لمكاتلا نيوكت - ثدحألا تارادصإلاو ACS 5.x مع Microsoft AD

المحتويات

المقدمة

يقدم هذا المستند نموذجا لتكوين دمج Microsoft Active Directory مع نظام التحكم في الوصول الآمن ((ACS 5.x من Cisco والإصدارات الأحدث. يستخدم (ACS Active Directory (AD من Microsoft كمخزن هوية خارجي لتخزين موارد مثل المستخدمين والأجهزة والمجموعات والسمات. يصادق ACS هذه الموارد مقابل AD.

المتطلبات الأساسية

المتطلبات

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

- يجب أن يكون مجال Windows Active Directory المراد إستخدامه مهيأ ومشغلا بالكامل.
- أستخدم مجال Microsoft Windows Server 2003 أو مجال Microsoft Windows Server 2008 أو مجال Microsoft Windows Server 2008 R2 حيث إن هذه المجالات مدعومة من قبل ACS 5.x.**ملاحظة:** يتم دعم دمج مجال Microsoft Windows Server 2008 R2 مع ACS من ACS 5.2 والإصدارات الأحدث.

المكونات المستخدمة

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

- Cisco Secure ACS 5.3
- مجال Microsoft Windows Server 2003

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.

معلومات أساسية

يوفر Windows Active Directory العديد من الميزات التي يتم إستخدامها في الاستخدام اليومي للشبكة. ويتيح دمج ACS 5.x مع AD إستخدام مستخدمي AD الحاليين، والآلات، ورسم الخرائط الخاصة بمجموعاتهم.

يقدم ACS 5.x المدمج مع AD الميزات التالية:

1. مصادقة الجهاز
2. إسترداد السمة للتخويل
3. إسترداد الشهادة لمصادقة EAP-TLS
4. تقييد حساب المستخدم والآلة
5. قيود الوصول إلى الجهاز
6. التحقق من أذونات الطلب
7. خيارات رد الاتصال لمستخدمي الطلب الهاتفي
8. سمات دعم الطلب

التكوين

تكوين محرك نشر التطبيق (ADE-OS) ACS 5.x

قبل دمج ACS 5.x إلى AD، تأكد من مطابقة **المنطقة الزمنية والتاريخ والوقت** في ACS مع وحدة التحكم بالمجال الأساسية AD. قم أيضا بتحديد خادم DNS على ACS لتتمكن من حل اسم المجال من ACS 5.x. أتمت هذا steps in order to شكلت ACS 5.x تطبيق نشر محرك (ADE-OS):

1. SSH إلى جهاز ACS وأدخل بيانات اعتماد CLI.
2. قم بإصدار الأمر **clock timezone** في وضع التكوين كما هو موضح لتكوين **المنطقة الزمنية** على ACS للمطابقة مع ذلك على وحدة التحكم في المجال.

```
clock timezone Asia/Kolkata
```

ملاحظة: آسيا/كلكتا هي المنطقة الزمنية المستخدمة في هذا المستند. يمكنك العثور على منطقتك الزمنية المحددة بواسطة أمر وضع EXEC **show timezone**.

3. في حالة مزامنة وحدة التحكم بمجال AD مع خادم NTP الموجود في شبكتك، يوصى بشدة باستخدام نفس خادم NTP على ACS. إذا لم يكن لديك خادم NTP، فقم بالتخطي إلى **الخطوة 4**. هذه هي الخطوات لتكوين خادم NTP:يمكن تكوين خادم NTP باستخدام الأمر **ntp server <ip address** الخاص **بخادم NTP>**في وضع التكوين كما هو موضح.

```
ntp server 192.168.26.55
.The NTP server was modified
.If this action resulted in a clock modification, you must restart ACS
```

راجع ACS 5.x: مزامنة Cisco ACS مع مثال تكوين خادم NTP للحصول على مزيد من المعلومات حول تكوين NTP.

4. لتكوين التاريخ والوقت يدويا، أستخدم الأمر **clock set** في **وضع EXEC**. ويتم توضيح مثال هنا:

```
clock set Jun 8 10:36:00 2012
.Clock was modified. You must restart ACS
Do you want to restart ACS now? (yes/no) yes
.Stopping ACS
.....Stopping Management and View
......Stopping Runtime
....Stopping Database
.....Cleanup
.... Starting ACS

To verify that ACS processes are running, use the
.show application status acs' command'
```

5. تحقق الآن من **المنطقة الزمنية** والتاريخ و**الوقت** باستخدام الأمر **show clock**. يتم عرض إخراج الأمر show clock هنا:

```
acs51/admin# show clock
Fri Jun  8 10:36:05 IST 2012
```

6. قم بتكوين DNS على ACS باستخدام الأمر **<ip name-server <ip address of the DNS>** في **وضع التكوين** كما هو موضح هنا:

```
ip name-server 192.168.26.55
```

ملاحظة: يقوم مسؤول مجال Windows بتوفير عنوان DNS IP.

