تكوين APIC لإدارة الأجهزة باستخدام ISE و TACACS+

المحتويات

المقدمة

يصف هذا المستند إجراء دمج APIC مع ISE لمصادقة مستخدمي المسؤول مع بروتوكول TACACS+.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- وحدة التحكم الخاصة بتطبيق سياسة البنية الأساسية (APIC)
- محرك خدمات كشف الهوية (ISE)
- بروتوكول Tacacs

المكونات المستخدمة

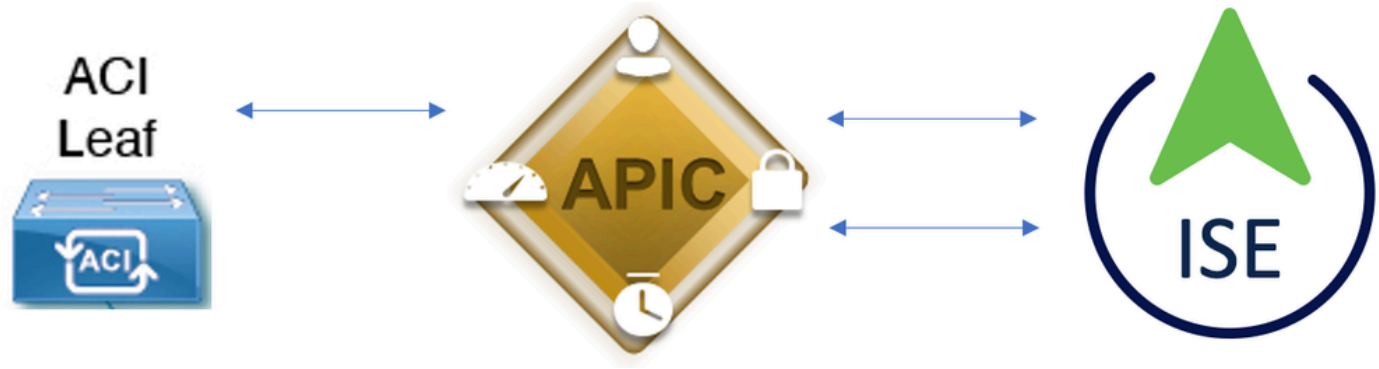
تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- APIC الإصدار 4.2(7u)
- ISE الإصدار 3.2 تصحيح 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.

التكوين

الرسم التخطيطي للشبكة



الرسم التخطيطي للتكامل

إجراء المصادقة

الخطوة 1.سجل الدخول إلى تطبيق APIC باستخدام مسوغات المستخدم المسؤول.

الخطوة 2. تقوم عملية المصادقة بتشغيل بيانات الاعتماد والتحقق من صحتها محليا أو من خلال خدمة Active Directory.

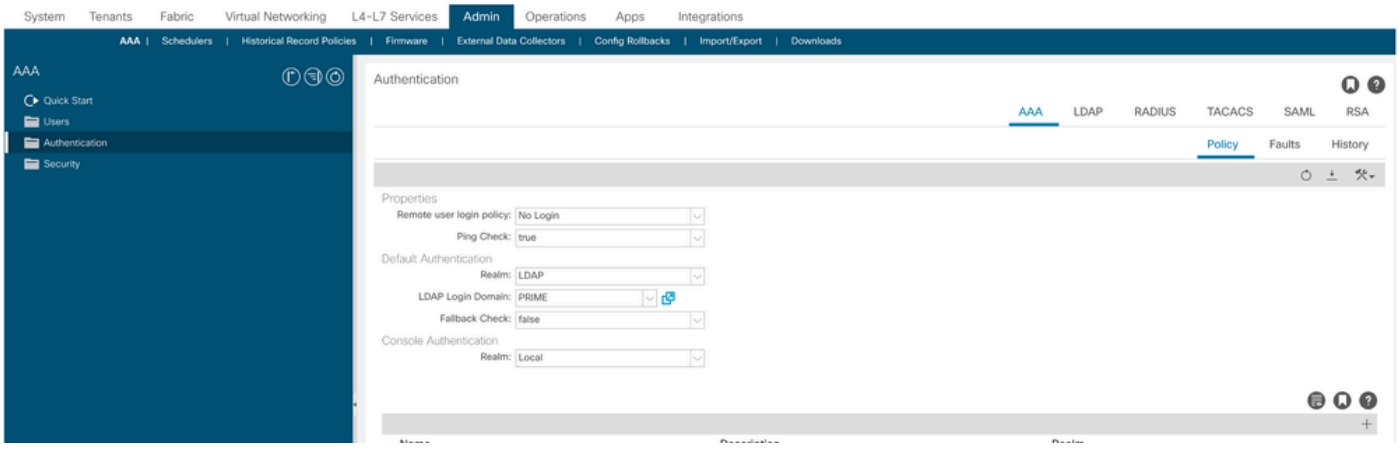
الخطوة 3. بمجرد نجاح المصادقة، يرسل ISE حزمة سماح لتخويل الوصول إلى APIC.

الخطوة 4. يعرض ISE سجلا مباشرا للمصادقة ناجحا.

ملاحظة: تقوم APIC بنسخ تكوين TACACS+ إلى المحولات الطرفية التي هي جزء من البنية.

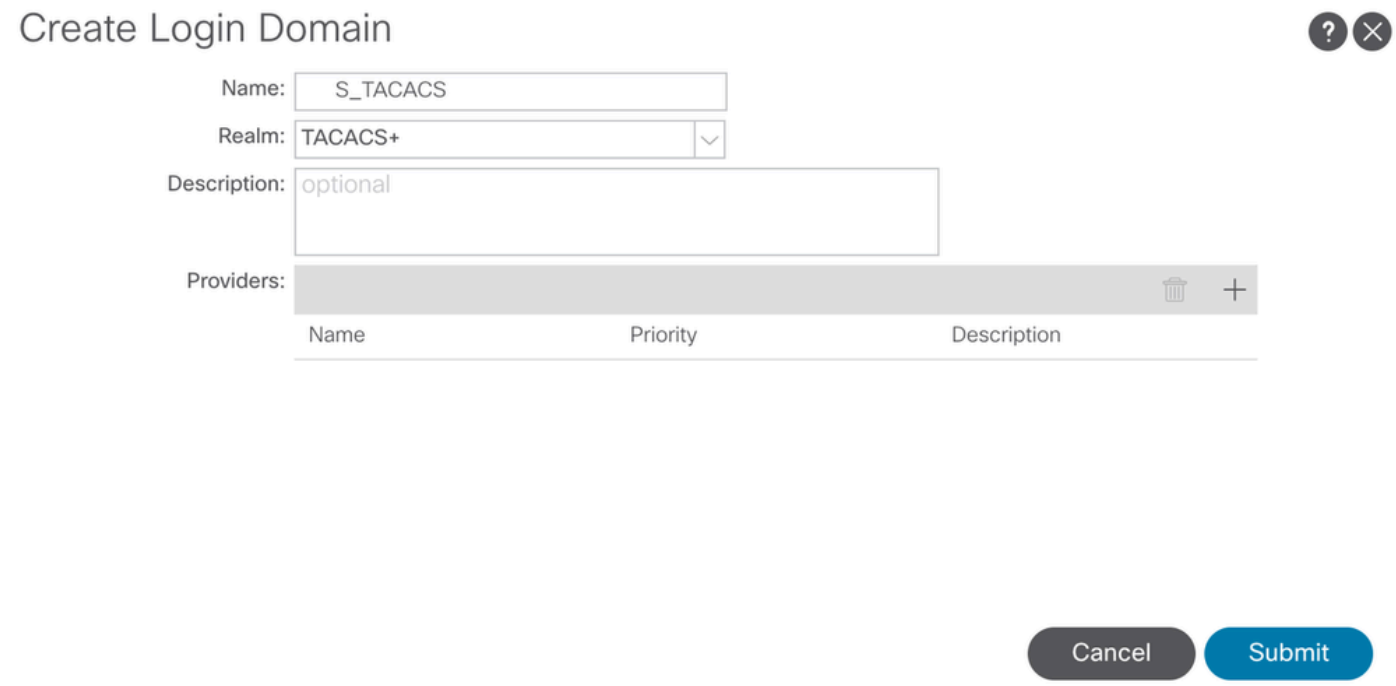
تكوين APIC

الخطوة 1. انتقل إلىAdmin > AAA > Authentication > AAA+واختر أيقونة لإنشاء مجال تسجيل دخول جديد.

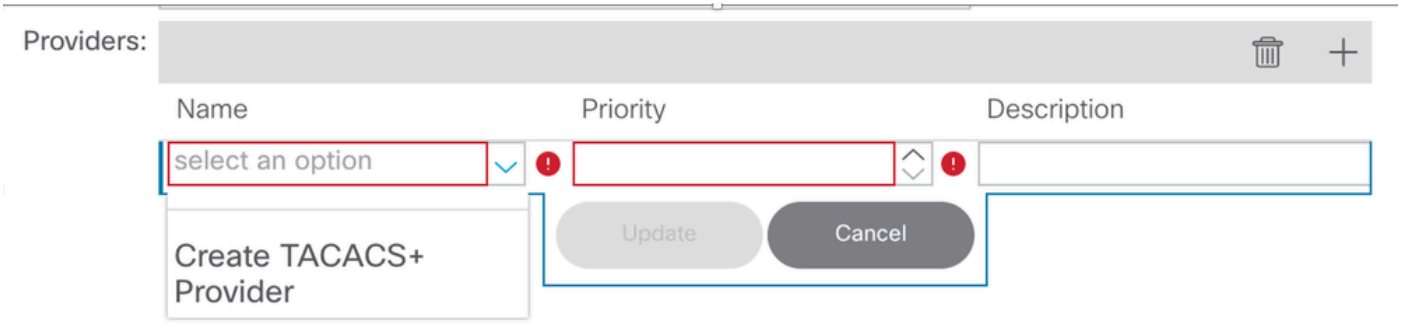


تكوين مسؤول تسجيل دخول APIC

الخطوة 2. قم بتحديد اسم وعالم لمجال تسجيل الدخول الجديد وانقر+فوق موفرين لإنشاء موفر جديد.

