تكوين المصادقة والتفويض الخارجيين لـ FDM باستخدام ISE باستخدام RADIUS

المحتويات

المقدمة

يصف هذا المستند إجراء دمج Cisco Firepower Device Manager (FDM) مع Identity Services Engine (ISE) لمصادقة مستخدمي المسؤول مع بروتوكول RADIUS للوصول إلى واجهة المستخدم الرسومية (GUI) وواجهة سطر الأوامر (CLI).

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- مدير جهاز Firepower (FDM)
- محرك خدمات الهوية (ISE)
- بروتوكول RADIUS

المكونات المستخدمة

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

- جهاز الدفاع عن تهديد Firepower (FTD)، جميع الأنظمة الأساسية إصدار 6.3.0+ من مدير أجهزة FirePOWER (FDM)
- ISE الإصدار 3.0

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.

قابلية التشغيل البيني

- خادم RADIUS المزود بمستخدمين تم تكوينهم بأدوار مستخدمين
- يجب تكوين أدوار المستخدمين على خادم RADIUS باستخدام زوج أجهزة Cisco-AV
- Cisco-av-pair = fdm.userRole.authority.admin
- يمكن إستخدام ISE كخادم RADIUS

الترخيص

الترخيص الأساسي كاف، ال يتطلب ترخيص محدد

معلومات أساسية

تتيح هذه الميزة للعملاء تكوين المصادقة الخارجية باستخدام RADIUS وأدوار المستخدمين المتعددة لعملاء المستخدمين.

دعم RADIUS للوصول إلى الإدارة من خلال 3 أدوار محددة بواسطة النظام للمستخدمين:

- Read_Only
- READ_WRITE (ال يمكن تنفيذ الإجراءات الهامة للنظام مثل الترقية والاستعادة وما إلى ذلك)
- المسؤول

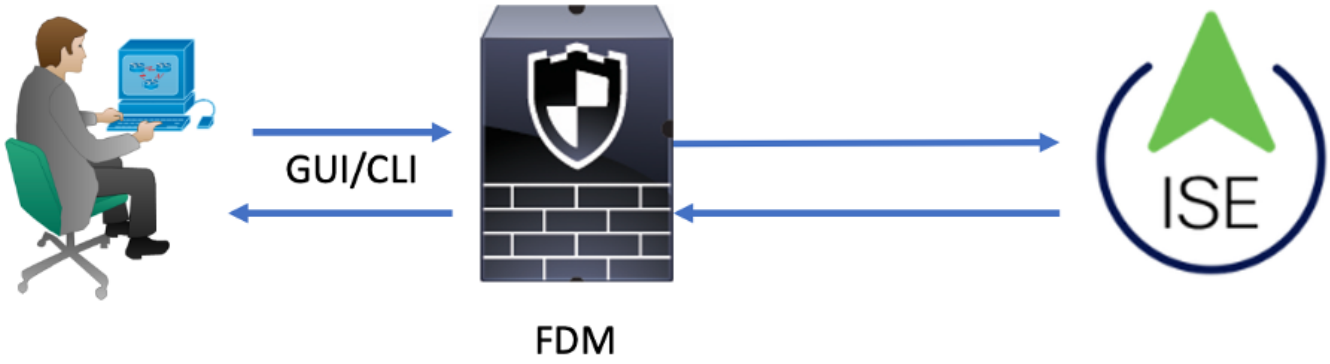
هناك القدرة على إختبار تكوين خادم RADIUS ومراقبة جلسات عمل المستخدم النشطة وحذف جلسة عمل المستخدم.

تم تنفيذ الميزة في الإصدار 6.3.0 من FDM. قبل إصدار 6.3.0، كان لدى FDM دعم لمستخدم واحد (مسؤول) فقط.

وبشكل افتراضي، يقوم مدير أجهزة FirePOWER من Cisco بمصادقة المستخدمين محلياً، ويمكنك إستخدام مركزية تفويض ومصادقة طريقة للوصول على خادم RADIUS. وتخويلهم من خلال بروتوكول RADIUS من Cisco من خلال هوية المستخدم.

الرسم التخطيطي للشبكة

توفر الصورة التالية مثال لطوبولوجيا الشبكة



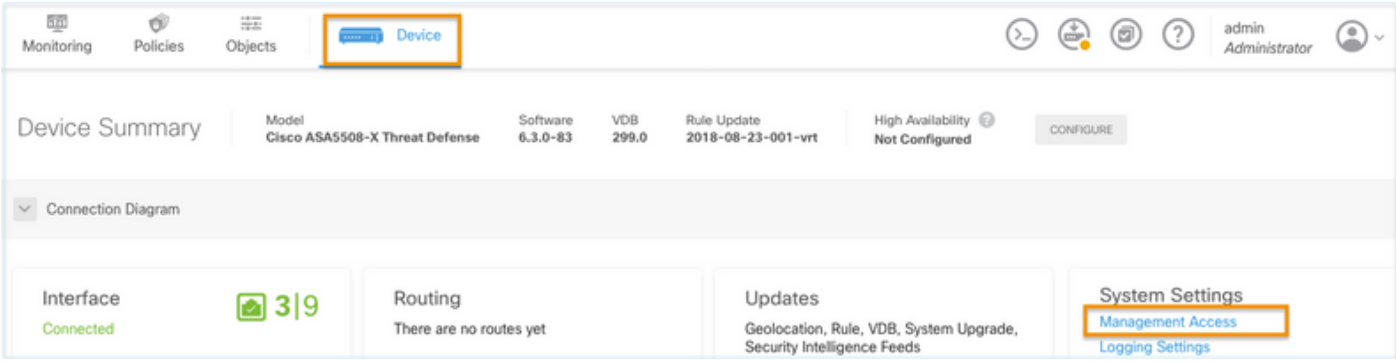
العملية:

1. يقدم مستخدم المسؤول بيانات الاعتماد الخاصة به.
2. تم تشغيل عملية المصادقة ويقوم ISE بالتحقق من صحة بيانات الاعتماد محليا أو من خلال Active Directory.
3. وبمجرد نجاح المصادقة، يرسل ISE حزمة السماح لمعلومات المصادقة والتفويض إلى FDM.
4. يتم تنفيذ الحساب على ISE ويحدث سجل نشط للمصادقة الناجحة.

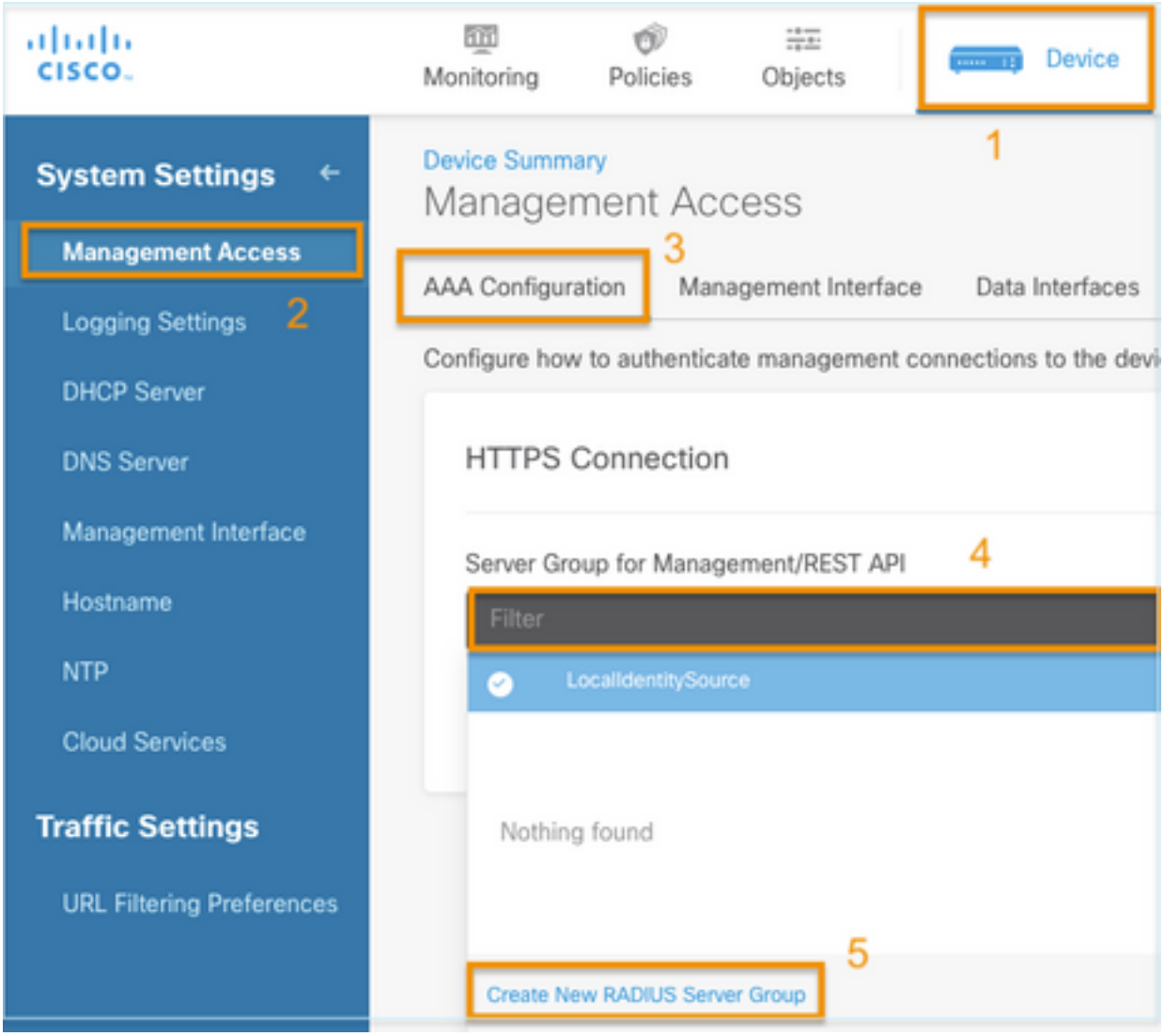
التكوين

تكوين FDM

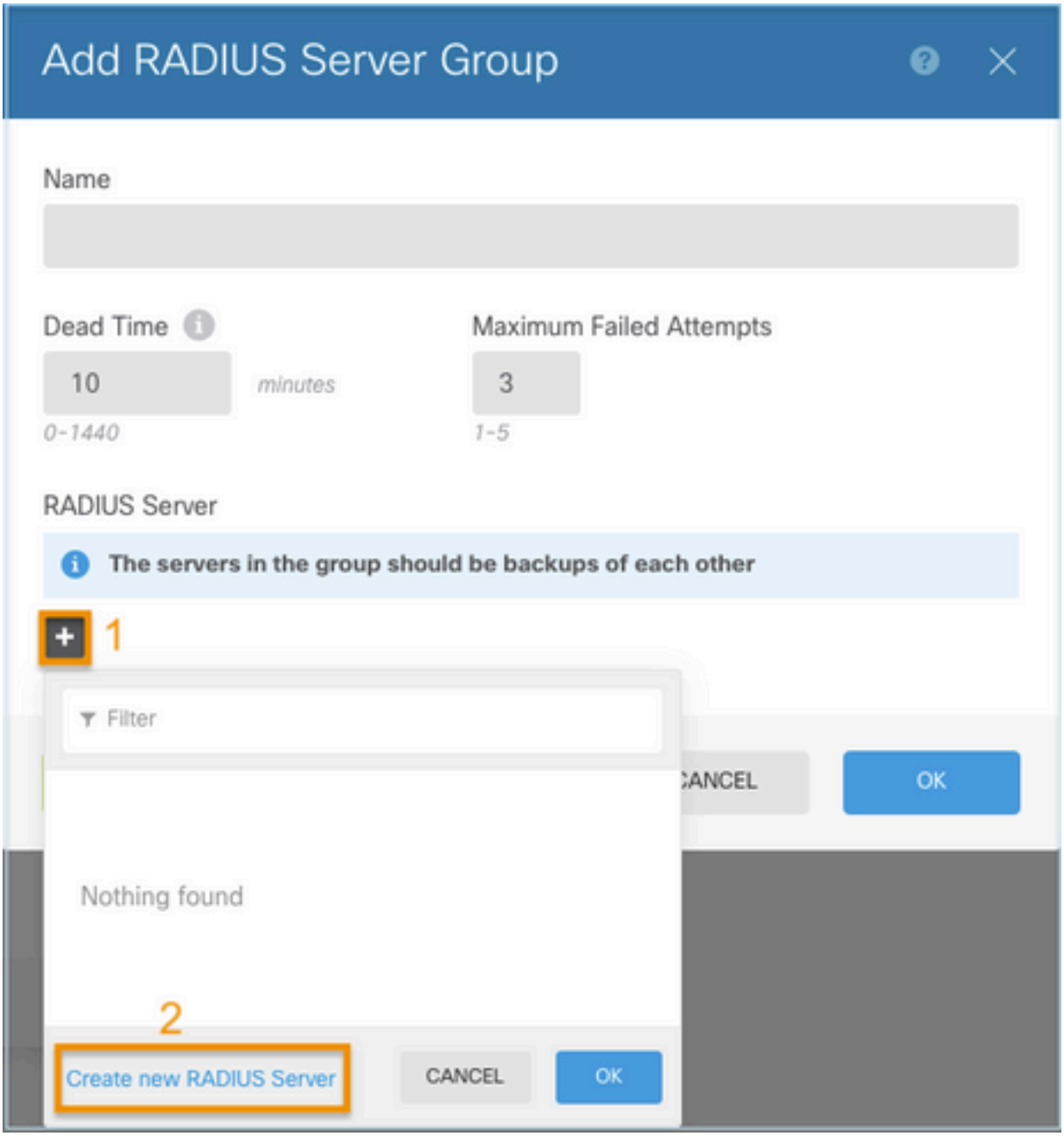
الخطوة 1. سجل الدخول في FDM وانتقل إلى جهاز > إعدادات النظام > علامة تبويب الوصول إلى الإدارة

