تكوين TACACS+ عبر TLS 1.3 على جهاز Nexus باستخدام ISE

المحتويات

المقدمة

يصف هذا المستند كيفية تكوين TACACS+ عبر TLS مع محرك خدمات الهوية (ISE) من Cisco كخادم وجهاز NX-OS كعميل.

نظرة عامة

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

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 السري 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 NX-OS من Cisco.
· الجزء 1 - تكوين ISE لمسؤول الجهاز
· الجزء 2 - تكوين نظام تشغيل Cisco NX-OS ل TACACS+ عبر TLS

المتطلبات الأساسية

المتطلبات

المتطلبات الأساسية لتكوين 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 أدناه:

- الجهاز الظاهري ISE VMware، الإصدار 3. 4 Patch 2.
- Nexus 9000 switch model C9364D-GX2A، Cisco NX-OS، الإصدار 10.5(3t).

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.

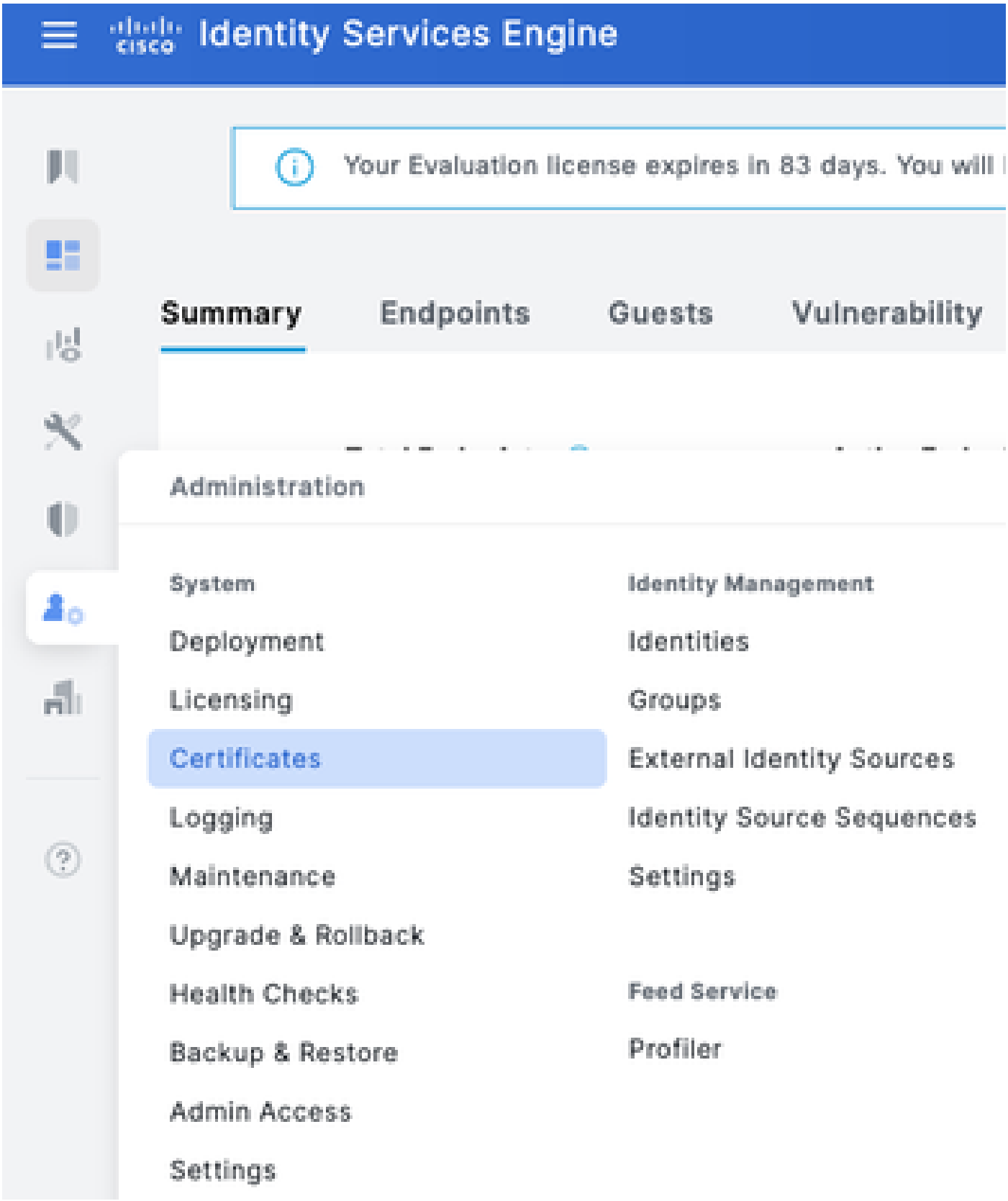
تكوين ISE لمسؤول الجهاز

إنشاء طلب توقيع الشهادة لمصادقة خادم TACACS+

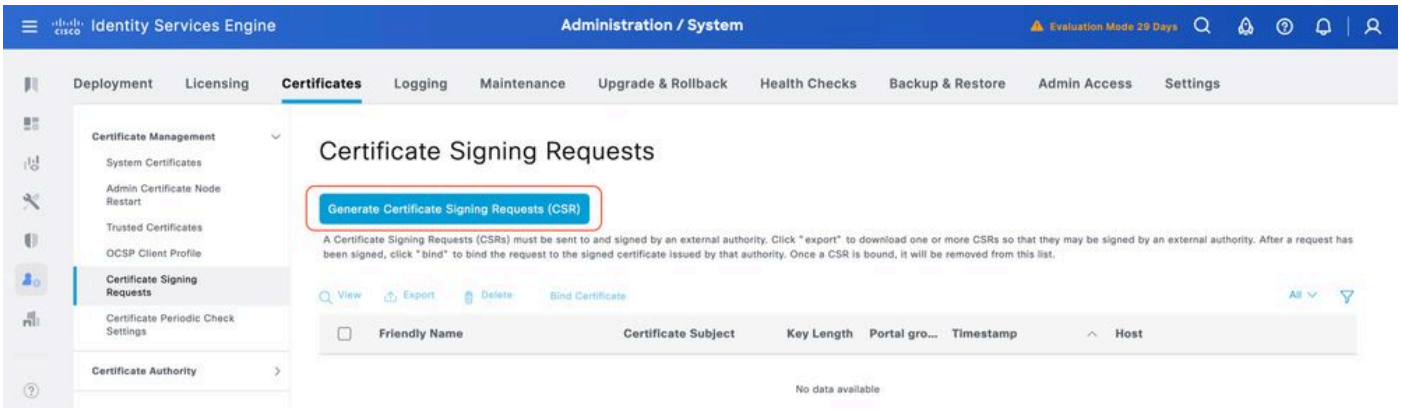
الخطوة 1. سجل الدخول إلى بوابة إدارة ISE على الويب باستخدام أحد المستعرضات المدعومة.

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.

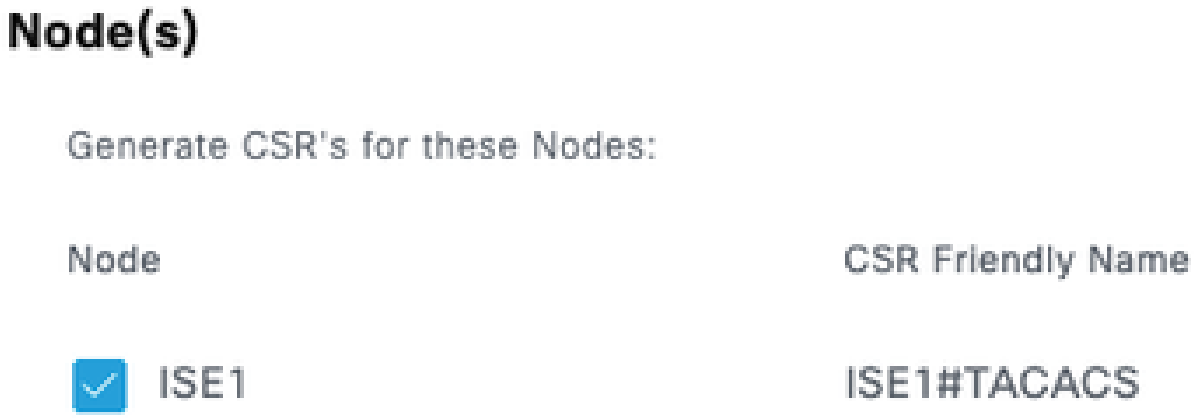


الخطوة 3. تحت طلبات توقيع الشهادة، انقر إنشاء طلب توقيع الشهادة.

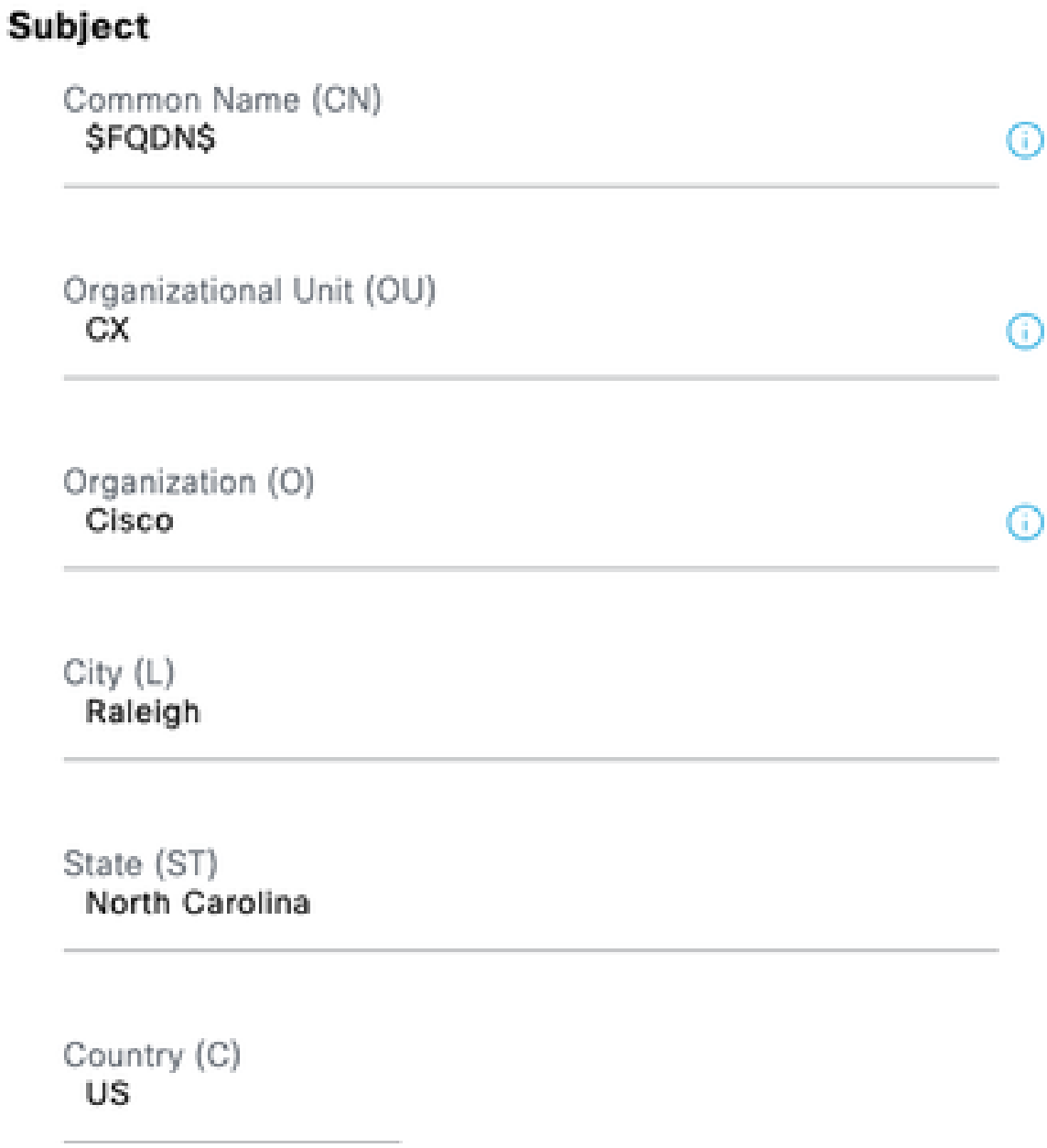


الخطوة 4. حدد TACACS في الاستخدام.

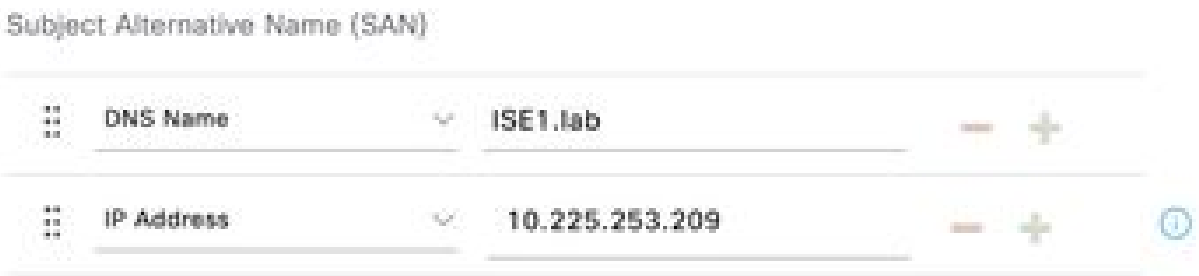
الخطوة 5. حدد شبكات PSN التي تم تمكين TACACS+ لها.



الخطوة 6. املأ حقول الموضوع بالمعلومات المناسبة.



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

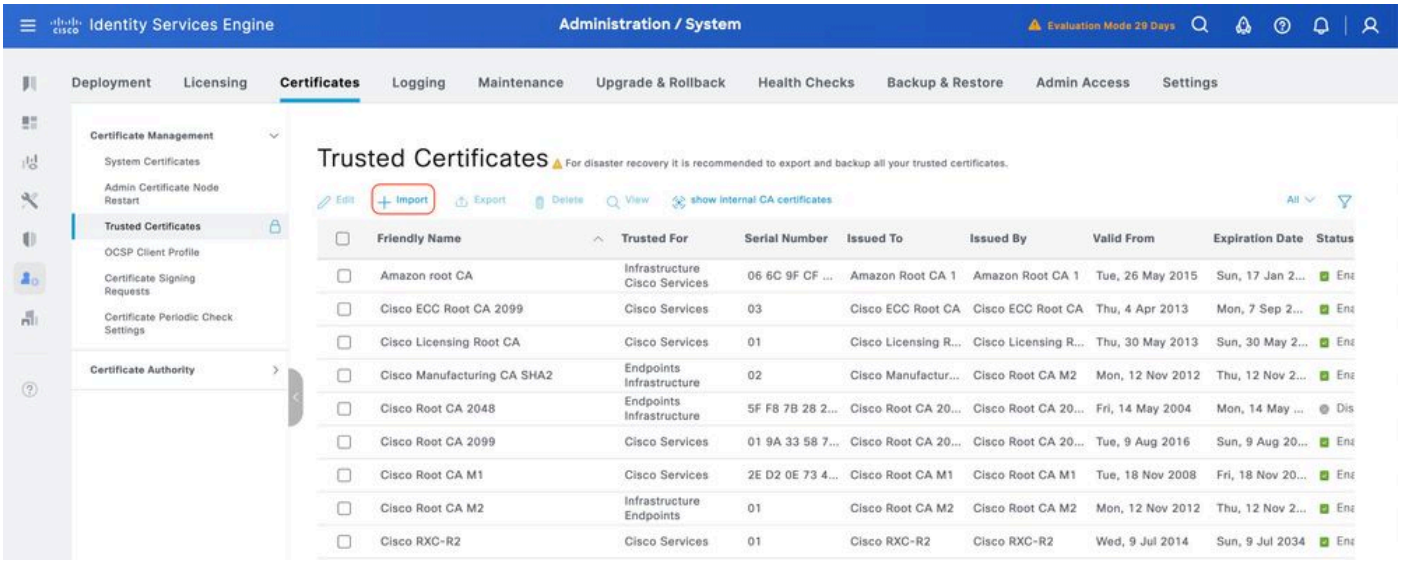


الخطوة 8. انقر فوق إنشاء ثم تصدير.

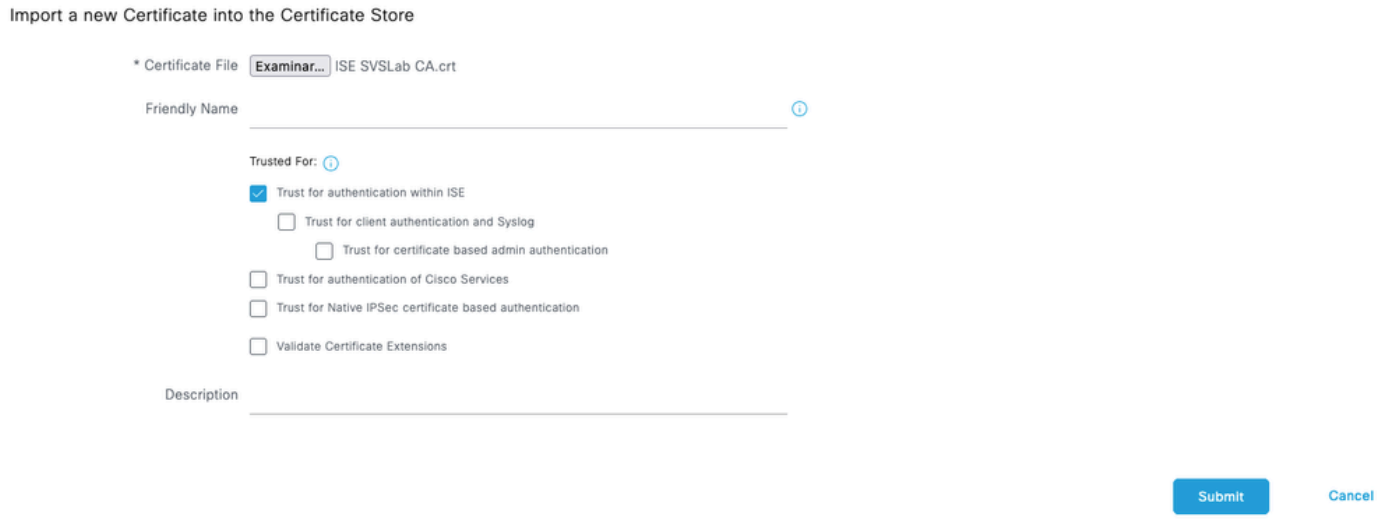
الآن، يمكنك الحصول على الشهادة (CRT) موقعة من هيئة الترخيص (CA).

