ASA 8.0: تكوين مصادقة RADIUS لمستخدمي WebVPN

المحتويات

المقدمة

يوضح هذا المستند كيفية تكوين جهاز الأمان القابل للتكيف (ASA) من Cisco لاستخدام خادم خدمة مصادقة طلب اتصال المستخدم البعيد (RADIUS) لمصادقة مستخدمي WebVPN. خادم RADIUS في هذا المثال هو خادم Cisco Access Control Server (ACS)، الإصدار 4.1 يتم تنفيذ هذا التكوين باستخدام مدير أجهزة الأمان القابل للتكيف (ASDM) 6.0(2) على ASA الذي يشغل الإصدار 8.0(2) من البرنامج.

ملاحظة: في هذا المثال، يتم تكوين مصادقة RADIUS لمستخدمي WebVPN، ولكن يمكن إستخدام هذا التكوين لأنواع أخرى من شبكات VPN الخاصة بالوصول عن بعد كذلك. ما عليك سوى تعيين مجموعة خوادم AAA إلى ملف تعريف الاتصال المطلوب (مجموعة النفق) كما هو موضح.

المتطلبات الأساسية

- يلزم توفر تكوين WebVPN أساسي.
- يجب أن يحتوي مصدر المحتوى الإضافي من Cisco على مستخدمين تم تكوينهم لمصادقة المستخدم. راجع قسم إضافة حساب مستخدم أساسي في إدارة المستخدم للحصول على مزيد من المعلومات.

قم بتكوين خادم ACS

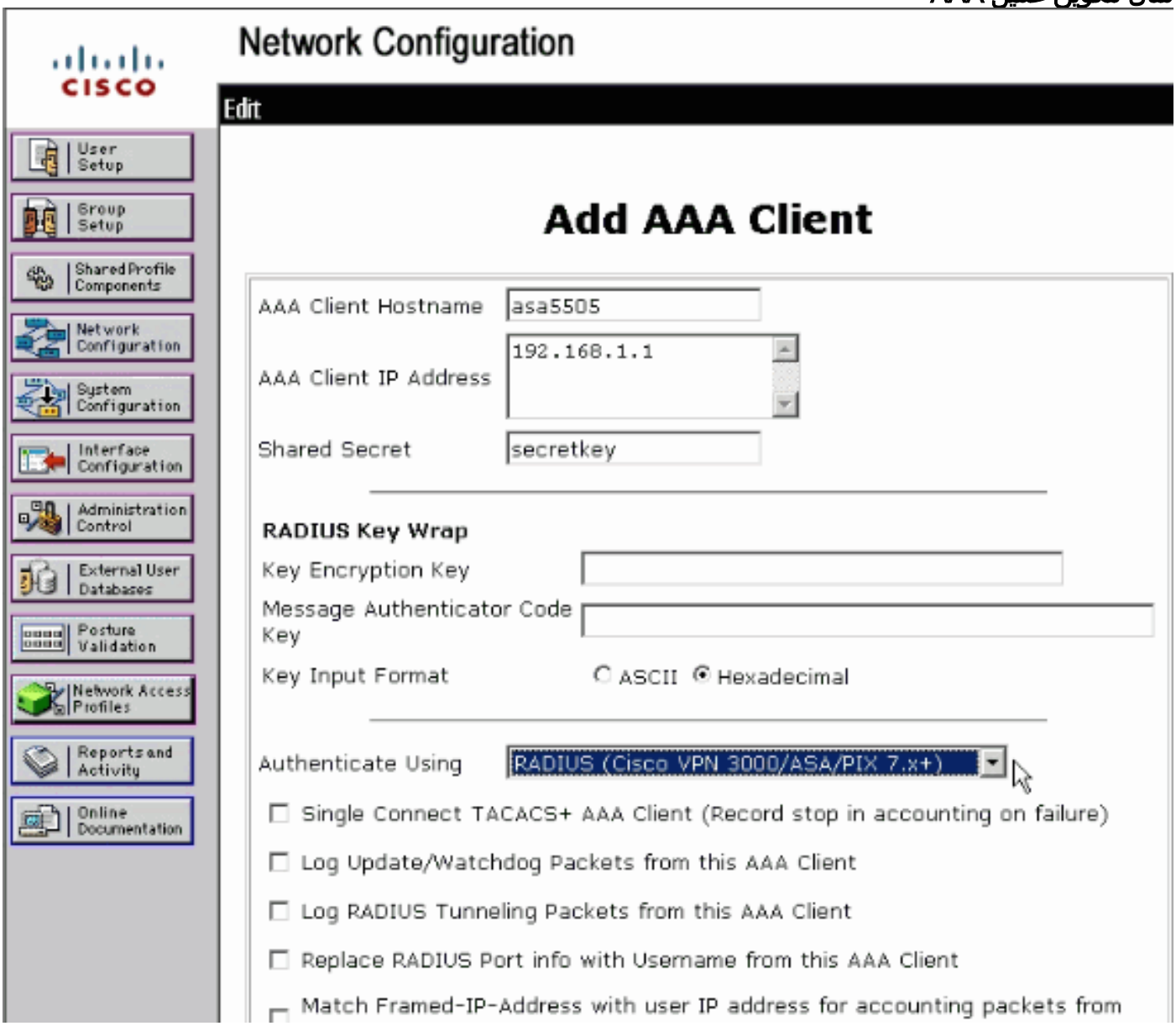
في هذا القسم، تقدم لك معلومات تكوين مصادقة RADIUS على ACS و ASA.

