ASA 8.3: مداخت‌سا‌ب ةقداصم TACACS ACS 5.x

المحتويات

المقدمة

يقدم هذا المستند معلومات حول كيفية تكوين جهاز الأمان لمصادقة المستخدمين للوصول إلى الشبكة.

المتطلبات الأساسية

المتطلبات

يفترض هذا المستند أن جهاز الأمان القابل للتكيف (ASA) قيد التشغيل الكامل وتم تكوينه للسماح لمدير أجهزة الأمان المعدلة (ASDM) أو CLI من Cisco بإجراء تغييرات التكوين.

ملاحظة: راجع السماح بوصول HTTPS لـ ASDM للحصول على مزيد من المعلومات حول كيفية السماح بتكوين الجهاز عن بعد بواسطة ASDM.

المكونات المستخدمة

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

- برنامج أجهزة الأمان المعدلة Cisco Adaptive Security Appliance، الإصدار 8.3 والإصدارات الأحدث
- Cisco Adaptive Security Device Manager، الإصدار 6.3 والإصدارات الأحدث
- خادم التحكم في الوصول الآمن x.5 من Cisco

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.

الاصطلاحات

راجع اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.

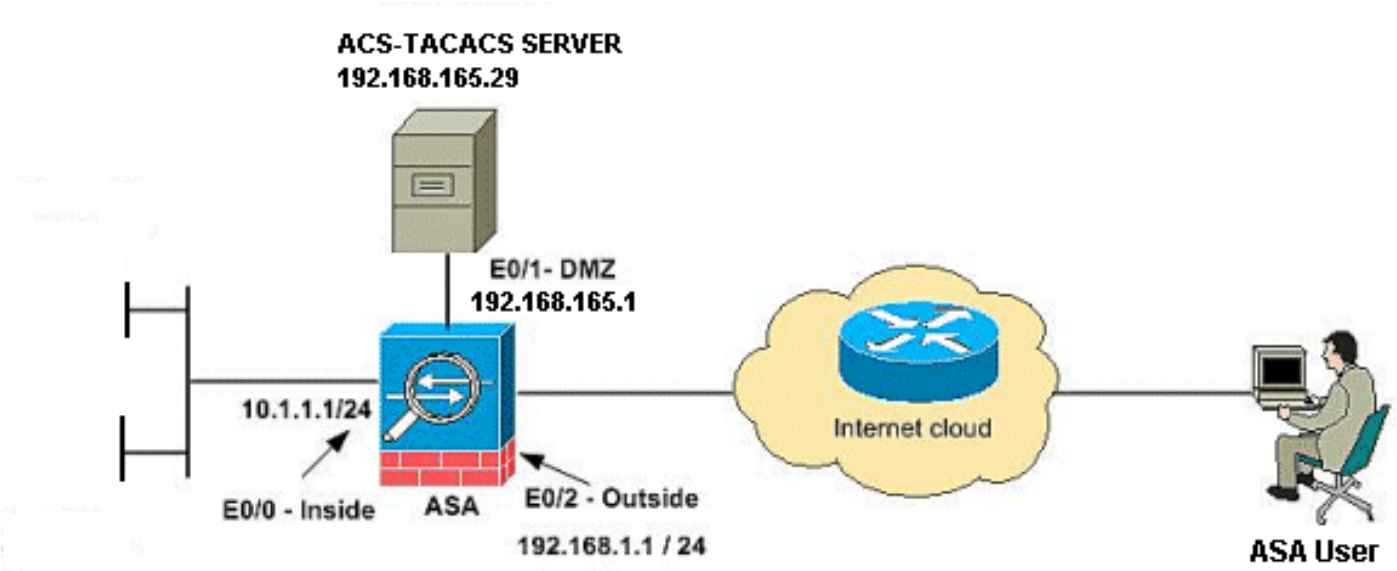
التكوين

في هذا القسم، تُقدّم لك معلومات تكوين الميزات الموضحة في هذا المستند.

ملاحظة: أستخدم أداة بحث الأوامر (للعملاء المسجلين فقط) للحصول على مزيد من المعلومات حول الأوامر المستخدمة في هذا القسم.

الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة التالي:



ملاحظة: ال ip ليس يخاطب خطة يستعمل في هذا تشكيل قانونيا routable على الإنترنت. هم rfc 1918 عنوان أي كان استعملت في مختبر بيئة.

تكوين ASA للمصادقة من خادم ACS باستخدام CLI (واجهة سطر الأوامر)

أنجزت هذا تشكيل ل ال ASA أن يصدق من ال ACS نادل:

```
configuring the ASA for TACACS server ASA(config)# aaa-server cisco protocol tacacs+ ---!
ASA(config-aaa-server-group)# exit !--- Define the host and the interface the ACS server is on.
ASA(config)# aaa-server cisco (DMZ) host 192.168.165.29 ASA(config-aaa-server-host)# key cisco
!--- Configuring the ASA for HTTP and SSH access using ACS and fallback method as LOCAL
authentication. ASA(config)#aaa authentication ssh console cisco LOCAL ASA(config)#aaa
authentication http console cisco LOCAL
```

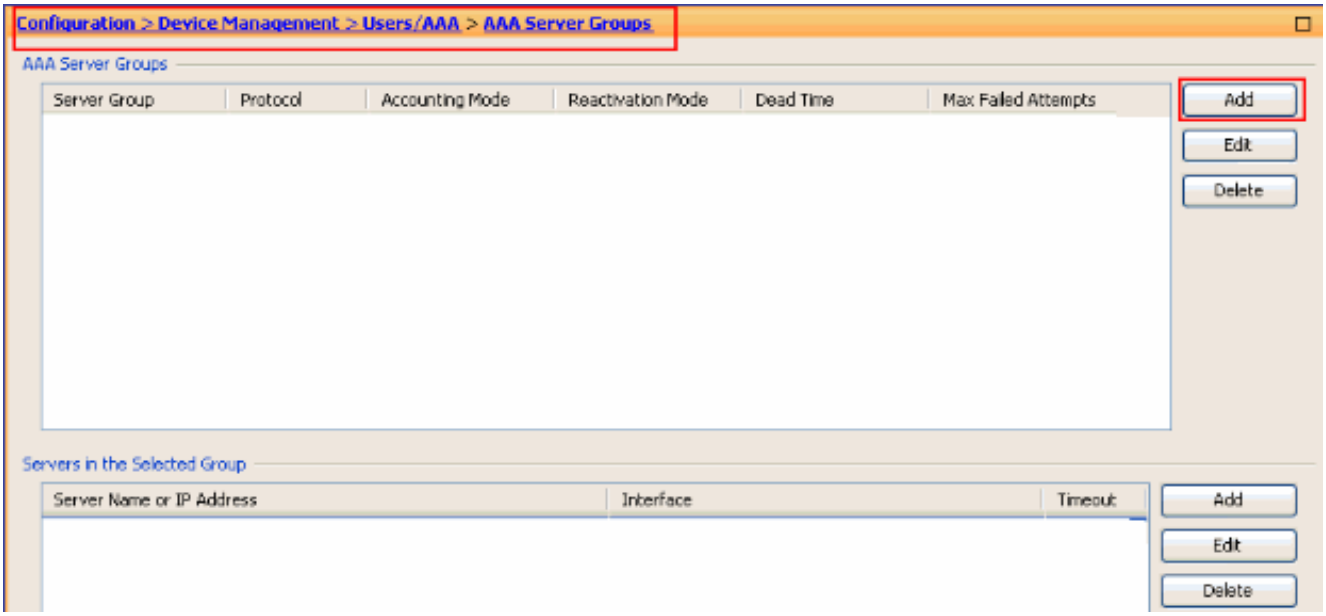
ملاحظة: قم بإنشاء مستخدم محلي على ASA باستخدام الأمر username cisco password cisco privilege 15 للوصول إلى ASDM باستخدام المصادقة المحلية عندما لا يكون ACS متوفرا.