تحميل شهادة المرجع المصدق الجذر لمصادقة خادم TACACS+

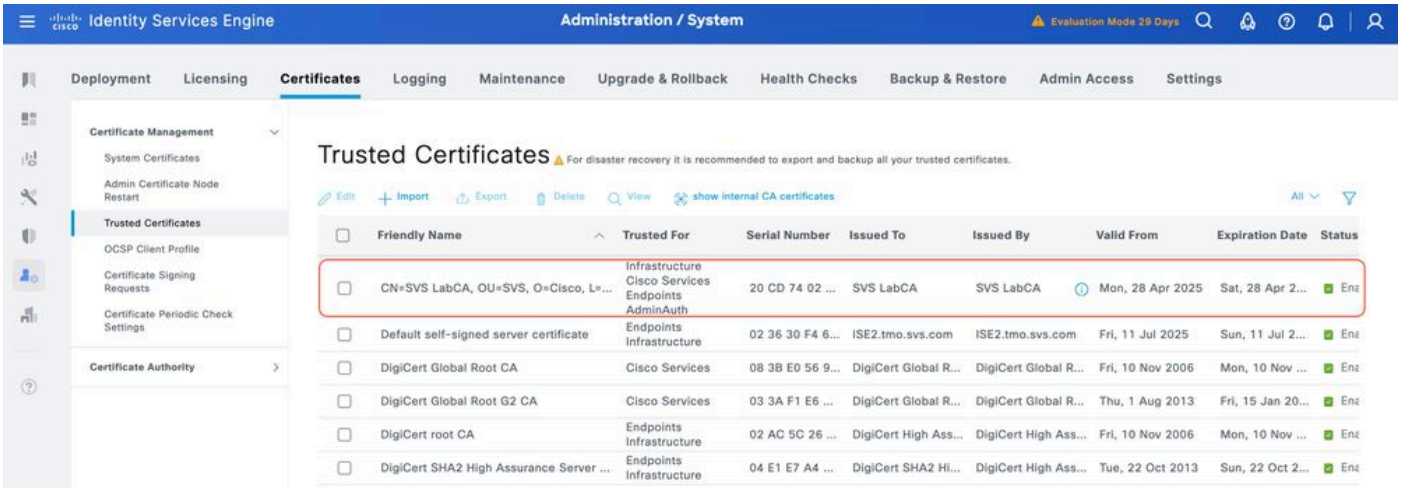
الخطوة 1. انتقل إلى الإدارة > النظام > الشهادات. تحت التراخيص المضمونة، انقر على إستيراد.



الخطوة 2. حدد الشهادة الصادرة عن المرجع المصدق (CA) التي وقعت طلب توقيع شهادة TACACS (CSR) الخاص بك. تأكد من تمكين خيار الثقة للمصادقة ضمن ISE.



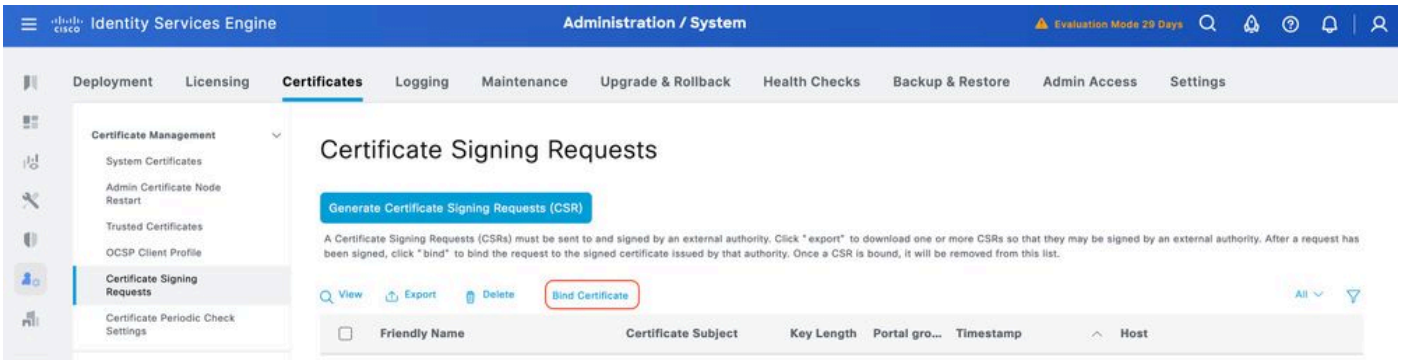
انقر على إرسال. يجب أن تظهر الشهادة الآن ضمن الشهادات الموثوق بها.



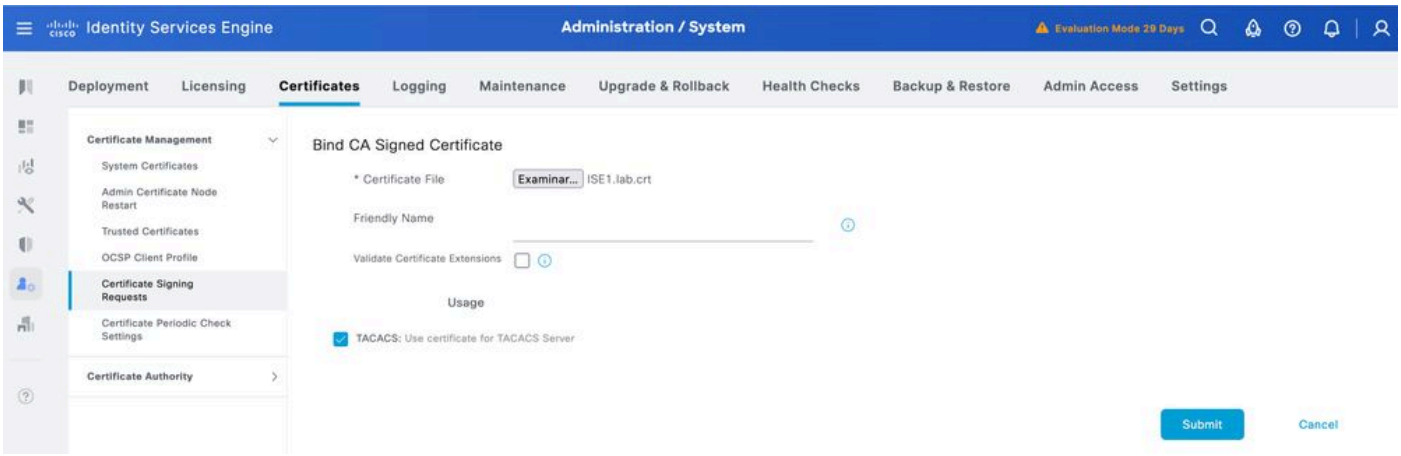
ربط طلب توقيع الشهادة الموقع (CSR) ب ISE

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.

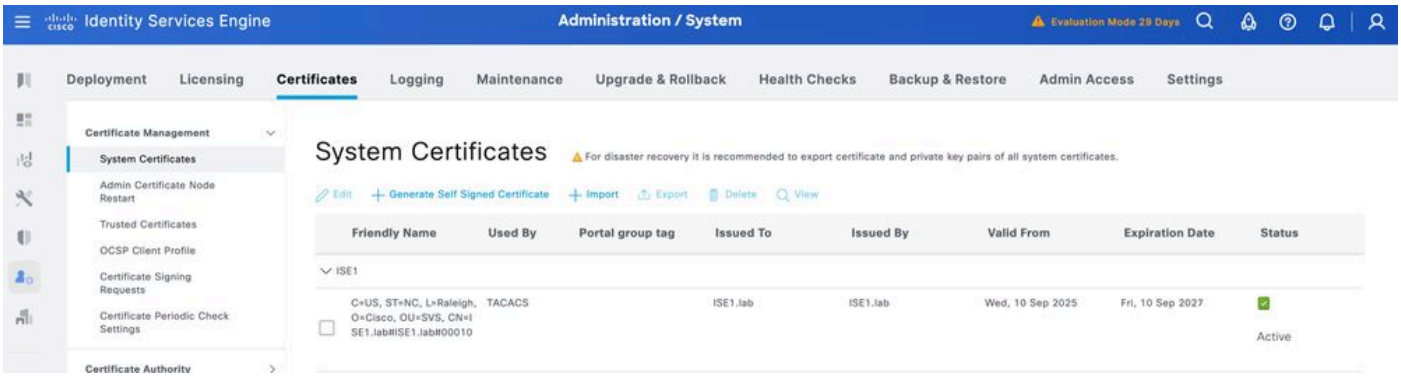


الخطوة 2. حدد الشهادة الموقعة وتأكد من أن خانة الاختيار TACACS الموجودة تحت الاستخدام لا تزال محددة.



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

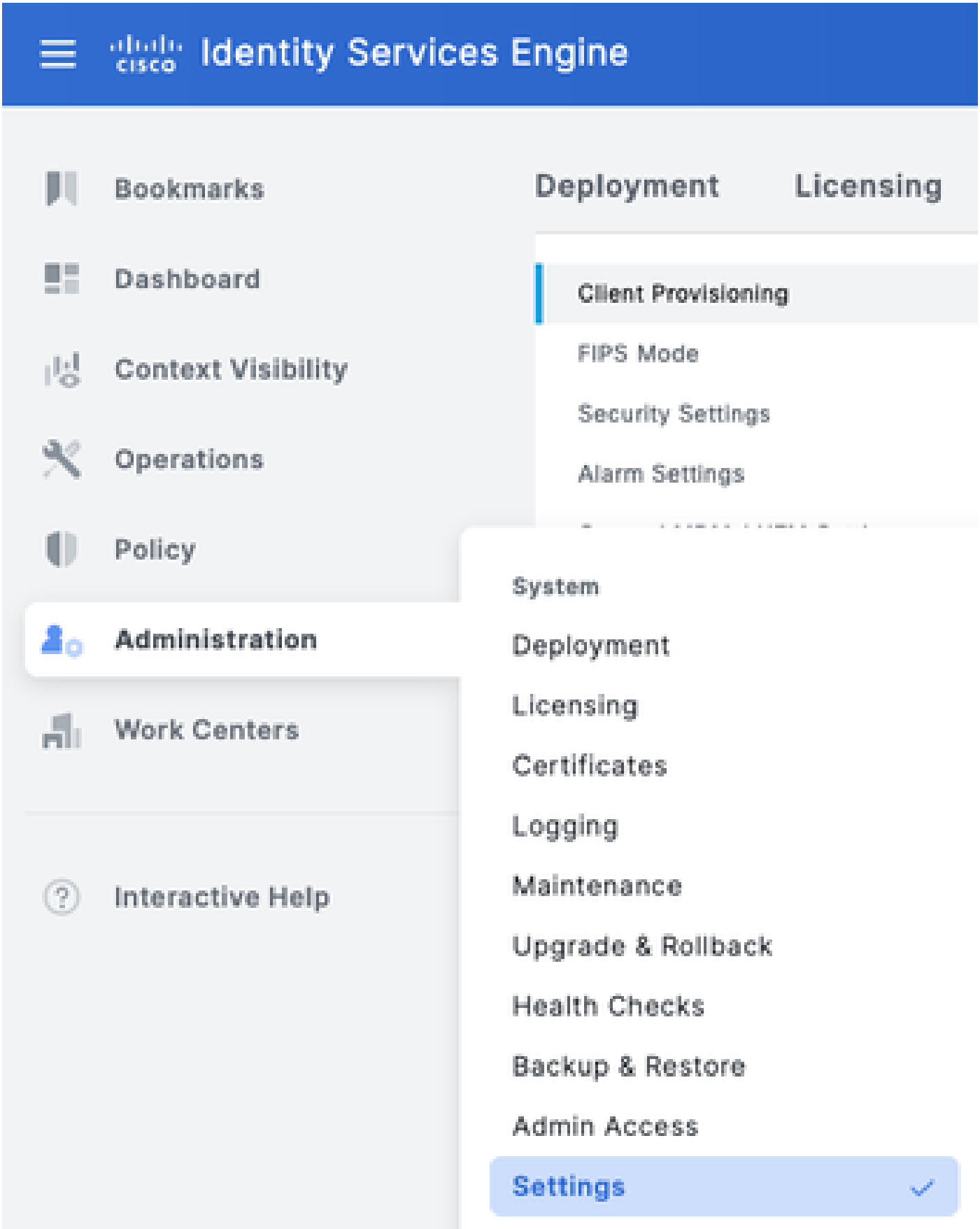
يجب تثبيت الشهادة الآن بشكل صحيح. يمكنك التحقق من ذلك ضمن شهادات النظام.



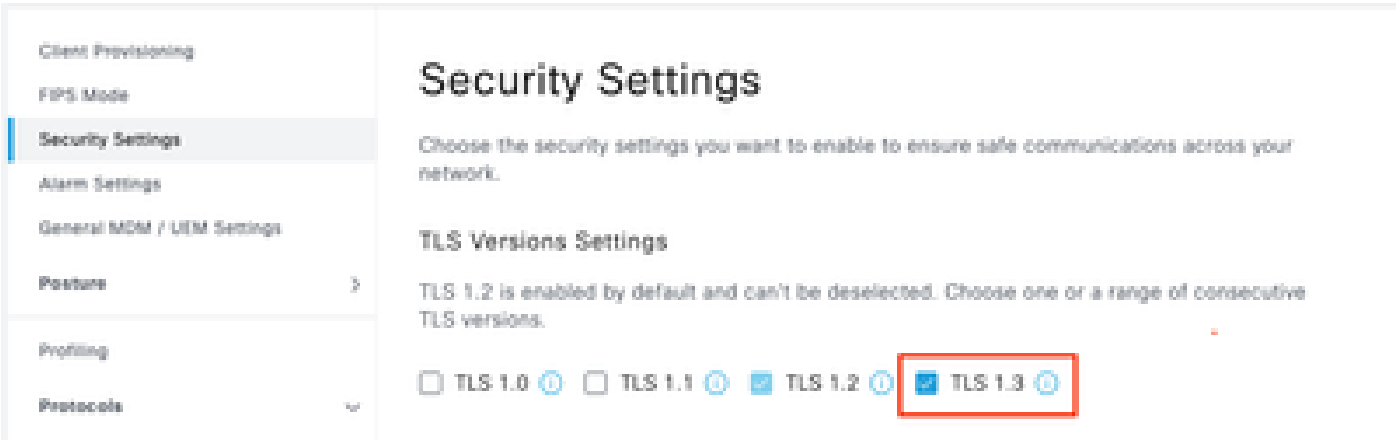
تمكين TLS 1.3

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

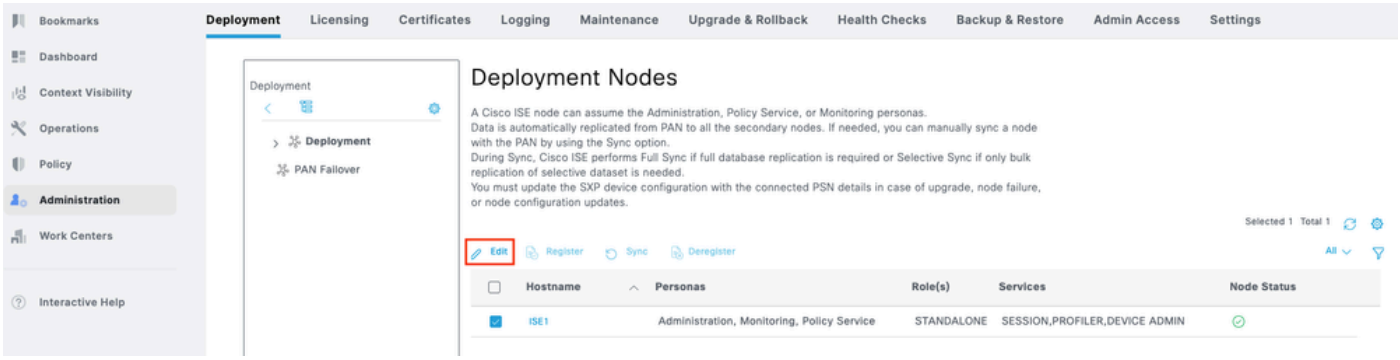


تحذير: عند تغيير إصدار TLS، تتم إعادة تشغيل خادم تطبيق Cisco ISE على جميع أجهزة النشر Cisco ISE.

