目次

概要

この資料に Cisco ACS TACACS+ 認証および許可プロファイルを異なる特権レベルで作成し WebUI にアクセスのための 5760 とそれを統合方法を説明されています。 この機能は 3.6.3 から前にサポートされます（ないこの書き込みの時間の 3.7.x で）。

前提条件

要件

読者が Cisco ACS およびコンバージしたアクセスコントローラ 設定について詳しく知っていることが仮定されます。 この資料は TACACS+ 許可の範囲内でそれらの 2 つのコンポーネント間の相互対話にだけ焦点を合わせます。

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。

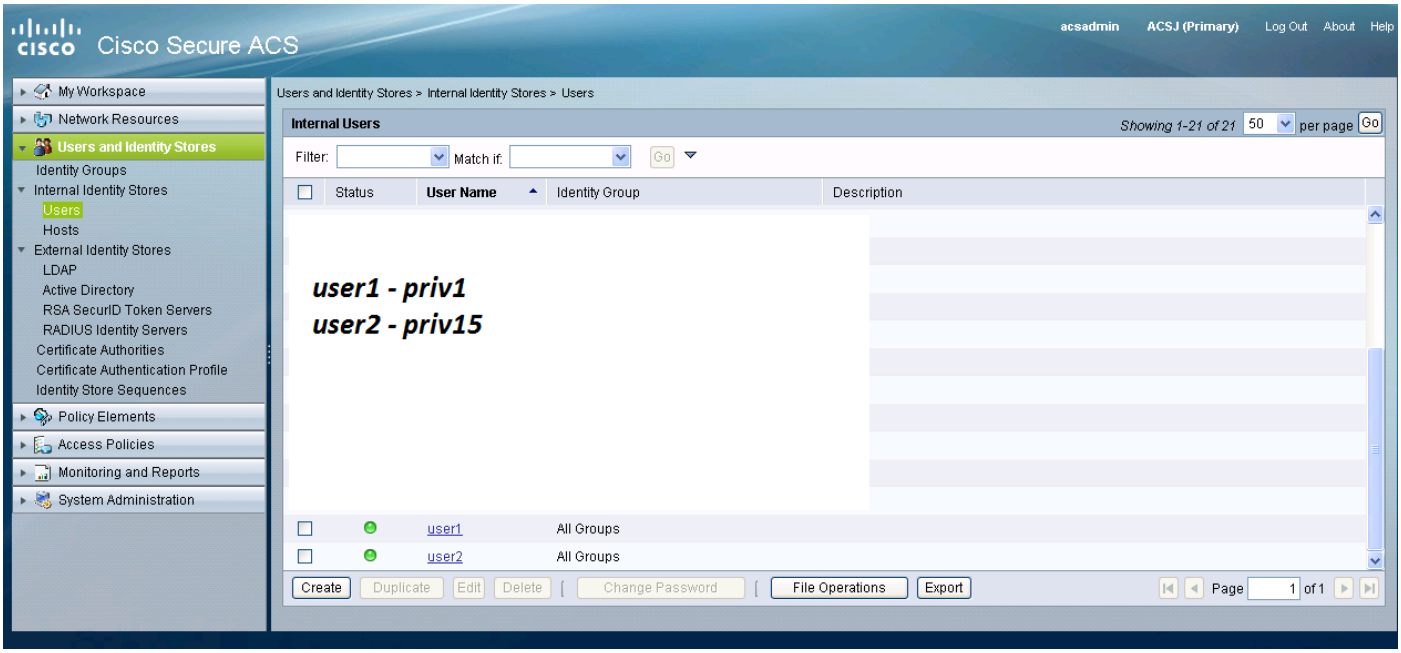
- Cisco はアクセス 5760、リリース 3.6.3 コンバージしました
- Cisco Acess コントロール サーバ（ACS） 5.2

設定

ACS の少数のテスト ユーザを作成して下さい

「ユーザ クリックすれば識別は」を保存しましたり、そして「ユーザ」を選択します。

後で説明されるのような少数のテスト ユーザを"Create"を クリックする、設定して下さい。



ポリシー要素およびシェル プロファイルの設定

アクセスの 2 つの異なる型のための 2 つのプロファイルを作成する必要があります。Cisco TACACS 世界の特権 15 は制約事項なしでデバイスへフルアクセスを提供することを意味します。 1 つに一方では一定限度のコマンドだけログインし、実行することを許可します特権を与えって下さい。cisco によって提供されるアクセスのレベルの短い 記述は下記にあります。

