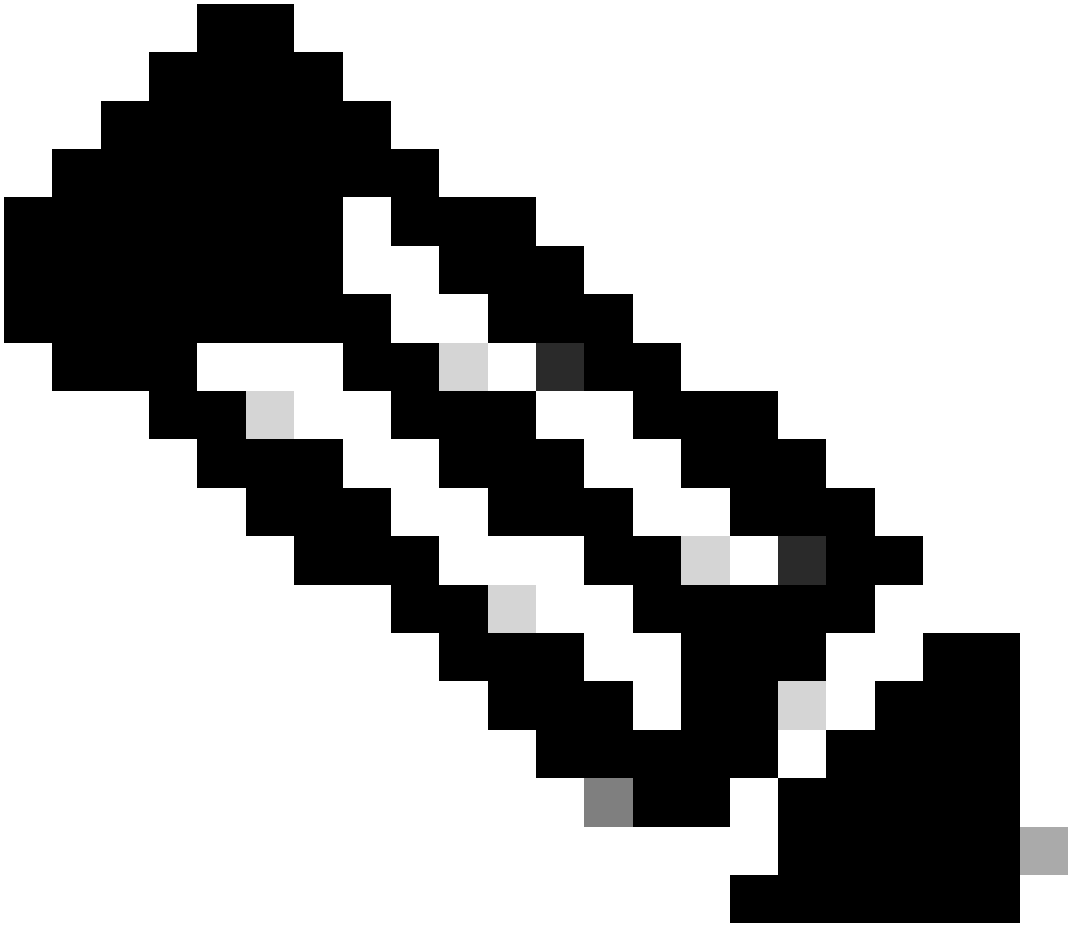
FMC_Upload_Secure_Client_イメージ

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

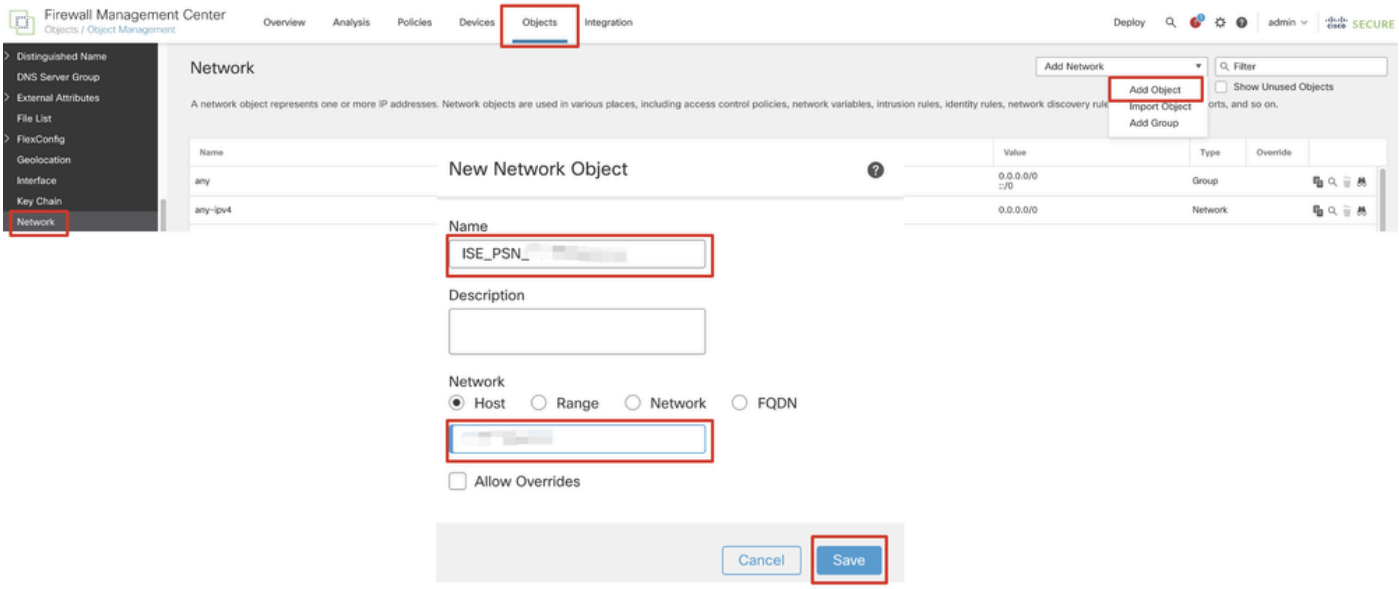


FMC_Add_Object_DNS（オプション）



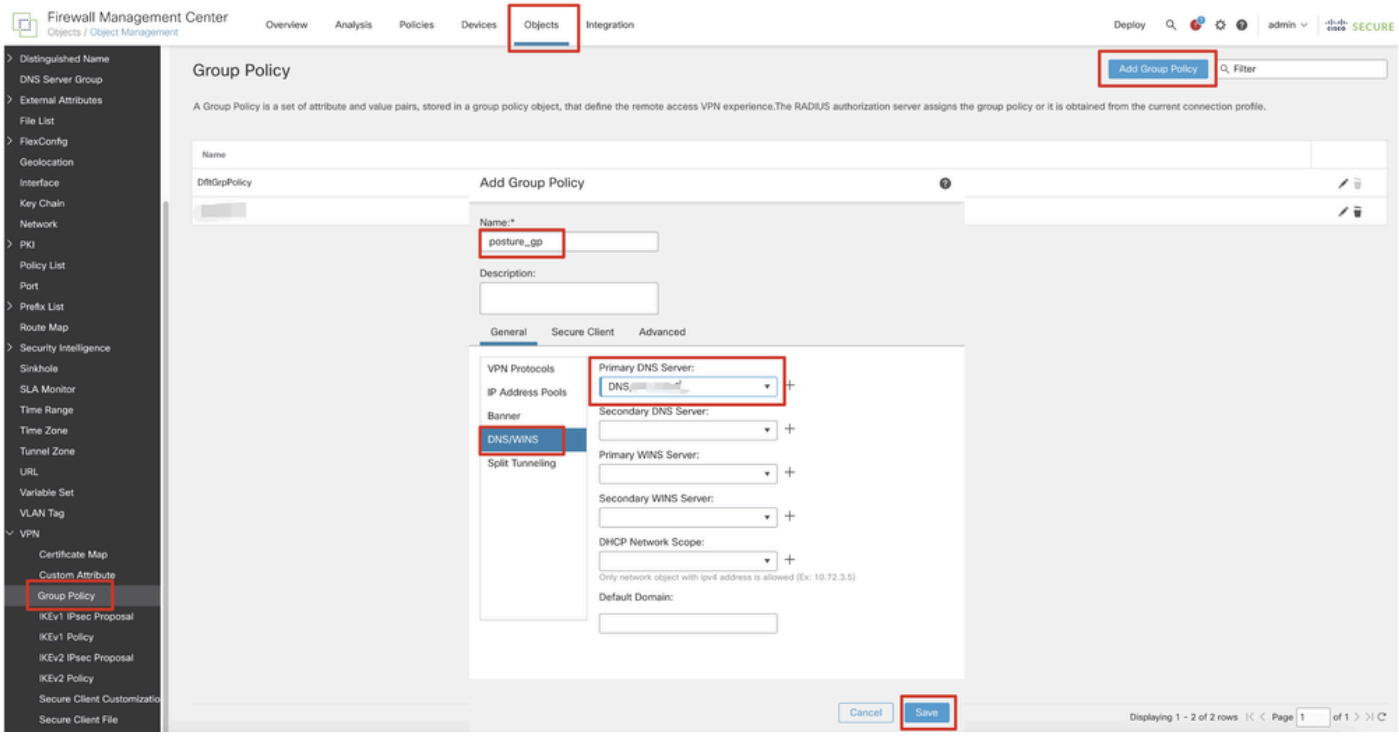
注：ここで設定するDNSサーバは、VPNユーザ用です。

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

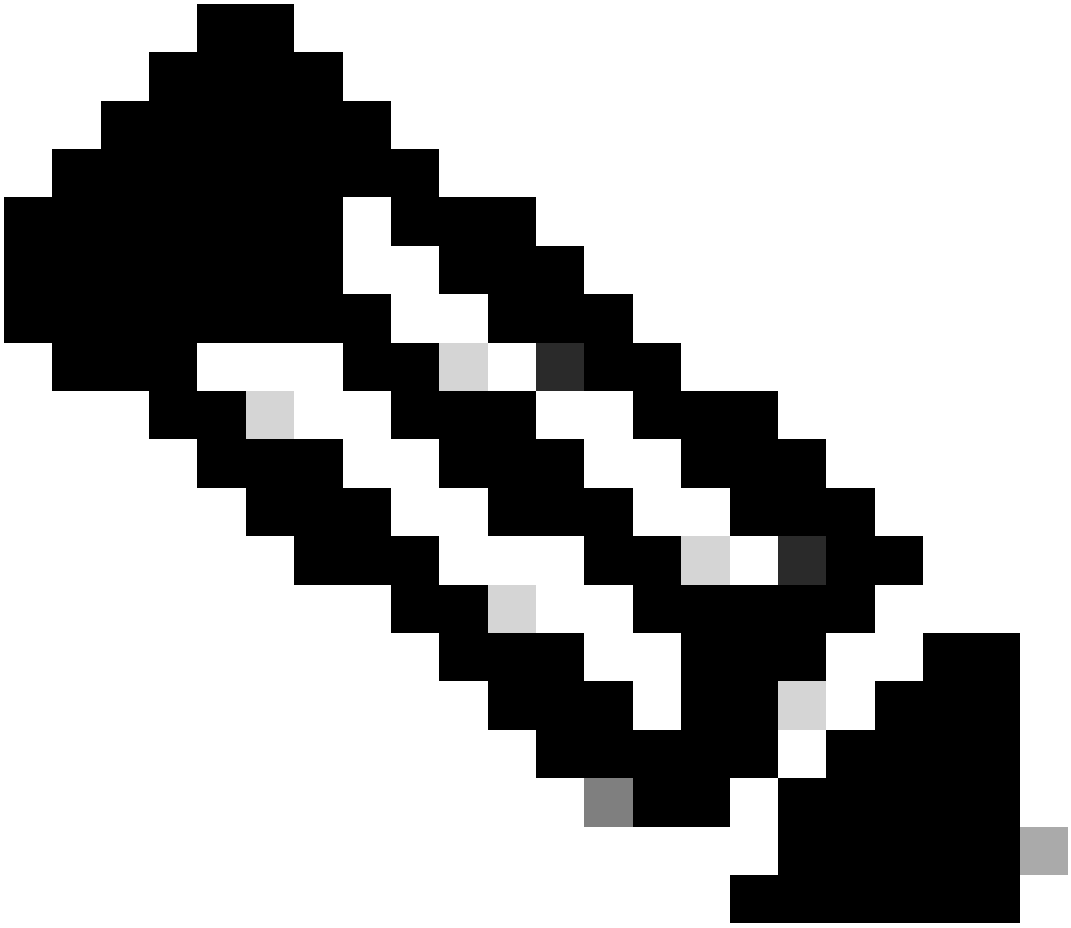


FMC_Add_Object_ISE（オプション）

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。

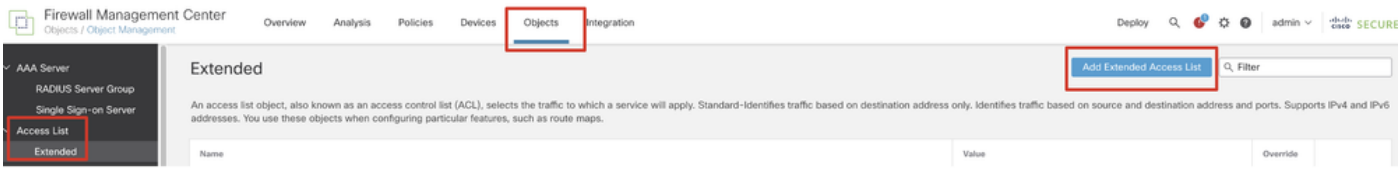


*FMC_Add_Group_*ポリシー



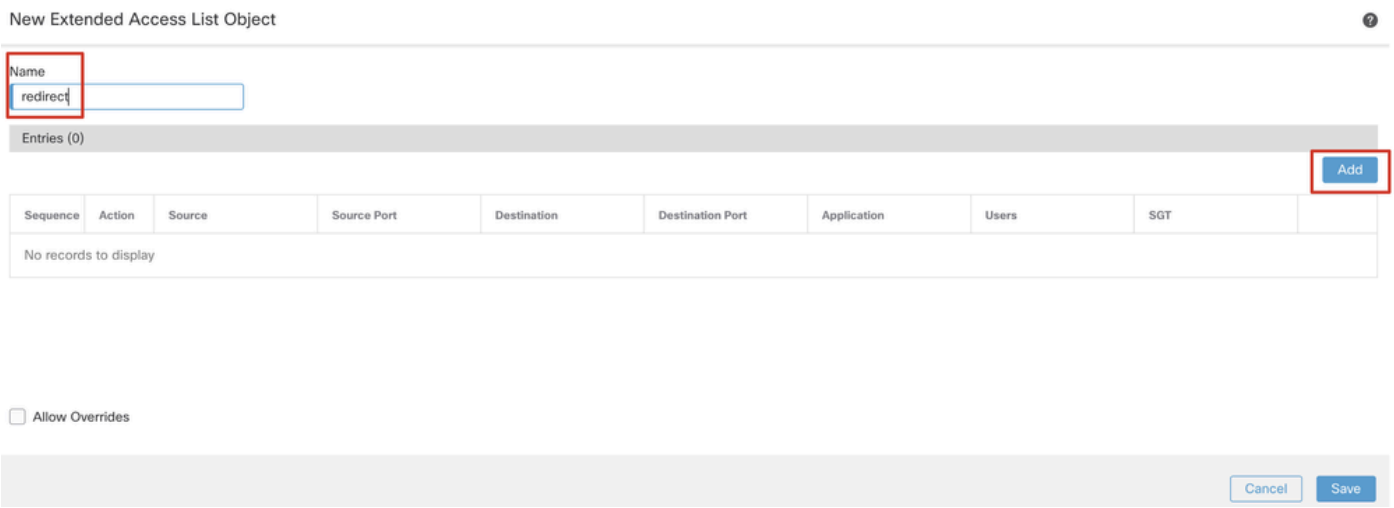
注：VPNグループポリシーで使用されるDNSサーバがISEクライアントプロビジョニングポータルのFQDNとenroll.cisco.comを解決できることを確認します。

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



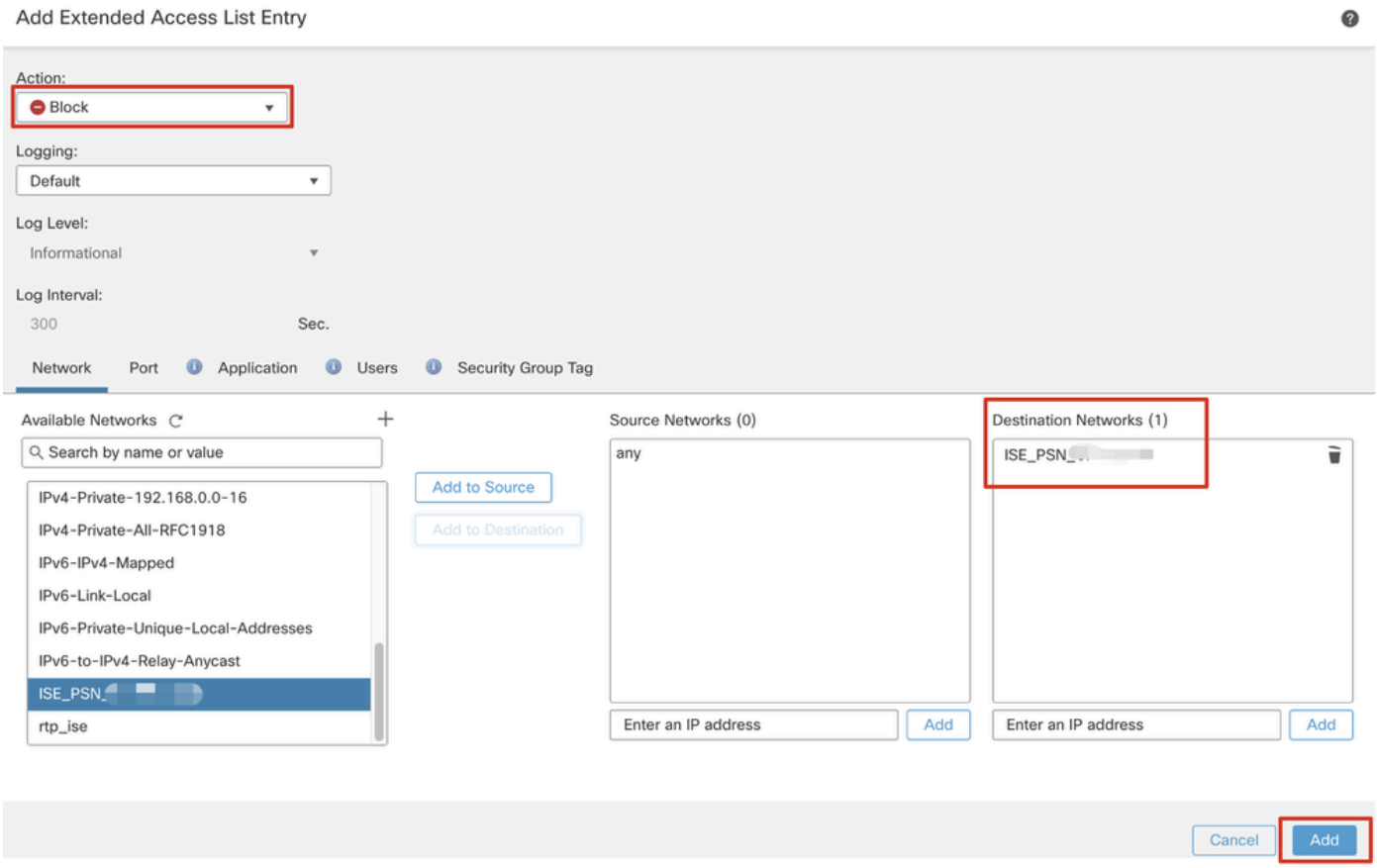
FMC_追加_リダイレクト_ACL

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

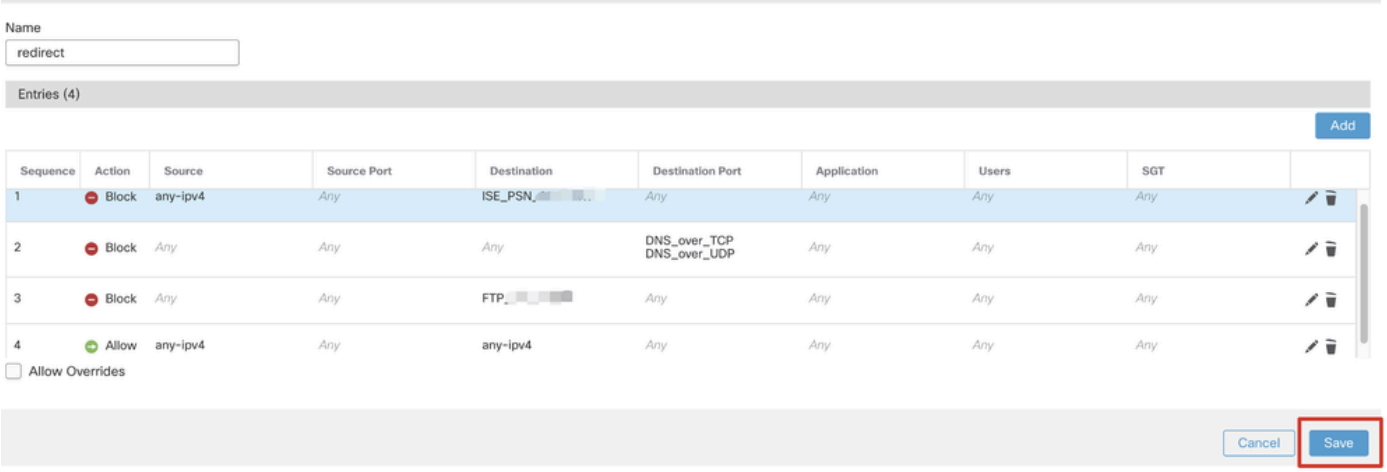


FMC_追加_リダイレクト_ACL_パート_1

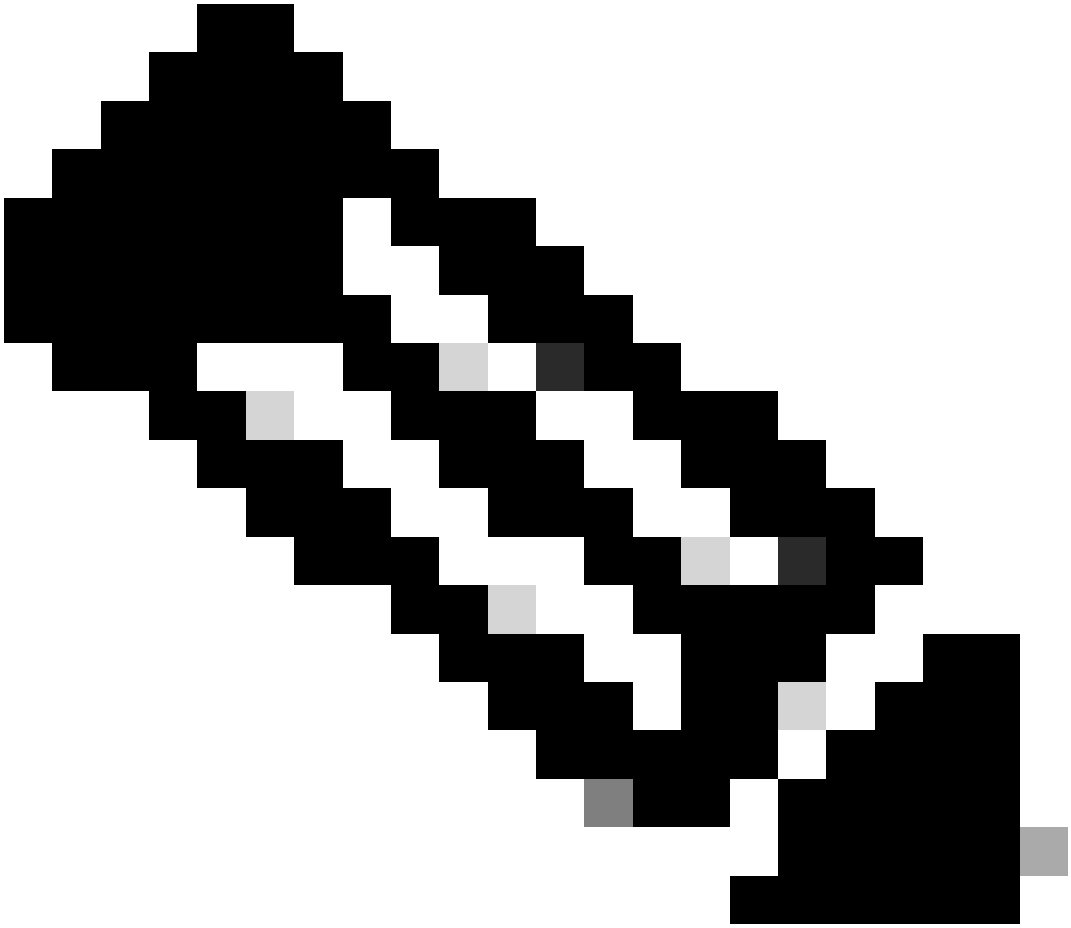
ステップ 6.2： DNSトラフィック、ISE PSN IPアドレスへのトラフィック、および修復サーバをブロックして、リダイレクトから除外します。残りのトラフィックを許可します。これにより、リダイレクトがトリガーされます。をクリックします。Save



