

ASA 8.3: ACS 5.x مداخلت ساب TACACS ةق داصم

المحتويات

[المقدمة](#)

[المتطلبات الأساسية](#)

[المتطلبات](#)

[المكونات المستخدمة](#)

[الاصطلاحات](#)

[التكوين](#)

[الرسم التخطيطي للشبكة](#)

[تكوين ASA للمصادقة من خادم ACS باستخدام CLI \(واجهة سطر الأوامر\)](#)

[تكوين ASA للمصادقة من خادم ACS باستخدام ASDM](#)

[تكوين ACS كخادم TACACS](#)

[التحقق من الصحة](#)

[استكشاف الأخطاء وإصلاحها](#)

[خطأ: AAA تميز x.x.x server TACACS+ في tacacs لمجموعة خوادم aaa على أنه فشل](#)

[معلومات ذات صلة](#)

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 ASDM لـ HTTPS](#) 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

الاصطلاحات

راجع [اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.](#)

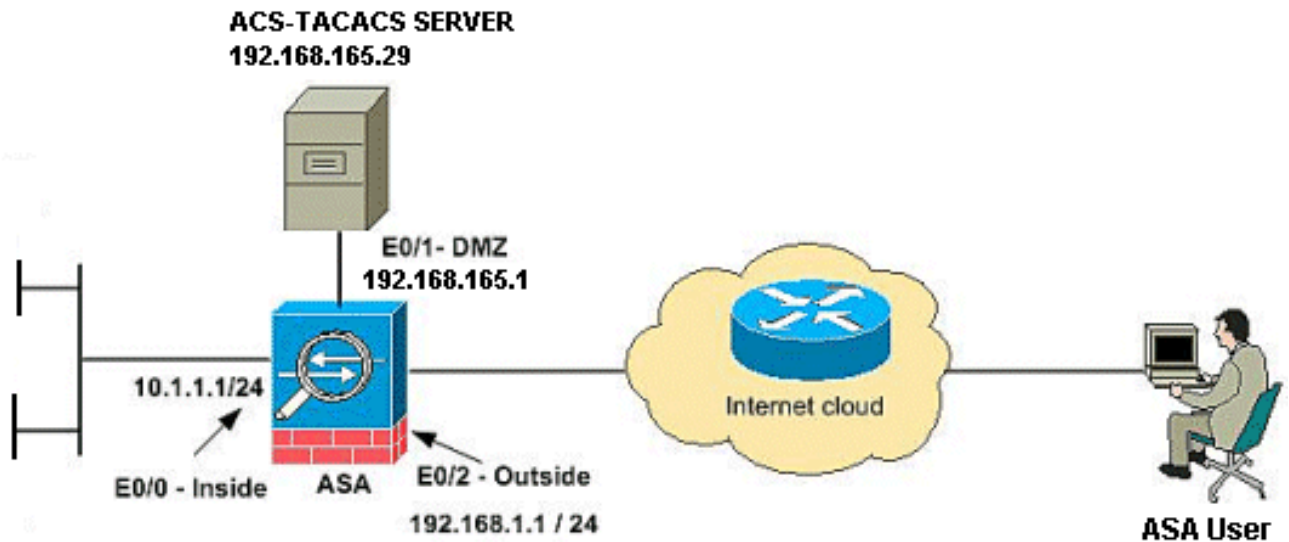
التكوين

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

ملاحظة: أستخدم [أداة بحث الأوامر](#) (للعلماء [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 1918 rfc 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

