IOS および ASA/PIX/FWSM での ACS シェル コマンドの Authorization Sets の設定例

目次

概要

このドキュメントでは、Cisco IOS® ルータまたはスイッチや Cisco Security Appliances（ASA/PIX/FWSM）などの AAA クライアントの Cisco Secure Access Control Server（ACS）のシェル コマンド許可セットを、TACACS+ を承認プロトコルとして設定する方法について説明します。

注: ACS Express はコマンド許可をサポートしていません。

前提条件

要件

このドキュメントでは、AAA クライアントと ACS の両方で基本設定が実行されていることを想

定しています。

ACS で [Interface Configuration] > [Advanced Options] を選択し、[Per-user TACACS+/RADIUS Attributes] チェックボックスがオンになっていることを確認します。

使用するコンポーネント

このドキュメントの情報は、ソフトウェア バージョン 3.3 以降が稼働する Cisco Secure Access Control Server（ACS）に基づいています。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

コマンド許可セット

コマンド許可セットは、任意のネットワーク デバイス上で発行された各コマンドの許可を制御する中心的なメカニズムとなります。 この機能で、許可の制限を設定するために必要なスケーラビリティと管理性が大幅に向上します。

ACS では、デフォルトのコマンド許可セットとして、シェル コマンド許可セットと PIX コマンド許可セットがあります。 CiscoWorks Management Center for Firewalls などのシスコ デバイス管理アプリケーションは、追加のコマンド許可セット タイプをサポートするように ACS に指示できます。

注: PIX コマンド許可セットでは、TACACS+ コマンド許可要求がサービスを *pixshell* として識別する必要があります。 このサービスが、ファイアウォールで使用される PIX OS のバージョンに実装されていることを確認します。 そうでない場合は、シェル コマンド許可セットを使用して、PIX デバイスのコマンド許可を実行します。 詳細については、「ユーザ グループのシェル コマンド許可セットの設定」を参照してください。

注: PIX OS バージョン 6.3 以降では、pixshell サービスは実装されていません。

注: Cisco Security Appliance（ASA/PIX）では、ユーザをログイン中に直接、イネーブル モードにすることはできません。 ユーザは、手動でイネーブル モードにする必要があります。

デバイスがホストする管理 Telnet セッションをより詳細に制御するために、TACACS+ を使用するネットワーク デバイスは、各コマンド ラインの許可を、その実行前に要求できます。 一連のコマンドを定義して、所定のデバイスでの特定のユーザによる実行が許可または拒否されるようにすることができます。 ACS は、次の機能で、この能力をさらに強化しています。

- **Reusable Named Command Authorization Sets**：ユーザもユーザ グループも直接引用せずに、コマンド許可の名前付きセットを作成できます。 さまざまなアクセス プロファイルを表す複数のコマンド許可セットを定義できます。 次に、例を示します。コマンド許可セット [Help desk] は、**show run** などの上位レベルのブラウジング コマンドへのアクセスを許可し

ますが、コンフィギュレーション コマンドはすべて拒否します。コマンド許可セット [All network engineers] には、企業のすべてのネットワーク技術者に許可するコマンドの限定リストを含めることができます。[Local network engineers] コマンド許可セットでは、すべてのコマンドを許可できます（また、IP アドレス設定コマンドを含むことができます）。

- **Fine Configuration Granularity**：名前付きコマンド許可セットとネットワーク デバイス グループ（NDG）の間の関連付けを作成できます。 したがって、ユーザがアクセスするネットワーク デバイスに応じて、ユーザに異なるアクセス プロファイルを定義できます。 1 つの名前付きコマンド許可セットを複数の NDG に関連付け、複数のユーザ グループで使用できます。 ACS では、データ整合性が強化されています。 名前付きコマンド許可セットは、ACS 内部データベースに保持されます。 ACS のバックアップ機能と復元機能を使用すると、バックアップや復元を実行できます。 さらに、コマンド許可セットを他の設定データとともにセカンダリ ACS に複製することもできます。

シスコ デバイス管理アプリケーションをサポートするコマンド許可セット タイプでは、コマンド許可セット使用時に同様の利点があります。 デバイス管理アプリケーションのユーザを含む ACS グループにコマンド許可セットを適用して、デバイス管理アプリケーションのさまざまな特権の許可を実行できます。 この ACS グループは、デバイス管理アプリケーションにある各種のロールに対応できるため、必要に応じて、各グループに異なるコマンド許可セットを適用できます。