FMC_追加_リダイレクト_ACL_パート_2

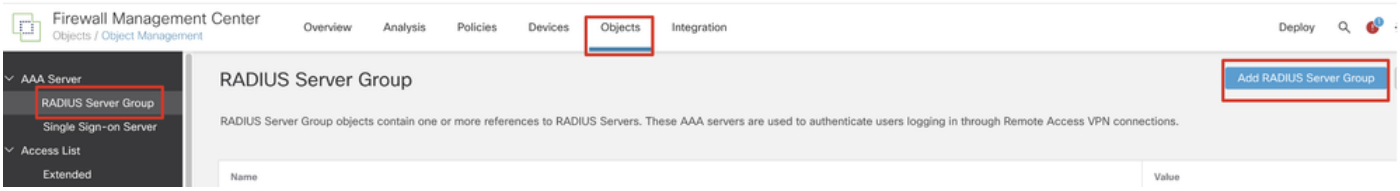


FMC_追加_リダイレクト_ACL_パート_3



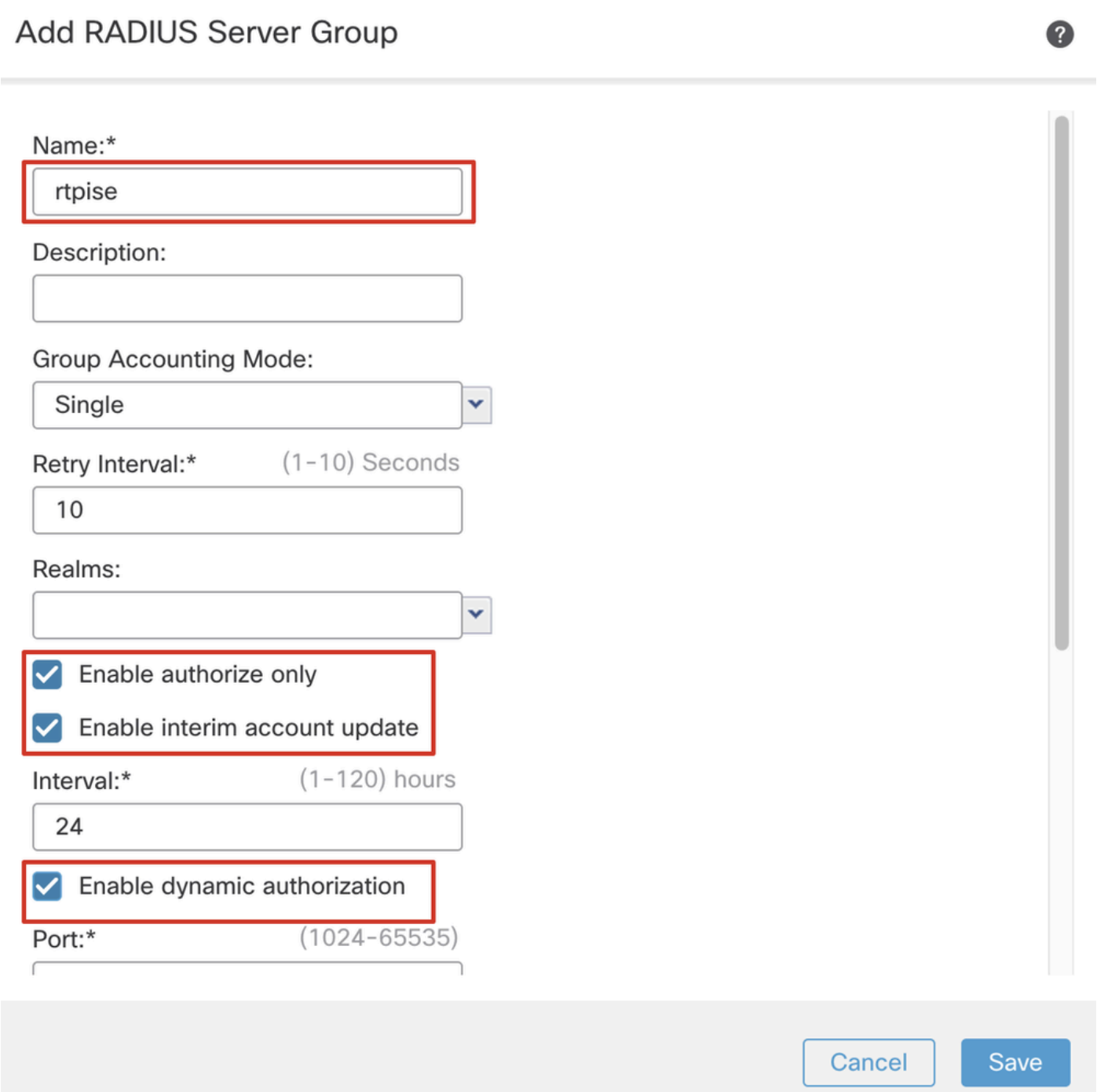
注：このリダイレクトACLの例では、宛先FTPが修復サーバの例として使用されています。

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



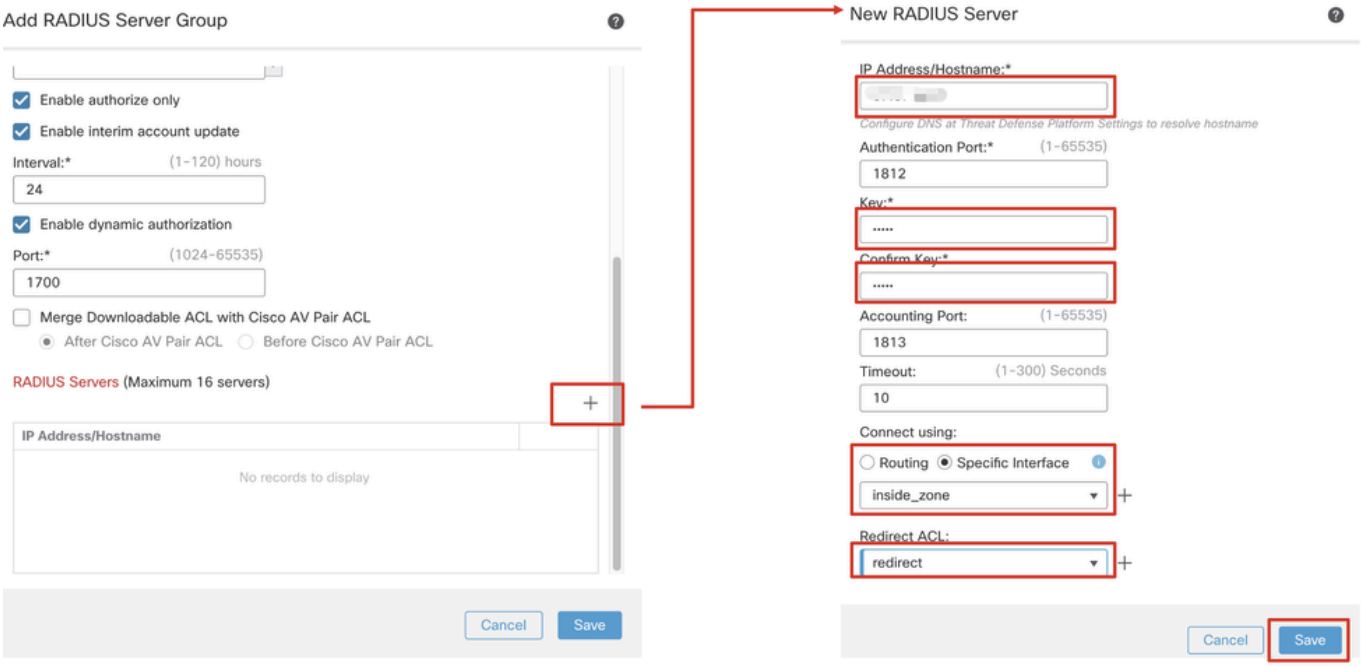
FMC_Add_New_Radius_サーバ_グループ

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



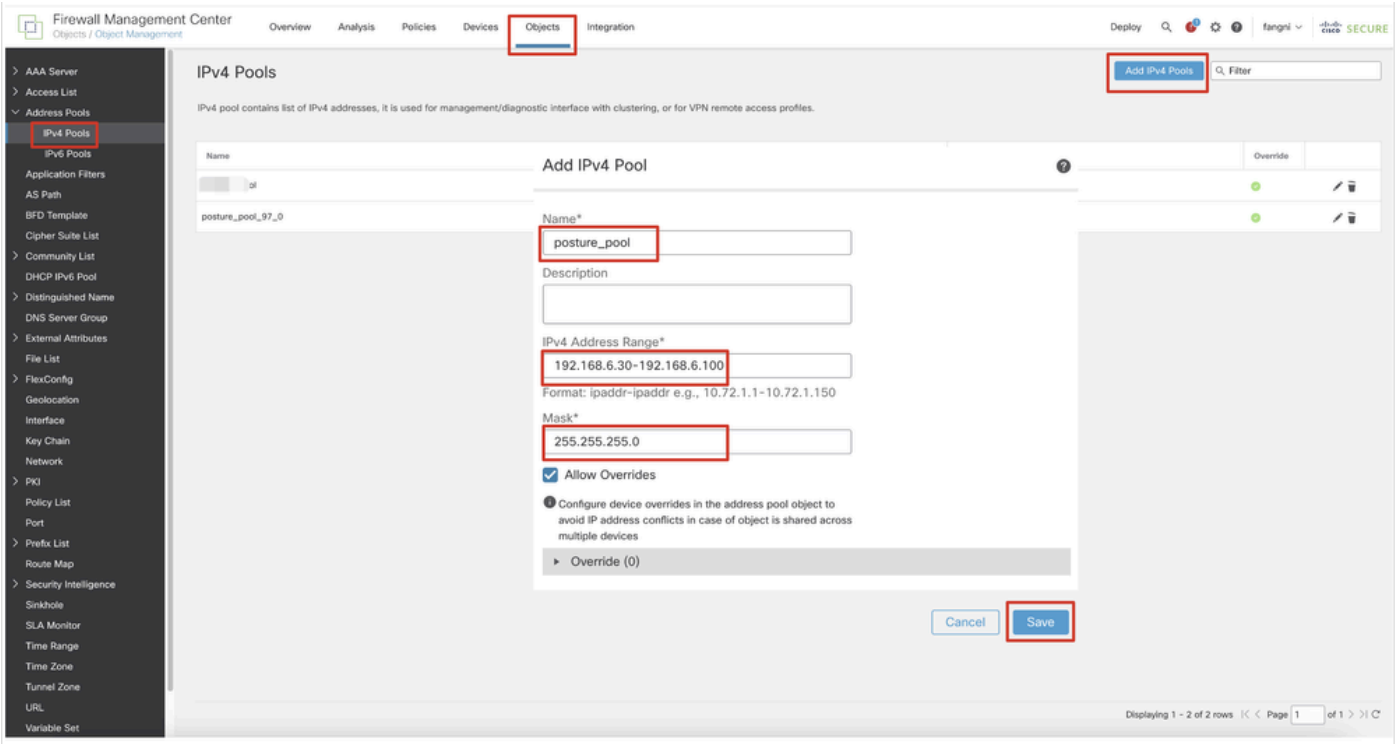
FMC_追加_新規_Radius_サーバ_グループ_パート_1

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。



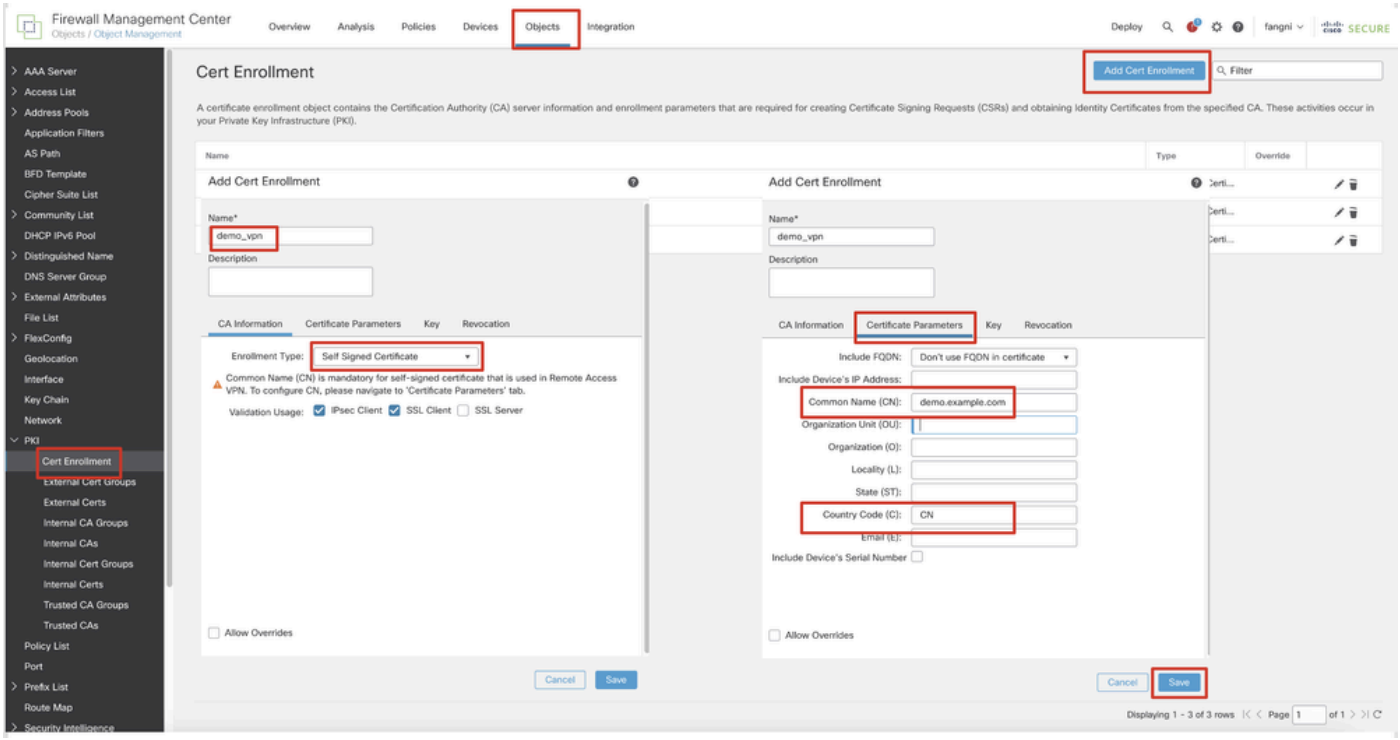
FMC_追加_新規_Radius_サーバ_グループ_パート_2

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。



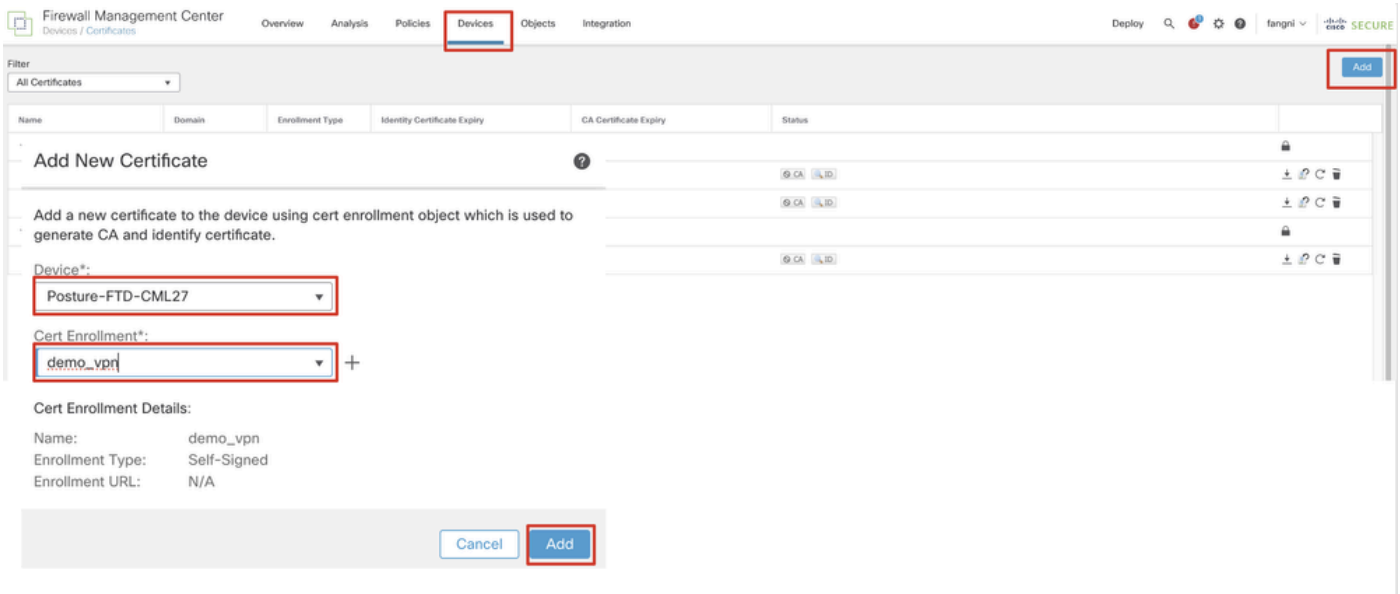
FMC_Add_New_プール

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 Certificatein 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）

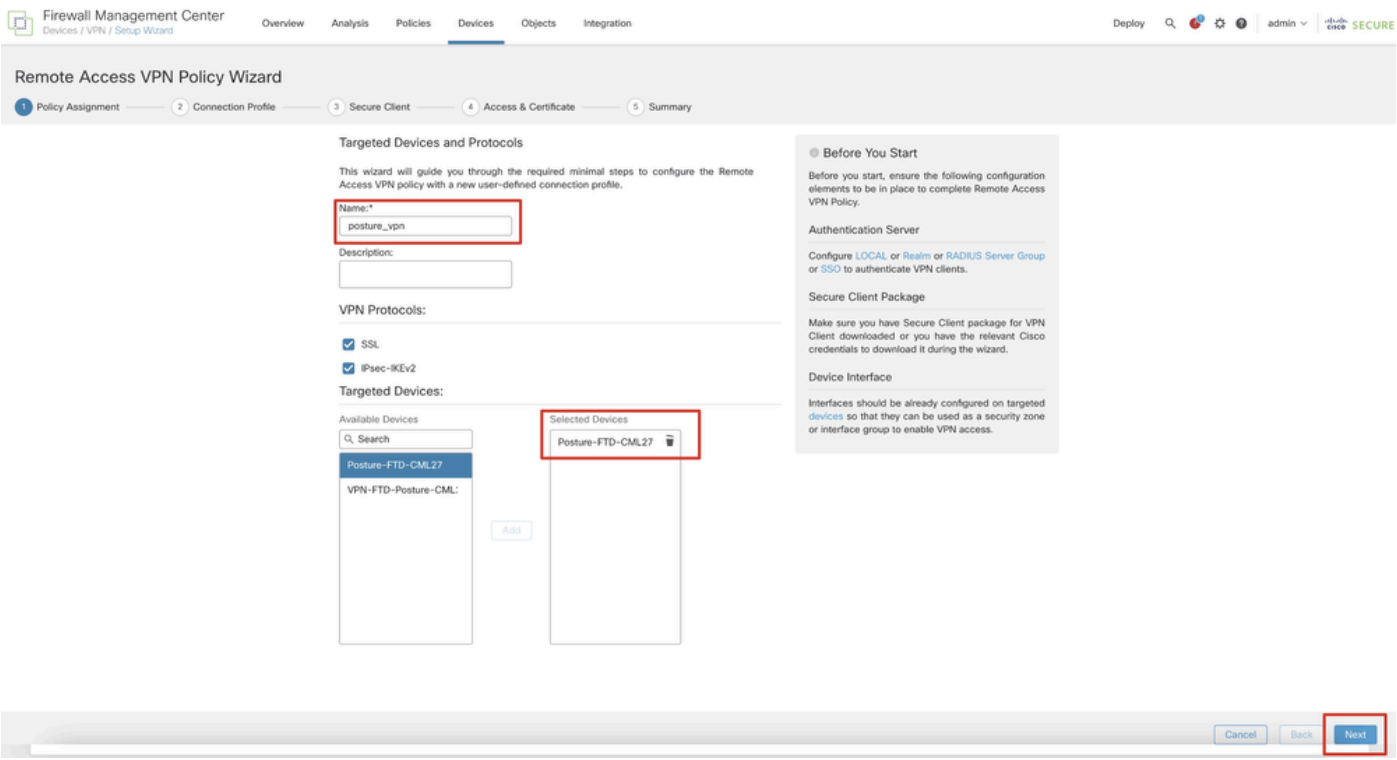
ステップ 10： Devices > Certificatesに移動します。Addをクリックし、DeviceでFTD名を選択し、Cert Enrollmentで以前に設定した登録を選択します。をクリックします。Add