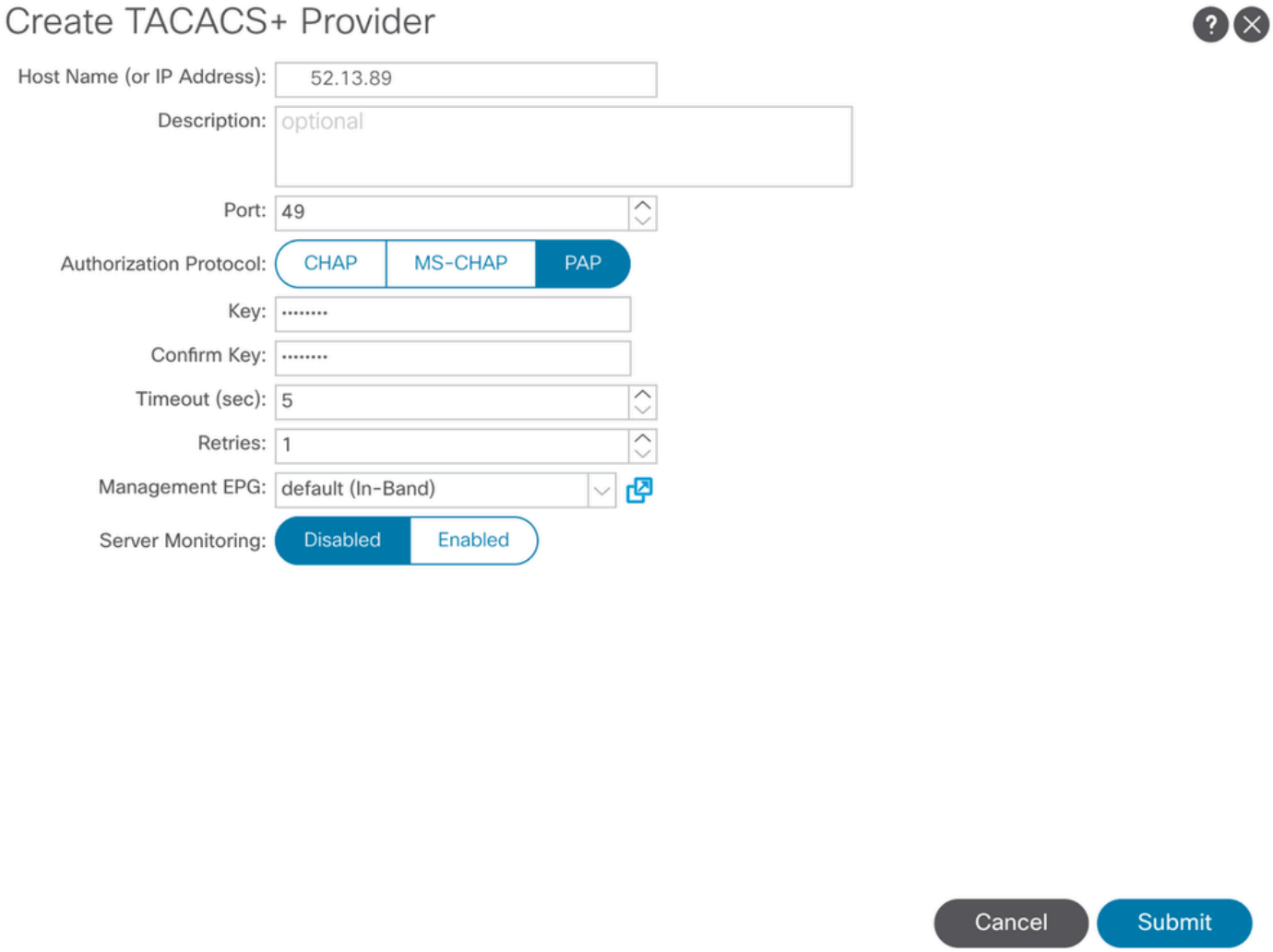


مسؤول تسجيل دخول APIC

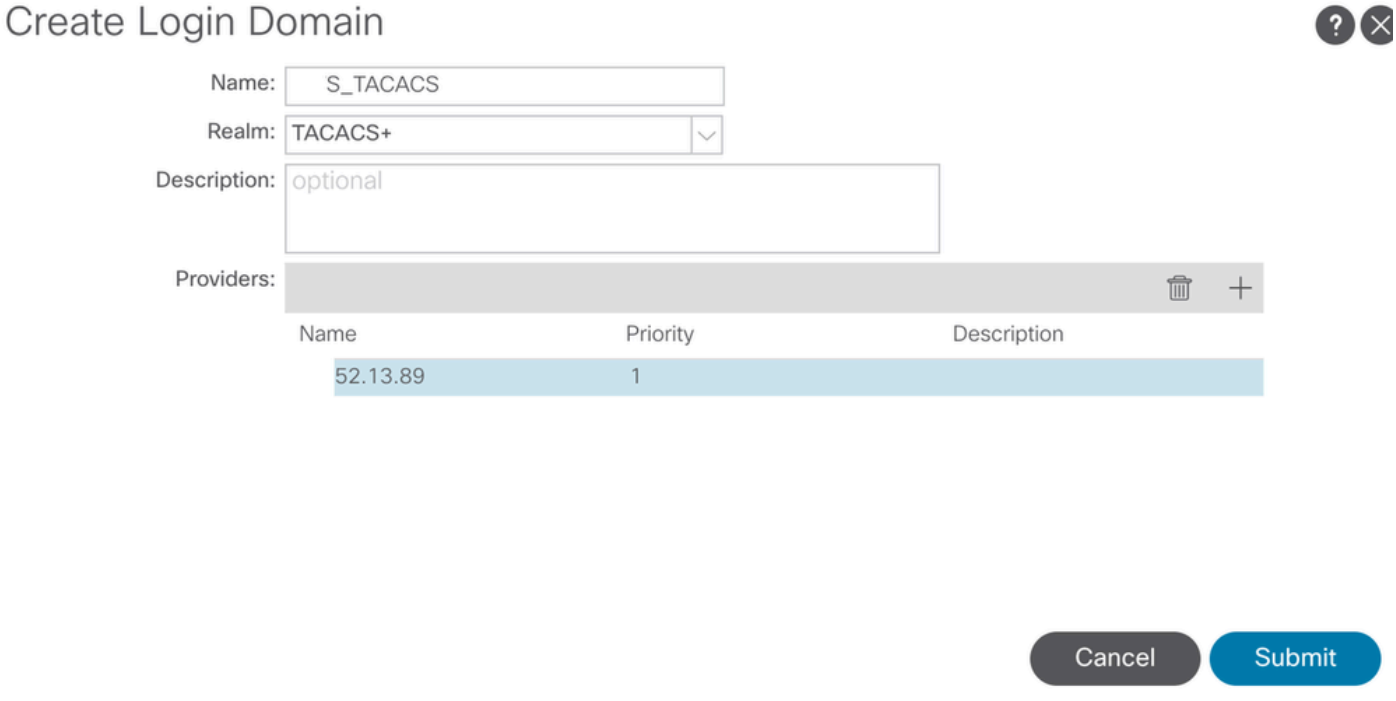


موفر APIC TACACS

الخطوة 3. حدد عنوان ISE IP أو اسم المضيف، وقم بتعريف سر مشترك، واختر مجموعة نهج نقطة النهاية للإدارة (EPG). انقرSubmitلإضافة موفر TACACS+ إلى مسؤول تسجيل الدخول.



