TACACS+ على نقطة وصول Aironet لمصادقة تسجيل الدخول باستخدام مثال تكوين واجهة المستخدم الرسومية

المحتويات

المقدمة

يشرح هذا المستند كيفية تمكين خدمات TACACS+ (TACACS+) على نقطة وصول Cisco Aironet (AP) لإجراء مصادقة تسجيل الدخول باستخدام خادم TACACS+.

المتطلبات الأساسية

المتطلبات

تأكد من استيفاء المتطلبات التالية قبل أن تحاول إجراء هذا التكوين:

- معرفة كيفية تكوين المعلمات الأساسية على نقاط الوصول من Aironet
- معرفة كيفية تكوين خادم TACACS+ مثل خادم التحكم في الوصول الآمن (ACS) من Cisco
- معرفة مفاهيم TACACS+

لمزيد من المعلومات حول كيفية عمل TACACS+، ارجع إلى قسم *فهم TACACS+* في تكوين خوادم RADIUS و TACACS+.

المكونات المستخدمة

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

- نقاط الوصول اللاسلكية Aironet 1240 / 1140 Series
- ACS الذي يشغل الإصدار 4.1 من البرنامج
- ACS الذي يشغل الإصدار 5.2 من البرنامج

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 مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

الاصطلاحات

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

التكوين

يشرح هذا القسم كيفية تكوين نقطة الوصول Aironet وخادم ACS) +TACACS) لمصادقة تسجيل الدخول المستندة إلى TACACS+.

يستخدم مثال التكوين هذا المعلمات التالية:

- عنوان IP الخاص ب ACS—172.16.1.1/255.255.0.0
- عنوان IP الخاص ب AP—172.16.1.30/255.255.0.0
- مفتاح سري مشترك يتم إستخدامه على نقطة الوصول وخادم TACACS+— **مثال**

هذه هي بيانات اعتماد المستخدم التي يقوم هذا المثال بتكوينها على ACS:

- username—**user1**
- كلمة السر—**Cisco**
- Group— **AdminUsers**

تحتاج إلى تكوين ميزات TACACS+ للتحقق من المستخدمين الذين يحاولون الاتصال بنقطة الوصول (AP) إما من خلال واجهة الويب أو من خلال واجهة سطر الأوامر (CLI). in order to أنجزت هذا تشكيل، أنت ينبغي أنجزت هذا مهمة:

1. قم بتكوين خادم TACACS+ لمصادقة تسجيل الدخول.
2. قم بتكوين نقطة الوصول Aironet لمصادقة TACACS+.

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

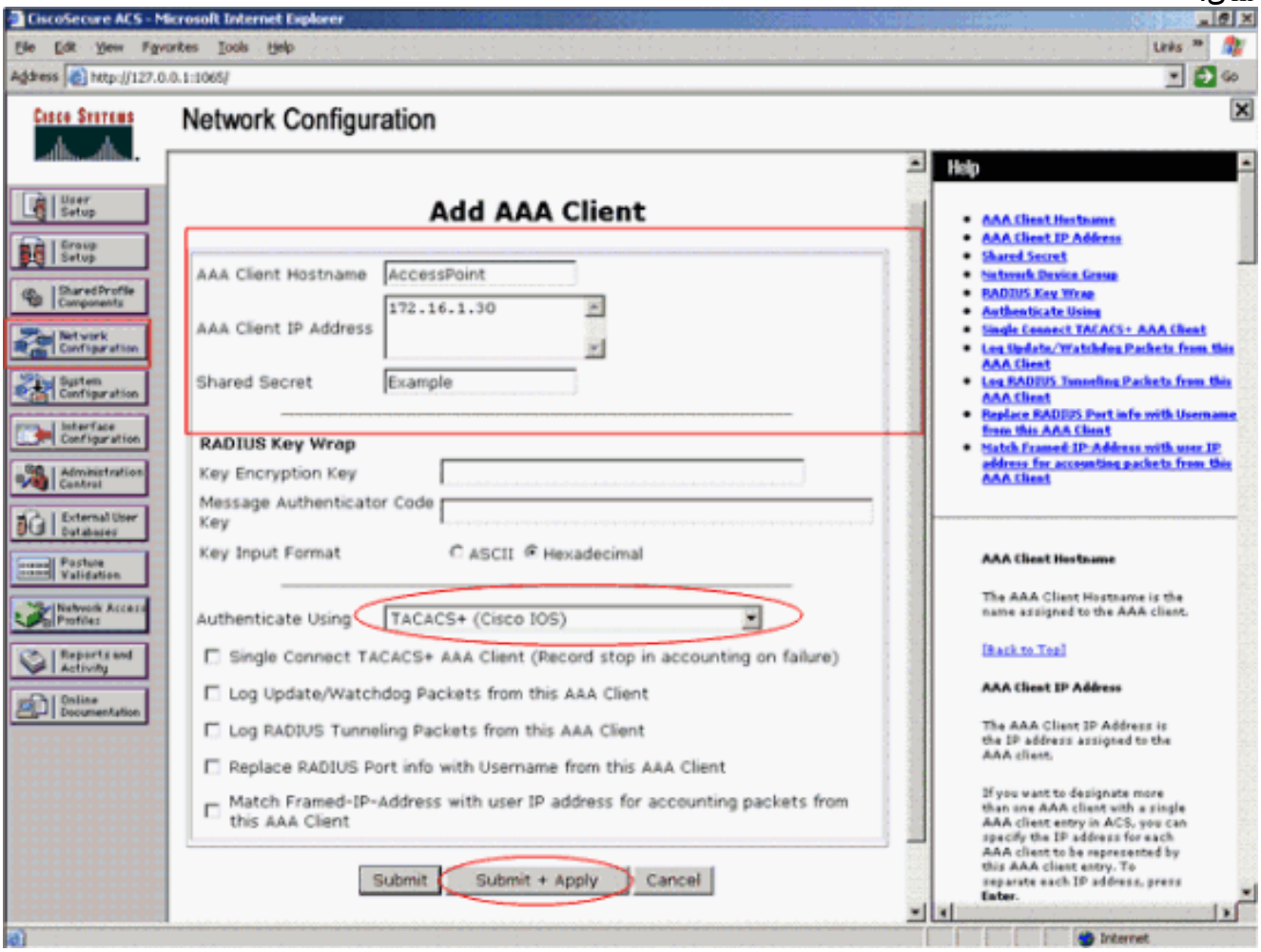
الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة التالي:

قم بتكوين خادم TACACS+ لمصادقة تسجيل الدخول - باستخدام ACS 4.1

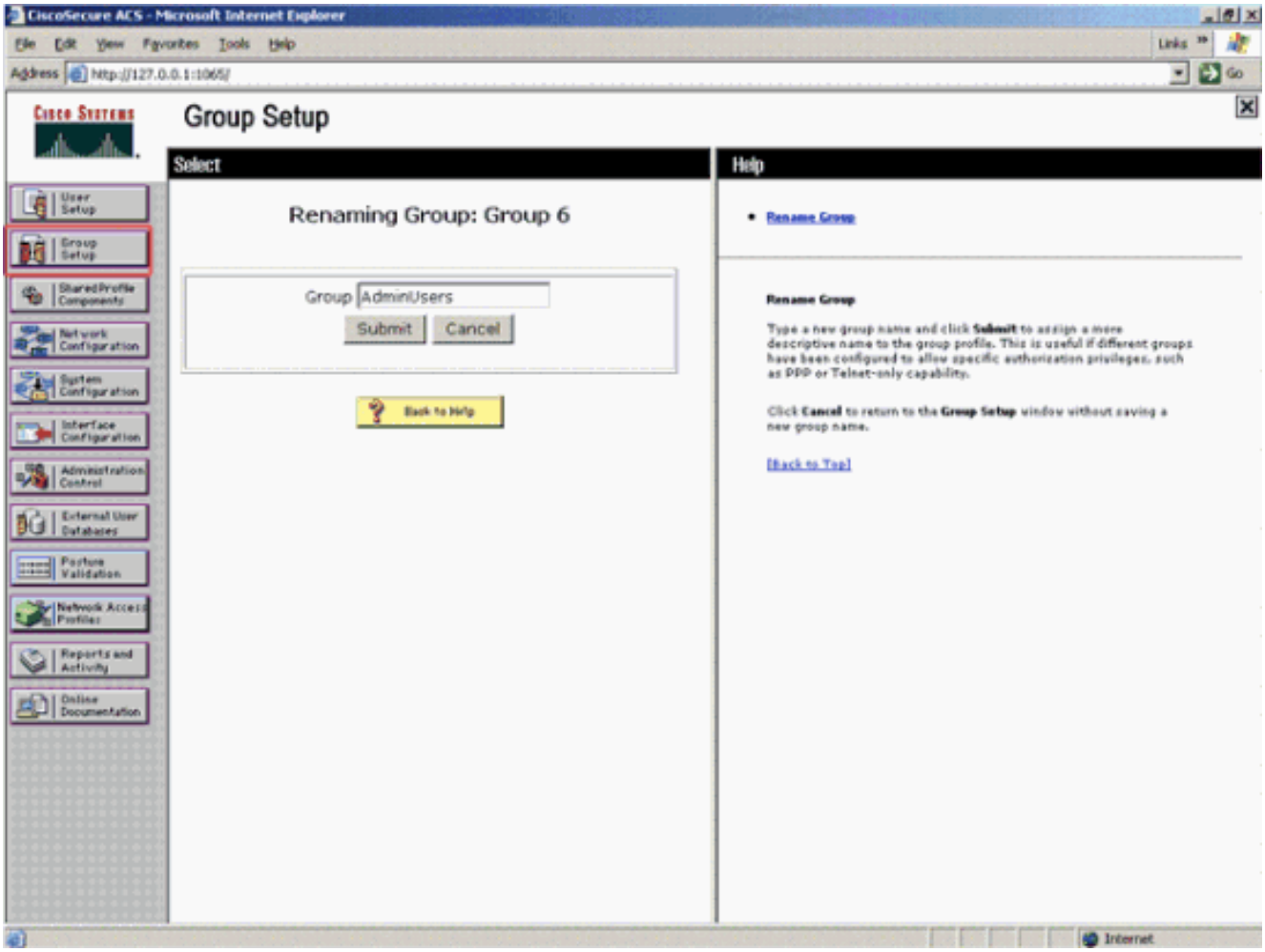
تتمثل الخطوة الأولى في إعداد برنامج اتصال TACACS+ للتحقق من المستخدمين الذين يحاولون الوصول إلى نقطة الوصول. يجب عليك إعداد ACS لمصادقة TACACS+ وإنشاء قاعدة بيانات مستخدم. يمكنك إستخدام أي خادم TACACS+. يستخدم هذا المثال ACS كخادم TACACS+. أكمل الخطوات التالية:

1. أتمت هذا steps in order to أضفت ال ap كمصادقة، تخويل، ومحاسبة (AAA) زبون:من واجهة المستخدم الرسومية (ACS)، انقر فوق علامة التبويب **تكوين الشبكة**.تحت عملاء AAA، انقر فوق **إضافة إدخال**.في نافذة إضافة عميل AAA، أدخل اسم مضيف AP وعنوان IP الخاص بنقطة الوصول ومفتاح سري مشترك.يجب أن يكون هذا المفتاح السري المشترك هو نفسه المفتاح السري المشترك الذي تقوم بتكوينه على نقطة الوصول.من القائمة المنسدلة مصادقة باستخدام، حدد **TACACS+ (Cisco IOS)**.انقر فوق **إرسال + إعادة تشغيل** لحفظ التكوين.فيما يلي
مثال:

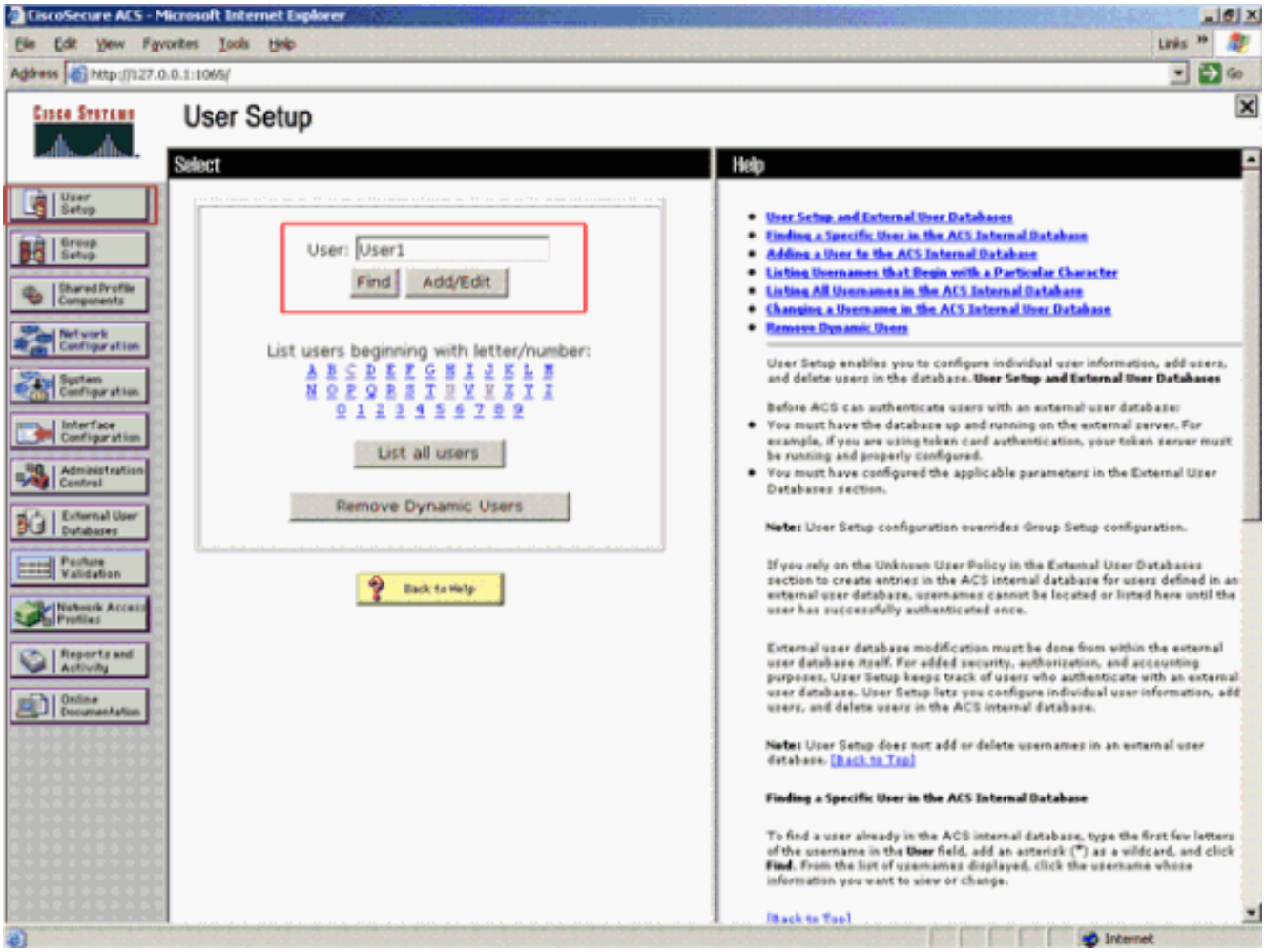


يستخدم هذا المثال:نقطة **الوصول** إلى اسم المضيف لعميل AAAالعنوان **16/172.16.1.30** كعنوان IP لعميل AAA**مثال** المفتاح السري المشترك

2. أتمت هذا steps in order to خلقت مجموعة أن يحتوي كل ال مدير مستعمل:انقر فوق **إعداد المجموعة** من القائمة الموجودة على اليسار.تظهر نافذة جديدة.في نافذة "إعداد المجموعة"، حدد مجموعة لتكوينها من القائمة المنسدلة وانقر فوق **إعادة تسمية مجموعة**.يحدد هذا المثال المجموعة 6 من القائمة المنسدلة ويعيد تسمية AdminUsers للمجموعة.انقر على **إرسال**.فيما يلي
مثال:

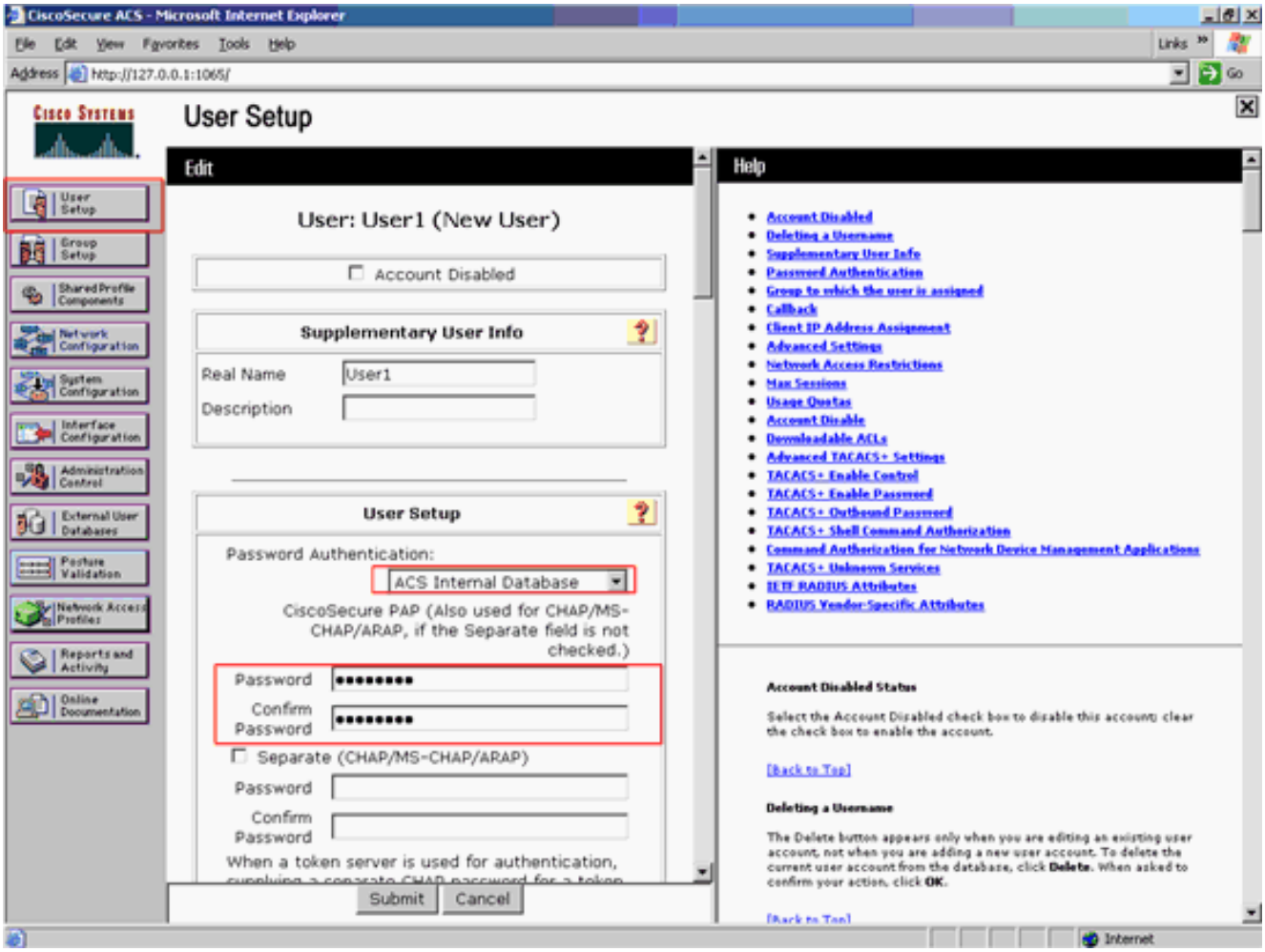


3. أكمل الخطوات التالية لإضافة المستخدمين إلى قاعدة بيانات TACACS+:انقر فوق علامة التبويب **إعداد المستخدم**.دخلت in order to خلقت جديد مستعمل، ال username في المستعمل مجال وطقطقة **يضيف/يحرر**.فيما يلي مثال، ينشئ **User1**:

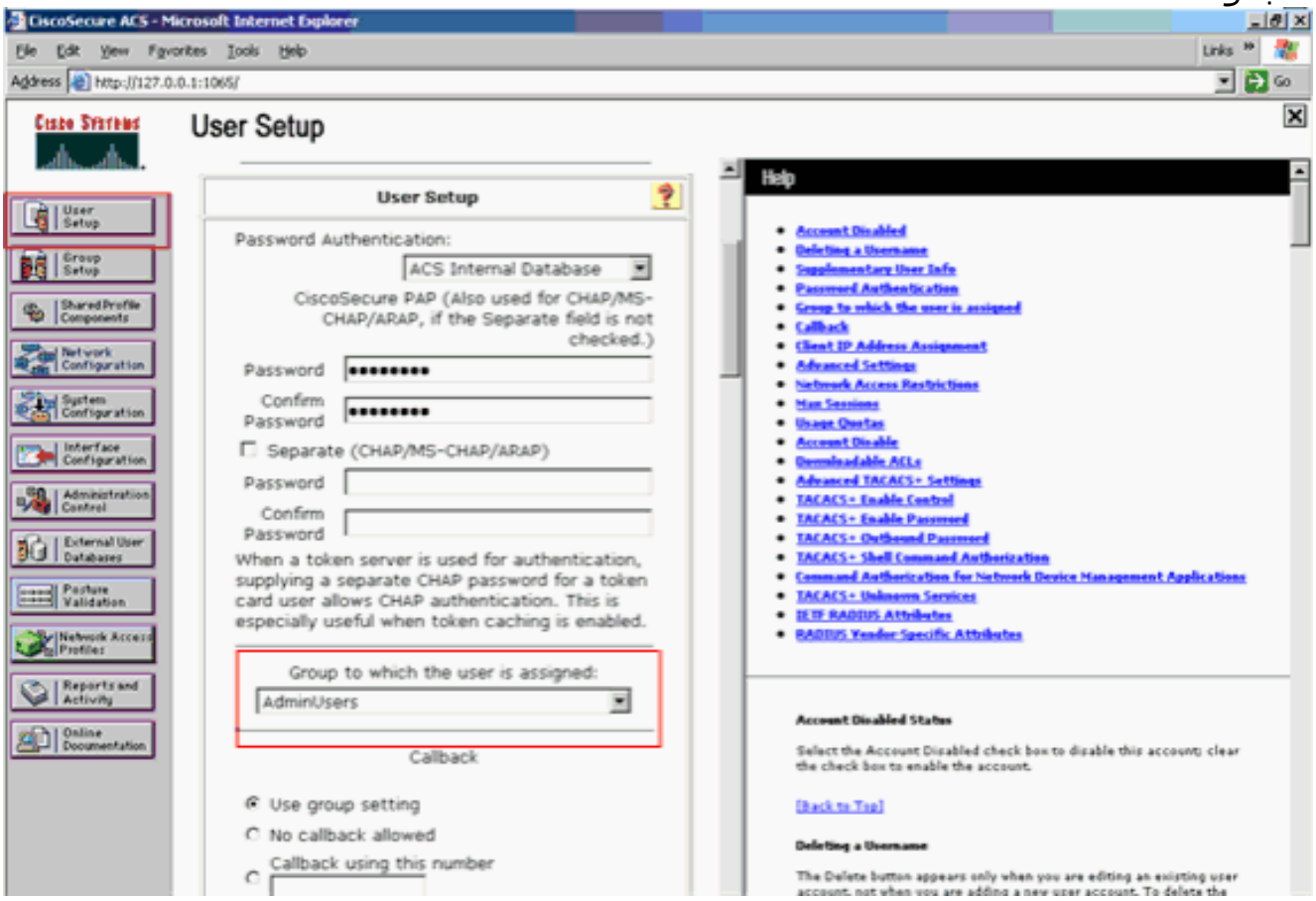


بعد النقر فوق إضافة/تحرير ، تظهر نافذة إضافة/تحرير لهذا المستخدم.

4. أدخل بيانات الاعتماد الخاصة بهذا المستخدم وانقر فوق **إرسال** لحفظ التكوين.تتضمن بيانات الاعتماد التي يمكنك إدخالها:معلومات المستخدم التكميليةإعداد المستخدمالمجموعة التي تم تعيين المستخدم إليهافيما يلي مثال:

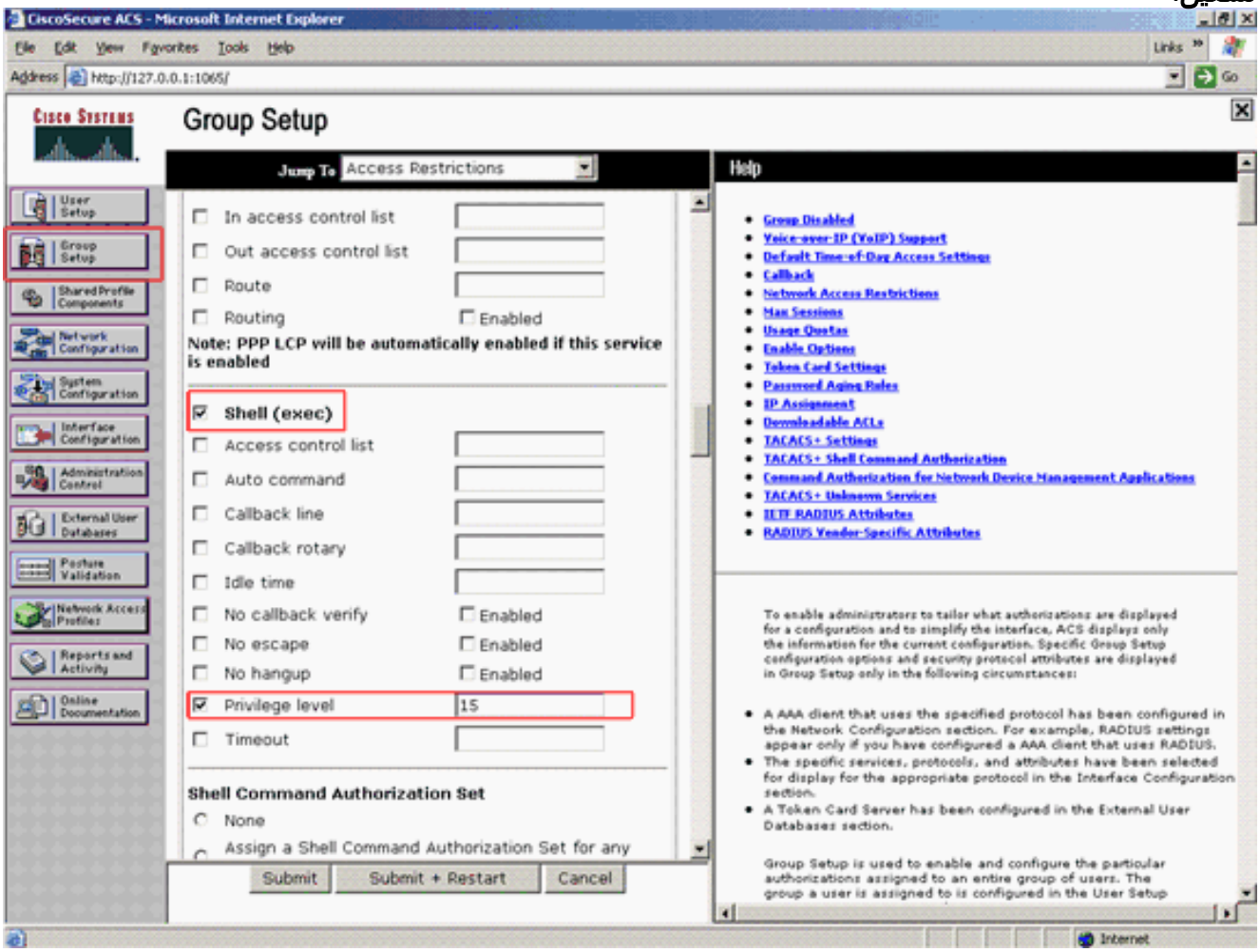


يمكنك ملاحظة أن هذا المثال يضيف المستخدم User1 إلى AdminUsers في المجموعة.



ملاحظة: إذا لم تقم بإنشاء مجموعة معينة، يتم تعيين المستخدمين للمجموعة الافتراضية.

أتمت هذا steps in order to عينت الامتياز مستوى:انقر فوق علامة التبويب **إعداد المجموعة**.حدد المجموعة 5. التي قمت بتعيينها مسبقا لهذا المستخدم وانقر فوق **تحرير الإعدادات**.يستخدم هذا المثال AdminUsers للمجموعة.ضمن إعدادات TACACS+، حدد خانة الاختيار **طبقة (exec)** وحدد خانة الاختيار **مستوى الامتياز** التي تحتوي على قيمة 15.انقر فوق **إرسال + إعادة تشغيل**.



ملاحظة: يجب تحديد مستوى الامتياز 15 لواجهة المستخدم الرسومية (GUI) وبرنامج Telnet لكي يمكن الوصول إليه كمستوى 15. وإلا، بشكل افتراضي، يمكن للمستخدم الوصول إلى المستوى 1 فقط. إن لا يعرف مستوى الامتياز يكون والمستعمل يحاول أن يدخل أسلوب enable على ال CLI (مع إستعمال من telnet)، ال ap يعرض هذا خطأ رسالة:

```
AccessPoint>enable
Error in authentication %
```

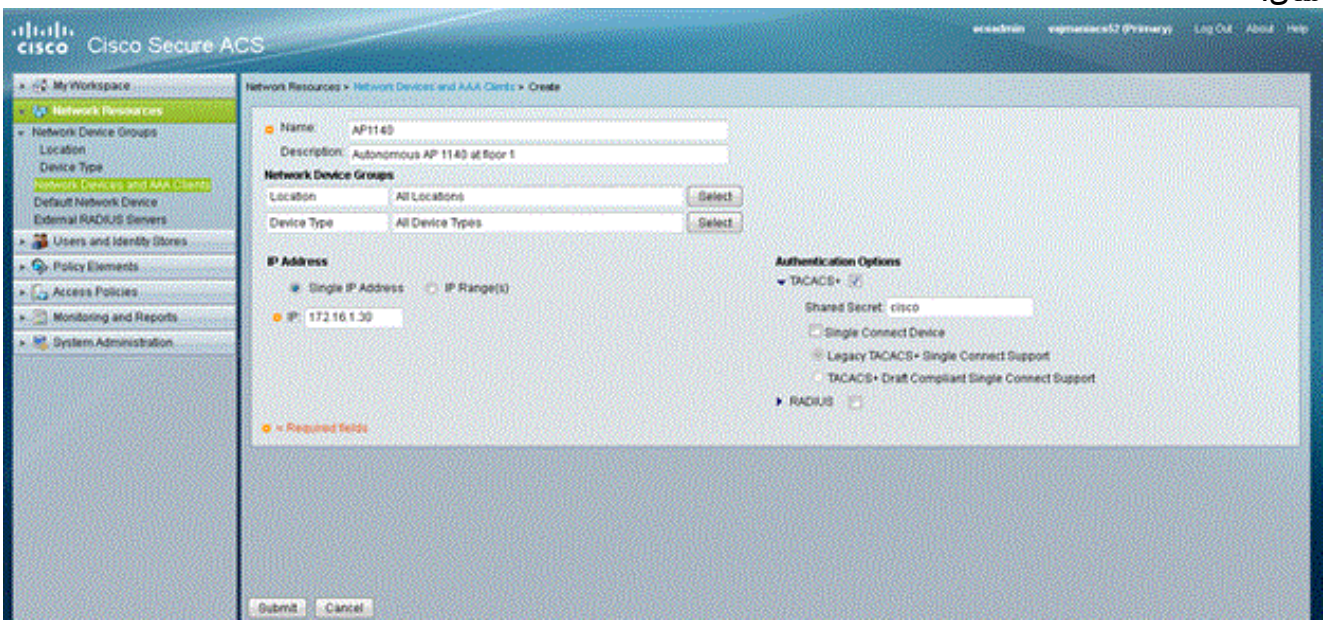
كرر الخطوات من 2 إلى 4 من هذا الإجراء إذا كنت تريد إضافة المزيد من المستخدمين إلى قاعدة بيانات TACACS+. بعد اكتمال هذه الخطوات، يكون خادم TACACS+ جاهزا للتحقق من المستخدمين الذين يحاولون تسجيل الدخول إلى نقطة الوصول. الآن، يجب عليك تكوين نقطة الوصول لمصادقة TACACS+.

