

# Cisco Access Control Server ( ACS ) を使用した 5760 Web インターフェイス特権レベルに基づく アクセス制御の設定例

## 目次

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[ACS での少数のテスト ユーザの作成](#)

[ポリシー要素とシェルプロファイルの設定](#)

[特権レベル 15 のシェル アクセス プロファイルの作成](#)

[管理者ユーザ用のコマンドセットの作成](#)

[読み取り専用ユーザのシェル プロファイルの作成](#)

[TACACS プロトコルに一致するサービス選択ルールの作成](#)

[フル管理アクセスのための認証ポリシーの作成](#)

[読み取り専用管理アクセスのための認証ポリシーの作成](#)

[TACACS に対応した 5760 の設定](#)

[2 つの異なるプロファイルを使用した同じ 5760 へのアクセス](#)

[Cisco サポート コミュニティ - 特集対話](#)

## 概要

このドキュメントでは、さまざまな特権レベルの Cisco ACS TACACS+ 認証および認可プロファイルを作成し、WebUI へのアクセスのために 5760 に統合する方法について説明します。この機能は 3.6.3 以降でサポートされています (ただし、このドキュメントの執筆時点では 3.7.x ではサポートされていません)。

## 前提条件

### 要件

このドキュメントでは、読者が Cisco ACS および Converged Access コントローラ コンフィギュレーションを理解していることを前提としています。このドキュメントは、TACACS+ 認証における次の 2 つのコンポーネント間のインタラクションのみに重点を置いています。

### 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Cisco Converged Access 5760 リリース 3.6.3

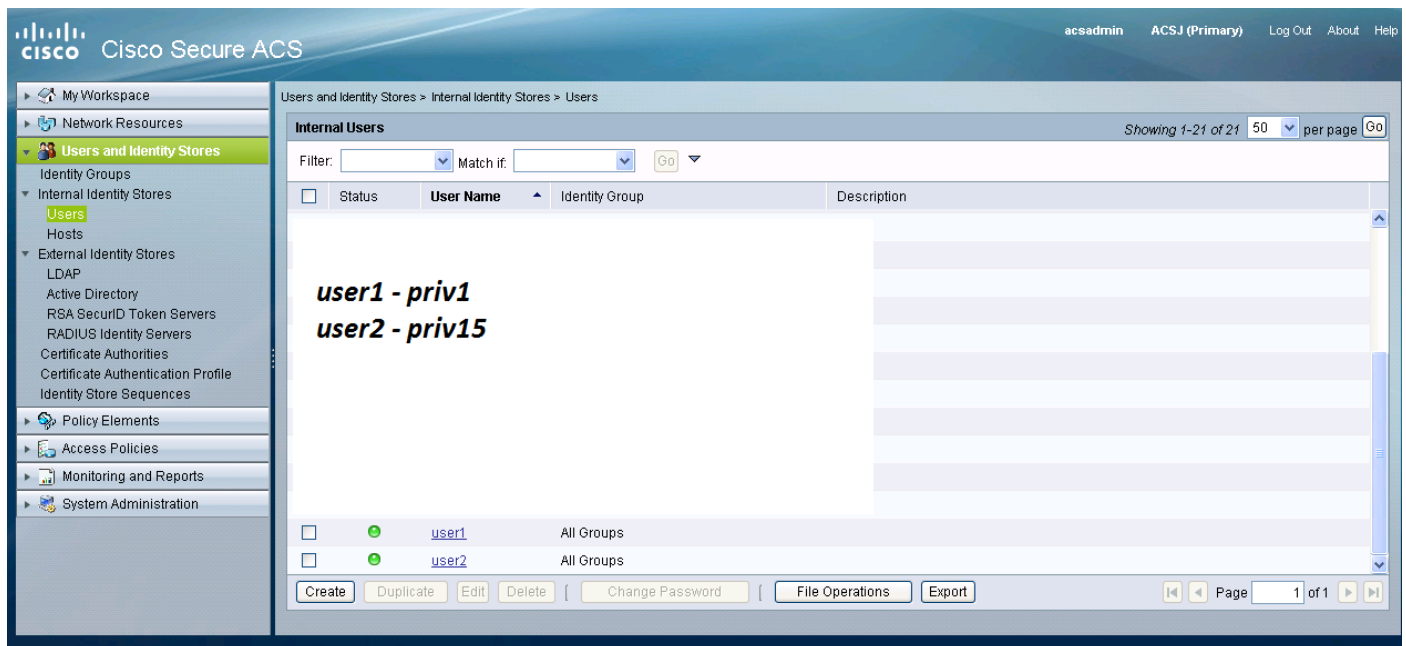
- Cisco Access Control Server ( ACS ) 5.2