特権レベル 1 = 無特権 (プロンプトは router> です) 、ログオ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 は = ほとんど使用されて、しかし 5 つのコマンドが含まれていません: disable、enable、exit、help、logout

5760 で、レベルはレベル 1.と 2-14 同じと考慮されます。 それらは 1.と同じ特権を与えられます。 **5760 のある特定のコマンドの tacacs 特権レベルを設定しないで下さい。** タブごとの UI アクセスは 5760 年にサポートされません。 Monitor タブ (priv1) にフルアクセス (priv15) またはアクセスだけあることができます。 また、特権レベル 0 を持つユーザはログインするために not alowed。

特権 15 水平なシェル アクセス プロファイルの作成

下記の Print 画面を使用するそのプロファイルを作成して下さい:

「ポリシー要素」をクリックして下さい。 「シェル プロファイル」をクリックして下さい。

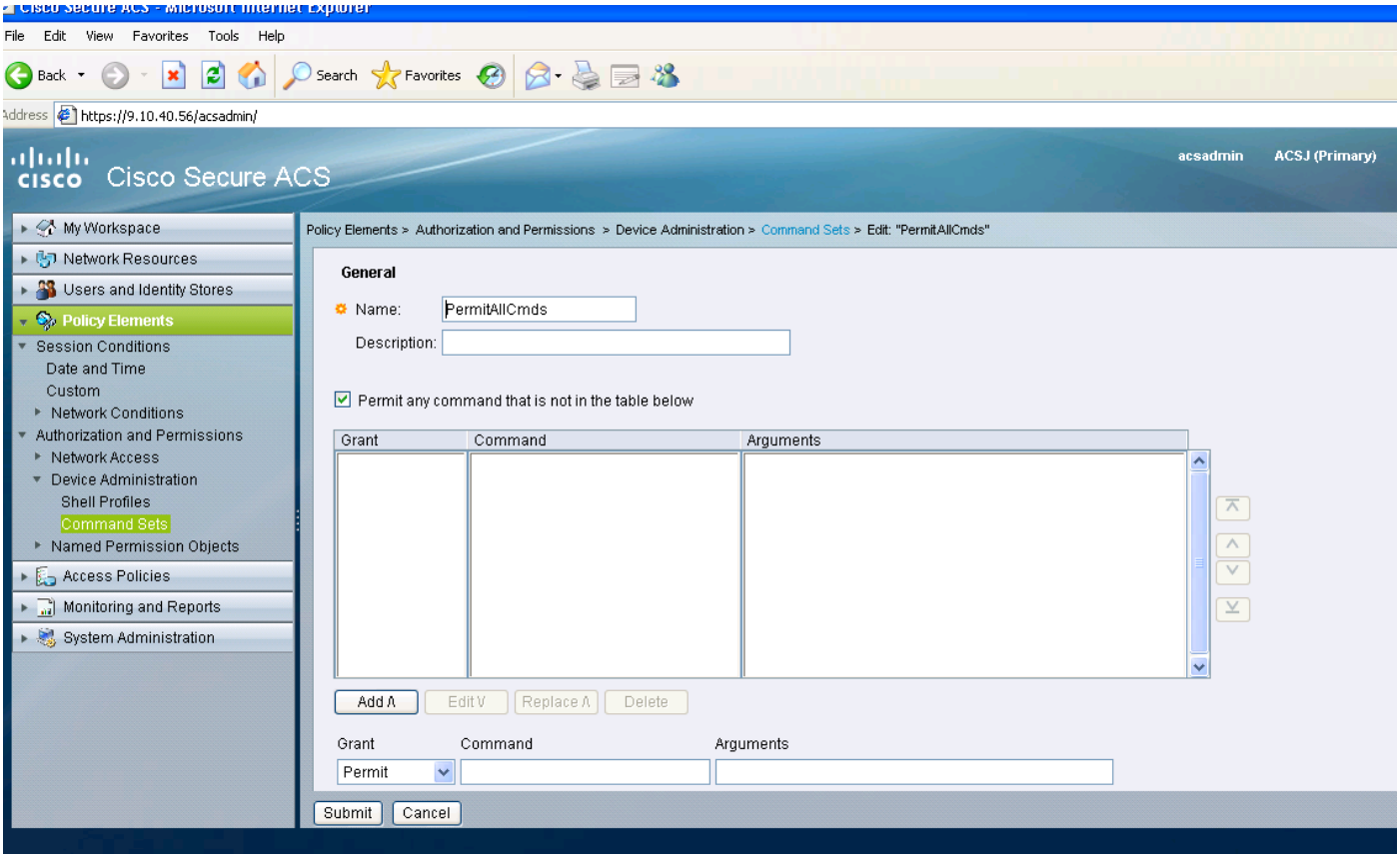
新しいものを作成して下さい。

「一般的なタスク」タブで入り、15 にデフォルトおよび最大 特権レベルを設定 して下さい。

管理者ユーザ向けのコマンド セットの作成

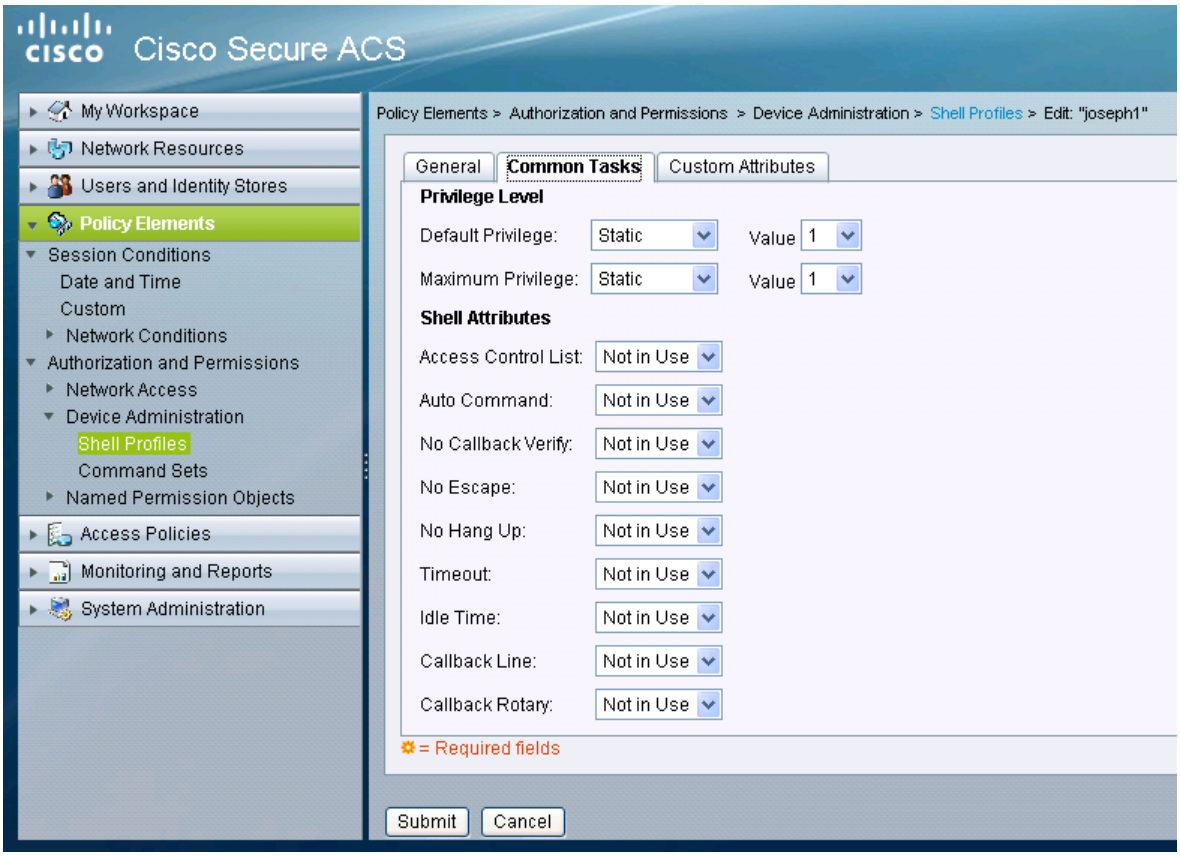
TACACS デバイスに作成して使用されるコマンドのセットです。それらが使用することがユーザができるコマンドを制限するのに使用することができます特定プロファ