تكوين ASA للمصادقة من خادم ACS باستخدام ASDM

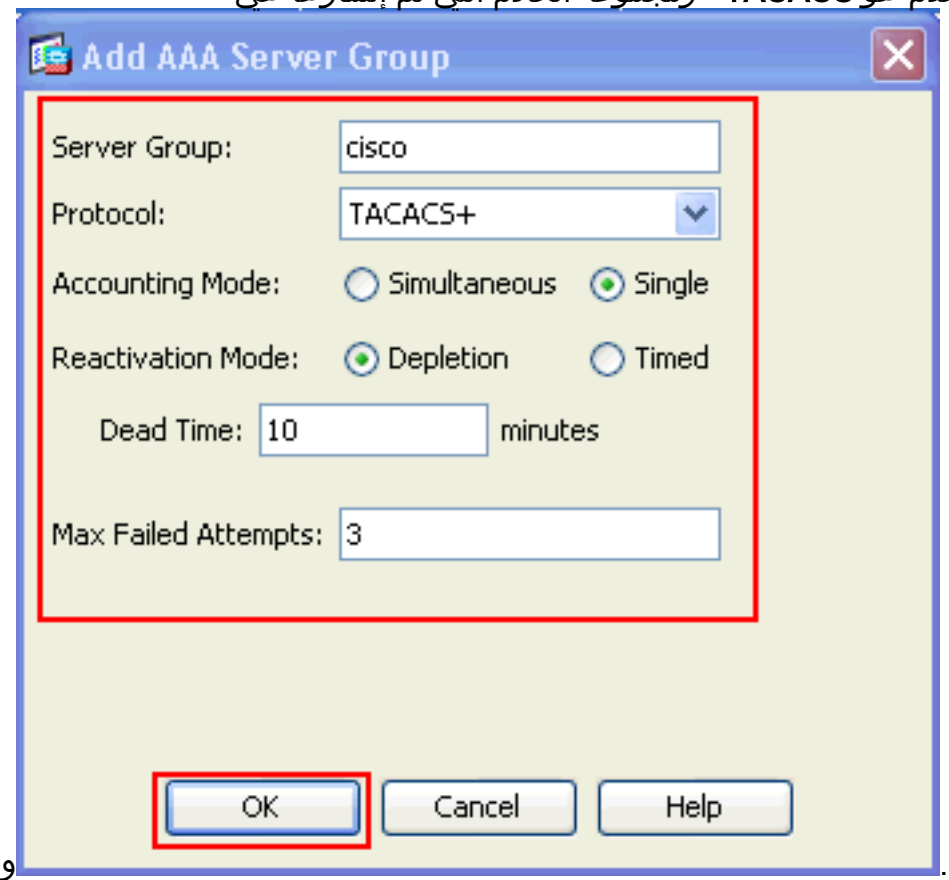
إجراء ASDM

أتمت هذا steps in order to شكلت ال ASA للمصادقة من ال acs نادل:

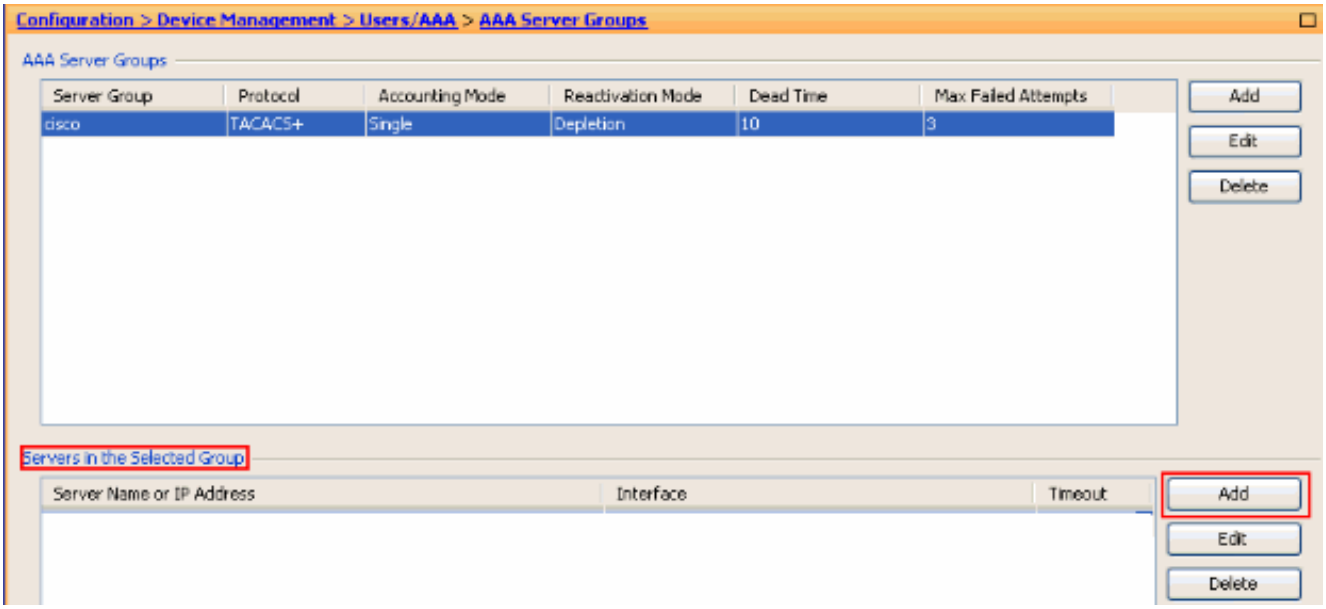
1. أختر **تكوين > إدارة الأجهزة > Users/AAA > مجموعات خوادم AAA > إضافة** لإنشاء **مجموعة خوادم AAA**.



