تكوين وضعية ISE باستخدام FlexVPN

المحتويات

المقدمة

يقدم هذه المستند مثال لكيفية تكوين وحدة الاستقبال والبث IOS XE للوصول عن بعد باستخدام بروتوكول مصادقة AnyConnect IKEv2 و EAP-Message Digest 5 (EAP-MD5).

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- تكوين VPN للوصول عن بعد إلى FlexVPN (RA) على IOS XE
- تكوين عميل AnyConnect (AC)
- Posture Flow على Identity Service Engine (ISE) 2.2 والإصدارات الأحدث
- تكوين مكونات الوضع على ISE
- تكوين خادم DNS على Windows Server 2008 R2

المكونات المستخدمة

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

- Cisco CSR1000V الذي يشغل IOS XE 16.8 [Fuji]
- AnyConnect Client الإصدار 4.5.03040 الذي يعمل على نظام التشغيل Windows 7
- Cisco ISE 2.3
- خادم Windows 2008 R2

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 مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

معلومات أساسية

لضمان أن ظل تدابير أمان الشبكة المفروضة مناسبة وفعالة، يتيح لك Cisco ISE التحقق من صحة إمكانات الأمان وصيانتها على أي جهاز عميل يذفذ الشبكة المحمية. من خلال إستخدام سياسات الوضع المصممة لضمان توفر أحدث إعدادات الأمان أو التطبيقات الأمنية على أجهزة العميل، يمكن لمسؤول Cisco ISE التأكد من أن أي جهاز عميل يصل إلى الشبكة يفي بمعايير الأمان المحددة للوصول إلى شبكة المؤسسة والي يازل يفي بها. توفر تقارير التوافق مع الوضع ل Cisco ISE لقطة من مستوى التوافق لجهاز العميل في وقت تسجيل دخول المستخدم، وكذلك أي وقت يتم فيه إعادة تقييم دوري.

يمكن تمثيل الوضع بثلاثة عناصر رئيسية:

1. ISE تقوم بتكوين سياسات الوضع (ما هي الشروط المحددة التي يجب استيفاؤها ولضع علامة على الجهاز كمتوافق مع الشركة) وسياسات إمداد العميل (ما هو البرنامج الوكيل الذي يجب تثبيته على أي نوع من الأجهزة) ونهج التخويل (ما نوع الأذونات التي يجب أن يتم تعيينها إلى تعتمد على حالة وضعها).

2. جهاز الوصول إلى الشبكة (NAD) كنقطة لتنفيذ السياسة. يتم تطبيق قيود التخويل الفعلية على جانب NAD في وقت مصادقة المستخدم. يوفر ISE كنقطة نهج معلومات تخويل مثل قائمة التحكم في الوصول (ACL).وبشكل تقليدي، من أجل حدوث تغيير في الوضع، يلزم NAD لدعم تغيير التخويل (CoA) لإعادة مصادقة المستخدم بعد تحديد حالة الوضع لنقطة النهاية. البدء من ISE 2.2 NADs غير مطلوب لدعم إعادة التوجيه.
ملاحظة: المومجات التي تشغل IOS XE لا تدعم إعادة التوجيه.**ملاحظة**: يجب أن يحتوي برنامج IOS XE على إصلاحات للعيوب التالية حتى تعمل CoA مع ISE بشكل كامل:
لا يعمل CSCve16269 IKEv2 CoA مع ISE
لا يعمل CSCvi90729 IKEv2 CoA مع ISE (Coa-push=true بدلا من true)
3. برنامج الوكيل لنقطة لجمع البيانات والتفاعل مع المستخدم النهائي. يستلم الوكيل معلومات حول متطلبات الوضع من ISE ويوفر تقريرا إلى ISE فيما يتعلق بحالة طلبات الشرعا. يستند هذا المستند إلى وحدة AnyConnect ISE Posture Module التي تكون الوحدة النمطية الوحيدة التي تدعم الوضع بشكل كامل دون إعادة التوجيه.

تم توثيق تدفق الوضع دون إعادة التوجيه بشكل جيد جدا في المادة مقارنة نمط ISE Posture (مقارنة نمط ISE) للpre and Post 2.2"، القسم "تدفق الوضع في ISE 2.2".

يمكن إجراء إمداد وحدة AnyConnect ISE Posture Module باستخدام FlexVPN بطريقتين مختلفتين:

- يدوي - يتم تثبيت الوحدة النمطية يدوي على عميل العميل من حزمة AnyConnect المتاحة على مدخل تنزيل برامج Cisco: https://software.cisco.com/download/home/283000185.
  يجب استيفاء الشروط التالية للعمل في الوضع مع توفير وحدة ISE Posture Module اليدوية:

  1. يجب أن يقوم خادم اسم المجال (DNS) بحل اسم المجال المؤهل بالكامل (FQDN) **enroll.cisco.com** إلى عقد خدمة السياسة (PSNs) IPs. أثناء محاولة الاتصال الأولي، ال تتوفر لدى وحدة Posture النمطية أي معلومات حول شبكات PSN المتاحة. يتم الآن إرسال مستكشفات للعثور على PSN المتوفرة. يتم إستخدام FQDN enroll.cisco.com في أحد هذه المستكشفات.

  2. يجب السماح **بمنفذ** TCP **8905** لشبكات PSN IPs. يمر الوضع عبر TCP ميناء 8905 في هذا سيناريو.

  3. يجب أن يكون **للشهادة المؤسوأل** على عقد PSN **login.cisco.com** في **حقل SAN**. يتم حماية الاتصال بين مستخدم شبكة VPN وعقدة PSN عبر TCP 8905 عبر شهادة المؤسوأل وسيحصل المستخدم على تحذير بالشهادة في حالة عدم وجود هذا الاسم "login.cisco.com" في شهادة المؤسوأل لعقدة PSN.

  ملاحظة: وفقا لشهادة RFC6125، يجب تجاهل CN إذا تم تحديد قيم شبكة منطقة التخزين (SAN). هذا يعني أننا بحاجة أيضا إلى إضافة CN لشهادة المؤسوأل في حقل SAN.

- الإمداد التلقائي عبر بوابة إمداد العميل (CPP) - يتم تنزيل الوحدة النمطية وتثبيتها من نظام ISE من خلال الوصول إلى CPP مباشرة عبر FQDN الخاص بالمدخل.
  يجب الوفاء بالشروط التالية للعمل في الوضع مع توفير وحدة ISE Posture Module التلقائية:

  1. يجب أن يقوم DNS بحل **FQDN الخاص ب CPP** إلى عقد خدمة السياسة (PSNs) IPs.

  2. يجب السماح **بمنافذ TCP 80 و 443 ذ منفذ CPP (8443 بشكل افتراضي)** للشبكات PSN IPs. يحتاج العميل إلى فتح CPP FQDN مباشرة عبر HTTP (سيتم إعادة توجيهه إلى HTTPS) أو HTTPS، وسيتم إعادة توجيه هذا الطلب إلى منفذ CPP (8443 بشكل افتراضي) ثم تنتقل الحالة عبر ذلك المنفذ.

  3. يجب أن تحتوي **شهادات Admin و CPP** على عقد PSN **على CPP FQDN** في **حقل SAN**. تتم حماية الاتصال بين مستخدم شبكة VPN وعقدة PSN عبر TCP 443 بواسطة شهادة CPP. يتم حماية الاتصال على منفذ CPP بواسطة شهادة المؤسوأل.

  ملاحظة: وفقا لشهادة RFC6125، يجب تجاهل CN إذا تم تحديد قيم شبكة منطقة التخزين (SAN). هذا يعني أننا بحاجة أيضا إلى إضافة CN من شهادات الإدارة و CPP في حقل SAN من الشهادات المقابلة.

  ملاحظة: إذا لم يكن برنامج ISE يحتوي على إصلاح ل CSCvj76466، فلن يعمل الوضع أو إمداد العميل إلا إذا تم توفير التخاب وأ إمداد العميل على PSN نفسه الذي تمت مصادقة العميل عليه.

في حالة الوضع باستخدام FlexVPN، يتضمن التدفق الخطوات التالية:

1. يتصل المستخدم بموزع FlexVPN باستخدام عميل AnyConnect.

2. يرسل ISE قبول الوصول إلى محور FlexVPN باسم قائمة التحكم في الوصول (ACL) التي يلزم تطبيقها لتقييد الوصول.

3a. الاتصال الأول بالإمداد اليدوي - تبدأ وحدة ISE Posture (وضعية محرك خدمات الهوية (ISE) في اكتشاف خادم النهج الذي يرسل المسار إلى enroll.cisco.com عبر منفذ TCP 8905. كنتيجة لذلك، تم تكوين ملف تعريف الوضع الخاص بالتنزيلات الخاصة بوحدة الوضع وتحديث وحدة التوافق النمطية على جانب العميل.

أثناء محاولات الاتصال التالية، سوف تستخدم وحدة ISE Posture (وضعية محرك خدمات الهوية (ISE) أيضا الأسماء و IPs المحددة في "قائمة الاتصال بالمنزل" لملف تعريف الوضع اكتشاف خادم النهج.

3b. الاتصال الأول بالإمداد التلقائي - يقوم العميل بفتح CPP عبر FQDN. يتم تنزيل "مساعد إعداد الشبكة" كنتيجة لذلك محطة عمل العميل، ثم يقوم بتنزيل وتثبيت وحدة ISE Posture النمطية ووحدة توافق ISE وموجز تعريف الوضع.

أثناء محاولات الاتصال التالية، سوف تستخدم وحدة وضعية محرك خدمات الهوية (ISE) أسماء و IPs المحددة في قائمة "الاتصال بالمنزل" لملف تعريف الوضع اكتشاف خادم النهج.

4. تبدأ وحدة الوضع عمليات التحقق من المتثال وترسل نتائج التحقق إلى ISE.

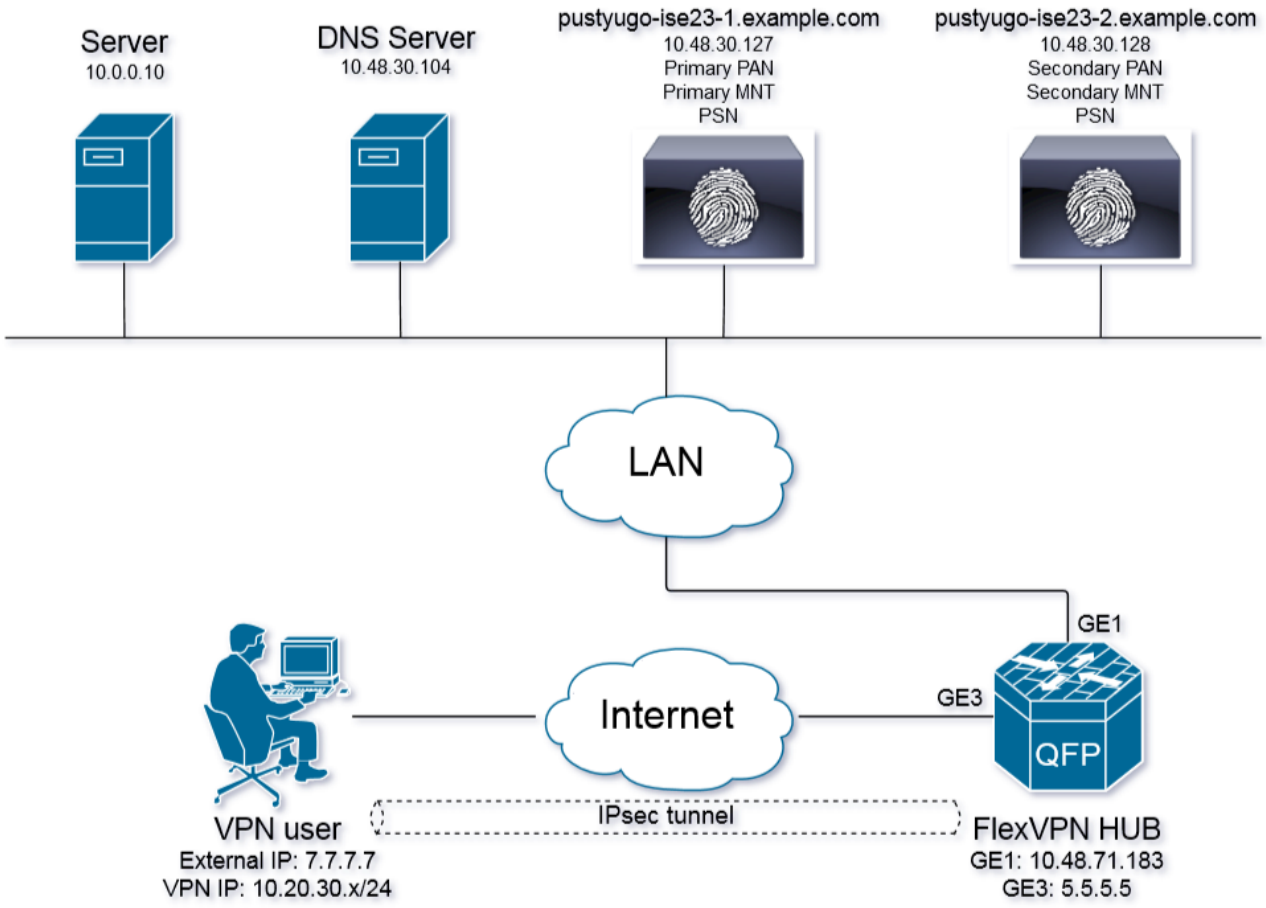
5. إذا كانت حالة العميل متوافقة، فعندئذ يقوم ISE بإرسال Access-Accept إلى محور FlexVPN باسم قائمة التحكم في الوصول (ACL) لكي يتم تطبيقها على العميل المتوافق.

6، يحصل العميل على حق الوصول إلى الشبكة.

مزيد من التفاصيل حول عملية الوضع التي يمكنك العثور عليها في المستند مقارنة طمن ISE Posture (مقارنة طمن ISE) للpre و Post 2.2".

التكوين

الرسم التخطيطي للشبكة

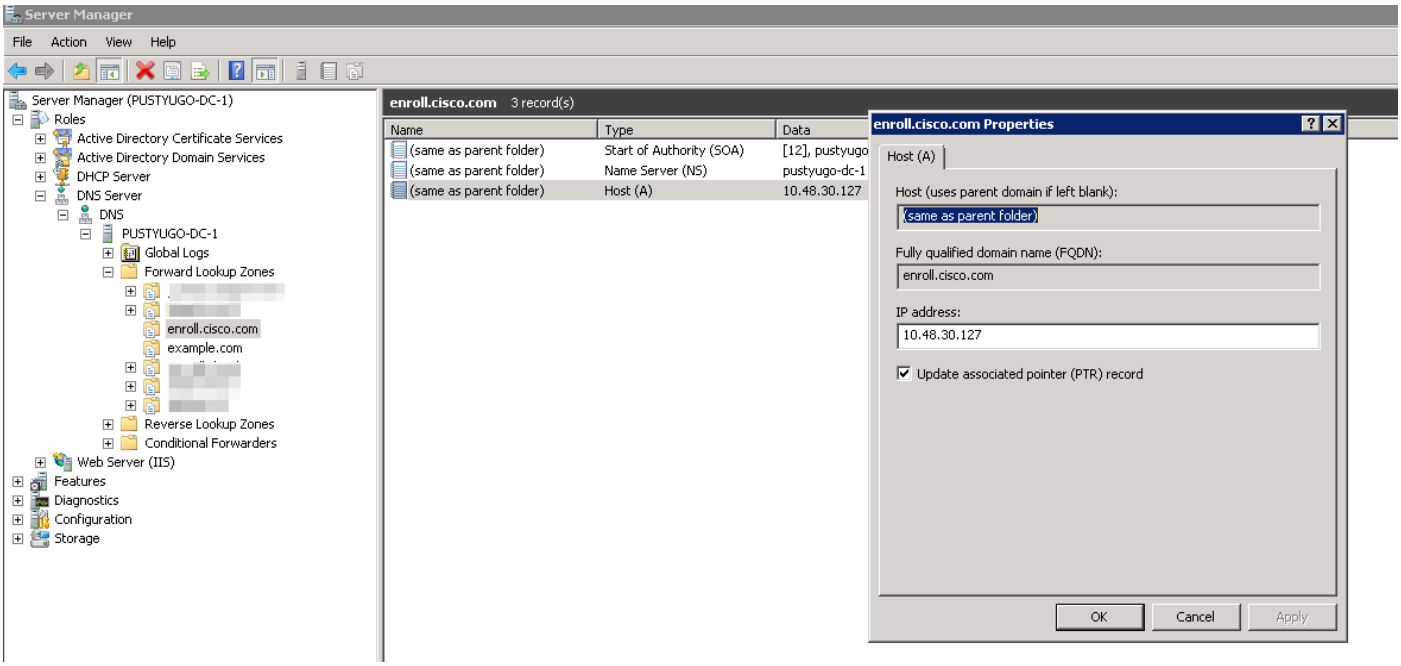


سيحصل مستخدم شبكة VPN على حق الوصول إلى الخادم (10.0.0.10) فقط إذا كانت حالة التوافق لديه.