قم بتكوين خادم TACACS+ لمصادقة تسجيل الدخول - باستخدام ACS 5.2

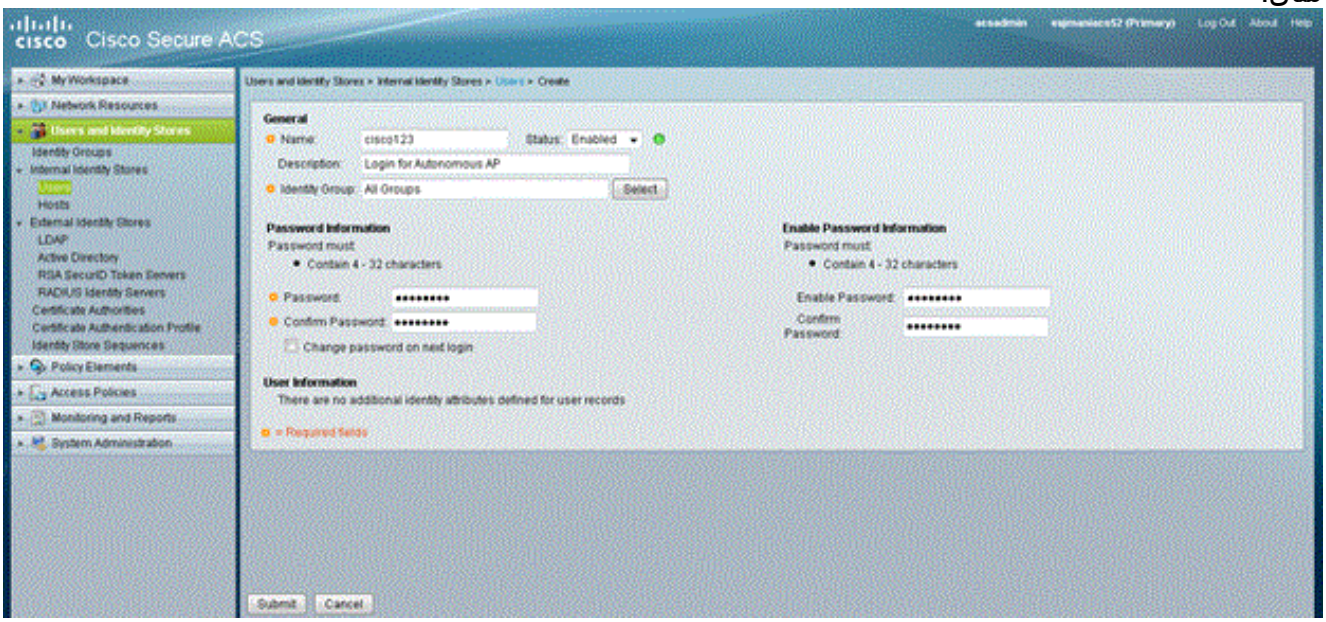
تتمثل الخطوة الأولى في إضافة نقطة الوصول كعميل AAA في ACS وإنشاء سياسة TACACS لتسجيل الدخول.

1. أتمت هذا steps in order to أضفت AP كعميل AAA:من واجهة المستخدم الرسومية (ACS)، انقر فوق **موارد الشبكة**، ثم انقر فوق **أجهزة الشبكة وعملاء AAA**.تحت أجهزة الشبكة، انقر فوق **إنشاء**.أدخل اسم المضيف لنقطة الوصول في **الاسم**، وقدم وصفا لنقطة الوصول.حدد **الموقع** و**نوع الجهاز** إذا كانت هذه الفئات محددة.بسبب تكوين نقطة وصول واحدة فقط، انقر فوق **عنوان IP واحد**. يمكنك إضافة نطاق عناوين IP لنقاط الوصول المتعددة بالنقر فوق **نطاق (نطاقات) IP**. بعد ذلك، أدخل عنوان IP لنقطة الوصول.تحت **خيارات**

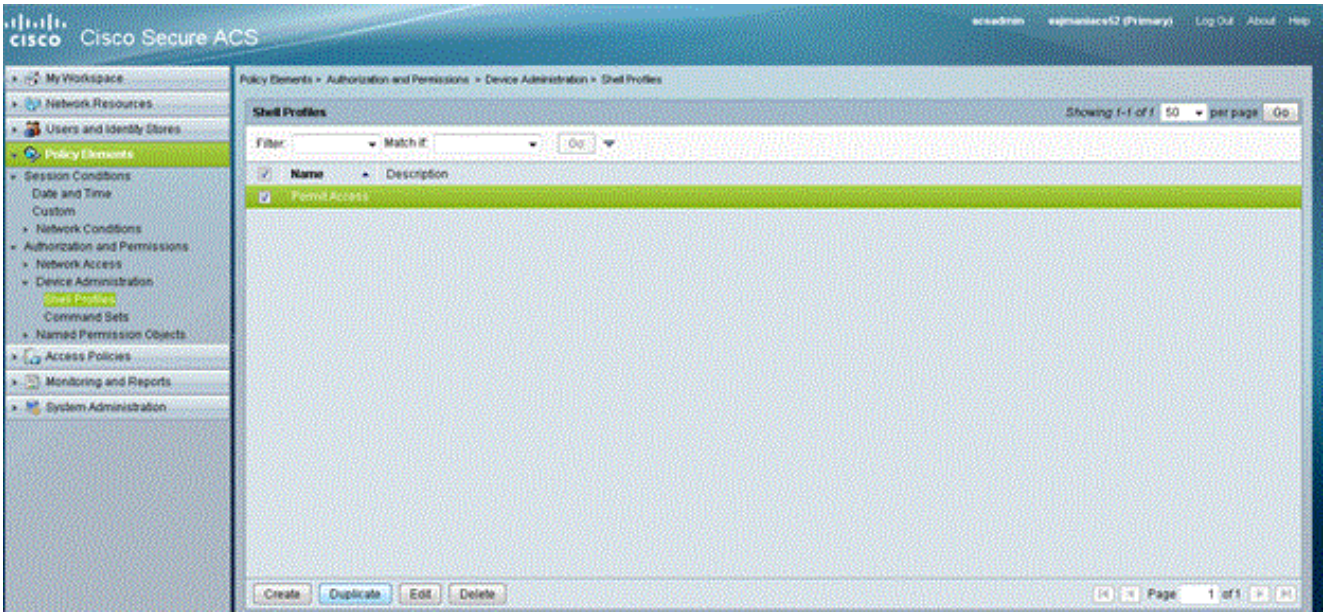
المصادقة، حدد مربع **TACACS+** وأدخل **السر المشترك**.فيما يلي
مثال:



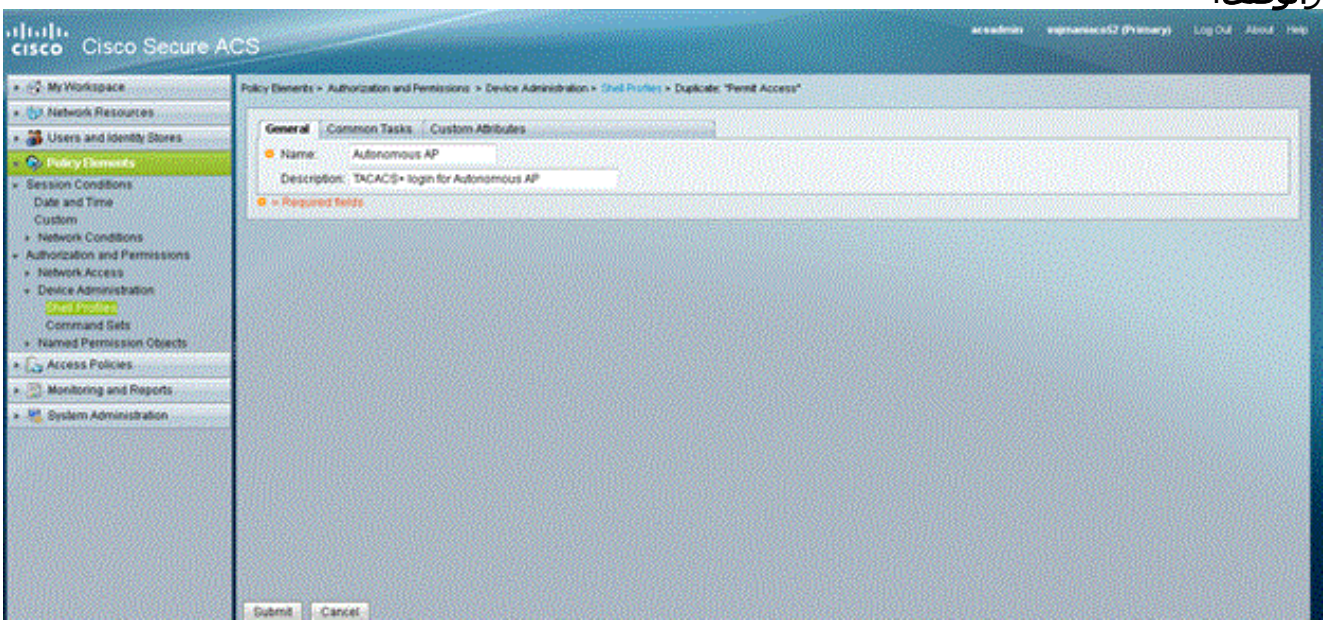
2. تتمثل الخطوة التالية في إنشاء اسم مستخدم وكلمة مرور لتسجيل الدخول:انقر فوق **المستخدمين ومخازن الهوية**، ثم انقر فوق **المستخدمين**.طقطقة **يخلق**.امنح اسم المستخدم تحت **الاسم**، وتقديم وصف.حدد **مجموعة الهوية**، إن وجدت.أدخل كلمة المرور تحت مربع نص **كلمة المرور**، وأعد الإدخال تحت **تأكيد كلمة المرور**.أنت يستطيع عدلت ال enable كلمة ب يدخل كلمة تحت **يمكن كلمة**. أعد الإدخال للتأكيد.فيما يلي
مثال:



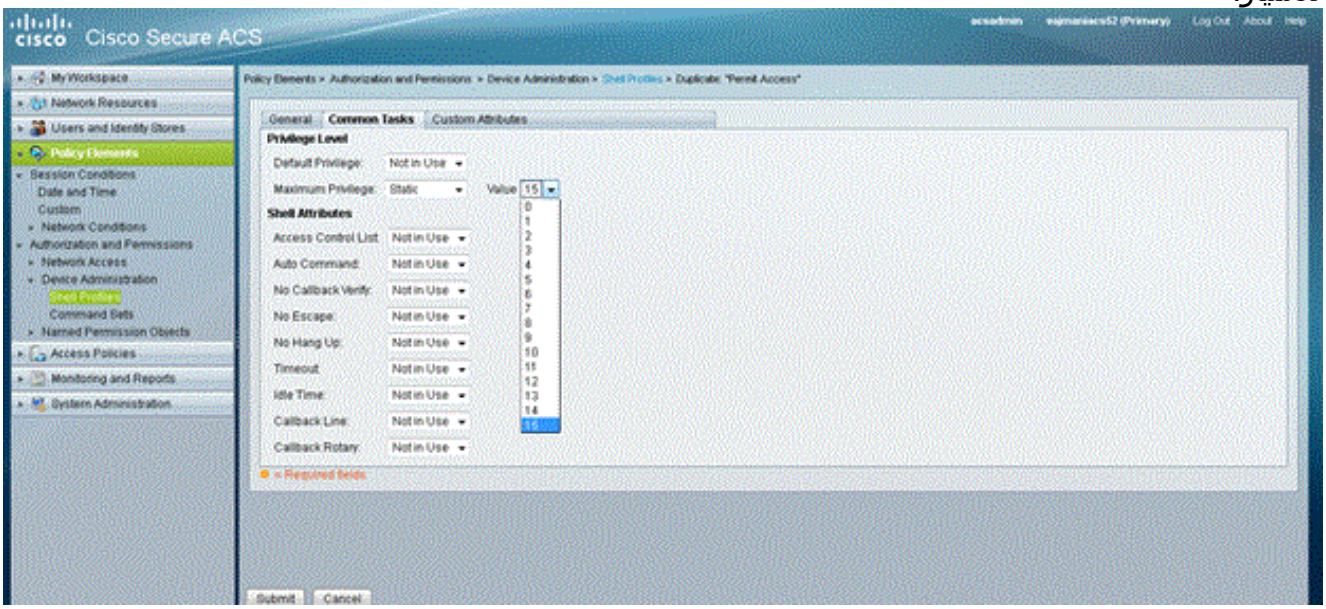
3. أتمت هذا steps in order to عينت الامتياز مستوى:انقر على **عناصر السياسة>أذون وأذونات>إدارة الأجهزة>توصيفات Shell**.حدد خانة الاختيار **السماح بالوصول** وانقر فوق **مضاعفة**.