7. قم بإصدار الأمر **nslookup <domain name>**للتحقق من إمكانية الوصول إلى اسم المجال كما هو موضح.

```
acs51/admin#nslookup MCS55.com
"Trying "MCS55.com
HEADER<<- opcode: QUERY, status: NOERROR, id: 60485<<- ;;
flags: qr aa rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1 ;;

:QUESTION SECTION ;;
MCS55.com.                      IN      ANY;

:ANSWER SECTION ;;
MCS55.com.              600     IN      A       192.168.26.55
.MCS55.com.             3600    IN      NS      admin-zq2ttn9ux.MCS55.com
.MCS55.com.             3600    IN      SOA     admin-zq2ttn9ux.MCS55.com
  hostmaster.MCS55.com. 635 900 600 86400 3600

:ADDITIONAL SECTION ;;
admin-zq2ttn9ux.MCS55.com. 3600 IN      A       192.168.26.55

Received 136 bytes from 192.168.26.55#53 in 0 ms
```

ملاحظة: إذا كان **قسم الإجابات** فارغا، فاتصل بمسؤول مجال Windows لمعرفة خادم DNS الصحيح للمجال.

8. قم بإصدار الأمر **ip domain-name <domain name>**من أجل تكوين **domain-name** على ACS كما هو موضح هنا:

```
ip domain-name MCS55.com
```

9. قم بإصدار الأمر **hostname <hostname>**لتكوين **اسم المضيف** على ACS كما هو موضح هنا:

```
hostname acs51
```

ملاحظة: نظرا لقيود نظام التشغيل NetBIOS، يجب أن تحتوي أسماء مضيفي ACS على أقل من أو تساوي 15 حرفا.

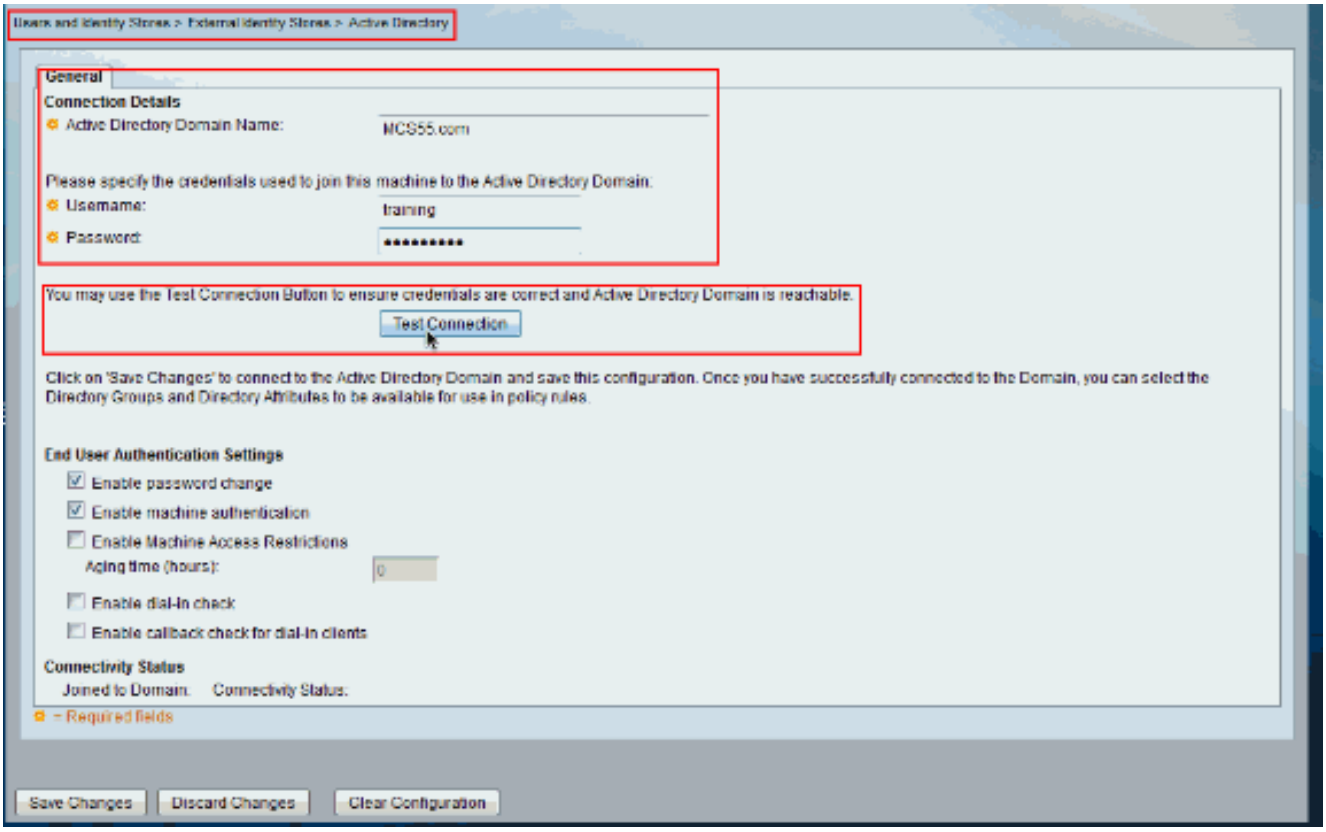
10. قم بإصدار الأمر **write memory** لحفظ التكوين في ACS.