أتمت هذا steps in order to شكلت ال ACS نادل أن يتصل مع ال ASA.

1. أختر **تكوين الشبكة** من القائمة اليسرى من شاشة ACS.
2. أختر **إضافة إدخال** ضمن **عملاء AAA**.

3. توفير معلومات العميل:**اسم مضيف عميل AAA** — اسم من إختيارك**عنوان AAA Client IP**—العنوان الذي يتصل جهاز الأمان منه ب ACS**سر مشترك** — مفتاح سري تم تكوينه على ACS وعلى جهاز الأمان
4. في **المصادقة باستخدام** القائمة المنسدلة **أختر RADIUS (Cisco VPN 3000/ASA/PIX 7.x+)**.
5. انقر فوق **إرسال+تطبيق**.

مثال لتكوين عميل AAA

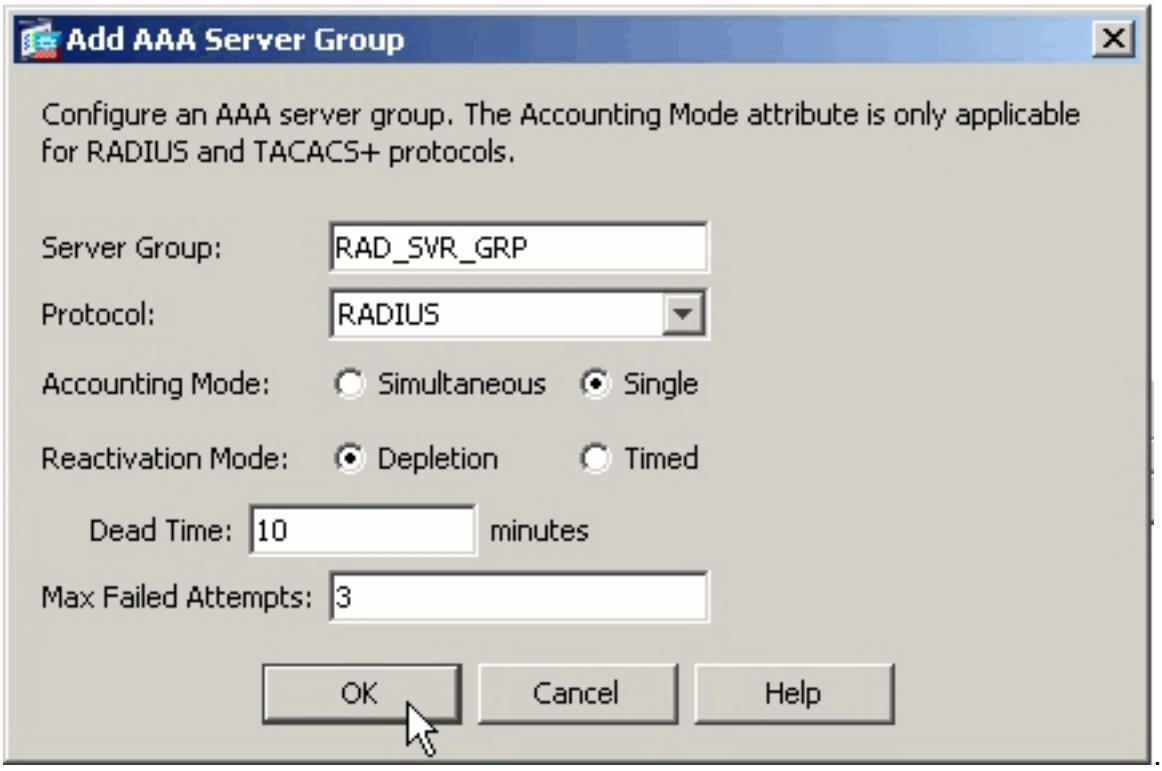


تكوين جهاز الأمان

ASDM

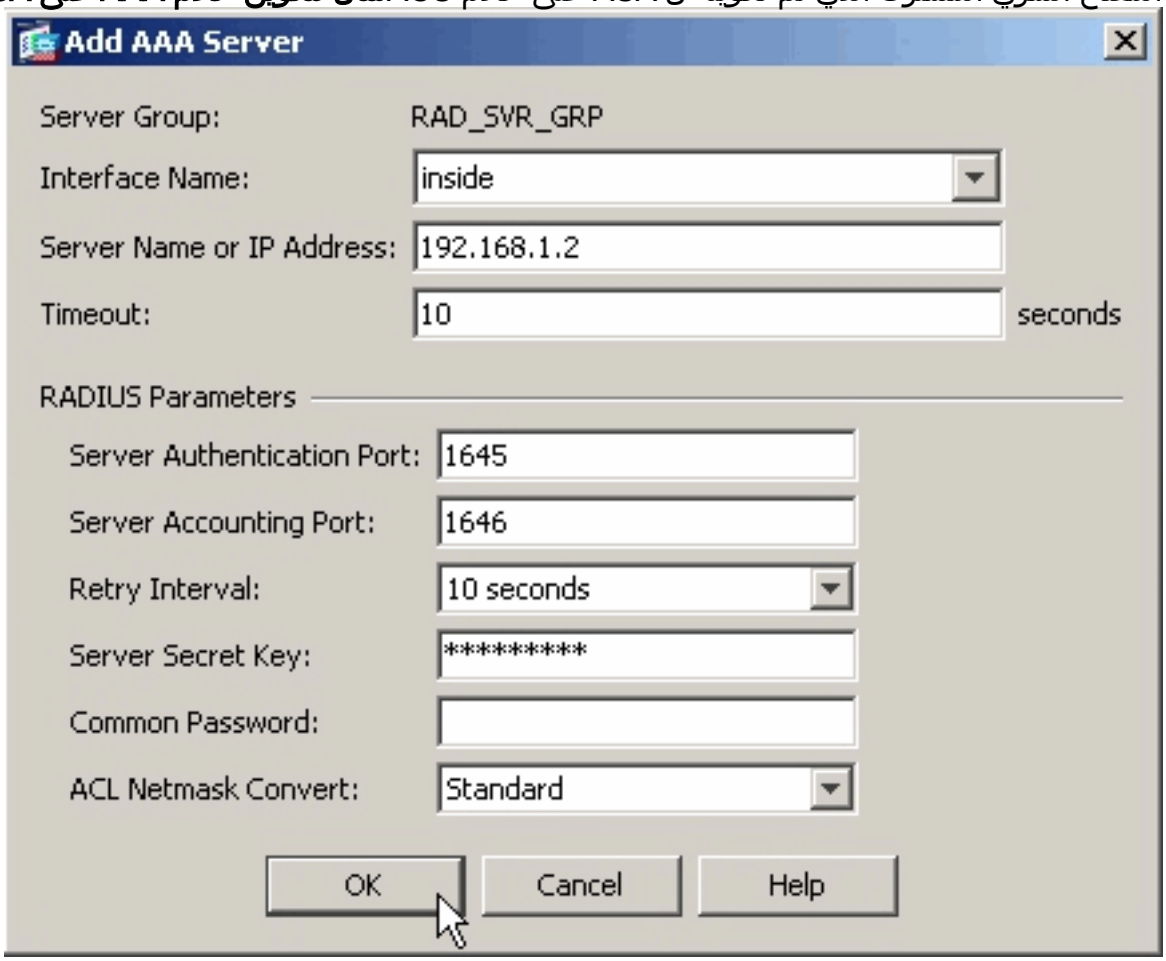
أتمت هذا steps في ال ASDM in order to شكلت ASA أن يتصل مع ال ACS نادل ومصادقة WebVPN زبون.

