

مدخات سمل ل وخذ ليجست ة قداصم : IPS 7.x مداخ نيوكتل لاثمك ACS 5.x مادختساب RADIUS

المحتويات

[المقدمة](#)

[المتطلبات الأساسية](#)

[المتطلبات](#)

[المكونات المستخدمة](#)

[الاصطلاحات](#)

[التكوين](#)

[تكوين IPS للمصادقة من خادم ACS باستخدام IME](#)

[تكوين ACS كخادم RADIUS](#)

[التحقق من الصحة](#)

[استكشاف الأخطاء وإصلاحها](#)

[معلومات ذات صلة](#)

[المقدمة](#)

يقدم هذا المستند معلومات حول كيفية تكوين نظام Cisco لمنع الاقتحام (IPS) لمصادقة تسجيل دخول المستخدم باستخدام خادم RADIUS. يتم استخدام ACS كخادم RADIUS.

[المتطلبات الأساسية](#)

[المتطلبات](#)

يفترض هذا المستند أن نظام Cisco لمنع الاقتحام (IPS) يعمل بالكامل ويتم تكوينه للسماح لمدير نظام منع الاقتحام (IME) أو CLI (واجهة سطر الأوامر) من Cisco بإجراء تغييرات التكوين. بالإضافة إلى مصادقة AAA المحلية، يمكنك الآن تكوين خوادم RADIUS لتنفيذ مصادقة المستخدم المستشعر. تتوفر القدرة على تكوين IPS لاستخدام مصادقة AAA RADIUS لحسابات المستخدم، والتي تساعد على تشغيل عمليات نشر IPS الكبيرة، في نظام Cisco لمنع الاقتحام الإصدار E4(4)7.0 والإصدارات الأحدث.

ملاحظة: لا يوجد خيار لتمكين المحاسبة على IPS. يوجد دعم مصادقة RADIUS في IPS 7.04، ولكن TACACS أو التفويض أو المحاسبة غير مدعومة.

[المكونات المستخدمة](#)

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

- نظام منع الاقتحام Cisco Intrusion Prevention System، الإصدار E4(4)7.0 والإصدارات الأحدث

• Cisco Intrusion Prevention System Manager Express، الإصدار 7.1(1) 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

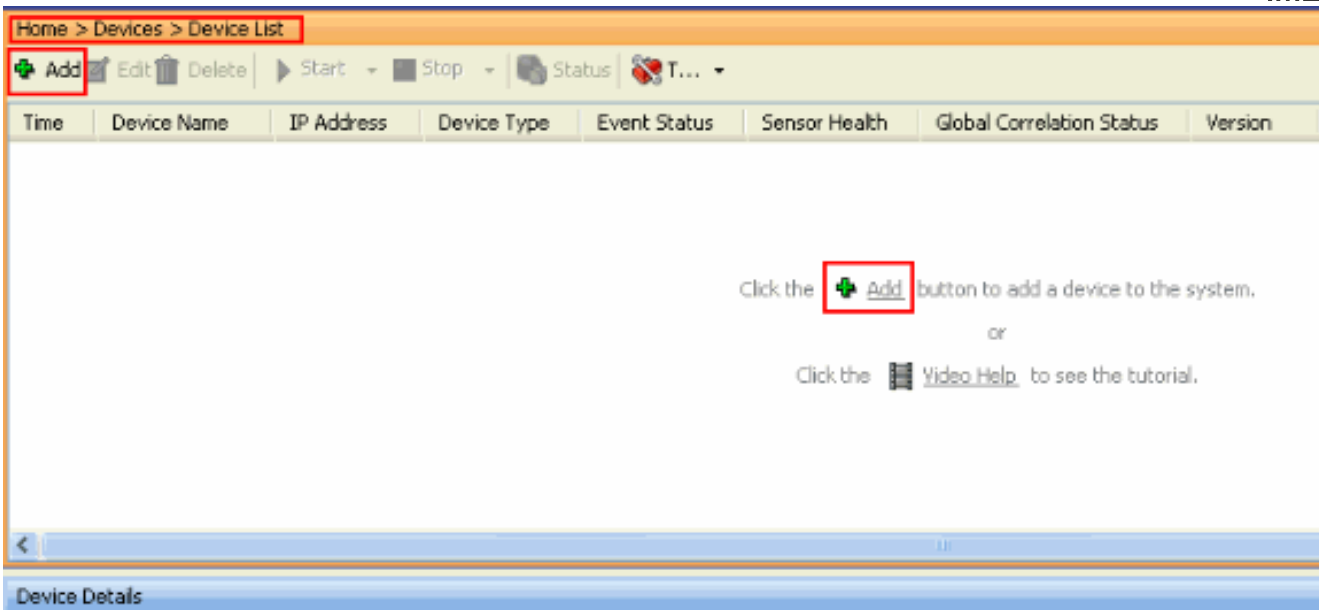
في هذا القسم، تُقدّم لك معلومات تكوين الميزات الموضحة في هذا المستند.