الانضمام إلى ACS 5.x إلى AD

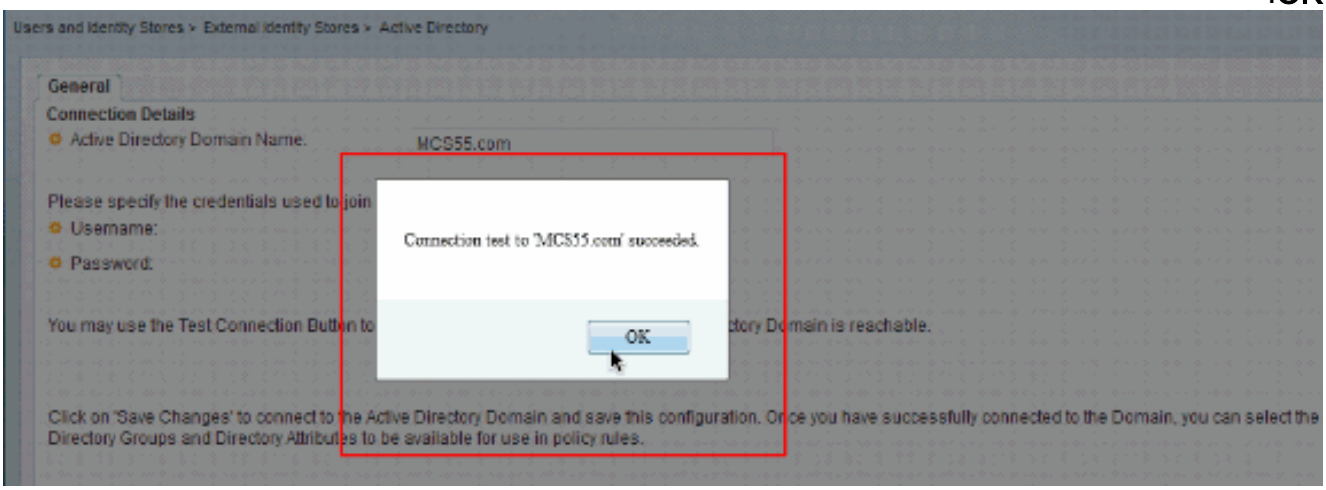
أكمل الخطوات التالية للانضمام إلى ACS5.x إلى AD:

1. أختر **Users and Identity Stores (المستخدمين ومتاجر الهوية) > External Identity Stores (مخازن الهوية الخارجية) > Active Directory (الدليل النشط)** وقم بتوفير اسم المجال وحساب AD (اسم المستخدم) وكلمة

