

# IOS和ASA/PIX/FWSM上的ACS Shell命令授權集配置示例

## 目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[慣例](#)

[命令授權集](#)

[新增Shell命令授權集](#)

[案例 1:讀/寫訪問許可權或完全訪問許可權的許可權](#)

[案例 2:只讀訪問特權](#)

[案例 3:受限訪問特權](#)

[將Shell命令授權集關聯到使用者組](#)

[將Shell命令授權集 \( 讀寫許可權 \) 關聯到使用者組 \( 管理組 \)](#)

[將Shell命令授權集 \( 只讀訪問 \) 關聯到使用者組 \( 只讀組 \)](#)

[將外殼命令授權集\(Restrict access\)與使用者關聯](#)

[IOS路由器配置](#)

[ASA/PIX/FWSM配置](#)

[疑難排解](#)

[錯誤：命令授權失敗](#)

[相關資訊](#)

## 簡介

本檔案介紹如何在思科安全存取控制伺服器(ACS)中為AAA使用者端(例如Cisco IOS<sup>®</sup>路由器或交換器)和思科安全裝置(ASA/PIX/FWSM)設定shell授權集，並將TACACS+作為授權通訊協定。

**注意：**ACS Express不支援命令授權。

## 必要條件

### 需求

本文檔假設在AAA客戶端和ACS中均設定了基本配置。

在ACS中，選擇Interface Configuration > Advanced Options，並確保選中Per-user TACACS+/RADIUS Attributes釐取方塊。

## 採用元件

本檔案中的資訊是根據執行軟體版本3.3和更新版本的思科安全存取控制伺服器(ACS)。

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。

## 慣例

請參閱[思科技術提示慣例以瞭解更多有關文件慣例的資訊。](#)

## 命令授權集

命令授權集提供了一種控制在任何給定網路裝置上發出的每個命令的授權的中央機制。此功能大大增強了設定授許可權制所需的可擴充性和可管理性。

在ACS中，預設命令授權集包括外殼命令授權集和PIX命令授權集。Cisco裝置管理應用程式 ( 例如 CiscoWorks防火牆管理中心 ) 可以指示ACS支援其他命令授權集型別。

**注意：**PIX命令授權集要求TACACS+命令授權請求將服務標識為*pixshell*。驗證此服務已在防火牆使用的PIX OS版本中實施；否則，請使用Shell命令授權集對PIX裝置執行命令授權。有關詳細資訊，請參閱[為使用者組配置Shell命令授權集](#)。

**註：**自PIX OS版本6.3起，尚未實現pixshell服務。

**注意：**思科安全裝置(ASA/PIX)當前不允許在登入期間將使用者直接置於啟用模式。使用者必須手動進入啟用模式。

为了更好地控制裝置託管的管理Telnet會話，使用TACACS+的網路裝置可以在執行每個命令列之前請求授權。您可以定義一組命令，允許或拒絕特定使用者在給定裝置上執行。ACS已使用以下功能進一步增強了此功能：

- **可重用命名命令授權集** — 無需直接引用任何使用者或使用者組，即可建立命名命令授權集。您可以定義多個命令授權集，以描述不同的訪問配置檔案。例如：*Help desk*命令授權集可以允許訪問高級瀏覽命令(如*show run*)，並拒絕任何配置命令。*All network engineers*命令授權集可能包含企業中任何網路工程師的允許命令有限清單。*本地網路工程師*命令授權集可以允許所有命令 ( 並包括IP地址配置命令 )。
- **精細配置粒度** — 您可以在命名命令授權集和網路裝置組(NDG)之間建立關聯。因此，您可以根據使用者訪問的網路裝置為使用者定義不同的訪問配置檔案。您可以將同一個命名命令授權集與多個NDG相關聯，並將其用於多個使用者組。ACS實施資料完整性。命名命令授權集儲存在ACS內部資料庫中。您可以使用ACS備份和還原功能來備份和還原它們。您還可以將命令授權集與其他配置資料一起複製到輔助ACS。

對於支援Cisco裝置管理應用的命令授權集型別，使用命令授權集時的優點相似。您可以將命令授權集應用於包含裝置管理應用程式使用者的ACS組，以在裝置管理應用程式中強制執行各種許可權的授權。ACS組可以對應於裝置管理應用程式中的不同角色，並且您可以根據情況對每個組應用不同的命令授權集。

