使用Linux配置Cisco ISE 3.1狀態

目錄

簡介

本文檔介紹為Linux和身份服務引擎(ISE)配置和實施檔案狀態策略的過程。

必要條件

需求

思科建議您瞭解以下主題：

- Anyconnect
- 身分識別服務引擎 (ISE)
- Linux

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Anyconnect 4.10.05085
- ISE版本3.1 P1
- Linux Ubuntu 20.04
- Cisco交換器Catalyst 3650。版本03.07.05.E(15.12(3)E5)

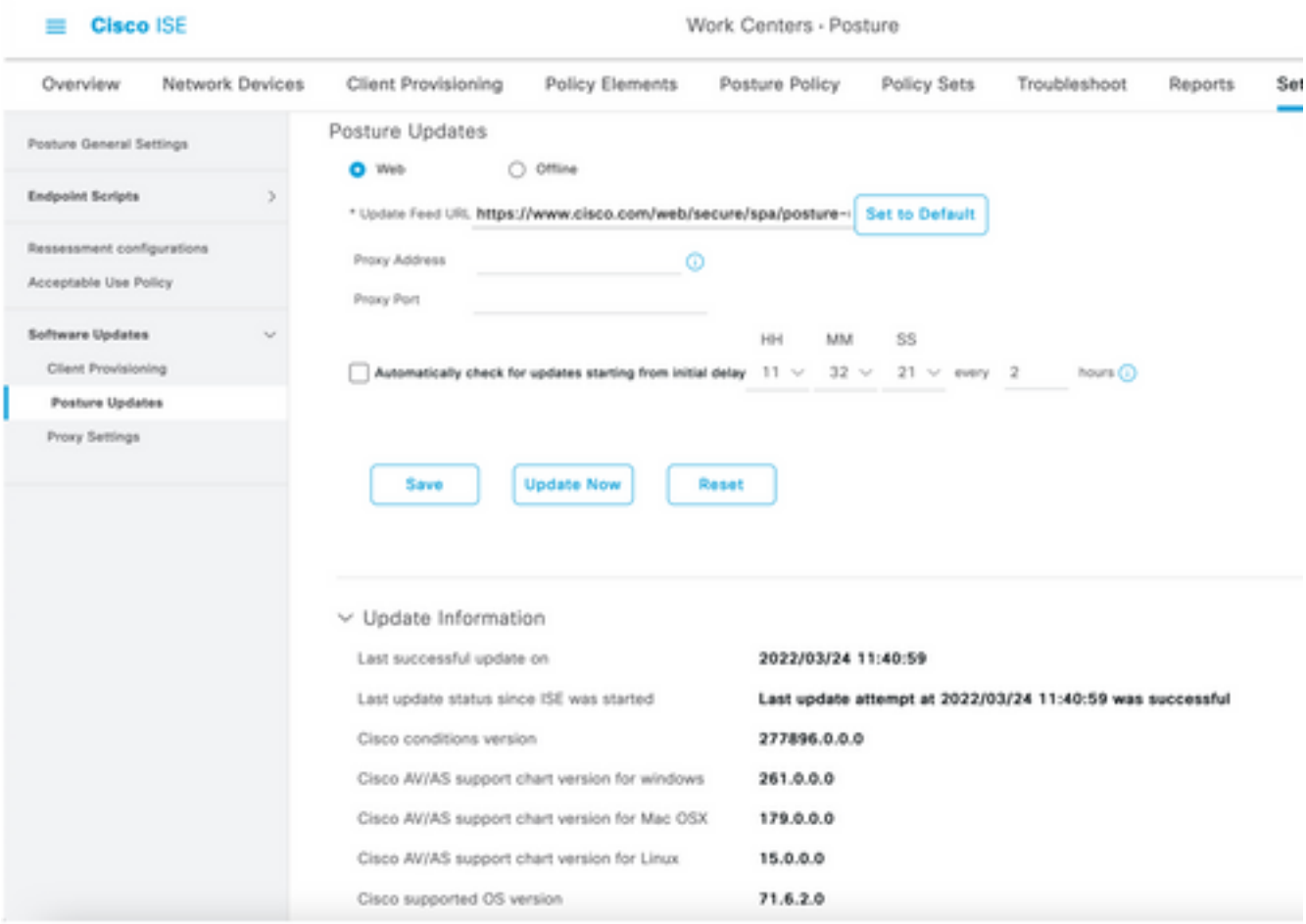
本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

設定

ISE上的配置

步驟1.更新狀態服務：

導航至Work Centers > Posture > Settings > Software Updates > Posture Updates。選擇「立即更新」並等待進程完成：

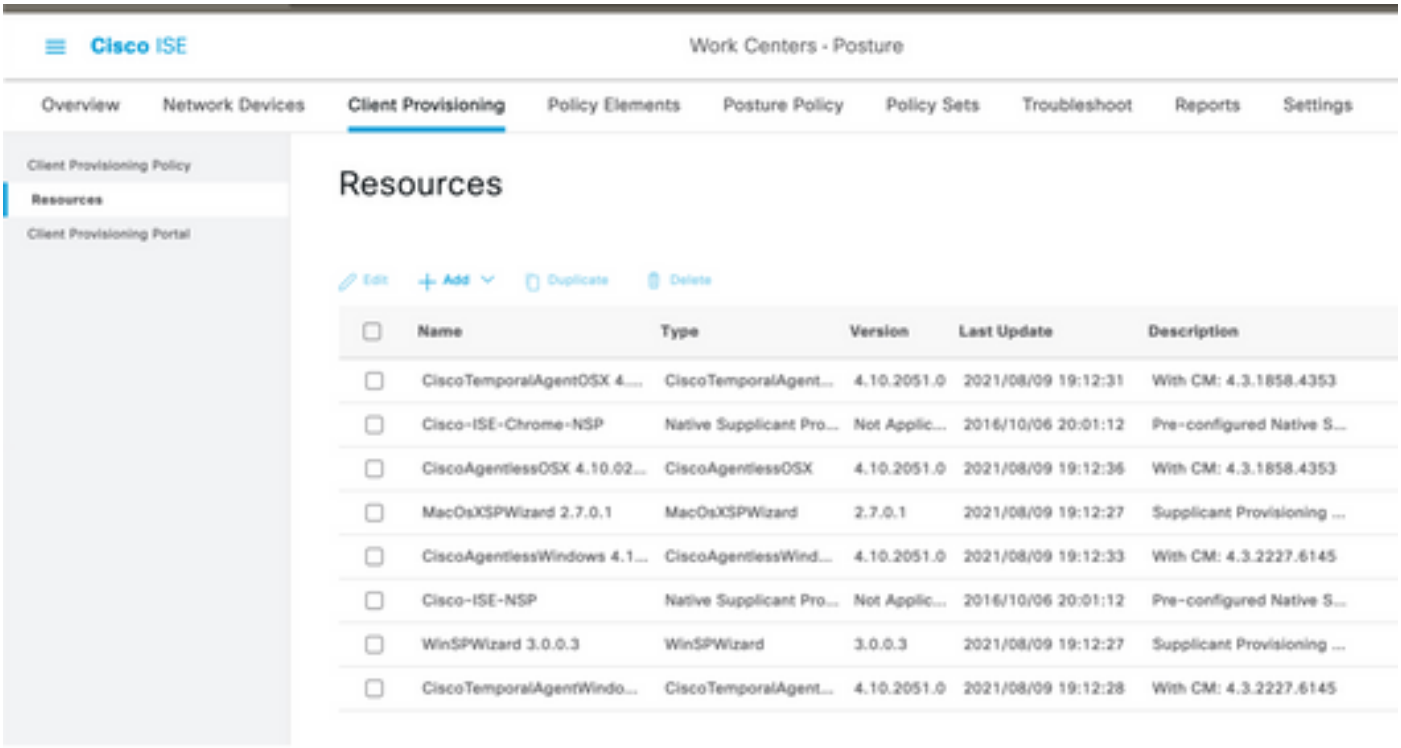


思科提供的軟體包是從Cisco.com站點下載的軟體包，例如AnyConnect軟體包。**客戶建立的包**是您在ISE使用者介面之外建立的配置檔案或配置，並且希望上傳到ISE用於安全評估評估。在本練習中，您可以下載AnyConnect webdeploy軟體包「anyconnect-linux64-4.10.05085-webdeploy-k9.pkg」。

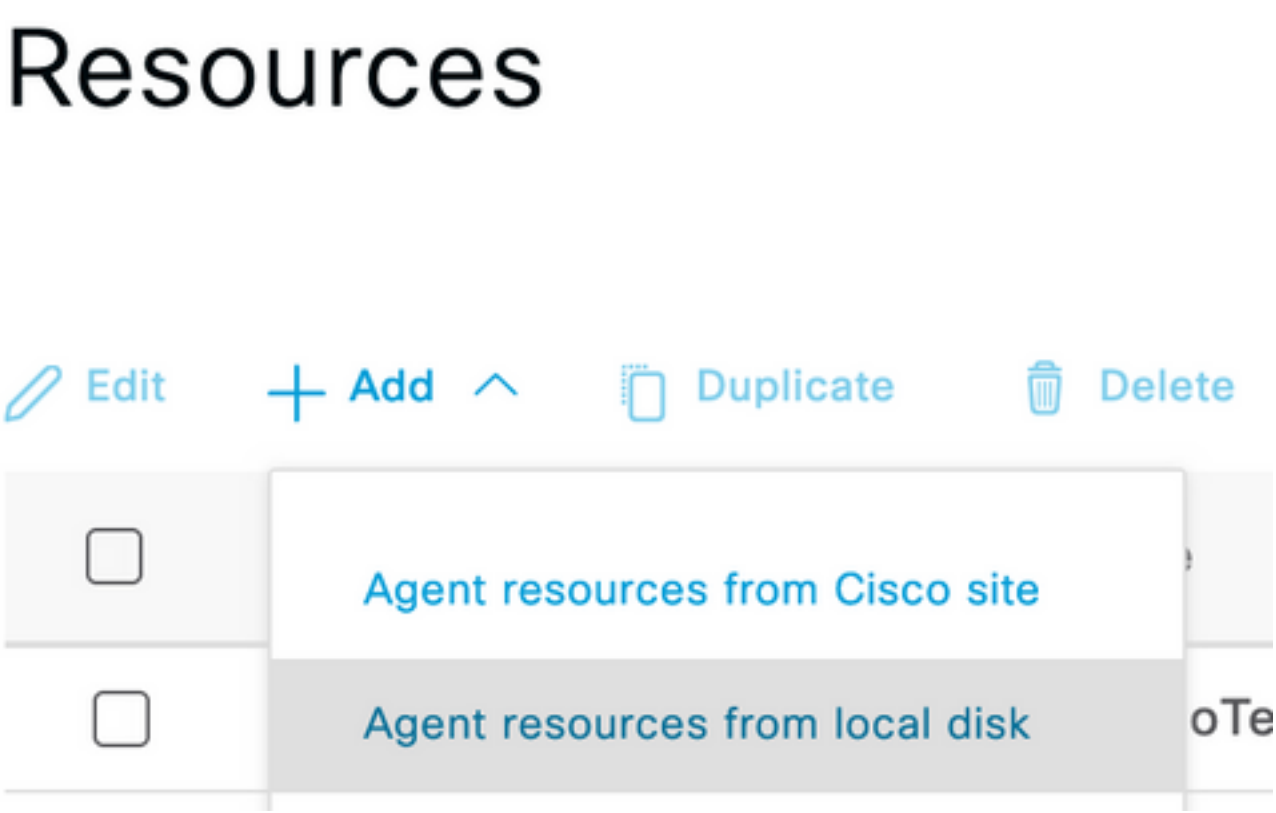
> **附註**：由於存在更新和補丁程式，因此建議的版本可能會更改。使用來自cisco.com站點的最新推薦版本。

步驟2.上傳AnyConnect軟體包：

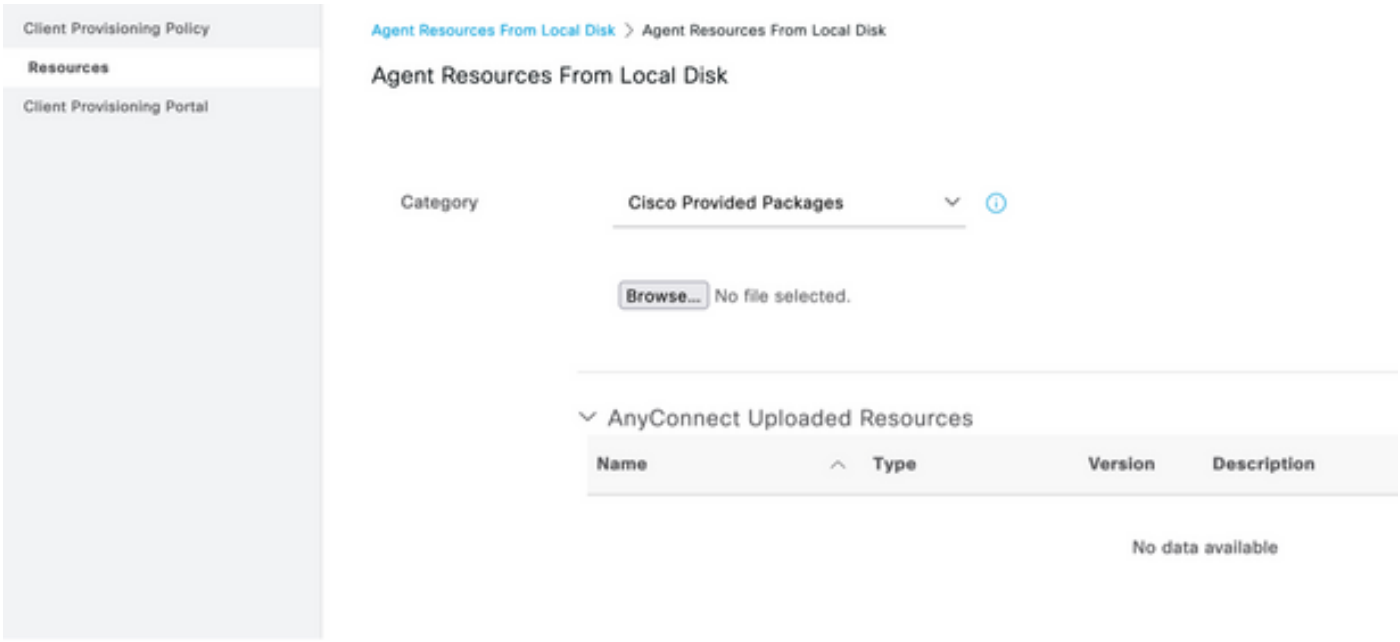
在Posture Work center中，導航至**Client Provisioning > Resources**



