تكوين وضعية Cisco ISE 3.1 مع Linux

المحتويات

المقدمة

يصف هذا وثيقة الإجراء أن يشكل وينفذ سياسة وضع ملف ل Linux ومحرك خدمات الهوية (ISE).

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- AnyConnect
- محرك خدمات الهوية (ISE)
- لينكس

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- AnyConnect 4.10.05085
- ISE الإصدار 3.1 P1
- Linux Ubuntu 20.04
- محول Catalyst 3650 من Cisco. الإصدار 03.07.05.E (15.12(3)E5)

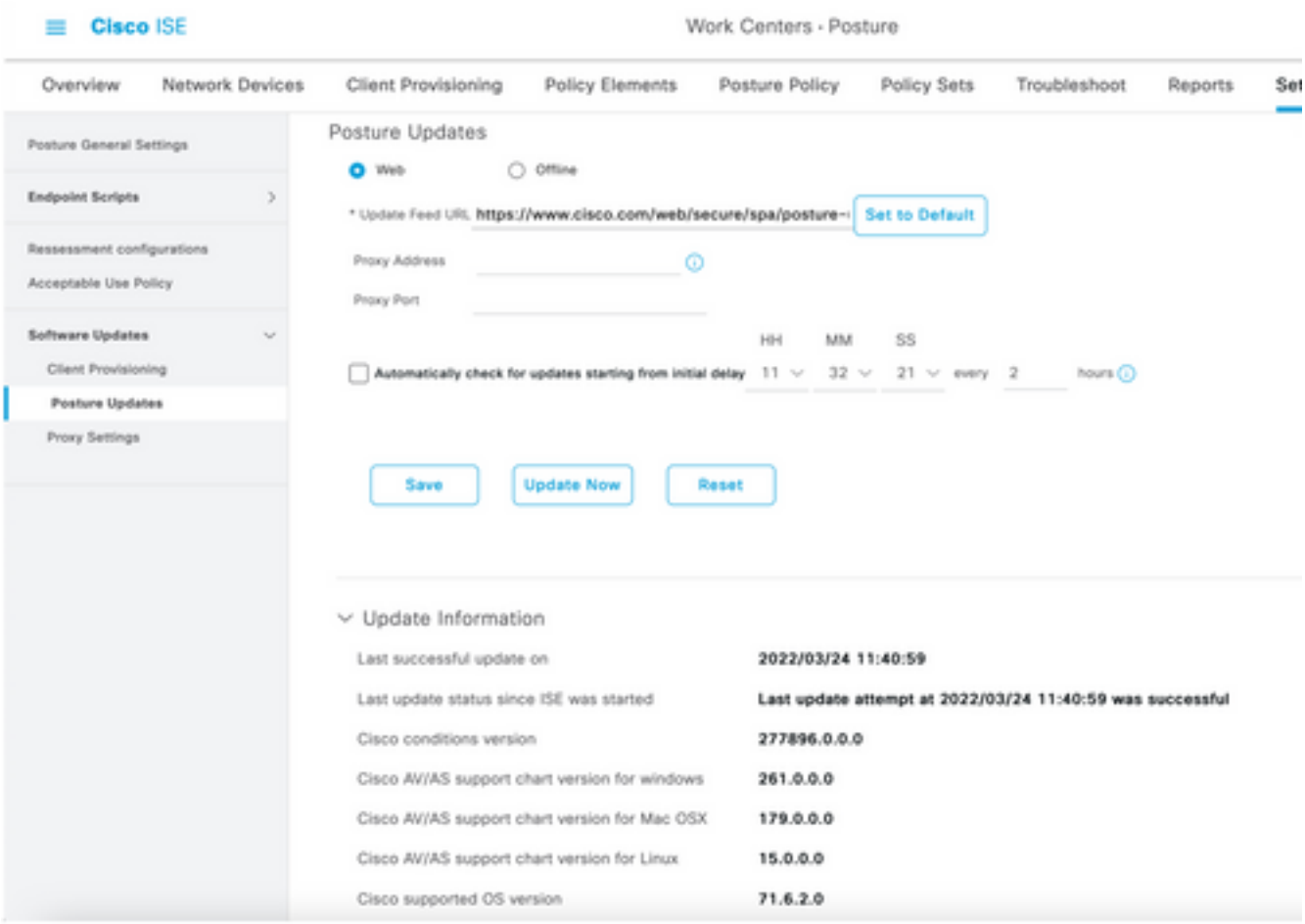
تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

التكوين

التكوينات على ISE

الخطوة 1. تحديث خدمة الوضع:

انتقل إلى مراكز العمل > الوضع > الإعدادات > تحديثات البرامج > تحديثات الوضع. حدد "تحديث" الآن وانتظر انتهاء العملية:

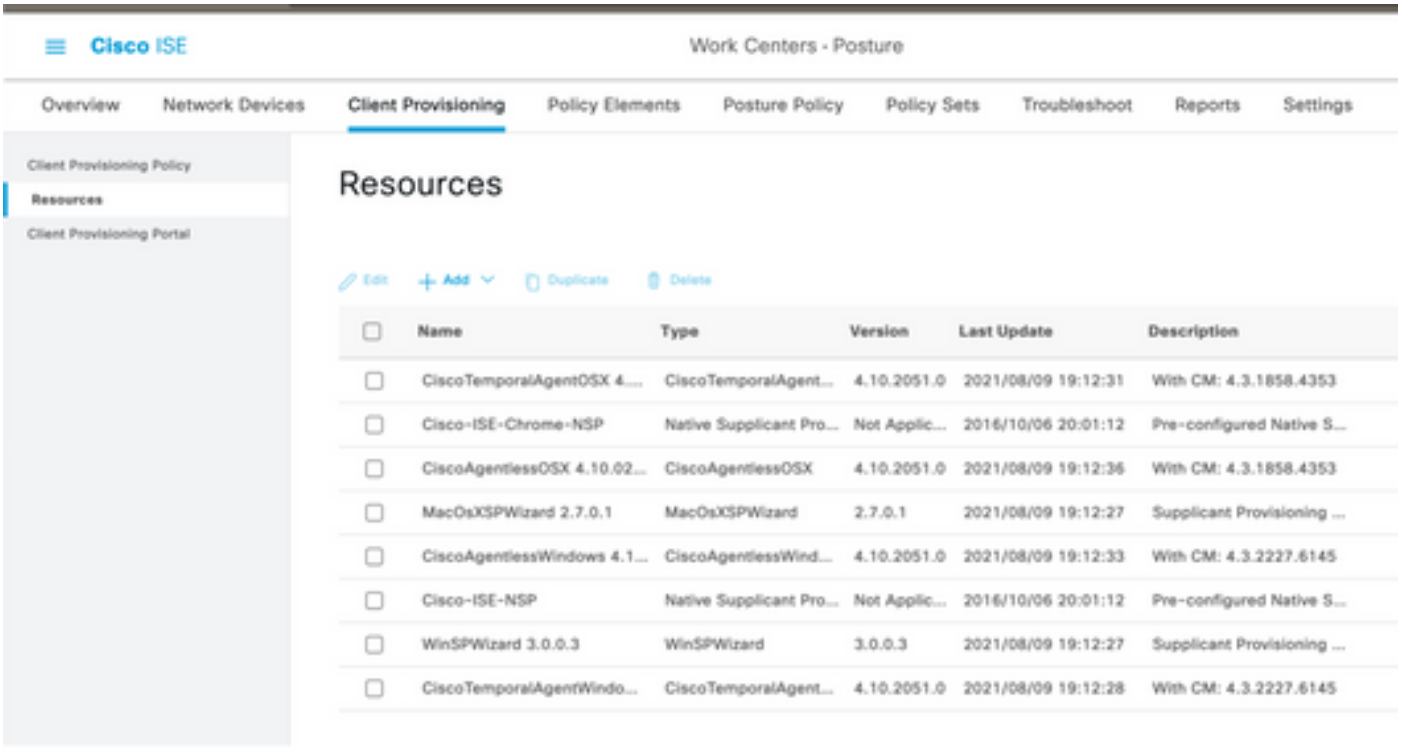


الحزمة المقدمة من Cisco هي حزمة برنامج تقوم بتنزيلها من موقع Cisco.com، مثل حزم برامج AnyConnect. الحزمة **التي أنشأها العميل** هي ملف تعريف أو تكوين أنشأته خارج واجهة مستخدم ISE وتريد تحميله إلى ISE للاستخدام مع تقييم الوضع. بالنسبة لهذا التمرين، يمكنك تنزيل حزمة AnyConnect Webdeploy "AnyConnect-Linux64-4.10.05085-webdeploy-k9.pkg".

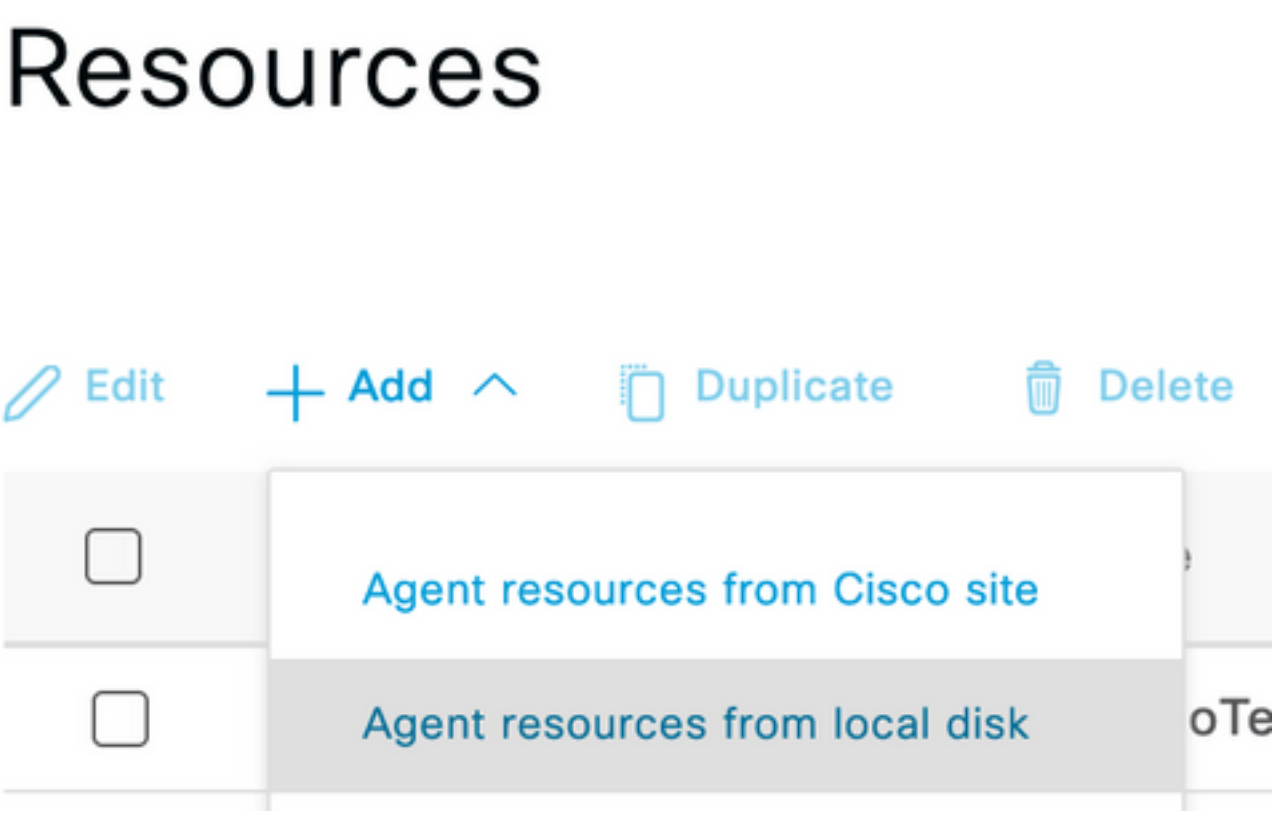
> **ملاحظة**: نظرا للتحديثات وبرامج التصحيح، يمكن تغيير الإصدار الموصى به. استخدم أحدث إصدار موصى به من الموقع cisco.com.

الخطوة 2. تحميل حزمة AnyConnect:

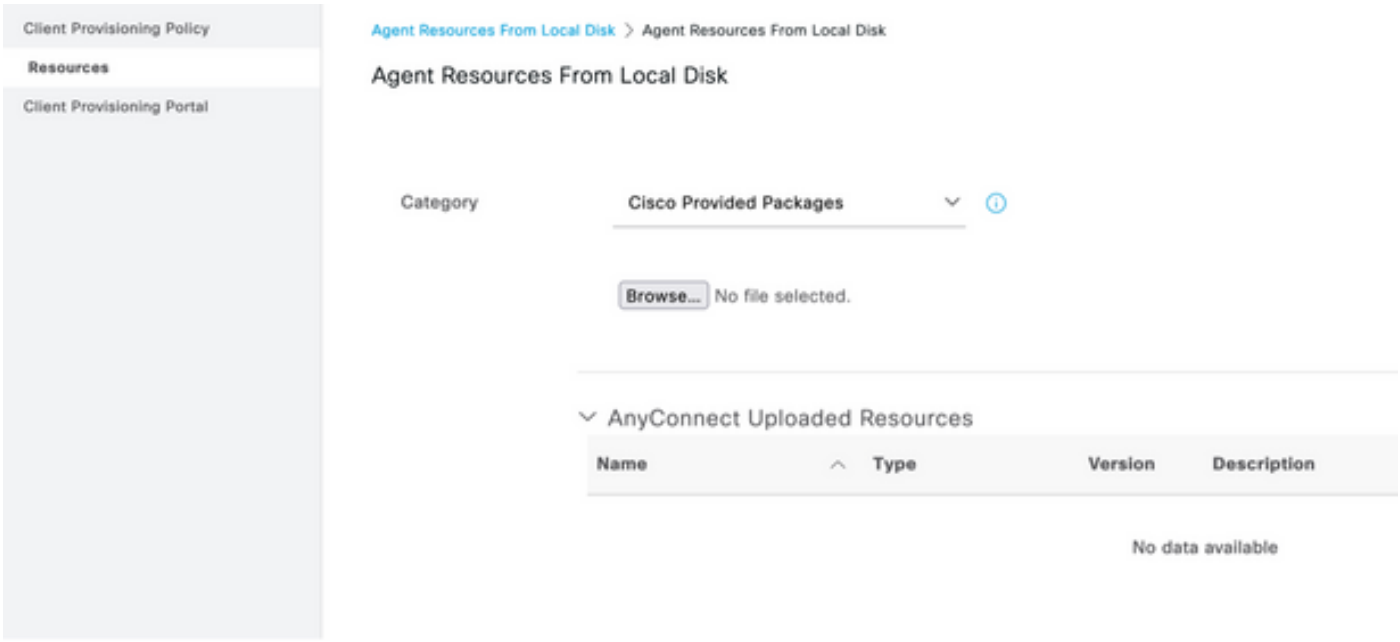
من داخل مركز عمل الوضع، انتقل إلى **إمداد العميل > الموارد**