## 設定

### ACS での少数のテスト ユーザの作成

[Users and Identity Stores] をクリックしてから、[Users] を選択します。

[Create] をクリックし、次に示すような少数のテスト ユーザを設定します。



### ポリシー要素とシェル プロファイルの設定

2 種類のアクセスのために 2 つのプロファイルを作成する必要があります。Cisco TACACS では、特権 15 は制約のないデバイスへの完全なアクセス権限を提供します。一方、特権 1 では、ログインと限られたコマンドの実行だけが許可されます。シスコが提供するアクセスレベルについて以下に簡単に説明します。

特権レベル 1 = 特権なし ( プロンプトは router> )、ログインのデフォルト レベル

特権レベル 15 = 特権あり ( プロンプトは router# )、イネーブル モードに入った後のレベル

特権レベル 0 = ほとんど使用されませんが、5 つのコマンド ( disable、enable、exit、help、および logout ) が含まれています。

5760 ではレベル 2 ~ 14 はレベル 1 と同等と見なされます。これらのレベルにはレベル 1 と同じ特権が付与されます。5760 の特定のコマンドに対して TACACS 特権レベルを設定しないでください。タブによる UI アクセスは 5760 ではサポートされていません。フル アクセス ( priv15 ) または [Monitor] タブへのアクセスのみ ( priv1 ) のいずれかが設定されます。特権レベル 0 のユーザは、ログインできません。

### 特権レベル 15 のシェル アクセス プロファイルの作成

次に示す画面を使用してこのプロファイルを作成します。

[Policy Elements] をクリックします。 [Shell Profiles] をクリックします。

新しいプロファイルを作成します。

[Common Tasks] タブに移動し、デフォルト特権レベルおよび最大特権レベルを 15 に設定します。



## 管理者ユーザ用のコマンドセットの作成

コマンドセットとは、すべての TACACS デバイスにより使用されるコマンドの集合です。コマンドセットを使用して、特定のプロファイルに割り当てられているユーザが使用できるコマンドを制限できます。5760 では、渡された特権レベルに基づいて WebUI コードで制限が設定されるため、レベル 1 とレベル 15 の両方のコマンドセットは同一になります。

Cisco Secure ACS - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Search Favorites

Address <https://9.10.40.56/acsadmin/>

acesadmin ACSJ (Primary)

**Cisco Secure ACS**

Policy Elements > Authorization and Permissions > Device Administration > Command Sets > Edit: "PermitAllCmds"

**General**

Name:

Description:

Permit any command that is not in the table below

Grant	Command	Arguments
-------	---------	-----------

Grant:  Command:  Arguments:

## 読み取り専用ユーザのシェル プロファイルの作成

読み取り専用ユーザのシェル プロファイルを作成します。このプロファイルは、特権レベルが 1 に設定されていることが異なります。

Policy Elements > Authorization and Permissions > Device Administration > Shell Profiles > Edit: "joseph1"

General **Common Tasks** Custom Attributes

**Privilege Level**

Default Privilege: Static  Value 1

Maximum Privilege: Static  Value 1

**Shell Attributes**

Access Control List: Not in Use

Auto Command: Not in Use

No Callback Verify: Not in Use

No Escape: Not in Use


No Hang Up: Not in Use

Timeout: Not in Use

Idle Time: Not in Use

Callback Line: Not in Use

Callback Rotary: Not in Use

 = Required fields

Submit Cancel

## TACACS プロトコルに一致するサービス選択ルールの作成

ポリシーと設定に基づき、5760 から送信される TACACS と一致するルールがあることを確認します。

Access Policies > Access Services > Service Selection Rules

Single result selection Rule based result selection

Service Selection Policy

Filter: Status Match it Equals Enabled Clear Filter Go

	Status	Name	Protocol	Conditions	Results	Hit Count
1	<input type="checkbox"/>	Rule-1	match	Tacacs	Default Device Admin	0

General  
Name: Rule-1 Status: Enabled

The Customize button in the lower right area of the policy rules screen controls which policy conditions and results are available here for use in policy rules.

