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

المحتويات

[المقدمة]
[نظرة عامة]
[استخدام هذا الدليل]
[المتطلبات الأساسية]
[المتطلبات]
[المكونات المستخدمة]
[الترخيص]
[الجزء 1 -ConfigureISE لإدارة الأجهزة]
[إنشاء طلب توقيع الشهادة لمصادقة خادم TACACS+]
[تحميل شهادة المرجع المصدق الجذر لمصادقة خادم TACACS+]
[ربط طلب توقيع الشهادة الموقع (CSR) ب ISE]
[تمكين TLS 1.3]
[تمكين إدارة الأجهزة على ISE]
[تمكين TACACS عبر TLS]
[إنشاء مجموعات أجهزة الشبكة وأجهزة الشبكة]
[متجر ConfigureIdentity]
[تكوين ملفات تعريف TACACS+]
[IOS XE_RW - ملف تعريف المسؤول]
[IOS XE_RO - ملف تعريف المشغل]
[مجموعات أوامر configureTACACS+]
[Cisco_IOS XE_RW - مجموعة أوامر المسؤول]
[Cisco_IOS XE_RO - مجموعة أوامر المشغل]
[تكوين مجموعات نهج مسؤول الجهاز]
[الجزء 2 - تكوين Cisco IOS XE ل TACACS+ عبر TLS 1.3]
[أسلوب التكوين 1 - زوج مفاتيح تم إنشاؤه بواسطة الجهاز]
[تكوين خادم TACACS+]
[تكوين TrustPoint]
[TACACS & AAA مع تكوين TLS]
[أسلوب التكوين 2 - زوج مفاتيح تم إنشاؤه بواسطة CA]
[TACACS & AAA مع تكوين TLS]
[التحقق]

المقدمة

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

نظرة عامة

يتيح بروتوكول نظام مراقبة الدخول إلى وحدة تحكم الوصول إلى المحطة الطرفية (TACACS+) [RFC8907] إمكانية المركزية للمصادقة 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 XE.
· الجزء 1 - تكوين ISE لمسؤول الجهاز
· الجزء 2 - تكوين Cisco IOS XE 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
- برنامج Cisco IOS XE، الإصدار 17.15+

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

TACACS+ على عقدة خدمة سياسة واحدة في زوج HA.

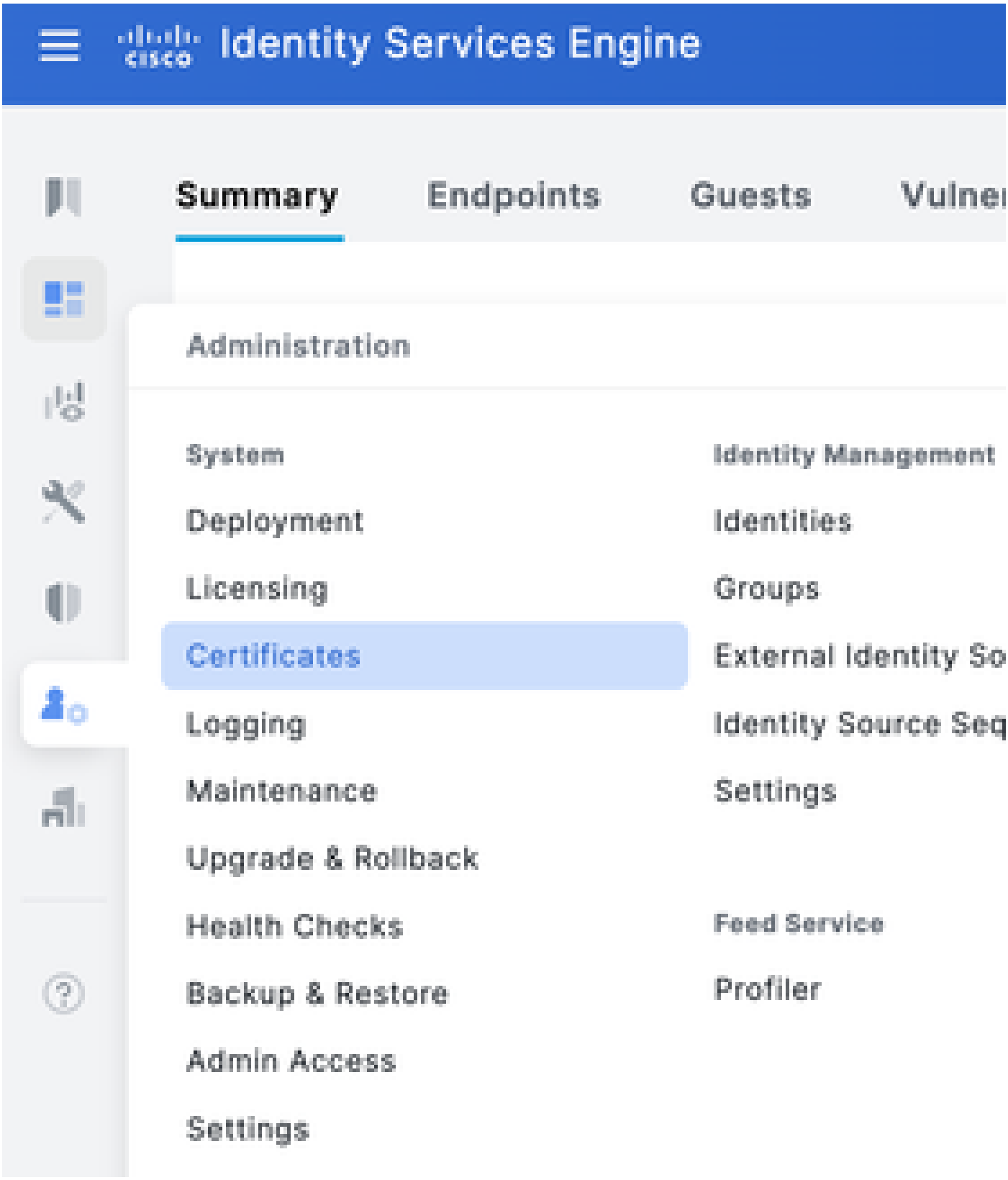
الجزء 1 - تكوين ISE لإدارة الأجهزة

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).

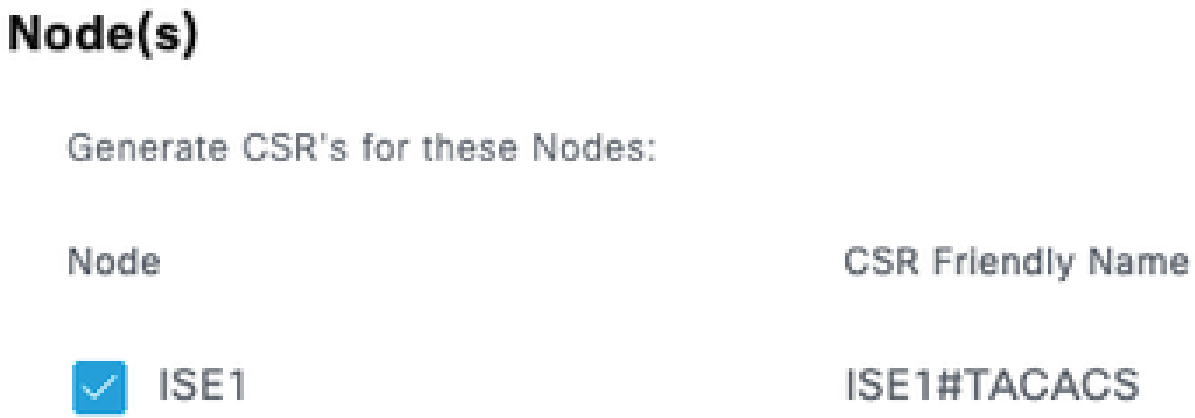
الخطوة 2.انتقل إلى الإدارة > النظام > الشهادات.



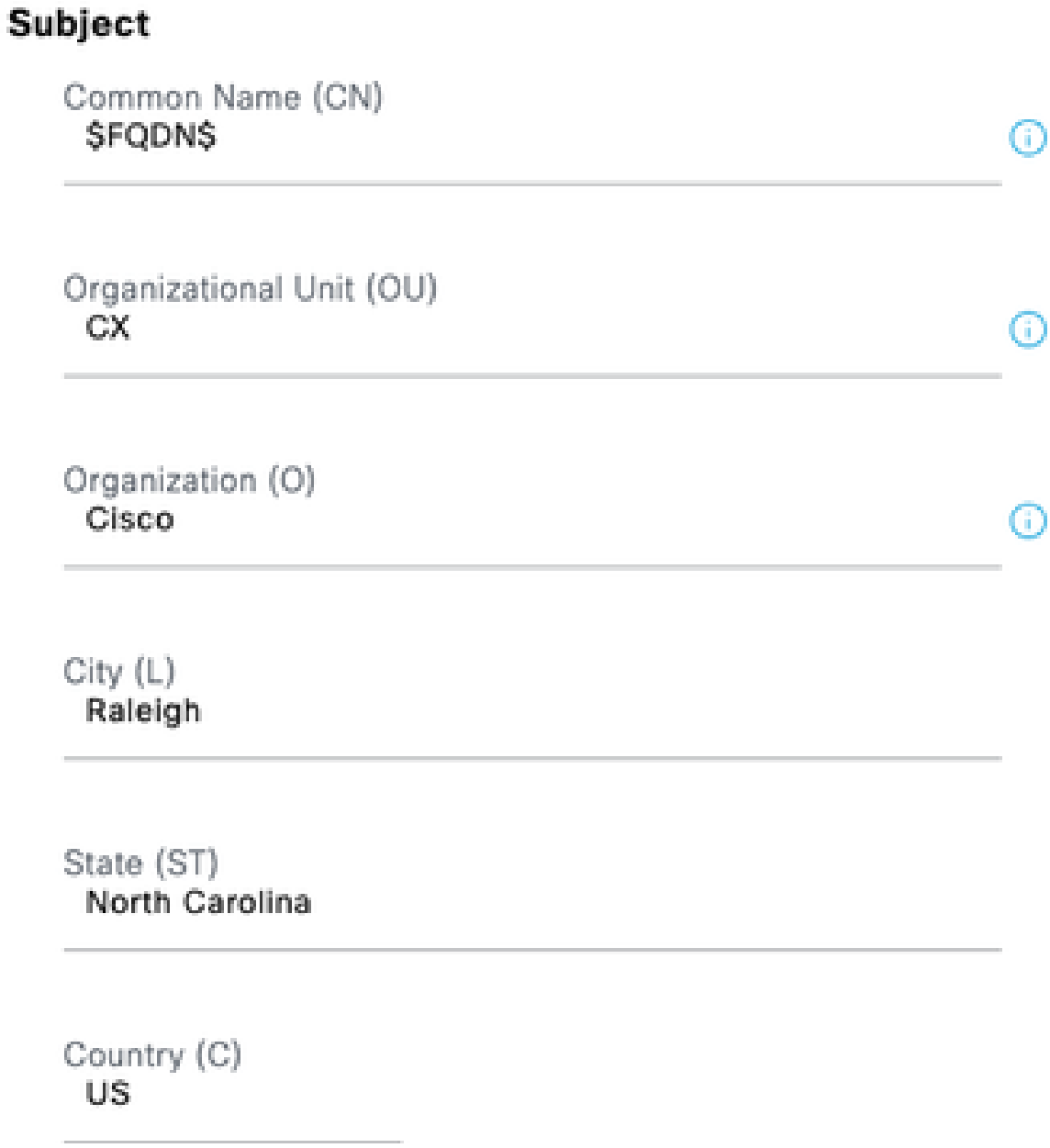
الخطوة 3. تحت طلبات توقيع الشهادة، انقر إنشاء طلب توقيع الشهادة.

الخطوة 4.حدد TACACS في الاستخدام.

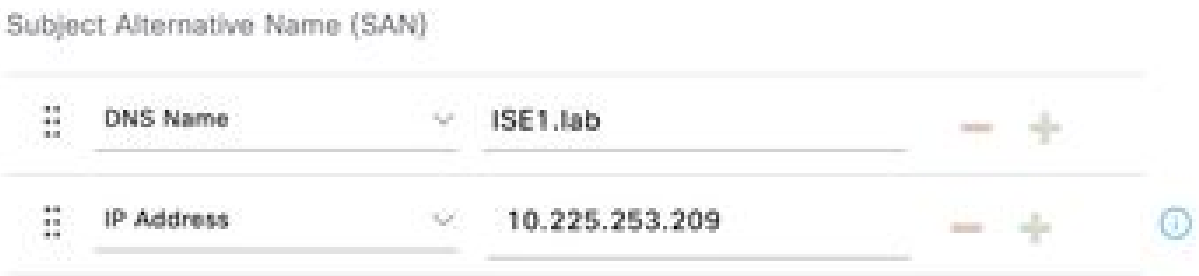
الخطوة 5.حدد شبكات PSN التي سيتم تمكين TACACS+ لها.



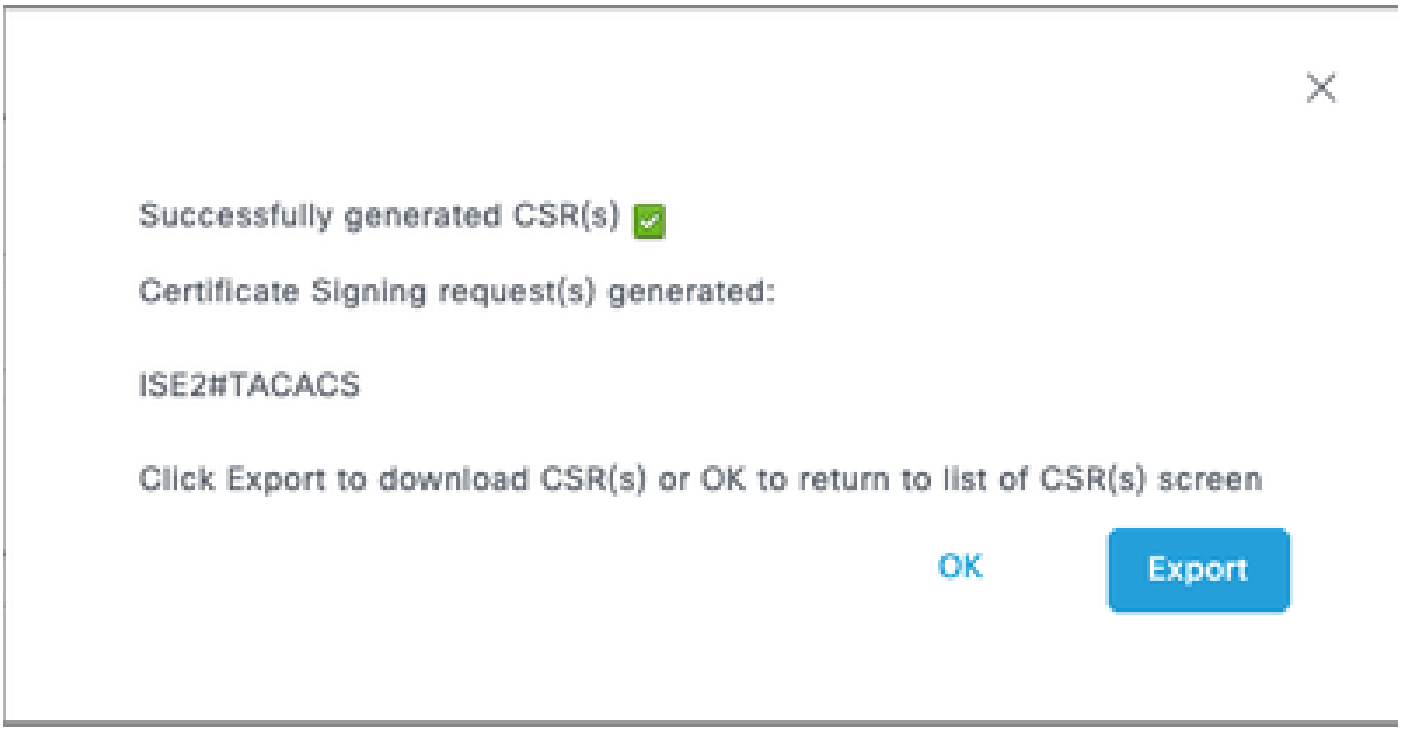
الخطوة 6. املأ حقول الموضوع بالمعلومات المناسبة.



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



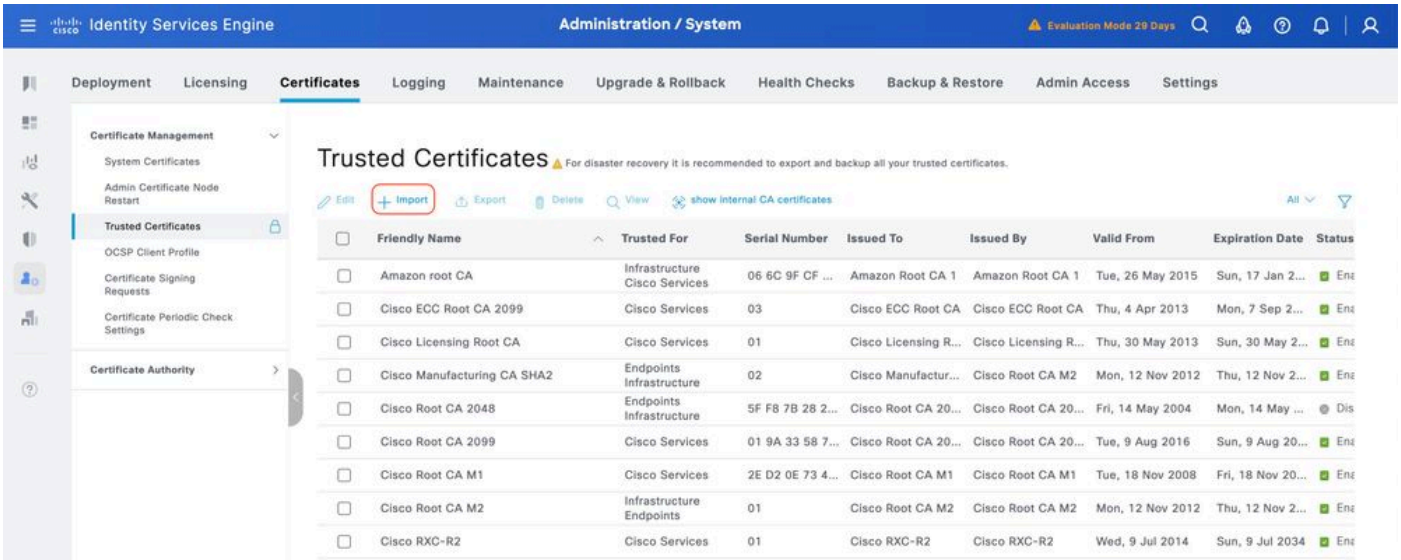
الخطوة 8.انقر فوق إنشاء ثم تصدير.