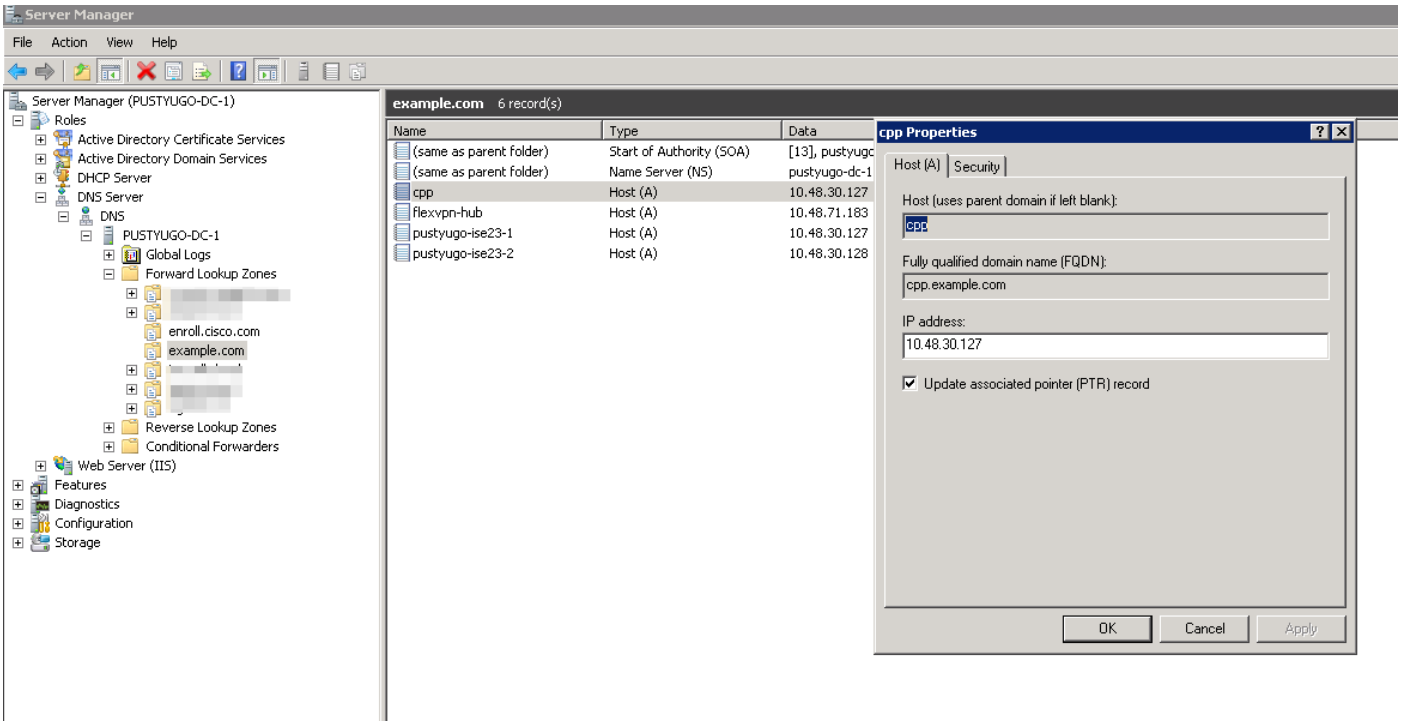
تكوين خادم DNS

في هذا المستند، يتم إستخدام Windows Server 2008 R2 كخادم DNS.

الخطوة 1. إضافة سجل **المضيف (A)** لـ **login.cisco.com** يشير إلى **IP لـ PSN**:



الخطوة 2. إضافة سجل **المضيف (A)** ل CPP FQDN (**CPP.example.com** المستخدم في هذا المثال) يشير إلى **IP ل PSN**:



التكوين الأولي IOS XE

تكوين شهادة الهوية

سيستخدم الموجه الشهادة لمصادقة نفسه على عميل AnyConnect. يجب أن يكون ترخيص الموجه موثوقا به من قبل نظام التشغيل الخاص بالمستخدم لتجنب تحذير الشهادة أثناء مرحلة تأسيس الاتصال.

يمكن تقديم شهادة الهوية بإحدى الطرق التالية:

ملاحظة: إستخدام الشهادات الموقعة ذاتيا غير مدعوم مع IKEv2 FlexVPN.

الخيار 1 - تكوين خادم المرجع المصدق (CA) على الموجه

ملاحظة: يمكن إنشاء خادم CA على موجه IOS نفسه أو موجه آخر. في هذه المقالة، يتم إنشاء CA على الموجه نفسه.

ملاحظة: تحتاج إلى مزامنة الوقت مع خادم NTP قبل التمكن من تمكين خادم CA.

ملاحظة: يرجى ملاحظة أن المستخدم لن يتمكن من التحقق من صحة هذه الشهادة، وبالتالي لن تكون بيانات المستخدم محمية ضد هجمات الدخيل إلا إذا تم التحقق من شهادة المرجع المصدق يدويا وتم إستيرادها إلى جهاز المستخدم قبل تأسيس الاتصال.

الخطوة 1. إنشاء مفاتيح RSA لخادم CA:

```
FlexVPN-HUB(config)# crypto key generate rsa label ROOT-CA modulus 2048
```

الخطوة 2. إنشاء مفاتيح RSA لشهادة الهوية:

```
FlexVPN-HUB(config)# crypto key generate rsa label FLEX-1 modulus 2048
```

التحقق:

```
FlexVPN-HUB# show crypto key mypubkey rsa

 ---- output truncated -----

Key name: ROOT-CA
Key type: RSA KEYS
 Storage Device: private-config
 Usage: General Purpose Key
 Key is not exportable. Redundancy enabled.
 Key Data:
 30820122 300D0609 2A864886 F70D0101 01050003 82010F00 3082010A 02820101
 00C01F04 E0AF3AB8 97CED516 3B31152A 5C3678A0 829A0D0D 2F46D86C 2CBC9175
----- output truncated ------ ----- output truncated ------ Key name: FLEX-1
Key type: RSA KEYS
 Storage Device: private-config
 Usage: General Purpose Key
 Key is not exportable. Redundancy enabled.
 Key Data:
 30820122 300D0609 2A864886 F70D0101 01050003 82010F00 3082010A 02820101
 009091AE 4185DC96 4F561F7E 506D56E8 240606D0 CC16CC5E E4E24EEB 1664E42C ----- output truncated
------
```

الخطوة 3. قم بتكوين المرجع المصدق:

```
ip http server
crypto pki server ROOT-CA
 issuer-name cn=ROOT-CA.example.com
 hash sha256
 lifetime certificate 1095
 lifetime ca-certificate 3650
 eku server-auth
 no shutdown
```

التحقق:

```
FlexVPN-HUB# show crypto pki server

Certificate Server ROOT-CA:
   Status: enabled
   State: enabled
   Server's configuration is locked  (enter "shut" to unlock it)
   Issuer name: cn=ROOT-CA.example.com
   CA cert fingerprint: A5522AAB 1410E645 667F0D70 49AADA45
   Granting mode is: auto
   Last certificate issued serial number (hex): 3
   CA certificate expiration timer: 18:12:07 UTC Mar 26 2021
   CRL NextUpdate timer: 21:52:55 UTC May 21 2018
   Current primary storage dir: nvram:
   Database Level: Minimum - no cert data written to storage
```

الخطوة 4. تكوين TrustPoint:

```
interface loopback 0
ip address 10.10.10.10 255.255.255.255
crypto pki trustpoint FLEX-TP-1
 enrollment url http://10.10.10.10:80
 fqdn none
 subject-name cn=flexvpn-hub.example.com
 revocation-check none
 rsakeypair FLEX-1
```

الخطوة 5. مصادقة المرجع المصدق:

```
FlexVPN-HUB(config)#crypto pki authenticate FLEX-TP-1
Certificate has the following attributes:
      Fingerprint MD5: A5522AAB 1410E645 667F0D70 49AADA45
     Fingerprint SHA1: F52EAB1A D39642E7 D8EAB804 0EB30973 7647A860

% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
```

الخطوة 6. تسجيل الموجه إلى CA:

```
FlexVPN-HUB(config)#crypto pki enroll FLEX-TP-1
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this
  password to the CA Administrator in order to revoke your certificate.
  For security reasons your password will not be saved in the configuration.
  Please make a note of it.

Password:
Re-enter password:

% The subject name in the certificate will include: cn=flexvpn-hub.example.com
% The fully-qualified domain name will not be included in the certificate
% Include the router serial number in the subject name? [yes/no]: no
% Include an IP address in the subject name? [no]: no
Request certificate from CA? [yes/no]: yes
% Certificate request sent to Certificate Authority
% The 'show crypto pki certificate verbose FLEX-TP-1' commandwill show the fingerprint.

May 21 16:16:55.922: CRYPTO_PKI:  Certificate Request Fingerprint MD5: 80B1FAFD 35346D0F
D23F6648 F83F039B
May 21 16:16:55.924: CRYPTO_PKI:  Certificate Request Fingerprint SHA1: A8401EDE 35EE4AF8
46C4D619 8D653BFD 079C44F7
```

تحقق من طلبات الشهادات المعلقة على المرجع المصدق وتأكد من مطابقة بصمة الإصبع:

```
FlexVPN-HUB#show crypto pki server ROOT-CA requests
Enrollment Request Database:

Subordinate CA certificate requests:
ReqID  State      Fingerprint                      SubjectName
--------------------------------------------------------------

RA certificate requests:
ReqID  State      Fingerprint                      SubjectName
--------------------------------------------------------------

Router certificates requests:
```

```
ReqID  State      Fingerprint                       SubjectName
--------------------------------------------------------------
1      pending    80B1FAFD35346D0FD23F6648F83F039B cn=flexvpn-hub.example.com
```

الخطوة 7. منح الشهادة باستخدام ReqID المناسب:

```
FlexVPN-HUB#crypto pki server ROOT-CA grant 1
```

انتظر حتى يطلب الموجه للشهادة مرة أخرى (وقوا له اذا التكوين سيتم التحقق 10 مرات مرة واحدة في الدقيقة). ابحث عن رسالة syslog:

```
May 21 16:18:56.375: %PKI-6-CERTRET: Certificate received from Certificate Authority
```

تحقق من تثبيت الشهادة:

```
FlexVPN-HUB#show crypto pki certificates FLEX-TP-1
Certificate
 Status: Available
 Certificate Serial Number (hex): 04
 Certificate Usage: General Purpose
 Issuer:
   cn=ROOT-CA.example.com
 Subject:
   Name: flexvpn-hub.example.com
   cn=flexvpn-hub.example.com
 Validity Date:
   start date: 16:18:16 UTC May 21 2018
   end   date: 18:12:07 UTC Mar 26 2021
 Associated Trustpoints: FLEX-TP-1

CA Certificate
 Status: Available
 Certificate Serial Number (hex): 01
 Certificate Usage: Signature
 Issuer:
   cn=ROOT-CA.example.com
 Subject:
   cn=ROOT-CA.example.com
 Validity Date:
   start date: 18:12:07 UTC Mar 27 2018
   end   date: 18:12:07 UTC Mar 26 2021
 Associated Trustpoints: FLEX-TP-1 ROOT-CA
 Storage: nvram:ROOT-CAexamp#1CA.cer
```

الخيار 2 - استيراد شهادة موقعة خارجيا

```
FlexVPN-HUB(config)# crypto pki import FLEX-TP-2 pkcs12 ftp://cisco:cisco@10.48.30.130/ password
cisco123
% Importing pkcs12...
Address or name of remote host [10.48.30.130]?
Source filename [FLEX-TP-2]? flexvpn-hub.example.com.p12
Reading file from ftp://cisco@10.48.30.130/flexvpn-hub.example.com.p12!
[OK - 4416/4096 bytes]
% The CA cert is not self-signed.
% Do you also want to create trustpoints for CAs higher in
% the hierarchy? [yes/no]:
May 21 16:55:26.344: %CRYPTO_ENGINE-5-KEY_ADDITION: A key named FLEX-TP-2 has been generated or
imported
```

```
yes
CRYPTO_PKI: Imported PKCS12 file successfully.
FlexVPN-HUB(config)#
May 21 16:55:34.396: %PKI-6-PKCS12IMPORT_SUCCESS: PKCS #12 Successfully Imported.
FlexVPN-HUB(config)#
```

تكوين IKEv2

الخطوة 1. تكوين خادم RADIUS و CoA:

```
aaa group server radius FlexVPN-AuthC-Server-Group-1
 server-private 10.48.30.127 key Cisco123
server-private 10.48.30.128 key Cisco123



aaa server radius dynamic-author
 client 10.48.30.127 server-key Cisco123
client 10.48.30.128 server-key Cisco123
 server-key Cisco123
 auth-type any
```

الخطوة 2. تكوين قوائم المصادقة والتفويض:

```
aaa new-model
aaa authentication login FlexVPN-AuthC-List-1 group FlexVPN-AuthC-Server-Group-1
aaa authorization network FlexVPN-AuthZ-List-1 local
aaa accounting update newinfo
aaa accounting network FlexVPN-Accounting-List-1 start-stop group FlexVPN-AuthC-Server-Group-1
```

الخطوة 3. إنشاء نهج تخويل IKEv2:

```
crypto ikev2 authorization policy FlexVPN-Local-Policy-1
 pool FlexVPN-Pool-1
 dns 10.48.30.104
 netmask 255.255.255.0
 def-domain example.com
```

الخطوة 4. إنشاء ملف تعريف IKEv2:

```
crypto ikev2 profile FlexVPN-IKEv2-Profile-1
 match identity remote key-id example.com
 identity local dn
 authentication local rsa-sig
 authentication remote eap query-identity
 pki trustpoint FLEX-TP-2
 dpd 60 2 on-demand
 aaa authentication eap FlexVPN-AuthC-List-1
 aaa authorization group eap list FlexVPN-AuthZ-List-1 FlexVPN-Local-Policy-1
 aaa authorization user eap cached
 aaa accounting eap FlexVPN-Accounting-List-1
 virtual-template 10
```

الخطوة 5. إنشاء مجموعة تحويل وملف تعريف IPSec:

```
crypto ipsec transform-set FlexVPN-TS-1 esp-aes esp-sha-hmac
 mode tunnel
crypto ipsec profile FlexVPN-IPsec-Profile-1
 set transform-set FlexVPN-TS-1
```

```
 set ikev2-profile FlexVPN-IKEv2-Profile-1
```
الخطوة 6. إنشاء واجهة قالب ظاهري:

```
interface Virtual-Template10 type tunnel
 ip unnumbered GigabitEthernet3
 tunnel mode ipsec ipv4
 tunnel protection ipsec profile FlexVPN-IPsec-Profile-1
```
الخطوة 7. إنشاء تجمع محلي:

```
ip local pool FlexVPN-Pool-1 10.20.30.100 10.20.30.200
```
الخطوة 8. قم بإنشاء قائمة تحكم في الوصول (ACL) لتقييد وصول العملاء غير المتوافقين. أثناء حالة الوضع غير المعروف، يجب توفير هذه الأذونات على الأقل:

- حركة مرور DNS
- حركة المرور إلى ISE PSNs عبر المنافذ 80 و 443 و 8905
- حركة المرور إلى ISE PSNs التي يشير إليها اسم المجال المؤهل بالكامل لـ CPP FQDN
- حركة مرور البيانات إلى خوادم الإصلاح إذا لزم الأمر

هذا مثال على قائمة التحكم في الوصول (ACL) بدون خوادم الإصلاح، تتم إضافة الرفض الصريح لشبكة 10.0.0.0/24 لإمكانية الرؤية، كما يوجد ضمني "deny ip any any" في نهاية قائمة التحكم في الوصول:

```
ip access-list extended DENY_SERVER
 permit udp any any eq domain
 permit tcp any host 10.48.30.127 eq 80
 permit tcp any host 10.48.30.127 eq 443
 permit tcp any host 10.48.30.127 eq 8443
 permit tcp any host 10.48.30.127 eq 8905
 permit tcp any host 10.48.30.128 eq 80
 permit tcp any host 10.48.30.128 eq 443
 permit tcp any host 10.48.30.128 eq 8443
 permit tcp any host 10.48.30.128 eq 8905
 deny   ip any 10.0.0.0 0.0.0.255
```
الخطوة 9. إنشاء قائمة تحكم في الوصول (ACL) للسماح بالوصول إلى العملاء المتوافقين:

```
ip access-list extended PERMIT_ALL
 permit ip any any
```
الخطوة 10. تكوين النفق المنقسم (إختياري)

بشكل افتراضي، سيتم توجيه جميع حركات مرور البيانات عبر شبكة VPN. in order to أنفق حركة مرور فقط إلى الشبكات المحددة، أنت يستطيع عينت هم في ال ikeV2 تخويل سياسة قسم. من الممكن إضافة عبارات متعددة أو إستخدام قائمة الوصول القياسية.

```
crypto ikev2 authorization policy FlexVPN-Local-Policy-1
     route set remote ipv4 10.0.0.0 255.0.0.0
```
الخطوة 11. الوصول إلى الإنترنت للأجهزة العميلة البعيدة (إختياري)

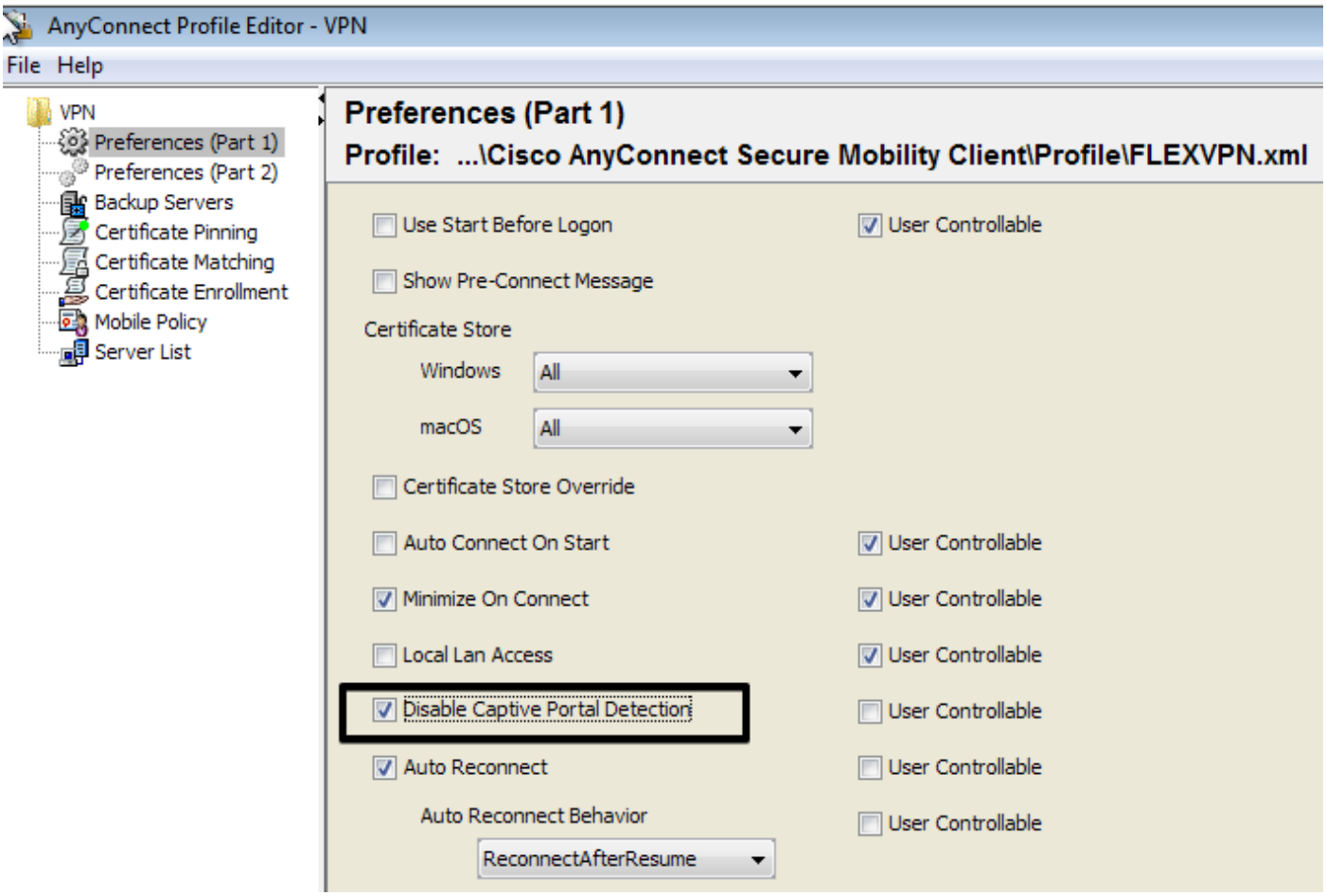
in order to شكلت الاتصالات الصادرة من ال بعيد منفذ زبون إلى المضيف في الإنترنت أن يكون NAT-ed إلى العالمي ip عنوان من المسحاج تخديد، ال nat ترجمة:

```
ip access-list extended NAT
 permit ip 10.20.30.0 0.0.0.255 any

ip nat inside source list NAT interface GigabitEthernet1 overload extended

interface GigabitEthernet1
ip nat outside

interface Virtual-Template 10
ip nat inside
```