ACS には、コマンド許可フィルタリングに関する一連の 3 つの段階があります。 各コマンド許可要求は、次のリストの順に評価されます。

1. **Command Match**：ACS は、処理されたコマンドが、コマンド許可セットに含まれるコマンドに一致するかどうかを判断します。 コマンドが一致しない場合は、[Unmatched Commands] 設定の *permit* または *deny* でコマンド許可が決定されます。 一致するコマンドが見つかった場合は、評価が続行されます。
2. **Argument Match**：ACS は、提示されたコマンド引数が、コマンド許可セットに含まれるコマンド引数と一致するかどうかを判断します。どの引数も一致しない場合は、[Permit Unmatched Args] オプションが有効かどうかでコマンド許可が決定されます。 一致しない引数が許可されている場合は、コマンドが許可され、評価が終了します。 それ以外の場合は、コマンドが許可されず、評価が終了します。すべての引数が一致した場合は、評価が続行されます。
3. **Argument Policy**：ACS は、コマンドの引数がコマンド許可セットの引数と一致すると判断した後は、各コマンド引数が明示的に許可されているかどうかを判断します。 すべての引数が明示的に許可されている場合、ACS はコマンド許可を付与します。 許可されない引数がある場合、ACS はコマンド許可を拒否します。

シェル コマンド許可セットの追加

このセクションには、コマンド許可セットの追加方法を説明する以下のシナリオが含まれます。

- シナリオ 1： 読み取り/書き込みアクセスまたはフル アクセスの権限
- シナリオ 2： 読み取り専用アクセスの権限
- シナリオ 3： 制限付きアクセスの権限

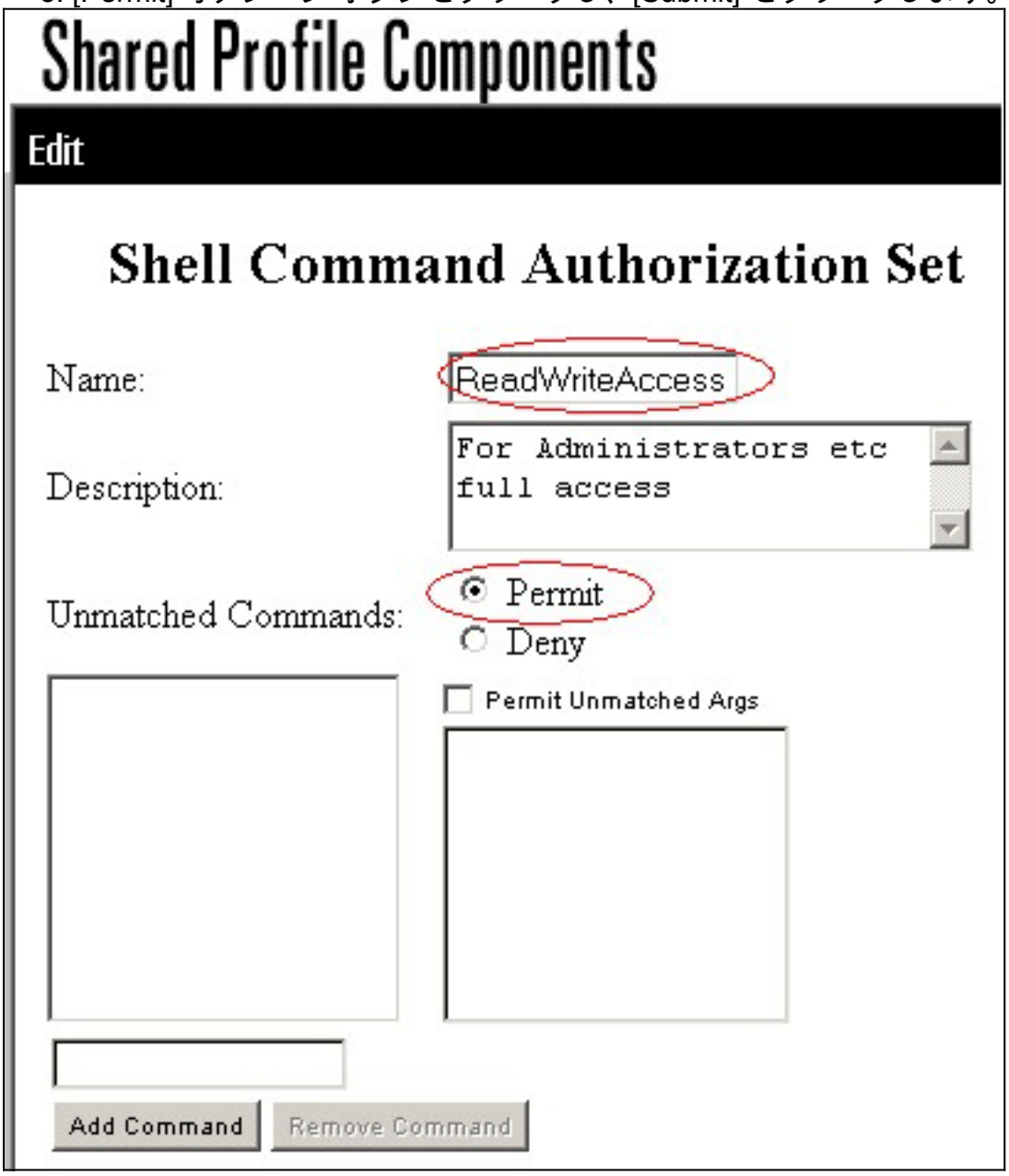
注: コマンド許可セットの作成方法に関する情報については、『Cisco Secure Access Control Server 4.1 ユーザ ガイド』の「コマンド許可セットの追加」セクションを参照してください。 コマンド許可セットの編集方法と削除方法に関する情報については、「コマンド許可セットの編集」および「コマンド許可セットの削除」を参照してください。

