

ةق داصم ل ل ISE 2.0: ASA CLI TACACS+ لاثم رماوأل اضي وفت ني وكتو

المحتويات

- [المقدمة](#)
- [المتطلبات الأساسية](#)
- [المتطلبات](#)
- [المكونات المستخدمة](#)
- [التكوين](#)
- [الرسم التخطيطي للشبكة](#)
- [التكوينات](#)
- [تكوين ISE للمصادقة والتفويض](#)
- [إضافة جهاز شبكة](#)
- [تكوين مجموعات هوية المستخدم](#)
- [تكوين المستخدمين](#)
- [تمكين خدمة إدارة الجهاز](#)
- [تكوين مجموعات أوامر TACACS](#)
- [تكوين ملف تعريف TACACS](#)
- [تكوين سياسة تفويض TACACS](#)
- [تكوين جدار حماية Cisco ASA للمصادقة والتفويض](#)
- [التحقق من الصحة](#)
- [التحقق من جدار حماية Cisco ASA](#)
- [التحقق من ISE 2.0](#)
- [استكشاف الأخطاء وإصلاحها](#)
- [معلومات ذات صلة](#)
- [مناقشات مجتمع دعم Cisco ذات الصلة](#)

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 ISE و ASA
- 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.

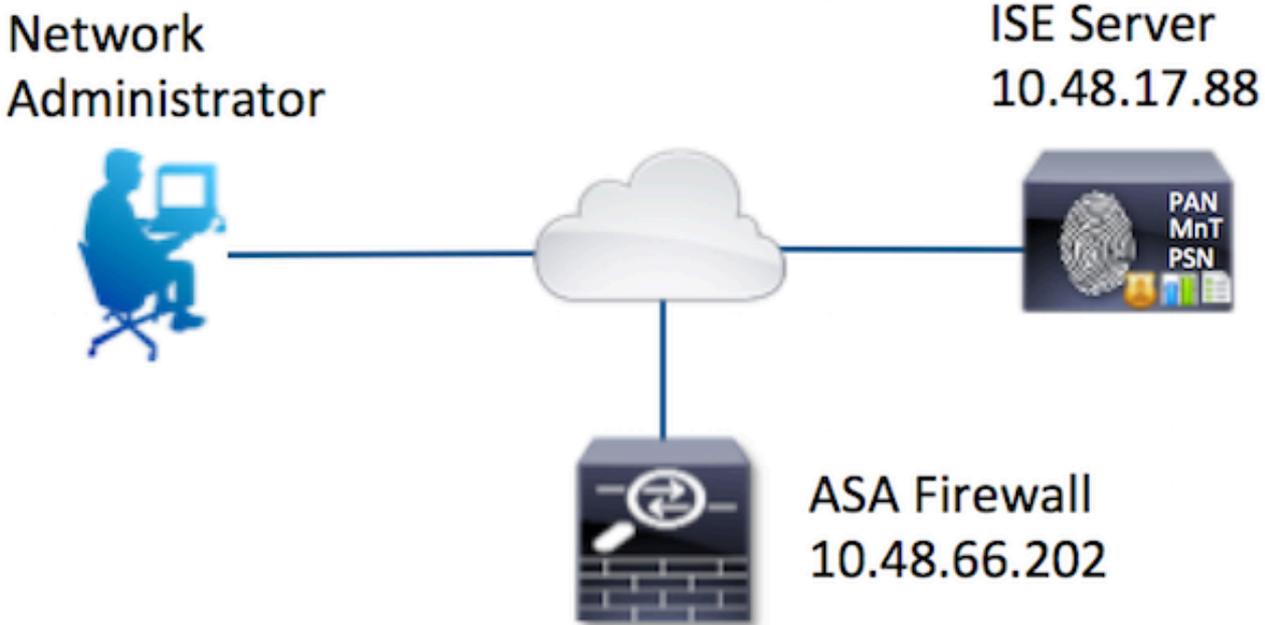
راجع [اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.](#)

التكوين

الهدف من التكوين هو:

- مصادقة مستخدم ssh عبر مخزن الهوية الداخلي
- قم بتحويل 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



