ISE 2.0:ASA CLI TACACS+驗證和命令授權配置示例

目錄

簡介

本檔案介紹如何在具有身分識別服務引擎(ISE)2.0及更新版本的思科調適型安全裝置(ASA)上設定TACACS+驗證和命令授權。ISE使用本地身份儲存來儲存資源，如使用者、組和終端。

必要條件

需求

思科建議您瞭解以下主題：

- ASA防火牆完全正常運行
- ASA和ISE之間的連線
- ISE伺服器已引導

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 思科身分識別服務引擎2.0
- Cisco ASA軟體版本9.5(1)

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

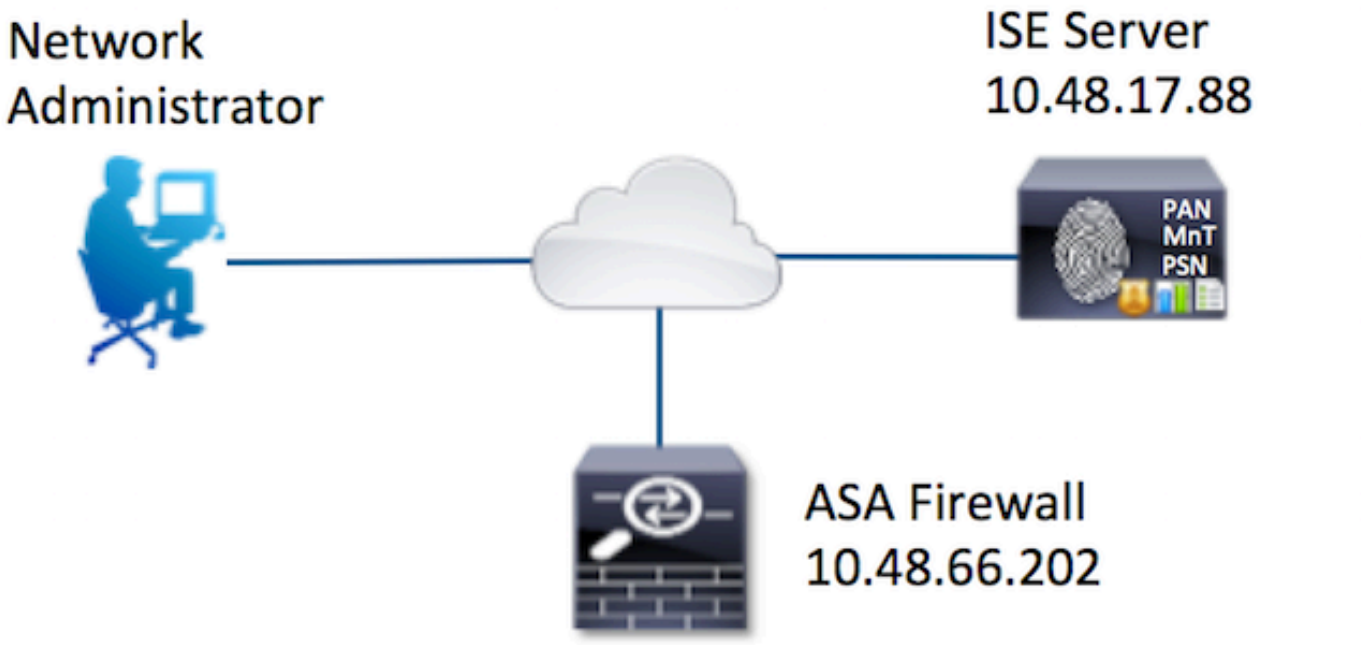
如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