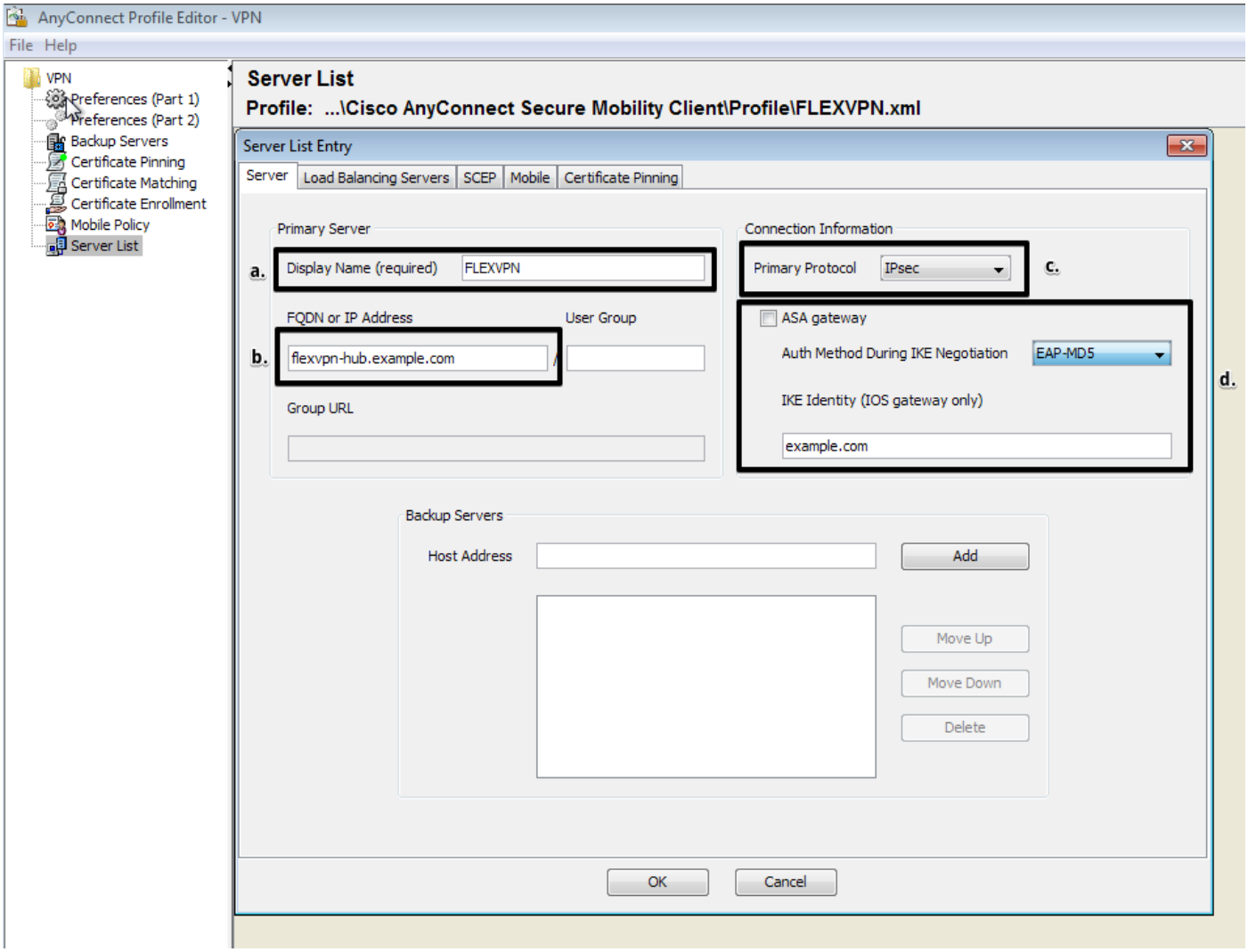
تكوين ملف تعريف عميل AnyConnect

قم بتكوين ملف تعريف العميل باستخدام محرر ملف تعريف AnyConnect. يتم حفظ ملفات تعريف AnyConnect Security Mobile Client على Windows 7 و 10 في **%ProgramData%\Cisco\Cisco AnyConnect Secure Mobility Client\Profile**.

الخطوة 1. تعطيل ميزة "كشف البوابة المقيدة". إذا لم يتم تعطيل خادم HTTP على لوحة وصل FlexVPN، فستتسبب ميزة اكتشاف البوابة المقيدة ل AnyConnect في فشل الاتصال. الرجاء ملاحظة أن خادم CA لن يعمل بدون خادم HTTP.



الخطوة 2. تكوين قائمة الخوادم:



- أدخل اسم العرض.
- دخلت **FQDN** أو **ip** عنوان من FlexVPN صرة.
- حدد **IPsec** كبروتوكول أساسي.
- قم بإلغاء تحديد خانة الاختيار "عبارة ASA" وحدد **EAP-MD5** كطريقة مصادقة. أدخل هوية IKE تمامًا كما هو الحال في تكوين ملف تعريف IKEv2 على لوحة وصل FlexVPN (في هذا المثال، يتم تكوين ملف تعريف IKEv2 باستخدام الأمر "match identity remote key-id example.com"، لذلك نحتاج إلى إستخدام **example.com** كهوية IKE).

الخطوة 3. احفظ ملف التعريف في **%ProgramData%\Cisco\Cisco AnyConnect Secure Mobility Client\Profile** وأعد تشغيل التاي المتردد.

مرادف XML لملف التعريف:

```
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://schemas.xmlsoap.org/encoding/ AnyConnectProfile.xsd">
   <ClientInitialization>
       <UseStartBeforeLogon UserControllable="true">false</UseStartBeforeLogon>
       <AutomaticCertSelection UserControllable="true">true</AutomaticCertSelection>
       <ShowPreConnectMessage>false</ShowPreConnectMessage>
       <CertificateStore>All</CertificateStore>
       <CertificateStoreMac>All</CertificateStoreMac>
```

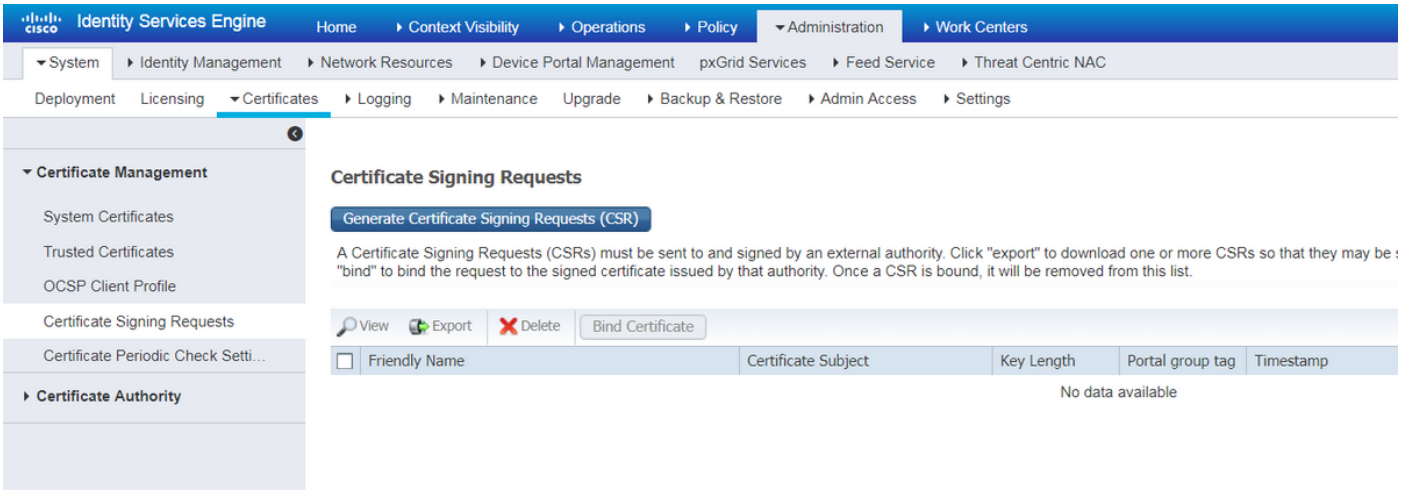
```
        <CertificateStoreOverride>false</CertificateStoreOverride>
        <ProxySettings>Native</ProxySettings>
        <AllowLocalProxyConnections>false</AllowLocalProxyConnections>
        <AuthenticationTimeout>12</AuthenticationTimeout>
        <AutoConnectOnStart UserControllable="true">false</AutoConnectOnStart>
        <MinimizeOnConnect UserControllable="true">true</MinimizeOnConnect>
        <LocalLanAccess UserControllable="true">false</LocalLanAccess>
        <DisableCaptivePortalDetection
UserControllable="false">true</DisableCaptivePortalDetection>
        <ClearSmartcardPin UserControllable="true">false</ClearSmartcardPin>
        <IPProtocolSupport>IPv4,IPv6</IPProtocolSupport>
        <AutoReconnect UserControllable="false">true
            <AutoReconnectBehavior
UserControllable="false">ReconnectAfterResume</AutoReconnectBehavior>
        </AutoReconnect>
        <AutoUpdate UserControllable="false">true</AutoUpdate>
        <RSASecurIDIntegration UserControllable="false">Automatic</RSASecurIDIntegration>
        <WindowsLogonEnforcement>SingleLocalLogon</WindowsLogonEnforcement>
        <WindowsVPNEstablishment>LocalUsersOnly</WindowsVPNEstablishment>
        <AutomaticVPNPolicy>false</AutomaticVPNPolicy>
        <PPPExclusion UserControllable="false">Automatic
            <PPPExclusionServerIP UserControllable="false"></PPPExclusionServerIP>
        </PPPExclusion>
        <EnableScripting UserControllable="false">false</EnableScripting>
        <EnableAutomaticServerSelection UserControllable="true">false
            <AutoServerSelectionImprovement>20</AutoServerSelectionImprovement>
            <AutoServerSelectionSuspendTime>4</AutoServerSelectionSuspendTime>
        </EnableAutomaticServerSelection>
        <RetainVpnOnLogoff>false
        </RetainVpnOnLogoff>
        <AllowManualHostInput>true</AllowManualHostInput>
    </ClientInitialization>
    <ServerList>
        <HostEntry>
            <HostName>FLEXVPN</HostName>
            <HostAddress>flexvpn-hub.example.com</HostAddress>
            <PrimaryProtocol>IPsec
                <StandardAuthenticationOnly>true
                    <AuthMethodDuringIKENegotiation>EAP-MD5</AuthMethodDuringIKENegotiation>
                    <IKEIdentity>example.com</IKEIdentity>
                </StandardAuthenticationOnly>
            </PrimaryProtocol>
        </HostEntry>
    </ServerList>
</AnyConnectProfile>
```

تكوين ISE

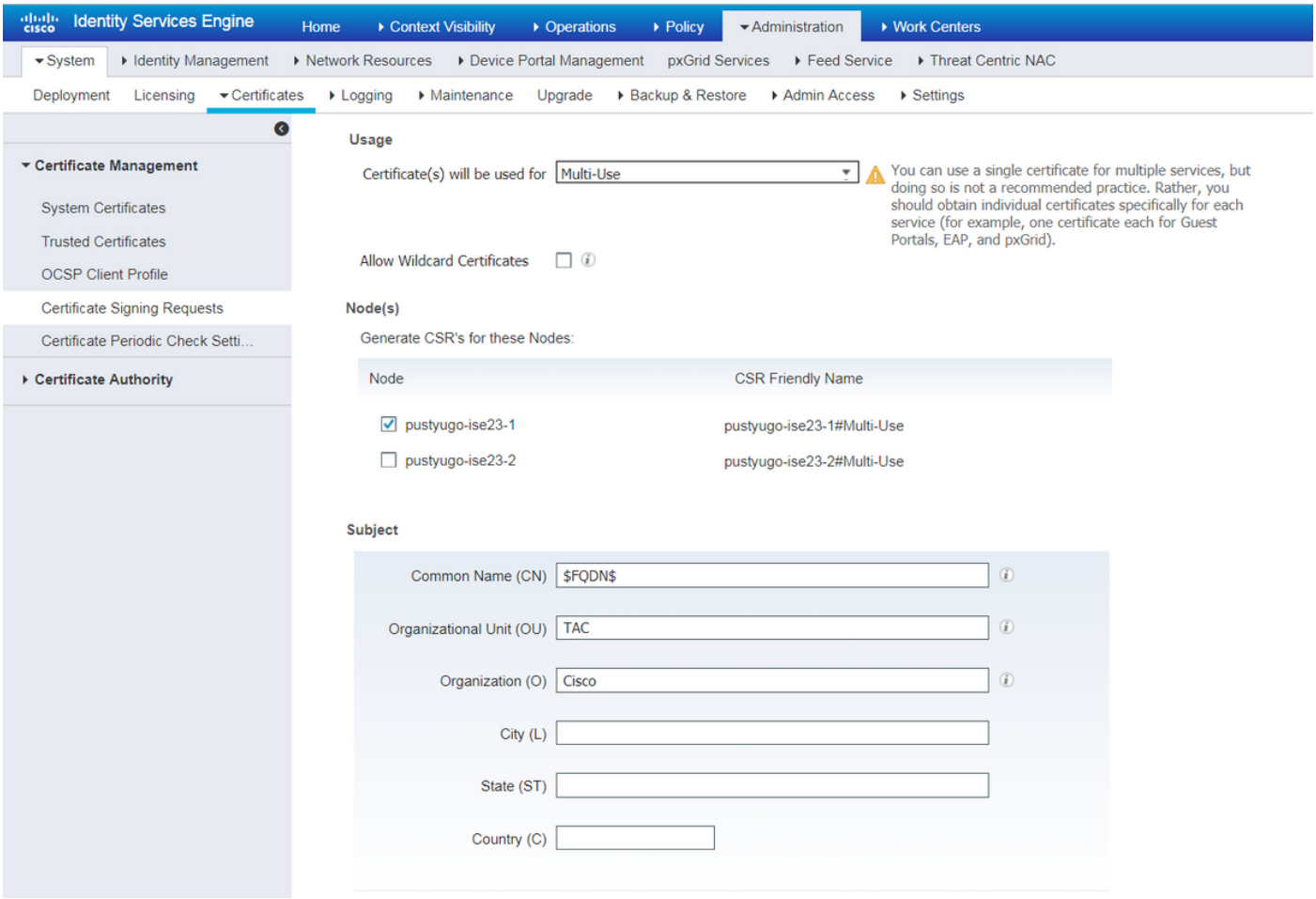
تكوين شهادات المسؤول و CPP

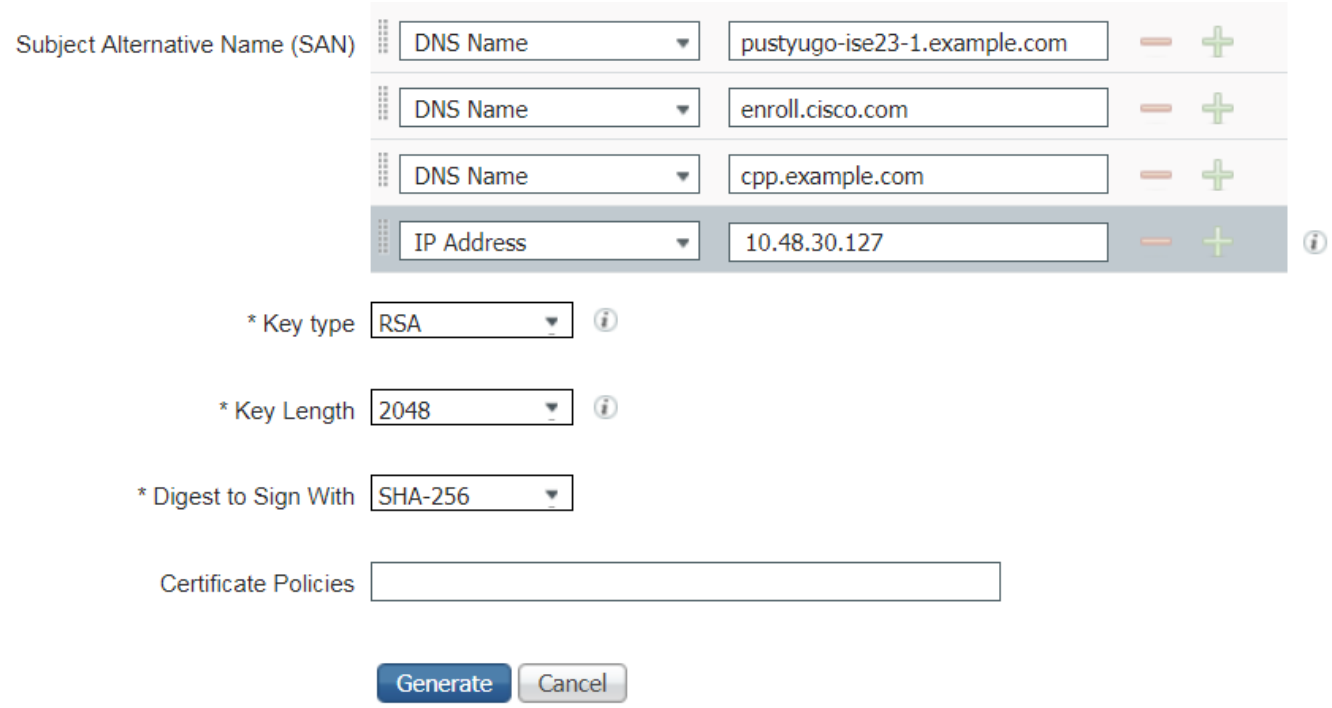
> **ملاحظة**: سيؤدي تغيير شهادة المسؤول إلى إعادة تشغيل العقدة التي تم تغيير الشهادة عليها.