المرور الخاصة به وانقر فوق **إختبار الاتصال**.**ملاحظة:** يجب أن يحتوي حساب AD المطلوب للوصول إلى المجال في ACS على أي مما يلي:إضافة محطات عمل إلى حق مستخدم المجال في المجال المطابق.إنشاء كائنات كمبيوتر أو إذن حذف كائنات كمبيوتر على حاوية أجهزة الكمبيوتر المقابلة حيث يتم إنشاء حساب جهاز ACS قبل ربط جهاز ACS بالمجال.**ملاحظة:** توصي Cisco بتعطيل سياسة التأمين لحساب ACS وتكوين البنية الأساسية AD لإرسال تنبيهات إلى المسؤول في حالة إستخدام كلمة مرور خاطئة لذلك الحساب. وذلك لأنك إذا قمت بإدخال كلمة مرور غير صحيحة، فإن ACS لا يقوم بإنشاء أو تعديل حساب جهازه عندما يكون ذلك ضروريا وبالتالي من المحتمل رفض جميع المصادقات.**ملاحظة:** يمكن وضع حساب Windows AD، الذي يضم ACS إلى مجال AD، في وحدته التنظيمية الخاصة. يوجد في OU الخاص به إما عندما يتم إنشاء الحساب أو في وقت لاحق مع قيد ينص على أن اسم الجهاز يجب أن يطابق اسم حساب AD.

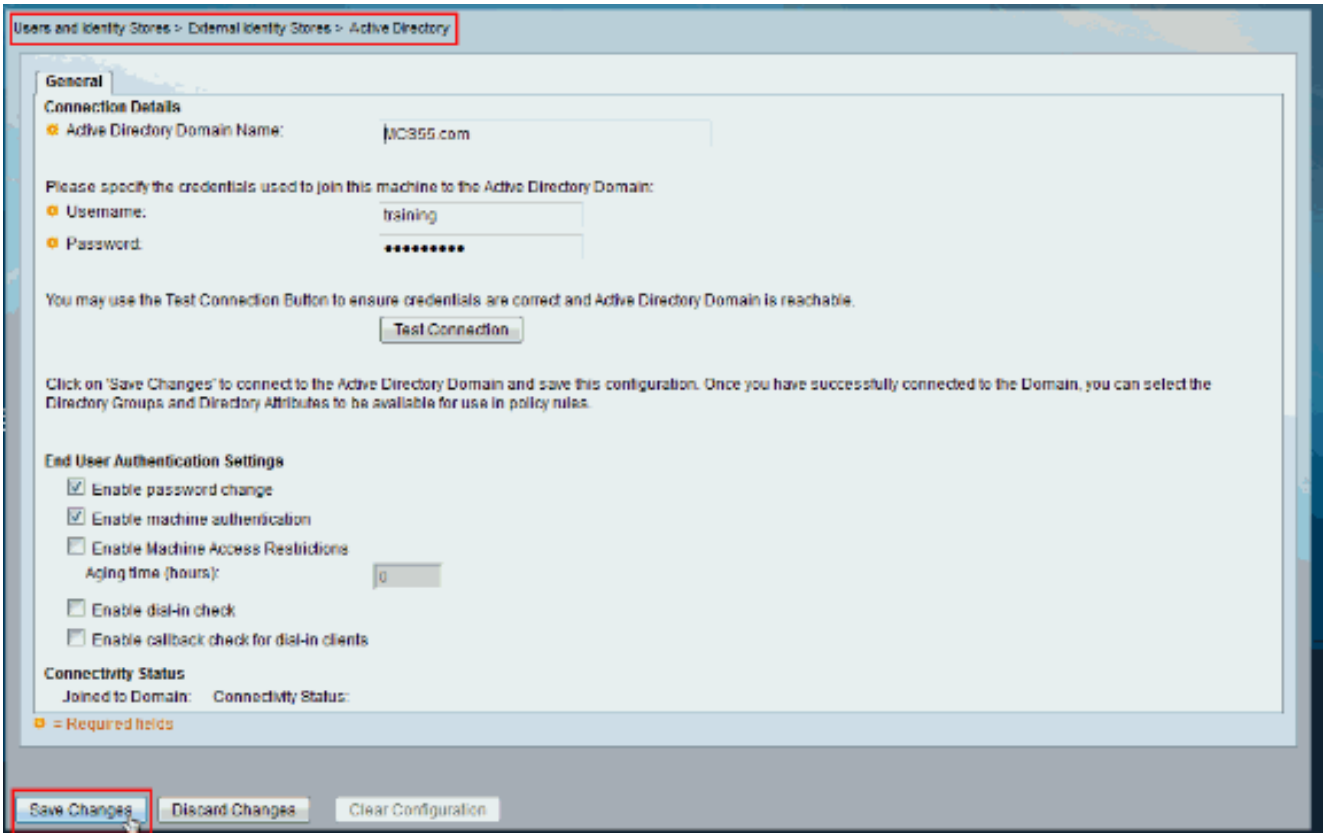


2. توضح لقطة الشاشة هذه أن إختبار الاتصال بالإعلان ناجح. ثم انقر فوق **OK**.