ملاحظة: استخدم [أداة بحث الأوامر](#) (للعلماء [المسجلين](#) فقط) للحصول على مزيد من المعلومات حول الأوامر المستخدمة في هذا القسم.

تكوين IPS للمصادقة من خادم ACS باستخدام IME

أتمت هذا steps in order to أضفت ال ips إلى IME وبعد ذلك شكلت ال ips للمصادقة من ال acs نادل:

1. أخترت منزل <أداة> قائمة أداة <يضيف in order to أضفت IPS إلى IME.



2. أكمل الحقول الموجودة في نافذة **إضافة جهاز**، كما هو موضح هنا، لتوفير تفاصيل حول IPS. اسم المستشعر المستخدم هنا هو IPS. وانقر فوق

Add Device [Close]

Sensor Name:

Sensor IP Address:

Web Server Port:

Communication protocol

Use encrypted connection (https)

Use non-encrypted connection (http)

Authentication

Configuration User Name: [Info]

Configuration Password:

Use the Same Account for Configuration and Event Subscription (This is not recommended):

Event Subscription User Name: [Info]

Event Subscription Password:

Event Start Time (UTC)

Most Recent Alerts

Start Date (YYYY:MM:DD): : :

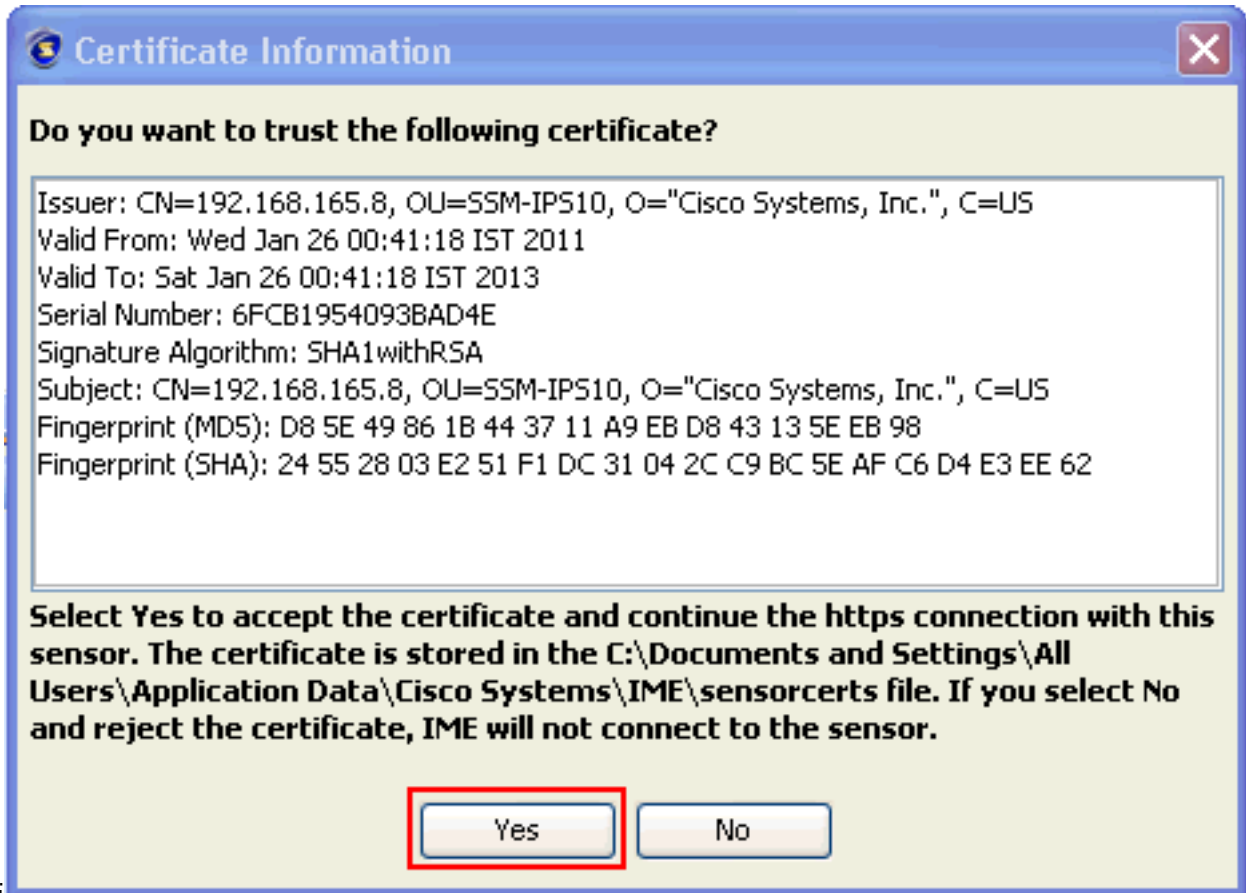
Start Time (HH:MM:SS): : :

