تكوين TACACS+ عبر TLS 1.3 على جهاز IOS XR باستخدام ISE

المحتويات

المقدمة

يصف هذا المستند مثال ل TACACS+ عبر TLS مع Cisco Identity Services Engine (ISE) كخادم وجهاز Cisco IOS® XR كعميل.

نظرة عامة

يتيح بروتوكول نظام مراقبة الدخول إلى وحدة تحكم الوصول إلى المحطة الطرفية (TACACS+) [RFC8907] إمكانية الإدارة المركزية للجهاز للموجهات وخوادم الوصول إلى الشبكة والأجهزة الأخرى المتصلة بالشبكة من خلال خادم TACACS+ واحد أو أكثر. وهو يوفر خدمات المصادقة والتفويض والمحاسبة (AAA)، المصممة خصيصا لحالات إستخدام إدارة الأجهزة.

يعمل TACACS+ عبر TLS 1.3 [RFC8446] على تحسين البروتوكول من خلال إدخال طبقة نقل آمنة، مما يعمل على حماية البيانات شديدة الحساسية. يضمن هذا التكامل السرية والنزاهة والمصادقة للاتصال وحركة مرور الشبكة بين عملاء TACACS+ والخوادم.

إستخدام هذا الدليل

يقسم هذا الدليل الأنشطة إلى جزئين لتمكين ISE من إدارة الوصول الإداري لأجهزة الشبكة المستندة إلى Cisco IOS XR.
· الجزء 1 - تكوين ISE لمسؤول الجهاز
· الجزء 2 - تكوين Cisco IOS XR لـ TACACS+ عبر TLS

المتطلبات الأساسية

المتطلبات

متطلبات تكوين TACACS+ عبر TLS:

- مرجع مصدق (CA) لتوقيع الشهادة المستخدمة من قبل TACACS+ عبر TLS لتوقيع شهادات ISE وأجهزة الشبكة.
- الشهادة الجذر من جهة منح الشهادة (CA).
- تحتوي أجهزة الشبكة و ISE على إمكانية الوصول إلى DNS ويمكنها حل أسماء المضيف.

المكونات المستخدمة

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

- الجهاز الظاهري ISE VMware، الإصدار 3.4 Patch 2
- الموجه Cisco 8201، الإصدار 25.3.1

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.

الترخيص

يسمح كل ترخيص إدارة الأجهزة باستخدام خدمات TACACS+ على عقدة خدمة السياسة. في عملية نشر مستقلة (HA) عالية التوفر، يسمح كل ترخيص إدارة الأجهزة باستخدام خدمات

TACACS+ على عقدة خدمة سياسة واحدة في زوج HA.

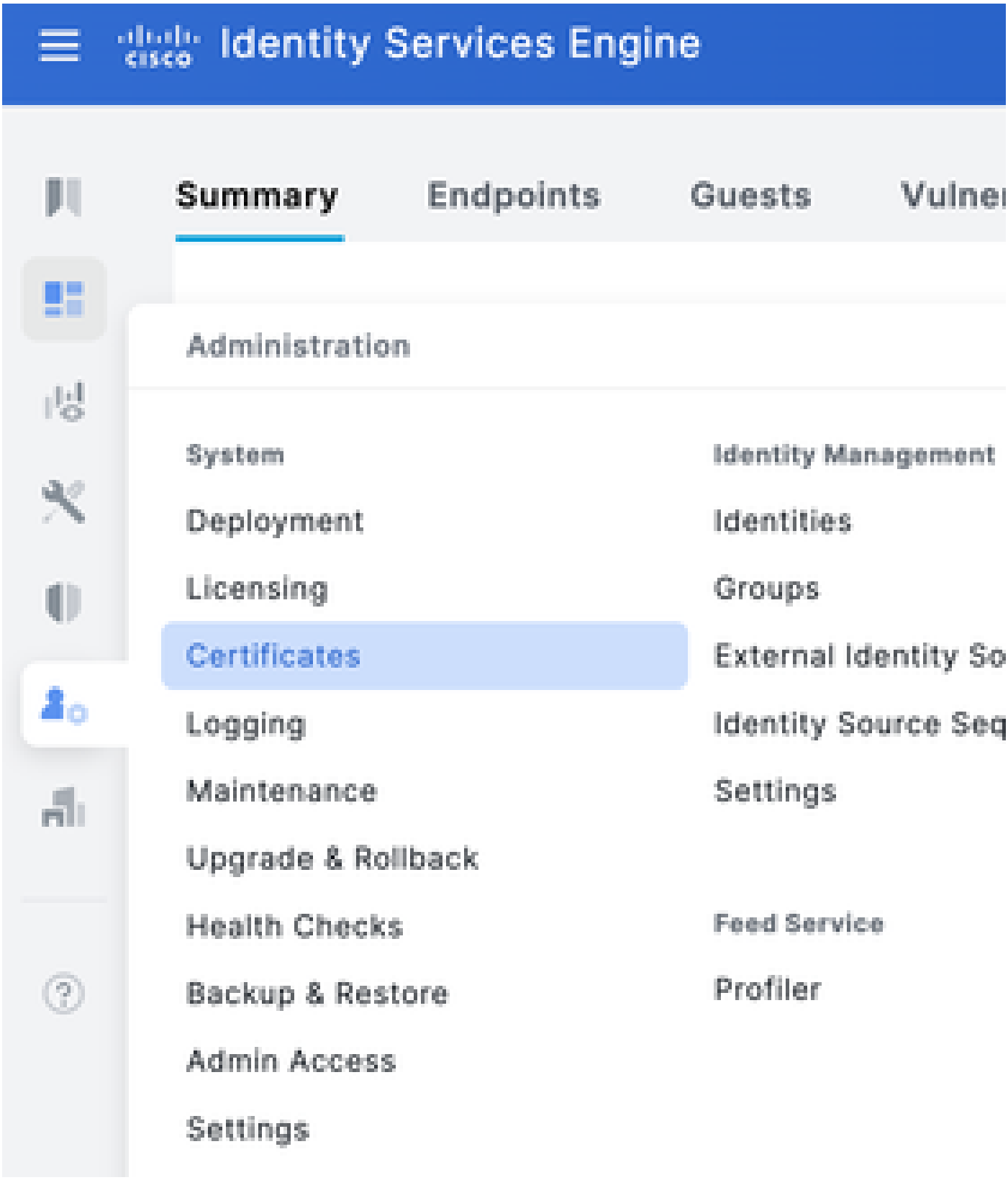
الجزء 1 - تكوين ISE لإدارة الأجهزة

إنشاء طلب توقيع الشهادة لمصادقة خادم TACACS+

الخطوة 1. سجل الدخول إلى بوابة إدارة ISE على الويب باستخدام أحد المستعرضات المدعومة.

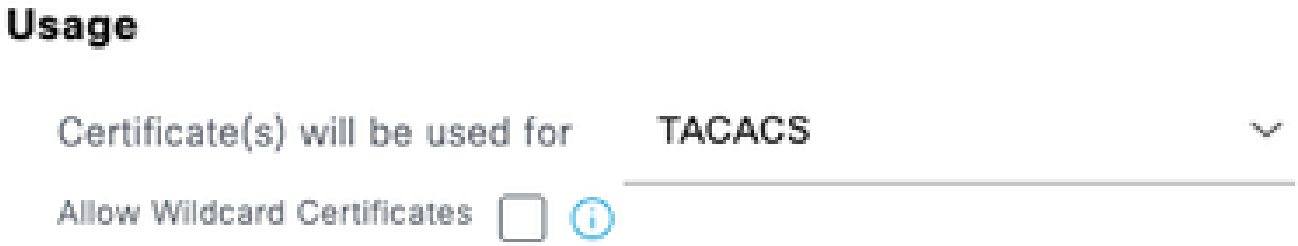
وبشكل افتراضي، يستخدم ISE شهادة موقعة ذاتيا لجميع الخدمات. تتمثل الخطوة الأولى في إنشاء طلب توقيع شهادة (CSR) لتوقيعه من قبل المرجع المصدق (CA).

الخطوة 2. انتقل إلى الإدارة > النظام > الشهادات.

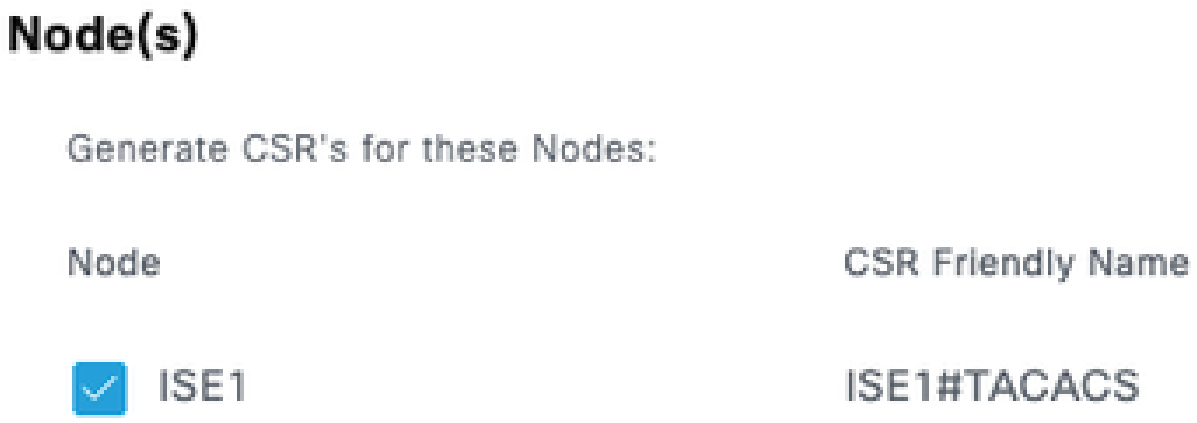


الخطوة 3. تحت طلبات توقيع الشهادة، انقر إنشاء طلب توقيع الشهادة. 

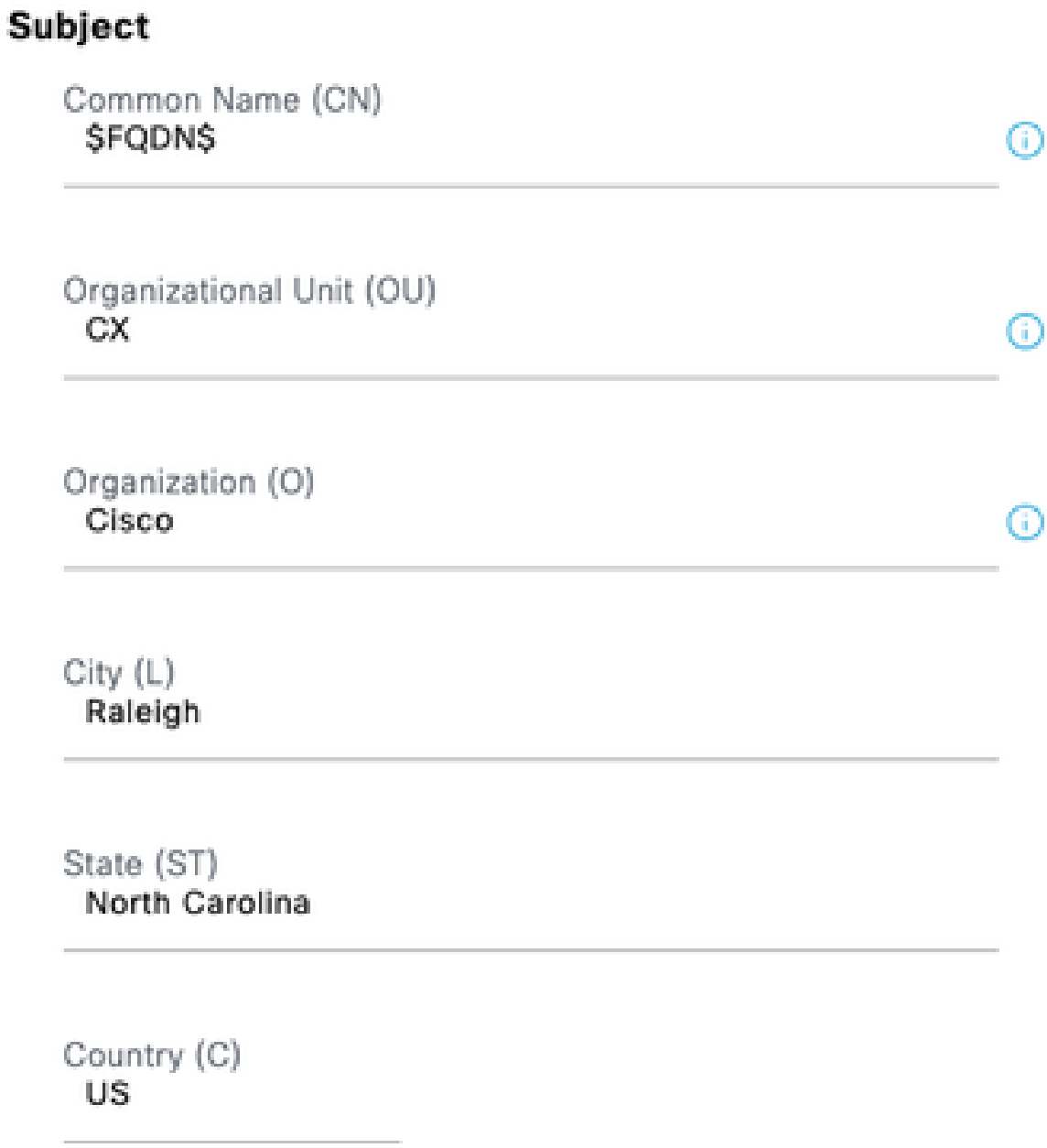
الخطوة 4. حدد TACACS قيد الاستخدام.



الخطوة 5. حدد شبكات PSN التي تم تمكين TACACS+ لها.

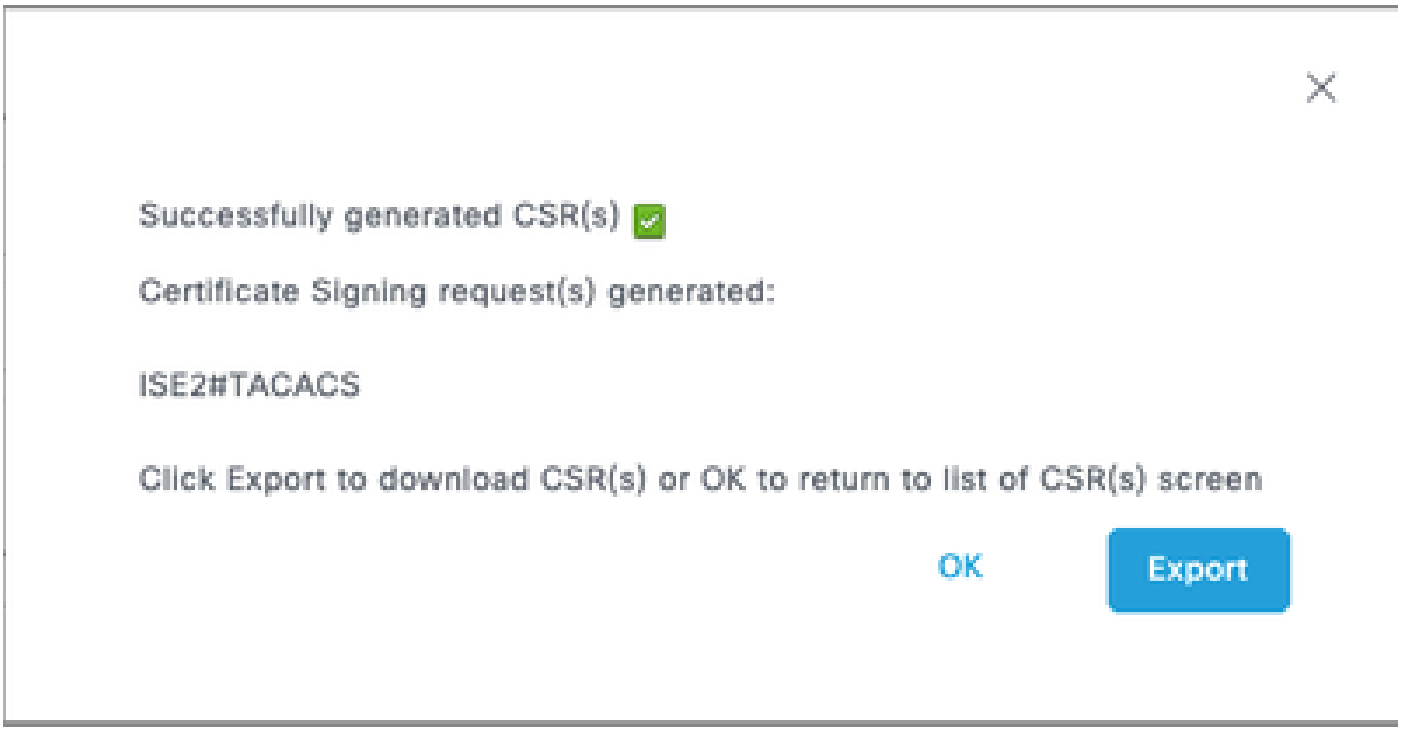


الخطوة 6. املأ حقول الموضوع بالمعلومات المناسبة.



الخطوة 7. أضف اسم DNS وعنوان IP تحت الموضوع اسم بديل (SAN).

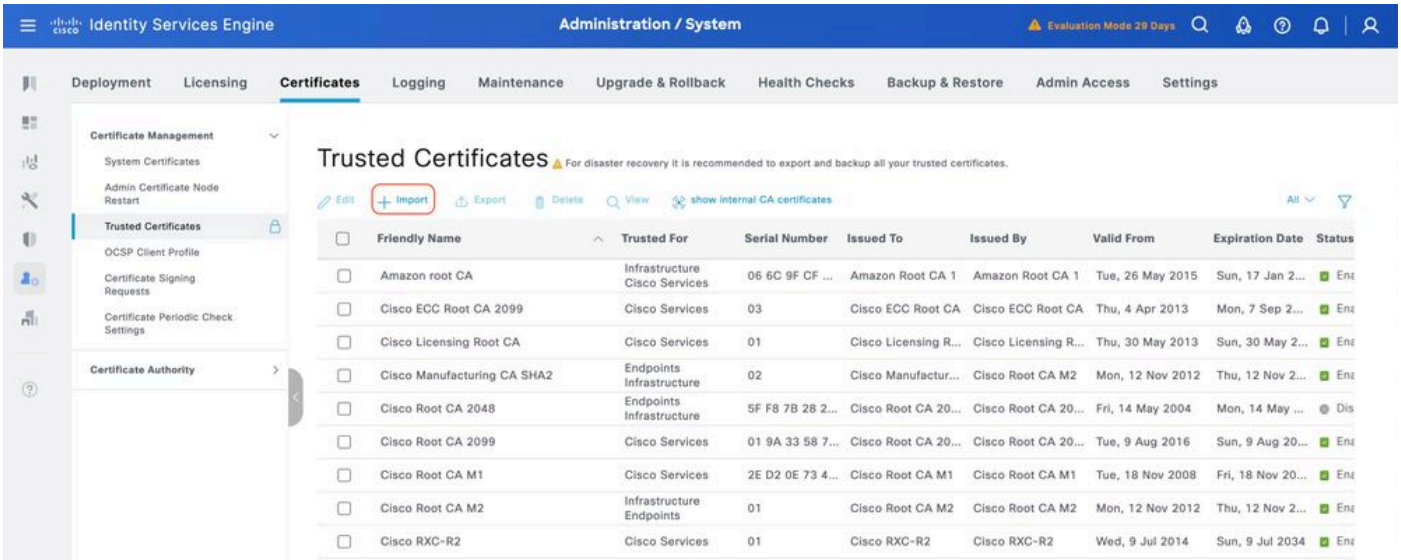
الخطوة 8. انقر فوق إنشاء ثم فوق التصدير.



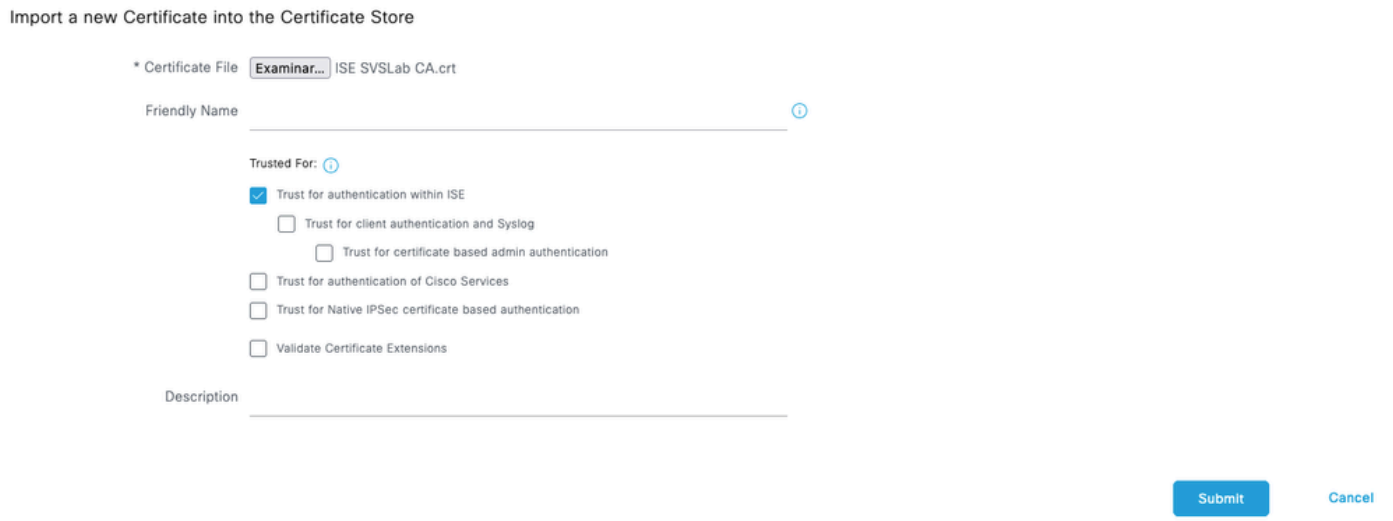
الآن، يمكنك الحصول على الشهادة (CRT) موقعة من المرجع المصدق (CA).

