ISE 2.0: ASA CLI TACACS+ للمصادقة وتكوين تفويض الأوامر مثال

المحتويات

المقدمة

يوضح هذا المستند كيفية تكوين مصادقة TACACS+ وتفويض الأوامر على جهاز الأمان القابل للتكيف (ASA) من Cisco باستخدام محرك خدمة الهوية (ISE) 2.0 والإصدارات الأحدث. يستخدم ISE مخزن الهوية المحلي لتخزين الموارد مثل المستخدمين والمجموعات ونقاط النهاية.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- جدار حماية ASA يعمل بشكل كامل
- الاتصال بين ASA و ISE
- خادم ISE تم تمهيده

المكونات المستخدمة

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

- Cisco Identity Service Engine 2.0
- برنامج Cisco ASA، الإصدار 9.5(1)

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.

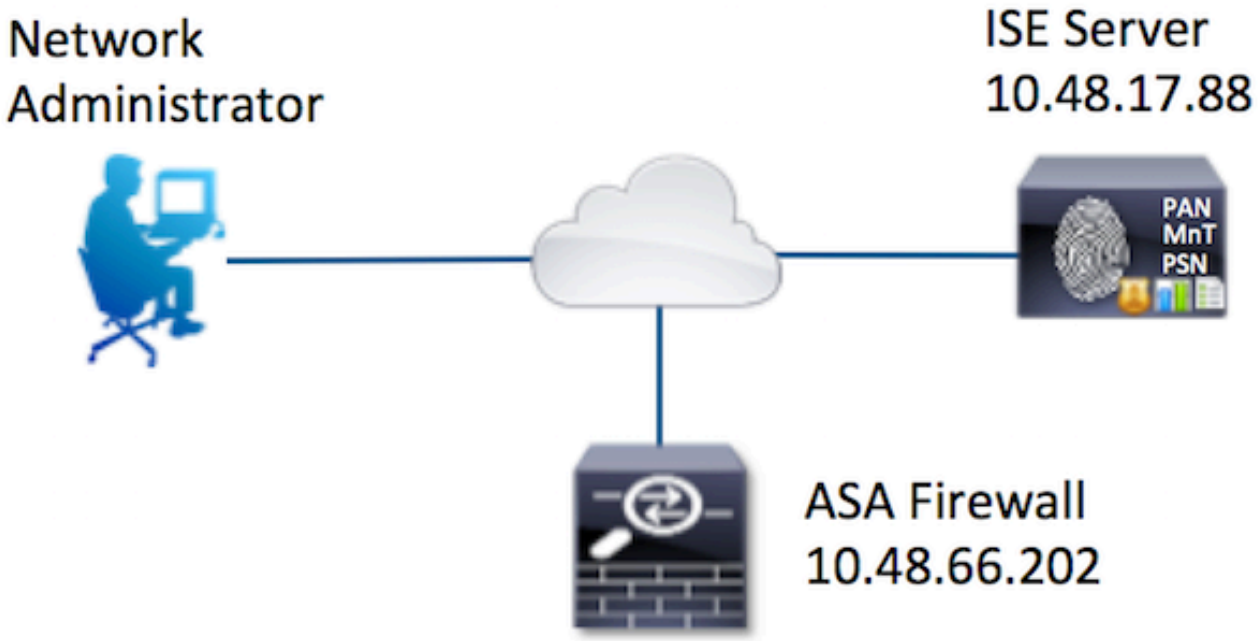
راجع اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.

التكوين

الهدف من التكوين هو:

- مصادقة مستخدم ssh عبر مخزن الهوية الداخلي
- قم بتخويل مستخدم ssh حتى يتم وضعه في وضع EXEC ذي الامتيازات بعد تسجيل الدخول
- تحقق من كل أمر يتم تنفيذه وإرساله إلى ISE للتحقق