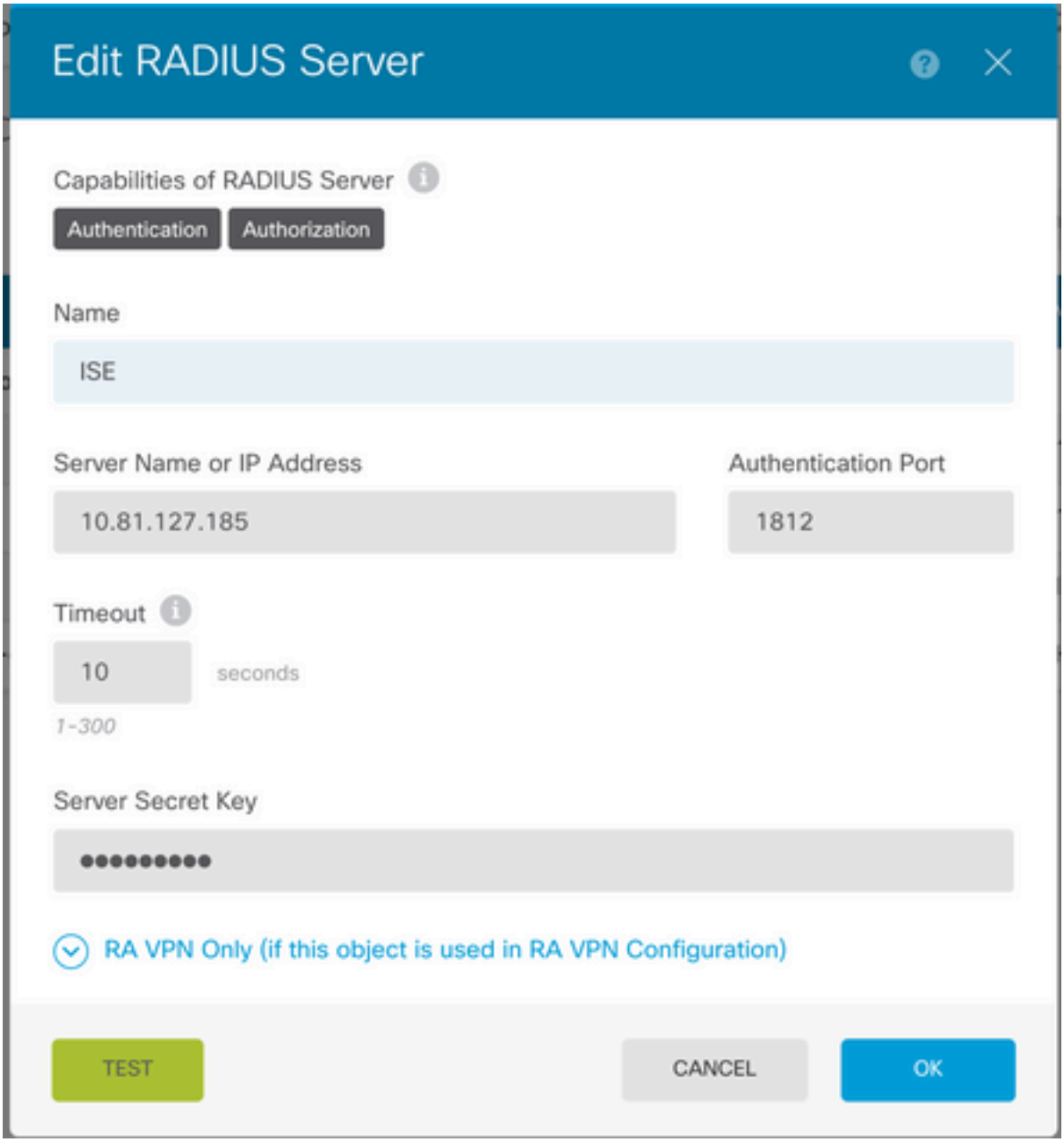


الخطوة 2. إنشاء مجموعة خوادم RADIUS جديدة

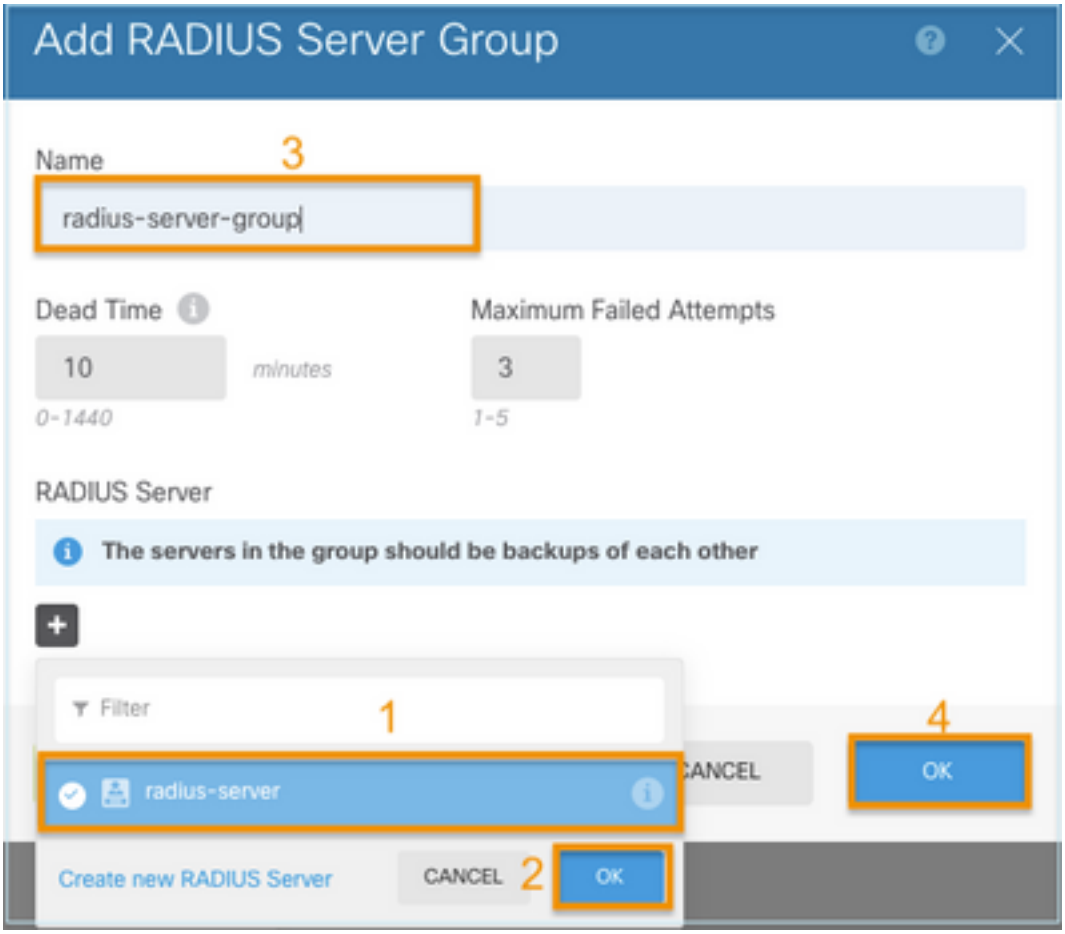


الخطوة 3. إنشاء خادم RADIUS جديد

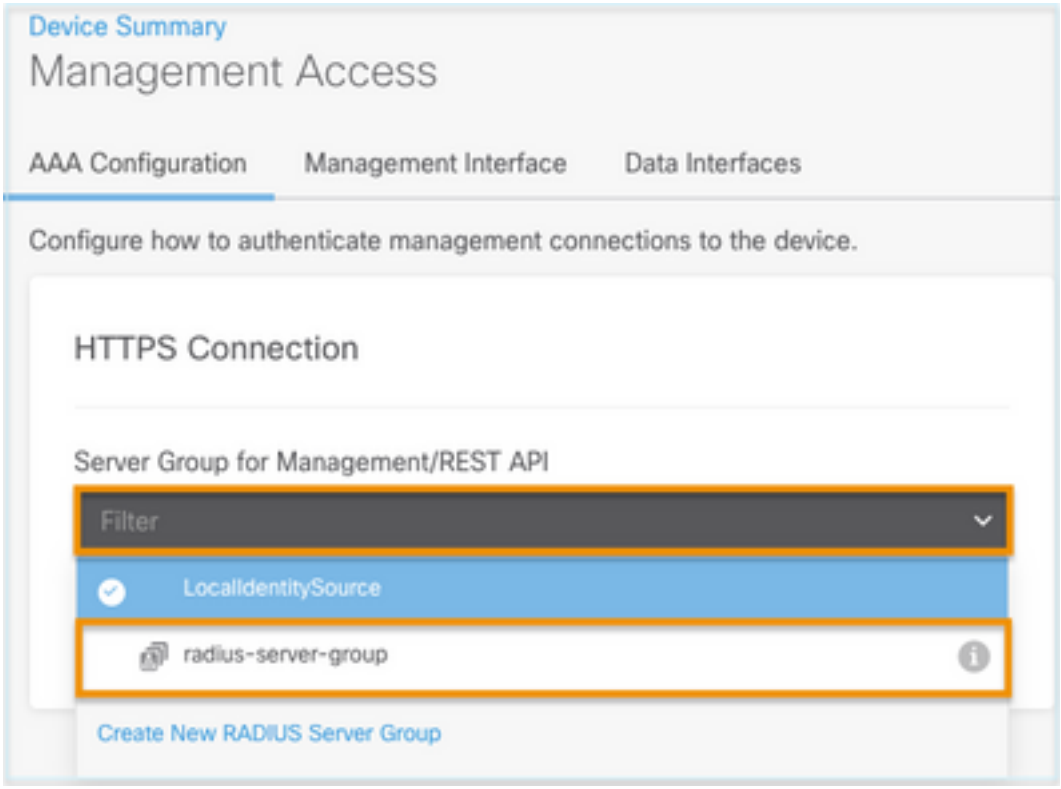

Add RADIUS Server Group
Name
Dead Time
10
minutes
0-1440
Maximum Failed Attempts
3
1-5
RADIUS Server
The servers in the group should be backups of each other
1
Filter
CANCEL
OK
Nothing found
2
Create new RADIUS Server
CANCEL
OK