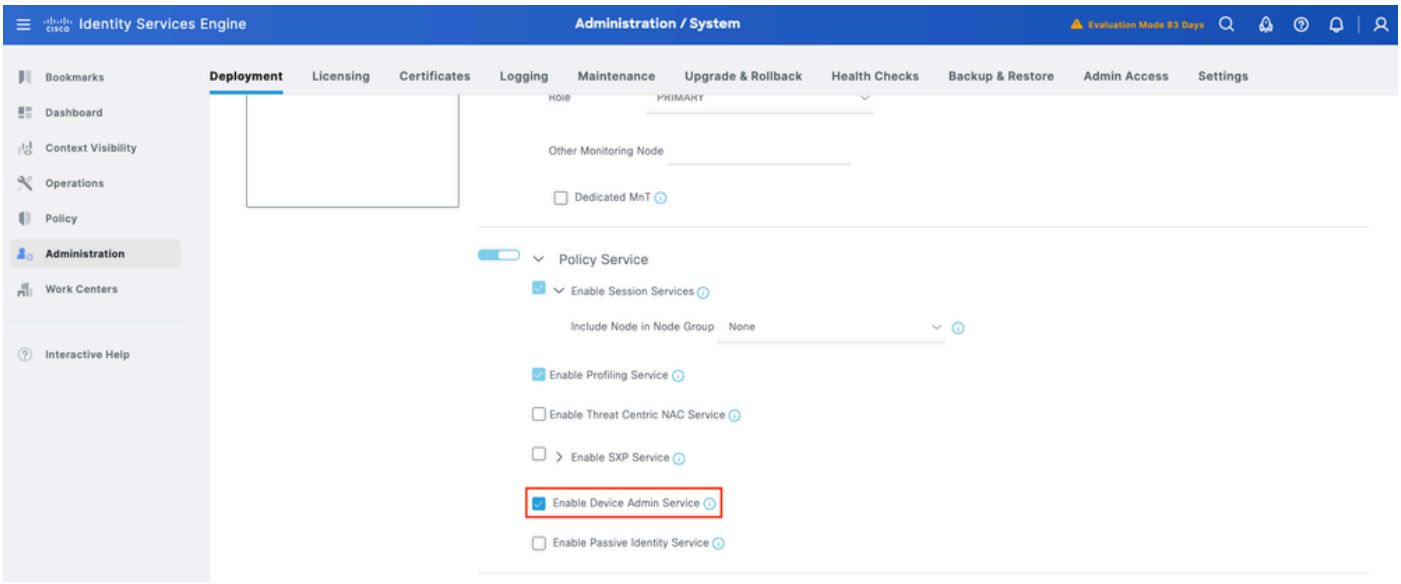
تمكين إدارة الأجهزة على ISE

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

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



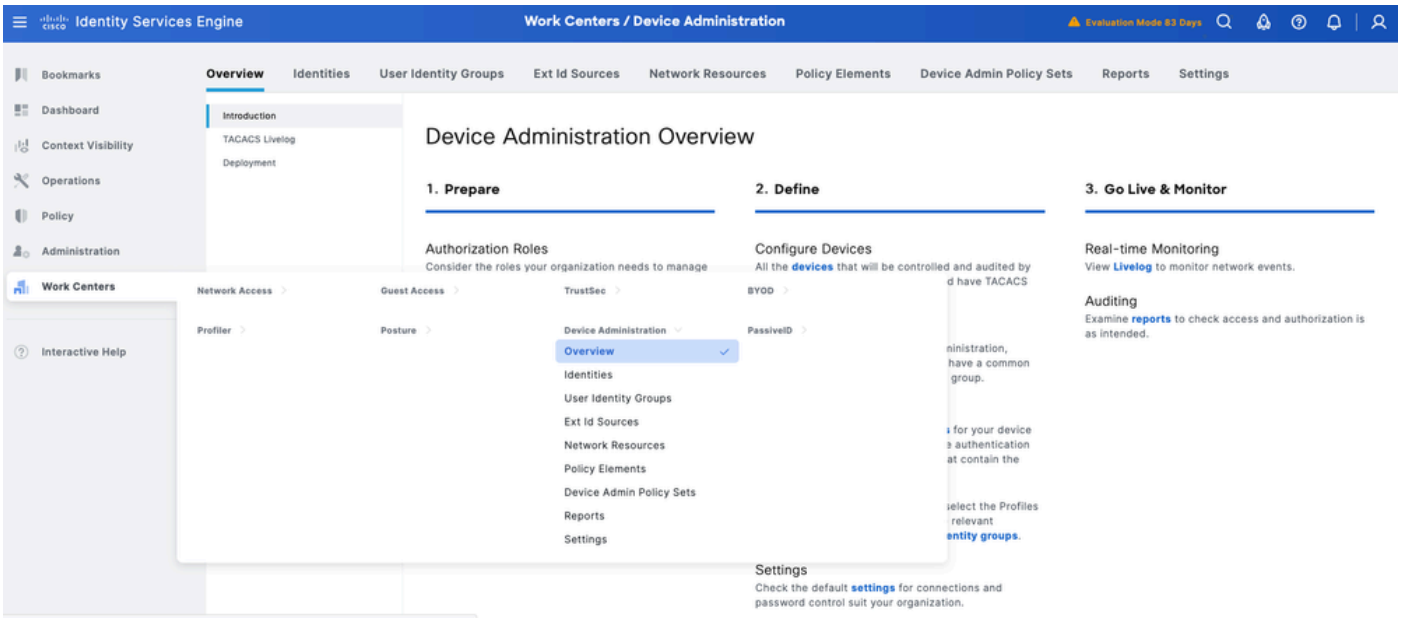
الخطوة 2. تحت الإعدادات العامة، قم بالتمرير إلى أسفل وحدد خانة الاختيار المجاورة ل تمكين خدمة إدارة الأجهزة.



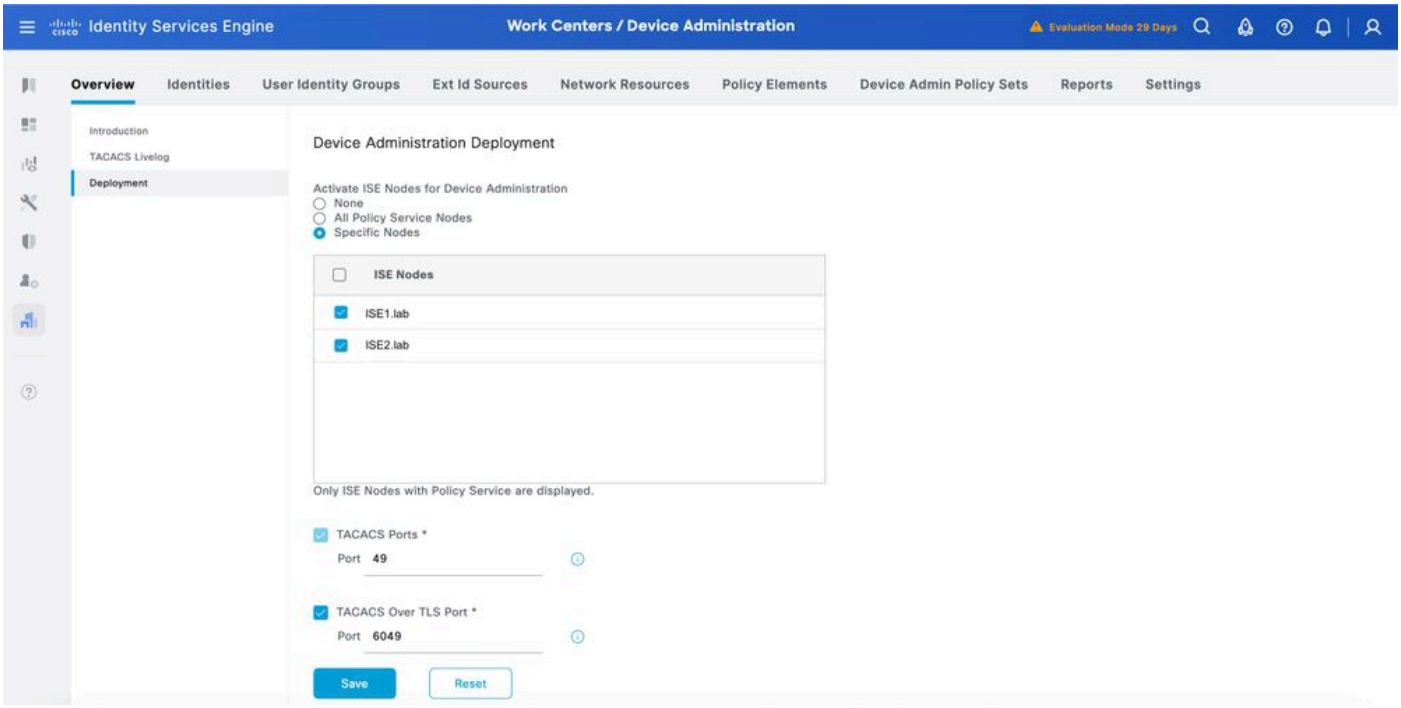
الخطوة 3. احفظ التكوين. تم تمكين "خدمة مسؤول الجهاز" الآن على ISE.

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.

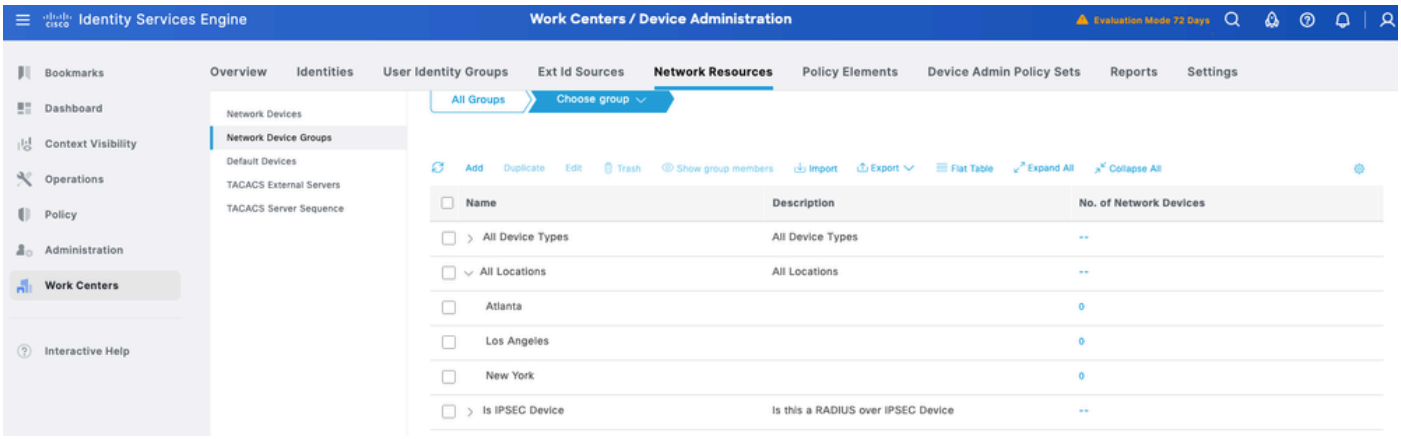


الخطوة 3. احفظ المنفذ الافتراضي 6049 أو حدد منفذ TCP مختلف لـ TACACS عبر TLS، ثم انقر فوق حفظ.

أجهزة الشبكة ومجموعات أجهزة الشبكة

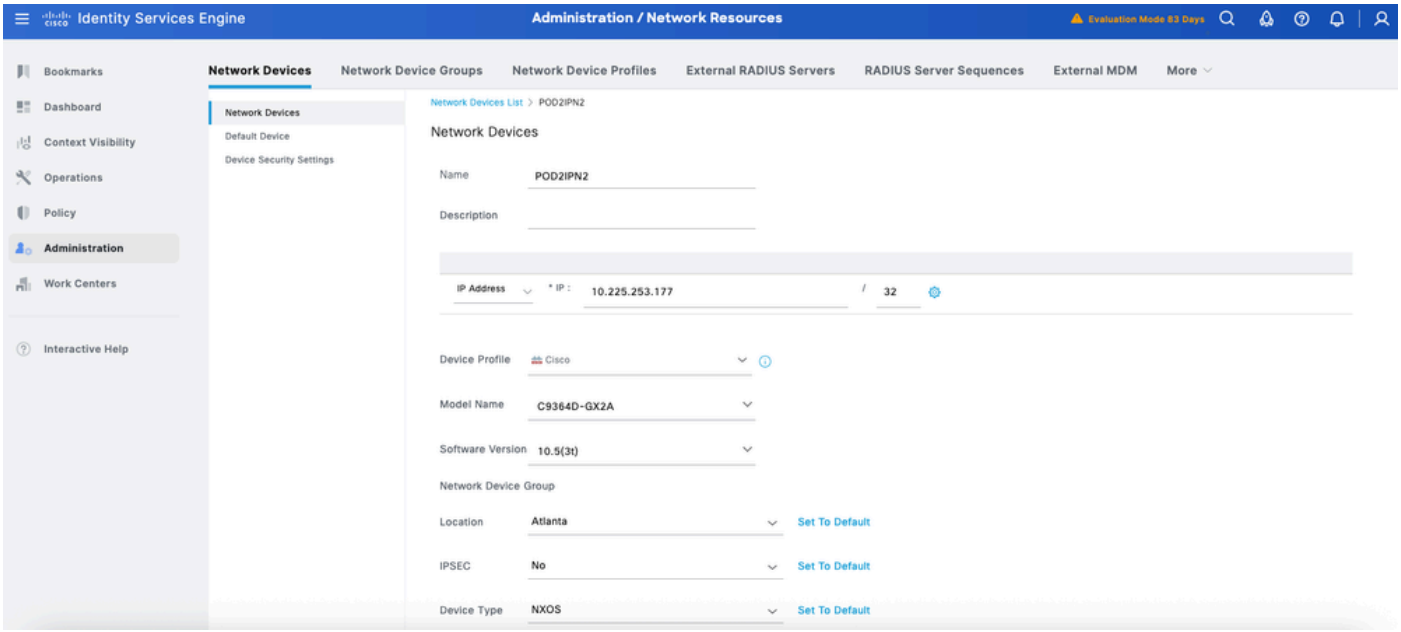
يوفر ISE تجميعا قويا للأجهزة بتسلسلات هرمية متعددة لمجموعات الأجهزة. يمثل كل تسلسل هيكلي تصنيفا متميزا ومستقلا لأجهزة الشبكة.

الخطوة 1. انتقل إلى مراكز العمل > إدارة الأجهزة > موارد الشبكة. انقر فوق مجموعات أجهزة الشبكة.