الرسم التخطيطي للشبكة



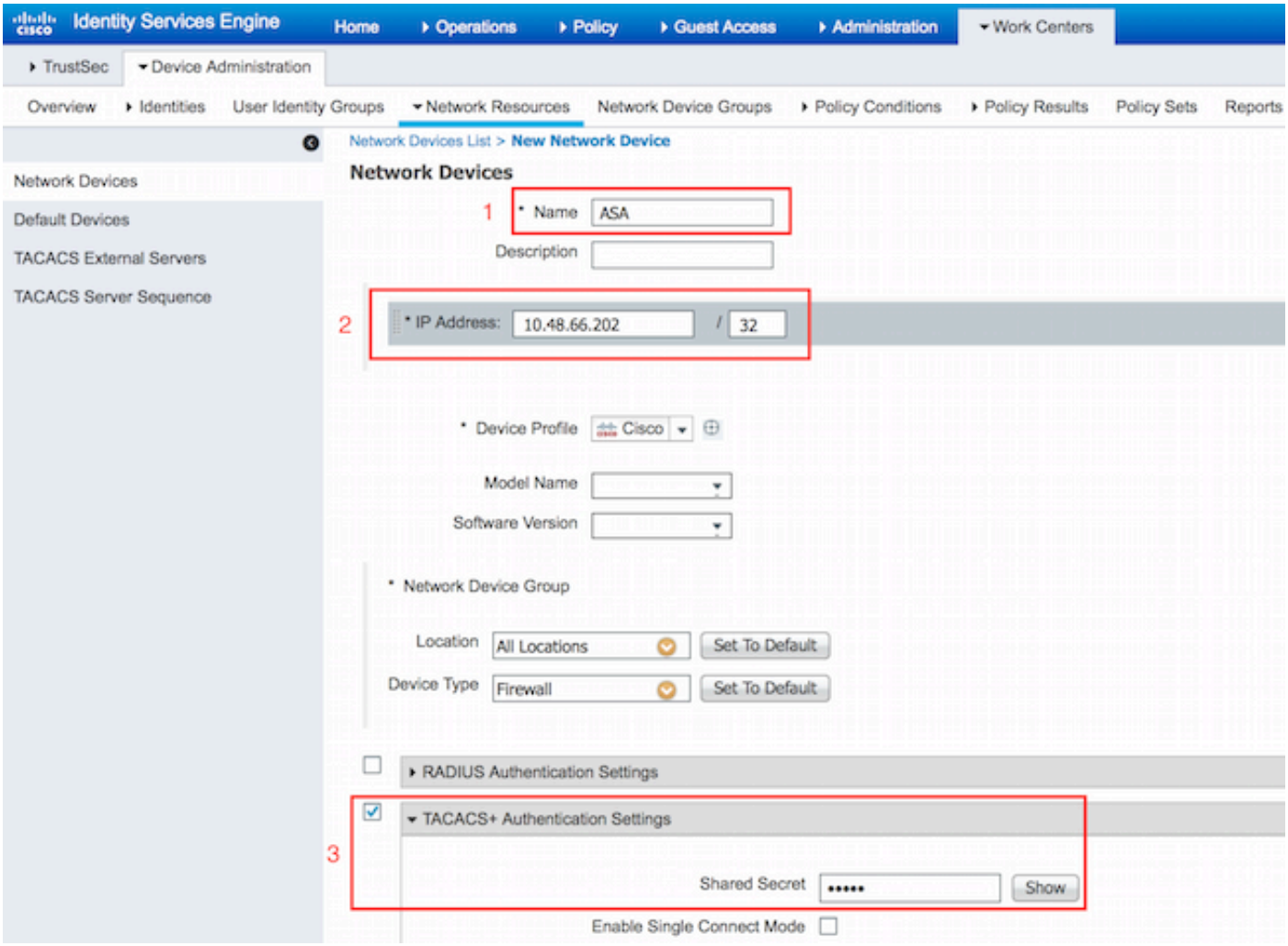
التكوينات

تكوين ISE للمصادقة والتفويض

تم إنشاء إثنين من المستخدمين. يعد **مسؤول** المستخدم جزءا من مجموعة الهوية المحلية **لمسؤولي الشبكات** على ISE. هذا المستخدم لديه امتيازات CLI كاملة. **المستخدم** جزء من مجموعة الهوية المحلية **لفريق صيانة الشبكة** على ISE. يسمح لهذا المستخدم بإظهار الأوامر واختبار الاتصال فقط.

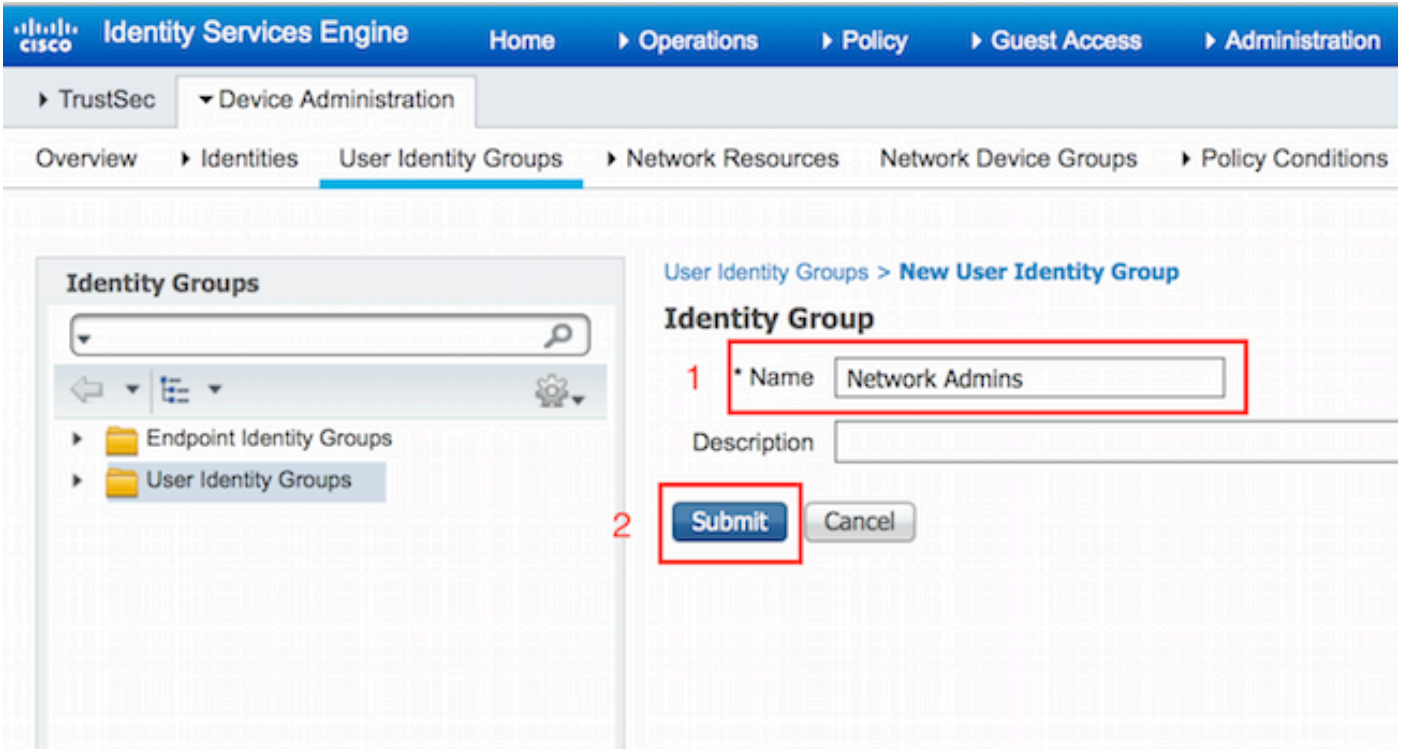
إضافة جهاز شبكة

انتقل إلى **مراكز العمل > إدارة الجهاز > موارد الشبكة > أجهزة الشبكة.** انقر فوق **إضافة (Add).** قم بتوفير الاسم وعنوان IP وحدد خانة الاختيار **لإعدادات مصادقة TACACS+** وقم بتوفير مفتاح **سري مشترك**. يمكن تحديد نوع/موقع الجهاز بشكل إختياري.