تحميل شهادة المرجع المصدق الجذر لمصادقة خادم TACACS+

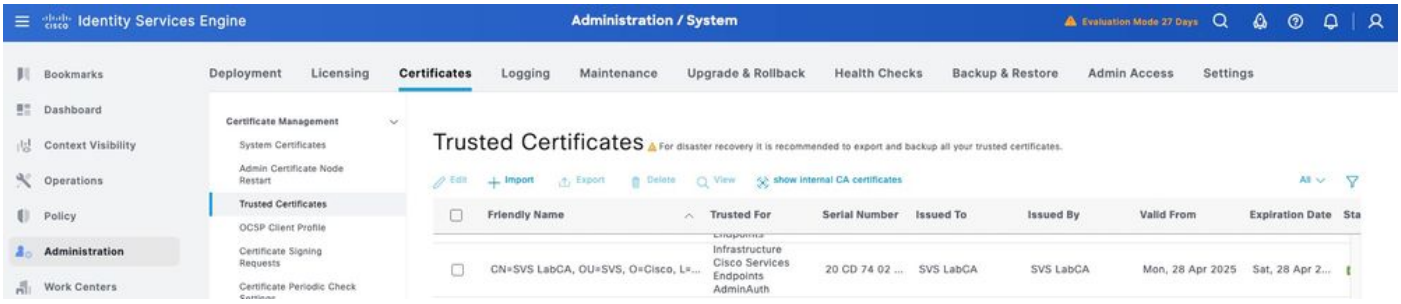
الخطوة 1.انتقل إلى الإدارة > النظام > الشهادات. تحت التراخيص المضمونة، انقر إدراج.



الخطوة 2. حدد الشهادة الصادرة عن المرجع المصدق (CA) الذي وقع طلب توقيع شهادة TACACS (CSR) الخاص بك. تأكد من أن الثقة بالمصادقة داخل ISE الخيار ممكن.



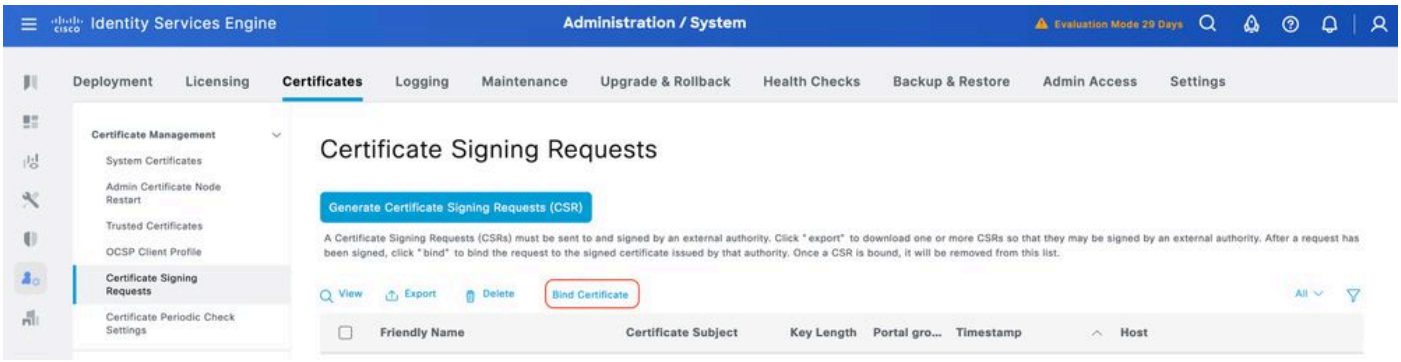
انقر فوق إرسال. يجب أن تظهر الشهادة الآن تحت شهادات موثوق بها.



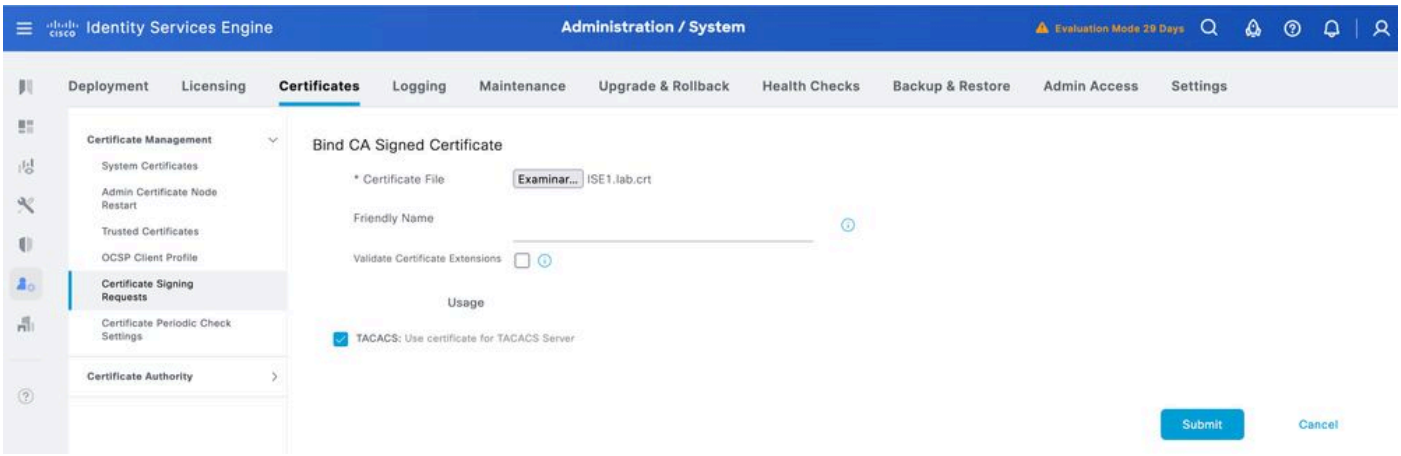
ربط طلب توقيع الشهادة الموقع (CSR) ب ISE

بمجرد توقيع طلب توقيع الشهادة (CSR)، يمكنك تثبيت الشهادة الموقعة على ISE.

الخطوة 1.انتقل إلى الإدارة > النظام > الشهادات. تحت طلبات توقيع الشهادة، حدد TACACS CSR الذي تم إنشاؤه في الخطوة السابقة وانقر فوق ربط الشهادة.

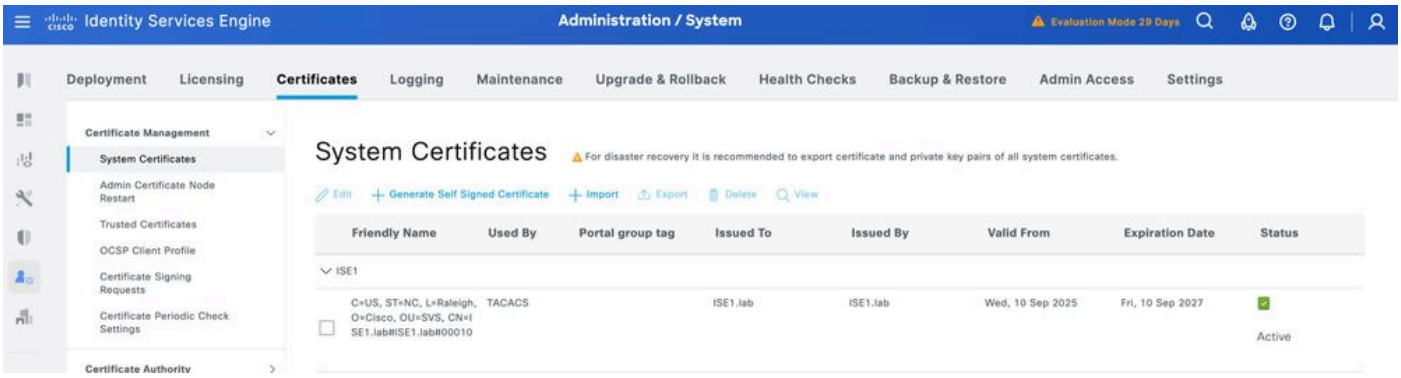


الخطوة 2.حدد الشهادة الموقعة وتأكد من أن خانة الاختيار TACACS الموجودة تحت الاستخدام لا تزال محددة.



الخطوة 3. انقر فوق إرسال. إذا تلقيت تحذيرا حول إستبدال الشهادة الموجودة، انقر فوق نعم للمتابعة.

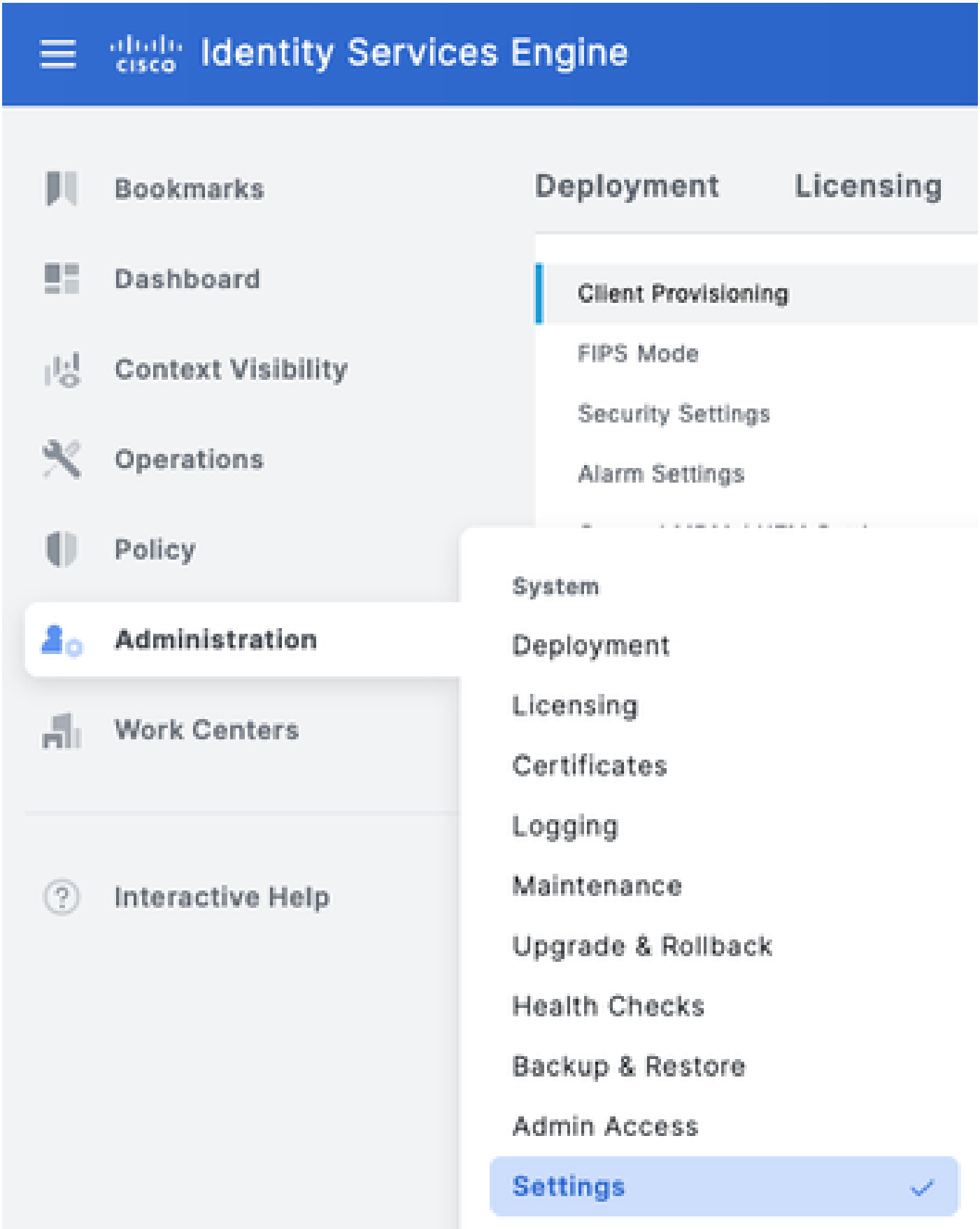
يجب تثبيت الشهادة الآن بشكل صحيح. يمكنك التحقق من ذلك ضمن شهادات النظام.



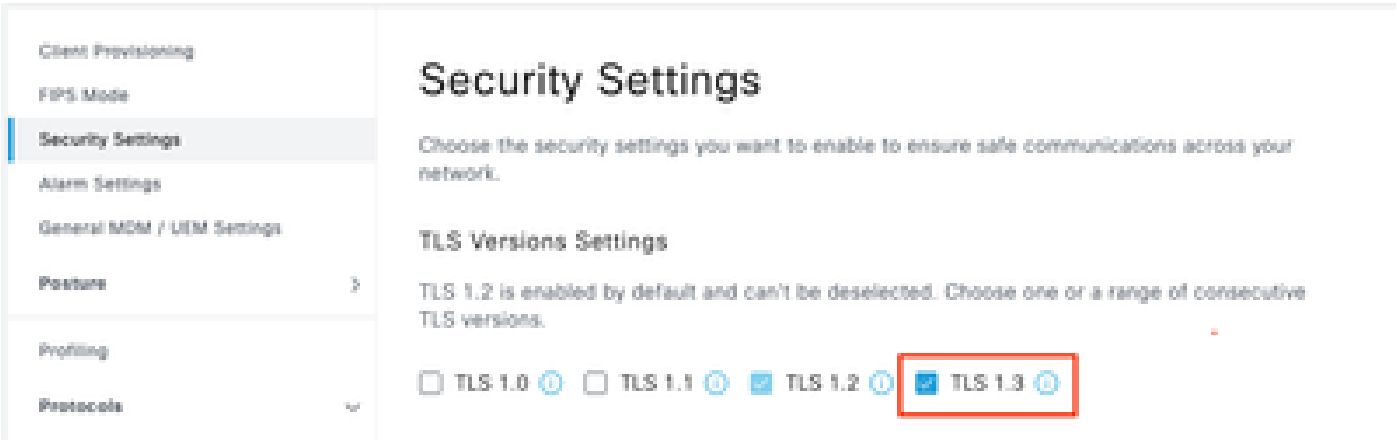
تمكين TLS 1.3

ال يتم تمكين TLS 1.3 بشكل افتراضي في ISE 3.4.x. ويجب تمكينه يدويا.

الخطوة 1.انتقل إلى الإدارة > النظام > الإعدادات.



الخطوة 2. انقر فوق إعدادات الأمان، وحدد خانة الاختيار المجاورة ل TLS1.3 ضمن إعدادات إصدار TLS، ثم انقر فوق حفظ.

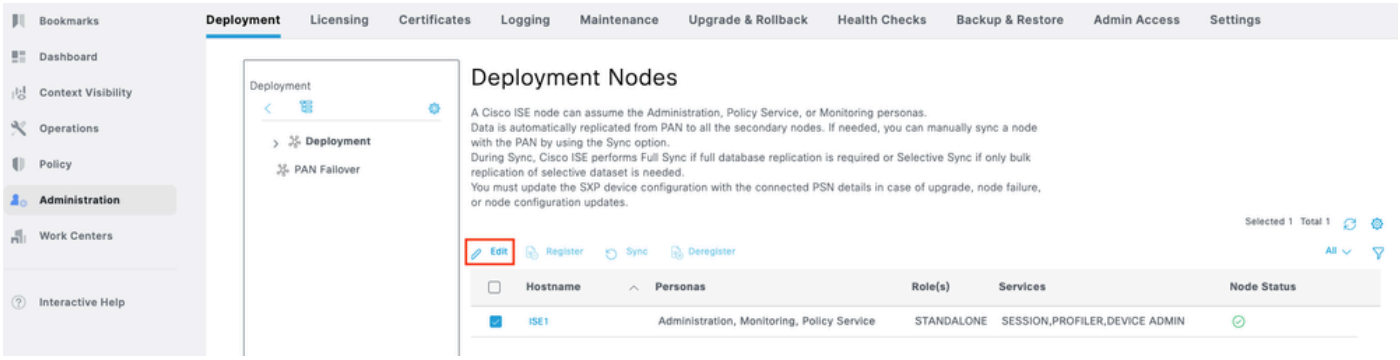


تحذير: عند تغيير إصدار TLS، تتم إعادة تشغيل خادم تطبيق Cisco ISE على جميع أجهزة النشر Cisco ISE.

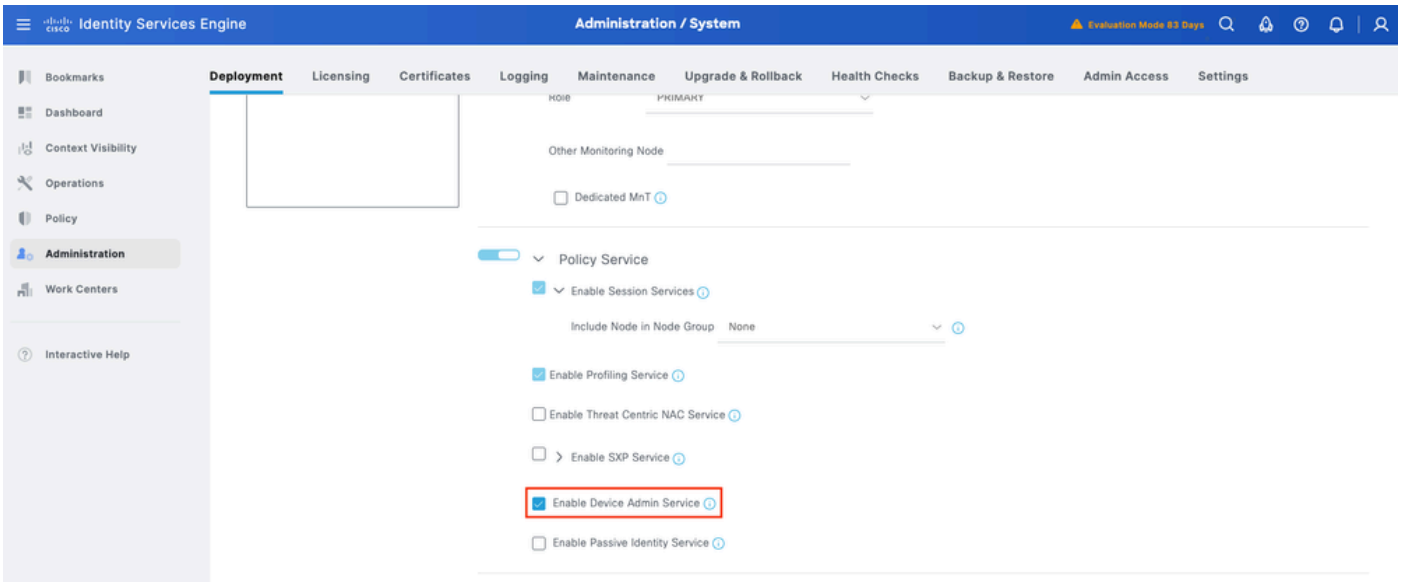
تمكين إدارة الأجهزة على ISE

ال يتم تمكين خدمة إدارة الأجهزة (TACACS+) بشكل افتراضي على عقدة ISE. لتمكين TACACS+ على عقدة PSN:

الخطوة 1. انتقل إلى الإدارة > النظام > النشر. حدد خانة الاختيار المجاورة لعقدة ISE وانقر فوق تحرير.



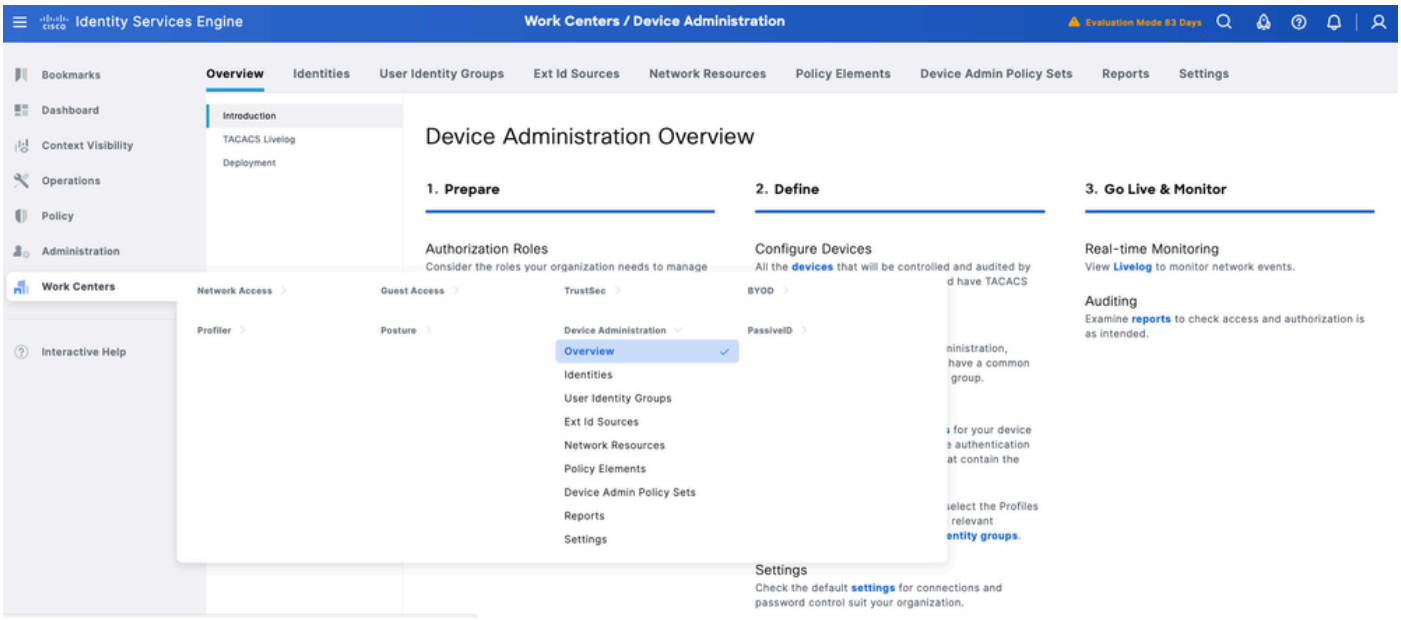
الخطوة 2.تحت GeneralSettings، قم بالتمرير إلى أسفل وحدد خانة الاختيار المجاورة لتمكين خدمة إدارة الأجهزة.