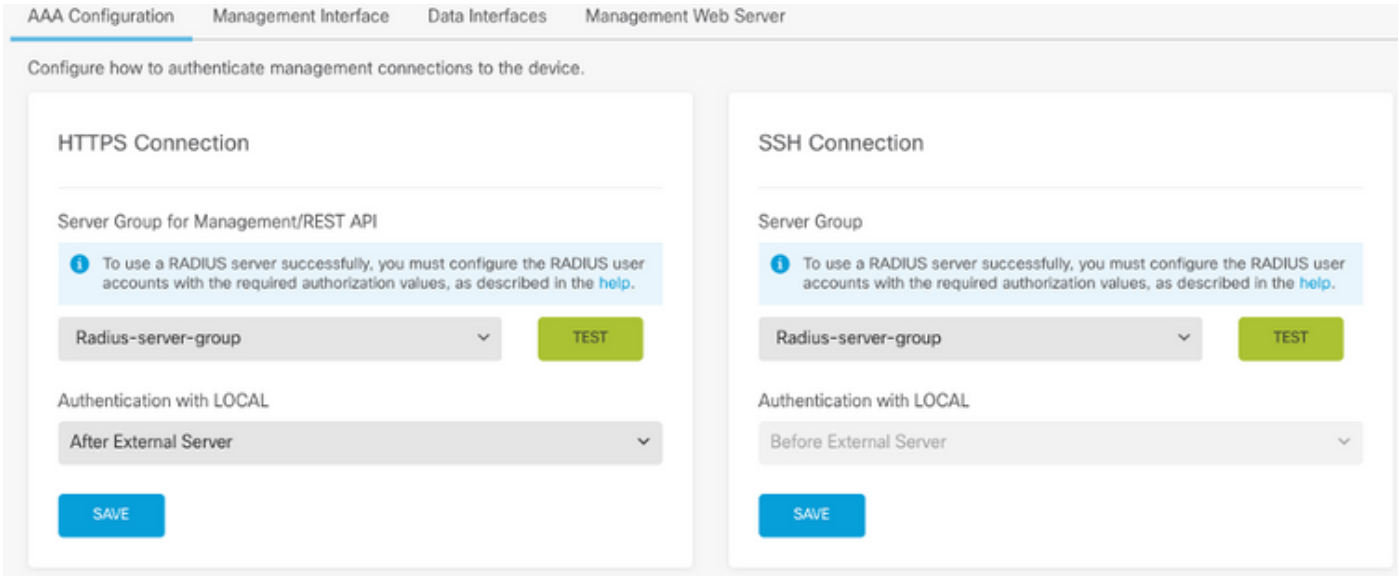


الخطوة 4. إضافة خادم RADIUS إلى مجموعة خوادم RADIUS

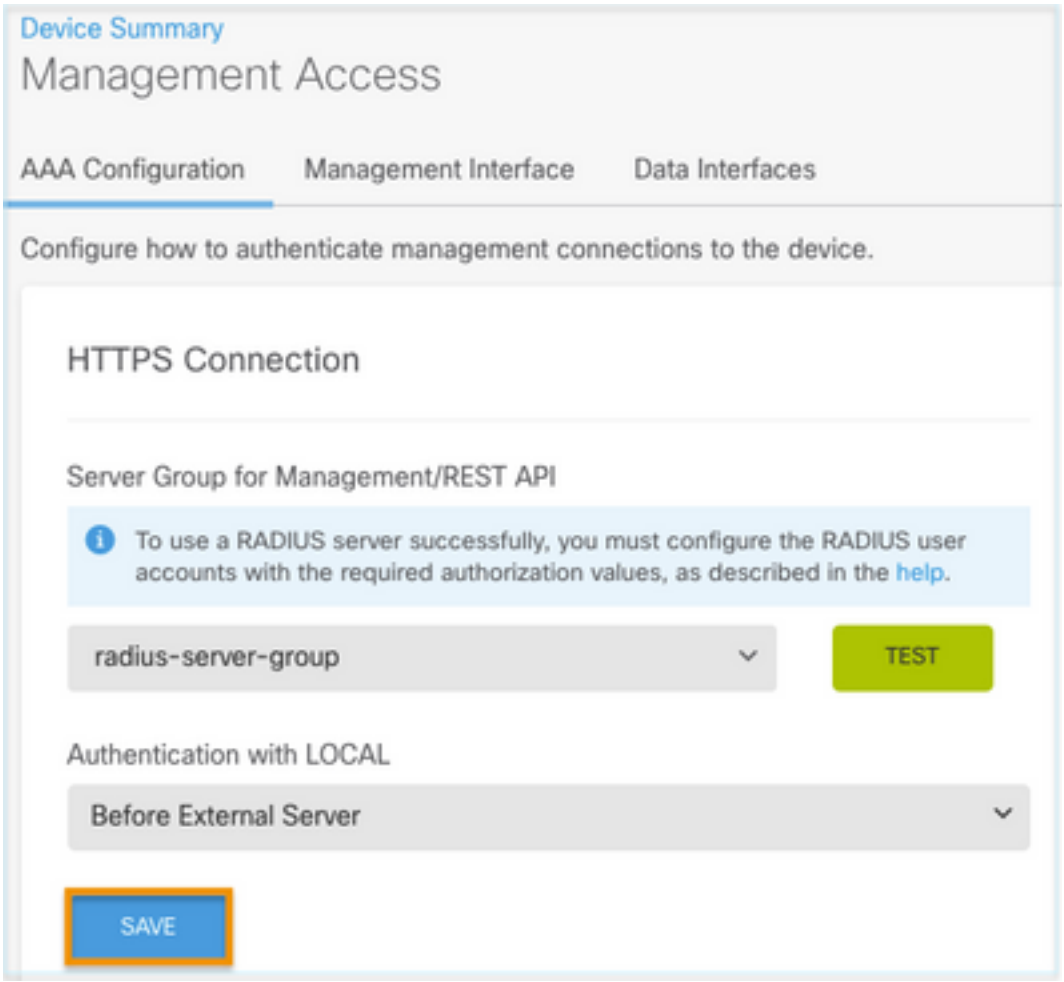


الخطوة 5. تحديد المجموعة التي تم إنشاؤها كمجموعة خوادم للإدارة



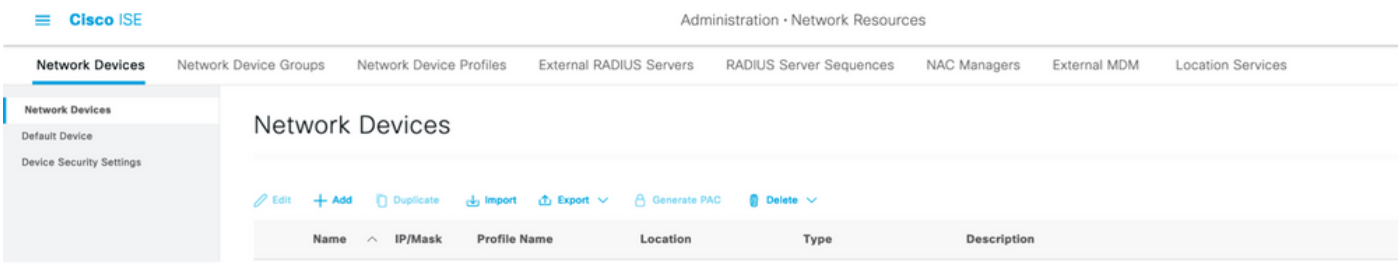


الخطوة 6. حفظ التكوين

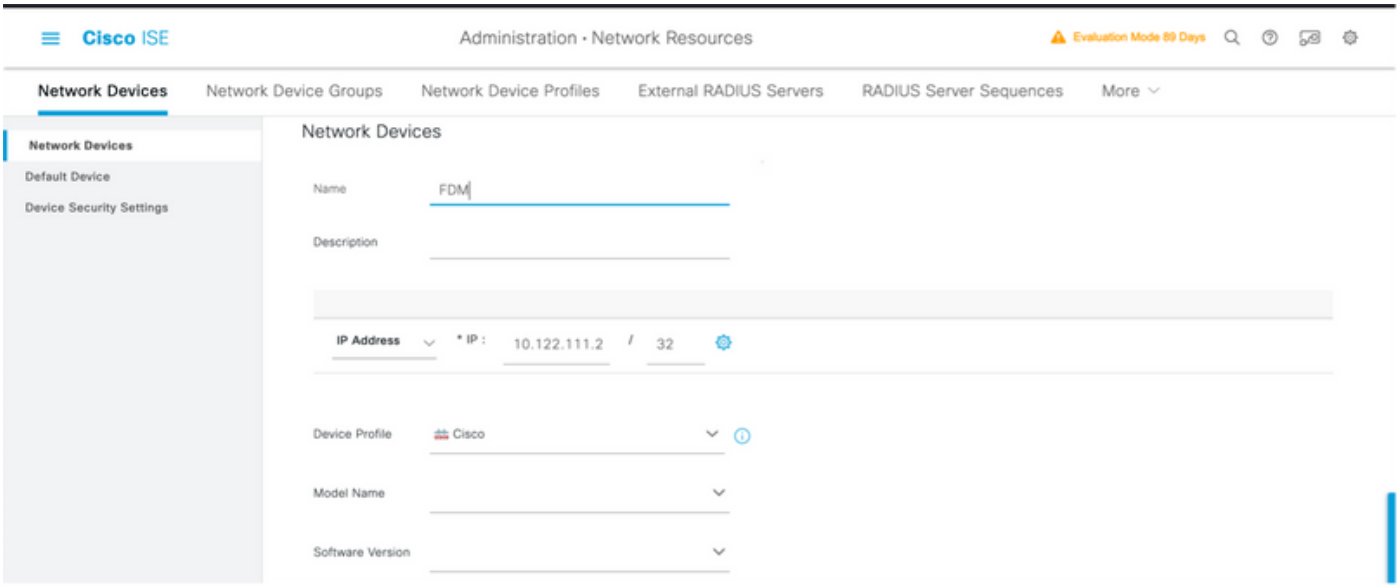


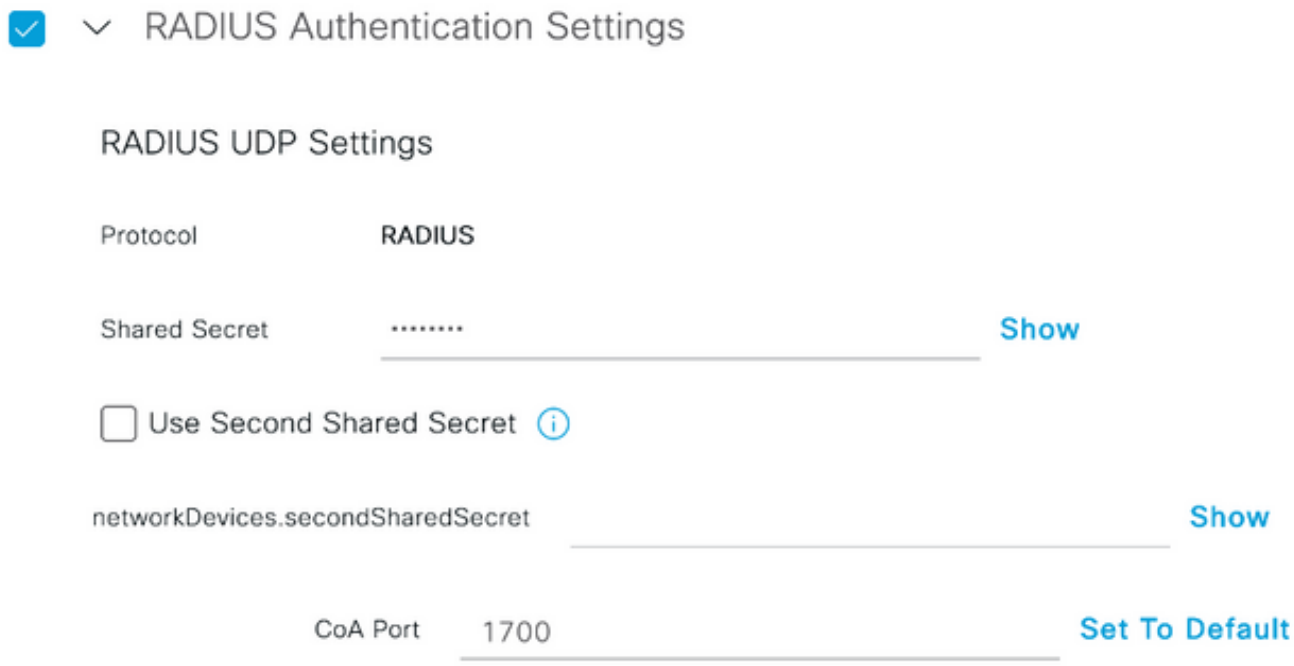
تكوين ISE

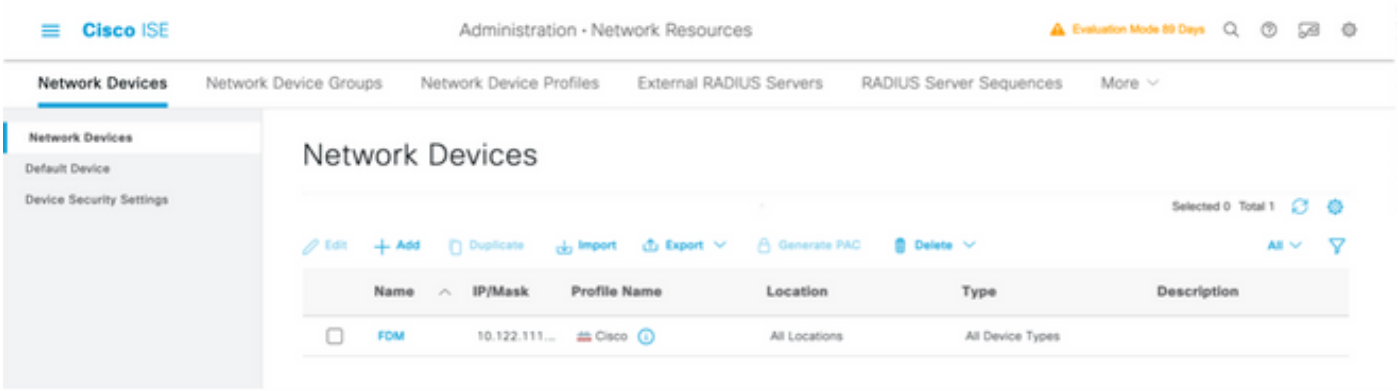
الخطوة 1. انتقل إلى أيقونة ثلاثة أسطر موجود في الزاوية العلوية اليسرى وحدد إدارة > موارد الشبكة > أجهزة الشبكة



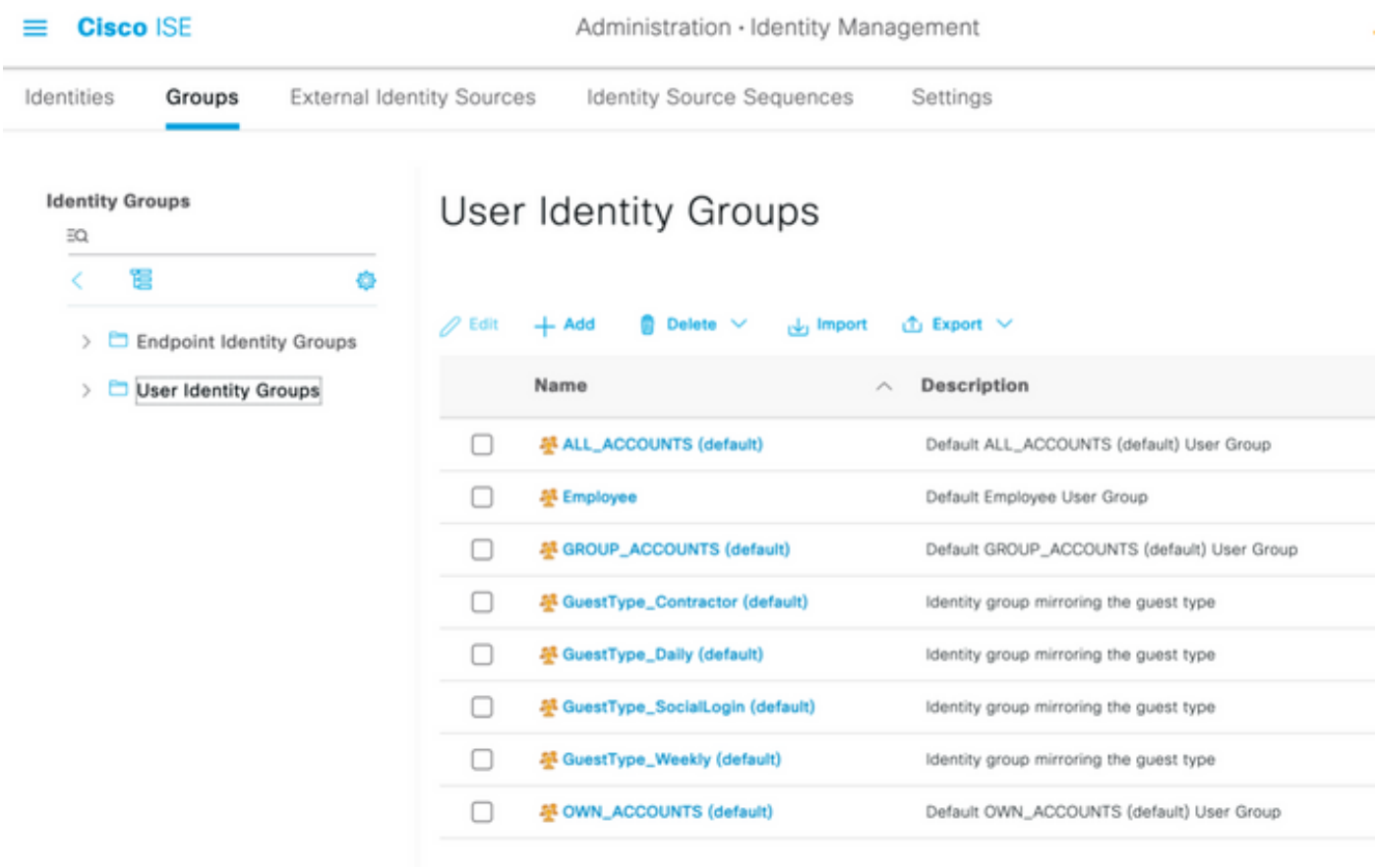
الخطوة 2. حدد الزر **+إضافة** وحدد اسم جهاز الوصول إلى الشبكة وكلمة المرور، ثم حدد خانة إختيار RADIUS وحدد سرا مشتركا. تحديد عند **الإرسال**



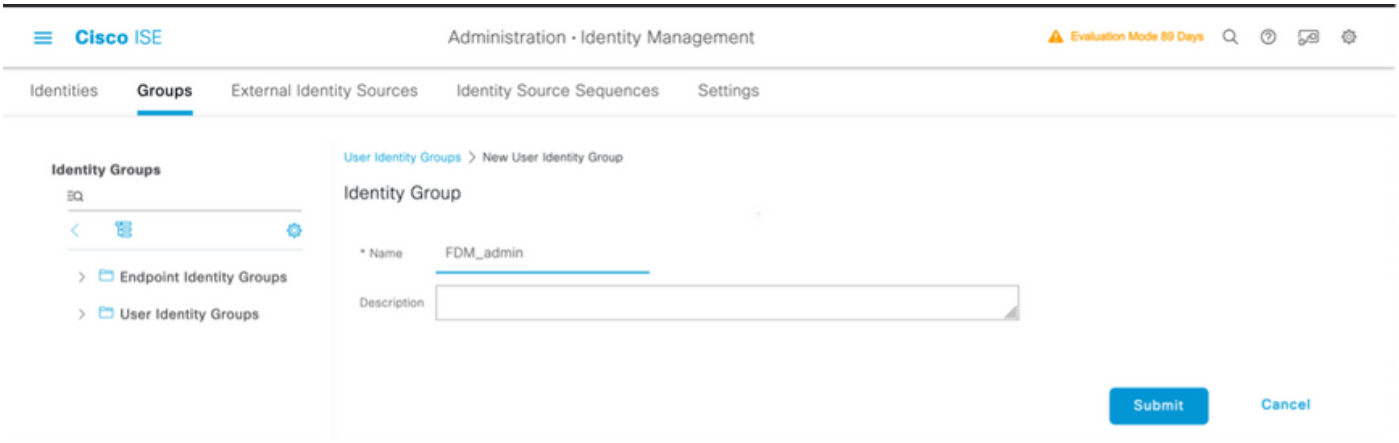


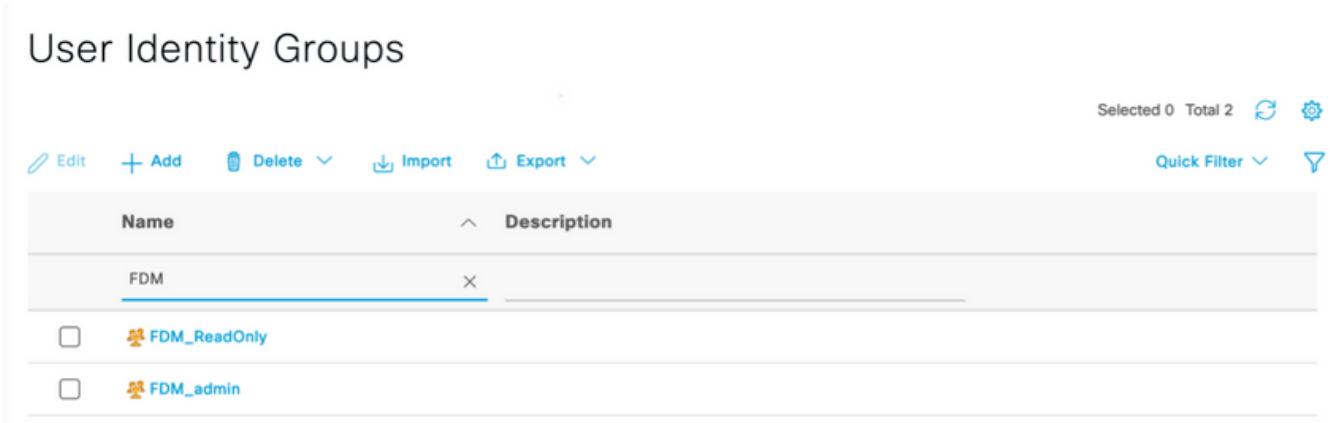


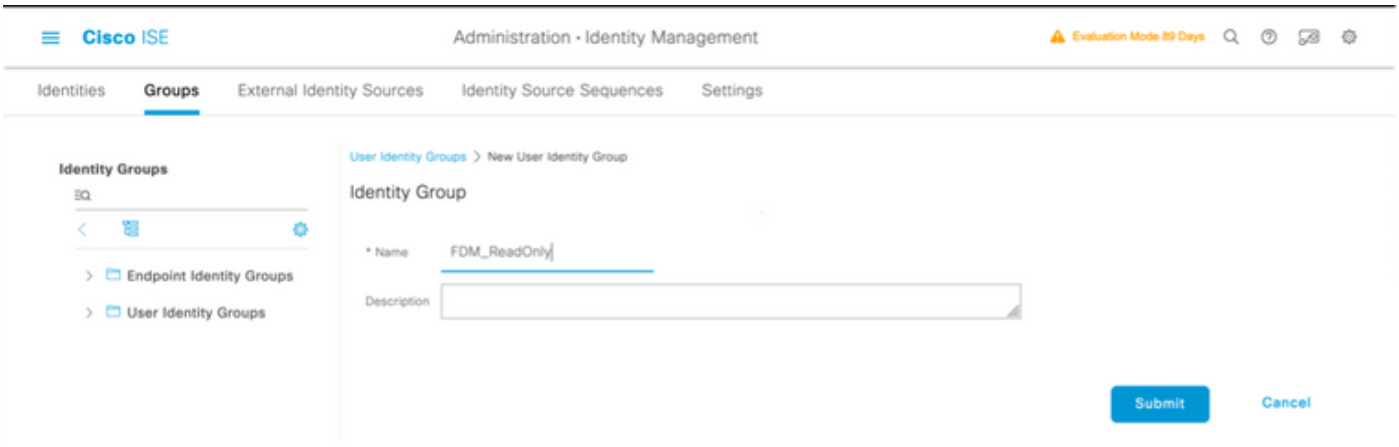
الخطوة 3. انتقل إلى أيقونة ثلاثة أسطر موجود في الزاوية العلوية اليسرى وحدد على **إدارة > إدارة الهوية > المجموعات**