FMC_Add_New_Cert_To_FTD（オプション）

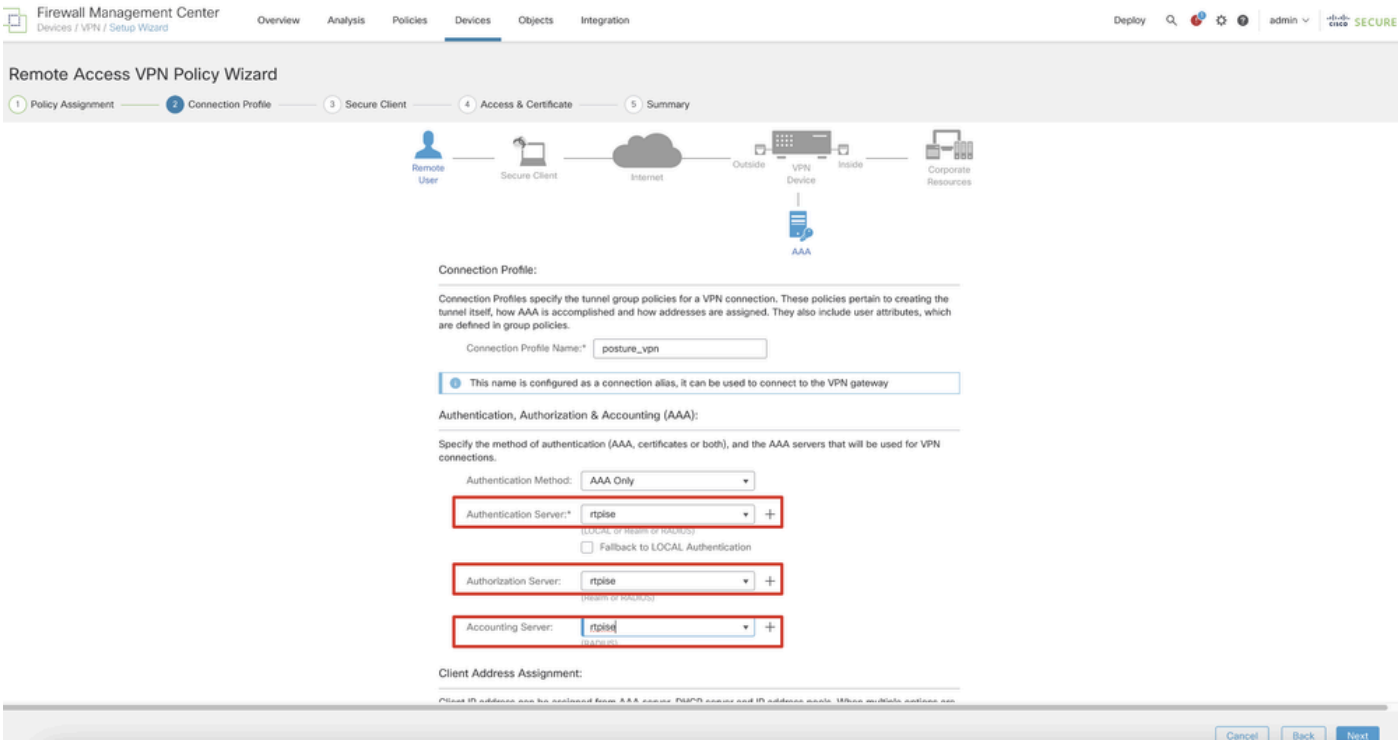
ステップ 11 Devices > VPN > Remote Accessに移動します。をクリックします。Add

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



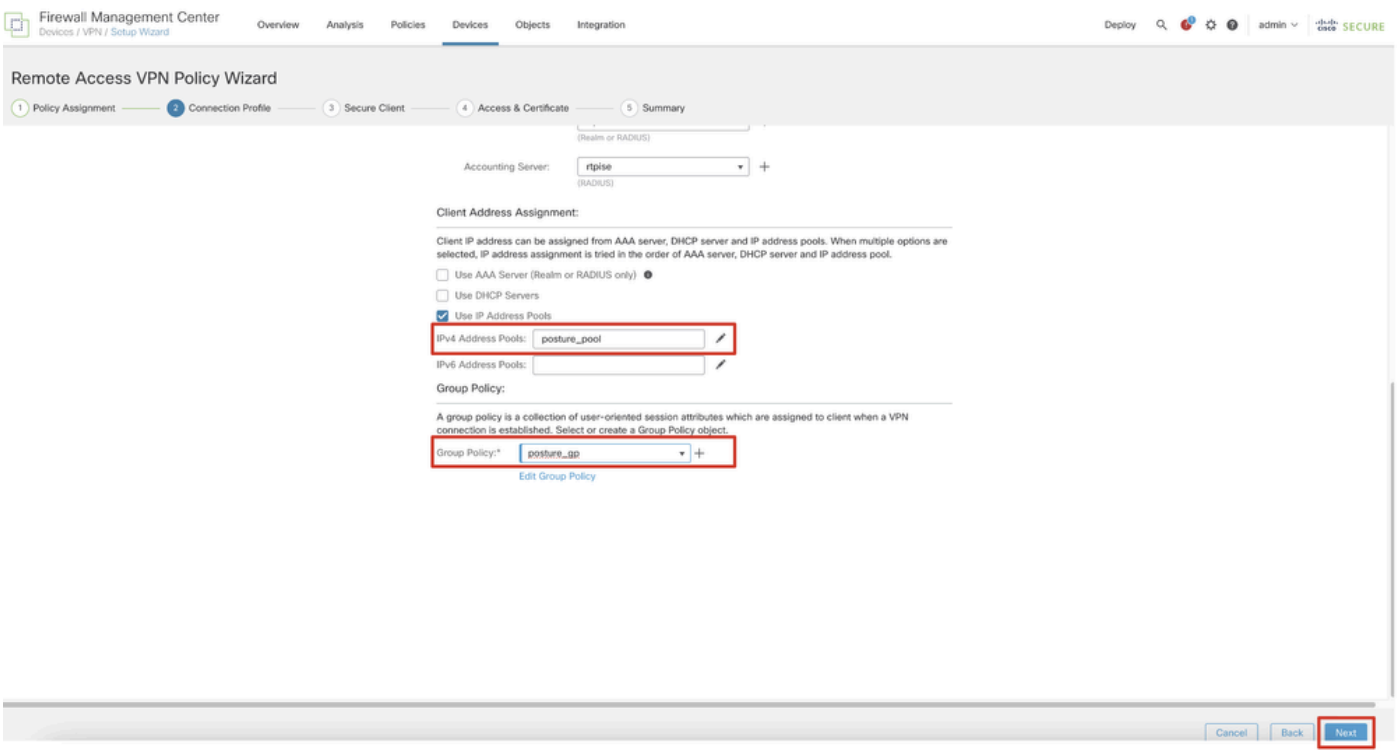
FMC_New_RAVPN_Wizard_1

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。



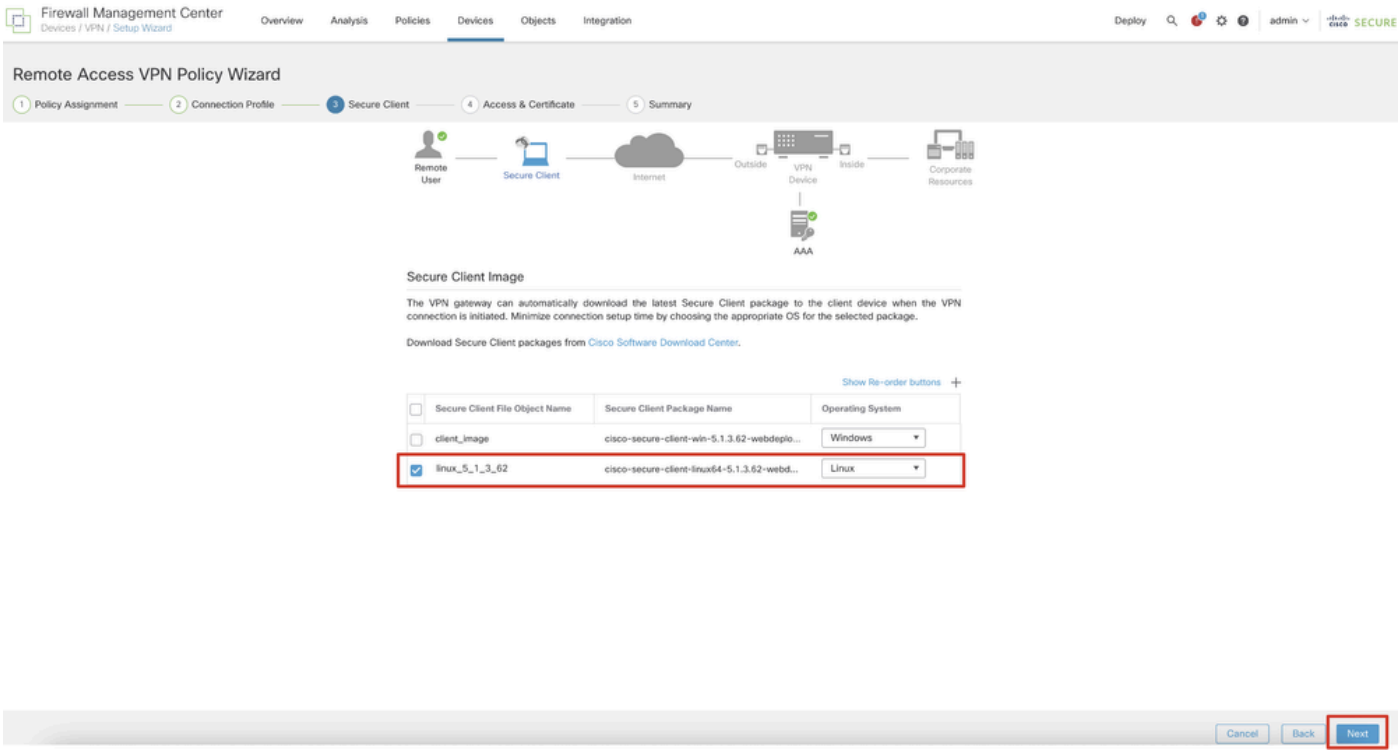
FMC_New_RAVPN_Wizard_2

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。



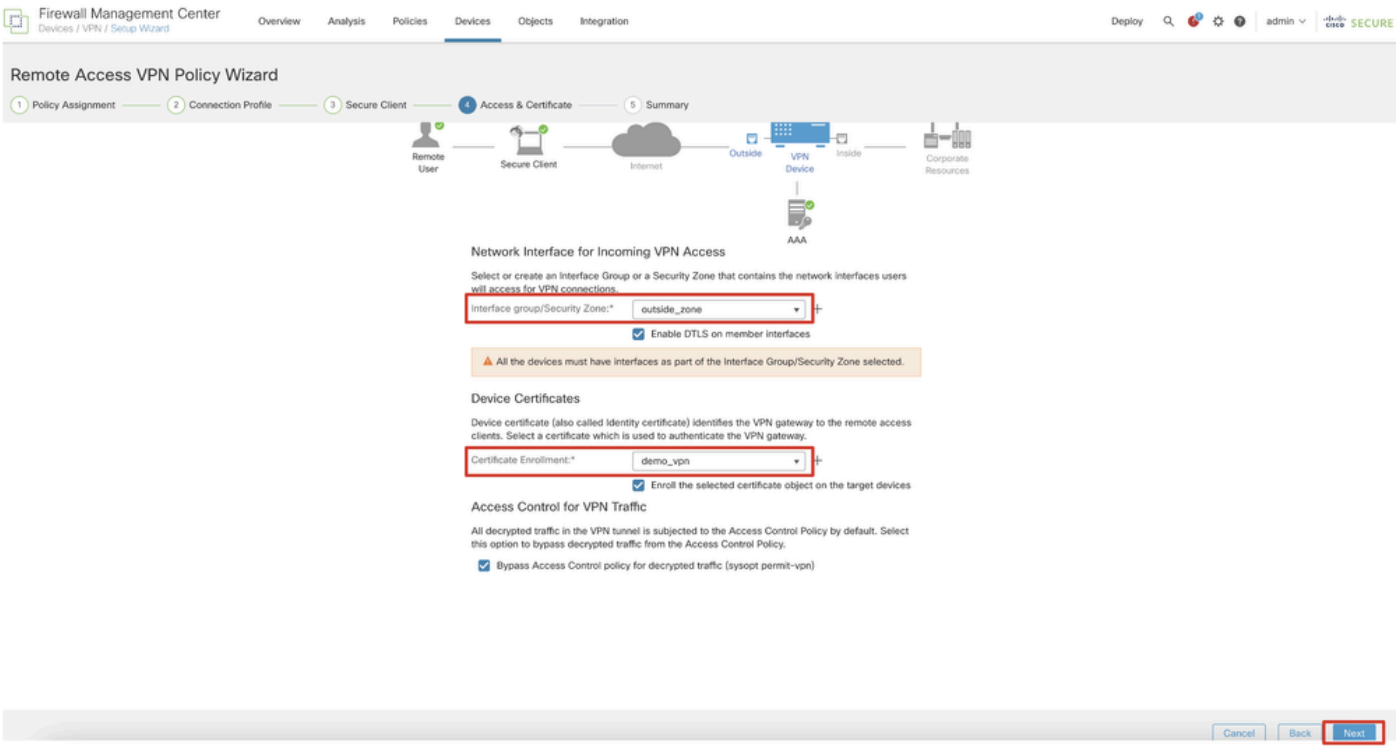
FMC_New_RAVPN_Wizard_3（推奨）

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



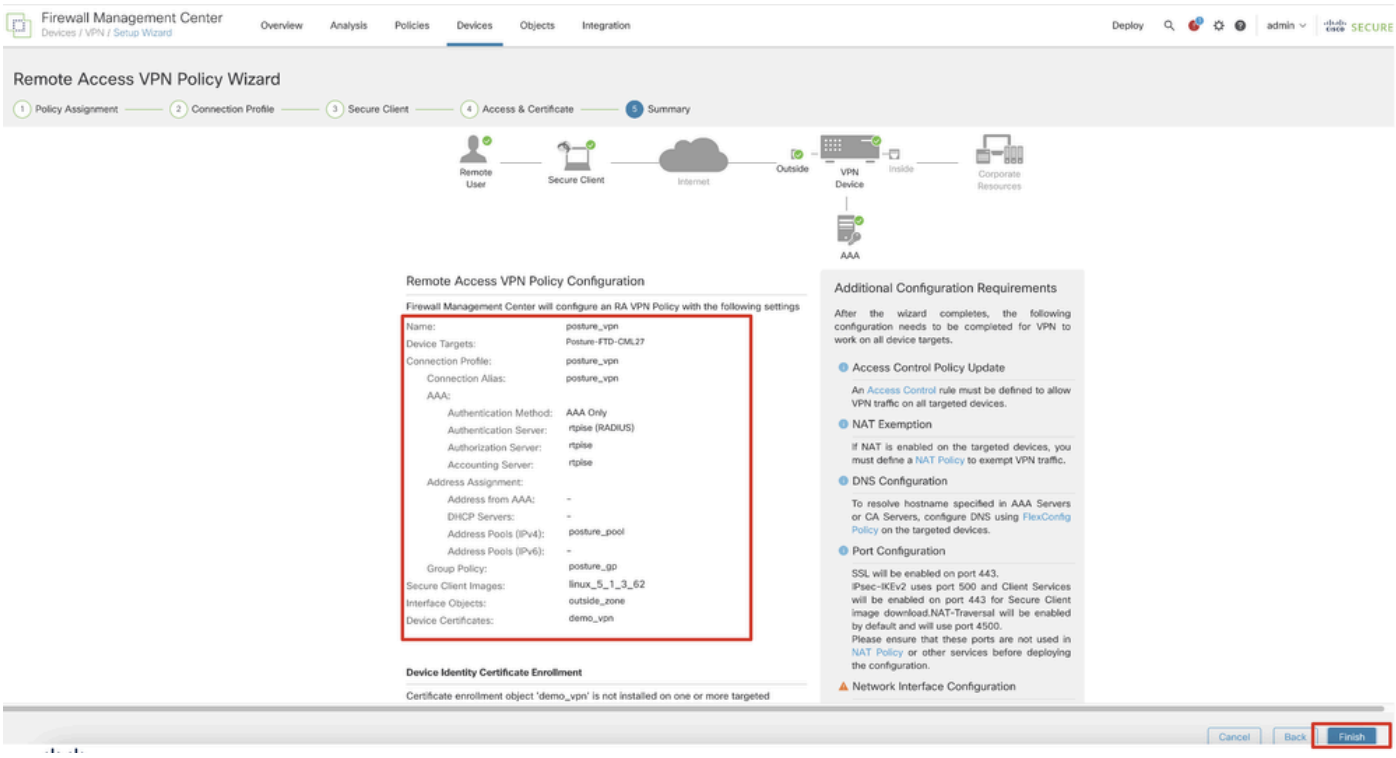
FMC_New_RAVPN_Wizard_4（推奨）

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



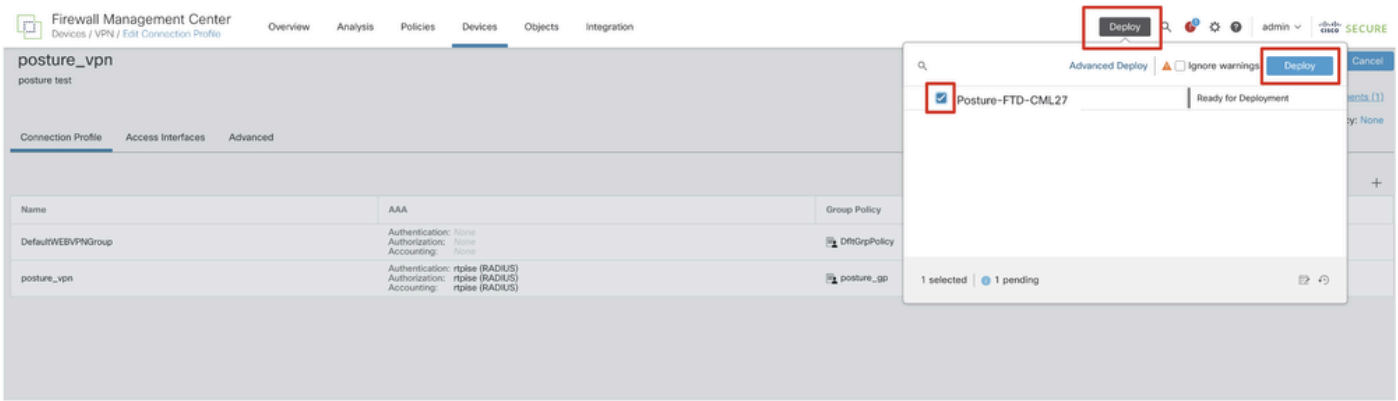
FMC_New_RAVPN_Wizard_5

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。



FMC_New_RAVPN_Wizard_6（推奨）

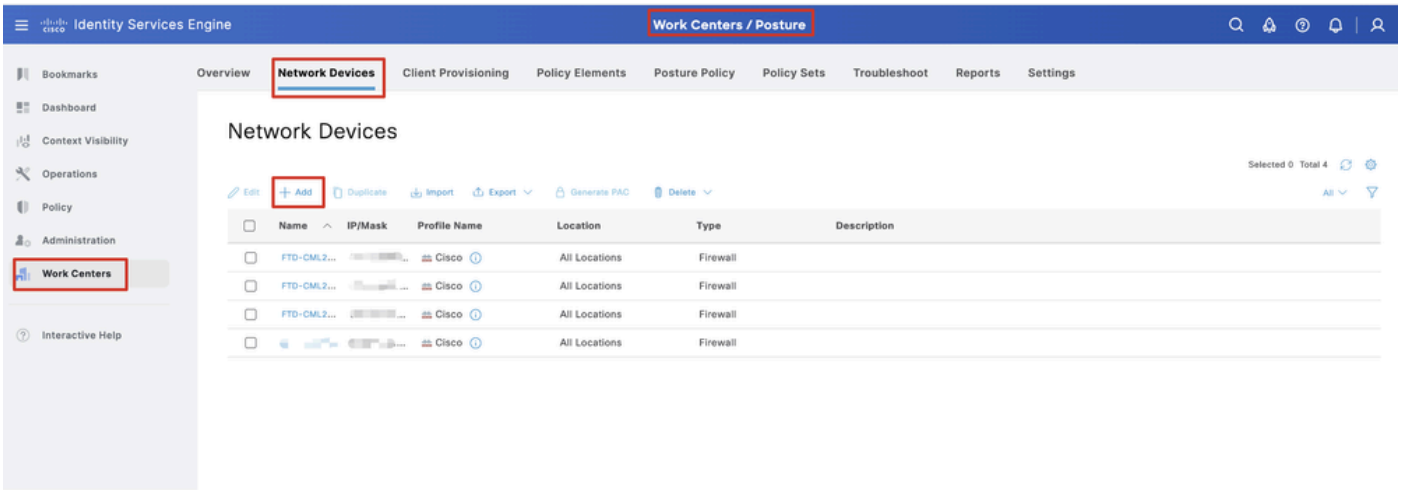
ステップ 12新しい設定をFTDに展開して、リモートアクセスVPNの設定を完了します。