Conditions  
 Protocol: match Tacacs Select

Results  
Service: Default Device Admin

Create... Duplicate... Edit Delete

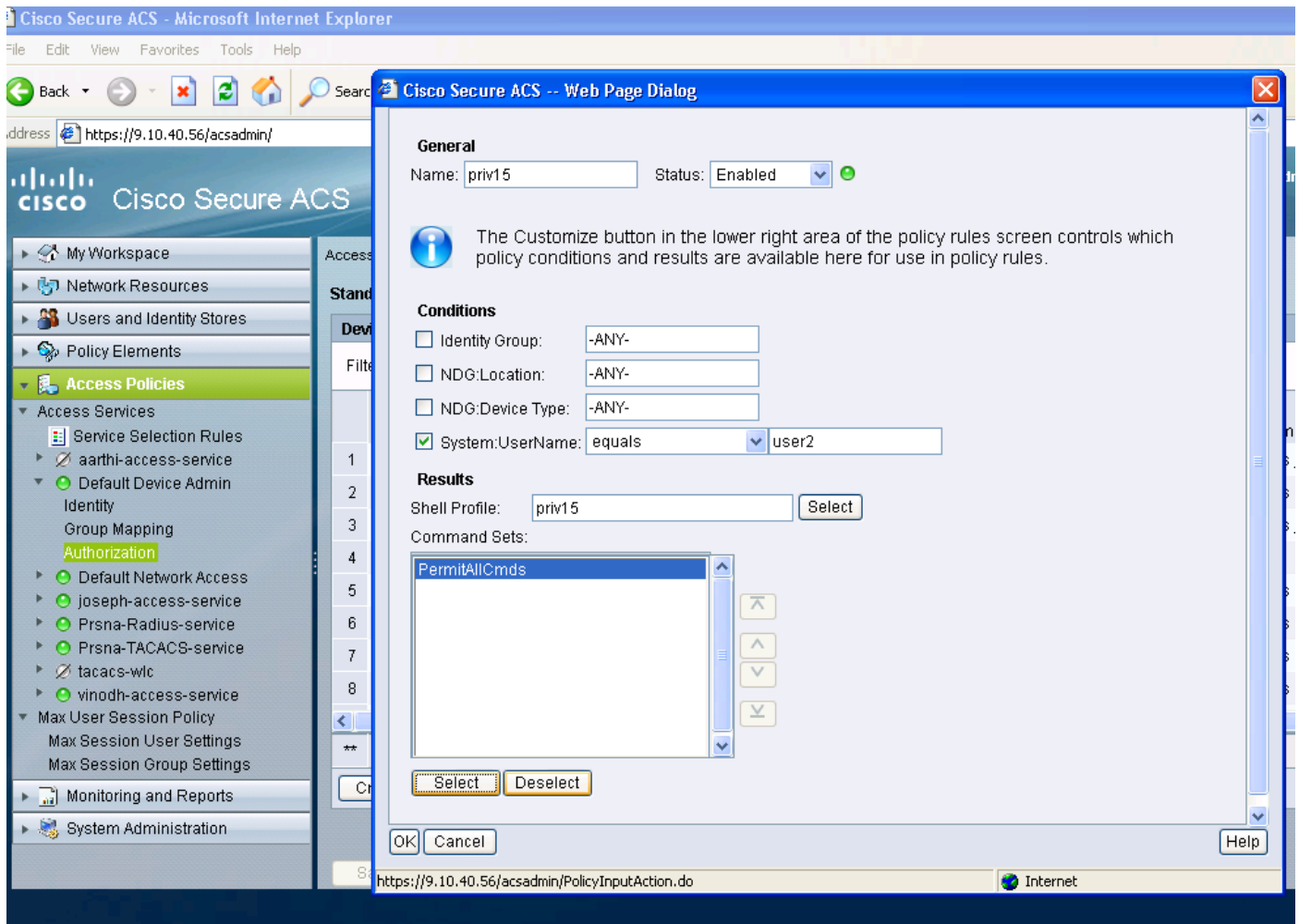
Save Changes Discard Changes

Customize Hit Count

Create service selection rule. Match protocol tacacs and map it to access service.

