نظام التشغيل القابل للتشغيل (FXOS) Firepower 2.2: مصادقة الهيكل والتفويض للإدارة عن بعد باستخدام TACACS+.

المحتويات

المقدمة

يوضح هذا المستند كيفية تكوين مصادقة TACACS+ والتفويض لهيكل نظام التشغيل القابل للتشغيل ((FXOS Firepower عبر خادم التحكم في الوصول (ACS).

يتضمن هيكل FXOS أدوار المستخدم التالية:

- المسؤول - وصول كامل للقراءة والكتابة إلى النظام بالكامل. يتم تعيين هذا الدور بشكل افتراضي لحساب المسؤول الافتراضي ولا يمكن تغييره.
- للقراءة فقط - وصول للقراءة فقط إلى تكوين النظام بدون امتيازات لتعديل حالة النظام.
- العمليات - الوصول للقراءة والكتابة إلى تكوين NTP، والتكوين الذكي ل Call Home للترخيص الذكي، وسجلات النظام، بما في ذلك خوادم syslog والأعطال. قراءة الوصول إلى باقي النظام.
- الوصول إلى المصادقة والتفويض والمحاسبة (AAA) - وصول للقراءة والكتابة إلى المستخدمين والأدوار وتكوين المصادقة والتفويض والمحاسبة (AAA). قراءة الوصول إلى باقي النظام.

يمكن ملاحظة ذلك عبر واجهة سطر الأوامر (CLI) على النحو التالي:

دور العرض security /FPR4120-TAC-A* #

الدور:

اسم الدور Priv

— —

aaa aaa

مسؤول

عمليات العمليات

للقراءة فقط

تمت المساهمة من قبل توني ريميريز، خوسيه سوتو، مهندسي TAC من Cisco.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- معرفة نظام التشغيل FXOS) Firepower Xsible)
- معرفة تكوين ACS

المكونات المستخدمة

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

- جهاز الأمان Cisco Firepower 4120، الإصدار 2.2
- Cisco Access Control Server، الإصدار 5.8.0.32

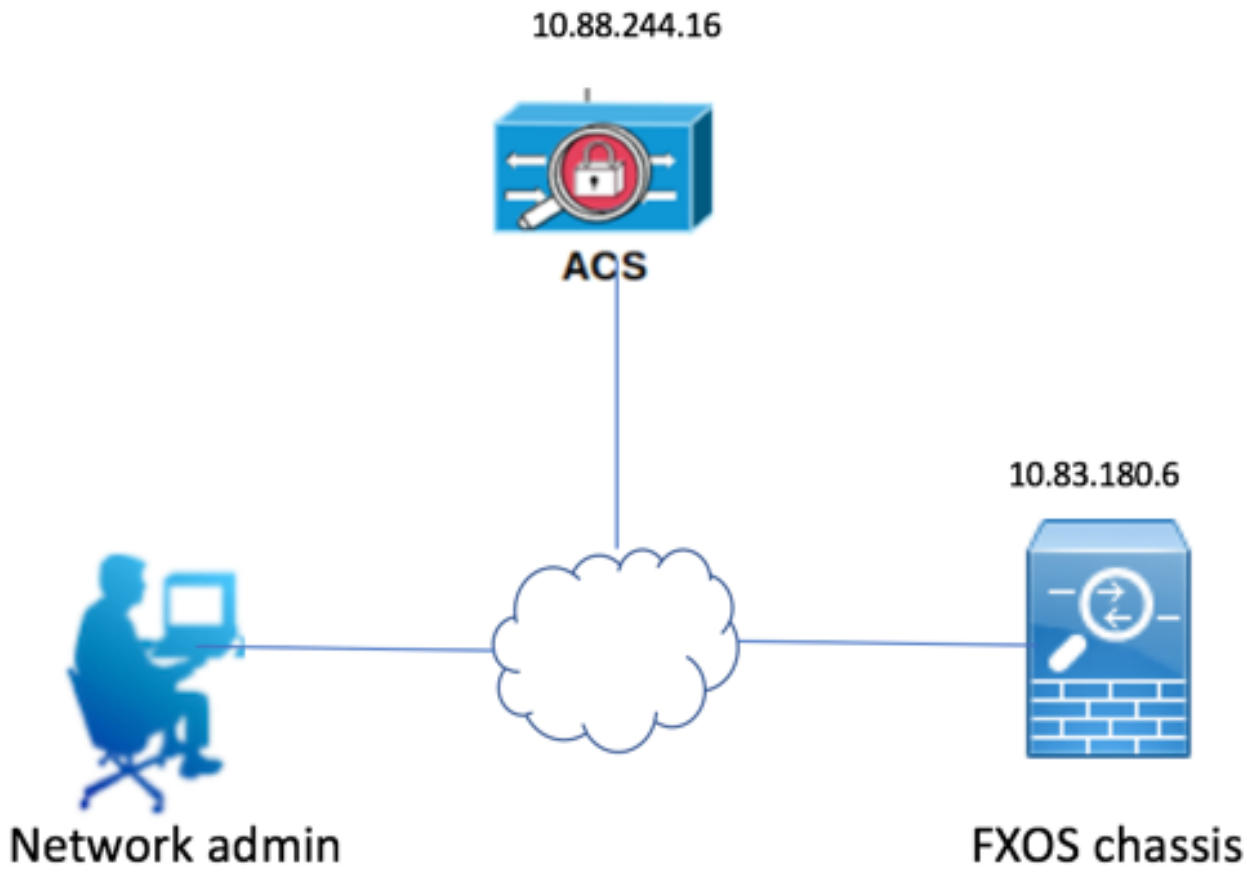
تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