FMC_Deploy_FTD

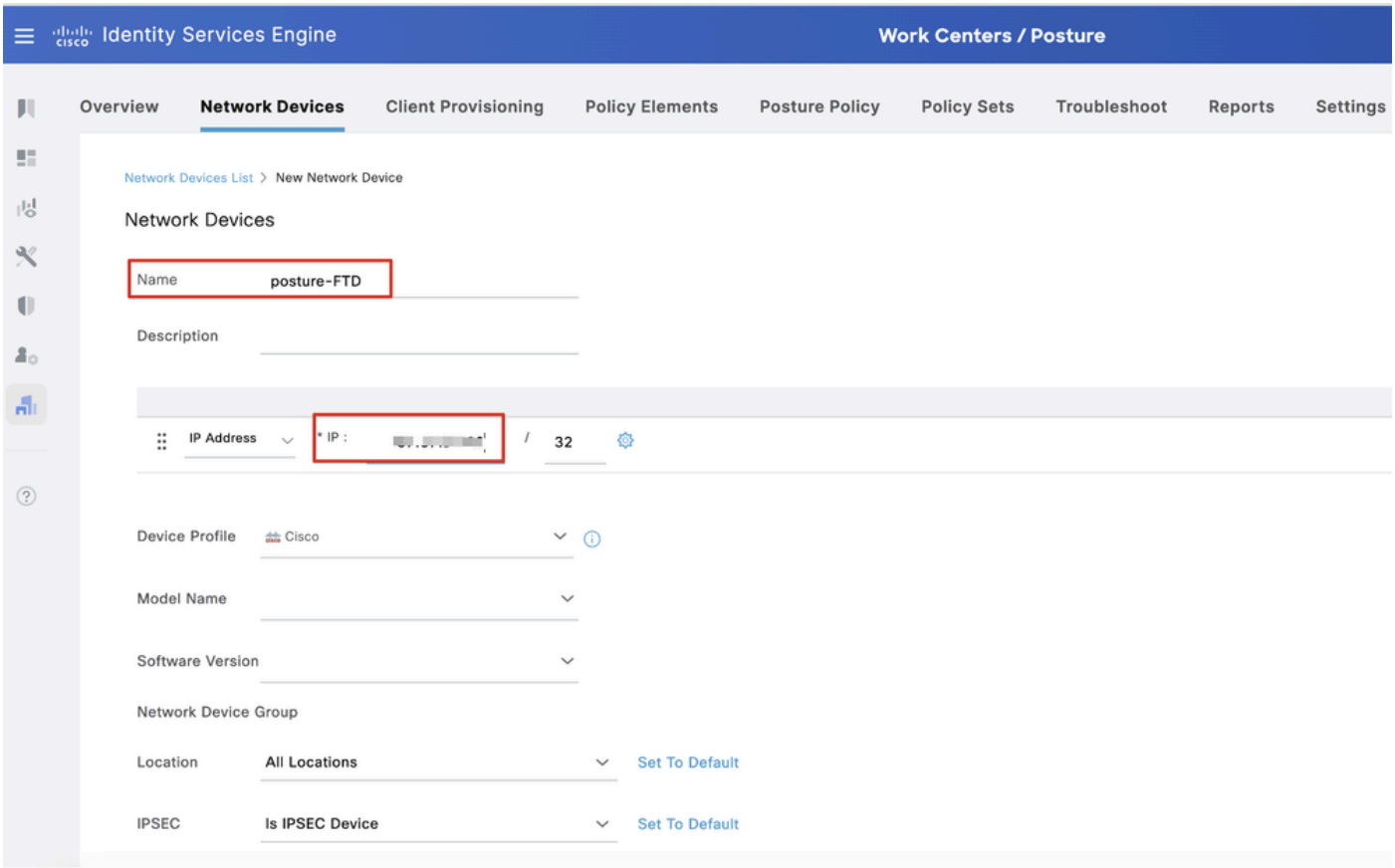
ISEでの設定

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



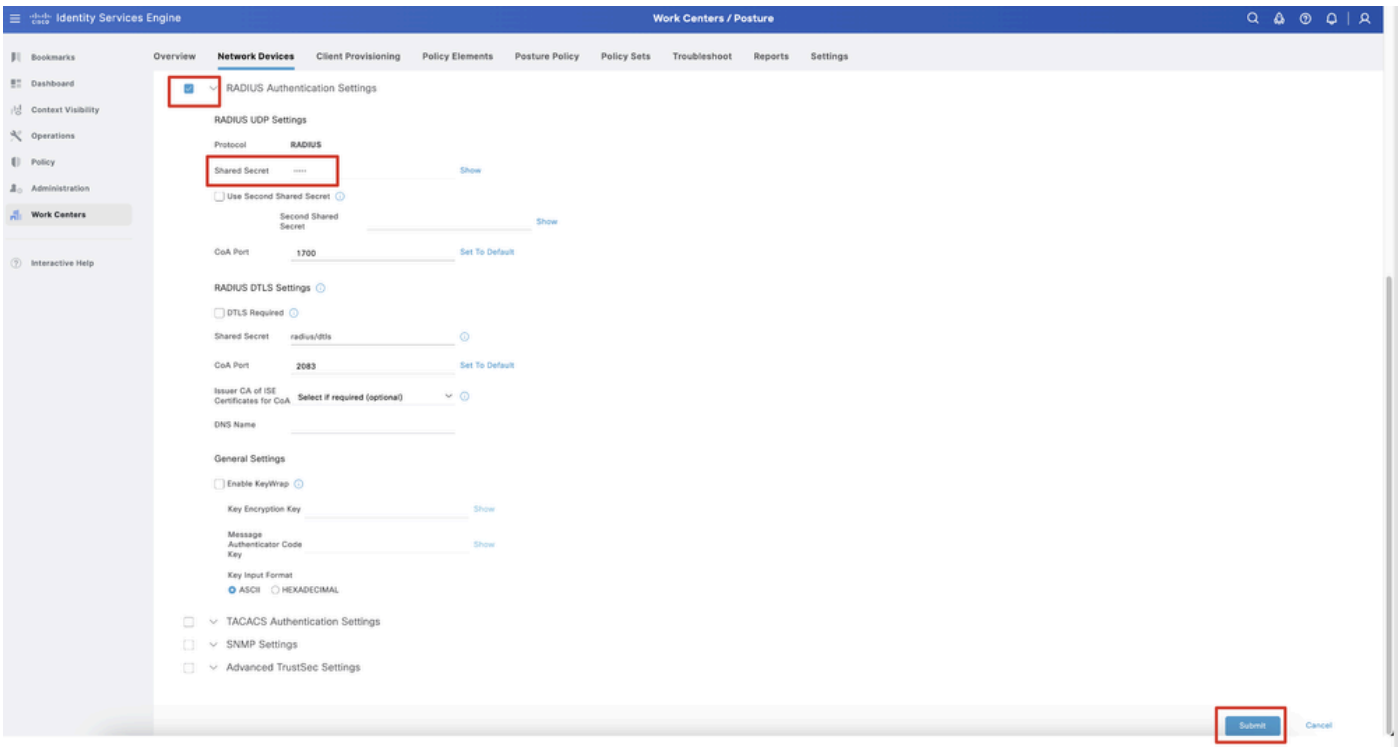
ISE_Add_New_デバイス

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。



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

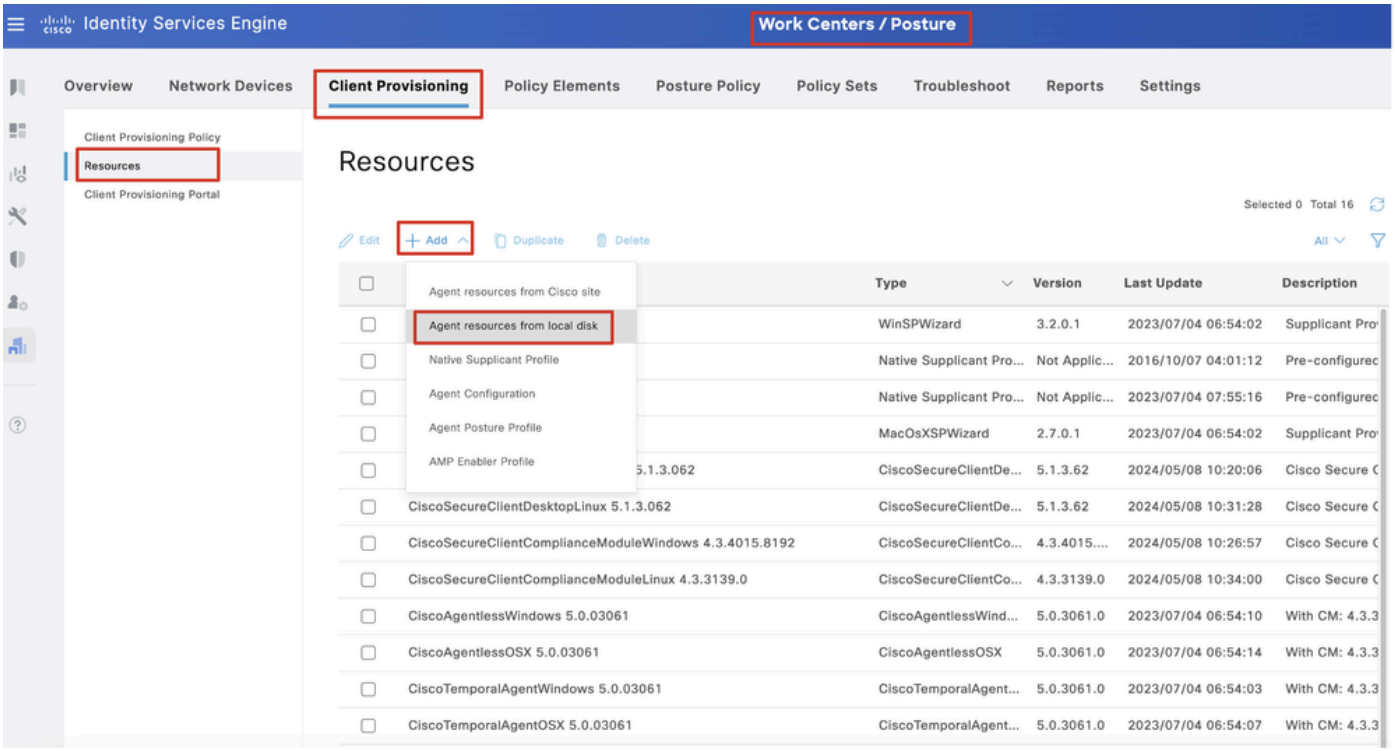


ISE_Add_New_Devices_2

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

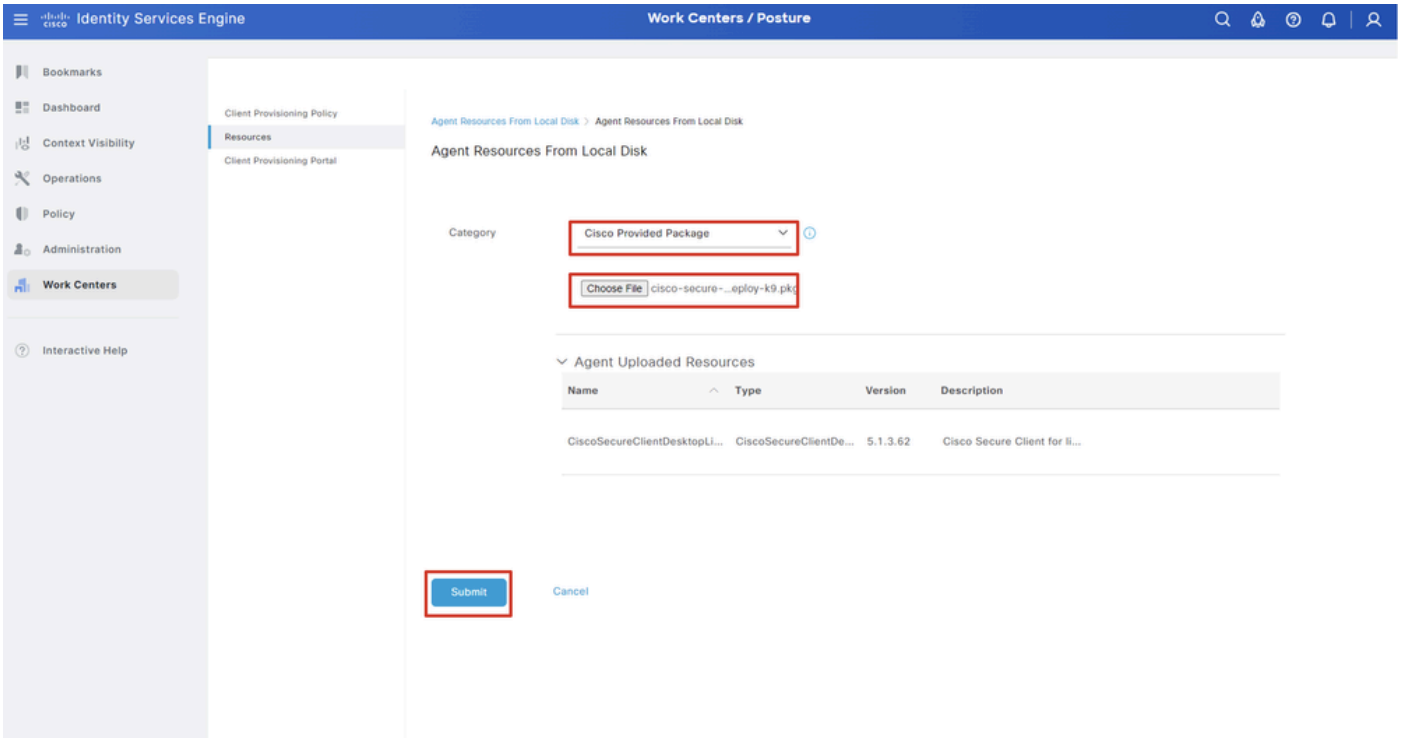
ンロードし、ダウンロードしたファイルのmd5チェックサムが[Cisco Software Download page](#)と同じであることを確認して、ファイルの状態が良好であることを確認します。 パッケージ名cisco-secure-client-linux64-5.1.3.62-webdeploy-k9.pkgは手順1で正常にダウンロードされました。

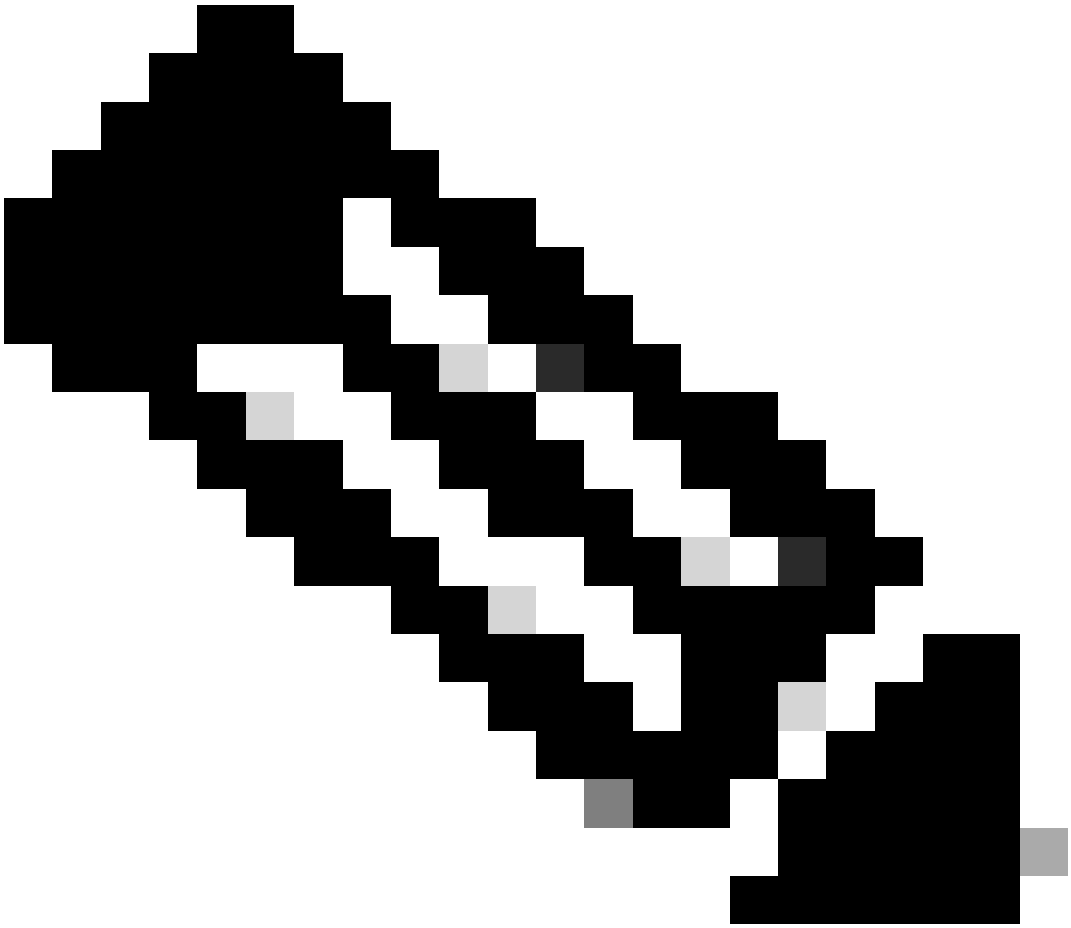
ステップ 15： Work Centers > Posture > Client Provisioning > Resourcesに移動します。をクリックします。AddAgent resources from local diskを選択します。



ISE_Upload_Resource

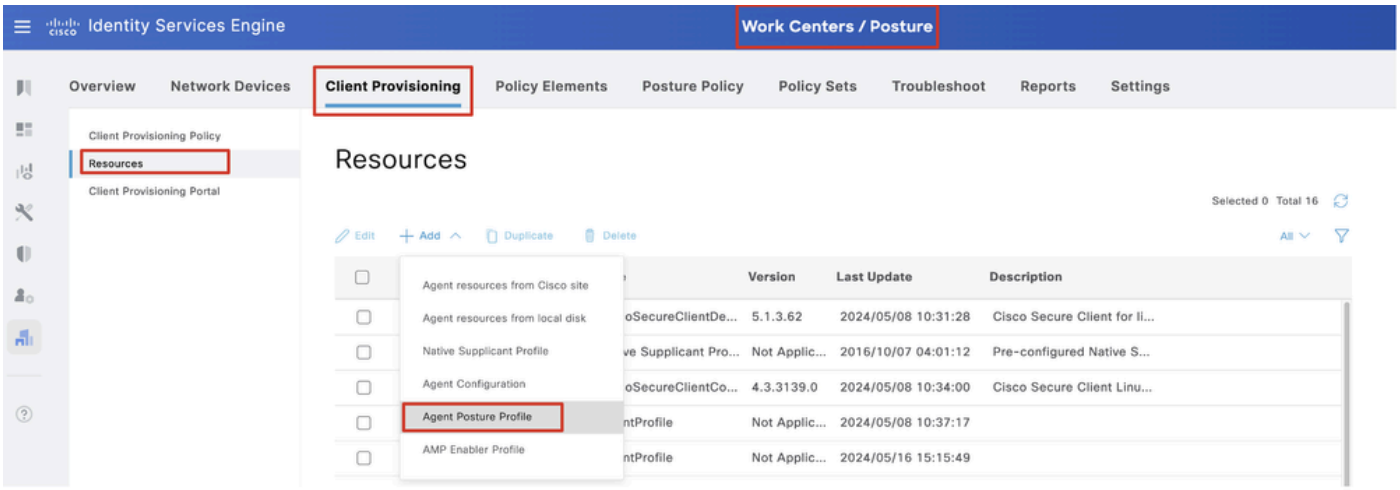
ステップ 15.1：Cisco Provided Packageを選択します。Choose Fileをクリックして、cisco-secure-client-linux64-5.1.3.62-webdeploy-k9.pkgをアップロードします。をクリックします。Submit