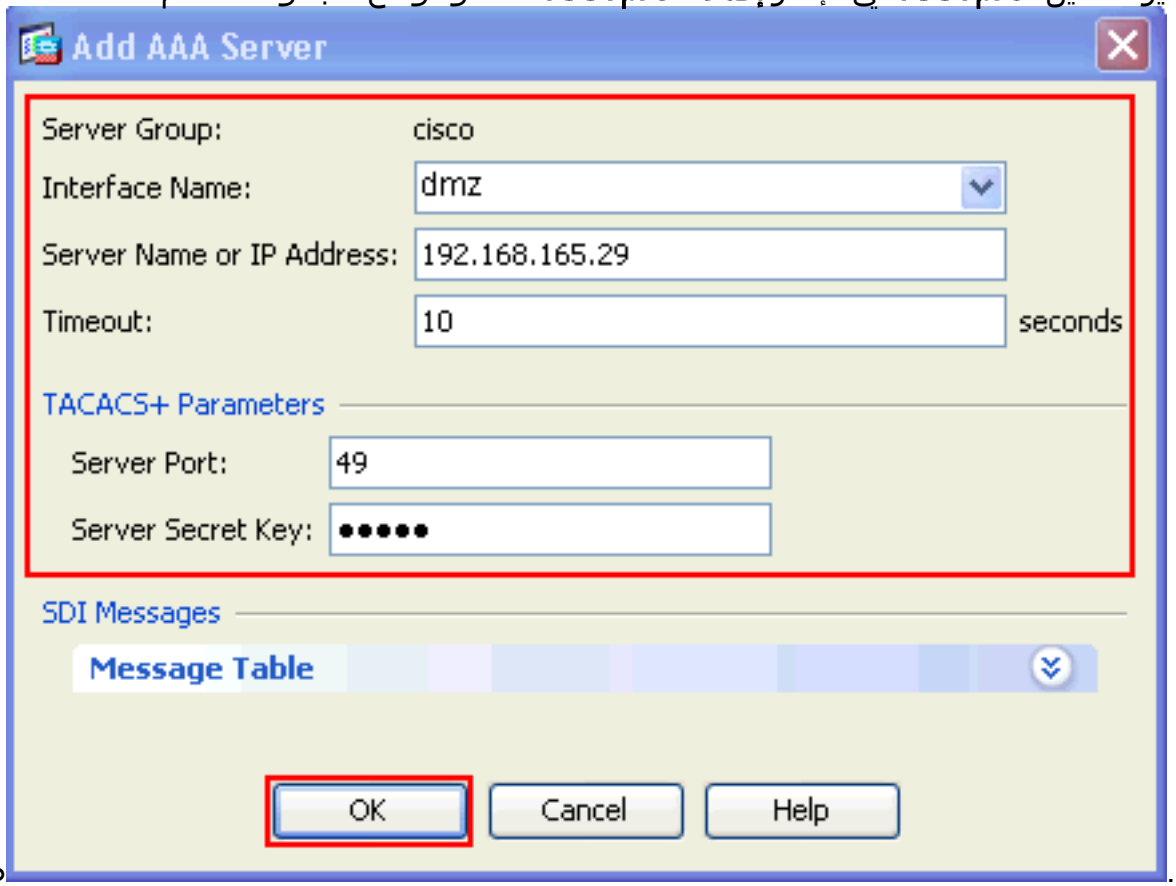
2. قم بتوفير تفاصيل **مجموعة خوادم AAA** في نافذة **إضافة مجموعة خوادم AAA** كما هو موضح. البروتوكول المستخدم هو **TACACS+** ومجموعة الخادم التي تم إنشاؤها هي **Cisco**. وانقر فوق **OK**.



3. أخترت **تشكيل>أداة إدارة>مستعمل/AAA>AAA نادل مجموعة** و طقطقة **يضيف** تحت **نادل في المجموعة المحددة** in order to أضفت ال AAA نادل.



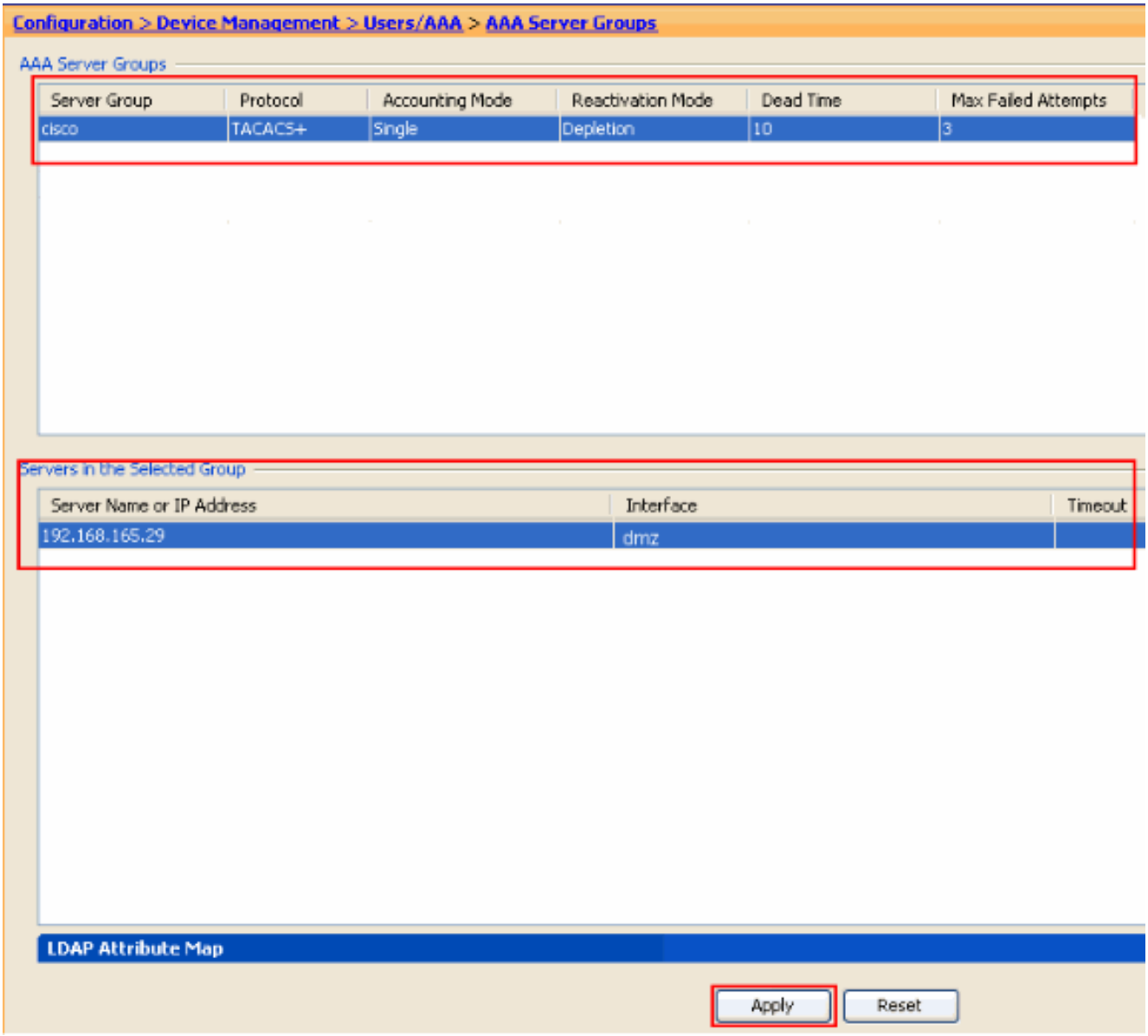
4. قم بتوفير تفاصيل **خادم AAA** في الإطار **إضافة خادم AAA** كما هو موضح. مجموعة الخادم المستخدمة هي