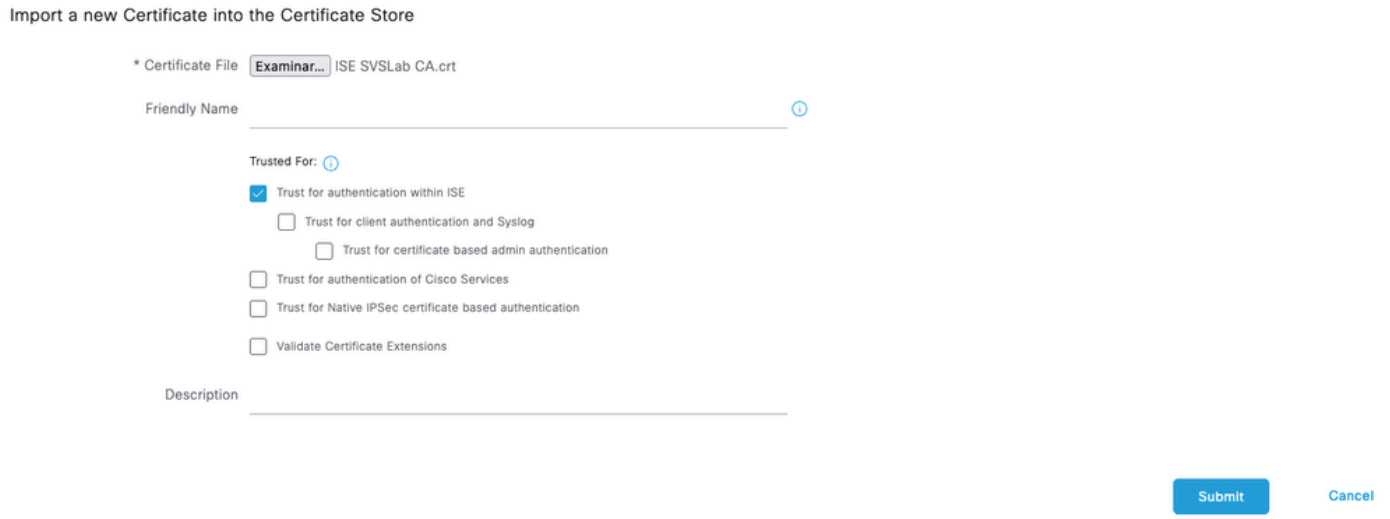
الآن، يمكنك الحصول على الشهادة (CRT) موقعة من هيئة الترخيص (CA).

تحميل شهادة المرجع المصدق الجذر لمصادقة خادم TACACS+

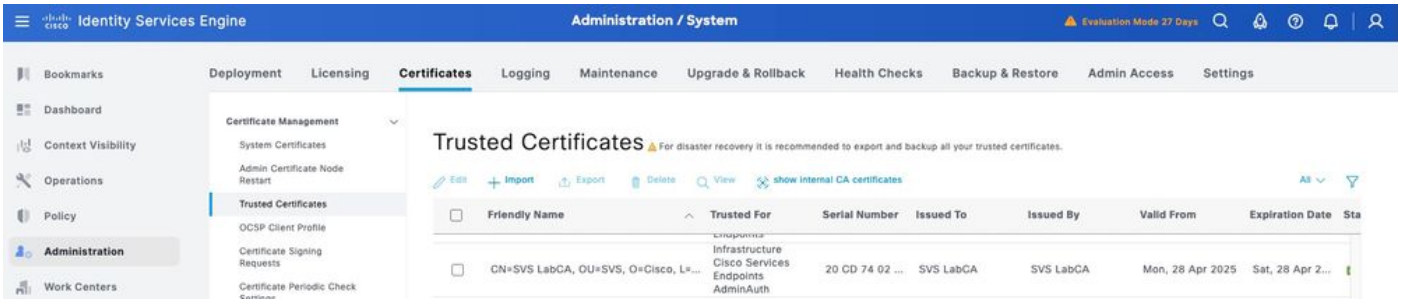
الخطوة 1. انتقل إلى الإدارة > النظام > الشهادات. تحت الترخيص المضمونة، انقر إدراج.



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



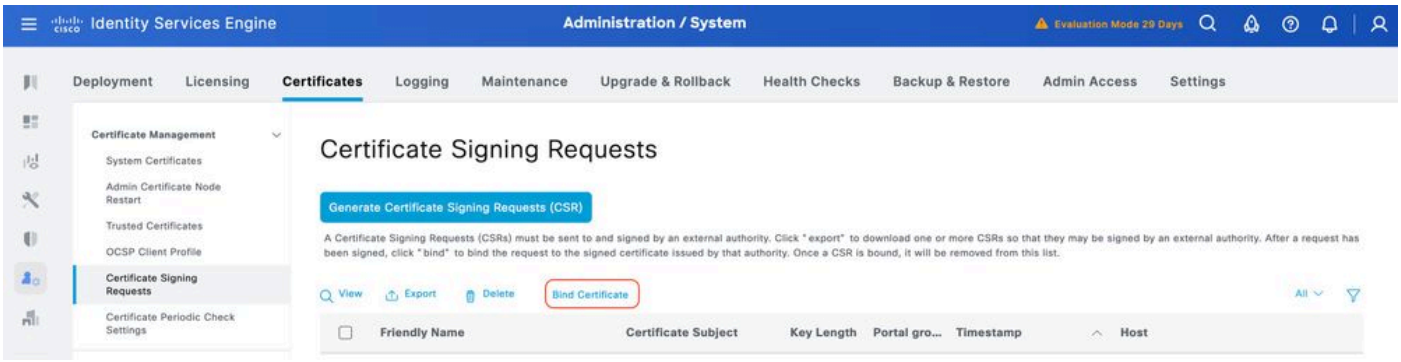
الخطوة 3. انقر فوق إرسال. يجب أن تظهر الشهادة الآن ضمن الشهادات الموثوق بها.



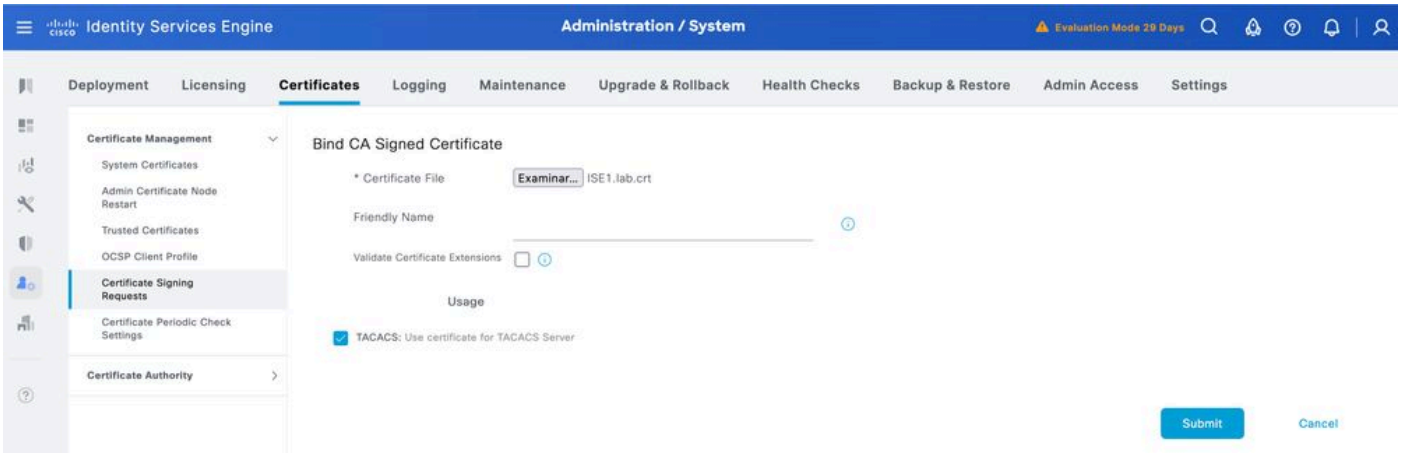
ربط طلب توقيع الشهادة الموقع (CSR) ب ISE

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.

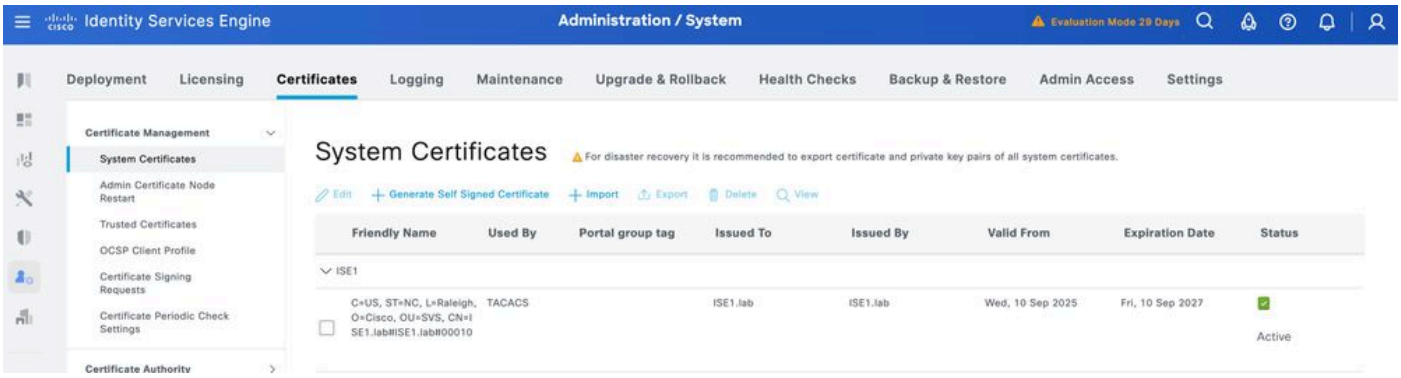


الخطوة 2.حدد الشهادة الموقعة وتأكد من أن خانة الاختيار TACACS الموجودة تحت الاستخدام ستظل محددة.



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

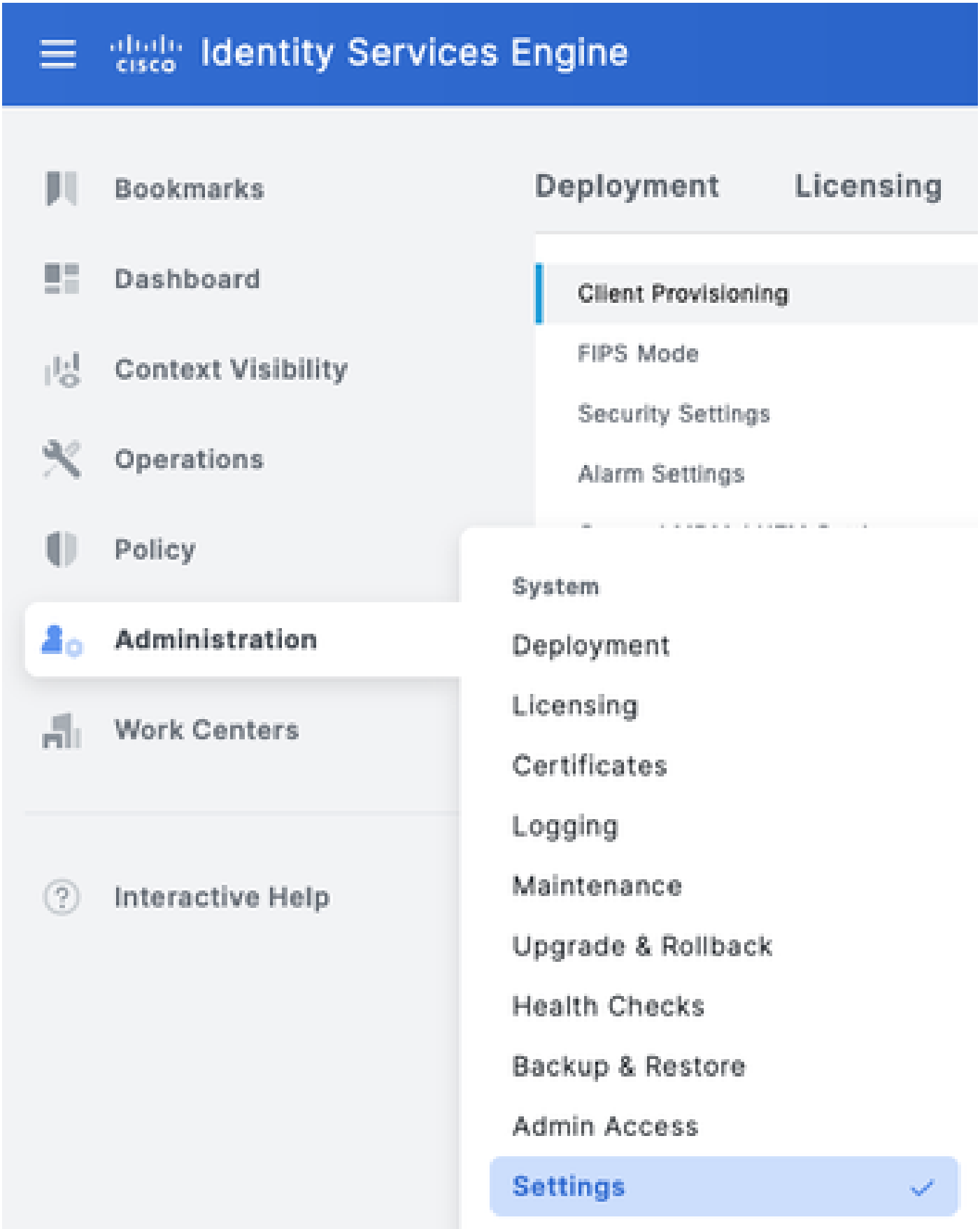
يجب تثبيت الشهادة الآن بشكل صحيح. يمكنك التحقق من ذلك ضمن شهادات النظام.



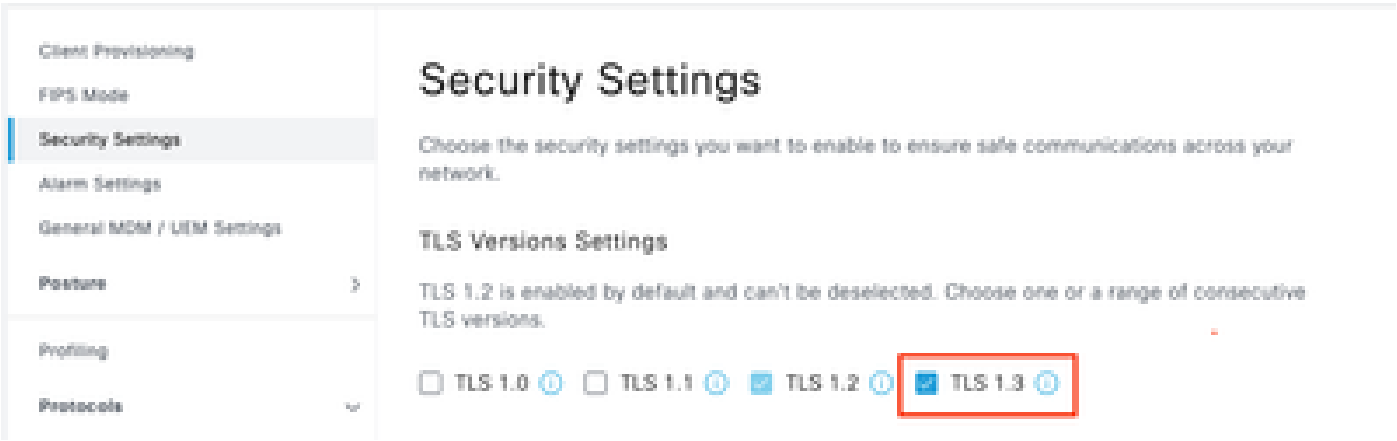
تمكين TLS 1.3

ال يتم تمكين TLS 1.3 بشكل افتراضي في ISE 3.4.x. يجب تمكينها يدويا.

الخطوة 1.انتقل إلى الإدارة > النظام > الإعدادات.



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

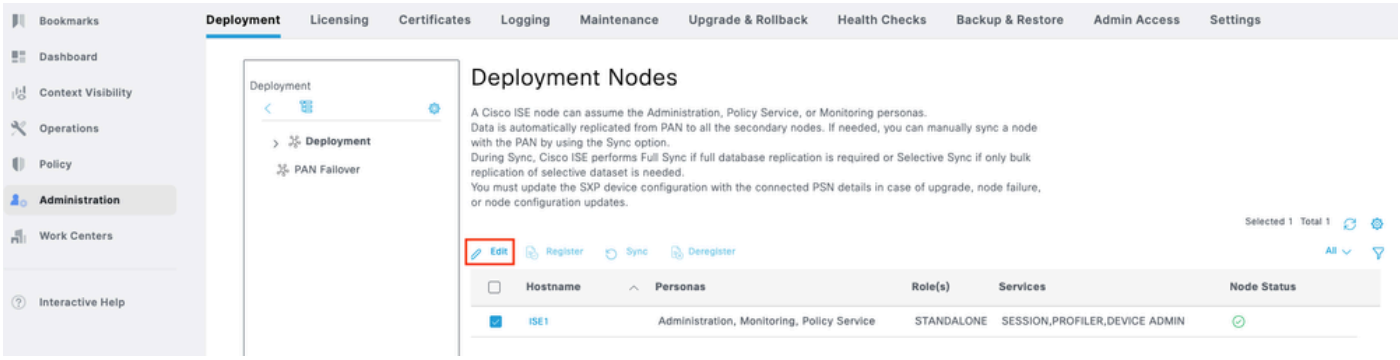


تحذير: عند تغيير إصدار TLS، تتم إعادة تشغيل خادم تطبيق Cisco ISE على جميع أجهزة النشر Cisco ISE.