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。

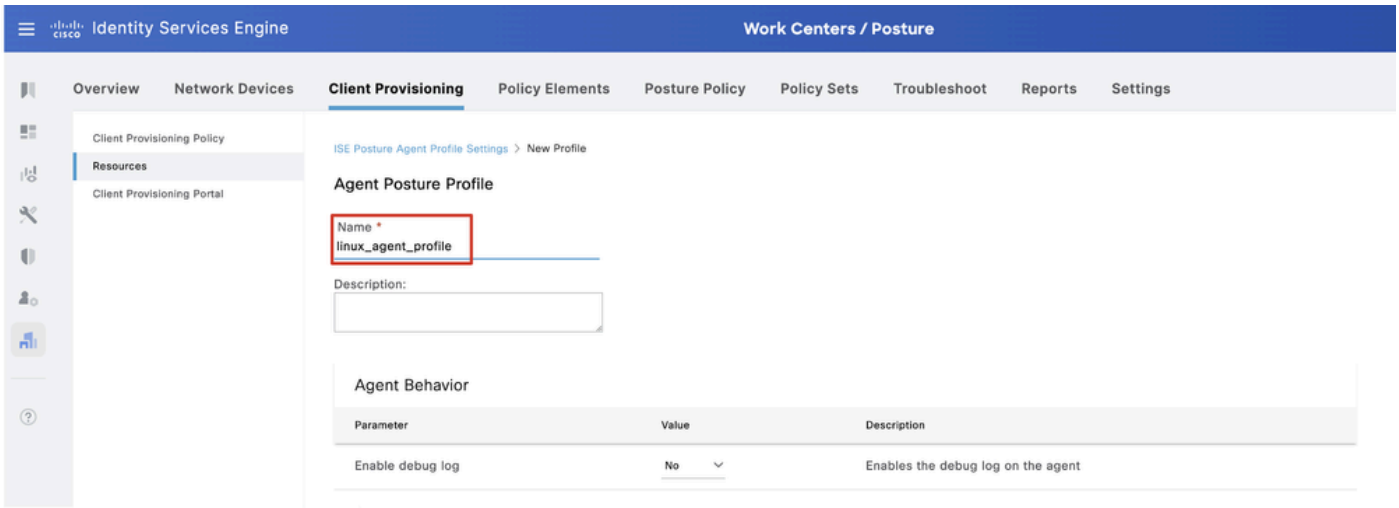


ISE_Add_Agent_Posture_プロファイル

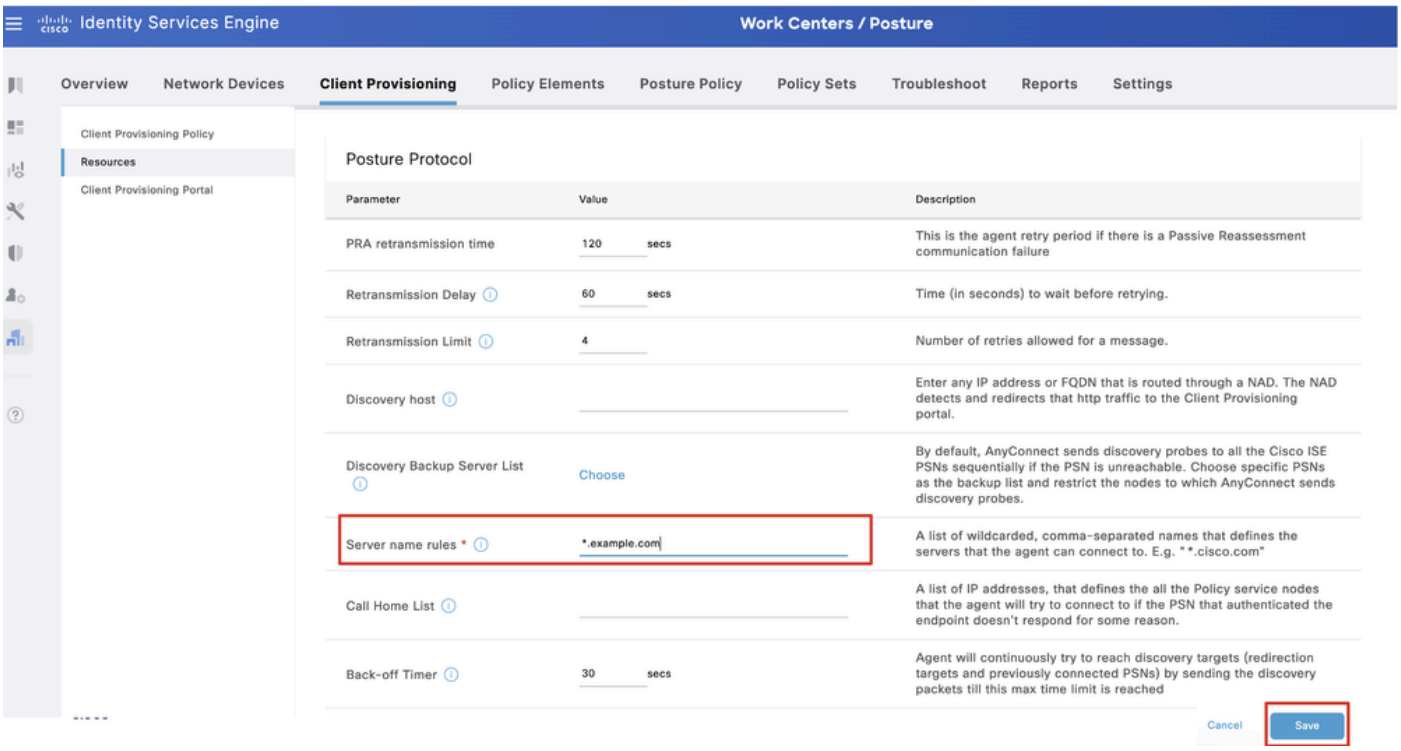
ステップ 16.1：Name, Server name rulesを指定し、その他はデフォルトのままにします。をクリックします。Save