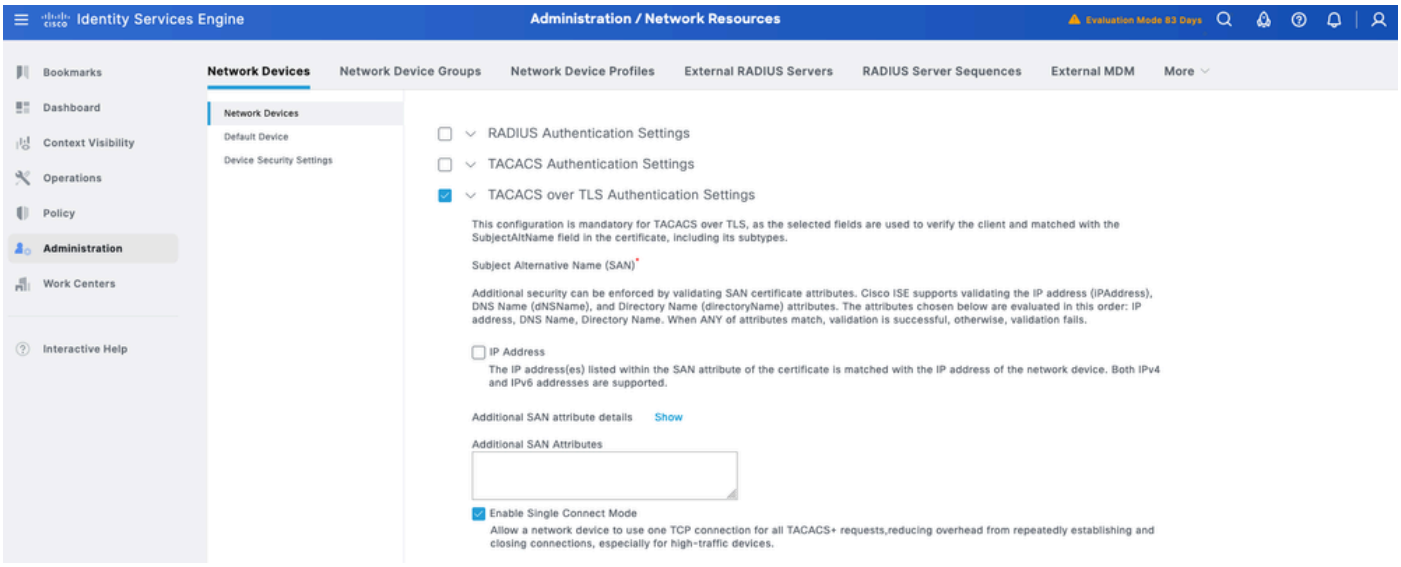


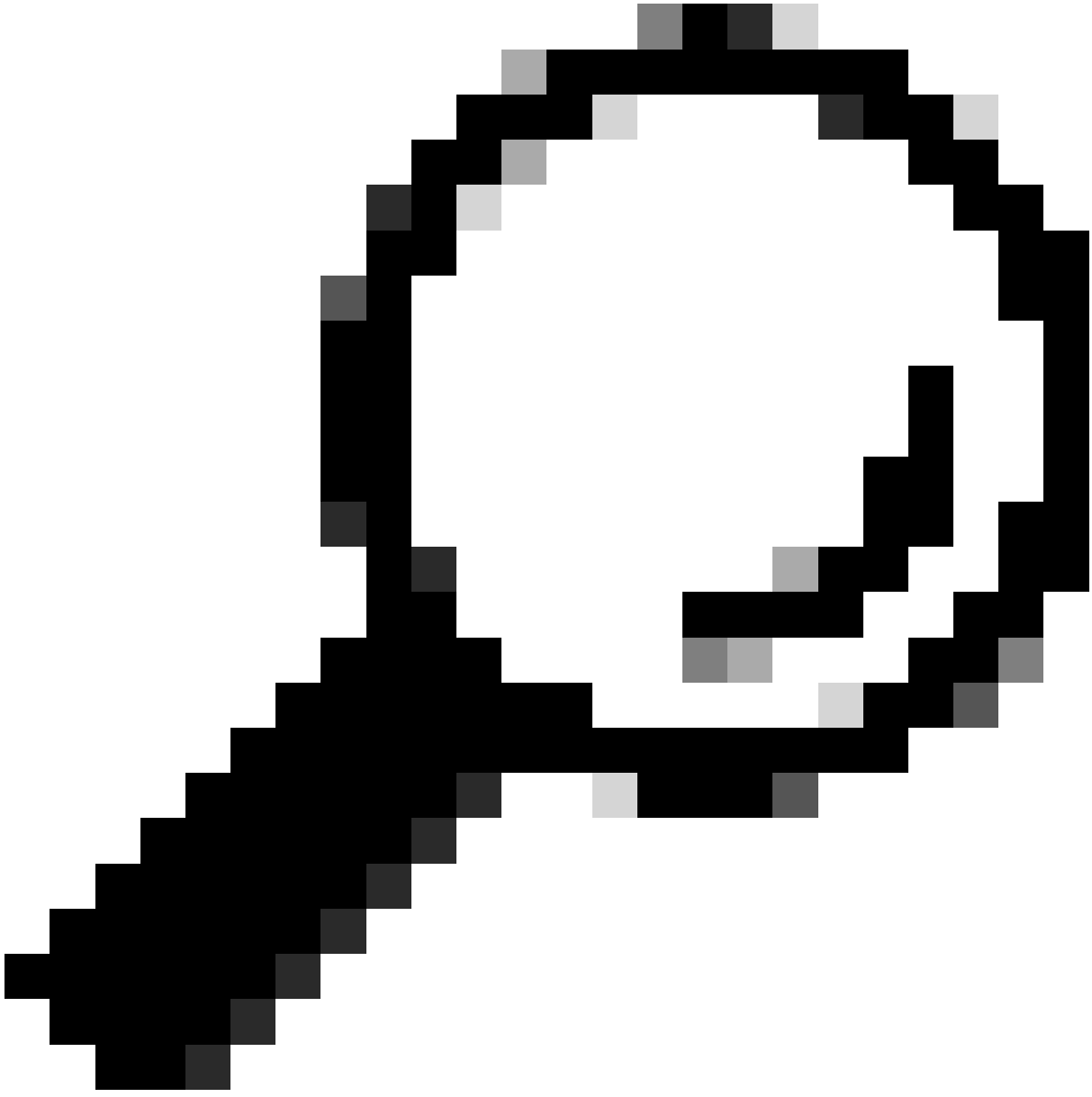
تعد جميع أنواع الأجهزة وكافة المواقع تسلسلات هرمية افتراضية يتم توفيرها بواسطة ISE. تقوم بإضافة التدرجات الهرمية الخاصة بك وتعريف المكونات المختلفة في تعريف جهاز الشبكة الذي يمكن إستخدامه لاحقا في حالة النهج.

الخطوة 2. الآن، أضف جهاز NS-OX كجهاز شبكة. انتقل إلى مركز العمل > إدارة الجهاز > موارد الشبكة. انقر على إضافة لإضافة جهاز شبكة جديد POD2IPN2.



يدخل خطوة 3. العنوان من الأداة ويتأكد أن يعين الموقع وأداة نوع للجهاز. أخيرا، قم بتمكين إعدادات مصادقة TACACS+ عبر TLS.


Identity Services Engine
Administration / Network Resources
Evaluation Mode 83 Days
Bookmarks
Dashboard
Context Visibility
Operations
Policy
Administration
Work Centers
Interactive Help
Network Devices
Network Device Groups
Network Device Profiles
External RADIUS Servers
RADIUS Server Sequences
External MDM
More
Network Devices
Default Device
Device Security Settings
RADIUS Authentication Settings
TACACS Authentication Settings
TACACS over TLS Authentication Settings
This configuration is mandatory for TACACS over TLS, as the selected fields are used to verify the client and matched with the SubjectAltName field in the certificate, including its subtypes.
Subject Alternative Name (SAN)*
Additional security can be enforced by validating SAN certificate attributes. Cisco ISE supports validating the IP address (IPAddress), DNS Name (dNSName), and Directory Name (directoryName) attributes. The attributes chosen below are evaluated in this order: IP address, DNS Name, Directory Name. When ANY of attributes match, validation is successful, otherwise, validation fails.
IP Address
The IP address(es) listed within the SAN attribute of the certificate is matched with the IP address of the network device. Both IPv4 and IPv6 addresses are supported.
Additional SAN attribute details
Show
Additional SAN Attributes
Enable Single Connect Mode
Allow a network device to use one TCP connection for all TACACS+ requests,reducing overhead from repeatedly establishing and closing connections, especially for high-traffic devices.

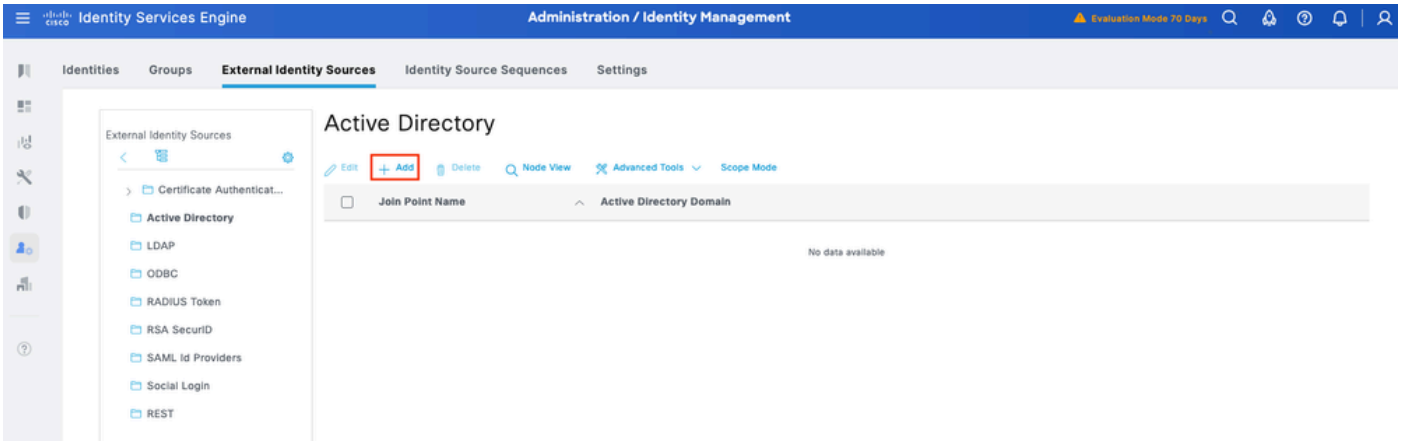


تلميح: يوصى بتمكين وضع الاتصال المفرد لتجنب إعادة تشغيل جلسة عمل TCP في كل مرة يتم إرسال أمر فيها إلى الجهاز.

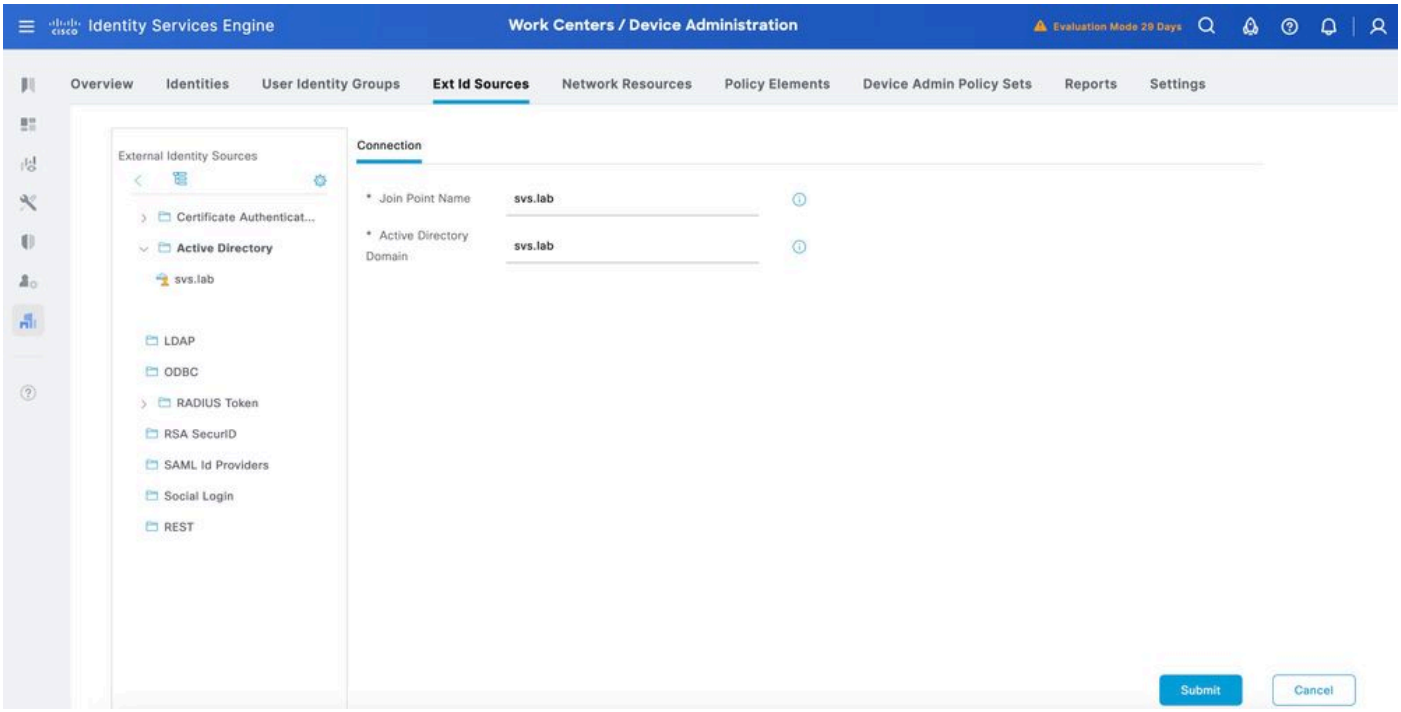
تكوين مخازن الهوية

يحدد هذا القسم مخزن هوية لمسؤولي الأجهزة، والذي يمكن أن يكون مستخدمي ISE الداخليين وأي 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 إضافة لتحديد نقطة AD مشتركة جديدة.

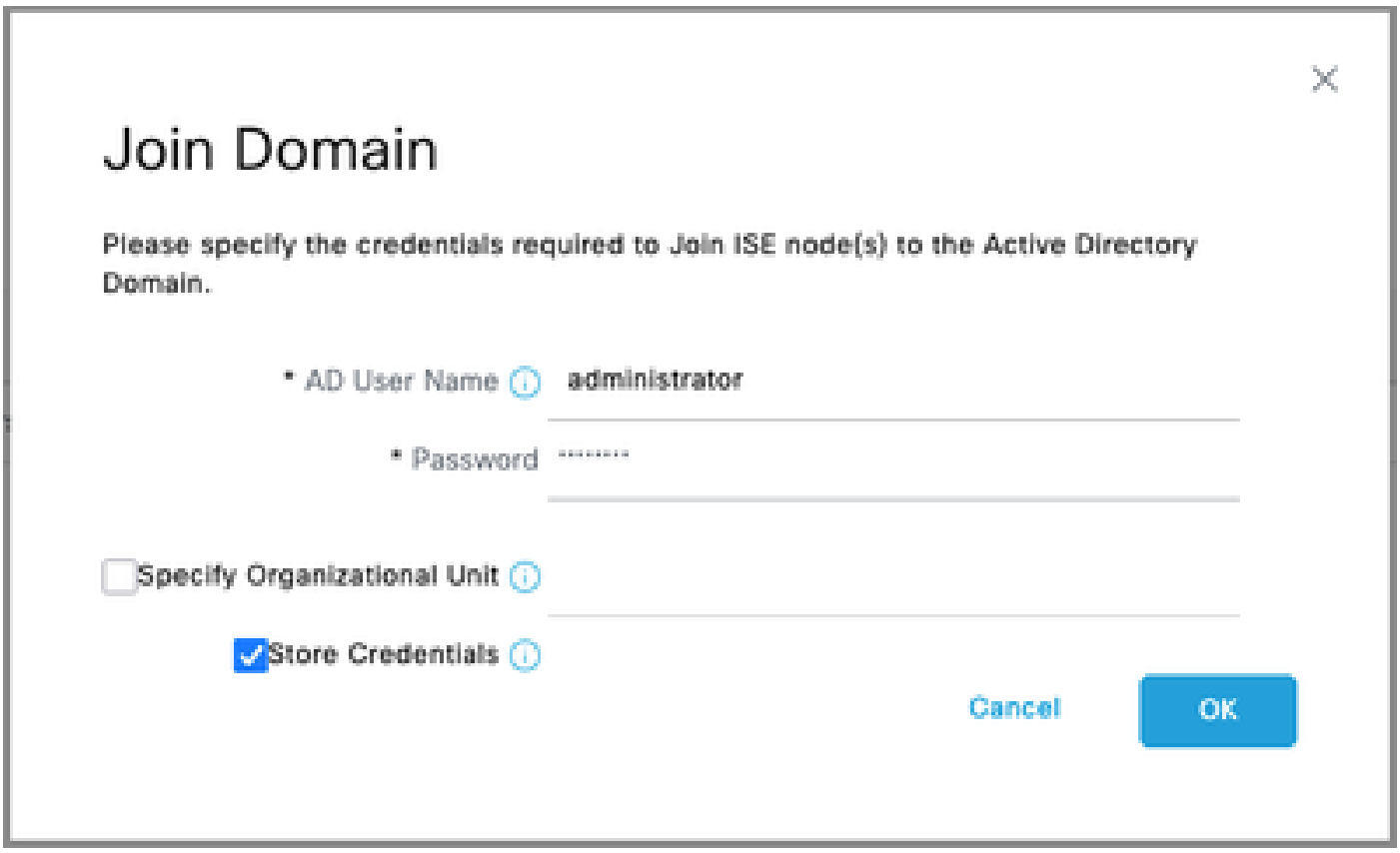


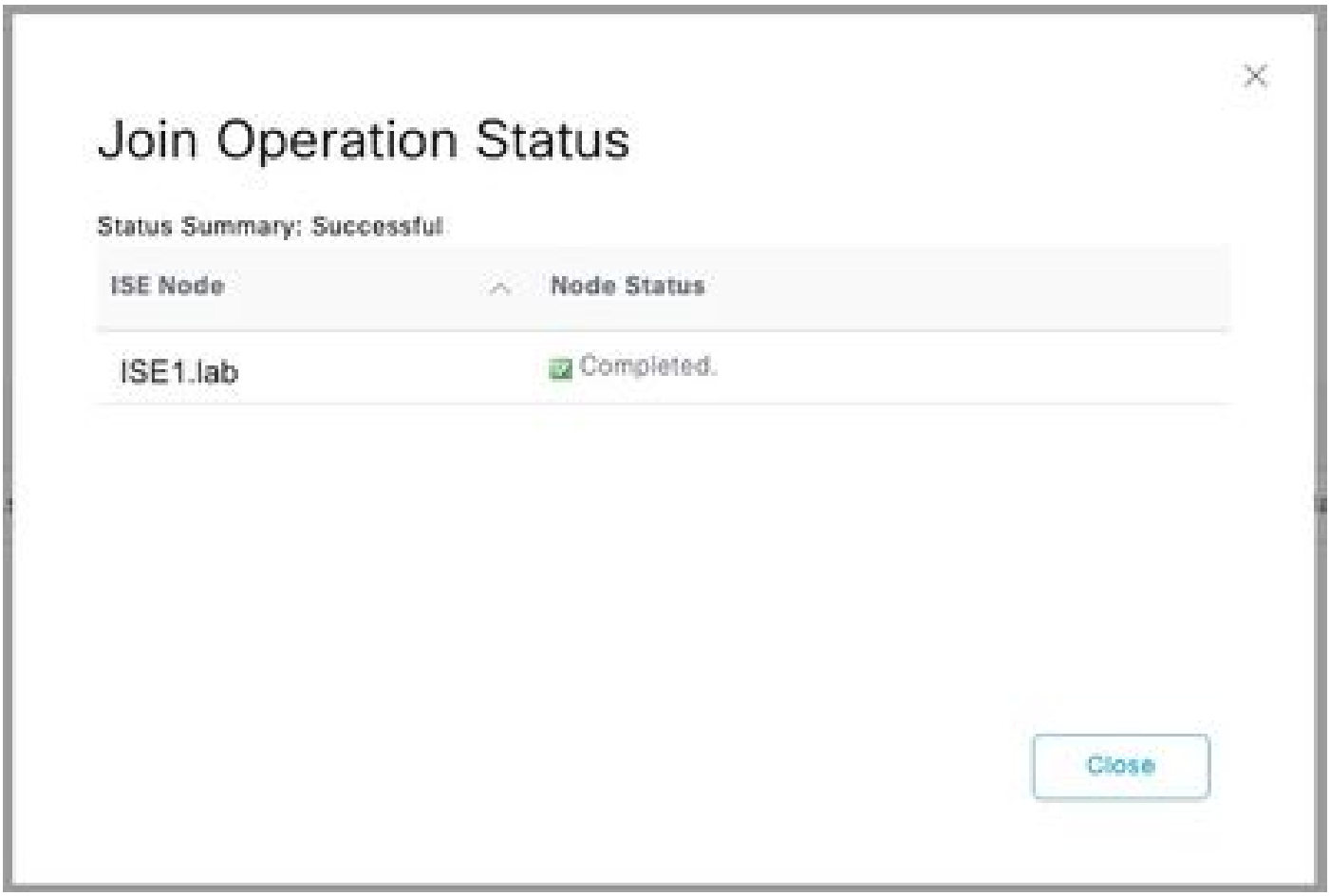
الخطوة 2. حدد اسم نقطة الربط واسم مجال AD وانقر إرسال.