الخطوة 3. حدد إضافة > موارد الوكيل من القرص المحلي

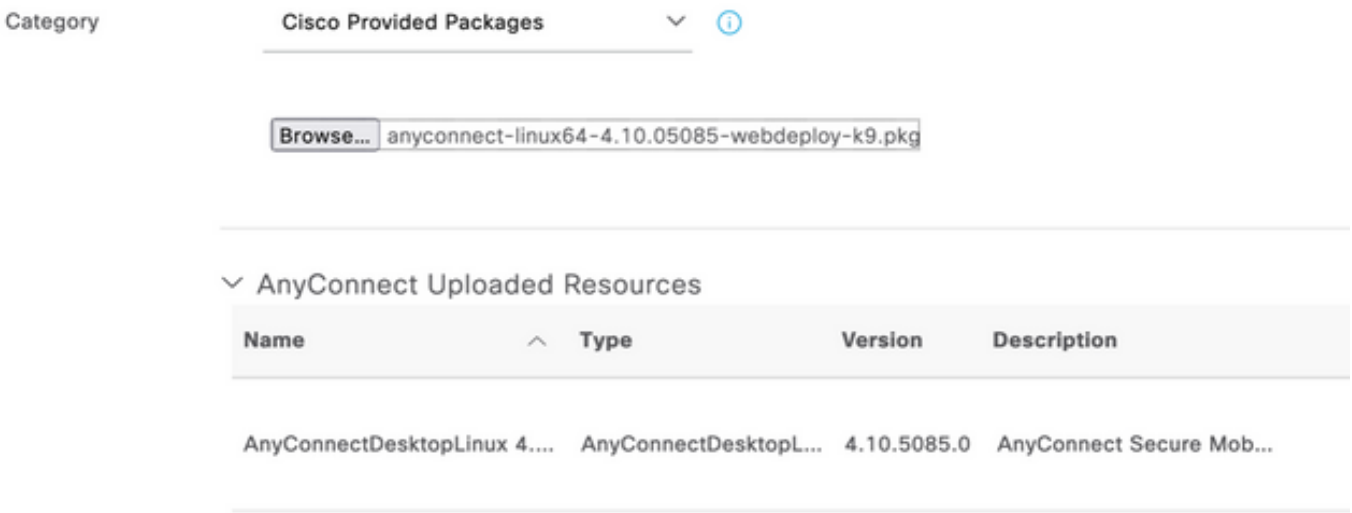


الخطوة 4. حدد **حزم Cisco المقدمة** من القائمة المنسدلة للفئة.



الخطوة 5. انقر تصفح.

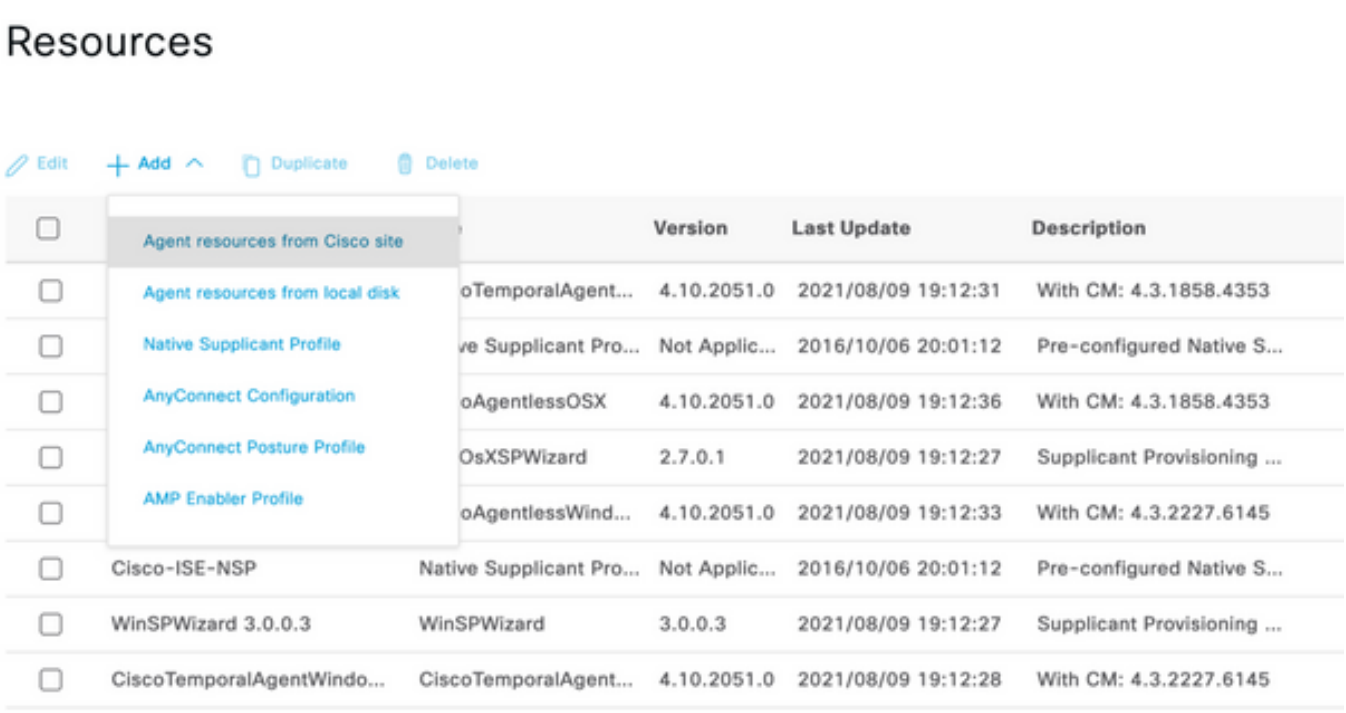
الخطوة 6. أختر أحد حزم AnyConnect التي قمت بتنزيلها في الخطوة السابقة. تتم معالجة صورة AnyConnect، ويتم عرض معلومات حول الحزمة



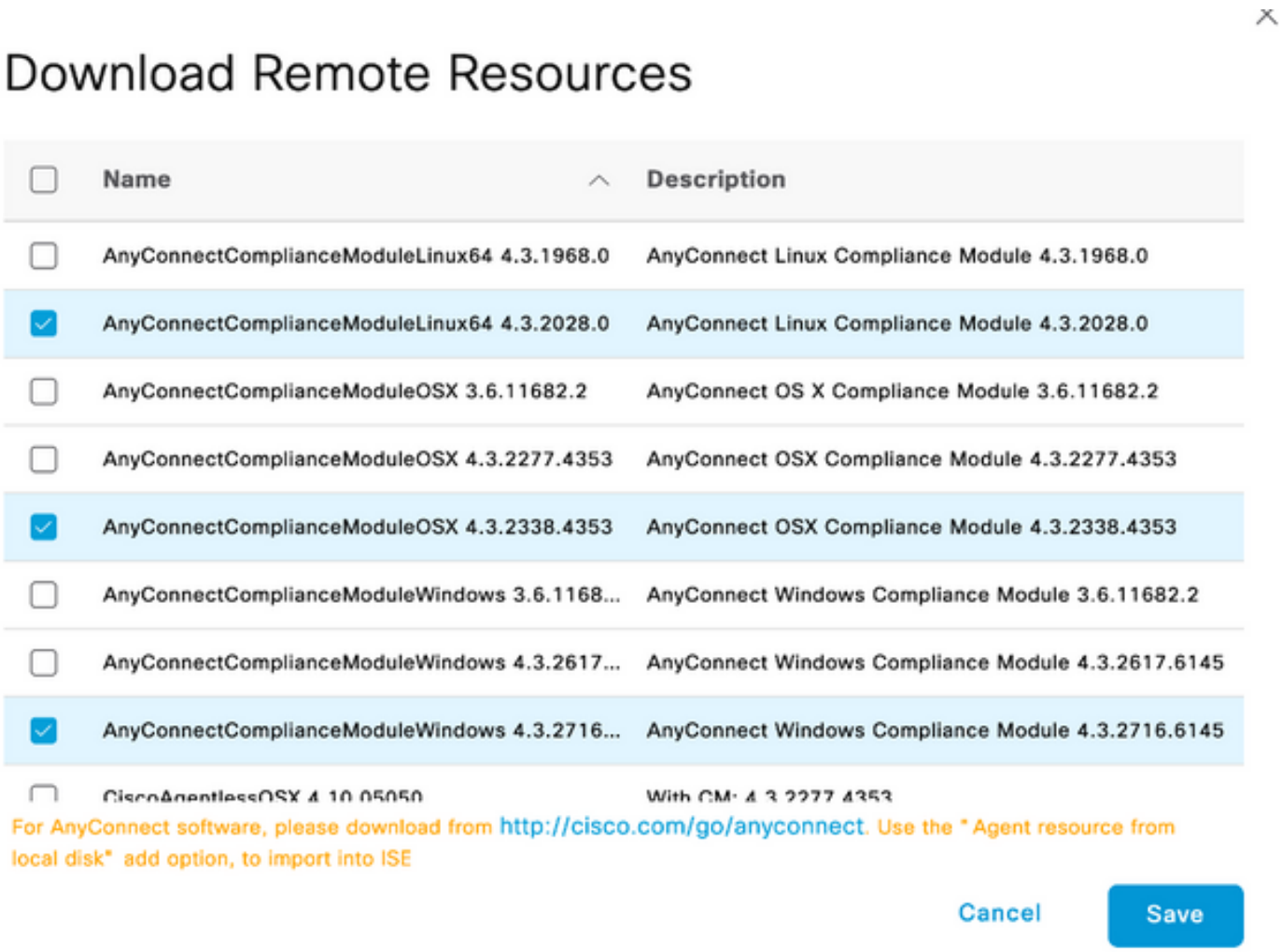
الخطوة 7. انقر على إرسال. الآن بعد تحميل AnyConnect إلى ISE، يمكنك الحصول على جهة اتصال ISE والحصول على موارد العميل الأخرى من Cisco.com.

> **ملاحظة:** تتضمن موارد العميل وحدات نمطية يستخدمها عميل AnyConnect توفر القدرة على تقييم توافق نقطة نهاية لمجموعة متنوعة من عمليات التحقق من الحالة مثل مكافحة الفيروسات وبرامج مكافحة التجسس وبرامج مكافحة البرامج الضارة وجدار الحماية وتشفير الأقراص والملف وما إلى ذلك.

الخطوة 8. انقر فوق إضافة > موارد الوكيل من موقع Cisco Site. يستغرق علم الإطار دقيقة بينما يصل ISE إلى Cisco.com ويسترجع بيانات بكل الموارد المنشورة لتزويد العميل.



الخطوة 9. حدد أحدث وحدات التوافق مع AnyConnect لنظام التشغيل Linux. بالإضافة إلى ذلك، يمكنك أيضا تحديد وحدة التوافق النمطية ل Windows و Mac.



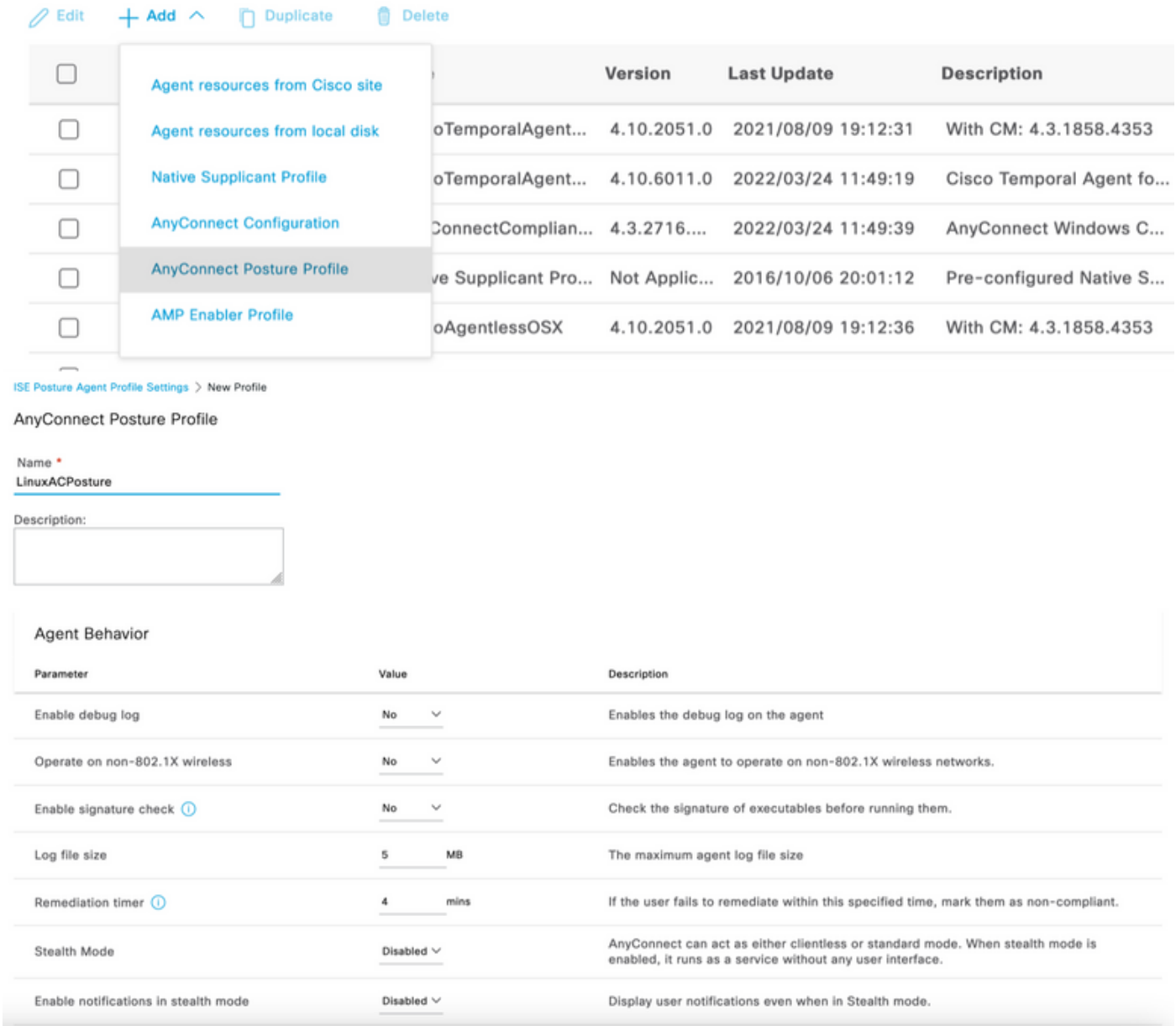
الخطوة 10. حدد أحدث الوكلاء المؤقتين ل Windows و Mac.