ACS具有三個命令授權過濾的連續階段。每個命令授權請求按列出的順序進行評估：

1. **Command Match** - ACS確定處理的命令是否與命令授權集中列出的命令匹配。如果命令不匹

配，則命令授權由Unmatched Commands設定確定：*permit* or *deny*。否則，如果命令匹配，則繼續評估。

2. **Argument Match** - ACS確定提供的命令引數是否與命令授權集中列出的命令引數匹配。如果任何引數不匹配，命令授權取決於是否啟用Permit Unmatched Args選項。如果允許不匹配的引數，則該命令是授權的，計算結束；否則，命令未獲得授權且評估結束。如果所有引數都匹配，則繼續計算。
3. **Argument Policy** — 一旦ACS確定命令中的引數與命令授權集中的引數匹配，ACS就會確定是否明確允許每個命令引數。如果明確允許所有引數，ACS將授予命令授權。如果不允許任何引數，ACS將拒絕命令授權。

## 新增Shell命令授權集

本節包括以下案例，說明如何新增命令授權集：

- [案例 1:讀/寫訪問許可權或完全訪問許可權的許可權](#)
- [案例 2:只讀訪問特權](#)
- [案例 3:受限訪問特權](#)

**註：**有關如何建立命令授權集的詳細資訊，請參閱[思科安全訪問控制伺服器4.1使用手冊](#)的[新增命令授權集](#)部分。有關如何編輯和刪除命令授權集的詳細資訊，請參閱[編輯命令授權集](#)和[刪除命令授權集](#)。

### 案例 1:讀/寫訪問許可權或完全訪問許可權的許可權

在這種情況下，使用者被授予讀取/寫入（或完全）訪問許可權。

在「共用配置檔案元件」視窗的「外殼命令授權集」區域中，配置以下設定：

1. 在「名稱」欄位中，輸入**ReadWriteAccess**作為命令授權集名稱。
2. 在Description欄位中，輸入命令授權集的說明。
3. 按一下**Permit**單選按鈕，然後按一下**Submit**。

# Shared Profile Components

Edit

## Shell Command Authorization Set

Name:

ReadWriteAccess

Description:

For Administrators etc  
full access

Unmatched Commands:

Permit

Deny

Permit Unmatched Args

Add Command

Remove Command

### 案例 2: 只讀訪問特權

在此案例中，使用者只能使用show指令。

在「共用配置檔案元件」視窗的「外殼命令授權集」區域中，配置以下設定：

1. 在「名稱」欄位中，輸入ReadOnlyAccess作為命令授權集的名稱。
2. 在Description欄位中，輸入命令授權集的說明。
3. 按一下Deny單選按鈕。
4. 在Add Command按鈕上方的欄位中輸入show命令，然後按一下Add Command。
5. 選中Permit Unmatched Args覈取方塊，然後按一下Submit

# Shared Profile Components

Edit

## Shell Command Authorization Set

Name:

ReadOnlyAccess

Description:

Users are allowed to  
run only show commands

Unmatched Commands:

Permit  
 Deny

show

Permit Unmatched Args

Add Command

Remove Command

### 案例 3:受限訪問特權

在這種情況下，使用者可以使用選擇性指令。

在「共用配置檔案元件」視窗的「外殼命令授權集」區域中，配置以下設定：

1. 在名稱欄位中，輸入**Restrict\_access**作為命令授權集的名稱。
2. 按一下**Deny**單選按鈕。
3. 輸入您要在AAA客戶端上允許的命令。在Add Command按鈕上方的欄位中，輸入**show**命令，然後按一下**Add Command**。

# Shared Profile Components

Edit

## Shell Command Authorization Set

Name:

Restrict\_access

Description:

Unmatched Commands:

bandwidth  
configure  
description  
ethernet  
interface  
show  
timeout

- Permit  
 Deny

Permit Unmatched Args

輸入configure命令，然後按一下Add Command。選擇configure命令，然後在右側欄位中輸入permit terminal。

# Shared Profile Components

Edit

## Shell Command Authorization Set

Name:

Description:

Unmatched Commands:  Permit  
 Deny

Permit Unmatched Args

bandwidth	
<b>configure</b>	permit terminal
description	
ethernet	
interface	
show	
timeout	

輸入interface命令

, 然後按一下Add Command。選擇interface命令，並在右側欄位中輸入permit Ethernet。



# Shared Profile Components

Edit

## Shell Command Authorization

Name:

Description:

Unmatched Commands:

Permit  
 Deny

Permit Unmatched Args

bandwidth  
configure  
description  
ethernet  
interface  
show  
timeout

輸入ethernet命令，然後按

一下Add Command。選擇interface命令，並在右側欄位中輸入permit timeout、permit bandwidth和permit description。