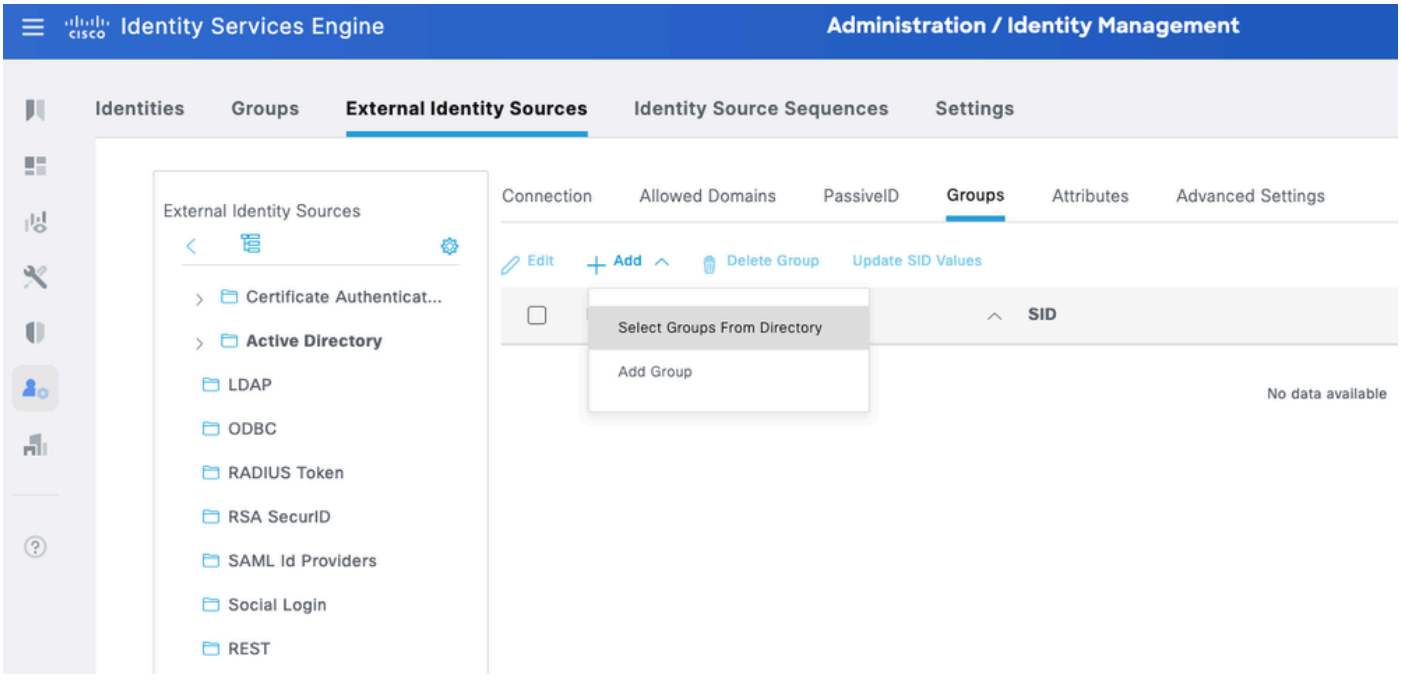
الخطوة 3. انقر فوق نعم عند مطالبتك "هل ترغب في ضم جميع عقد ISE إلى مجال Active Directory هذا؟ "

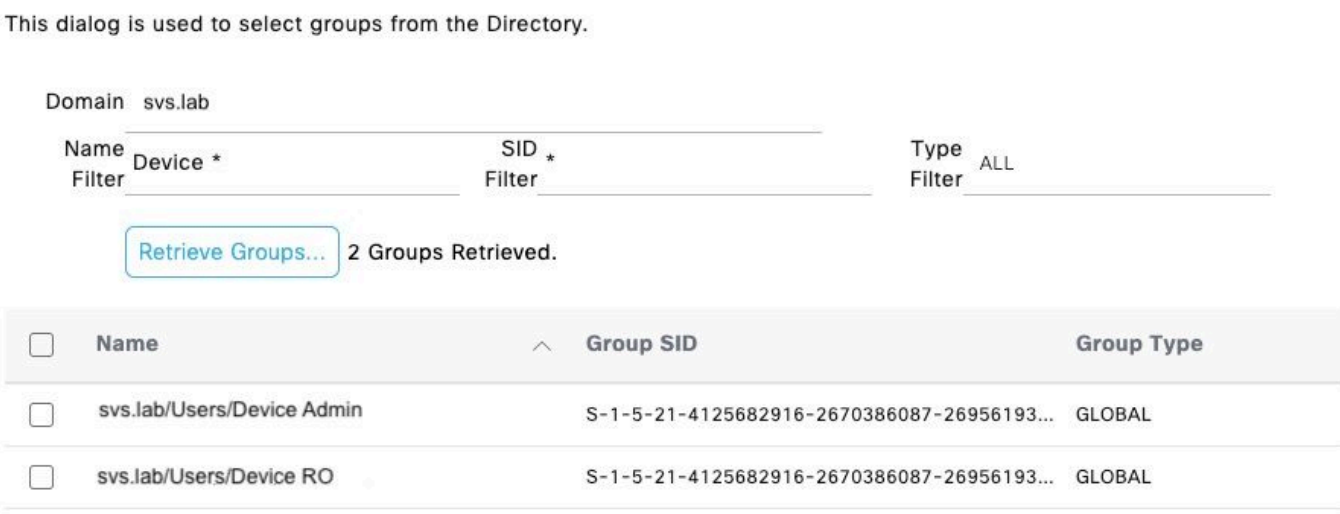
الخطوة 4. أدخل بيانات الاعتماد بامتيازات AD Join وانضم ISE إلى AD. تحقق من الحالة للتحقق من أنها تعمل.

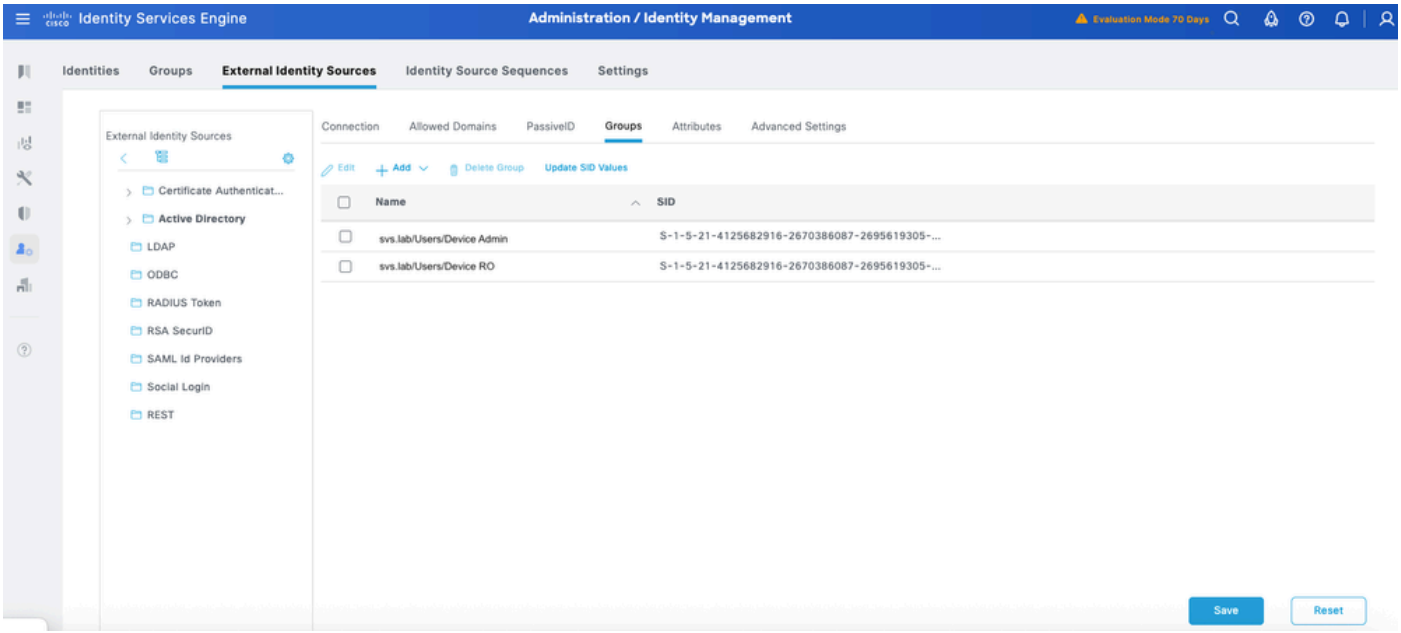




الخطوة 5. انتقل إلى علامة التبويب مجموعات، وانقر فوق إضافة للحصول على جميع المجموعات المطلوبة على أساس المجموعات المسموح للمستخدمين بالوصول إليها من قبل الجهاز. يوضح هذا المثال المجموعات المستخدمة في نهج التخويل في هذا الدليل.







تكوين ملفات تعريف TACACS+ Shell

بخلاف أجهزة Cisco IOS، التي تستخدم مستويات الامتيازات للتفويض، تقوم أجهزة Cisco NX-OS بتنفيذ التحكم في الوصول المستند إلى الدور (RBAC). في ISE، يمكنك تعيين توصيفات TACACS+ لأدوار المستخدمين على أجهزة Cisco NX-OS باستخدام المهام المشتركة من نوع Nexus.

تختلف الأدوار المحددة مسبقا على أجهزة NX-OS بين أنظمة NX-OS الأساسية. إثنان من الأشياء الشائعة هما:

- network-admin - يحتوي دور مسؤول الشبكة المحدد مسبقا على وصول كامل للقراءة والكتابة إلى جميع الأوامر على المحول؛ متوفر في سياق الجهاز الظاهري الافتراضي (VDC) فقط إذا كانت الأجهزة (على سبيل المثال، Nexus 7000) تحتوي على العديد من منافذ VDC. أستخدم الأمر NX-OS CLI show cli بناء أدوار الشبكة-admin للاطلاع على

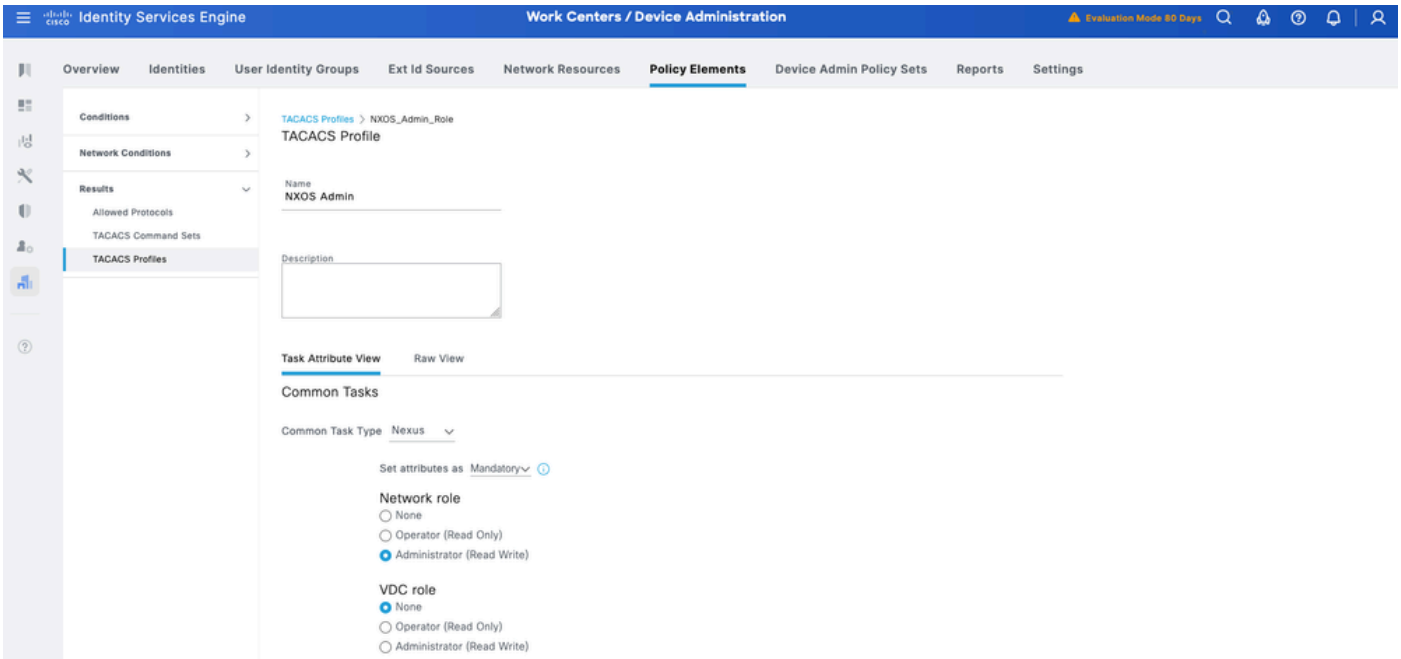
قائمة الأوامر الكاملة المتوفرة لهذا الدور.
- network-operator - يتمتع دور مسؤول الشبكة المحدد مسبقا بحق الوصول الكامل للقراءة إلى جميع الأوامر على المحول؛ متوفر في وحدة التحكم في الوصول عن بعد (VDC) الافتراضية فقط إذا كانت الأجهزة (على سبيل المثال، Nexus 7000) تحتوي على العديد من نقاط الوصول عن بعد (VDC). أستخدم الأمر NX-OS CLI show cli syntax roles network-operator لعرض قائمة الأوامر الكاملة المتوفرة لهذا الدور.

وبعد ذلك، يتم تحديد ملف تعريف TACACS - مسؤول NXOS ومكتب المساعدة NXOS.

إدارة NX-OS

الخطوة 1. أضف ملف تعريف آخر واسمه إدارة NX-OS.

الخطوة 2. حدد إلزامي من تعيين السمات كقائمة منسدلة. حدد مسؤول من خيار دور الشبكة ضمن المهام المشتركة.



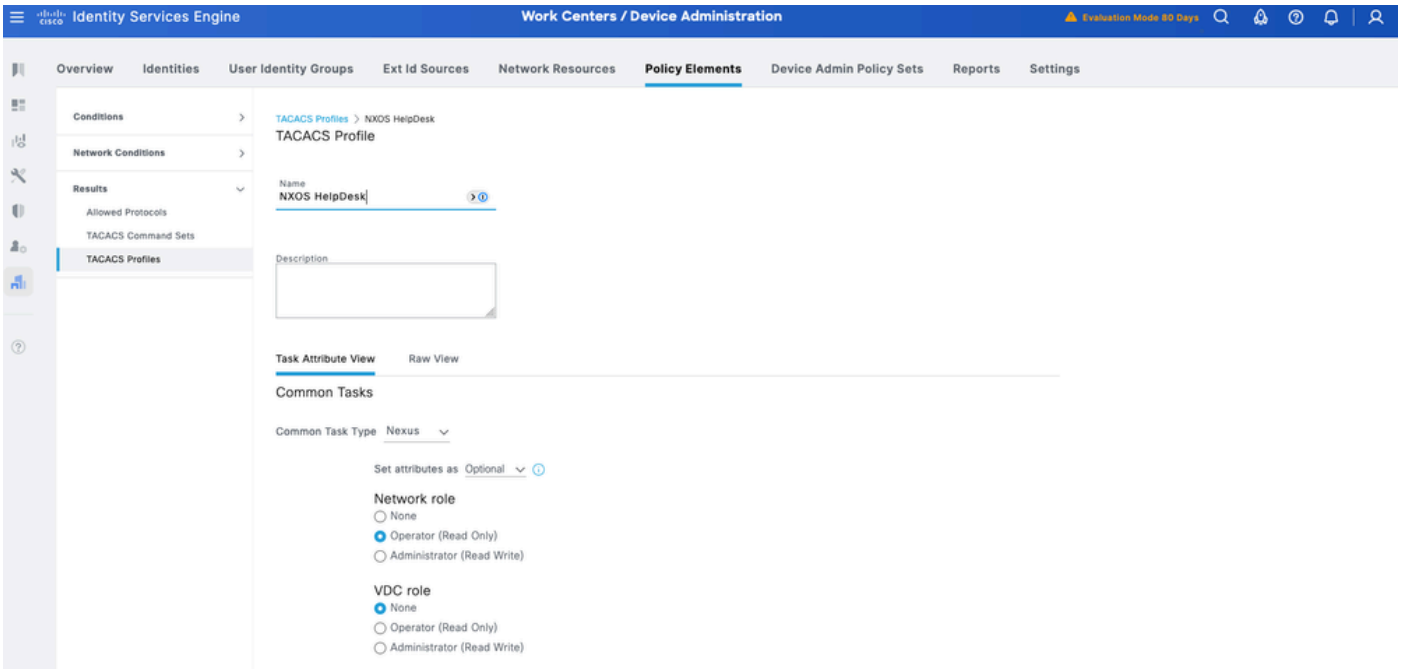
الخطوة 3. انقر على إرسال لحفظ ملف التعريف.

مكتب مساعدة NX-OS

الخطوة 1. من واجهة مستخدم ISE، انتقل إلى مراكز العمل > إدارة الأجهزة > عناصر السياسة > النتائج > ملفات تعريف TACACS. قم بإضافة ملف تعريف TACACS جديد وتسميته NXOS HelpDesk. انتقل إلى القائمة المنسدلة "نوع المهمة المشتركة" واختر Nexus.