الخطوة 11. طقطقة حفظ.

ملاحظة: توجد تكوينات MAC و Windows Posture خارج نطاق دليل التكوين هذا.

عند هذه النقطة، لقد قمت بتحميل وتحديث جميع الأجزاء المطلوبة. لقد حان الوقت الآن لإنشاء التكوين والتوصيفات المطلوبة لاستخدام هذه المكونات.

الخطوة 12. انقر على إضافة > وكيل NAC أو توصيف AnyConnect Posture.



المعلمات التي يجب تعديلها هي:

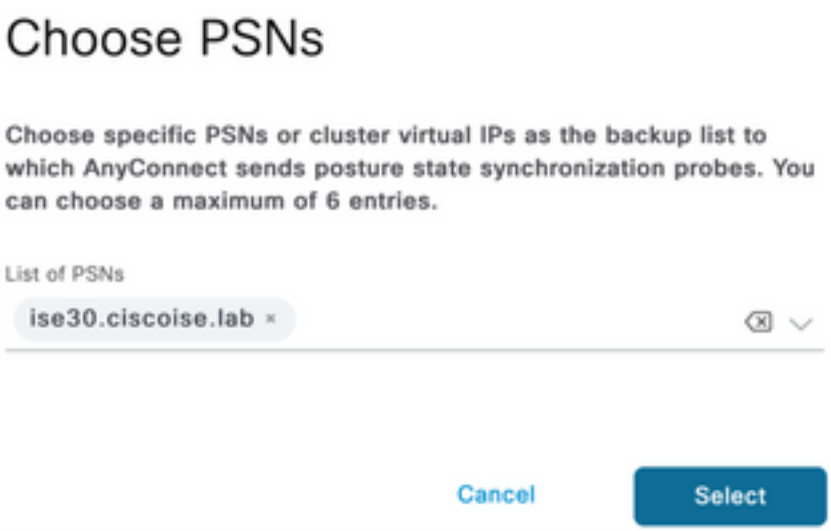
- **الفاصل الزمني لاكتشاف شبكة VLAN**: يمكنك هذا الإعداد من تعيين عدد الثواني التي ينتظرها الوحدة النمطية بين التحقق من تغييرات شبكة VLAN. التوصية هي 5 ثوان.
- **ping أو ARP**: هذه هي طريقة اكتشاف تغيير شبكة VLAN الفعلية. يمكن أن يقوم الوكيل بإختبار اتصال البوابة الافتراضية أو مراقبة ذاكرة تخزين ARP المؤقتة لإدخال البوابة الافتراضية للمهلة أو كليهما. الإعداد الموصى به هو ARP.

- **مؤقت الإصلاح**: عندما تكون وضعية نقطة نهاية غير معروفة، يتم وضع نقطة النهاية من خلال تدفق تقييم الوضع. يستغرق إصلاح عمليات التحقق من الوضع الفاشلة وقتا؛ الوقت الافتراضي هو 4 دقائق قبل وضع عالمة على نقطة النهاية على أنها غير متوافقة، ولكن يمكن أن تتراوح القيم من 1 إلى 300 دقيقة (5 ساعات). والتوصية هي 15 دقيقة؛ بيد أن ذلك قد يتطلب إجراء تعديلات إذا كان من المتوقع أن يستغرق الإصلاح وقتا أطول.

ملاحظة: لا تدعم وضعية ملف Linux المعالجة التلقائية.

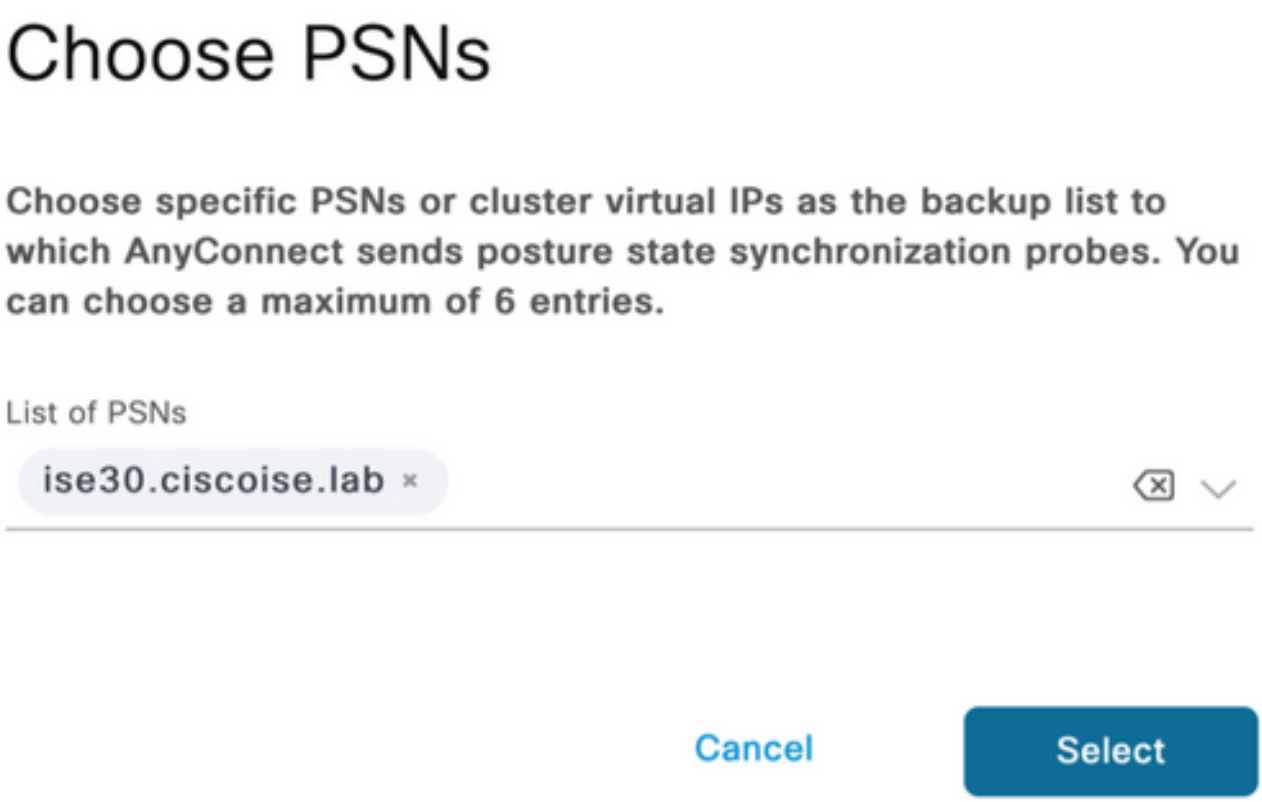
للحصول على وصف شامل لجميع المعلمات، يرجى الرجوع إلى وثائق ISE أو AnyConnect Posture.

الخطوة 13. حدد سلوك الوكيل قائمة النسخ الاحتياطي لاستكشاف الوضع وحدد إختياري، وحدد FQDN المستقل/PSN وحدد **حفظ**



الخطوة 14. تحت بروتوكولات Posture (وضعية) > مضيف الاكتشاف حدد عنوان IP للعقدة PSN/Standalone.

الخطوة 15. من **قائمة خادم النسخ الاحتياطي للاكتشاف** وحدد **الاختياري**، حدد PSN أو FQDN المستقل وحدد **التحديد.**

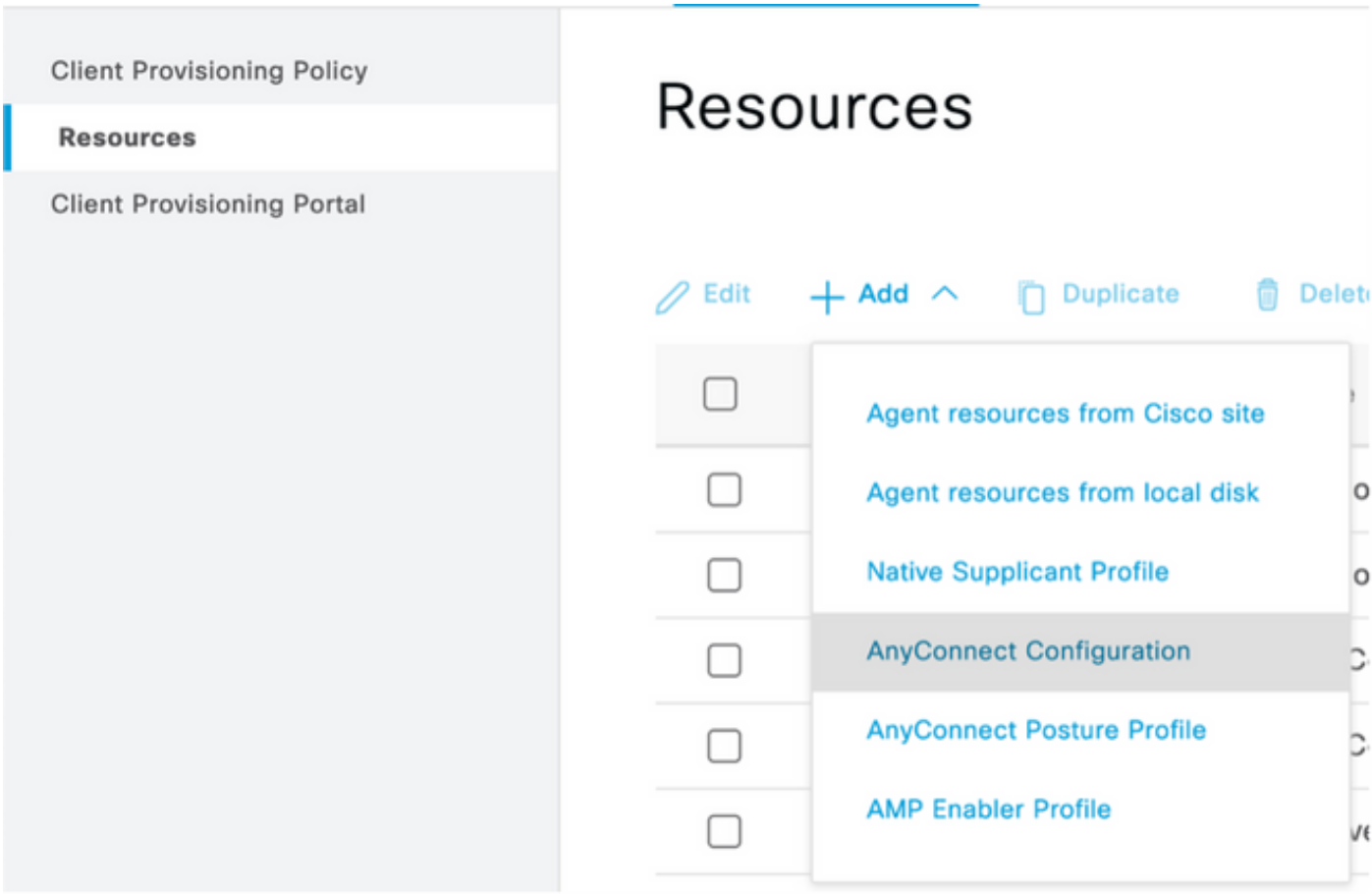


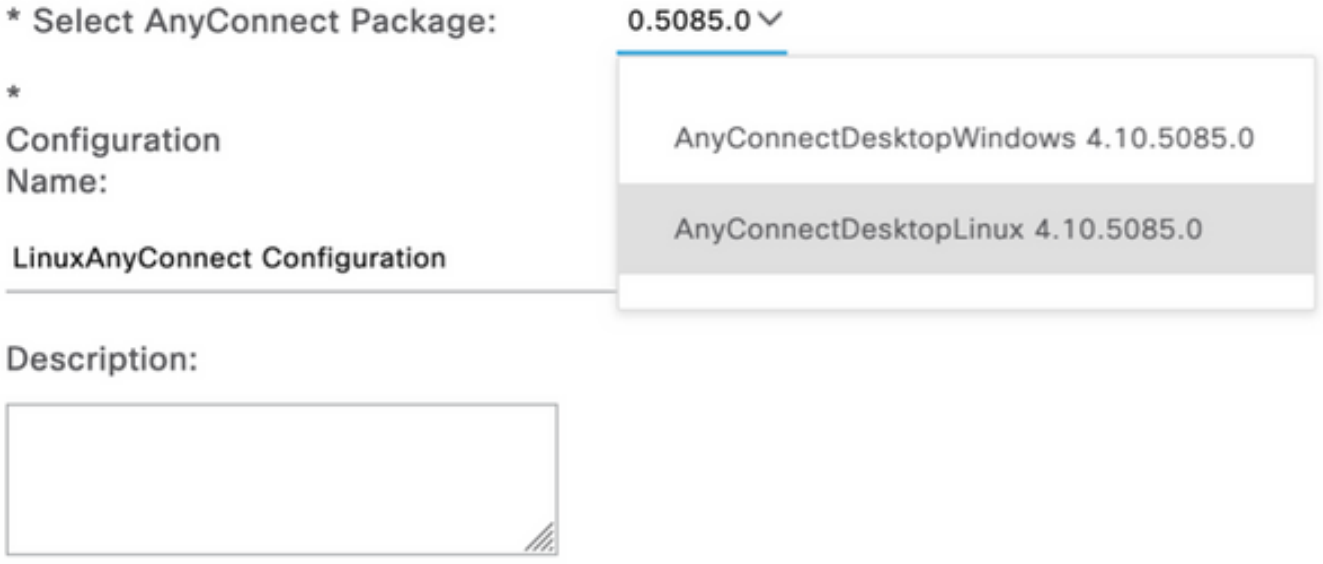
الخطوة 16. تحت **نوع قواعد اسم الخادم** * للاتصال بجميع الخوادم وتحديد عنوان IP المستقل/PSN ضمن **قائمة الاتصال بالمنزل.** بدلا من ذلك، يمكن إستخدام حرف بدل لمطابقة جميع شبكات PSN المحتملة في شبكتك (أي *.acme.com).