الخطوة 1. انتقل إلى **الإدارة -> النظام -> الشهادات -> طلبات توقيع الشهادات**، انقر على **إنشاء طلبات توقيع الشهادات (CSR):**



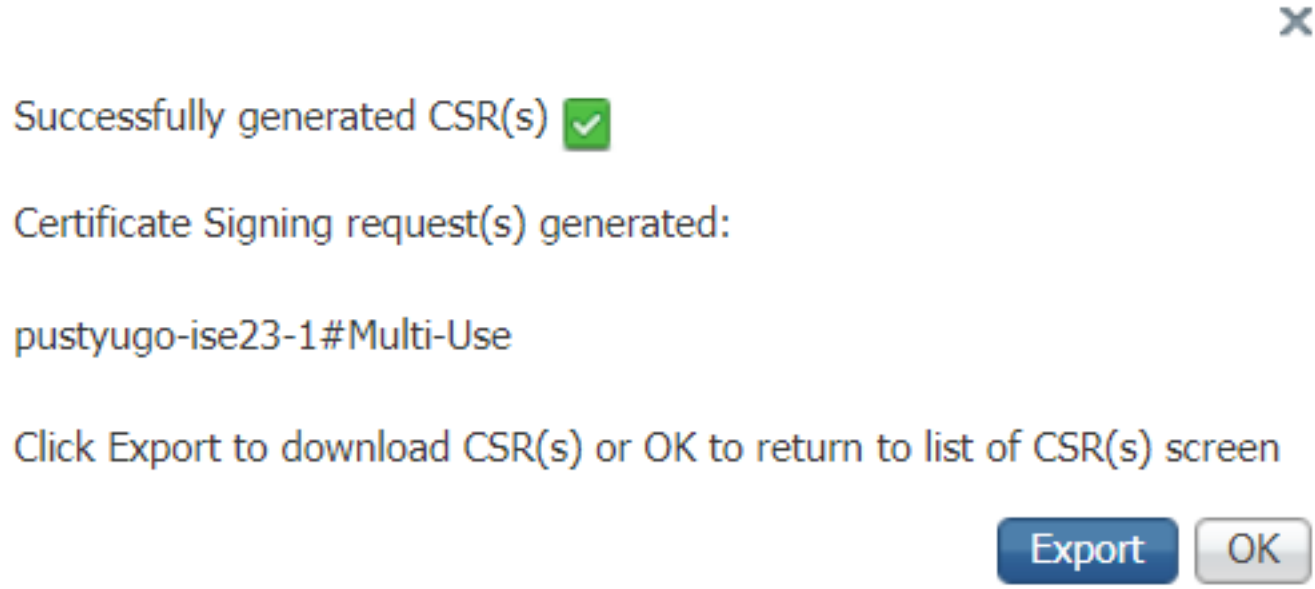
الخطوة 2. في الصفحة المفتوحة حدد عقدة PSN الضرورية، وقم بتعبئة الحقول الضرورية وإضافة FQDN للعقدة، enroll.cisco.com، cpp.example.com وعنوان IP للعقدة في حقول SAN وانقر **إنشاء**:





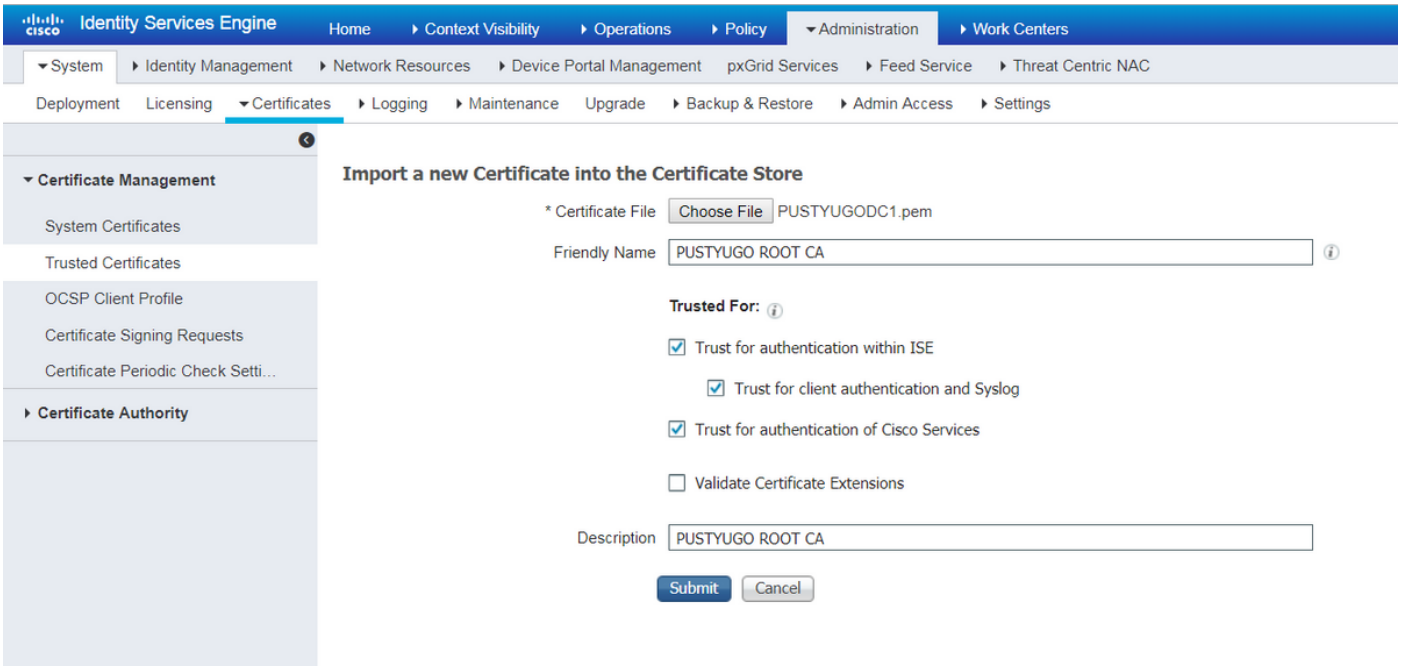
ملاحظة: إذا قمت بتحديد **إستخدام متعدد** في هذه الخطوة، فيمكنك إستخدام نفس الشهادة للمدخل أيضا.

في الإطار الظاهر، انقر فوق **تصدير** لحفظ CSR بتنسيق pem إلى محطة العمل المحلية:



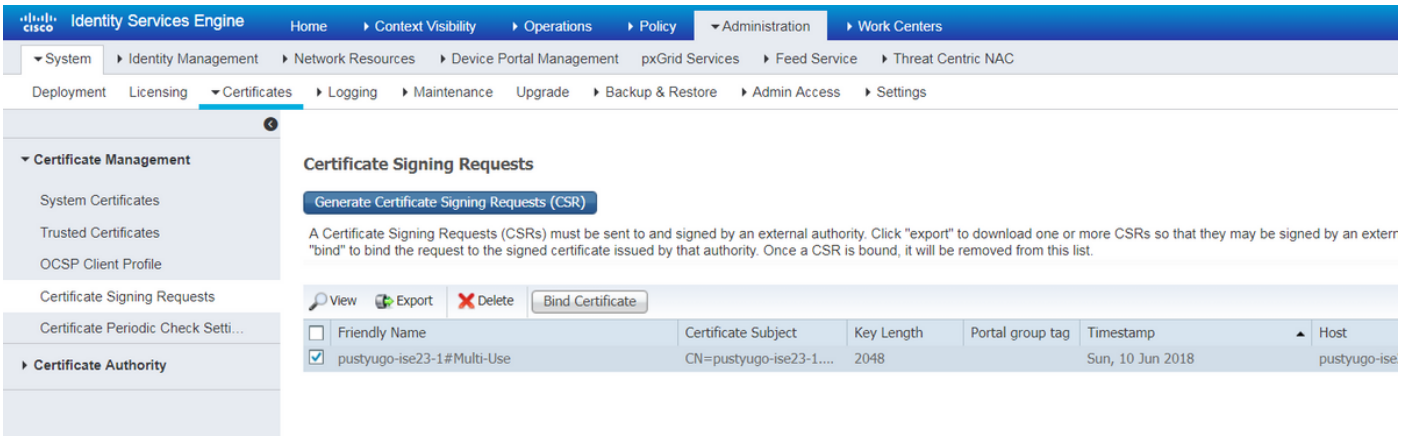
الخطوة 3. يغني ال CSR مع CA موثوق به ويحصل على ملف الترخيص من ال CA بالإضافة إلى السلسلة الكاملة من شهادات CA (الجذر والوسيط).

الخطوة 4. انتقل إلى **الإدارة -> النظام -> الشهادات -> الشهادات الموثوق بها**، انقر فوق **إستيراد. في الشاشة التالية انقر فوق إختيار ملف** وحدد ملف ترخيص CA **الجذر**، قم بتعبئة الاسم والوصف المألوف إذا لزم الأمر، وحدد ضروري **الخيارات الموثوق بها** وانقر فوق **إرسال:**

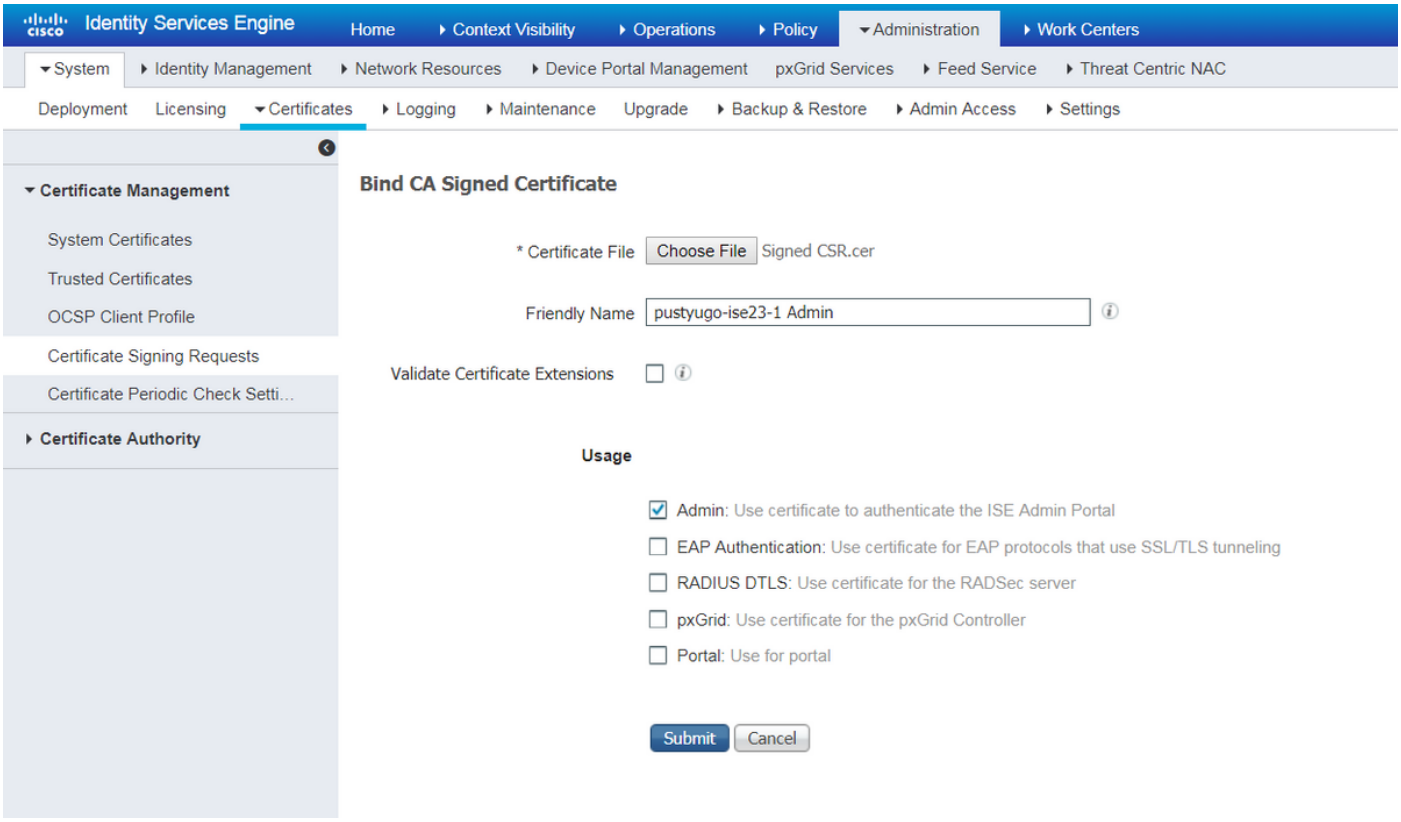


كرر هذه الخطوة لجميع الشهادات المتوسطة في السلسلة إذا كان هناك أي.

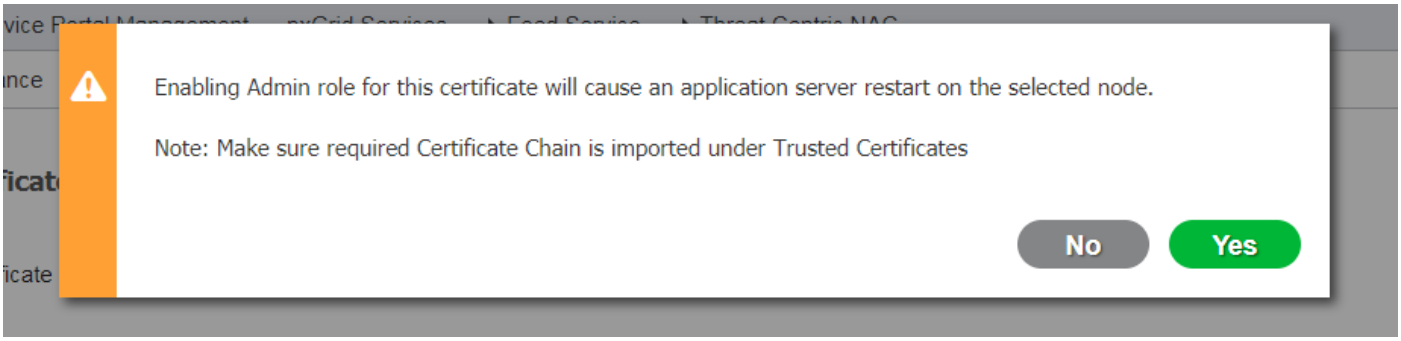
الخطوة 5. رجوع إلى **الإدارة -> النظام -> الشهادات -> طلبات توقيع الشهادات**، حدد CSR اللازم وانقر فوق **ربط الشهادة:**



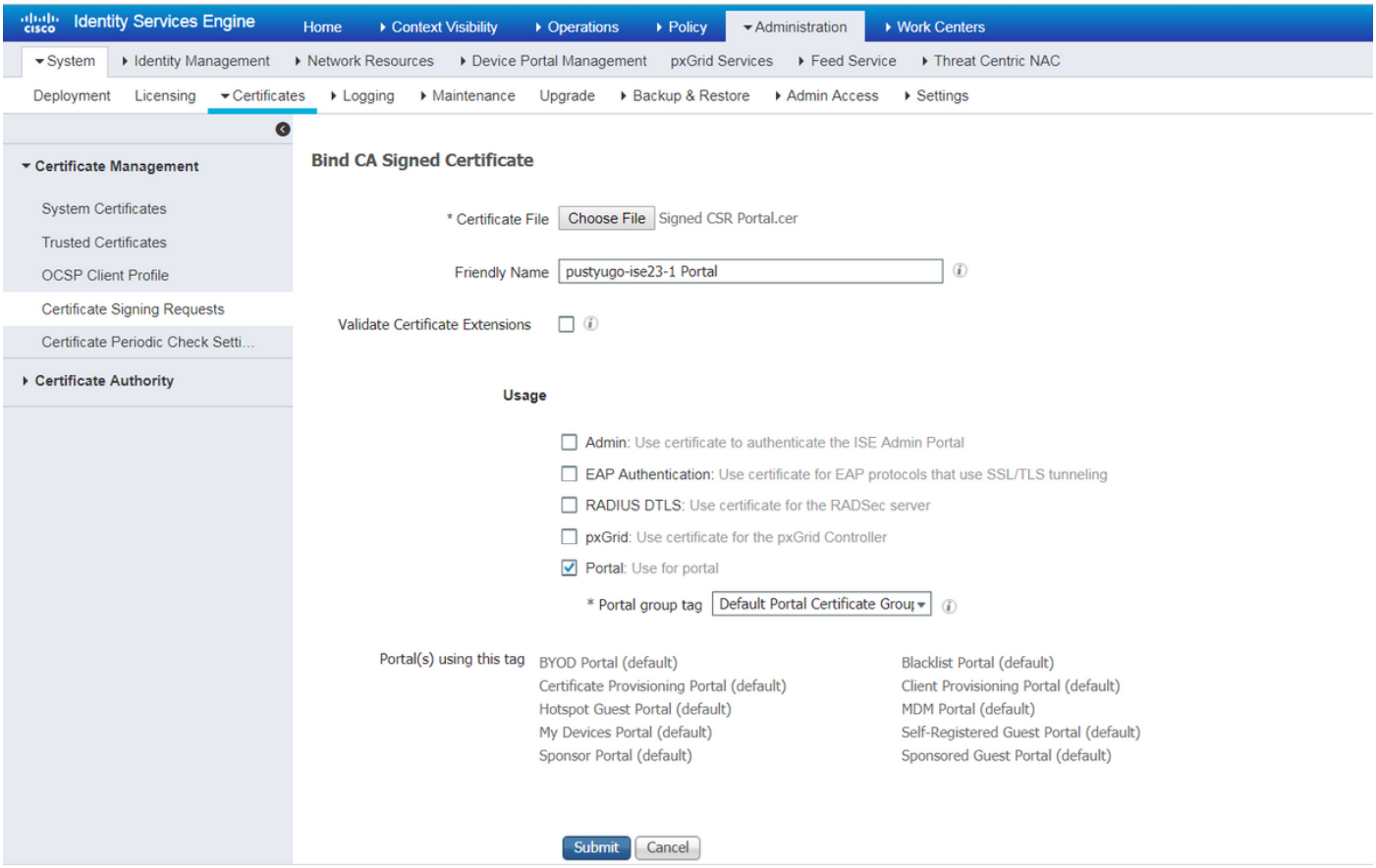
الخطوة 6. في الصفحة المفتوحة انقر فوق إختيار ملف، حدد ملف الشهادة الذي تم إستلامه من المرجع المصدق، ثم قم بإدخال اسم مألوف إذا لزم الأمر، ثم حدد **إستخدام: مسؤول** (**إستخدام: مدخل** أيضا يمكن تحديده انه إذا تم إنشاء CSR باستخدام **متعدد الاستخدام**) وانقر فوق **إرسال**:



الخطوة 7. في التحذير المنبثق، انقر فوق **نعم** لإنهاء الاستيراد. سيتم إعادة تشغيل العقدة المتأثرة بتغيير شهادة المسؤول:



كرر خطوات تغيير شهادة CPP إذا قررت إستخدام شهادة منفصلة للمدخل. في الخطوة 6 حدد **إستخدام: مدخل** وانقر فوق **إرسال:**

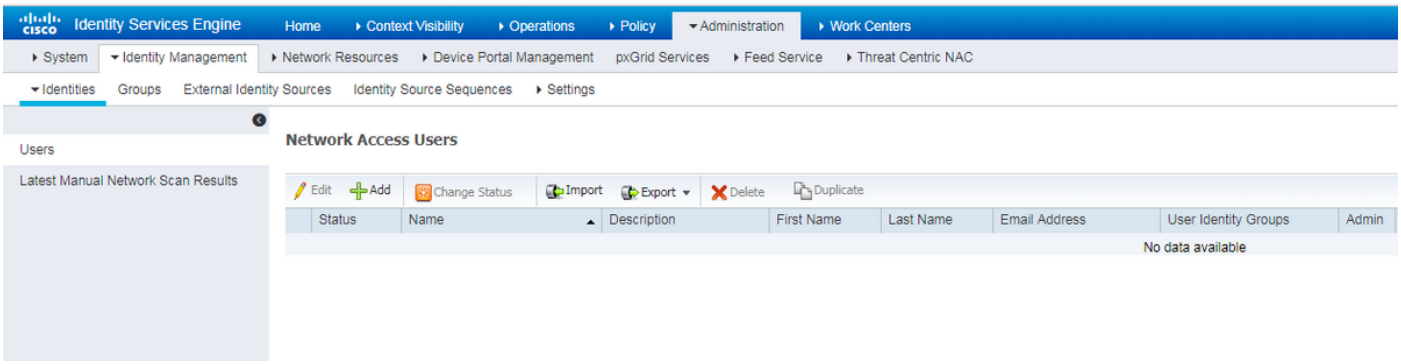


كرر الخطوات لجميع شبكات PSN في نشر ISE.

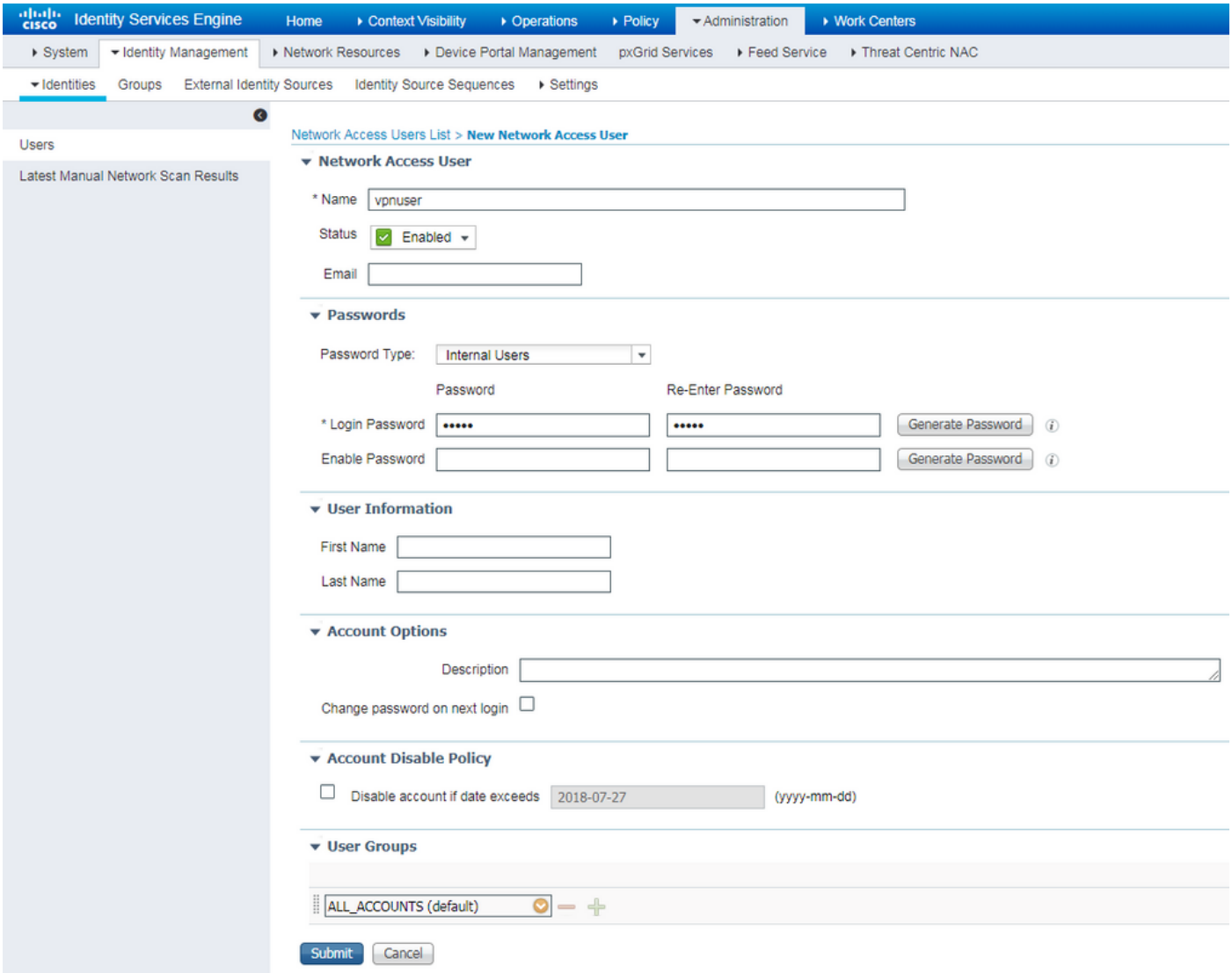
إنشاء مستخدم محلي على ISE

ملاحظة: باستخدام أسلوب EAP-MD5، يتم دعم المستخدمين المحليين فقط على ISE.

الخطوة 1. انتقل إلى **الإدارة -> إدارة الكيان المستقل -> الهويات -> المستخدمون**، انقر فوق **إضافة**.

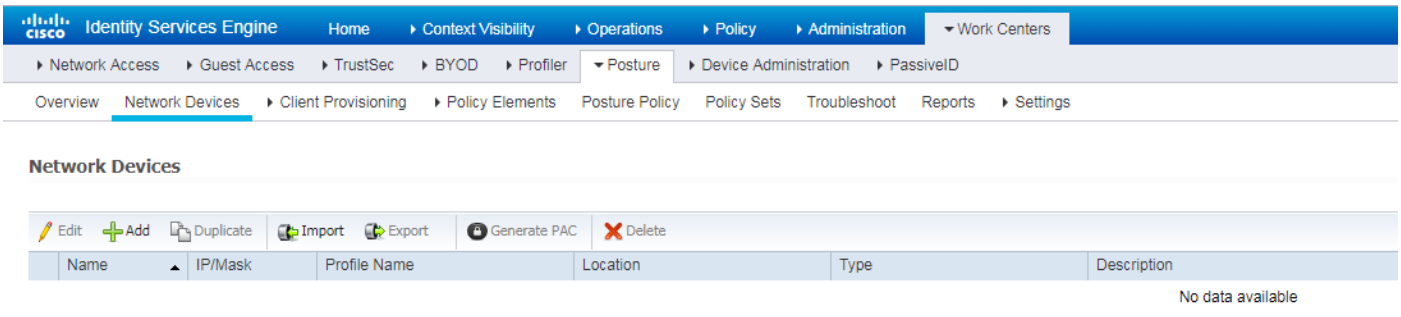


الخطوة 2. في الصفحة المفتوحة أدخل اسم المستخدم وكلمة المرور والمعلومات الضرورية الأخرى وانقر على **إرسال**.

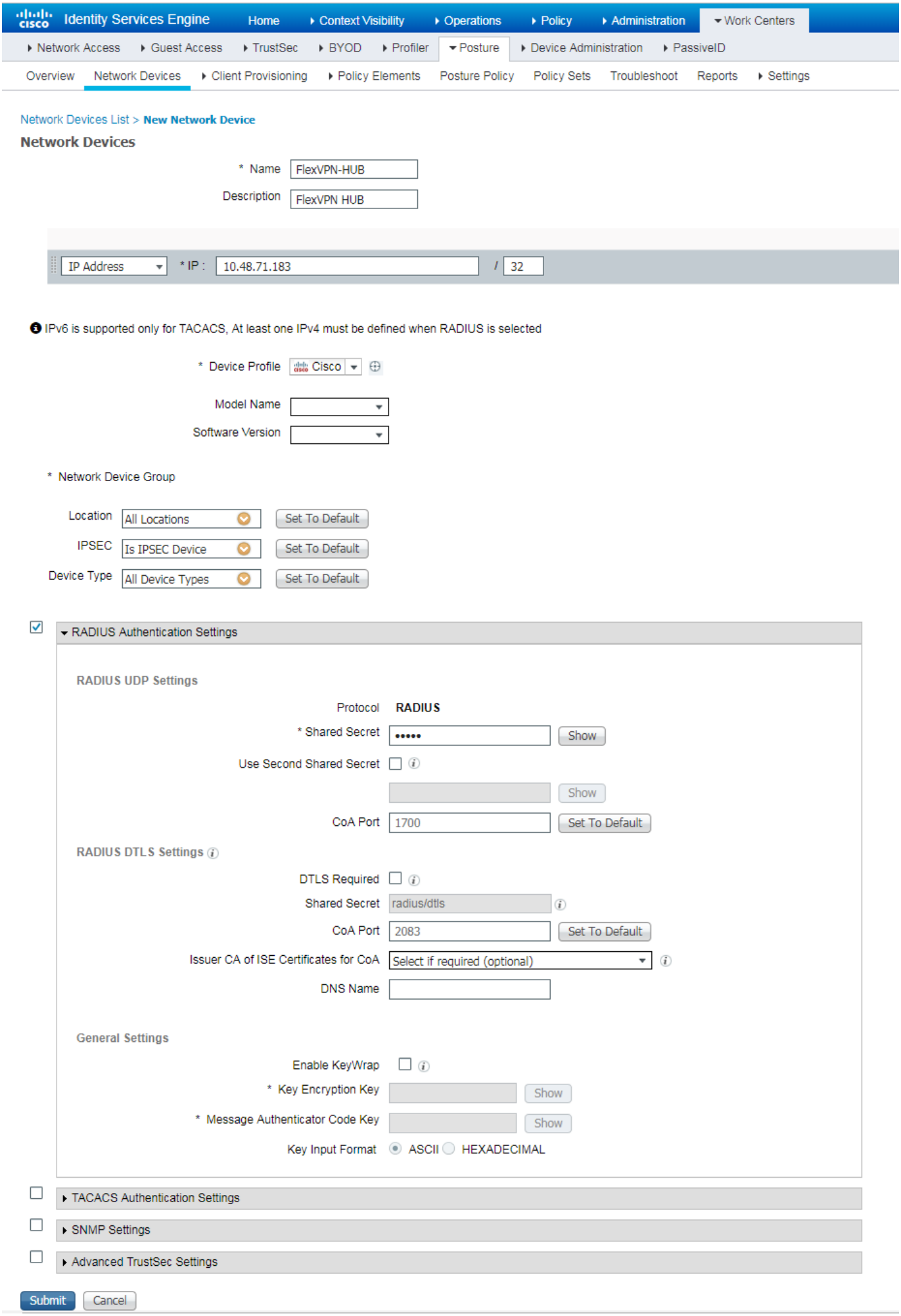


إضافة موزع FlexVPN كعميل RADIUS

الخطوة 1. انتقل إلى **مراكز العمل -> الوضع -> أجهزة الشبكة**، انقر **إضافة**.



ستير 2. في الصفحة المفتوحة أدخل اسم الجهاز، عنوان IP، المعلومات الضرورية الأخرى، حدد خانة الاختيار "إعدادات مصادقة RADIUS"، أدخل السر المشترك وانقر **إرسال** في أسفل الصفحة.

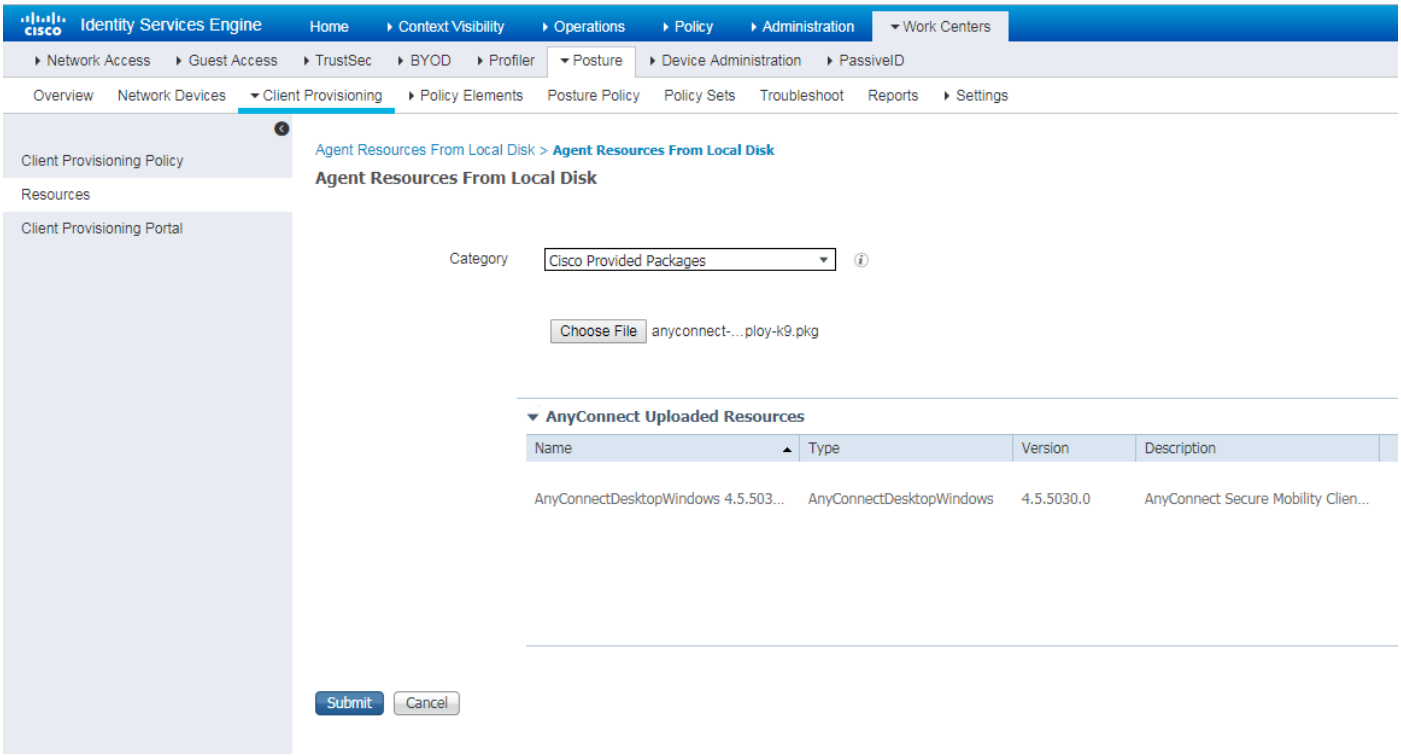

Identity Services Engine
Home
Context Visibility
Operations
Policy
Administration
Work Centers
Network Access
Guest Access
TrustSec
BYOD
Profiler
Posture
Device Administration
PassiveID
Overview
Network Devices
Client Provisioning
Policy Elements
Posture Policy
Policy Sets
Troubleshoot
Reports
Settings
Network Devices List > New Network Device
Network Devices
* Name
FlexVPN-HUB
Description
FlexVPN HUB
IP Address
* IP :
10.48.71.183
/
32
IPv6 is supported only for TACACS, At least one IPv4 must be defined when RADIUS is selected
* Device Profile
Cisco
Model Name
Software Version
* Network Device Group
Location
All Locations
Set To Default
IPSEC
Is IPSEC Device
Set To Default
Device Type
All Device Types
Set To Default
RADIUS Authentication Settings
RADIUS UDP Settings
Protocol
RADIUS
* Shared Secret
Show
Use Second Shared Secret
Show
CoA Port
1700
Set To Default
RADIUS DTLS Settings
DTLS Required
Shared Secret
radius/dtls
CoA Port
2083
Set To Default
Issuer CA of ISE Certificates for CoA
Select if required (optional)
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

تكوين إمداد العميل

هذه هي الخطوات لإعداد تكوين AnyConnect.