```

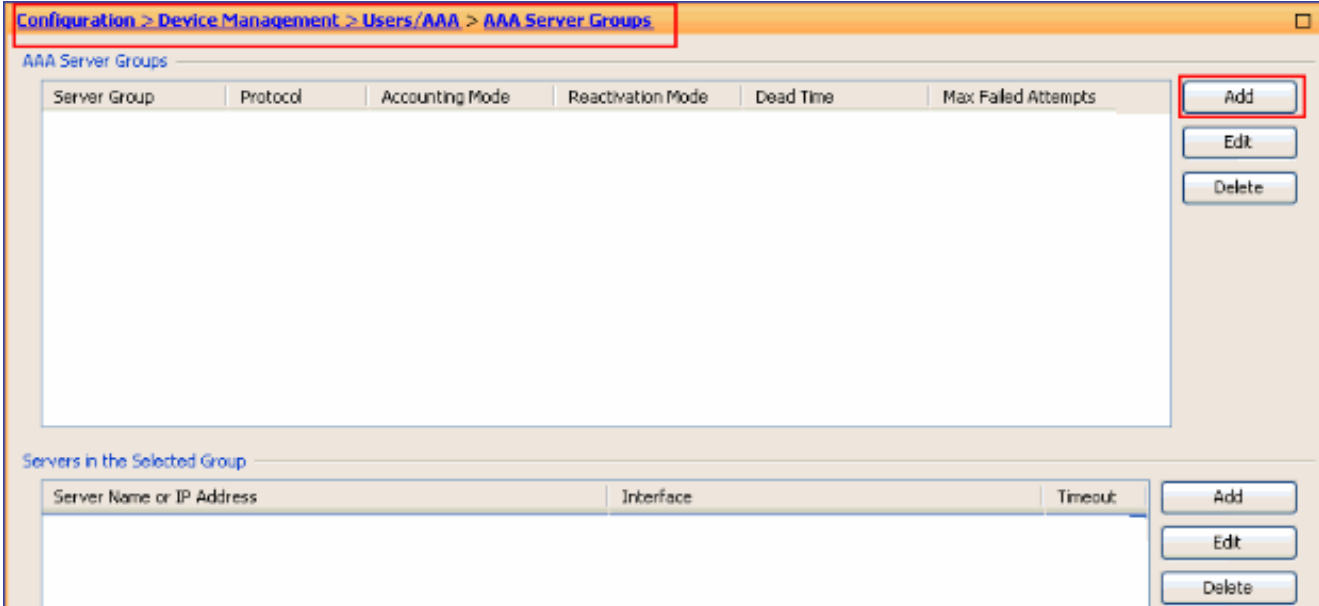
ملاحظة: قم بإنشاء مستخدم محلي على ASA باستخدام الأمر `username cisco password cisco privilege 15` للوصول إلى ASDM باستخدام المصادقة المحلية عندما لا يكون ACS متوفراً.

تكوين ASA للمصادقة من خادم ACS باستخدام ASDM

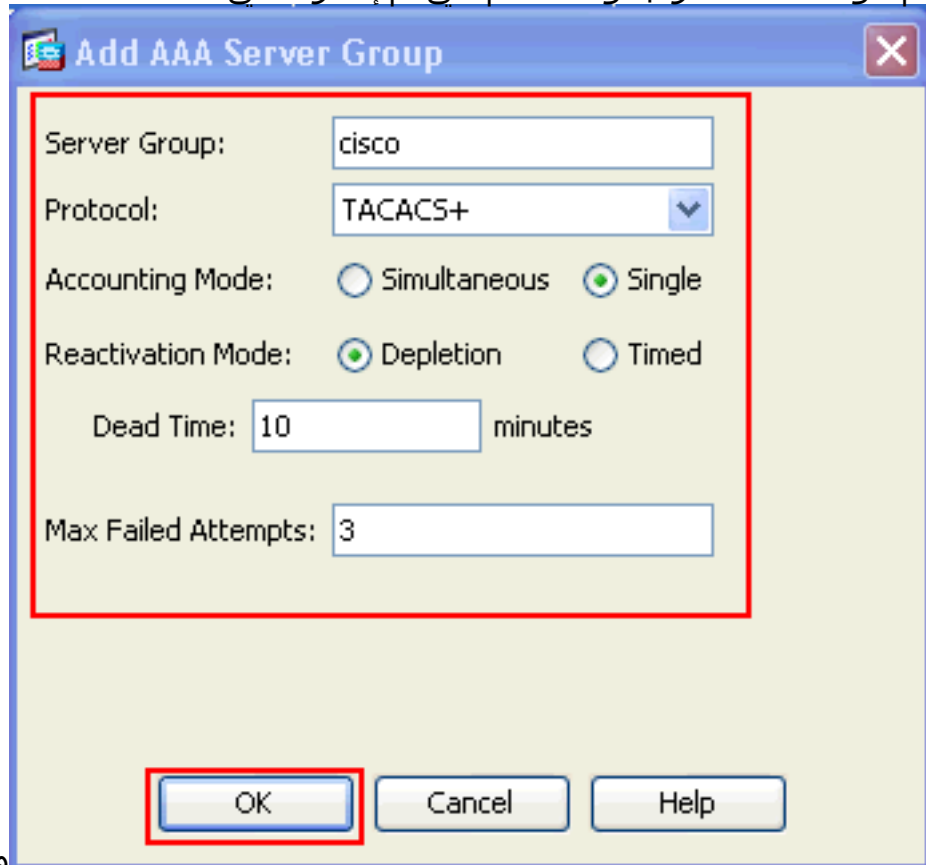
إجراء ASDM

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

1. أختار تكوين < إدارة الأجهزة < Users/AAA < مجموعات خوادم AAA < إضافة لإنشاء مجموعة خوادم AAA.



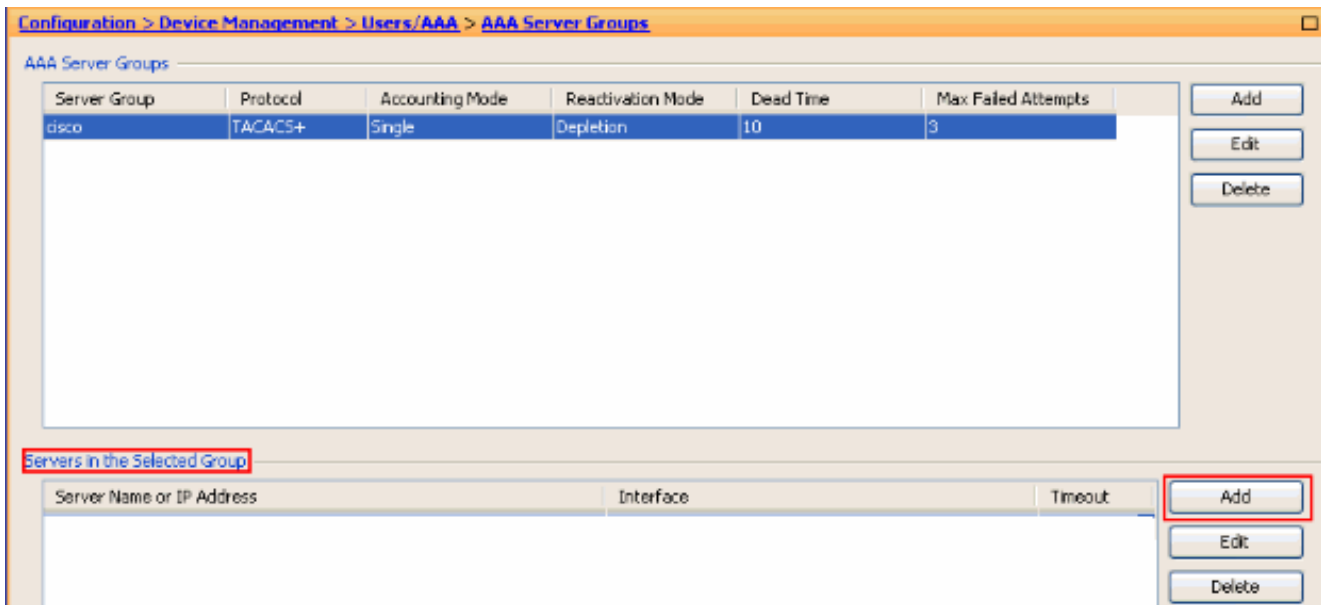
2. قم بتوفير تفاصيل مجموعة خوادم AAA في نافذة إضافة مجموعة خوادم AAA كما هو موضح. البروتوكول المستخدم هو TACACS+ ومجموعة الخادم التي تم إنشاؤها هي



وانقر فوق OK.

Cisco

3. أختارت تشكيل < أداة إدارة > مستعمل AAA > AAA نادل مجموعة و قطعة 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

Add AAA Server

Server Group: cisco

Interface Name: dmz

Server Name or IP Address: 192.168.165.29