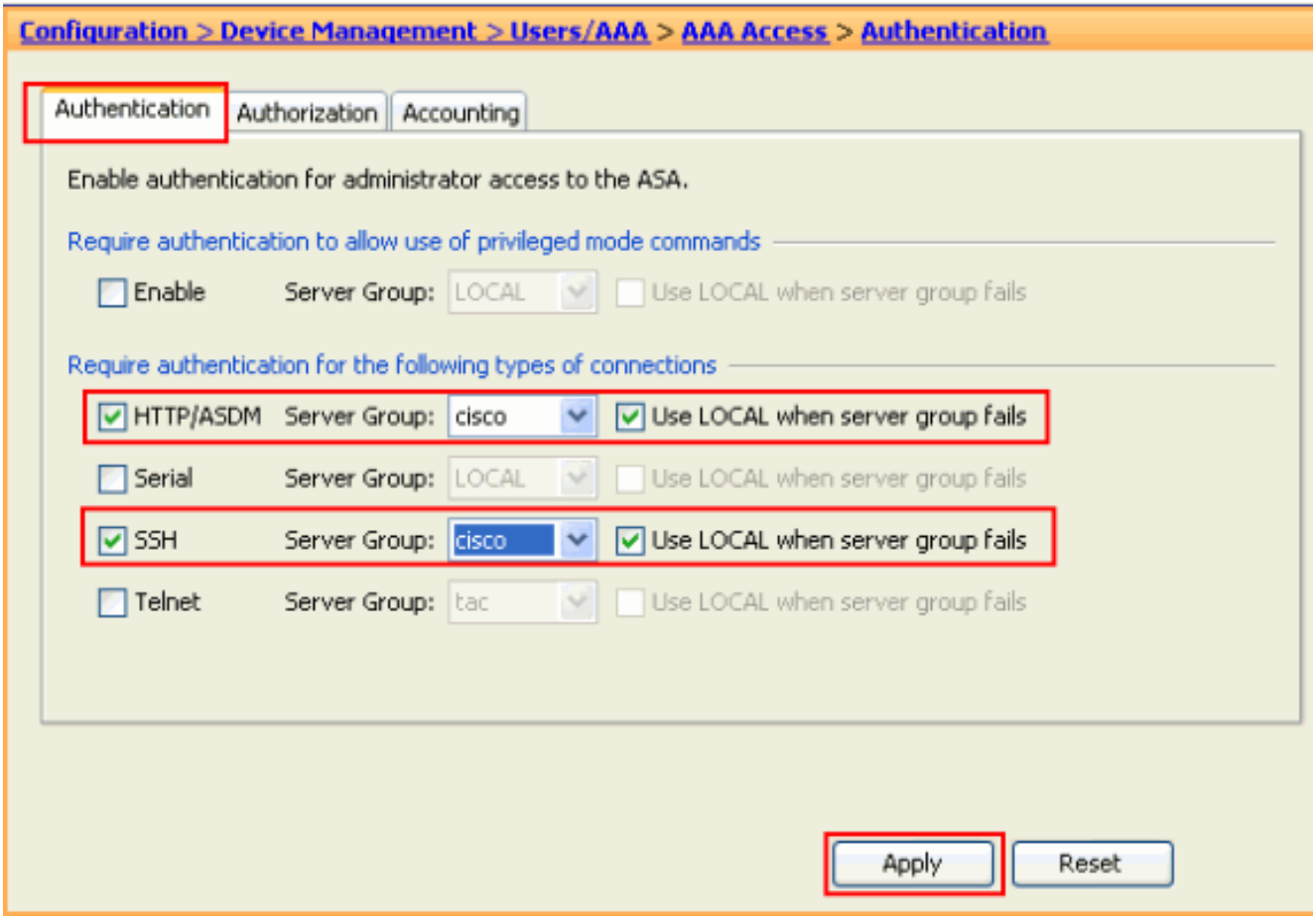
Cisco. طقط

قة **ok**، بعد ذلك طقطقة **يطبق**.سترى **مجموعة خوادم AAA** وخادم **AAA** الذي تم تكوينه على ASA.

5. طقطقة **يطبق**.