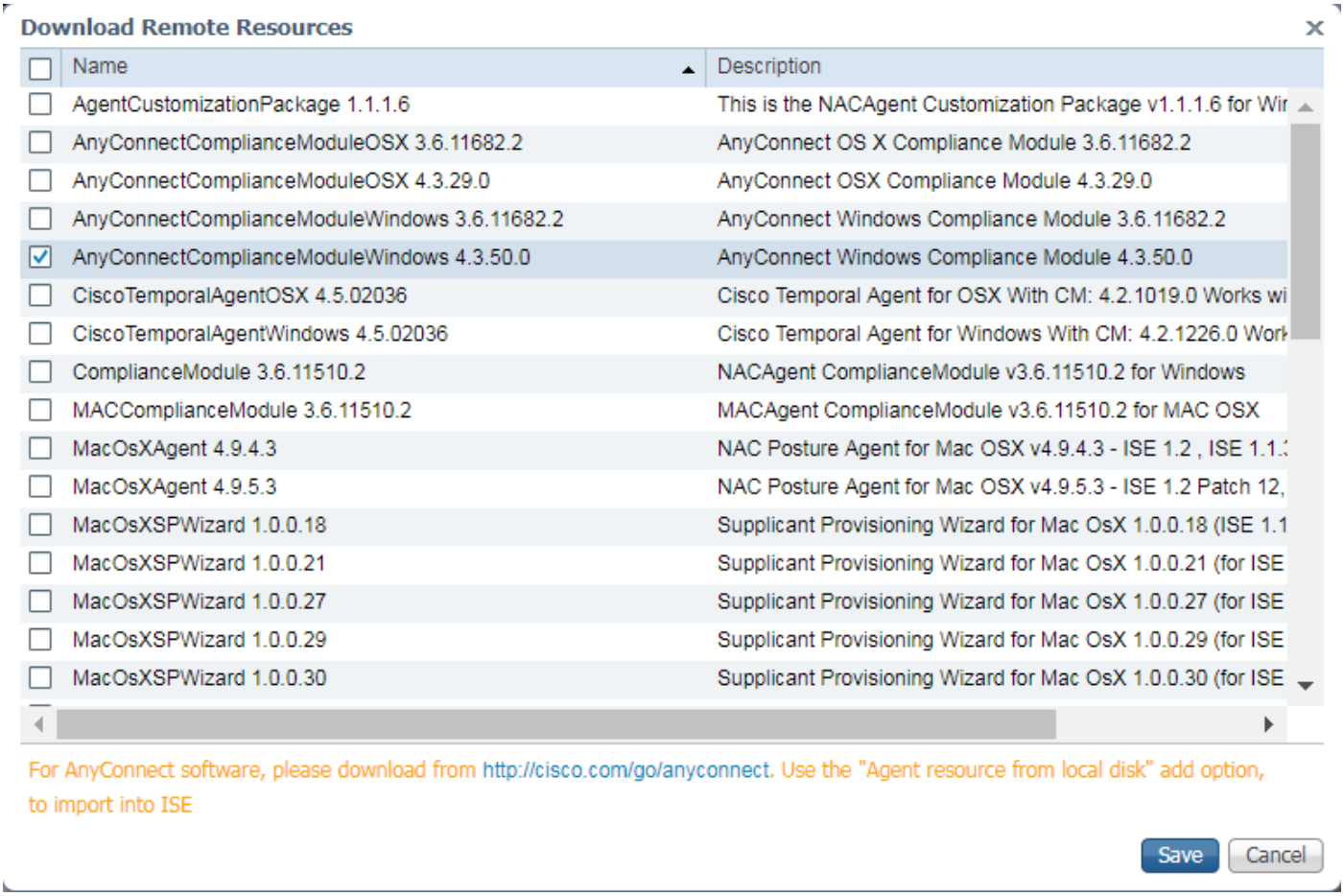
الخطوة 1. تنزيل حزمة AnyConnect. الا تتوفر حزمة AnyConnect نفسها للتنزيل المباشر من ISE، لذلك قبل البدء، تأكد من توفر التيار المتردد على الكمبيوتر الشخصي. يمكن إستخدام هذا الارتباط لتنزيل التيار المتردد - http://cisco.com/go/anyconnect. في هذا المستند يتم إستخدام حزمة AnyConnect-win-4.5.05030-webdeploy-k9.pkg.

الخطوة 2. in order to upload AC حزمة إلى ISE، انتقل إلى **مراكز العمل -> Posture -> Client Provisioning ->** ResourceSand طقطقة **يضيف**. أختر **موارد "الوكيل" من القرص المحلي**. في الإطار الجديد، أختر **حزم Cisco المزودة**، انقر على **إختيار ملف** وحدد حزمة AC على الكمبيوتر الخاص بك.

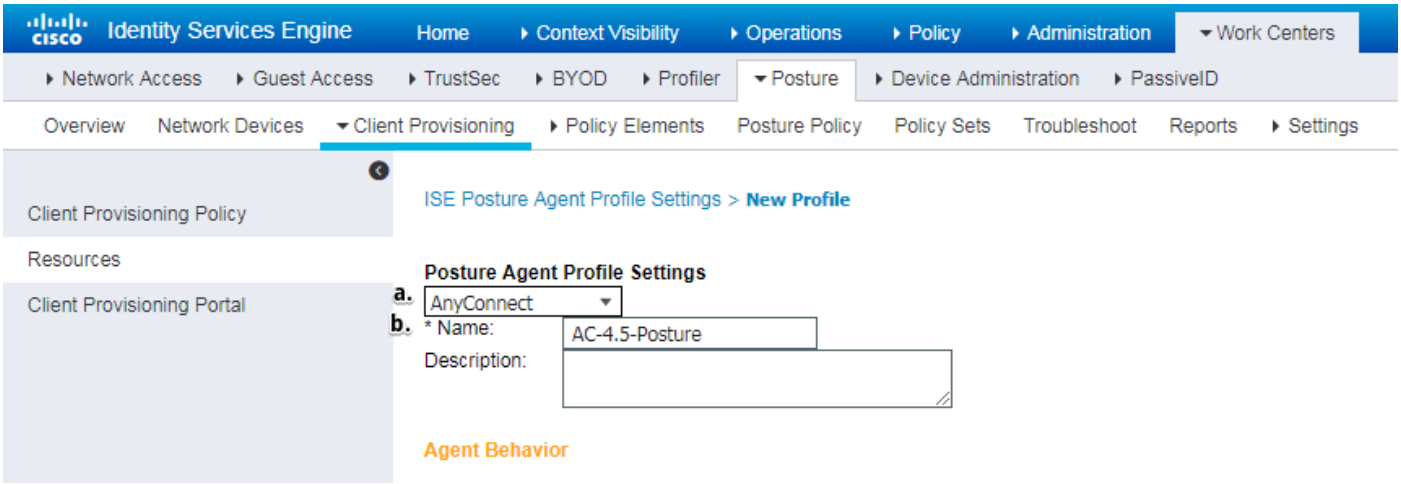


انقر فوق **إرسال** لإنهاء الاستيراد. تحقق من تجزئة الحزمة واضغط على **تأكيد**.

الخطوة 3. يجب تحميل وحدة التوافق النمطية إلى ISE. في نفس الصفحة (**مراكز العمل -> الوضع -> إمداد العميل -> الموارد**) انقر فوق **إضافة** واختر **موارد الوكيل من موقع Cisco**. في قائمة الموارد يجب التحقق من وحدة التوافق النمطية وانقر فوق **حفظ**. لهذا المستند يتم إستخدام وحدة التوافق النمطية AnyConnectComplianceModule بنظام التشغيل Windows 4.3.50.0.



الخطوة 4. يجب إنشاء ملف تعريف AC Posture الآن. انقر على **إضافة** واختر **وكيل NAC** أو **ملف تعريف وضعية AnyConnect**.



- أختر نوع التوصيف. يجب إستخدام AnyConnect لهذا السيناريو.
- حدد اسم ملف التعريف. انتقل إلى قسم **بروتوكول الوضع** في ملف التعريف

Posture Protocol

Parameter	Value	Notes
PRA retransmission time	120 secs	
Discovery host		
* Server name rules	* a.	need to be blank by default to force admin to enter a value. "*" means agent will connect to all
Call Home List	pustyugo-ise23-1.exampl b.	List of IP addresses, FQDNs with or without port must be comma-separated and with colon in between the IP address/FQDN and the port. Example: IPaddress/FQDN:Port (Port number should be the same, specified in the Client Provisioning portal)
Back-off Timer	30 secs	Enter value of back-off timer in seconds, the supported range is between 10s - 600s.

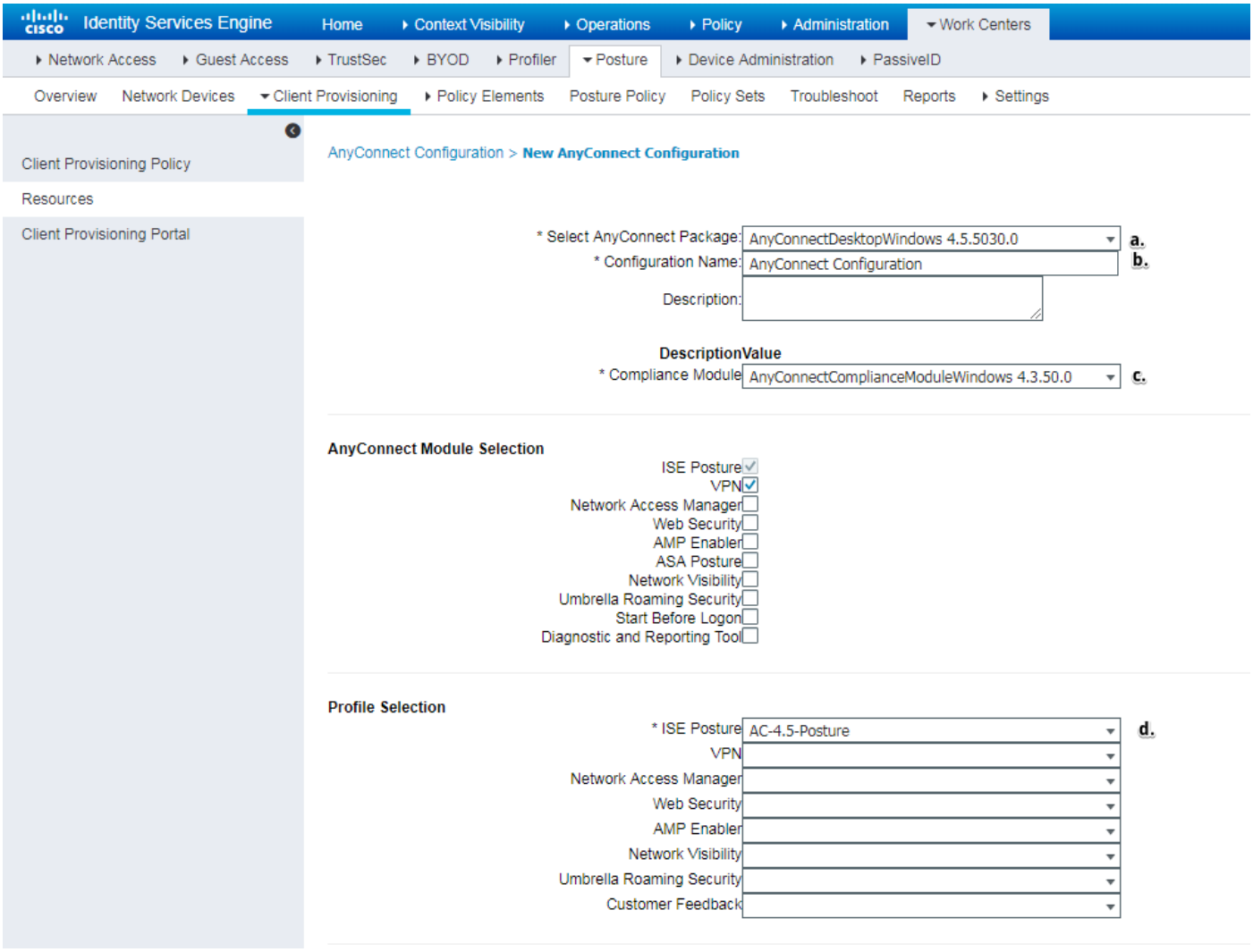
Note: It is recommended that a separate profile be created for Windows and OSX deployments

Submit Cancel

- حدد **قواعد اسم الخادم**، ال يمكن أن يكون هذا الحقل فارغا. يمكن أن يحتوي الحقل على FQDN بحرف البدل الذي يقيد اتصال وحدة وضعية التيار المتردد ب PSNs من مساحة الاسم المناسبة. وضع نجمة إذا كان يجب السماح بأي FQDN.

- الأسماء و IPs المحددة هنا قيد الاستخدام أثناء المرحلة 2 من اكتشاف الوضع (راجع "قسم تدفق الوضع في ISE 2.2" من الخطوة 14). يمكنك إضافة أسماء منفصلة حسب COMA وكذلك رقم المنفذ بعد FQDN/IP باستخدام النقطتين.

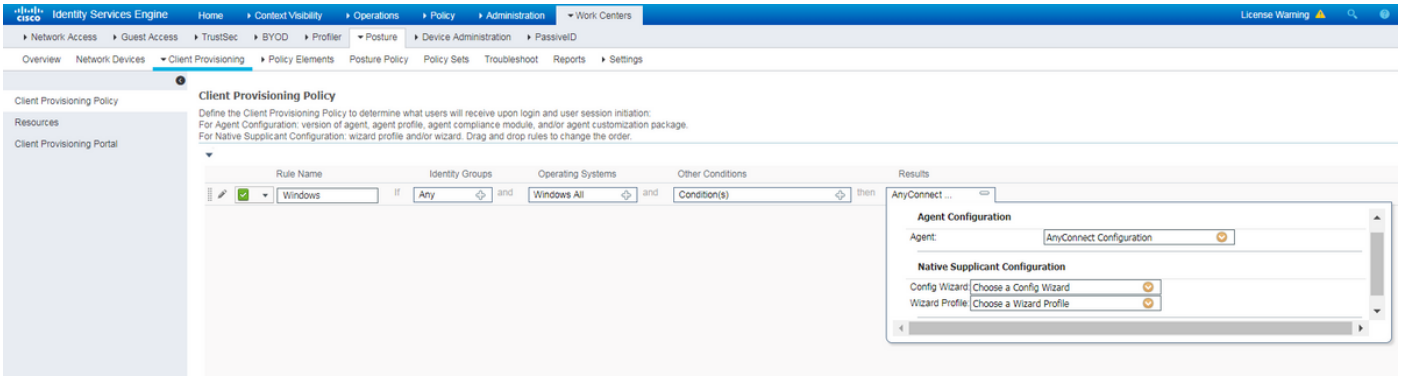
الخطوة 5.قم بإنشاء تكوين AC. انتقل إلى **مراكز العمل -> Posture (وضعية) -> Client Provisioning (تزويد العملاء) -> الموارد** وانقر فوق **إضافة**، ثم حدد **تكوين AnyConnect**.



- حدد حزمة تيار متردد.
- قم بتوفير اسم تكوين التيار المتردد.
- أختر إصدار وحدة التوافق النمطية.
- حدد ملف تعريف تكوين وضعية التيار المتردد من القائمة المنسدلة.

الخطوة 6. تكوين نهج توفير العميل. انتقل إلى **مراكز العمل -> الوضع -> إمداد العميل**. في حالة التكوين الأولي، يمكنك تعبئة القيم الفارغة في النهج المقدم مع الافتراضيات. في حالة الحاجة إلضافة نهج إلى تكوين الوضع الموجود، انتقل إلى النهج الذي يمكن إعادة إستخدامه واختر **تكرار أعلاه** أو **تكرار أدناه**. كما يمكن إنشاء نهج جديد للعملاء التجارية.

هذا مثال على السياسة المستخدمة في المستند.

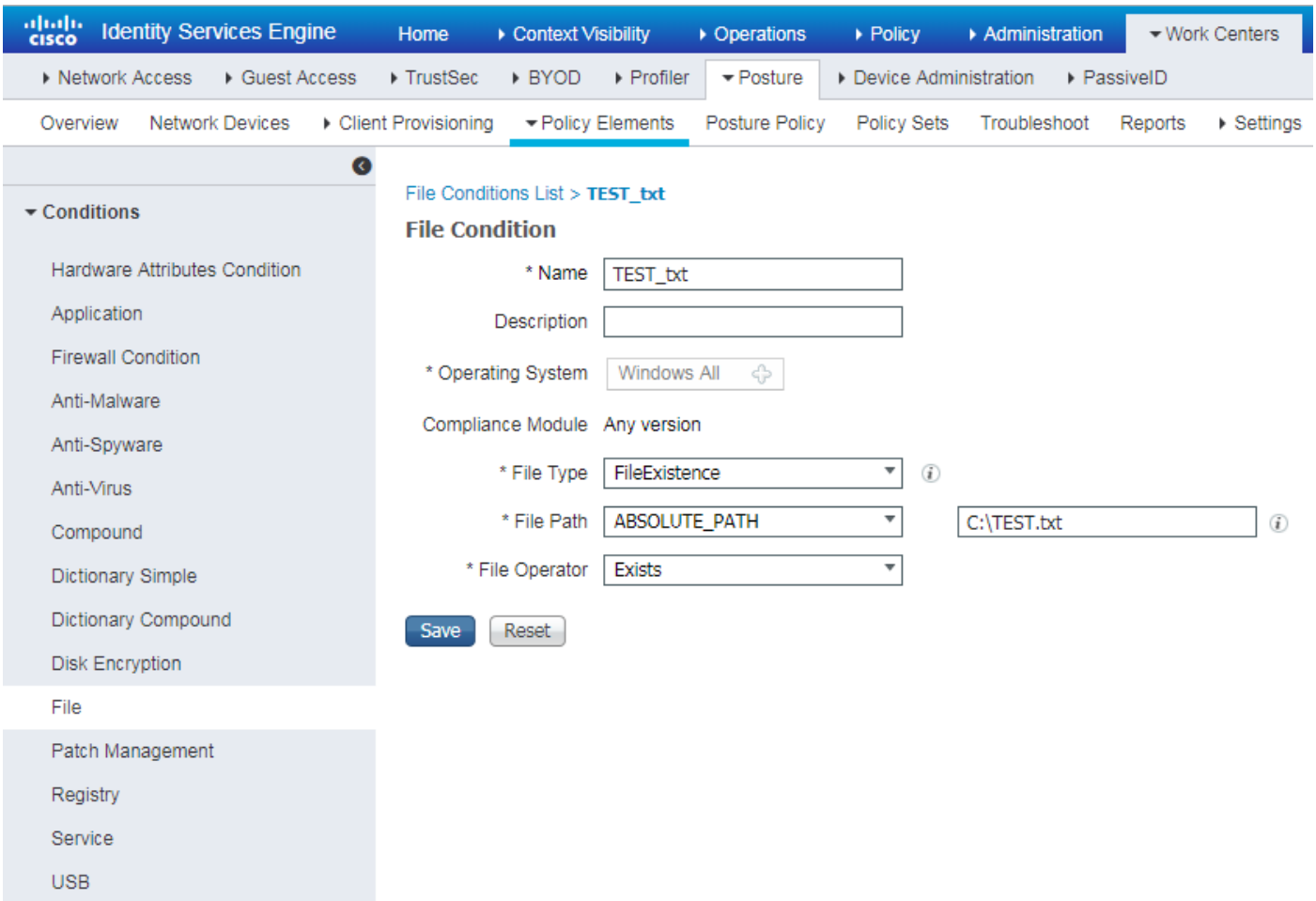


أختر تكوين التيار المتردد في قسم النتائج.