الخطوة 4. حدد على مجموعات هوية المستخدم وحدد على **+إضافة** زر. قم بتحديد اسم وحدد عند الإرسال

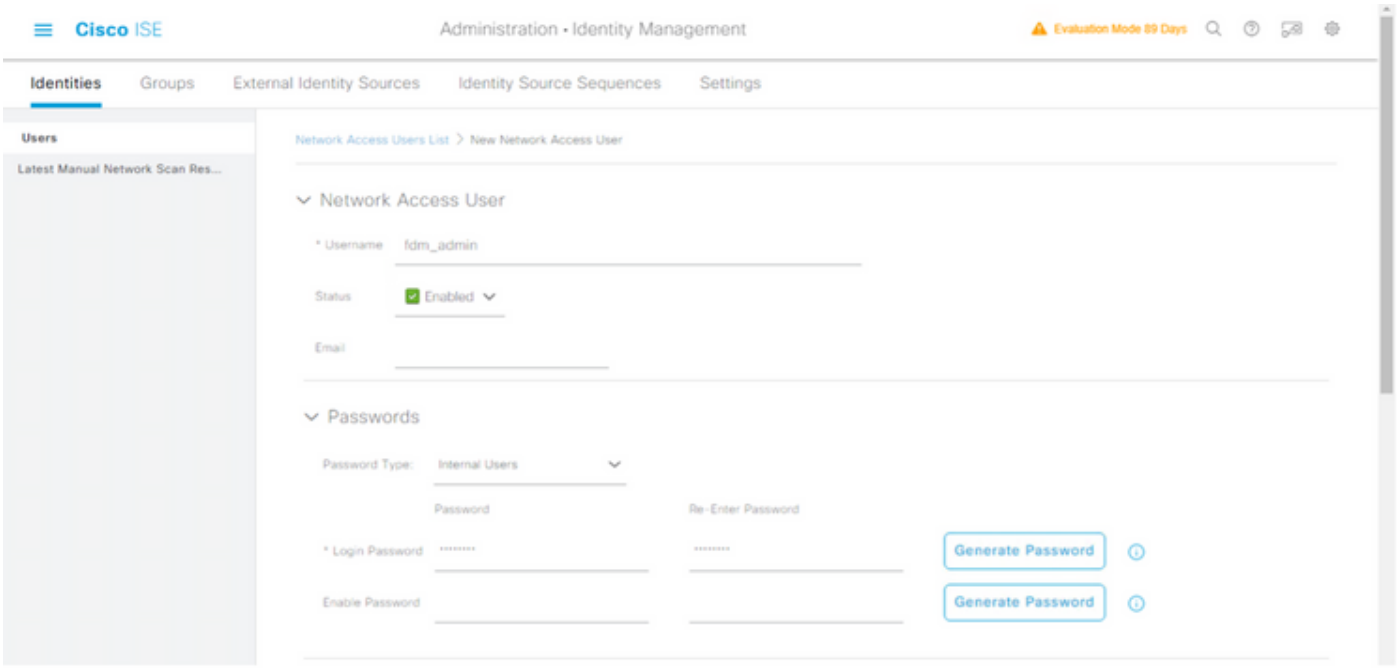


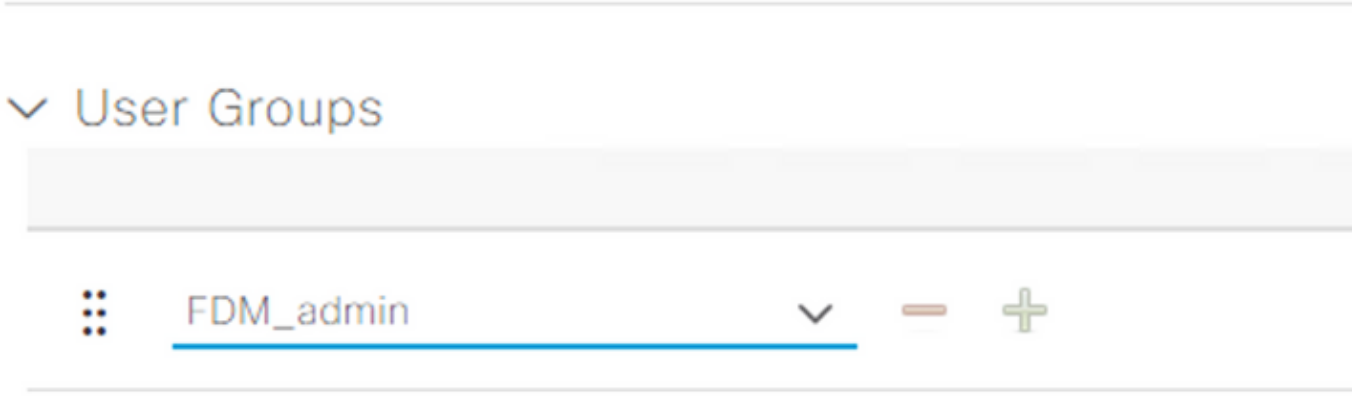


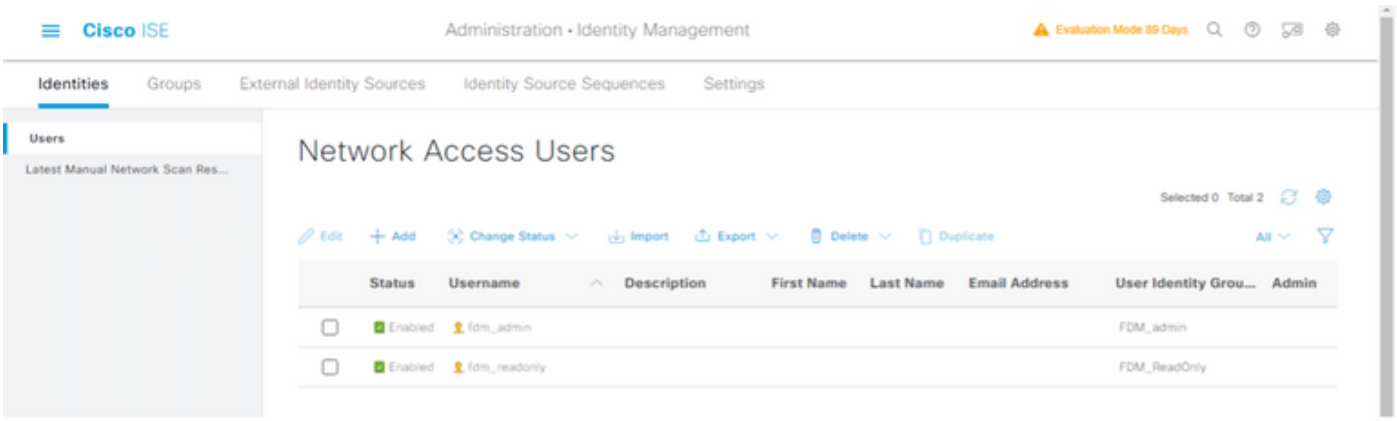


ملاحظة: في هذا المثال، تم إنشاء مجموعات هوية FDM_Admin و FDM_ReadOnly، يمكنك تكرار الخطوة 4 لكل نوع من أنواع مستخدمي المسؤول المستخدمين على FDM.

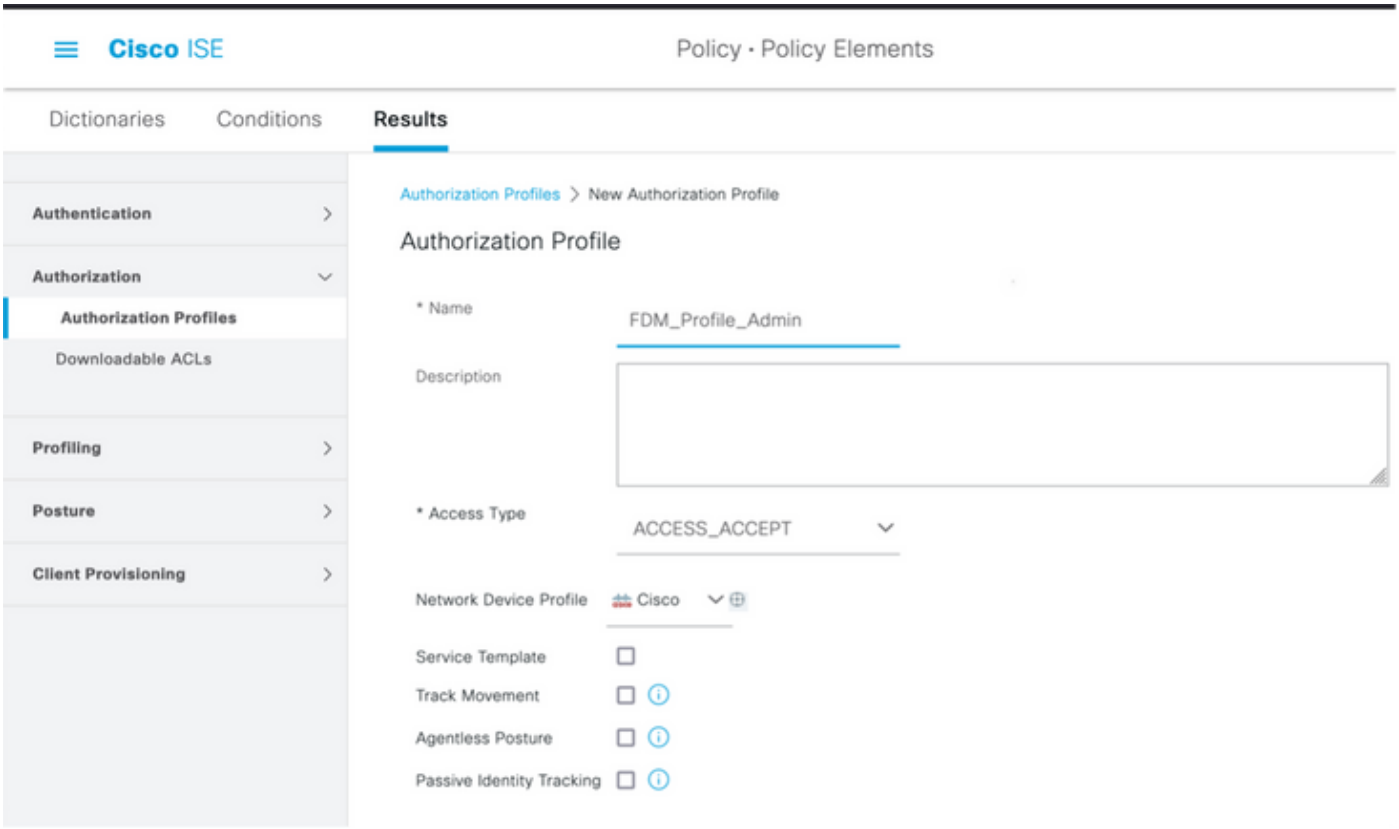
الخطوة 5. انتقل إلى أيقونة ثلاثة أسطر موجودة في الزاوية العلوية اليسرى وحدد إدارة > إدارة الهوية > الهويات. حدد على **+إضافة** وقم بتعريف اسم المستخدم وكلمة المرور، ثم حدد المجموعة التي ينتمي إليها المستخدم. في هذا المثال، تم إنشاء مستخدمي FDM_admin و fdm_readonly وتخصيصهم لمجموعة FDM_Admin و FDM_ReadOnly على التوالي.