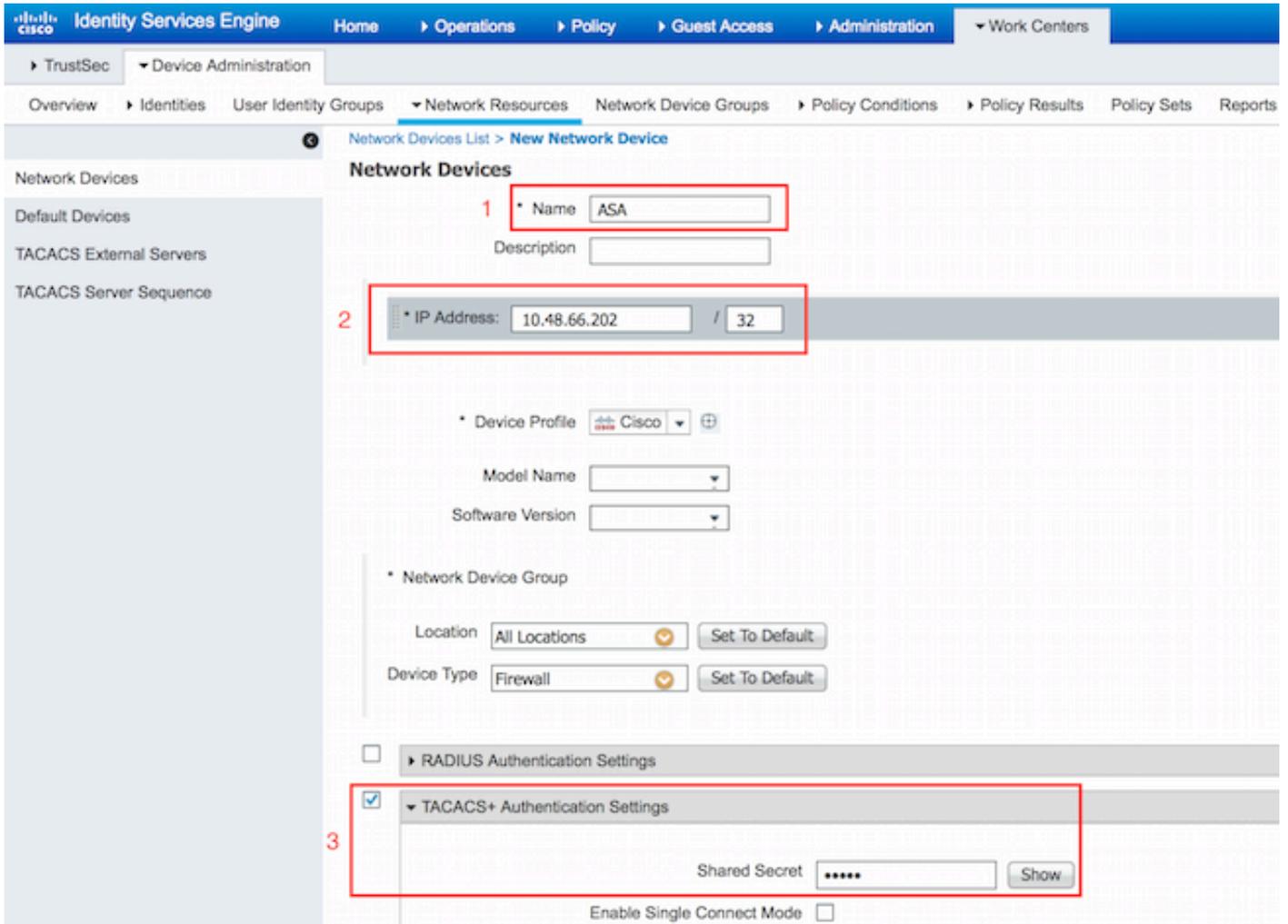
التكوينات

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 اختياري.