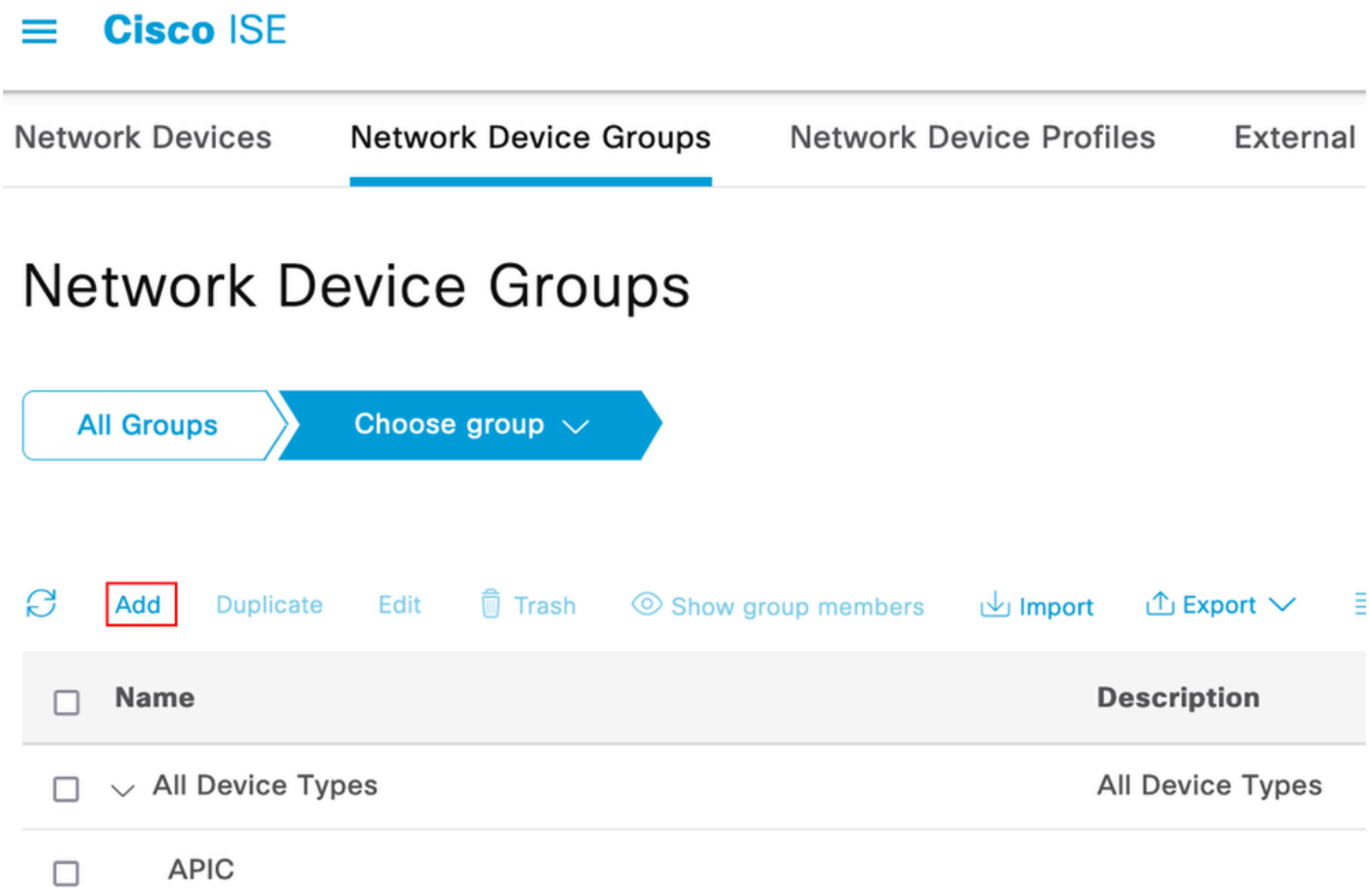
إعدادات موفر APIC TACACS



طريقة عرض موفر Tacacs

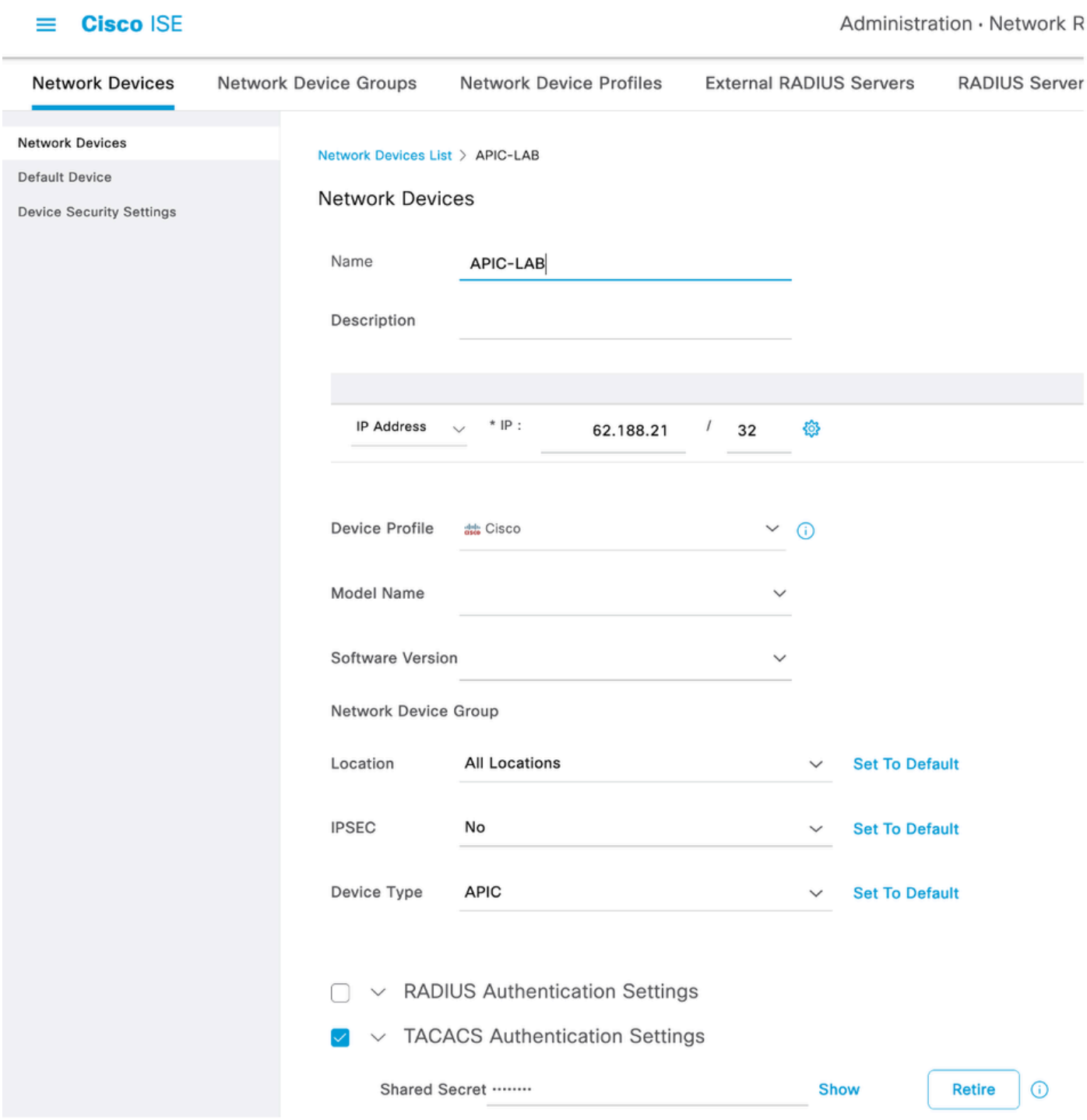
تكوين ISE

الخطوة 1. انتقل إلى ☰>إدارة > موارد الشبكة > مجموعات أجهزة الشبكة. إنشاء مجموعة أجهزة شبكة ضمن جميع أنواع الأجهزة.



مجموعات أجهزة شبكة ISE

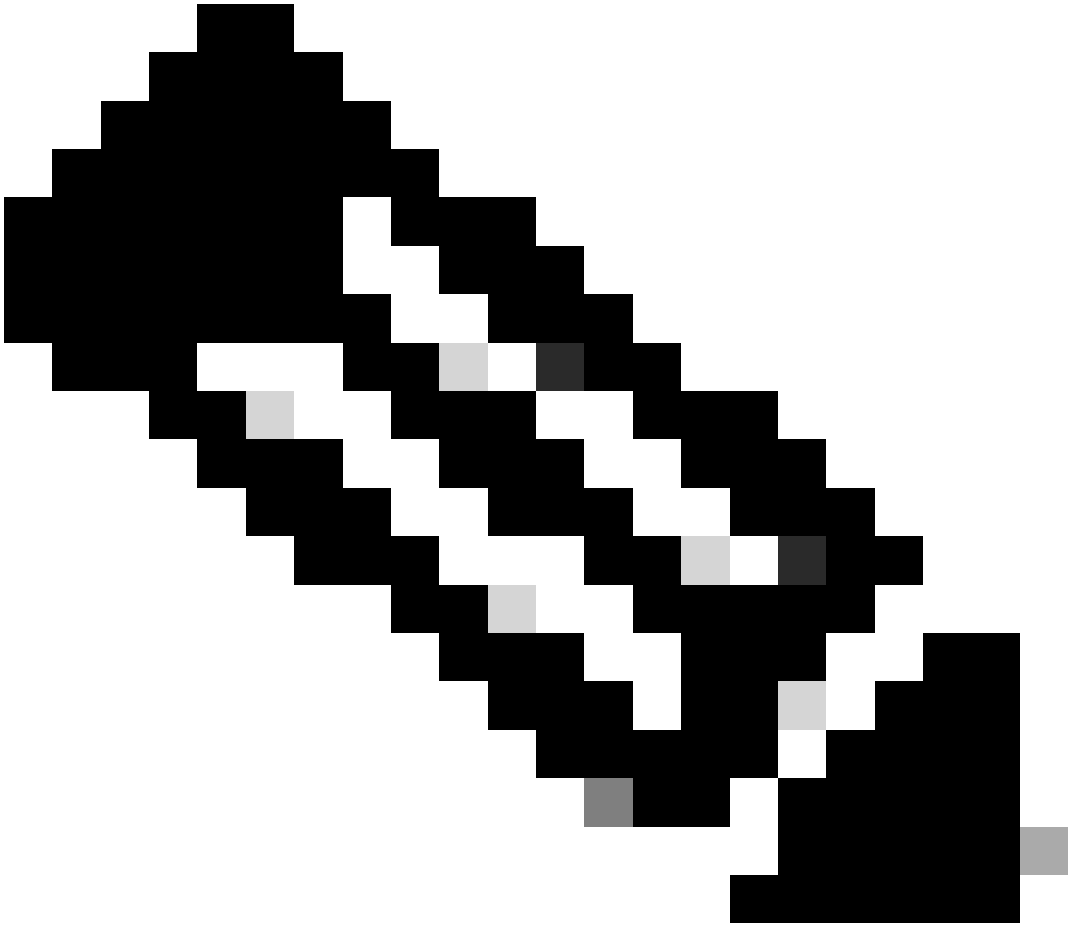
الخطوة 2. انتقل إلىAdministration > Network Resources > Network Devices. أختارAddتعريف اسم APIC وعنوان IP، واختر APIC تحت نوع الجهاز وخط إختياري TACACS+، وحدد كلمة المرور المستخدمة على تكوين موزع APIC TACACS+. انقر.Submit



كرر الخطوة 1. والخطوة 2. للمحولات الطرفية.