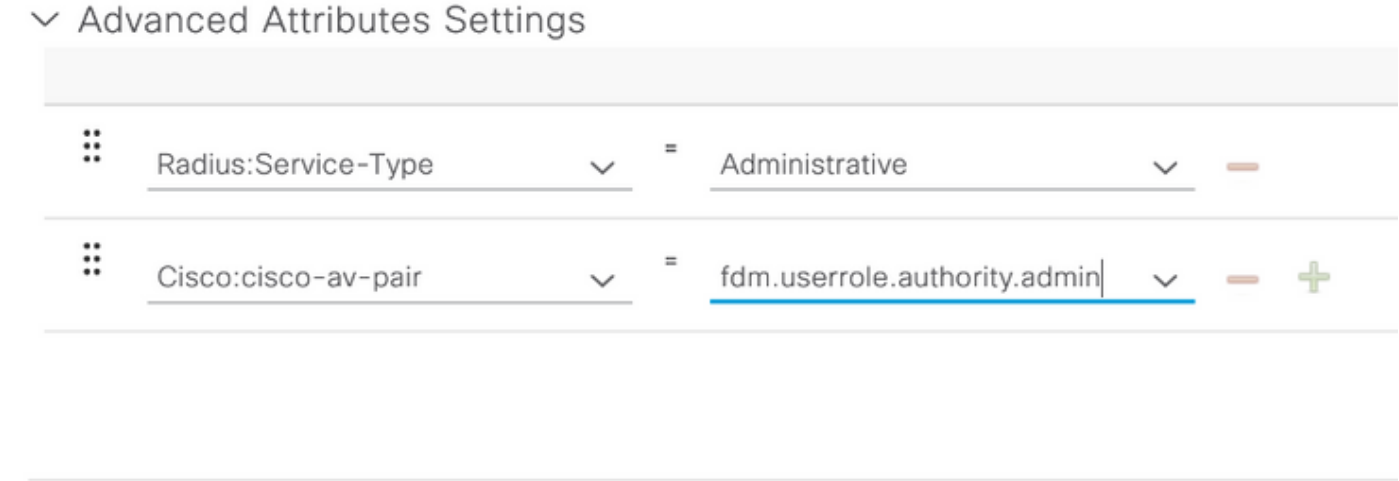


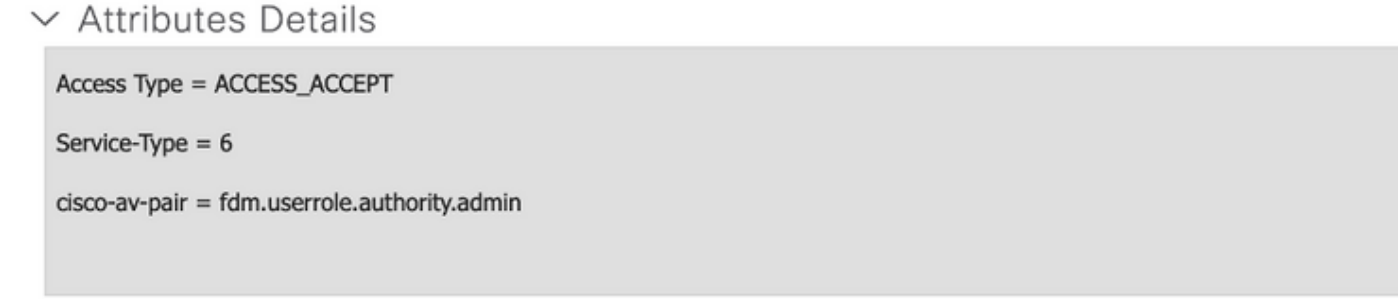


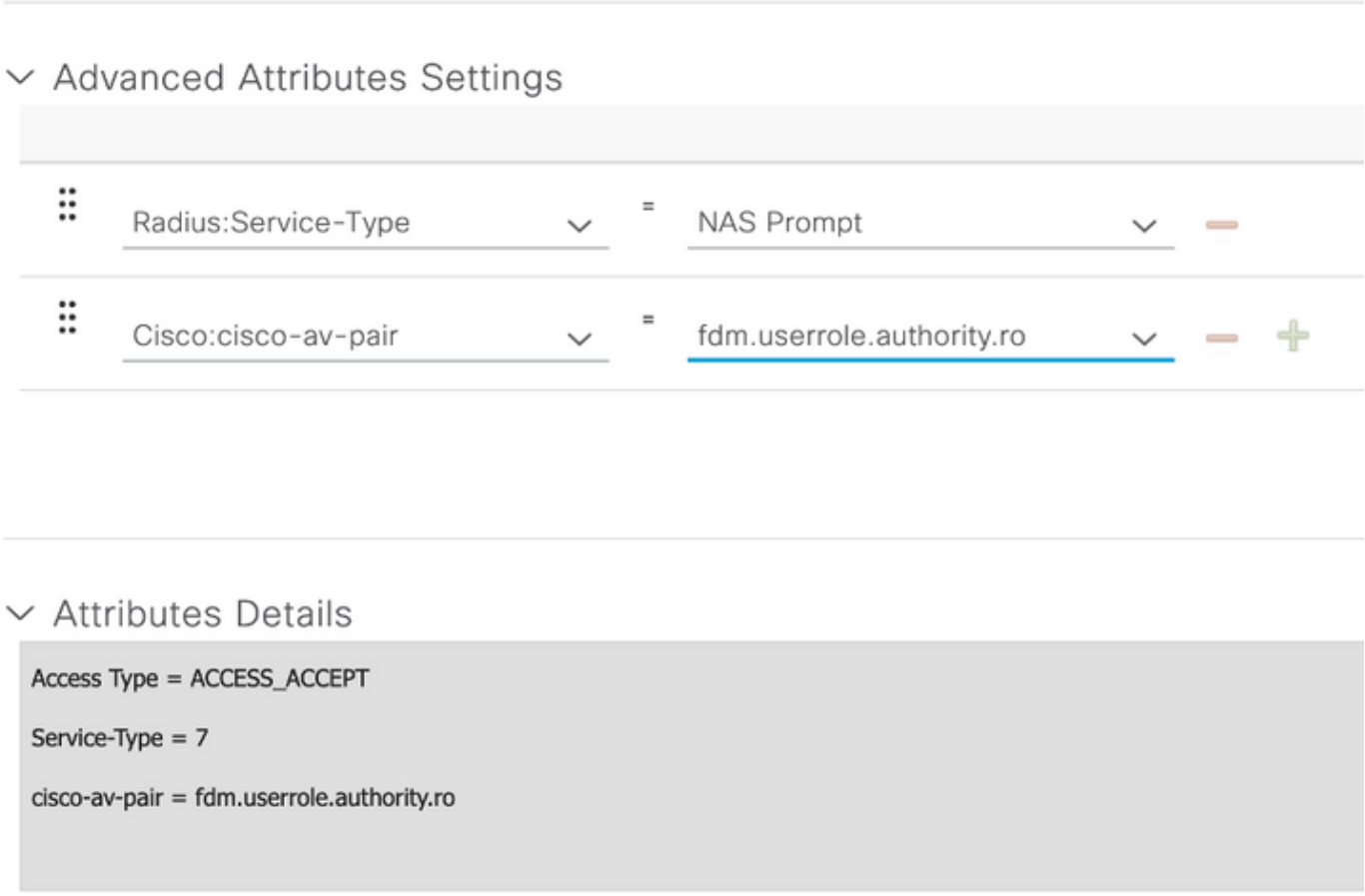


الخطوة 6. حدد أيقونة الأسطر الثلاثة الموجودة في الركن الأعلى الأيسر وتصفح إلى **السياسة > عناصر السياسة > النتائج > التخويل > ملفات تخصيص التخويل**، حدد على **+إضافة**، قم بتعريف اسم لملف تخصيص **التخويل**. حدد **نوع خدمة Radius** وحدد **Administrative**، ثم حدد **زوج Cisco-AV** ولصق الدور الذي يحصل عليه المستخدم المسؤول، في هذه الحالة، يتلقى المستخدم امتياز مسؤول كامل (fdm.serrole.authoority.admin). تحديد عند **الإرسال**. كرر هذه الخطوة لكل دور، تم تكوين مستخدم للقراءة فقط كمثال آخر في هذا المستند.


Cisco ISE
Policy · Policy Elements
Dictionaries
Conditions
Results
Authentication
Authorization
Authorization Profiles
Downloadable ACLs
Profiling
Posture
Client Provisioning
Authorization Profiles > New Authorization Profile
Authorization Profile
* Name
FDM_Profile_Admin
Description
* Access Type
ACCESS_ACCEPT
Network Device Profile
Cisco
Service Template
Track Movement
Agentless Posture
Passive Identity Tracking


Advanced Attributes Settings
Radius:Service-Type
=
Administrative
Cisco:cisco-av-pair
=
fdm.userrole.authority.admin

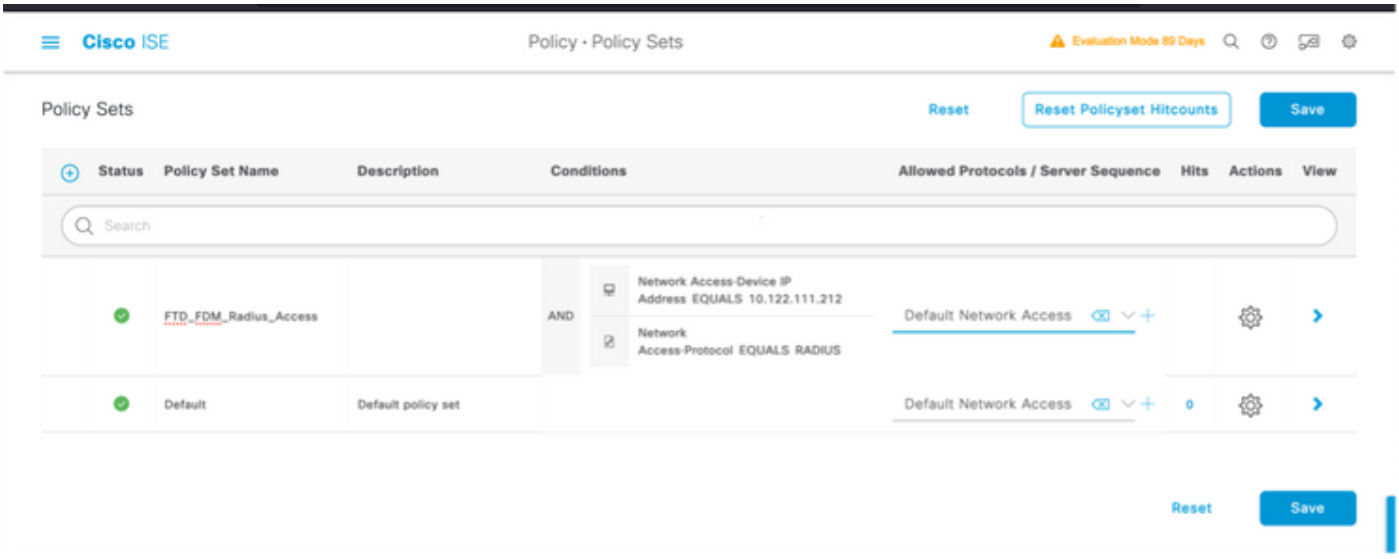

Attributes Details
Access Type = ACCESS_ACCEPT
Service-Type = 6
cisco-av-pair = fdm.userrole.authority.admin



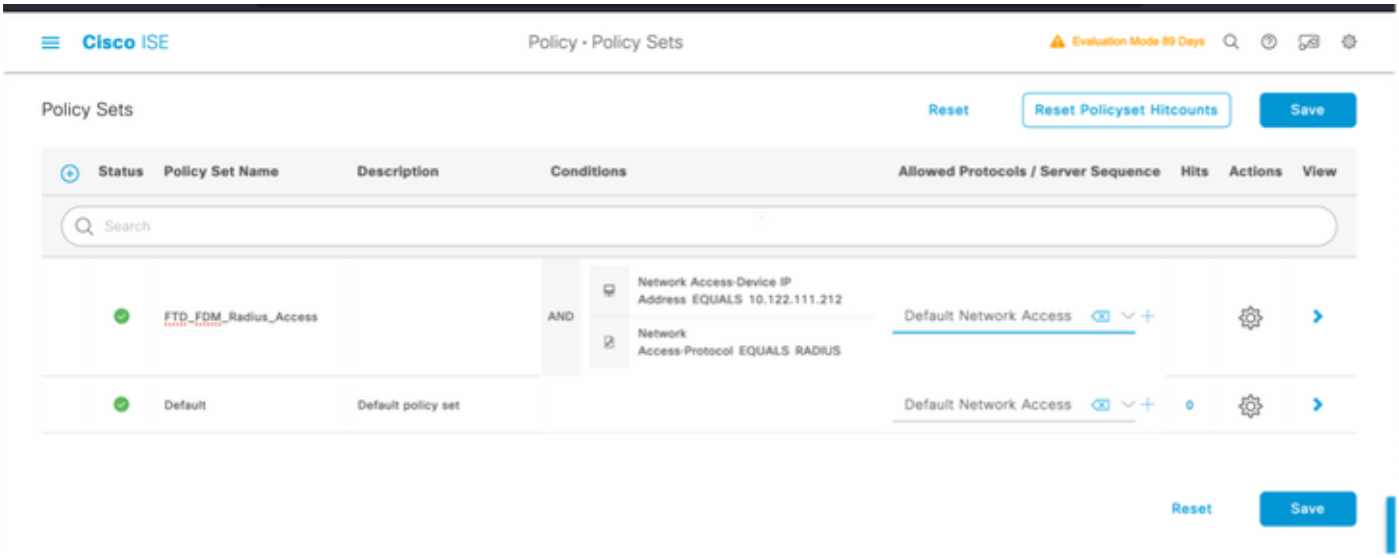
ملاحظة: تأكد من أن ترتيب قسم سمات المتقدم وه مثل مثال الصور لتجنب نتيجة غير متوقعة عند تسجيل الدخول باستخدام GUI و CLI.

الخطوة 8. حدد أيقونة الأسطر الثلاثة وانتقل إلى السياسة > مجموعات السياسات. تحديد **الزر الموجود أسفل عنوان مجموعات النهج، قم بتعريف اسم وحدد على الزر + في** **على المنتصف لإضافة شرط جديد.**

الخطوة 9. تحت إطار الشرط، حدد إضافة سمة ثم حدد على رمز **جهاز الشبكة** متبوعا بعنوان IP لجهاز الوصول إلى الشبكة. حدد **قيمة السمة** وأضف عنوان IP ل FDM. أضف شرطا جديدا وحدد على **الوصول إلى الشبكة** متبوعا بخيار البروتوكول، وحدد على **RADIUS** وحدد عن الاستخدام بمجرد الانتهاء.



الخطوة 10. تحت قسم السماح بالبروتوكولات، حدد **المسؤول الافتراضي للجهاز**. التحديد عند الحفظ



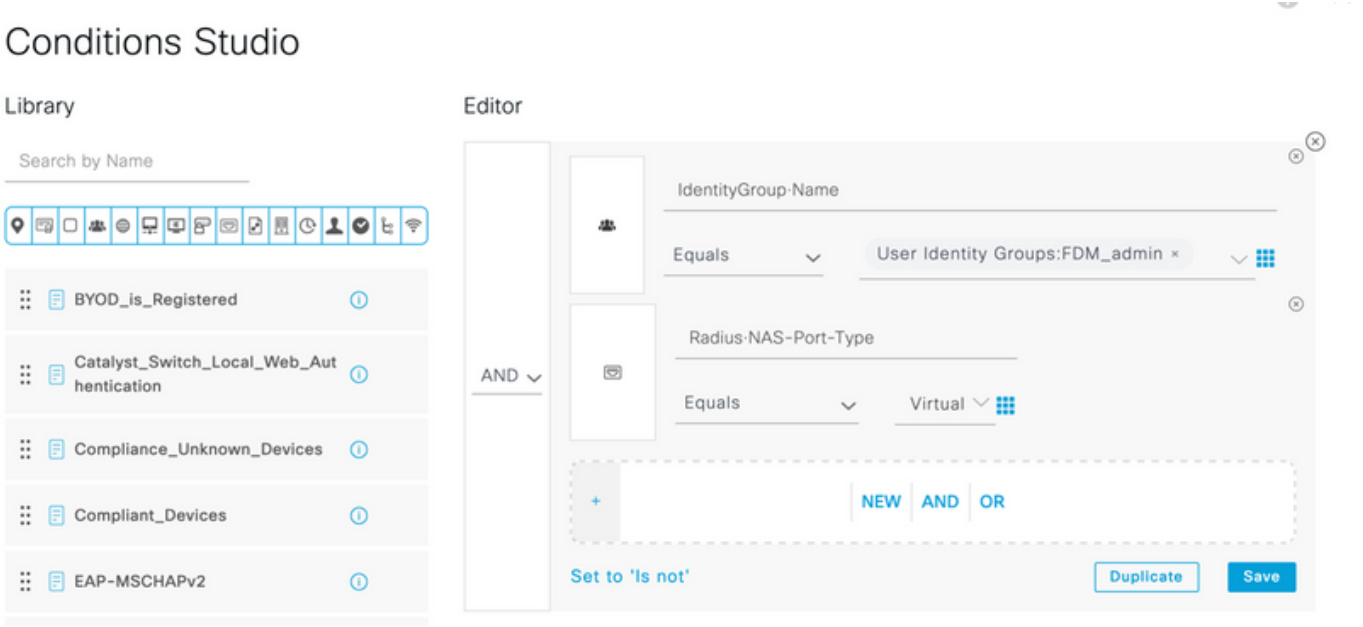
الخطوة 11. تحديد على السهم الأيمن رمز "مجموعة النهج" لتعريف سياسات المصادقة والتفويض

الخطوة 12. تحديد على  موجود أسفل عنوان نهج المصادقة، قم بتحديد اسم وحدد على + في المنتصف لإضافة شرط جديد. تحت إطار الشرط، حدد إضافة سمة ثم حدد على رمز جهاز الشبكة يتبع عنوان IP لجهاز الوصول إلى الشبكة. حدد على قيمة السمة وأضف عنوان IP ل FDM. تحديد عند الاستخدام بمجرد الانتهاء

الخطوة 13. حدد المستخدمين الداخليين كمخزن هوية وحدد على حفظ

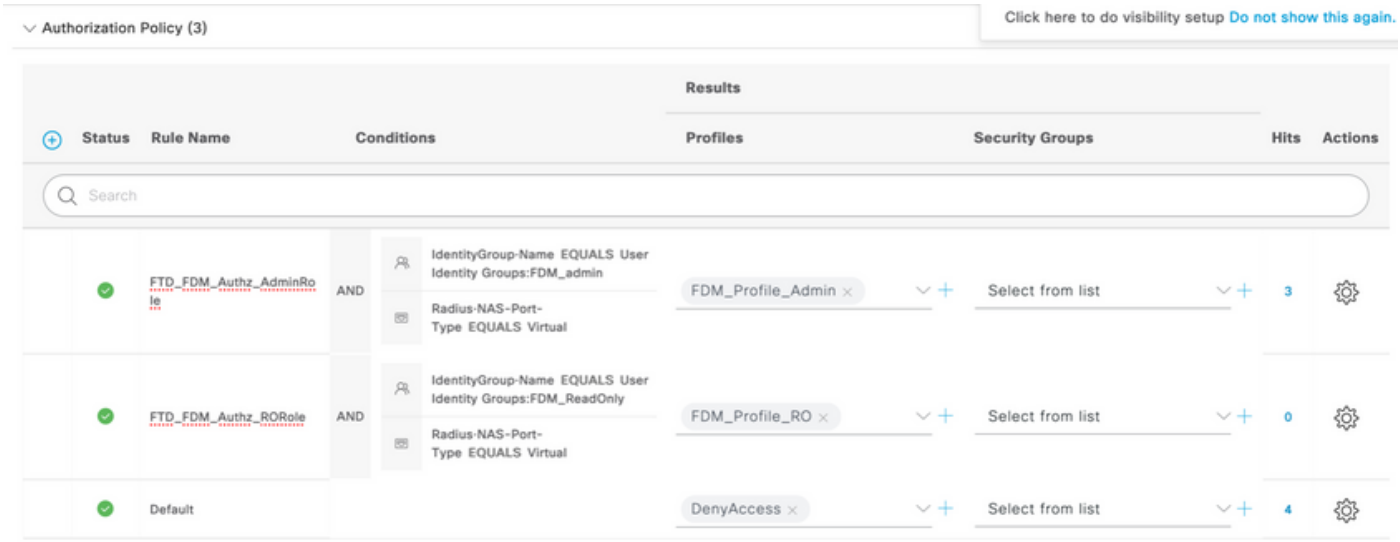
ملاحظة: يمكن تغيير مخزن الهوية إلى مخزن AD في حالة انضمام ISE إلى Active Directory.