تكوين مجموعات هوية المستخدم

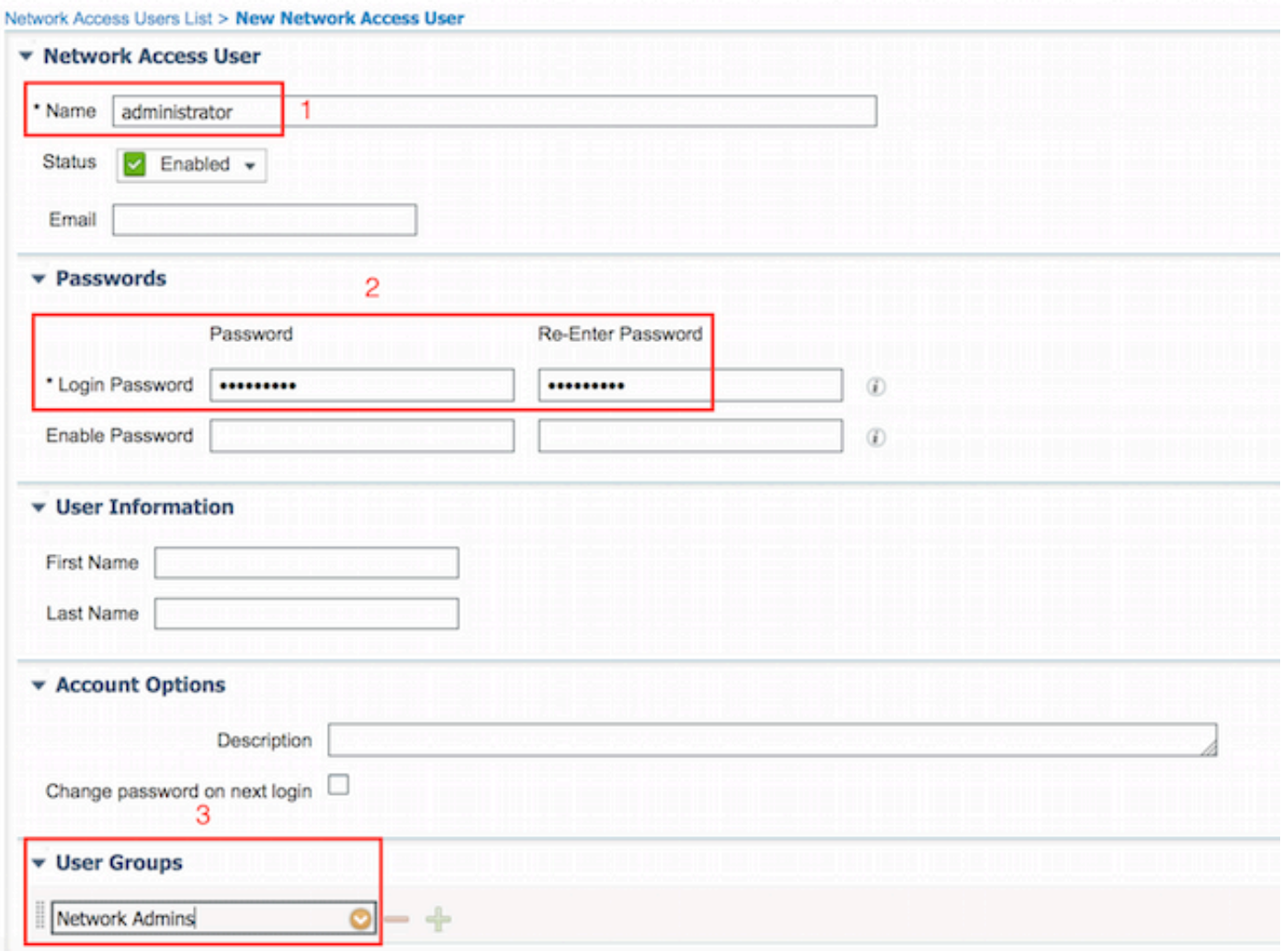
انتقل إلى **مراكز العمل > إدارة الجهاز > مجموعات هوية المستخدم.** انقر فوق **إضافة (Add).** قم بتوفير الاسم وانقر فوق **إرسال.**



كرر الخطوة نفسها لتكوين مجموعة هوية مستخدم **فريق صيانة الشبكة**.

تكوين المستخدمين

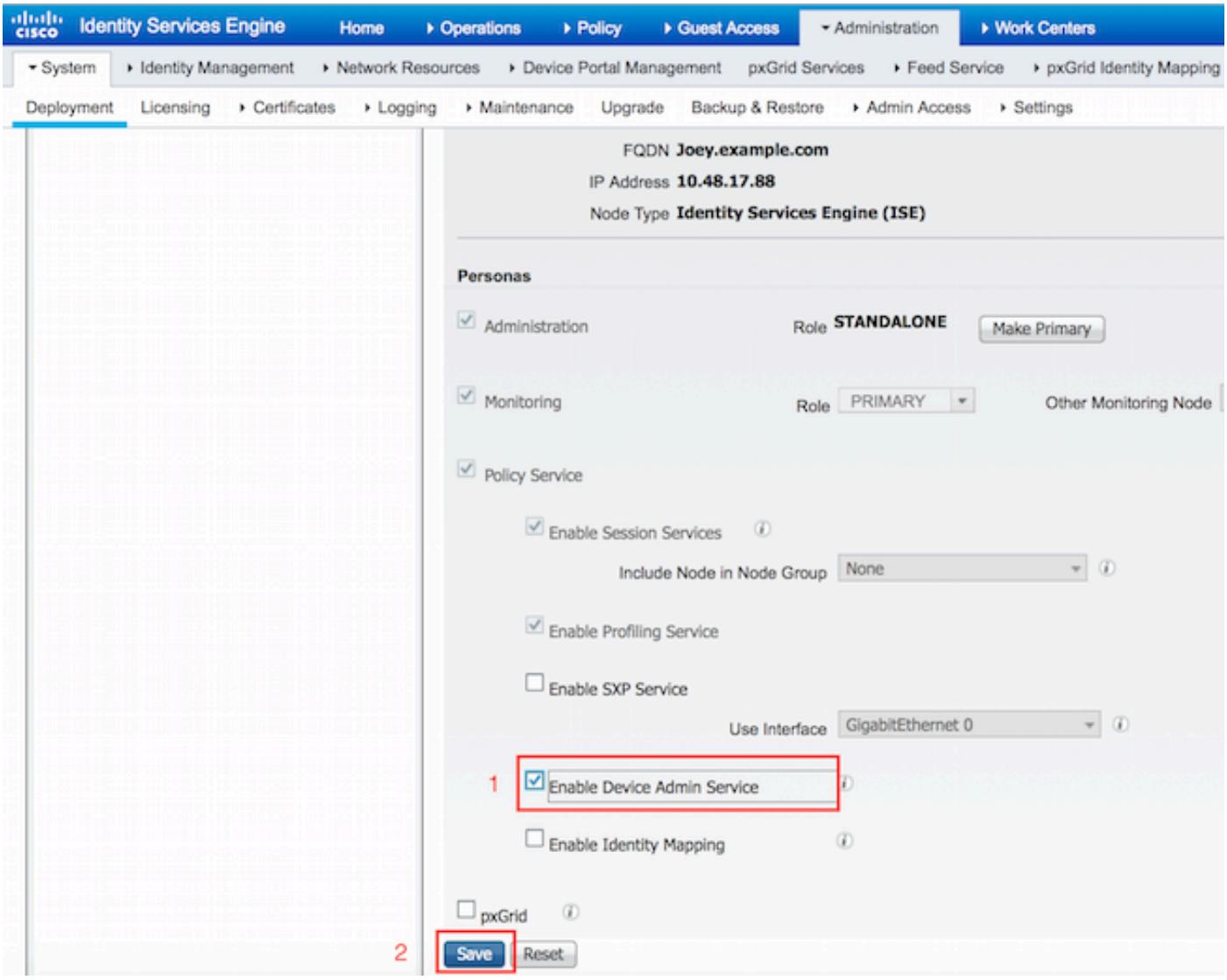
انتقل إلى **مراكز العمل > إدارة الأجهزة > الهويات > المستخدمين**. انقر فوق **إضافة (Add)**. أدخل الاسم، كلمة مرور تسجيل الدخول حدد مجموعة المستخدمين وانقر فوق **إرسال**.