Timeout: 10 seconds

TACACS+ Parameters

Server Port: 49

Server Secret Key: ●●●●●●

SDI Messages

Message Table

OK Cancel Help

طقط

.Cisco

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

5. طقطقة

يطبق.

AAA Server Groups

| Server Group | Protocol | Accounting Mode | Reactivation Mode | Dead Time | Max Failed Attempts |
|--------------|----------|-----------------|-------------------|-----------|---------------------|
| cisco | TACACS+ | Single | Depletion | 10 | 3 |

Servers in the Selected Group

| Server Name or IP Address | Interface | Timeout |
|---------------------------|-----------|---------|
| 192.168.165.29 | dmz | |

LDAP Attribute Map

6. أختار تكوين < إدارة الأجهزة < Users/AAA < الوصول إلى AAA < المصادقة وانقر فوق خانة الاختيار المجاورة ل HTTP/ASDM وSSH. بعد ذلك، أختار Cisco كمجموعة خوادم وانقر فوق تطبيق.

Authentication Authorization Accounting

Enable authentication for administrator access to the ASA.

Require authentication to allow use of privileged mode commands

Enable Server Group: LOCAL Use LOCAL when server group fails

Require authentication for the following types of connections

HTTP/ASDM Server Group: cisco Use LOCAL when server group fails

Serial Server Group: LOCAL Use LOCAL when server group fails

SSH Server Group: cisco Use LOCAL when server group fails

Telnet Server Group: tac Use LOCAL when server group fails

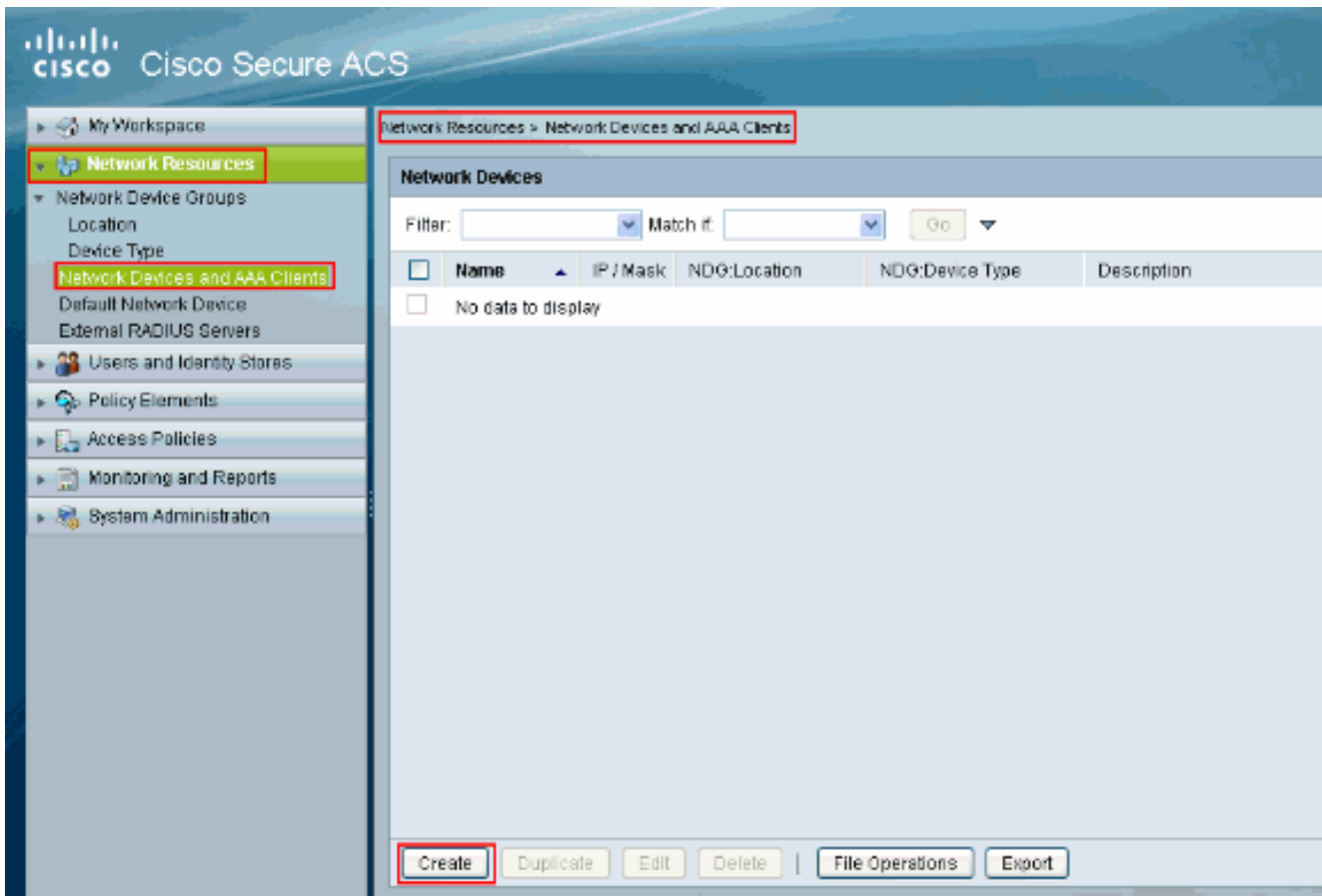
Apply

Reset

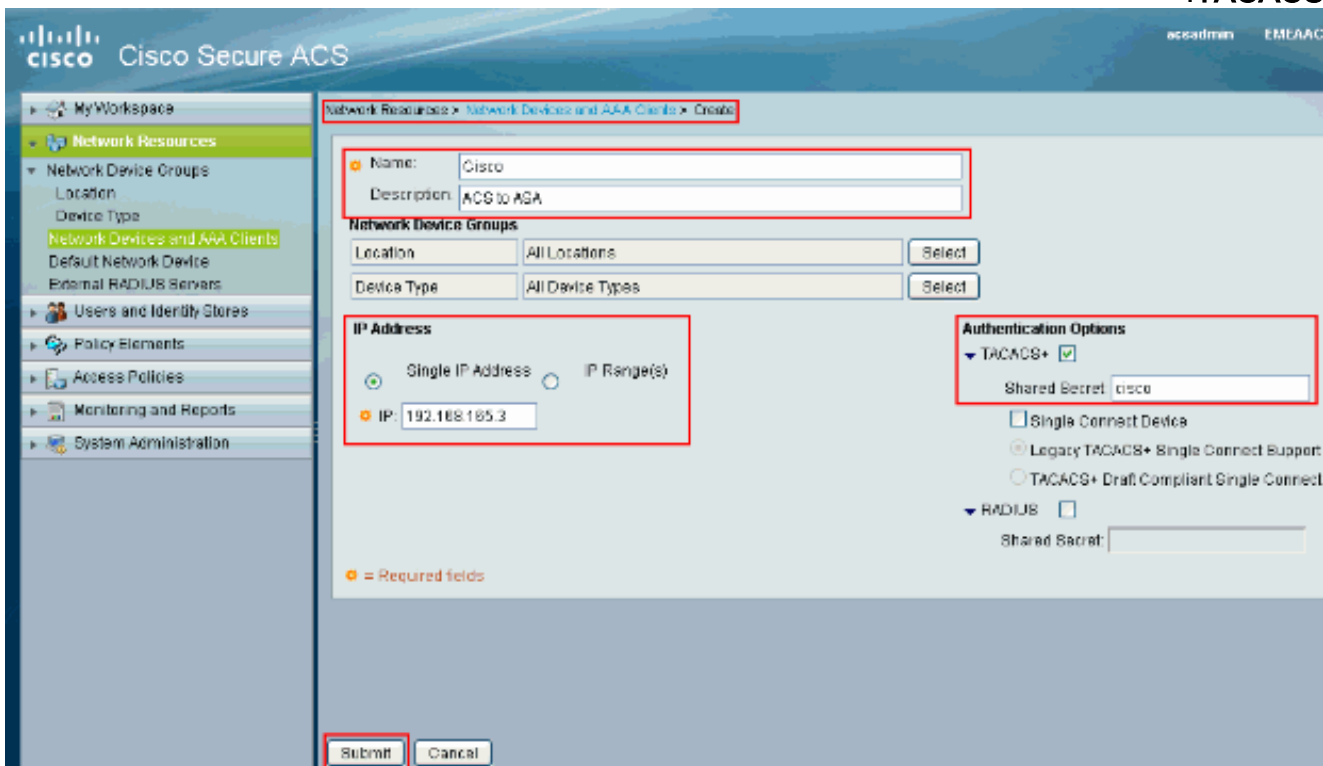
تكوين ACS كخادم TACACS

أكمل هذا الإجراء لتكوين ACS كخادم TACACS:

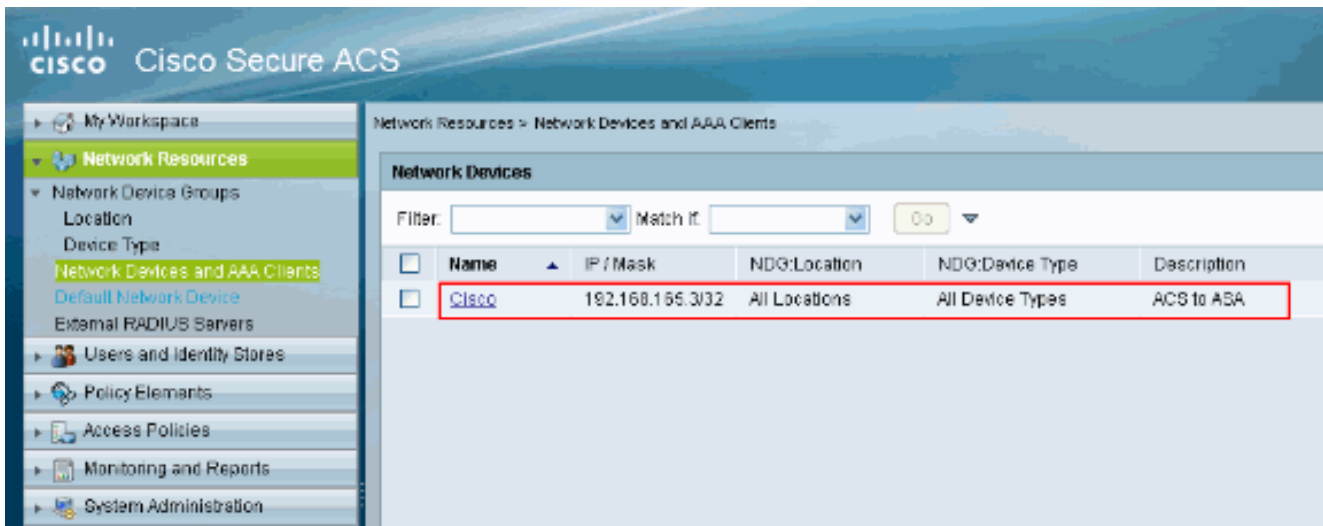
1. اخترت شبكة مورد < شبكة أداة و AAA زبون و قطعة يخلق in order to أضفت ال ASA إلى ال ACS نادل.



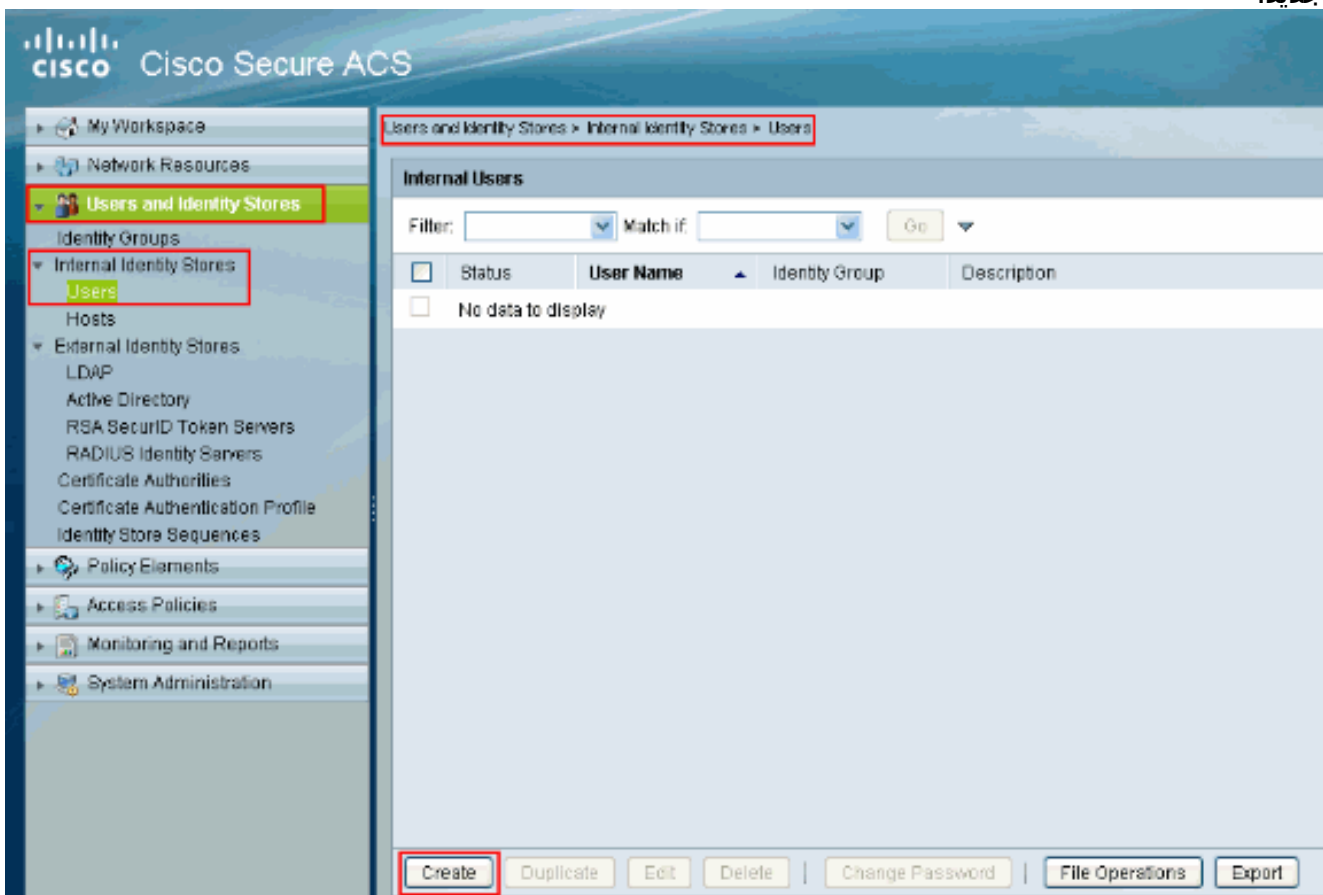
2. قم بتوفير المعلومات المطلوبة حول العميل (ASA هو العميل هنا) وانقر فوق إرسال. يتيح هذا الخيار ل ASA أن تتم إضافته إلى خادم ACS. وتتضمن التفاصيل عنوان IP الخاص ب ASA وتفاصيل خادم TACACS.