الخطوة 14. تحديد على  يوجد أسفل عنوان نهج التخويل، قم بتحديد اسم وحدد في + في المنتصف لإضافة شرط جديد. تحت نافذة الشرط، حدد إضافة سمة ثم حدد على أيقونة مجموعة الهوية متبوعة بمستخدم داخلي:مجموعة هوية. حدد مجموعة FDM_Admin، وحدد AND with NEW لإضافة شرط جديد، ثم حدد على أيقونة المنفذ يتبعها رمز RADIUS NAS-Port-type:Virtual وحدد عند الاستخدام.



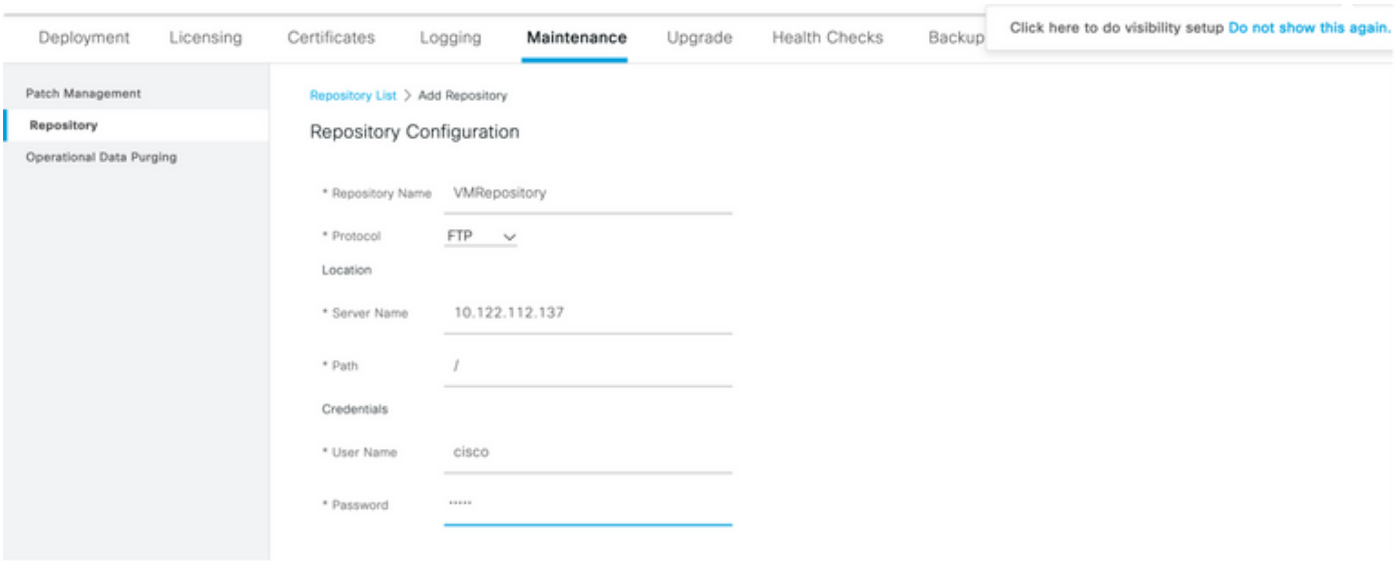
الخطوة 15. تحت التوصيفات، حدد التوصيف الذي تم إنشاؤه في الخطوة 6 ثم حدد عند الحفظ

كرر الخطوة 14 و 15 لمجموعة FDM_ReadOnly



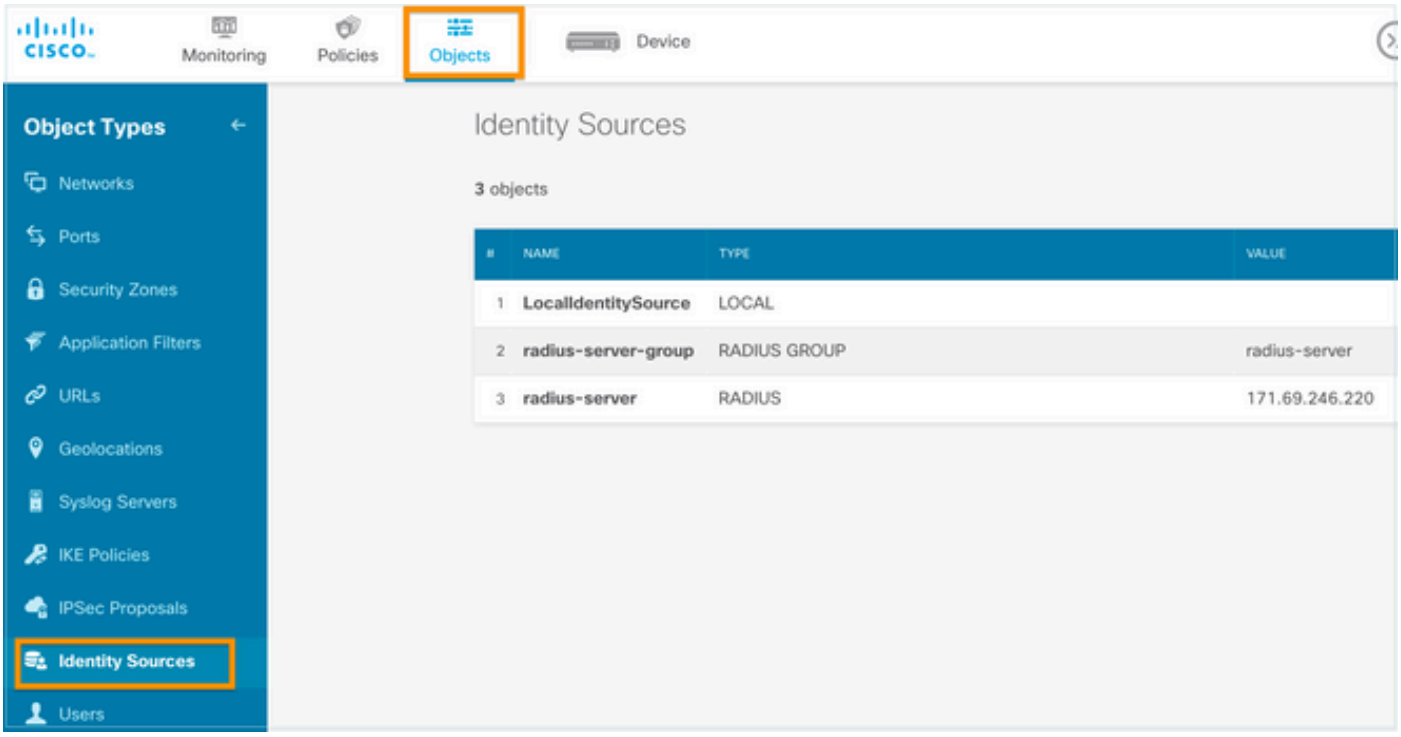
الخطوة 16 (اختيارية). انتقل إلى أيقونة ثلاثة أسطر موجودة في الركن العلوي الأيسر وحدد على إدارة > نظام > صيانة > مستودع وحدد على +إضافة لإضافة مستودع يستخدم لتخزين ملف تفريغ TCP لأغراض استكشاف الأخطاء وإصلاحها.

الخطوة 17 (اختيارية). قم بتعريف اسم المستودع والبروتوكول واسم الخادم والمسار وبيانات الاعتماد. حدد عند الإرسال بمجرد الانتهاء.

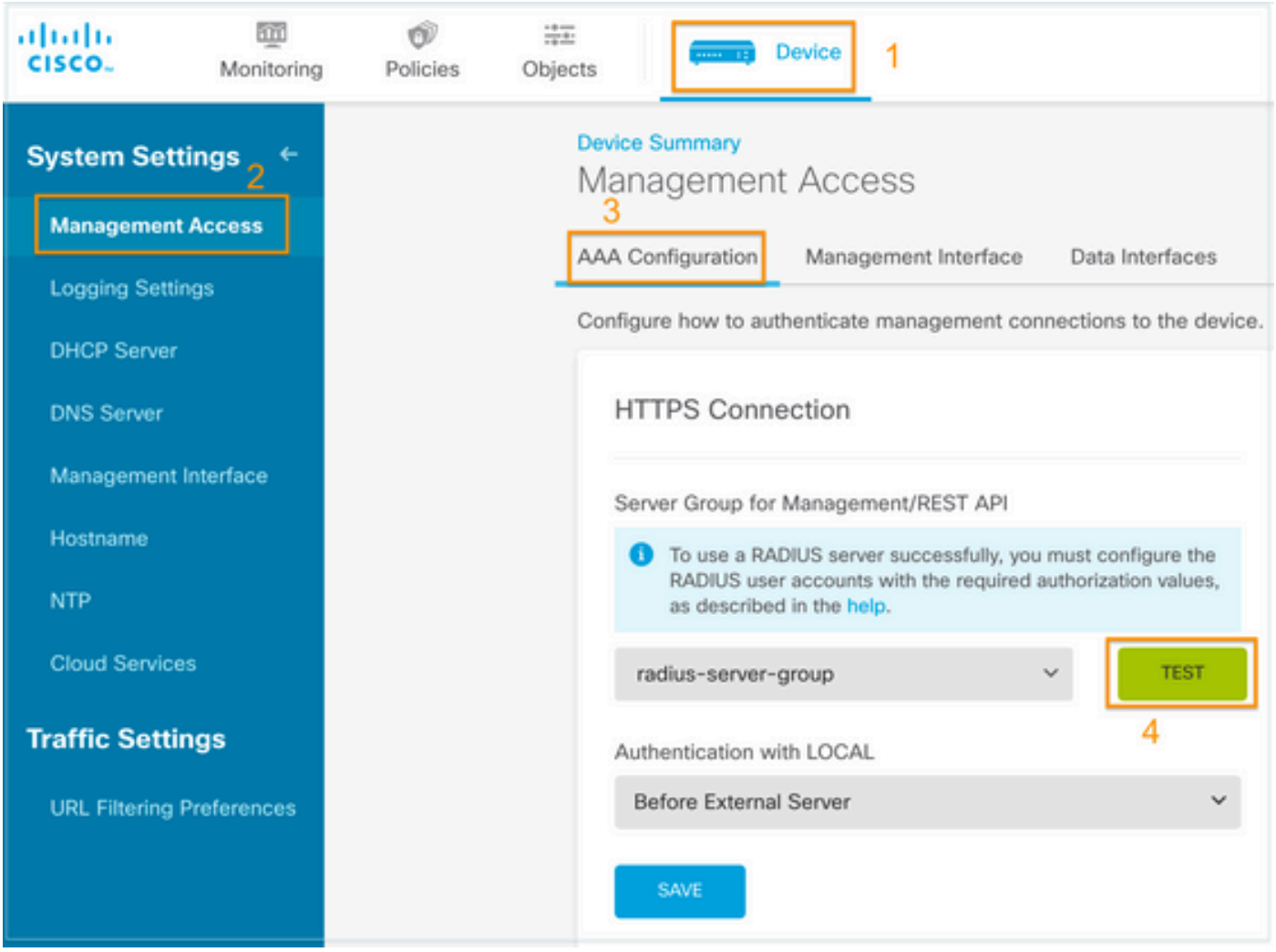


التحقق من الصحة

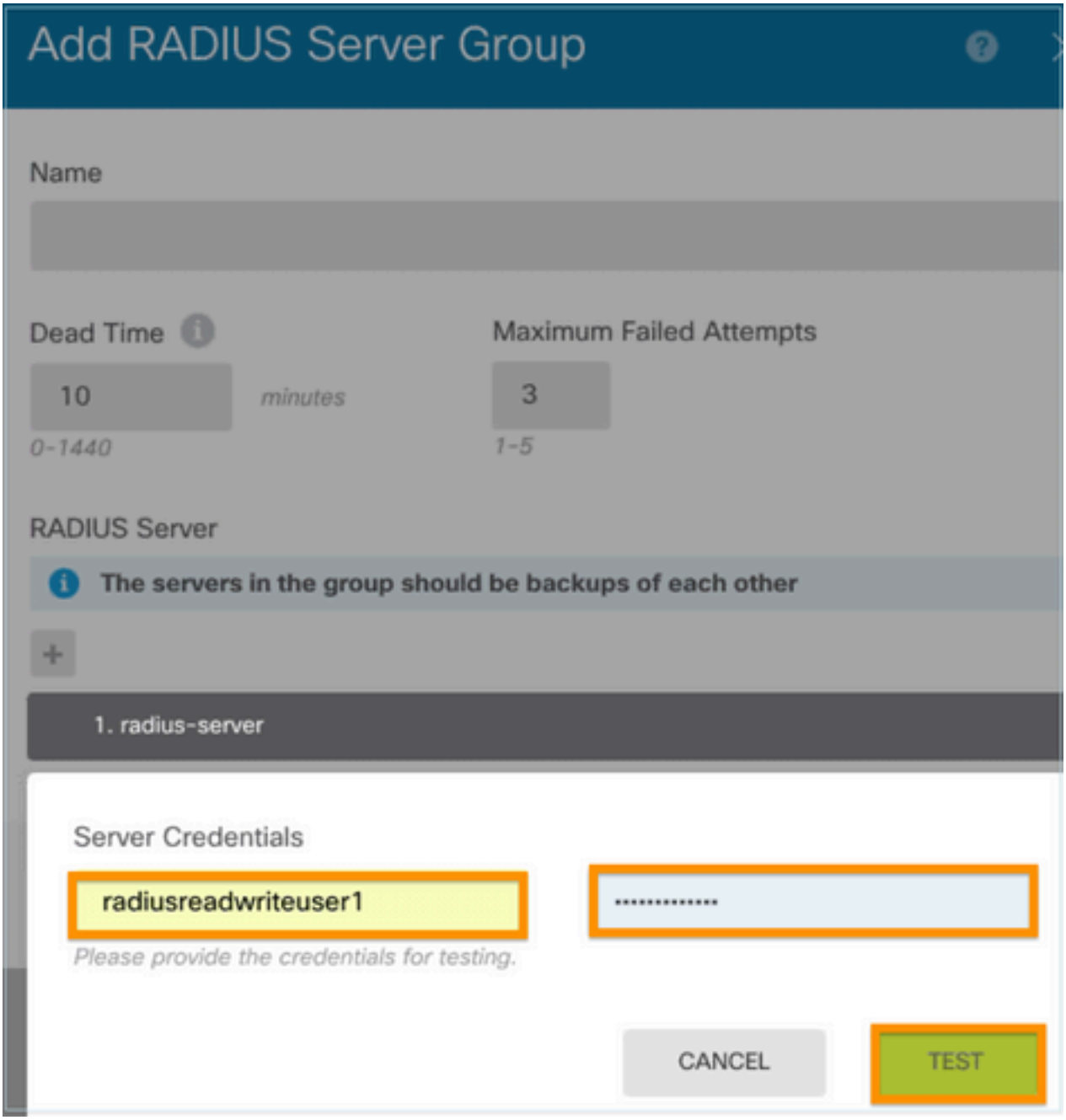
الخطوة 1. انتقل إلى الكائنات > عالمة التبويب مصادر الهوية وتحقق من تكوين خادم RADIUS وخادم المجموعة