名前： linux_agent_profile

サーバー名の規則： *.example.com

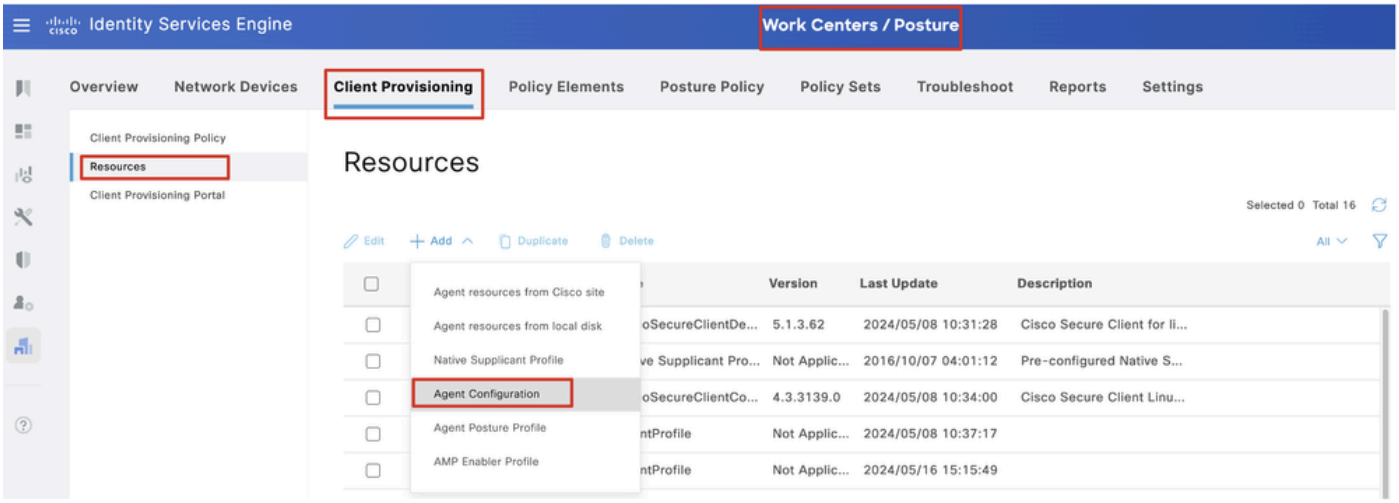


ISE_追加_エージェント_ポスチャ_プロファイル_1



ISE_追加_エージェント_ポスチャ_プロファイル_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

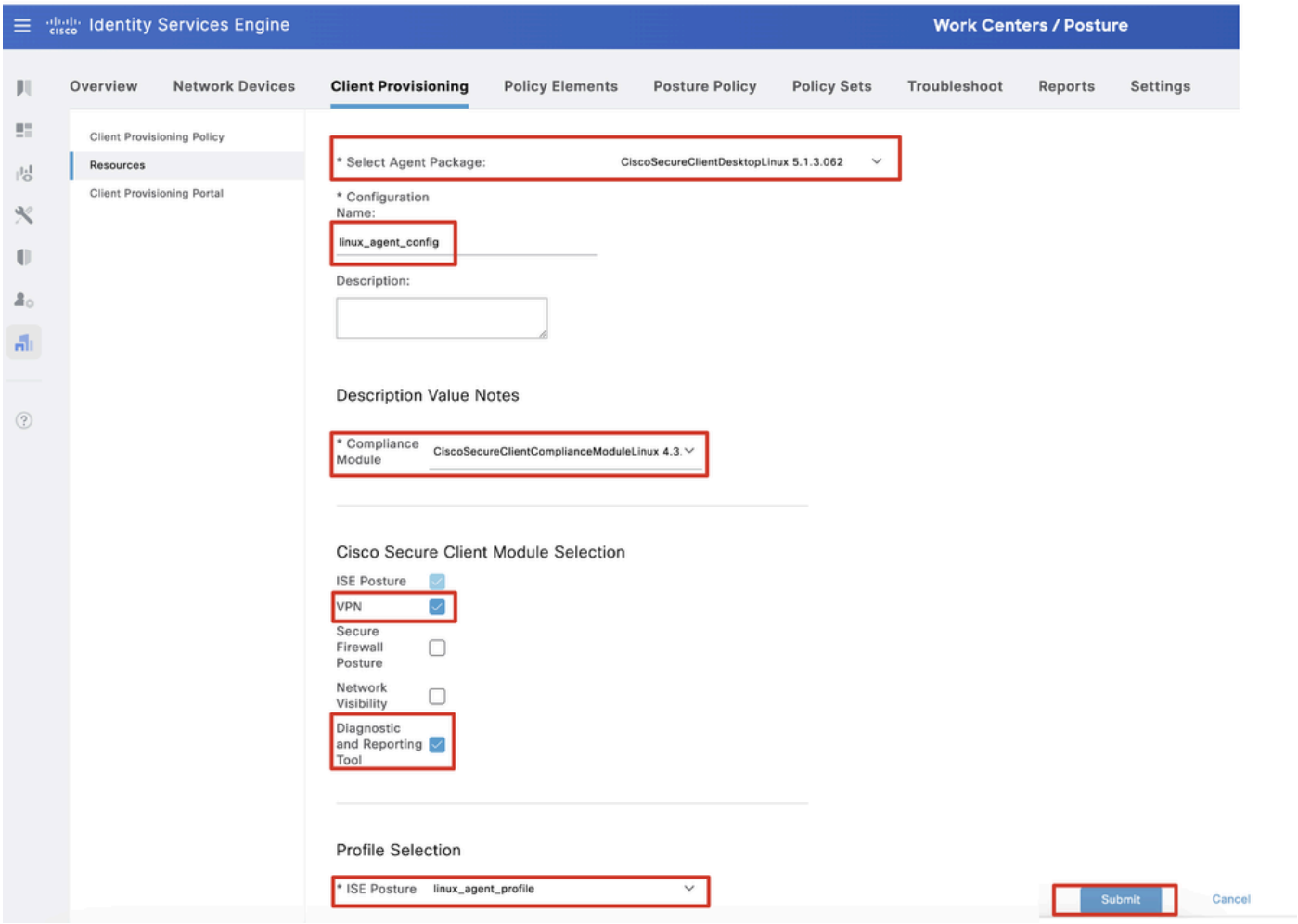
名前： linux_agent_config

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

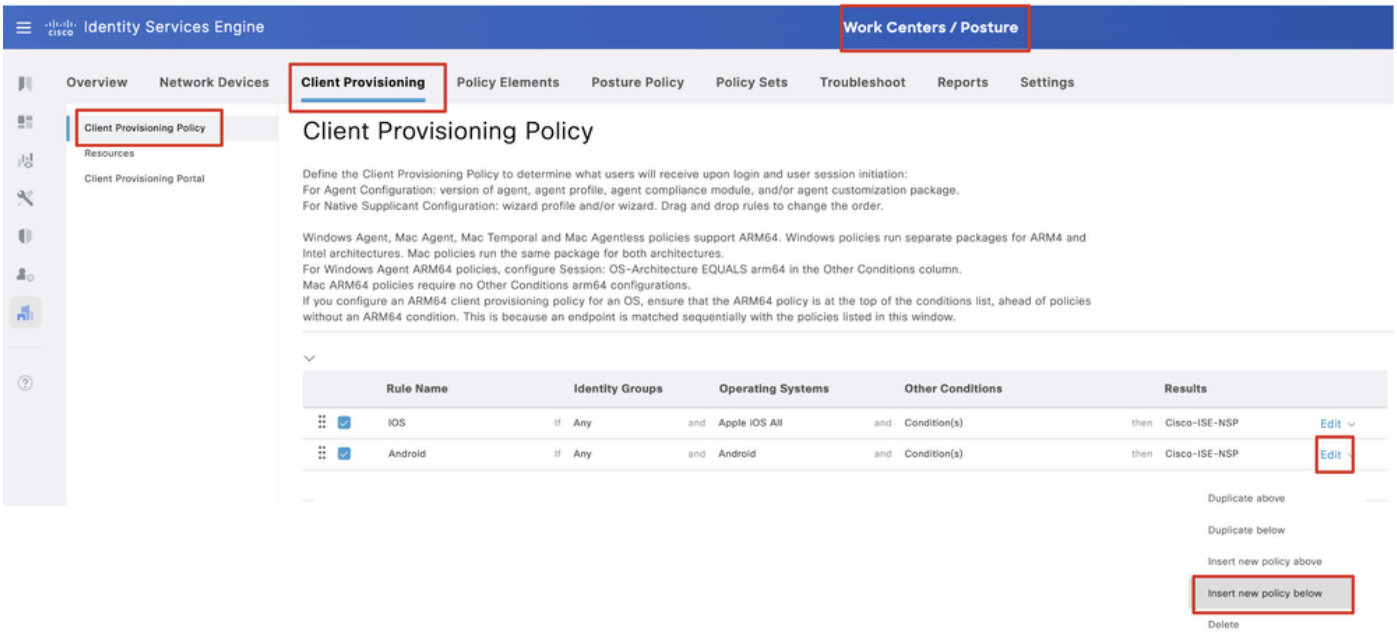
プロファイル選択ISEポスチャ：linux_agent_profile

をクリックします。Submit



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。



*ISE_Add_New_Provisioning_*

ポリシー

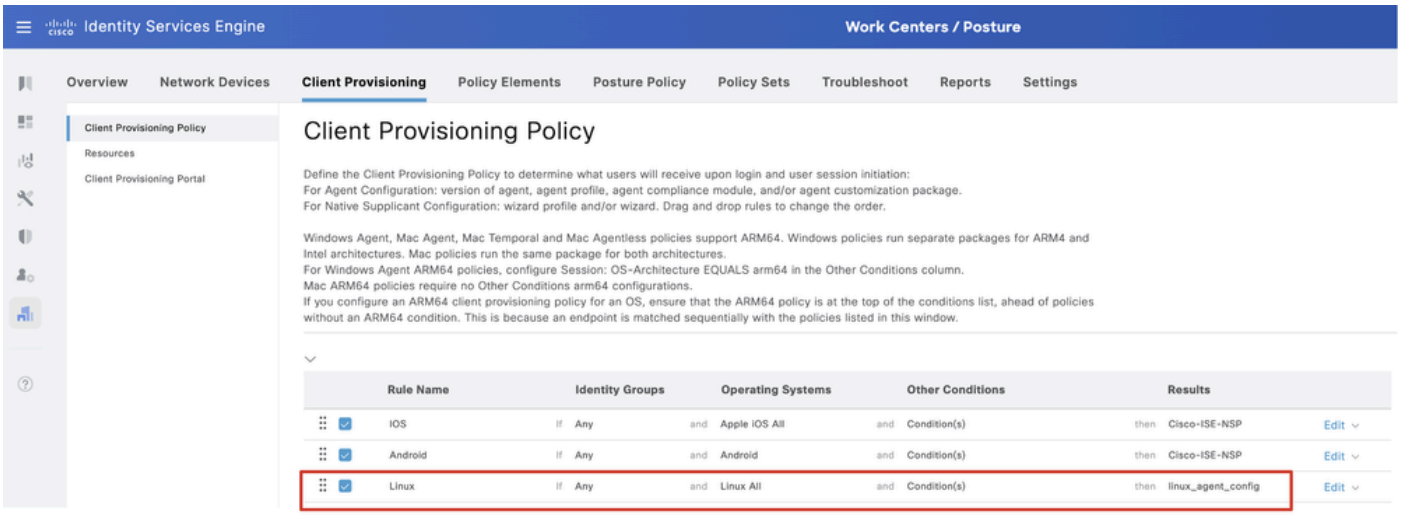
ステップ 18.1： 詳細を設定します。

ルール名： Linux

オペレーティングシステム：すべてLinux

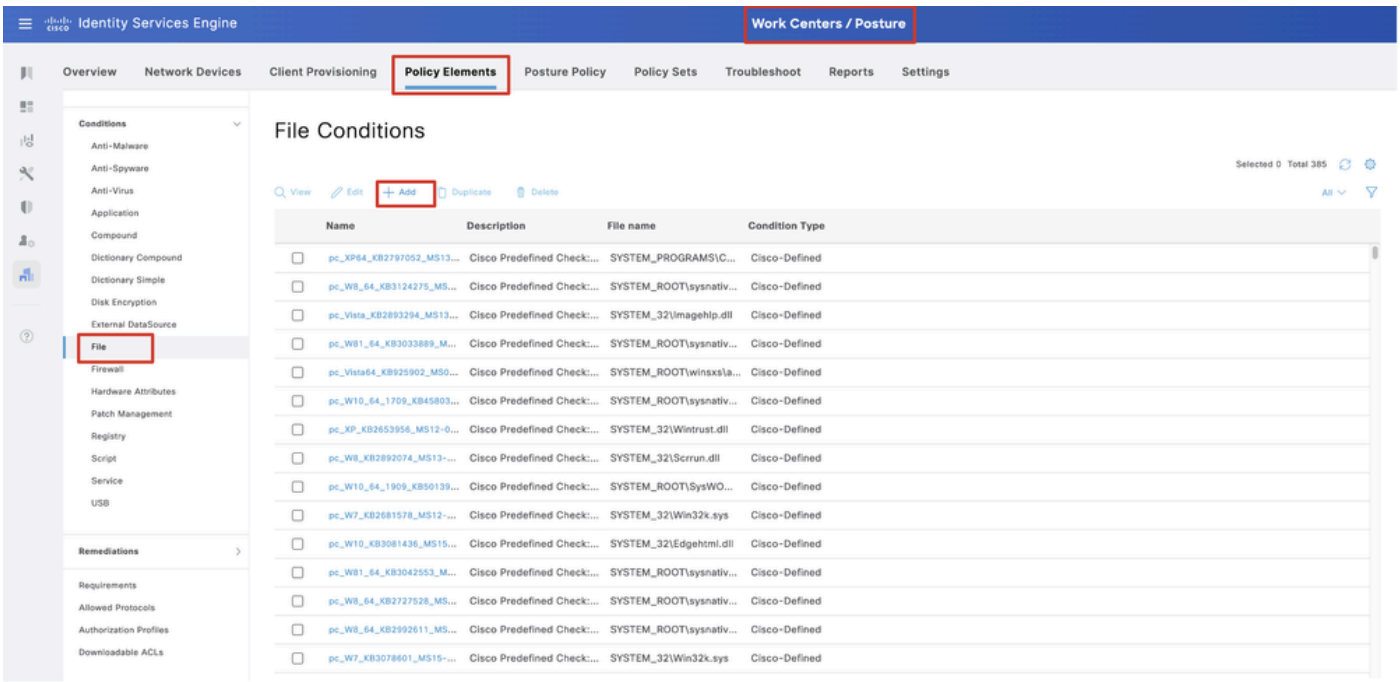
結果： linux_agent_config

Done およびSaveをクリックします。



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



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

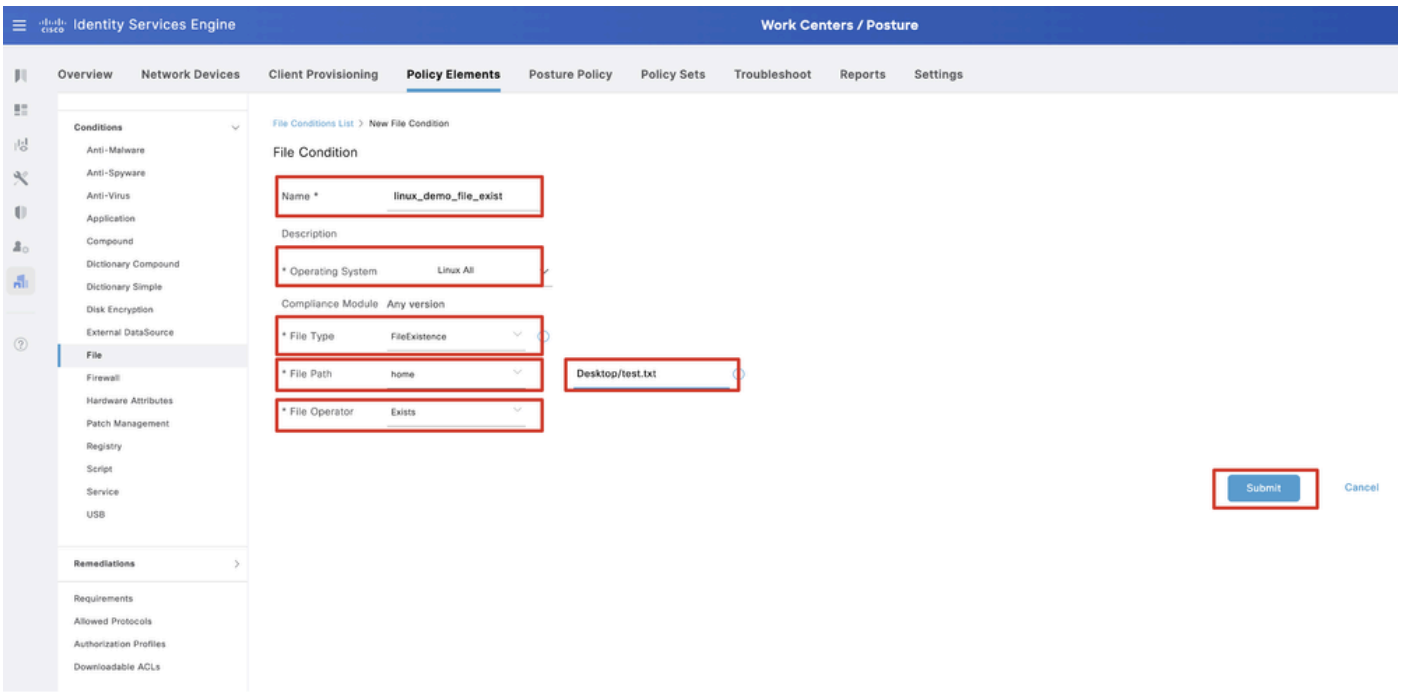
オペレーティングシステム：すべてLinux

ファイルの種類： FileExistence

ファイルパス：home、Desktop/test.txt

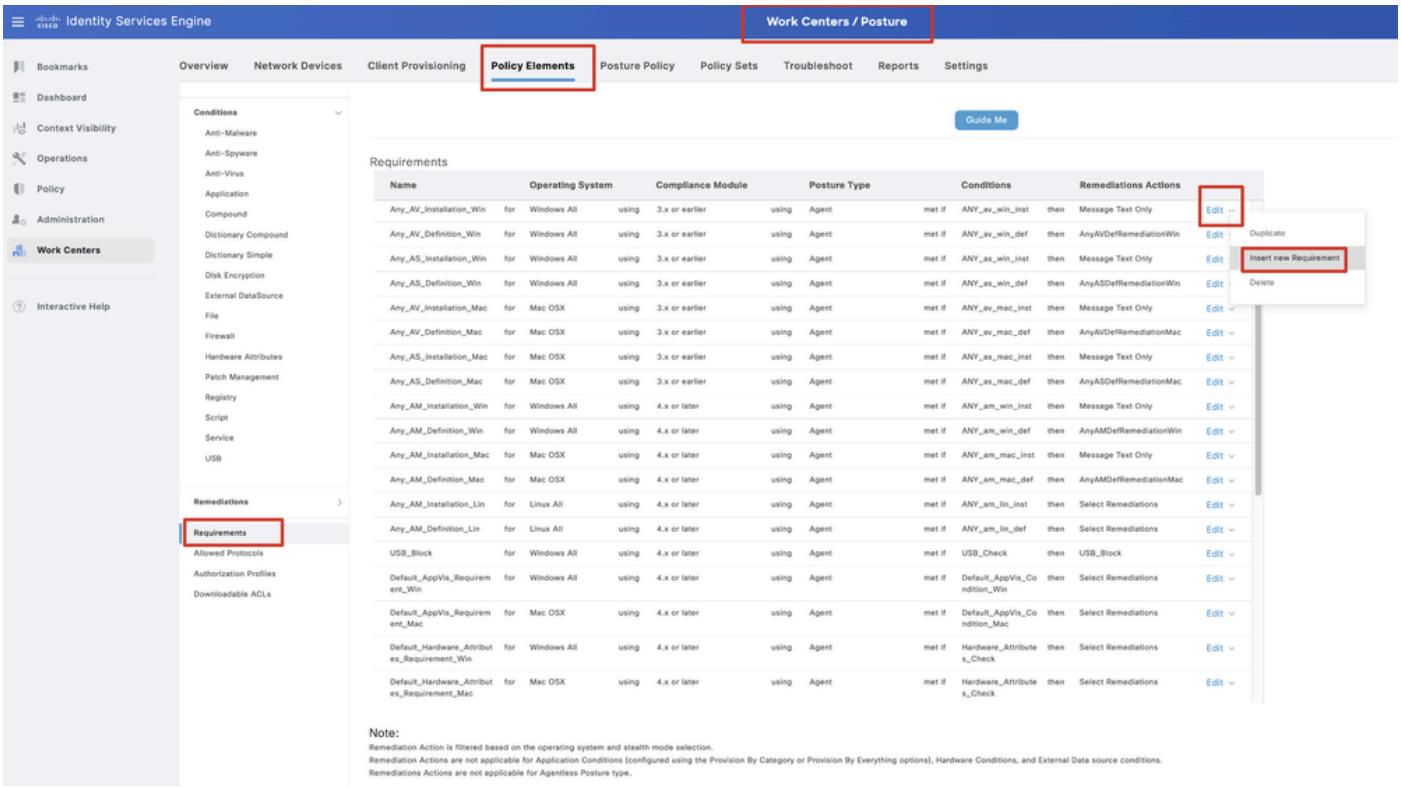
ファイル演算子：存在します

をクリックします。Submit



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。



ISE_Add_New_Posture_Requirement

ステップ 20.1： 詳細を設定します。

名前： Test_exist_linux

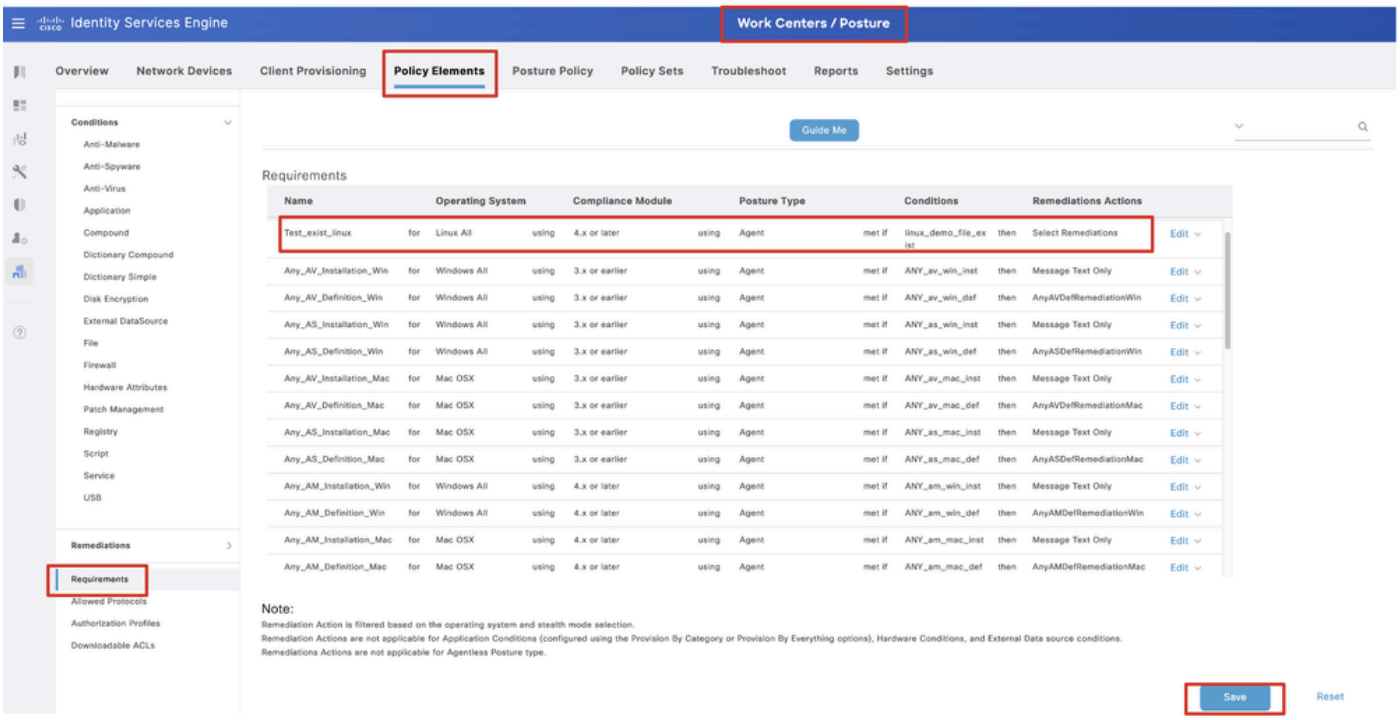
オペレーティングシステム：すべてLinux

コンプライアンスモジュール：4.x以降

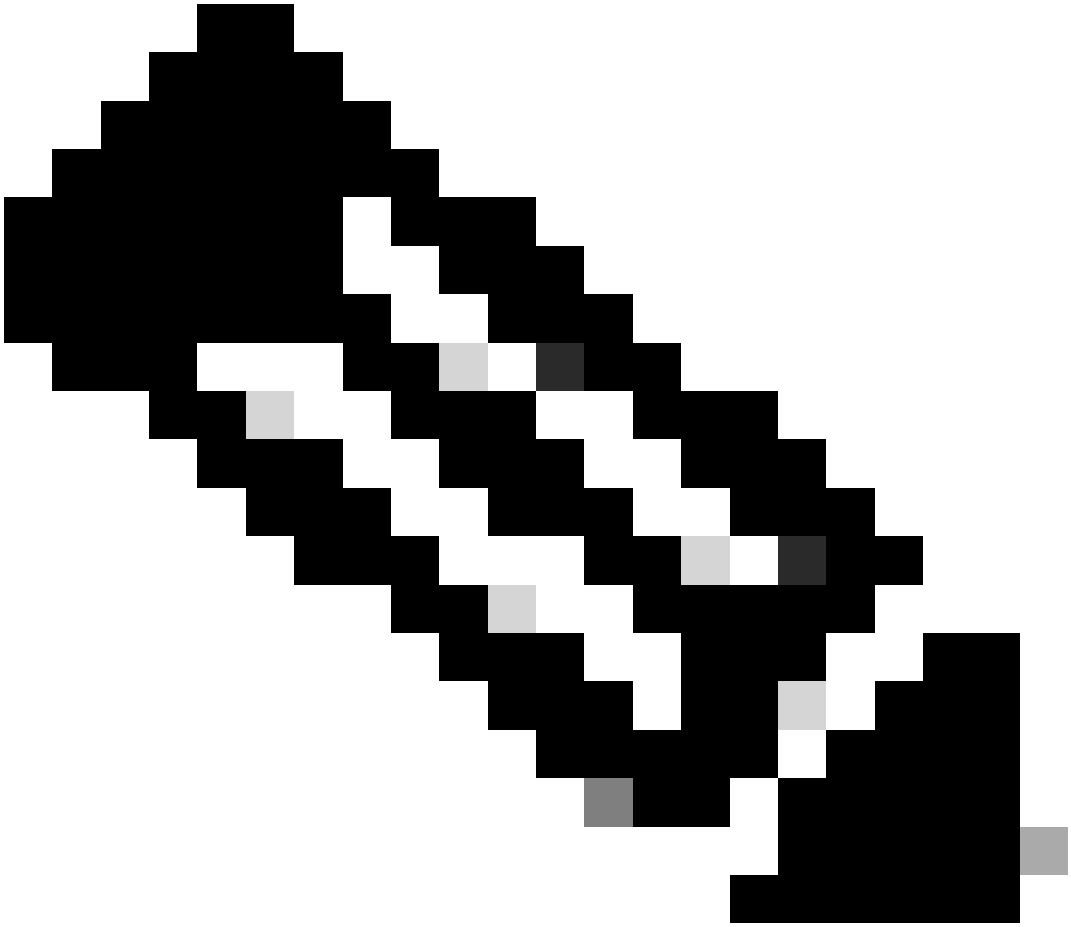
ポスチャタイプ：Agent

条件： linux_demo_file_exist

Done およびSaveをクリックします。



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。

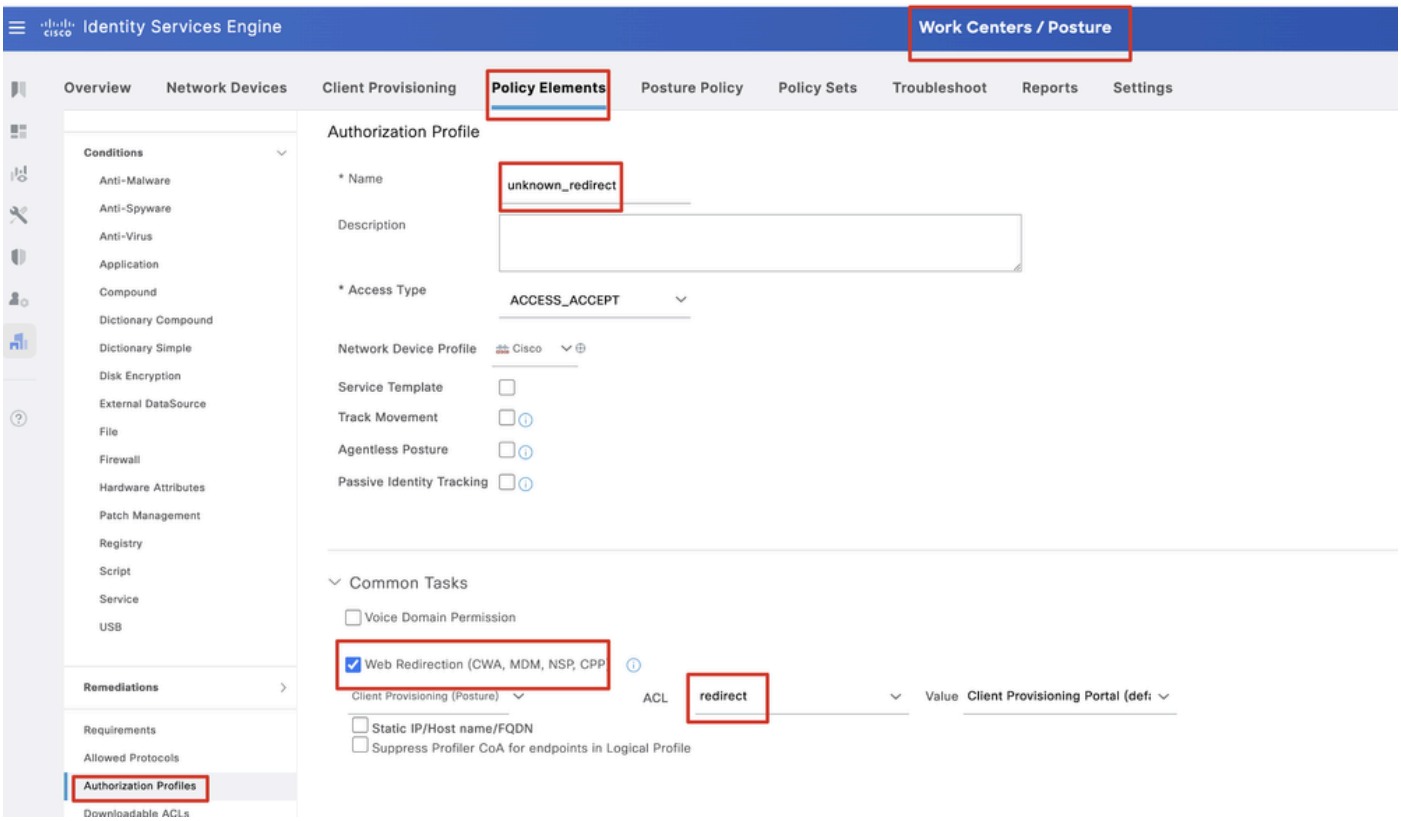
名前：unknown_redirect

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

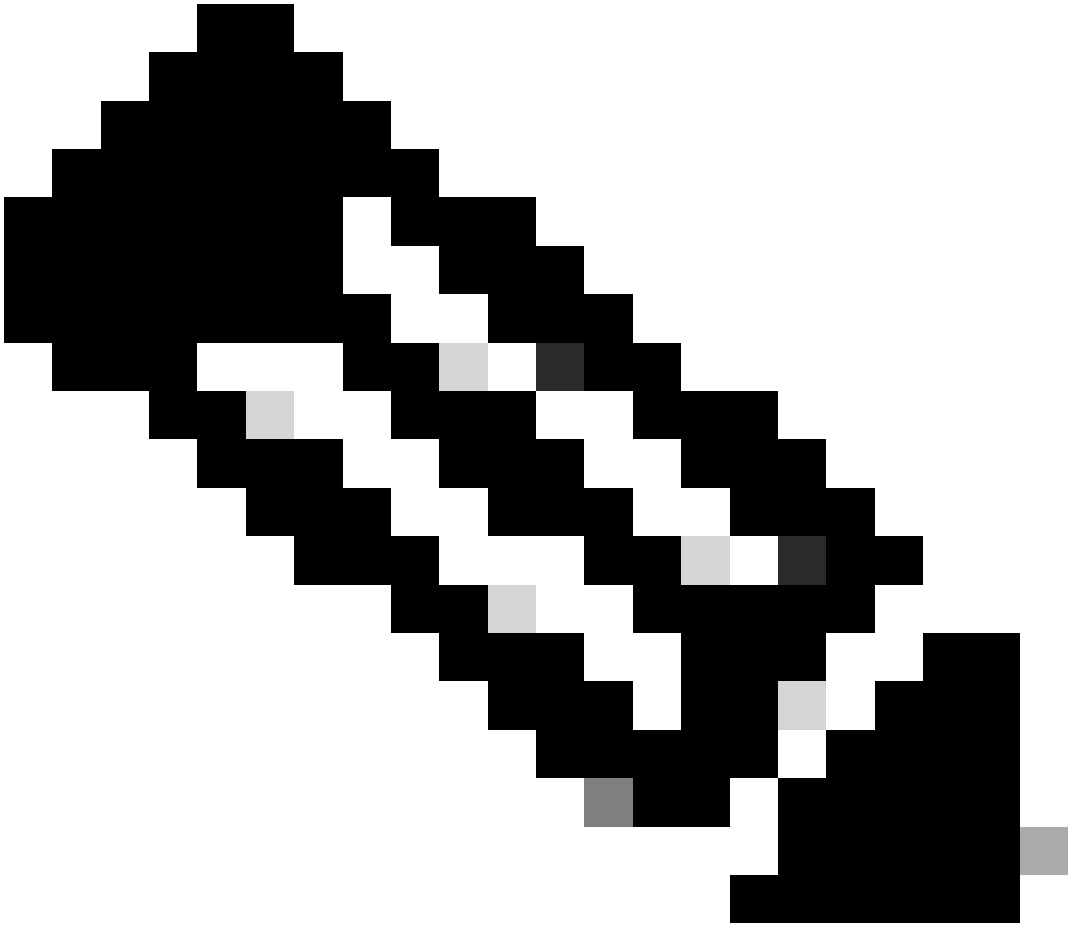
選択 Client Provisioning(Posture)

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）



*ISE_Add_New_Authorization_*プロファイル_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。

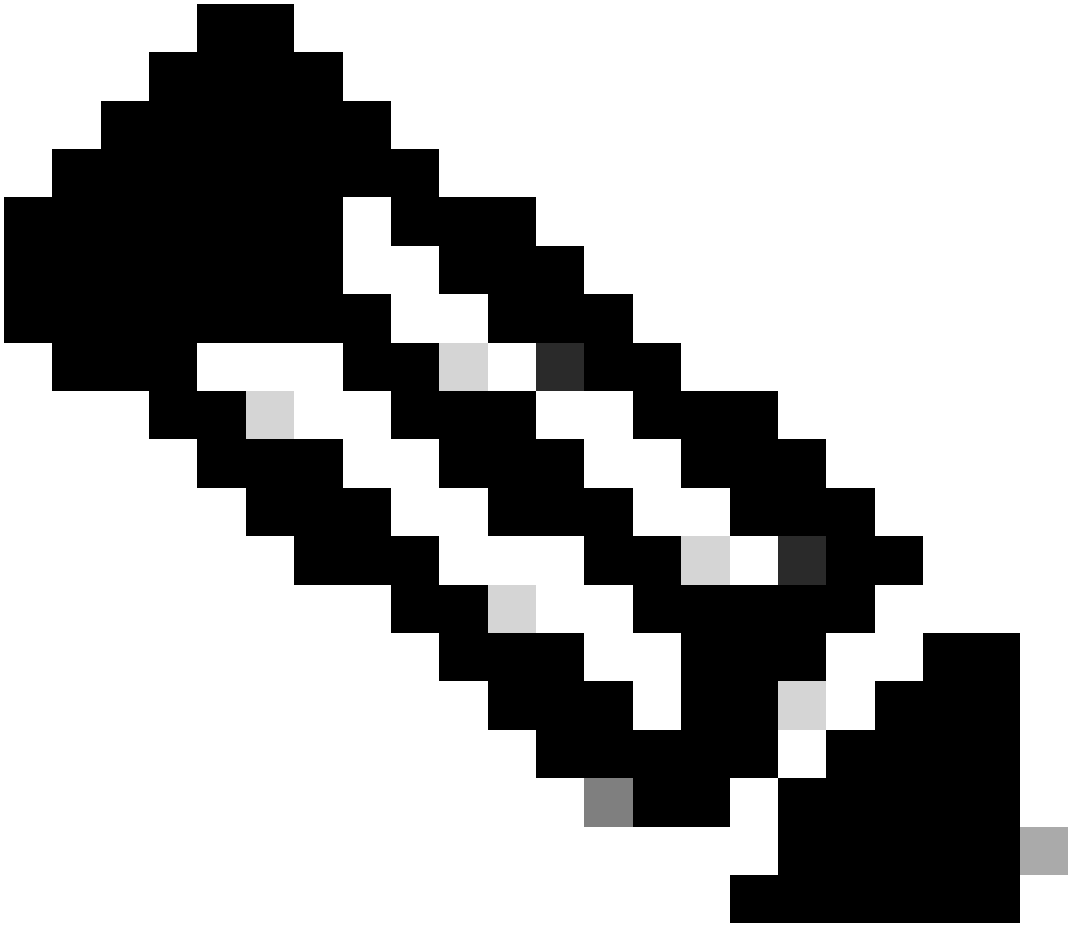
ステップ 21.2：Add を繰り返し、詳細を含む、準拠していないエンドポイントと準拠しているエンドポイント用に別の2つの認可プロファイルを作成します。