Exclude alerts of the following severity level(s)

Informational Low Medium High

.OK

3. انقر فوق نعم لقبول الشهادة ومتابعة اتصال HTTPS بالمستشعر. يجب قبول الشهادة للاتصال بالمستشعر والوصول



إليه.
 م إضافة IPS المسمى IPS إلى تطبيق Intrusion Prevention System Manager Express ((IME).

Time	Device Name	IP Address	Device Type	Event Status	Global Correlation Status	Version
	JPS	192.168.165.8	ips-4240-k9	Connected	Connected	7.0(4)E4

4. أختار التكوين < IPS < إعداد المستشعر < المصادقة، وإكمال الخطوات التالية: انقر فوق زر راديو خادم RADIUS لتحديد خادم RADIUS كجهاز مصادقة. قم بتوفير معلمات مصادقة RADIUS، كما هو موضح. أختار محلي و RADIUS كمصادقة لوحدة التحكم، لذلك يتم استخدام المصادقة المحلية عندما لا يكون خادم RADIUS متاحاً. طقطقة يطبق.

Configuration > IP5 > Sensor Setup > Authentication

Refresh

User Authentication: Local Radius Server

Local Authentication

Specify the users that have access to the sensor. The service role is a special role that allows you to bypass the CLI if needed. Only one service account is allowed.

Username	Role	Status
dsco	Administrator	Active
service	Service	Active

Add Edit Delete

Radius Authentication

Network Access ID: IP5 Default User Role: Administrator

Allow Local Authentication if all Radius Servers are Unresponsive

Primary Radius Server

Server IP Address: 192.168.165.29
 Authentication Port: 1812
 Timeout (seconds): 3
 Shared Secret: dsco

Secondary Radius Server (optional)