ستشاهد Cisco العميل تتم إضافته إلى خادم ACS.



3. أختار 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 اختياري. عند الانتهاء، انقر فوق إرسال.

Users and Identity Stores > Internal Identity Stores > Users > Create

General

Name: Status:

Description:

Identity Group:

Password Information

Password must

- Contain 4 - 32 characters

Password:

Confirm Password:

Change password on next login

Enable Password Information

Password must

- Contain 4 - 32 characters

Enable Password:

Confirm Password:

User Information

There are no additional identity attributes defined for user records

= Required fields

ستشاهد المستخدم cisco تم إضافته إلى خادم .ACS

Users and Identity Stores > Internal Identity Stores > Users

Internal Users

Filter: Match if:

| <input type="checkbox"/> | Status | User Name | Identity Group | Description |
|--------------------------|-------------------------------------|-----------------------|----------------|-------------|
| <input type="checkbox"/> | <input checked="" type="checkbox"/> | cisco | All Groups | Test User |

[التحقق من الصحة](#)

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

استعملت الاختبار aaa-نادل صحة هوية cisco مضيف 192.168.165.29 cisco cisco كلمة username 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.

The screenshot shows a window titled "Command Line Interface" with a blue header and a close button in the top right corner. Below the header, there is a paragraph of instructions: "Type a command to be sent directly to the device. For command help, type a command followed by a question mark. For commands that would prompt for confirmation, add an appropriate noconfirm option as parameter to the command and send it to the device. To make the changes permanent, use the File > Save Running Configuration to Flash menu option to save the configuration to flash."