Posture Protocol

Parameter	Value	Description
PRA retransmission time	120 secs	This is the agent retry period if there is a Passive Reassessment communication failure
Retransmission Delay	60 secs	Time (in seconds) to wait before retrying.
Retransmission Limit	4	Number of retries allowed for a message.
Discovery host	10.52.13.173	Enter any IP address or FQDN that is routed through a NAD. The NAD detects and redirects that http traffic to the Client Provisioning portal.
Discovery Backup Server List	1 PSN(s)	By default, AnyConnect sends discovery probes to all the Cisco ISE PSNs sequentially if the PSN is unreachable. Choose specific PSNs as the backup list and restrict the nodes to which AnyConnect sends discovery probes.
Server name rules *	*	A list of wildcarded, comma-separated names that defines the servers that the agent can connect to. E.g. "*.cisco.com"
Call Home List	10.52.13.173	A list of IP addresses, that defines the all the Policy service nodes that the agent will try to connect to if the PSN that authenticated the endpoint doesn't respond for some reason.
Back-off Timer	30 secs	Anyconnect agent will continuously try to reach discovery targets (redirection targets and previously connected PSNs) by sending the discovery packets till this max time limit is reached

الخطوة 17. انقر على **إضافة > تكوين** AnyConnect


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

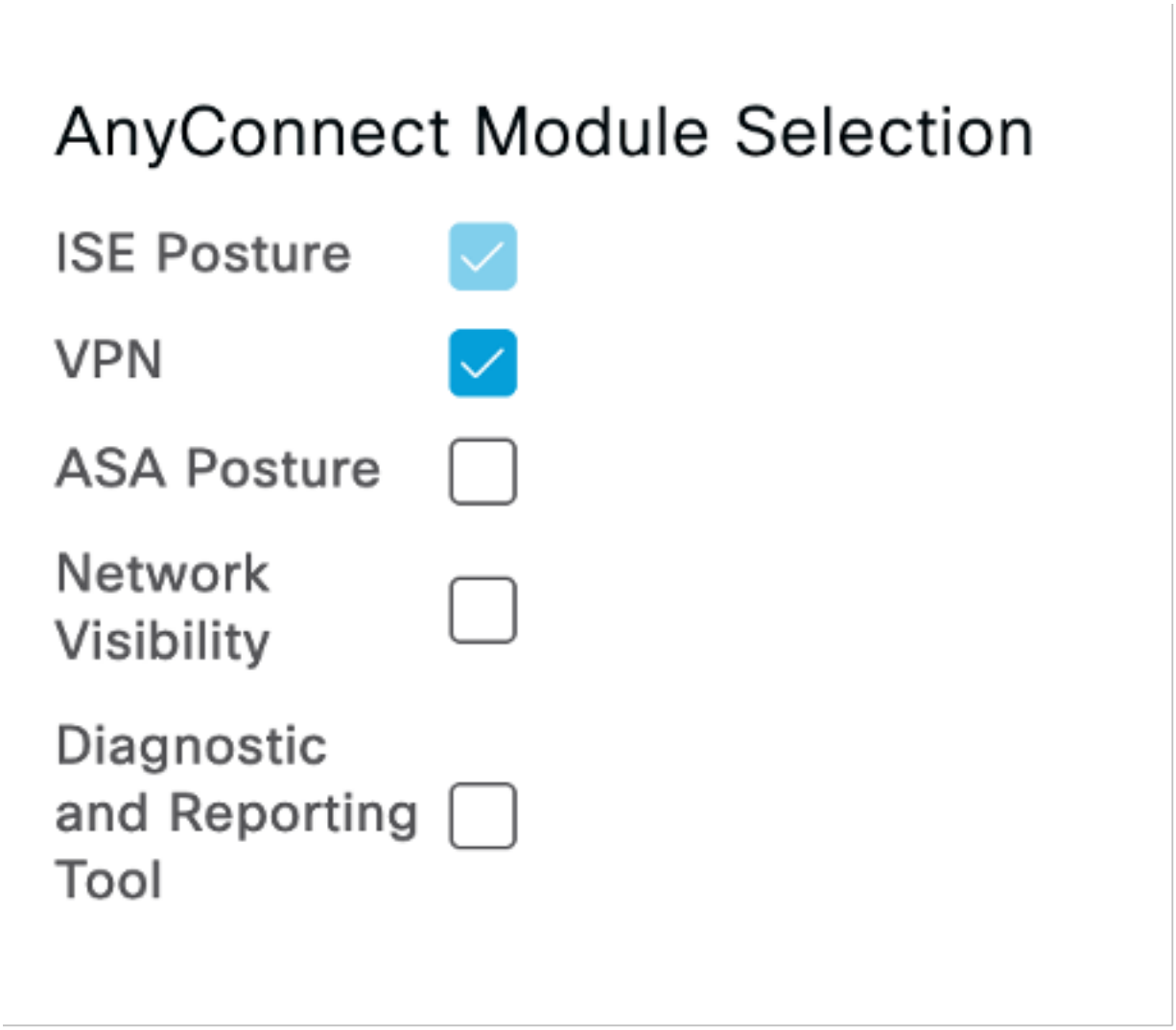
Description Value Notes

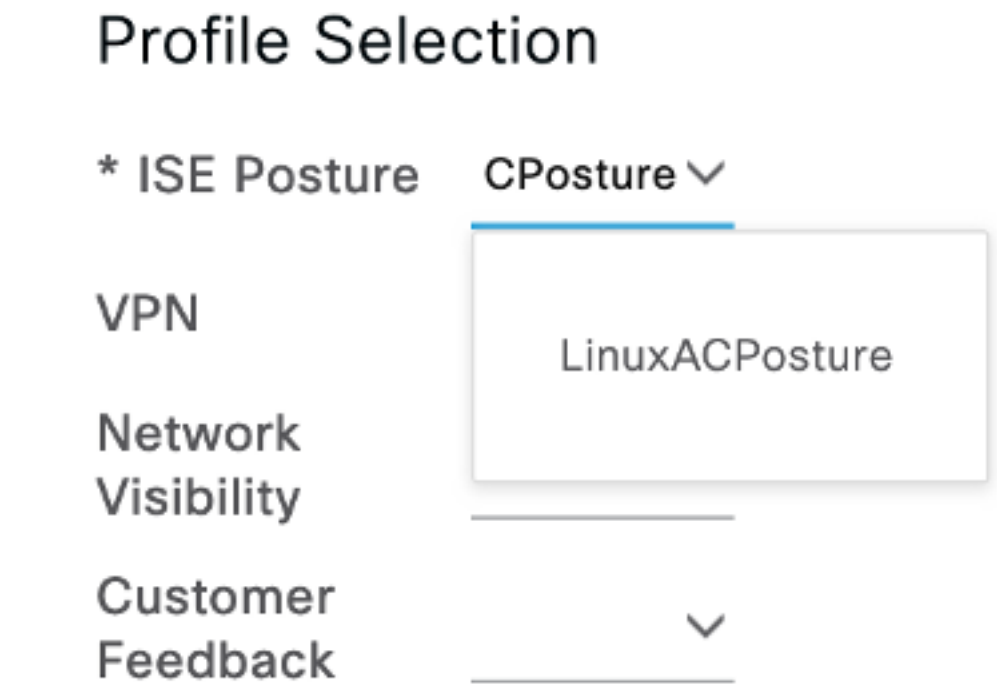
* Compliance Module 3.2028.0

AnyConnectComplianceModuleLinux64 4.3.1676.0

AnyConnectComplianceModuleLinux64 4.3.2028.0

AnyConnect

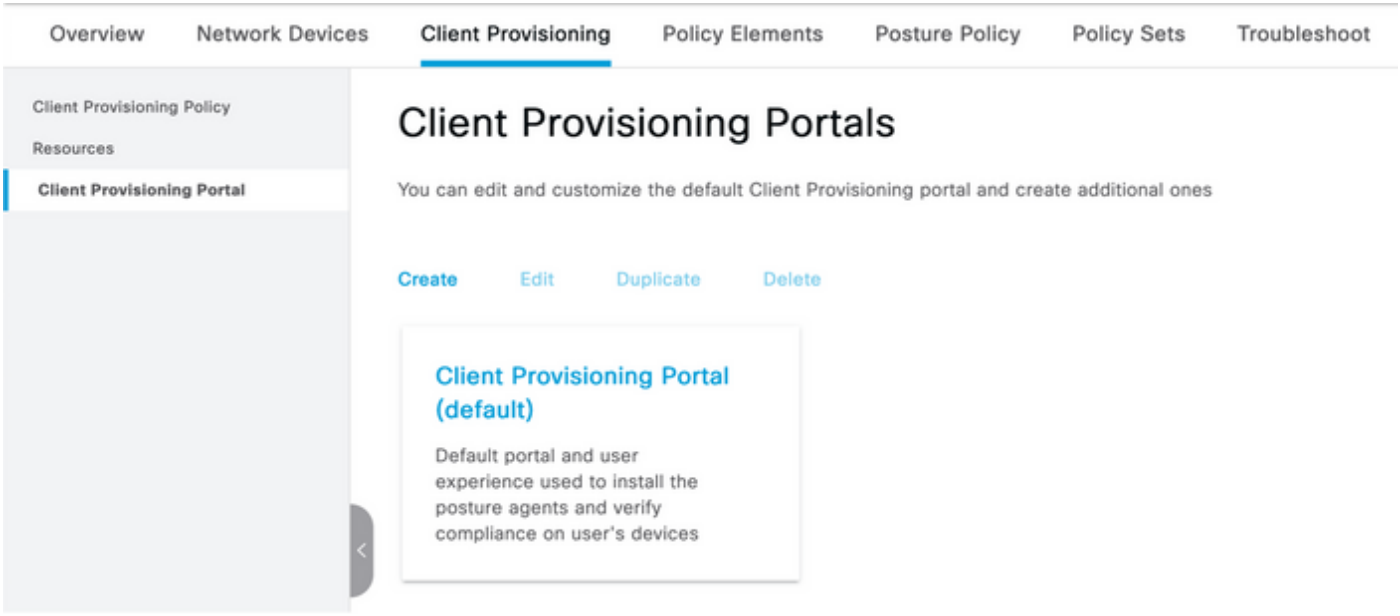




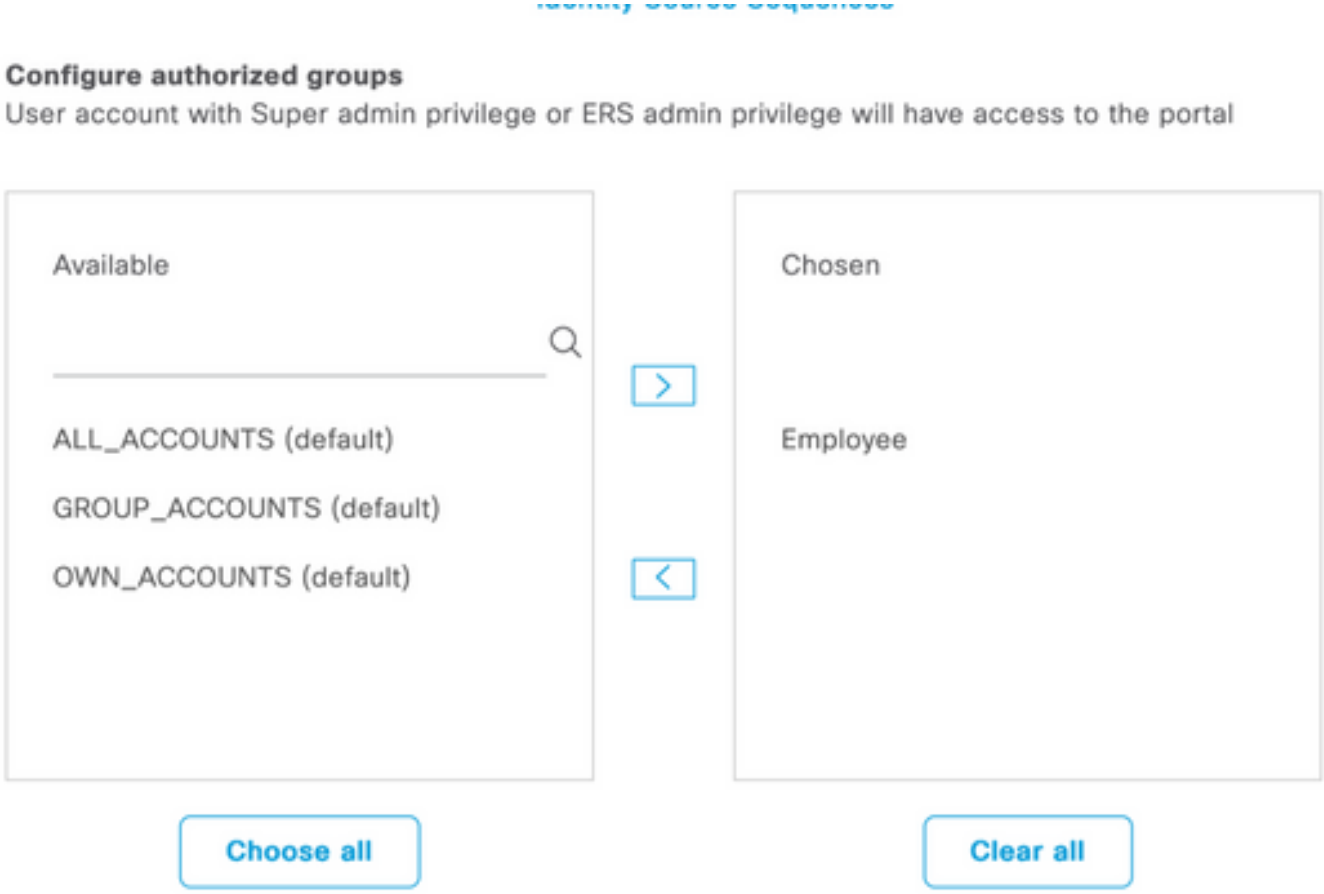
قم بالتمرير لأسفل وحدد إرسال

الخطوة 18. عندما تنتهي من عمل التحديدات، انقر فوق إرسال.