1. أختر **تكوين > Remote Access VPN (الوصول عن بعد) > إعداد AAA > مجموعات خوادم AAA**.
2. انقر فوق **إضافة** بجوار مجموعات خوادم AAA.
3. في النافذة التي تظهر، حدد اسم لمجموعة خوادم AAA الجديدة واختر **RADIUS** كبروتوكول. طقطقة **ok**



عندما إنتهيت.

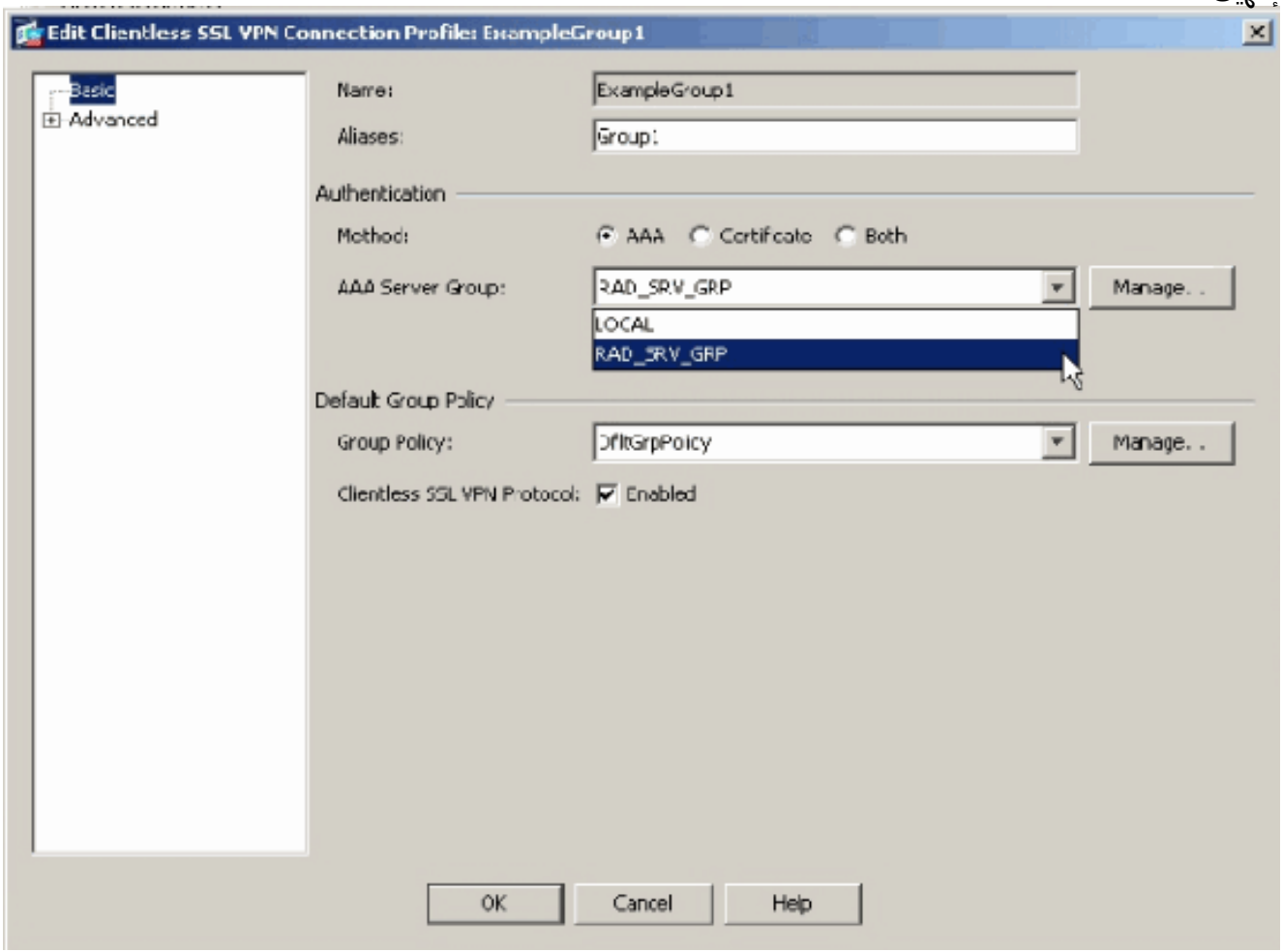
4. تأكد من تحديد مجموعتك الجديدة في اللوحة العليا وانقر فوق **إضافة** إلى يمين اللوحة السفلى.
5. توفير معلومات الخادم:**اسم الواجهة**— الواجهة التي يجب أن يستخدمها ASA للوصول إلى خادم ACS**اسم الخادم أو عنوان IP**— العنوان الذي يجب على ASA إستخدامه للوصول إلى خادم ACS**مفتاح سر الخادم**— المفتاح السري المشترك الذي تم تكوينه ل ASA على خادم ACS**مثال لتكوين خادم AAA على ASA**