Console Authentication

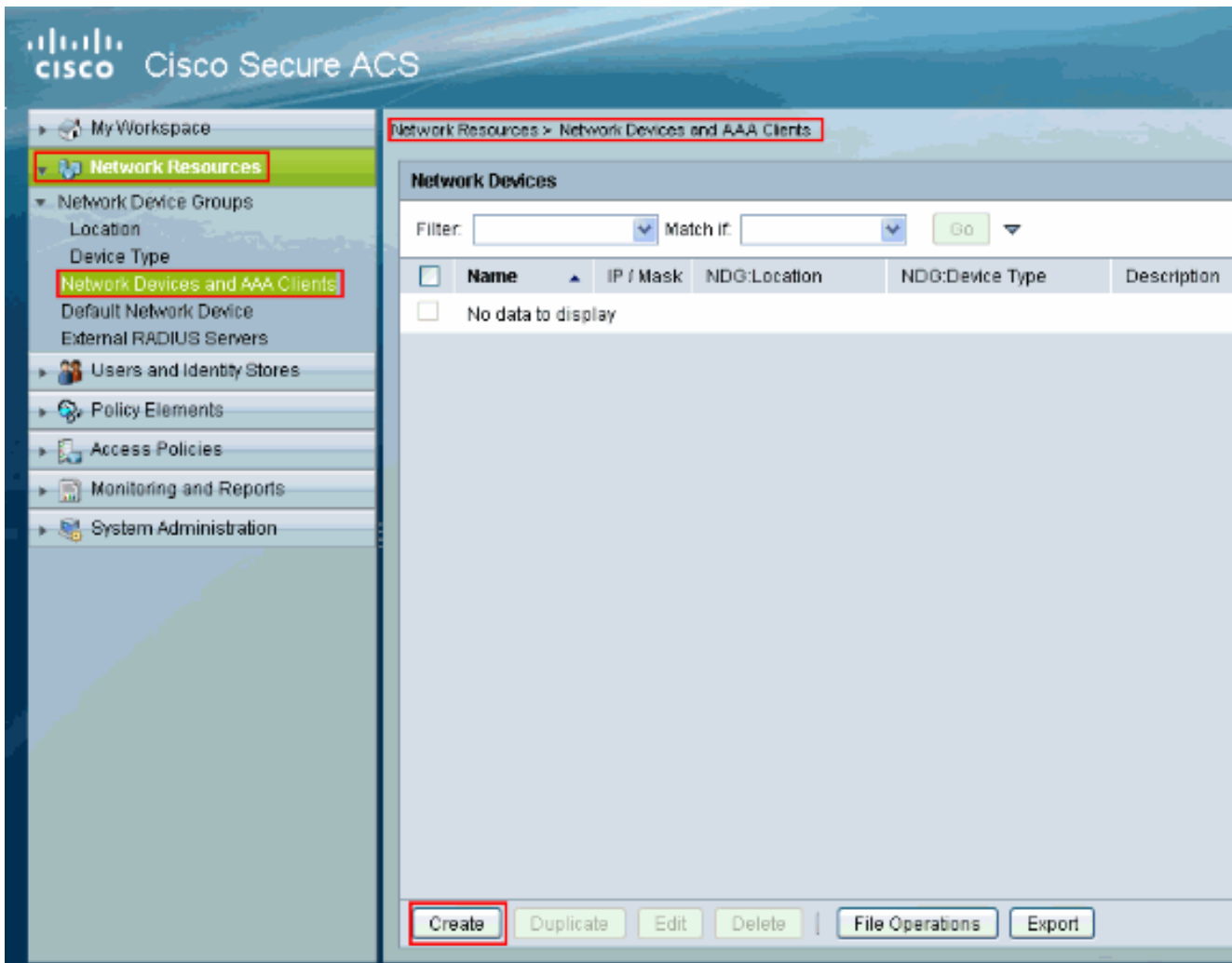
Console Authentication: Local and RADIUS