設定

組態的目的是：

- 通過內部身份庫驗證ssh使用者
- 授權ssh使用者，使其在登入後進入特權執行模式
- 檢查並將每個執行的命令傳送到ISE進行驗證

網路圖表



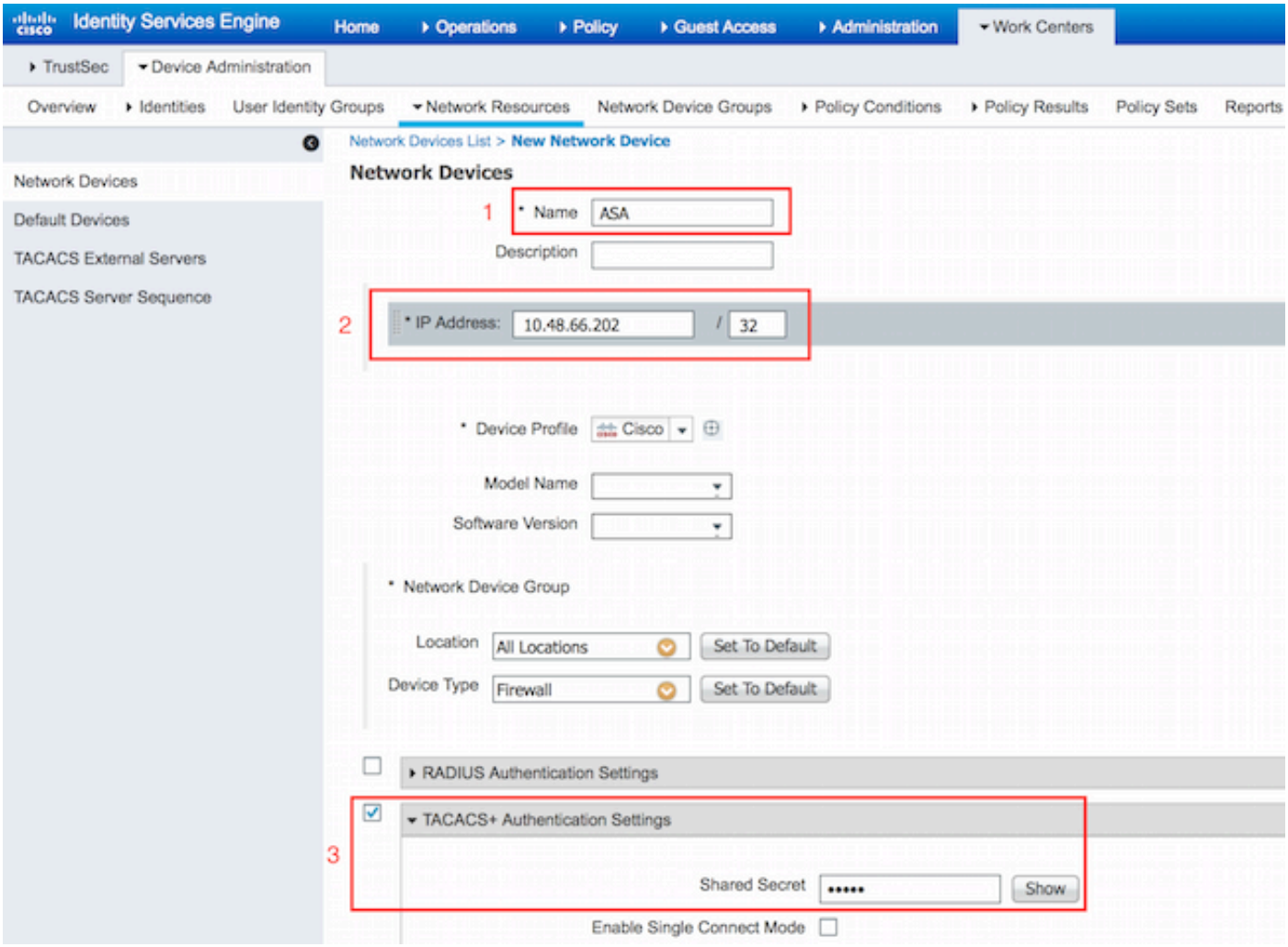
組態

配置ISE進行身份驗證和授權

建立了兩個使用者。使用者**administrator**是ISE上**Network Admins** local Identity Group的一部分。