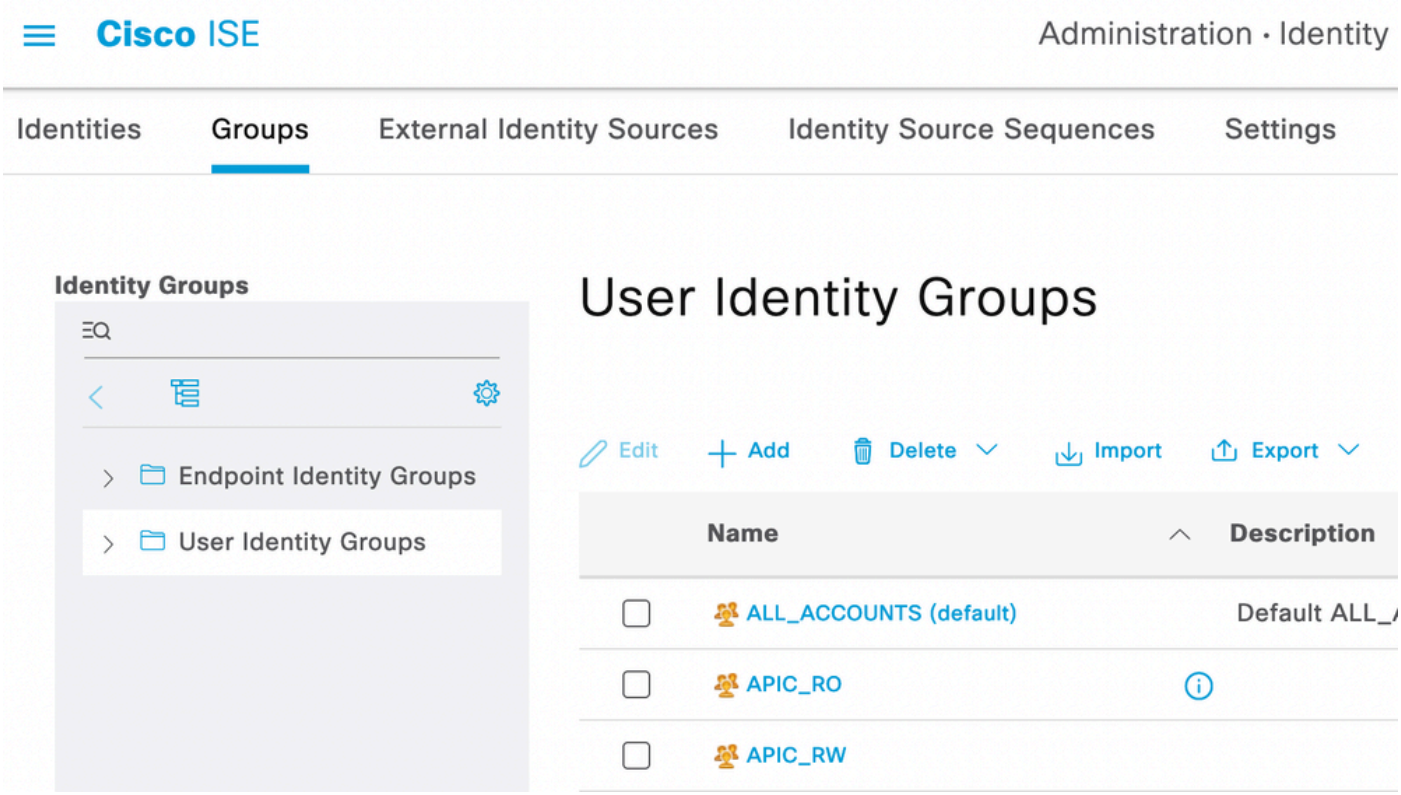
الخطوة 3. أستخدم الإرشادات الموجودة على هذا الارتباط من أجل دمج ISE مع Active Directory؛

https://www.cisco.com/c/en/us/support/docs/security/identity-services-engine/217351-ad-integration-for-cisco-ise-gui-and-cli.html.



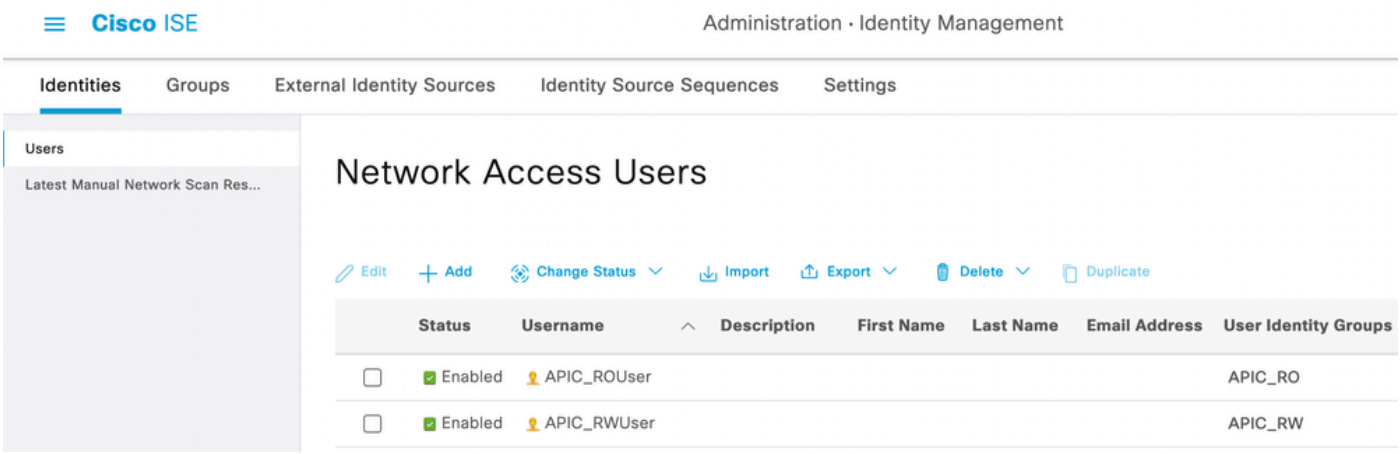
ملاحظة: يتضمن هذا المستند كل من المستخدمين الداخليين ومجموعات مسؤول AD كمصادر هوية، ومع ذلك، يتم إجراء الاختبار باستخدام مصدر هوية المستخدمين الداخليين. النتيجة هي نفسها لمجموعات AD.

الخطوة 4. (إختياري) انتقل إلى ☰ >Administration > Identity Management > Groups. أختارUser Identity Groupsوانقر فوق Add. قم بإنشاء مجموعة واحدة لمستخدمي Admin ومستخدمي Admin للقراءة فقط.

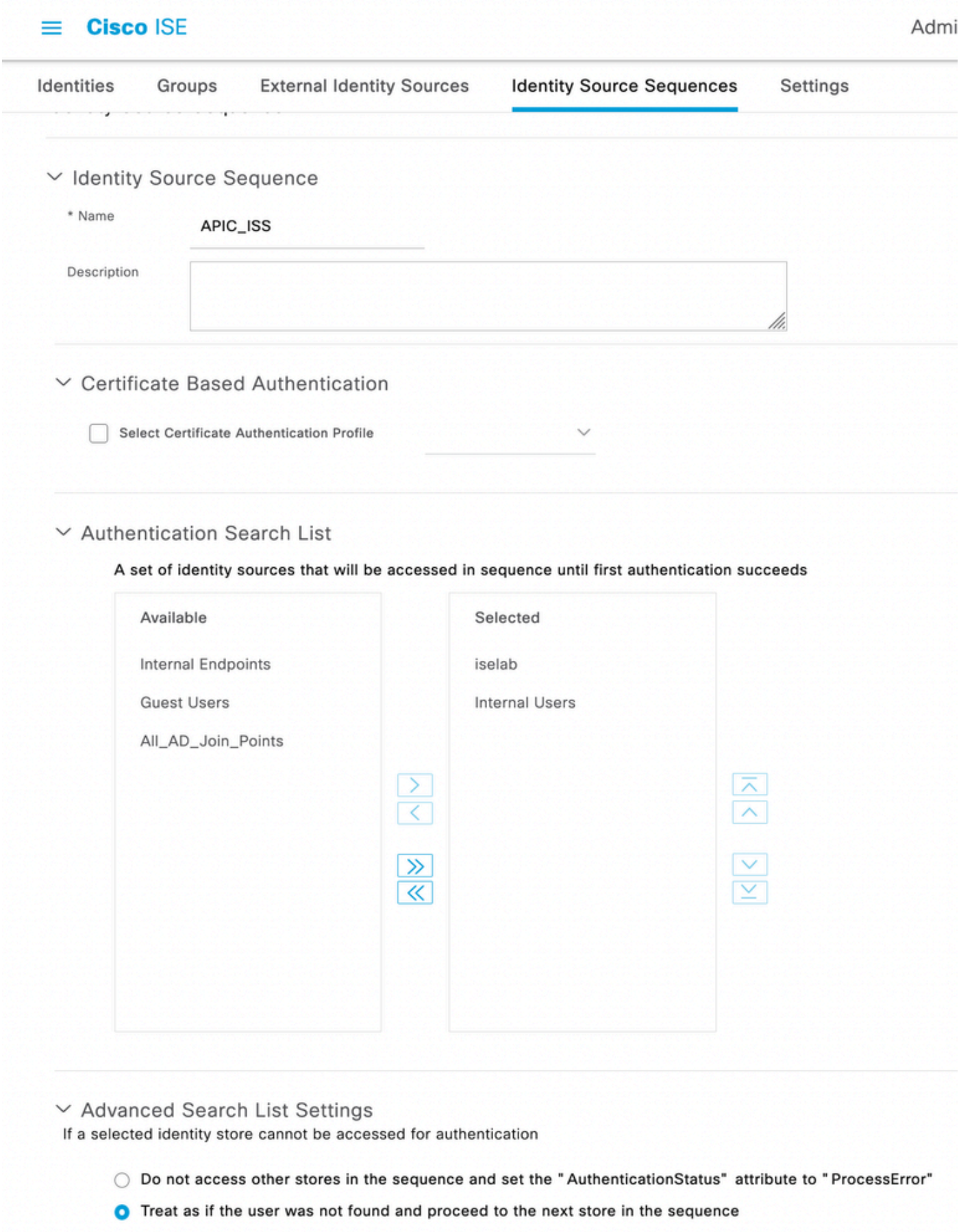


مجموعة الهوية

الخطوة 5. (إختياري) انتقل إلى ☰Administration > Identity Management > Identity.انقرAddوأنشئRead Only AdminمستخدمAdminومستخدم. قم بتعيين كل مستخدم لكل مجموعة تم إنشاؤها في الخطوة 4.