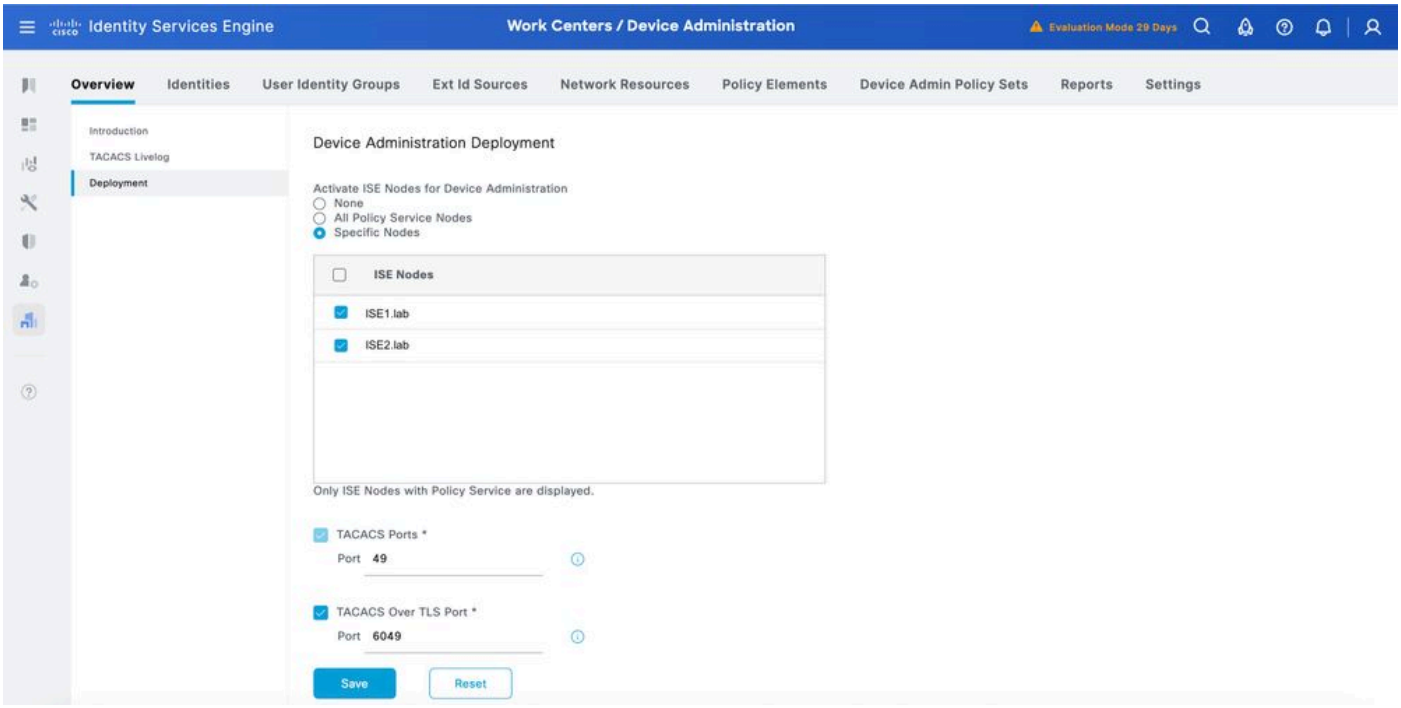
الخطوة 3. احفظ التكوين. تم تمكين "خدمة مسؤول الجهاز" الآن على ISE.

تمكين TACACS عبر TLS

الخطوة 1.انتقل إلى مراكز العمل > إدارة الأجهزة > نظرة عامة.



الخطوة 2.انقر فوق النشر. حدد عقد PSN حيث تريد تمكين TACACS عبر TLS.

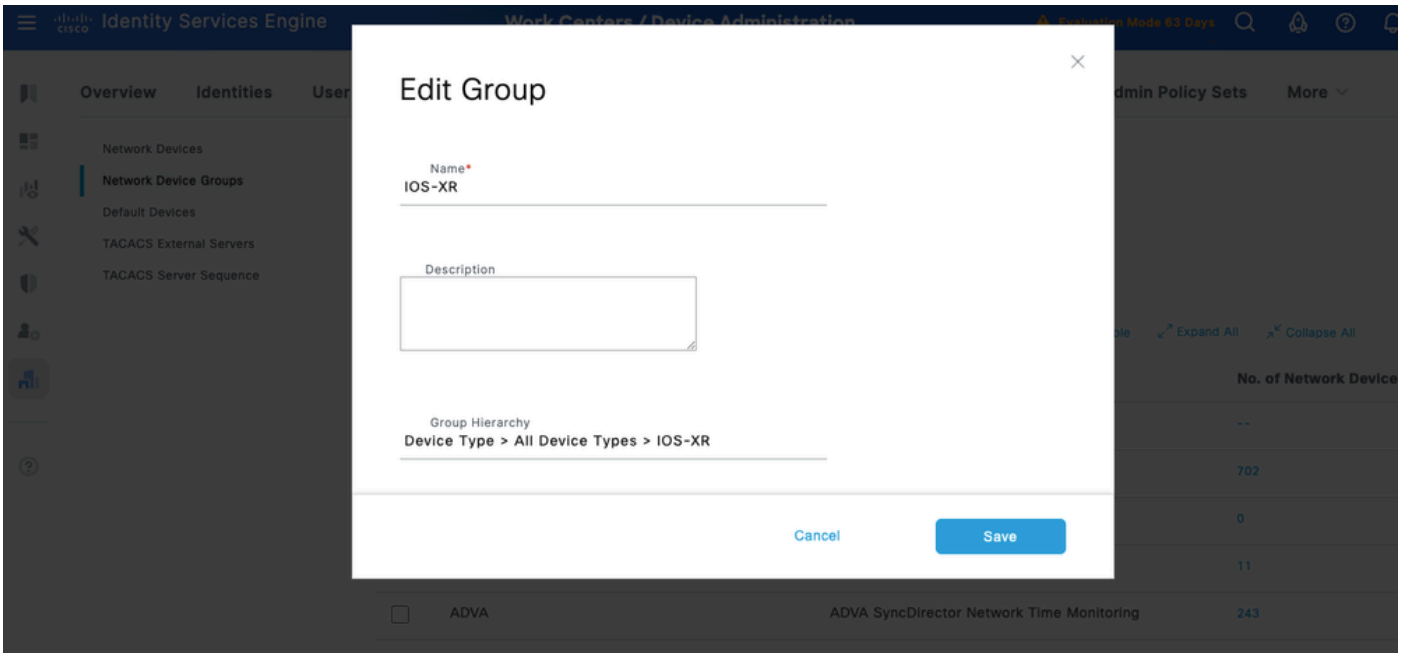


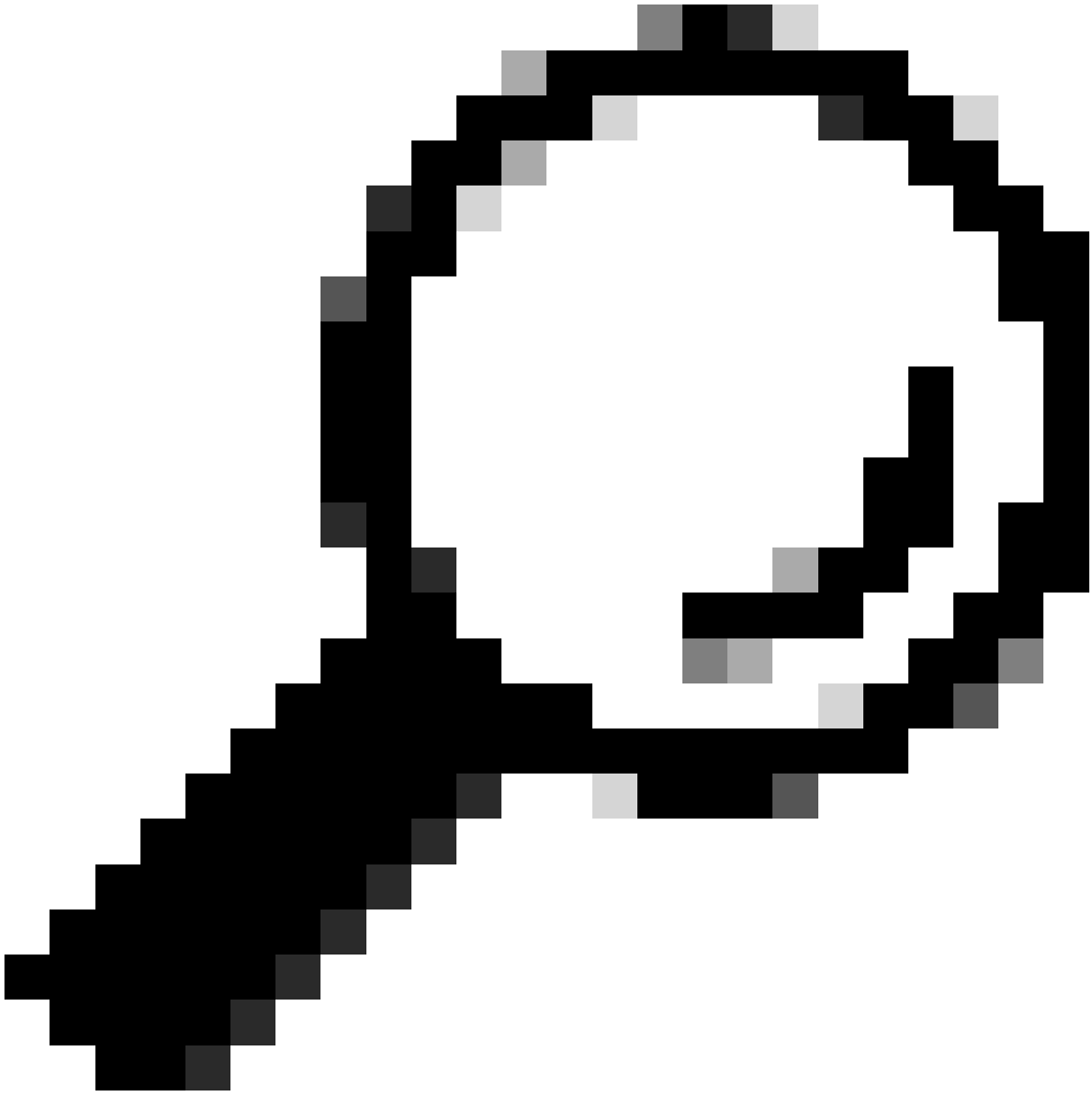
الخطوة 3.احتفظ بالمنفذ الافتراضي 6049 أو حدد منفذ TCP مختلف لـ TACACS عبر TLS، ثم انقر فوق حفظ.

إنشاء مجموعات أجهزة الشبكة وأجهزة الشبكة

يوفر ISE تجميعا قويا للأجهزة بتسلسلات هرمية متعددة لمجموعات الأجهزة. يمثل كل تسلسل هيكلي تصنيفا متميزا ومستقلا لأجهزة الشبكة.

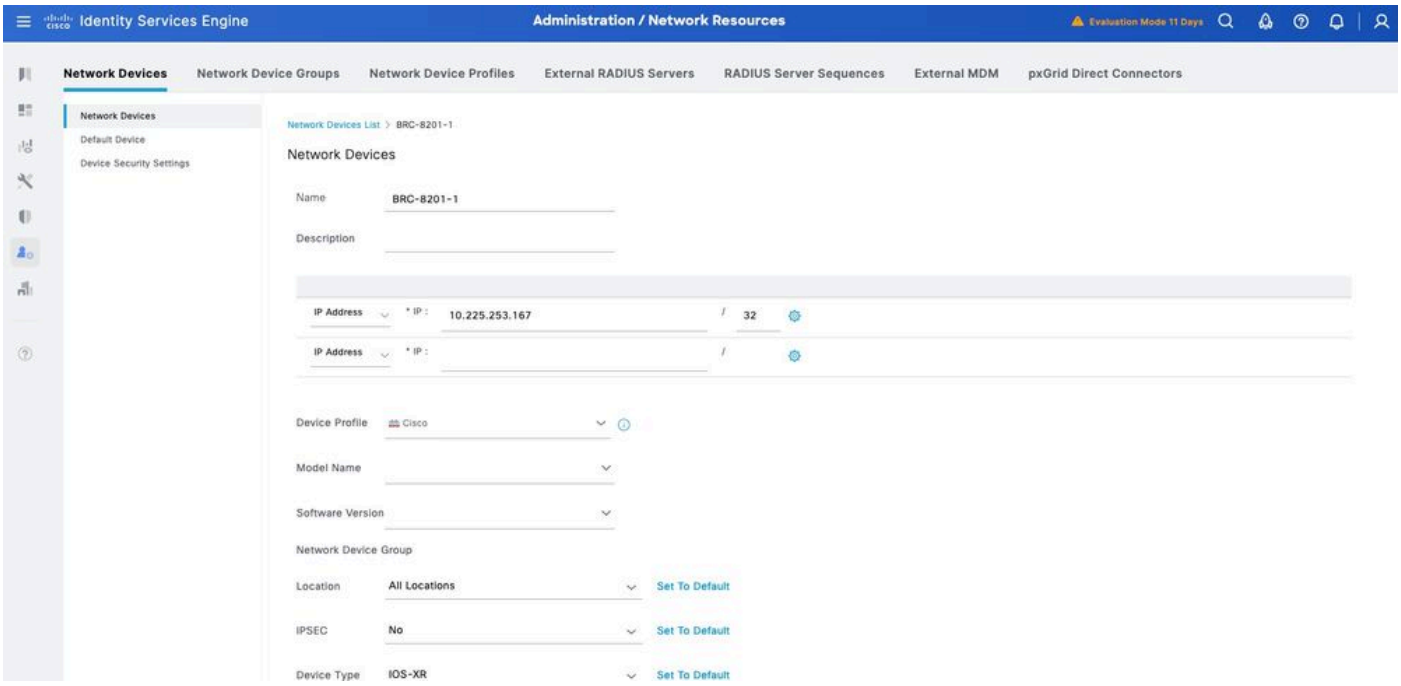
الخطوة 1.انتقل إلى مركز العمل > إدارة الجهاز > موارد الشبكة.انقر فوق مجموعات أجهزة الشبكة وأنشئ مجموعة باسم IOS XR.


Identity Services Engine
Work Centers / Device Administration
Overview
Identities
User
Admin Policy Sets
More
Network Devices
Network Device Groups
Default Devices
TACACS External Servers
TACACS Server Sequence
Expand All
Collapse All
No. of Network Device
Edit Group
Name*
IOS-XR
Description
Group Hierarchy
Device Type > All Device Types > IOS-XR
Cancel
Save
ADVA
ADVA SyncDirector Network Time Monitoring
243

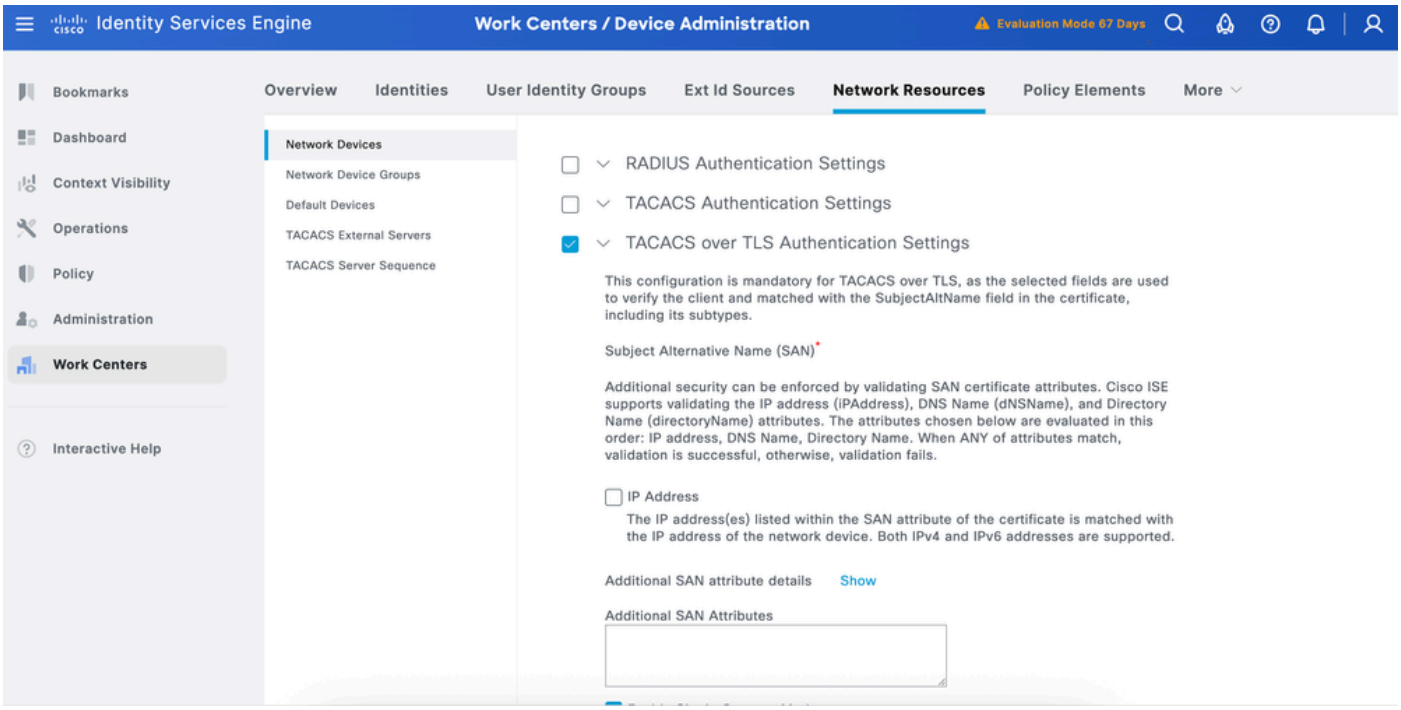


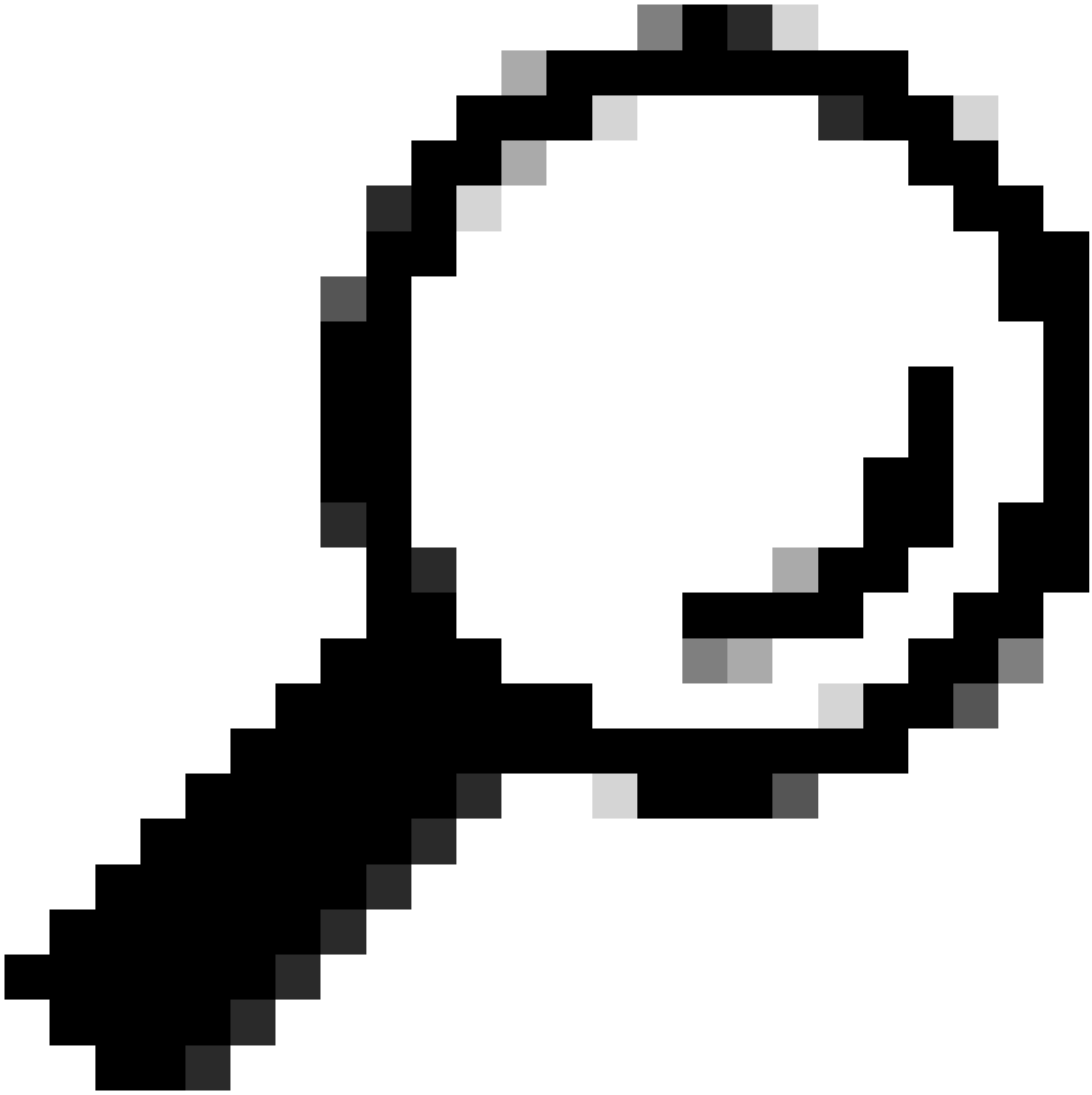
تلميح: تعد جميع أنواع الأجهزة وكافة المواقع تسلسلات هرمية افتراضية يتم توفيرها بواسطة ISE. يمكنك إضافة التدرجات الهرمية الخاصة بك وتعريف المكونات المختلفة في تعريف جهاز الشبكة الذي يمكن إستخدامه لاحقا في حالة السياسة

الخطوة 2. الآن، أضف جهاز Cisco IOS XR كجهاز شبكة. انتقل إلى مركز العمل > إدارة الجهاز > موارد الشبكة > أجهزة الشبكة. انقر على إضافة لإضافة جهاز شبكة جديد.