6. بمجرد تكوين مجموعة خوادم AAA والخادم، انتقل إلى التكوين > Remote Access VPN (الوصول عن بعد) > ClientWithout SSL VPN Access > ملفات تعريف الاتصال لتكوين WebVPN لاستخدام تكوين AAA الجديد.**ملاحظة:** على الرغم من أن هذا المثال يستخدم WebVPN، يمكنك تعيين أي ملف تعريف لاتصال

الوصول عن بعد (مجموعة النفق) لاستخدام إعداد AAA هذا.

7. أختر ملف التعريف الذي تريد تكوين AAA له، وانقر فوق **تحرير**.
8. تحت **المصادقة** أختر مجموعة خوادم RADIUS التي قمت بإنشائها سابقا. طقطقة **ok** عندما إنتهيت.



واجهة سطر الأوامر

أتمت هذا steps في الأمر خط قارن (in order to CLI) شكلت ال ASA أن يتصل مع ال ACS نادل ومصادقة WebVPN زبون.

```
ciscoasa#configure terminal

Configure the AAA Server group. ciscoasa(config)# aaa-server RAD_SRV_GRP protocol RADIUS ---!
ciscoasa(config-aaa-server-group)# exit !--- Configure the AAA Server. ciscoasa(config)# aaa-
server RAD_SRV_GRP (inside) host 192.168.1.2 ciscoasa(config-aaa-server-host)# key secretkey
ciscoasa(config-aaa-server-host)# exit !--- Configure the tunnel group to use the new AAA setup.
ciscoasa(config)# tunnel-group ExampleGroup1 general-attributes ciscoasa(config-tunnel-general)#
authentication-server-group RAD_SRV_GRP
```

التحقق من الصحة

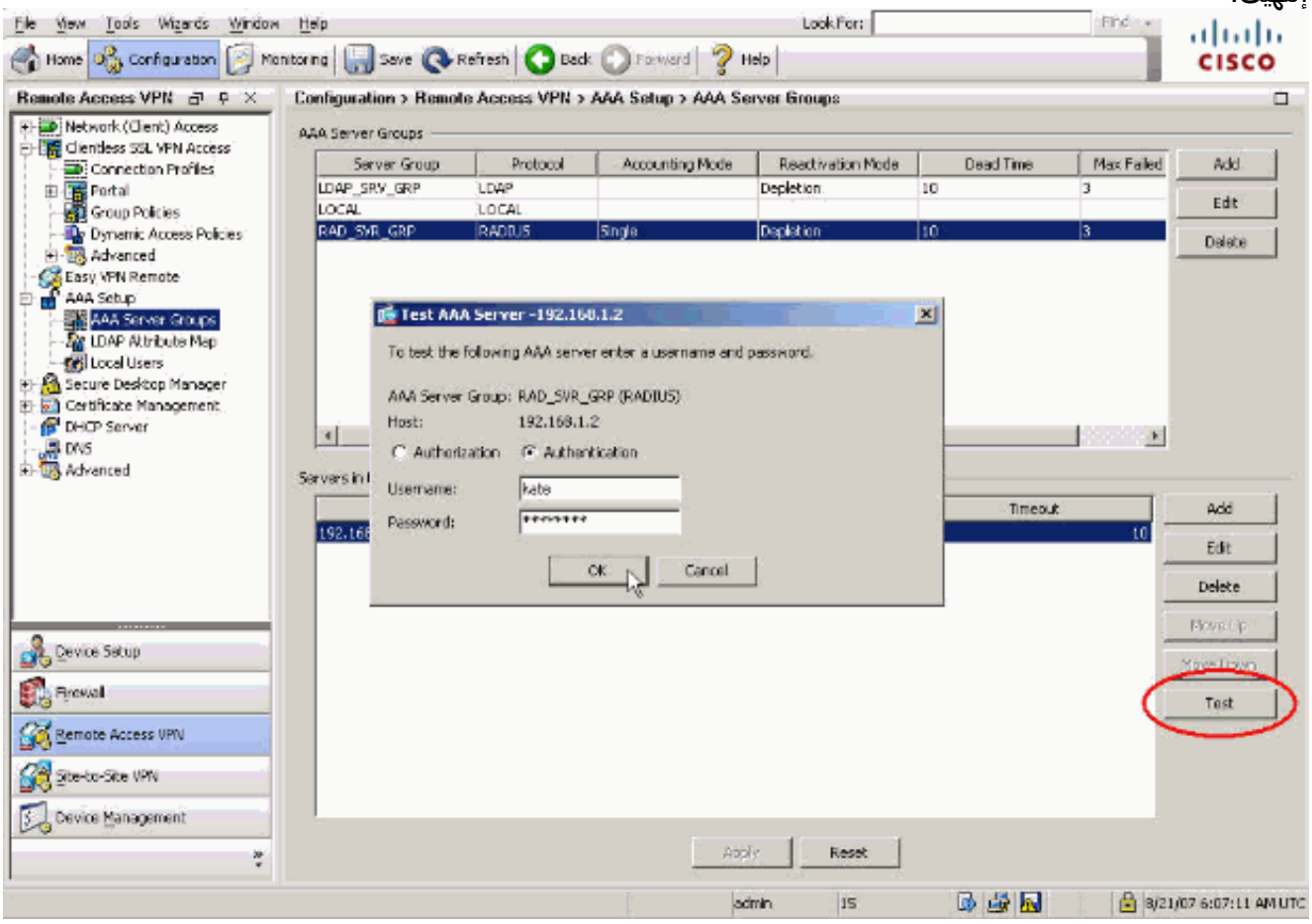
استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