シナリオ 1： 読み取り/書き込みアクセスまたはフル アクセスの権限

このシナリオでは、ユーザに読み取り/書き込み（またはフル）アクセスが許可されています。

[Shared Profile Components] ウィンドウの [Shell Command Authorization Set] 領域で、次のように設定します。

1. [Name] フィールドに、コマンド許可セット名として **ReadWriteAccess** と入力します。
2. [Description] フィールドに、コマンド許可セットの説明を入力します。
3. [Permit] オプション ボタンをクリックし、[Submit] をクリックします。



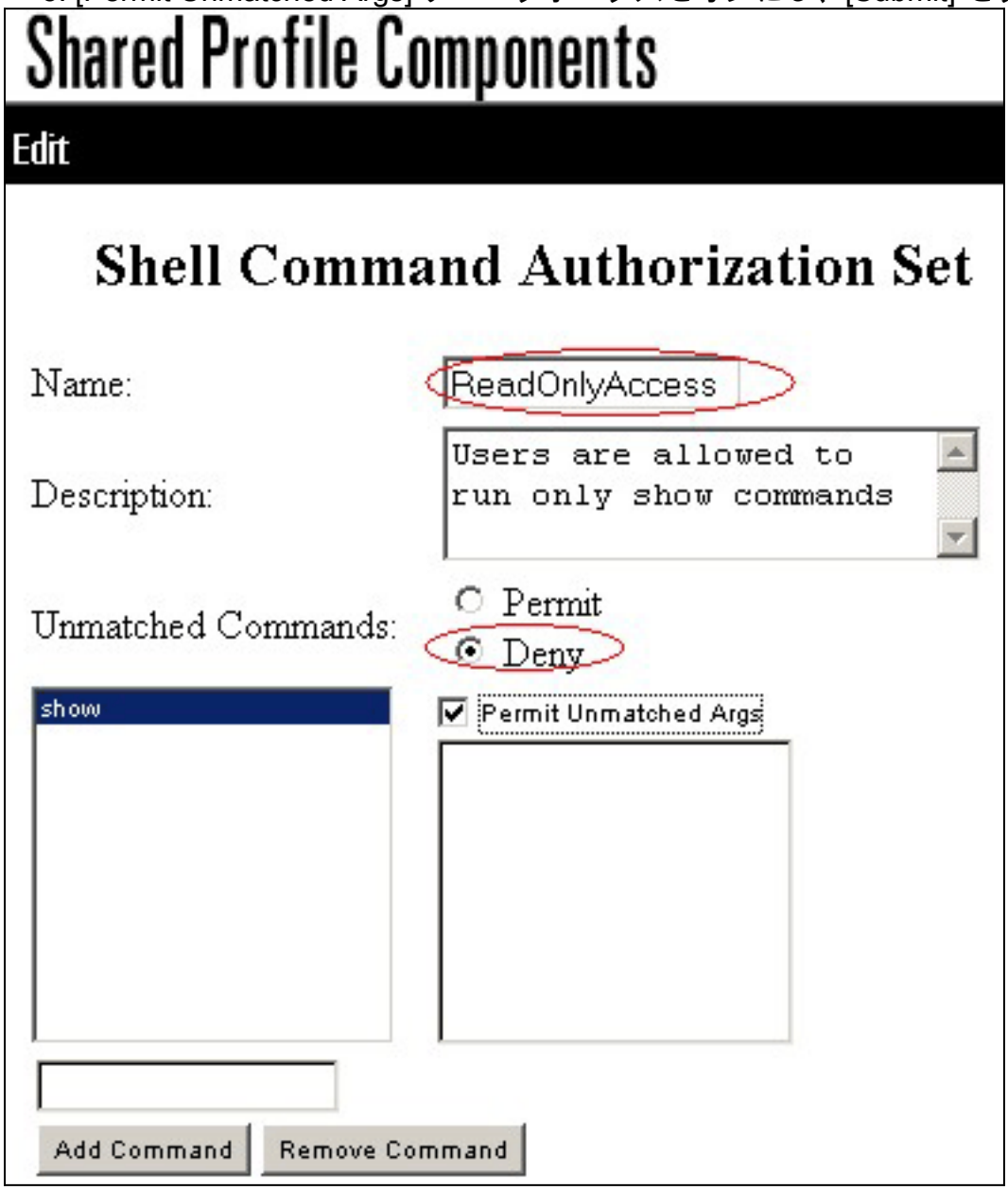
シナリオ 2： 読み取り専用アクセスの権限

このシナリオでは、ユーザは **show** コマンドだけを使用できます。

[Shared Profile Components] ウィンドウの [Shell Command Authorization Set] 領域で、次のように設定します。

1. [Name] フィールドに、コマンド許可セット名として **ReadOnlyAccess** と入力します。

2. [Description] フィールドに、コマンド許可セットの説明を入力します。
3. [Deny] オプション ボタンをクリックします。
4. [Add Command] ボタンの上のフィールドに **show** コマンドを入力し、[Add Command] をクリックします。
5. [Permit Unmatched Args] チェックボックスをオンにし、[Submit] をクリックします。