أدخل **الاسم** و**الوصف**.

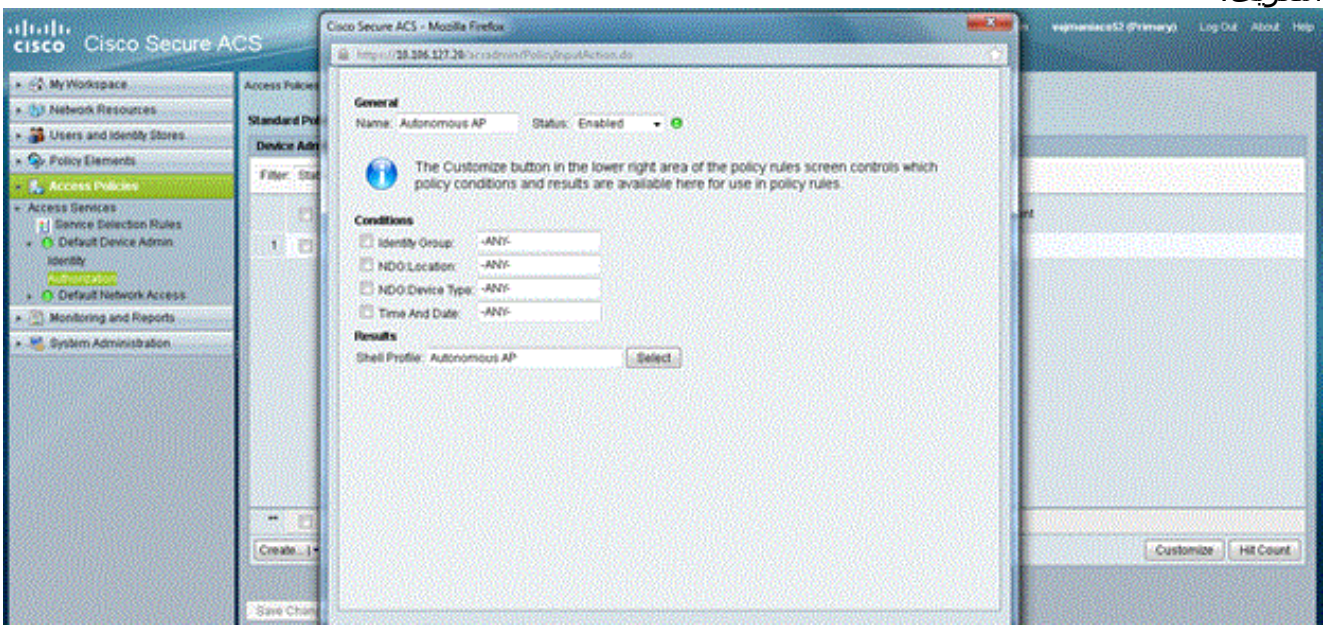


حدد علامة التبويب "مهام مشتركة" واختر **15** للحصول على الحد الأقصى للامتياز.

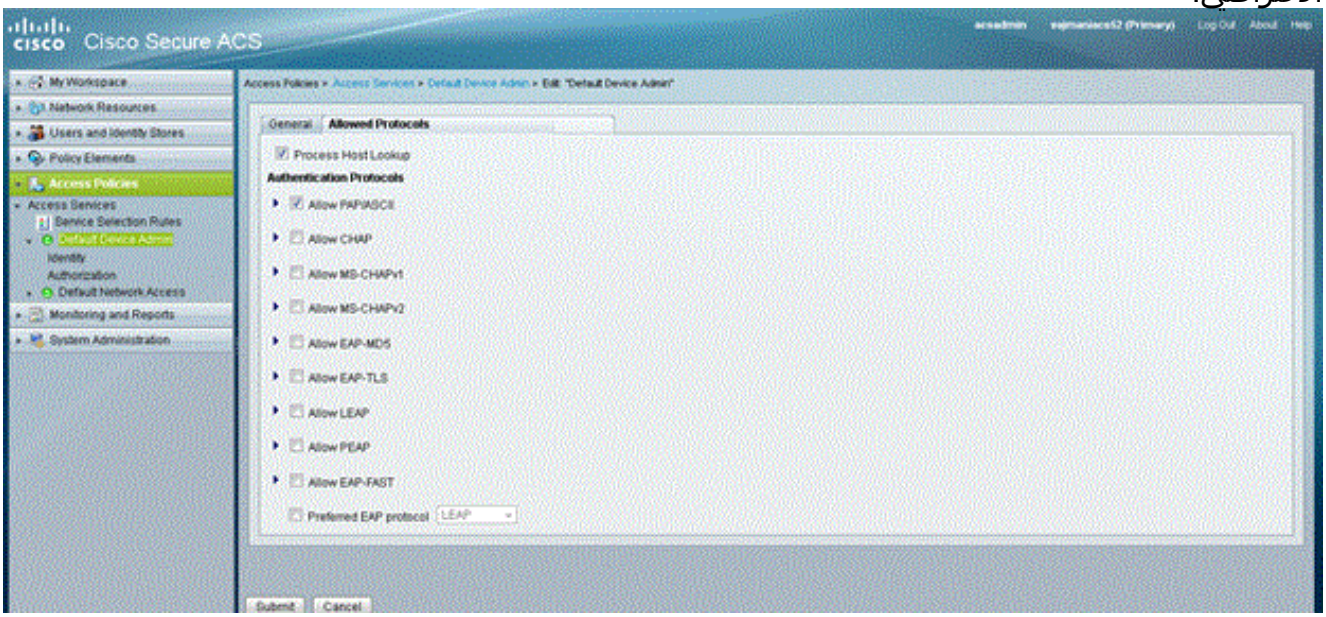


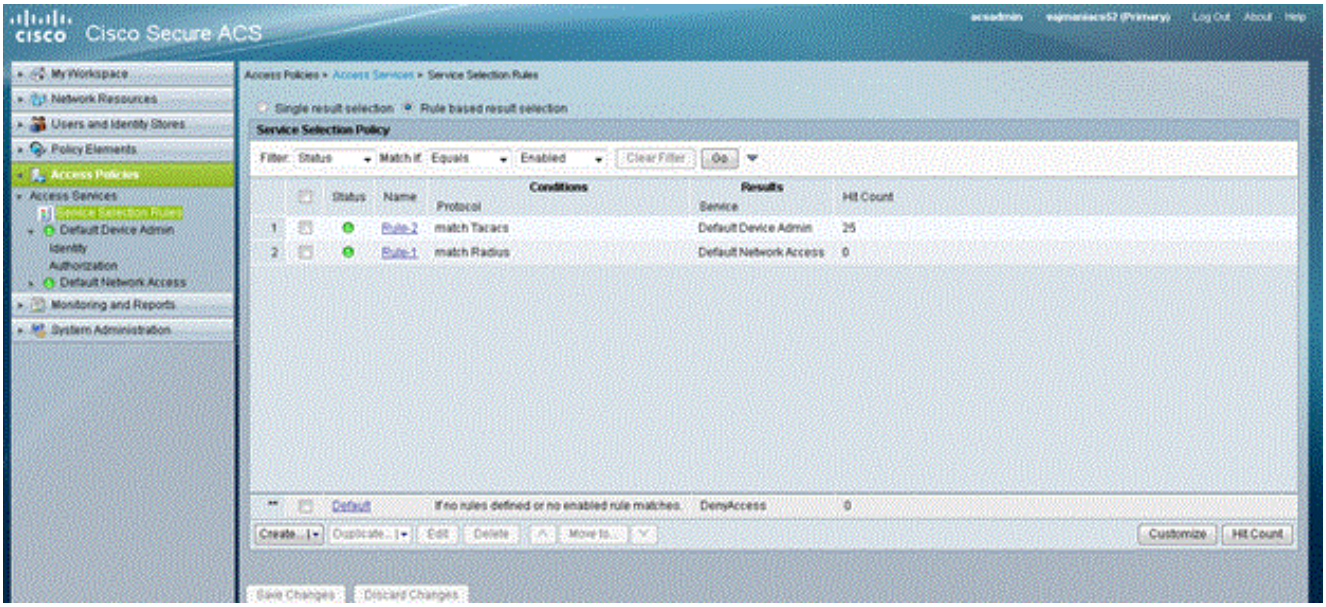
انقر على **إرسال**.

4. أكمل الخطوات التالية لإنشاء نهج تخويل:انقر فوق **سياسات الوصول>خدمات الوصول>مسؤول الجهاز الافتراضي>التفويض**.انقر فوق **إنشاء** لإنشاء نهج تخويل جديد.يظهر منبثق جديد لإنشاء قواعد لنهج التخويل.حدد **مجموعة الهوية**، **الموقع** وما إلى ذلك لاسم المستخدم المحدد وعميل AAA) AP)، إن وجد.انقر على **تحديد** لملف تعريف Shell لاختيار نقطة الوصول المستقلة التي تم إنشاؤها لملف التعريف.



بمجرد القيام بذلك، انقر فوق **حفظ التغييرات**.انقر فوق **مسؤول الجهاز الافتراضي** ، ثم انقر فوق **البروتوكولات المسموح بها**.تحقق من **السماح ب PAP/ASCII**، ثم انقر فوق **إرسال**.انقر فوق **قواعد تحديد الخدمة** للتأكد من وجود قاعدة تطابق TACACS وتشير إلى مسؤول الجهاز الافتراضي.