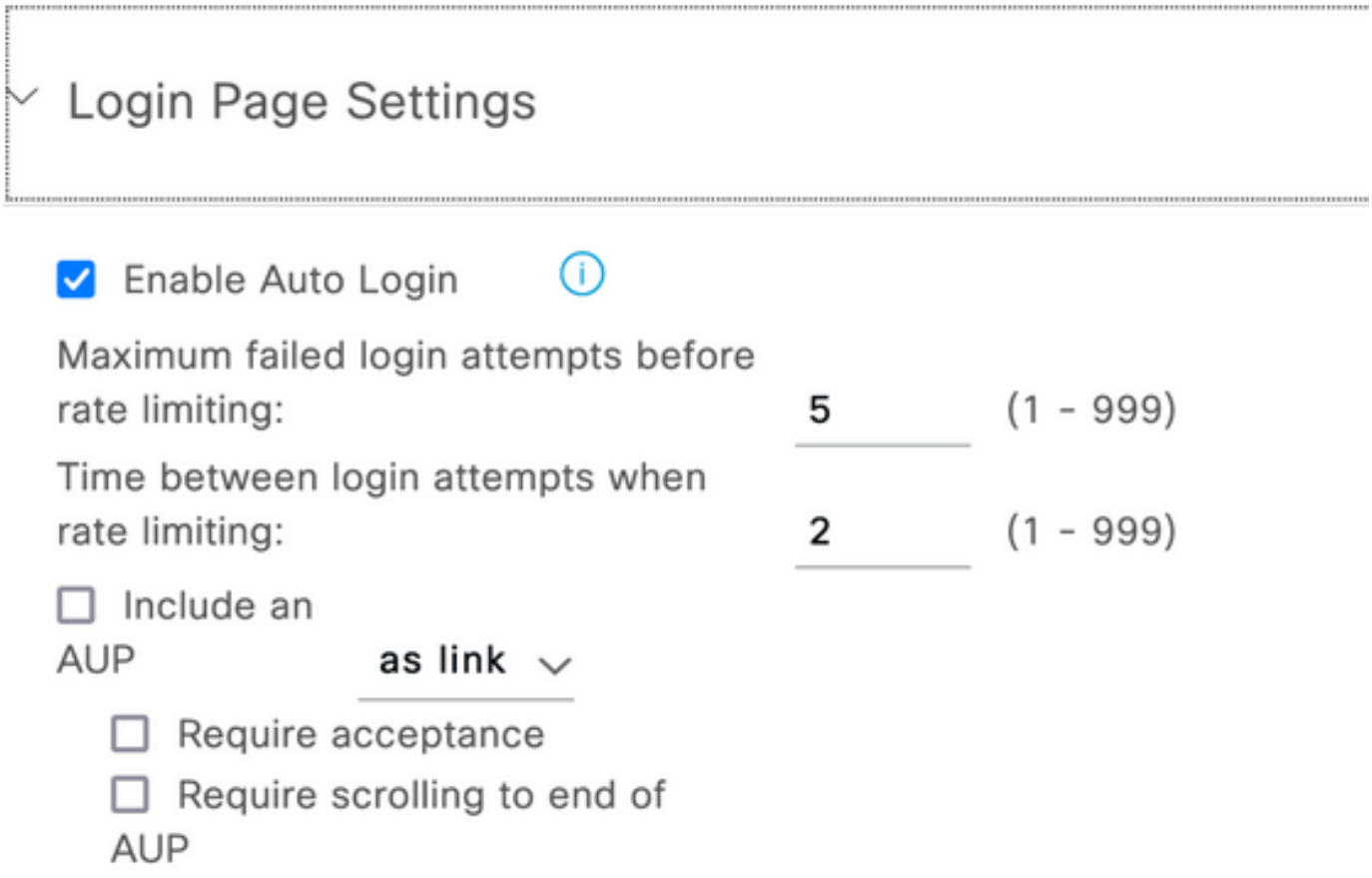
الخطوة 19. حدد مراكز العمل > الوضع > إمداد العميل > بوابات إمداد العميل.



الخطوة 20. تحت قسم إعدادات المدخل، حيث يمكنك تحديد الواجهة والمنفذ، بالإضافة إلى المجموعات المعتمدة للصفحة تحديد الموظف و SISE_Users ومستخدمي المجال.



الخطوة 21. ضمن إعدادات صفحة تسجيل الدخول، تأكد من تمكين خيار **تمكين تسجيل الدخول التلقائي**



الخطوة 22. في الزاوية العلوية اليمنى، حدد **حفظ**

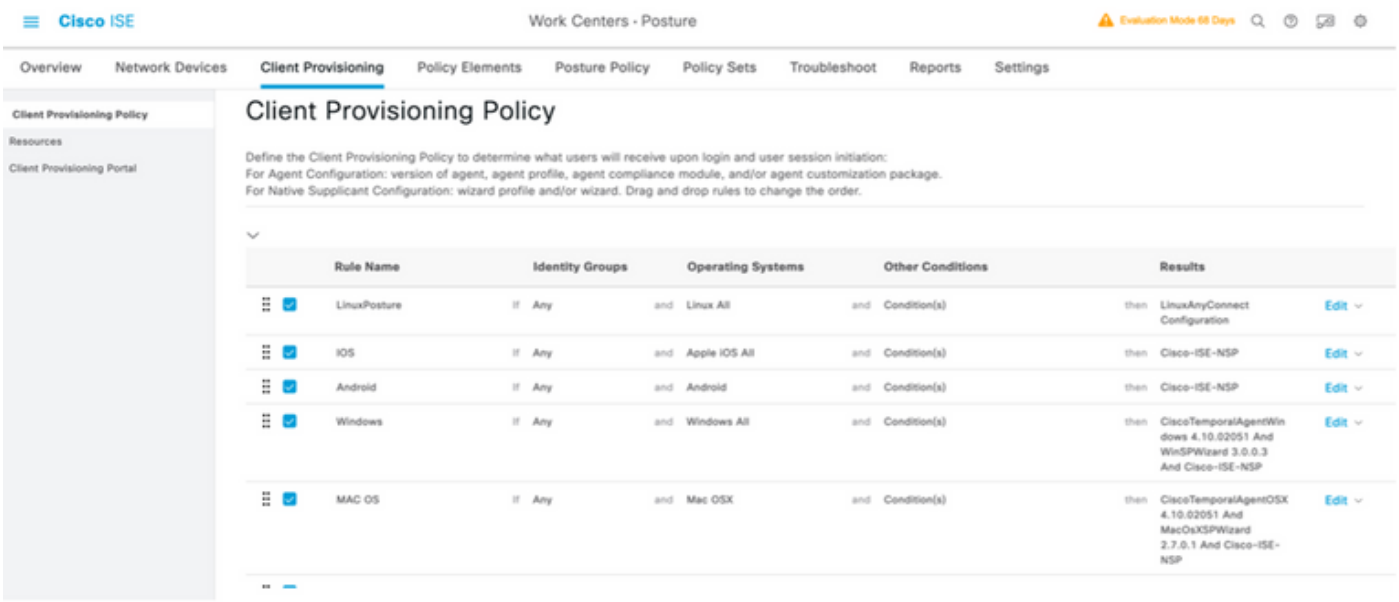
الخطوة 23. حدد **مراكز العمل > الوضع > إمداد العميل > سياسة إمداد العميل.**

الخطوة 24. انقر فوق السهم لأسفل الموجود بجوار **قاعدة IOS** في CPP واختر **المضاعفة أعلاه**

الخطوة 25. تسمية القاعدة **LinuxPosture**

الخطوة 26. للنتائج، حدد **تكوين AnyConnect** كعميل.

> **ملاحظة**: في هذه الحالة، لا ترى قائمة منسدلة لوحدة التوافق النمطية لأنه تم تكوينها كجزء من تكوين AnyConnect.



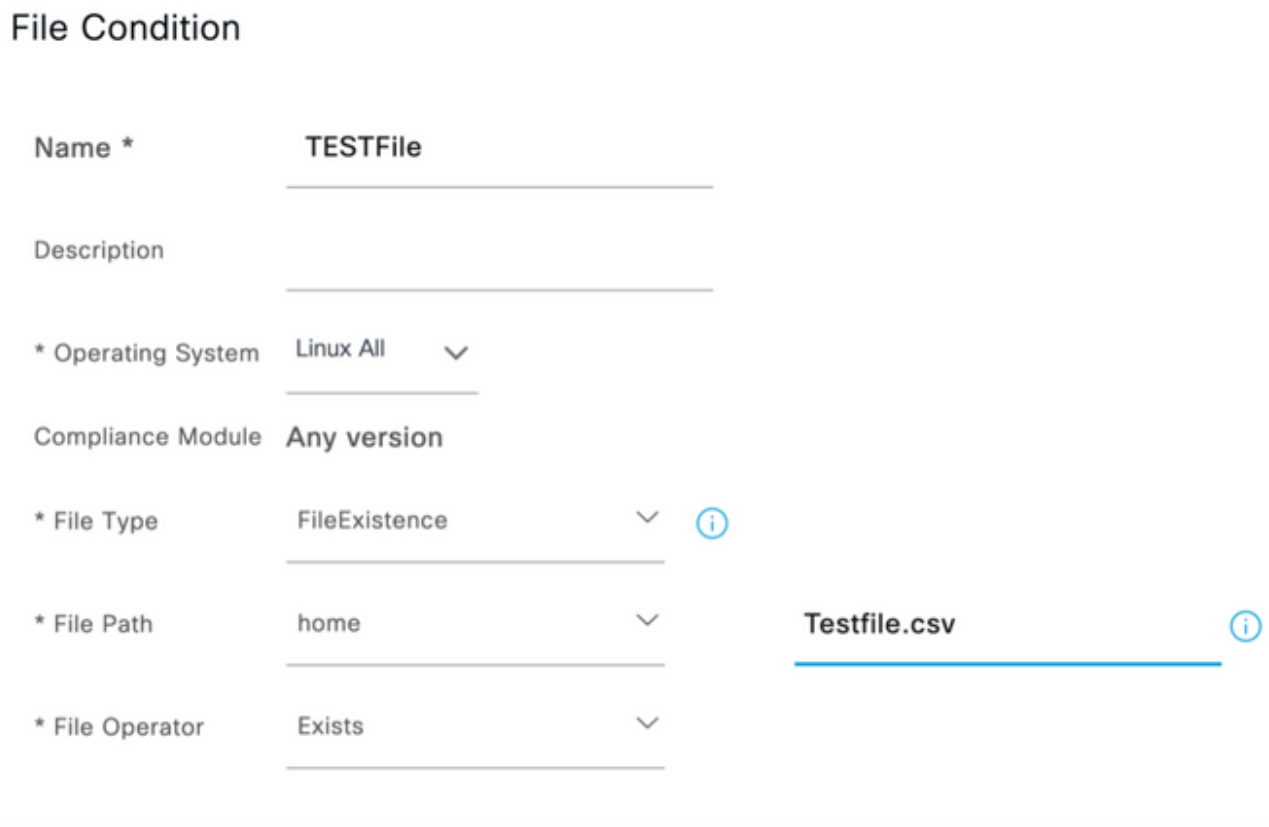
الخطوة 27. انقر فوق **تم**.

الخطوة 28. **طقطقة حفظ**.

عناصر سياسة الوضع

الخطوة 29. حدد **مراكز العمل > الوضع > عناصر السياسة > الشروط > الملف**. حدد **إضافة**.

الخطوة 30.قم بتعريف **TESTFile** كاسم شرط الملف وقم بتعريف القيم التالية

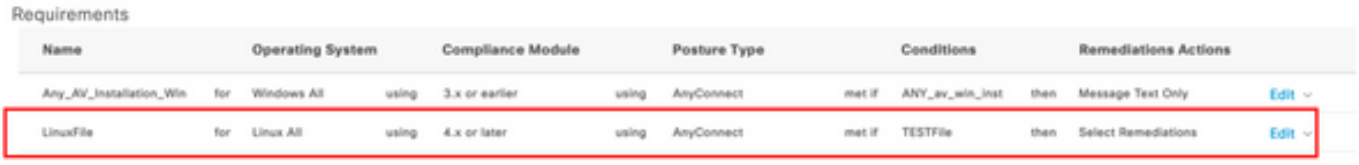


ملاحظة: يعتمد المسار على موقع الملف.