此使用者具有完全的CLI許可權。使用者**user**是ISE上**網路維護團隊**本地身份組的一部分。此使用者只能執行show命令和ping。

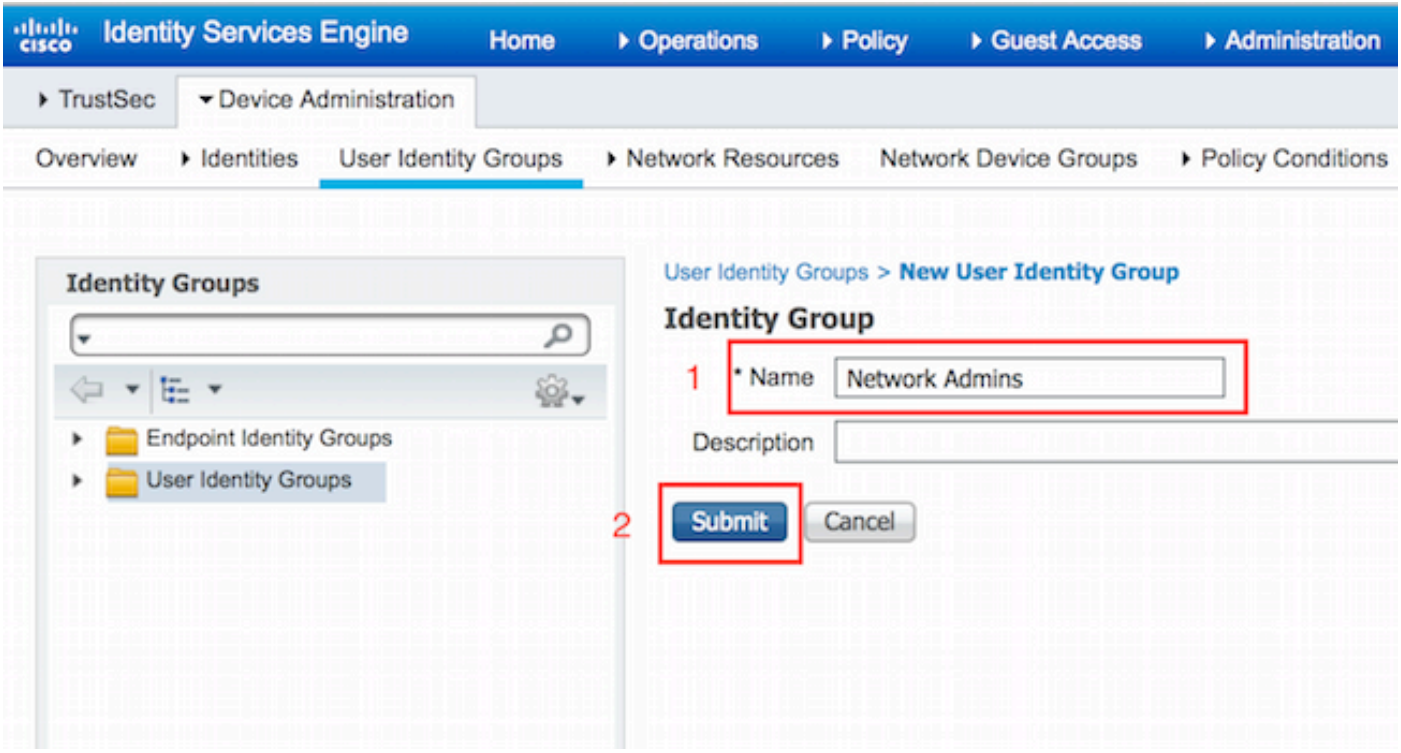
新增網路裝置

導航至**工作中心>裝置管理>網路資源>網路裝置。按一下「Add」。**提供名稱、IP地址，選中**TACACS+身份驗證設定**覈取方塊並提**供共用密鑰**。可以選擇指定裝置型別/位置。