سياسات وشروط الوضع

يتم إستخدام فحص الوضع البسيط. تم تكوين ISE للتحقق من وجود الملف C:\TEST.txt على جانب الجهاز الطرفي. قد تكون سيناريوهات الحياة الواقعية أكثر تعقيدا ولكن خطوات التكوين العام هي نفسها.

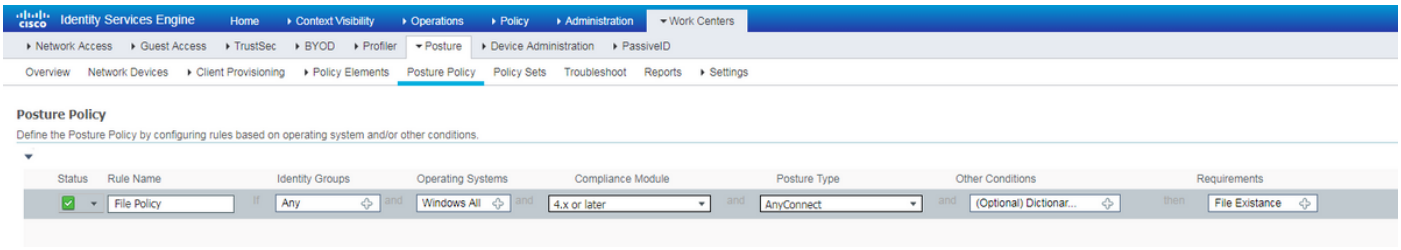
الخطوة 1. قم بإنشاء حالة. توجد شروط الوضع في **مراكز العمل -> الوضع -> عناصر السياسة -> الشروط**. *أختر نوع شرط الوضع* وانقر **إضافة**. حدد المعلومات الضرورية وانقر **حفظ**. أدناه، يمكنك العثور على مثال لشرط الخدمة الذي يجب التحقق من وجود الملف C:\TEST.txt.



خطوة 2.Posture متطلب تشكيل. انتقل إلى **مراكز العمل -> الوضع -> عناصر النهج -> المتطلبات**. هذا مثال على وجود TEST.txt للملف:

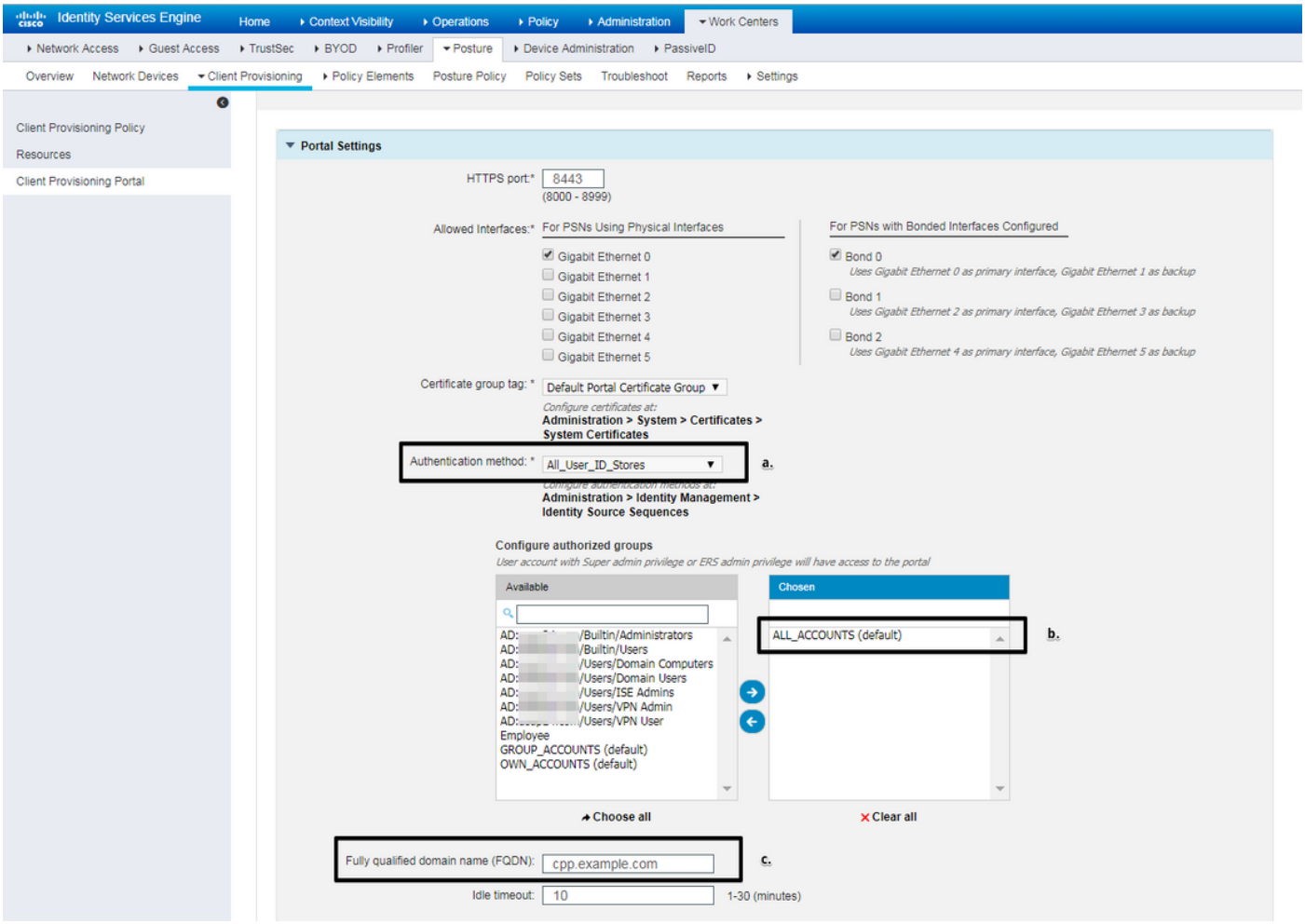
أختر شرط الوضع الخاص بك في متطلب جديد وحدد إجراء إصلاح.

الخطوة 3. تكوين نهج الوضع. انتقل إلى **مراكز العمل -> الوضع -> نهج الوضع**. أدناه يمكنك العثور على مثال للنهج المستخدم لهذا المستند. يحتوي النهج على متطلب "وجود الملف" الذي تم تعيينه كإلزامي ولا يحتوي على أي شروط أخرى تم تعيينها.



تكوين مدخل توفير العميل

بالنسبة للوضع بدون إعادة التوجيه، يجب تحرير تكوين مدخل توفير العميل. انتقل إلى **مراكز العمل -> الوضع -> إمداد العميل ->مدخل إمداد العميل** يمكنك استخدام البوابة الافتراضية أو إنشاء البوابة الخاصة بك.



يجب تحرير هذه الإعدادات في تكوين المدخل لسيناريو عدم إعادة التوجيه:

- في المصادقة، حدد تسلسل مصدر الهوية الذي يجب إستخدامه إذا تعذر على SSO تحديد

موقع جلسة المستخدم.

- وقف القائمة "تسلسل مصدر الهوية" المحددة، يتم علق القائمة المجموعات المتاحة. عند هذه النقطة، تحتاج إلى تحديد المجموعات المعتمدة لتسجيل الدخول إلى المدخل.

- يجب تحديد FQDN لمدخل تزويد العميل. يجب حل FQDN هذا إلى ISE PSNs IPs. يجب توجيه المستخدمين لتحديد FQDN في مستعرض الويب أثناء محاولة الاتصال الأولى.

تكوين توصيفات التخويل والنهج

يلزم تقييد الوصول الأولي للعميل عندما تكون حالة الوضع غير متوفرة. ومن الممكن تحقيق هذه الغاية بطرق متعددة:

- RADIUS Filter-ID - باستخدام هذه السمة، يمكن تعيين قائمة التحكم في الوصول (ACL) المعرفة محليا على NAD للمستخدم الذي لديه حالة وضع غير معروفة. ونظرا لأن هذه سمة قياسية لمحول RFC، فيجب أن يعمل هذا النهج بشكل جيد لجميع موردي NAD.

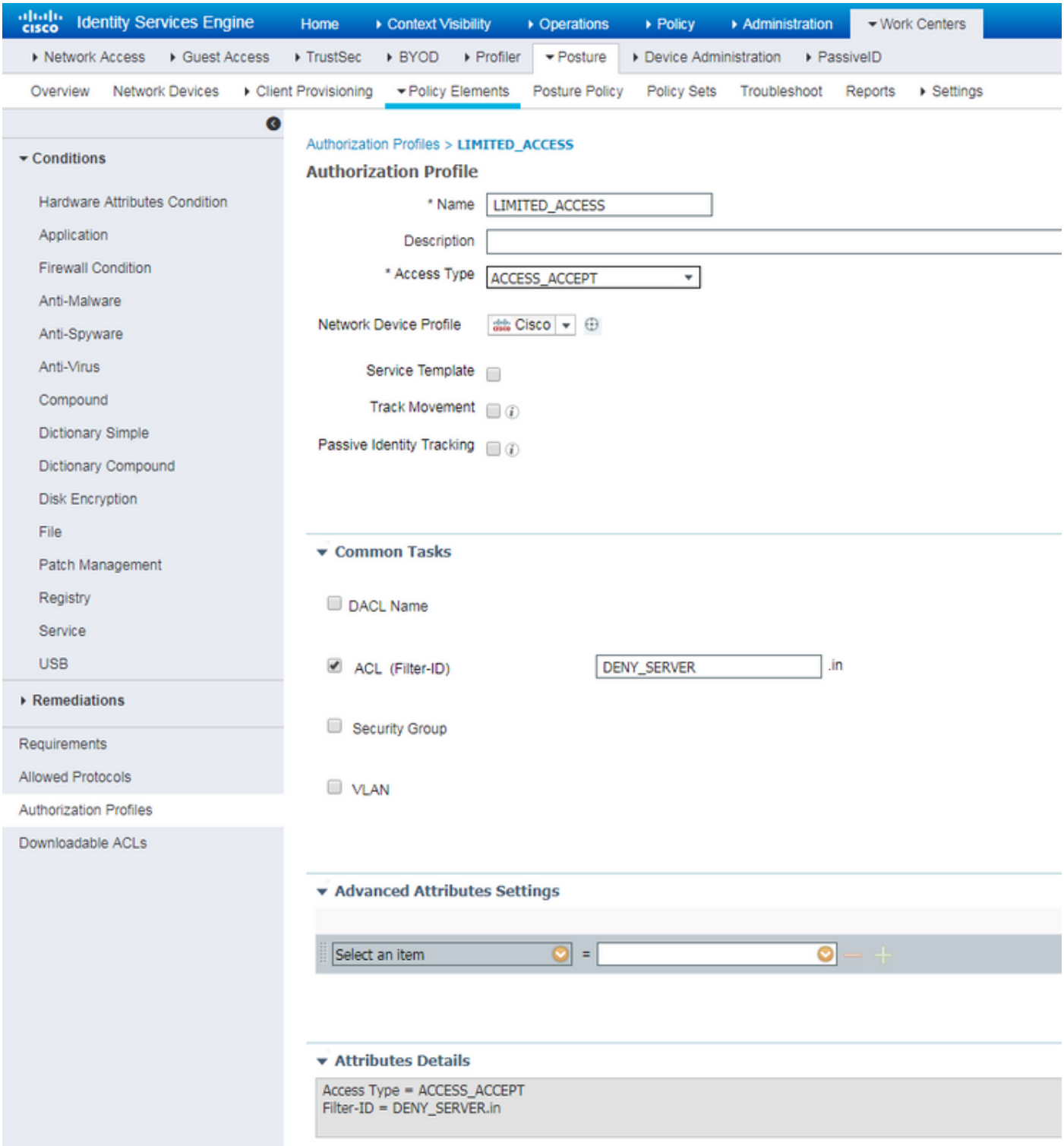
- Cisco:Cisco:AV-pair = ip:interface-config - مماثل جدا ل Radius Filter-ID، يمكن تعيين قائمة التحكم في الوصول (ACL) المعرفة محليا على NAD للمستخدم بحالة الوضع غير المعروف. مثال على التكوين:
  Cisco-av-pair = ip:interface-config=ip access-group deny_server في

الخطوة 1. تكوين ملف تعريف التخويل.

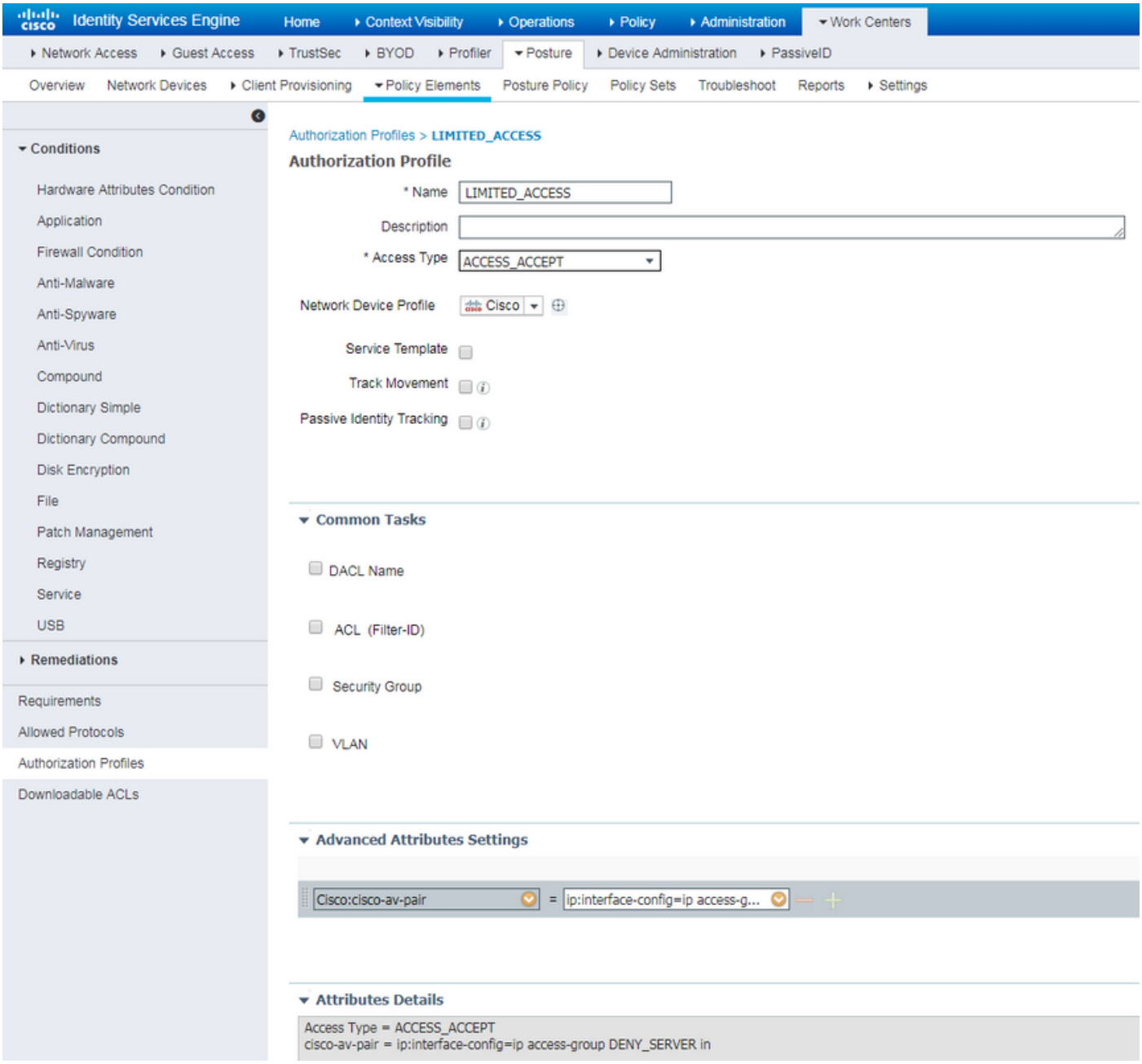
كما هو معتاد بالنسبة للوضع، يلزم وجود توصيف تخويل. يجب أن يحتوي الخيار الأول على أي نوع من أنواع قيود الوصول إلى الشبكة. يمكن تطبيق ملف التعريف هذا على عمليات المصادقة التي تواجه حالة الوضع لها التوافق. قد يحتوي ملف تعريف التخويل الثاني على إمكانيات سماح فقط ويمكن تطبيقه على جلسة عمل بالحالة "وضعية" تواجه التوافق.

لإنشاء ملف تعريف التخويل، انتقل إلى **مراكز العمل -> الوضع -> عناصر النهج -> ملفات تعريف التخويل**.