كرر الخطوات لتكوين **مستخدم** وتعيين مجموعة معرف مستخدم **فريق صيانة الشبكة**.

تمكين خدمة إدارة الجهاز

انتقل إلى **الإدارة > النظام > النشر**. حدد العقدة المطلوبة. حدد خانة الاختيار **تمكين خدمة إدارة الجهاز** وانقر فوق **حفظ**.

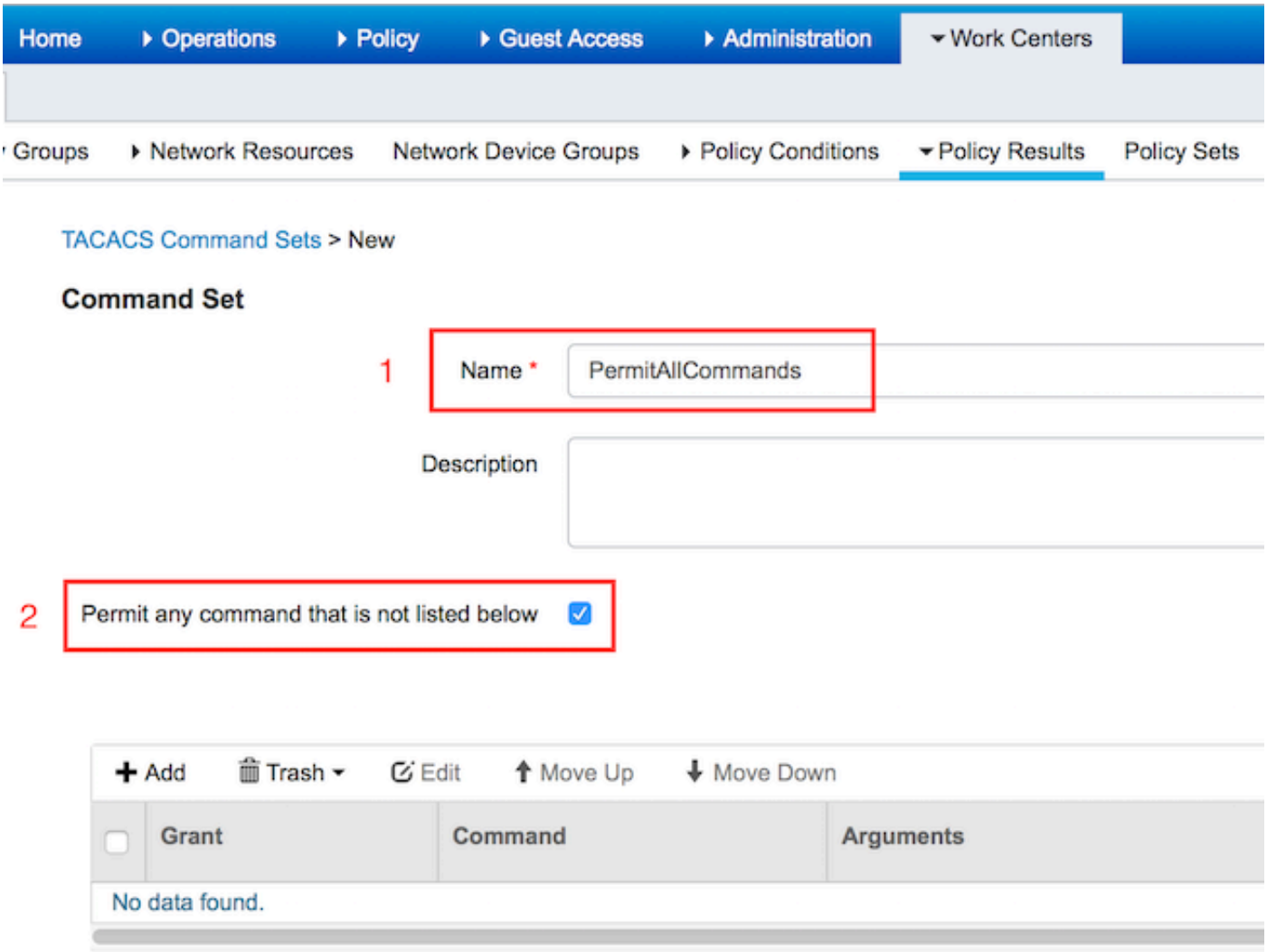


ملاحظة: بالنسبة إلى TACACS، يلزمك تثبيت ترخيص منفصل.