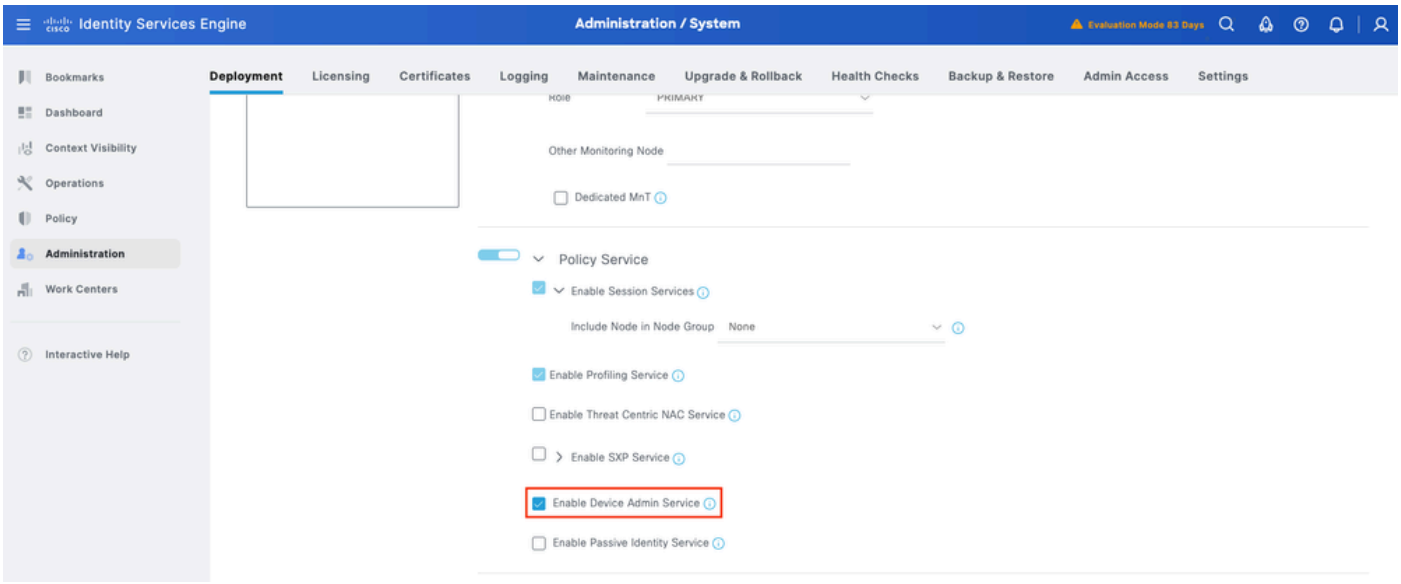
تمكين إدارة الأجهزة على ISE

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

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



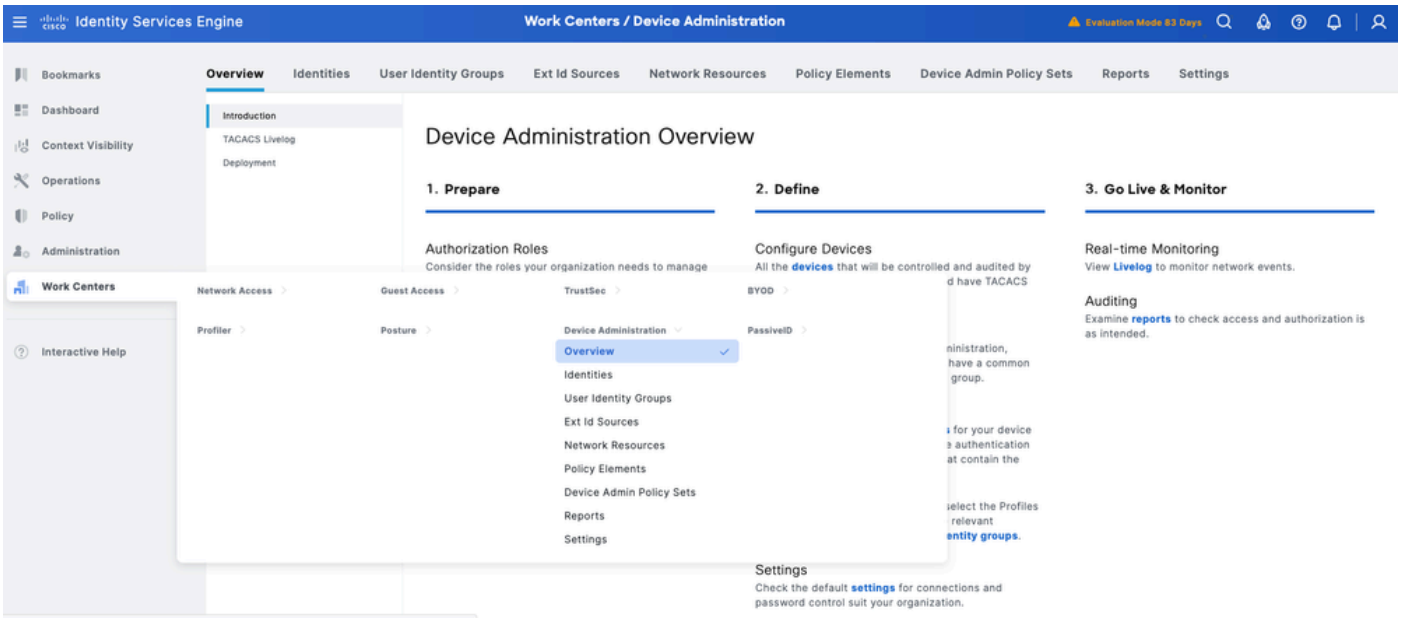
الخطوة 2.تحت GeneralSettings، قم بالتمرير إلى أسفل وحدد خانة الاختيار المجاورة ل تمكين خدمة إدارة الأجهزة.



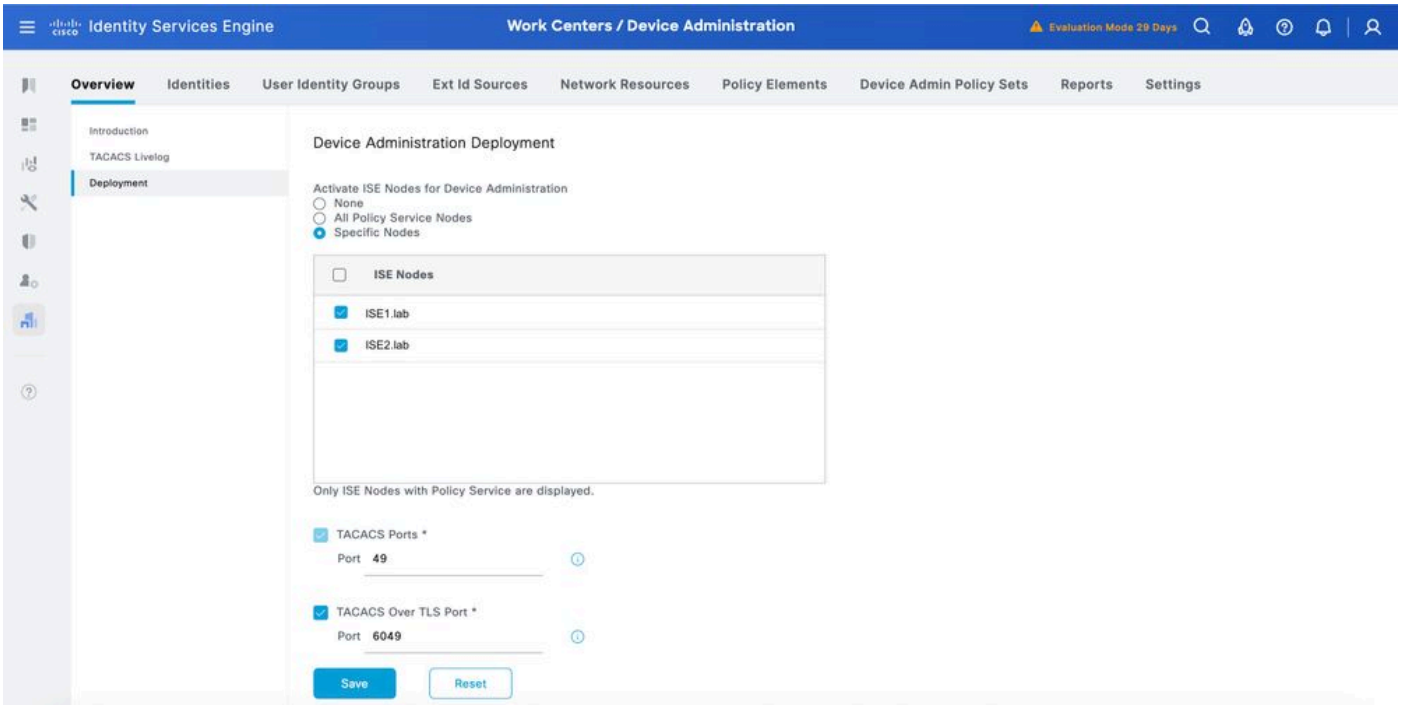
الخطوة 3. احفظ التكوين. تم تمكين "خدمة مسؤول الجهاز" الآن على ISE.

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.

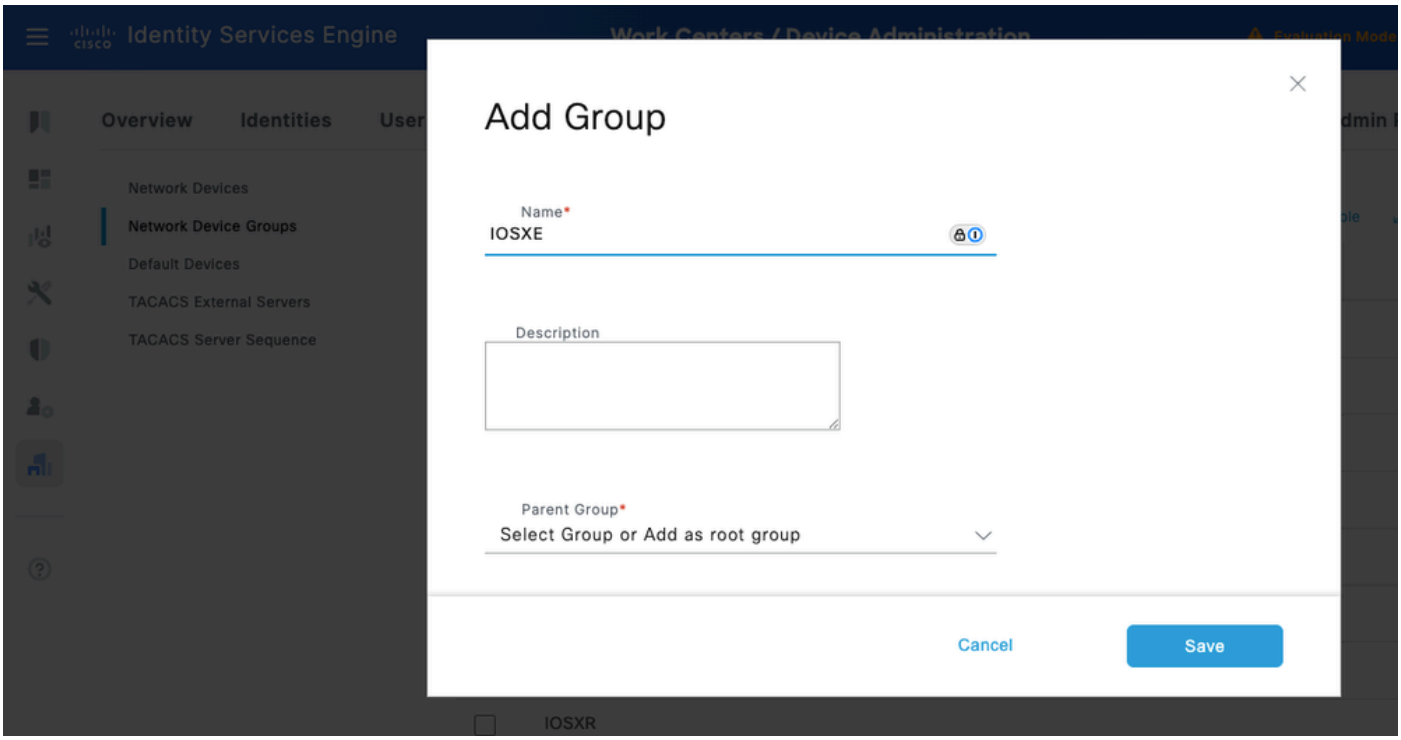


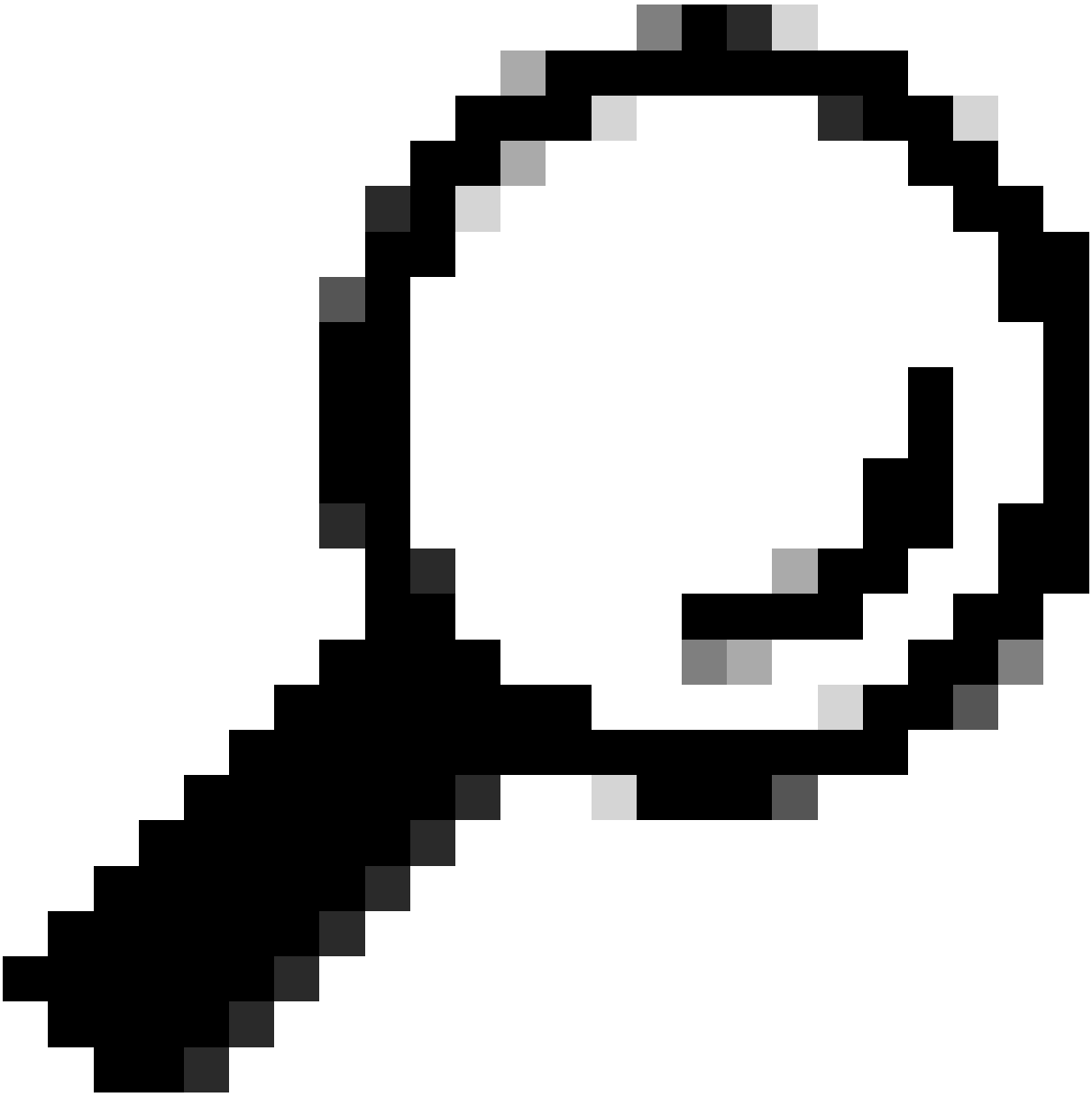
الخطوة 3.احتفظ بالمنفذ الافتراضي 6049 أو حدد منفذ TCP مختلف لـ TACACS عبر TLS، ثم انقر فوق حفظ.