الخطوة 3.أدخل عنوان IP للجهاز وتأكد من تعيين الموقع ونوع الجهاز(IOS XR) للجهاز. أخيرا، قم بتمكين إعدادات مصادقة TACACS+ عبر TLS.



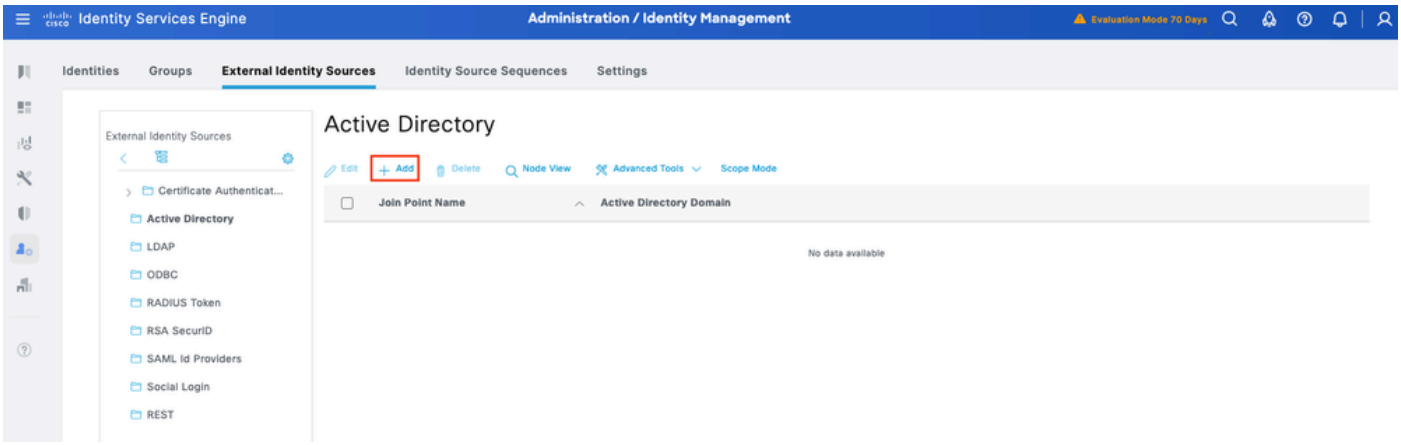


تلميح: يوصى بتمكين وضع الاتصال المفرد لتجنب إعادة تشغيل جلسة عمل TCP في كل مرة يتم إرسال أمر فيها إلى الجهاز.

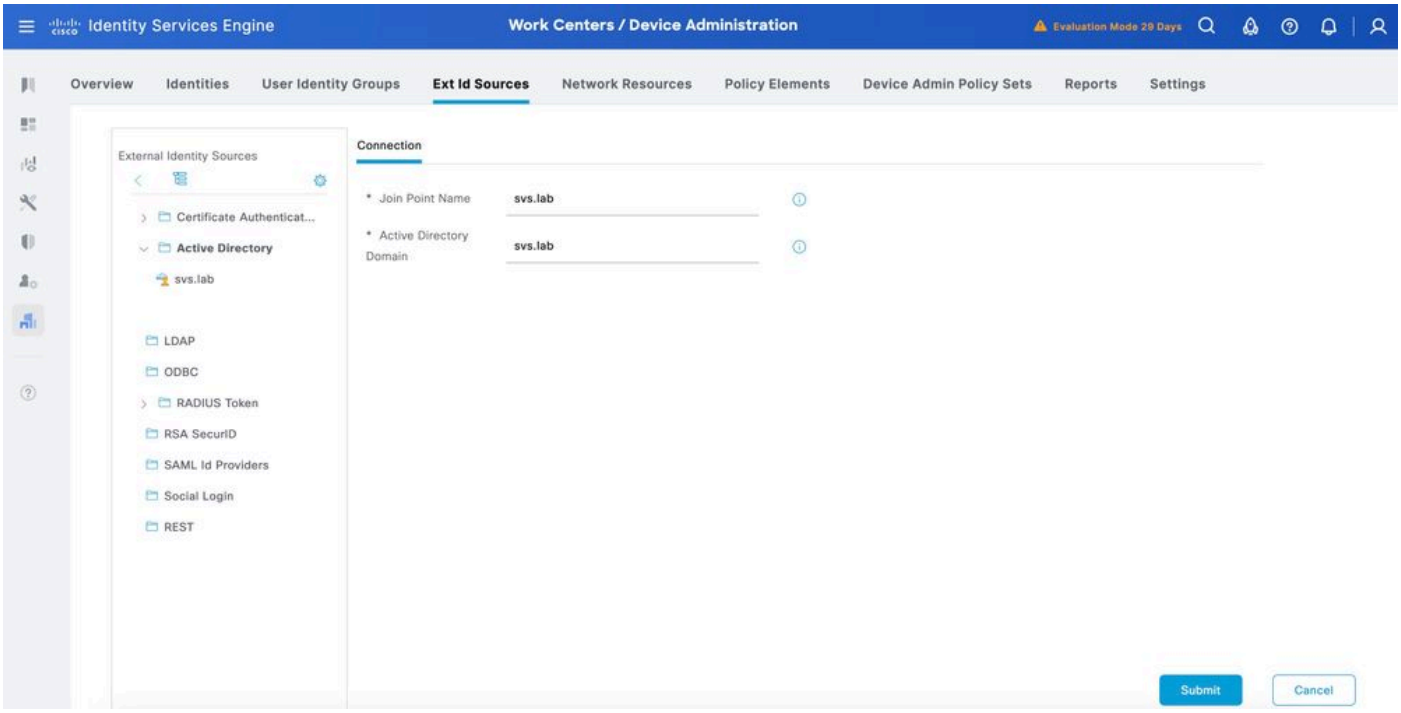
متاجر ConfigureIdentity

يحدد هذا القسم مخزن هوية لمسؤولي الأجهزة، والذي يمكن أن يكون مستخدمي ISE الداخليين أو أي مصادر هوية خارجية مدعومة. هنا يستخدم Active Directory (AD)، مصدر هوية خارجي.

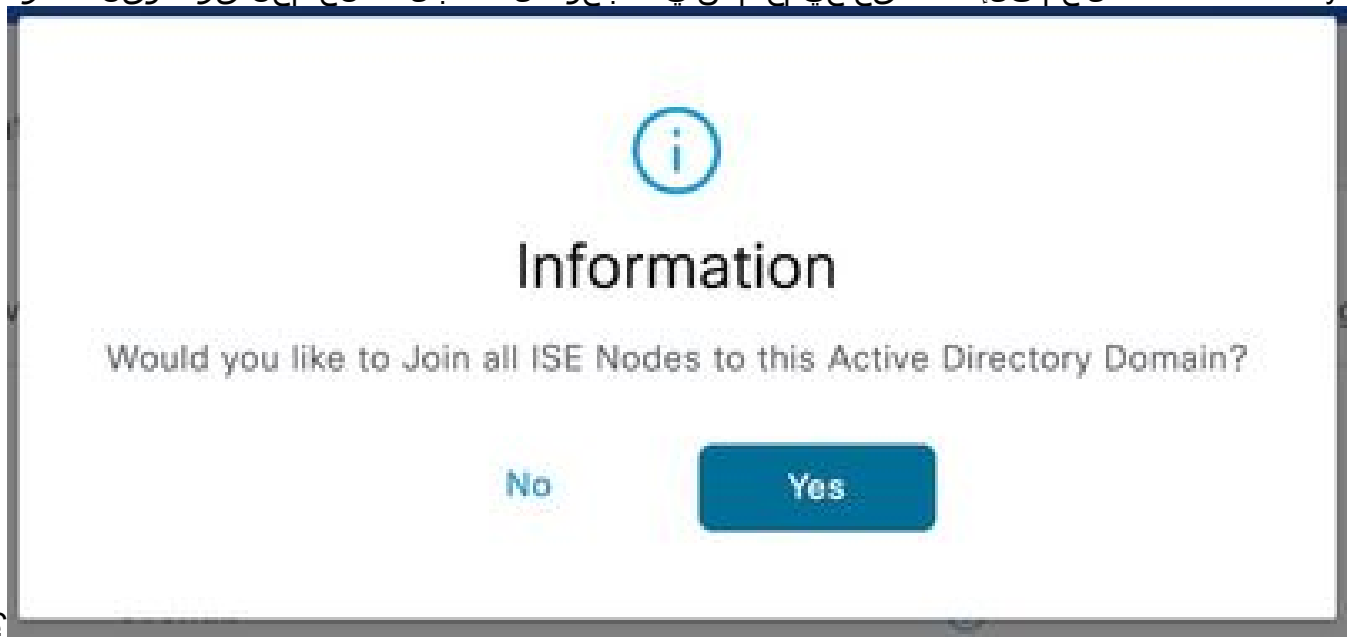
الخطوة 1. انتقل إلى الإدارة > إدارة الهوية > مخازن الهوية الخارجية > Active Directory. انقر فوق إضافة لتحديد نقطة AD مشتركة جديدة.



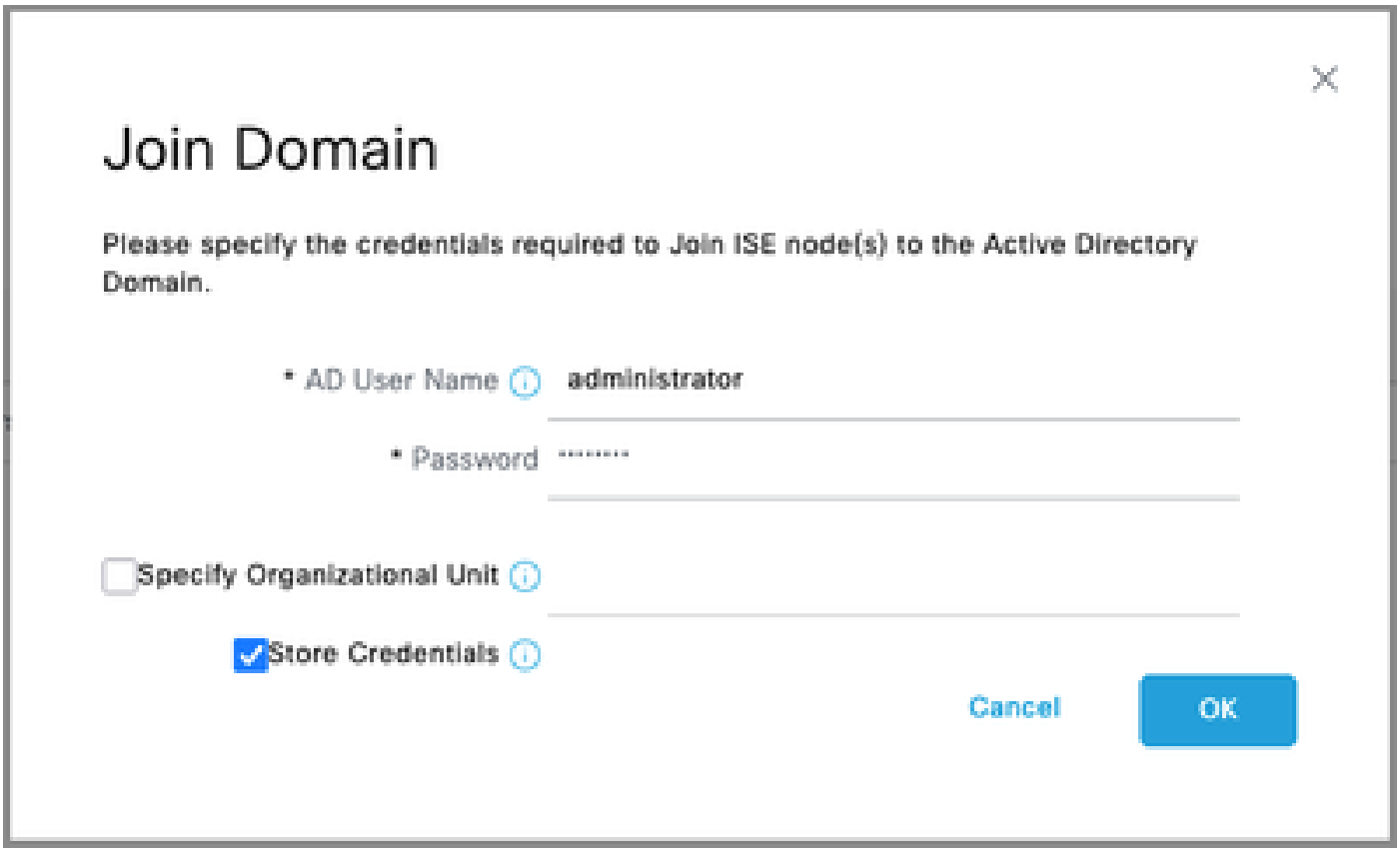
الخطوة 2. حدد اسم نقطة الربط واسم مجال AD وانقر إرسال.

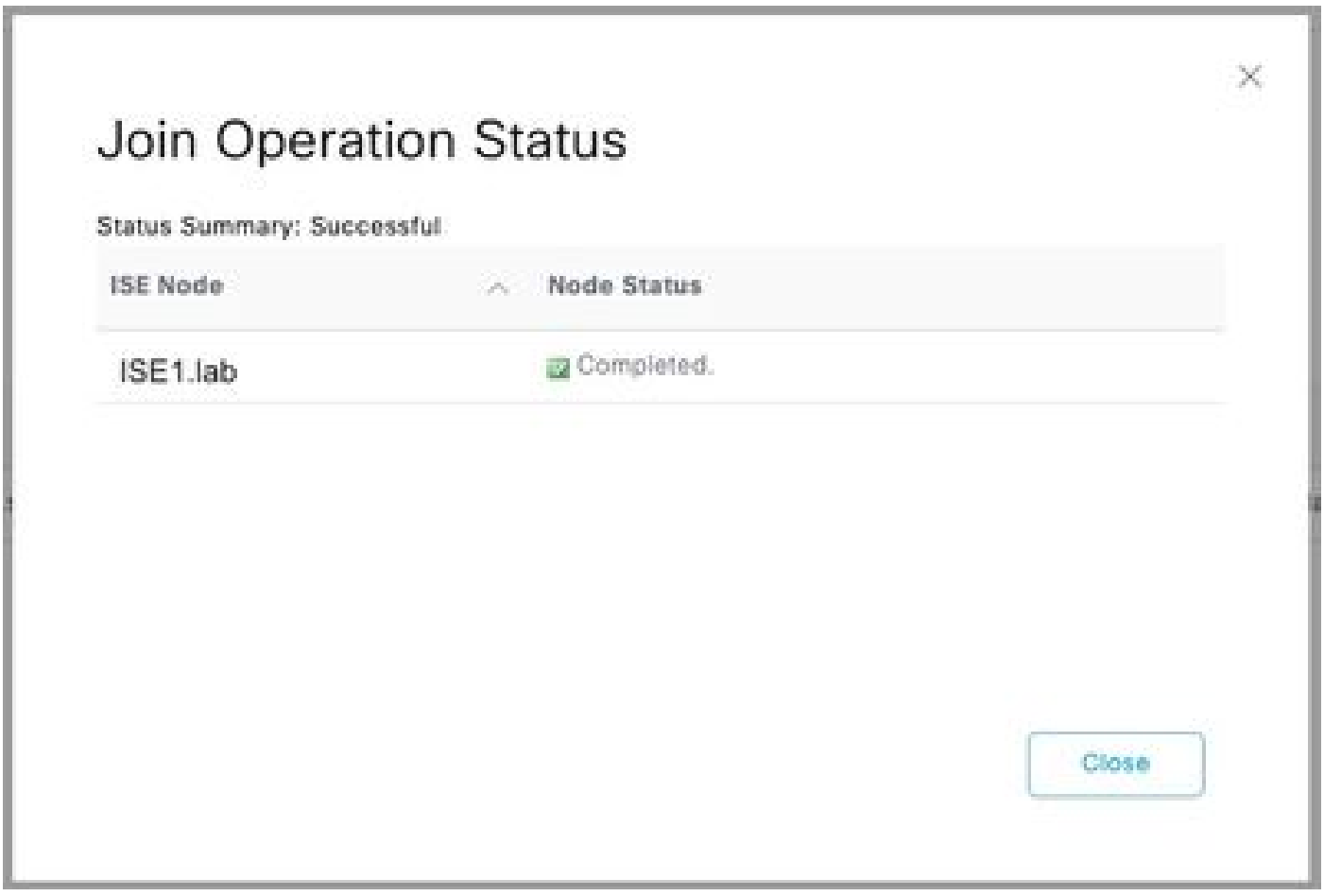


الخطوة 3.انقر فوق نعم عند طلبها، هل ترغب في ضم جميع عقد ISE إلى مجال Active Directory هذا؟

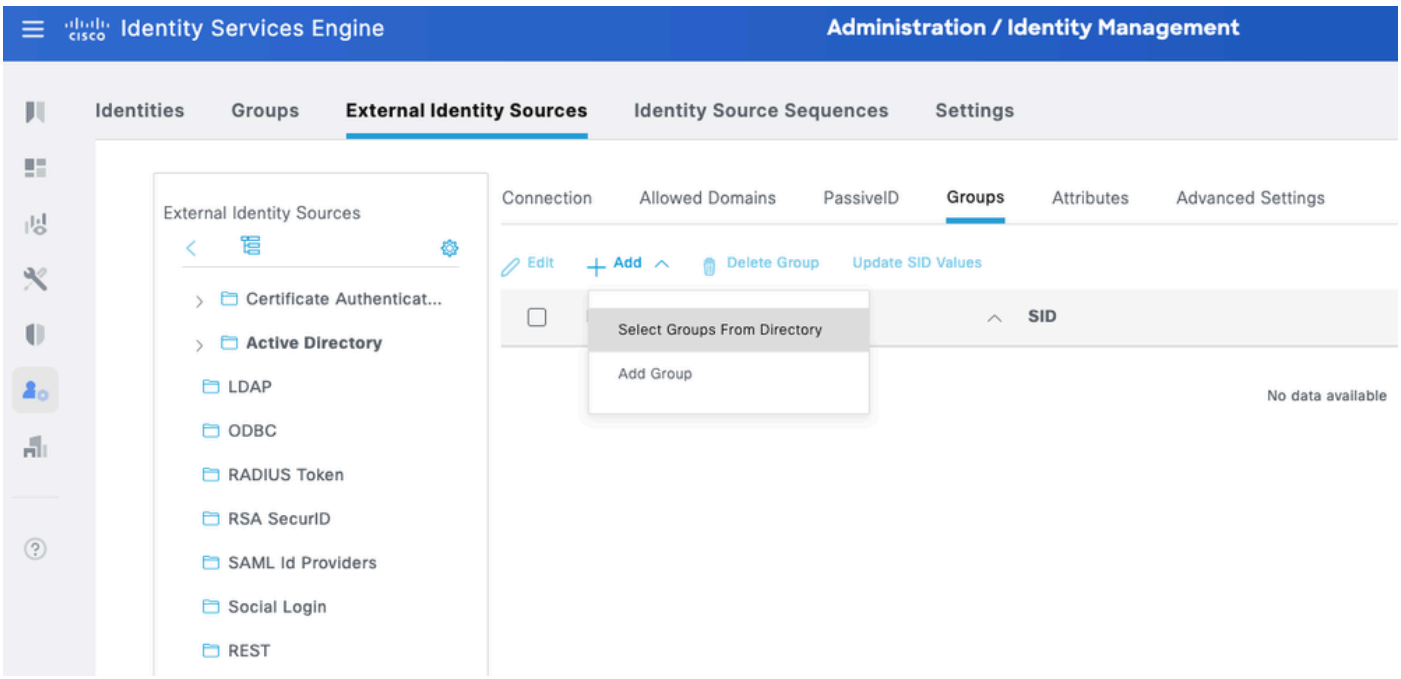


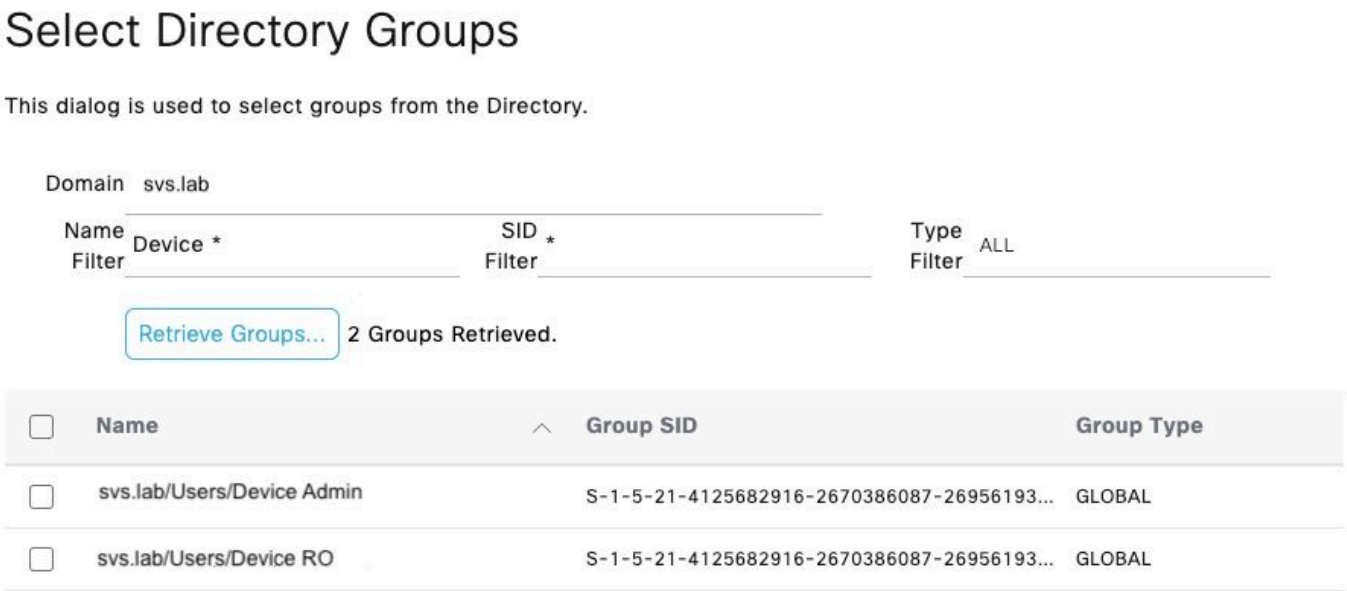
الخطوة 4.أدخل بيانات الاعتماد بامتيازات AD Join وانضم ISE إلى AD. تحقق من الحالة للتحقق من أنها تعمل.