إختبار مع ASDM

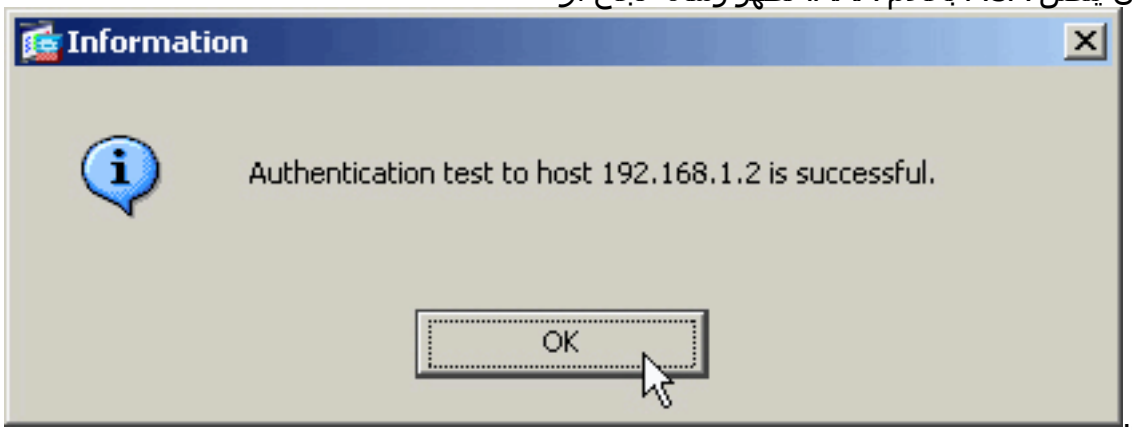
تحقق من تكوين RADIUS الخاص بك باستخدام الزر **Test** على شاشة تكوين مجموعات خوادم AAA. ما إن يزود

أنت username وكلمة، يسمح هذا زر أنت أن يرسل إختبار مصادقة طلب إلى ال ACS نادل.

1. أختر **تكوين > Remote Access VPN (الوصول عن بعد) > إعداد AAA > مجموعات خوادم AAA**.
2. حدد مجموعة خوادم AAA المطلوبة في الجزء العلوي.
3. حدد خادم AAA الذي تريد إختباره في الجزء السفلي.
4. انقر فوق زر **إختبار** الموجود على يمين الجزء السفلي.
5. في الإطار الذي يظهر، انقر زر **مصادقة** الراديو، وقم بتوفير المسوغات التي تريد إختبارها. طقطقة **ok** عندما إنتهيت.



6. بعد أن يتصل ASA بخادم AAA، تظهر رسالة نجاح أو



فشل.