يمكنك رؤية تغييرات القالب الخاصة بدور المستخدم. يمكنك تحديد هذه الخيارات المتوافقة مع دور المستخدم الذي تريد تكوينه.

الخطوة 2. حدد إلزامي من تعيين السمات كقائمة منسدلة. حدد عامل التشغيل من خيار دور الشبكة ضمن المهام المشتركة.

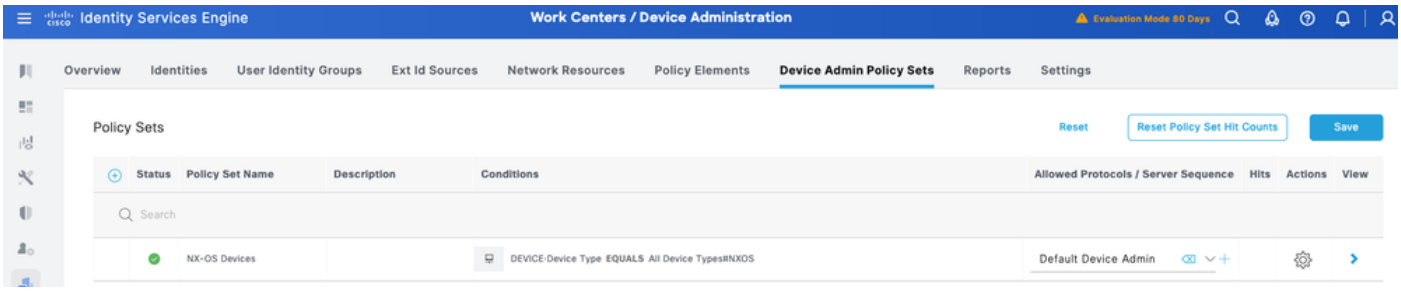


الخطوة 3. انقر على حفظ لحفظ ملف التخصيص.

تكوين مجموعات نهج مسؤول الجهاز

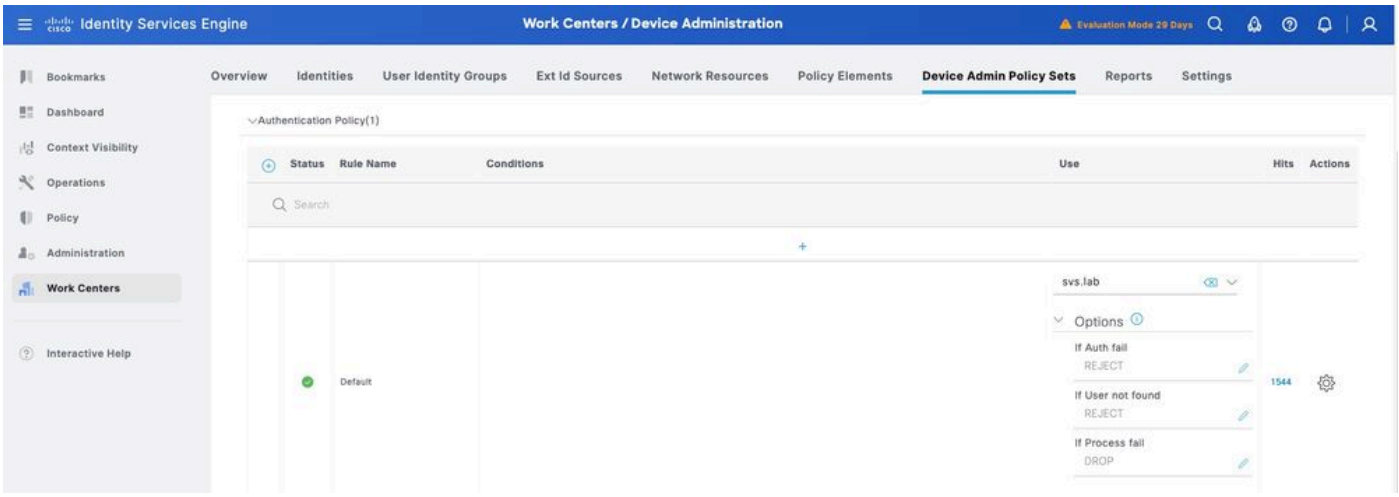
يتم تمكين مجموعات النهج بشكل افتراضي لإدارة الأجهزة. يمكن أن تقسم مجموعات السياسات استنادا إلى أنواع الأجهزة لتسهيل تطبيق ملفات تعريف TACACS. على سبيل المثال، تستخدم أجهزة Cisco IOS مستويات الامتيازات و/أو مجموعات الأوامر بينما تستخدم أجهزة NX-OS من Cisco سمات مخصصة.

الخطوة 1. انتقل إلى مراكز العمل > إدارة الأجهزة > مجموعات سياسات إدارة الأجهزة. إضافة أجهزة NX-OS لمجموعة نهج جديدة. تحت شرط، حدد DEVICE:Device Type يساوي جميع أنواع الأجهزة#NXOS. تحت البروتوكولات المسموح بها، حدد مسؤول الجهاز الافتراضي.



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

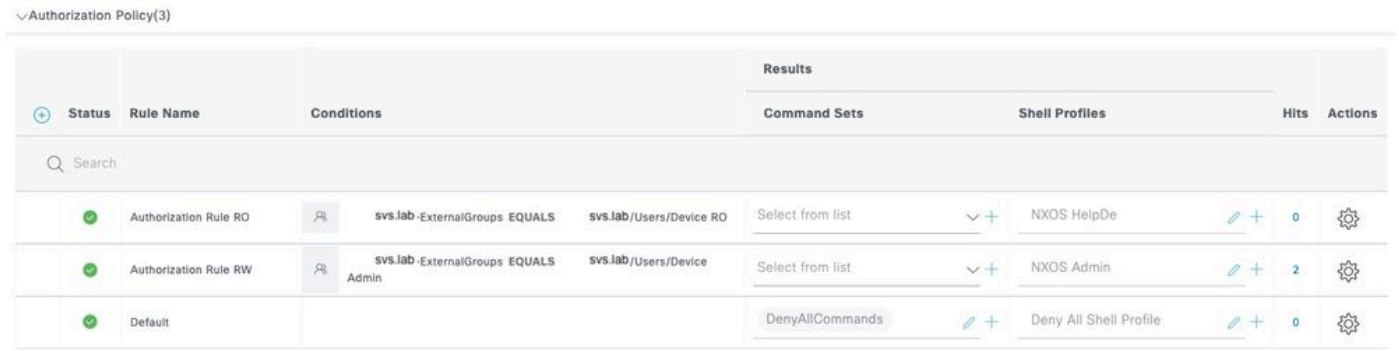
الخطوة 3. إنشاء سياسة المصادقة. للمصادقة، تستخدم AD كمخزن معرف. أترك الخيارات الافتراضية تحت إذا فشلت المصادقة، إذا لم يتم العثور على المستخدم وإذا فشلت العملية.



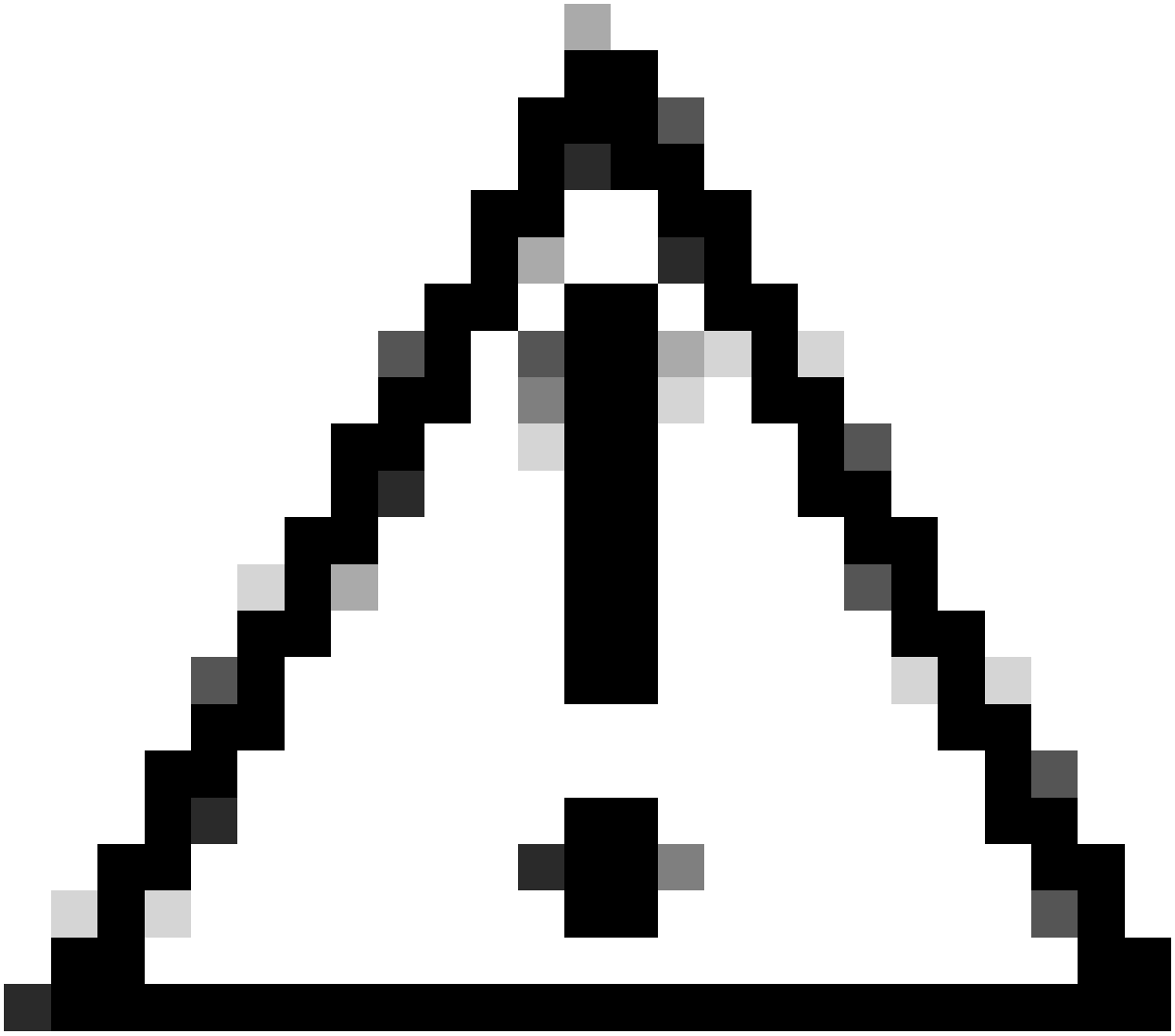
الخطوة 4. تحديد سياسة التفويض.

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

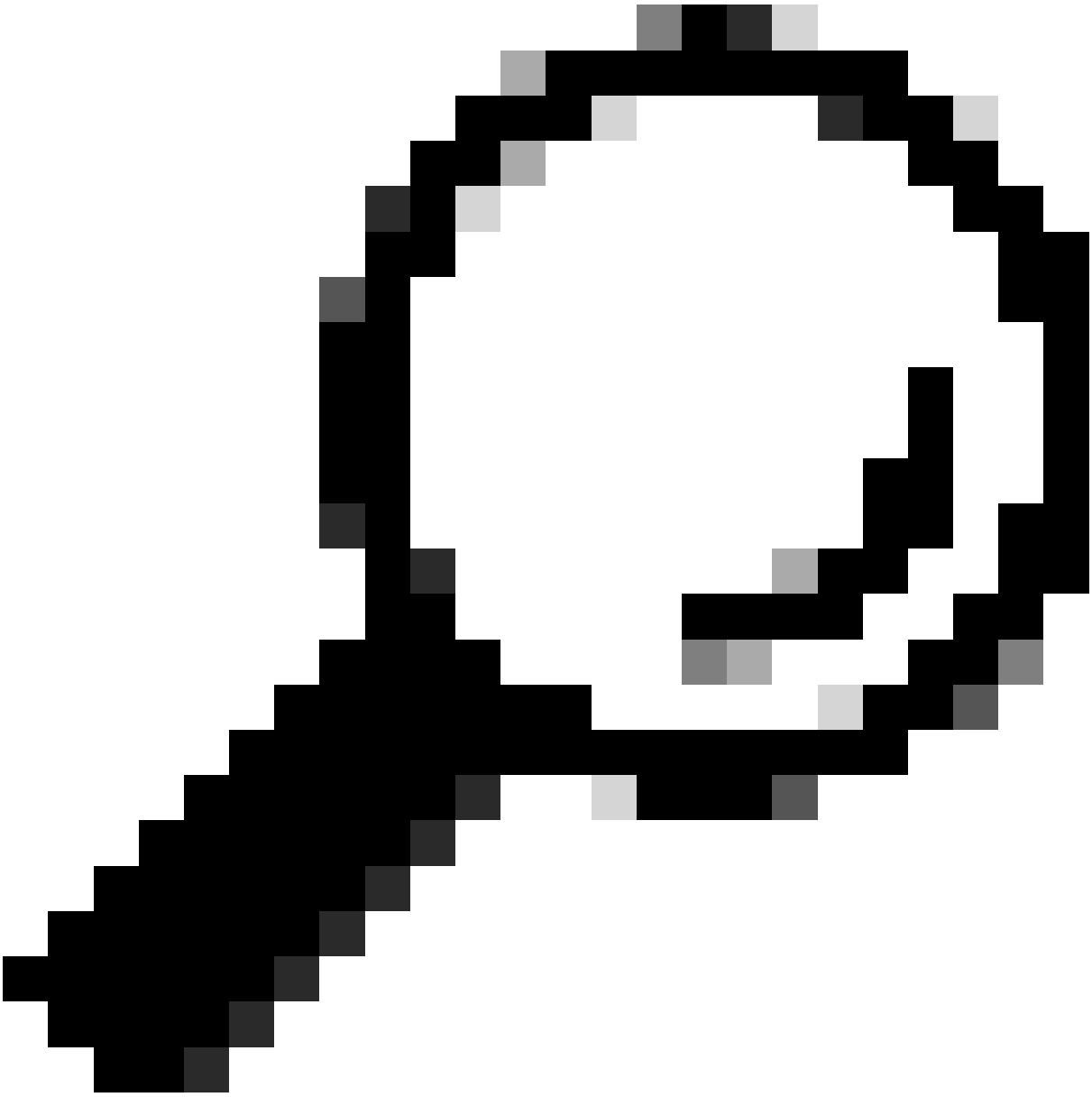
على سبيل المثال:
· يتم تعيين ملف تعريف TACACS الخاص بإدارة NXOS للمستخدمين في مسؤول مجموعة AD.
· يتم تعيين ملف تعريف TACACS لمكتب تعليمات NXOS للمستخدمين في جهاز مجموعة AD أو.



تكوين Cisco NX-OS ل TACACS+ عبر TLS



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 حسابه خارج الجهاز.

تكوين خادم TACACS+

الخطوة 1. التكوين الأولي.

```
POD2IPN2# sho run tacacs

feature tacacs+

tacacs-server host 10.225.253.209 key 7 "F1whg.123"
aaa group server tacacs+ tacacs2
```

```
  server 10.225.253.209
  use-vrf management
```

تكوين TrustPoint

الخطوة 1. قم بإنشاء تسمية مفتاح، في حالتك، أستخدم زوج مفاتيح ECC.

<#root>

POD2IPN2(config)#

crypto key generate ecc label ec521-label exportable modulus 521

الخطوة 2. أربط هذه النقطة الثقة.

<#root>

POD2IPN2(config)#

crypto ca trustpoint ec521-tp

POD2IPN2(config-trustpoint)#

ecckeypair ec521-label

الخطوة 3. قم بتثبيت المفتاح العام CA.