التكوين

الهدف من التكوين هو:

- مصادقة المستخدمين الذين يقومون بتسجيل الدخول إلى واجهة المستخدم الرسومية (GUI) المستندة إلى الويب و SSH باستخدام ACS.
- السماح للمستخدمين بتسجيل الدخول إلى واجهة المستخدم الرسومية (GUI) القائمة على الويب و SSH القائمة على FXOS وفقا لدور المستخدم الخاص بهم من خلال ACS.
- تحقق من التشغيل السليم للمصادقة والتفويض على FXOS بواسطة ACS.

الرسم التخطيطي للشبكة



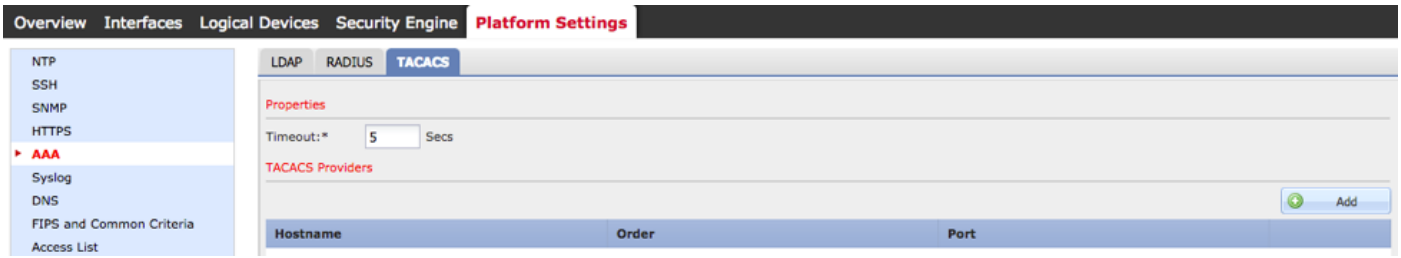
التكوينات

تهيئة هيكل FXOS

إنشاء موفر TACACS باستخدام مدير الهيكل

الخطوة 1. انتقل إلى **إعدادات النظام الأساسي > AAA**.

الخطوة 2. انقر فوق علامة التبويب **TACACS**.