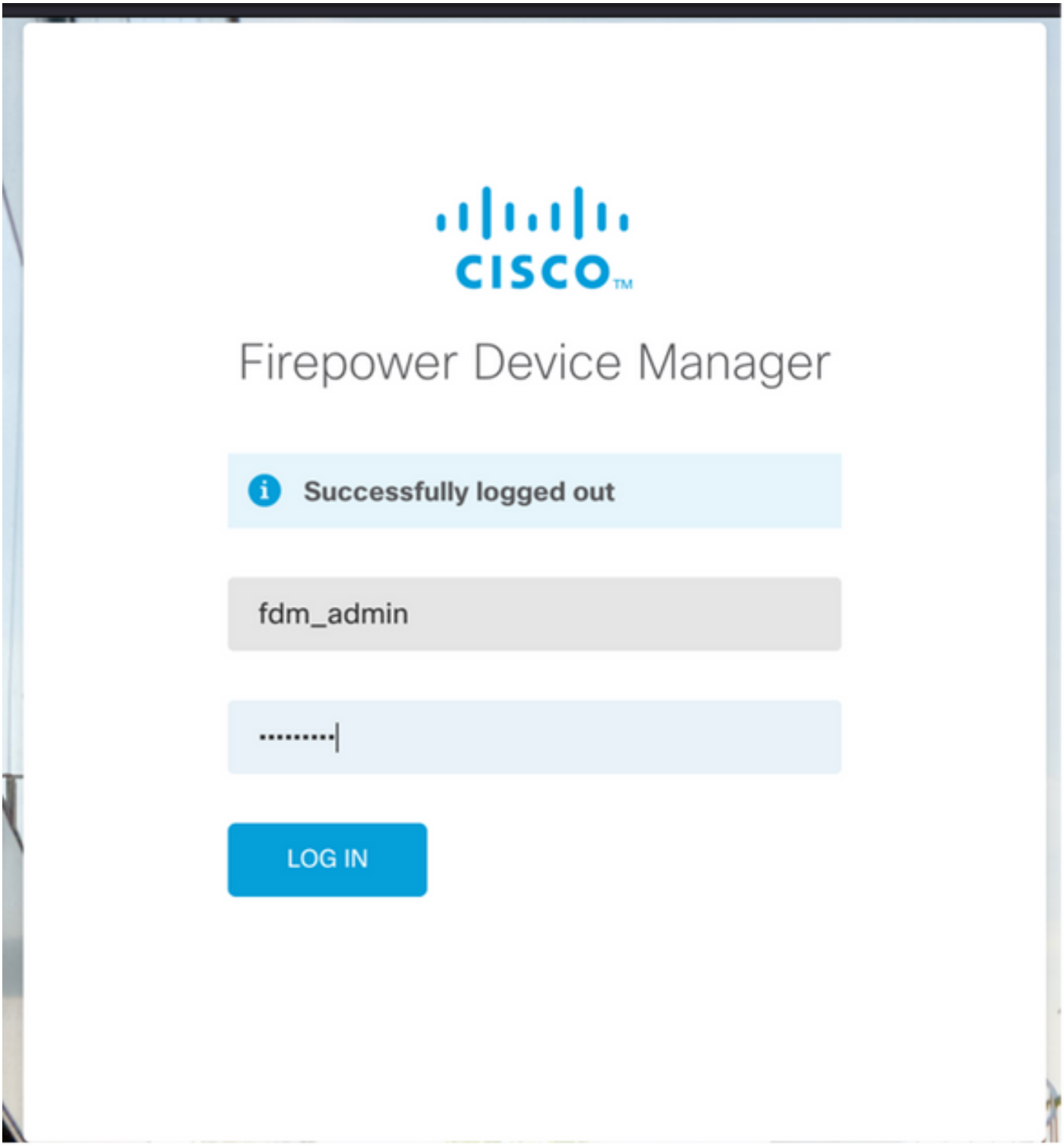
الخطوة 2. انتقل إلى الجهاز > إعدادات النظام > عالمة التبويب الوصول إلى الإدارة وحدد زر الاختبار



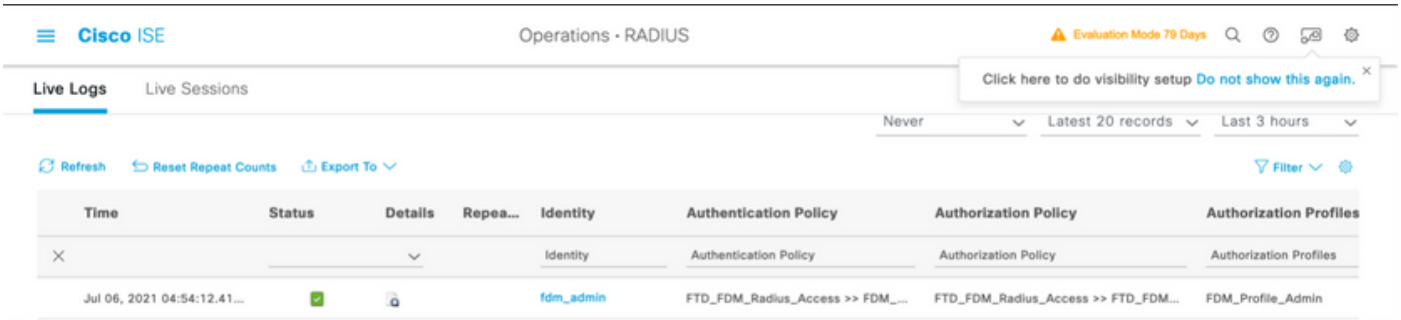
الخطوة 3. قم بإدراج بيانات اعتماد المستخدم وحدد زر الاختبار



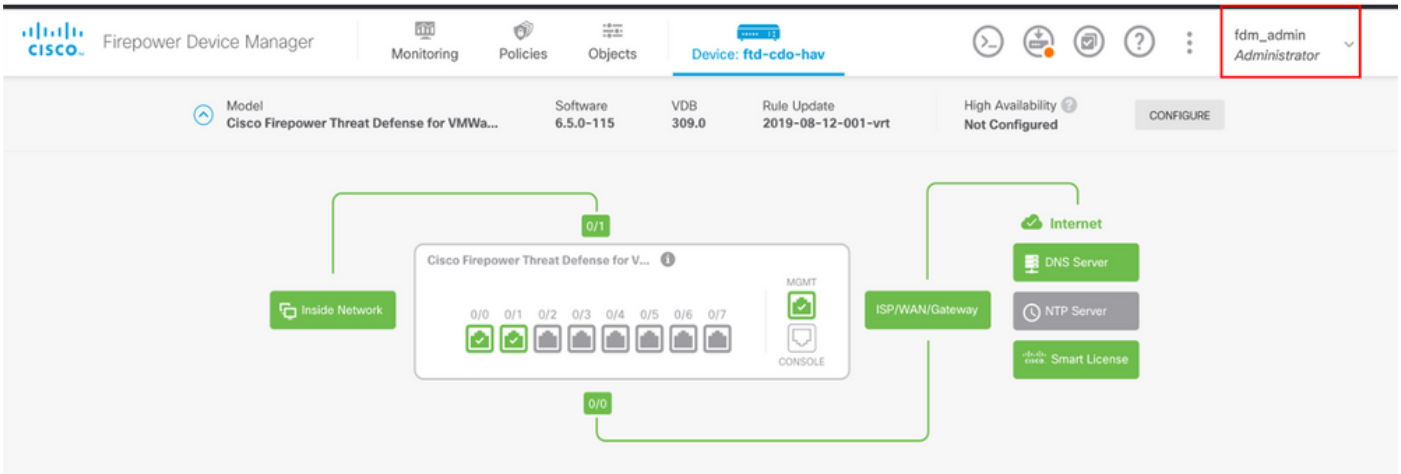
الخطوة 4. افتح مستعرض نافذة جديد واكتب https://fdm_ip_address، واستخدم اسم مستخدم fdm_admin وكلمة المرور التي تم إنشاؤها في الخطوة 5 ضمن قسم تكوين ISE.



يمكن التحقق من محاولة تسجيل الدخول الناجحة على سجلات ISE RADIUS المباشرة



يمكن أيضا مراجعة مستخدم المسؤول على FDM في الركن العلوي الأيمن



Cisco Firepower Device Manager CLI (مستخدم مسؤول)

```
ECANOGUT-M-D4N7:~ ecanogut$ ssh fdm_admin@10.122.111.212
The authenticity of host '10.122.111.212 (10.122.111.212)' can't be established.
ECDSA key fingerprint is SHA256:sqpyFmCcGBslEjjDMdHnrkqdw40qvc7ne1I+Pjw6fJs.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.122.111.212' (ECDSA) to the list of known hosts.
Password:
!!! New external username identified. Please log in again to start a session. !!
!

Copyright 2004-2019, Cisco and/or its affiliates. All rights reserved.
Cisco is a registered trademark of Cisco Systems, Inc.
All other trademarks are property of their respective owners.

Cisco Fire Linux OS v6.5.0 (build 4)
Cisco Firepower Threat Defense for VMWare v6.5.0 (build 115)

Connection to 10.122.111.212 closed.
```

```
ECANOGUT-M-D4N7:~ ecanogut$ ssh fdm_admin@10.122.111.212
Password:
Last login: Tue Jul  6 17:01:20 UTC 2021 from 10.24.242.133 on pts/0

Copyright 2004-2019, Cisco and/or its affiliates. All rights reserved.
Cisco is a registered trademark of Cisco Systems, Inc.
All other trademarks are property of their respective owners.

Cisco Fire Linux OS v6.5.0 (build 4)
Cisco Firepower Threat Defense for VMWare v6.5.0 (build 115)

>
```

استكشاف الأخطاء وإصلاحها

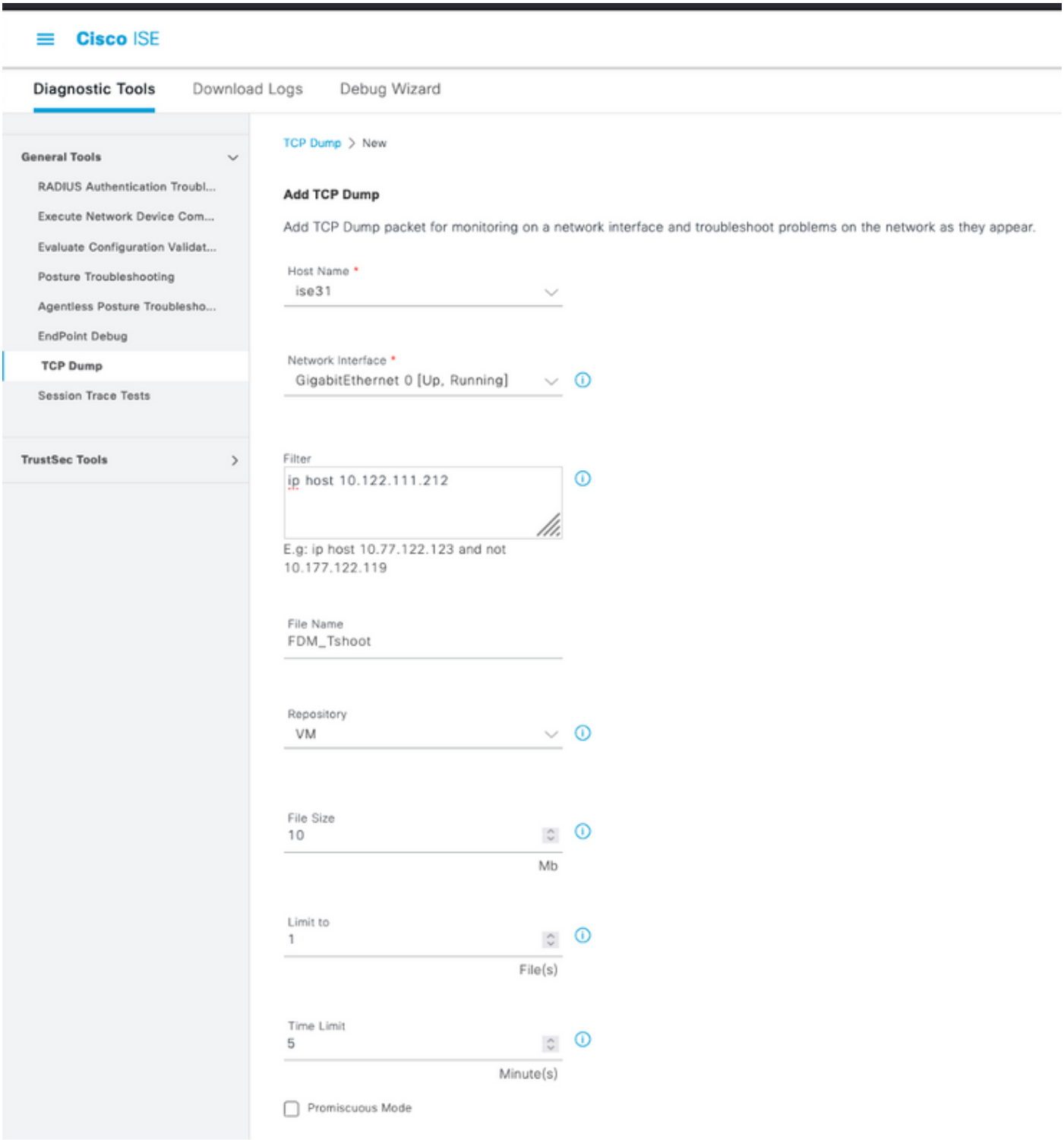
يوفر هذا القسم المعلومات التي يمكنك إستخدامها لاستكشاف أخطاء التكوين وإصلاحها.