## Shell Command Authorization Set

Name:

Description:

Unmatched Commands:

Permit  
 Deny

Permit Unmatched Args

bandwidth  
configure  
description  
ethernet  
interface  
show  
timeout

輸入bandwidth命令

，然後按一下Add Command。



# Shared Profile Components

Edit

## Shell Command Authorization Set

Name:

Description:

Unmatched Commands:  Permit  
 Deny

Permit Unmatched Args

bandwidth	
configure	
description	
ethernet	
interface	
show	
timeout	

輸入timeout命令

, 然後按一下Add Command。

# Shared Profile Components

Edit

## Shell Command Authorization Set

Name:

Description:

Unmatched Commands:  
 Permit  
 Deny

Permit Unmatched Args

輸入description命

令，然後按一下Add Command。

# Shared Profile Components

## Edit

### Shell Command Authorization Set

Name:

Description:

Unmatched Commands:

Permit  
 Deny

Permit Unmatched Args

4. 按一下「Submit」。

## 將Shell命令授權集關聯到使用者組

有關如何為使用者組配置shell命令授權集配置的詳細資訊，請參閱[思科安全訪問控制伺服器4.1使用手冊](#)的[為使用者組配置shell命令授權集](#)部分。

## 將Shell命令授權集（讀寫許可權）關聯到使用者組（管理組）

1. 在ACS視窗中，按一下Group Setup，然後從Group下拉選單中選擇Admin Group。

# Group Setup

## Select

Group:

2. 按一下「Edit Settings」。

3. 在「跳至」下拉式清單中選擇「啟用選項」。

4. 在Enable Options區域中，按一下Max Privilege for any AAA client單選按鈕，然後從下拉選單中選擇Level 15。



The screenshot shows the 'Group Setup' configuration page. At the top, there is a 'Jump To' dropdown menu with 'Enable Options' selected. Below this, the 'Enable Options' section is displayed. It contains three radio button options: 'No Enable Privilege', 'Max Privilege for any AAA Client' (which is selected), and 'Define max Privilege on a per network device group basis'. Under the selected option, there is a dropdown menu showing 'Level 15'. At the bottom of the page, there are two columns labeled 'Device Group' and 'Privilege'.

5. 在「跳至」下拉式清單中選擇TACACS+。
6. 在TACACS+設定區域中，選中Shell(exec)覈取方塊，選中Privilege level覈取方塊，並在許可權級別欄位中輸入15。

# Group Setup

Jump To TACACS+

## TACACS+ Settings

**PPP IP**

In access control list

Out access control list

Route

Routing

Enabled

**Note: PPP LCP will be automatically enabled if this service**

**Shell (exec)**

Access control list

Auto command

Callback line

Callback rotary

Idle time

No callback verify

Enabled

No escape

Enabled

No hangup

Enabled

Privilege level

15

7. 在Shell Command Authorization Set區域中，按一下Assign a Shell Command Authorization Set for any network device單選按鈕，然後從下拉選單中選擇ReadWriteAccess。

## Group Setup

**Jump To** TACACS+ ▼

Privilege level

Timeout

---

### Shell Command Authorization Set

None

Assign a Shell Command Authorization Set for any network device  
 ▼

Assign a Shell Command Authorization Set on a per Network Device Group Basis

8. 按一下Submit

### 將Shell命令授權集（只讀訪問）關聯到使用者組（只讀組）

1. 在ACS視窗中，按一下Group Setup，然後從Group下拉選單中選擇Read-Only Group。

## Group Setup

### Select

Group : 2: Read-Only Group ▼

Users in Group   Edit Settings   Rename Group

2. 按一下「Edit Settings」。

3. 在「跳至」下拉式清單中選擇「啟用選項」。

4. 在Enable Options區域中，按一下Max Privilege for any AAA client單選按鈕，然後從下拉選單中選擇Level 1。

# Group Setup

Jump To

## Enable Options

- No Enable Privilege
- Max Privilege for any AAA Client
  -
- Define max Privilege on a per network device group basis

5. 在TACACS+設定區域中，選中Shell(exec)覈取方塊，選中Privilege level覈取方塊，然後在Privilege level欄位中輸入1。