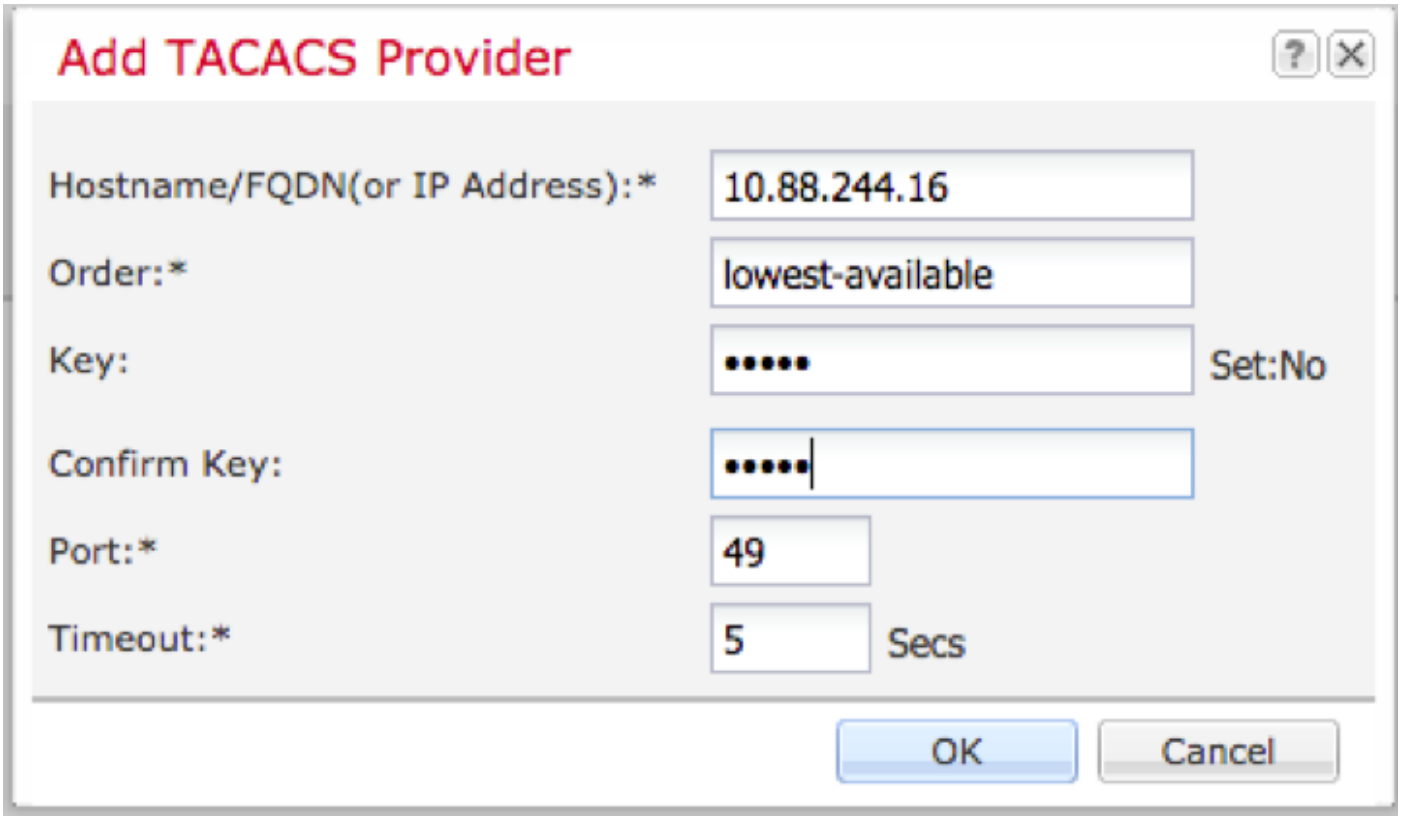


الخطوة 3. لكل موفر TACACS+ تريد إضافته (حتى 16 موفرا).