步驟3.選擇**Add > Agent Resources from Local Disk**

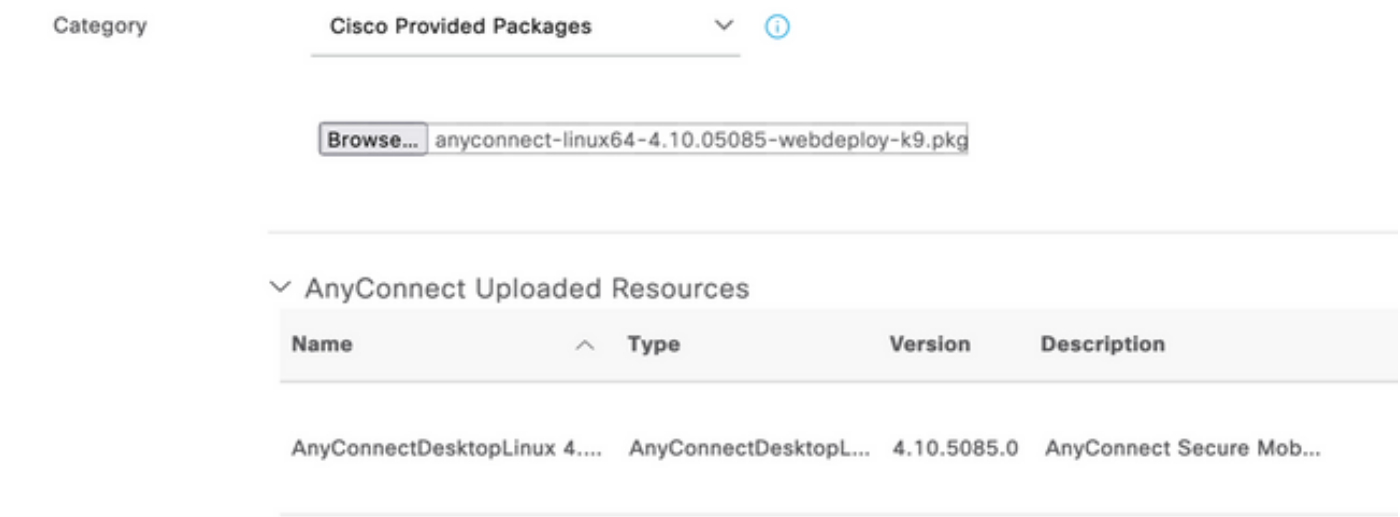


步驟4.從「Category」下拉式清單中選擇**Cisco** Provided Packages。



步驟5.按一下Browse。

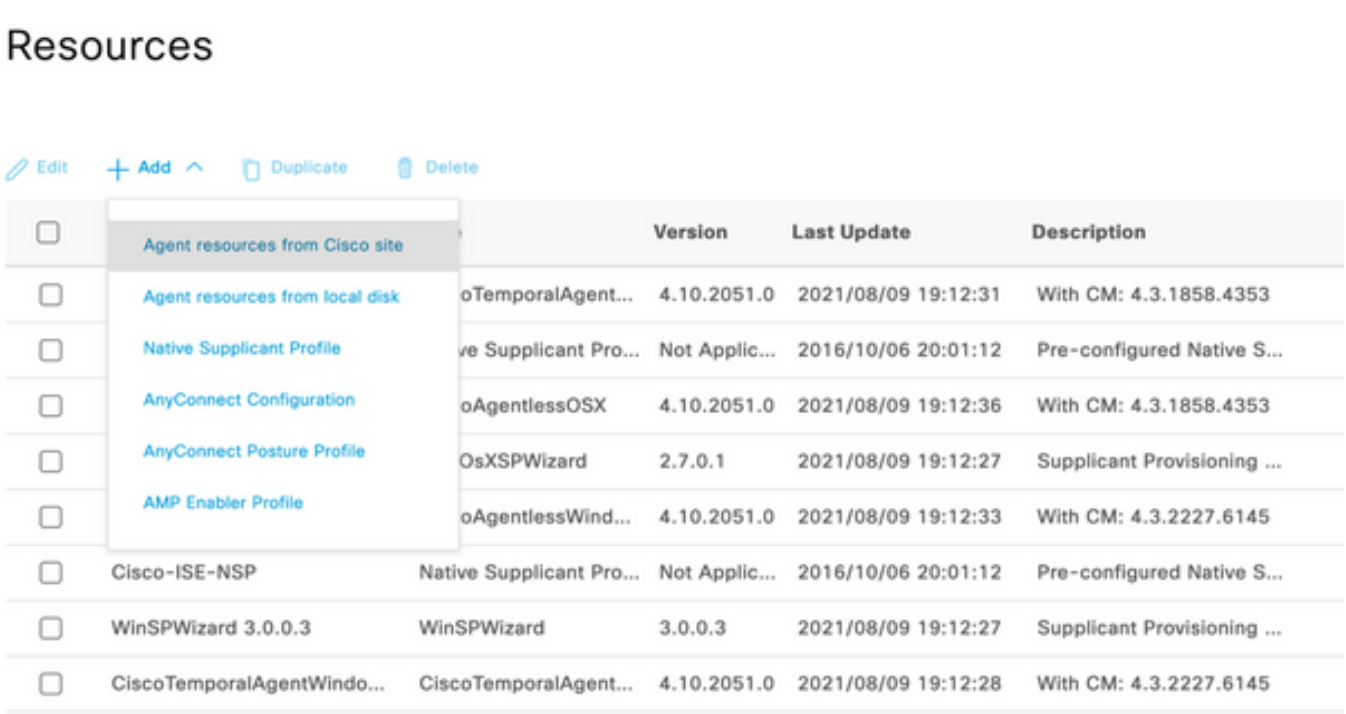
步驟6.選擇您在上一步中下載的其中一個AnyConnect軟體包。處理AnyConnect影象，並顯示有關軟體包的資訊



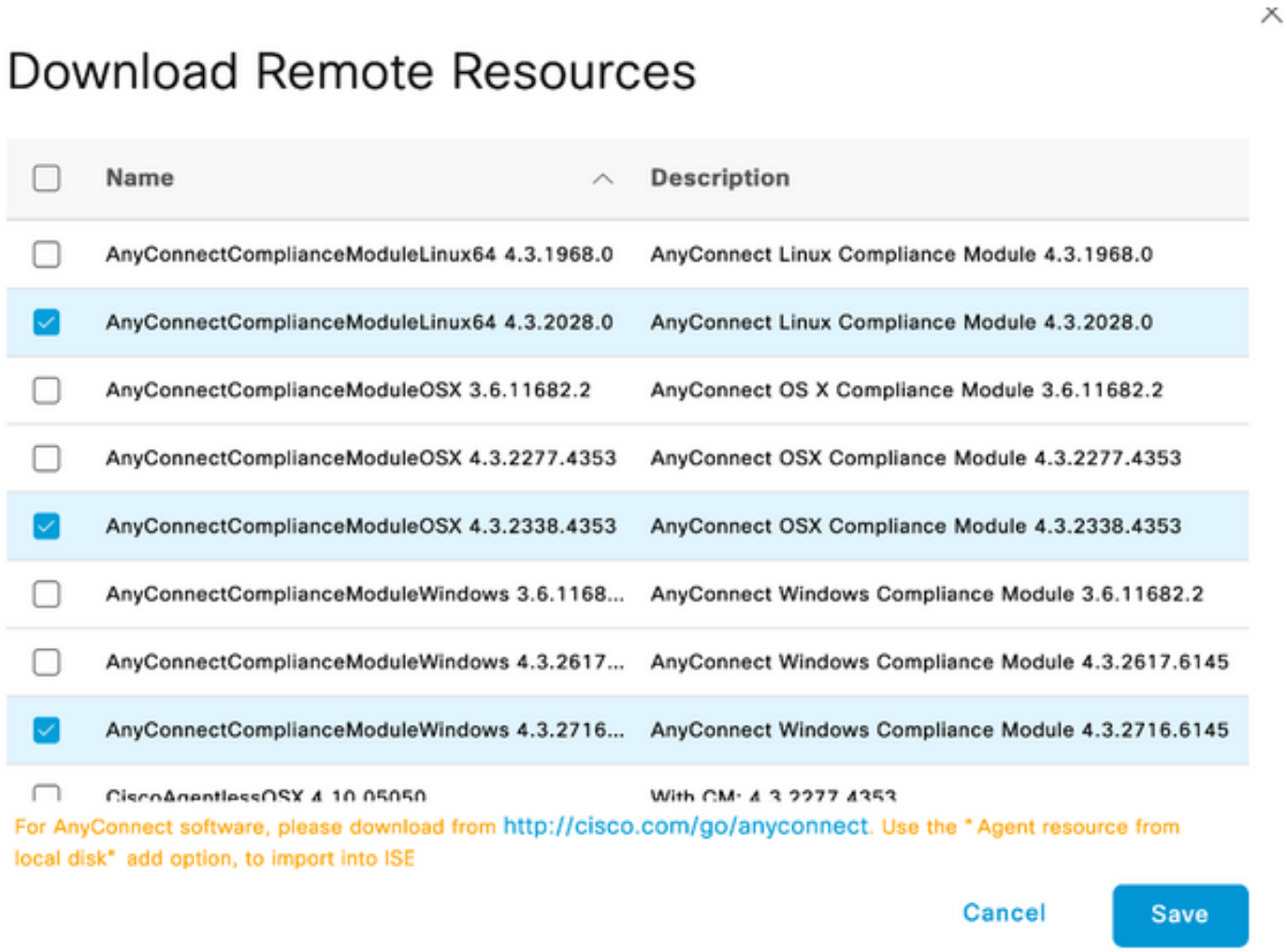
步驟7.按一下**Submit**。現在，AnyConnect上傳到ISE，您可以與ISE聯絡並從Cisco.com獲取其他客戶端資源。

> **附註**：代理資源包括AnyConnect客戶端使用的模組，該模組能夠評估終端對各種狀況檢查的合規性，例如防病毒、防間諜軟體、防惡意軟體、防火牆、磁碟加密、檔案等。

步驟8.按一下**Add > Agent Resources from Cisco Site**。當ISE訪問Cisco.com並檢索所有已發佈的客戶端調配資源的清單時，該視窗需要花費一分鐘時間進行填充。



步驟9.選擇適用於Linux的最新AnyConnect合規性模組。此外，您還可以選擇Windows和Mac的合規性模組。



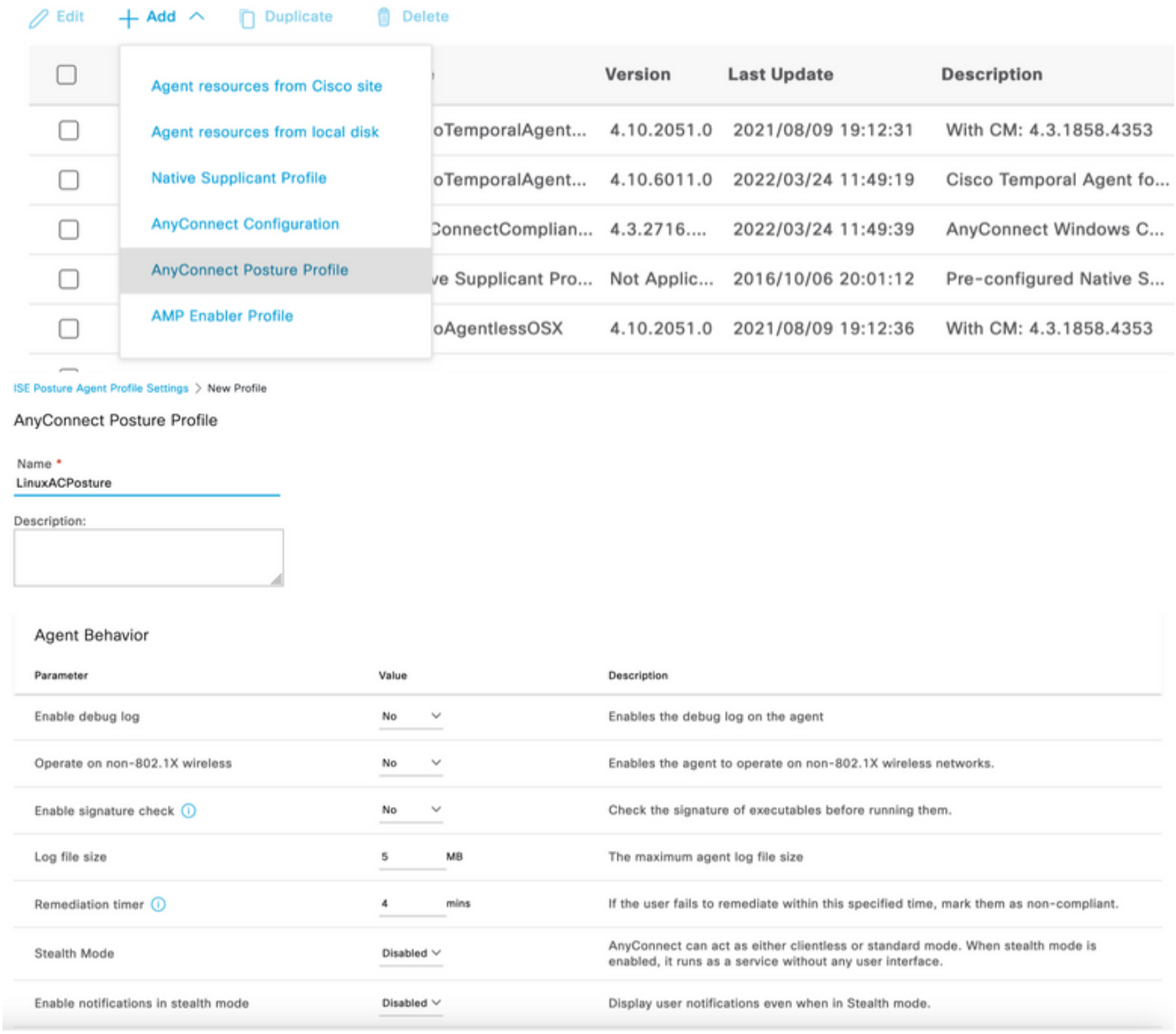
步驟10.選擇Windows和Mac的最新臨時代理。

步驟11.按一下**Save**。

附註：MAC和Windows終端安全評估配置不屬於本配置指南的範圍。

此時，您已經上載並更新了所有必需的部件。現在應該構建使用這些元件所需的配置和配置檔案。

步驟12.按一下Add > NAC Agent或AnyConnect Posture Profile。



需要修改的引數包括：

- **VLAN檢測間隔**:通過此設定，可以設定模組在探測VLAN更改之間等待的秒數。建議時間為5秒

。

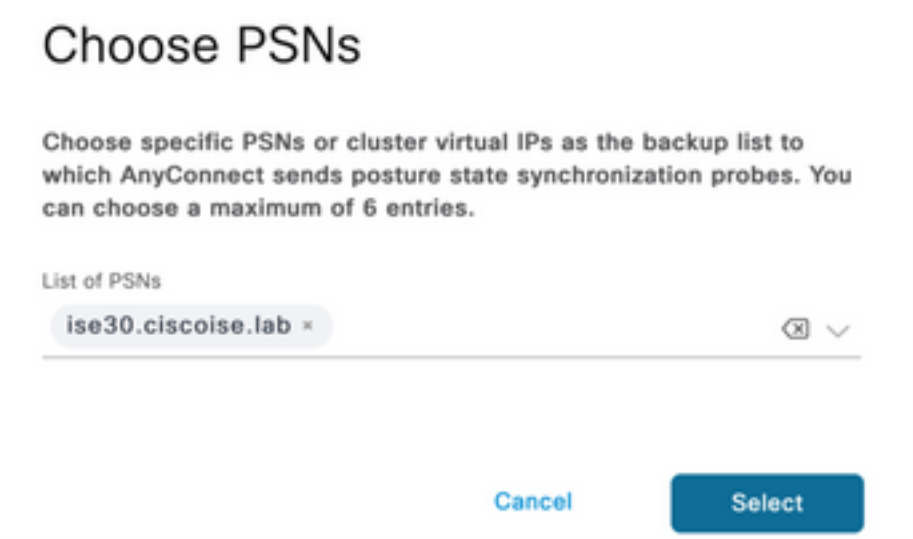
- **Ping或ARP**:這是實際的VLAN更改檢測方法。代理可以ping預設網關，或監控ARP快取，使預設網關條目超時或同時超時。推薦設定為ARP。