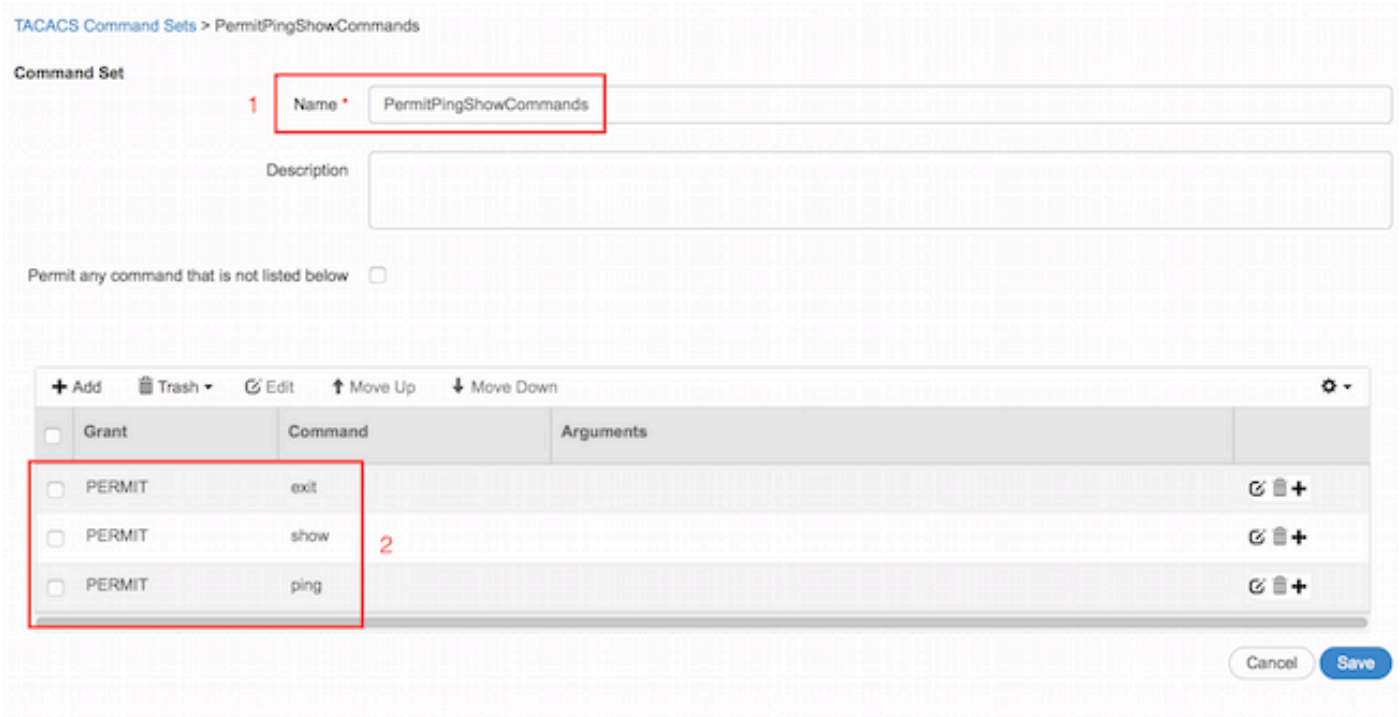
تكوين مجموعات أوامر TACACS

تم تكوين مجموعتين من الأوامر. أول **PermitAllCommands** لمستخدم **المسؤول** الذي يسمح بكل الأوامر على الجهاز. ثانيا **يسمحPingShowCommands** للمستخدم **المستخدم** الذي يسمح فقط بإظهار أوامر إختبار الاتصال.

1. انتقل إلى **مراكز العمل > إدارة الأجهزة > نتائج السياسة > مجموعات أوامر TACACS**. انقر فوق **إضافة (Add)**. قم بتوفير اسم **PermitAllCommands**، حدد **السماح بأي أمر غير مدرج أدناه** خانة الاختيار وانقر فوق **إرسال**.

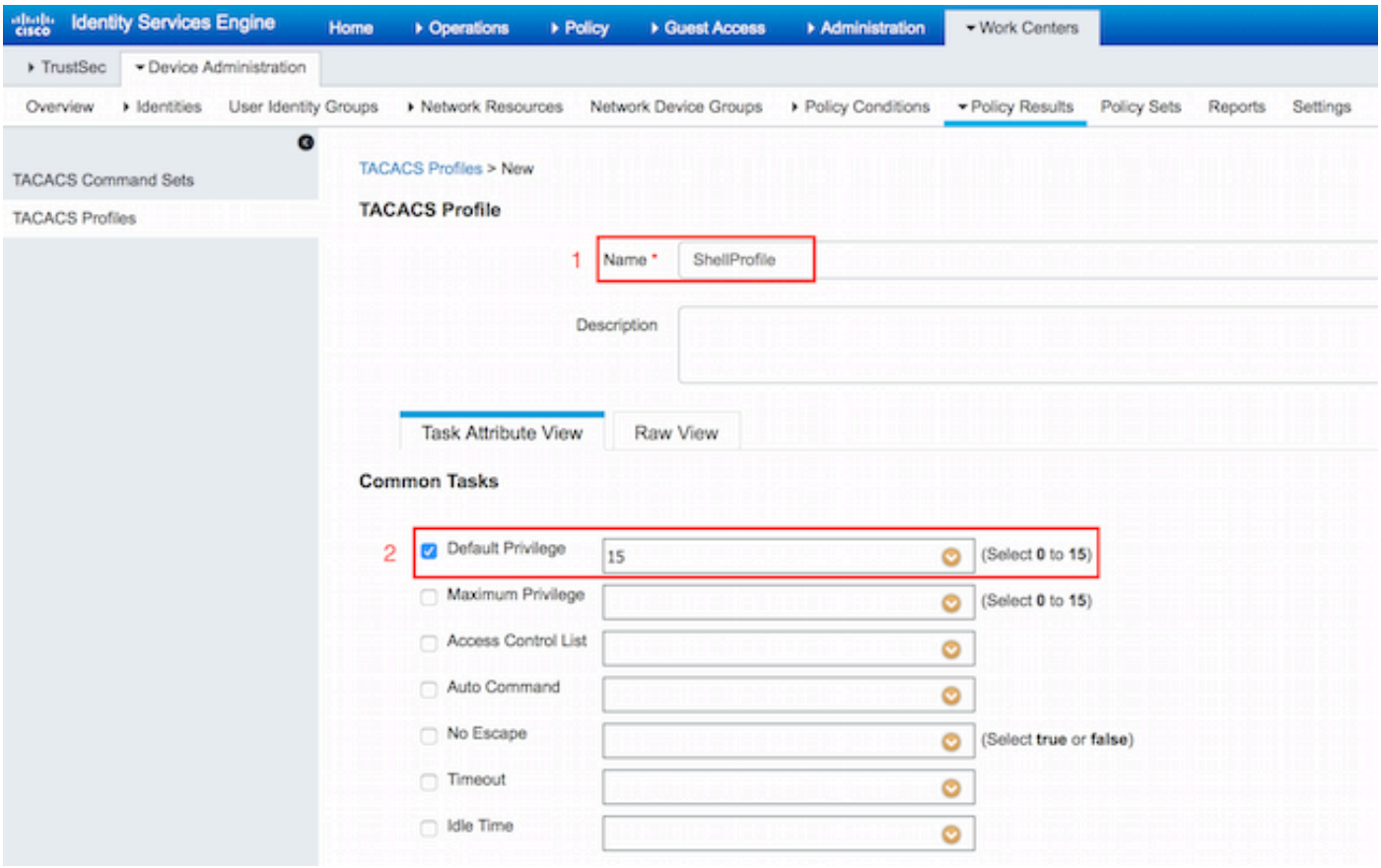


2. انتقل إلى **مراكز العمل > إدارة الأجهزة > نتائج السياسة > مجموعات أوامر TACACS**. انقر فوق **إضافة (Add)**. توفر الاسم **يسمح**pingShowCommands، انقر فوق **إضافة** والسماح **بإظهار**، **إختبار الاتصال و**أوامر الخروج. بشكل افتراضي، إذا تركت الوسيطات فارغة، يتم تضمين جميع الوسيطات. انقر على **إرسال.**