イルしなさいこと場合割り当てられた。 5760 で、制約事項が渡される特権レベルに基づいて Webui コードでされるのでコマンドは両方の特権 level1 のために設定 し、15 は同じです。



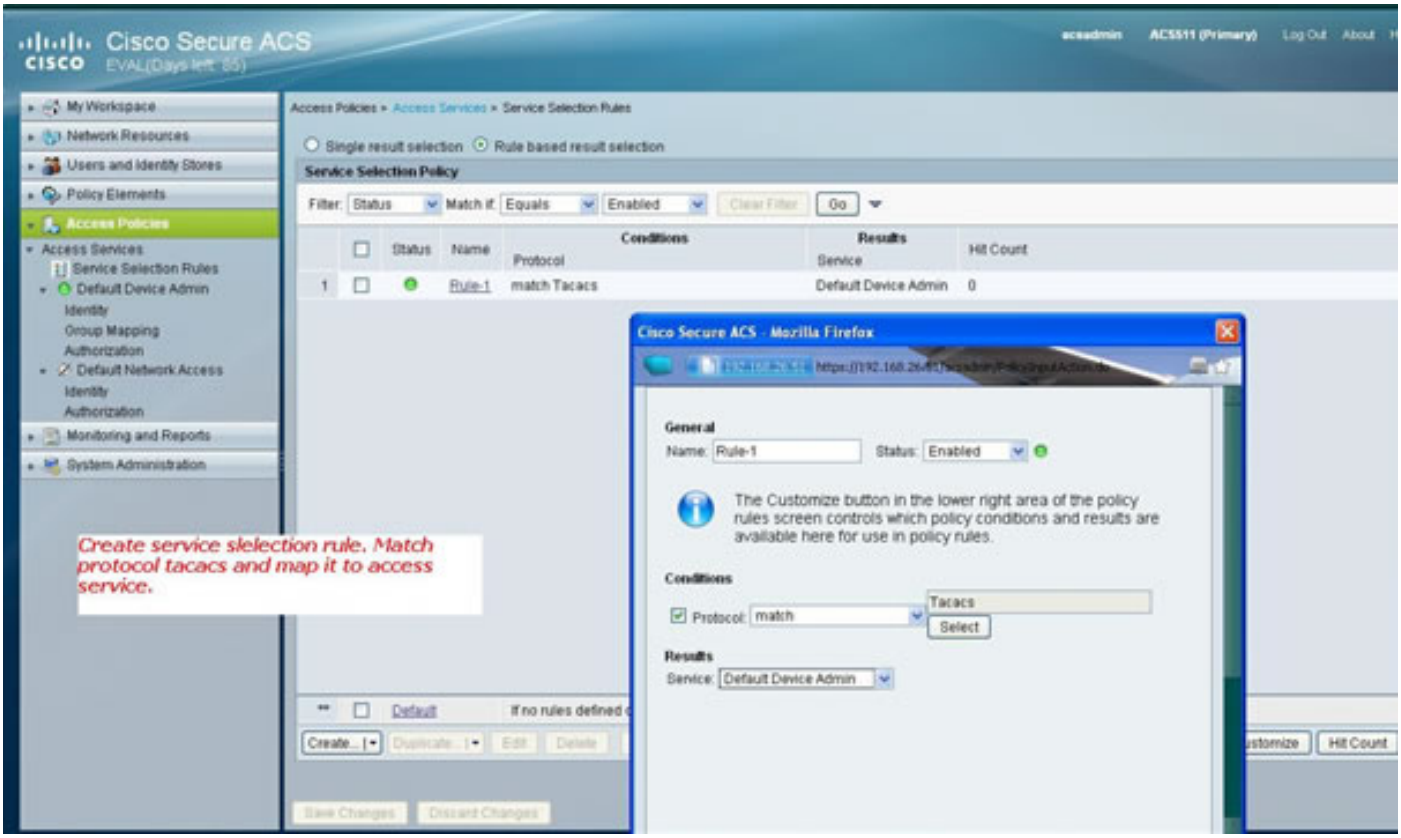
read only ユーザ向けのシェル プロファイルの作成