- **補救計時器**:當終端的狀態未知時，終端將進入狀態評估流程。修復失敗的狀況檢查需要時間；預設時間是4分鐘，之後將終端標籤為不合規，但值的範圍可以是1到300分鐘（5小時）。 建議時間為15分鐘；但是，如果預計補救需要更長時間，則需要進行調整。

  附註：Linux檔案狀態不支援自動補救。

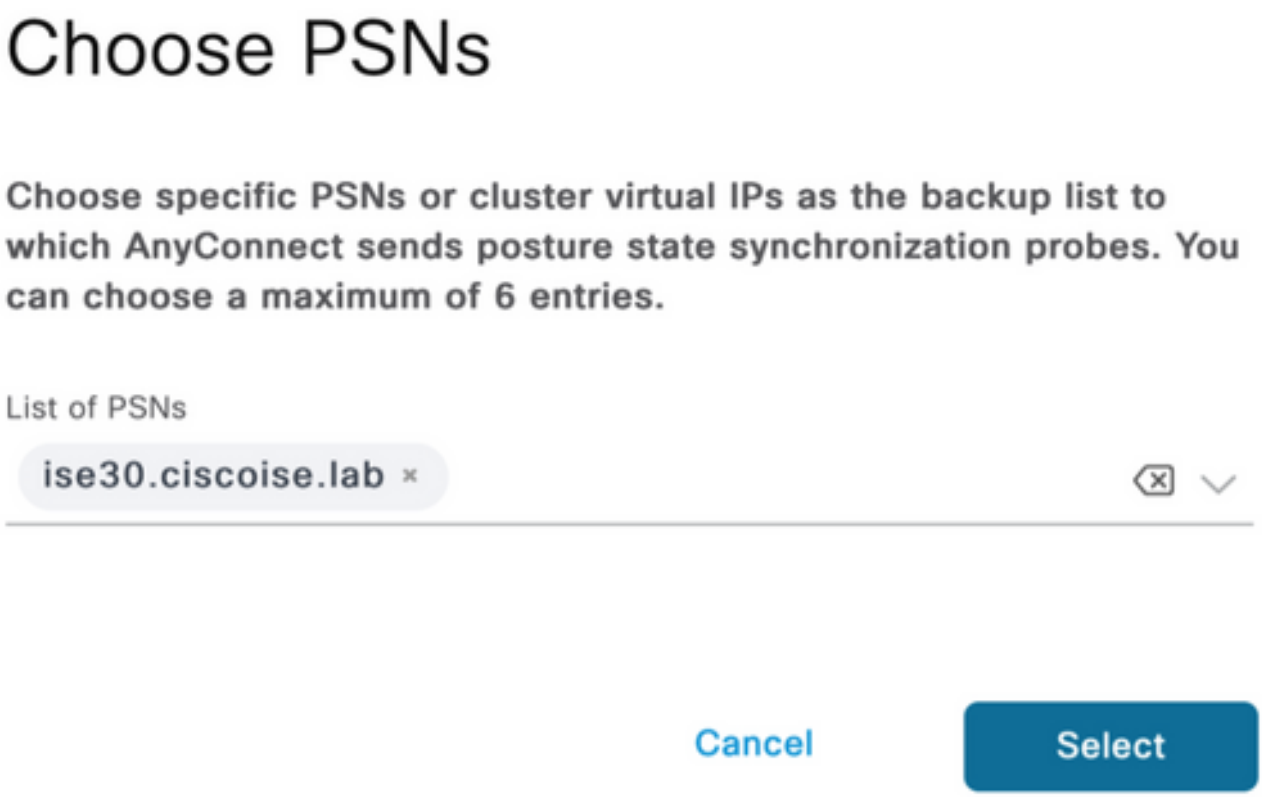
有關所有引數的全面說明，請參閱ISE或AnyConnect終端安全評估文檔。

步驟13.代理行為選擇狀態探測備份清單，然後選擇**選擇**，選擇PSN/獨立FQDN並選擇**儲存**

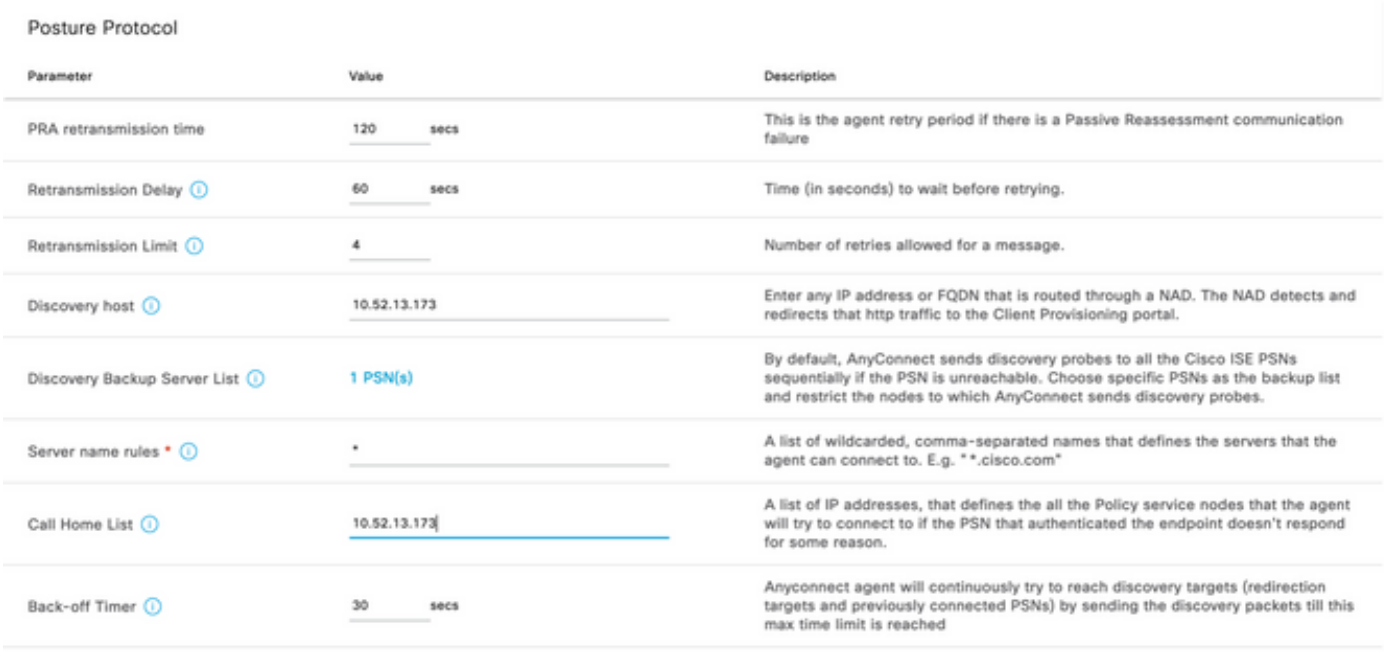


步驟14.在 Posture Protocols > Discovery Host下定義PSN/獨立節點IP地址。

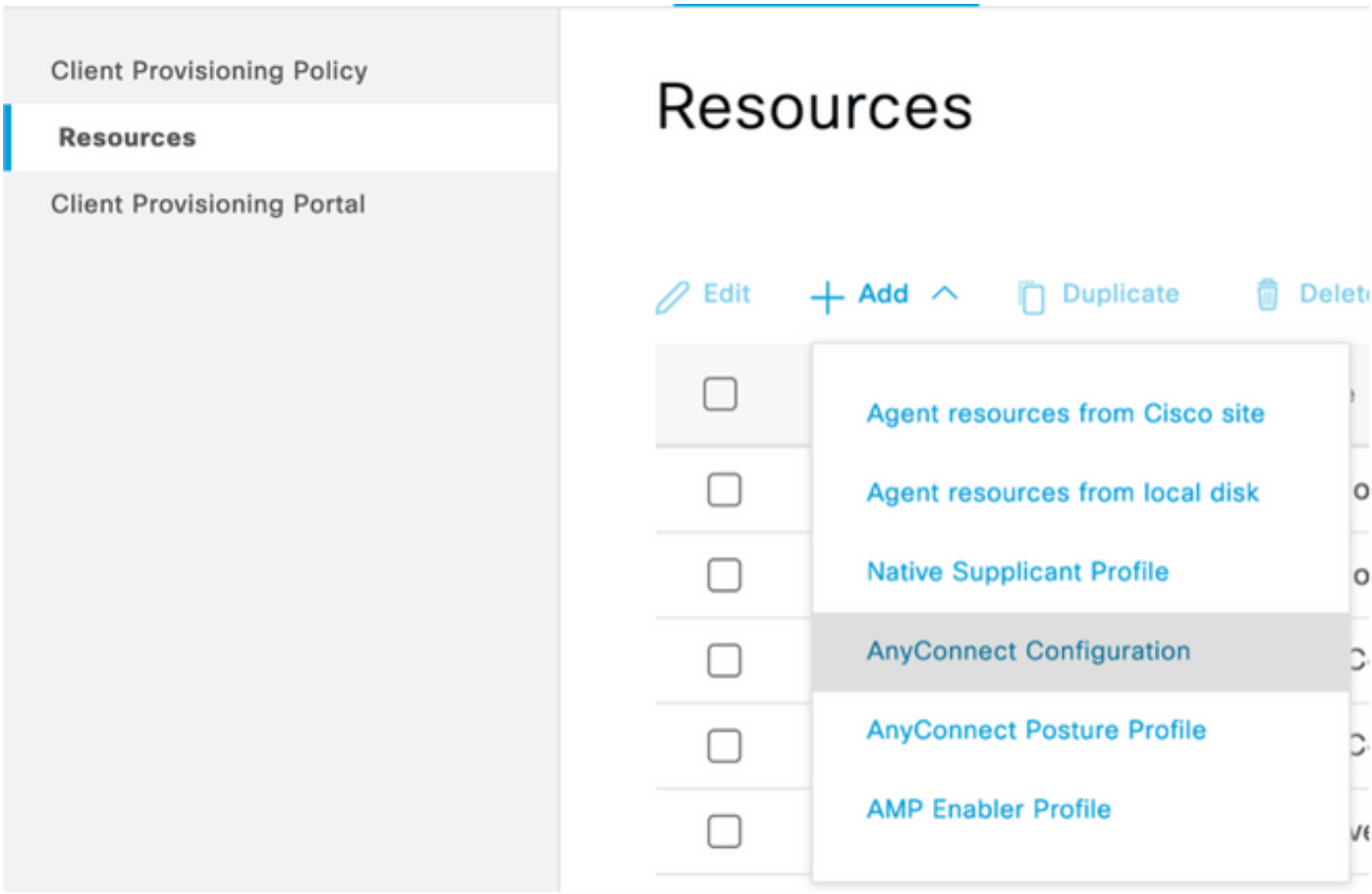
步驟15.從**Discovery backup server list**和Select**中選擇**您的PSN或獨立FQDN，然後選擇**Select。**

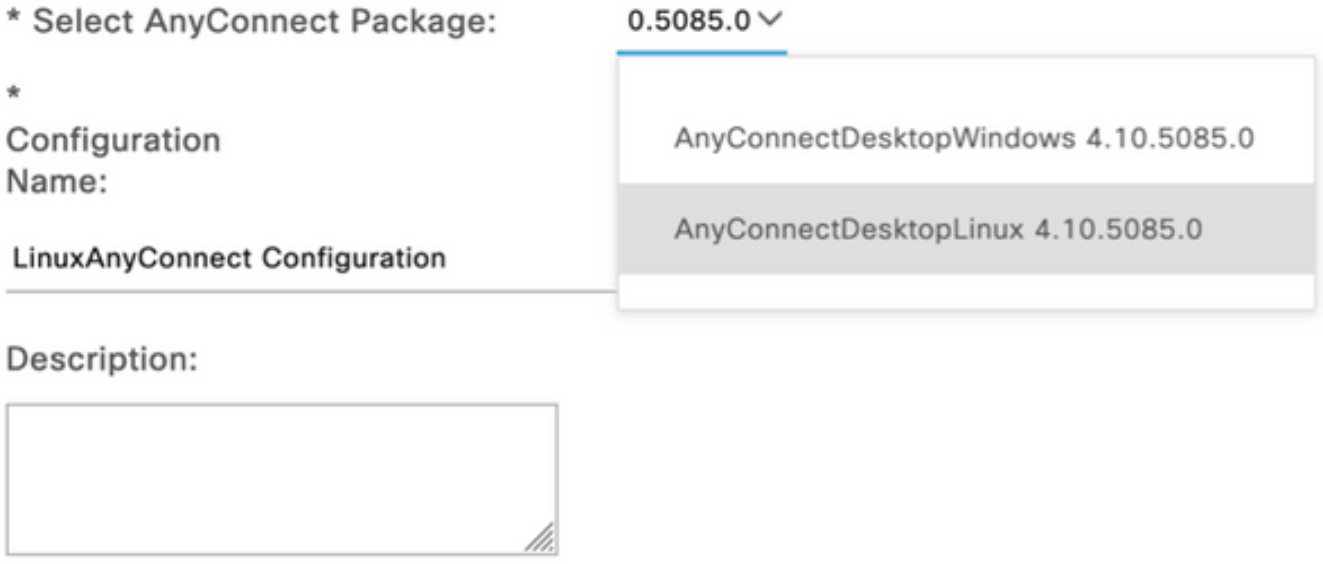


步驟16.在**Server name rules下，鍵入*聯絡所有伺服器，並在call home list下定義PSN/獨立IP地址**。或者，可以使用萬用字元匹配網路中的所有潛在PSN(即*.acme.com)。



步驟17.單擊Add > AnyConnect Configuration


Client Provisioning Policy
Resources
Client Provisioning Portal
Resources
Edit
Add
Duplicate
Agent resources from Cisco site
Agent resources from local disk
Native Supplicant Profile
AnyConnect Configuration
AnyConnect Posture Profile
AMP Enabler Profile


* Select AnyConnect Package:
0.5085.0
*
Configuration
Name:
LinuxAnyConnect Configuration
Description:
AnyConnectDesktopWindows 4.10.5085.0
AnyConnectDesktopLinux 4.10.5085.0