配置使用者身份組

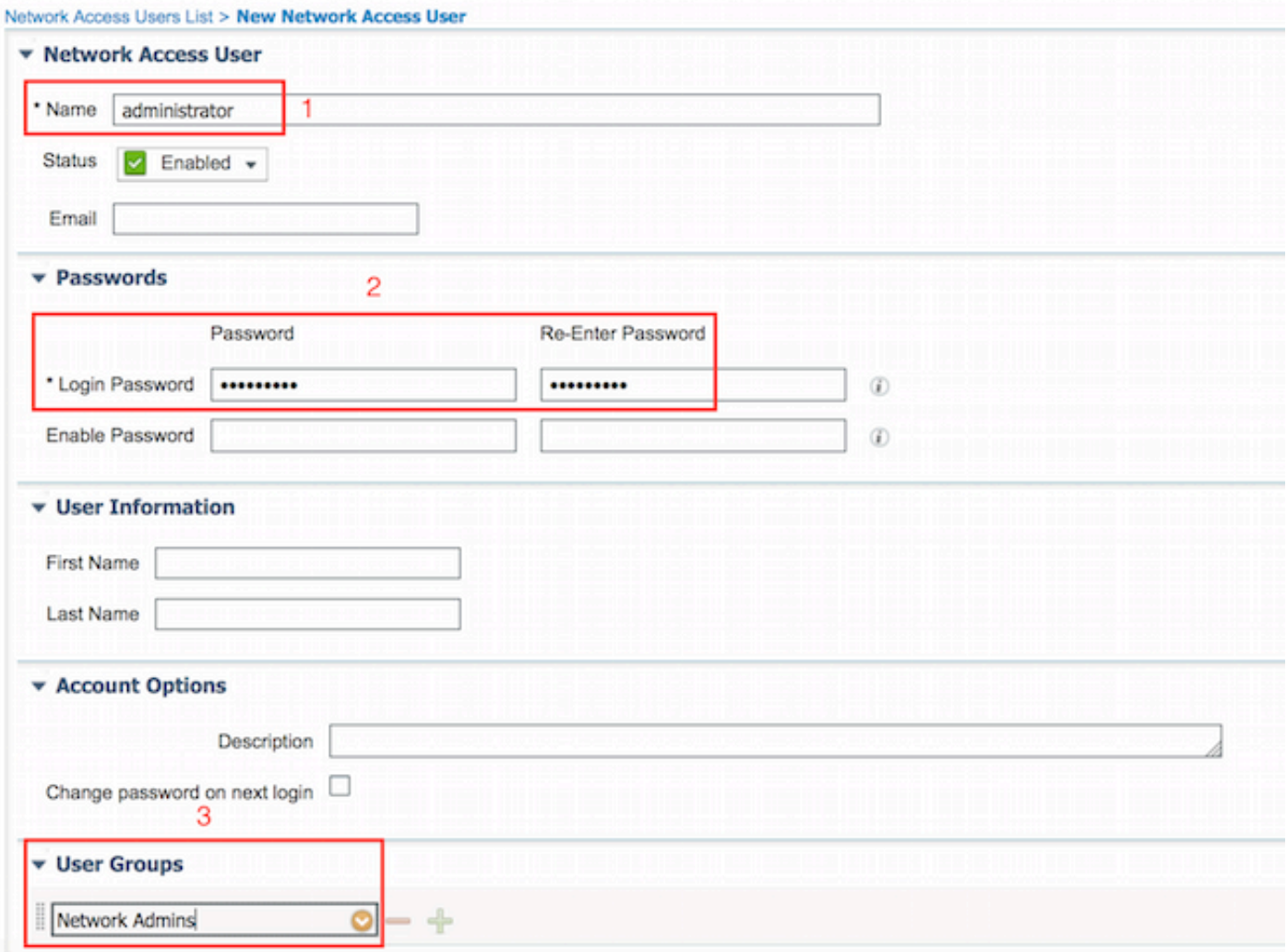
導航至**工作中心>裝置管理>使用者身份組。按一下「Add」。**提供名稱並點選**提交。**



重複相同步驟以配置**網路維護團隊**使用者身份組。

配置使用者

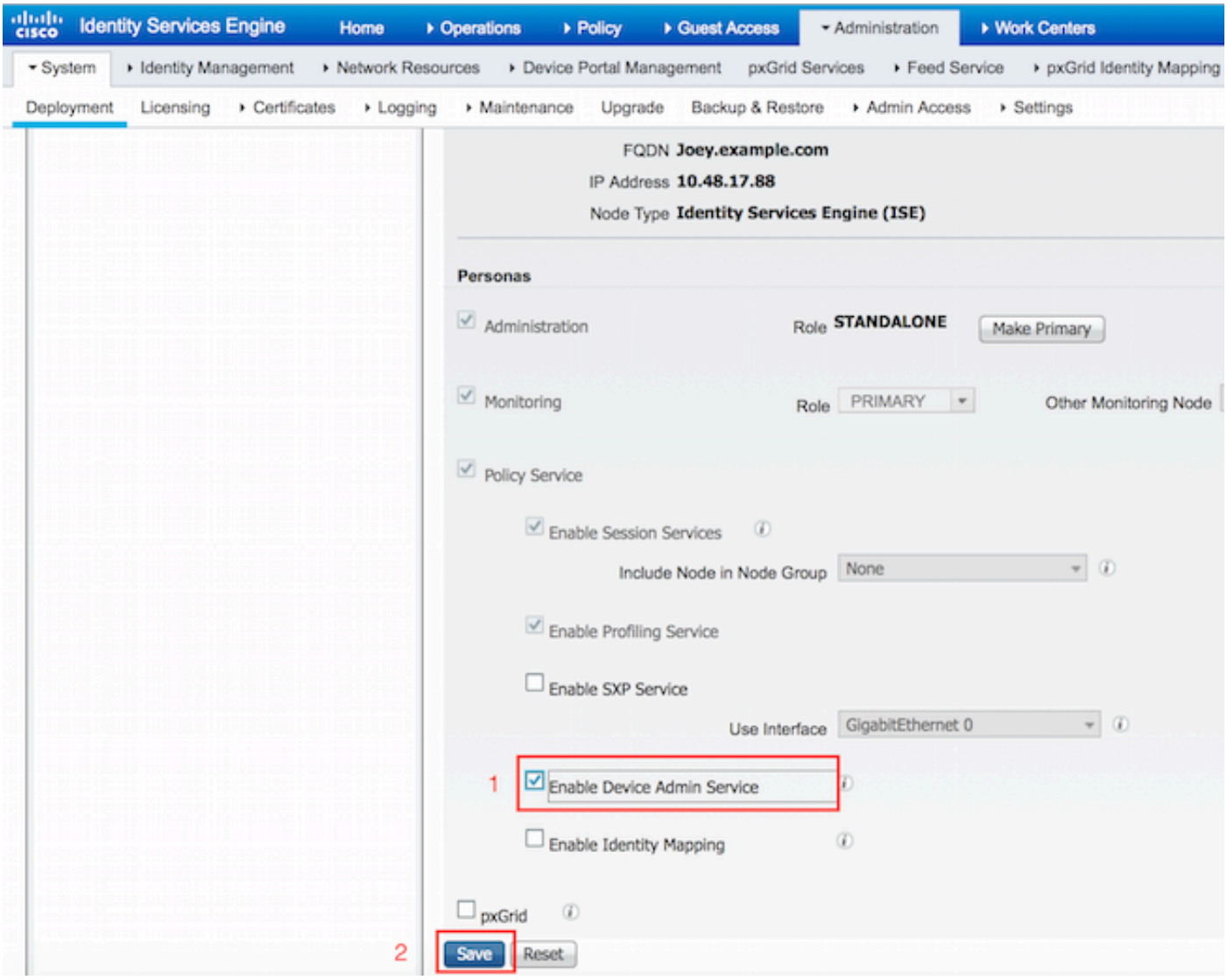
導航至**工作中心>裝置管理>身份>使用者。按一下「Add」。**提供名稱，登入密碼指定使用者組，然後按一下**提交**。