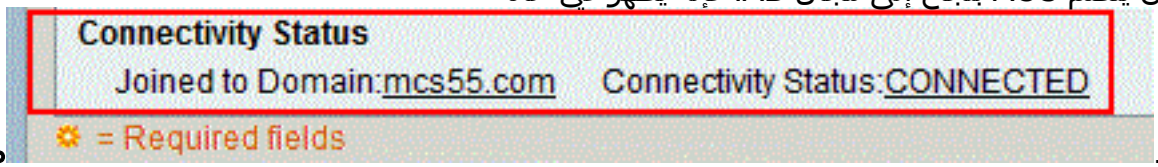


ملاحظة: يتأثر التكوين المركزي وينفصل أحيانا عندما تكون هناك إستجابة بطيئة من الخادم أثناء إختبار اتصال ACS بمجال AD. ومع ذلك، فهو يعمل بشكل جيد مع التطبيقات الأخرى.

3. انقر فوق **حفظ التغييرات** ل ACS للانضمام إلى AD.



4. بمجرد أن ينضم ACS بنجاح إلى مجال AD، فإنه يظهر في حالة الاتصال.

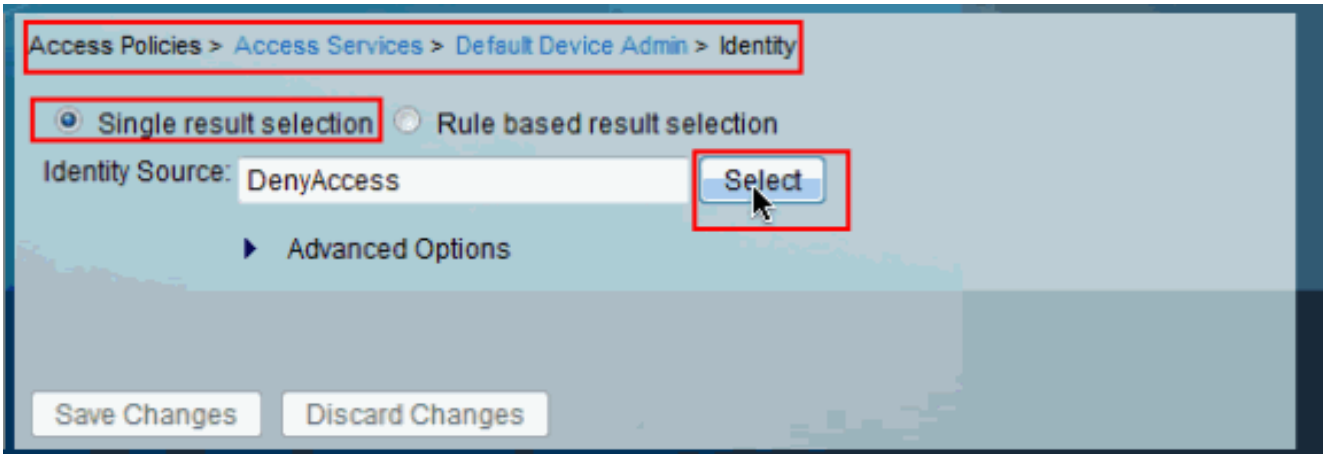


ملاحظة: عند تكوين مخزن هوية AD، يقوم ACS أيضا بإنشاء:قاموس جديد لذلك المخزن ذو سمتين: ExternalGroups وسمة أخرى لأي سمة تم إستردادها من صفحة سمات الدليل.سمة جديدة، IdentityAccessRestricted. يمكنك إنشاء شرط مخصص لهذه السمة يدويا.شرط مخصص لتعيين المجموعة من سمة ExternalGroup؛ اسم الشرط المخصص هو AD1:ExternalGroups وشرط مخصص آخر لكل سمة محددة في صفحة سمات الدليل، على سبيل المثال، AD1:cn.