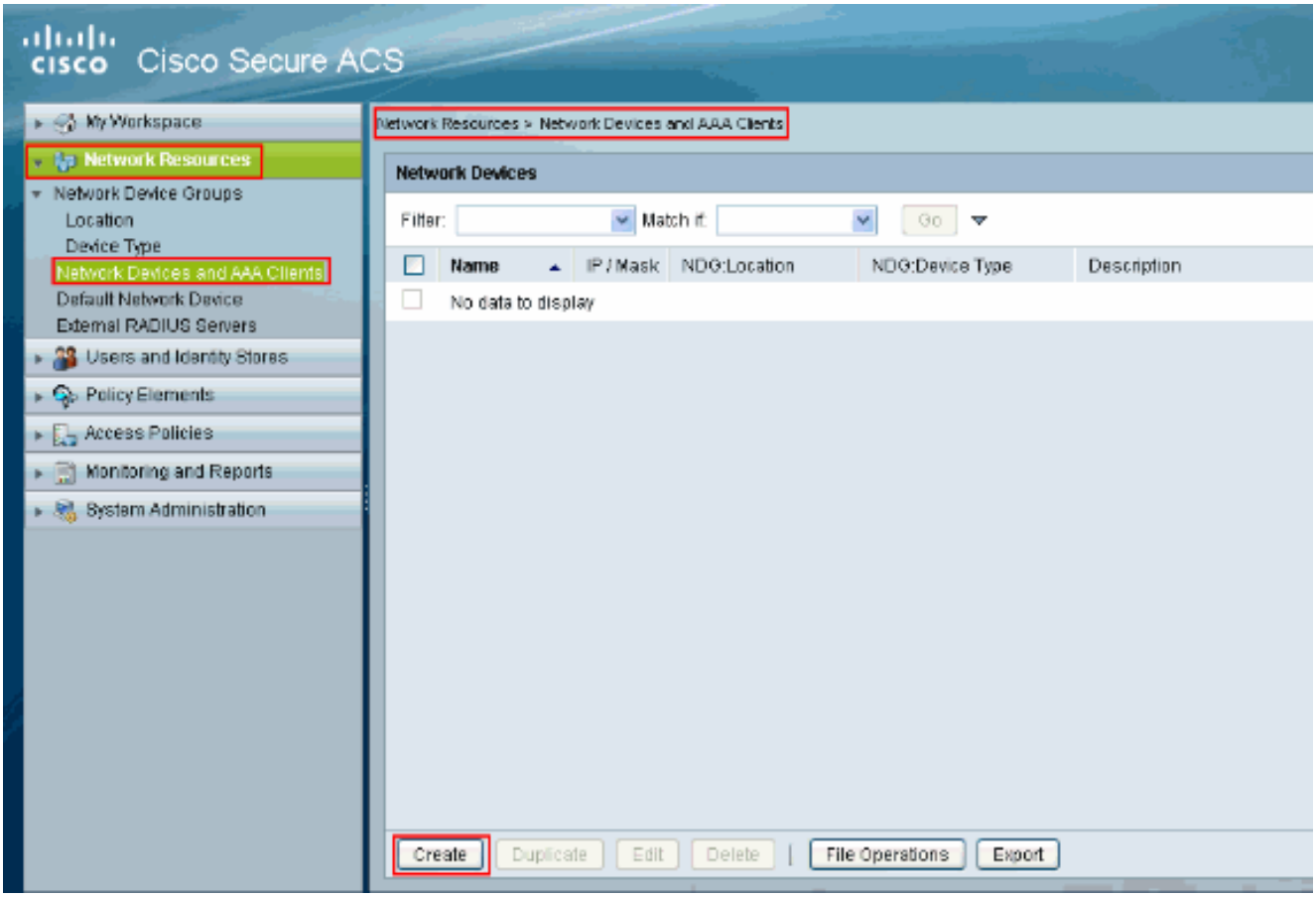
6. أختر **تكوين > إدارة الأجهزة > Users/AAA > الوصول إلى AAA > المصادقة** وانقر فوق خانات الاختيار المجاورة ل **HTTP/ASDM** و**SSH**. بعد ذلك، أختر **Cisco** كمجموعة خوادم وانقر فوق **تطبيق**.



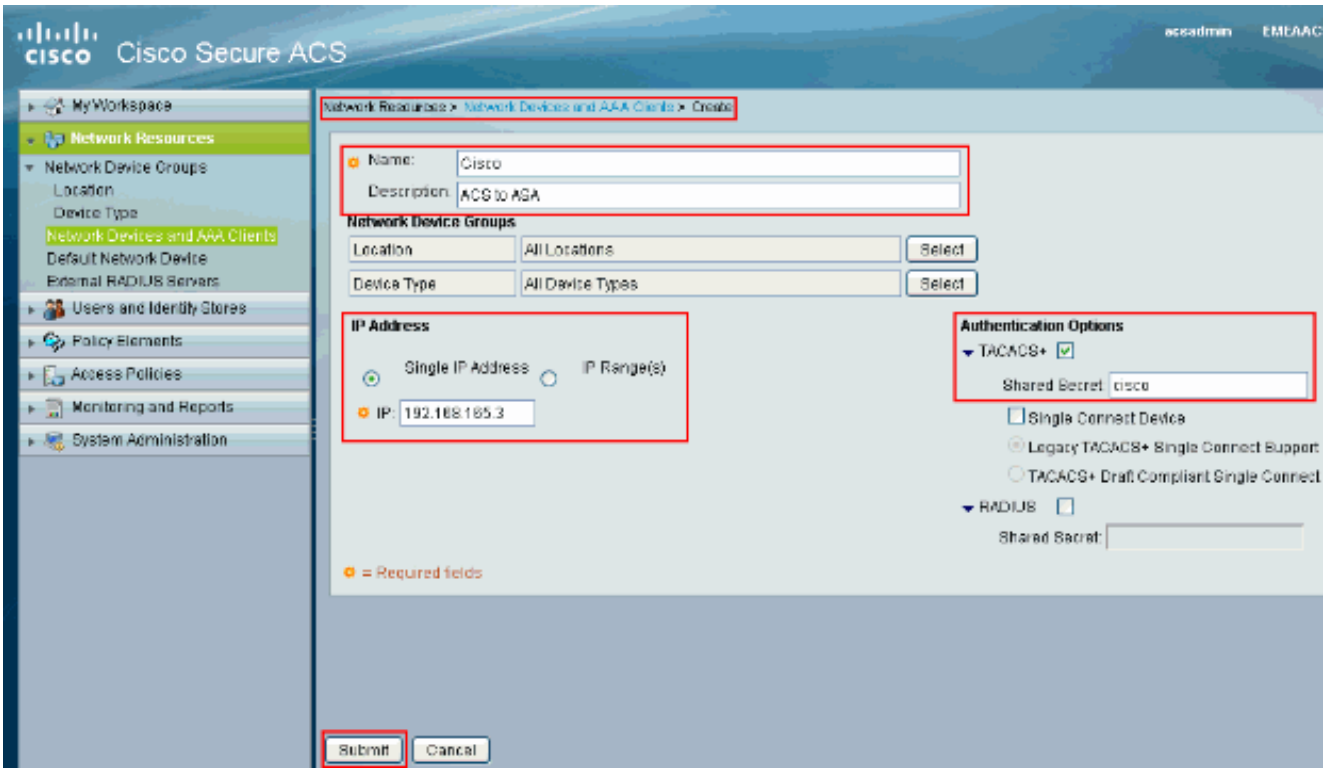
تكوين ACS كخادم TACACS

أكمل هذا الإجراء لتكوين ACS كخادم TACACS:

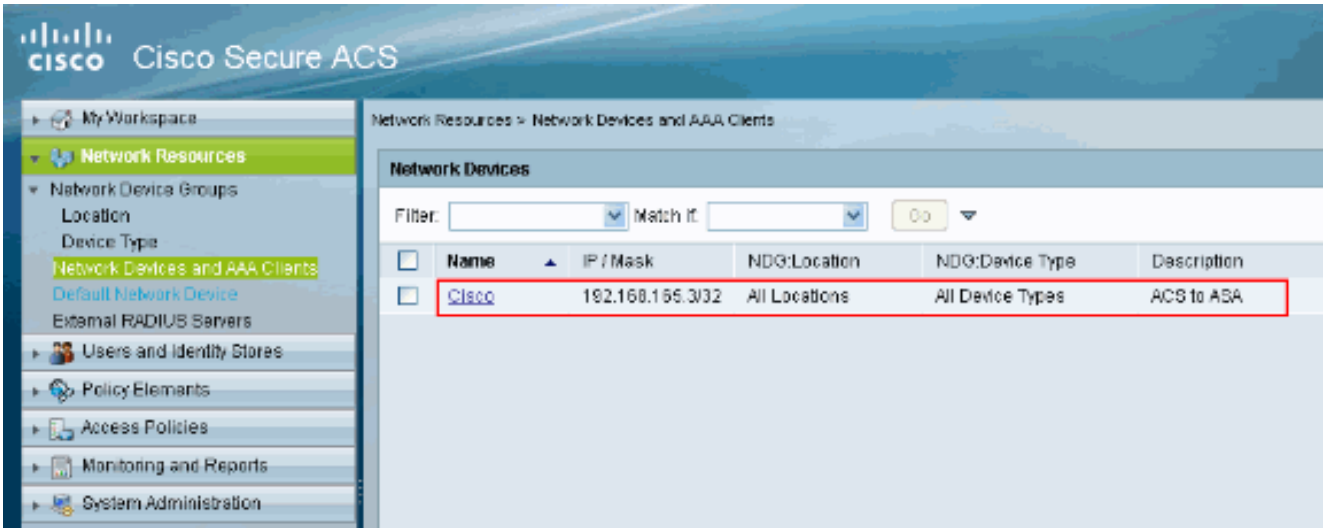
1. أخترت **شبكة مورد>شبكة أداة و AAA زبون** وطقطقة **يخلق** in order to أضفت ال ASA إلى ال ACS نادل.



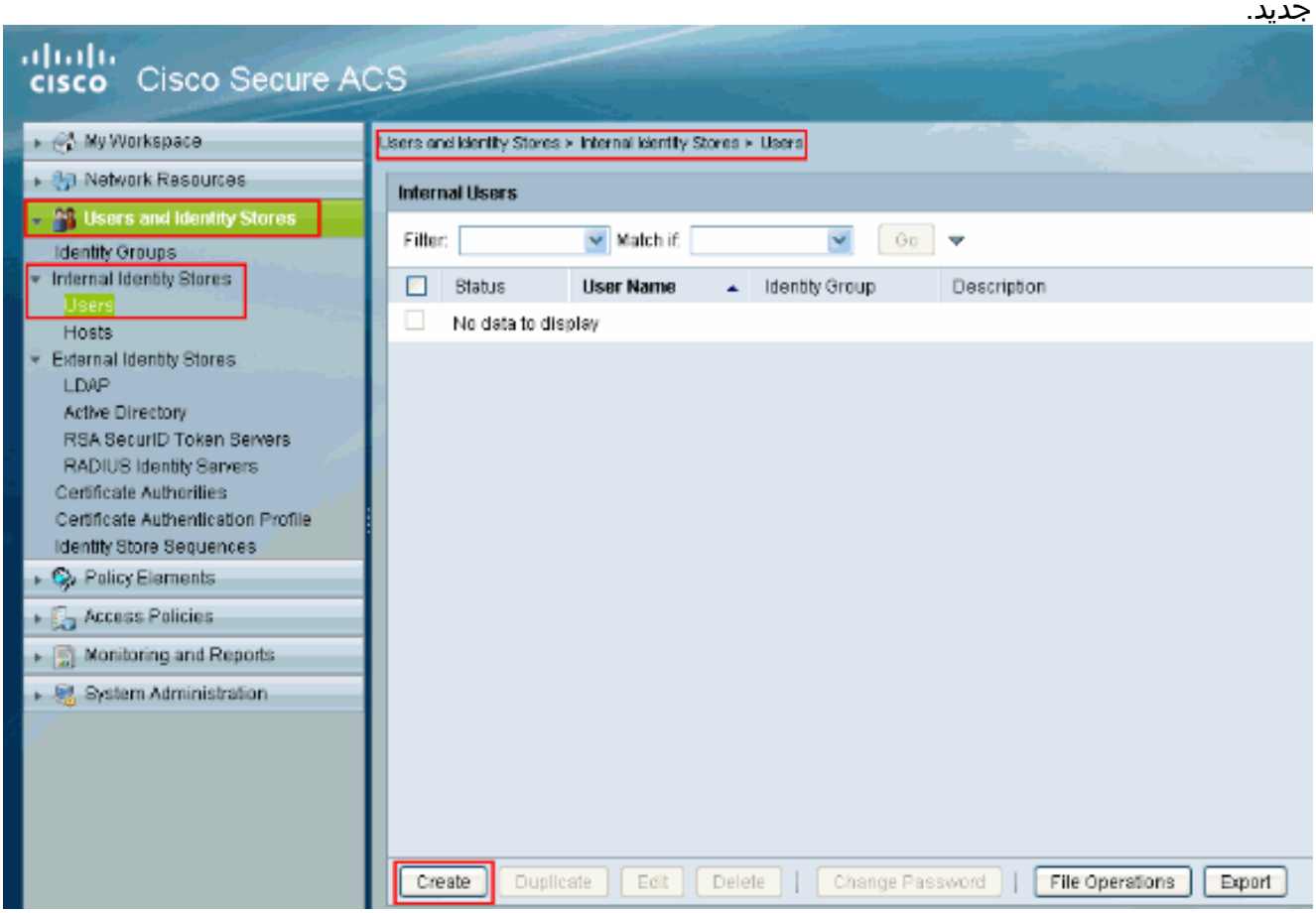
2. قم بتوفير المعلومات المطلوبة حول **العميل** (ASA هو العميل هنا) وانقر فوق **إرسال**. يتيح هذا الخيار ل ASA أن تتم إضافته إلى خادم ACS. وتتضمن التفاصيل **عنوان IP** الخاص ب ASA وتفاصيل **خادم TACACS**.