名前： non_compliant_profile

DACL名：DENY_ALL_IPv4_TRAFFIC

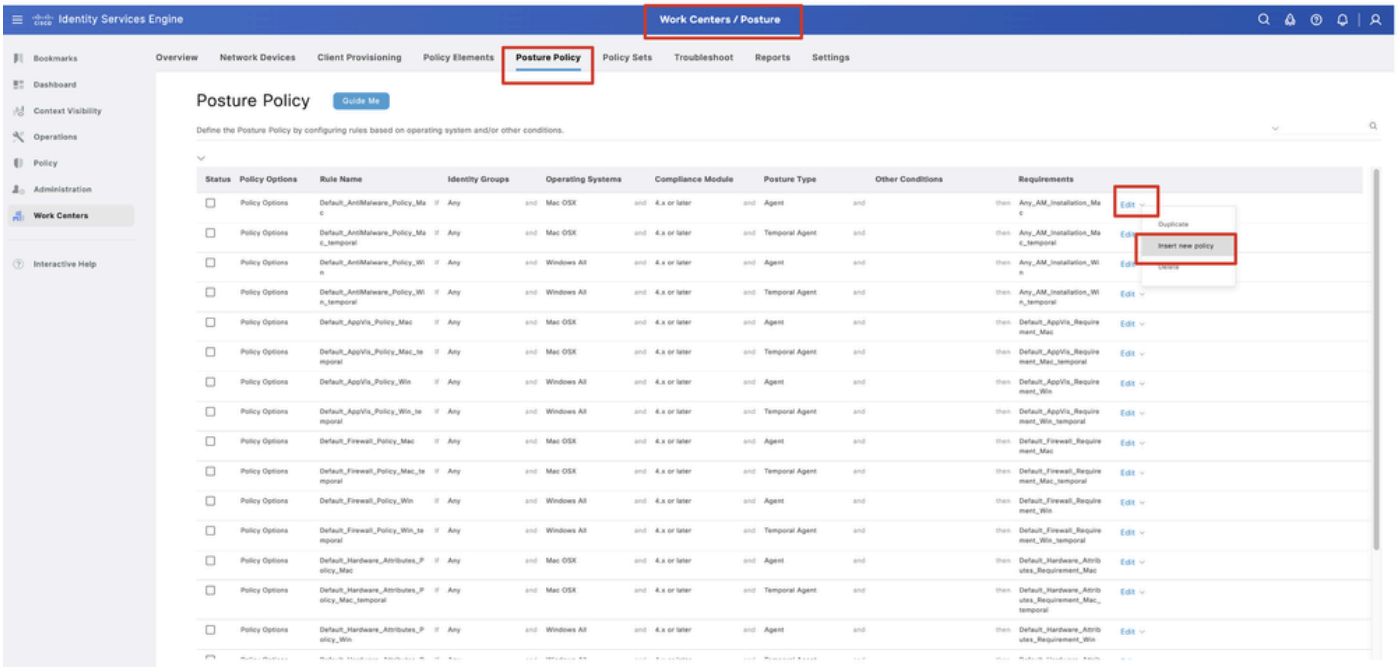
名前： compliant_profile

DACL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。



*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

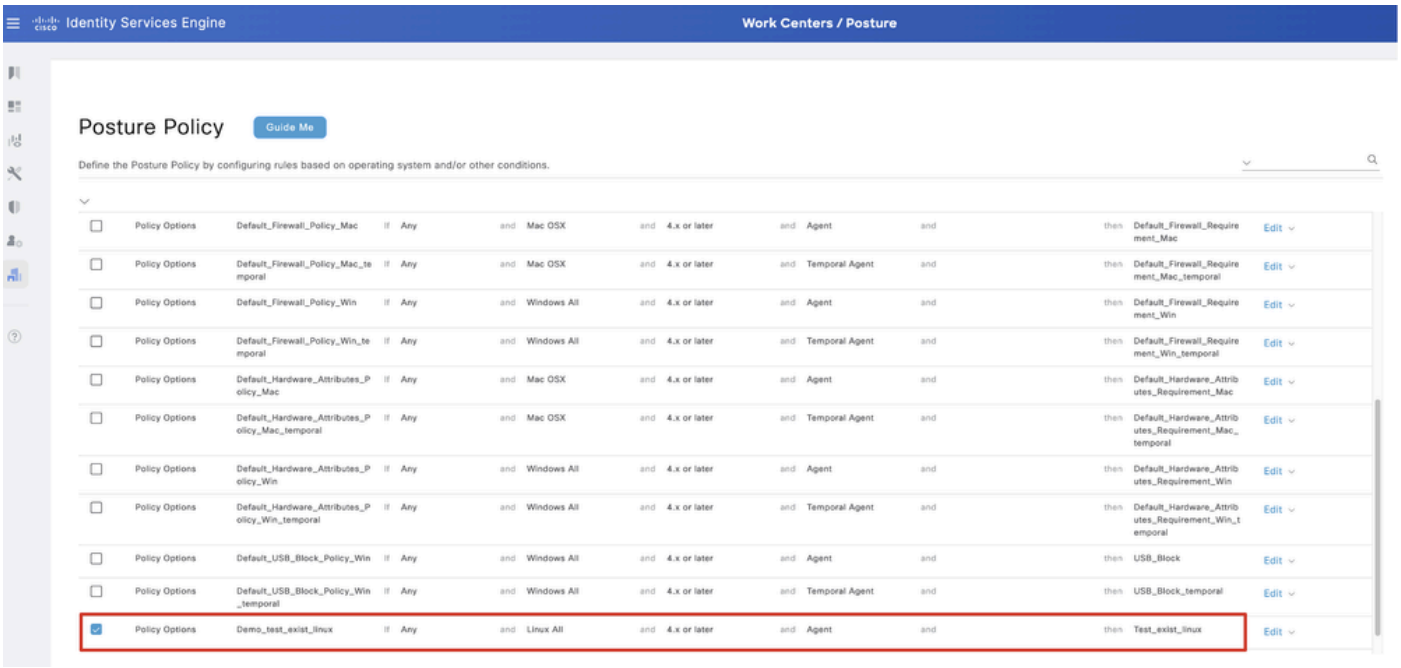
オペレーティングシステム：すべてLinux

コンプライアンスモジュール：4.x以降

ポスチャタイプ：Agent

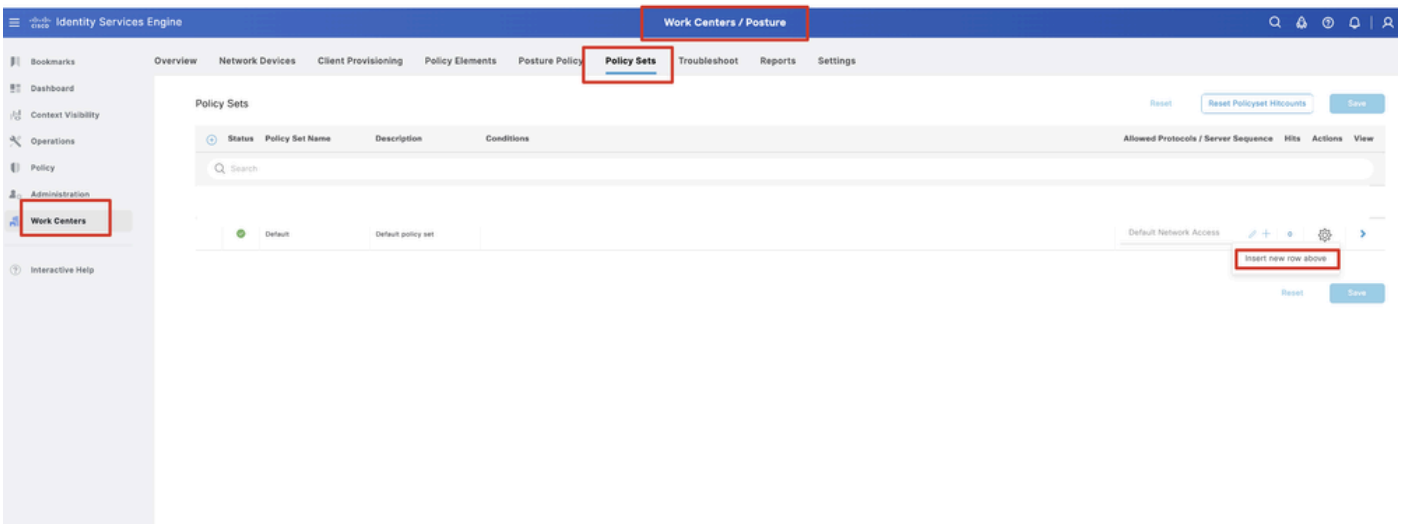
要件：Test_exist_linux

Done およびSaveをクリックします。



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。



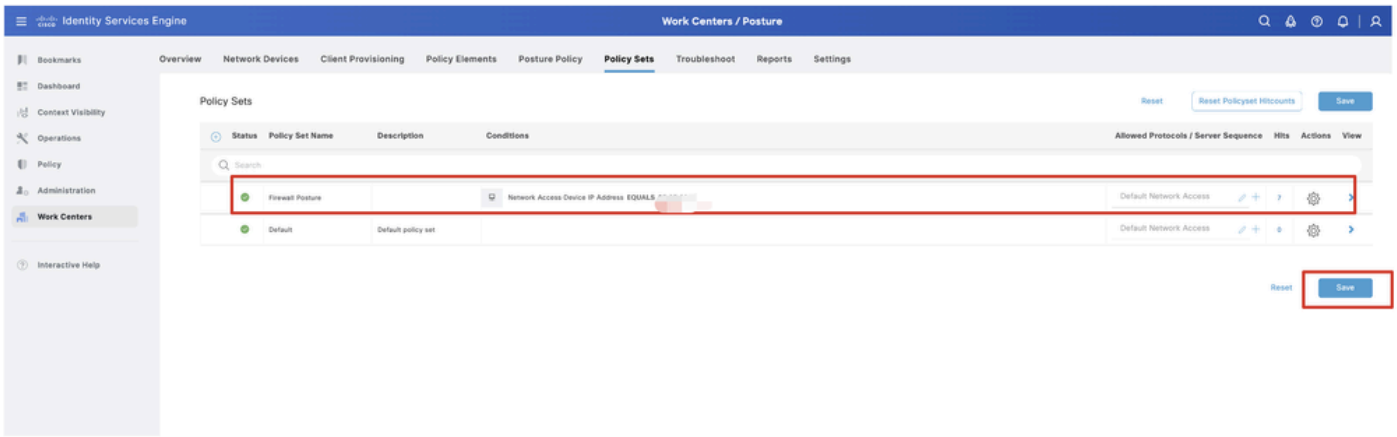
ISE_Add_New_ポリシー_セット

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



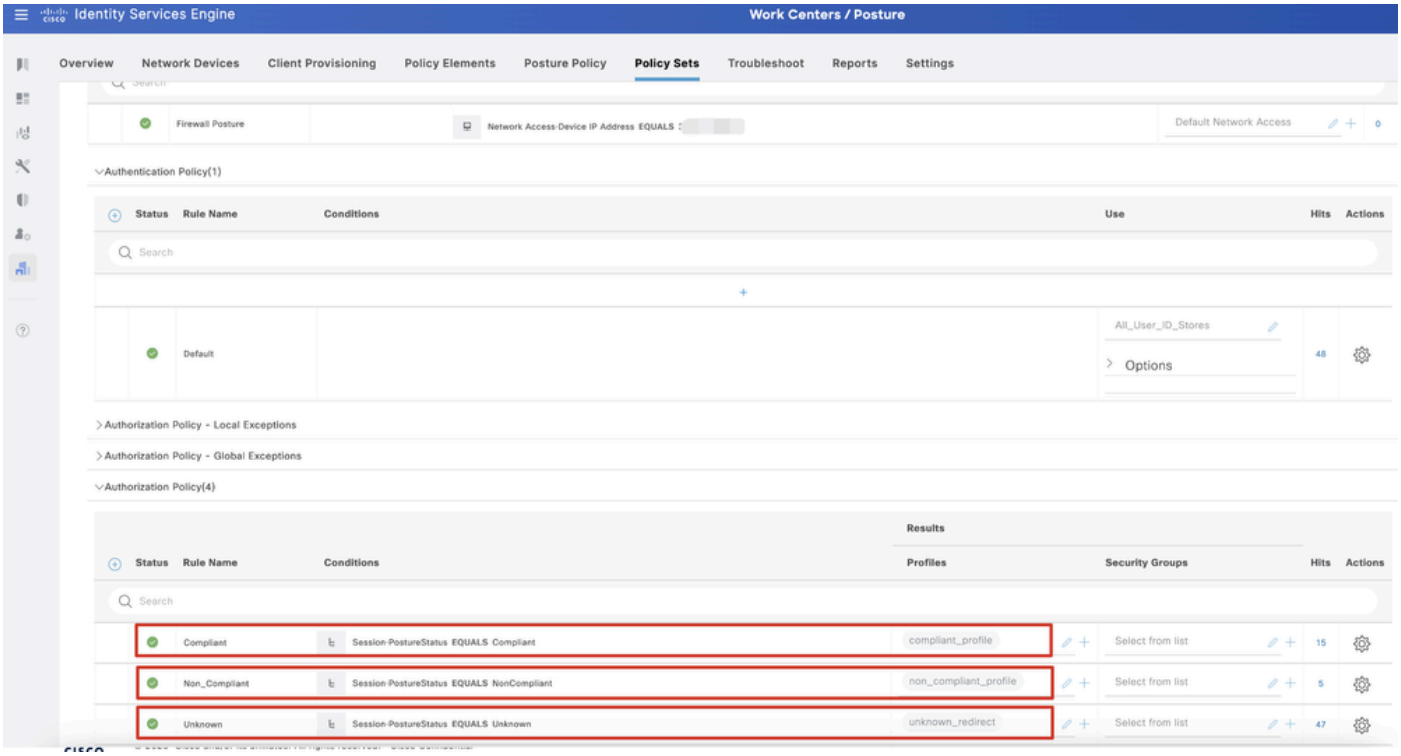
ISE_Add_New_Policy_Set_1

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

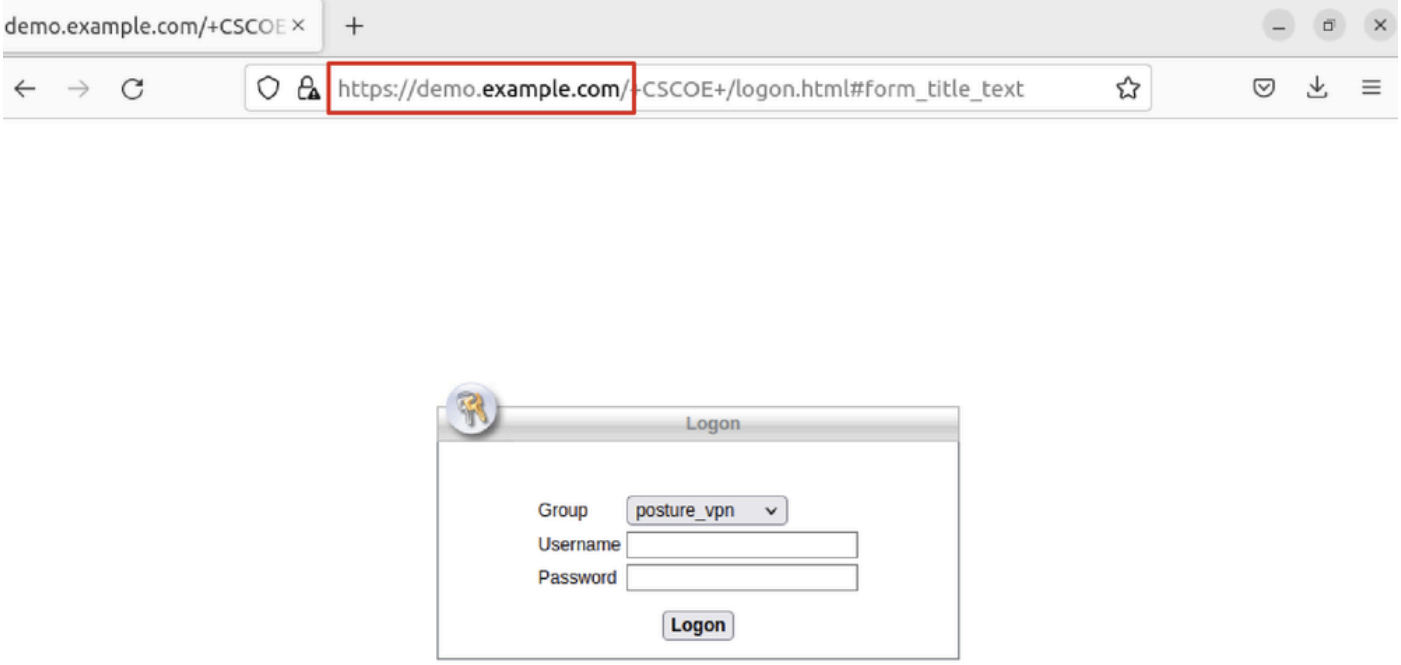
unknown_redirectによる不明



ISE_Add_New_Policy_Set_2

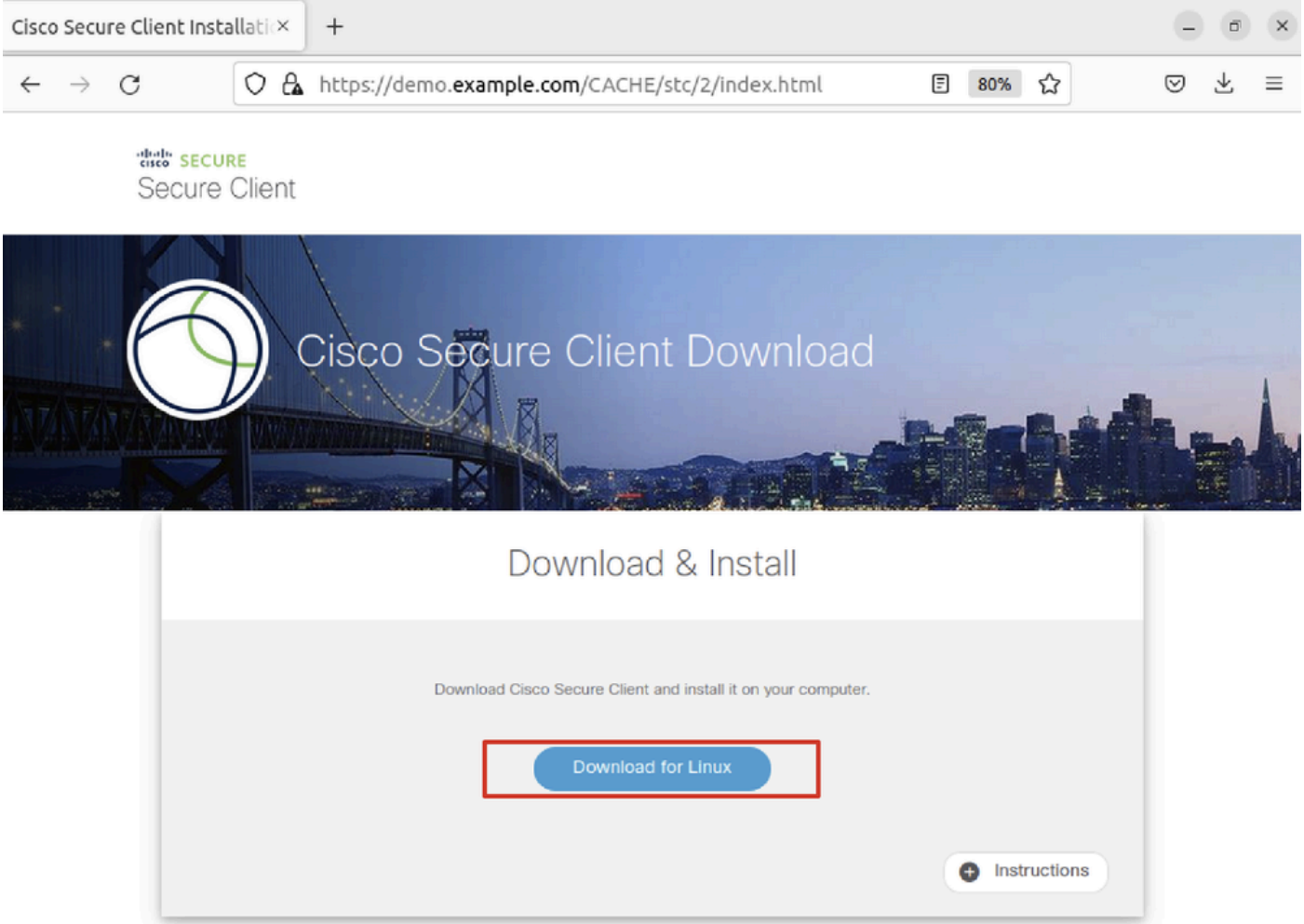
Ubuntuでの設定

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。



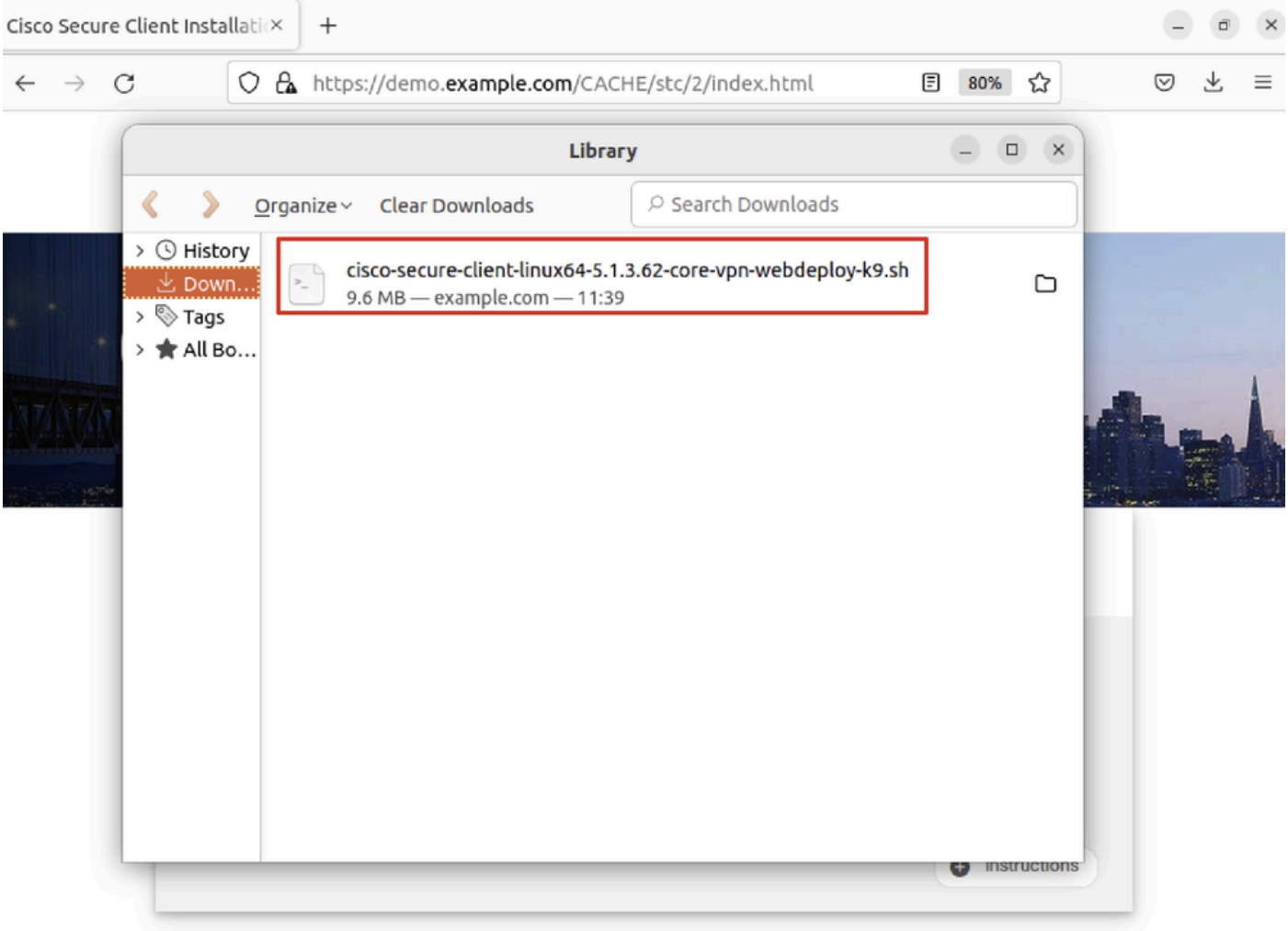
Ubuntu_Browser_VPN_ログイン

ステップ 25：をクリックします。Download for Linux



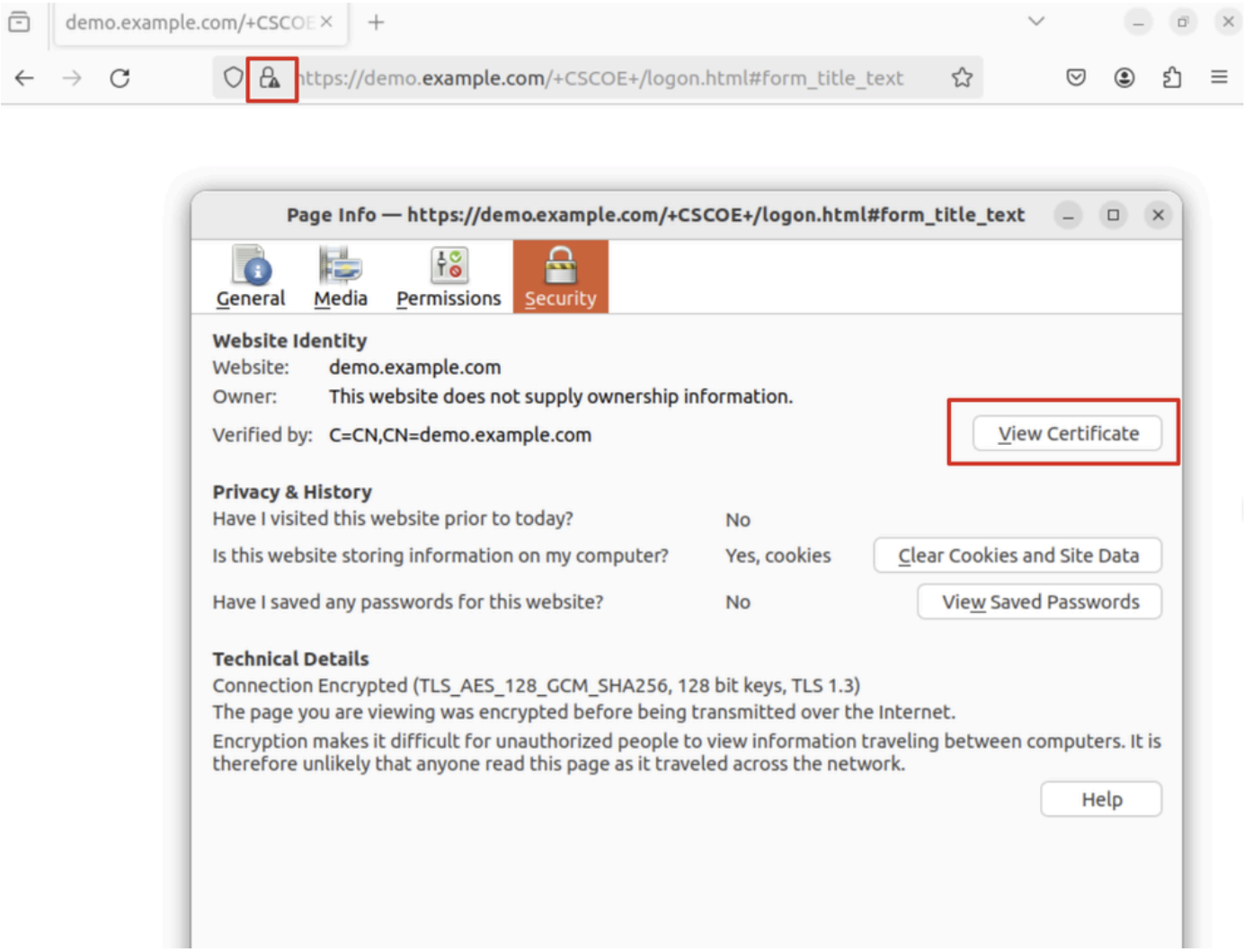
Ubuntu_Browser_VPN_ダウンロード_1

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...
```