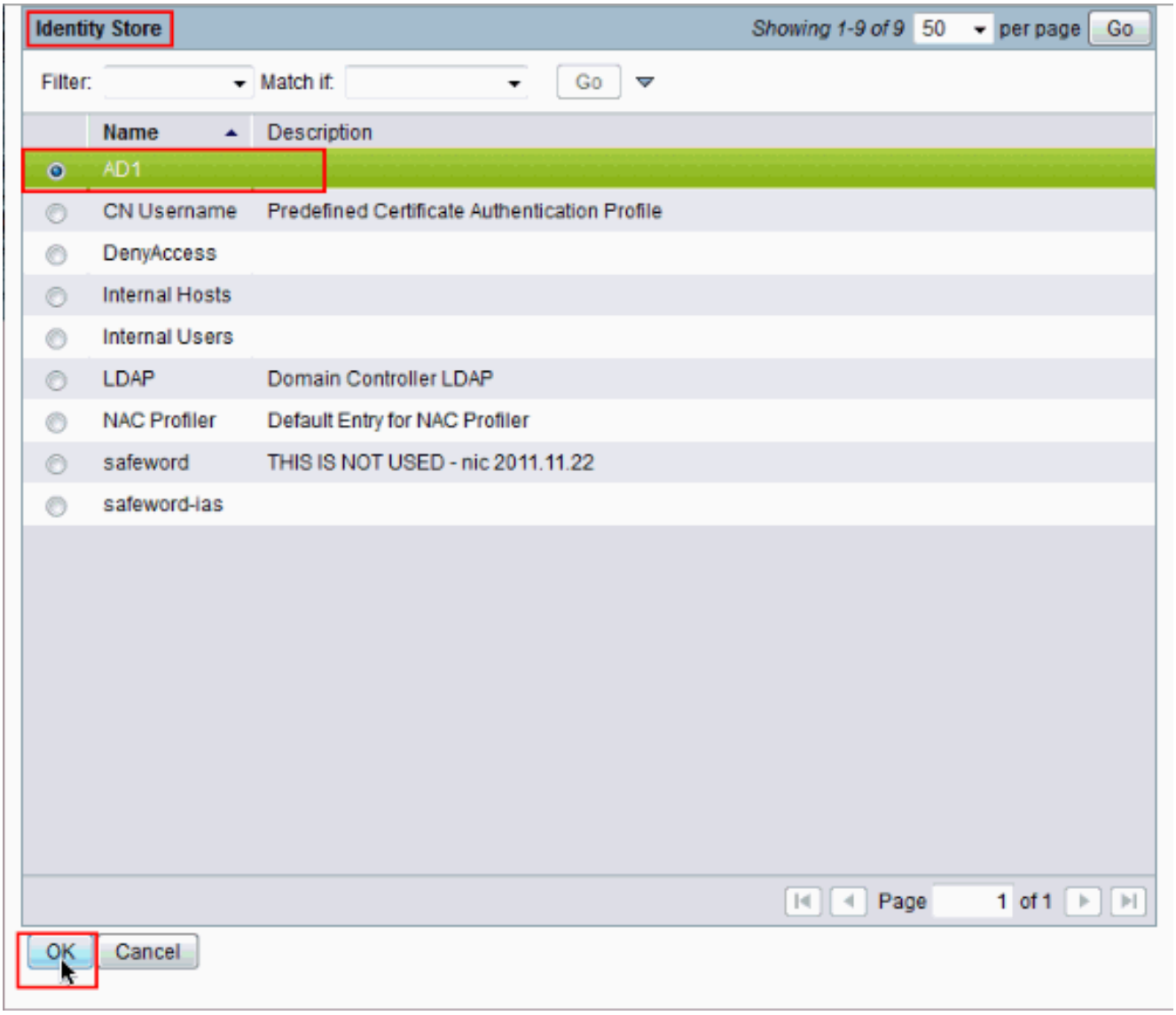
تكوين خدمة الوصول

أكمل هذه الخطوات لإكمال تكوين خدمة الوصول حتى يمكن ل ACS إستخدام AD Integration الذي تم تكوينه حديثا.