重複這些步驟以配置使用者**使用者**並分配**網路維護團隊**使用者身份組。

啟用裝置管理服務

導航到**管理>系統>部署。**選擇所需的節點。選中Enable Device Admin Service覈取方塊，然後按一下Save。

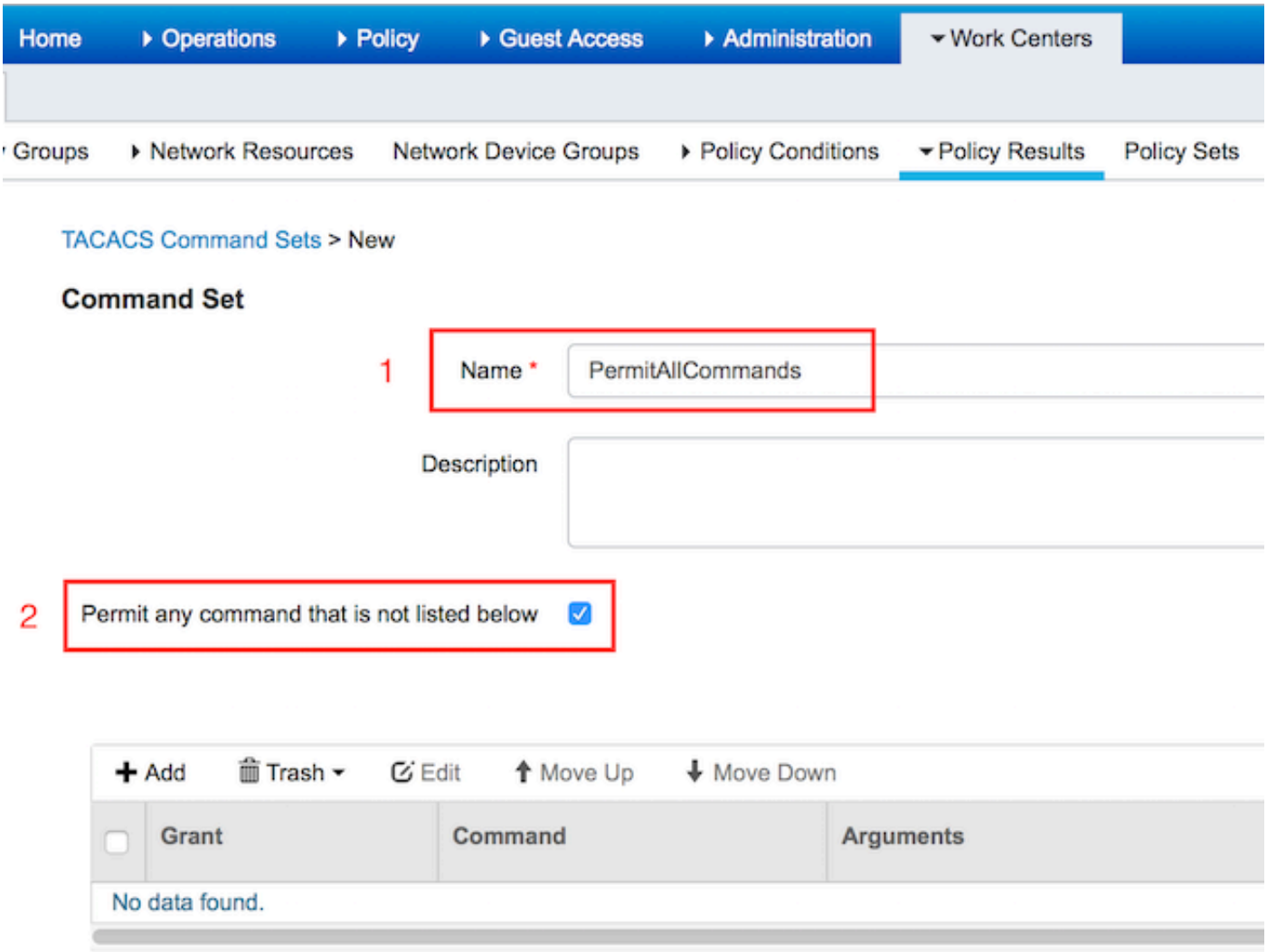


附註：對於TACACS，您需要安裝單獨的許可證。

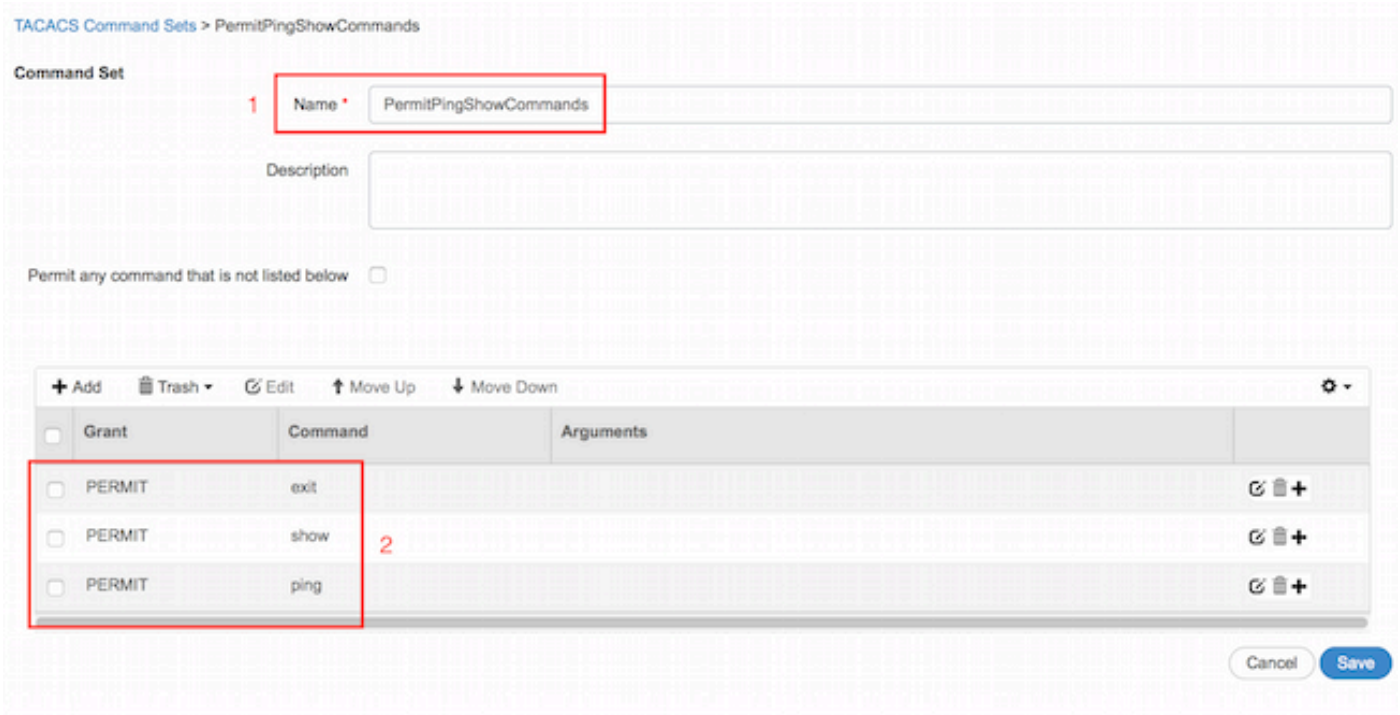
配置TACACS命令集

配置了兩個命令集。首先為administrator使用者輸入PermitAllCommands，該使用者允許裝置上的所有命令。用於**使用者**的第二個PermitPingShowCommands，該使用者僅允許show和ping命令。

1.導航至**工作中心>裝置管理>策略結果> TACACS命令集。按一下「Add」。**提供名稱PermitAllCommands，選中Permit any command that not listed below覈取方塊，然後按一下Submit。