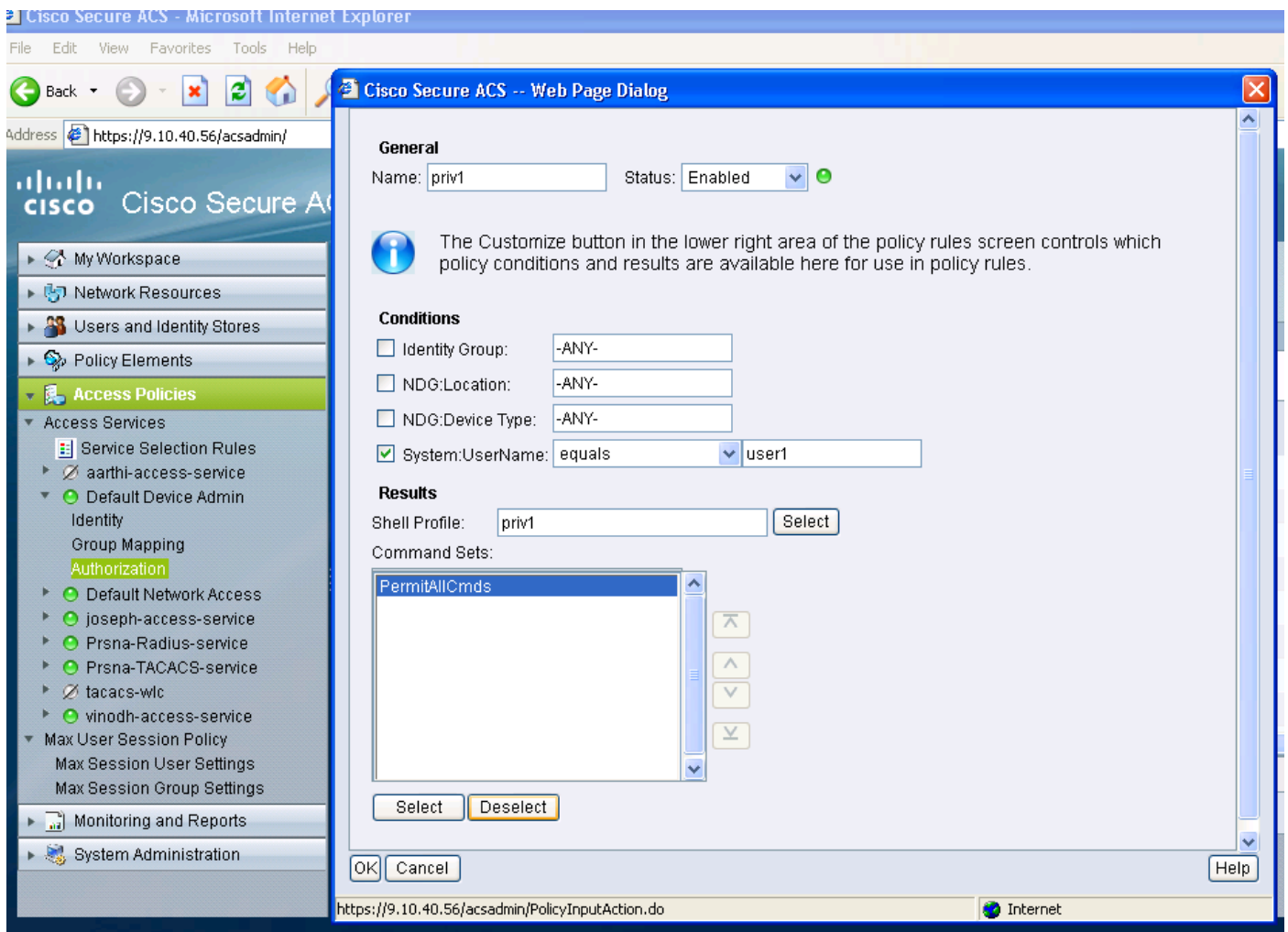
## フル管理アクセスのための認証ポリシーの作成

TACACS プロトコルの選択に使用する Default Device Admin ポリシーは、評価ポリシー プロセスの一部として選択されます。認証に TACACS プロトコルを使用する場合、選択されるサービスポリシーは Default Device Admin ポリシーと呼ばれます。このポリシーは 2 つのセクションで構成されています。アイデンティティとは、ユーザが誰であるか、ユーザがどのグループに属しているか（ローカルまたは外部）、および設定されている認証プロファイルに基づいてユーザがどの操作を実行できるかを示します。設定するユーザに関連するコマンドセットを割り当てます。



## 読み取り専用管理アクセスのための認証ポリシーの作成

読み取り専用ユーザにも同様の内容が該当します。この例では、ユーザ 1 に特権レベル 1 シェルプロファイルを設定し、ユーザ 2 に特権レベル 15 シェルプロファイルを設定します。