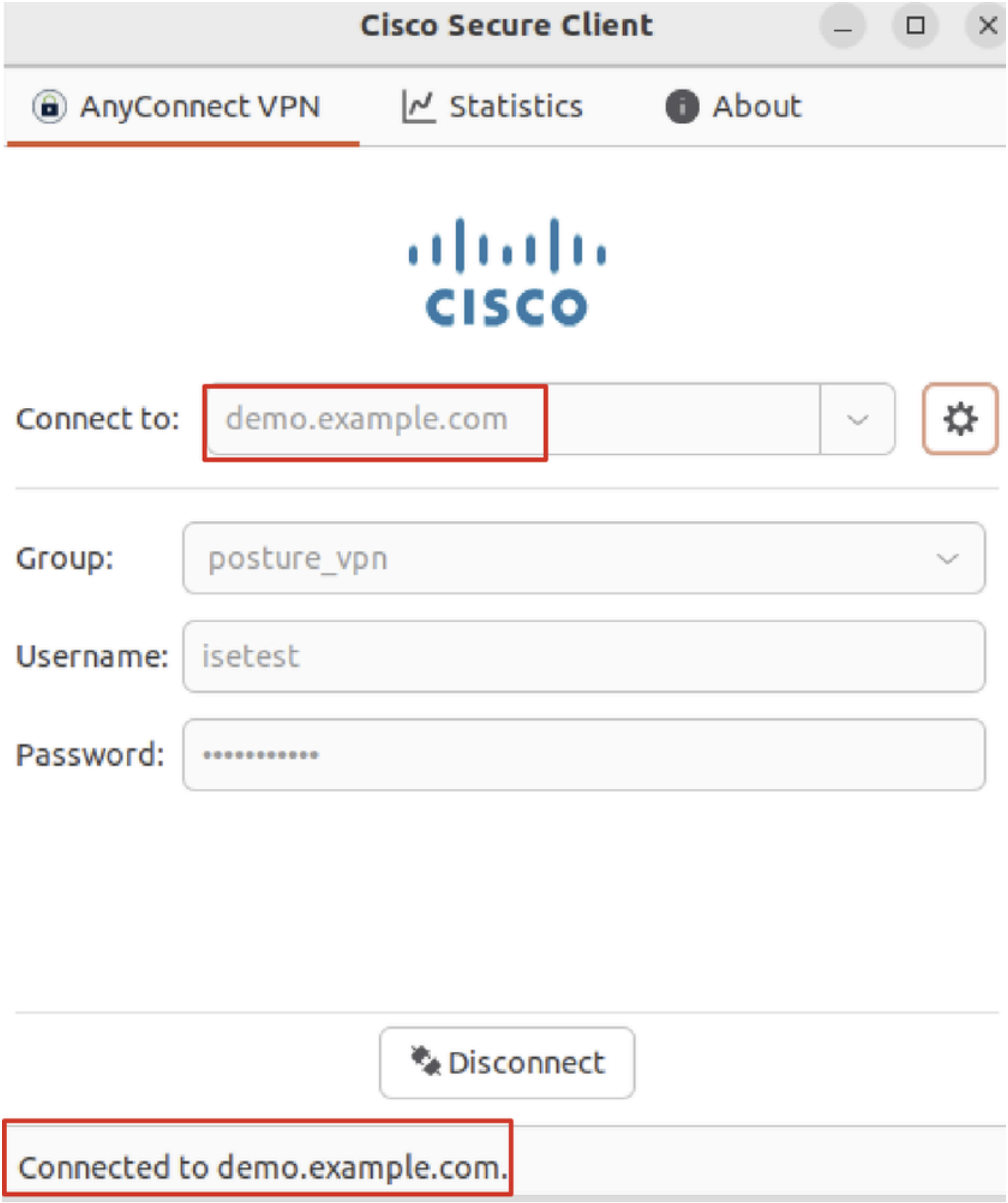
```
done.

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

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

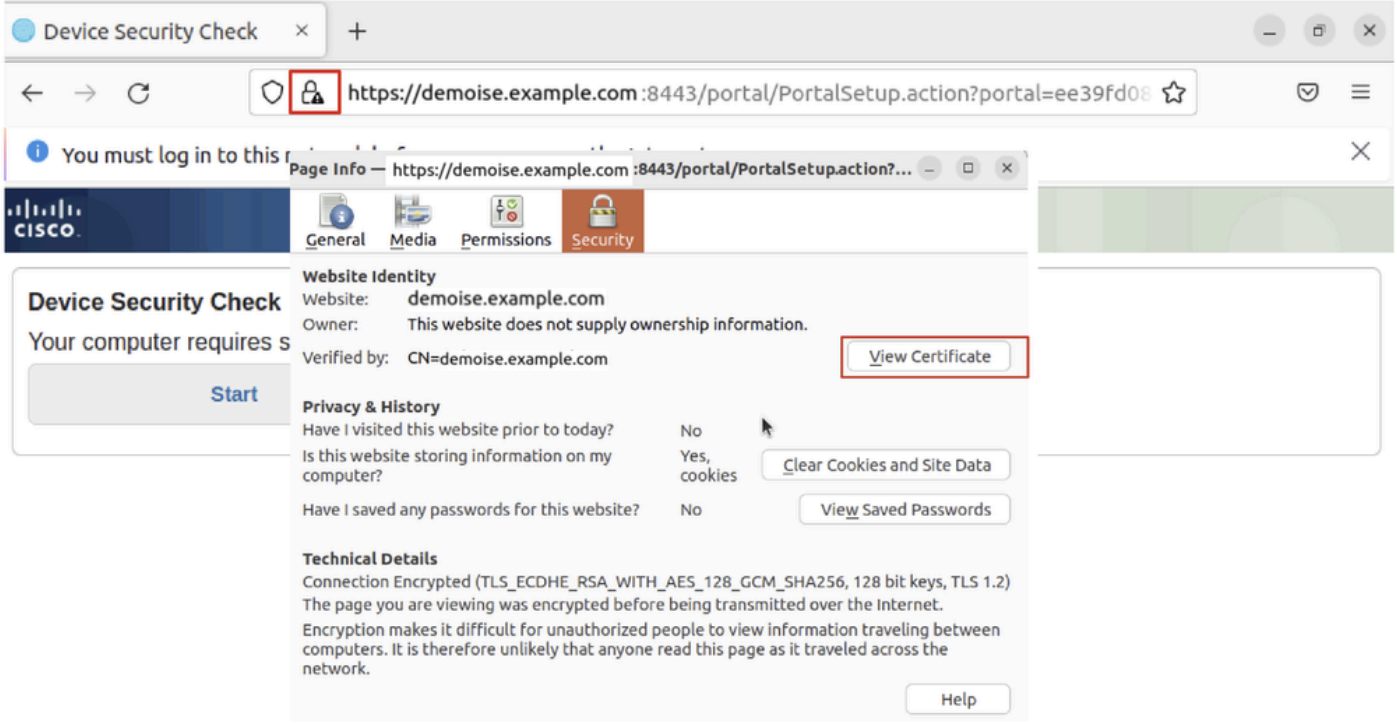
```
demo-example-com.crt: OK
```

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$
```

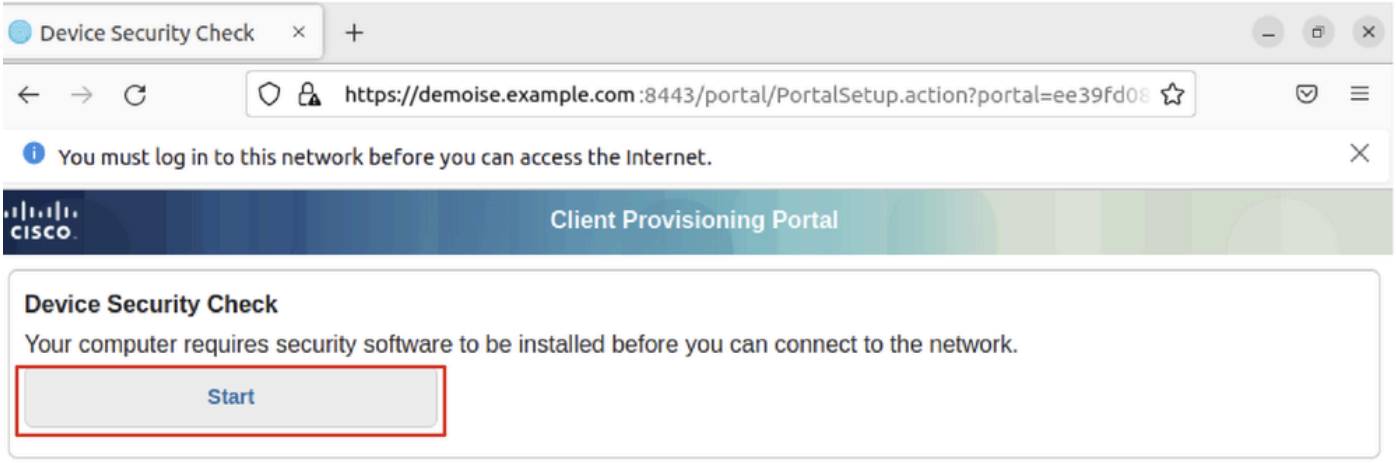
sudo update-ca-certificates

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

1 added

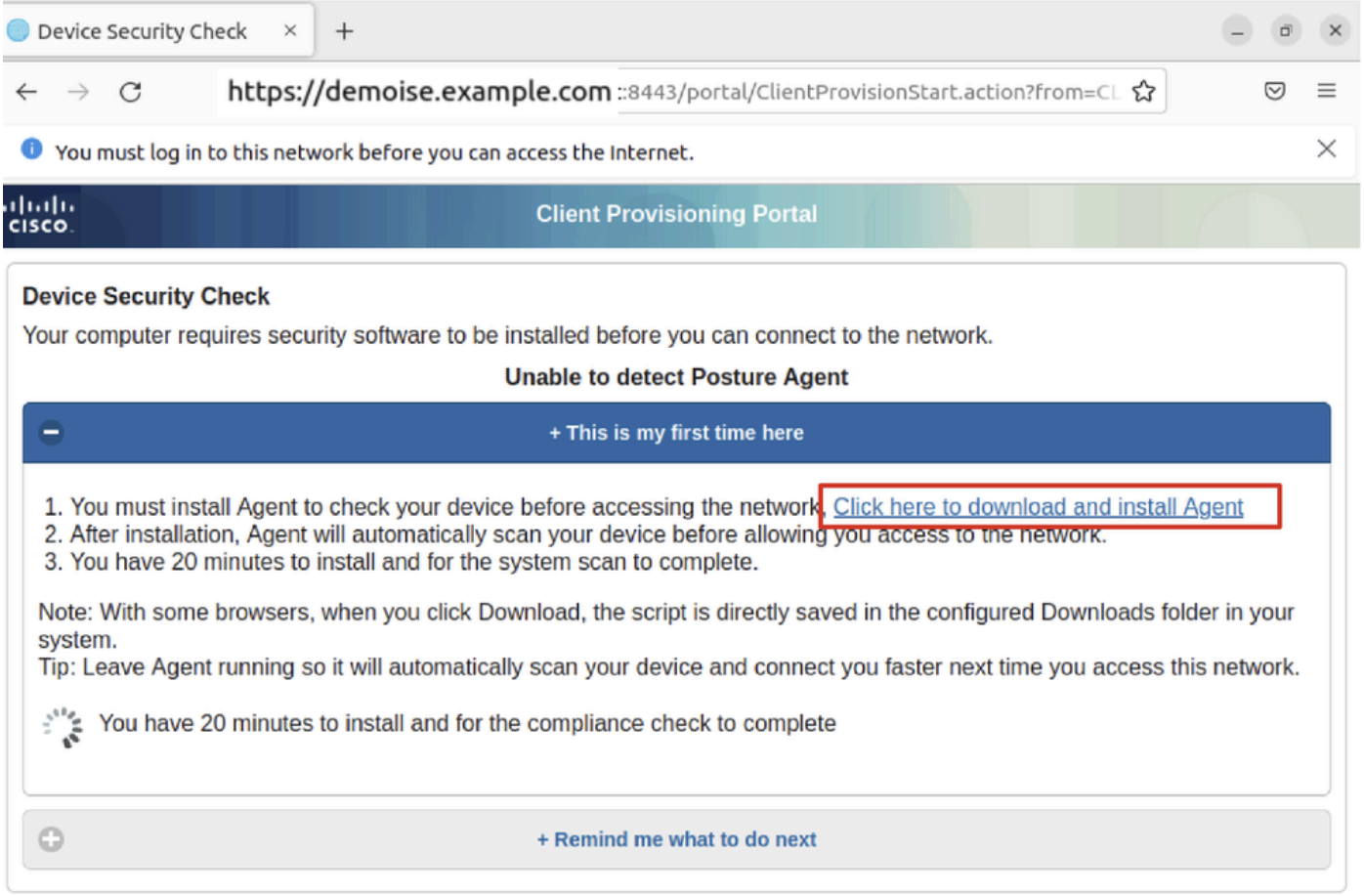
```
, 0 removed; done.
Running hooks in /etc/ca-certificates/update.d...
done.
```

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_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.
```

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
```

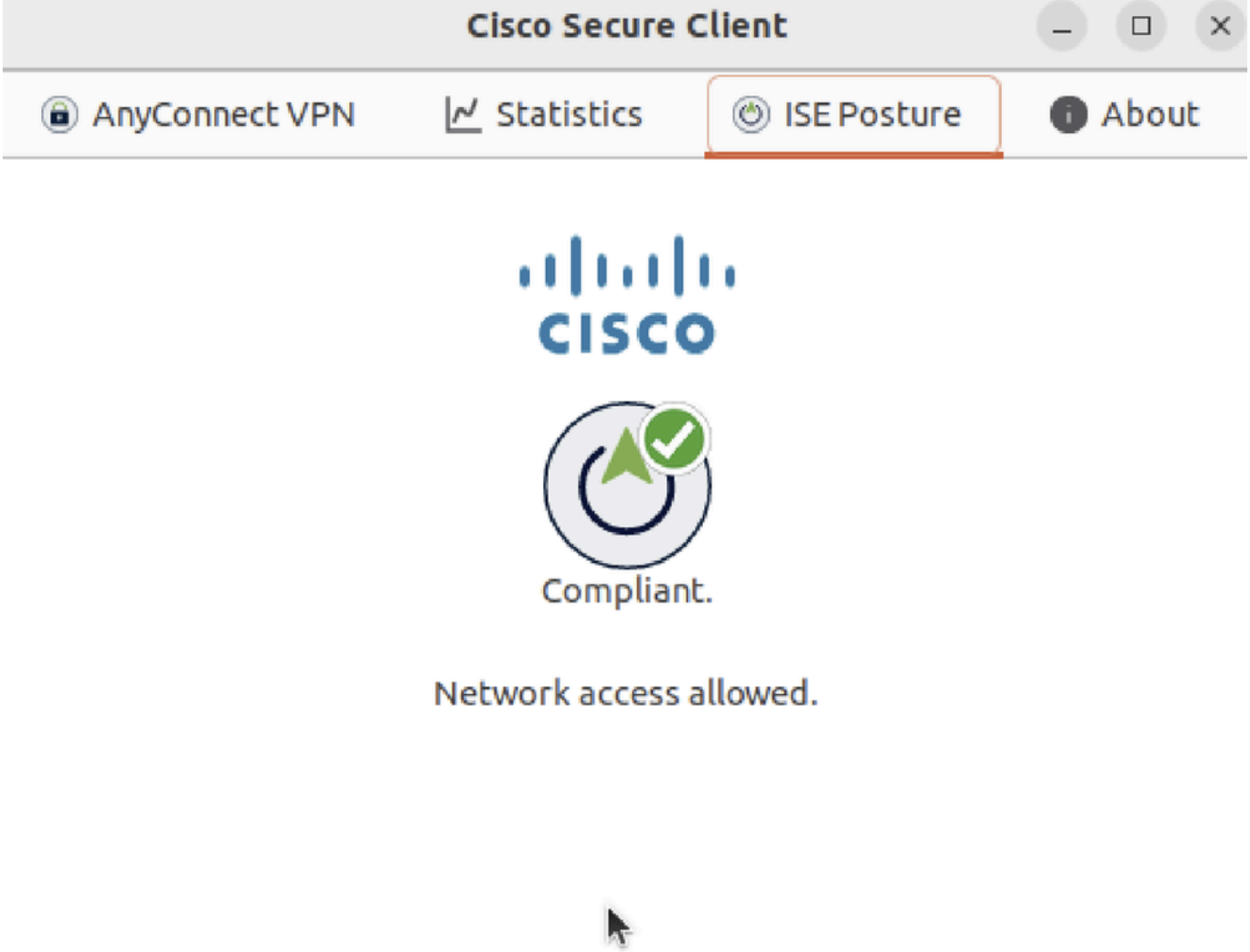
確認

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。

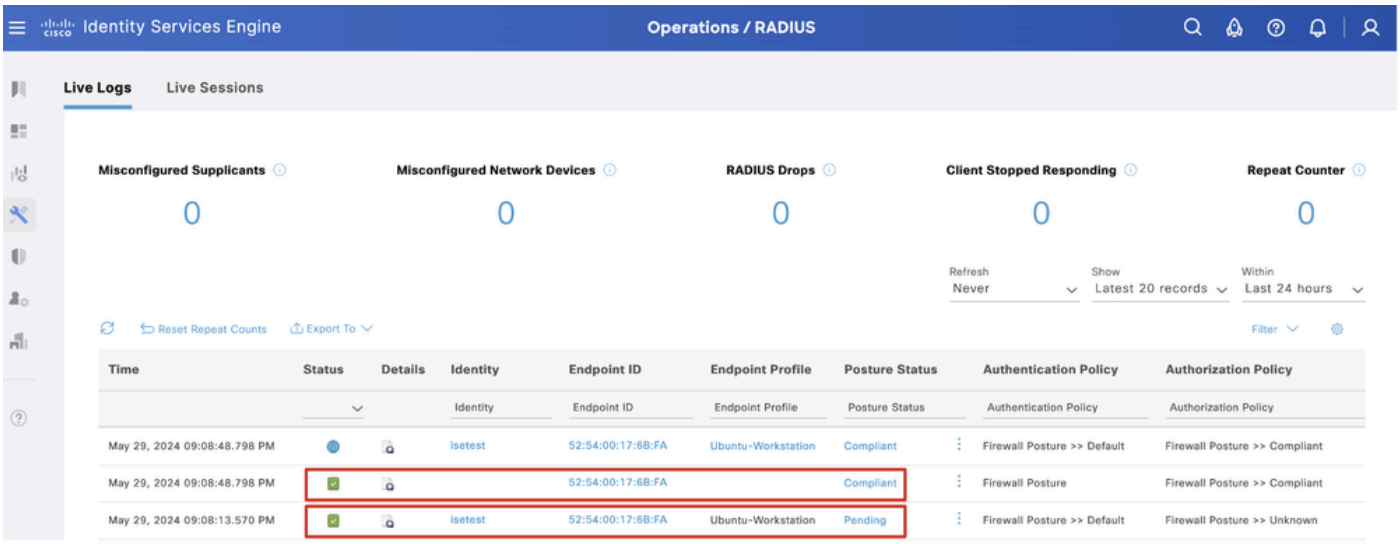
確認_*Ubuntu*_セキュア_クライアント_接続

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。



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 : cb0071820002100006659d871
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
```

トラブルシュート

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。