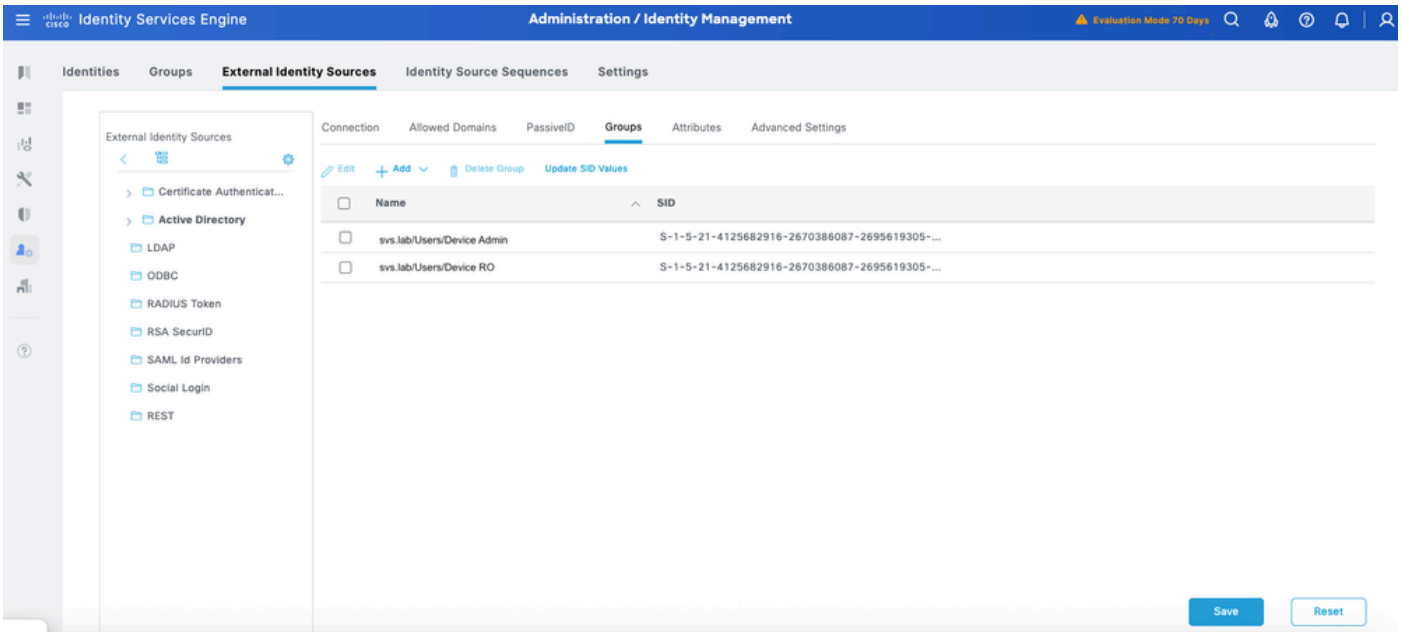




الخطوة 5.انتقل إلى علامة التبويب مجموعات، وانقر فوق إضافة للحصول على جميع المجموعات المطلوبة استنادا إلى أي من المستخدمين مخولين للوصول إلى الجهاز. يوضح هذا المثال المجموعات المستخدمة في نهج التخويل.







تكوين توصيفات TACACS+

تخطيط توصيفات TACACS+ لأدوار المستخدمين على أجهزة Cisco IOS XR. في هذا المثال، يتم تعريف ما يلي:

- Root System Administrator (مدير النظام الجذري) - هذا هو الدور الأكثر امتيازات في الجهاز. يتمتع المستخدم صاحب دور مسؤول النظام الجذري بحق الوصول الإداري الكامل إلى جميع أوامر النظام وإمكانات التكوين.
- عامل التشغيل - يهدف هذا الدور إلى المستخدمين الذين يحتاجون إلى وصول للقراءة فقط إلى النظام لأغراض المراقبة واستكشاف الأخطاء وإصلاحها.

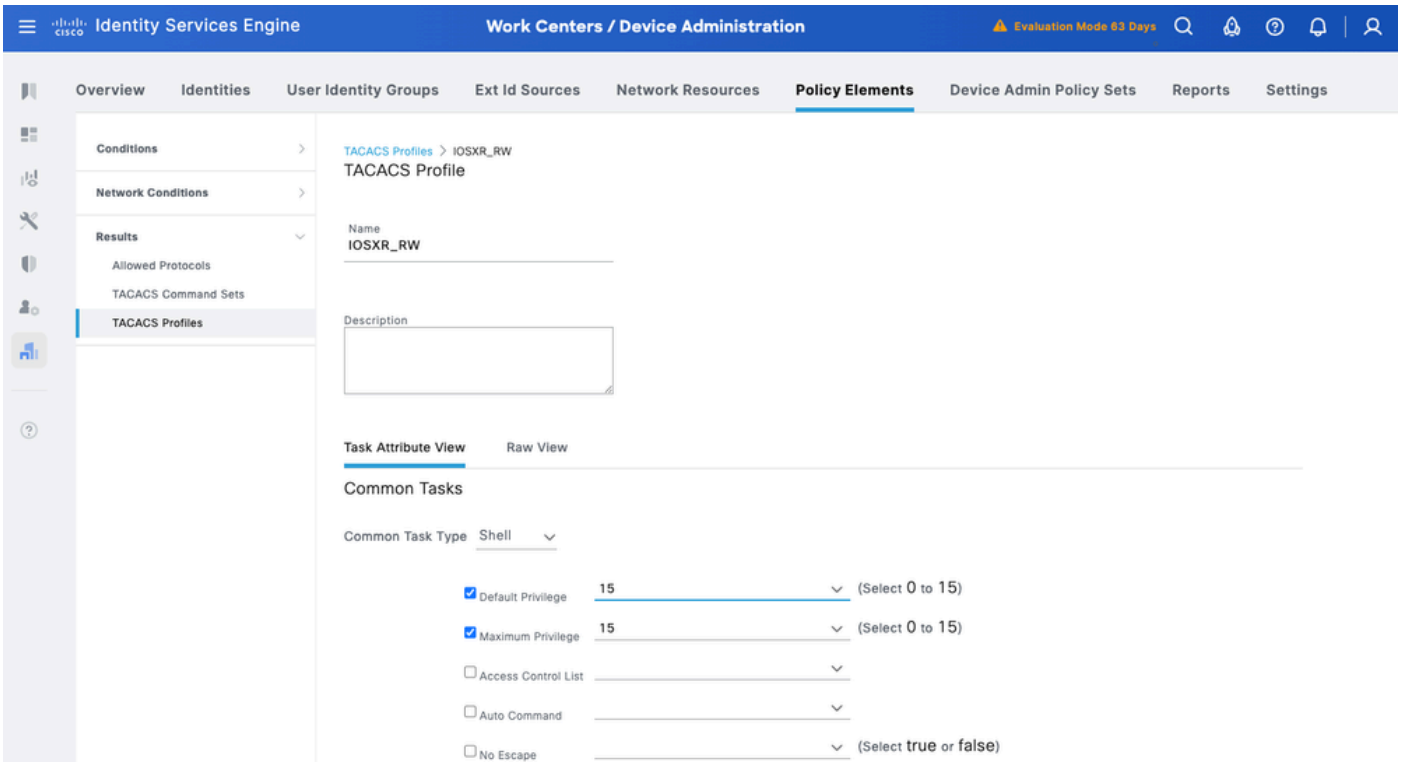
تحديد توصيفي TACACS+: IOSXR_RW و IOSXR_RO.

IOS XR_RW - ملف تعريف المسؤول

الخطوة 1. انتقل إلى مراكز العمل > إدارة الأجهزة > عناصر السياسة > النتائج > ملفات تعريف TACACS. قم بإضافة ملف تعريف TACACS جديد وتسميته IOSXR_RW.

خطوة 2. فحصت وعينت التقصير امتياز والحد الأقصى امتياز ك 15.

الخطوة 3. أكد التكوين والحفظ.

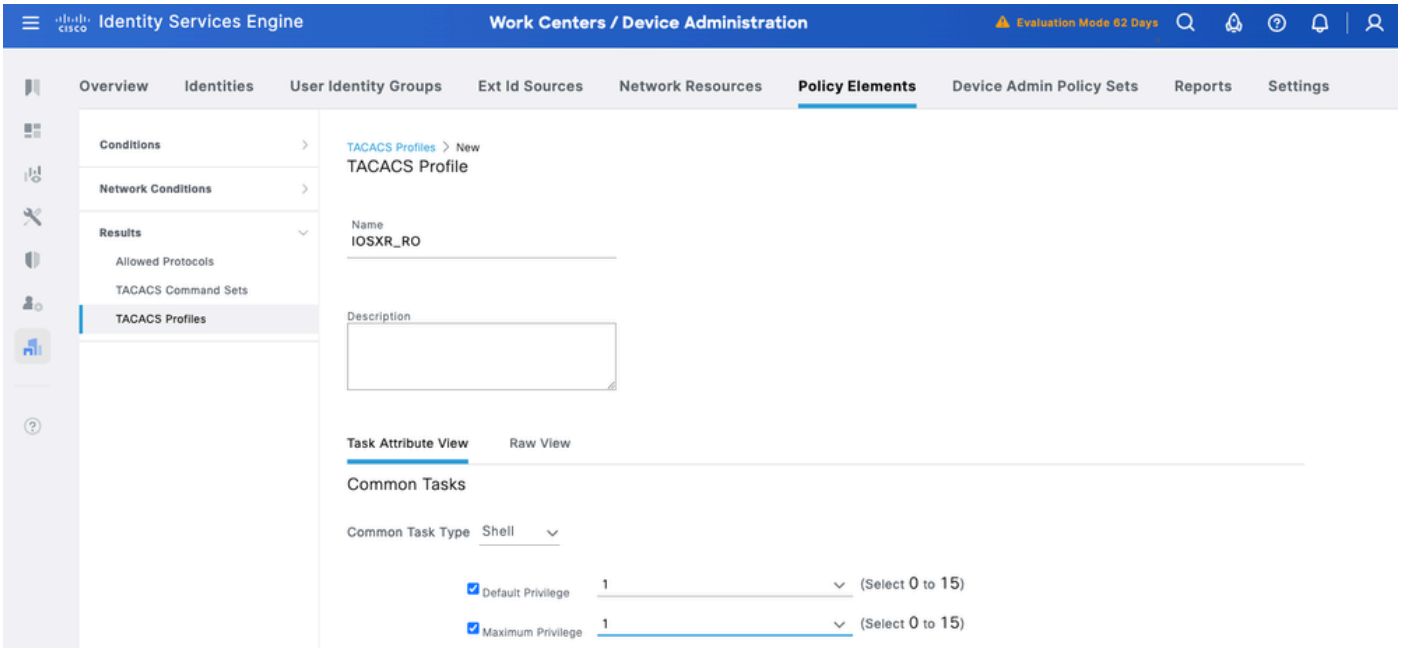


IOS XR_RO - ملف تعريف المشغل

الخطوة 1. انتقل إلى مراكز العمل > إدارة الأجهزة > عناصر السياسة > النتائج > ملفات تعريف TACACS. أضف ملف تعريف TACACS جديد وقم بتسميته IOSXR_RO.

خطوة 2. فحصت وعينت التقصير امتياز واحد الأقصى امتياز ك 1.

الخطوة 3.تأكد من التكوين والحفظ.



مجموعات أوامر configureTACACS+

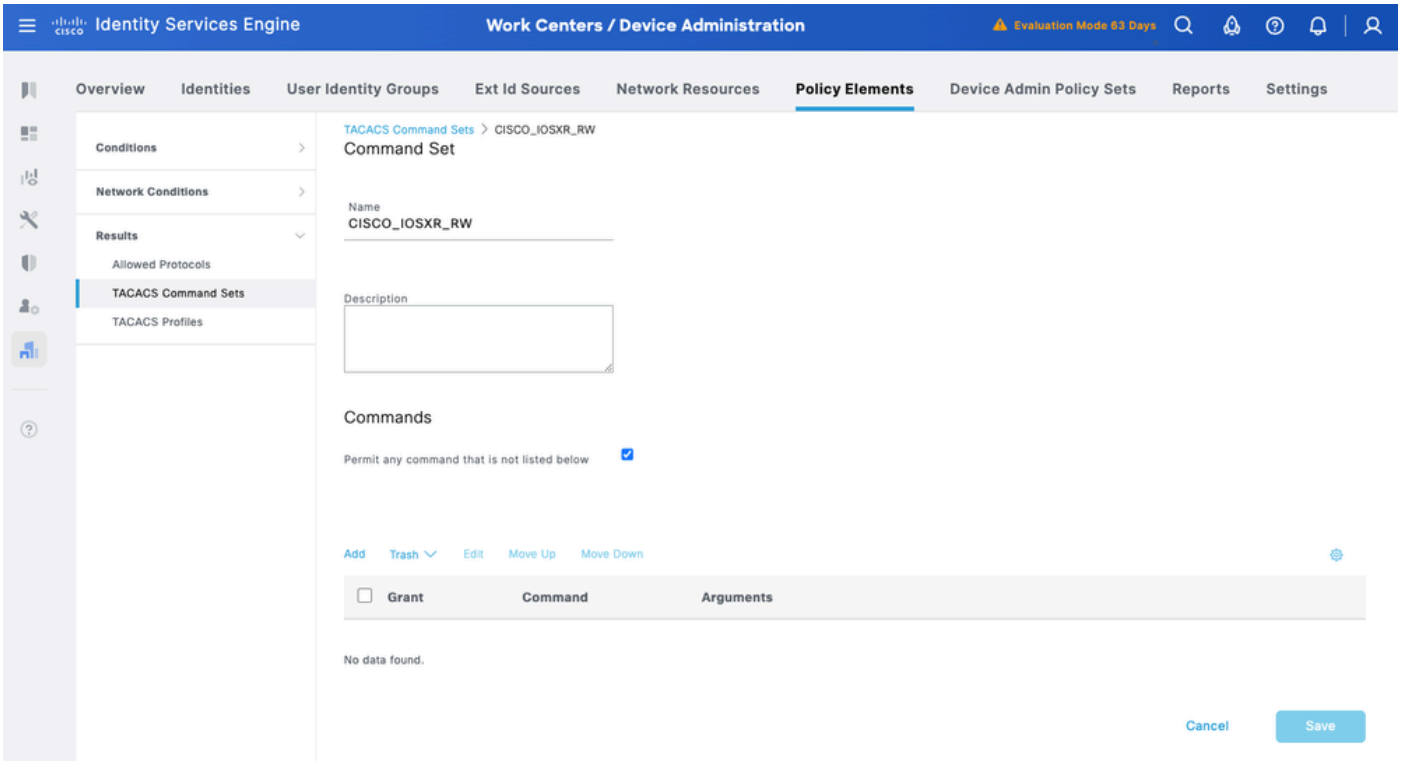
تعريف مجموعات أوامر TACACS+: في هذا المثال، يتم تحديد هذه التطبيقات على

Cisco_IOSXR_RW و Cisco_IOSXR_RO.

Cisco IOS XR RW - مجموعة أوامر المسؤول

الخطوة 1. انتقل إلى مراكز العمل > إدارة الجهاز > عناصر السياسة > النتائج > مجموعات أوامر TACACS. أضف مجموعة أوامر TACACS جديدة وقم بتسميتها Cisco_IOSXR_RW.

الخطوة 2. حدد خانة الاختيار السماح بأي أمر غير مدرج أدناه (وهذا يسمح بأي أمر لدور المسؤول) وانقر فوق حفظ.



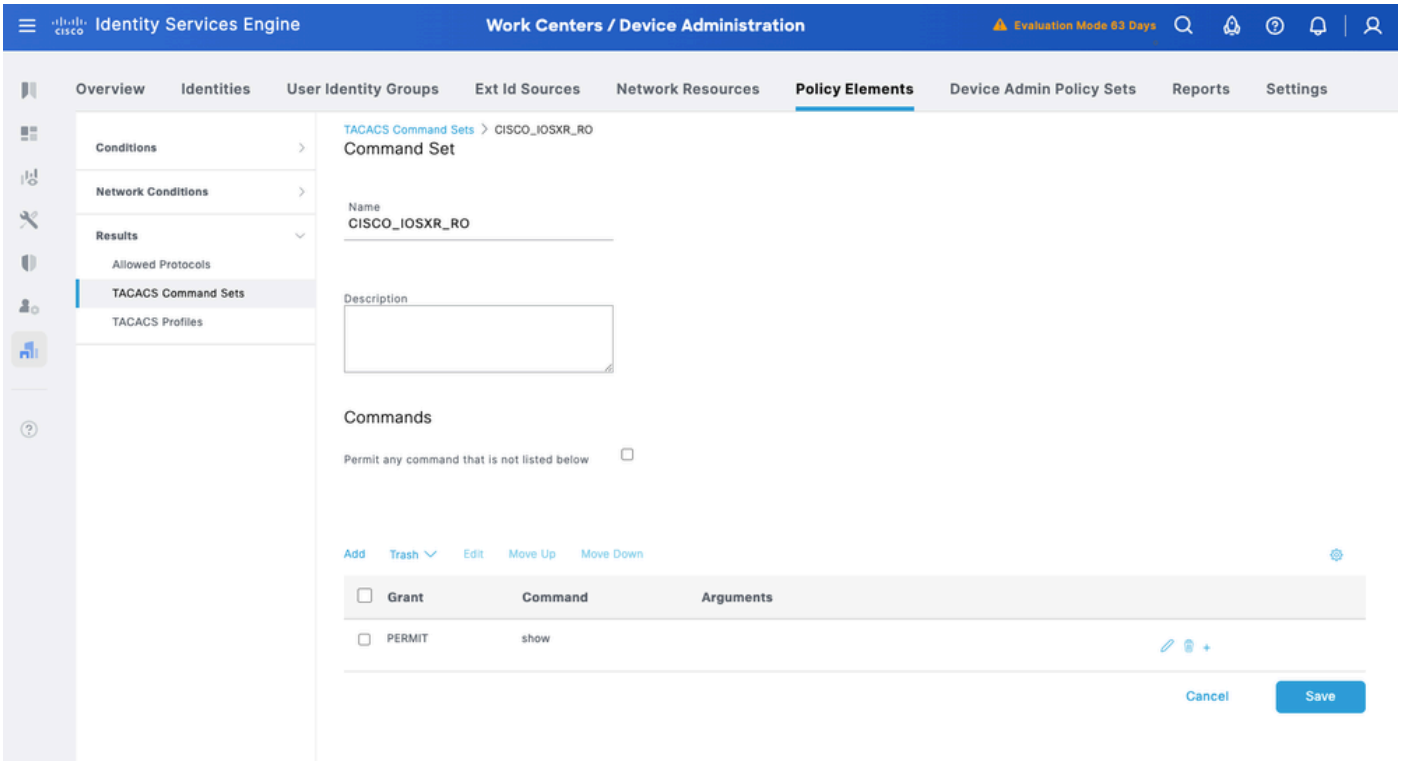
مجموعة أوامر المشغل Cisco IOS XR RO

الخطوة 1. من واجهة مستخدم ISE، انتقل إلى مراكز العمل > إدارة الجهاز > عناصر السياسة > النتائج > مجموعات أوامر TACACS. قم بإضافة مجموعة أوامر TACACS جديدة وقم بتسميتها Cisco_IOSXR_RO.

الخطوة 2. في قسم الأوامر ، أضف أمر جديد.

الخطوة 3. حدد السماح من القائمة المنسدلة لعمود المنحة وأدخل العرض في عمود الأمر؛ وانقر فوق سهم الشيك.

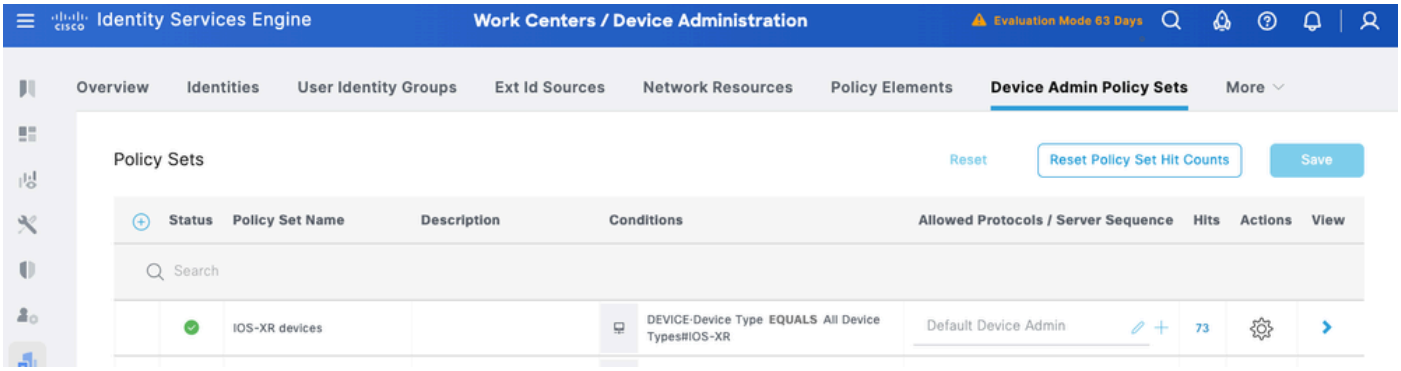
الخطوة 4. تأكد من البيانات وانقر فوق حفظ.