The main area of the window is divided into two sections. The top section is labeled "Command" and contains a red-bordered box. Inside this box, there are two radio buttons: "Single Line" (which is selected) and "Multiple Line". To the right of these buttons is a checked checkbox labeled "Enable context sensitive help (?)". Below these options is a text input field containing the command: "test aaa-server authentication cisco host 192.168.165.29 username cisco password cisco".

The bottom section is labeled "Response:" and contains a text area with the following output: "Result of the command: "test aaa-server authentication cisco host 192.168.165.29 username cisco password cisco". INFO: Attempting Authentication test to IP address <192.168.165.29> (timeout: 30). INFO: Authentication Successful". Below the text area is a horizontal scrollbar. At the bottom right of the window is a "Clear Response" button. At the bottom center, there are three buttons: "Send" (which is highlighted with a red border), "Close", and "Help".

تدعم أداة مترجم الإخراج (للعلماء المسجلين فقط) بعض أوامر show. استخدم أداة مترجم الإخراج (OIT) لعرض تحليل مخرج الأمر show.

استكشاف الأخطاء وإصلاحها

خطأ: AAA تمييز server x.x.x TACACS+ 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 ASA 5500 Series من Cisco](#)
- [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](#)

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسم ل ا ذه Cisco ت مچرت
م ل ا ل ا ا ن ا ع مچ ي ف ن ي م دخت س م ل ل م عد ي و ت ح م م ي دقت ل ة ي ر ش ب ل و
ا م ك ة ق ي ق د ن و ك ت ن ل ة ل ا ة مچرت ل ض ف ا ن ا ة ظ ح ا ل م ي ج ر ي . ة ص ا خ ل ا م ه ت غ ل ب
Cisco ي ل خ ت . ف ر ت ح م مچرت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة مچرت ل ا ع م ل ا ح ل ا و ه
ي ل ا م ا ة ا د ع و ج ر ل ا ب ي ص و ت و ت ا مچرت ل ا هذه ق د ن ع ا ه ت ي ل و ئ س م Cisco
Systems (ر ف و ت م ط ب ا ر ل ا) ي ل ص ا ل ا ي ز ي ل ج ن ا ل ا دن ت س م ل ا