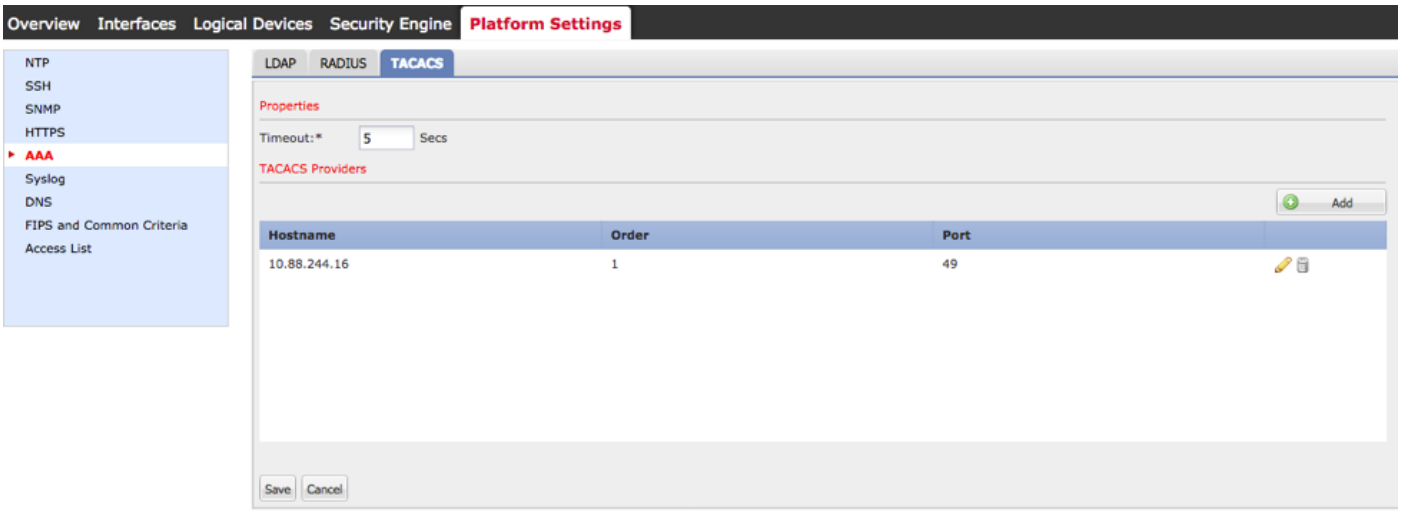
3.1. في منطقة موفري TACACS، انقر فوق **إضافة**.

3.2. في شاشة إضافة مزود TACACS، أدخل القيم المطلوبة.

3.3. انقر فوق **موافق** لإغلاق مربع الحوار إضافة موفر TACACS.

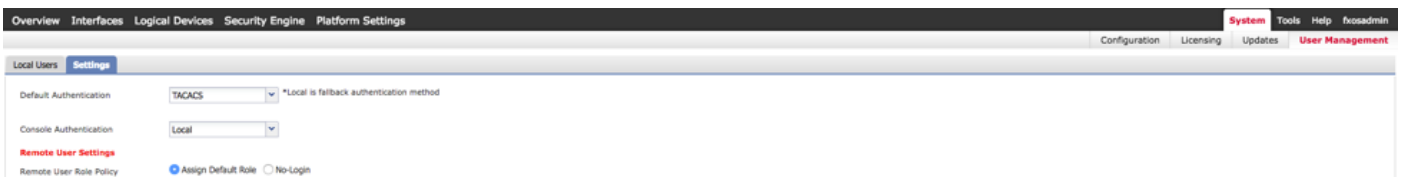


الخطوة 4. طقطقة **حفظ**.



الخطوة 5. انتقل إلى **النظام > إدارة المستخدم > إعدادات**.

الخطوة 6. تحت المصادقة الافتراضية أختر **TACACS**.



إنشاء موفر TACACS+ باستخدام CLI (واجهة سطر الأوامر)

الخطوة 1. لتمكين مصادقة TACACS، قم بتشغيل الأوامر التالية.

أمان **النطاق** #FPR4120-TAC-A

FPR4120-TAC-A /security # **scope default-auth**

FPR4120-TAC-A /security/default-auth # **set domain tacacs**

الخطوة 2. أستخدم الأمر **show detail** لعرض النتائج.