تكوين مجموعات نهج مسؤول الجهاز

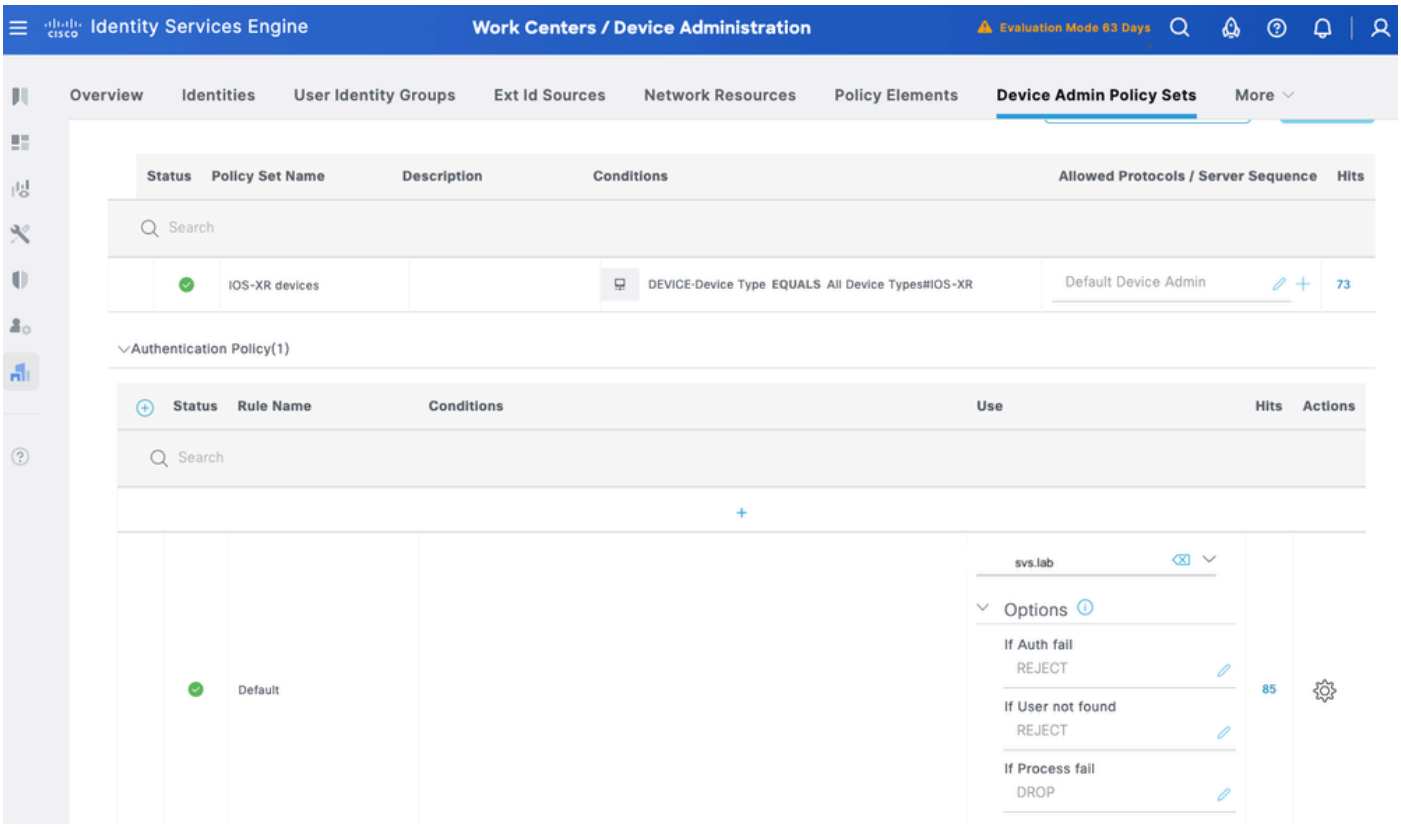
يتم تمكين مجموعات النهج بشكل افتراضي لإدارة الأجهزة. يمكن أن تقسم مجموعات السياسات استنادا إلى أنواع الأجهزة لتسهيل تطبيق ملفات تعريف TACACS.

الخطوة 1.انتقل إلى مراكز العمل > إدارة الجهاز > مجموعات سياسات إدارة الأجهزة. إضافة أجهزة IOS XR الجديدة لمجموعة السياسات. تحت شرط حدد أداة:نوع الجهاز يساوي كل أنواع الأجهزة#IOS XR. تحت البروتوكولات المسموح بها، حدد مسؤول الجهاز الافتراضي.



الخطوة 2. انقر فوق Saveld وانقر فوق السهم الأيمن لتكوين مجموعة النهج هذه.

الخطوة 3. إنشاء سياسة المصادقة. للمصادقة، تستخدم AD كمخزن المعرف. أترك الخيارات الافتراضية تحت إذا فشلت المصادقة، إذا لم يفشل المستخدم في العملية.

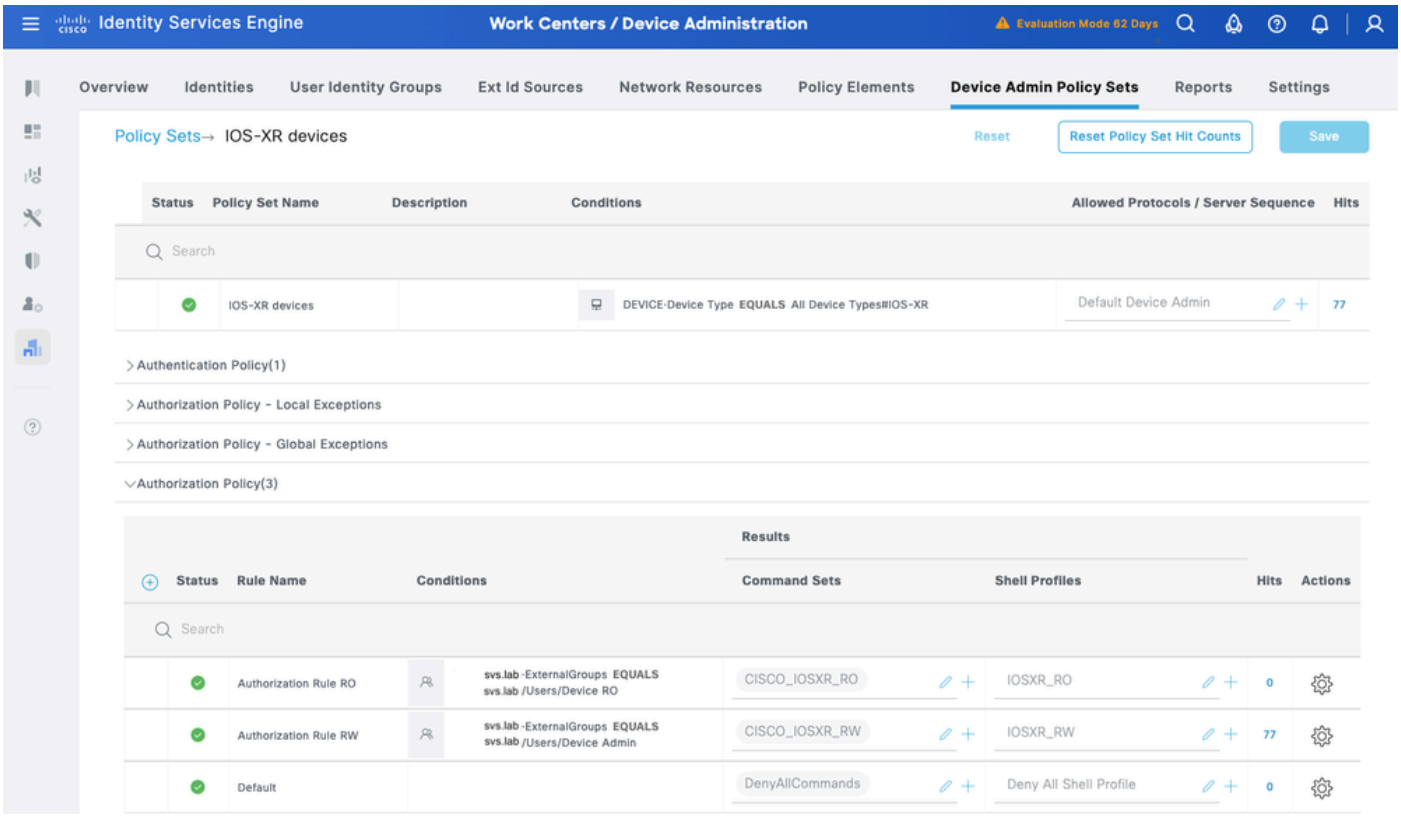


الخطوة 4. تحديد سياسة التفويض.

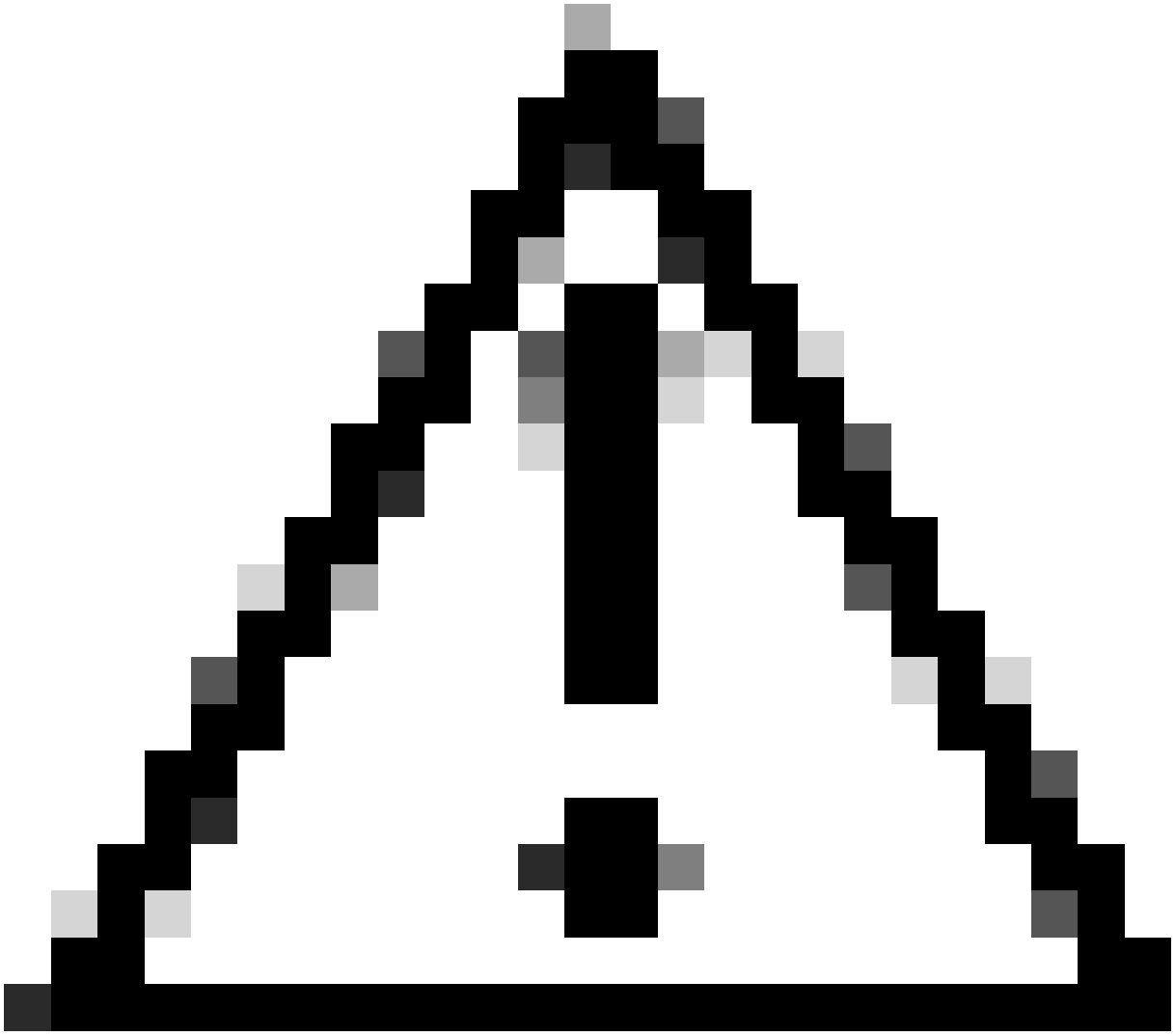
قم بإنشاء نهج التخويل استنادا إلى مجموعات المستخدمين في Active Directory (AD).

على سبيل المثال:

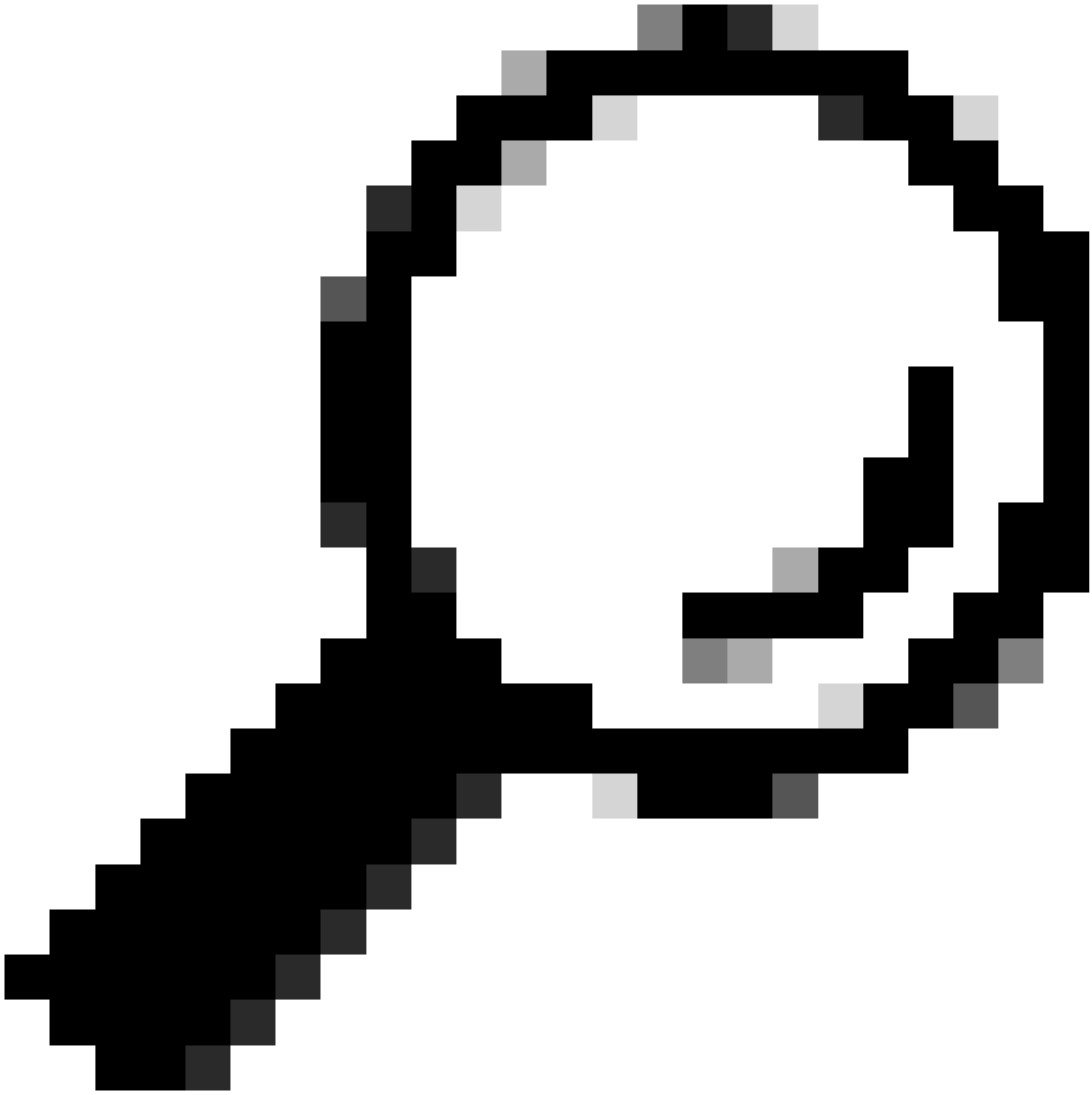
- يتم تعيين المستخدمين في مجموعة الإعلانات للجهاز مجموعة الأوامر cisco_iosxr_ro وملف تعريف IOSXR_RO Shell.
- يتم تعيين المستخدمين في مسؤول جهاز مجموعة الإعلانات لمجموعة الأوامر CISCO_IOSXR_RW وملف تعريف IOSXR_RW Shell.



الجزء 2 - تكوين Cisco IOS XR لـ TACACS+ عبر TLS 1.3



تحذير: تأكد من إمكانية الوصول إلى اتصال وحدة التحكم وعمله بشكل صحيح.



تلميح: يوصى بتكوين مستخدم مؤقت وتغيير طرق مصادقة AAA والتفويض لاستخدام بيانات الاعتماد المحلية بدلا من TACACS أثناء إجراء تغييرات التكوين، لتجنب قفل حسابك خارج الجهاز.

عمليات التهيئة الأولية

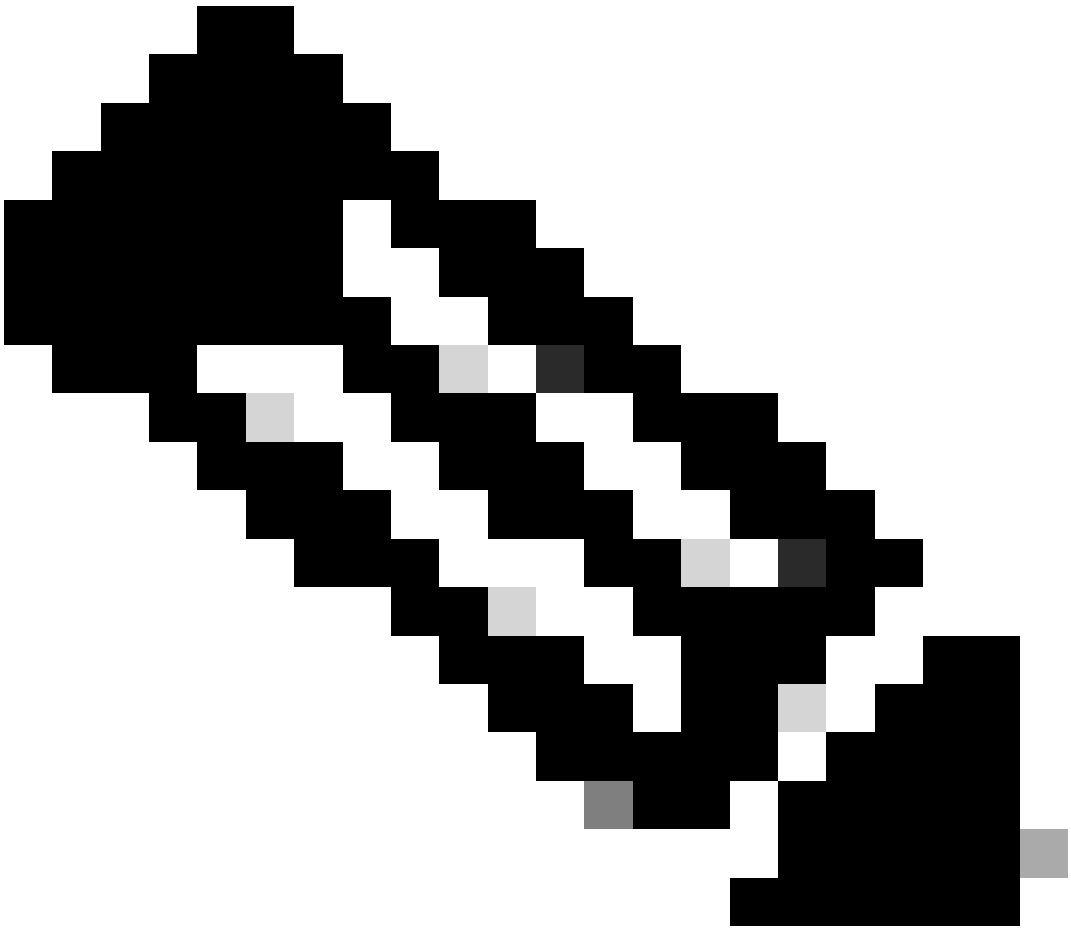
الخطوة 1. تأكد من تكوين خادم الاسم (DNS) ومن قدرة الموجه على حل أسماء المجالات المؤهلة بشكل متكرر (FQDNs) بنجاح، وخاصة FQDN لخادم ISE.

```
domain vrf mgmt name svs.lab
domain vrf mgmt name-server 10.225.253.247
no domain vrf mgmt lookup disable

RP/0/RP0/CPU0:BRC-8201-1#ping vrf mgmt ise1.svs.lab
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.225.253.209 timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

الخطوة 2. قم بمسح أي نقاط ثقة وشهادات قديمة/غير مستخدمة. تأكد من عدم وجود نقاط ثقة وشهادات قديمة. إذا كنت ترى أي إدخالات قديمة، فقم بإزالتها/مسحها.