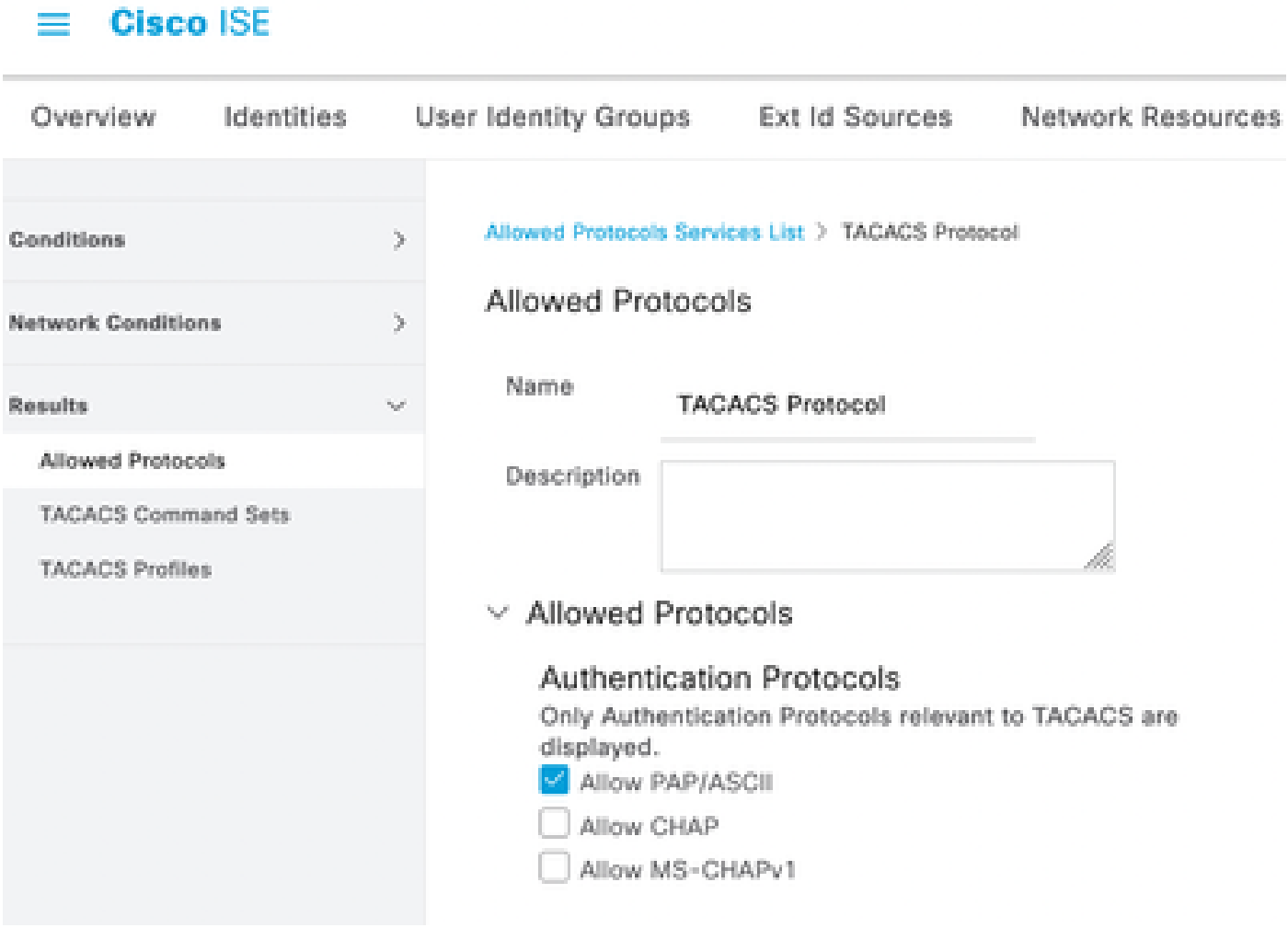
الخطوة 6. انتقل إلى ☰ >Administration > Identity Management > Identity Source Sequence. أختارAdd، وقم بتعريف اسم، واختارAD Join PointsInternal Usersمصدر هوية من القائمة. أختارTreat as if the user was not found and proceed to the next store in the sequenceأدناهAdvanced Search List SettingsوانقرSave.



تسلسل مصدر الهوية

7. انتقل إلى ☰>**Work Centers** > **Device Administration** > **Policy Elements** > **Results** > **Allowed Protocols**. حدد إضافة،

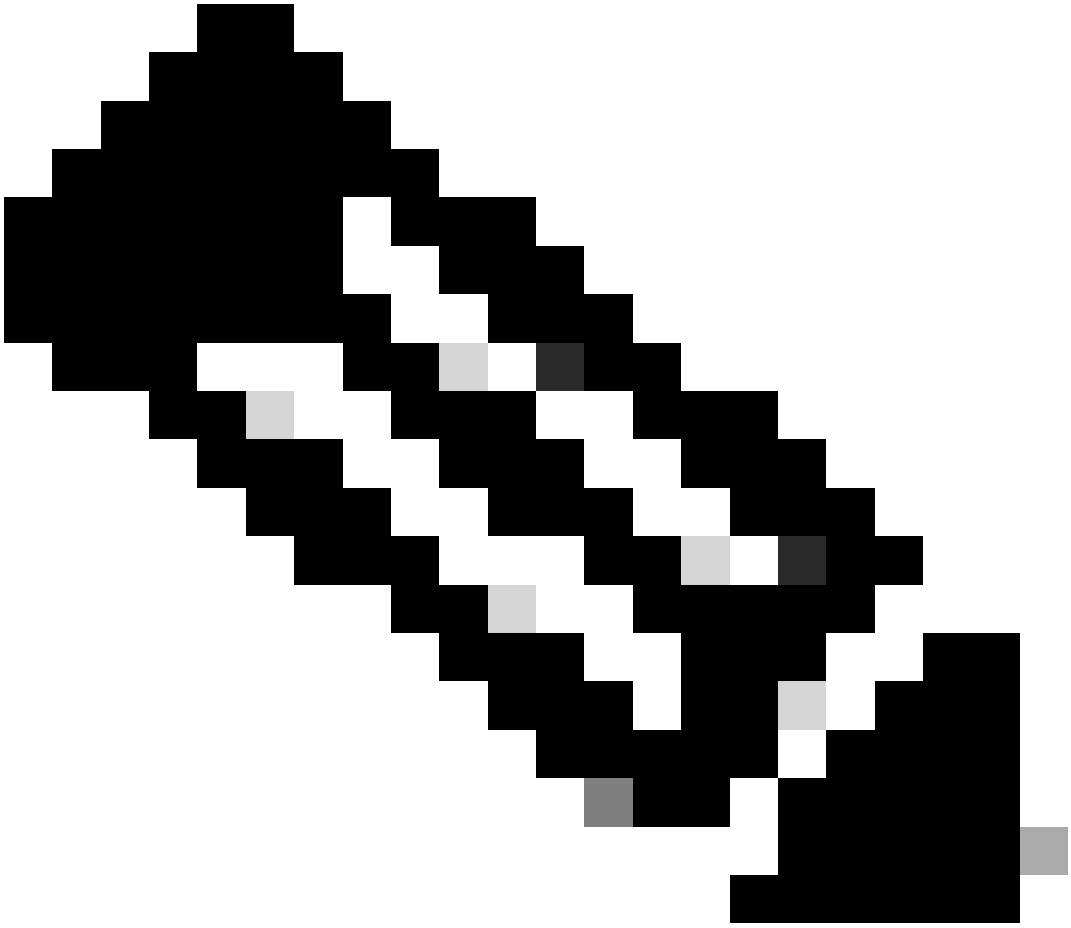
وعرف اسما، وألغي تحديد السماح ب CHAP والسماح ب MS-CHAPv1 من قائمة بروتوكول المصادقة. حدد حفظ.



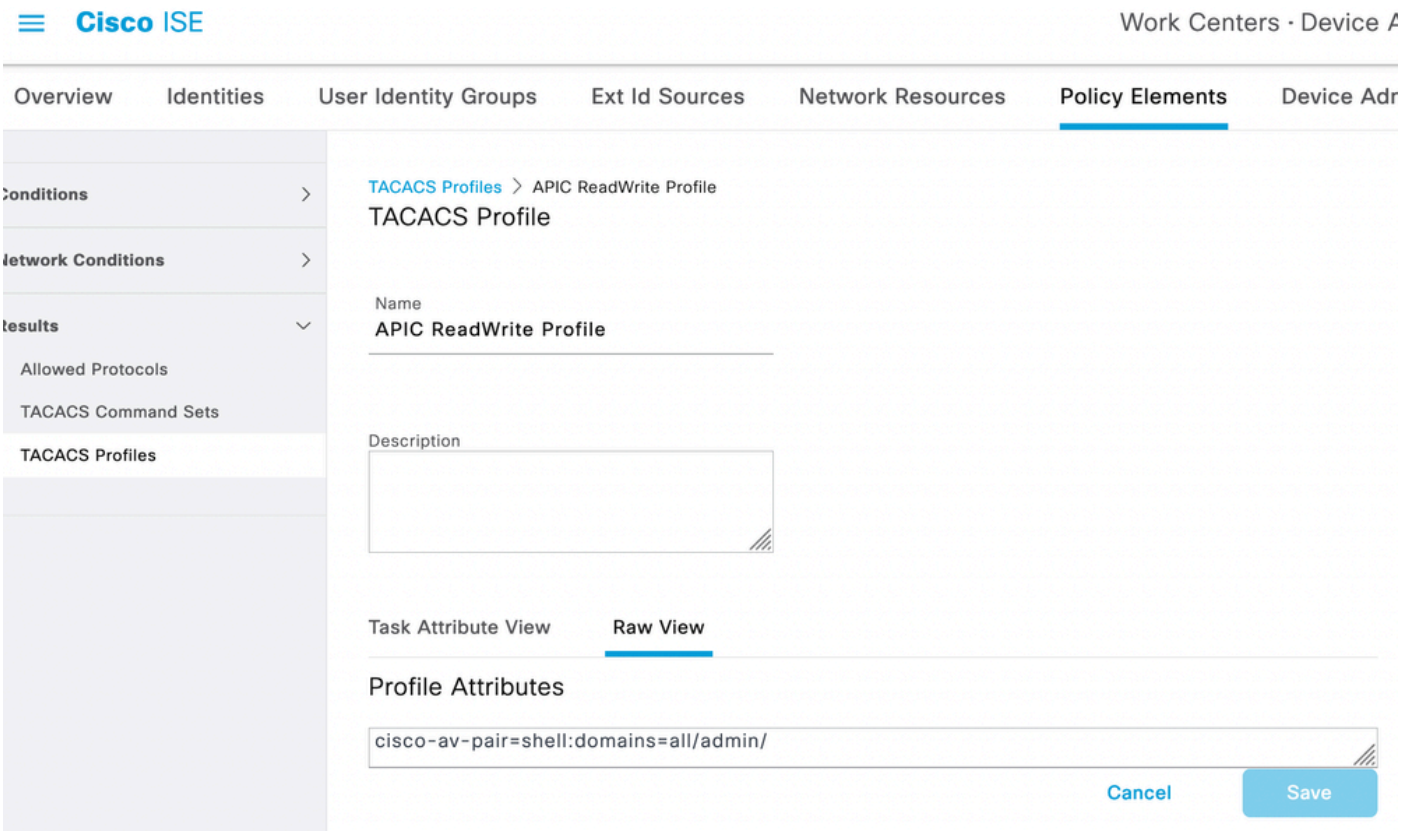
بروتوكول السماح ل Tacacs

8. انتقل إلى ☰ >Work Centers > Device Administration > Policy Elements > Results > TACACS Profile. انقر وأنشئaddتوصيفين بناءا على السمات الموجودة في القائمة تحتRaw View. انقر.Save