إنشاء مجموعات أجهزة الشبكة وأجهزة الشبكة

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

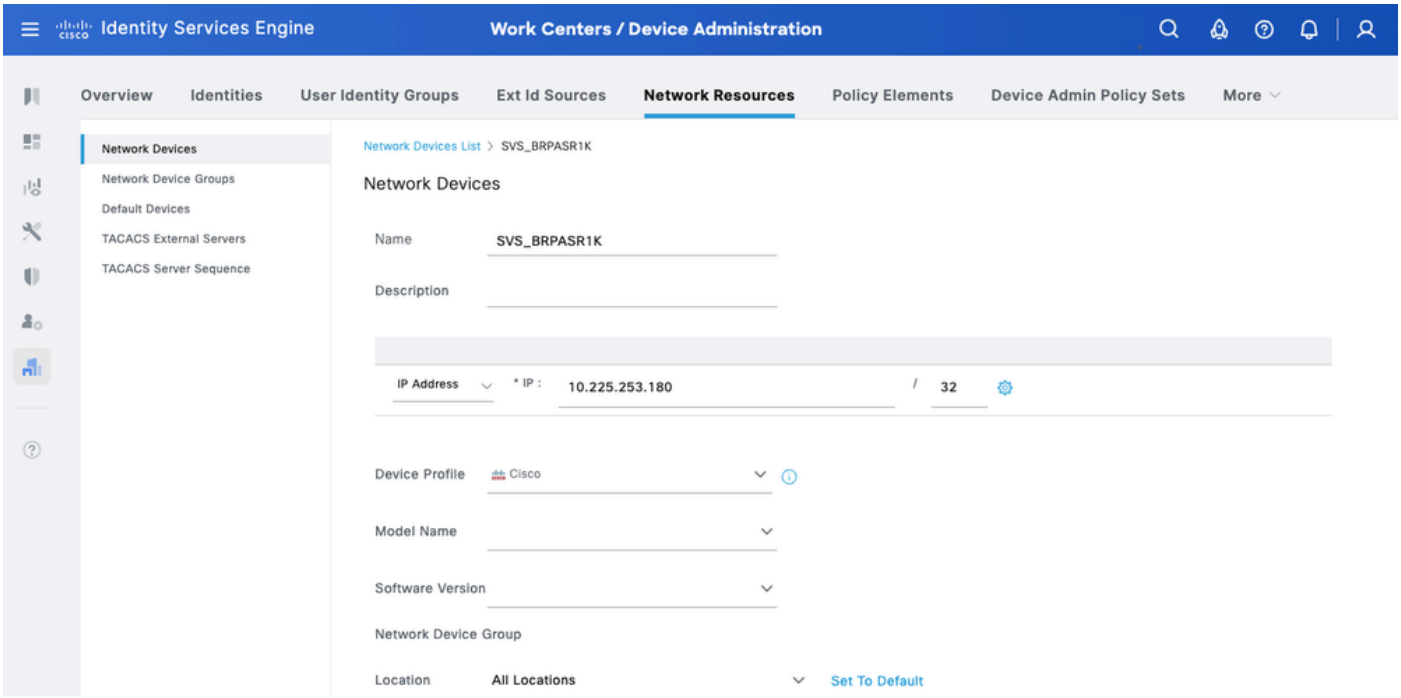
الخطوة 1. انتقل إلى مركز العمل > إدارة الجهاز > موارد الشبكة.انقر فوق مجموعات أجهزة الشبكة وأنشئ مجموعة باسم IOS XE.


Identity Services Engine
Overview
Identities
Network Devices
Network Device Groups
Default Devices
TACACS External Servers
TACACS Server Sequence
Add Group
Name*
IOSXE
Description
Parent Group*
Select Group or Add as root group
Cancel
Save
IOSXR

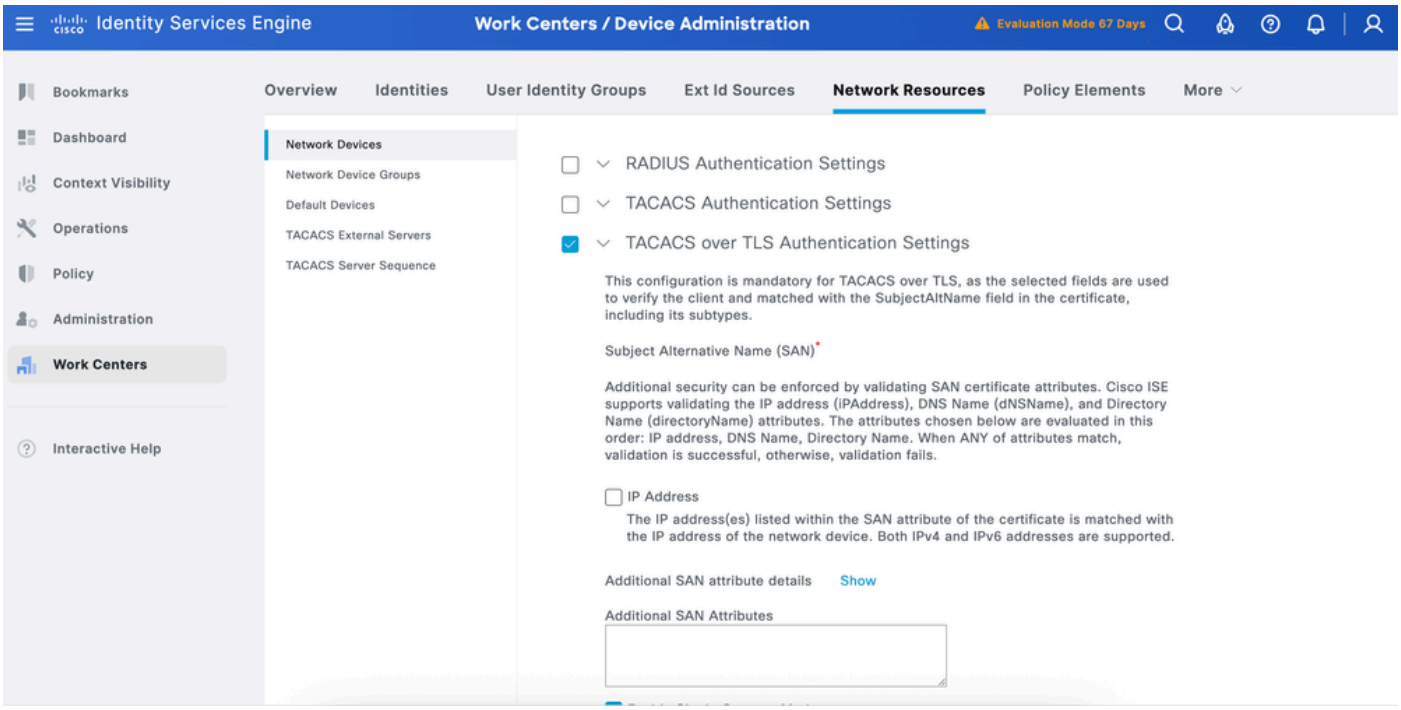


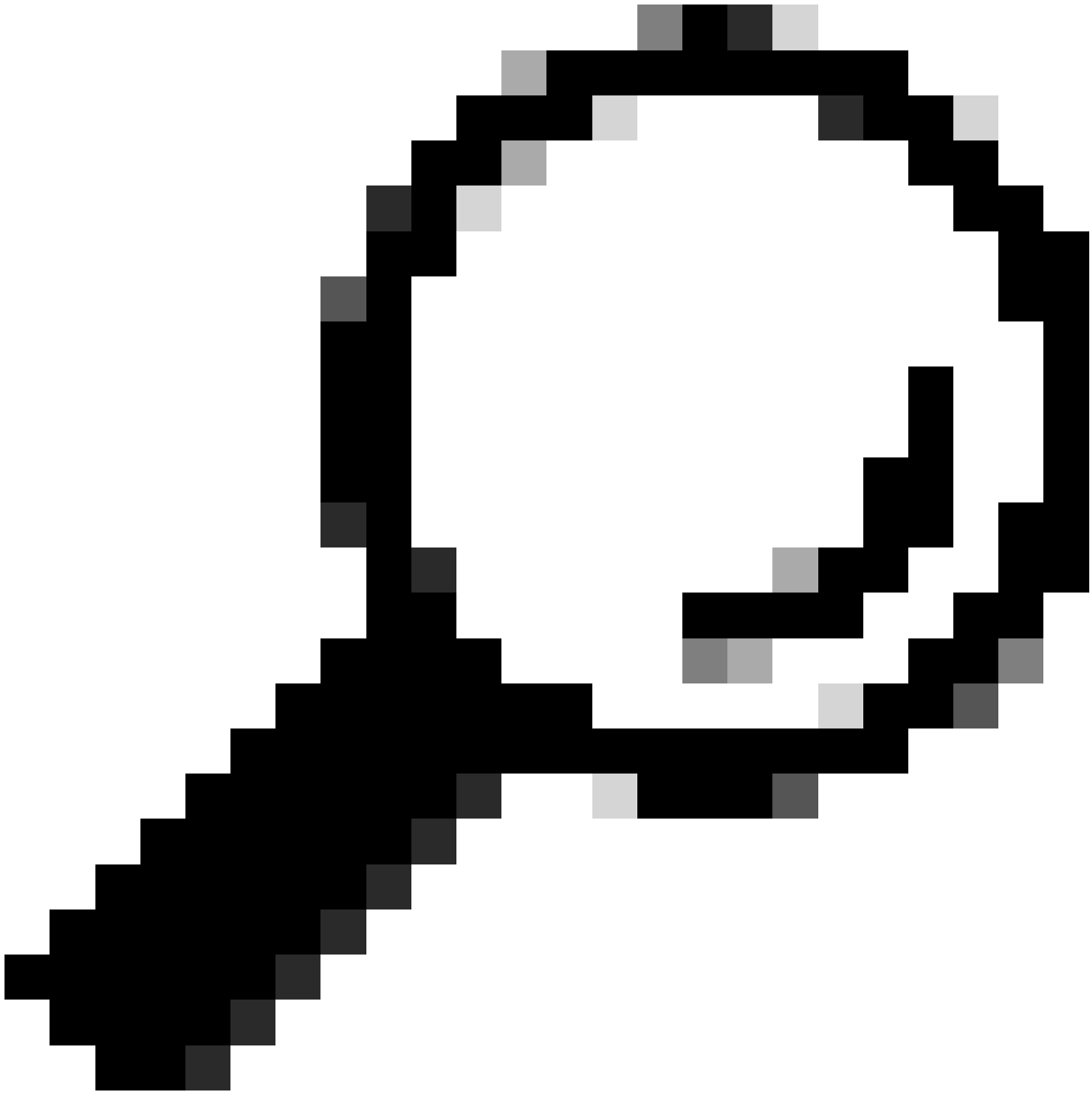
تلميح: تعد جميع أنواع الأجهزة وكافة المواقع تسلسلات هرمية افتراضية يتم توفيرها بواسطة ISE. يمكنك إضافة التدرجات الهرمية الخاصة بك وتعريف المكونات المختلفة في تعريف جهاز الشبكة الذي يمكن إستخدامه لاحقا في حالة السياسة

الخطوة 2.الآن، أضف جهاز Cisco IOS XE كجهاز شبكة. انتقل إلى مركز العمل > إدارة الجهاز > موارد الشبكة > أجهزة الشبكة. انقر على إضافة لإضافة جهاز شبكة جديد. لهذا الاختبار، سيكون SVS_BRPASR1K.



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



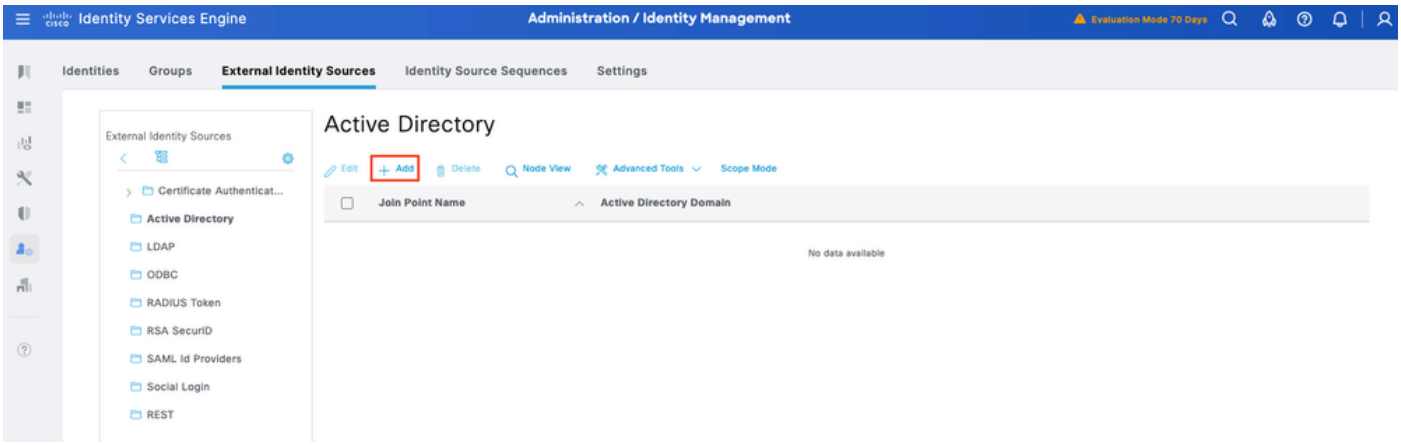


تلميح: يوصى بتمكين وضع الاتصال المفرد لتجنب إعادة تشغيل جلسة عمل TCP في كل مرة يتم إرسال أمر فيها إلى الجهاز.

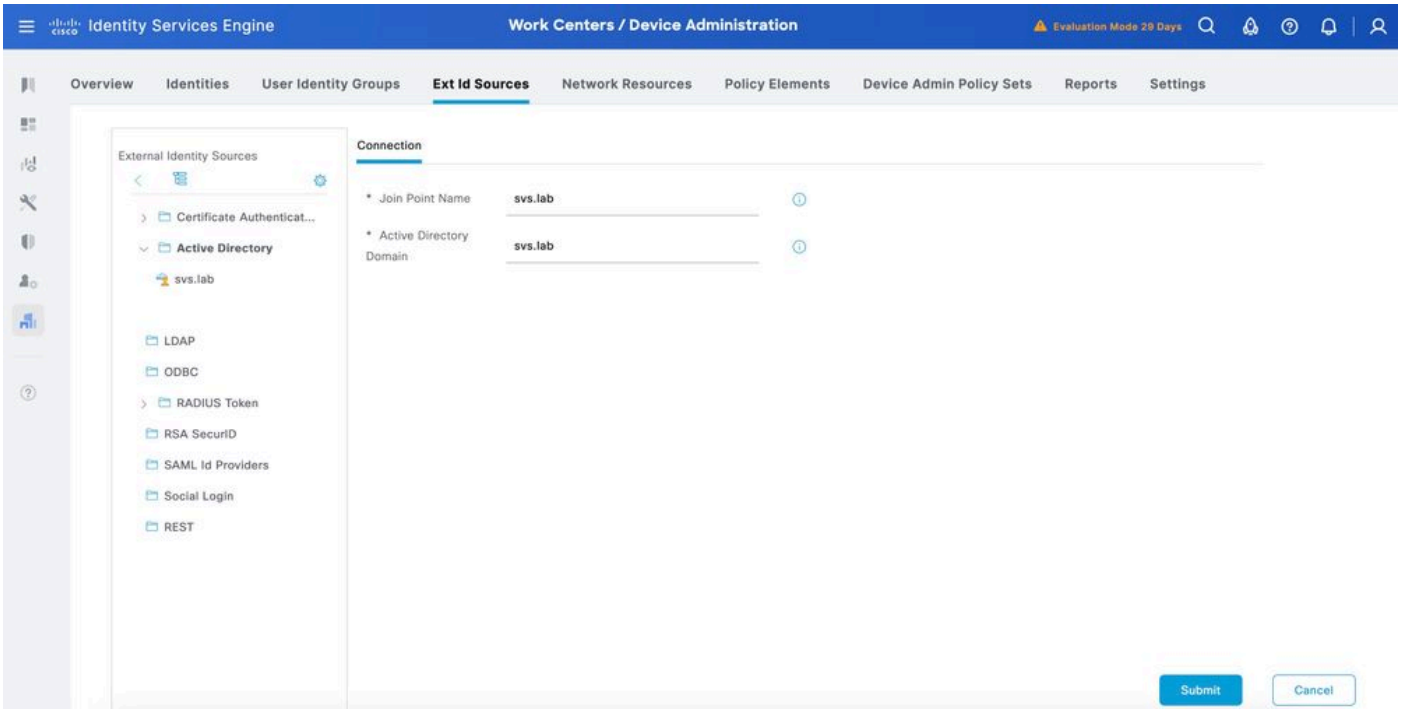
متاجر ConfigureIdentity

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.

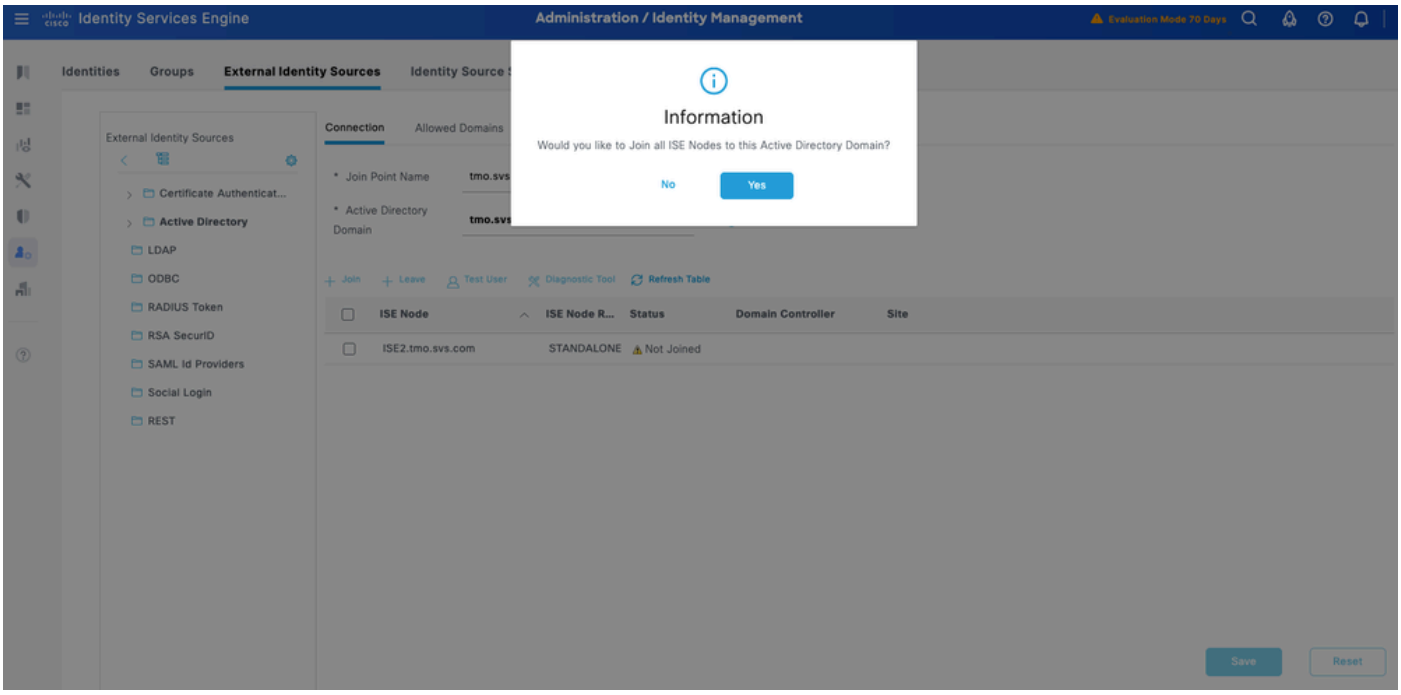
الخطوة 1. انتقل إلى الإدارة > إدارة الهوية > مخازن الهوية الخارجية > Active Directory. انقر فوق إضافة لتحديد نقطة AD مشتركة جديدة.