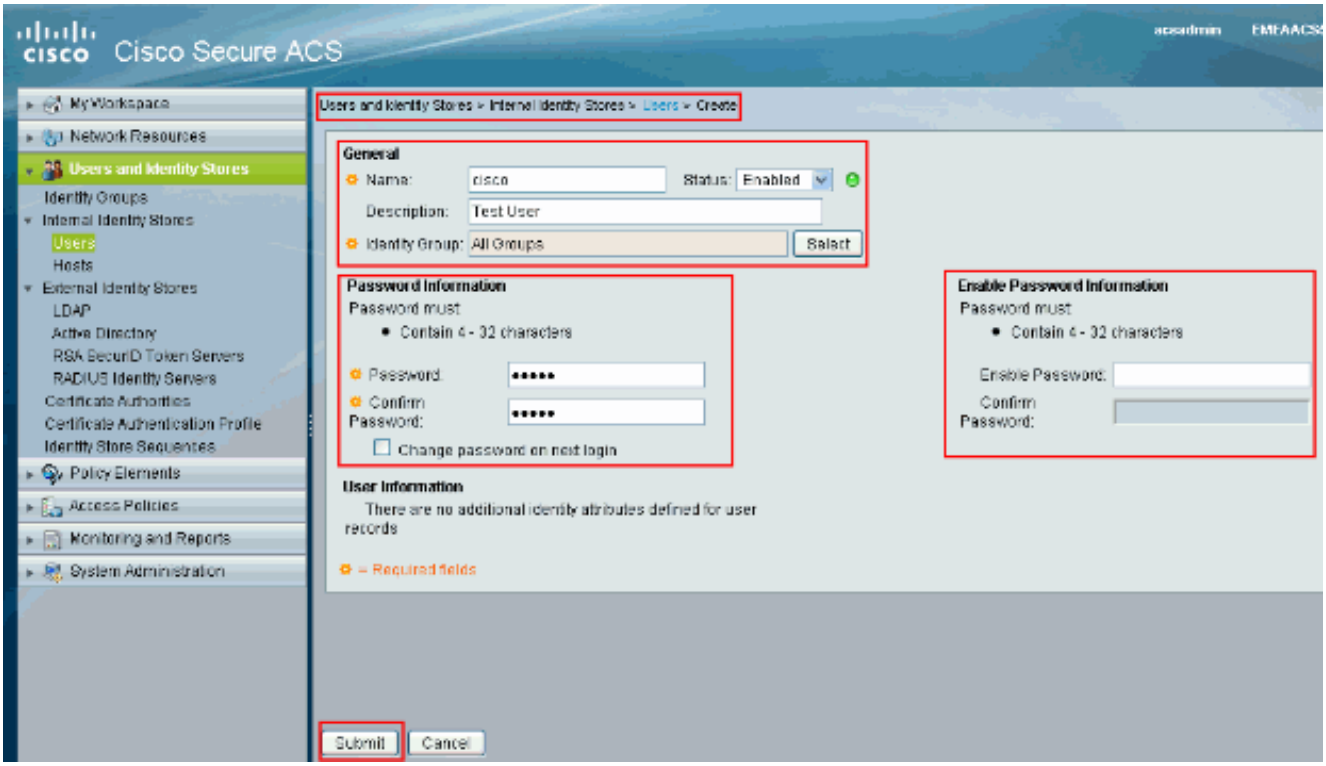
ستشاهد **Cisco** العميل تتم إضافته إلى خادم ACS.



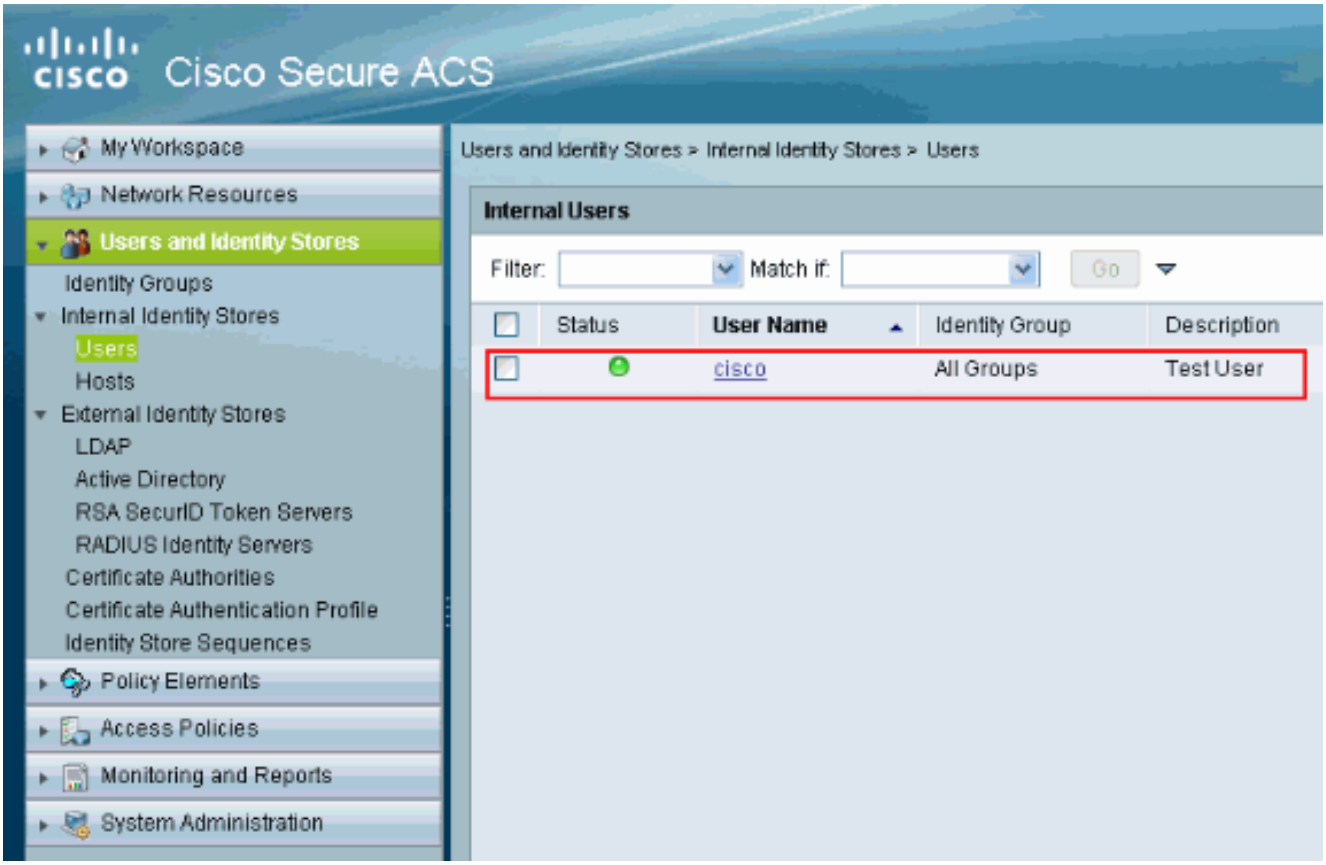
3. أختر **المستخدمين ومخازن الهوية > مخازن الهوية الداخلية > المستخدمين** وانقر فوق **إنشاء** لإنشاء مستخدم جديد.