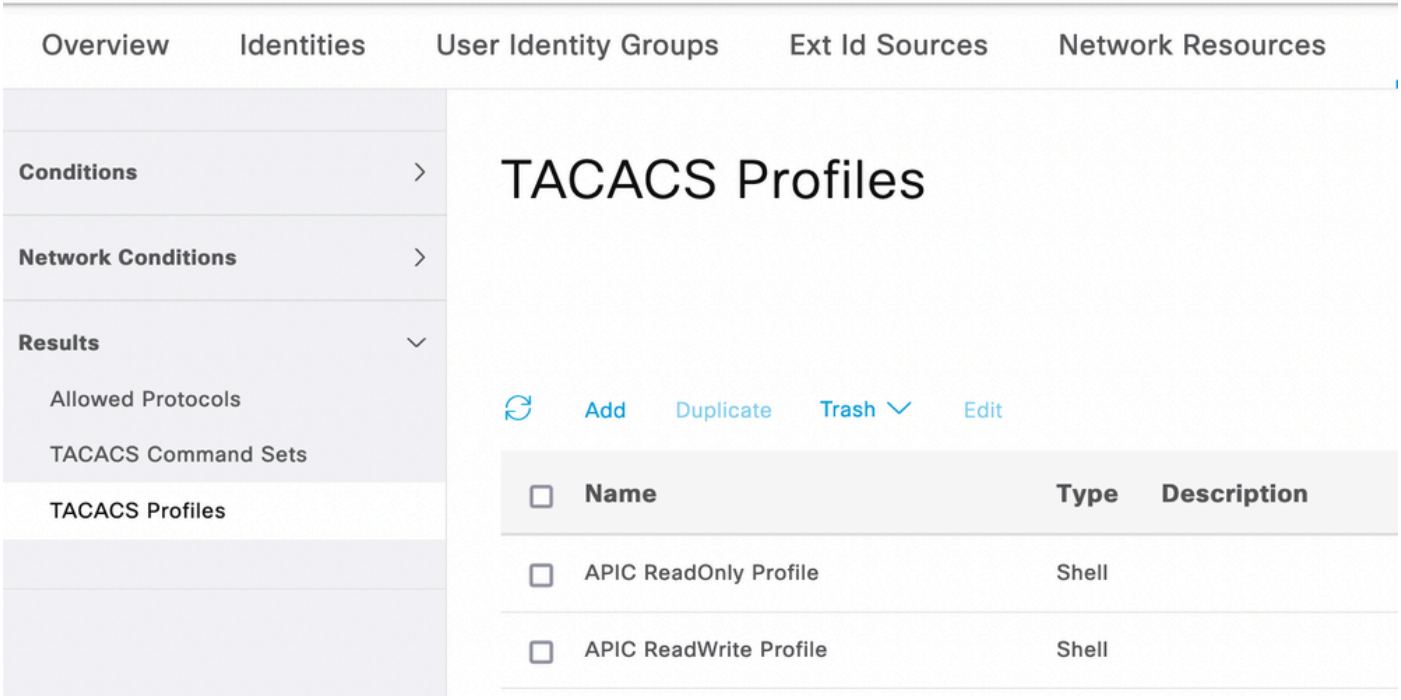
- مستخدم المسؤول: cisco-av-pair=shell:domains=all/admin/
- قراءة مستخدم مسؤول فقط: cisco-av-pair=shell:domains=all//read-all



ملاحظة: في حالة مسافة أو حرف إضافية، تفشل مرحلة التخويل.

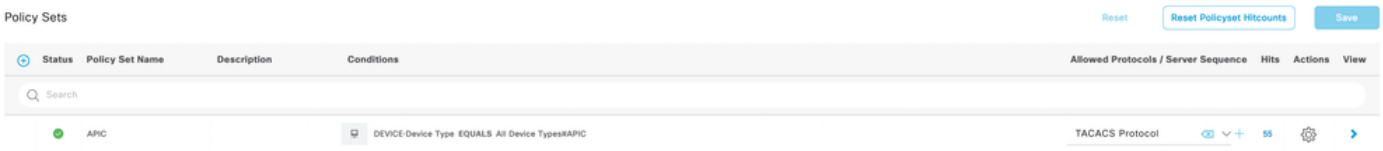


ملف تعريف TACACS



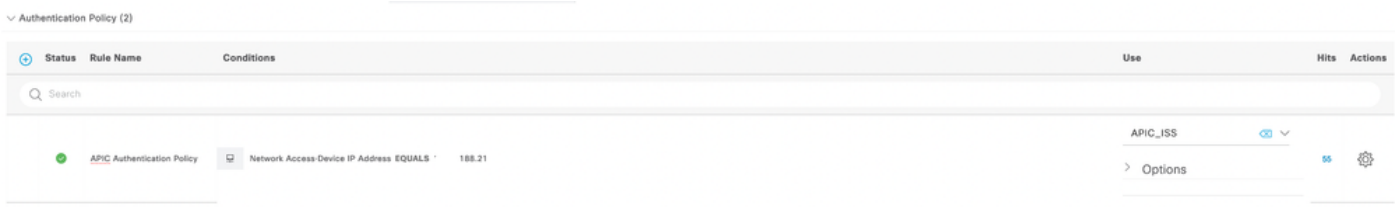
ملفات تعريف مسؤول TACACS و ReadOnly

الخطوة 9. انتقل إلى ☰ >Work Centers > Device Administration > Device Admin Policy Set. قم بإنشاء مجموعة نهج جديدة، وقم بتحديد اسم، واختر نوع الجهاز الذيAPICتم إنشاؤه في الخطوة 1. أختارTACACS Protocolالذي تم إنشاؤه في الخطوة 7. كبروتوكول مسموح به، وانقرSave.

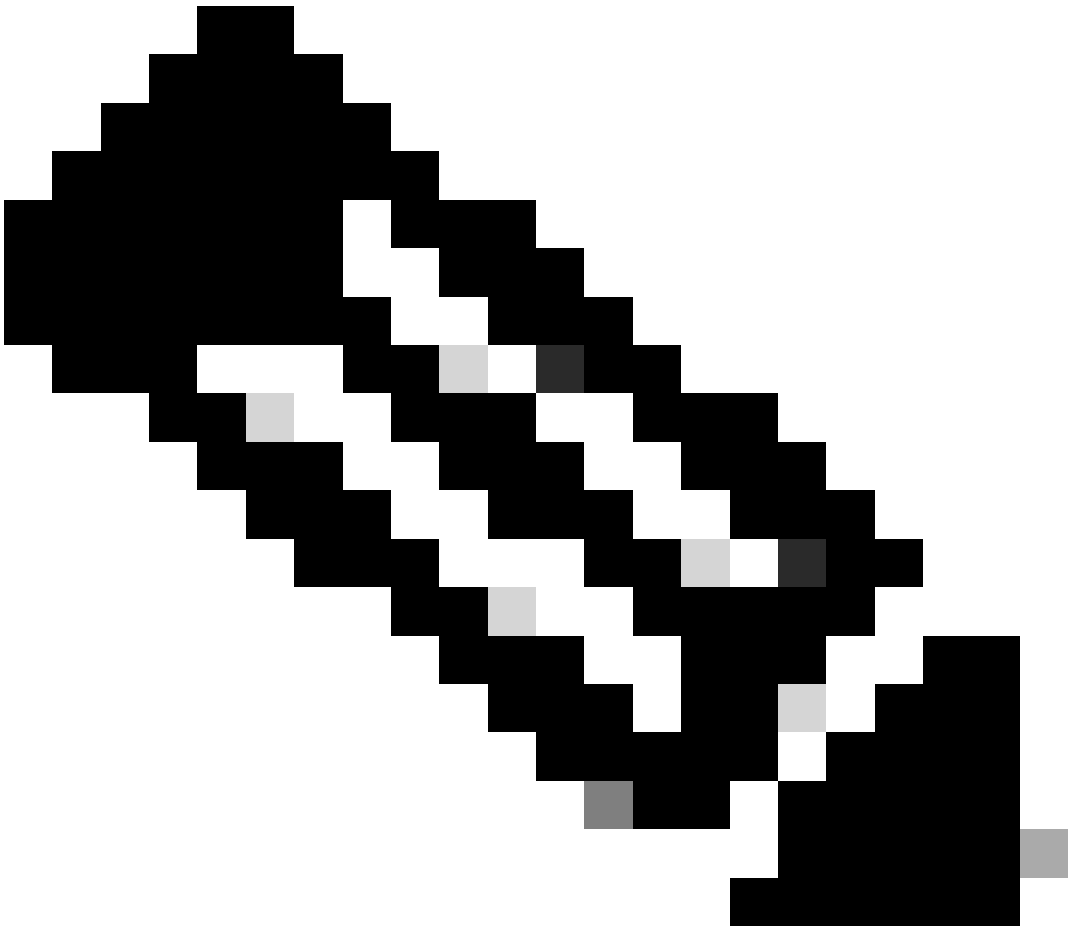


مجموعة نهج TACACS

الخطوة 10. تحت جديدPolicy Setانقر فوق السهم>الأيمن وقم بإنشاء سياسة مصادقة. قم بتعريف اسم واختر عنوان IP للجهاز كشرط. ثم أختر تسلسل مصدر الهوية الذي تم إنشاؤه في الخطوة 6.