```
show crypto ca trustpoint
show crypto ca certificates

(config)# no crypto ca trustpoint <tp-name>
# clear crypto ca certificates <tp-name>
```



ملاحظة: يمكنك إنشاء زوج مفاتيح RSA جديد يدويا وإرفاقه تحت TrustPoint. إذا لم

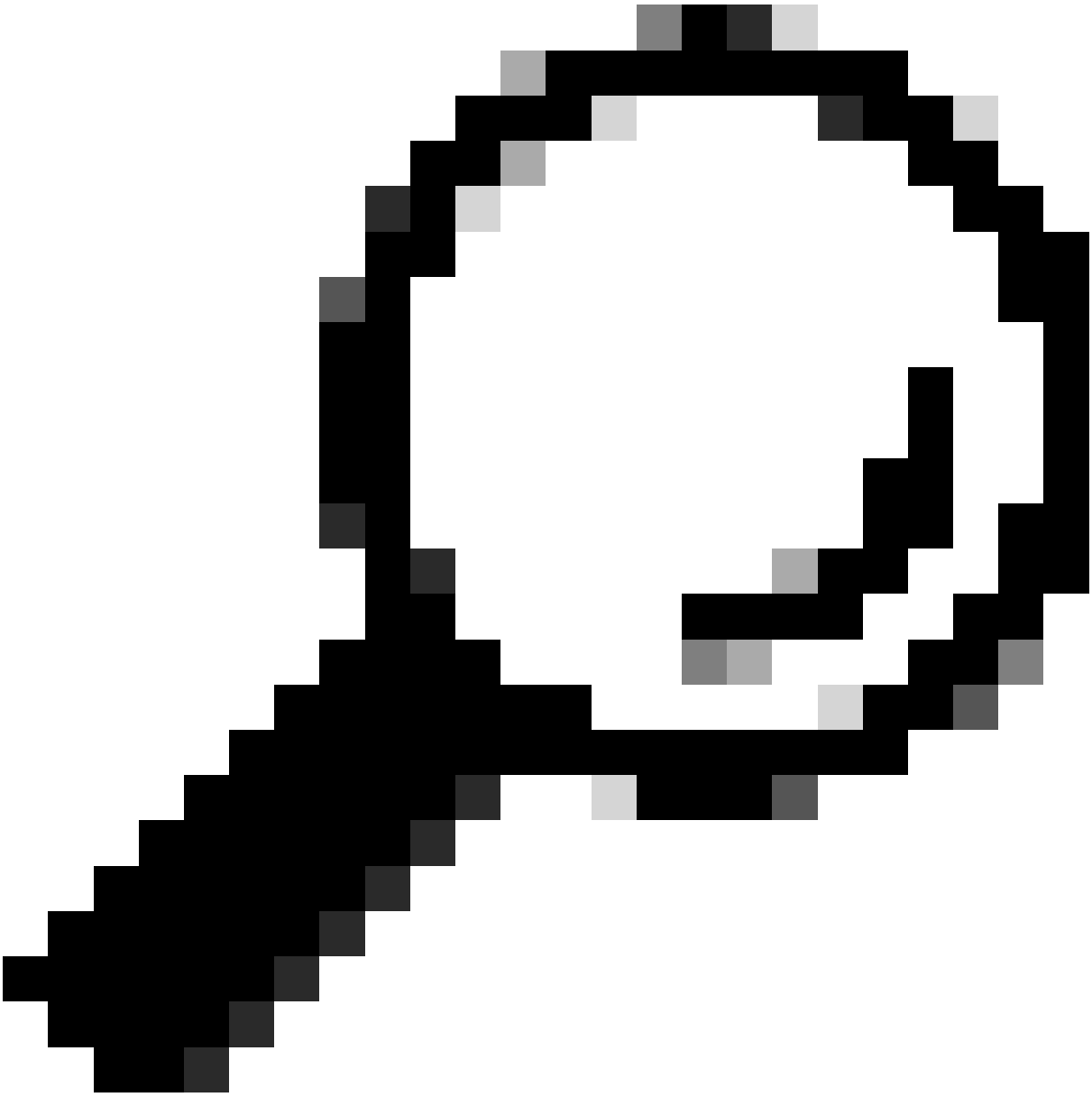
تقم بإنشاء واحد، سيتم إستخدام زوج المفاتيح الافتراضي. ال يتم حاليا اعتماد تعريف زوج مفاتيح ECC ضمن TrustPoint.

تكوين TrustPoint

الخطوة 1. تكوين زوج المفاتيح (إختياري).

```
<#root>
RP/0/RP0/CPU0:BRC-8201-1(config)#
crypto key generate rsa

          4096

RP/0/RP0/CPU0:BRC-8201-1(config)#
crypto ca trustpoint

RP/0/RP0/CPU0:BRC-8201-1(config-trustp)#
rsakeypair
```

الخطوة 2. إنشاء نقطة ثقة.



تلميح: تكوين DNS لاسم الموضوع البديل إختياري (في حالة تمكينه على ISE)، ولكن يوصى به.

<#root>

RP/0/RP0/CPU0:BRC-8201-1(config)#

crypto ca trustpoint svs

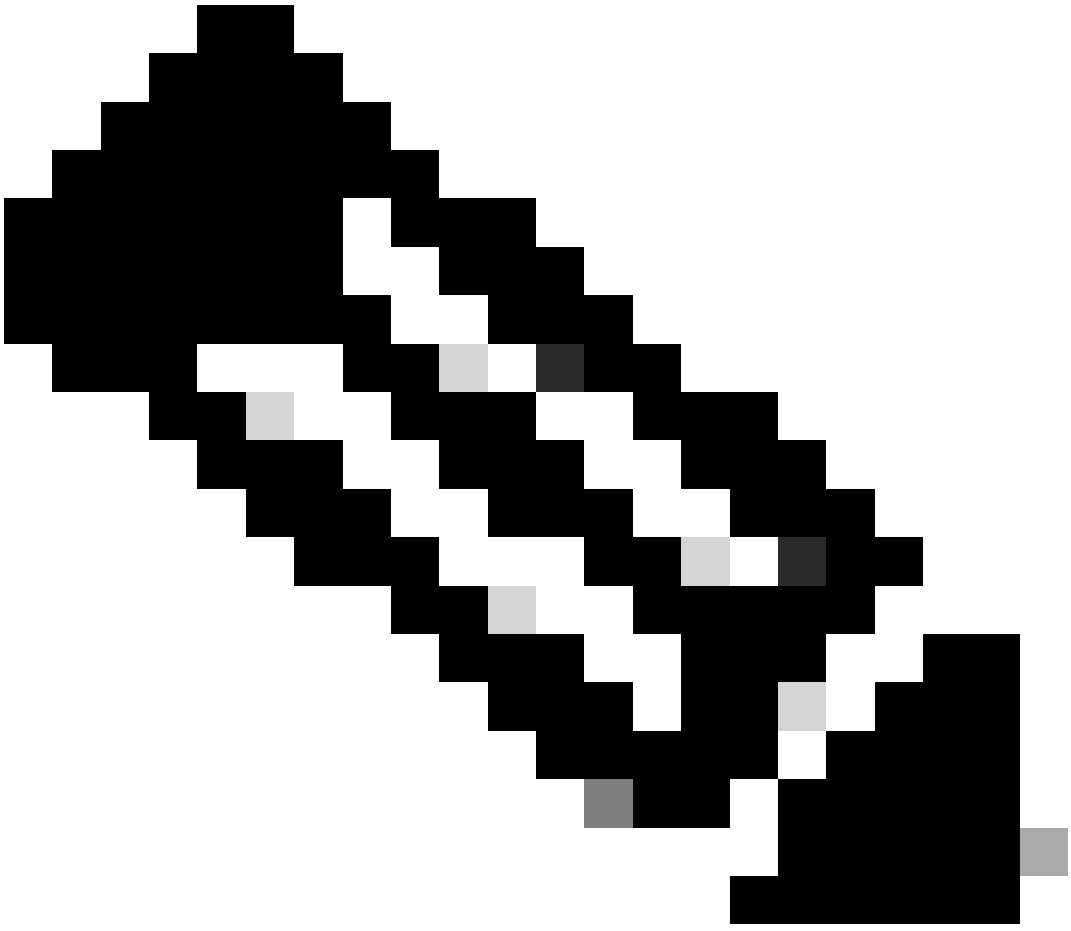
RP/0/RP0/CPU0:BRC-8201-1(config-trustp)#

vrf mgmt

RP/0/RP0/CPU0:BRC-8201-1(config-trustp)#

crl optional

```
RP/0/RP0/CPU0:BRC-8201-1(config-trustp)#
subject-name C=US,ST=NC,L=RTP,O=Cisco,OU=SVS,CN=brc-8201-1.svs.lab

RP/0/RP0/CPU0:BRC-8201-1(config-trustp)#
subject-alternative-name IP:10.225.253.167,DNS:brc-8201-1.svs.lab

RP/0/RP0/CPU0:BRC-8201-1(config-trustp)#
enrollment url terminal
RP/0/RP0/CPU0:BRC-8201-1(config-trustp)#
rsakeypair svs-4096

RP/0/RP0/CPU0:BRC-8201-1(config-trustp)#
commit
```



ملاحظة: إذا احتجت لاستخدام فاصلة في O أو O، يمكنك إستخدام شرطة مائلة عكسية (\) قبل الفاصلة. على سبيل المثال: o=Cisco Systems\، Inc.

الخطوة 3. مصادقة TrustPoint بتثبيت شهادة CA.

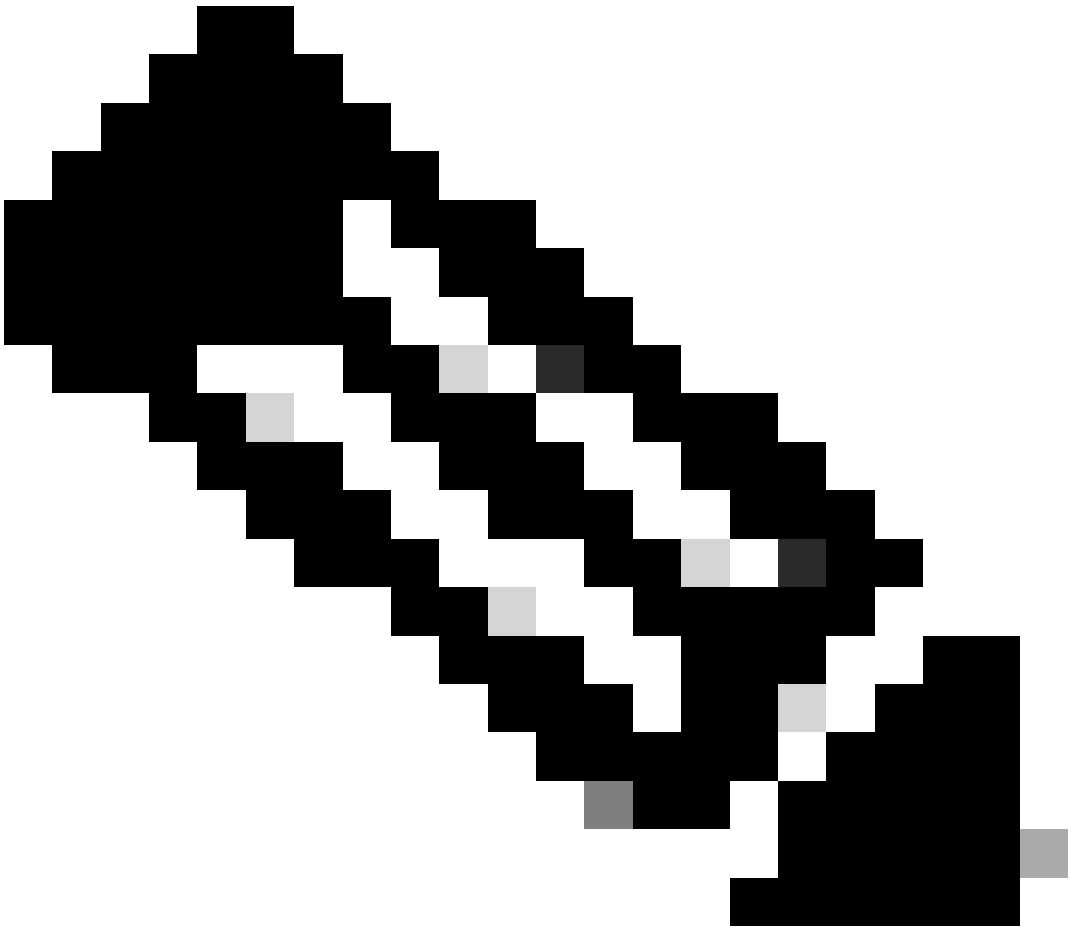
<#root>

```
RP/0/RP0/CPU0:BRC-8201-1#

crypto ca authenticate svs



Enter the base64/PEM encoded certificate/certificates.
Please note: for multiple certificates use only PEM.
End with a blank line or the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----
MIIFlDCCA3ygAwIBAgIIIM10AsTaN/UwDQYJKoZIhvcNAQELBQAwajELMAkGA1UE
BhMCVVMxFzAVBgNVBAgTDk5vcnRoIENhcm9saW5hMRAwDgYDVQQHEwdSYWxlaWdo
MQ4wDAYDVQQKEwVDaXNjbzEMMAoGA1UECxMDU1ZTMRIwEAYDVQQDEwlTVlMgTGFi
Q0EwHhcNMjUwNDI4MTcwNTAwWhcNMzUwNDI4MTcwNTAwWjBqMQswCQYDVQQGEwJV
UzEXMBUGA1UECBMOTm9ydGggQ2Fyb2xpbmExEDAOBgNVBAcTB1JhbGVpZ2gxDjAM
BgNVBAoTBUNpc2NvMQwwCgYDVQQLEwNTVlMxEjAQBgNVBAMTCVNWUyBMYWJDQTCC
AiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBAJvZUOyn2vIn6gKbx3M7vaRq
2YjwZlzSH6EkEvxnJTy+kksiFD33GyHQepk7vfp4NFU5OtQ4HC7t/AOv9grDa3QW
VwvV4MBbJhFM3s0J/ejgDYcMZhIAaPy0Zo5WLboOkXEiKjPLatkXojB8FVrhLF3O
jMBSqwa4/Wlniy5S+7s4FFxsCf2OCOWfBAsnrs0tatIIhmcnx+VLJP7MRm8f0w4m
mutNo7IhbJSrgAFXmjlbBjMmgspObULo/wxMHdTbtPBf11HRHTkNIo3qyO4UADL2
WpoGhgT/FaxxBo2UBcnYVaP+jjRE0NYT973MCbVAAxtNVU6bEBR0z+LWniACzupm
+qh23SL43uW5A3iSw/BuU1E9p7BOe8oDNKU6gXlojKyLP/gC7j8AePO3ir+KZui8
b8X4iYn/67SbzZFhwxn3chkW4JYhQ4AImW1An2Q1+DMoZL7zRtSqQ3g9ZqRIMzQN
gJ+kQXe7QtT/u6m1MrtjE3gAEVpL334rTIxy9hpKZIkB86t2ZA3JX8CLsbCa13sA
z1XCoONX+6a1ekmXuAOI+t3c1sNbN2AtFi4cJovTAO1xh6OI4QnK+MNQKpTjt/E4
ydHl0rrurXsZummj9QBnkX4pqY7cDLHhdMKpbjDwg7jVLl783nTc9wYptQEPi5sw
83g9EMgKV0ARIiVUa/qlAgMBAAGjPjA8MAwGA1UdEwQFMAMBAf8wEQYJYIZIAYb4
QgEBBAQDAgAHMBkGCWCGSAGG+EIBDQQMFgpTVlMgTGFiIENBMA0GCSqGSIb3DQEB
CwUAA4ICAQAIT3O8oL2L6j/7Kk9VdcouuaBsN9o2pNEk3KXeZ8ykarNoxa87sFYr
AwXIwfAtk8uEHfnWu1QcZ3LkEJM9rHVCZuKsYd3D6qojo54HTpxRLgo5oKOdGayi
iSEkSSX9qyfLfINHR2JSVqJU6jLsy86X7q7RmIPMS7XfHzuddFNI4YDoXRX67X+v
O+ja6zTQqjO6lqJhmrSkyFbYf/ZTpe4d1OzJsZjNsNOr8bF9nOA/7qNZLp3Z3cpU
PUOKdbiSvRqnPw3e8TfITVmAzcx8COI2SrYFMSUazolVBvDy+xRKxyAtMbneGz6n
YdykCimThCKoKwp/pWpYBEqIEOf5ay1PKURO/8aj/B7aluJapXkmnj5qPeGhNOpB
Q9r14reov4so2EspkXS7CrH9yGfpIyTprokz1UvZBZ8vloI7YZmjFmem+5rT6Gnk
eU/lX7nV61SYG5W5K+I8uaKuyBHOMn7Amy3DYL5c5GJBqxpSZERbLXV+Q1tIgRU8
8ggzlPOdsS/i6Lo7ypYXOeB9HgVDCkzQsLXQuHGj/2WsgPgdRcjkvnyURk4Jx+Ib
xDrmo7e0XPpSW4l72a6Kl8CR3U2Cr4wsuvndPEq/qd2NRSBWffF0XE/AJHQG7STT
HaXLU9r2Ko6O3oecu8ysGTwLlIt/9T1/FOb0xZRugWcpJrVoTgDGuA==
-----END CERTIFICATE-----


quit


   Serial Number : AB:CD:87:FD:41:12:C3:FE:FD:87:D5
   Subject:
      CN=SVS LabCA,OU=SVS,O=Cisco,L=Raleigh,ST=North Carolina,C=US
   Issued By :
      CN=SVS LabCA,OU=SVS,O=Cisco,L=Raleigh,ST=North Carolina,C=US
```

```
   Validity Start : 17:05:00 UTC Mon Apr 28 2025
   Validity End : 17:05:00 UTC Sat Apr 28 2035
RP/0/RP0/CPU0:May 9 14:52:20.961 UTC: pki_cmd[66362]: %SECURITY-PKI-6-LOG_INFO_DETAIL : Fingerprint: 2A
   SHA1 Fingerprint:
      0EB181E95A3ED7803BC5A8059A854A95C83AC737
Do you accept this certificate? [yes/no]:
```

yes

```
RP/0/RP0/CPU0:May 9 14:52:23.437 UTC: cepki[153]: %SECURITY-CEPKI-6-INFO : certificate database updated
```



ملاحظة: إذا كان لديك نظام مرجع مصدق تابع، تحتاج الاستيراد كل من شهادات المرجع المصدق الجذر وشهادات المرجع المصدق الفرعية. أستخدم الأمر نفسه مع المرجع المصدق الفرعي في الأعلى والمصدر في الأسفل.

الخطوة 4. إنشاء طلب توقيع الشهادة (CSR).

<#root>

```
RP/0/RP0/CPU0:BRC-8201-1#
```

crypto ca enroll svs

```
Fri May 9 14:52:44.030 UTC
% 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: C=US,ST=NC,L=RTP,O=Cisco,OU=SVS,CN=10.225.253.167
% The subject name in the certificate will include: BRC-8201-1.svs.lab
% Include the router serial number in the subject name? [yes/no]:
```

yes

```
% The serial number in the certificate will be: 4090843b
% Include an IP address in the subject name? [yes/no]:
```

yes

```
Enter IP Address[]
```

10.225.253.167

```
Fingerprint: 36354532 38324335 43434136 42333545
Display Certificate Request to terminal? [yes/no]:
```

yes

```
Certificate Request follows:

-----BEGIN CERTIFICATE REQUEST-----
MIIDQTCCAikCAQAwcjELMAkGA1UEBhMCVVMxCzAJBgNVBAgMAk5DMQwwCgYDVQQH
DANSVFAxDjAMBgNVBAoMBUNpc2NvMQwwCgYDVQQLDANTVlMxFzAVBgNVBAMMDjEw
LjIyNS4yNTMuMTY3MREwDwYDVQQFEwg0MDkwODQzYjCCASIwDQYJKoZIhvcNAQEB
BQADggEPADCCAQoCggEBALwx9w4DnTtrloDH9iOZxPvEDARwN0t4WrPEjaQclZUA
6ax6Cxq/0JlQiUf2+eQv+4rKZqAZ1xDhiaiMGqETnO0LKpwmtx10IqXL7UYMHHwF
9vRII52zomkWA8a63Wx66UkExaXoeXaf5HkLoqDu68X83U7LPvMe1sMwvmq7Rmy2
DAu30HB/JfYlQCHmTVFz3M5fBt86xx4t1nxTFU/4lRWMC73UdL5YdKJLjMpBT2tN
E3piZ+kL4p1c9U4RIBkU8/G4drzFbGvHCIkWkwI0cb1X2HgtbVQdCXTAwJDmr2O9
zd2ZCa5enTbOKHbNXuHjpy0k8MewKOV2muwxVcQbej8CAwEAAaCBiTAYBgkqhkiG
9w0BCQcxCxMJQzFzY28uMTIzMG0GCSqGSIb3DQEJDjFgMF4wDgYDVR0PAQH/BAQD
AgWgMCAGA1UdJQEB/wQWMBQGCCsGAQUFBwMBBggrBgEFBQcDAjAJBgNVHRMEAjAA
MB8GA1UdEQQYMBaCDjEwLjIyNS4yNTMuMTY3hwQK4f2nMA0GCSqGSIb3DQEBBQUA
A4IBAQBBXOeWF5ZUz7O1GFjuQHBBDgYb+3lhFOxbYm9psIWfv1uwjkKoL297tGHv
Iux7nMyrDVkSJ81i5BSTdd9FE6AbSFswjlYpO+IxkUM971Ejwg2rj+jABDR7I8SU
O6YO6mS9x2ZJYqImeq8xwIr19Hi+7tyaLe6apfTIljdgVxB+XyzOFJMckIO5US3j
T/3aw/115RcXerdrh36oMUHEepUjIx/15u9s1c7e1mxACoQE6f9OA+fdg2zYtOME
Z6VAw64cY+YF6iLbYv7c4lizO5Zj2NJbUKpeqijkFAkY/1rIxTHypzH/p2ma4zuS
46a+kLXsVHZ716ZMB3WrUzB2ZNOO
```

```
-----END CERTIFICATE REQUEST-----
---End - This line not part of the certificate request---
Redisplay enrollment request? [yes/no]:
```

no

الخطوة 5. إستيراد الشهادة الموقعة من المرجع المصدق.

<#root>