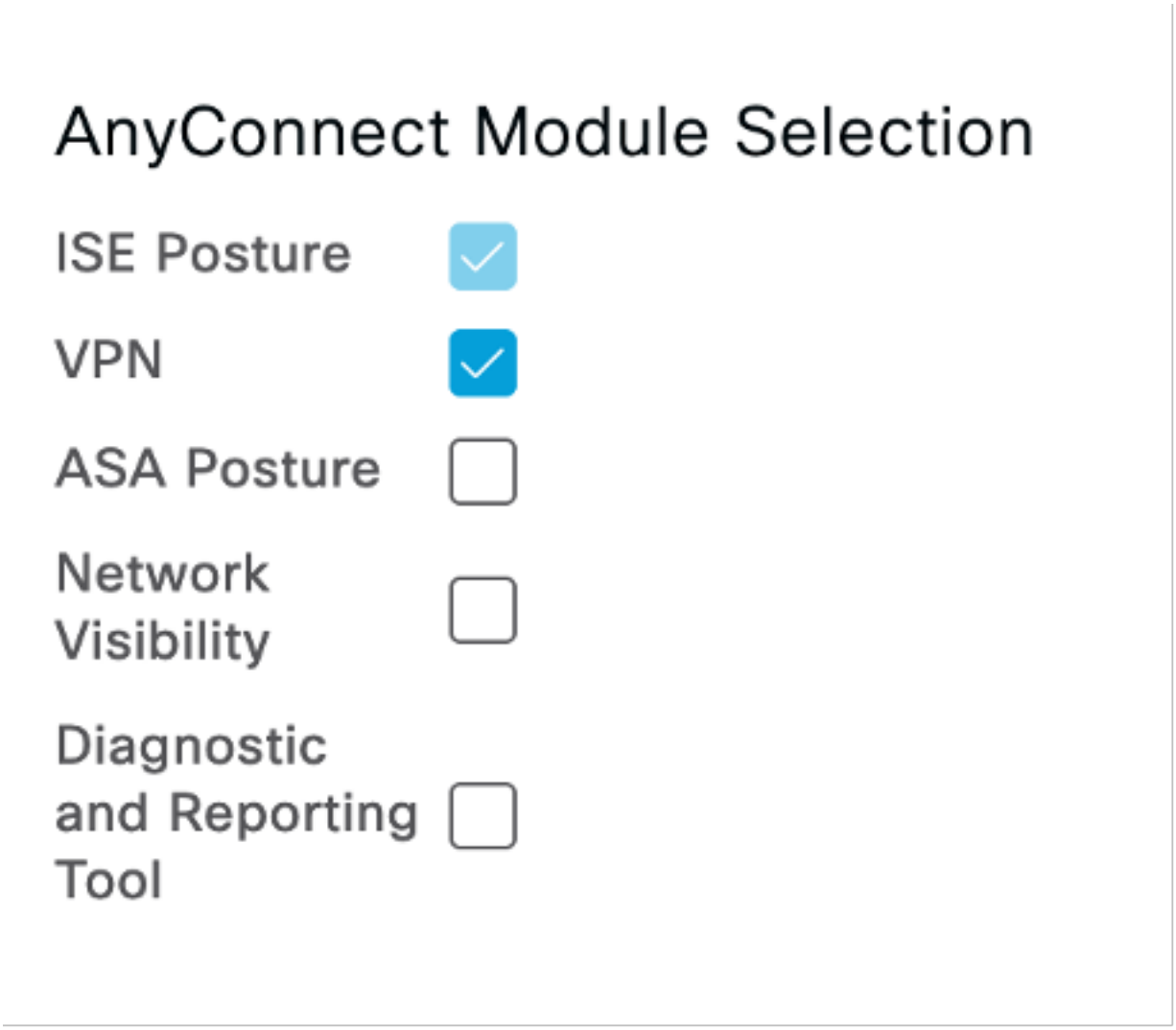
Description Value Notes

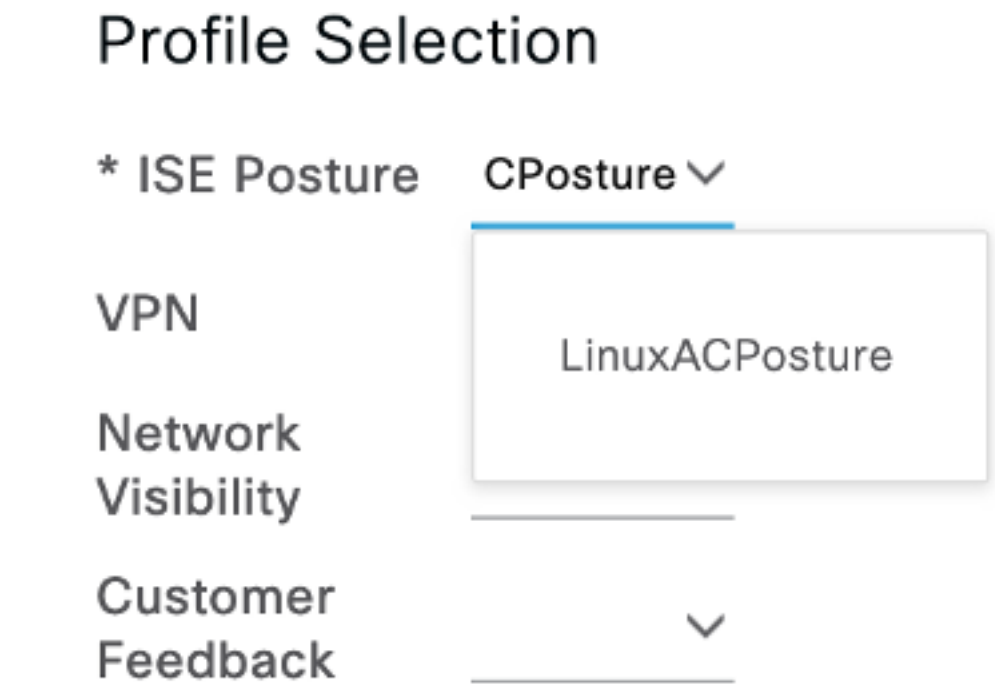
* Compliance Module 3.2028.0

AnyConnectComplianceModuleLinux64 4.3.1676.0

AnyConnectComplianceModuleLinux64 4.3.2028.0

AnyConnect

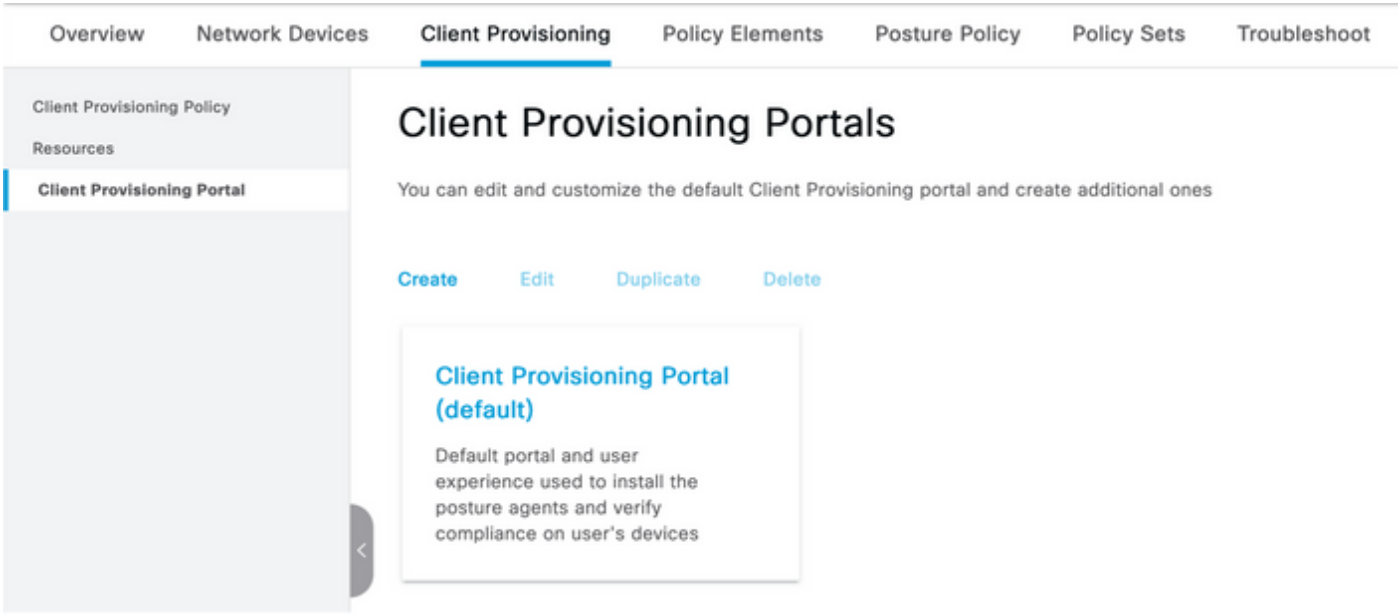




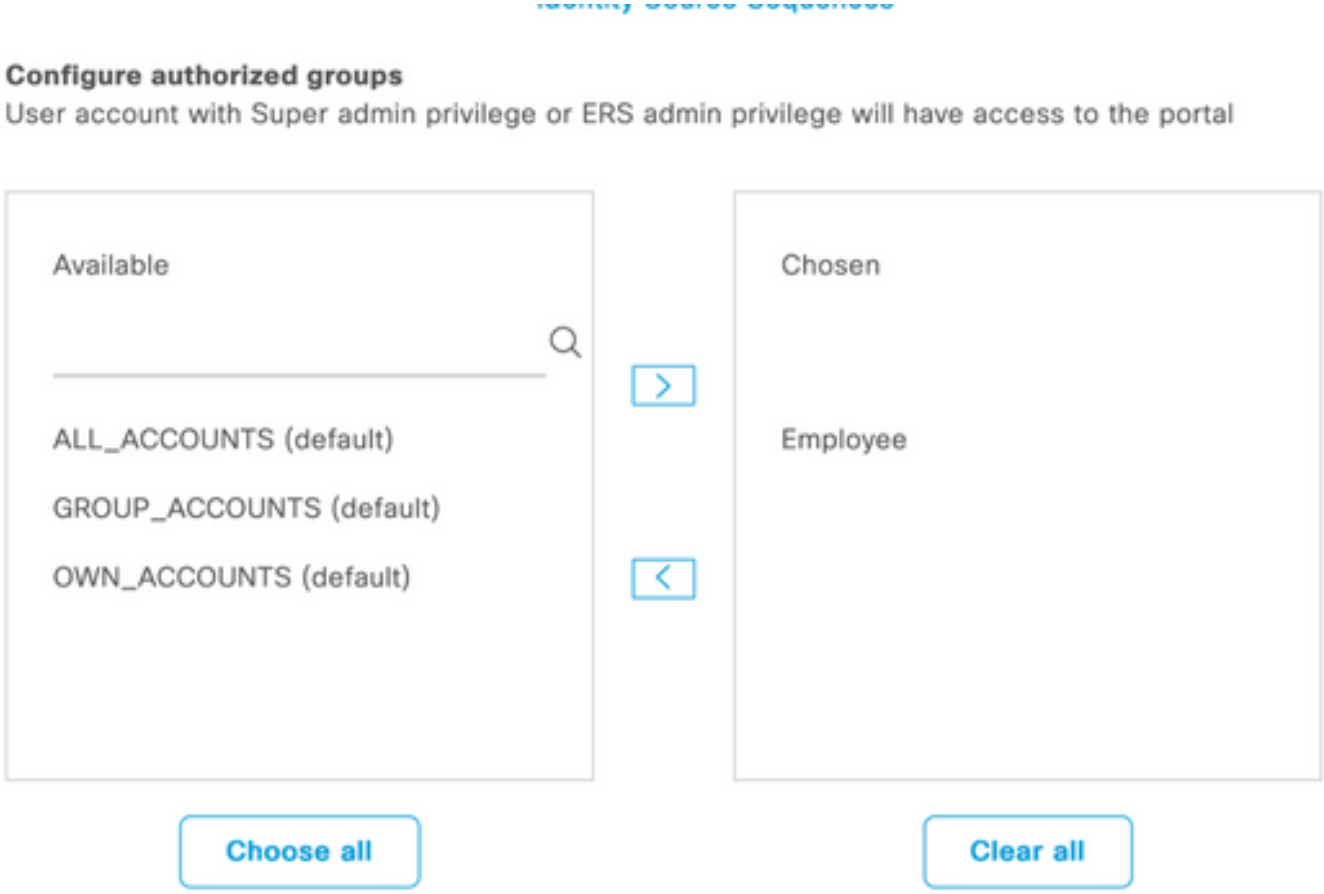
向下滾動並選擇提交

步驟18.完成選擇後，按一下**提交**。

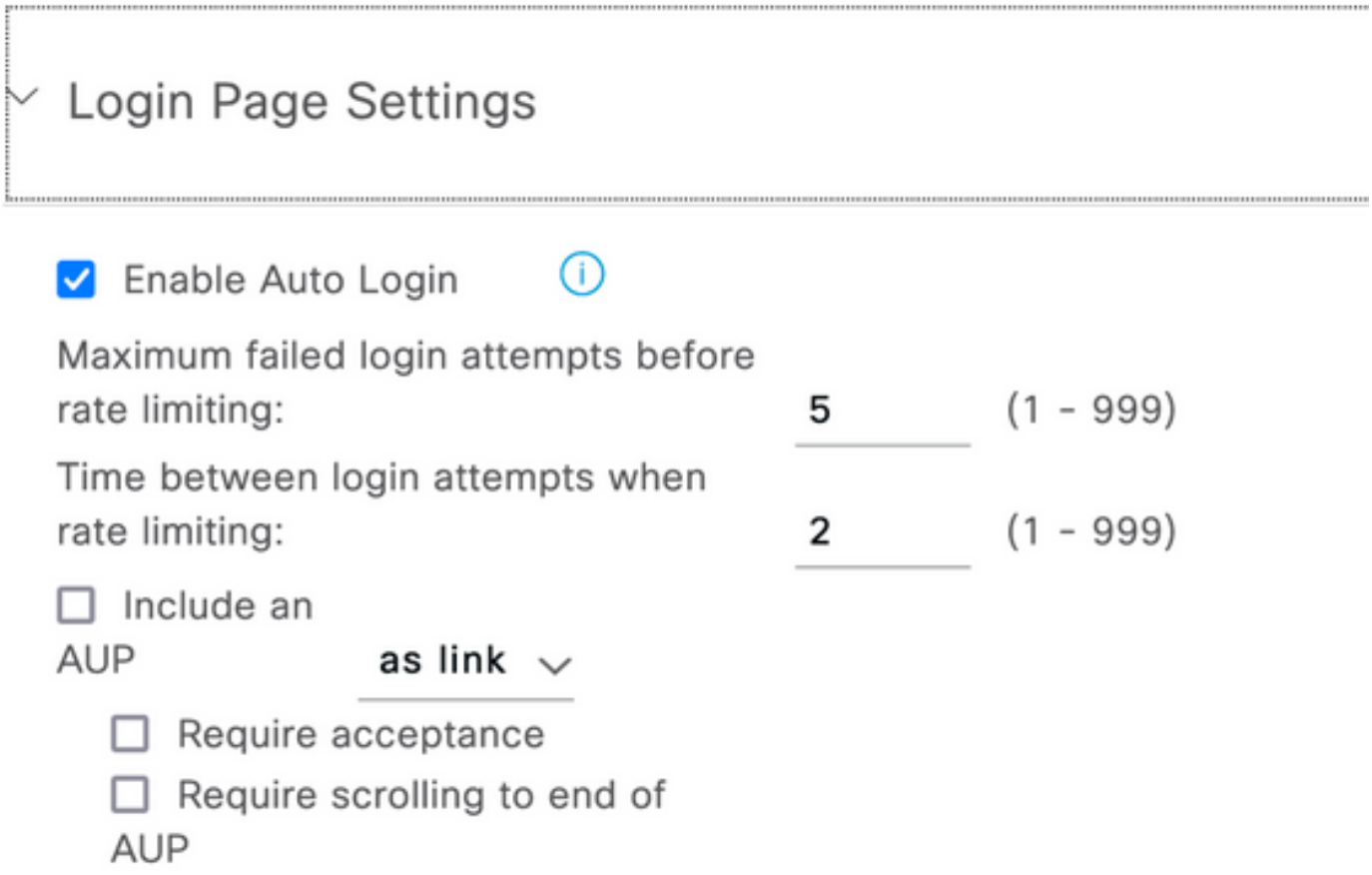
步驟19.選擇**Work Centers > Posture > Client Provisioning > Client Provisioning Portals**。