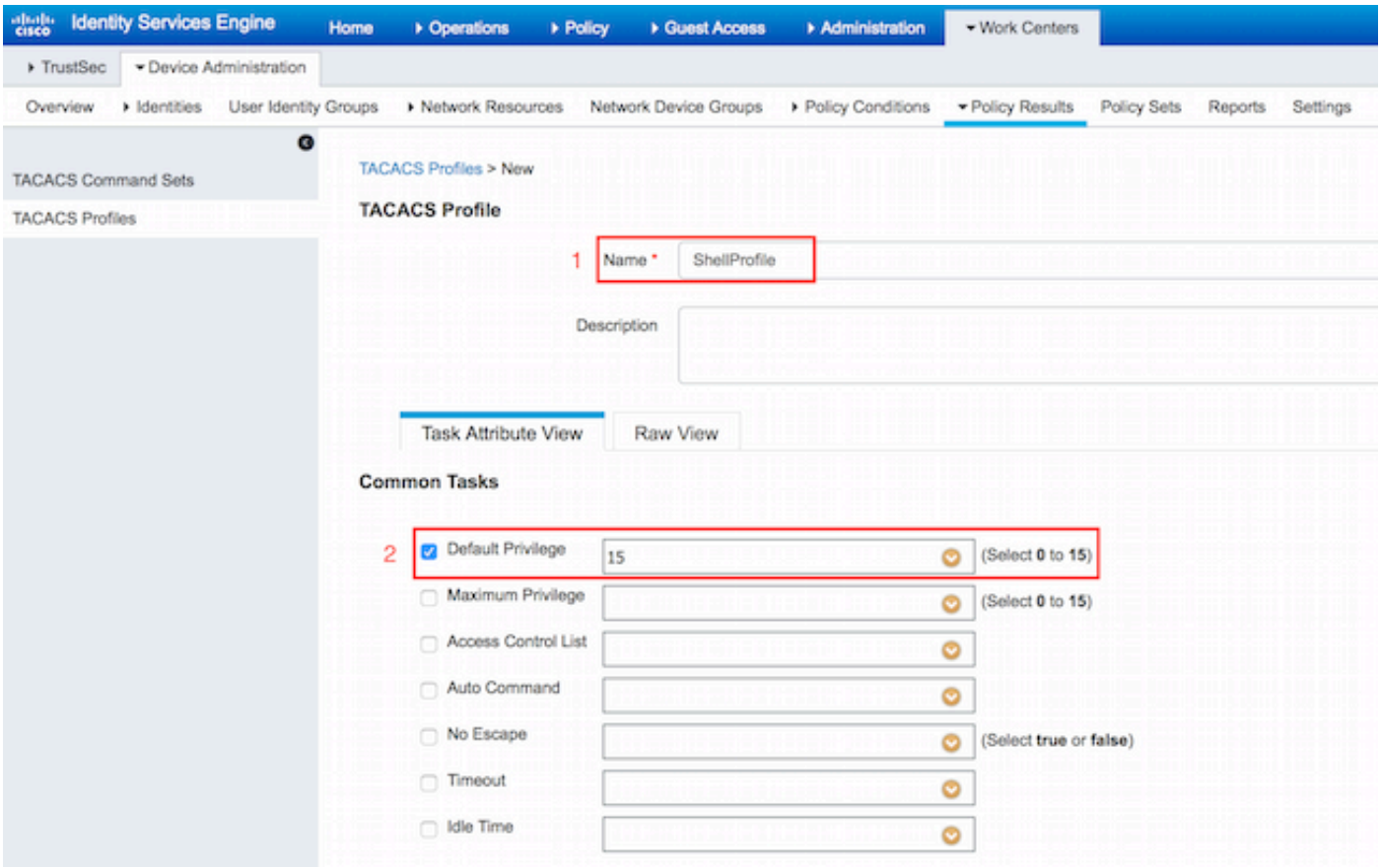


2.導航到**工作中心>裝置管理>策略結果> TACACS命令集。**按一下**「Add」。**提供名稱**PermitPingShowCommands**，單擊**Add**並允許**show**、ping和**exit**命令。預設情況下，如果「引數」留空，則包括所有引數。按一下**Submit（提交）。**



配置TACACS配置檔案

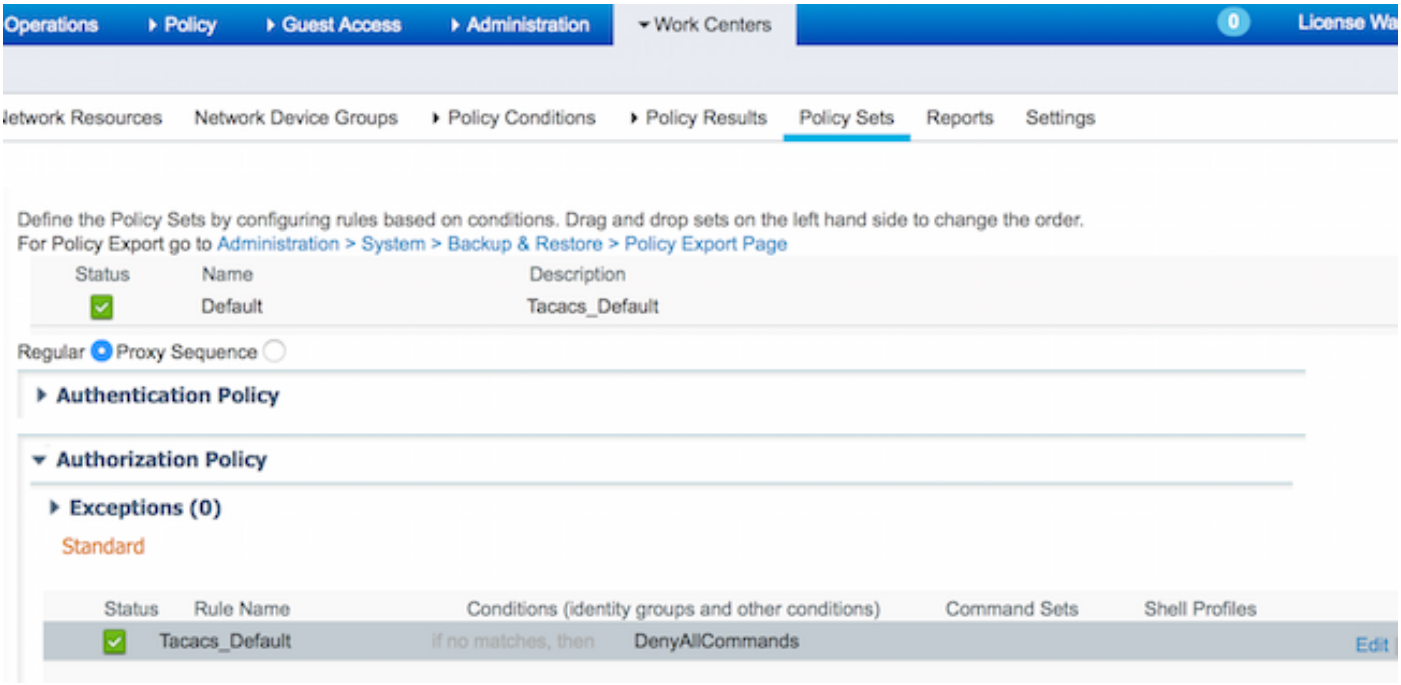
將配置單個TACACS配置檔案。將通過命令集執行實際的命令。導航到**工作中心(Work Centers)>裝置管理(Device Administration)>策略結果(Policy Results)> TACACS配置檔案(TACACS Profiles)。按一下「Add」。**提供名稱**ShellProfile，選擇Default Privilege**覈取方塊，然後輸入值15。按一下Submit。