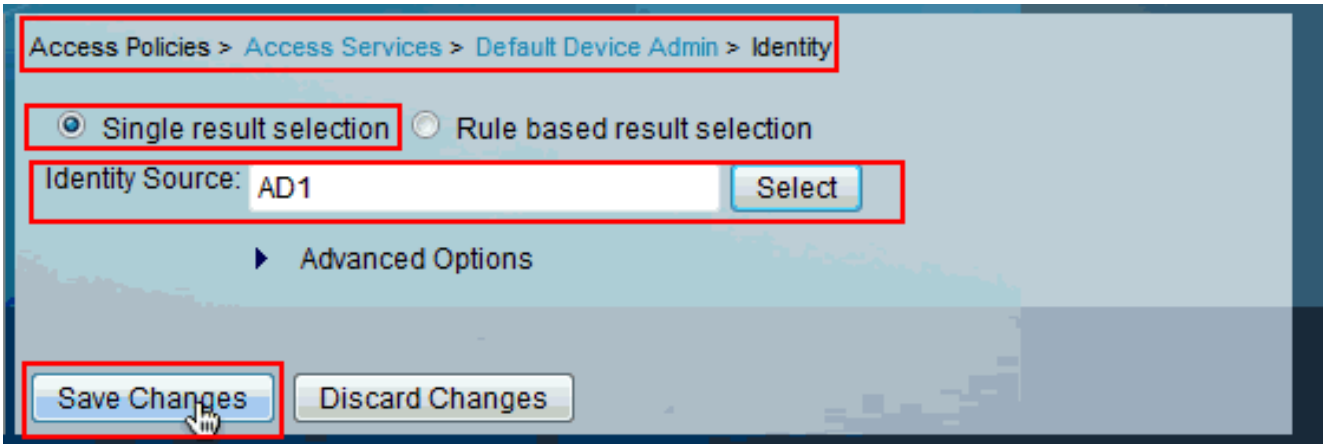
1. أختر الخدمة من حيث تريد مصادقة المستخدمين من AD وانقر فوق **الهوية**. انقر الآن على **تحديد** بجوار حقل مصدر
الهوية.



2. أخترت **AD1** وطقطقة **ok**.



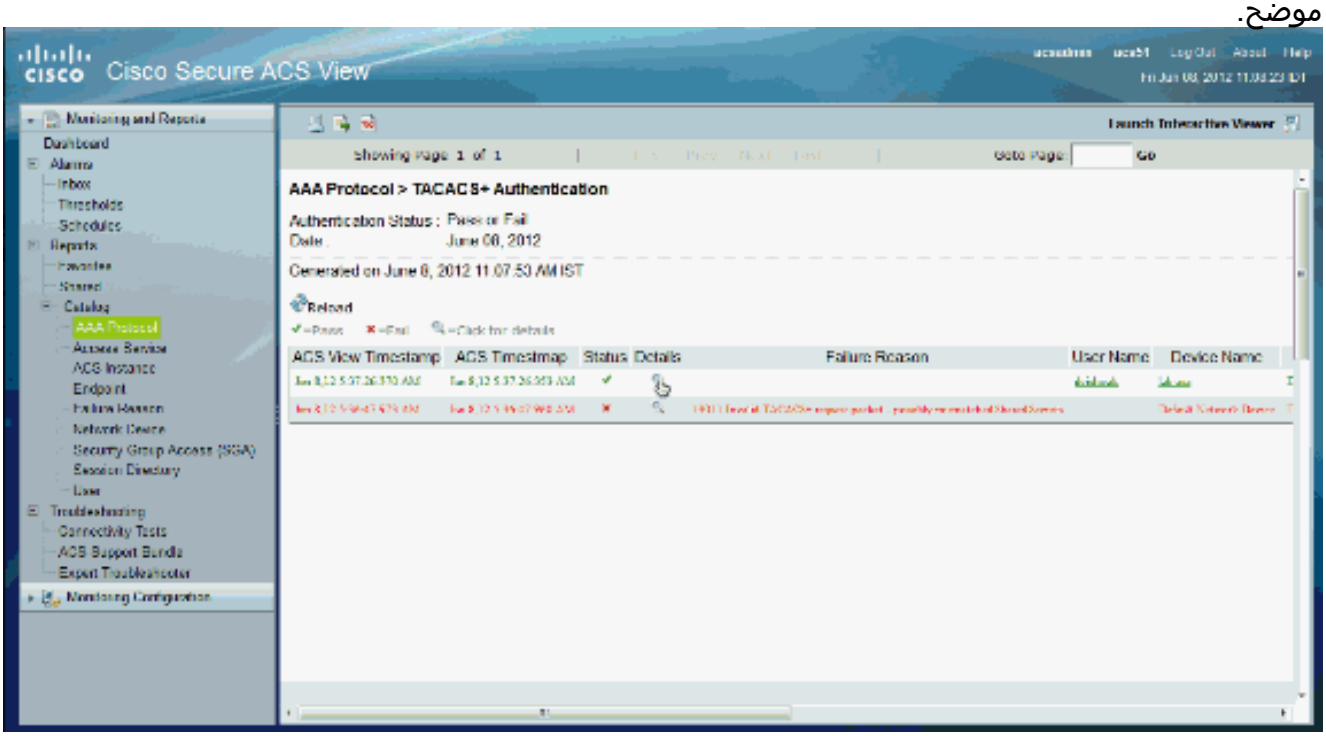
3. انقر فوق **حفظ التغييرات**.