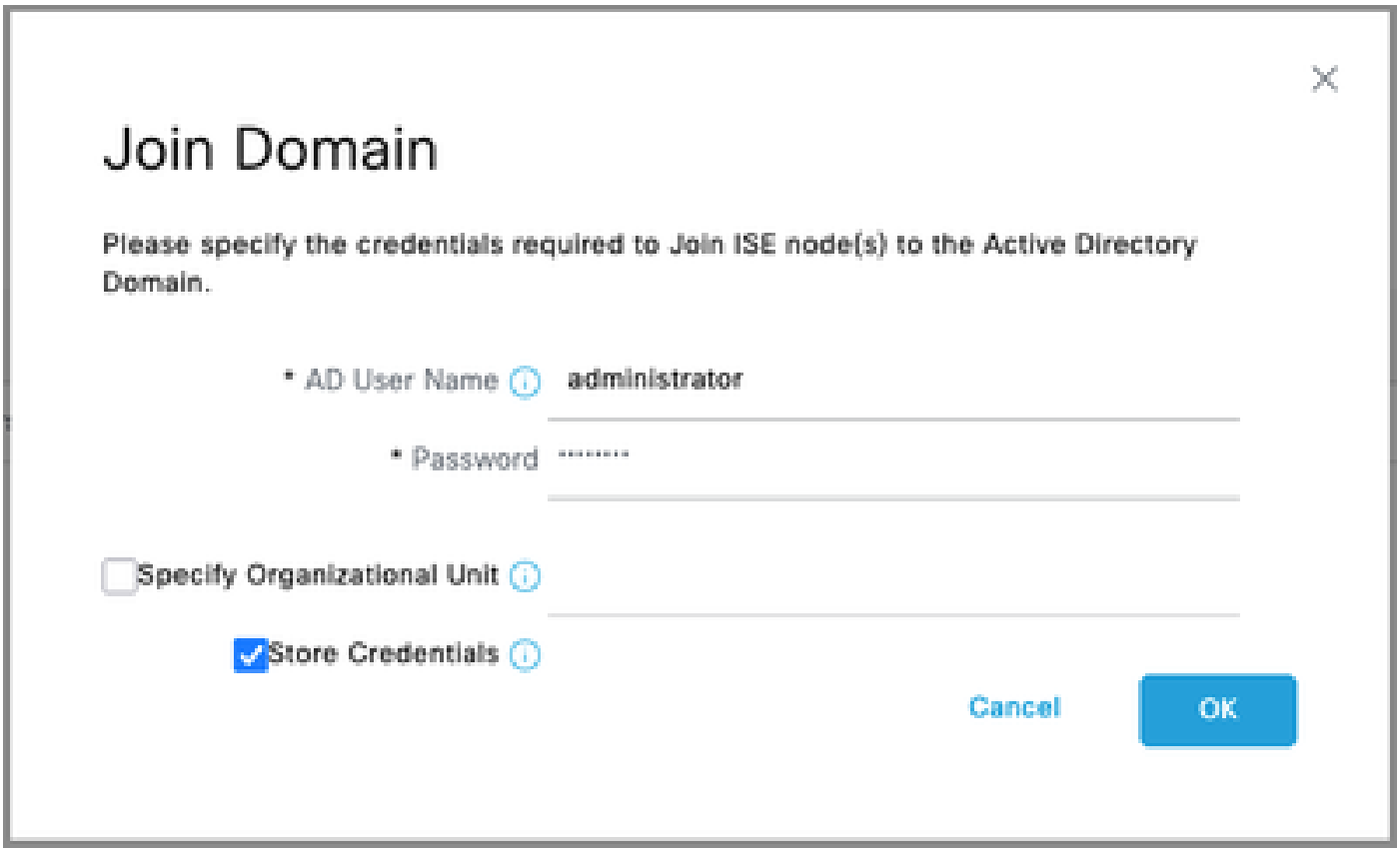
الخطوة 2. حدد اسم نقطة الربط واسم مجال AD وانقر إرسال.

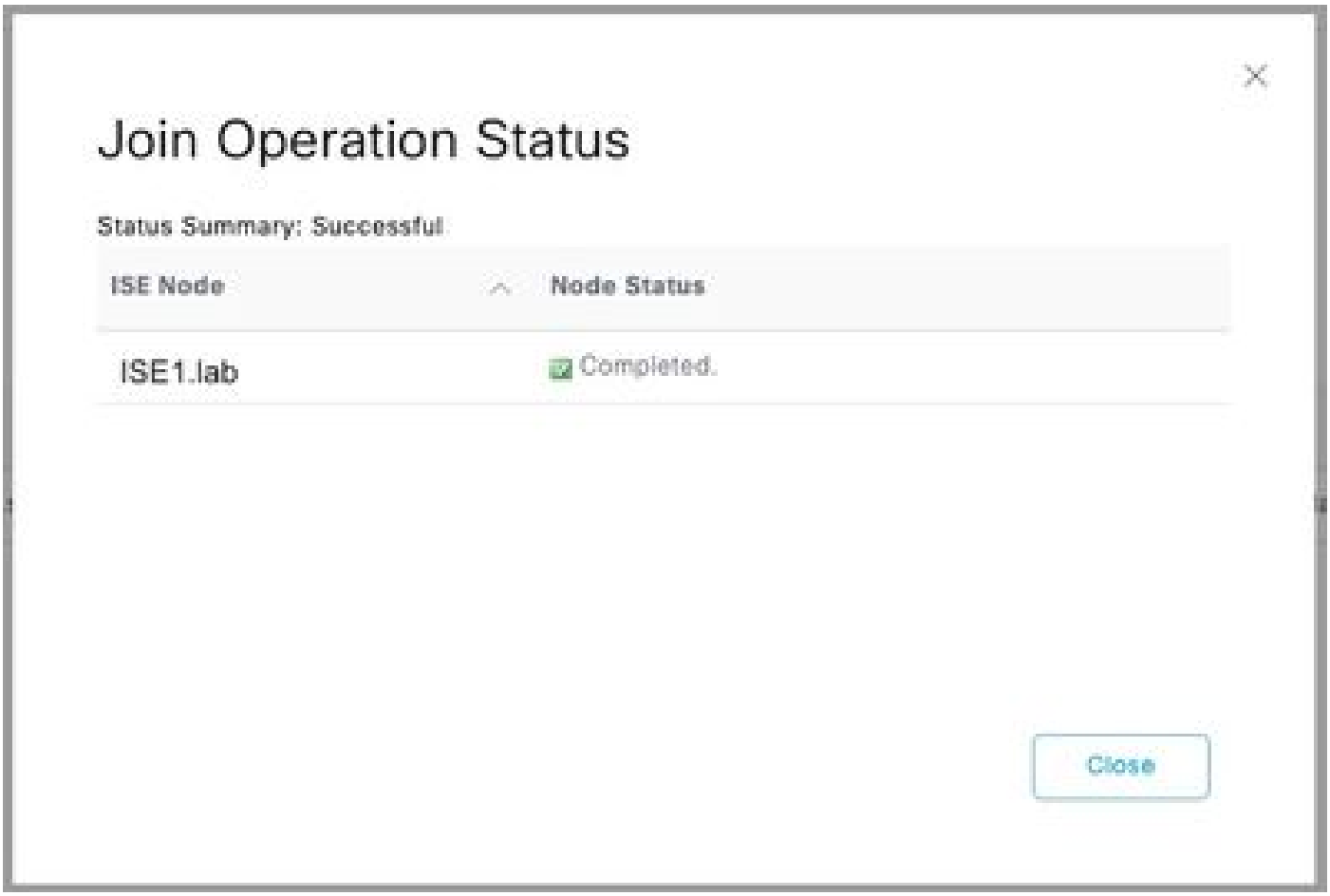


الخطوة 3. انقر فوق نعم عند المطالبة هل ترغب في ضم جميع عقد ISE إلى مجال Active Directory هذا؟

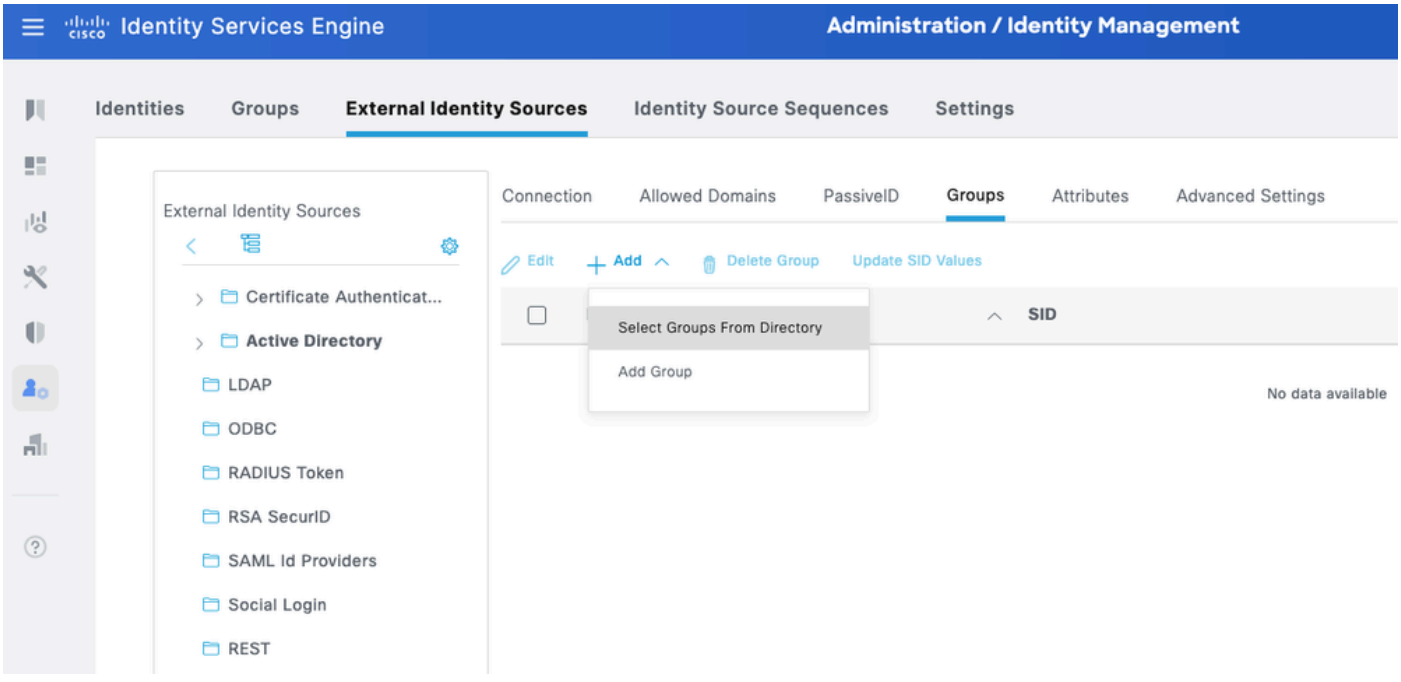


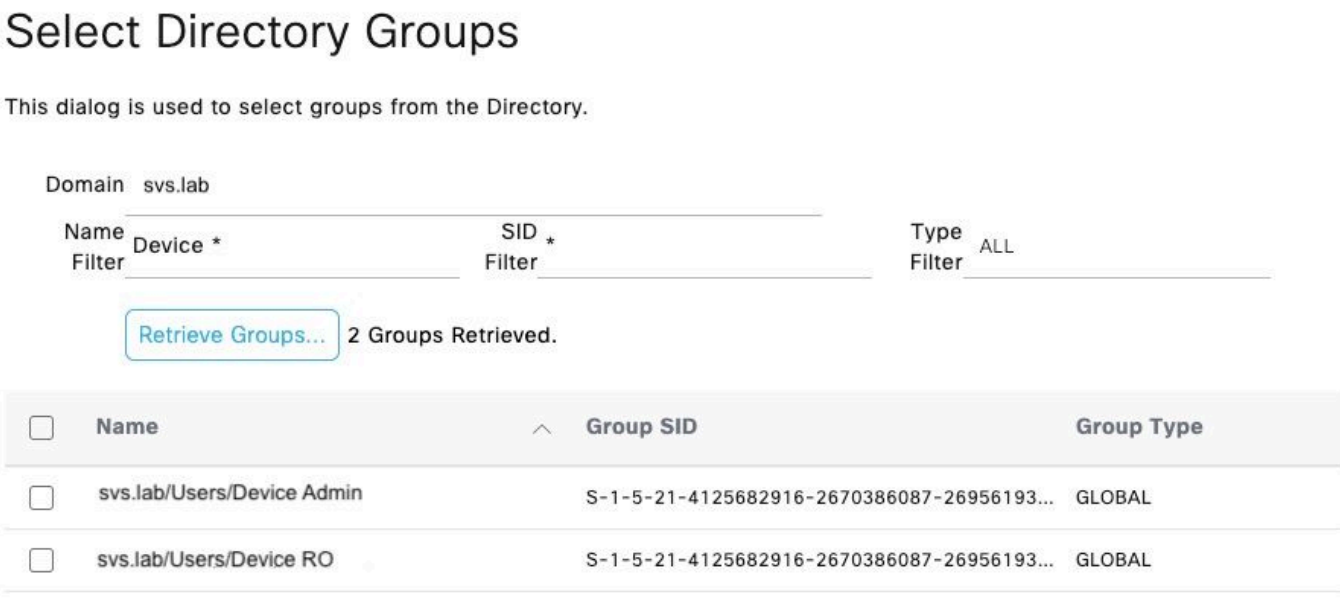
الخطوة 4. أدخل بيانات الاعتماد بامتيازات AD Join وانضم ISE إلى AD. تحقق من الحالة للتحقق من أنها تعمل.

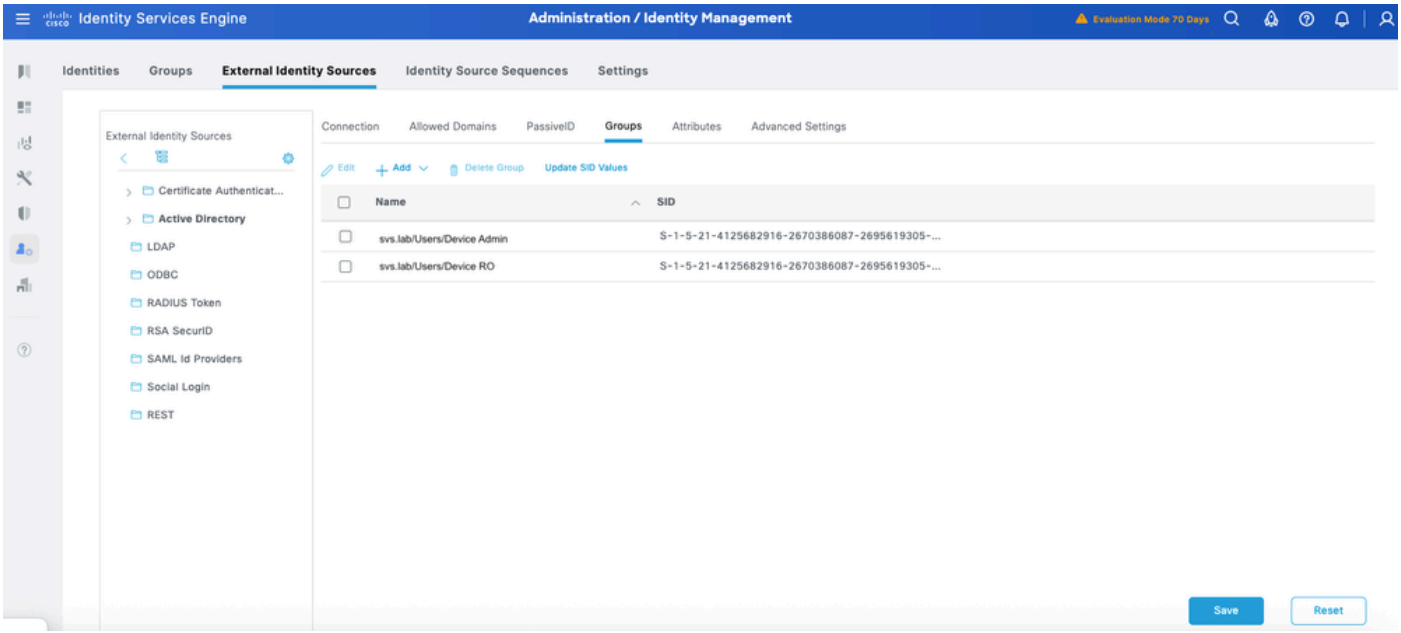




الخطوة 5. انتقل إلى علامة التبويب مجموعات، وانقر فوق إضافة للحصول على جميع المجموعات المطلوبة استنادا إلى أي من المستخدمين مخولين للوصول إلى الجهاز. يوضح هذه المثال المجموعات المستخدمة في نهج التخويل في هذا الدليل







تكوين ملفات تعريف TACACS+

أنت ذاهب إلى تعيين توصيفات TACACS+ إلى دورين مستخدمين رئيسيين على أجهزة Cisco IOS XE:

- 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.