تفاصيل العرض FPR4120-TAC-A /security/default-auth #

المصادقة الافتراضية:

مجال الإدارة: **TACACS**

النطاق التشغيلي: **TACACS**

فترة تحديث جلسة ويب (بالثواني): 600

مهلة جلسة العمل (بالثواني) للويب و ssh و telnet جلسات: 600

مهلة جلسة العمل المطلقة (بالثواني) للويب و SSH و telnet جلسات: 3600

مهلة جلسة عمل وحدة التحكم التسلسلية (بالثواني): 600

مهلة الجلسة المطلقة لوحدة التحكم التسلسلية (بالثواني): 3600

مجموعة خوادم مصادقة المسؤول:

مجموعة خوادم المصادقة التشغيلية:

إستخدام العامل الثاني: لا

الخطوة 3. تقوم معلمات خادم TACACS بتشغيل الأوامر التالية.

أمان **النطاق** FPR4120-TAC-A#

FPR4120-TAC-A /security # **scope tacacs**

FPR4120-TAC-A /security/tacacs # **أدخل الخادم 10.88.244.50**

FPR4120-TAC-A /security/tacacs/server # **مجموعة إدارة "خادم ACS"**

FPR4120-TAC-A /security/tacacs/server* # **مفتاح المجموعة**

أدخل المفتاح: *****

تأكيد المفتاح: *****

الخطوة 4. أستخدم الأمر **show detail** لعرض النتائج.

FPR4120-TAC-A /security/tacacs/server* # **تفاصيل العرض**

خادم TACACS+:

اسم المضيف أو FQDN أو عنوان IP: 10.88.244.50

إدارة الحقوق:

الطلب: 1

المنفذ: 49

المفتاح: ***

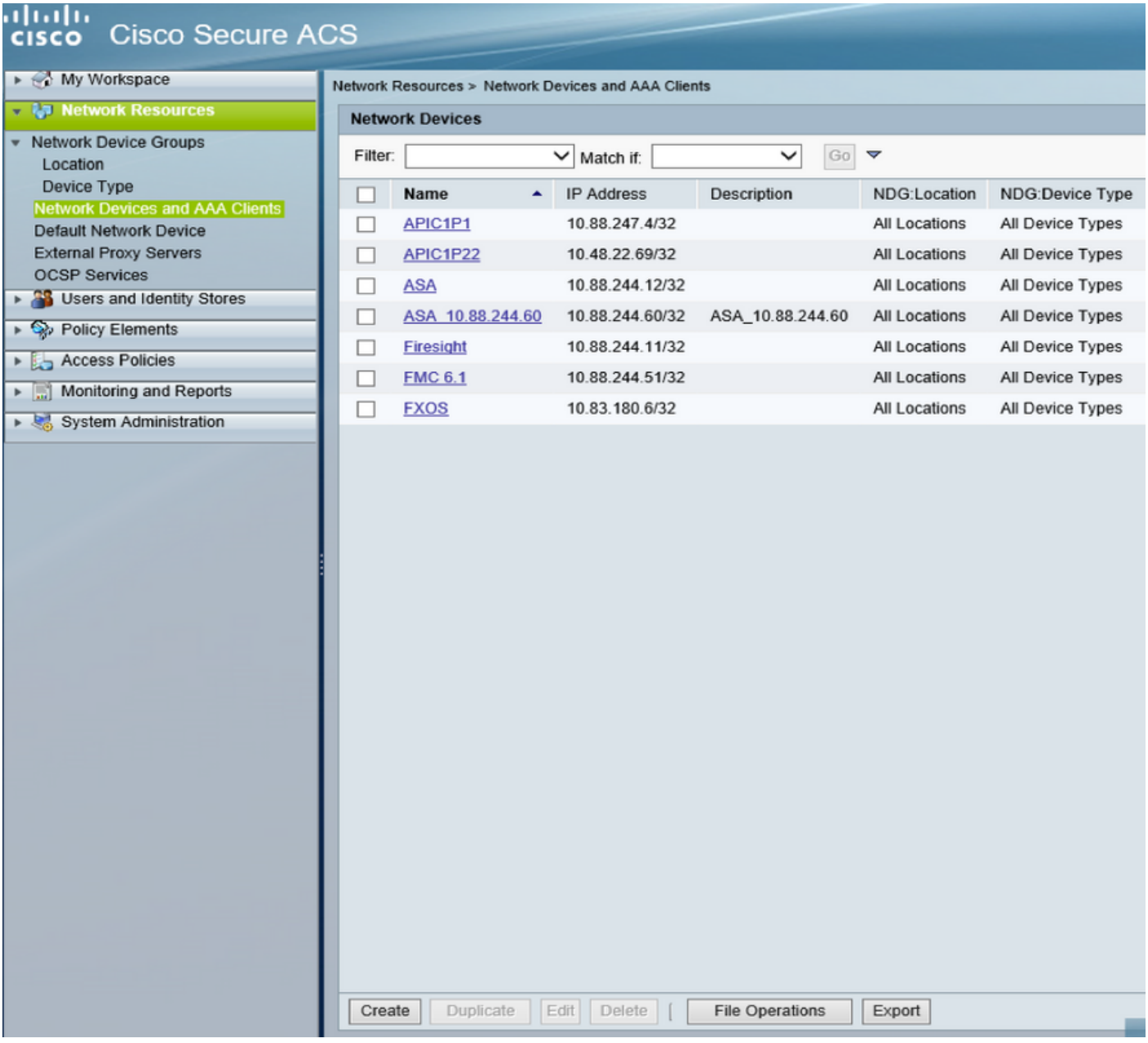
المهلة: 5

تكوين خادم ACS

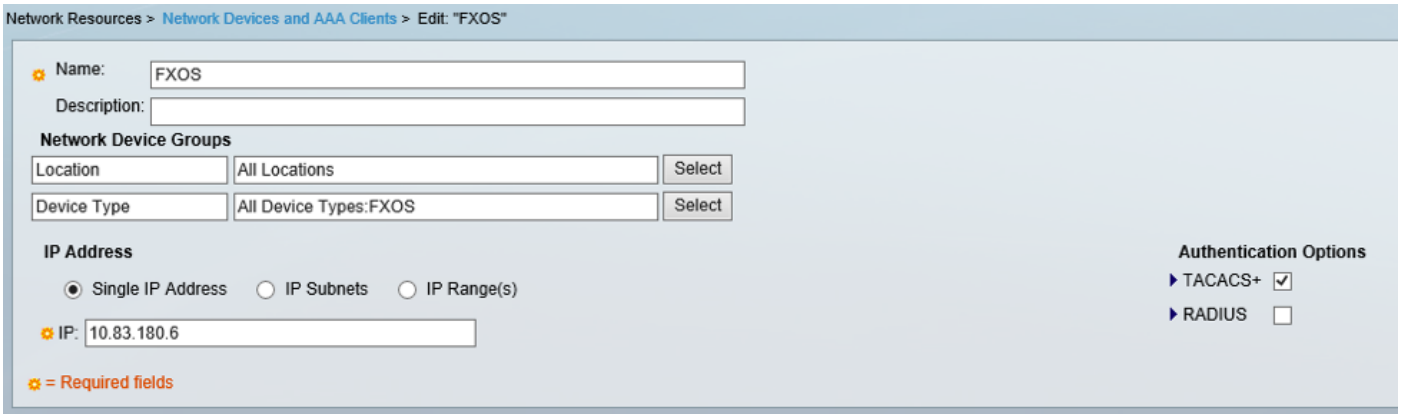
إضافة FXOS كمورد شبكة

الخطوة 1. انتقل إلى **موارد الشبكة > أجهزة الشبكة وعملاء AAA**.

الخطوة 2. انقر فوق **إنشاء**.



الخطوة 3. أدخل القيم المطلوبة (الاسم وعنوان IP ونوع الجهاز وتمكين TACACS+ وإضافة المفتاح).



الخطوة 4. انقر على **إرسال**.

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).