読み取り専用ユーザ向けの別のシェル プロファイルを作成して下さい。 このプロファイルは特権レベルが 1.に設定 されるファクトによって異なります。



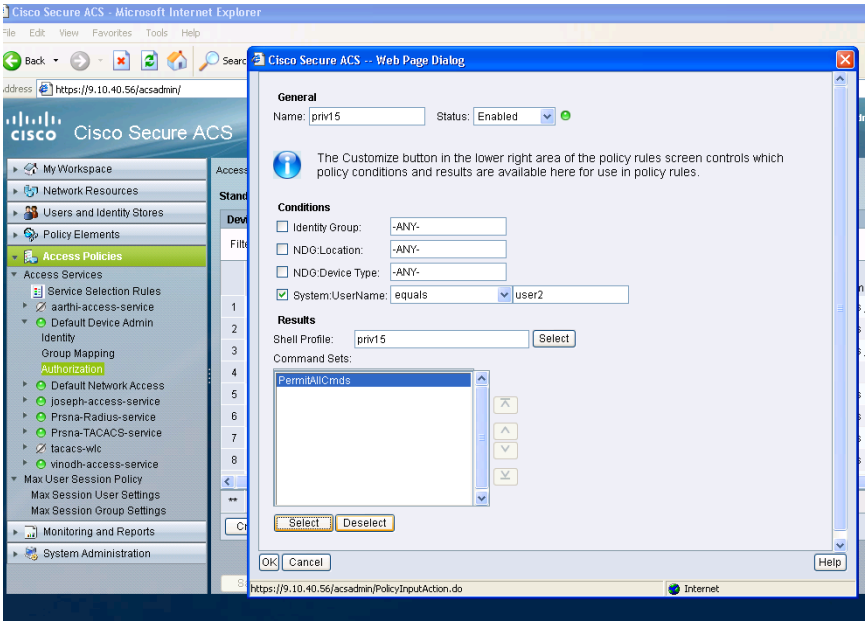
tacacs プロトコルを一致する サービス セレクション ルールを作成して下さい