Apply Reset

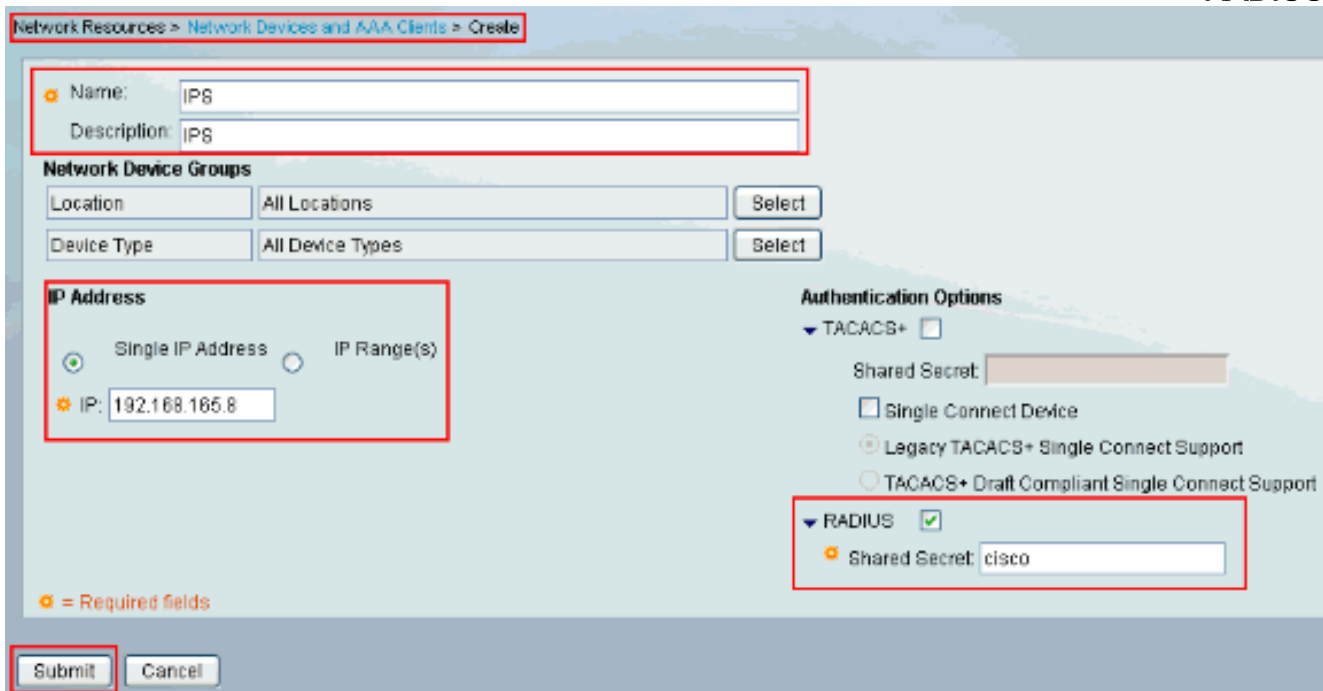
[تكوين ACS كخادم RADIUS](#)

أتمت هذا steps in order to شكلت ال ACS ك RADIUS نادل:

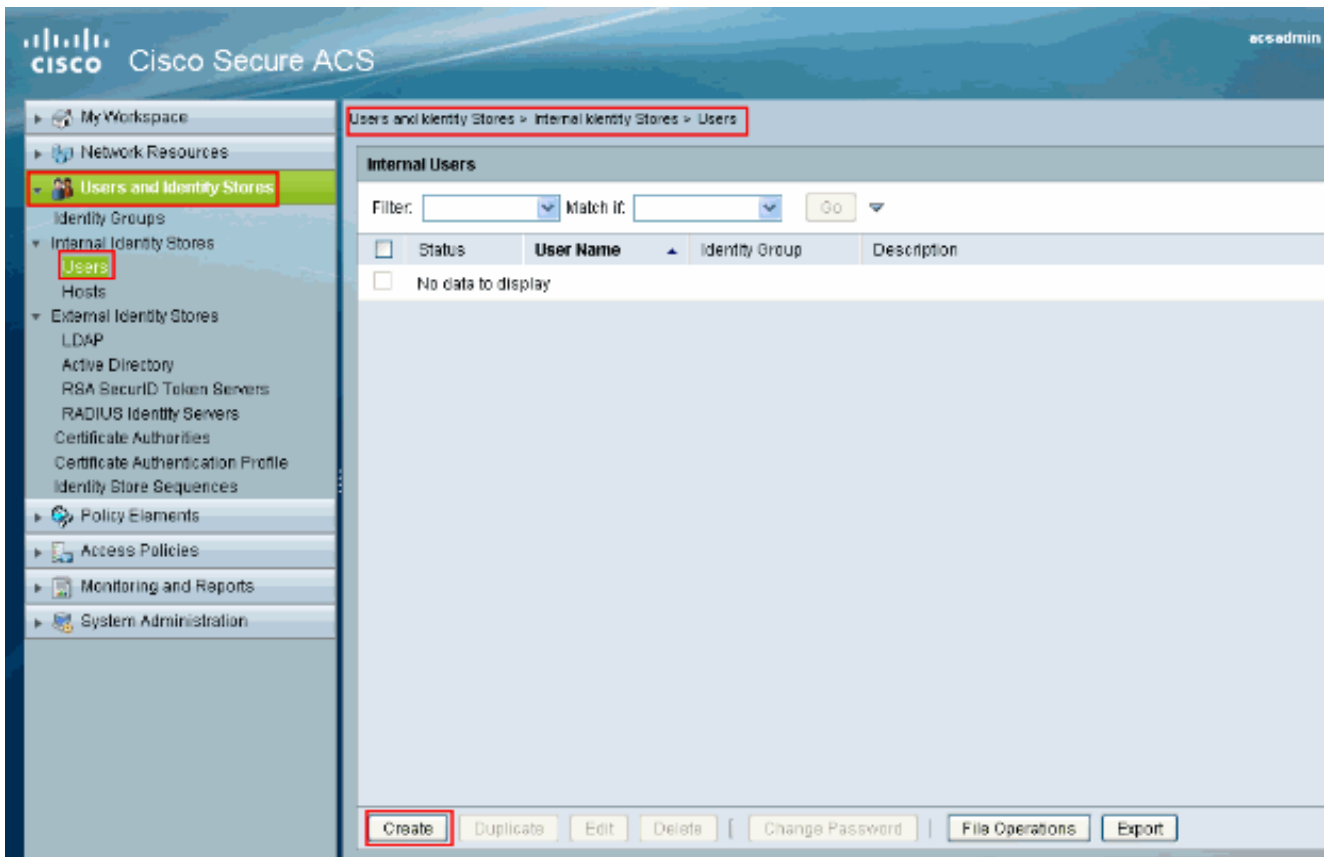
1. أخترت شبكة مورد<شبكة أداة و AAA زبون، وطقطقة يخلق in order to أضفت ال ips إلى ال acs نادل.