<#root>

POD2IPN2(config)#

crypto ca authenticate ec521-tp

```
input (cut & paste) CA certificate (chain) in PEM format;
end the input with a line containing only END OF INPUT :
-----BEGIN CERTIFICATE-----
MIIFlDCCA3ygAwIBAgIIIM1OAsTaN/UwDQYJKoZIhvcNAQELBQAwajELMAkGA1UE
BhMCVVMxFzAVBgNVBAgTDk5vcnRoIENhcm9saW5hMRAwDgYDVQQHEwdSYWxlaWdo
MQ4wDAYDVQQKEwVDaXNjbzEMMAoGA1UECxMDU1ZTMRIwEAYDVQQDEwlTVlMgTGFi
QOEwHhcNMjUwNDI4MTcwNTAwWhcNMzUwNDI4MTcwNTAwWjBqMQswCQYDVQQGEwJV
UzEXMBUGA1UECBMOTm9ydGggQ2Fyb2xpbmExEDAOBgNVBAcTB1JhbGVpZ2gxDjAM
BgNVBAoTBUNpc2NvMQwwCgYDVQQLEwNTVlMxEjAQBgNVBAMTCVNWUyBMYWJDQTCC
AiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIBAJvZUOyn2vIn6gKbx3M7vaRq
2YjwZlzSH6EkEvxnJTy+kksiFD33GyHQepk7vfp4NFU5OtQ4HC7t/AOv9grDa3QW
VwvV4MBbJhFM3s0J/ejgDYcMZhIAaPyOZo5WLboOkXEiKjPLatkXojB8FVrhLF3O
jMBSqwa4/Wlniy5S+7s4FFxsCf2OCOWfBAsnrs0tatIIhmcnx+VLJP7MRm8fOw4m
mutNo7IhbJSrgAFXmjlbBjMmgspObULo/wxMHdTbtPBf11HRHTkNIo3qyO4UADL2
WpoGhgT/FaxxBo2UBcnYVaP+jjRE0NYT973MCbVAAxtNVU6bEBR0z+LWniACzupm
+qh23SL43uW5A3iSw/BuU1E9p7B0e8oDNKU6gXlojKyLP/gC7j8AePO3ir+KZui8
```

```
b8X4iYn/67SbzZFhwxn3chkW4JYhQ4AImW1An2Q1+DMoZL7zRtSqQ3g9ZqRIMzQN
gJ+kQXe7QtT/u6m1MrtjE3gAEVpL334rTIxy9hpKZIkB86t2ZA3JX8CLsbCa13sA
z1XCoONX+6a1ekmXuAOI+t3c1sNbN2AtFi4cJovTAO1xh6OI4QnK+MNQKpTjt/E4
ydHlOrrurXsZummj9QBnkX4pqY7cDLHhdMKpbjDwg7jVLl783nTc9wYptQEPi5sw
83g9EMgKVOARIiVUa/qlAgMBAAGjPjA8MAwGA1UdEwQFMAMBAf8wEQYJYIZIAYb4
QgEBBAQDAgAHMBkGCWCGSAGG+EIBDQQMFgpTVlMgTGFiIENBMAOGCSqGSIb3DQEB
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/qd2NRSBWffFOXE/AJHQG7STT
HaXLU9r2Ko6O3oecu8ysGTwLlIt/9T1/FOb0xZRugWcpJrVoTgDGuA==
-----END CERTIFICATE-----
```

END OF INPUT

```
Fingerprint(s): SHA1
Fingerprint=0E:B1:81:E9:5A:3E:D7:80:3B:C5:A8:05:9A:85:4A:95:C8:3A:C7:37

Do you accept this certificate? [yes/no]:yes
POD2IPN2(config)#
POD2IPN2(config)#
```

show crypto ca certificates ec521-tp

```
Trustpoint: ec521-tp
CA certificate 0:
subject=C = US, ST = North Carolina, L = Raleigh, O = Cisco, OU = SVS, CN = SVS LabCA
issuer=C = US, ST = North Carolina, L = Raleigh, O = Cisco, OU = SVS, CN = SVS LabCA
serial=20CD7402C4DA37F5
notBefore=Apr 28 17:05:00 2025 GMT
notAfter=Apr 28 17:05:00 2035 GMT
SHA1 Fingerprint=0E:B1:81:E9:5A:3E:D7:80:3B:C5:A8:05:9A:85:4A:95:C8:3A:C7:37
purposes: sslserver sslclient
POD2IPN2(config)#
```

الخطوة 4. إنشاء طلب شهادة هوية المحول.

<#root>

```
POD2IPN2(config)#
```

crypto ca enroll ec521-tp

```
 Create the certificate request ..
 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:C1sco.123
 The subject name in the certificate will be the name of the switch.
 Include the switch serial number in the subject name? [yes/no]:
```

yes

```
 The serial number in the certificate will be: FDO2649OP4T
 Include an IP address in the subject name [yes/no]:
```

yes

```
ip address:10.225.253.177
 Include the Alternate Subject Name ? [yes/no]:
```

no

```
 The certificate request will be displayed...
-----BEGIN CERTIFICATE REQUEST-----
MIIBtjCCARcCAQAwKTERMA8GA1UEAwwIUE9EMklQTjIxFDASBgNVBAUTC0ZETzI2
NDkwUDRUMIGbMBAGByqGSM49AgEGBSuBBAAjA4GGAAQBGYT0iw7OvqIKQ/a22Lkg
Na9IhqWQvetjxKq485gqTSBEo6LzpkOhPAGE4jBveNHxYeIA7PfNWvJ7xTBWjDNX
/IYBm6E7Hd7q42OmCe8Mef+bqJBdJ9wzpyEjhI2lIIoXt4814nBxObkIWWyR5cZN
IiXTLk8P4IMZvPq8jRnELRxd8RGgSTAYBgkqhkiG9w0BCQcxCwwJQzFzY28uMTIz
MC0GCSqGSIb3DQEJDjEgMB4wHAYDVR0RAQH/BBIwEIIIUE9EMklQTjKHBArh/bEw
CgYIKoZIzj0EAwIDgYwAMIGIAkIAtzQ/knrW2ovCVoHAuq1v2cr0n3NenS/44lul
+3H1y52vn4Rm4CGU3wkzXU3qGO3YjhNjCXjhp3+uN2afFf1Wf3ECQgC4bumHVsfj
b5rwPIC5tvXS/A8upqIzqc0yt3OhpaDDOTWzzvZY7qFflCOl5p6pvUpHigqoZNg5
9xhNdM1CQSykOg==
-----END CERTIFICATE REQUEST-----
```

الخطوة 5. إستيراد شهادة هوية المحول الموقعة من قبل CA.

<#root>

```
POD2IPN2(config)#
```

crypto ca import ec521-tp certificate

```
input (cut & paste) certificate in PEM format:
-----BEGIN CERTIFICATE-----
MIIDzTCCAbWgAwIBAgIIC6zS76XYDm8wDQYJKoZIhvcNAQELBQAwajELMAkGA1UE
BhMCVVMxFzAVBgNVBAgTDk5vcnRoIENhcm9saW5hMRAwDgYDVQQHEwdSYWxlaWdo
MQ4wDAYDVQQKEwVDaXNjbzEMMAoGA1UECxMDU1ZTMRIwEAYDVQQDEwlTVlMgTGFi
QOEwHhcNMjUwNTA3MTkxMDAwWhcNMjYwNTA3MTkxMDAwWjApMREwDwYDVQQDDAhQ
TOQySVBOMjEUMBIGA1UEBRMLRkRPMjYOOTBQNFQwgZswEAYHKoZIzj0CAQYFK4EE
ACMDgYYABAEZhPSLDs6+ogpD9rbYuSA1r0iGpZC962PEqrjzmCpNIESjovOmQ6E8
AYTiMG940fFh4gDs981a8nvFMFaMM1f8hgGboTsd3urjY6YJ7wx5/5uokFOn3DOn
ISOEjaUgihe3jzXicHE5uQhZbJHlxk0iJdMuTw/ggxm8+ryNGcQtHF3xEaNAMD4w
HgYJYIZIAYb4QgENBBEWD3hjYSBjZXJ0aWZpY2F0ZTAcBgNVHREBAf8EEjAQgghQ
TOQySVBOMocECuH9sTANBgkqhkiG9w0BAQsFAAOCAgEANWGb6zm9TDPaM1yhPMx7
8uai/pF7VQC8NSCdOKqr4w4+695ZjJuzqFL3msodOQK0EdgxpQ4+pEa5msRtK0i8
mms2X/Px3/EShxoHrZO1PUXNTyZidXpGd/yTrdQAl5JzpW4pEudrbCJMZEEYtqoP
wD+4OE8vKoYEgyWlDrpRZOZG1usZczuUhLZ8orkjXMhWC26Q5aqiCKkyg10Nt6nb
liToeYy2Q0cTesSZCKvRBv6Ewj5JuSLemURyB4GHY+LT+A9UNmEUM2n+OSVEL329
3hS0qd/YVaEuxjjlg7jNiZb+UsW7IRx3Q8Rouo++ISACpH/PJ61LnlVxhXombiS6
INoa0GvQONrl+lFT8ADIdZ/Ukd5Ubhc9bh/sYzf4MWtkK1wVO16Hv7vGpSMYonD6
a271im+tJPyKnnezQ6OykzlGqsL/Ta6JOdip/fEYp8UmRq9InDh23gDjqrojWL7k
1R/bZpc+baMYXd/2pohHMSN0sKN3zNrJTlnuk5KCqFx//4P7mAoyZYiTIDp1pkYS
VK65fJKD+pYxIhSP9wN8rnwtzSCWb0Z78sgO06Y6wIXyTP0UB3FWhD+GxtTkmEce
ZnAQbgxpgrg5lhpAEVabpC/zRU4UzTuBmv/WoY12zwXCr5WLXEOWtIe8CwFjSnch
```

```
lfKuuebdZkbwz72r7OyyX/U=
-----END CERTIFICATE-----
POD2IPN2(config)#
```

تحقق من تسجيل شهادة هوية المحول.

<#root>

```
POD2IPN2(config)#
```

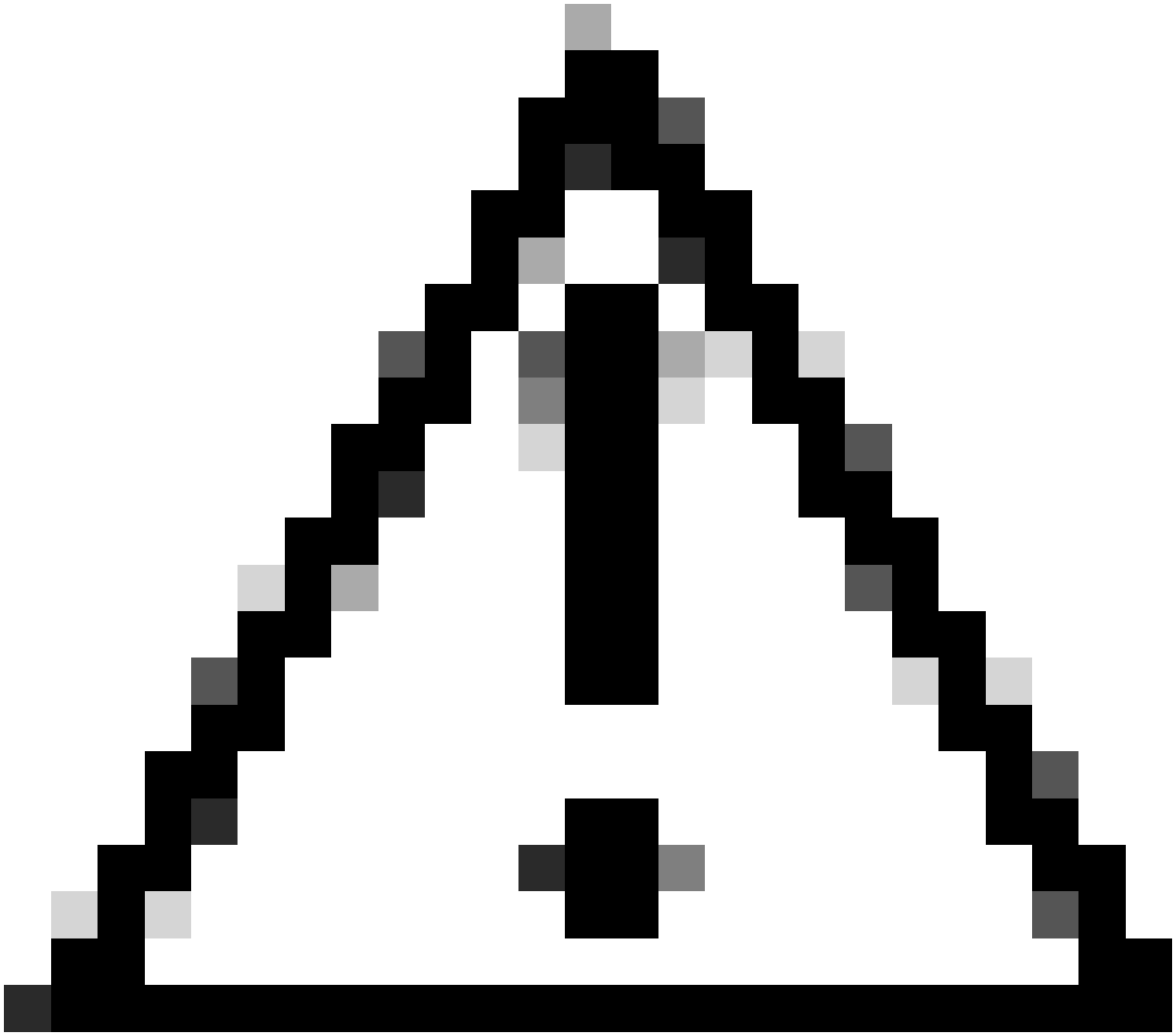
show crypto ca certificates ec521-tp

```
Trustpoint: ec521-tp
certificate:
subject=CN = POD2IPN2, serialNumber = FDO2649OP4T
issuer=C = US, ST = North Carolina, L = Raleigh, O = Cisco, OU = SVS, CN = SVS LabCA
serial=0BACD2EFA5D80E6F
notBefore=May  7 19:10:00 2025 GMT
notAfter=May  7 19:10:00 2026 GMT
SHA1 Fingerprint=CA:B2:BF:3F:ED:2F:06:0B:C1:E4:DC:21:9F:9D:54:61:98:32:C5:13
purposes: sslserver sslclient

CA certificate 0:
subject=C = US, ST = North Carolina, L = Raleigh, O = Cisco, OU = SVS, CN = SVS LabCA
issuer=C = US, ST = North Carolina, L = Raleigh, O = Cisco, OU = SVS, CN = SVS LabCA
serial=20CD7402C4DA37F5
notBefore=Apr 28 17:05:00 2025 GMT
notAfter=Apr 28 17:05:00 2035 GMT
SHA1 Fingerprint=0E:B1:81:E9:5A:3E:D7:80:3B:C5:A8:05:9A:85:4A:95:C8:3A:C7:37
purposes: sslserver sslclient

POD2IPN2(config)#
```

تكوين TACACS+ TLS



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

الخطوة 1. قم بتكوين قوائم التحكم في الوصول (TACACS) العامة.

<#root>

POD2IPN2(config)#

tacacs-server secure tls

الخطوة 2. قم بتغيير منفذ ISE إلى منفذ TLS الذي تم تكوين خادم ISE به.

<#root>

POD2IPN2(config)#

```
tacacs-server host 10.225.253.209 port 6049 timeout 60 single-connection
```

الخطوة 3. أربط تكوين خادم ISE على المحول بنقطة الثقة لاتصال TLS.

```
<#root>

POD2IPN2(config)#

tacacs-server host 10.225.253.209 tls client-trustpoint ec521-tp
```

الخطوة 4. إنشاء مجموعة خوادم TACACS.

```
<#root>

POD2IPN2(config)#

aaa group server tacacs+ tacacs2

POD2IPN2(config-tacacs+)#

server 10.225.253.209

POD2IPN2(config-tacacs+)#

use-vrf management
```

الخطوة 5. تحقق من التكوين.

```
<#root>

POD2IPN2#

sho run tacacs

feature tacacs+

tacacs-server secure tls
tacacs-server host 10.225.253.209 port 6049 timeout 60 single-connection
tacacs-server host 10.225.253.209 tls client-trustpoint ec521-tp
aaa group server tacacs+ tacacs2
    server 10.225.253.209
    use-vrf management
```

الخطوة 6. اختبر المستخدم البعيد قبل تكوين مصادقة AAA.

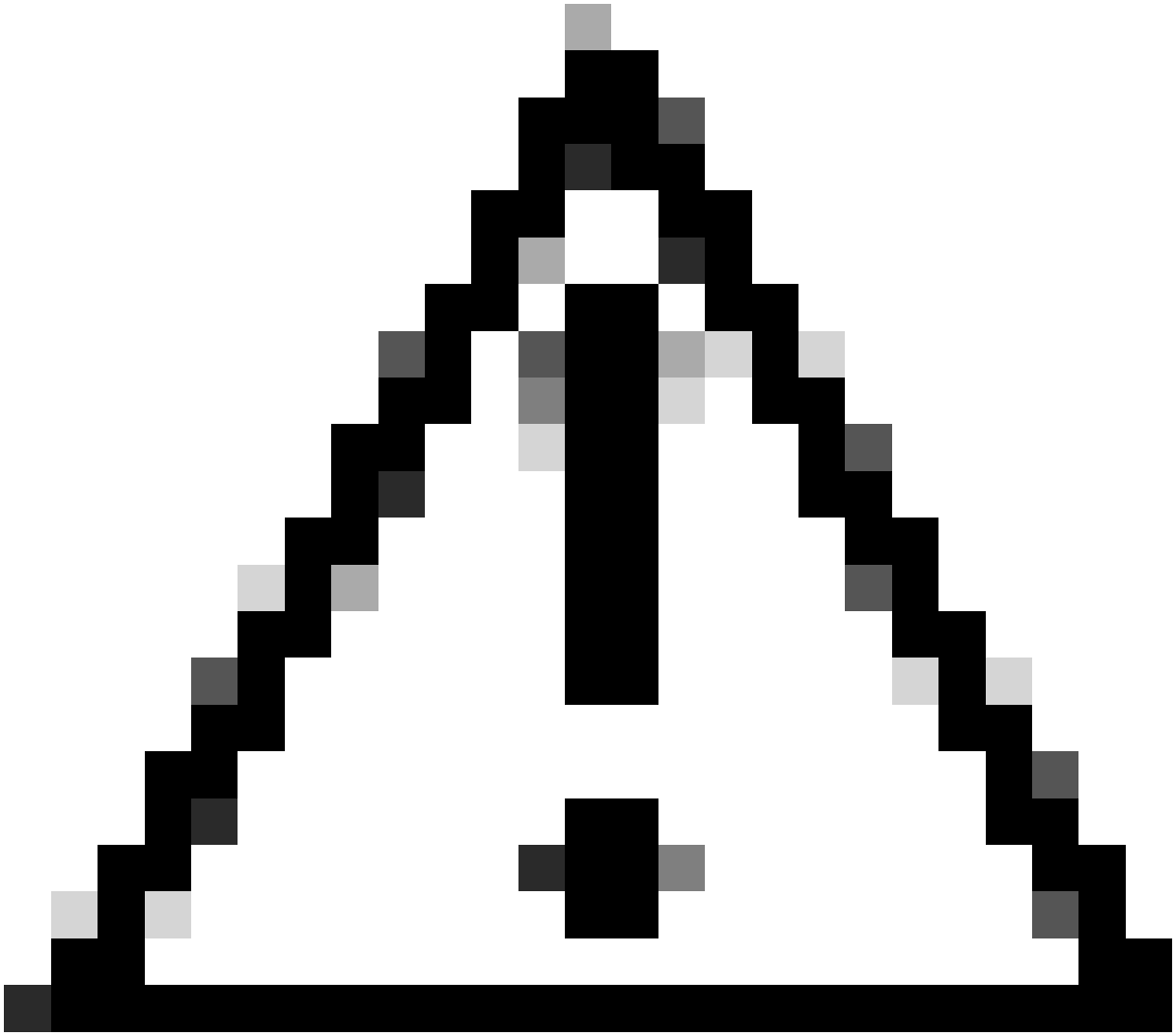
```
<#root>
```

```
POD2IPN2#
test aaa group tacacs2



user has been authenticated
POD2IPN2#
```

تكوين AAA



تحذير: تأكد من نجاح مصادقة المستخدم عن بعد قبل متابعة تكوينات AAA.