步驟20. 在**Portal Settings**部分下，可以選擇介面和埠以及授權到選擇員工、SISE_Users和域使用者頁面的組。



步驟21.在 Log in Page Settings下，確保啟用**Enable auto Log In**選項



步驟22.在右上角選擇**Save**

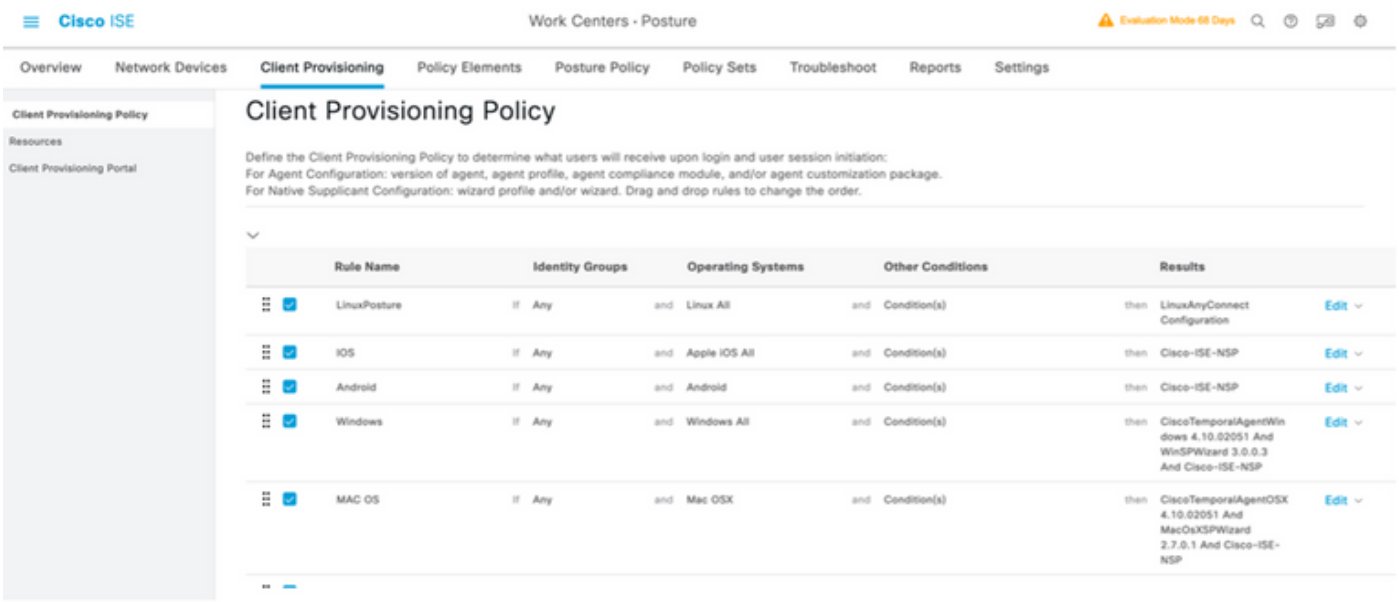
步驟23.選擇**Work Centers > Posture > Client Provisioning > Client Provisioning Policy。**

步驟24.在CPP中按一下IOS規則旁**邊的下**箭頭，然**後選**擇「**Duplicate Above**」

步驟25.將規則命名為**LinuxPosture**

步驟26.對於Results，選擇**AnyConnect Configuration**作為代理。

> **附註**：在這種情況下，您看不到合規性模組下拉選單，因為它被配置為AnyConnect配置的一部分。



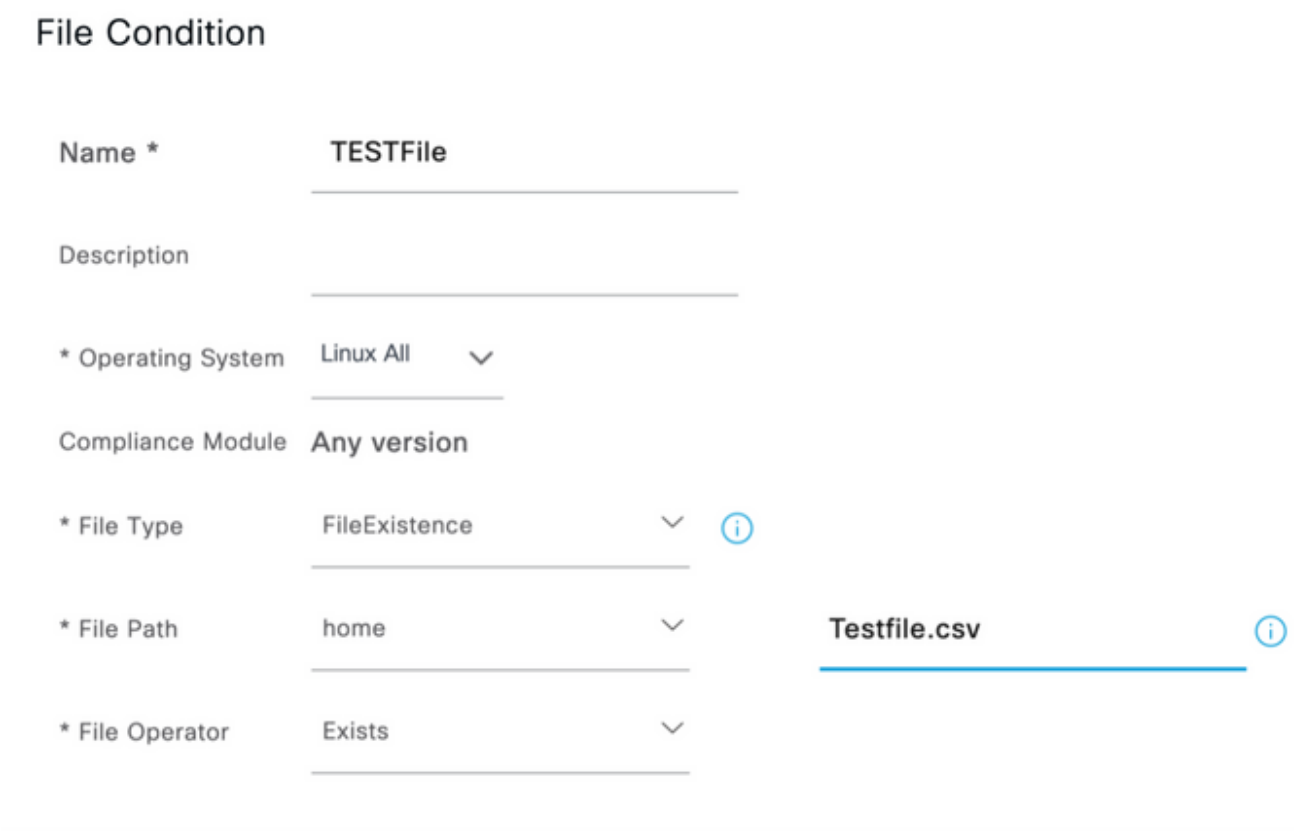
步驟27.按一下「**Done**」。

步驟28.按一下**Save**。

狀態策略元素

步驟29.選擇**Work Centers > Posture > Policy Elements > Conditions > File。**選擇**新增。**

步驟30.將**TESTFile**定義為檔案條件名稱並定義下一個值

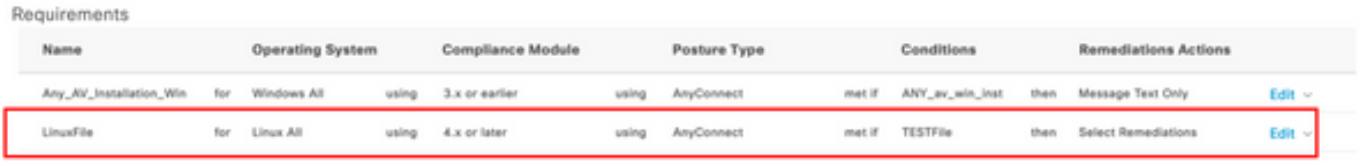


附註：路徑取決於檔案位置。

步驟31.選擇**Save**

FileExistence.此檔案型別的條件檢視檔案是否存在於其應該存在的系統中，僅此而已。選擇此選項後，完全不需要驗證檔案日期、雜湊等

步驟32.選擇要求並按如下所示建立新策略：



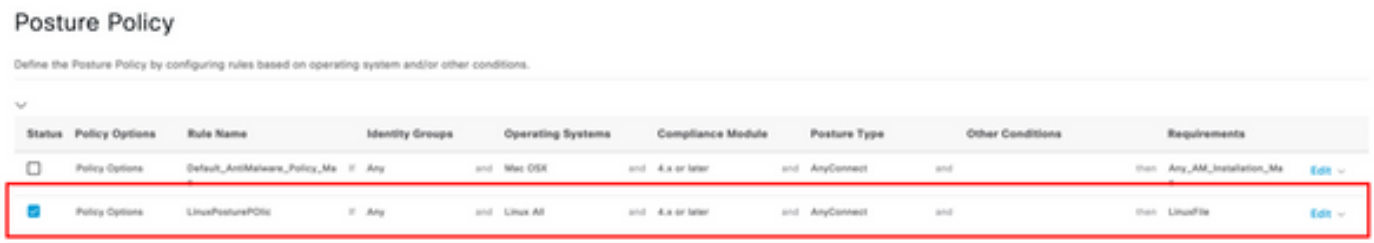
附註：Linux不支援僅作為補救操作的消息文本

需求元件

- **作業系統**：Linux全部
- **合規性模組**：4.x
- **狀態型別**：AnyConnect
- **狀況:**合規性模組和代理（在您選擇作業系統後可用）
- **補救操作**：選擇所有其他條件後可供選擇的補救。

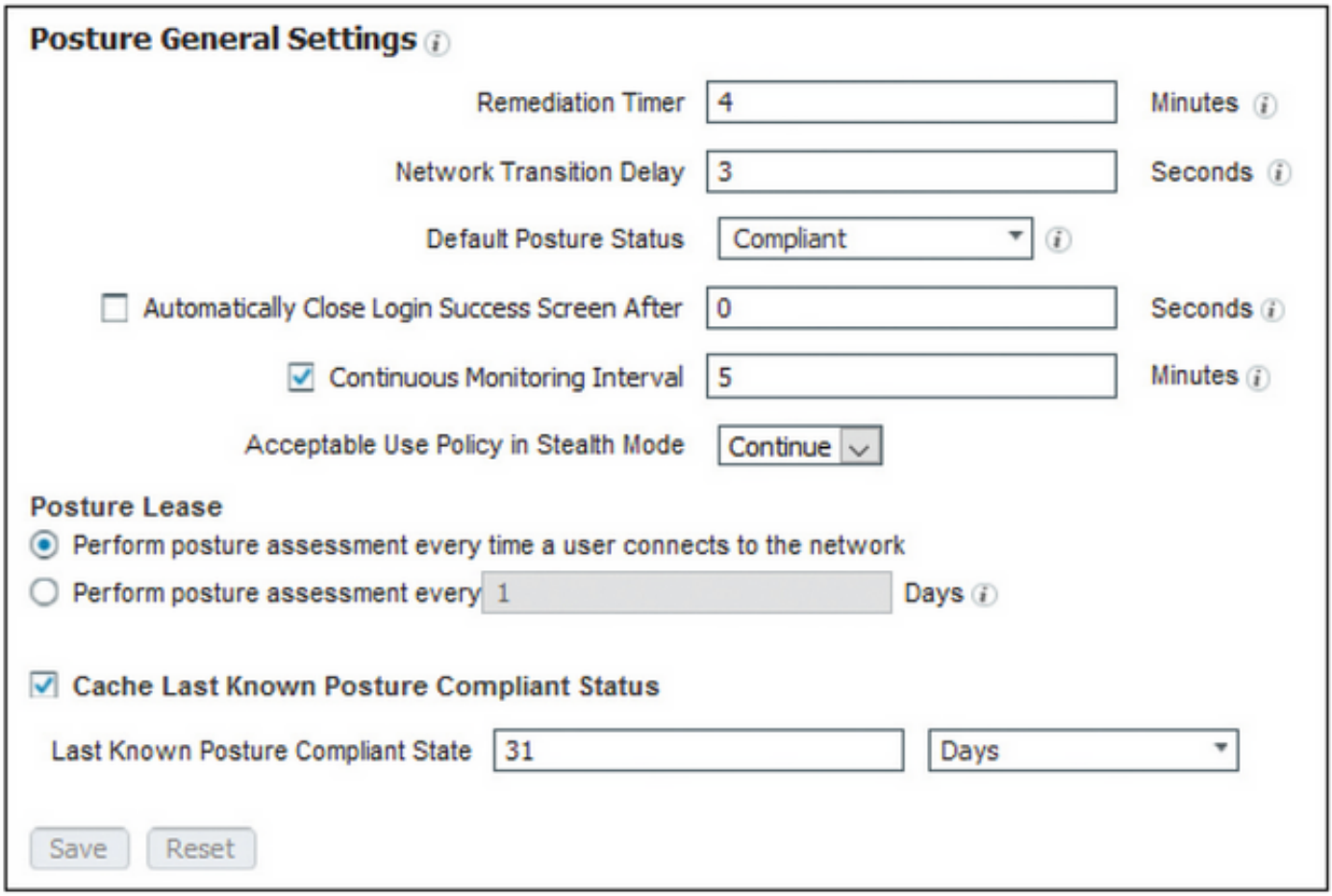
步驟33.選擇**Work Centers > Posture > Posture Policy**

步驟34.選擇Edit on any policy，然後選擇Insert New policy Define **LinuxPosturePolicy Policy作為名稱，並確保新增您在步驟32中建立的需求。**



步驟35.選擇**完成**並保存

其他重要狀態設定（「狀態常規設定」部分）



安全評估常規設定部分中的重要設定如下：

- **修正計時器**:此設定定義客戶端更正故障狀態條件所需的時間。AnyConnect配置中還有補救計時器；此計時器用於ISE，而不是AnyConnect。
- **預設狀態狀態**:此設定為沒有狀態代理的裝置或無法運行臨時代理的作業系統（例如基於Linux的作業系統）提供狀態狀態。
- **連續監視間隔**:此設定適用於清點端點的應用程式和硬體條件。該設定指定AnyConnect必須傳送監控資料的頻率。
- **隱藏模式中的可接受使用策略**:此設定僅有的兩個選項是阻止或繼續。如果未確認AUP，則阻止隱藏模式AnyConnect客戶端繼續。繼續操作允許隱身模式客戶端在不確認AUP的情況下繼續操作（使用AnyConnect的隱身模式設定時，AUP通常是其意圖）。