2. قم بتوفير المعلومات المطلوبة حول العميل (IPS هو العميل هنا)، وانقر فوق إرسال. وهذا يمكن IPS من الحصول على إضافة إلى خادم ACS. وتتضمن التفاصيل عنوان IP الخاص ب IPS وتفاصيل خادم RADIUS.



3. أختار المستخدمين ومخازن الهوية < مخازن الهوية الداخلية > المستخدمين، وانقر إنشاء لإنشاء مستخدم جديد.

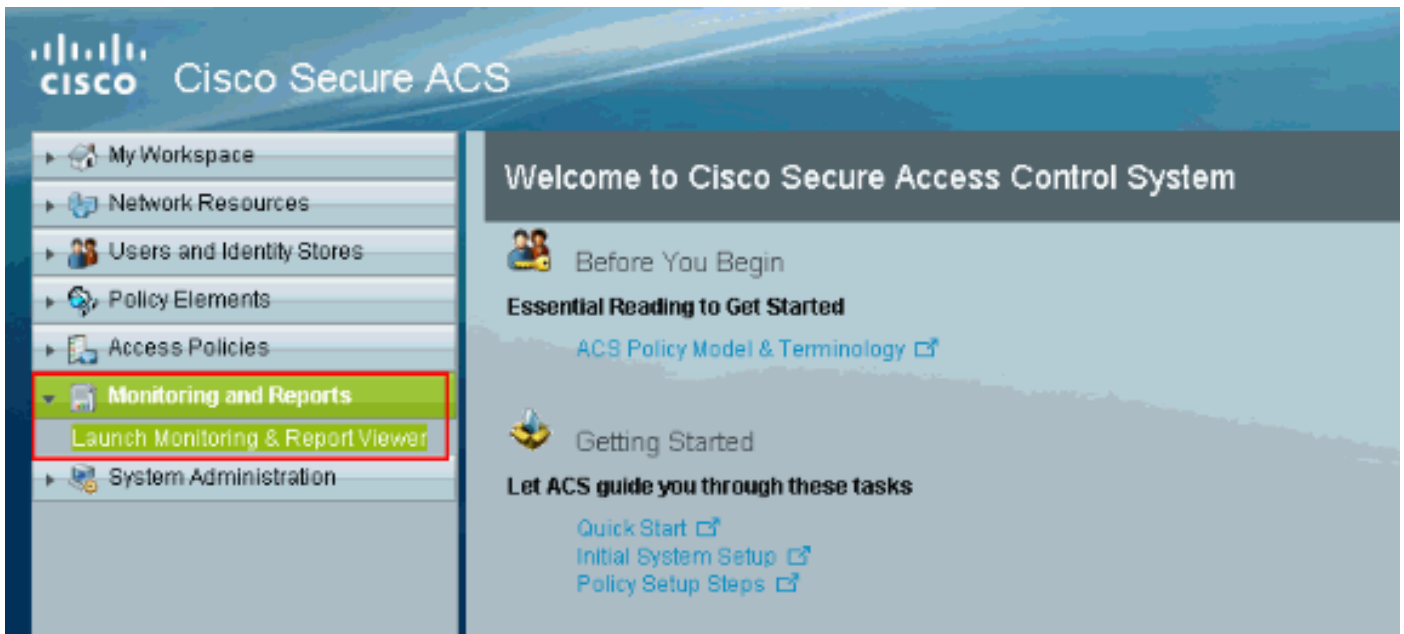


4. قم بتوفير معلومات الاسم وكلمة المرور. عند الانتهاء، انقر فوق إرسال.

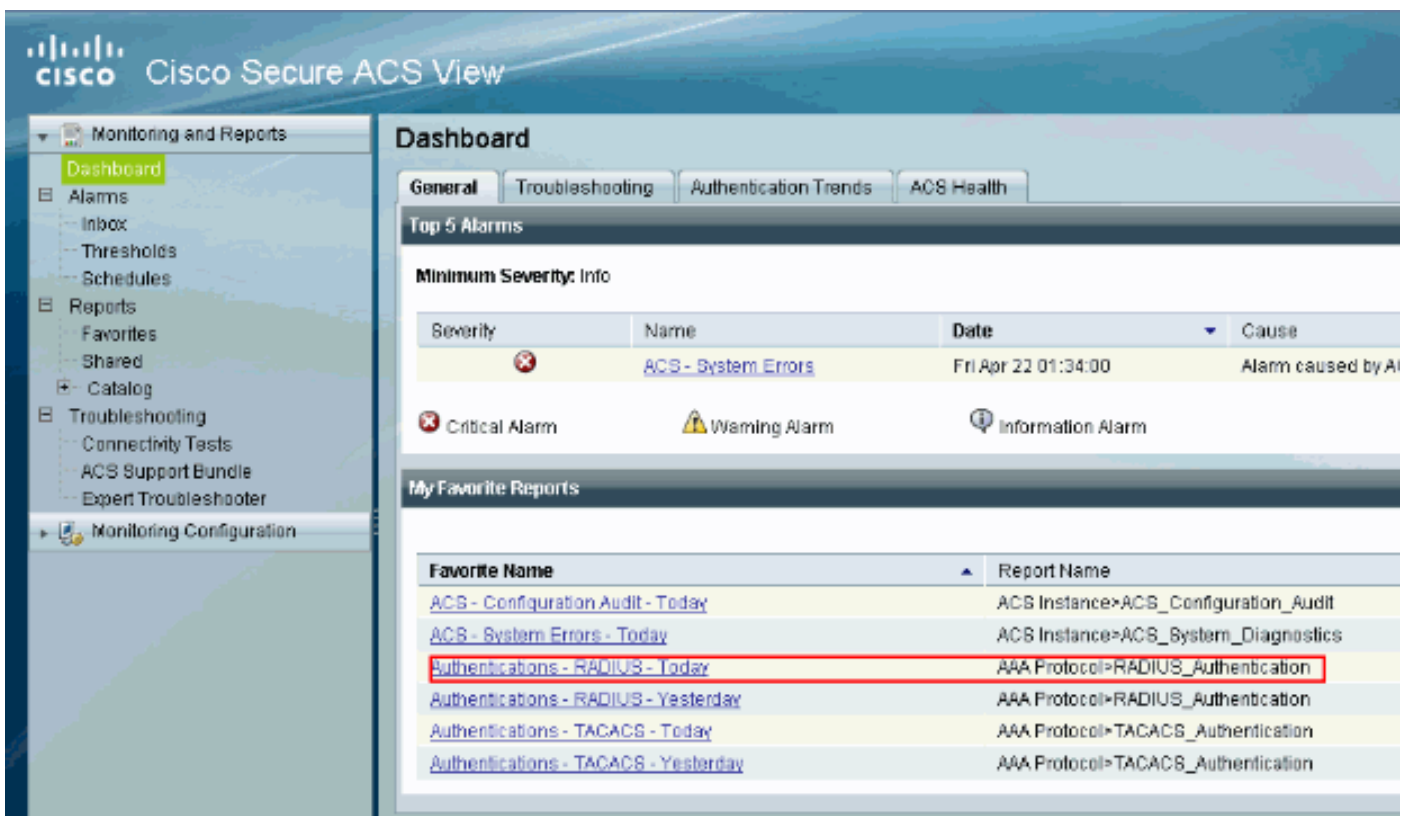
[التحقق من الصحة](#)