4. قم بتوفير معلومات **كلمة المرور والاسم** وكلمة المرور **والتمكين** لها. **تمكين كلمة المرور إختياري**. عند الانتهاء، انقر فوق
إرسال.



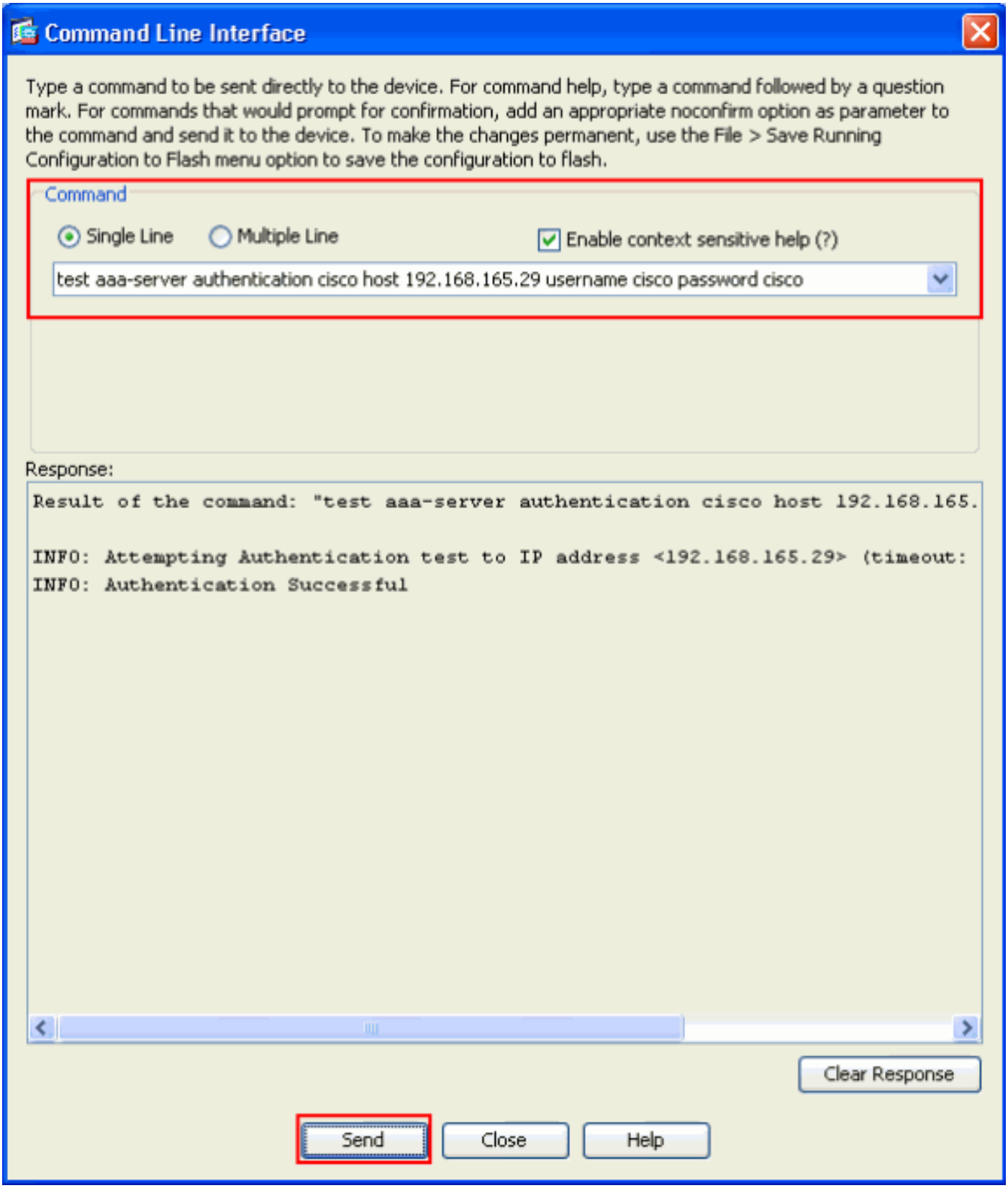
ستشاهد المستخدم **cisco** تتم إضافته إلى خادم ACS.



التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

استعملت **الاختبار aaa-نادل صحة هوية cisco مضيف 192.168.165.29 username cisco كلمة cisco cisco** أمر أن يتحقق إن التشكيل يعمل بشكل صحيح. توضح هذه الصورة أن المصادقة ناجحة وأنه قد تمت مصادقة المستخدم الذي يتصل ب ASA بواسطة خادم ACS.



تدعم أداة مترجم الإخراج (للعملاءالمسجلين فقط) بعض أوامر **show**. استخدم أداة مترجم الإخراج (OIT) لعرض تحليل مُخرَج الأمر **show** .

استكشاف الأخطاء وإصلاحها

خطأ: AAA تمييز TACACS+ server x.x.x في tacacs لمجموعة خوادم aaa على أنه فشل

تعني هذه الرسالة أن Cisco ASA فقدت الاتصال بخادم x.x.x.x. تأكد من أن لديك اتصال صالح على TCP 49

بالخادم x.x.x.x من ASA. يمكنك أيضا زيادة المهلة على ASA لخادم TACACS+ من 5 إلى العدد المرغوب من الثواني في حالة وجود زمن انتقال للشبكة. لن يرسل ASA طلب مصادقة إلى الخادم الفاشل x.x.x.x. ومع ذلك، فإنه سيستخدم الخادم التالي في tacacs لمجموعة خوادم aaa.

معلومات ذات صلة

- صفحة دعم أجهزة الأمان القابلة للتكيف Cisco من ASA 5500 Series
- مراجع أوامر أجهزة الأمان المعدلة Cisco ASA 5500 Series Adaptive Security Appliances Command References
- مدير أجهزة حلول الأمان المعدلة من Cisco
- صفحة دعم مفاوضة IPsec/بروتوكولات IKE
- خادم التحكم في الوصول الآمن من Cisco لأنظمة التشغيل Windows
- طلبات التعليقات (RFCs)
- الدعم التقني والمستندات - Cisco Systems

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).