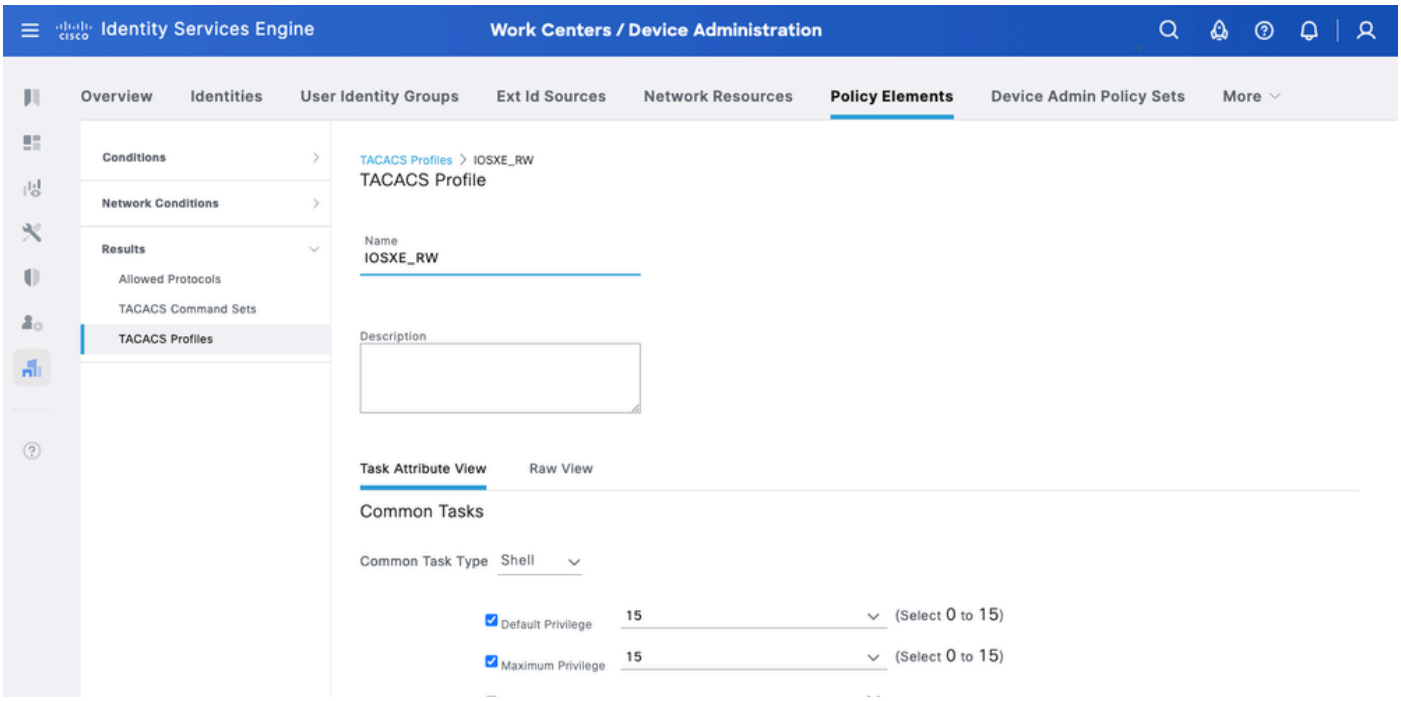
ويشار إلى أن هذه التوصيفات توصيفان من TACACS+: IOS XE_RW و IOSXR_RO.

IOS XE_RW - ملف تعريف المسؤول

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

خطوة 2. فحص وعين التقصير امتياز والحد الأقصى امتياز ك 15.

الخطوة 3.تأكد من التكوين والحفظ.

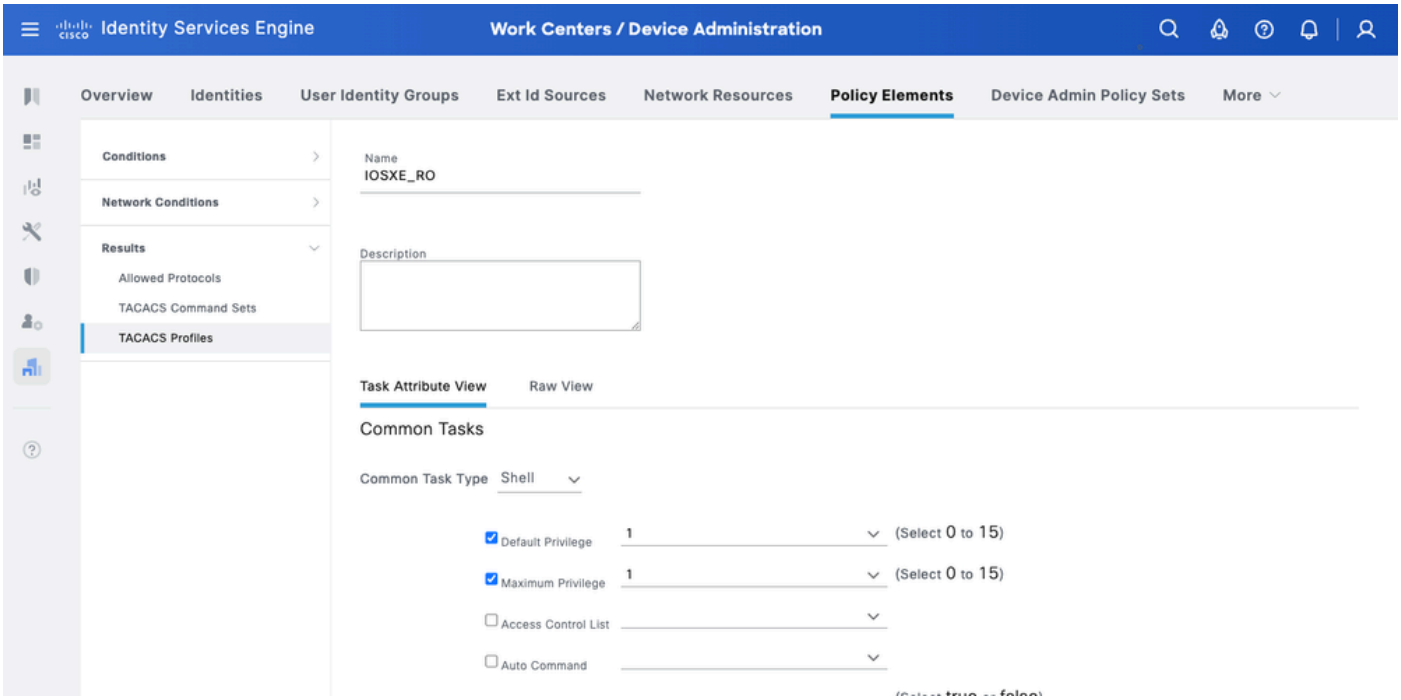


IOS XE_RO - ملف تعريف المشغل

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

خطوة 2. فحص وعين التقصير امتياز والحد الأقصى امتياز ك 1.

الخطوة 3.تأكد من التكوين والحفظ.



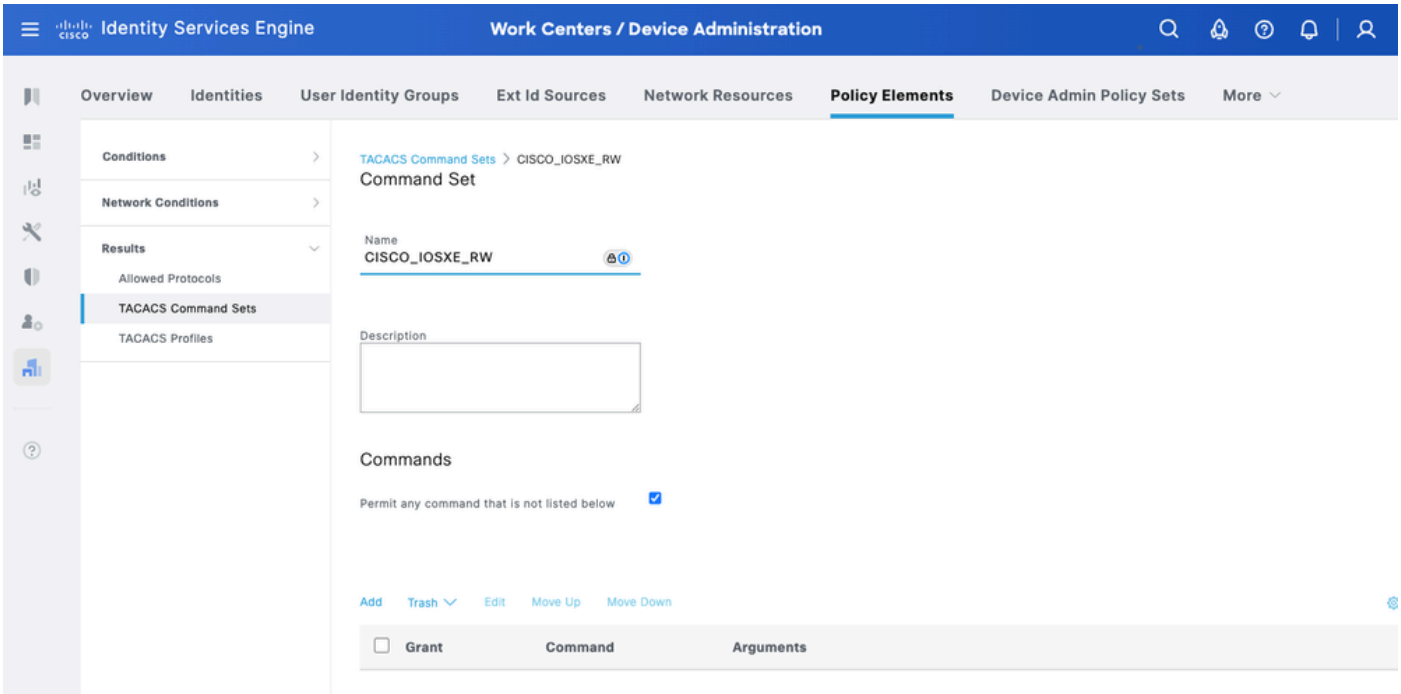
مجموعات أوامر configureTACACS+

ويتم تعريف هذه العناصر على أنها مجموعات أوامر TACACS+: Cisco_IOS XE_RW وCisco_IOS XE_RO.

Cisco_IOS XE_RW - مجموعة أوامر المسؤول

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

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



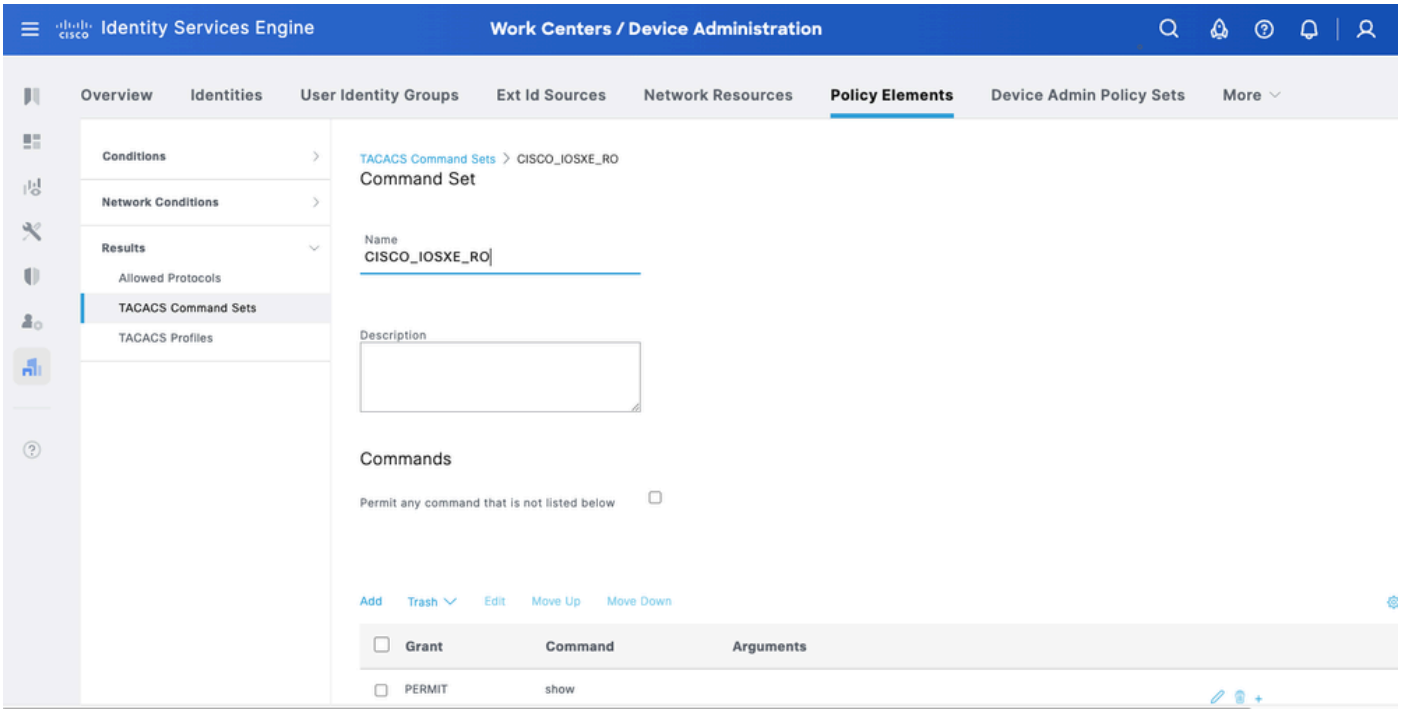
Cisco_IOS XE_RO - مجموعة أوامر المشغل

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

الخطوة 2. في قسم الأوامر، أضف أمر جديد.

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

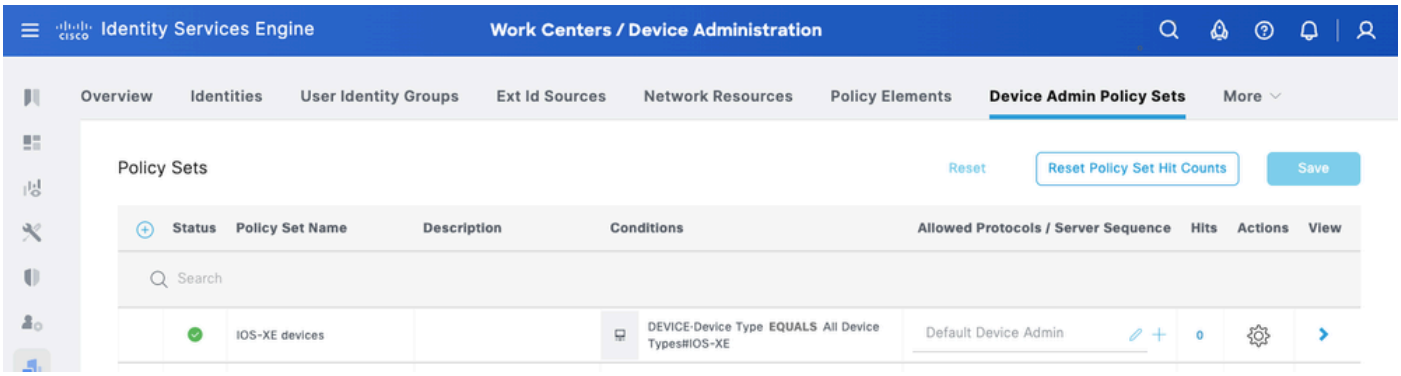
الخطوة 4. تأكد من البيانات وانقر فوق حفظ.



تكوين مجموعات نهج مسؤول الجهاز

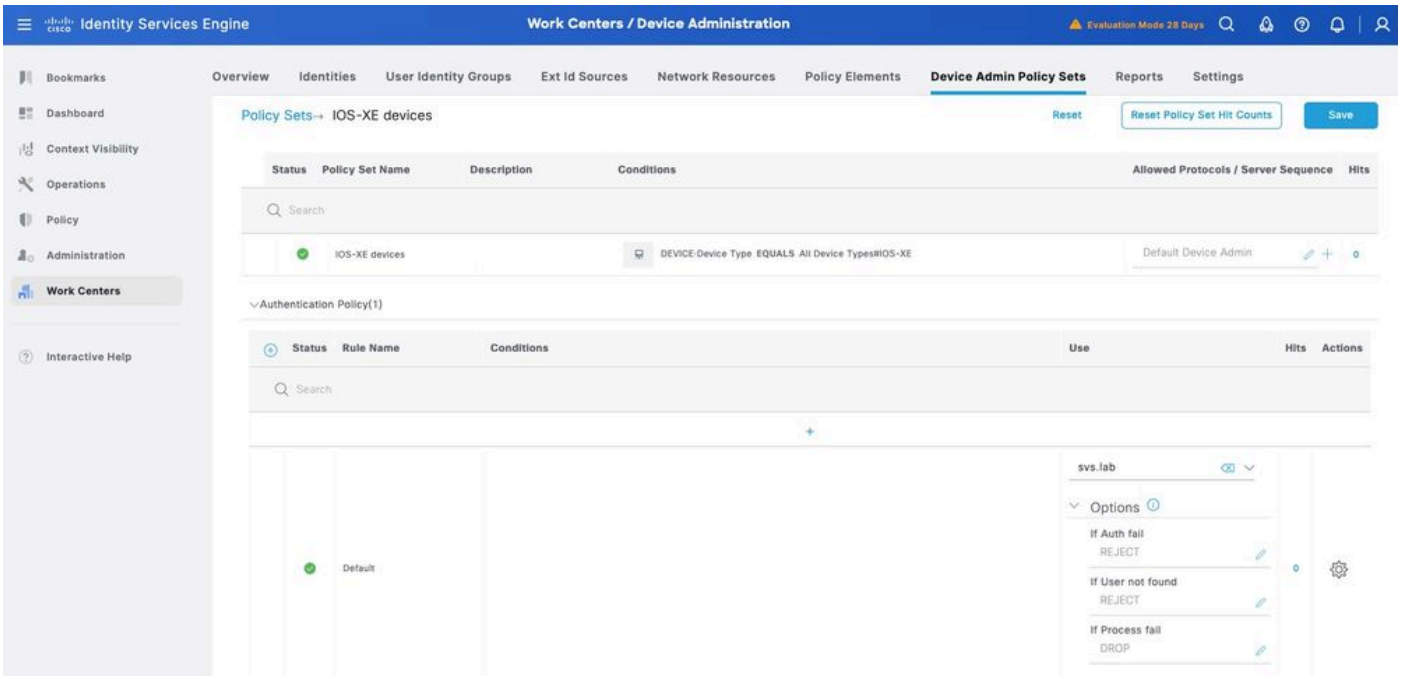
يتم تمكين مجموعات النهج بشكل افتراضي لإدارة الأجهزة. يمكن أن تقسم مجموعات السياسات استنادا إلى أنواع الأجهزة لتسهيل تطبيق ملفات تعريف TACACS.