ポリシーおよび設定によっては、5760 から来るルール一致する tacacs があることを確かめて下さい。



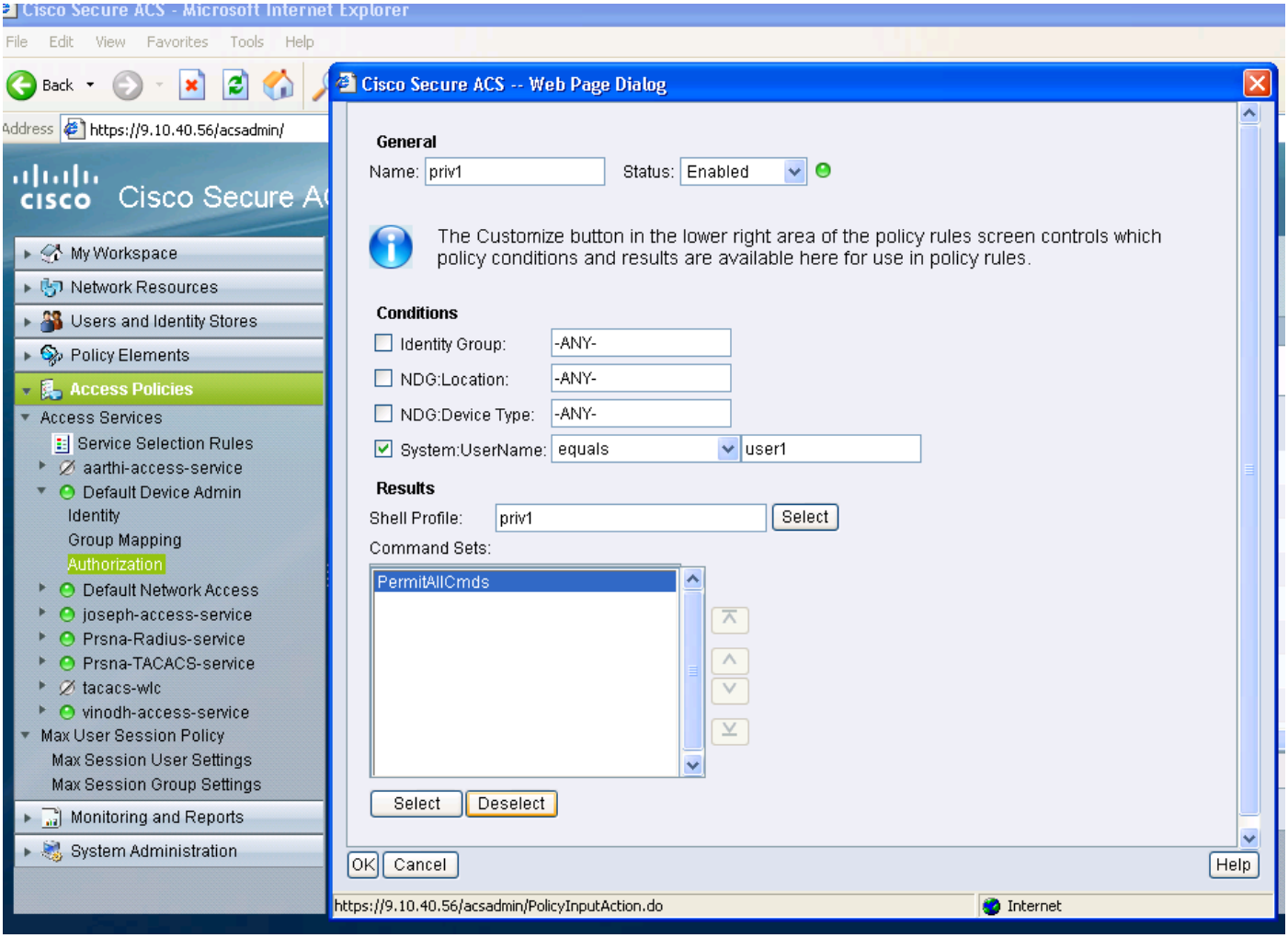
完全な管理 アクセスのための承認ポリシーを作成して下さい。

tacacs プロトコル 選択と使用されるデフォルト デバイ 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。 認証するのに tacacs プロトコルを使用するとき選択されるサービス ポリシーはデフォルト デバイ Admin ポリシーと呼ばれます。 ポリシーはそれ自体 2 つのセクションから成り立つこと。 Identiy はおよび彼が設定される許可 プロファイルに従ってすることができるか何をだれユーザがであり、どんなグループ彼がに属するか意味します (ローカルか外部)。 設定 される設定しているユーザに関するコマンドを割り当てて下さい。



read only 管理 アクセスのための承認ポリシーを作成して下さい。

同じは読み取り専用ユーザ向けにされます。 この例はユーザ 1 向けの特権レベル 1 シェル プロファイルをおよび特権 15 からユーザ 2.設定します。



tacacs のための 5760 の設定

1. Radius/TACACSサーバは設定される必要があります。

TACACSサーバ tac_acct

アドレス ipv4 9.1.0.100

キー cisco

1. サーバグループを設定して下さい

AAA グループ サーバ TACACS+ gtac

サーバ名 tac_acct

上記のステップまでの前提条件がありません。

1. 認証 および 権限 メソッドリストを設定して下さい

AAA認証ログイン <method-list> グループ <srv-grp>

aaa authorization exec <method-list> グループ srv-grp>

aaa authorization exec デフォルト グループ <srv-grp>　----http の tacacs を得る Ã 回避策。

上記の 3 つのコマンドおよび他の認証 および 権限 パラメータはすべて半径/tacacs またはローカル同じデータベースを使用する必要があります

たとえば、コマンド許可が必要とすれば、それまた同じデータベースを指す必要があります有効に なりました。

前のため:

AAA 許可コマンド 15 <method-list> グループ <srv-grp> か。か。> データベース (tacacs/半径かローカル) を指しているサーバグループは同じであるはずです。