إختبار مع CLI

يمكنك إستخدام الأمر **test** على سطر الأوامر لاختبار إعداد AAA الخاص بك. يتم إرسال طلب إختبار إلى خادم AAA، وتظهر النتيجة على سطر الأوامر.

```
ciscoasa#test aaa-server authentication RAD_SVR_GRP host 192.168.1.2 username kate password
```

cisco123
(INFO: Attempting Authentication test to IP address <192.168.1.2> (timeout: 12 seconds
INFO: Authentication Successful

استكشاف الأخطاء وإصلاحها

يمكن أن يساعدك الأمر **debug radius** على أستكشاف أخطاء المصادقة وإصلاحها في هذا السيناريو. يتيح هذا الأمر تصحيح جلسات RADIUS بالإضافة إلى فك تشفير حزمة RADIUS. في كل إخراج تصحيح أخطاء يتم تقديمه، فإن الحزمة الأولى التي تم فك ترميزها هي الحزمة التي يتم إرسالها من ASA إلى خادم ACS. الحزمة الثانية هي الاستجابة من خادم ACS.

ملاحظة: ارجع إلى معلومات مهمة حول أوامر التصحيح قبل إستخدام أوامر **debug**.

عندما تكون المصادقة ناجحة، يرسل خادم RADIUS رسالة **قبول الوصول**.

ciscoasa#**debug radius**

First Packet. Authentication Request. ciscoassa#radius mkreq: 0x88 alloc_rip 0xd5627ae4 new *---!*
request 0x88 --> 52 (0xd5627ae4) got user '' got password add_req 0xd5627ae4 session 0x88 id 52
RADIUS_REQUEST radius.c: rad_mkpkt RADIUS packet decode (authentication request) ----------
---------- Raw packet data (length = 62)..... 01 34 00 3e 18 71 56 d7 c4 ad e2 73
30 a9 2e cf | .4.>.qV....s0... 5c 65 3a eb 01 06 6b 61 74 65 02 12 0e c1 28 b7 |
\e:...kate....(. 87 26 ed be 7b 2c 7a 06 7c a3 73 19 04 06 c0 a8 | .&..{,z.|.s..... 01 01 05 06
00 00 00 34 3d 06 00 00 00 05 | ....4=..... Parsed packet data..... Radius: Code = 1 (0x01)
Radius: Identifier = 52 (0x34) Radius: Length = 62 (0x003E) Radius: Vector:
187156D7C4ADE27330A92ECF5C653AEB Radius: Type = 1 (0x01) User-Name Radius: Length = 6 (0x06)
Radius: Value (String) = 6b 61 74 65 | kate Radius: Type = 2 (0x02) User-Password Radius: Length
= 18 (0x12) Radius: Value (String) = 0e c1 28 b7 87 26 ed be 7b 2c 7a 06 7c a3 73 19 |
..(..&..{,z.|.s. Radius: Type = 4 (0x04) NAS-IP-Address Radius: Length = 6 (0x06) Radius: Value
(IP Address) = 192.168.1.1 (0xC0A80101) Radius: Type = 5 (0x05) NAS-Port Radius: Length = 6
(0x06) Radius: Value (Hex) = 0x34 Radius: Type = 61 (0x3D) NAS-Port-Type Radius: Length = 6
(0x06) Radius: Value (Hex) = 0x5 send pkt 192.168.1.2/1645 rip 0xd5627ae4 state 7 id 52
rad_vrfy() : response message verified rip 0xd544d2e8 : chall_state '' : state 0x7 : timer 0x0 :
reqauth: 18 71 56 d7 c4 ad e2 73 30 a9 2e cf 5c 65 3a eb : info 0x88 session_id 0x88 request_id
0x34 user 'kate' response '***' app 0 reason 0 skey 'secretkey' sip 192.168.1.2 type 1 *!---*
Second Packet. Authentication Response. RADIUS packet decode (response) ----------
---------- Raw packet data (length = 50)..... 02 34 00 32 35 a1 88 2f 8a bf 2a 14 c5 31 78
59 | .4.25../..*..1xY 60 31 35 89 08 06 ff ff ff ff 19 18 43 41 43 53 | `15.........CACS 3a 30
2f 32 61 36 2f 63 30 61 38 30 31 30 31 2f | :0/2a6/c0a80101/ 35 32 | 52 Parsed packet data.....
Radius: Code = 2 (0x02) Radius: Identifier = 52 (0x34) Radius: Length = 50 (0x0032) Radius:
Vector: 35A1882F8ABF2A14C531785960313589 Radius: Type = 8 (0x08) Framed-IP-Address Radius:
Length = 6 (0x06) Radius: Value (IP Address) = 255.255.255.255 (0xFFFFFFFF) Radius: Type = 25
(0x19) Class Radius: Length = 24 (0x18) Radius: Value (String) = 43 41 43 53 3a 30 2f 32 61 36
2f 63 30 61 38 30 | CACS:0/2a6/c0a80 31 30 31 2f 35 32 | 101/52 **rad_procpkt: ACCEPT**
RADIUS_ACCESS_ACCEPT: normal termination
RADIUS_DELETE
remove_req 0xd5627ae4 session 0x88 id 52
free_rip 0xd5627ae4
radius: send queue empty