تكوين ملف تعريف TACACS

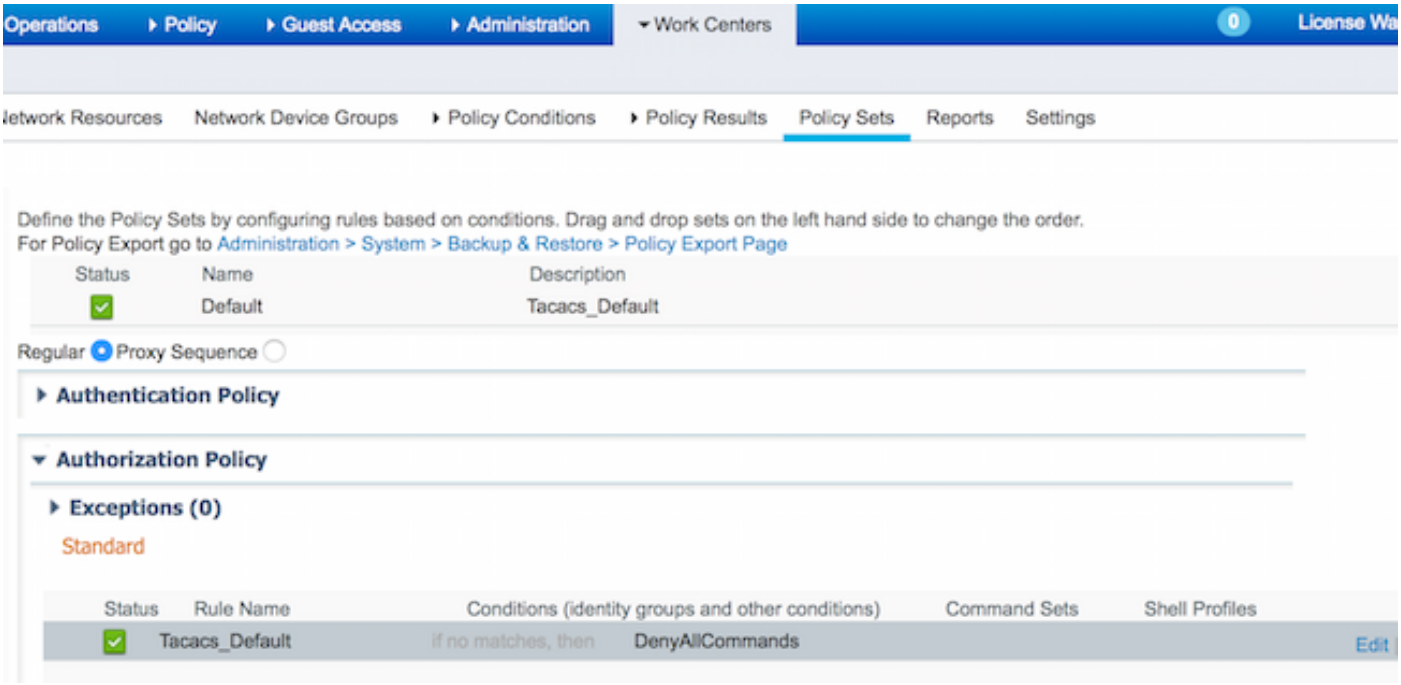
سيتم تكوين ملف تعريف TACACS أحادي. سيتم تنفيذ الأمر بشكل فعلي عبر مجموعات الأوامر. انتقل إلى **مراكز العمل > إدارة الأجهزة > نتائج السياسة > ملفات تعريف TACACS**. انقر فوق **إضافة (Add)**. قم بتوفير اسم **ShellProfile**، حدد خانة الاختيار **الافتراضي للامتياز** وأدخل القيمة 15. انقر على **إرسال**.