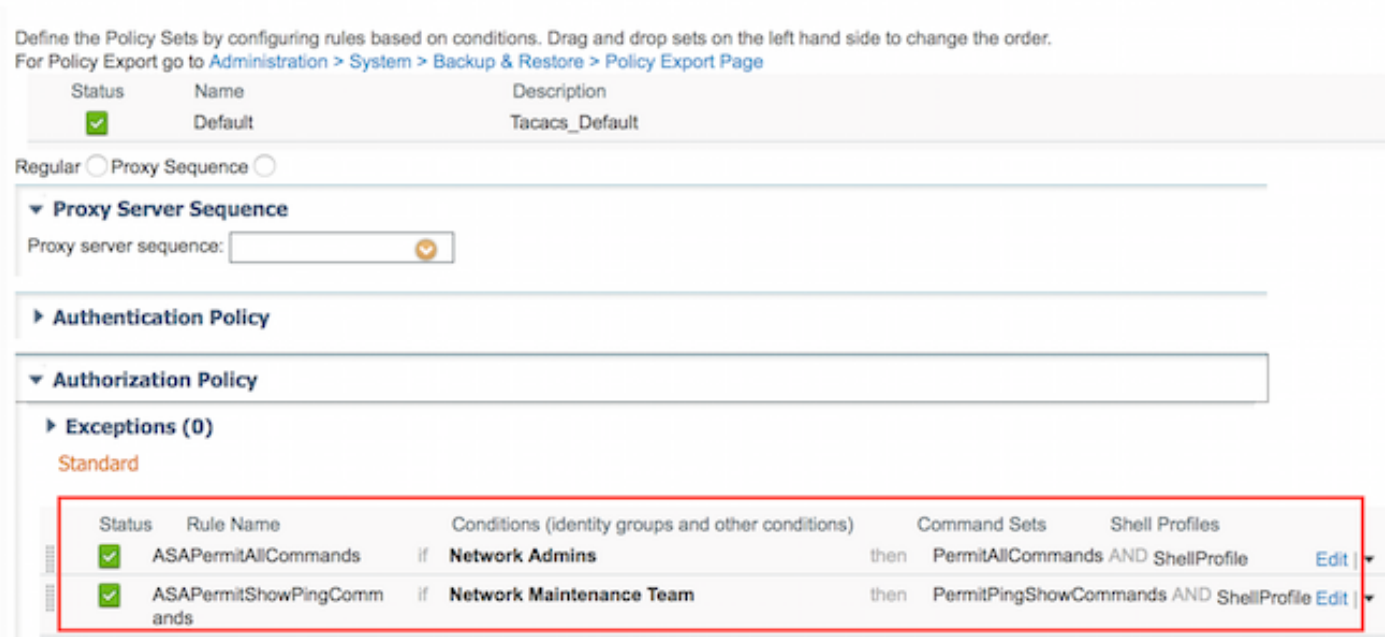
配置TACACS授權策略

預設情況下，「身份驗證策略」指向All_User_ID_Stores，包括本地儲存，因此它保持不變。

導航到**Work Centers > Device Administration > Policy Sets > Default > Authorization Policy > Edit > Insert New Rule above。**



配置了兩個授權規則，第一個規則根據**Network Admins** User Identity Group成員身份分配TACACS配置檔案**ShellProfile**和命令Set **PermitAllCommands**。第二個規則根據**網路維護團隊使用者身份組成員身份分配TACACS配置檔案ShellProfile**和命令Set **PermitPingShowCommands**。



配置Cisco ASA防火牆進行身份驗證和授權

1.使用**username**命令建立具有完全回退許可權的本地使用者，如下所示

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

2.定義TACACS伺服器ISE，指定介面、協定IP地址和**tacacs**金鑰。

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

附註：伺服器金鑰應與ISE伺服器上較早定義的金鑰相匹配。

3.使用test aaa命令測試TACACS伺服器的可達性，**如下所示。**

```
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
```

上一個命令的輸出顯示TACACS伺服器可訪問且使用者已成功通過身份驗證。

4.配置ssh、exec授權和命令授權的身份驗證，如下所示。在**aaa authorization exec authentication-server auto-enable**下，您將自動置於特權EXEC模式。

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

附註：使用上述命令，在ISE上完成身份驗證，使用者直接進入許可權模式，然後進行命令授權。

5.在mgmt介面上允許shh。

```
ssh 0.0.0.0 0.0.0.0 mgmt
```

驗證

Cisco ASA防火牆驗證

1.以**屬於完全訪問使用者身份組的管理員**身份向ASA防火牆發出ssh命令。**Network Admins**組對映到ISE上**設定**的ShellProfile和**PermitAllCommands命令。**嘗試運行任何命令以確保完全訪問。

```
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#
```

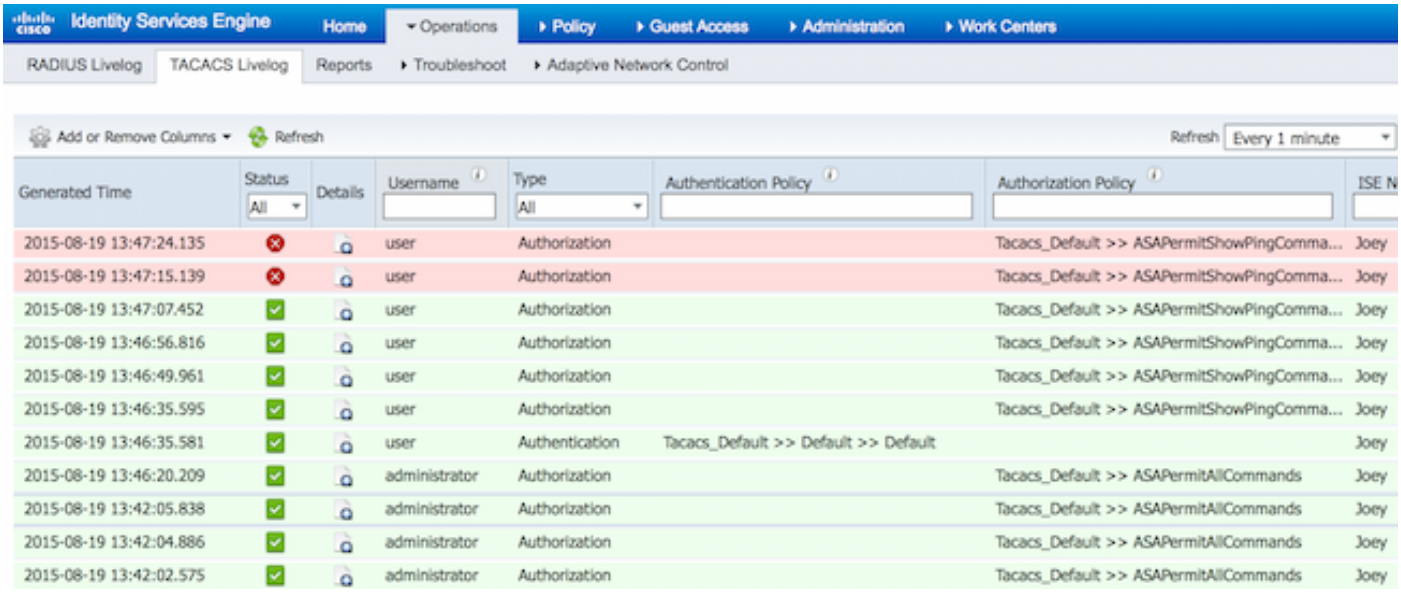
2.以**屬於受限訪問使用者身份組的使用者**身份通過SSH連線到ASA防火牆。**網路維**護組對映到ISE**上設定的ShellProfile**和PermitPingShowCommands命令。嘗試運行任何命令以確保只能發出show和ping命令。

```
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
```