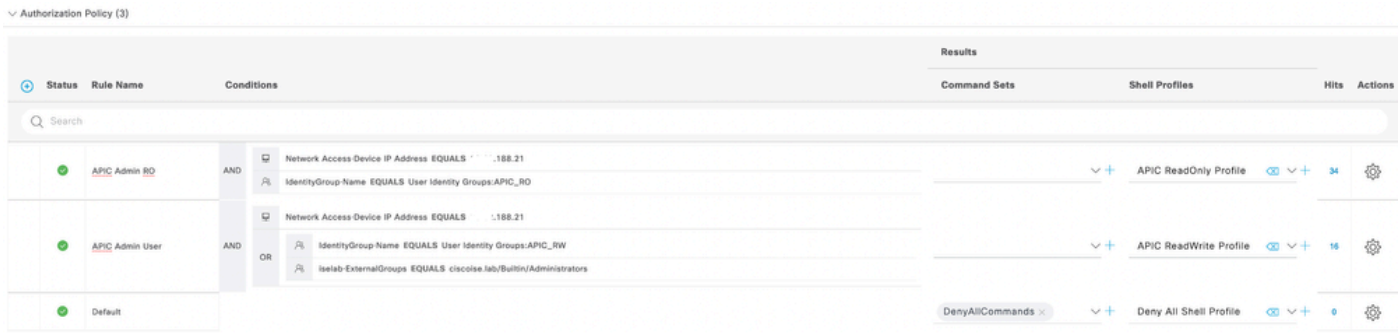


نهج المصادقة



ملاحظة: يمكن إستخدام الموقع أو السمات الأخرى كشرط مصادقة.

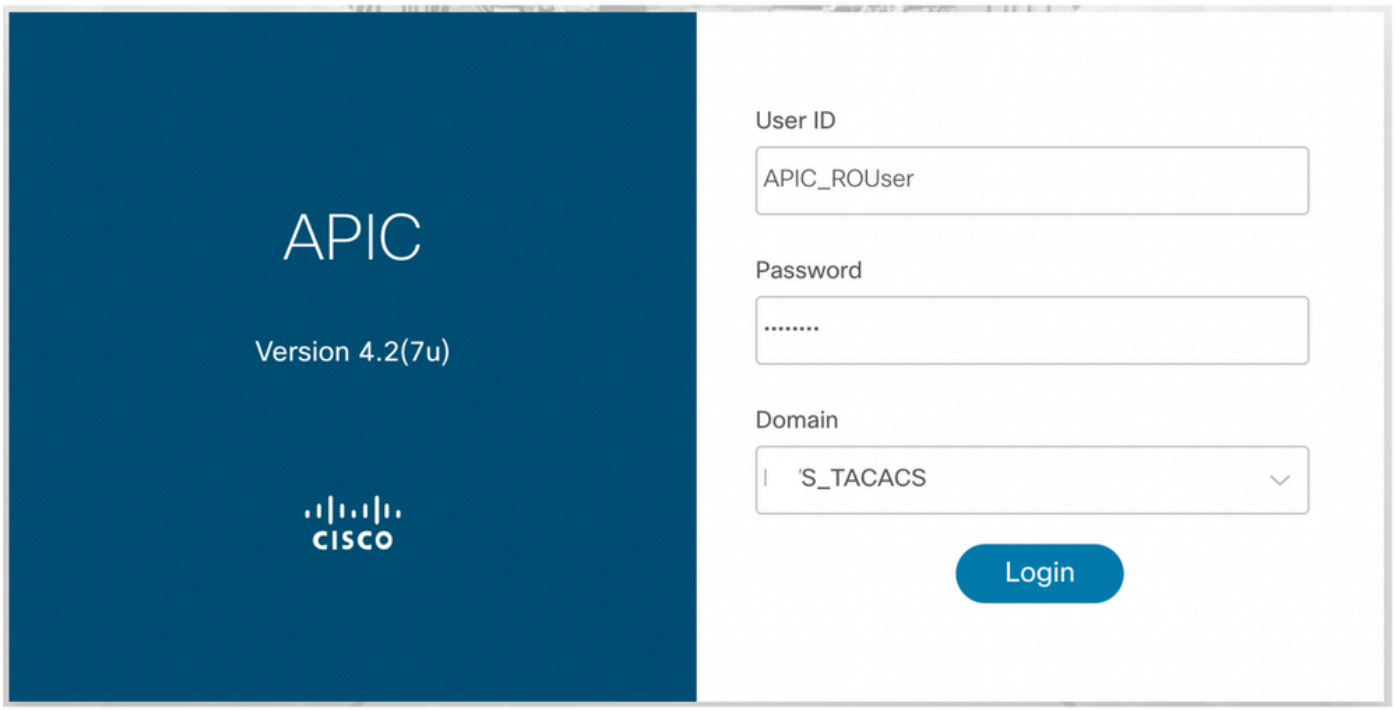
الخطوة 11. قم بإنشاء ملف تعريف تخويل لكل نوع مستخدم مسؤول، وقم بتعريف اسم، واختر مستخدم داخلي و/أو مجموعة مستخدم AD كشرط. يمكن إستخدام شروط إضافية مثل APIC. أختر ملف تعريف Shell المناسب في كل نهج تخويل وانقرSave.



ملف تعريف تفويض TACACS

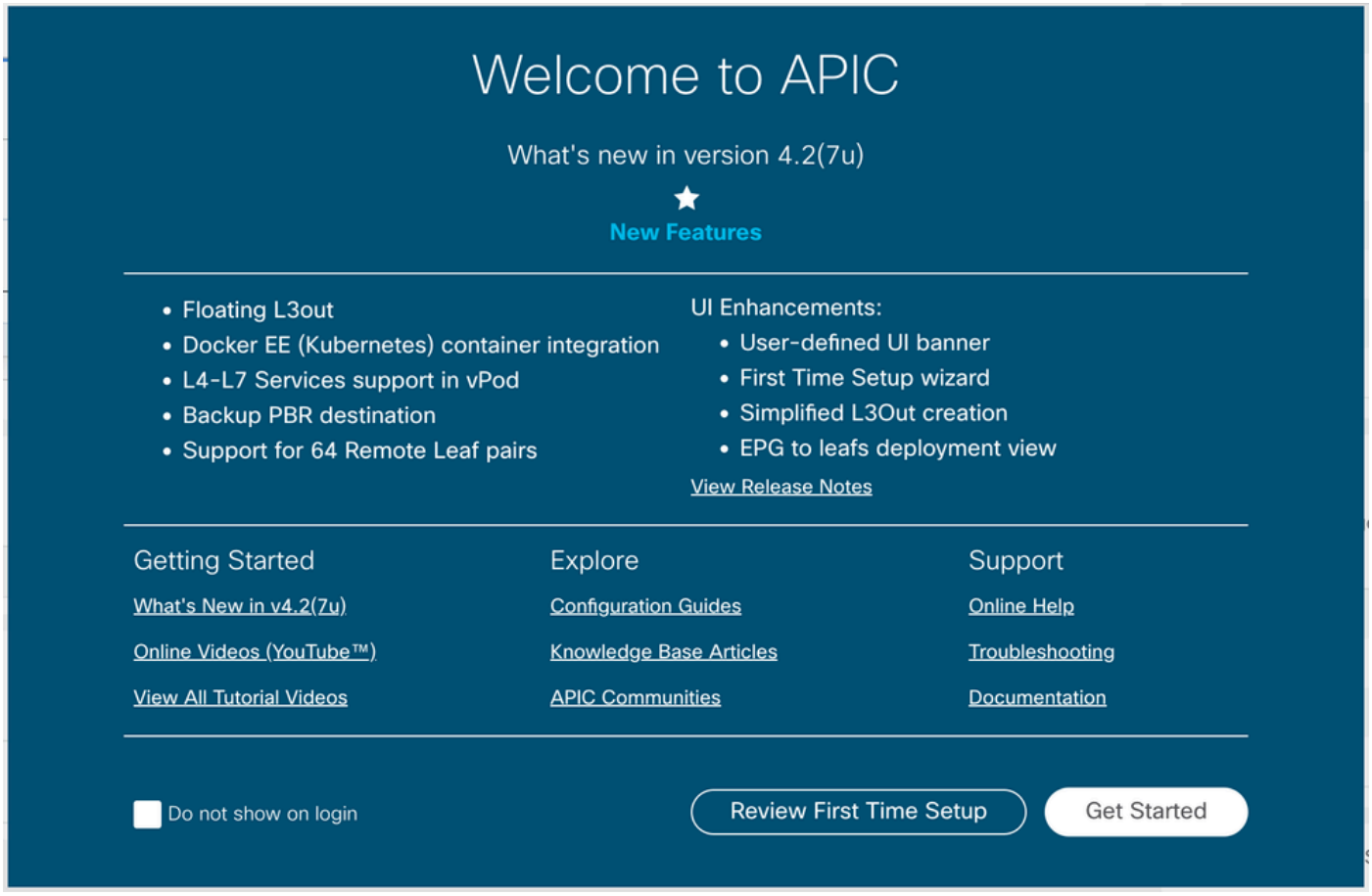
التحقق من الصحة

الخطوة 1. سجل الدخول إلى واجهة مستخدم APIC باستخدام مسوغات مسؤول المستخدم. أختر خيار TACACS من القائمة.