重新評估配置

狀況重新評估是狀況工作流程的重要組成部分。您在「終端安全評估協定」一節中看到了如何配置

AnyConnect代理進行終端安全評估的功能。代理定期檢查基於該配置中的計時器定義的PSN。

當請求到達PSN時，PSN會根據該終端角色的ISE配置確定是否需要狀態重新評估。如果客戶端通過重新評估，則PSN會保持終端的狀態符合狀態，並且狀態租用會被重置。如果終端未通過重新評估，狀態狀態將更改為不合規狀態，並且已經存在的任何狀態租賃都會被刪除。

步驟36.選擇**Policy > Policy Elements > Results > Authorization > Authorization Profile**。選擇**新增**

步驟37.將**Wired_Redirect定義為授權配置檔案，並配置下一個引數**

步驟38.選擇保存

步驟39.配置授權策略

安全狀態有三種預配置的授權規則：

1. 第一個配置為在身份驗證成功時匹配，並且裝置的合規性未知。
2. 第二個規則將成功的身份驗證與不符合的終端相匹配。

   附註：前兩個規則具有相同的結果，即使用預配置的授權配置檔案，該配置檔案將終端重定向到客戶端調配門戶。

3. 最終規則匹配成功的身份驗證和狀態相容終端，並使用預構建的PermitAccess授權配置檔案。

選擇**Policy > Policy** Set，然後為前一實驗中的**Wired 802.1x - MAB** Created選擇右箭頭。

步驟40.選擇Authorization Policy並建立下一個規則

交換器上的組態

附註：以下配置是指IBNS 1.0。支援IBNS 2.0的交換機可能有差異。它包括低影響模式部署。

```
username <admin> privilege 15 secret <password>
aaa new-model
```

```
!
aaa group server radius RAD_ISE_GRP
server name <isepsnnode_1> server name ! aaa authentication dot1x default group RAD_ISE_GRP aaa
authorization network default group RAD_ISE_GRP aaa accounting update periodic 5 aaa accounting
dot1x default start-stop group RAD_ISE_GRP aaa accounting dot1x default start-stop group
RAD_ISE_GRP ! aaa server radius dynamic-author client server-key client server-key ! aaa
session-id common ! authentication critical recovery delay 1000 access-session template monitor
epm logging ! dot1x system-auth-control dot1x critical eapol ! # For Access Interfaces:
interface range GigabitEthernetx/y/z - zz
 description VOICE-and-Data
 switchport access vlan
 switchport mode access
 switchport voice vlan
 ip access-group ACL_DEFAULT in
 authentication control-direction in # If supported
 authentication event fail action next-method
 authentication host-mode multi-auth
 authentication open
 authentication order dot1x mab
 authentication priority dot1x mab
 authentication port-control auto

 # Enables preiodic re-auth, default = 3,600secs
 authentication periodic
 # Configures re-auth and inactive timers to be sent by the server
 authentication timer reauthenticate server
 authentication timer inactivity server
 authentication violation restrict
 mab
 snmp trap mac-notification change added
 snmp trap mac-notification change removed
 dot1x pae authenticator
 dot1x timeout tx-period 10
 dot1x timeout server-timeout 10
 dot1x max-req 3
 dot1x max-reauth-req 3
 auto qos trust

# BEGIN - Dead Server Actions -
 authentication event server dead action authorize vlan
 authentication event server dead action authorize voice
 authentication event server alive action reinitialize
# END - Dead Server Actions -
 spanning-tree portfast
!

# ACL_DEFAULT #
! This ACL can be customized to your needs, this is the very basic access allowed prior
! to authentication/authorization. Normally ICMP, Domain Controller, DHCP and ISE
! http/https/8443 is included. Can be tailored to your needs.
!
ip access-list extended ACL_DEFAULT
 permit udp any eq bootpc any eq bootps
 permit udp any any eq domain
 permit icmp any any
 permit udp any any eq tftp
 permit ip any host
 permit ip any host
 permit tcp any host  eq www
 permit tcp any host  eq 443
 permit tcp any host  eq 8443
 permit tcp any host  eq www
 permit tcp any host  eq 443
 permit tcp any host  eq 8443
```

```
!
# END-OF ACL_DEFAULT #
!

# ACL_REDIRECT #
! This ACL can be customized to your needs, this ACL defines what is not redirected
! (with deny statement) to the ISE. This ACL is used for captive web portal,
! client provisioning, posture remediation, and so on.
!
ip access-list extended ACL_REDIRECT_AV
 remark Configure deny ip any host  to allow access to
 deny   udp any any eq domain
 deny   tcp any any eq domain
 deny   udp any eq bootps any
 deny   udp any any eq bootpc
 deny   udp any eq bootpc any
 remark deny redirection for ISE CPP/Agent Discovery
 deny   tcp any host  eq 8443
 deny   tcp any host  eq 8905
 deny   udp any host  eq 8905
 deny   tcp any host  eq 8909
 deny   udp any host  eq 8909
 deny   tcp any host  eq 8443
 deny   tcp any host  eq 8905
 deny   udp any host  eq 8905
 deny   tcp any host  eq 8909
 deny   udp any host  eq 8909
 remark deny redirection for remediation AV servers
 deny   ip any host
 deny   ip any host
 remark deny redireciton for remediation Patching servers
 deny   ip any host
 remark redirect any http/https
 permit tcp any any eq www
 permit tcp any any eq 443
!
# END-OF ACL-REDIRECT #
!
ip radius source-interface
!
radius-server attribute 6 on-for-login-auth
radius-server attribute 6 support-multiple
radius-server attribute 8 include-in-access-req
radius-server attribute 55 include-in-acct-req
radius-server attribute 55 access-request include
radius-server attribute 25 access-request include
radius-server attribute 31 mac format ietf upper-case
radius-server attribute 31 send nas-port-detail
radius-server vsa send accounting
radius-server vsa send authentication
radius-server dead-criteria time 30 tries 3
!
ip http server
ip http secure-server
ip http active-session-modules none
ip http secure-active-session-modules none
!
radius server
 address ipv4  auth-port 1812 acct-port 1813
 timeout 10
 retransmit 3
 key
!
radius server
```

```
 address ipv4  auth-port 1812 acct-port 1813
 timeout 10
 retransmit 3
 key
!
aaa group server radius RAD_ISE_GRP
 server name
 server name
!
mac address-table notification change
mac address-table notification mac-move
```

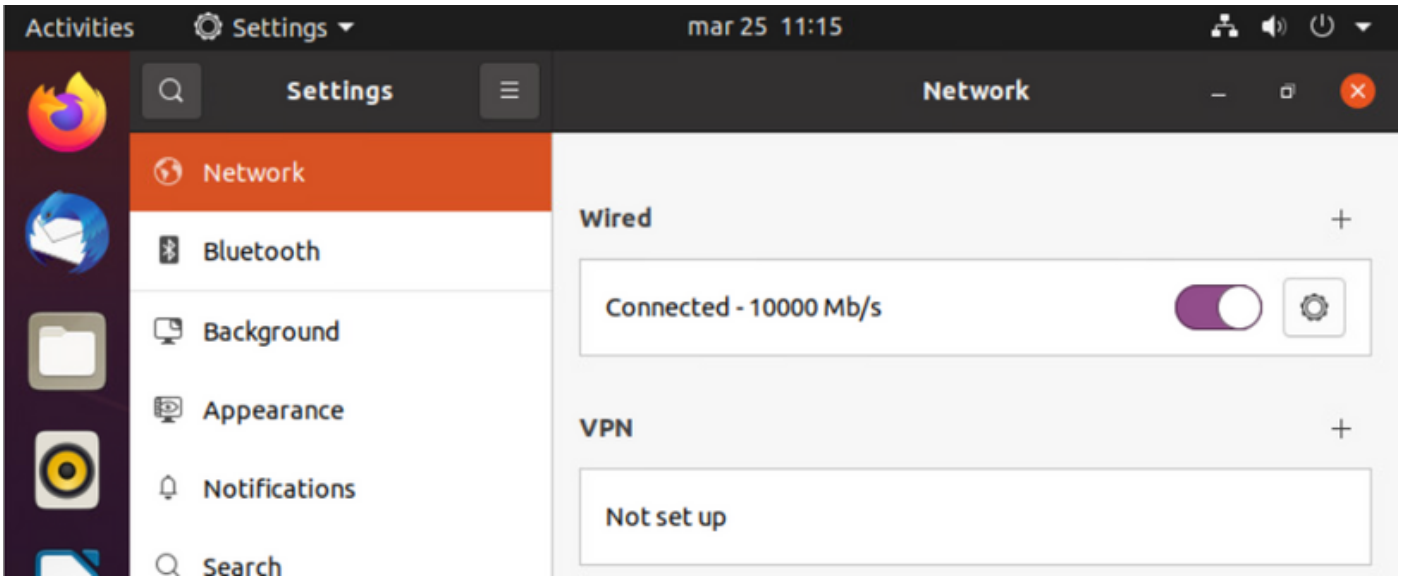
驗證

ISE驗證：

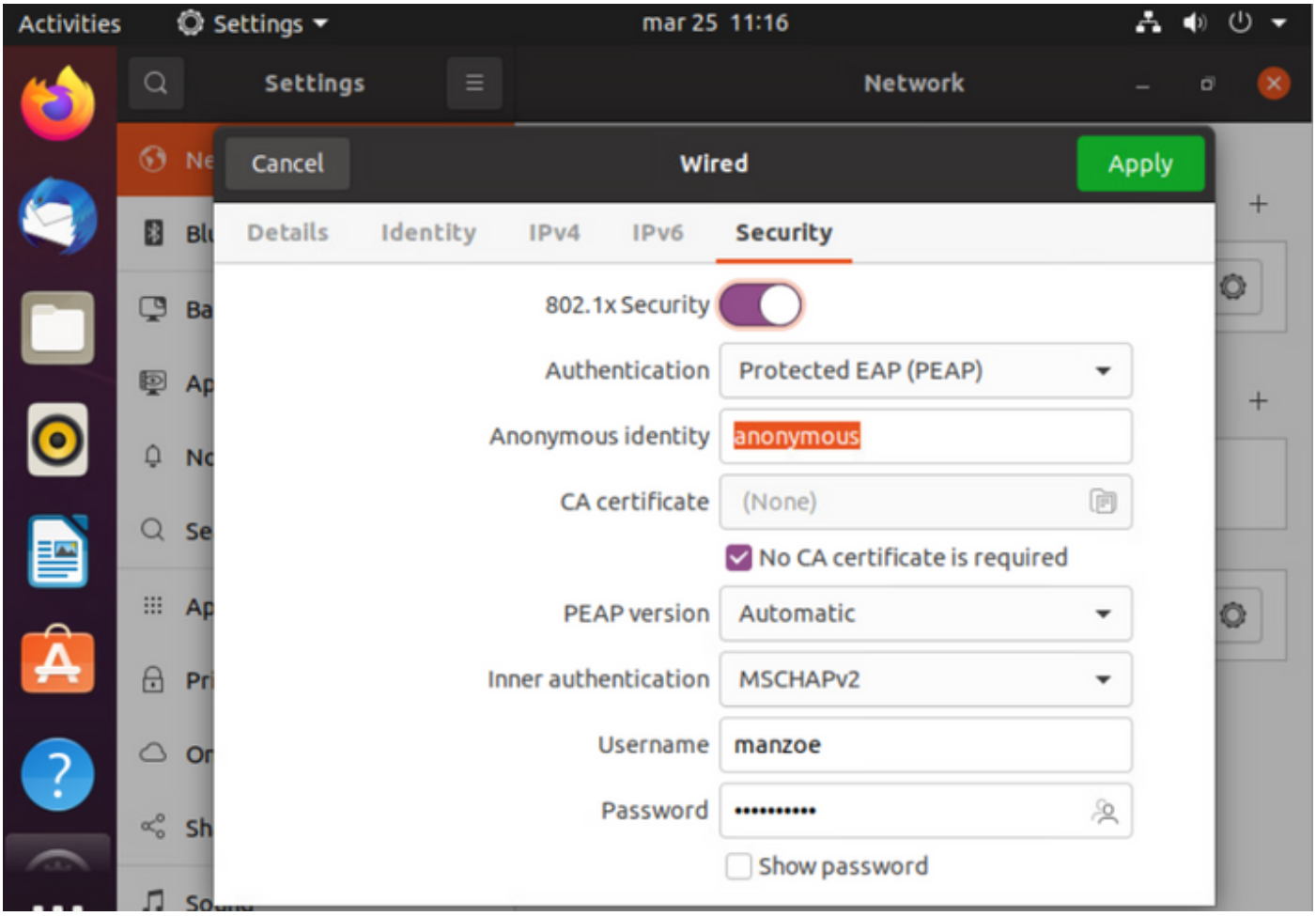
本節假設之前已在Linux系統上安裝了帶有ISE狀態模組的AnyConnect。