The screenshot displays the 'New Network Device' configuration page in the Cisco Identity Services Engine (ISE) interface. The page is divided into several sections:

- Network Devices List > New Network Device**: The main heading.
- Network Devices**: The main configuration area, containing:
 - Name**: A text input field containing 'ASA', highlighted with a red box and labeled '1'.
 - Description**: An empty text input field.
 - IP Address**: A text input field containing '10.48.66.202' and a dropdown menu set to '32', highlighted with a red box and labeled '2'.
 - Device Profile**: A dropdown menu set to 'Cisco'.
 - Model Name**: An empty dropdown menu.
 - Software Version**: An empty dropdown menu.
 - Network Device Group**:
 - Location**: A dropdown menu set to 'All Locations' with a 'Set To Default' button.
 - Device Type**: A dropdown menu set to 'Firewall' with a 'Set To Default' button.
 - RADIUS Authentication Settings**: A section with a checkbox that is unchecked.
 - TACACS+ Authentication Settings**: A section with a checked checkbox, highlighted with a red box and labeled '3'. It contains a 'Shared Secret' field with masked characters and a 'Show' button.
 - Enable Single Connect Mode**: A checkbox that is unchecked.

تكوين مجموعات هوية المستخدم

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

Identity Services Engine Home Operations Policy Guest Access Administration

TrustSec Device Administration

Overview Identities User Identity Groups Network Resources Network Device Groups Policy Conditions

Identity Groups

User Identity Groups > New User Identity Group

Identity Group

1 * Name Network Admins

Description

2 Submit Cancel

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.

Network Access User

* Name 1

Status Enabled

Email

Passwords 2

Password Re-Enter Password

* Login Password ⓘ

Enable Password ⓘ

User Information

First Name

Last Name

Account Options

Description

Change password on next login

User Groups 3

ⓘ - +

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.

Identity Services Engine Home Operations Policy Guest Access Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service pxGrid Identity Mapping

Deployment Licensing Certificates Logging Maintenance Upgrade Backup & Restore Admin Access Settings

FQDN **Joey.example.com**
 IP Address **10.48.17.88**
 Node Type **Identity Services Engine (ISE)**

Personas

Administration Role **STANDALONE** Make Primary

Monitoring Role **PRIMARY** Other Monitoring Node

Policy Service

Enable Session Services i
 Include Node in Node Group **None** i

Enable Profiling Service

Enable SXP Service i
 Use Interface **GigabitEthernet 0** i

1 **Enable Device Admin Service** i

Enable Identity Mapping i

pxGrid i

2 Save Reset

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. ثانياً يسمح **PingShowCommands** للمستخدم المستخدم الذي يسمح فقط بإظهار أوامر اختبار 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.

TACACS Command Sets > New

Command Set

1

Name * PermitAllCommands

Description

2

Permit any command that is not listed below

<input type="checkbox"/>	Grant	Command	Arguments
No data found.			

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، اختبار الاتصال وأوامر الخروج. بشكل افتراضي، إذا تركت الوسيطات فارغة، يتم تضمين جميع الوسيطات. انقر على إرسال.

TACACS Command Sets > PermitPingShowCommands

Command Set

1

Name * PermitPingShowCommands

Description

Permit any command that is not listed below

<input type="checkbox"/>	Grant	Command	Arguments	
<input type="checkbox"/>	PERMIT	exit		
<input type="checkbox"/>	PERMIT	show		
<input type="checkbox"/>	PERMIT	ping		

2

Cancel Save

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.

The screenshot shows the Cisco Identity Services Engine (ISE) configuration interface for a new TACACS Profile. The page is titled "TACACS Profiles > New" and "TACACS Profile". The "Name" field is set to "ShellProfile" and is highlighted with a red box. The "Description" field is empty. Below the "Name" field, there are two tabs: "Task Attribute View" (selected) and "Raw View". Under the "Common Tasks" section, the "Default Privilege" dropdown menu is set to "15" and is highlighted with a red box. Other options include "Maximum Privilege", "Access Control List", "Auto Command", "No Escape", "Timeout", and "Idle Time", each with a dropdown menu. The "No Escape" dropdown menu has a note "(Select true or false)".

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 التحويل < تحرير < إدراج قاعدة جديدة أعلاه.