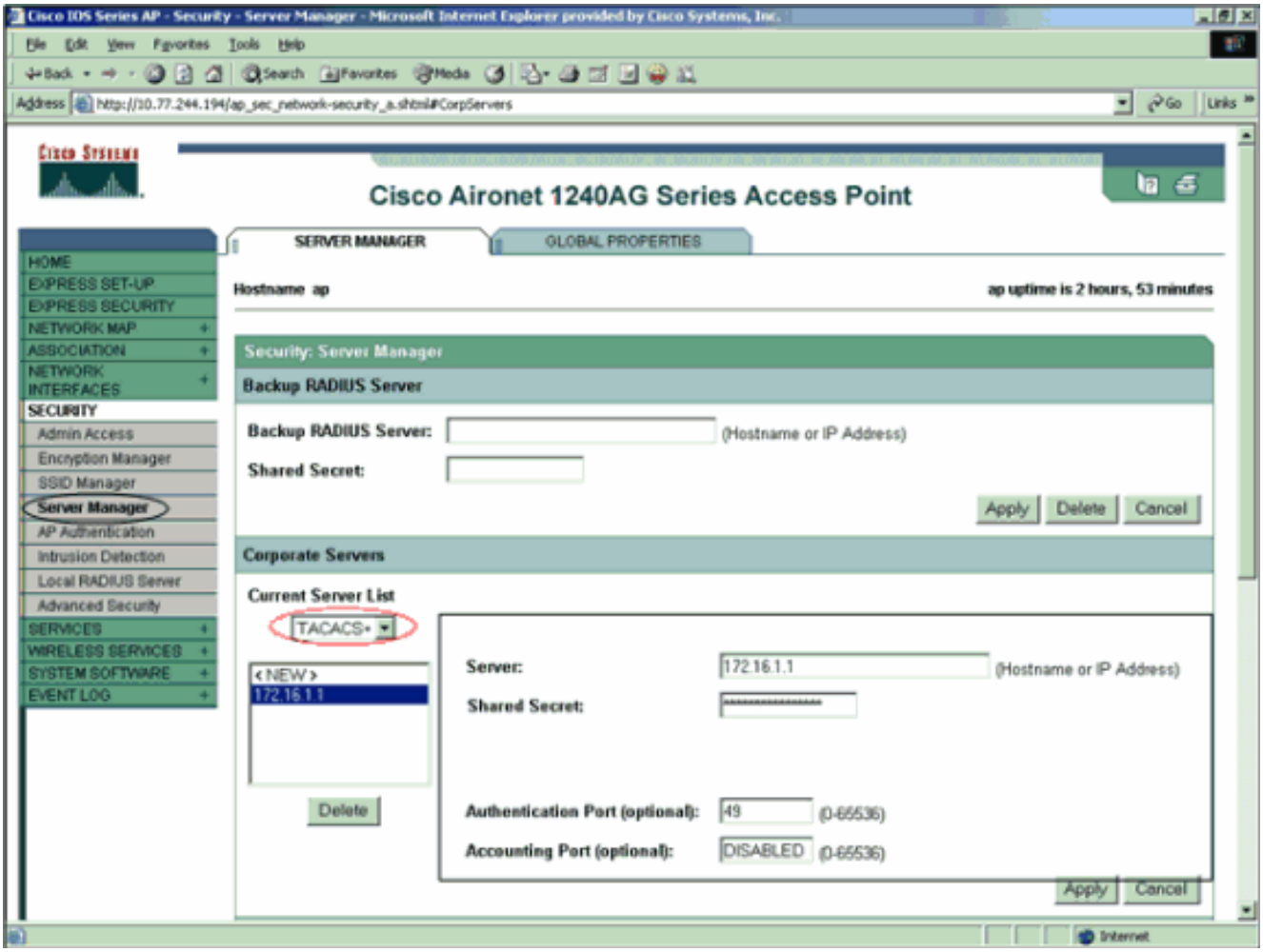


تكوين نقطة الوصول Aironet لمصادقة TACACS+

يمكنك إستخدام إما CLI أو GUI لتمكين ميزات TACACS+ على نقطة الوصول Aironet AP. يشرح هذا القسم كيفية تكوين نقطة الوصول لمصادقة تسجيل الدخول إلى TACACS+ باستخدام واجهة المستخدم الرسومية (GUI).

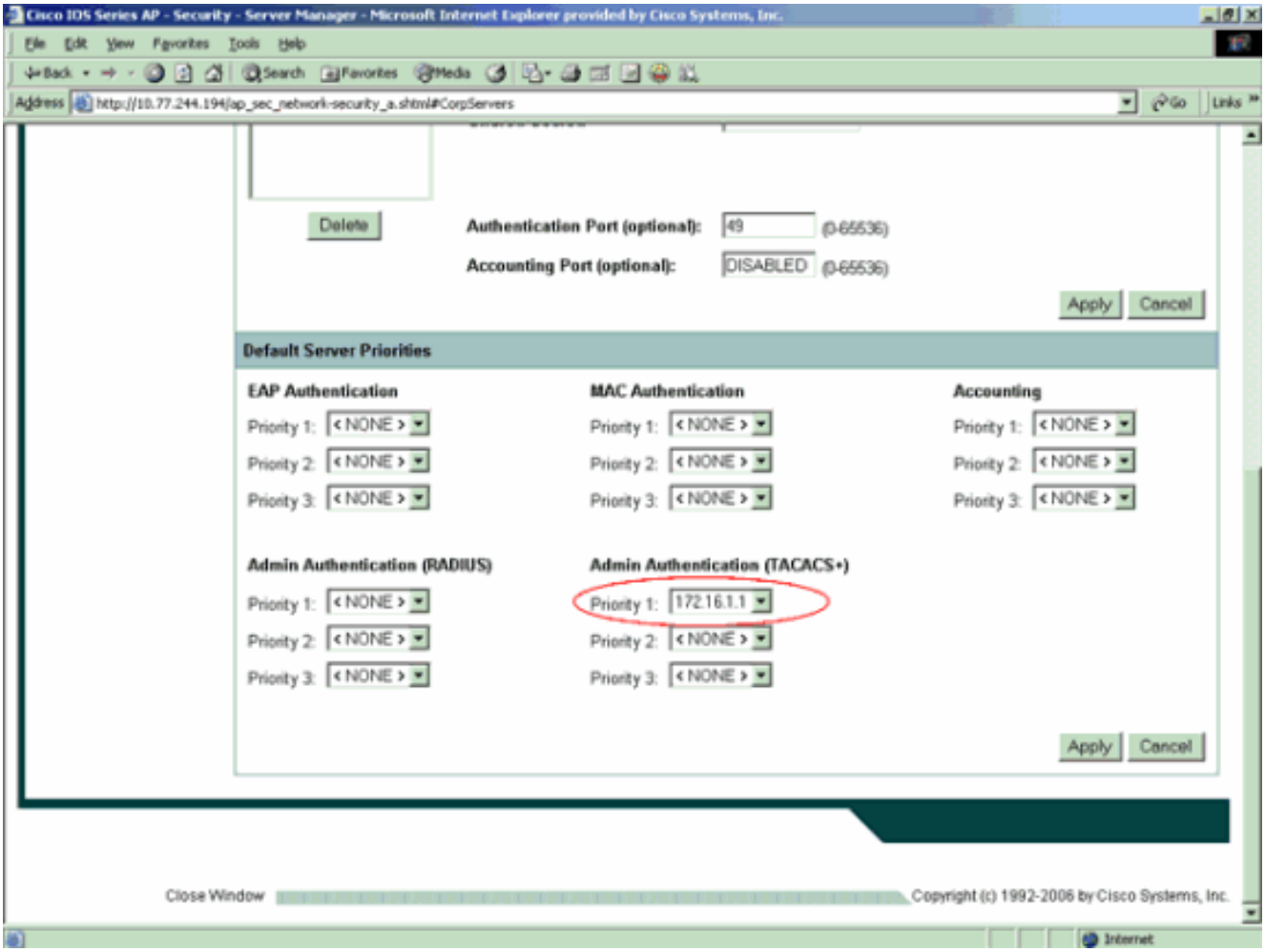
أتمت هذا steps in order to شكلت TACACS+ على ال ap مع إستعمال ال gui:

1. أكمل الخطوات التالية لتحديد معلمات خادم TACACS+:من واجهة المستخدم الرسومية (GUI) لنقطة الوصول، أختر **التأمين > مدير الخادم**.يظهر نافذة Security: Server Manager.في منطقة "خوادم الشركة"، حدد **TACACS+** من القائمة المنسدلة لقائمة الخوادم الحالية.في هذه المنطقة نفسها، أدخل عنوان IP والسر المشترك ورقم منفذ المصادقة لخادم TACACS+.طقطقة **يطبق**.فيما يلي مثال:

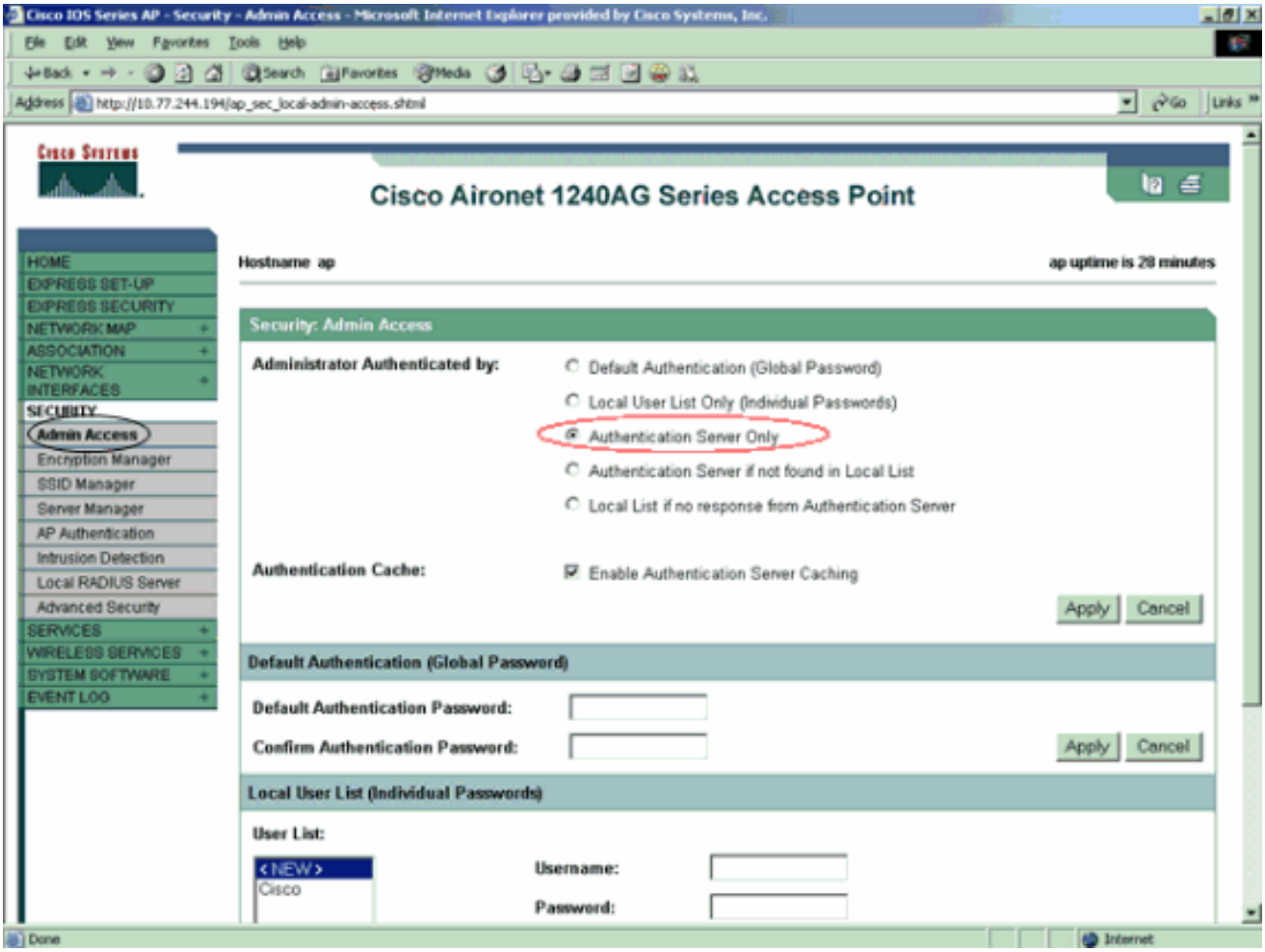


ملاحظة: يستخدم TACACS+ منفذ TCP رقم 49 بشكل افتراضي.**ملاحظة:** يجب أن يتطابق المفتاح السري المشترك الذي تقوم بتكوينه على ACS و AP.