عند فشل المصادقة، يرسل خادم ACS رسالة **رفض الوصول**.

ciscoasa#**debug radius**

First Packet. Authentication Request. ciscoasa# radius mkreq: 0x85 alloc_rip 0xd5627ae4 new *---!*
request 0x85 --> 49 (0xd5627ae4) got user '' got password add_req 0xd5627ae4 session 0x85 id 49
RADIUS_REQUEST radius.c: rad_mkpkt RADIUS packet decode (authentication request) ----------

```
---------- Raw packet data (length = 62)..... 01 31 00 3e 88 21 46 07 34 5d d2 a3
                a0 59 1e ff | .1.>.!F.4]...Y.. cc 15 2a 1b 01 06 6b 61 74 65 02 12 60 eb 05 32 |
..*...kate..`..2 87 69 78 a3 ce d3 80 d8 4b 0d c3 37 04 06 c0 a8 | .ix.....K..7.... 01 01 05 06
 00 00 00 31 3d 06 00 00 00 05 | .......1=..... Parsed packet data..... Radius: Code = 1 (0x01)
                    Radius: Identifier = 49 (0x31) Radius: Length = 62 (0x003E) Radius: Vector:
    88214607345DD2A3A0591EFFCC152A1B Radius: Type = 1 (0x01) User-Name Radius: Length = 6 (0x06)
Radius: Value (String) = 6b 61 74 65 | kate Radius: Type = 2 (0x02) User-Password Radius: Length
          = 18 (0x12) Radius: Value (String) = 60 eb 05 32 87 69 78 a3 ce d3 80 d8 4b 0d c3 37 |
 `..2.ix.....K..7 Radius: Type = 4 (0x04) NAS-IP-Address Radius: Length = 6 (0x06) Radius: Value
     (IP Address) = 192.168.1.1 (0xC0A80101) Radius: Type = 5 (0x05) NAS-Port Radius: Length = 6
     (0x06) Radius: Value (Hex) = 0x31 Radius: Type = 61 (0x3D) NAS-Port-Type Radius: Length = 6
         (0x06) Radius: Value (Hex) = 0x5 send pkt 192.168.1.2/1645 rip 0xd5627ae4 state 7 id 49
rad_vrfy() : response message verified rip 0xd544d2e8 : chall_state '' : state 0x7 : timer 0x0 :
 reqauth: 88 21 46 07 34 5d d2 a3 a0 59 1e ff cc 15 2a 1b : info 0x85 session_id 0x85 request_id
     0x31 user 'kate' response '***' app 0 reason 0 skey 'secretkey' sip 192.168.1.2 type 1 !---
Second packet. Authentication Response. RADIUS packet decode (response) ----------------------
  -------------- Raw packet data (length = 32)..... 03 31 00 20 70 98 50 af 39 cc b9 ba df a7 bd
 ff | .1. p.P.9....... 06 af fb 02 12 0c 52 65 6a 65 63 74 65 64 0a 0d | ......Rejected.. Parsed
     packet data..... Radius: Code = 3 (0x03) Radius: Identifier = 49 (0x31) Radius: Length = 32
(0x0020) Radius: Vector: 709850AF39CCB9BADFA7BDFF06AFFB02 Radius: Type = 18 (0x12) Reply-Message
                                                 = (Radius: Length = 12 (0x0C) Radius: Value (String
                                        ..6a 65 63 74 65 64 0a 0d                    |  Rejected 65 52
                                                                                  rad_procpkt: REJECT
                                                                                       RADIUS_DELETE
                                                                    remove_req 0xd5627ae4 session 0x85 id 49
                                                                                  free_rip 0xd5627ae4
                                                                              radius: send queue empty
```

معلومات ذات صلة

- خدمة مصادقة طلب اتصال المستخدم البعيد (RADIUS)
- 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).