# Group Setup

Jump To TACACS+

## TACACS+ Settings

**PPP IP**

In access control list

Out access control list

Route

Routing

Enabled

**Note: PPP LCP will be automatically enabled if this service**

**Shell (exec)**

Access control list

Auto command

Callback line

Callback rotary

Idle time

No callback verify

Enabled

No escape

Enabled

No hangup

Enabled

**Privilege level**

1

6. 在Shell Command Authorization Set區域中，按一下Assign a Shell Command Authorization Set for any network device單選按鈕，然後從下拉選單中選擇ReadOnlyAccess。

Group Setup

Jump To TACACS+

Shell Command Authorization Set

None

Assign a Shell Command Authorization Set for any network

ReadOnlyAccess

7. 按一下Submit

## [將外殼命令授權集\(Restrict\\_access\)與使用者關聯](#)

有關如何為使用者配置shell命令授權集配置的詳細資訊，請參閱[思科安全訪問控制伺服器4.1使用手冊](#)的[為使用者配置shell命令授權集](#)部分。

**注意：**使用者級設定會覆蓋ACS中的組級設定，這表示如果使用者在使用者級設定中設定了shell命令授權，則會覆蓋組級設定。

1. 按一下User Setup > Add/Edit以建立一個名為Admin\_user的新使用者，使其成為管理員組的一部分。

# User Setup

**Edit**

## User: Admin\_user (New User)

Account Disabled

### Supplementary User Info

Real Name:

Description:

---

### User Setup

Password Authentication:

- 從使用者分配到的組下拉選單中選擇Admin Group。

# User Setup

When a token server is used for authentication, supplying a separate CHAP password for a token card user allows CHAP authentication. This is especially useful when token caching is enabled.

---

Group to which the user is assigned:

- 在Shell Command Authorization Set區域中，按一下Assign a Shell Command Authorization Set for any network device單選按鈕，然後從下拉選單中選擇Restrict\_access。注意：在此方案中，此使用者是管理員組的一部分。Restrict\_access shell授權集適用；ReadWrite Access

## User Setup

Idle time   
 No callback verify  Enabled  
 No escape  Enabled  
 No hangup  Enabled  
 Privilege level   
 Timeout

---

## Shell Command Authorization Set

None  
 As Group  
 Assign a Shell Command Authorization Set for any network device  
 Assign a Shell Command Authorization Set on a per Network Device Group Basis

shell授權集不適用。

：在「介面配置」區域的TACACS+(Cisco)部分，確保在「使用者」列中選中Shell(exec)選項

注意

## IOS路由器配置

除預設組態外，IOS路由器或交換器上還需要以下命令，才能透過ACS伺服器實作命令授權：

```

aaa new-model
aaa authorization config-commands
aaa authorization commands 0 default group tacacs+ local
aaa authorization commands 1 default group tacacs+ local
aaa authorization commands 15 default group tacacs+ local
tacacs-server host 10.1.1.1
tacacs-server key cisco123

```

## ASA/PIX/FWSM配置

除了預置配置之外，還需要在ASA/PIX/FWSM上使用這些命令，以便透過ACS伺服器實施命令授權：

```

aaa-server authserver protocol tacacs+
aaa-server authserver host 10.1.1.1
aaa authorization command authserver

```

**注意：**不能使用RADIUS協定來限制使用者訪問ASDM以只讀目的。由於RADIUS封包同時包含驗證和授權，因此在RADIUS伺服器中進行驗證的所有使用者都具有15的許可權層級。您可以透過執行

指令授權集的TACACS來實現此功能。

**注意：**即使ACS無法執行命令授權，ASA/PIX/FWSM也需要很長時間才能執行鍵入的每個命令。如果ACS不可用且ASA已配置命令授權，ASA仍會為每個命令請求命令授權。

## 疑難排解

### 錯誤：命令授權失敗

#### 問題

透過TACACS記錄登入防火牆後，指令無法使用。輸入命令時，會收到以下錯誤：

#### 解決方案

完成以下步驟即可解決此問題：

1. 確保使用了正確的使用者名稱，且所有必需的特權都已分配給使用者。
2. 如果使用者名稱和許可權正確，請驗證ASA與ACS具有連線性且ACS處於活動狀態。

**注意：**如果管理員錯誤地為本地以及TACACS使用者配置了命令授權，也會發生此錯誤。在這種情況下，請執行密碼復原以解決問題。

## 相關資訊

- [Cisco PIX防火牆軟體](#)
- [Cisco Secure PIX防火牆命令參考](#)
- [安全產品現場通知 \(包括PIX\)](#)
- [要求建議 \(RFC\)](#)
- [思科安全控制存取控制伺服器支援頁面](#)
- [技術支援與文件 - Cisco Systems](#)

## 關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。