2. أختر **أولويات الخادم الافتراضية > مصادقة المسؤول (TACACS+)**، وحدد من القائمة المنسدلة الأولوية 1 عنوان IP لخادم TACACS+ الذي قمت بتكوينه، وانقر فوق **تطبيق**.فيما يلي مثال:



3. أخترت **أمن>Admin منفذ** و، للمسؤول يصادق ب:، **مصادقة نادل فقط** وطقطقة **يطبق**.يضمن هذا التحديد مصادقة المستخدمين الذين يحاولون تسجيل الدخول إلى نقطة الوصول بواسطة خادم مصادقة.فيما يلي مثال:



هذا هو تكوين CLI لمثال التكوين:

منفذ نقطة

```
AccessPoint#show running-config

Current configuration : 2535 bytes
!
version 12.3
no service pad
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname AccessPoint
!
!
ip subnet-zero
!
!
aaa new-model
Enable AAA. ! ! aaa group server radius rad_eap ! ---!
    aaa group server radius rad_mac ! aaa group server
   radius rad_acct ! aaa group server radius rad_admin
cache expiry 1 cache authorization profile admin_cache
  cache authentication profile admin_cache ! aaa group
                                    server tacacs+ tac_admin
    Configure the server group tac_admin. server ---!
                                                172.16.1.1
  Add the TACACS+ server 172.16.1.1 to the server ---!
                                    group. cache expiry 1
```

```
Set the expiration time for the local cache as 24 ---!
hours. cache authorization profile admin_cache
cache authentication profile admin_cache
!
aaa group server radius rad_pmip
!
aaa group server radius dummy
!
aaa authentication login default group tac_admin
Define the AAA login authentication method list to ---!
use the TACACS+ server. aaa authentication login
eap_methods group rad_eap aaa authentication login
mac_methods local aaa authorization exec default group
tac_admin
Use TACACS+ for privileged EXEC access ---!
authorization !--- if authentication was performed with
use of TACACS+. aaa accounting network acct_methods
start-stop group rad_acct aaa cache profile admin_cache
all ! aaa session-id common ! ! username Cisco password
7 00271A150754 ! bridge irb ! ! interface Dot11Radio0 no
ip address no ip route-cache shutdown speed basic-1.0
basic-2.0 basic-5.5 basic-11.0 station-role root bridge-
group 1 bridge-group 1 subscriber-loop-control bridge-
group 1 block-unknown-source no bridge-group 1 source-
learning no bridge-group 1 unicast-flooding bridge-group
1 spanning-disabled ! interface Dot11Radio1 no ip
address no ip route-cache shutdown speed station-role
root bridge-group 1 bridge-group 1 subscriber-loop-
control bridge-group 1 block-unknown-source no bridge-
group 1 source-learning no bridge-group 1 unicast-
flooding bridge-group 1 spanning-disabled ! interface
FastEthernet0 no ip address no ip route-cache duplex
auto speed auto bridge-group 1 no bridge-group 1 source-
learning bridge-group 1 spanning-disabled ! interface
BVI1 ip address 172.16.1.30 255.255.0.0 no ip route-
cache ! ip http server ip http authentication aaa
Specify the authentication method of HTTP users as ---!
AAA. no ip http secure-server ip http help-path
http://www.cisco.com/warp/public/779/smbiz/prodconfig/he
lp/ea ip radius source-interface BVI1 ! tacacs-server
host 172.16.1.1 port 49 key 7 13200F13061C082F tacacs-
server directed-request radius-server attribute 32
include-in-access-req format %h radius-server vsa send
accounting ! control-plane ! bridge 1 route ip ! ! !
line con 0 transport preferred all transport output all
line vty 0 4 transport preferred all transport input all
transport output all line vty 5 15 transport preferred
all transport input all transport output all ! end
```

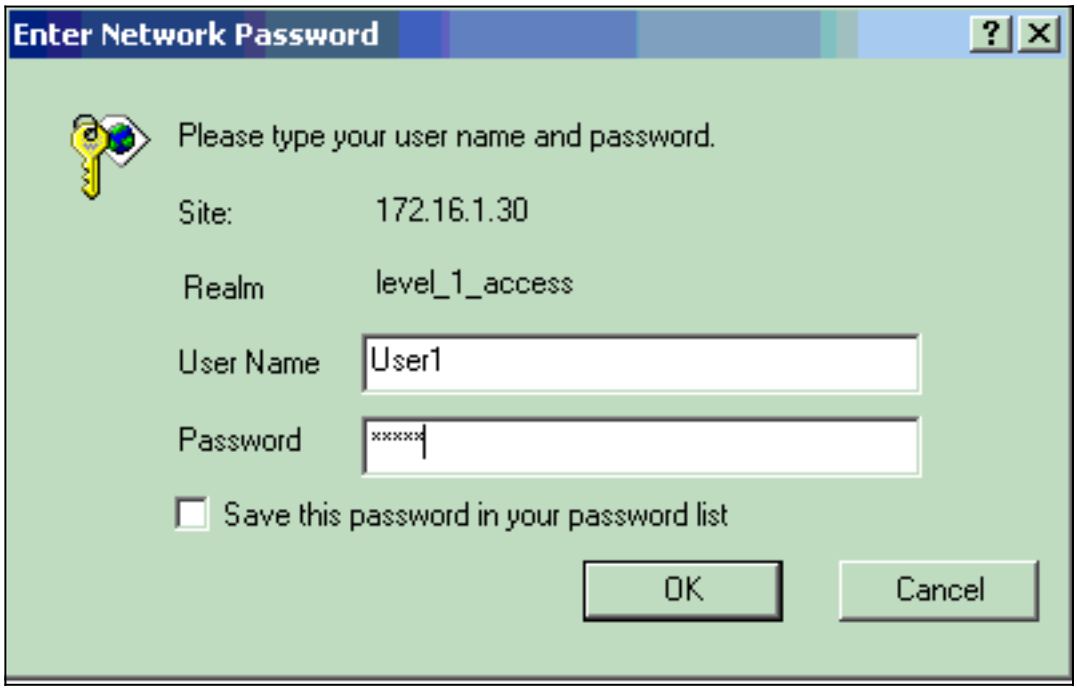
ملاحظة: يجب أن يكون لديك الإصدار JA(7)12.3 من برنامج Cisco IOS Software أو إصدار أحدث حتى تعمل جميع الأوامر في هذا التكوين بشكل صحيح. قد لا يحتوي إصدار أقدم من برنامج Cisco IOS Software على جميع هذه الأوامر متوفرة.

التحقق من الصحة

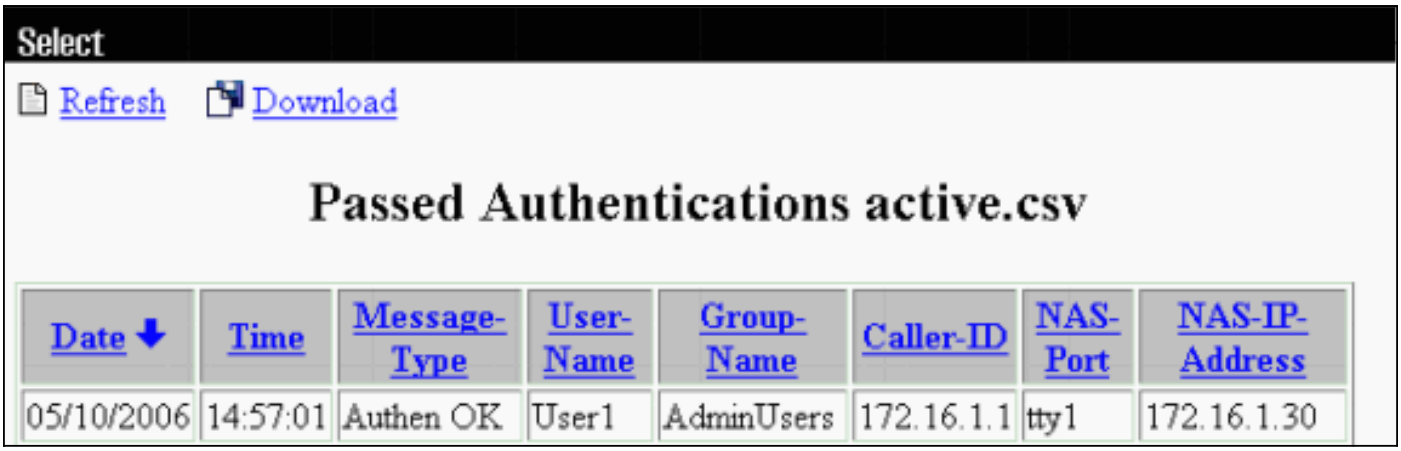
استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

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

حاولت in order to دققت التشكيل، أن يدون إلى ال ap مع إستعمال من ال gui أو ال CLI. عندما يحاول أنت أن ينفذ ال ap، ال ap يطالبك ب username وكلمة.