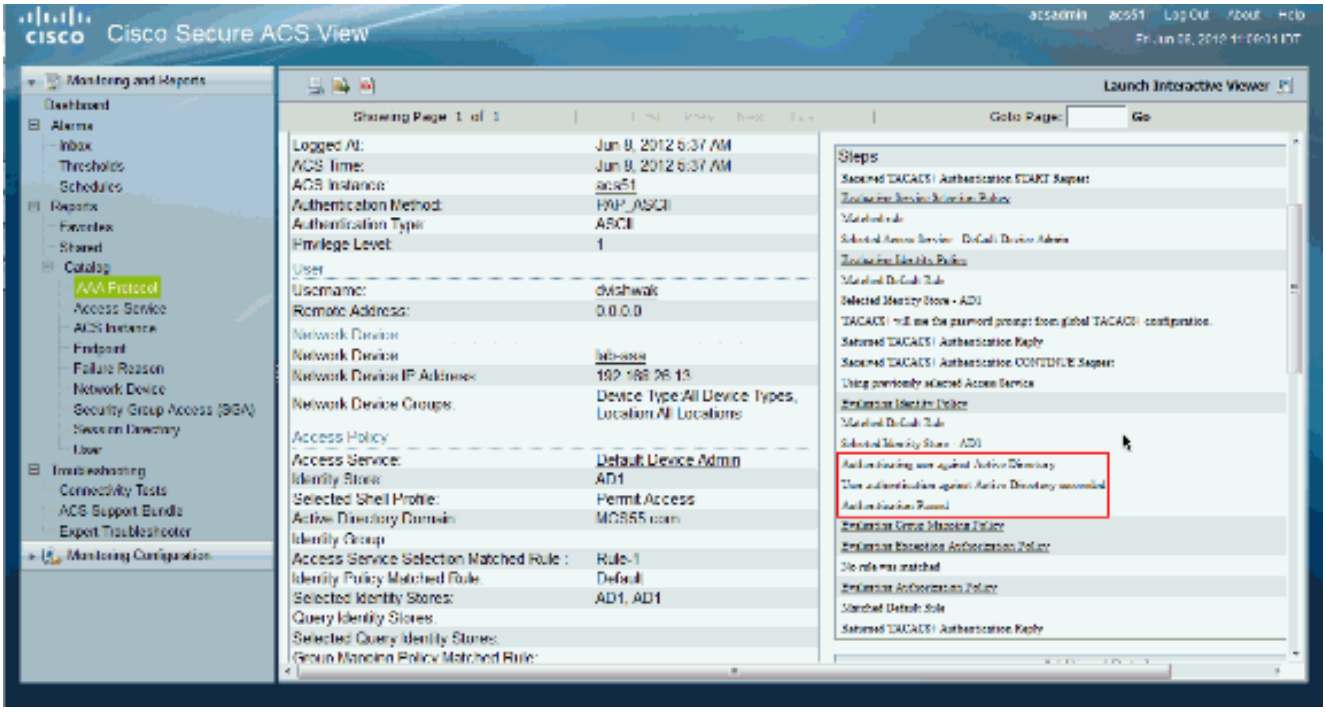
التحقق من الصحة

للتحقق من مصادقة AD، أرسل طلب مصادقة من NAS مع مسوغات AD. تأكد من تكوين NAS على ACS وسيتم معالجة الطلب بواسطة خدمة الوصول التي تم تكوينها في القسم السابق.

1. بعد مصادقة ناجحة من NAS قم بتسجيل الدخول إلى واجهة المستخدم الرسومية (GUI) ل ACS واختر **المراقبة وإعداد التقارير > بروتوكول TACACS+AAA > المصادقة**. تعرف على المصادقة التي تم تمريرها من القائمة وانقر على رمز **العدسة المكبرة** كما هو موضح.



2. يمكنك التحقق من الخطوات التي قام ACS بإرسال طلب المصادقة إلى AD.



معلومات ذات صلة

- نظام التحكم في الوصول الآمن من Cisco
- 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).