```
RP/0/RP0/CPU0:BRC-8201-1#
```

crypto ca import svs certificate

```
Fri May 9 15:00:35.426 UTC


Enter the base64/PEM encoded certificate/certificates.
Please note: for multiple certificates use only PEM.
End with a blank line or the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----
MIIE3zCCAsegAwIBAgIINL1NAUzx14UwDQYJKoZIhvcNAQELBQAwajELMAkGA1UE
BhMCVVMxFzAVBgNVBAgTDk5vcnRoIENhcm9saW5hMRAwDgYDVQQHEwdSYWxlaWdo
MQ4wDAYDVQQKEwVDaXNjbzEMMAoGA1UECxMDU1ZTMRIwEAYDVQQDEwlTVlMgTGFi
QOEwHhcNMjUwNTA5MTQ1NzAwWhcNMjYwNTA5MTQ1NzAwWjByMQswCQYDVQQGEwJV
UzELMAkGA1UECAwCTkMxDDAKBgNVBAcMA1JUUDEOMAwGA1UECgwFQ2lzY28xDDAK
BgNVBAsMA1NWUzEXMBUGA1UEAwwOMTAuMjI1LjI1My4xNjcxETAPBgNVBAUTCDQw
OTA4NDNiMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAvDH3DgOdO2uW
gMf2I5nE+8QMBHA3S3has8SNpByVlQDprHoLGr/QmVCJR/b55C/7ispmoBnXEOGJ
qIwaoROc7QsqnCa3HXQipcvtRgwcfAX29EgjnbOiaRYDxrrdbHrpSQTFpeh5dp/k
eQuioO7rxfzdTss+8x7WwzC+artGbLYMC7fQcH8l9iVAIeZNUXPczl8G3zrHHi3W
fFMVT/iVFYwLvdROvlhOokuMykFPaOOTemJn6QvinVz1ThEgGRTz8bh2vMVsa8cI
iRaTAjRxvVfYeC1tVBOJdMDAkOavY73N3ZkJrl6dNs4ods1e4eOnLSTwx7Ao5Xaa
7DFVxBt6PwIDAQABo4GAMH4wHgYJYIZIAYb4QgENBBEWD3hjYSBjZXJOaWZpY2F0
ZTAOBgNVHQ8BAf8EBAMCBaAwIAYDVR0lAQH/BBYwFAYIKwYBBQUHAwEGCCsGAQUF
BwMCMAkGA1UdEwQCMAAwHwYDVR0RBBgwFoIOMTAuMjI1LjI1My4xNjeHBArh/acw
DQYJKoZIhvcNAQELBQADggIBAARpS5bEck+ojO121O6WxedDQ8VduObBtrnOH+Nt
94EA1co7HEe4USf1FiASAX7rNveLpY3ICmLh+tQZYTZrQ93tb9mMTZg7exqN89ZU
VlXoB2UOTri5Kl0/+izEGgyNq42/ytAP8YOO7HR/2jf7gfhoRvwcR5QNOEHv4o6l
Zma5Xio1sBbkA7JB2mpzzZg4ZjsyV8lRGXxxgyt1mwNmb7EiAc8lodRcgyp7FNh3
F/k9cMMMr5lM4Ysvoltx1k9AeLjzb2syv5/fG6QuOZdWwTaaQhOY2h/cVDiV97wg
ODlmEfdSv6QrxQSujZr22RzVyKKHltuiV2B74pthUuGRBtfHS5XFy7uTTbfGX8M6
ZJw8rX1SADr8tDplrf1ZIrPmv3ZPP7woTB22yWzydOuse+5IalbOw7OtwN4t/IIw
8CJu6HfnDXLDPZOjsC8steffrSlopwGccp3j6aZKPFz+I/Purb44a9WxEWa2TA7H
+rloynBcGMetOHxVLnptlsC7Q4mN/MDXeGyW+OTNCirNEG/gqcu+dn9EnNKkE2WV
oF537Ow+uNHoK8Bdt8mqadUT4OoUSqY8ArVOBomO5tzbemreVPmQAZ/IahZ7TqKo
3dGNonTAfFTESM1iujQ81iRKsikDHySnwcCM2nilCKZrhVq5IB8NK6jKRJZOeQAX
vMt1
-----END CERTIFICATE-----
```

quit

```
Serial Number : C2:F4:AB:34:02:D2:76:74:65:34:FE:D5
Subject:
serialNumber=4090843b,CN=10.225.253.167,OU=SVS,O=Cisco,L=RTP,ST=NC,C=US
Issued By :
CN=SVS LabCA,OU=SVS,O=Cisco,L=Raleigh,ST=North Carolina,C=US
```

```
Validity Start : 14:57:00 UTC Fri May 09 2025
Validity End : 14:57:00 UTC Sat May 09 2026
SHA1 Fingerprint:
21E4DA0B02181D08B6E51F0CC754BCE5B815C792
```

تحقق من تسجيل شهادة هوية الموجه.

<#root>

```
RP/0/RP0/CPU0:BRC-8201-1#
```

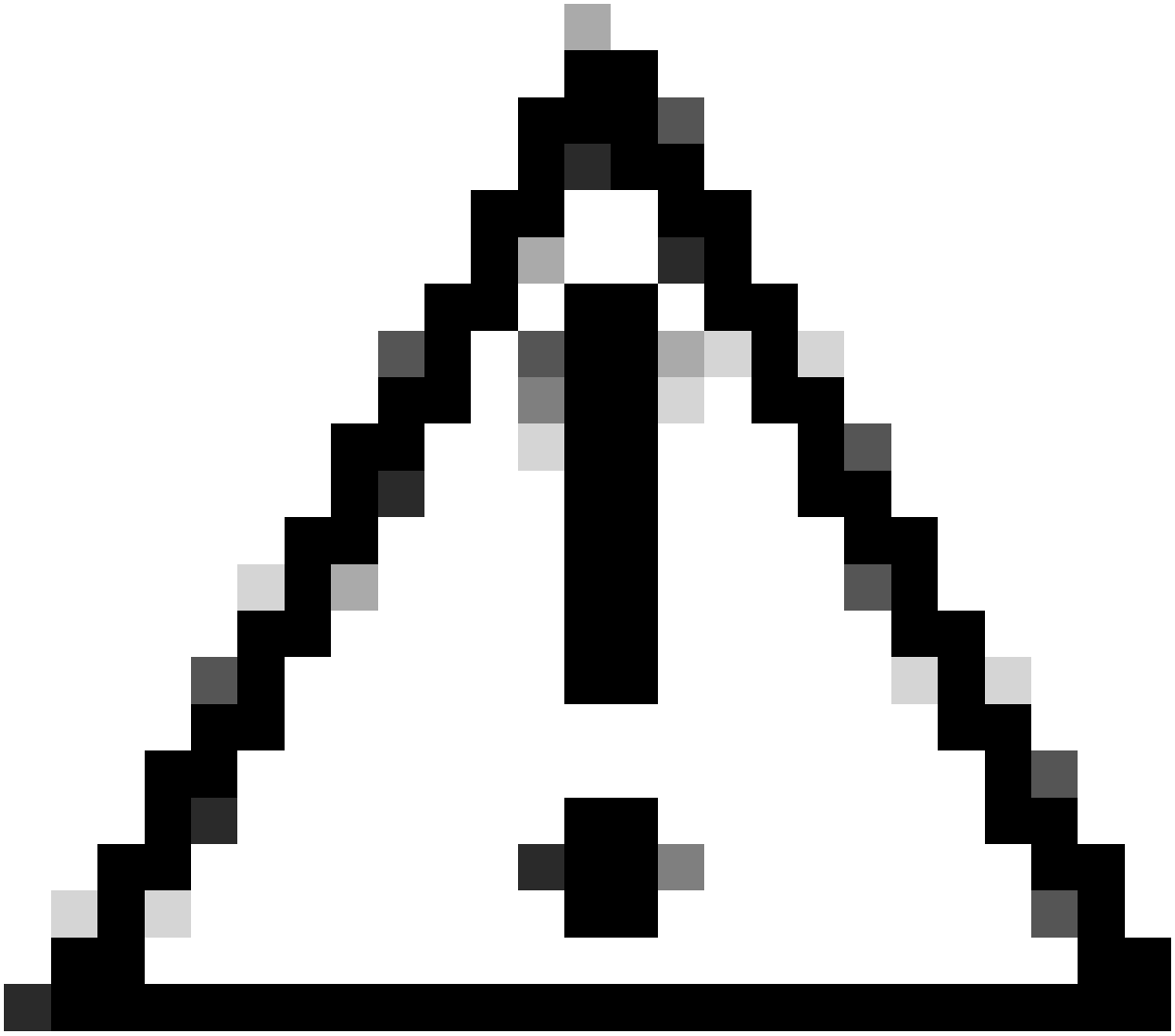
show crypto ca trustpoint svs detail

```
Trustpoint        :svs-new
================================================================
KeyPair Label: the_default
CRL:optional
enrollment: terminal
subject name: C=US,ST=NC,L=RTP,O=Cisco,OU=SVS,CN=brc-8201-1.svs.lab

RP/0/RP0/CPU0:BRC-8201-1#
```

show crypto ca certificates svs

```
Wed May 14 14:55:58.173 UTC

Trustpoint       : svs-new
================================================
CA certificate
  Serial Number  : 20:01:20:1F:B6:9D:C3:FE:43:78:FF:64
  Subject:
        CN=SVS LabCA,OU=SVS,O=Cisco,L=Raleigh,ST=North Carolina,C=US
  Issued By      :
        CN=SVS LabCA,OU=SVS,O=Cisco,L=Raleigh,ST=North Carolina,C=US
  Validity Start : 17:05:00 UTC Mon Apr 28 2025
  Validity End   : 17:05:00 UTC Sat Apr 28 2035
  SHA1 Fingerprint:
         0EB181E95A3ED7803BC5A8059A854A95C83AC737
Router certificate
  Key usage      : General Purpose
  Status         : Available
  Serial Number  : FD:AC:20:1F:B6:9D:C3:FE:98:43:ED
  Subject:
        serialNumber=4090843b,CN=brc-8201-1.svs.lab,OU=SVS,O=Cisco,L=RTP,ST=NC,C=US
  Issued By      :
        CN=SVS LabCA,OU=SVS,O=Cisco,L=Raleigh,ST=North Carolina,C=US
  Validity Start : 19:59:00 UTC Fri May 09 2025
  Validity End   : 19:59:00 UTC Sat May 09 2026
  SHA1 Fingerprint:
         AC17E4772D909470F753BDBFA463F2DF522CC2A6
Associated Trustpoint: svs
```

تكوين TACACS & AAA باستخدام TLS



تحذير: قم بإجراء تغييرات التكوين من خلال وحدة التحكم باستخدام بيانات الاعتماد المحلية.

الخطوة 1. قم بتكوين خادم TACACS+.

```
tacacs source-interface MgmtEth0/RP0/CPU0/0 vrf mgmt
tacacs-server host 10.225.253.209 port 49
  key 7 072C705F4D0648574453

aaa group server tacacs+ tacacs2
 server 10.225.253.209
 vrf mgmt
```

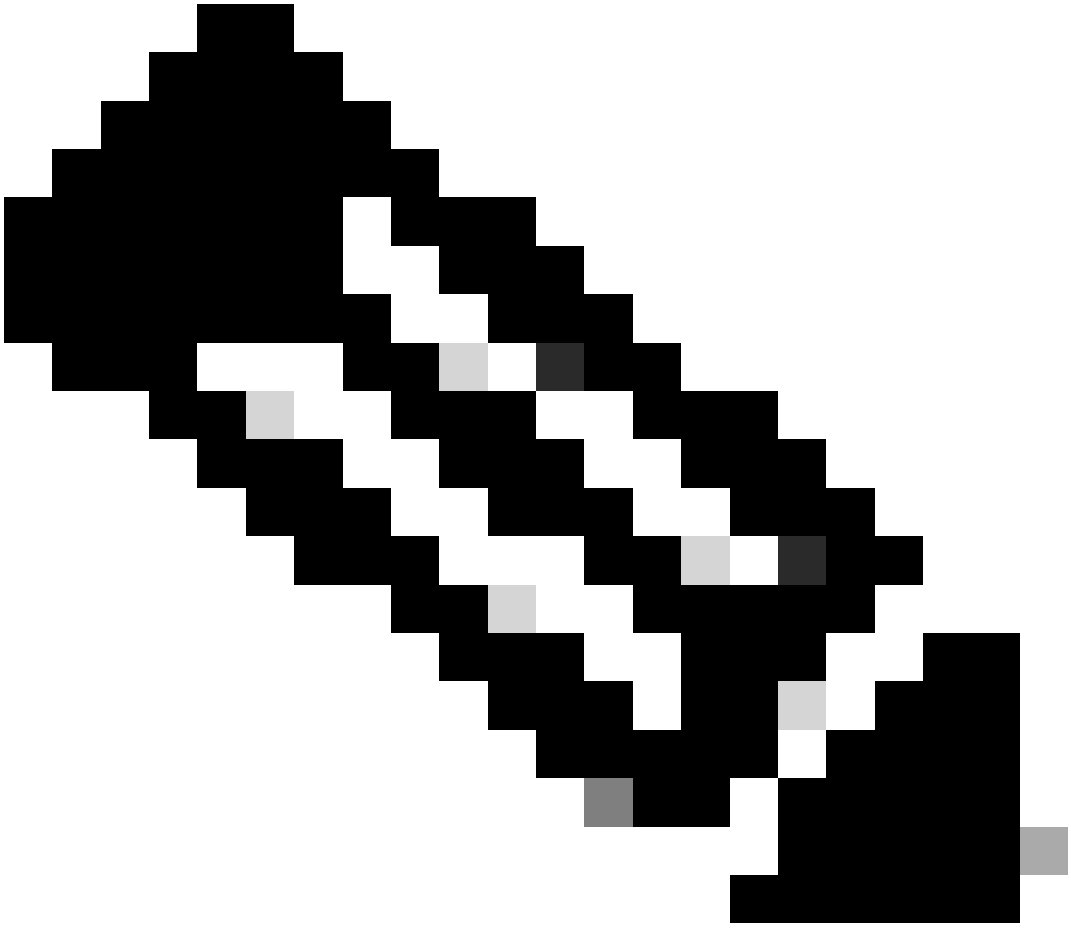
الخطوة 2. تكوين مجموعة AAA.

```
aaa group server tacacs+ tac_tls_sc
 vrf mgmt
 server-private 10.225.253.209 port 6049
  timeout 10
  tls
   trustpoint svs
  !
  single-connection
```

الخطوة 2. تكوين AAA.

```
aaa accounting exec default start-stop group tac_tls_sc
aaa accounting system default start-stop group tac_tls_sc
aaa accounting network default start-stop group tac_tls_sc
aaa accounting commands default stop-only group tac_tls_sc
aaa authorization exec default group tac_tls_sc local
aaa authorization commands default group tac_tls_sc none
aaa authentication login default group tac_tls_sc local
```

تجديد الشهادة



ملاحظة: لا يلزم إزالة نقطة الثقة من تكوين TACACS+ أثناء التجديد.

الخطوة 1. تحقق من تواريخ صلاحية الشهادة الحالية.

```
RP/0/RP0/CPU0:BRC-8201-1#show crypto ca certificates svs-new
Thu Aug 14 15:13:37.465 UTC

Trustpoint : svs-new
================================================
CA certificate
  Serial Number : 30:A2:10:14:C9:5E:B0:E0:07:CE:0A:24:16:69:90:ED:D1:34:B5:9B
  Subject:
        CN=Test Drive Sub CA G1,OU=Certification Authorities,O=Keyfactor Command,C=US
  Issued By :
        CN=Test Drive Root CA G1,OU=Certification Authorities,O=Keyfactor Command,C=US
  Validity Start : 22:13:17 UTC Thu Jun 26 2025
  Validity End : 22:13:16 UTC Tue Jun 25 2030

  CRL Distribution Point
```

```
http://svs.lab:8080/ejbca/publicweb/crls/search.cgi?iHash=m9uBlQsZDYy6wxomiFWB5Gv0AZM

  SHA1 Fingerprint:
        EA8FB276563B927FCAF0174D9FD1C58F3E8B5FF2
Trusted Certificate Chain
  Serial Number : 1F:A6:6E:2E:F8:AB:CE:B4:9C:B8:07:5A:9F:2B:32:02:B4:56:5C:96
  Subject:
        CN=Test Drive Root CA G1,OU=Certification Authorities,O=Keyfactor Command,C=US
  Issued By :
        CN=Test Drive Root CA G1,OU=Certification Authorities,O=Keyfactor Command,C=US
  Validity Start : 22:13:17 UTC Thu Jun 26 2025
  Validity End : 22:13:16 UTC Sun Jun 24 2035
  SHA1 Fingerprint:
        E225647FF9BDA176D2998D5A3A9770270F37D2A7
Router certificate
  Key usage : General Purpose
  Status : Available
  Serial Number : 7A:13:EB:C0:6A:8D:66:68:09:0B:32:C7:0C:D8:05:BD:81:72:9B:4E
  Subject:
        CN=brc-8201-1.svs.lab,OU=SVS,O=Cisco,L=RTP,ST=NC,C=US
  Issued By :
        CN=Test Drive Sub CA G1,OU=Certification Authorities,O=Keyfactor Command,C=US
  Validity Start : 16:38:36 UTC Wed Jul 30 2025
  Validity End : 16:38:35 UTC Thu Jul 30 2026
  CRL Distribution Point

http://svs.lab:8080/ejbca/publicweb/crls/search.cgi?iHash=X4as2q+6I9Bd4QglQa8g1xoH8GY
  SHA1 Fingerprint:
        B562F3CF507CE7F97893F28BC896794CFF6995C1
Associated Trustpoint: svs-new
```

الخطوة 2. حذف شهادة TrustPoint الموجودة.

```
RP/0/RP0/CPU0:BRC-8201-1#clear crypto ca certificates KF_TP
Thu Aug 14 15:25:26.286 UTC
certificates cleared for trustpoint KF_TP
RP/0/RP0/CPU0:Aug 14 15:25:26.577 UTC: cepki[382]: %SECURITY-CEPKI-6-INFO : certificate database update
RP/0/RP0/CPU0:BRC-8201-1#
RP/0/RP0/CPU0:BRC-8201-1#
RP/0/RP0/CPU0:BRC-8201-1#show crypto ca certificates KF_TP
Thu Aug 14 15:25:37.270 UTC
RP/0/RP0/CPU0:BRC-8201-1#
```

الخطوة 3. إعادة مصادقة نقطة الثقة وتسجيلها كما هو موضح في الخطوات تحت تكوين نقطة الثقة.

الخطوة 4. تأكد من تحديث تواريخ صلاحية الشهادة.

```
RP/0/RP0/CPU0:BRC-8201-1#show crypto ca certificates KF_TP
Thu Aug 14 15:31:28.309 UTC

Trustpoint : KF_TP
==================================================
```

```
CA certificate
  Serial Number : 30:A2:10:14:C9:5E:B0:E0:07:CE:0A:24:16:69:90:ED:D1:34:B5:9B
  Subject:
CN=Test Drive Sub CA G1,OU=Certification Authorities,O=Keyfactor Command,C=US
  Issued By :
        CN=Test Drive Root CA G1,OU=Certification Authorities,O=Keyfactor Command,C=US
  Validity Start : 22:13:17 UTC Thu Jun 26 2025
  Validity End : 22:13:16 UTC Tue Jun 25 2030

  CRL Distribution Point

http://svs.lab:8080/ejbca/publicweb/crls/search.cgi?iHash=m9uBlQsZDYy6wxomiFWB5Gv0AZM
  SHA1 Fingerprint:
        EA8FB276563B927FCAF0174D9FD1C58F3E8B5FF2
Trusted Certificate Chain
  Serial Number : 1F:A6:6E:2E:F8:AB:CE:B4:9C:B8:07:5A:9F:2B:32:02:B4:56:5C:96
  Subject:
        CN=Test Drive Root CA G1,OU=Certification Authorities,O=Keyfactor Command,C=US
  Issued By :
        CN=Test Drive Root CA G1,OU=Certification Authorities,O=Keyfactor Command,C=US
  Validity Start : 22:13:17 UTC Thu Jun 26 2025
  Validity End : 22:13:16 UTC Sun Jun 24 2035
  SHA1 Fingerprint:
        E225647FF9BDA176D2998D5A3A9770270F37D2A7
Router certificate
  Key usage : General Purpose
  Status : Available
  Serial Number : 1F:B0:AE:44:CF:8E:24:62:83:42:2F:34:BF:D0:82:07:DF:E4:49:0B
  Subject:
        CN=brc-8201-1.svs.lab,OU=SVS,O=Cisco,L=RTP,ST=NC,C=US
  Issued By :
        CN=Test Drive Sub CA G1,OU=Certification Authorities,O=Keyfactor Command,C=US
  Validity Start : 15:17:29 UTC Thu Aug 14 2025
  Validity End : 15:17:28 UTC Fri Aug 14 2026

  CRL Distribution Point

http://svs.lab:8080/ejbca/publicweb/crls/search.cgi?iHash=X4as2q+6I9Bd4QglQa8g1xoH8GY
  SHA1 Fingerprint:
        D3CE0AEB51C5E8009F626A1A9FD633FB9AFA96DE
Associated Trustpoint: KF_TP
```

التحقق

التحقق من التكوين.

```
show crypto ca certificates [detail]
show crypto ca trustpoint detail
show tacacs details
```

تصحيح أخطاء TACACS+

```
debug tacacs tls
```

debug TLS

```
debug ssl error
debug ssl events
```

اختبر المستخدم البعيد قبل تكوين مصادقة AAA.

<#root>

test aaa group tacacs2

```
user has been authenticated
```

استكشاف الأخطاء وإصلاحها

مسح الشهادات (يؤدي هذا إلى حذف كل الشهادات المرتبطة بنقطة ثقة).

```
clear crypto ca certificate <trustpoint name>
```

إعادة تشغيل عملية TACACS (إذا لزم الأمر)

```
process restart tacacsd
```

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).