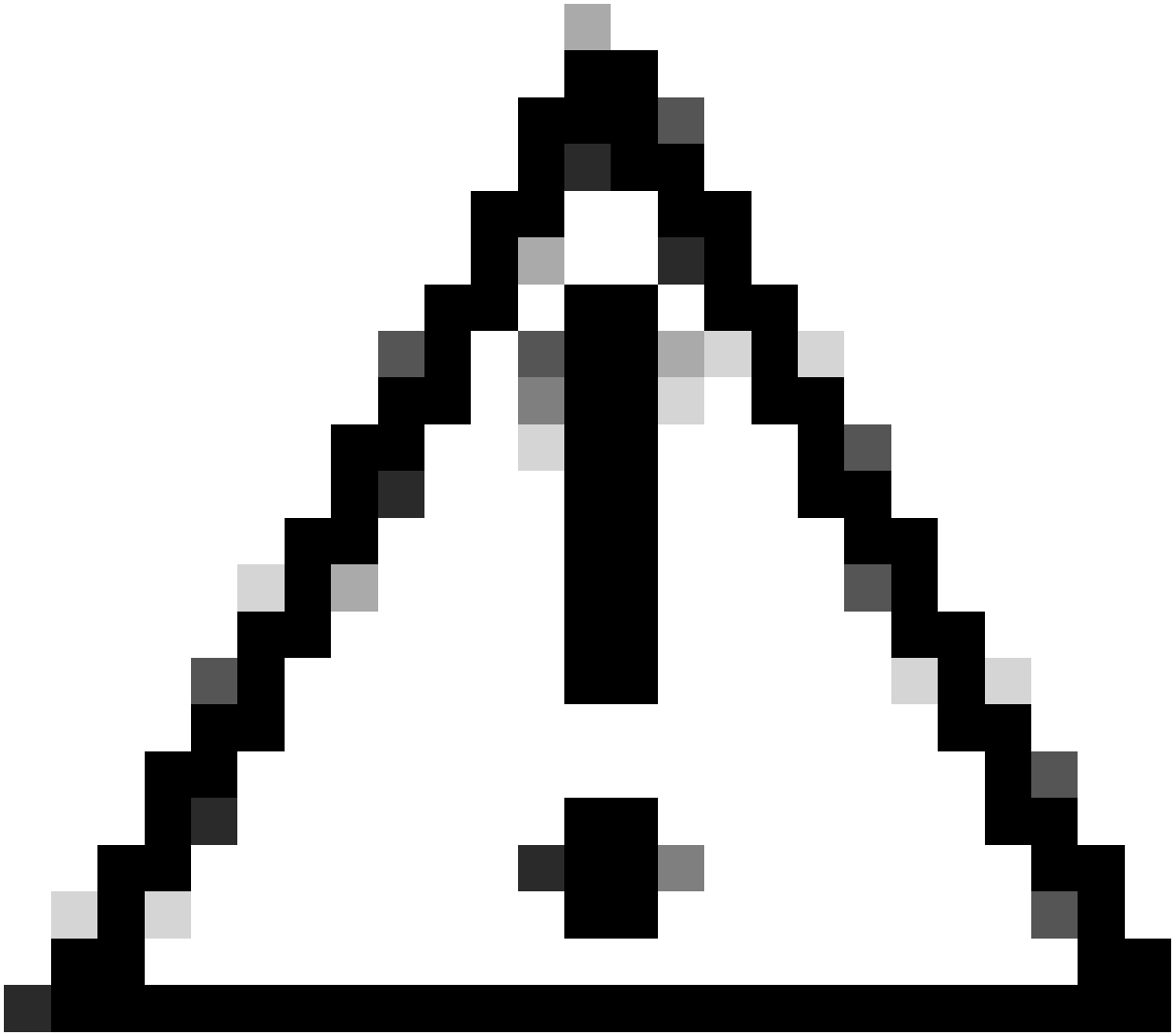
الخطوة 1. تكوين مصادقة AAA عن بعد.

<#root>

POD2IPN2(config)#

aaa authentication login default group tacacs2

الخطوة 2. قم بتكوين التفويض عن بعد ل AAA بعد إختبار الأمر.



تحذير: تأكد من أن حالة التخويل هي "aaa_author_status_pass_add.

<#root>

POD2IPN2#

test aaa authorization command-type config-commands default user

```
        command "feature bgp"
```

```
sending authorization request for: user: pamemart, author-type:3, cmd "feature bgp"
user pamemart, author type 3, command: feature bgp, authorization-status:0x1(AAA_AUTHOR_STATUS_PASS_ADD)
```

الخطوة 3. تكوين أمر AAA وتفويض config-command.

```
<#root>
POD2IPN2(config)#
aa authorization config-commands default group tacacs2 local

POD2IPN2(config)#
aa authorization commands default group tacacs2 local
```

إختبار واستكشاف أخطاء وصول المستخدم إلى NX-OS وإصلاحها

التحقق

اكتمل تكوين إدارة الجهاز ل Cisco NX-OS. تحتاج إلى التحقق من صحة التكوين.

الخطوة 1. بروتوكول SSH وتسجيل الدخول إلى أجهزة NX-OS كأدوار مختلفة.

خطوة 2. من إن على الأداة خط قارن (CLI)، دقق أن المستعمل يتلقى منفذ إلى الأمر يمين. على سبيل المثال، يجب أن يكون أحد مستخدمي مكتب المساعدة قادرا على إختبار اتصال عنوان IP عادي (على سبيل المثال، 10.225.253.129) ولكن تم رفضه لإظهار التكوين الجاري تشغيله.

```
POD2IPN1# ping 10.225.253.129 vrf management
PING 10.225.253.129 (10.225.253.129): 56 data bytes
64 bytes from 10.225.253.129: icmp_seq=0 ttl=254 time=0.817 ms
64 bytes from 10.225.253.129: icmp_seq=1 ttl=254 time=0.638 ms
64 bytes from 10.225.253.129: icmp_seq=2 ttl=254 time=0.642 ms
64 bytes from 10.225.253.129: icmp_seq=3 ttl=254 time=0.651 ms
64 bytes from 10.225.253.129: icmp_seq=4 ttl=254 time=0.712 ms

--- 10.225.253.129 ping statistics ---
5 packets transmitted, 5 packets received, 0.00% packet loss
```

```
round-trip min/avg/max = 0.638/0.692/0.817 ms
POD2IPN1#
POD2IPN1# show running-config
% Permission denied for the role
```

استكشاف الأخطاء وإصلاحها

التحقق من صحة تكوين NX-OS.

```
POD2IPN2# show crypto ca certificates
POD2IPN2# show crypto ca trustpoints
POD2IPN2# show tacacs-server statistics <server ip>
```

لإظهار إتصالات المستخدم والدور (الأدوار)، أستخدم هذه الأوامر.

```
show users
show user-account [<user-name>]
A sample output is shown below:
POD2IPN1# show users
NAME LINE TIME IDLE PID COMMENT
Admin-ro pts/5 May 15 23:49 . 16526 (10.189.1.151) session=ssh *
POD2IPN1# show user-account Admin-ro
user:Admin-ro
roles:network-operator
account created through REMOTE authentication
Credentials such as ssh server key will be cached temporarily only for this user account
Local login not possible...
```

هذه هي أخطاء مفيدة في أستكشاف أخطاء TACACS+ وإصلاحها:

```
debug TACACS+ aaa-request
2016 Jan 11 03:03:08.652514 TACACS[6288]:  process_aaa_tplus_request:Checking for state of mgmt0 port w
2016 Jan 11 03:03:08.652543 TACACS[6288]:  process_aaa_tplus_request: Group demoTG found. corresponding
2016 Jan 11 03:03:08.652552 TACACS[6288]:  process_aaa_tplus_request: checking for mgmt0 vrf:management
2016 Jan 11 03:03:08.652559 TACACS[6288]:  process_aaa_tplus_request:port_check will be done
2016 Jan 11 03:03:08.652568 TACACS[6288]:  state machine count 0
2016 Jan 11 03:03:08.652677 TACACS[6288]:  is_intf_up_with_valid_ip(1258):Proper IOD is found.
2016 Jan 11 03:03:08.652699 TACACS[6288]:  is_intf_up_with_valid_ip(1261):Port is up.
2016 Jan 11 03:03:08.653919 TACACS[6288]:  debug_av_list(797):Printing list
2016 Jan 11 03:03:08.653930 TACACS[6288]:  35 : 4 : ping
2016 Jan 11 03:03:08.653938 TACACS[6288]:  36 : 12 : 10.1.100.255
2016 Jan 11 03:03:08.653945 TACACS[6288]:  36 : 4 : <cr>
2016 Jan 11 03:03:08.653952 TACACS[6288]:  debug_av_list(807):Done printing list, exiting function
2016 Jan 11 03:03:08.654004 TACACS[6288]:  tplus_encrypt(659):key is configured for this aaa sessin.
2016 Jan 11 03:03:08.655054 TACACS[6288]:  num_inet_addrs: 1 first s_addr: -1268514550 10.100.1.10 s6_a
2016 Jan 11 03:03:08.655065 TACACS[6288]:  non_blocking_connect(259):interface ip_type: IPV4
2016 Jan 11 03:03:08.656023 TACACS[6288]:  non_blocking_connect(369): Proceeding with bind
2016 Jan 11 03:03:08.656216 TACACS[6288]:  non_blocking_connect(388): setsockopt success error:22
```

```
2016 Jan 11 03:03:08.656694 TACACS[6288]:  non_blocking_connect(489): connect() is in-progress for serv
2016 Jan 11 03:03:08.679815 TACACS[6288]:  tplus_decode_authen_response: copying hostname into context
```

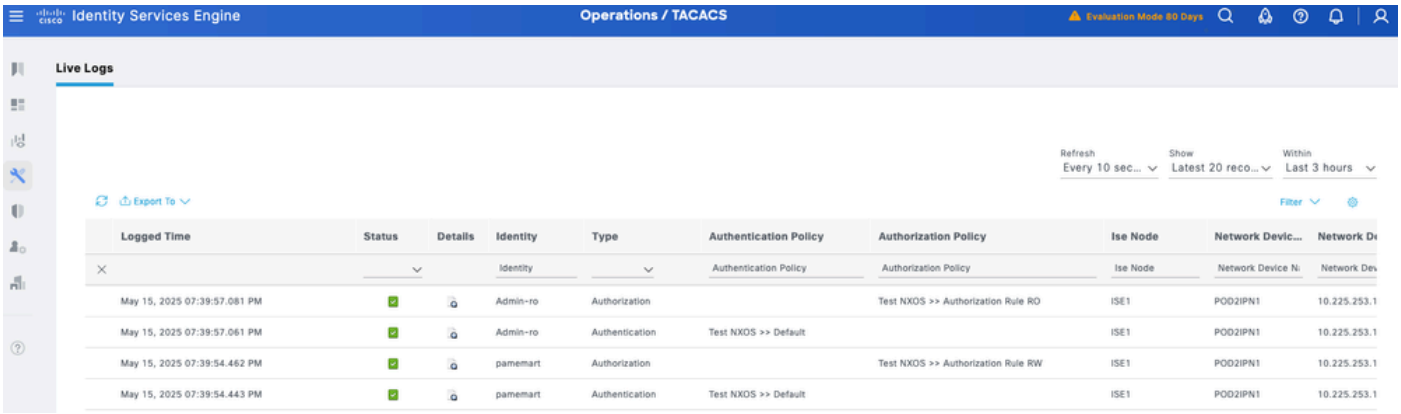
قم بتمكين تصحيح أخطاء SSL.

```
touch '/bootflash/.enable_ssl_debugs'
```

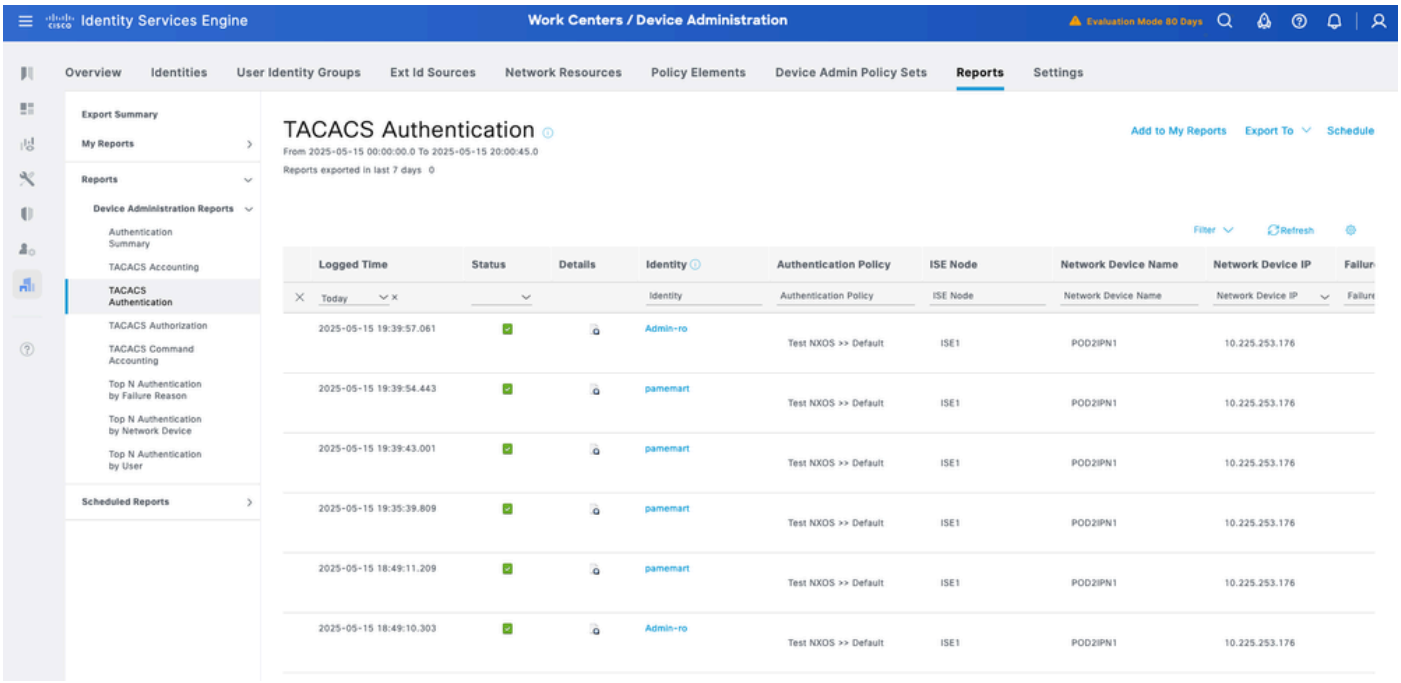
إظهار محتويات ملف تصحيح الأخطاء.

```
cat /tmp/ssl_wrapper.log.*
```

من واجهة المستخدم الرسومية (GUI) لنظام التشغيل ISE، انتقل إلى العمليات > TACACS Livelog. يتم التقاط جميع طلبات مصادقة TACACS والتفويض هنا، وبوفر زر التفاصيل معلومات تفصيلية حول سبب تمرير/فشل معاملة معينة.



في التقارير التاريخية: انتقل إلى مراكز العمل > إدارة الأجهزة > التقارير > إدارة الأجهزة للحصول على تقارير المصادقة والتفويض والمحاسبة.


Identity Services Engine
Work Centers / Device Administration
Evaluation Mode 80 Days
Overview
Identities
User Identity Groups
Ext Id Sources
Network Resources
Policy Elements
Device Admin Policy Sets
Reports
Settings
Export Summary
My Reports
Reports
Device Administration Reports
Authentication Summary
TACACS Accounting
TACACS Authentication
TACACS Authorization
TACACS Command Accounting
Top N Authentication by Failure Reason
Top N Authentication by Network Device
Top N Authentication by User
Scheduled Reports
TACACS Authentication
From 2025-05-15 00:00:00.0 To 2025-05-15 20:00:45.0
Reports exported in last 7 days 0
Add to My Reports
Export To
Schedule
Filter
Refresh
Logged Time
Status
Details
Identity
Authentication Policy
ISE Node
Network Device Name
Network Device IP
Today
Identity
Authentication Policy
ISE Node
Network Device Name
Network Device IP
2025-05-15 19:39:57.061
Admin-ro
Test NXOS >> Default
ISE1
POD2IPN1
10.225.253.176
2025-05-15 19:39:54.443
pamemart
Test NXOS >> Default
ISE1
POD2IPN1
10.225.253.176
2025-05-15 19:39:43.001
pamemart
Test NXOS >> Default
ISE1
POD2IPN1
10.225.253.176
2025-05-15 19:35:39.809
pamemart
Test NXOS >> Default
ISE1
POD2IPN1
10.225.253.176
2025-05-15 18:49:11.209
pamemart
Test NXOS >> Default
ISE1
POD2IPN1
10.225.253.176
2025-05-15 18:49:10.303
Admin-ro
Test NXOS >> Default
ISE1
POD2IPN1
10.225.253.176

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).