الخطوة 31. حدد **حفظ**

FilePresence.يدب ون ع الملف اذه كشرط لمعرفة ام إذا كان الملف موجودا في النظام حيث يفترض أن يكون موجودا، وهذا كل شيء. مع تحديد هذا الخيار، ال يوجد أي اهتمام على الإطلاق للتحقق من تواريخ الملف، التجزئة، وهكذا

الخطوة 32. حدد المتطلبات وقم بإنشاء سياسة جديدة كما يلي:



ملاحظة: ال يدعم Linux نص الرسالة فقط كإجراء للمعالجة

مكونات المتطلبات

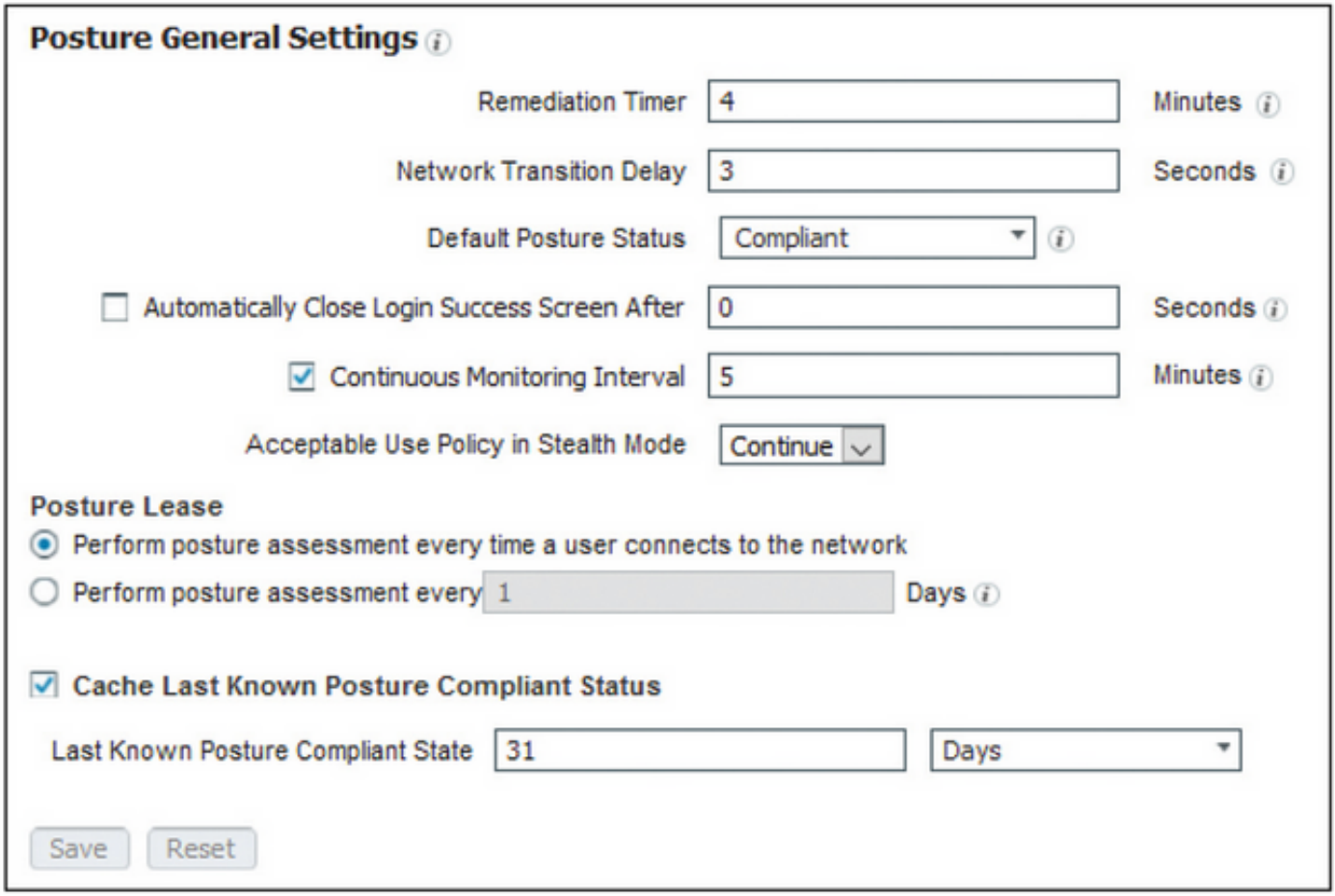
- **نظام التشغيل:** لينوكس الكل
- **وحدة التوافق:** 4.x
- **نوع الوضع:** AnyConnect
- **الشروط:** وحدات التوافق ووكلائه (التي تصبح متوفرة بعد تحديد نظام التشغيل)
- **إجراءات المعالجة:** المعالجات التي تصبح متاحة للتحديد بعد إختيار جميع الشروط الأخرى.

الخطوة 33. حدد **مراكز العمل > الوضع > سياسة الوضع**

الخطوة 34. حدد Edit (تحرير) في أي نهج وحدد Insert New Policy Define **LinuxPosturePolicy** (تحديد **LinuxPosturePolicy**) كاسم وتأكد من إضافة متطلباتك التي تم إنشاؤها في الخطوة 32.

الخطوة 35. تحديد **تم وحفظ**

إعدادات الوضع المهمة الأخرى (قسم إعدادات الوضع العامة)



الإعدادات المهمة في قسم الإعدادات العامة للوضع كما يلي:

- **مؤقت الإصلاح**: يحدد هذا الإعداد مقدار الوقت الذي يجب على العميل تصحيح حالة فشل. هناك أيضا مؤقت إصلاح في تكوين AnyConnect؛ وهذا المؤقت لـ ISE، وليس AnyConnect.
- **حالة الوضع الافتراضي**: يوفر هذا الإعداد حالة الوضع للأجهزة التي لا تحتوي على عامل الوضع أو أنظمة التشغيل التي لا يمكنها تشغيل العامل المؤقت، مثل أنظمة التشغيل المستندة إلى Linux.
- **الفاصل الزمني للمراقبة المستمرة**: ينطبق هذا الإعداد على شروط التطبيق والأجهزة التي تقوم بجرد نقطة النهاية. يحدد الإعداد عدد المرات التي يجب فيها على AnyConnect إرسال بيانات المراقبة.
- **نهج الاستخدام المقبول في وضع التخفي**: لا يوجد سوى خيارين لهذا الإعداد هما الحظر أو

المتابعة. يمنع الحظر عملاء AnyConnect في وضع التخفي من المتابعة إذا لم يتم الاعتراف ب AUP. تسمح المتابعة لعميل وضع التخفي بالمتابعة حتى دون التعرف على بروتوكول AUP (والذي غالبا ما يكون هو المقصود عند إستخدام إعداد وضع التخفي ل AnyConnect).

تكوينات إعادة التقييم

تعد عمليات إعادة تقييم الوضع مكونا هاما لسير عمل الوضع. لقد رأيت كيفية تكوين "بروتوكول الوضع" في قسم إعادة تقييم الوضع ل AnyConnect. يتحقق العميل بشكل دوري من الدخول باستخدام PSNs المحددة استنادا إلى المؤقت في هذا التكوين.

عندما يصل طلب إلى PSN، تحدد PSN ما إذا كانت هناك حاجة إلى إعادة تقييم الوضع، استنادا إلى تكوين ISE لدور نقطة النهاية تلك. إذا مرر العميل عملية إعادة التقييم، فإن PSN تحتفظ بحالة التوافق مع وضعية نقطة النهاية، وتم إعادة تعيين إيجار الوضع. إذا فشلت نقطة النهاية في إعادة التقييم، فإن حالة الوضع تتغير إلى غير متوافق، وتم إزالة أي تأجير وضعي موجود.

الخطوة 36. حدد **سياسة > عناصر السياسة > النتائج > التخويل > ملف تخصيص التخويل.** حدد **إضافة**

الخطوة 37. قم بتعريف wired_redirect كملف تعريف التخويل ثم قم بتكوين المعلمات التالية

الخطوة 38. حدد **حفظ**

الخطوة 39. تكوين سياسات التخويل

هناك ثلاث قواعد تخويل تم تكوينها مسبقا للوضع:

1. يتم تكوين الأول للمطابقة عند نجاح المصادقة، كما أن توافق الجهاز غير معروف.
2. وتطابق القاعدة الثانية عمليات المصادقة الناجحة مع نقاط النهاية غير المتوافقة.

   ملاحظة: تحتوي كل من القاعدتين الأوليين على النتيجة نفسها، وهي إستخدام ملف تعريف تخويل مكون مسبقا يعمل على إعادة توجيه نقطة النهاية إلى مدخل إمداد العميل.

3. وتطابق القاعدة النهائية المصادقة الناجحة ونقاط النهاية المتوافقة مع الوضع وتستخدم ملف تعريف تفويض PermitAccess الذي تم تصميمه مسبقا.

حدد **سياسة > مجموعة السياسات** وحدد السهم الأيمن ل **802.1x السلكي - MAB** الذي تم إنشاؤه في المختبر السابق.

الخطوة 40. تحديد **نهج التخويل** وإنشاء القواعد التالية

التكوينات على المحول

ملاحظة: يشير التكوين التالي إلى IBNS 1.0. يمكن أن تكون هناك إختلافات لمبدلات IBNS 2.0 القادرة. وهو يتضمن نشر في وضع أقل تأثيرا.

```
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
```

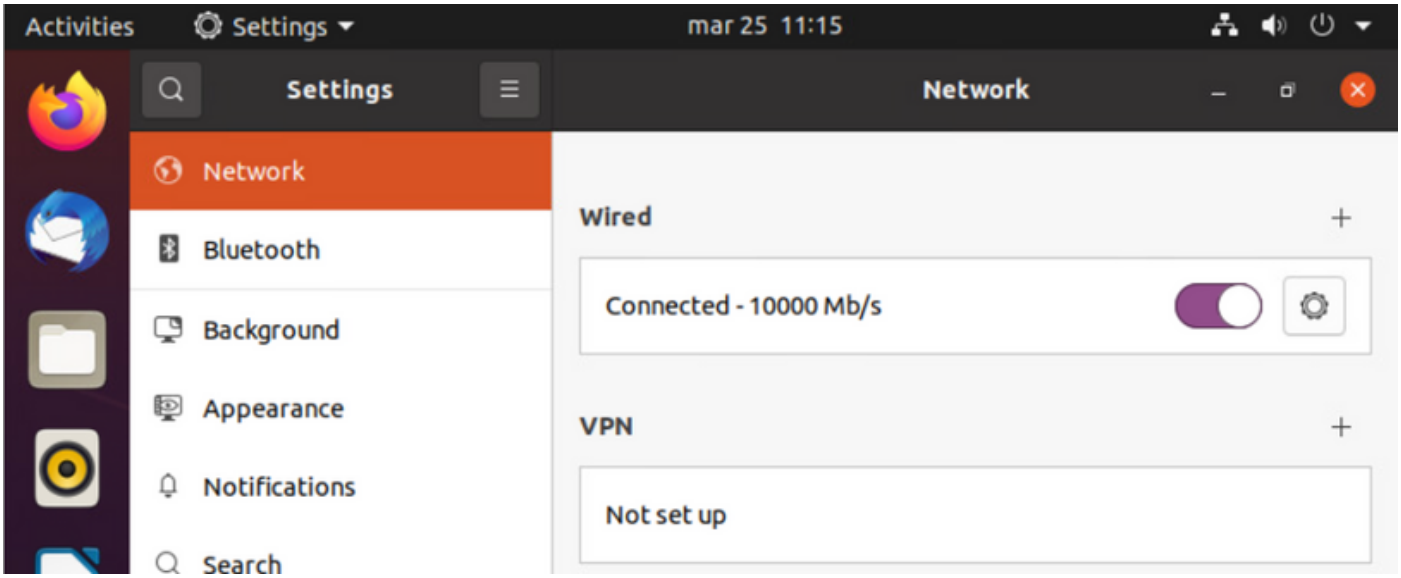
التحقق من الصحة

التحقق من ISE:

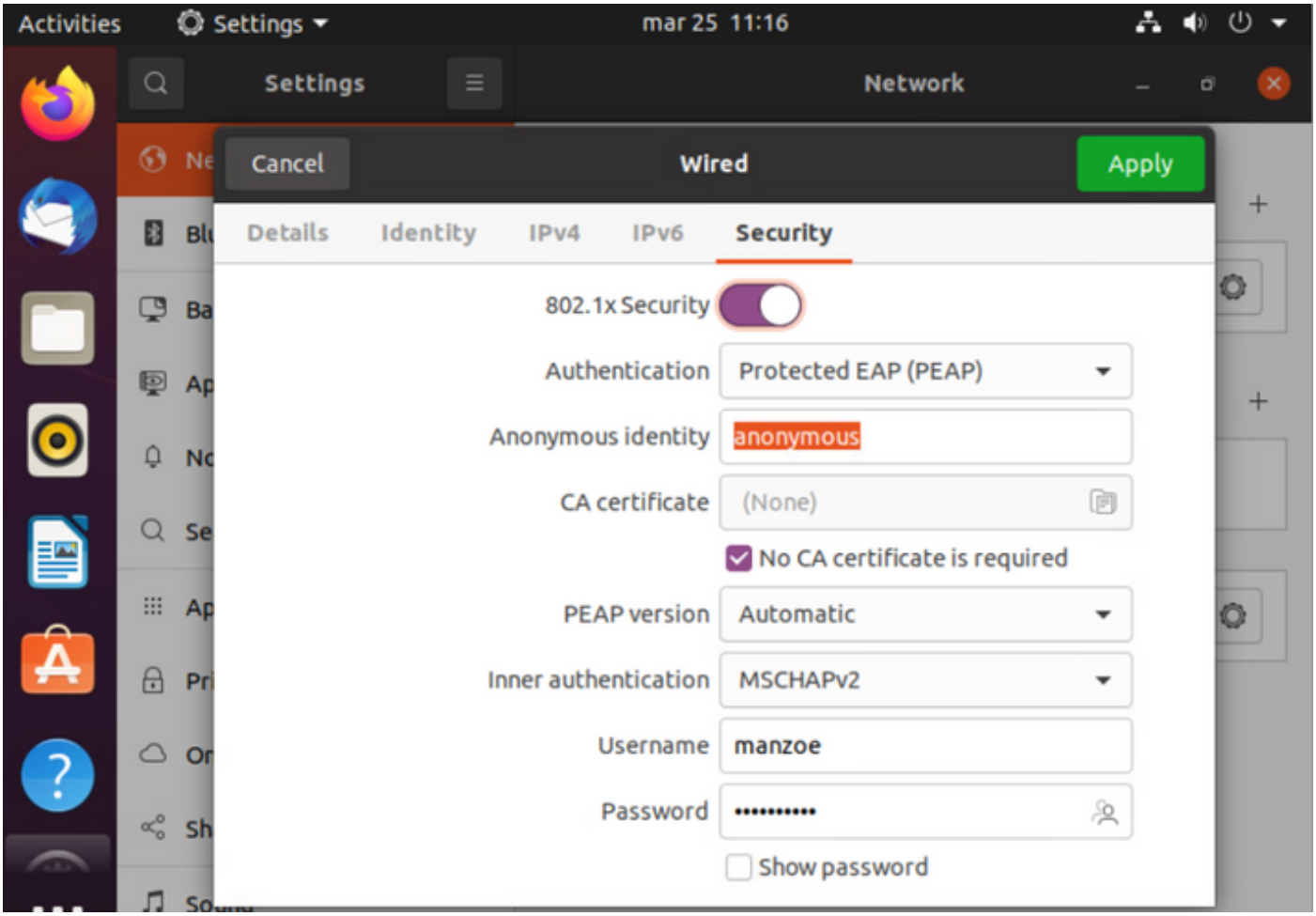
يفترض هذه القسم أنه قد تم تثبيت AnyConnect بوحدة ISE Posture (وضعية محرك خدمات الهوية (ISE)) مسبقا على نظام Linux.