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



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

الخطوة 3.قم بإنشاء سياسة المصادقة. للمصادقة، تستخدم AD كمخزن المعرف. أترك الخيارات الافتراضية تحت إذا فشلت المصادقة، إذا لم يعثر المستخدم وإذا فشلت العملية.



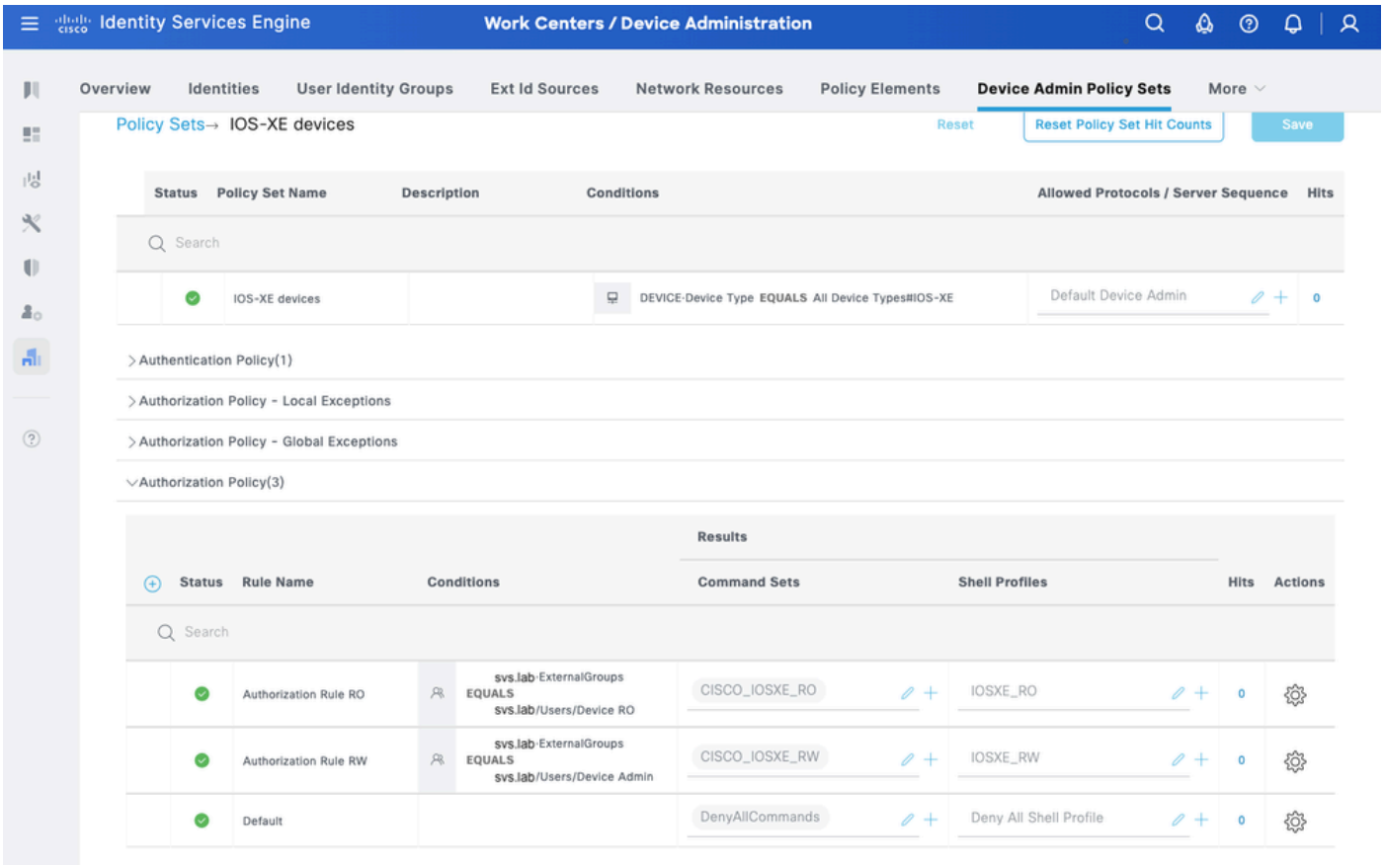
الخطوة 4. تحديد سياسة التفويض.

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

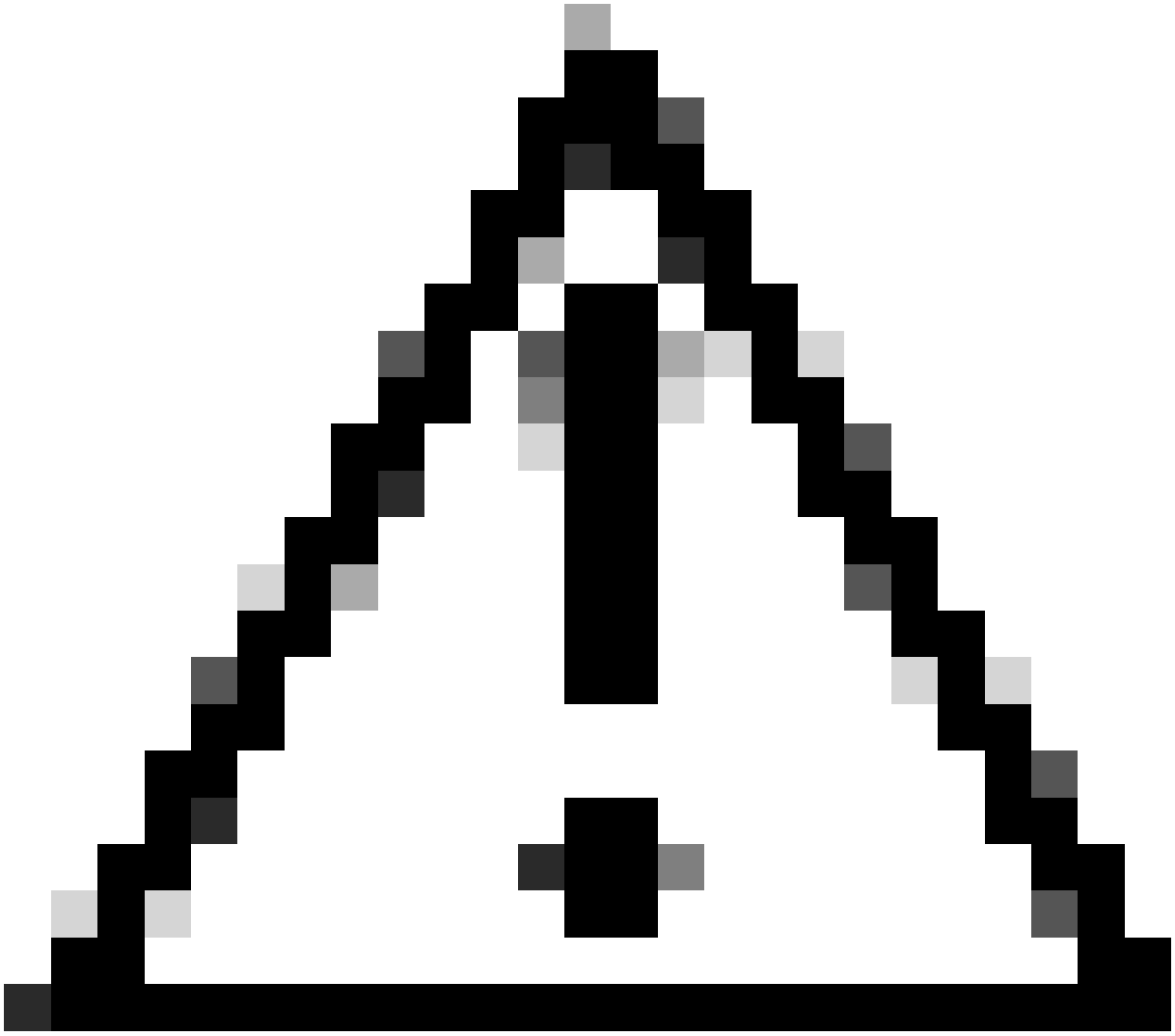
على سبيل المثال:

يتم تعيين المستخدمين في جهاز أو مجموعة AD لمجموعة الأوامر Cisco_IOSXR_RO وملف تعريف IOSXR_RO Shell.

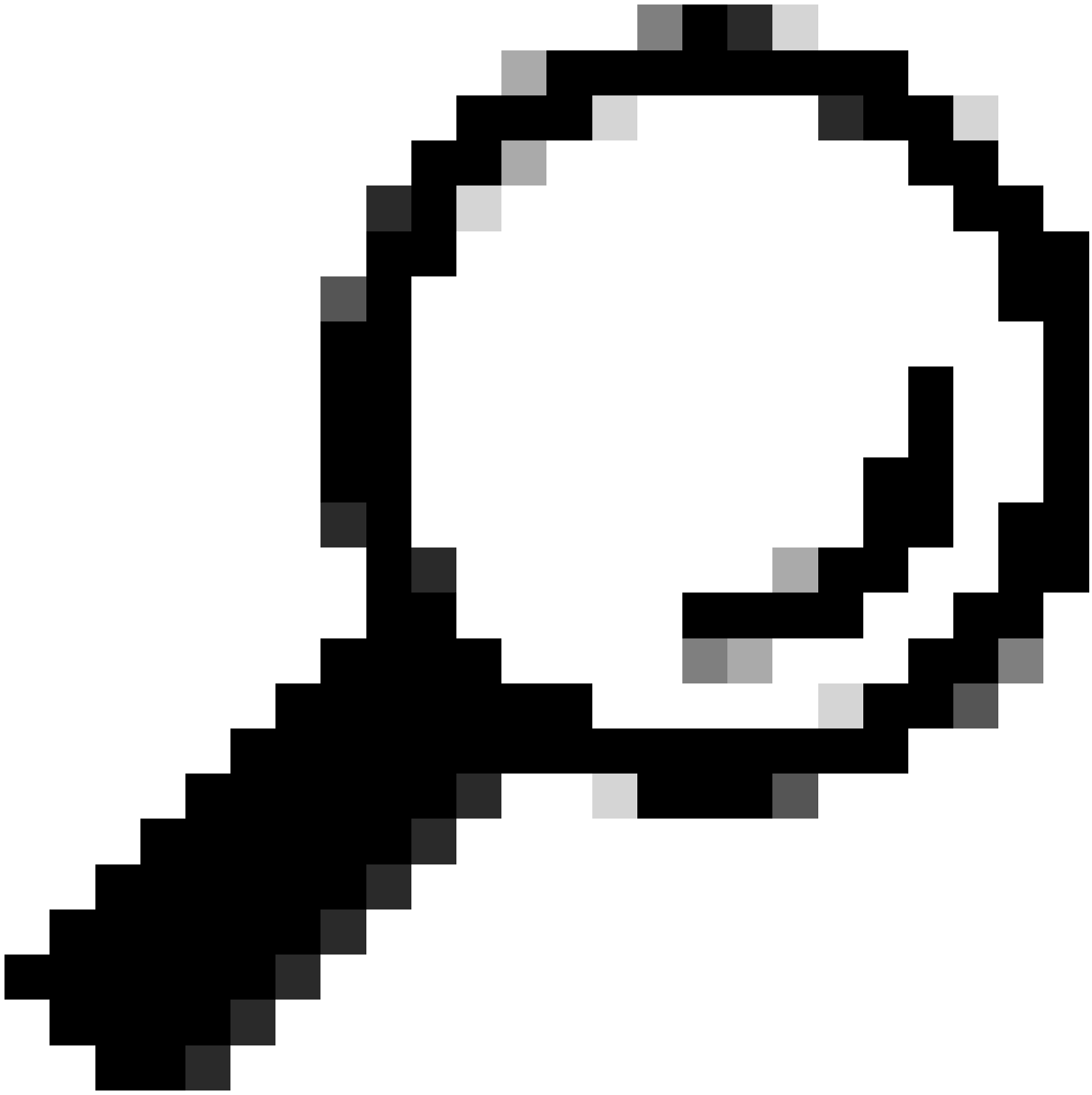
يتم تعيين المستخدمين في مسؤول جهاز مجموعة AD لمجموعة الأوامر Cisco_IOSXR_RW وملف تعريف طبقة IOSXR_RW.



الجزء 2 - تكوين Cisco IOS XE 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.

أسلوب التكوين 1 - زوج مفاتيح تم إنشاؤه بواسطة الجهاز

تكوين خادم TACACS+

الخطوة 1 قم بتكوين اسم المجال وإنشاء زوج مفاتيح يستخدمه Router TrustPoint.

```
ip domain name svs.lab

crypto key generate ec keysize 256 label svs-256ec-key
```

تكوين TrustPoint

الخطوة 1 أنشئ نقطة ثقة للموجه وأقران زوج المفاتيح.

```
crypto pki trustpoint svs_cat9k
  enrollment terminal pem
  subject-name C=US,ST=NC,L=RTP,O=Cisco,OU=SVS,CN=cat9k.svs.lab
  serial-number none
  ip-address none
  revocation-check none
  eckeypair svs-256ec-key
```

الخطوة 2. مصادقة TrustPoint بتثبيت شهادة CA.

<#root>

cat9k(config)#

crypto pki authenticate svs_cat9k

Enter the base 64 encoded CA certificate.

End with a blank line or the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----

MIIFlDCCA3ygAwIBAgIIIM10AsTaN/UwDQYJKoZIhvcNAQELBQAwajELMAkGA1UE
BhMCVVMxFzAVBgNVBAgTDk5vcnRoIENhcm9saW5hMRAwDgYDVQQHEwdSYWxlaWdo
MQ4wDAYDVQQKEwVDaXNjbzEMMAoGA1UECxMDU1ZTMRIwEAYDVQQDEwlTVlMgTGFi
QOEwHhcNMjUwNDI4MTcwNTAwWhcNMzUwNDI4MTcwNTAwWjBqMQswCQYDVQQGEwJV
UzEXMBUGA1UECBMOTm9ydGggQ2Fyb2xpbmExEDAOBgNVBAcTB1JhbGVpZ2gxDjAM
BgNVBAoTBUNpc2NvMQwwCgYDVQQLEwNTVlMxEjAQBgNVBAMTCVNWUyBMYWJDQTCC
AiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBAJvZUOyn2vIn6gKbx3M7vaRq
2YjwZlzSH6EkEvxnJTy+kksiFD33GyHQepk7vfp4NFU5OtQ4HC7t/AOv9grDa3QW
VwvV4MBbJhFM3s0J/ejgDYcMZhIAaPy0Zo5WLboOkXEiKjPLatkXojB8FVrhLF3O
jMBSqwa4/Wlniy5S+7s4FFxsCf20COWfBAsnrs0tatIIhmcnx+VLJP7MRm8f0w4m
mutNo7IhbJSrgAFXmjlbBjMmgspObULo/wxMHdTbtPBf11HRHTkNIo3qyO4UADL2
WpoGhgT/FaxxBo2UBcnYVaP+jjRE0NYT973MCbVAAxtNVU6bEBR0z+LWniACzupm
+qh23SL43uW5A3iSw/BuU1E9p7B0e8oDNKU6gXlojKyLP/gC7j8AeP03ir+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
xDrmo7eOXPpSW4l72a6Kl8CR3U2Cr4wsuvndPEq/qd2NRSBWffF0XE/AJHQG7STT
HaXLU9r2Ko6O3oecu8ysGTwLlIt/9T1/FOb0xZRugWcpJrVoTgDGuA==

-----END CERTIFICATE-----

Certificate has the following attributes:
   Fingerprint MD5: D9C404B2 EC08A260 EC3539E7 F54ED17D
   Fingerprint SHA1: 0EB181E9 5A3ED780 3BC5A805 9A854A95 C83AC737

% Do you accept this certificate? [yes/no]:

yes


Trustpoint CA certificate accepted.
% Certificate successfully imported

cat9k(config)#
```

الخطوة 3. إنشاء طلب توقيع الشهادة (CSR).

```
<#root>

cat9k(config)#

crypto pki enroll svs_cat9k


% Start certificate enrollment ..