Operations Policy Guest Access Administration Work Centers 0 License Wa

Network Resources Network Device Groups Policy Conditions Policy Results Policy Sets Reports Settings

Define the Policy Sets by configuring rules based on conditions. Drag and drop sets on the left hand side to change the order.
For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

Status	Name	Description
<input checked="" type="checkbox"/>	Default	Tacacs_Default

Regular Proxy Sequence

Authentication Policy

Authorization Policy

Exceptions (0)

Standard

Status	Rule Name	Conditions (identity groups and other conditions)	Command Sets	Shell Profiles
<input checked="" type="checkbox"/>	Tacacs_Default	if no matches, then	DenyAllCommands	

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

Define the Policy Sets by configuring rules based on conditions. Drag and drop sets on the left hand side to change the order.
For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

Status	Name	Description
<input checked="" type="checkbox"/>	Default	Tacacs_Default

Regular Proxy Sequence

Proxy Server Sequence

Proxy server sequence:

Authentication Policy

Authorization Policy

Exceptions (0)

Standard

Status	Rule Name	Conditions (identity groups and other conditions)	Command Sets	Shell Profiles
<input checked="" type="checkbox"/>	ASAPermitAllCommands	if Network Admins	then PermitAllCommands AND ShellProfile	Edit
<input checked="" type="checkbox"/>	ASAPermitShowPingComm ands	if Network Maintenance Team	then PermitPingShowCommands AND ShellProfile	Edit

تكوين جدار حماية Cisco ASA للمصادقة والتفويض

1. قم بإنشاء مستخدم محلي بامتياز كامل للتعين 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 تلقائياً في وضع EXEC ذي الامتيازات تلقائياً.

```
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.

Generated Time	Status	Details	Username	Type	Authentication Policy	Authorization Policy	ISE N
2015-08-19 13:47:24.135	✘		user	Authorization	Tacacs_Default >> ASAPermitShowPingComma...	Joey	
2015-08-19 13:47:15.139	✘		user	Authorization	Tacacs_Default >> ASAPermitShowPingComma...	Joey	
2015-08-19 13:47:07.452	✔		user	Authorization	Tacacs_Default >> ASAPermitShowPingComma...	Joey	
2015-08-19 13:46:56.816	✔		user	Authorization	Tacacs_Default >> ASAPermitShowPingComma...	Joey	
2015-08-19 13:46:49.961	✔		user	Authorization	Tacacs_Default >> ASAPermitShowPingComma...	Joey	
2015-08-19 13:46:35.595	✔		user	Authorization	Tacacs_Default >> ASAPermitShowPingComma...	Joey	
2015-08-19 13:46:35.581	✔		user	Authentication	Tacacs_Default >> Default >> Default	Joey	
2015-08-19 13:46:20.209	✔		administrator	Authorization	Tacacs_Default >> ASAPermitAllCommands	Joey	
2015-08-19 13:42:05.838	✔		administrator	Authorization	Tacacs_Default >> ASAPermitAllCommands	Joey	
2015-08-19 13:42:04.886	✔		administrator	Authorization	Tacacs_Default >> ASAPermitAllCommands	Joey	
2015-08-19 13:42:02.575	✔		administrator	Authorization	Tacacs_Default >> ASAPermitAllCommands	Joey	

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

Overview

Request Type	Authorization
Status	Fail
Session Key	Joey/229297775/274
Message Text	Failed-Attempt: Command Authorization failed
Username	user
Authorization Policy	Tacacs_Default >> ASAPermitShowPingCommands
Shell Profile	
Matched Command Set	
Command From Device	traceroute 8.8.8.8

استكشاف الأخطاء وإصلاحها

خطأ: فشل المحاولة: فشل تفويض الأوامر

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

معلومات ذات صلة

[الدعم التقني والمستندات - Cisco Systems](#)

[ملاحظات إصدار ISE 2.0](#)

[دليل تشيئ 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](#)

ةمچرتل هذه لوج

ةللأل تاي نقتل نمة ومة مادختساب دن تسمل اذة Cisco تمةرت
ملاعلاء انء مء مء نمة دختسمل معد و تمة مء دقتل ةر شبل او
امك ةق قء نوك ت نل ةللأل ةمچرت لصف أن ةظحال مء ءرء. ةصاأل مء تءل ب
Cisco ةلخت. فرتمة مچرت مء دقء ةل ةل ةفارتحال ةمچرتل عم لاعل او
ىل إأمءءاد ءوچرلاب ةصوء و تامةرتل هذه ةقء نء اهءل وئس م Cisco
Systems (رفوتم طبارل) ةلصلأل ةزءل ءنل دن تسمل