مصادقة الكمبيوتر باستخدام dot1x

الخطوة 1. انتقل إلى إعدادات الشبكة

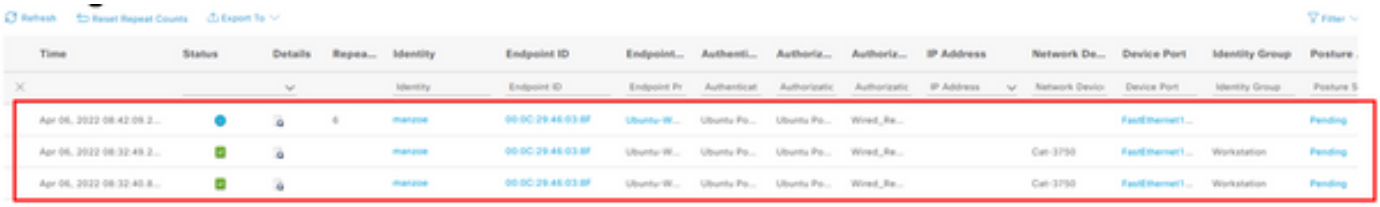


الخطوة 2. حدد علامة التبويب تأمين وقم بتوفير تهيئة 802.1x وبيانات اعتماد المستخدم



الخطوة 3. انقر فوق **"تطبيق".**

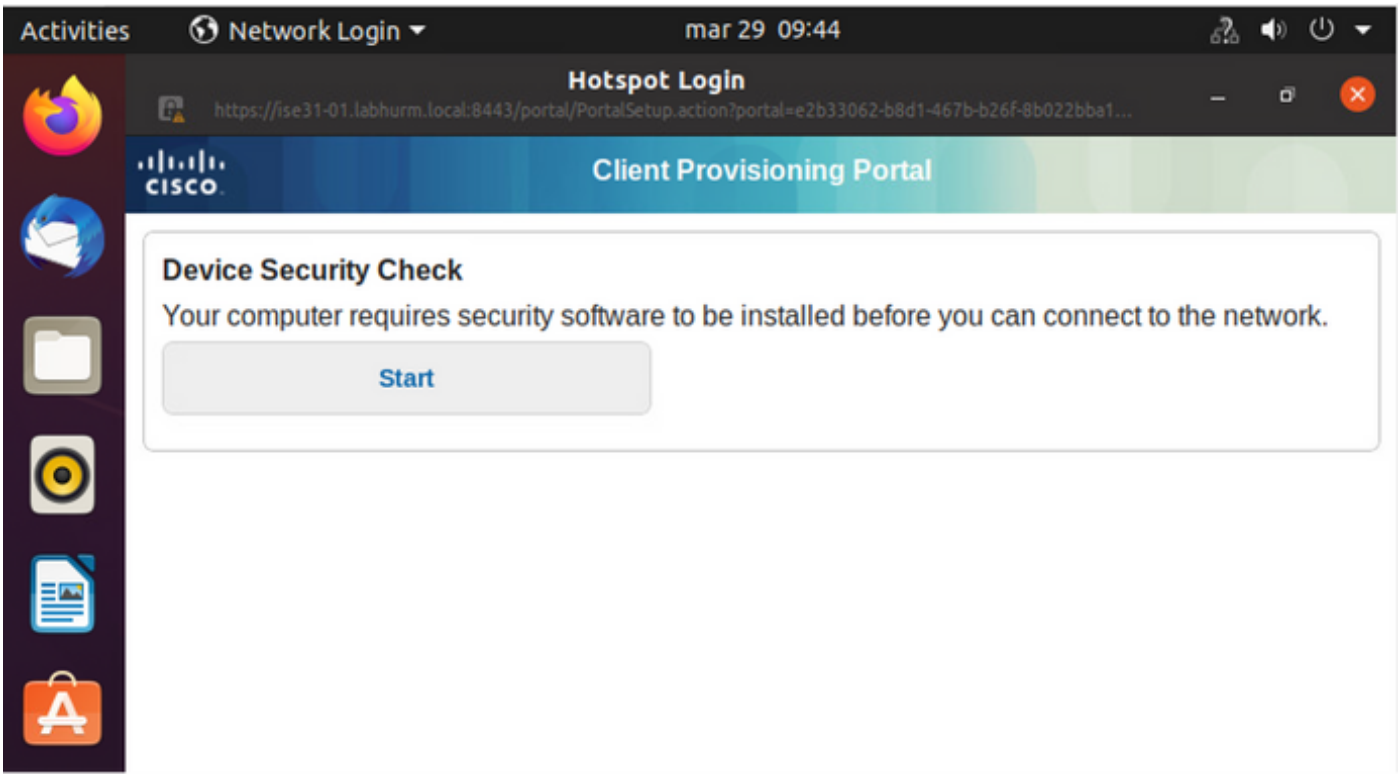
الخطوة 4. قم بتوصيل نظام Linux بالشبكة السلكية 802.1x والتحقق منه في سجل ISE Live:



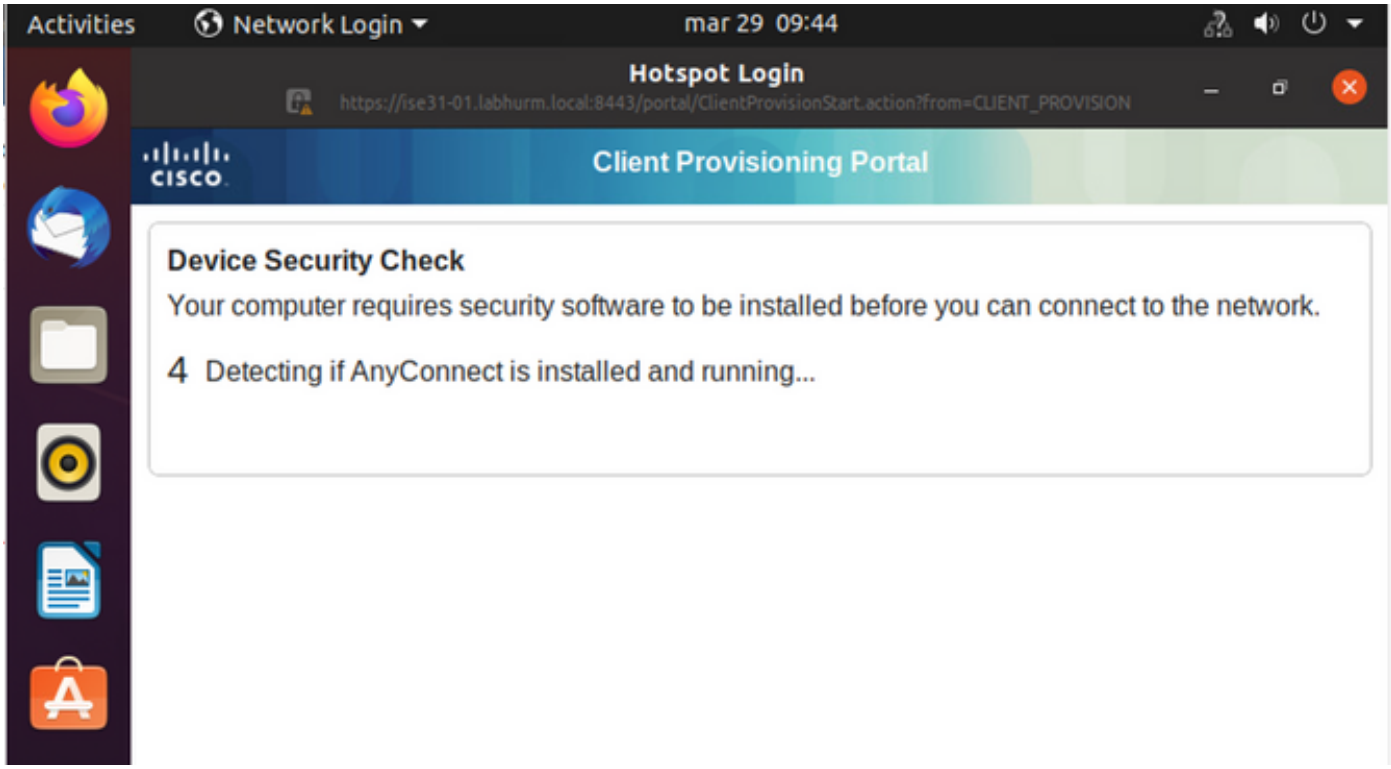
في ISE، أستخدم شريط التمرير الأفقي لعرض معلومات إضافية، مثل PSN الذي خدم حالة التدفق أو الوضع:

Authoriz...	Authoriz...	IP Address	Network De...	Device Port	Identity Group	Posture ...	Server
Authorizatic	Authorizatic	IP Address	Network Devic	Device Port	Identity Group	Posture Sta	Server
Ubuntu Po...	Wired_Re...			FastEthernet1...		Pending	ise31-01
Ubuntu Po...	Wired_Re...		Cat-3750	FastEthernet1...	Workstation	Pending	ise31-01
Ubuntu Po...	Wired_Re...		Cat-3750	FastEthernet1...	Workstation	Pending	ise31-01

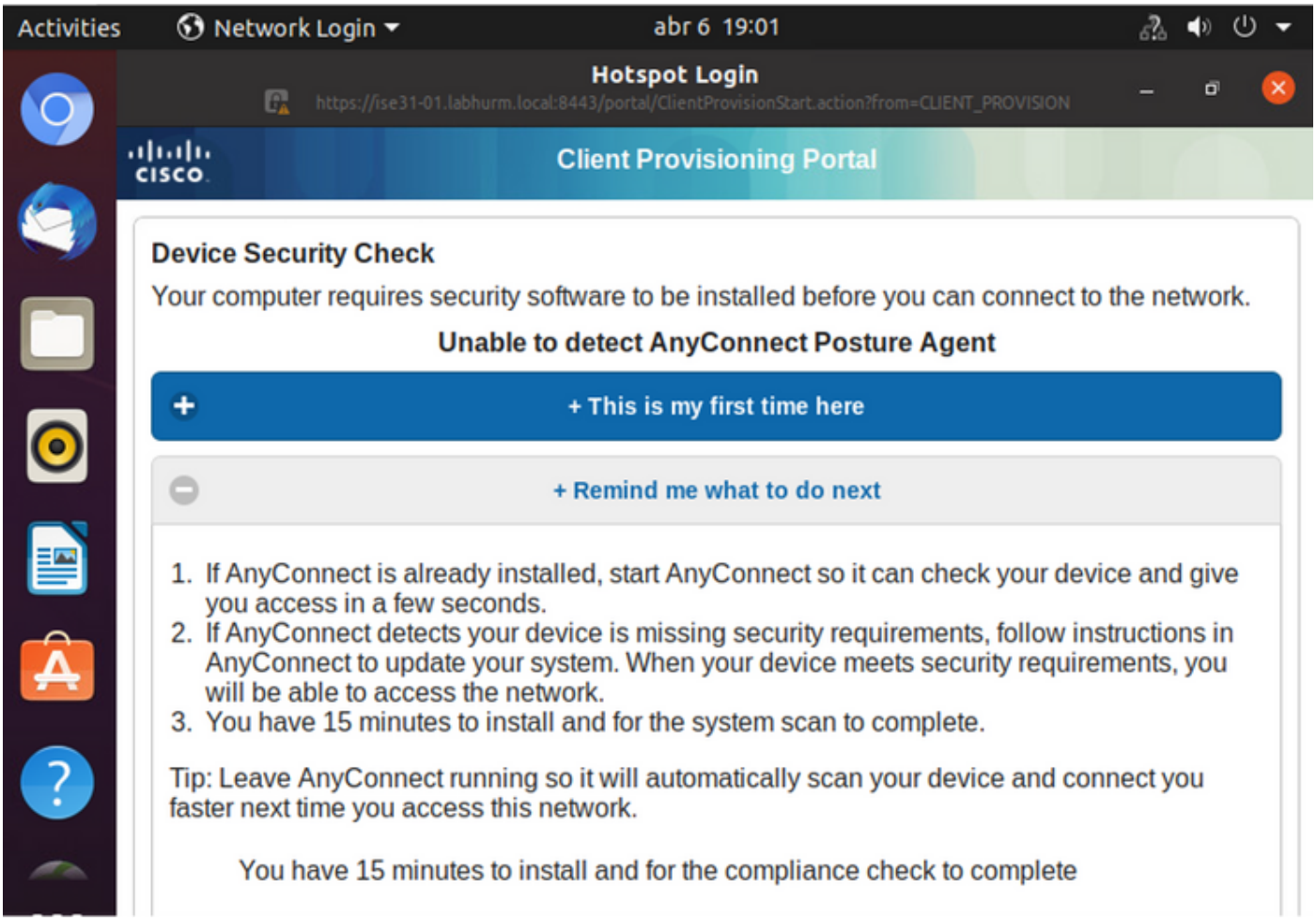
الخطوة 5. في عميل Linux، يقع إعادة التوجيه، وهو يقدم مدخل إمداد العميل يشير إلى حدوث تدقيق الوضع ولنقر **بداية:**



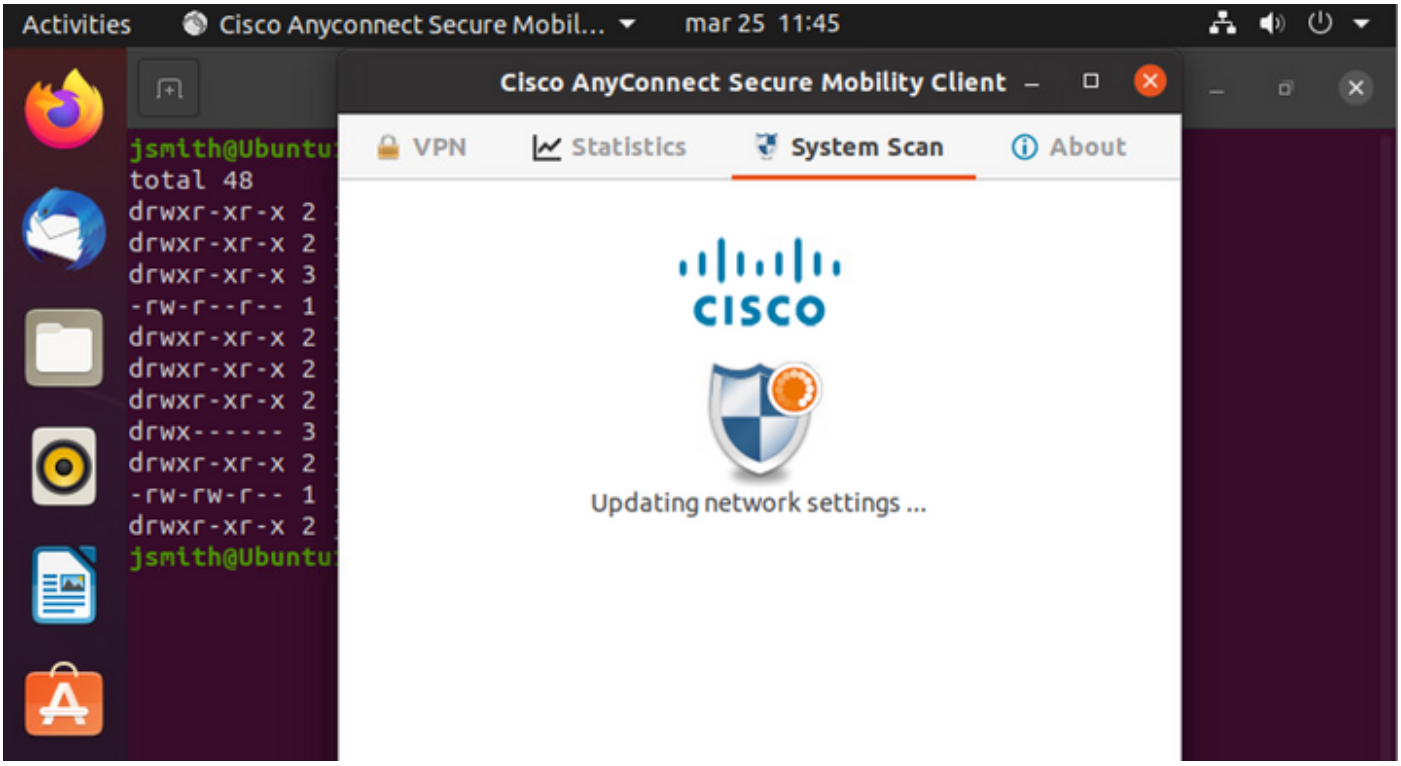
انتظر بضع ثوان بينما يحاول الموصل اكتشاف AnyConnect:



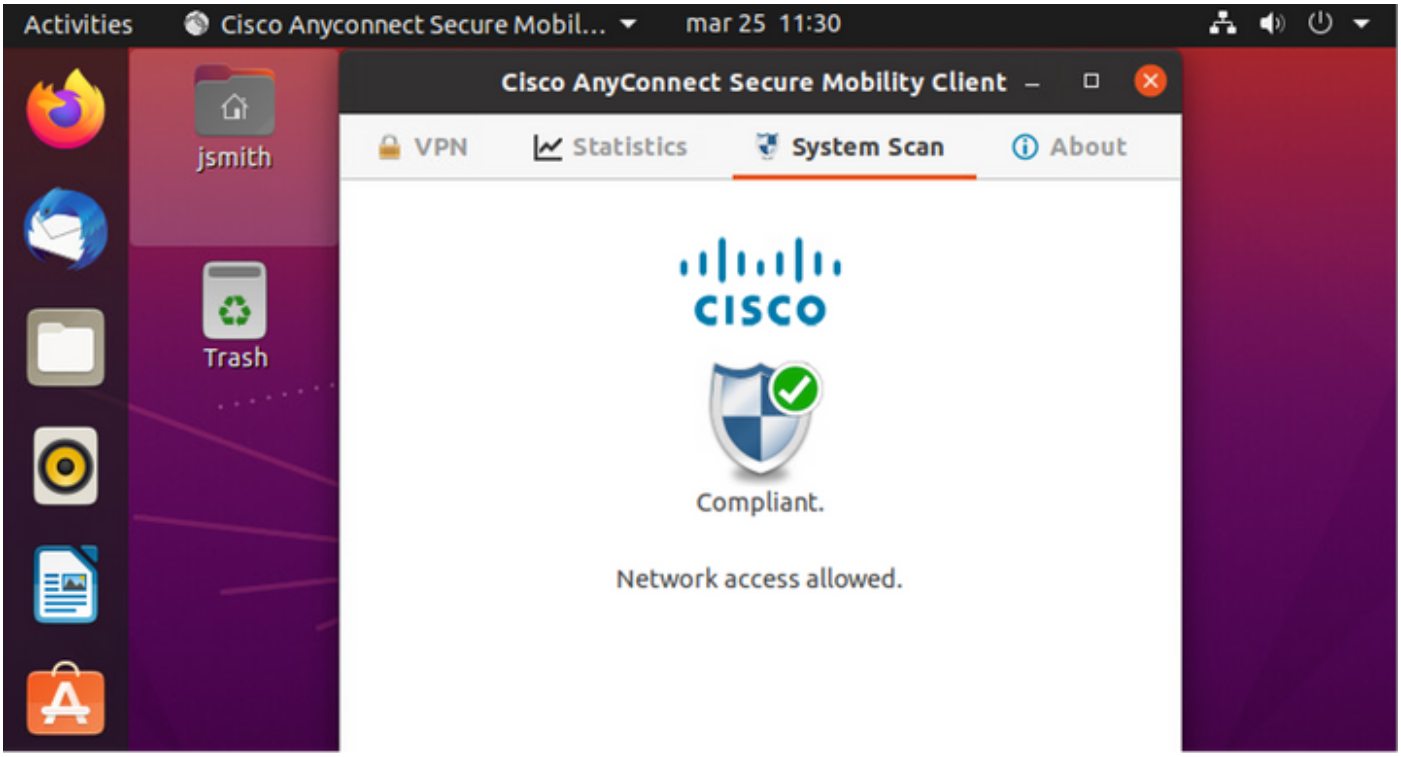
بسبب تحذير معروف، حتى إذا تم تثبيت AnyConnect، فإنه لا يكتشفه. أستخدم **Alt-Tab** أو قائمة **الأنشطة** للتبديل إلى عميل AnyConnect.

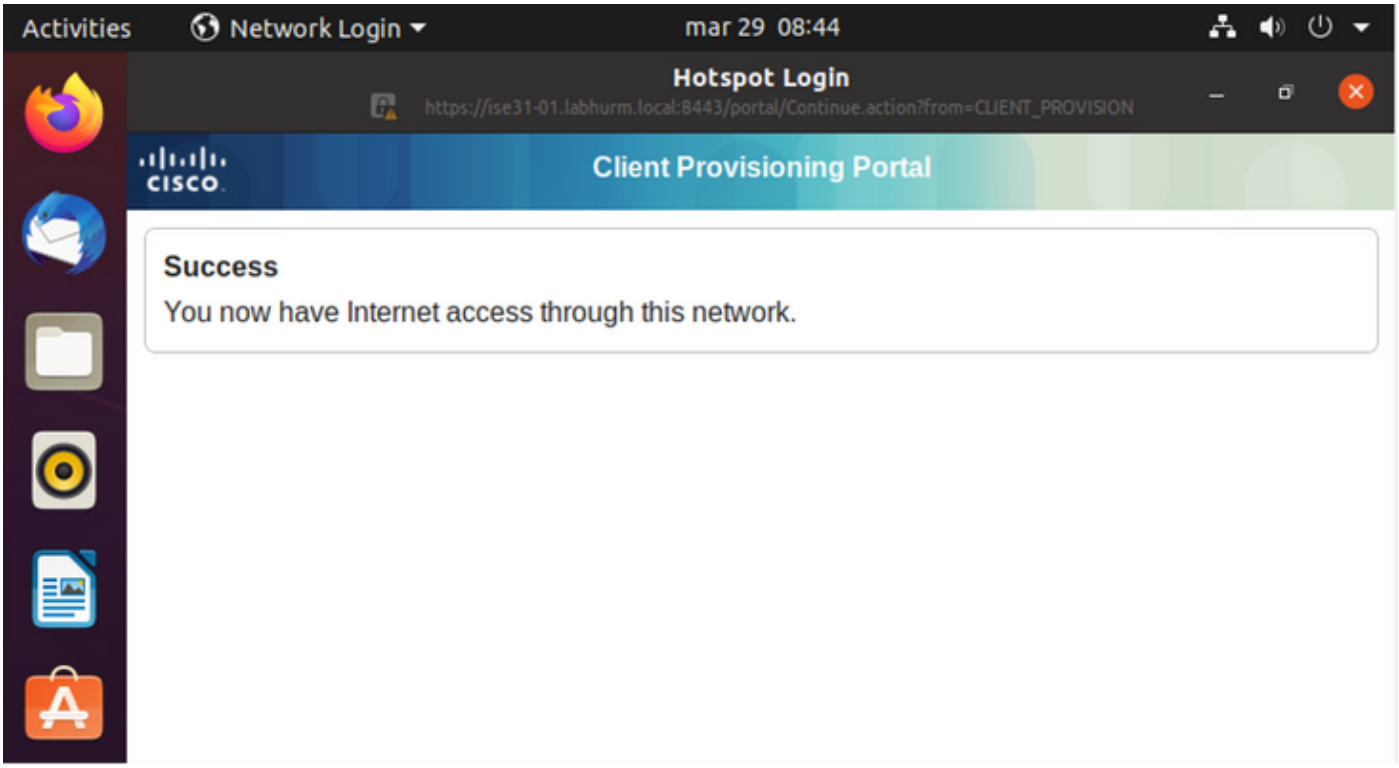


يحاول AnyConnect الوصول إلى سياسة وضع PSN وتقييم نقطة النهاية ضدها.



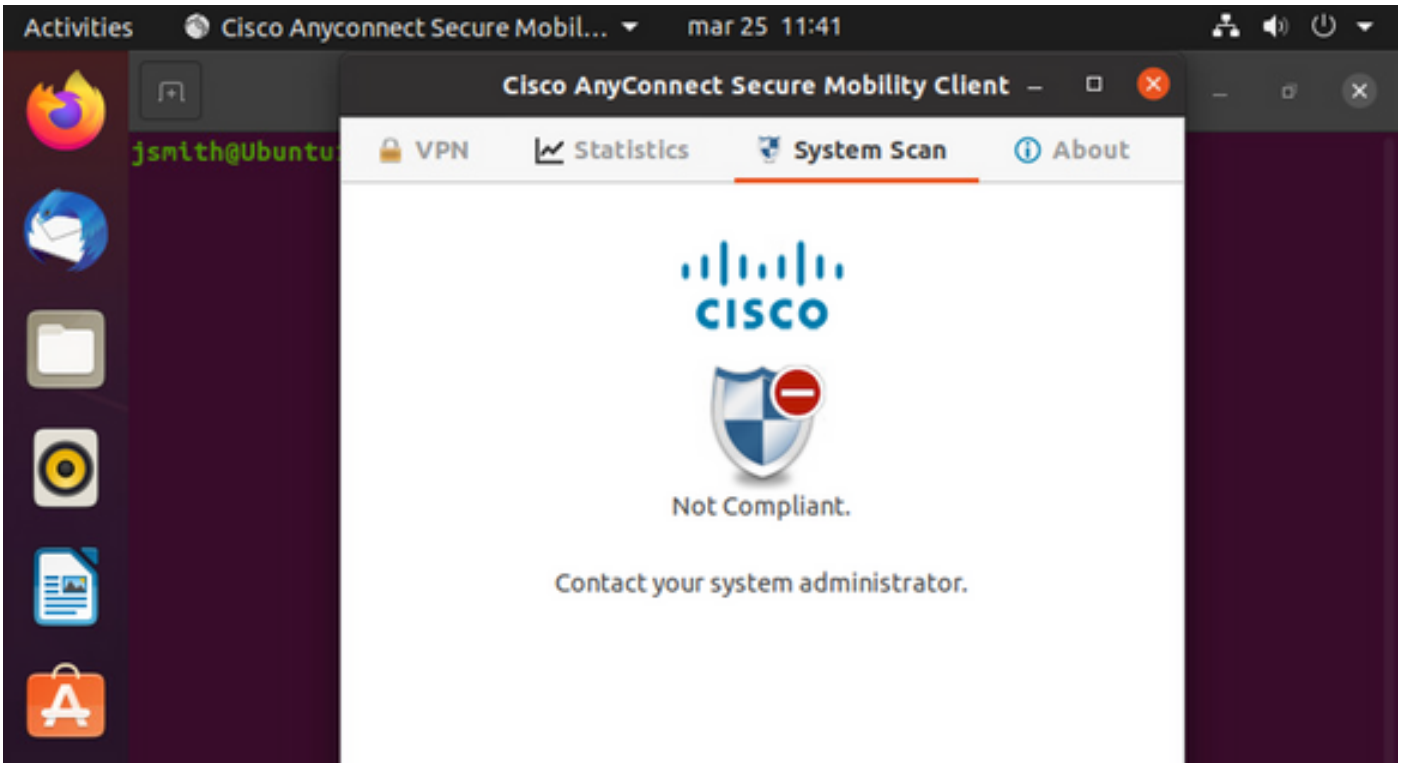
يبلغ AnyConnect عن تصميمه على سياسة الوضع مرة أخرى إلى ISE. في هذه الحالة، متوافق

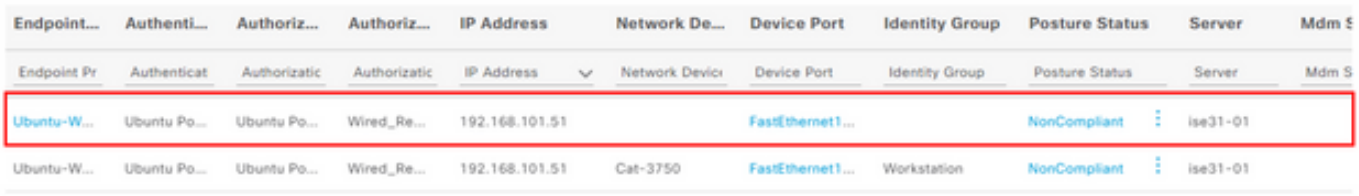




Endpoint Profile	Authenti...	Authorizati...	Authorization P...	IP Address	Network De...	Device Port	Identity Group	Posture Status	Server
Endpoint Profile	Authenticat	Authorization I	Authorization Profile	IP Address	Network Devic	Device Port	Identity Group	Posture Status	Server
Ubuntu-Workstation	Wired 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

من ناحية أخرى، إذا لم يكن الملف موجودا، فإن وحدة AnyConnect النمطية للوضعية تبلغ عن التصميم على 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 Devici	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	

ملاحظة: يلزم حل ISE FQDN على نظام Linux من خلال DNS أو ملف المضيف المحلي.

استكشاف الأخطاء وإصلاحها

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

إعادة التوجيه في الموقع:

```
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
```

نجح التخويل:

```
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:  C0A8C883000000010008044A
     Acct Session ID:  0x00000004
              Handle:  0xEB000001

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

غير متوافق، تم النقل إلى عزل شبكة VLAN وقوائم التحكم في الوصول (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:  C0A86E0100000000001724F
     Acct Session ID:  0x00000003
              Handle:  0x9A000000

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

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).