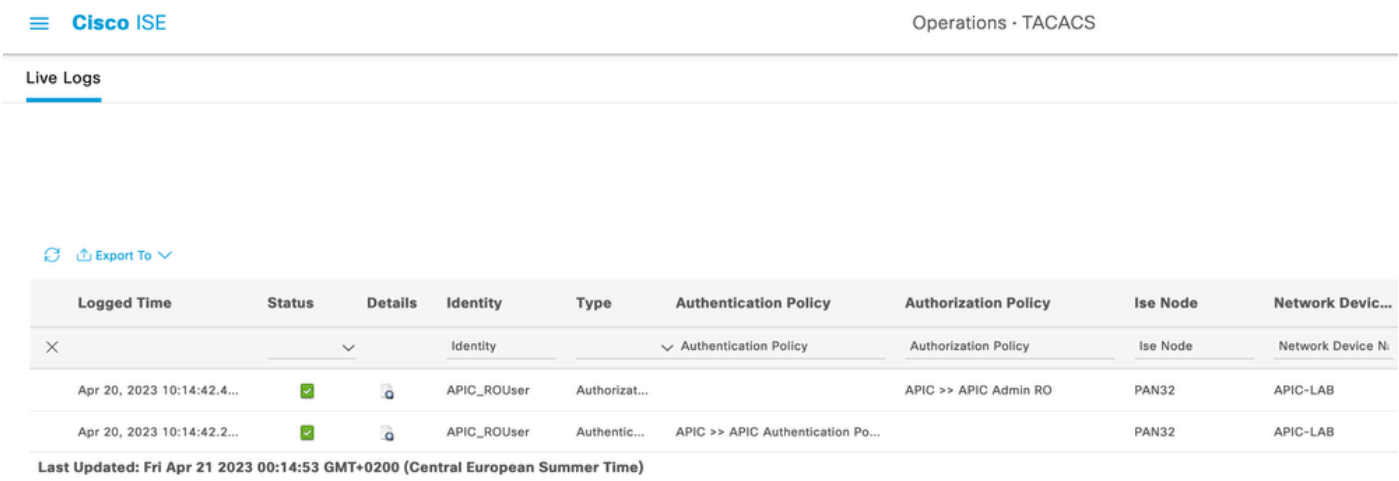
تسجيل دخول APIC

الخطوة 2. تحقق من الوصول إلى واجهة مستخدم APIC وتم تطبيق السياسات المناسبة على سجلات TACACS Live.



رسالة ترحيب APIC

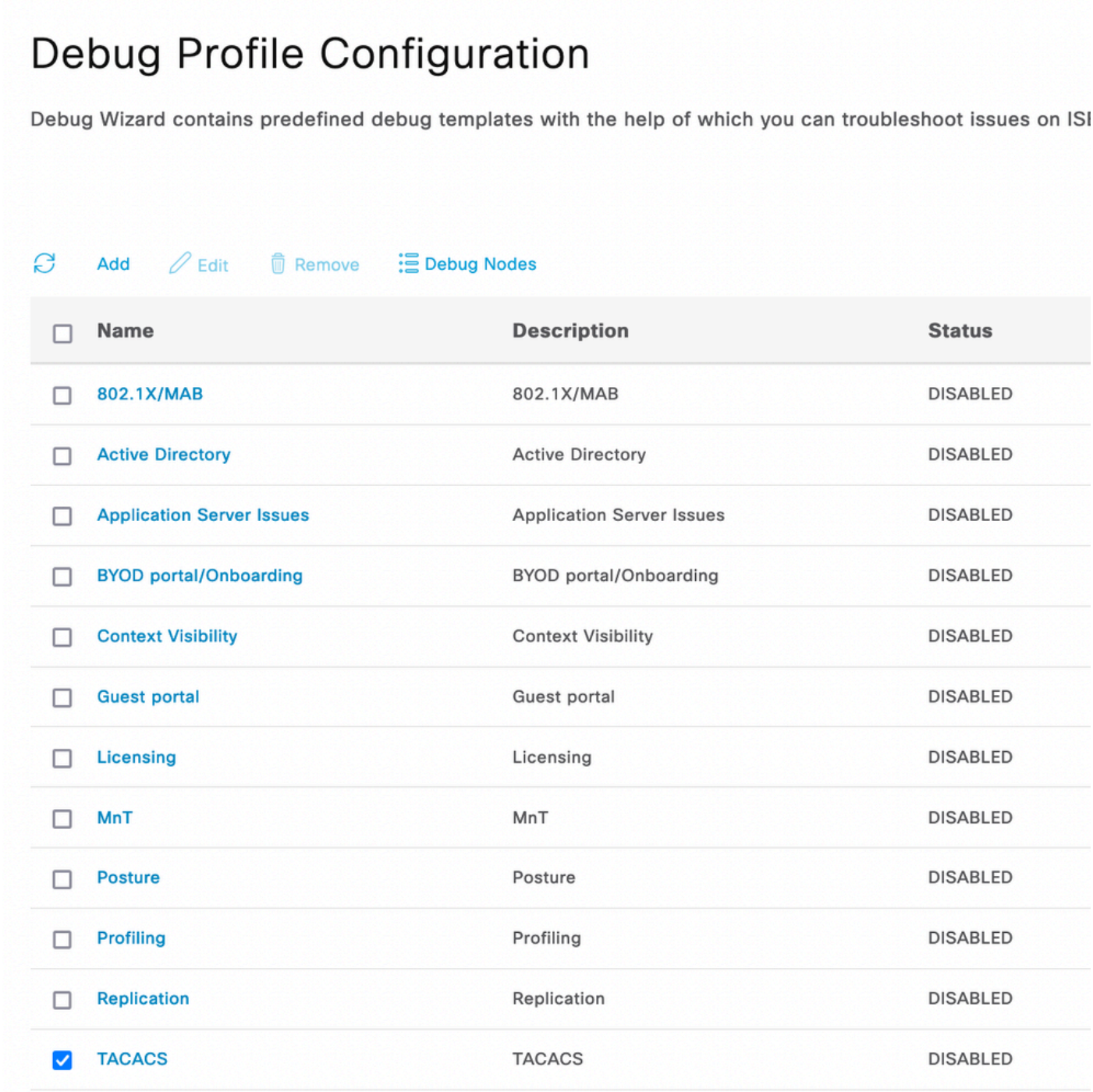
كرر الخطوات 1 و 2 لمستخدمي إدارة القراءة فقط.



سجلات TACACS+ المباشرة

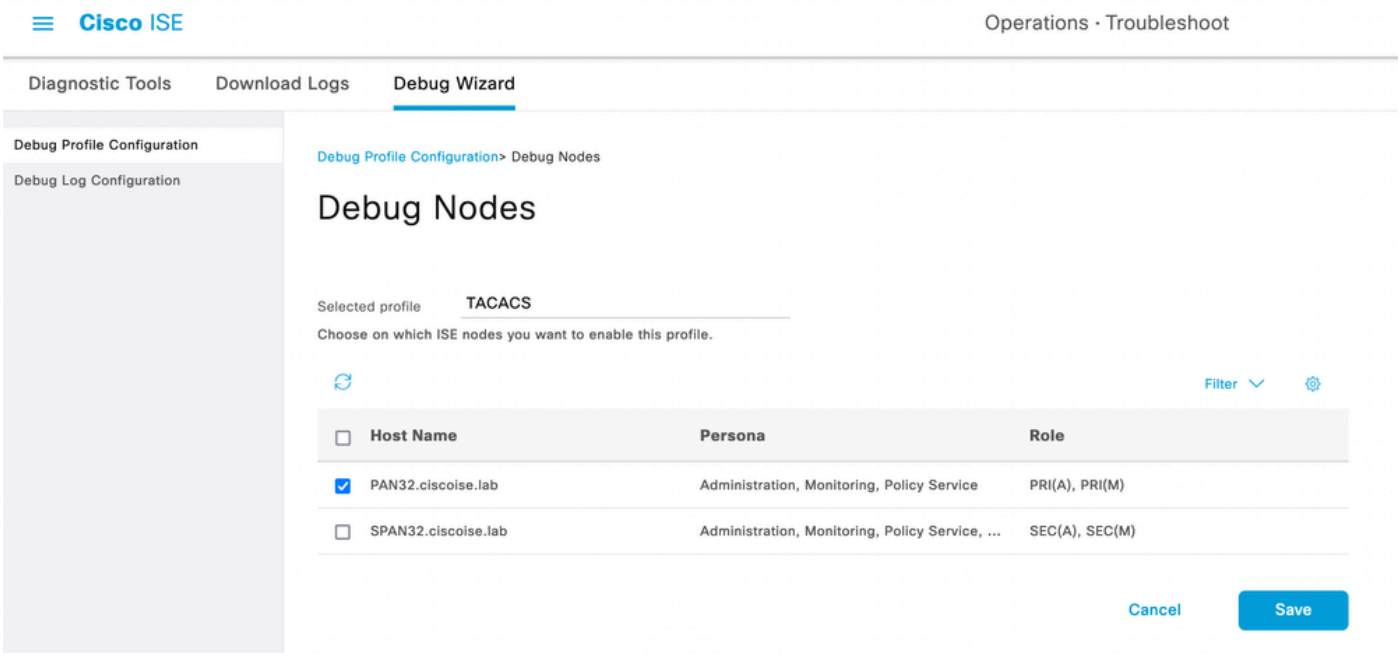
استكشاف الأخطاء وإصلاحها

الخطوة 1. انتقل إلى ☰ >Operations > Troubleshoot > Debug Wizard. أختر TACACSوانقر فوق Debug Nodes.



تكوين ملف تعريف التصحيح

الخطوة 2. أختر العقدة التي تستلم حركة المرور وانقرSave.



تحديد عقد تصحيح الأخطاء

الخطوة 3. قم بإجراء إختبار جديد وقم بتنزيل السجلات الواردةOperations > Troubleshoot > Download logs كما هو موضح:

```
AcsLogs,2023-04-20 22:17:16,866,DEBUG,0x7f93cabc7700,cntx=0004699242,sesn=PAN32/469596415/70,CPMSession
```

في حالة عدم إظهار تصحيح الأخطاء معلومات المصادقة والتفويض، قم بالتحقق من صحة ما يلي:

1. يتم تمكين خدمة "إدارة الأجهزة" على عقدة ISE.
2. تمت إضافة عنوان ISE الصحيح إلى تكوين APIC.
3. في حالة وجود جدار حماية في المنتصف، فتحقق من أن المنفذ 49 (TACACS) مسموح به.

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).