使用dot1x驗證PC

步驟1.導覽至Network Settings

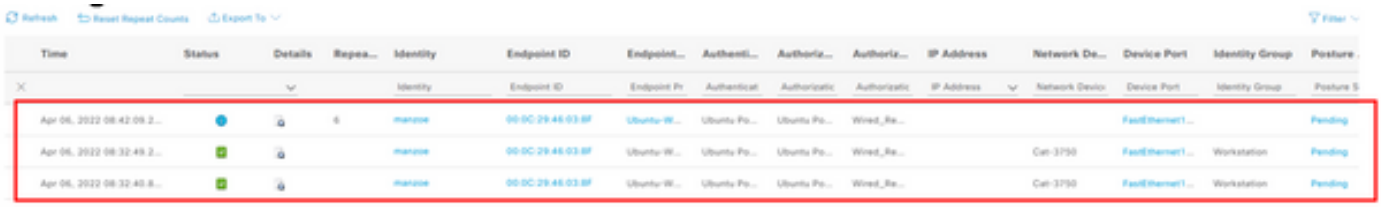


步驟2.選擇Security頁籤並提供802.1x配置和使用者憑據

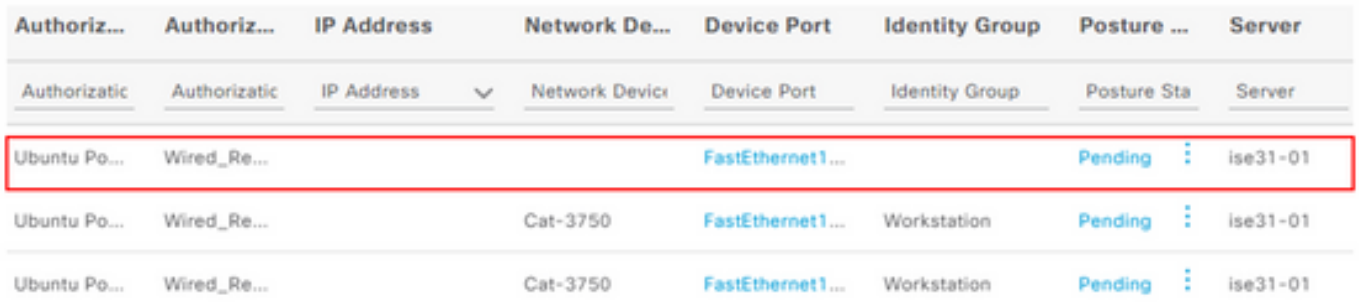


步驟3.按一下「**Apply**」。

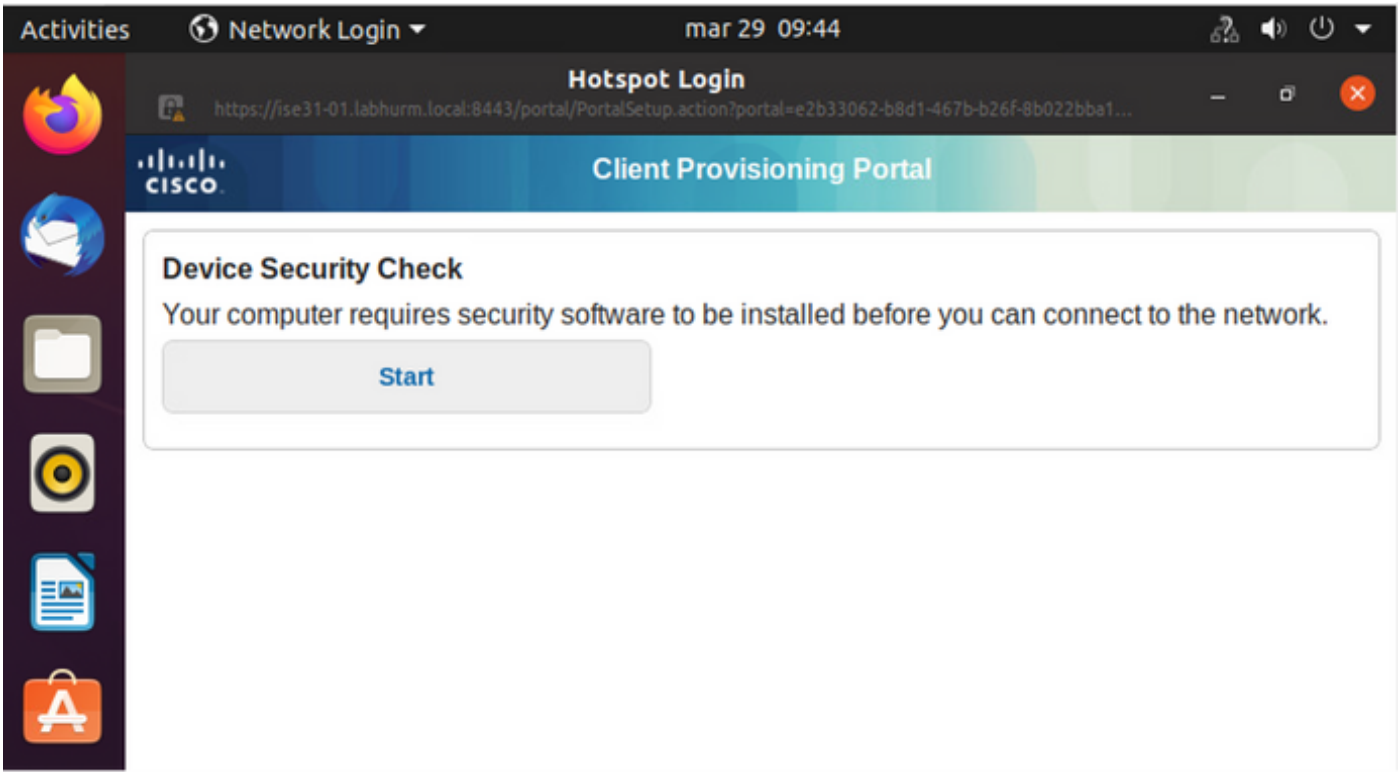
步驟4.將Linux系統連線到802.1x有線網路並在ISE即時日誌中驗證：



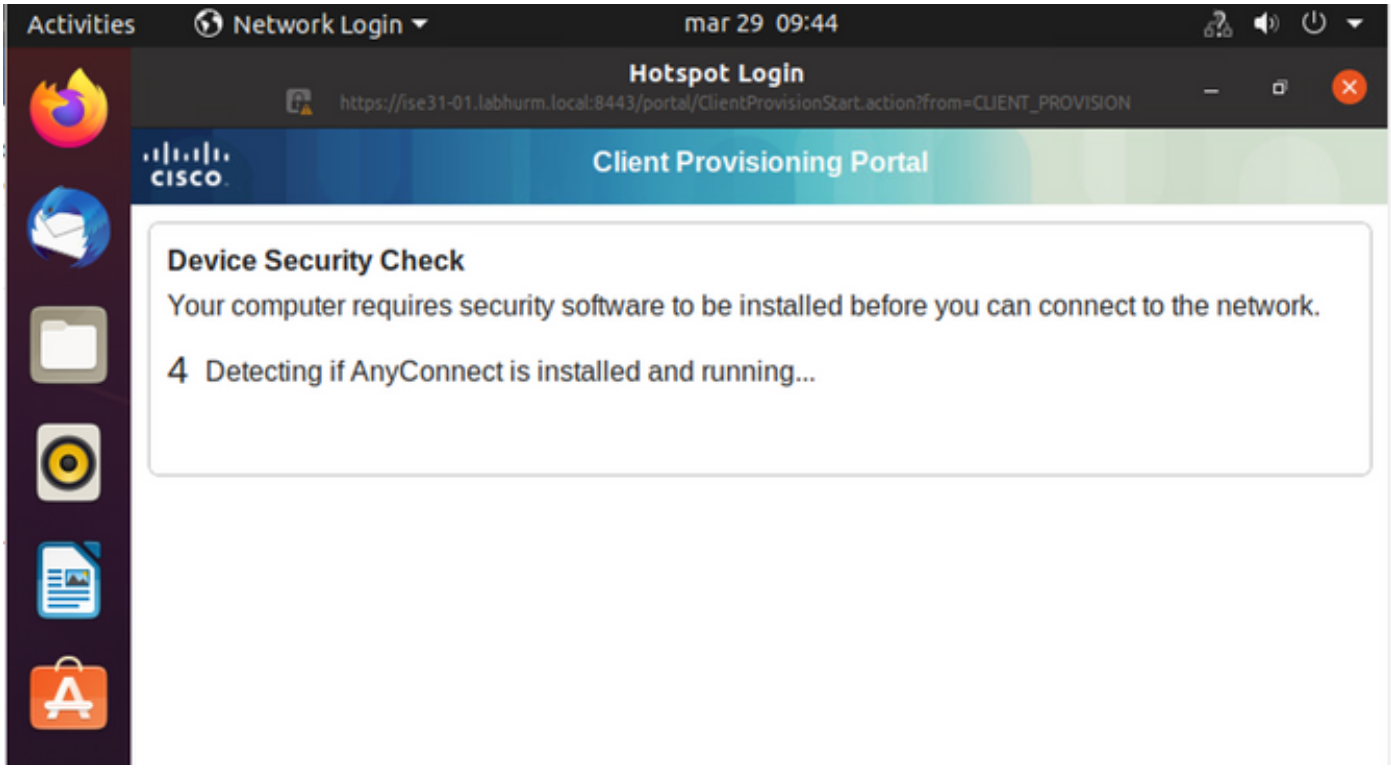
在ISE中，使用水準捲軸檢視其他資訊，例如提供流量的PSN或狀態狀態：



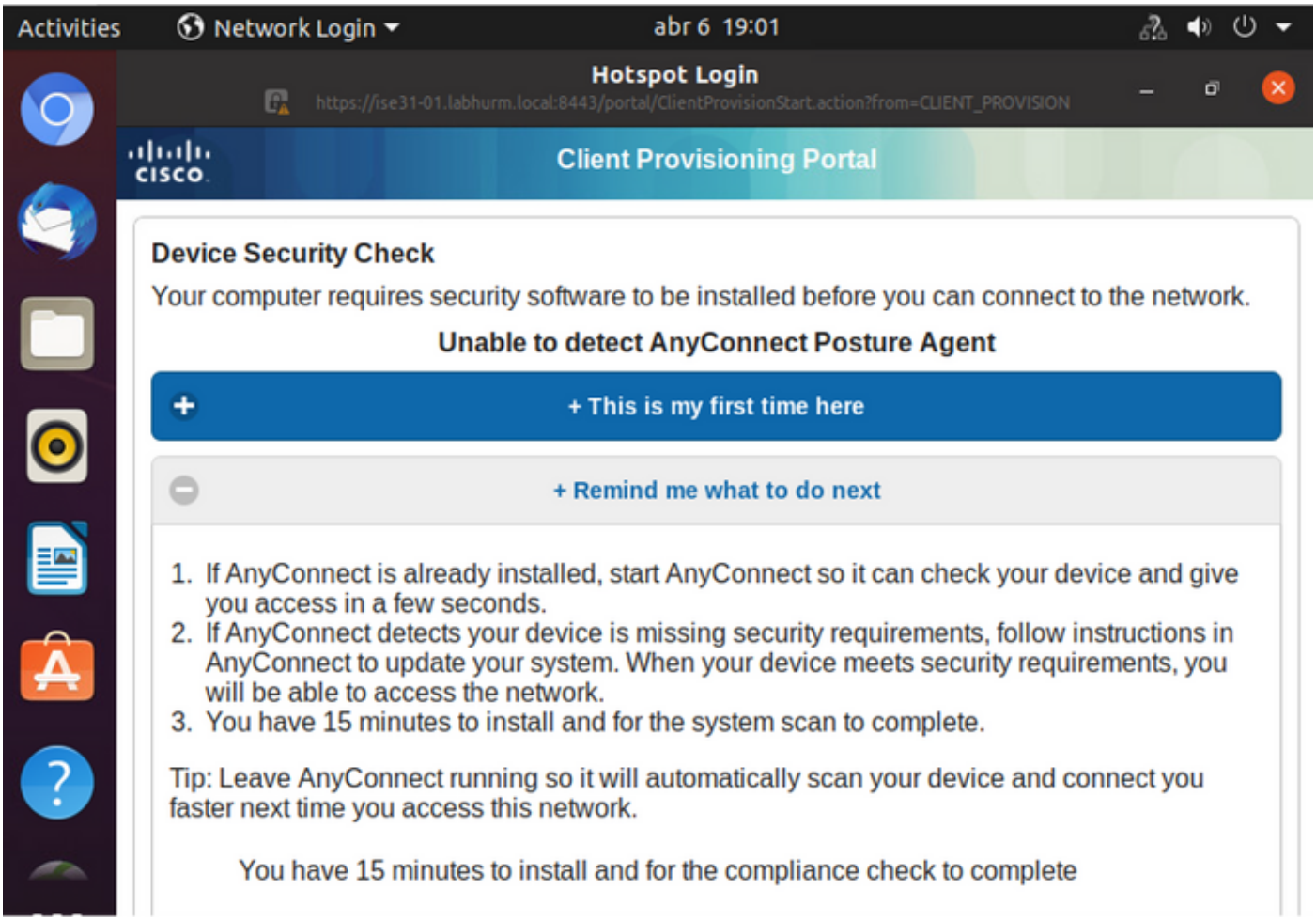
步驟5.在 Linux使用者端**上**，必須發生重新導向，且會提供使用者端布建入口網站，指示進行狀態檢查並單**擊「開始」**：