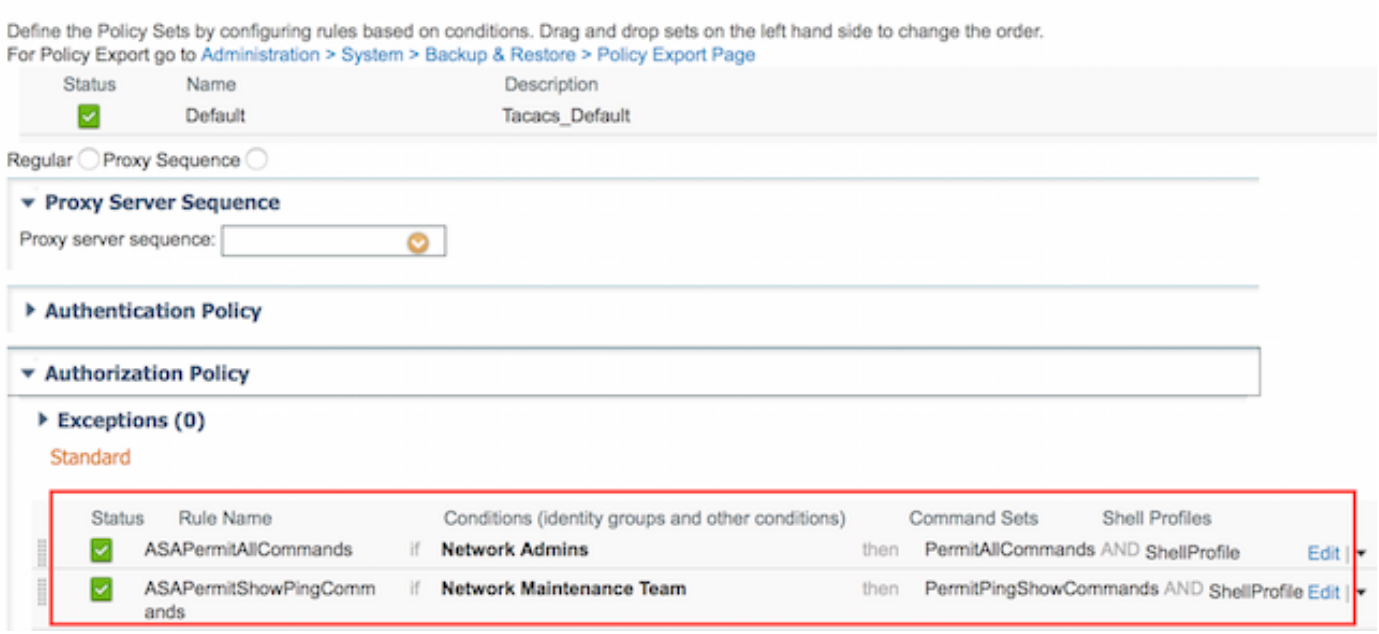
تكوين سياسة تفويض TACACS

يشير نهج المصادقة بشكل افتراضي إلى all_user_id_stores، التي تتضمن المتجر المحلي أيضا، لذلك لم يتغير.

انتقل إلى **مراكز العمل > إدارة الأجهزة > مجموعات السياسات > الافتراضي > نهج التخويل > تحرير > إدراج قاعدة جديدة أعلاه.**



تم تكوين قاعدتين للتخويل، تقوم القاعدة الأولى بتعيين **ملف تعريف** TACACS ShellProfile ومجموعة الأوامر PermitAllCommands استنادا إلى **مسؤولي الشبكة** عضوية مجموعة تعريف المستخدم. تعين القاعدة الثانية **توصيفات** ShellProfile TACACS ومجموعة الأوامر PermitPingShowCommands استنادا إلى عضوية مجموعة تعريف المستخدم ل **فريق صيانة الشبكة**.



تكوين جدار حماية Cisco ASA للمصادقة والتفويض

1. قم بإنشاء مستخدم محلي بامتياز كامل للتعيين الاحتياطي باستخدام الأمر **username** كما هو موضح هنا

```
ciscoasa(config)# username cisco password cisco privilege 15
```

2. حدد ISE لخادم TACACS، وحدد الواجهة وعنوان IP للبروتوكول ومفتاح **TACACS**.

```
+aaa-server ISE protocol tacacs
aaa-server ISE (mgmt) host 10.48.17.88
 key cisco
```

ملاحظة: يجب أن يتطابق مفتاح الخادم مع التعريف الموجود على خادم ISE في وقت سابق.

3. اختبر إمكانية الوصول إلى خادم TACACS باستخدام أمر الاختبار **aaa** كما هو موضح.

```
ciscoasa# test aaa authentication ISE host 10.48.17.88 username administrator Krakow123
(INFO: Attempting Authentication test to IP address <10.48.17.88> (timeout: 12 seconds
INFO: Authentication Successful
```

يوضح إخراج الأمر السابق أن خادم TACACS يمكن الوصول إليه وقد تمت مصادقة المستخدم بنجاح.

4. تكوين المصادقة ل SSH وتفويض EXEC وترخيص الأوامر كما هو موضح أدناه. باستخدام **تفويض AAA**، **يتم** وضع **مصادقة خادم EXEC تلقائيا** في وضع EXEC ذي الامتيازات تلقائيا.

```
aaa authentication ssh console ISE
aaa authorization command ISE
aaa authorization exec authentication-server auto-enable
```

ملاحظة: باستخدام الأوامر الواردة أعلاه، يتم إجراء المصادقة على ISE، يتم وضع المستخدم مباشرة في وضع الامتيازات ويتم تفويض الأوامر.

5. اسمح بالعرض على واجهة الإدارة.

```
ssh 0.0.0.0 0.0.0.0 mgmt
```

التحقق من الصحة

التحقق من جدار حماية Cisco ASA

1. SSH إلى جدار حماية ASA **كمسؤول** ينتمي إلى مجموعة معرف المستخدم للوصول الكامل. يتم تعيين مجموعة **مسؤولي الشبكة** إلى مجموعة أوامر **ShellProfile** و**AllowedAll** على ISE. حاول تشغيل أي أمر لضمان الوصول الكامل.

```
EKORNEYC-M-K04E:~ ekorneyc$ ssh administrator@10.48.66.202
:administrator@10.48.66.202's password
.Type help or '?' for a list of available commands
#ciscoasa
ciscoasa# configure terminal
ciscoasa(config)# crypto ikev1 policy 10
ciscoasa(config-ikev1-policy)# encryption aes
ciscoasa(config-ikev1-policy)# exit
ciscoasa(config)# exit
#ciscoasa
```

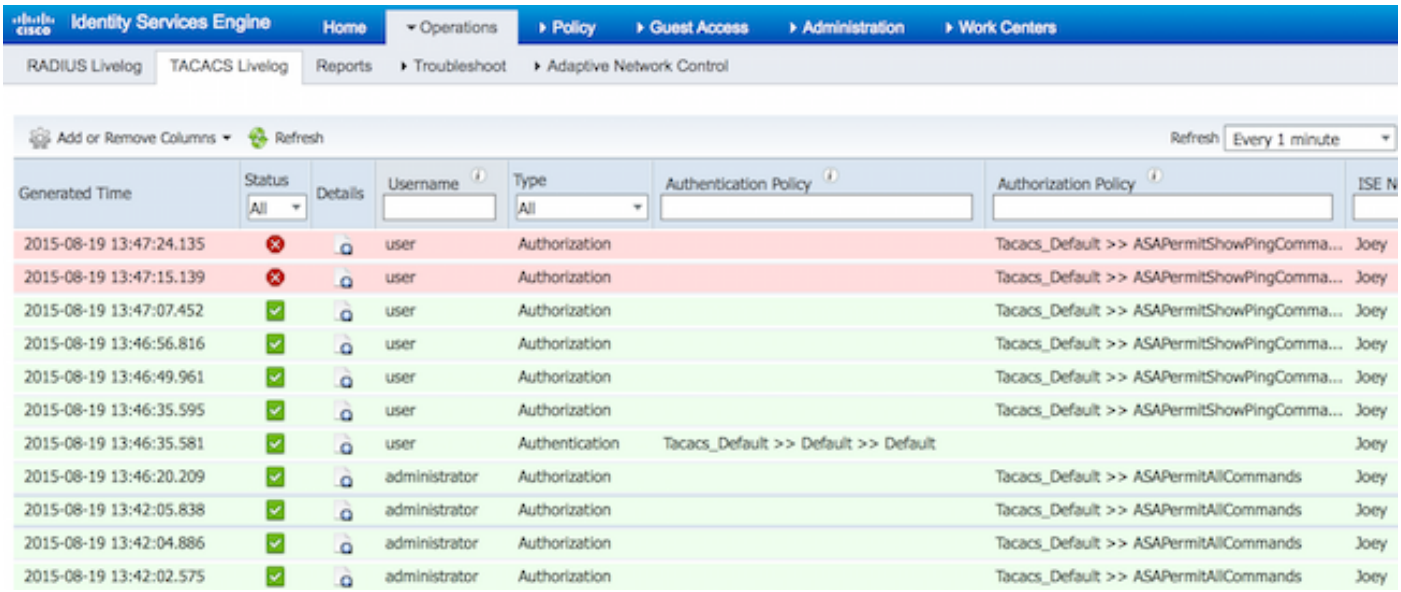
2. SSH إلى جدار حماية ASA **كمستخدم** ينتمي إلى مجموعة معرف المستخدم للوصول المحدود. يتم تعيين مجموعة **صيانة الشبكة** إلى **ShellProfile** ومجموعة أوامر **AllowPingShow** على ISE. حاول تشغيل أي أمر لضمان إمكانية إصدار أوامر show و ping فقط.

```
EKORNEYC-M-K04E:~ ekorneyc$ ssh user@10.48.66.202
:administrator@10.48.66.202's password
.Type help or '?' for a list of available commands
#ciscoasa
ciscoasa# show version | include Software
```