التحقق من الاتصال باستخدام أداة تفريغ TCP على ISE

الخطوة 1. قم بتسجيل الدخول إلى ISE وحدد أيقونة الخطوط الثلاثة الموجودة في الزاوية

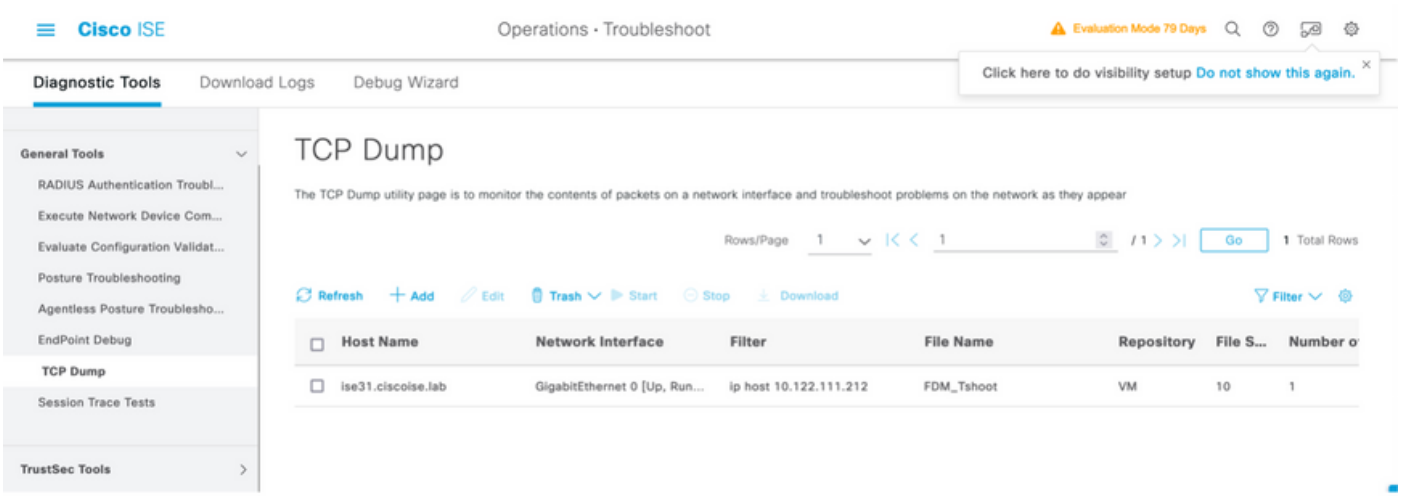
العلوية اليسرى وانتقل إلى **العمليات > أستكشاف الأخطاء وإصلاحها > أدوات التشخيص.**

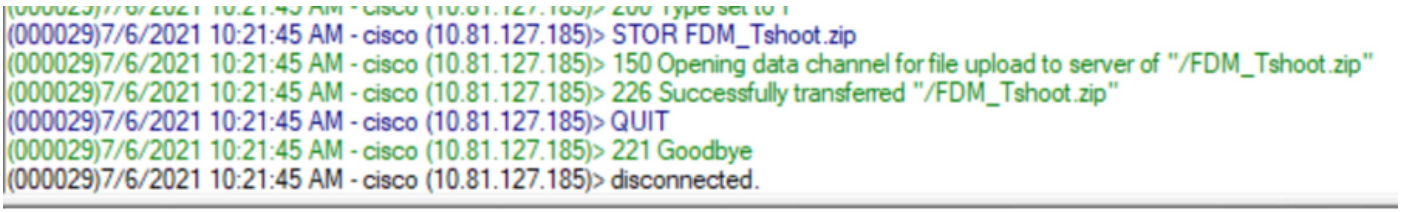
الخطوة 2. تحت أدوات عامة، حدد علي مكبات TCP ثم حدد علي **Add+**. حدد اسم المضيف واسم ملف واجهة الشبكة والمستودع وعامل تصفية إختياري لتجميع تدفق إتصالات عنوان IP فقط FDM. تحديد عند **الحفظ والتشغيل**

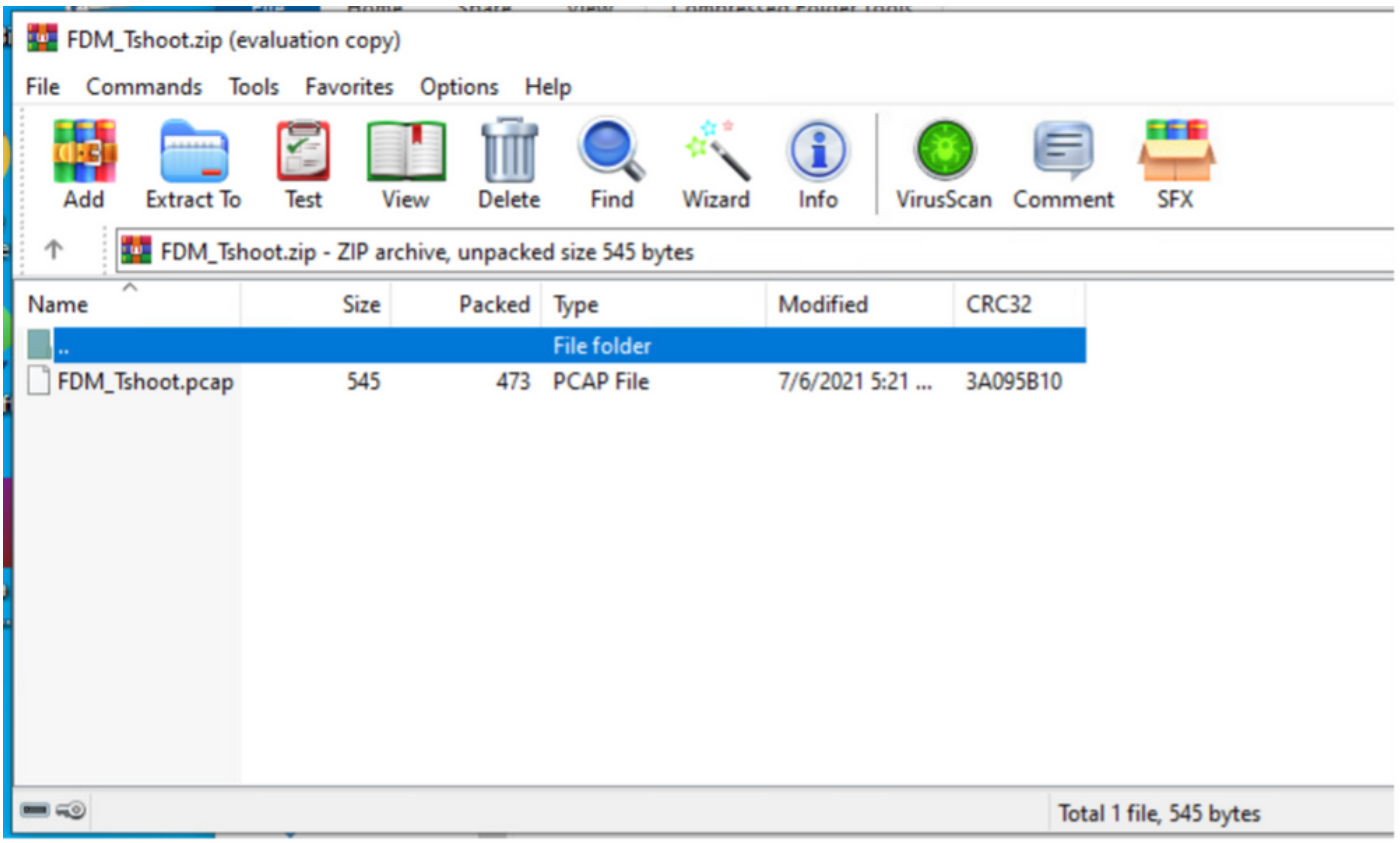


الخطوة 3. قم بتسجيل الدخول إلى واجهة مستخدم FDM واكتب بيانات اعتماد المسؤول.

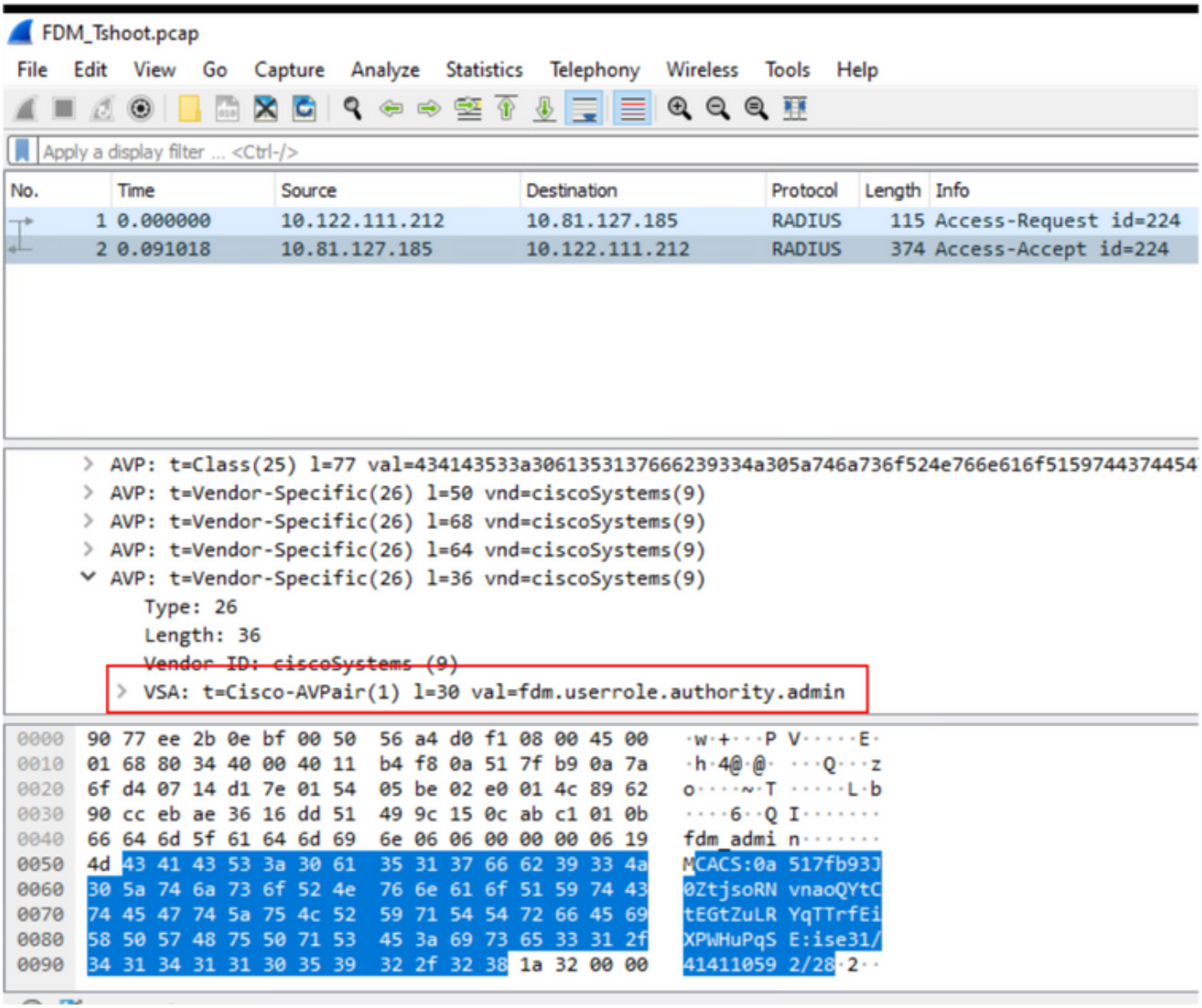
الخطوة 4. على ISE، حدد علي زر **إيقاف** وتأكد من أن ملف PCAP قد تم إرساله إلى المستودع المحدد.







الخطوة 5. افتح ملف PCAP للتحقق من الاتصال الناجح بين FDM و ISE.



إذا لم تظهر أي مدخلات على ملف PCAP، تحقق من الخيارات التالية:

1. تمت إضافة عنوان ISE IP الأيمن على تكوين FDM
2. في حالة وجود جدار حماية في منفذ التحقق الأوسط، يتم السماح بمنفذ 1812-1813.
3. التحقق من الاتصال بين ISE و FDM

التحقق من الاتصال باستخدام الملف الذي تم إنشاؤه بواسطة FDM.

في ملف أستكشاف الأخطاء وإصلاحه الذي تم إنشاؤه من صفحة جهاز FDM، ابحث عن الكلمات الأساسية:

- FDMpasswordLoginHelper
- NGFWDefaultUserMgmt
- AAAIdentitySourceStatusManager
- RadiusIdentitySourceManager

يمكن العثور على جميع السجلات المتعلقة بهذه الميزة في /var/log/cisco/ngfw-onbox.log

المراجع:

https://www.cisco.com/c/en/us/td/docs/security/firepower/640/fdm/fptd-fdm-config-guide-640/fptd-fdm-mgmt.html#id_73793

المشكلات الشائعة

الحالة 1 - المصادقة الخارجية لا تعمل

- تحقق من SecretKey أو المنفذ أو اسم المضيف
- تكوين خاطئ لـ AVPs على RADIUS
- يمكن أن يكون الخادم في "الوقت الميت"

الحالة 2 -Test IdentitySource يفشل

- تأكد من حفظ التغييرات على الكائن
- تأكد من صحة بيانات الاعتماد

القيود

- يسمح FDM بحد أقصى من 5 جلسات عمل نشطة لـ FDM.
- تم إبطال إنشاء جلسة العمل السادسة في الجلسة الأولى
- لا يمكن أن يكون اسم RadiusIdentitySourceGroup هو "LocalIdentitySource"
- الحد الأقصى لـ 16 RadiusIdentitySources إلى RadiusIdentitySourceGroup
- يؤدي التكوين الخاطئ لـ AVPs على RADIUS إلى رفض الوصول إلى FDM

أسئلة وأجوبة

س: هل تعمل هذه الميزة في وضع التقييم؟

نعم

س: إذا قام مستخدمان للقراءة فقط بتسجيل الدخول، حيث يكون لهما حق الوصول إلى المستخدم 1 للقراءة فقط، ويسجلان الدخول من مستعرضين مختلفين. كيف ستظهر؟ ماذا سيحدث؟

أ: يتم عرض جلستي عمل لكل من المستخدمين في صفحة جلسات عمل المستخدم النشطة التي تحمل نفس الاسم. كل مدخل يظهر قيمة منفردة لختم الوقت.

س: السلوك هو أن خادم RADIUS الخارجي يرفض الوصول مقابل "الـ إستجابة" إذا كان لديك مصادقة محلية تم تكوينها في المرة الثانية؟

أ: يمكنك تجربة المصادقة المحلية حتى إذا تم رفض الوصول أو لم يتم الرد إذا كنت لديك مصادقة محلية تم تكوينها الثانية.

س: كيف يفرق ISE بين طلب RADIUS لتسجيل دخول المسؤول مقابل طلب RADIUS لمصادقة مستخدم RA VPN

A: الـ يفرق ISE بين طلب RADIUS لمستخدمي Admin مقابل RAPN. تحث FDM في سمة Cisco-avpair للبحث عن تفويض وصول المسؤول. يرسل ISE كل السمات التي تم تكوينها للمستخدم في كلا الحالتين.

q: يعني ذلك أنه لا يمكن لسجلات ISE التمييز بين سجل مسؤول FDM وإدخال نفس المستخدم إلى شبكة VPN للوصول عن بعد على الجهاز نفسه. هل هناك أي سمة RADIUS تم تمريرها إلى ISE في طلب الوصول الذي يمكن ISE وضع المفتاح عليه؟

أ: فيما يلي سمات RADIUS للتدفق التي يتم إرسالها من FTD إلى ISE أثناء مصادقة RADIUS ل RAPN. الذي يتم إرساله هذه العناصر كجزء من طلب الوصول إلى إدارة المصادقة الخارجية ويمكن إستخدامها للتمييز بين سجل إدارة FDM في سجل دخول مستخدم VS RAPN.

146 - اسم مجموعة النفق أو اسم ملف تعريف الاتصال.

150 - نوع العميل (القيم القابلة للتطبيق: 2 = AnyConnect Client SSL VPN، 6 = AnyConnect Client IPsec VPN (IKEv2).

151 - نوع جلسة العمل (القيم القابلة للتطبيق: 1 = AnyConnect Client SSL VPN، 2 = AnyConnect Client IPSec VPN (IKEv2).

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).