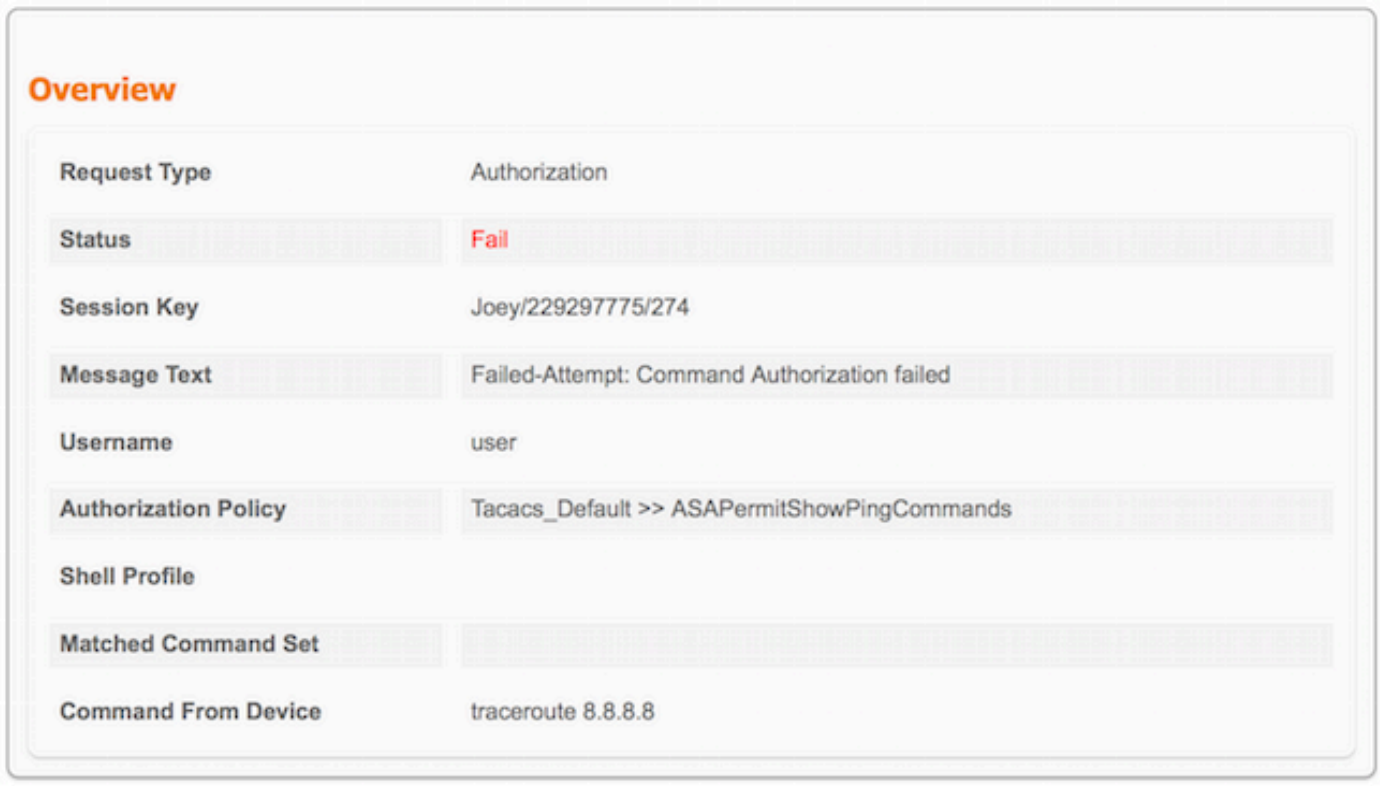
```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 20/24/30 ms
ciscoasa# configure terminal
Command authorization failed
ciscoasa# traceroute 8.8.8.8
Command authorization failed
```

ISE 2.0驗證

1.導覽至Operations > TACACS Livelog。確保看到上面完成的嘗試。



2.按一下其中一個紅色報告的詳細資訊，可以看到之前執行的失敗命令。



疑難排解

錯誤：Failed-Attempt:命令授權失敗

檢查SelectedCommandSet屬性以驗證預期命令集是否由授權策略選擇

相關資訊

技術支援與文件 - Cisco Systems

ISE 2.0版本說明

ISE 2.0硬體安裝指南

ISE 2.0升級指南

ACS到ISE遷移工具指南

ISE 2.0 Active Directory整合指南

ISE 2.0引擎管理員指南