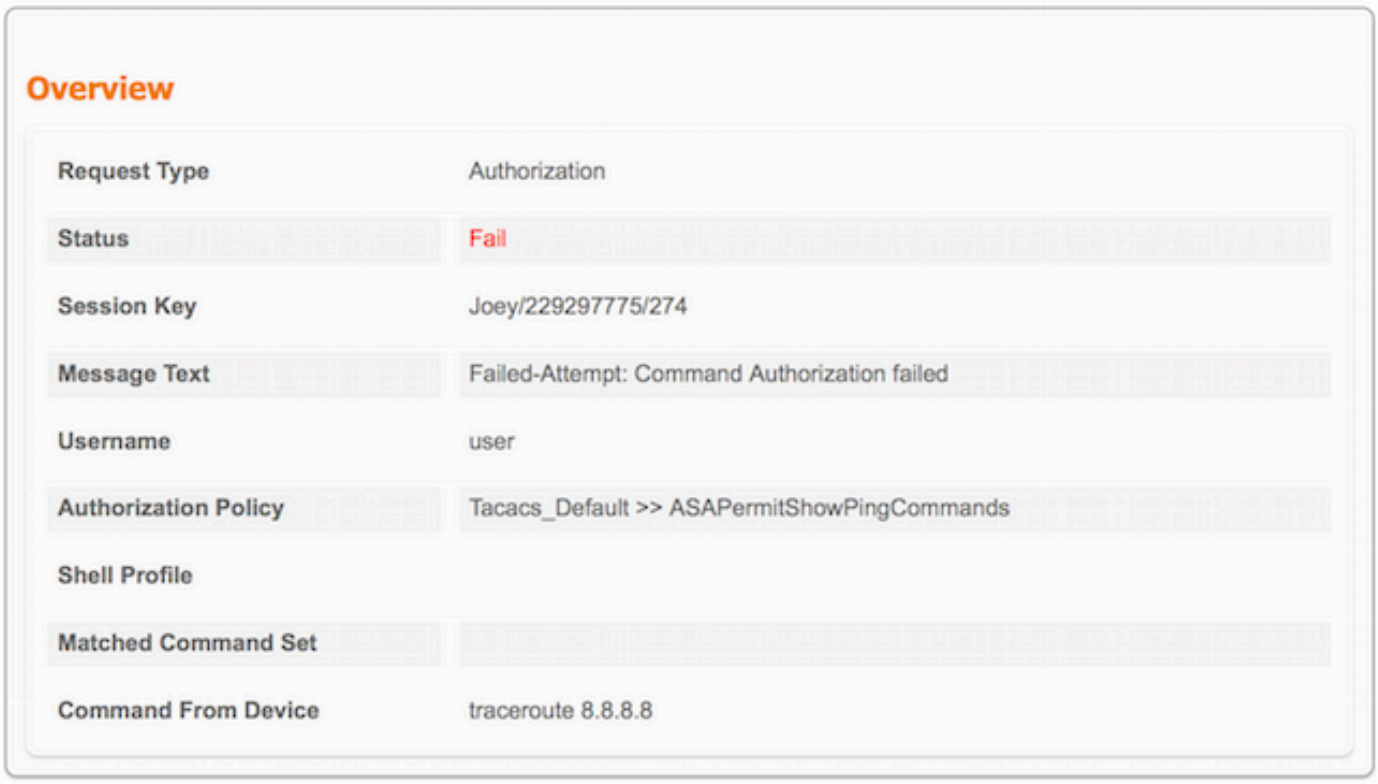
```
(Cisco Adaptive Security Appliance Software Version 9.5(1
                                                ciscoasa# ping 8.8.8.8
                                        .Type escape sequence to abort
                :Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds
                                                              !!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/24/30 ms
                                            ciscoasa# configure terminal
                                            Command authorization failed
                                            ciscoasa# traceroute 8.8.8.8
                                            Command authorization failed
```

التحقق من ISE 2.0

1. انتقل إلى **العمليات > TACACS Livelog**. تأكد من أن المحاولات المذكورة أعلاه ظاهرة للعيان.



2. انقر فوق تفاصيل أحد التقارير الحمراء، يمكن رؤية الأمر الذي فشل تنفيذه في وقت سابق.



استكشاف الأخطاء وإصلاحها

خطأ: فشل المحاولة: فشل تفويض الأوامر

تحقق من سمات SelectedCommandSet للتحقق من تحديد مجموعات الأوامر المتوقعة من خلال نهج التخويل

معلومات ذات صلة

الدعم التقني والمستندات - Cisco Systems

ملاحظات إصدار ISE 2.0

دليل تثبيت الأجهزة ISE 2.0

دليل ترقية ISE 2.0

مصدر المحتوى الإضافي لدليل أداة ترحيل ISE

دليل تكامل ISE 2.0 Active Directory

دليل مسؤول محرك ISE 2.0

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).