## TACACS に対応した 5760 の設定

1. RADIUS/TACACS サーバを設定する必要があります。

```
tacacs server tac_acct
```

```
address ipv4 9.1.0.100
```

```
key cisco
```

2. サーバグループの設定

```
aaa group server tacacs+ gtac
```

```
server name tac_acct
```

上記のステップまでは、前提条件はありません。

3. 認証および認可のメソッドリストを設定します。

```
aaa authentication login <method-list> group <srv-grp>
```

```
aaa authorization exec <method-list> group srv-grp>
```

```
aaa authorization exec default group <srv-grp> ----HTTP でトレースを取得する回避策。
```

上記の3つのコマンドとその他のすべての認証および認可パラメータでは、同じデータベース



( RADIUS/TACACS またはローカル ) を使用する必要があります。

たとえば、コマンド認可を有効にする必要がある場合は、コマンド認可が同じデータベースをポイントしている必要もあります。

例 :

aaa authorisation commands 15 <method-list> group <srv-grp> — —> データベース ( TACACS/RADIUS またはローカル ) をポイントするサーバグループが同一である必要があります。

4. 上記のメソッド リストを使用するように HTTP を設定します。

ip http authentication aaa login-auth <method-list> — — —> メソッド リストが「default」の場合でもここにメソッド リストを明示的に指定する必要があります。

```
ip http authentication aaa exec-auth <method-list>
```

## \*\* 注意点

- 「line vty」設定パラメータに対してメソッド リストを設定しないでください。上記の手順と line vty の設定が異なる場合は、line vty の設定が優先されます。
- データベースは SSH/Telnet や webui などのすべての管理設定タイプで同じにする必要があります。
- HTTP 認証では明示的にメソッド リストが定義されている必要があります。

## 2 つの異なるプロファイルを使用した同じ 5760 へのアクセス

限られたアクセス権限が付与される特権レベル 1 ユーザからのアクセスを次に示します。

The screenshot shows the Cisco Wireless Controller web interface. The browser address bar displays '9.12.137.95/wireless'. The navigation menu at the top includes 'Home', 'Monitor', and 'Help', with 'Home' circled in red. The main content area is divided into two columns. The left column contains a 'System Summary' section with the following data:

System Time	18:54:12.963 UTC Thu Jul 23 2015
Software Version	03.06.03.E.536 EARLY DEPLOYMENT [PROD BUILD] ENGINEERING NOVA_WEEKLY BUILD
System Name	JKAT-RFC
System Model	AIR-CT5760
Up Time	9 hours, 28 minutes
Wireless Management IP	9.12.137.95
802.11 a/n/ac Network State	Enabled
802.11 b/g/n Network State	Enabled

Below this is an 'Access Point Summary' table:

	Total	Up	Down
802.11a/n/ac Radios	1	1	0
802.11b/g/n Radios	1	1	0
All APs	1	1	0

The right column contains a 'Search' section with a 'Username' input field and a 'Search' button. Below that is a 'Top WLANs' section with a table:

Profile Name	Number of Clients
QM	0
jolouisan	0

Underneath is an 'AVC for WLAN : QM' section with the message 'AVC is not enabled on this WLAN'. At the bottom right, there is a 'Rogue APs' section showing 'Active Rogue APs' as 203 with a 'Detail' link.

フル アクセス権限が付与される特権レベル 15 ユーザからのアクセスを次に示します。

### System Summary

System Time	18:51:40.772 UTC Thu Jul 23 2015
Software Version	03.06.03.E.536 EARLY DEPLOYMENT [PROD BUILD] ENGINEERING NOVA_WEEKLY BUILD
System Name	JKAT-RFC
System Model	AIR-CTS760
Up Time	9 hours, 26 minutes
Wireless Management IP	9.12.137.95
802.11 a/n/ac Network State	Enabled
802.11 b/g/n Network State	Enabled
Software Activation	<a href="#">Detail</a>

### Access Point Summary

	Total	Up	Down
802.11a/n/ac Radios	1	1	0
802.11b/g/n Radios	1	1	0
All APs	1	1	0

### Client Summary

### Protocol Statistics

### Search

Username

### Top WLANs

Profile Name	Number of Clients
QM	0
jolouisan	0

### AVC for WLAN : QM

AVC is not enabled on this WLAN

### Rogue APs

Active Rogue APs 207 [Detail](#)