1. 上記のメソッドリストを使用するために http を設定して下さい

ip http authentication AAA ログインauth <method-list> か。か。か。> メソッドリストはメソッドリストがあっても、ここに明示的に 規定 されて必要としますか。デフォルトか。

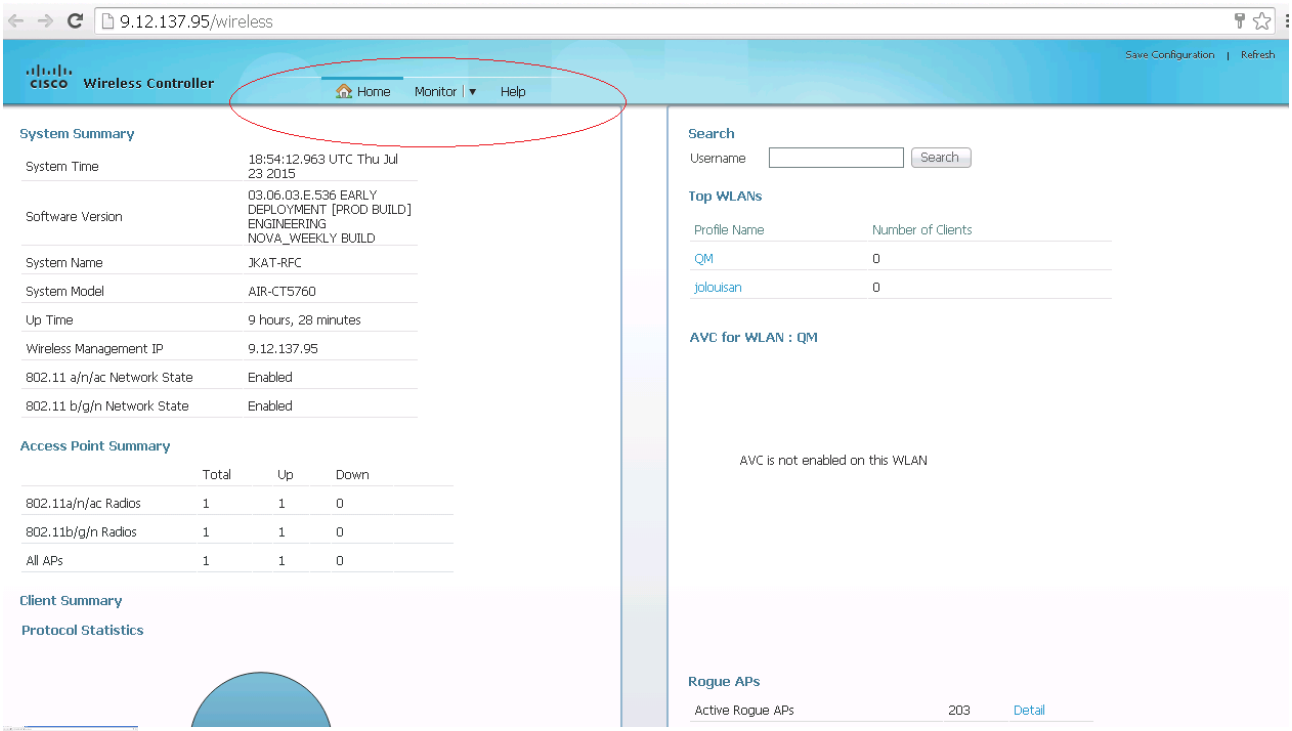
ip http authentication AAA EXECauth <method-list>

**注意するべきポイント

- のメソッドリストを設定しませんか。行 VTY か。　構成パラメータ。 上記のステップにおよび行 VTY に異なる構成がある場合、行 VTY 構成は優先します。
- データベースは ssh/telnet および webui のようなすべての管理設定型を渡って同じであるはずです。
- HTTP認証は明示的に定義されるメソッドリストがあるはずです。

2 つの異なるプロファイルとの同じ 5760 にアクセスする方法

下記は制限されたアクセスが与えられる特権レベル 1 ユーザからアクセスです




ルアクセスを与えられる特権レベル 15 ユーザからアクセスです