% The subject name in the certificate will include: C=US,ST=NC,L=RTP,O=Cisco,OU=SVS,CN=cat9k.svs.lab
% The subject name in the certificate will include: cat9k.svs.lab
Display Certificate Request to terminal? [yes/no]:

yes


Certificate Request follows:

-----BEGIN CERTIFICATE REQUEST-----
MIIBfDCCASMCAQAwgYQxGjAYBgNVBAMTEWNhdDlrLnRtby5zdnMuY29tMQwwCgYD
VQQLEwNTVlMxDjAMBgNVBAoTBUNpc2NvMQwwCgYDVQQHEwNSVFAxCzAJBgNVBAgT
Ak5DMQswCQYDVQQGEwJVUzEgMB4GCSqGSIb3DQEJAhYRY2F0OWsudG1vLnN2cy5j
b20wWTATBgcqhkjOPQIBBggqhkjOPQMBBwNCAATpYE7atscrtl4ddevCh3UgxjYi
4N4oBGWrpJBctKy4so8V5i6RXDt7kHgPzp14Qnf20bcXVODE1wtTAHHBrIXqoDww
OgYJKoZIhvcNAQkOMS0wKzAcBgNVHREEFTATghFjYXQ5ay50bW8uc3ZzLmNvbTAL
BgNVHQ8EBAMCB4AwCgYIKoZIzj0EAwQDRwAwRAIgZqP2QTwM3ZZrmIphJ7+jSTER
4OkTx2DiVs1c1Xf+vR4CIBcSb18DIYz84DmgMHUaf778/cmpe9cWakvdaxMWseBH
-----END CERTIFICATE REQUEST-----
```

```
---End - This line not part of the certificate request---

Redisplay enrollment request? [yes/no]:

no


cat9k(config)#
```

الخطوة 4. إستيراد الشهادة الموقعة من المرجع المصدق.

<#root>

```
cat9k(config)#

crypto pki import svs_cat9k certificate



Enter the base 64 encoded certificate.
End with a blank line or the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----
MIID8zCCAdugAwIBAgIIKfdYWg5WpskwDQYJKoZIhvcNAQELBQAwajELMAkGA1UE
BhMCVVMxFzAVBgNVBAgTDk5vcnRoIENhcm9saW5hMRAwDgYDVQQHEwdSYWxlaWdo
MQ4wDAYDVQQKEwVDaXNjbzEMMAoGA1UECxMDU1ZTMRIwEAYDVQQDEwlTVlMgTGFi
QOEwHhcNMjUwNTE0MTUxMjAwWhcNMjYwNTE0MTUxMjAwWjCBhDEaMBgGA1UEAxMR
Y2F0OWsudG1vLnN2cy5jb20xDDAKBgNVBAsTA1NWUzEOMAwGA1UEChMFQ2lzY28x
DDAKBgNVBAcTA1JUUDELMAkGA1UECBMCTkMxCzAJBgNVBAYTAlVTMSAwHgYJKoZI
hvcNAQkCFhFjYXQ5ay5Obw8uc3ZzLmNvbTBZMBMGByqGSM49AgEGCCqGSM49AwEH
A0IABOlgTtq2xyu2Xh1168KHdSDGNiLg3igEZaukkFyOrLiyjxXmLpFcO3uQeA/O
nXhCd/bRtxdU4MTXC1MAccGsheqjTTBLMB4GCWCGSAGG+EIBDQQRFg94Y2EgY2Vy
dGlmaWNhdGUwHAYDVR0RBBUwE4IRY2FOOWsudG1vLnN2cy5jb2OwCwYDVR0PBAQD
AgeAMA0GCSqGSIb3DQEBCwUAA4ICAQBObgKVykeyVC9UsvuuOAUsGaZHGwy2H9Yd
m5vIaui6PJczkCzIoAIghHPGQhIgpEcRqtGyXPZ2r8TCJP11WXNN/G73sFyWAhzY
RtmIM5KIojiDHLtifPayxv9juDuOZRx+wYR2PIQ5eLv1bafg7K8E82sqOCfOtcPr
OcONU8UCxqObdOgu4XsdBN1+wcWFqeQSDLmP7nxvhOOm/LXwCWUHwgVioOAuU2Fe
k5NthtvdxNAhRAImQdTyq6u/yB7vwTwJHcRiJc5USsyzCsTBb6RvL+HsXqBgXGc5
lxCSoLtYOdUxFIpJyK2MOZBY2zq2cNSc8Xbso5/OEQmnHtpWPvij4rSPUhQSY+4m
Qq2Sn3iqf4mGh/AO8T4iXfWDWfNezh7ZxMsCSCK/ZRlELZ2hj6OfzwX1H27Uf8XU
ecrOWx+WzRn7LVRCaGQzFkukfi8S4DLLNtxnNHfsLBVX5yHXCLEL+CQ7n8Z/pxcB
VVrPitwN3ZbO9poZyWiRLTnBsb42xNaWiL9bjQznAOiTDfmfFFourBsaAioz7ouY
2r1Mh+OpE83Uu+4lOTMawDgGiEv7iaiJ6xWc95EC+AdmOx3FvBXMtIM9qr7WwHW6
3C2hVYHJH254elV5+H8iiz7rovEPm8ZDsnvYpJn4Km3iDvBNqp/vvAHOFcyXrvG6
3i/1b9erGQ==
-----END CERTIFICATE-----

% Router Certificate successfully imported

cat9k(config)#
```

TACACS & AAA مع تكوين TLS

الخطوة 1. إنشاء خادم TACACSS ومجموعات AAA، وإقران TrustPoint للعميل (الموجه).

```
tacacs server svs_tacacs
 address ipv4 10.225.253.209
 single-connection
 tls port 6049
 tls idle-timeout 60
 tls connection-timeout 60
 tls trustpoint client svs_cat9k
 tls ip tacacs source-interface GigabitEthernet0/0
 tls ip vrf forwarding Mgmt-vrf
!
aaa group server tacacs+ svs_tls
 server name svs_tacacs
 ip vrf forwarding Mgmt-vrf
!
tacacs-server directed-request
```

الخطوة 2. تكوين أساليب AAA.

```
aaa authentication login default group svs_tls local enable
aaa authentication login console local enable
aaa authentication enable default group svs_tls enable
aaa authorization config-commands
aaa authorization exec default group svs_tls local if-authenticated
aaa authorization commands 1 default group svs_tls local if-authenticated
aaa authorization commands 15 default group svs_tls
aaa accounting exec default start-stop group svs_tls
aaa accounting commands 1 default start-stop group svs_tls
aaa accounting commands 15 default start-stop group svs_tls
aaa session-id common
```

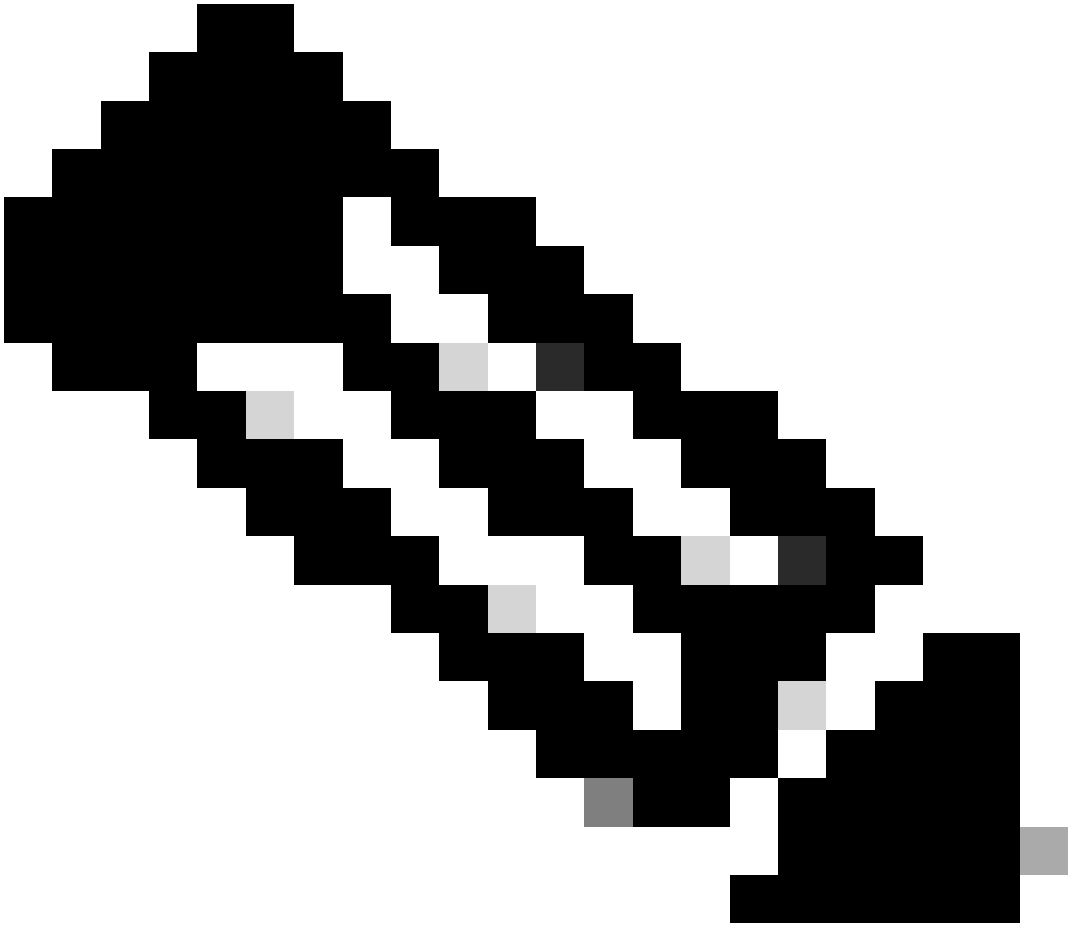
أسلوب التكوين 2 - زوج مفاتيح تم إنشاؤه بواسطة CA

إذا كنت تقوم باستيراد المفاتيح وكذلك شهادات الجهاز و CA مباشرة بتنسيق PKCS#12 من الدبلوماسية CSR، يمكنك استخدام هذه الطريقة.

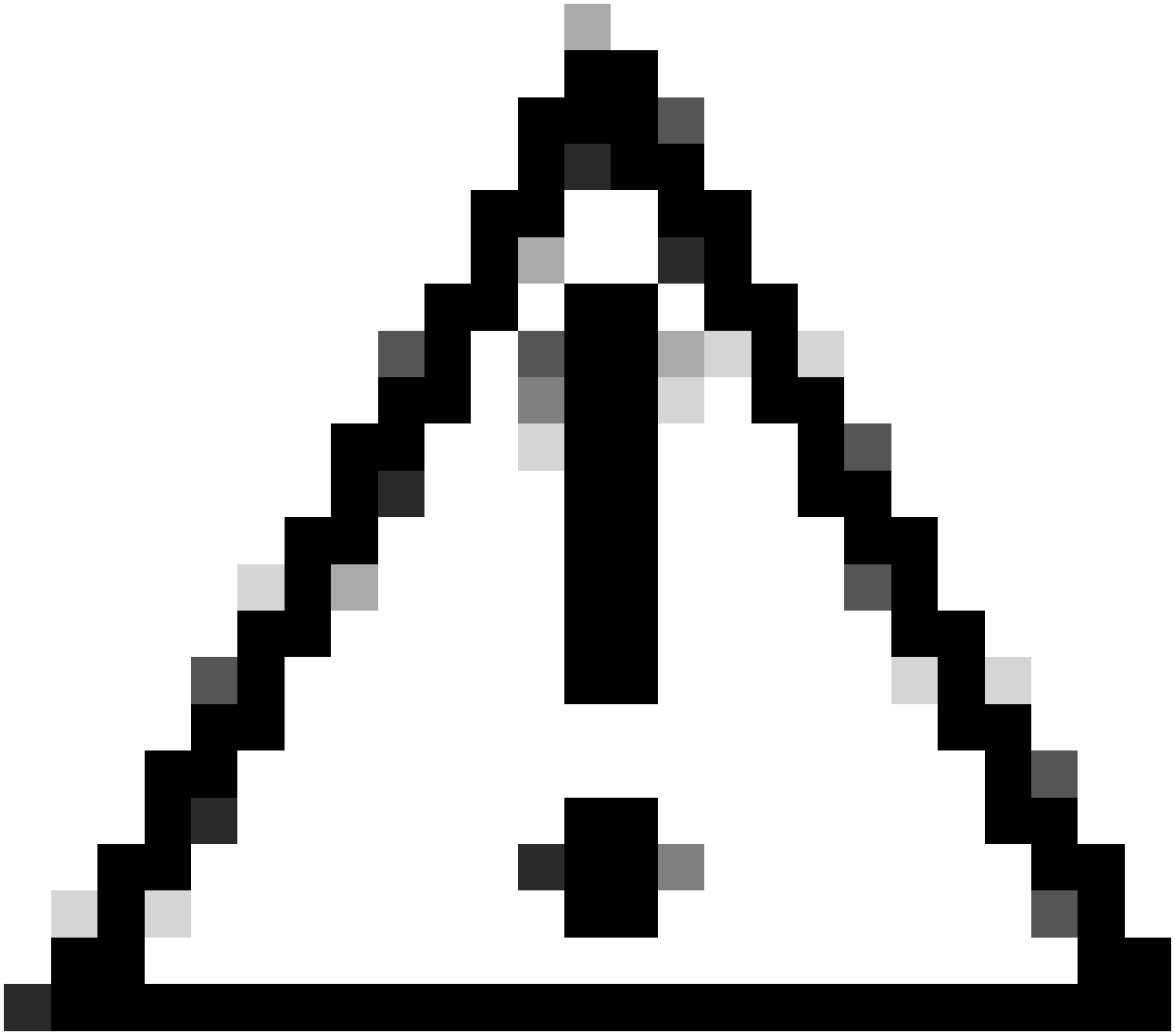
الخطوة 1. إنشاء TrustPoint للعميل.

```
cat9k(config)#crypto pki trustpoint svs_cat9k_25jun17
cat9k(ca-trustpoint)#revocation-check none
```

الخطوة 2. انسخ ملف PKCS#12 إلى bootflash.



ملاحظة: تأكد من أن ملف PKCS#12 يحتوي على سلسلة الشهادات الكاملة والمفتاح الخاص كملف مشفر.



تحذير: يجب أن تكون المفاتيح الموجودة في PKCS#12 المستوردة من RSA (على سبيل المثال: النوع RSA 2048)، ليس ECC.

<#root>

cat9k#

copy sftp bootflash: vrf Mgmt-vrf

```
Address or name of remote host [10.225.253.247]?
Source username [svs-user]?
Source filename [cat9k.svs.lab.pfx]? /home/svs-user/upload/cat9k-25jun17.pfx
Destination filename [cat9k-25jun17.pfx]?
Password:
!
2960 bytes copied in 3.022 secs (979 bytes/sec)
```

الخطوة 3. استورد ملف PKCS#12 باستخدام الأمر إستيراد.

<#root>

```
cat9k#

crypto pki import svs_cat9k_25jun17 pkcs12 bootflash:cat9k-25jun17.pfx

 password C1sco.123
% Importing pkcs12...Reading file from bootflash:cat9k-25jun17.pfx
CRYPTO_PKI: Imported PKCS12 file successfully.
cat9k#

cat9k#

show crypto pki certificates svs_cat9k_25jun17


Certificate
  Status: Available
  Certificate Serial Number (hex): 586OBF33A2O33365
  Certificate Usage: General Purpose
  Issuer:
    cn=SVS LabCA
    ou=SVS
    o=Cisco
    l=Raleigh
    st=North Carolina
    c=US
  Subject:
    Name: cat9k.svs.lab
    e=pkalkur@cisco.com
    cn=cat9k.svs.lab
    ou=svs
    o=cisco
    l=rtp
    st=nc
    c=us
  Validity Date:
    start date: 17:56:00 UTC Jun 17 2025
    end   date: 17:56:00 UTC Jun 17 2026
  Associated Trustpoints: svs_cat9k_25jun17

CA Certificate
  Status: Available
  Certificate Serial Number (hex): 2OCD74O2C4DA37F5
  Certificate Usage: General Purpose
  Issuer:
    cn=SVS LabCA
    ou=SVS
    o=Cisco
    l=Raleigh
    st=North Carolina
    c=US
  Subject:
    cn=SVS LabCA
    ou=SVS
    o=Cisco
    l=Raleigh
    st=North Carolina
    c=US
  Validity Date:
    start date: 17:05:00 UTC Apr 28 2025
    end   date: 17:05:00 UTC Apr 28 2035
  Associated Trustpoints: svs_cat9k_25jun17 svs_cat9k
```

```
  Storage: nvram:SVSLabCA#37F5CA.cer
```

TACACS & AAA مع تكوين TLS

الخطوة 1. إنشاء خادم TACACS ومجموعات AAA، وإقران TrustPoint للعميل (الموجه).

```
tacacs server svs_tacacs
 address ipv4 10.225.253.209
 single-connection
 tls port 6049
 tls idle-timeout 60
 tls connection-timeout 60
 tls trustpoint client svs_cat9k
 tls ip tacacs source-interface GigabitEthernet0/0
 tls ip vrf forwarding Mgmt-vrf
!
aaa group server tacacs+ svs_tls
 server name svs_tacacs
 ip vrf forwarding Mgmt-vrf
!
tacacs-server directed-request
```

الخطوة 2. تكوين أساليب AAA.

```
aaa authentication login default group svs_tls local enable
aaa authentication login console local enable
aaa authentication enable default group svs_tls enable
aaa authorization config-commands
aaa authorization exec default group svs_tls local if-authenticated
aaa authorization commands 1 default group svs_tls local if-authenticated
aaa authorization commands 15 default group svs_tls
aaa accounting exec default start-stop group svs_tls
aaa accounting commands 1 default start-stop group svs_tls
aaa accounting commands 15 default start-stop group svs_tls
aaa session-id common
```

التحقق

التحقق من التكوين.

```
show tacacs
show crypto pki certificates <>
show crypto pki trustpoints <>
```

تصحيح أخطاء المصادقة والتفويض والمحاسبة (AAA) و+TACACS.

```
debug aaa authentication
debug aaa authorization
debug aaa accounting
debug aaa subsys
debug aaa protocol local
debug tacacs authentication
debug tacacs authorization
debug tacacs accounting
debug tacacs events
debug tacacs packet
debug tacacs
debug tacacs secure

! Below debugs will be needed only if there is any issue with SSL Handshake
debug ip tcp transactions
debug ip tcp packet
debug crypto pki transactions
debug crypto pki API
debug crypto pki messages
debug crypto pki server
debug ssl openssl errors
debug ssl openssl msg
debug ssl openssl states
clear logging
```

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).