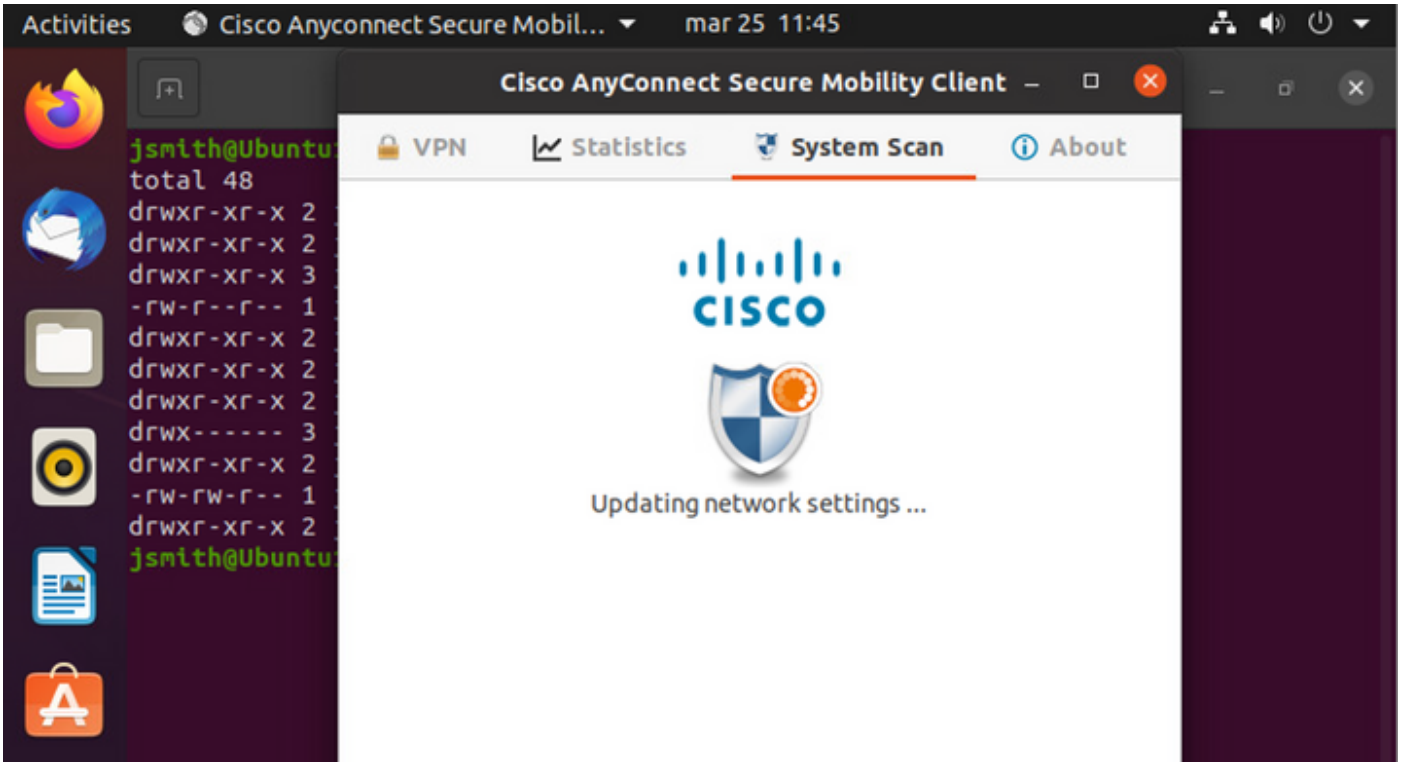
聯結器嘗試檢測AnyConnect時，請等待幾秒鐘：



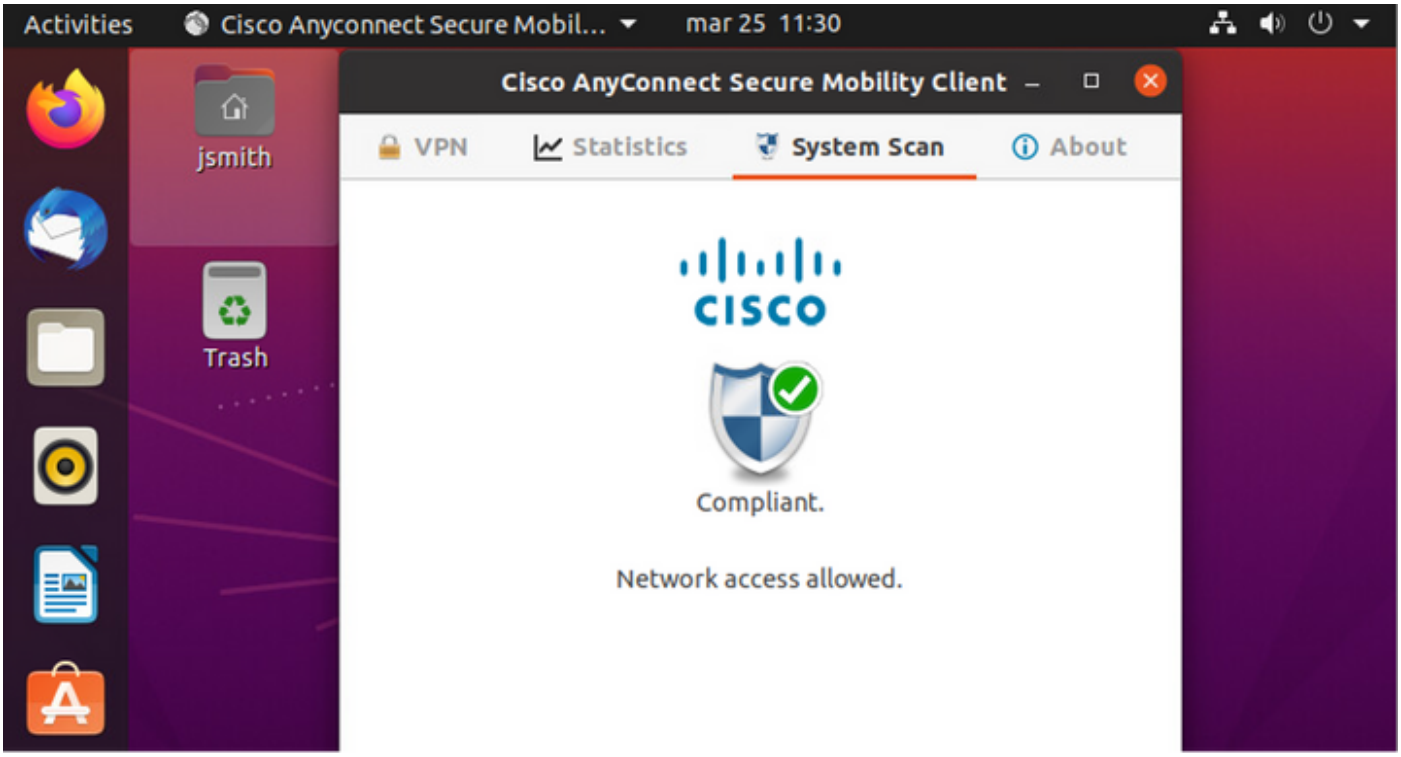
由於存在已知警告，即使安裝了AnyConnect，它也不會檢測到它。使用**Alt-Tab**或**活動**選單切換到AnyConnect客戶端。

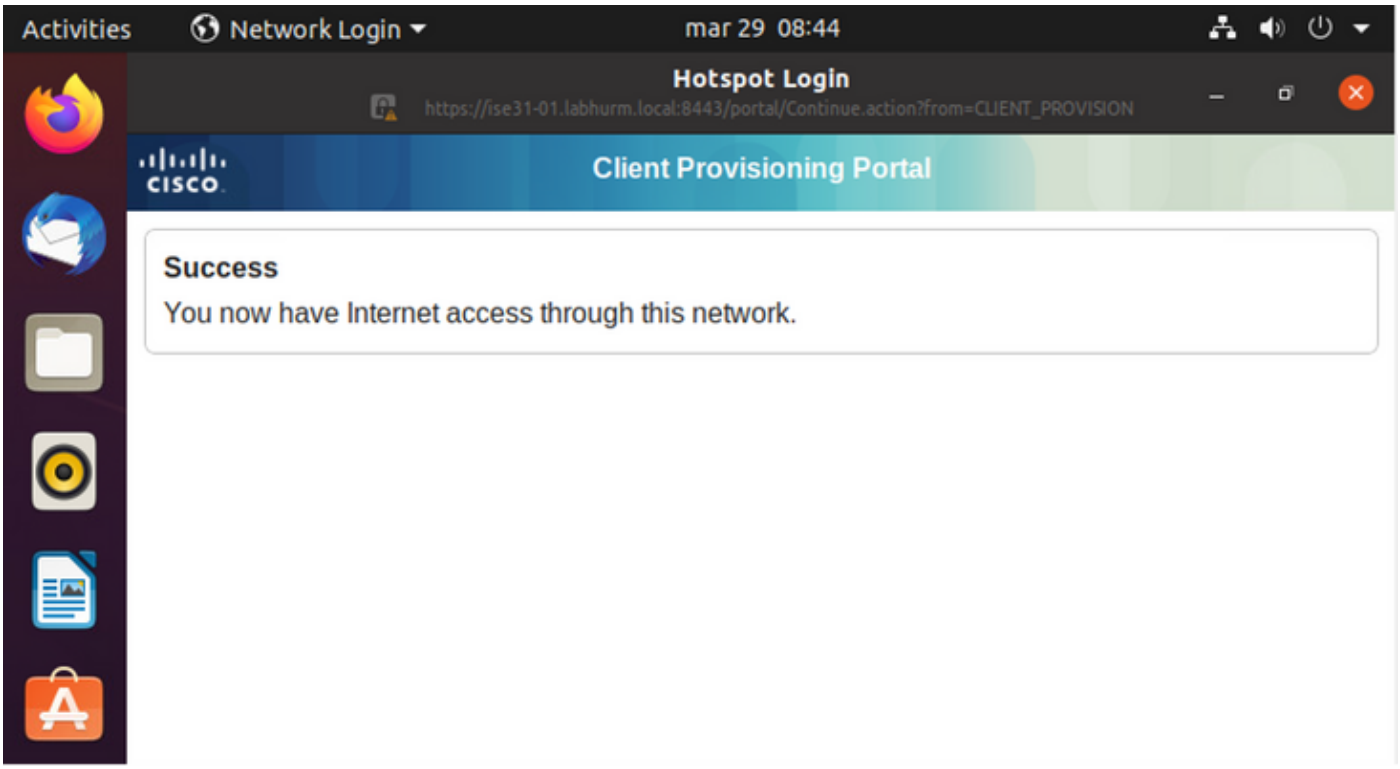


AnyConnect嘗試訪問PSN獲取終端安全評估策略，並根據該策略評估終端。



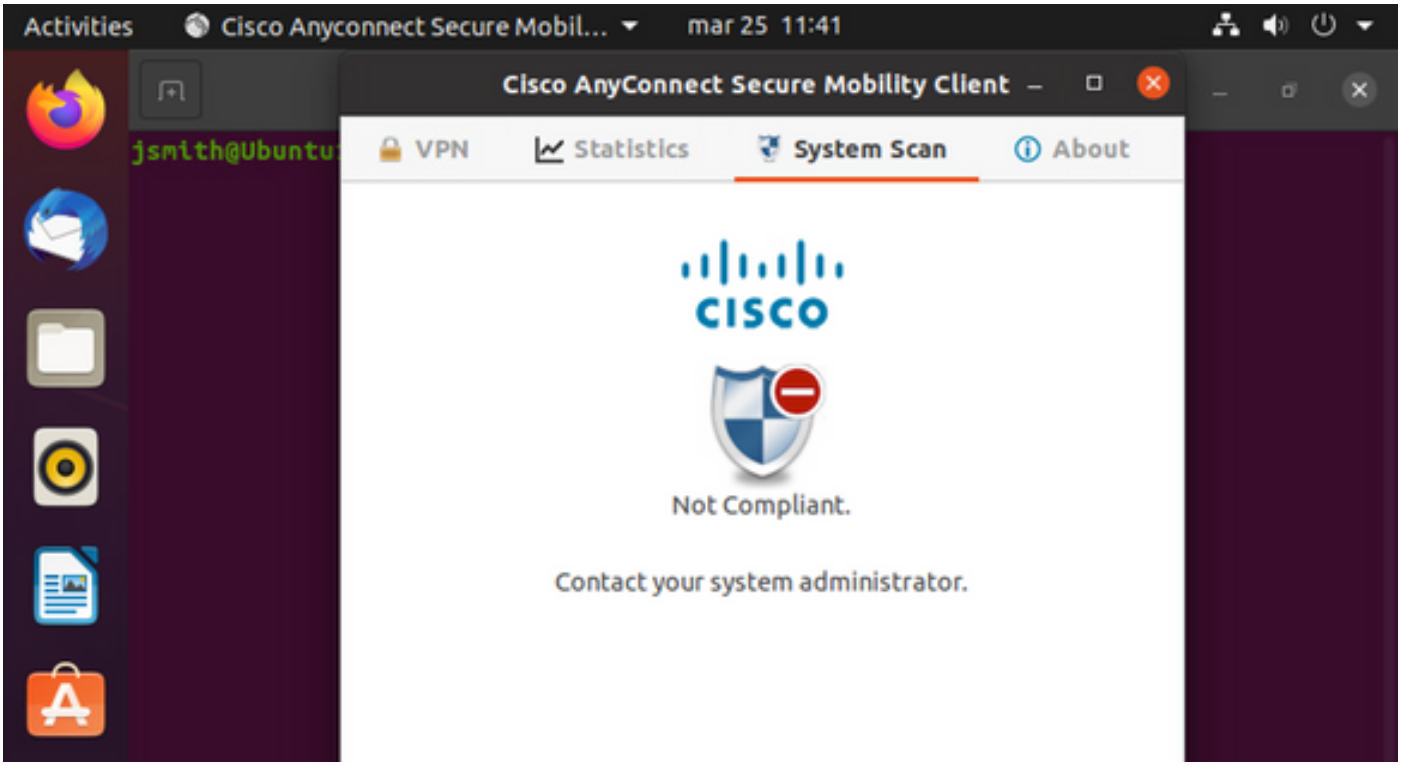
AnyConnect將其安全評估策略的確定報告回ISE。在這種情況下，符合





Endpoint Profile	Authenti...	Authorizati...	Authorization P...	IP Address	Network De...	Device Port	Identity Group	Posture Status	Server
Endpoint Profile	Authenticat	Authorization I	Authorization Profile	IP Address	Network Devic	Device Port	Identity Group	Posture Status	Server
Ubuntu-Workstation	Wired Mer...	Wired Merak...	PermitAccess	192.168.200.12				Compliant	ise31-01
Ubuntu-Workstation	Wired Mer...	Wired Merak...	PermitAccess		Mraki-SW		Workstation	Compliant	ise31-01
Ubuntu-Workstation	Wired Mer...	Wired Merak...	PermitAccess		Mraki-SW		Workstation	Compliant	ise31-01

另一方面，如果檔案不存在，AnyConnect終端安全評估模組會將確定結果報告給ISE



Endpoint...	Authenti...	Authoriz...	Authoriz...	IP Address	Network De...	Device Port	Identity Group	Posture Status	Server	Mdm S
Endpoint Pr	Authenticat	Authorizatic	Authorizatic	IP Address	Network Devic	Device Port	Identity Group	Posture Status	Server	Mdm S
Ubuntu-W...	Ubuntu Po...	Ubuntu Po...	Wired_Re...	192.168.101.51		FastEthernet1...		NonCompliant	ise31-01	
Ubuntu-W...	Ubuntu Po...	Ubuntu Po...	Wired_Re...	192.168.101.51	Cat-3750	FastEthernet1...	Workstation	NonCompliant	ise31-01	

附註：ISE FQDN需要通過DNS或本地主機檔案在Linux系統上可解析。

疑難排解

```
show authentication sessions int fa1/0/35
```

重定向到位：

```
LABDEMOAC01#show authentication sessions interface fastEthernet 1/0/35
            Interface:  FastEthernet1/0/35
          MAC Address:  000c.2946.038f
           IP Address:  192.168.101.51
            User-Name:  manzoe
               Status:  Authz Success
               Domain:  DATA
      Security Policy:  Should Secure
      Security Status:  Unsecure
       Oper host mode:  multi-auth
     Oper control dir:  both
        Authorized By:  Authentication Server
          Vlan Group:  N/A
     URL Redirect ACL:  ACL_REDIRECT_AV
         URL Redirect:  https://ise31-01.labhurm.local:8443/portal/gateway?sessionId=C0A8C883000000010008044A&p
33062-b8d1-467b-b26f-8b022bba10e7&action=cpp&token=05a438ecb872ce396c2912fecfe0d2aa
       Session timeout:  N/A
          Idle timeout:  N/A
     Common Session ID:  C0A8C883000000010008044A
       Acct Session ID:  0x00000004
                Handle:  0xEB000001

Runnable methods list:
       Method   State
       dot1x    Authc Success
```

授權成功：

```
LABDEMOAC01#show authentication sessions interface fastEthernet 1/0/35
           Interface:  FastEthernet1/0/35
         MAC Address:  000c.2946.038f
          IP Address:  192.168.101.51
           User-Name:  manzoe
              Status:  Authz Success
              Domain:  DATA
     Security Policy:  Should Secure
     Security Status:  Unsecure
      Oper host mode:  multi-auth
    Oper control dir:  both
       Authorized By:  Authentication Server
          Vlan Group:  N/A
             ACS ACL:  xACSACLx-IP-PERMIT_ALL_IPV4_TRAFFIC-57f6b0d3
     Session timeout:  28800s (server), Remaining: 28739s
      Timeout action:  Reauthenticate
        Idle timeout:  N/A
   Common Session ID:  C0A8C88300000000010008044A
     Acct Session ID:  0x00000004
              Handle:  0xEB000001

Runnable methods list:
       Method   State
       dot1x    Authc Success
       mab      Not run
```

不符合要求，已移至隔離VLAN和ACL:

```
LABDEMOAC01#sh authe sess int fas1/0/35
           Interface:  FastEthernet1/0/35
         MAC Address:  000c.2946.038f
          IP Address:  192.168.101.51
           User-Name:  manzoe
              Status:  Authz Success
              Domain:  DATA
     Security Policy:  Should Secure
     Security Status:  Unsecure
      Oper host mode:  multi-auth
    Oper control dir:  both
       Authorized By:  Authentication Server
         Vlan Policy:  777
             ACS ACL:  xACSACLx-IP-DENY_ALL_IPV4_TRAFFIC-57f6b0d3
     Session timeout:  N/A
        Idle timeout:  N/A
   Common Session ID:  C0A86E0100000000000001724F
     Acct Session ID:  0x00000003
              Handle:  0x9A000000

Runnable methods list:
       Method   State
       dot1x    Authc Success
       mab      Not run
```