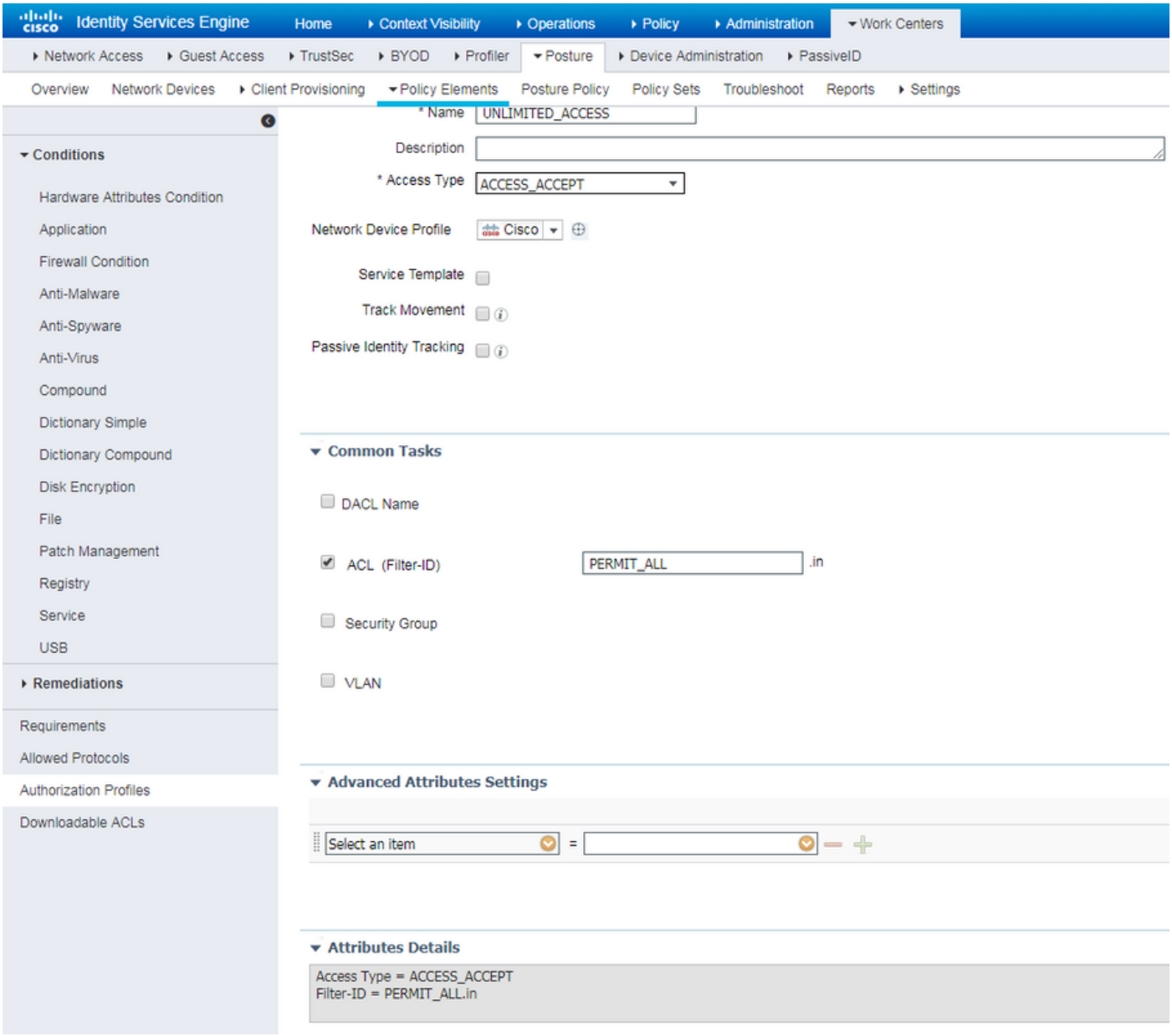
مثال على ملف تعريف الوصول المقيد باستخدام RADIUS Filter-ID:



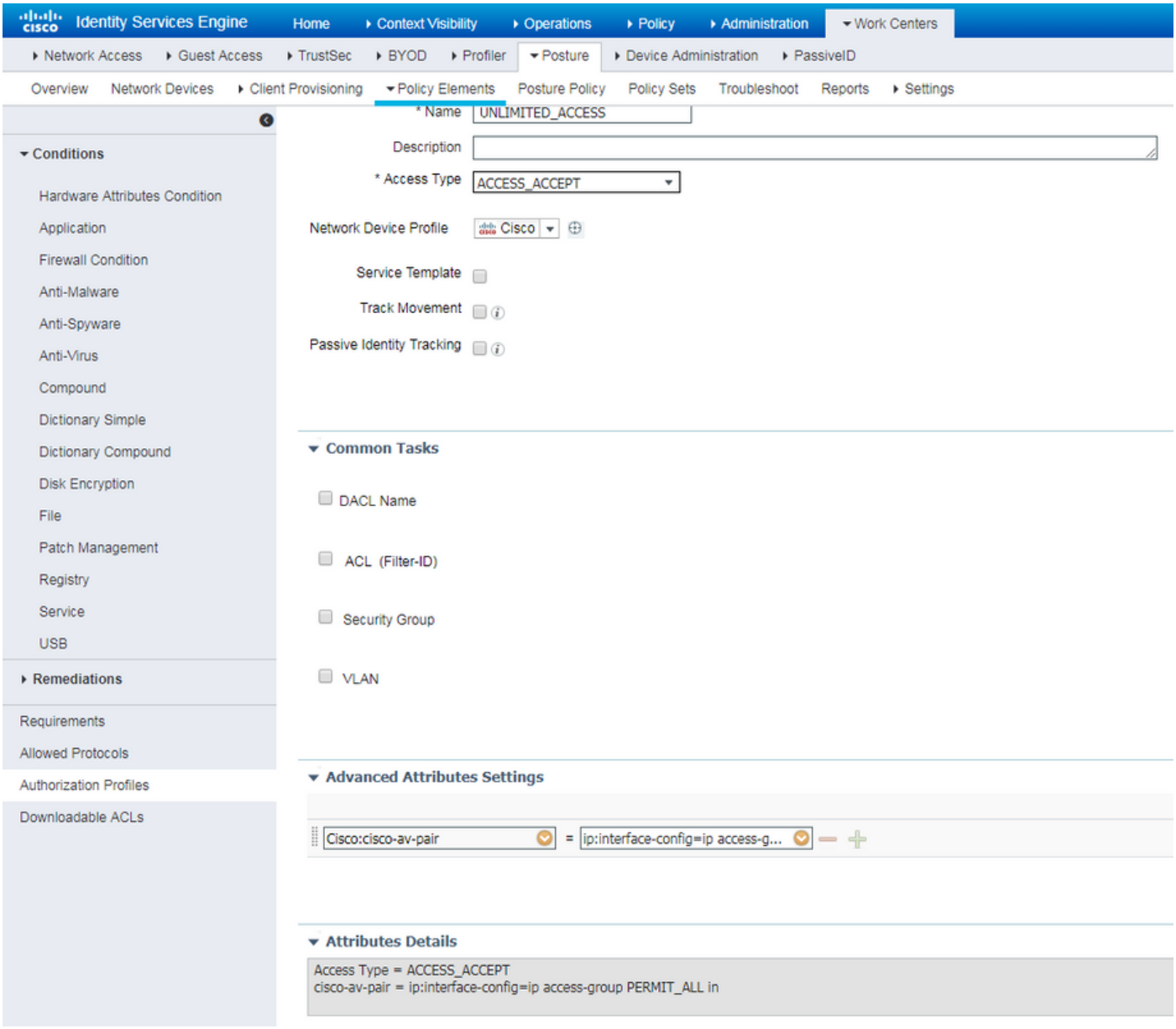
مثال على ملف تعريف الوصول المقيد باستخدام زوج أجهزة Cisco-AV:



مثال على ملف تخصيص الوصول غير المحدود مع معرف عامل تصفية RADIUS:



مثال على ملف تعريف الوصول غير المحدود باستخدام زوج منافذ Cisco-AV:



الخطوة 2. تكوين نمج التخويل. أثناء هذه الخطوة يجب إنشاء نمج تخويل إثنين. الأول لمطابقة طلب المصادقة الأولي مع حالة الوضع غير المعروف والثاني لتعيين الوصول الكامل بعد عملية الوضع الناجح.

إنه مثال على سياسات التخويل البسيطة لهذه الحالة:

تكوين نمج المصادقة ليس جزءا من هذا المستند ولكن يجب أن تضع في الاعتبار أن المصادقة يجب أن تكون ناجحة قبل بدء معالجة نمج التخويل.

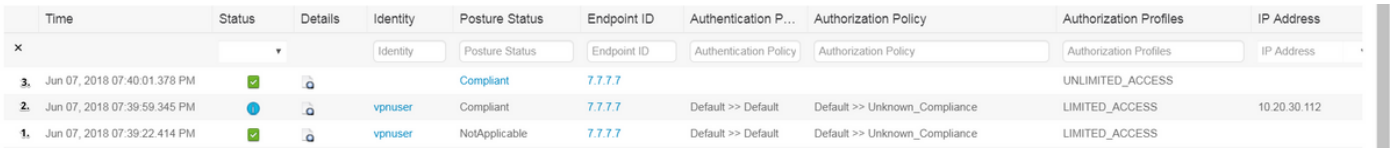
التحقق من الصحة

وقد يتألف التحقق الأساسي من التدفق من ثلاث خطوات رئيسية:

الخطوة 1. التحقق من جلسة عمل RA VPN على لوحة وصل FlexVPN:

```
show crypto session username vpnuser detail
Crypto session current status

Code: C - IKE Configuration mode, D - Dead Peer Detection
K - Keepalives, N - NAT-traversal, T - cTCP encapsulation
X - IKE Extended Authentication, F - IKE Fragmentation
R - IKE Auto Reconnect, U - IKE Dynamic Route Update

Interface: Virtual-Access1
Profile: FlexVPN-IKEv2-Profile-1
Uptime: 00:04:40
Session status: UP-ACTIVE
Peer: 7.7.7.7 port 60644 fvrf: (none) ivrf: (none)
     Phase1_id: example.com
     Desc: (none)
 Session ID: 20
 IKEv2 SA: local 5.5.5.5/4500 remote 7.7.7.7/60644 Active
         Capabilities:DNX connid:1 lifetime:23:55:20
 IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 host 10.20.30.107
       Active SAs: 2, origin: crypto map
       Inbound:  #pkts dec'ed 499 drop 0 life (KB/Sec) 4607933/3320
       Outbound: #pkts enc'ed 185 drop 0 life (KB/Sec) 4607945/3320

show crypto ikev2 sa detail
 IPv4 Crypto IKEv2  SA

Tunnel-id Local                 Remote                fvrf/ivrf            Status
1         5.5.5.5/4500          7.7.7.7/60644         none/none            READY
     Encr: AES-CBC, keysize: 256, PRF: SHA512, Hash: SHA512, DH Grp:5, Auth sign: RSA, Auth
verify: EAP
     Life/Active Time: 86400/393 sec
     CE id: 1010, Session-id: 8
     Status Description: Negotiation done
     Local spi: 54EC006180B502D8       Remote spi: C3B92D79A86B0DF8
     Local id: cn=flexvpn-hub.example.com
     Remote id: example.com
     Remote EAP id: vpnuser
     Local req msg id:  0              Remote req msg id:  19
     Local next msg id: 0              Remote next msg id: 19
     Local req queued:  0              Remote req queued:  19
     Local window:      5              Remote window:      1
     DPD configured for 60 seconds, retry 2
     Fragmentation not  configured.
     Dynamic Route Update: disabled
     Extended Authentication configured.
     NAT-T is detected  outside
     Cisco Trust Security SGT is disabled
     Assigned host addr: 10.20.30.107
     Initiator of SA : No

 IPv6 Crypto IKEv2  SA
```

الخطوة 2. التحقق من تدفق المصادقة (سجلات RADIUS المباشرة):



Time	Status	Details	Identity	Posture Status	Endpoint ID	Authentication P...	Authorization Policy	Authorization Profiles	IP Address
			Identity	Posture Status	Endpoint ID	Authentication Policy	Authorization Policy	Authorization Profiles	IP Address
3. Jun 07, 2018 07:40:01.378 PM	✓			Compliant	7.7.7.7			UNLIMITED_ACCESS	
2. Jun 07, 2018 07:39:59.345 PM	●		vpnuser	Compliant	7.7.7.7	Default >> Default	Default >> Unknown_Compliance	LIMITED_ACCESS	10.20.30.112
1. Jun 07, 2018 07:39:22.414 PM	✓		vpnuser	NotApplicable	7.7.7.7	Default >> Default	Default >> Unknown_Compliance	LIMITED_ACCESS	

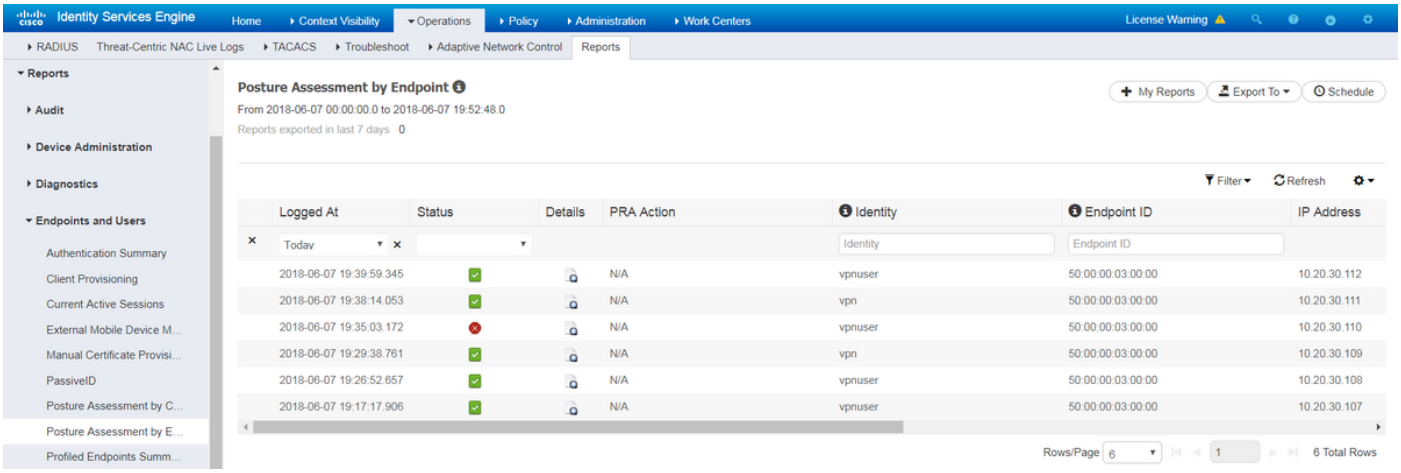
1. المصادقة الأولية. بالنسبة لهذه الخطوة، قد تكون مهتما بالتحقق من ملف تعريف التخويل الذي تم تطبيقه. في حالة تطبيق ملف تعريف تخويل غير متوقع، يرجى التحقق من تقرير المصادقة التفصيلي. يمكنك فتح هذا التقرير بالنقر فوق "تكبير الزجاج" في عمود "تفاصيل". يمكنك مقارنة السمات في تقرير المصادقة التفصيلي مع الشرط في نهج التخويل الذي توقع مطابقته.

2. تغيير بيانات جلسة العمل، في هذا المثال المعين تغيرت حالة جلسة العمل من NotApplicable إلى Compliant.

3. COA إلى جهاز الوصول إلى الشبكة. يجب أن تكون عملية COA هذه ناجحة لدفع المصادقة الجديدة من جانب NAD وتعيين سياسة تخويل جديدة من جانب ISE. في حالة فشل COA، يمكنك فتح تقرير مفصل للتحقق من السبب. يمكن أن تكون أكثر القضايا شيوعا للكاكاو هي: مهلة COA - في هذه الحالة إما أن PSN الذي قام بإرسال الطلب لم يتم تكوينه كعميل COA على جانب NAD، أو تم إسقاط طلب COA في مكان ما على الطريق.ACK السالب للكاكاو - يشير إلى أن الكاكاو قد تم إستلامه من قبل NAD ولكن لسبب ما ال يمكن تأكيد عملية الكاكاو. وينبغي أن يتضمن التقرير المفصل لهذا السيناريو تفسيرا أكثر تفصيلا.

نظرا لاستخدام الموجه المستند إلى IOS XE كموجه NAD على هذا المثال، ال يمكنك مشاهدة أي طلب مصادقة الحق للمستخدم. وهذا يحدث نظرا لأن ISE يستخدم ميزة الدفع بالنقل لنظام التشغيل COA لنظام التشغيل IOS XE الذي يجنب تشغيل خدمة VPN. وفي هذا السيناريو، يحتوي COA نفسه على معلمات تخويل جديدة، لذلك ال تكون هناك حاجة إلى إعادة المصادقة.

الخطوة 3.Posture report verify - انتقل إلى **Operations -> Reports -> Reports -> Endpoint and Users -> Posture Assessment by Endpoint**.



يمكنك فتح تقرير مفصل من هنا لكل حدث معين للتحقق على سبيل المثال من معرف جلسة العمل الذي ينتمي إليه هذا التقرير، أي متطلبات الوضع المحددة تم تحديدها من قبل ISE لنقطة النهاية وكذلك حالة كل متطلب.

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك إستخدامها لاستكشاف أخطاء التكوين وإصلاحها.

1. تصحيح أخطاء IKEv2 للتجميع من وحدة الاستقبال والبث:

```
debug crypto ikev2
debug crypto ikev2 packet
debug crypto ikev2 internal
debug crypto ikev2 error
```

2. تصحيح أخطاء المصادقة والتفويض والمحاسبة (AAA) للاطلاع على تعيين السمات المحلية و/أو البعيدة:

```
debug aaa authorization
debug aaa authentication
debug aaa accounting
debug aaa coa
debug radius authentication
debug radius accounting
```

3. DART من عميل AnyConnect.
4. لاستكشاف أخطاء عملية الوضع وإصلاحها، يجب تمكين مكونات ISE هذه في تصحيح الأخطاء على عقد ISE حيث يمكن أن تحدث عملية الوضع:**client-webApp** - المكون المسؤول عن توفير الوكيل. ملفات السجل الهدف **guest.log** و**ise-psc.log**.**Guestess** - المكون المسؤول عن مكون خدمة تزويد العميل والبحث عن مالك الجلسة (عندما يأتي الطلب إلى PSN خاطئ). ملف السجل الهدف - **guest.log**.**الإمداد - المكون المسؤول عن معالجة سياسة توفير العميل. ملف السجل الهدف - guest.log.Posture (وضعية)** - جميع الأحداث المتعلقة بالأوضاع. ملف السجل الهدف - **ise-psc.log**
5. لاستكشاف أخطاء جانب العميل وإصلاحها، يمكنك إستخدام:**AnyConnect.txt** - يمكن العثور على هذا الملف في حزمة DART واستخدامه لاستكشاف أخطاء VPN هذا، يتم إنشاء العميل، على جانب العميل توفير لشف حالة في-**acisensa.log**.وإصلاحها NSA إليه (دليل التنزيلات ل Windows المجلد الذي تم تنزيل في نفس الملف عادة)،**AnyConnect_ISEPosture.txt** - يمكن العثور على هذا الملف في حزمة DART في **الوحدة النمطية Cisco AnyConnect ISE Posture Module**. يتم تسجيل جميع المعلومات حول اكتشاف ISE PSN والخطوات العامة لتدفق الوضع في هذا الملف.

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).