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

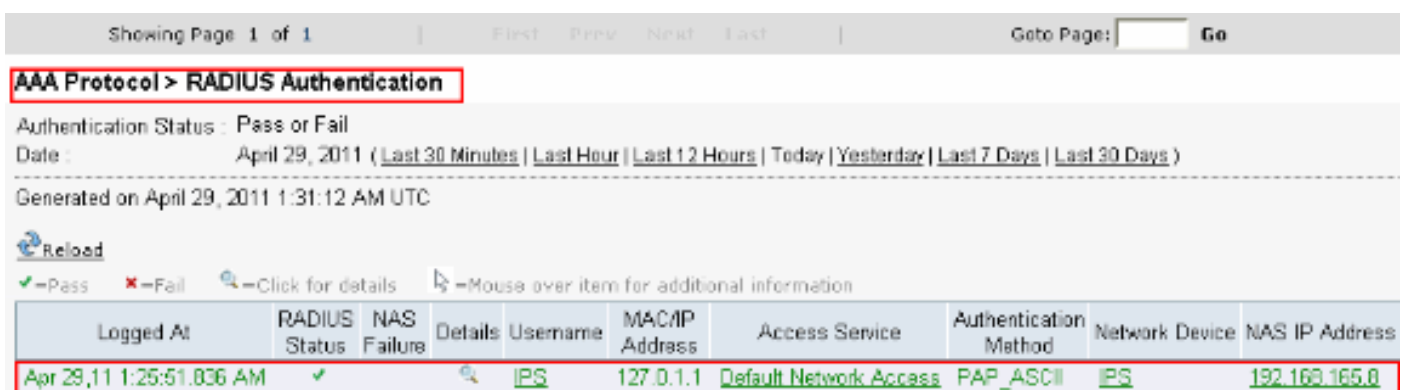
حاول تسجيل الدخول إلى IPS باستخدام المستخدم الذي تم إنشاؤه حديثًا. وفحص التقرير عن ACS بمجرد مصادقة المستخدم.



تقطعت ال authentication-RADIUS اليوم in order to شاهدت التقرير حالي.



تظهر هذه الصورة أن المستخدم الذي يتصل ب IPS مصدق بواسطة خادم ACS.



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

استكشاف الأخطاء وإصلاحها

لا تتوفر حاليًا معلومات محددة لاستكشاف الأخطاء وإصلاحها لهذا التكوين.

معلومات ذات صلة

- [صفحة دعم أجهزة الاستشعار Cisco IPS 4200 Series](#)
- [مراجع أوامر أجهزة الاستشعار Cisco IPS 4200 Series](#)
- [Cisco IPS Manager Express](#)
- [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 لوح

ةللأل تاي نقتل نم ةومچم مادختساب دن تسمل اذه Cisco تچرت
ملاعلاء انء مچي ف ني مدختسمل معد و تحم مي دقتل ةيرشبل او
امك ةقيد نوك تن ل ةللأل ةمچرت لصف أن ةظحال مچرئي. ةصاغل مه تلبل
Cisco يلخت. فرتحم مچرت مامدقي يتل ةيفارتحال ةمچرتل عم لالحل وه
ىل إأمئاد وچرلاب يصوت و تامچرتل هذه ةقदन ةتيلوئسم Cisco
Systems (رفوتم طبارل) يلصلأل يزي لچنل دن تسمل