عندما تقوم بتوفير مسوغات المستخدم، تقوم نقطة الوصول بإعادة توجيه المسوغات إلى خادم TACACS+. يتحقق خادم TACACS+ من بيانات الاعتماد على أساس المعلومات المتاحة في قاعدة بياناته ويوفر الوصول إلى نقطة الوصول (AP) عند المصادقة الناجحة. يمكنك إختيار **التقارير والنشاط > المصادقة** التي تم تمريرها على ACS واستخدام تقرير المصادقة الذي تم تمريره للتحقق من المصادقة الناجحة لهذا المستخدم. فيما يلي مثال:



يمكنك أيضا إستخدام الأمر **show tacacs** للتحقق من التكوين الصحيح لخادم TACACS+. فيما يلي مثال:

```
AccessPoint#show tacacs

Tacacs+ Server            : 172.16.1.1/49
   Socket opens:        348
   Socket closes:        348
   Socket aborts:          0
   Socket errors:          0
   Socket Timeouts:          0
   Failed Connect Attempts:          0
   Total Packets Sent:        525
   Total Packets Recv:        525
```

التحقق من مصدر المحتوى الإضافي 5.2

يمكنك التحقق من محاولات تسجيل الدخول الفاشلة/التي تم تمريرها من ACS 5.2:

1. انقر فوق **المراقبة والتقارير > مراقبة بدء التشغيل وعارض التقارير**.يتم فتح إطار منبثق جديد مع لوحة المعلومات.
2. انقر فوق **المصادقة-tacacs-اليوم**. يوضح هذا تفاصيل محاولات الفشل/المرور.

استكشاف الأخطاء وإصلاحها

أنت يستطيع استعملت هذا يضبط أمر على ال ap in order to تحريت تشكيلك:

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

- **debug tacacs events** — يعرض هذا الأمر تسلسل الأحداث التي تحدث أثناء مصادقة TACACS. هنا مثال من الإنتاج من هذا أمر:

```
Mar  1 00:51:21.113: TPLUS: Queuing AAA Authentication request 0 for*
processing
Mar  1 00:51:21.113: TPLUS: processing authentication start request id 0*
(Mar  1 00:51:21.113: TPLUS: Authentication start packet created for 0(User1*
Mar  1 00:51:21.114: TPLUS: Using server 172.16.1.1*
Mar  1 00:51:21.115: TPLUS(00000000)/0/NB_WAIT/C6DC40: Started 5 sec timeout*
Mar  1 00:51:21.116: TPLUS(00000000)/0/NB_WAIT: socket event 2*
Mar  1 00:51:21.116: TPLUS(00000000)/0/NB_WAIT: wrote entire 25 bytes request*
Mar  1 00:51:21.116: TPLUS(00000000)/0/READ: socket event 1*
Mar  1 00:51:21.117: TPLUS(00000000)/0/READ: Would block while reading*
Mar  1 00:51:21.120: TPLUS(00000000)/0/READ: socket event 1*
Mar  1 00:51:21.120: TPLUS(00000000)/0/READ: read entire 12 header bytes (expect*
(bytes data 16
Mar  1 00:51:21.120: TPLUS(00000000)/0/READ: socket event 1*
Mar  1 00:51:21.120: TPLUS(00000000)/0/READ: read entire 28 bytes response*
Mar  1 00:51:21.121: TPLUS(00000000)/0/C6DC40: Processing the reply packet*
(Mar  1 00:51:21.121: TPLUS: Received authen response status GET_PASSWORD (8*
Mar  1 00:51:21.121: TPLUS: Queuing AAA Authentication request 0 for processing*
Mar  1 00:51:21.121: TPLUS: processing authentication continue request id 0*
Mar  1 00:51:21.122: TPLUS: Authentication continue packet generated for 0*
Mar  1 00:51:21.122: TPLUS(00000000)/0/WRITE/C6DC40: Started 5 sec timeout*
Mar  1 00:51:21.122: TPLUS(00000000)/0/WRITE: wrote entire 22 bytes request*
Mar  1 00:51:21.178: TPLUS(00000000)/0/READ: socket event 1*
Mar  1 00:51:21.178: TPLUS(00000000)/0/READ: read entire 12 header bytes (expect*
(bytes data 6
Mar  1 00:51:21.178: TPLUS(00000000)/0/READ: socket event 1*
Mar  1 00:51:21.178: TPLUS(00000000)/0/READ: read entire 18 bytes response*
Mar  1 00:51:21.179: TPLUS(00000000)/0/C6DC40: Processing the reply packet*
(Mar  1 00:51:21.179: TPLUS: Received authen response status PASS (2*
```

- **debug ip http authentication**—أستخدم هذا الأمر لاستكشاف أخطاء مصادقة HTTP وإصلاحها. يعرض الأمر أسلوب المصادقة الذي حاول الموجه إستخدامه ورسائل الحالة الخاصة بالمصادقة.
- **debug aaa authentication**— يعرض هذا الأمر معلومات حول مصادقة AAA TACACS+.

إذا دخل المستخدم اسم مستخدم غير موجود على خادم TACACS+، فستفشل المصادقة. فيما يلي إخراج أمر **مصادقة tacacs** لـ**debug** لمصادقة فاشلة:

```
Mar  1 00:07:26.624: TPLUS: Queuing AAA Authentication request 0 for processing*
Mar  1 00:07:26.624: TPLUS: processing authentication start request id 0*
(Mar  1 00:07:26.624: TPLUS: Authentication start packet created for 0(User3*
Mar  1 00:07:26.624: TPLUS: Using server 172.16.1.1*
Mar  1 00:07:26.625: TPLUS(00000000)/0/NB_WAIT/A88784: Started 5 sec timeout*
Mar  1 00:07:26.626: TPLUS(00000000)/0/NB_WAIT: socket event 2*
```

```
Mar  1 00:07:26.626: TPLUS(00000000)/0/NB_WAIT: wrote entire 25 bytes request*
                     Mar  1 00:07:26.627: TPLUS(00000000)/0/READ: socket event 1*
                   Mar  1 00:07:26.627: TPLUS(00000000)/0/READ: Would block while reading*
                     Mar  1 00:07:26.631: TPLUS(00000000)/0/READ: socket event 1*
Mar  1 00:07:26.632: TPLUS(00000000)/0/READ: read entire 12 header bytes (expect 16*
                                                                        (bytes data
                     Mar  1 00:07:26.632: TPLUS(00000000)/0/READ: socket event 1*
            Mar  1 00:07:26.632: TPLUS(00000000)/0/READ: read entire 28 bytes response*
            Mar  1 00:07:26.632: TPLUS(00000000)/0/A88784: Processing the reply packet*
          (Mar  1 00:07:26.632: TPLUS: Received authen response status GET_PASSWORD (8*
       Mar  1 00:07:26.632: TPLUS: Queuing AAA Authentication request 0 for processing*
           Mar  1 00:07:26.633: TPLUS: processing authentication continue request id 0*
            Mar  1 00:07:26.633: TPLUS: Authentication continue packet generated for 0*
            Mar  1 00:07:26.634: TPLUS(00000000)/0/WRITE/A88784: Started 5 sec timeout*
           Mar  1 00:07:26.634: TPLUS(00000000)/0/WRITE: wrote entire 22 bytes request*
                     Mar  1 00:07:26.688: TPLUS(00000000)/0/READ: socket event 1*
 Mar  1 00:07:26.688: TPLUS(00000000)/0/READ: read entire 12 header bytes (expect 6*
                                                                        (bytes data
                     Mar  1 00:07:26.689: TPLUS(00000000)/0/READ: socket event 1*
            Mar  1 00:07:26.689: TPLUS(00000000)/0/READ: read entire 18 bytes response*
            Mar  1 00:07:26.689: TPLUS(00000000)/0/A88784: Processing the reply packet*
                  (Mar  1 00:07:26.689: TPLUS: Received authen response status FAIL (3*
```

يمكنك إختيار **التقارير والنشاط > المصادقة الفاشلة** لعرض محاولة المصادقة الفاشلة على ACS. فيما يلي مثال:

Date ⬇	Time	Message-Type	User-Name	Group-Name	Caller-ID	Authen-Failure-Code	Author-Failure-Code	Author-Data	NAS-Port
05/17/2006	19:40:14	Authen failed	User3	..	..	CS user unknown	..	..	..

إن يستعمل أنت cisco ios برمجية إطلاق على ال ap أن يكون مبكر من cisco ios برمجية إطلاق JA(7)12.3، أنت أمكن إصطدمت خطأ كل مرة أن أنت تحاول أن يدون إلى ال ap مع إستعمال HTTP. معرف تصحيح الأخطاء من Cisco هو CSCeb52431 (العملاء المسجلون فقط).

يتطلب تنفيذ Cisco IOS Software HTTP/AAA المصادقة المستقلة لكل اتصال HTTP منفصل. تتضمن واجهة المستخدم الرسومية (GUI) لبرنامج Cisco IOS اللاسلكية المرجع الخاص بالعديد من عشرات من الملفات المنفصلة داخل صفحة ويب واحدة (على سبيل المثال JavaScript و GIF). لذلك إذا قمت بتحميل صفحة واحدة في واجهة المستخدم الرسومية (GUI) لبرنامج Cisco IOS Software اللاسلكي، فيمكن لعشرات وعشرات طلبات المصادقة/التفويض المنفصلة الوصول إلى خادم AAA.

لمصادقة HTTP، أستخدم مصادقة RADIUS أو المصادقة المحلية. لا يزال خادم RADIUS خاضعا لطلبات المصادقة المتعددة. ولكن بروتوكول RADIUS أكثر قابلية للتوسع من بروتوكول TACACS+، ومن ثم فمن المرجح أن يوفر تأثيرا أقل سلبية على الأداء.

إذا كان ينبغي عليك إستخدام TACACS+ وأن يكون لديك كلمة Cisco ACS، فاستخدم الكلمة الأساسية **اتصال واحد** باستخدام الأمر **tacacs-server**. يؤدي إستخدام هذه الكلمة الأساسية مع الأمر إلى الاستغناء عن ACS معظم مصروفات إعداد/خفض اتصال TCP ومن المرجح أن يقلل الحمل على الخادم إلى حد معين.

ل cisco ios برمجية إطلاق JA (7)12.3 وفيما بعد على ال ap، البرمجية يتضمن إصلاح. يصف الجزء المتبقي من هذا القسم الإصلاح.

أستخدم ميزة ذاكرة التخزين المؤقت لمصادقة AAA لذاكرة التخزين المؤقت للمعلومات التي يرجعها خادم TACACS+. تتيح ميزة ذاكرة التخزين المؤقت لتوصيف المصادقة لنقطة الوصول إمكانية تخزين استجابات المصادقة/التخويل مؤقتا لمستخدم ما حتى لا تكون هناك حاجة لإرسال طلبات المصادقة/التخويل التالية إلى خادم AAA. استعملت in order to مكنت هذا سمة مع ال CLI، هذا أمر:

```
cache expiry
cache authorization profile
cache authentication profile
aaa cache profile
```

أحلت ل كثير معلومة على هذا سمة والأوامر، *يشكل المصادقة ذاكرة تخزين مؤقت وملف تعريف* قسم من يدير المنفذ نقطة.

أخترت in order to مكنت هذا سمة على ال gui، **أمن>إدارة منفذ** وفحصت ال **يمكن صحة نادل تخديد** تدقيق صندوق. لأن هذا المستند يستخدم برنامج Cisco IOS الإصدار JA(7)12.3، يستخدم المستند الإصلاح، كما توضح التكوينات.

معلومات ذات صلة

- تكوين خوادم RADIUS و TACACS+
- إشعار ميداني: تقوم نقطة وصول IOS بتقسيم خادم TACACS+ على الطلبات
- مصادقة EAP مع خادم RADIUS
- دعم المنتج اللاسلكي
- 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).