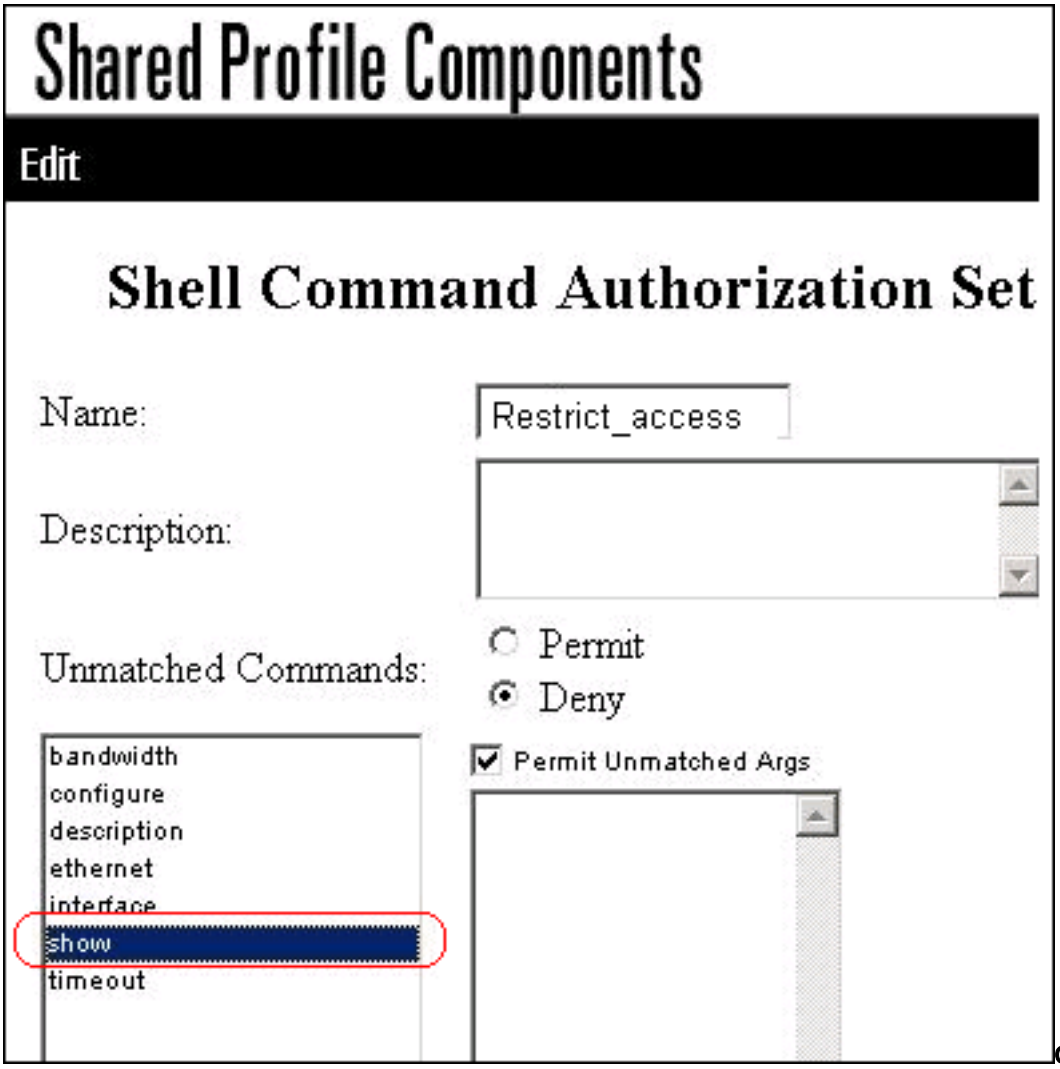


シナリオ 3： 制限付きアクセスの権限

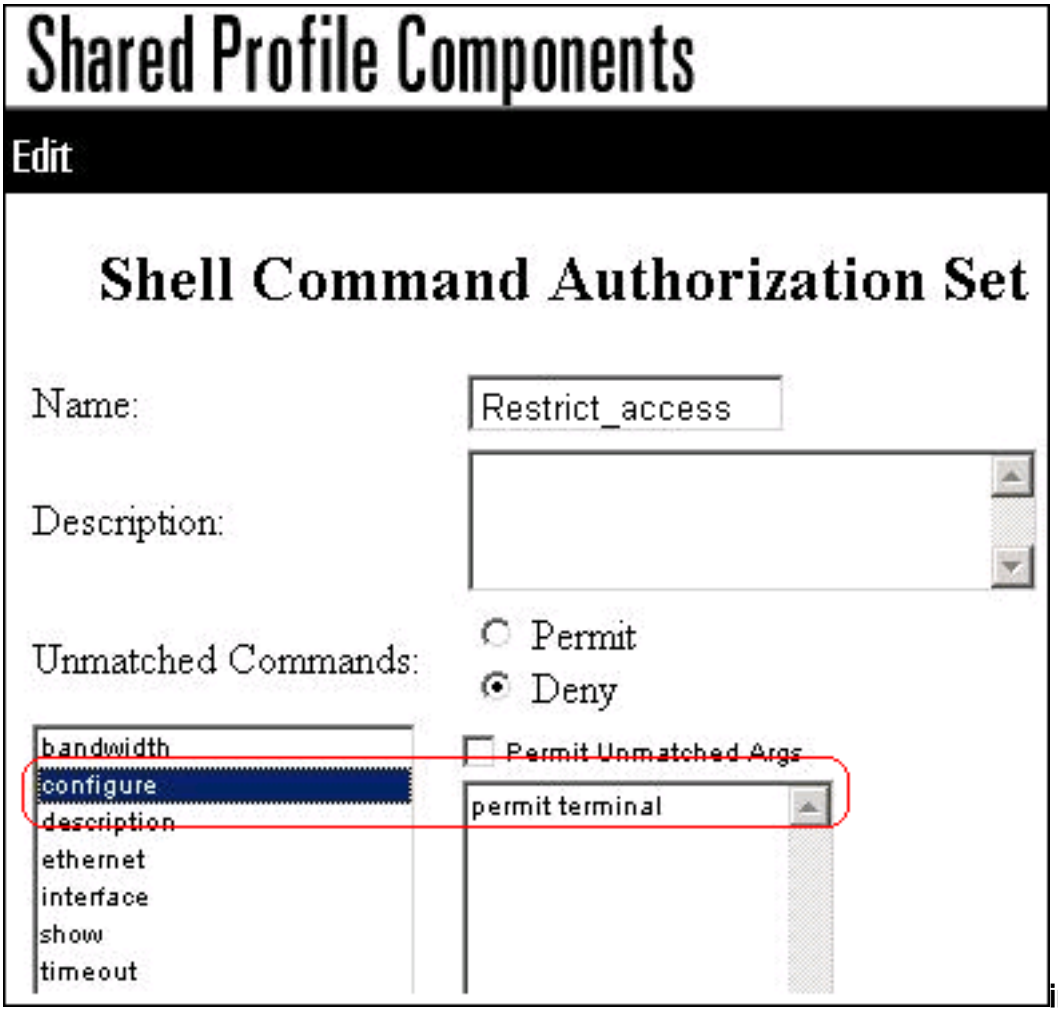
このシナリオでは、ユーザは選択コマンドを使用できます。

[Shared Profile Components] ウィンドウの [Shell Command Authorization Set] 領域で、次のように設定します。

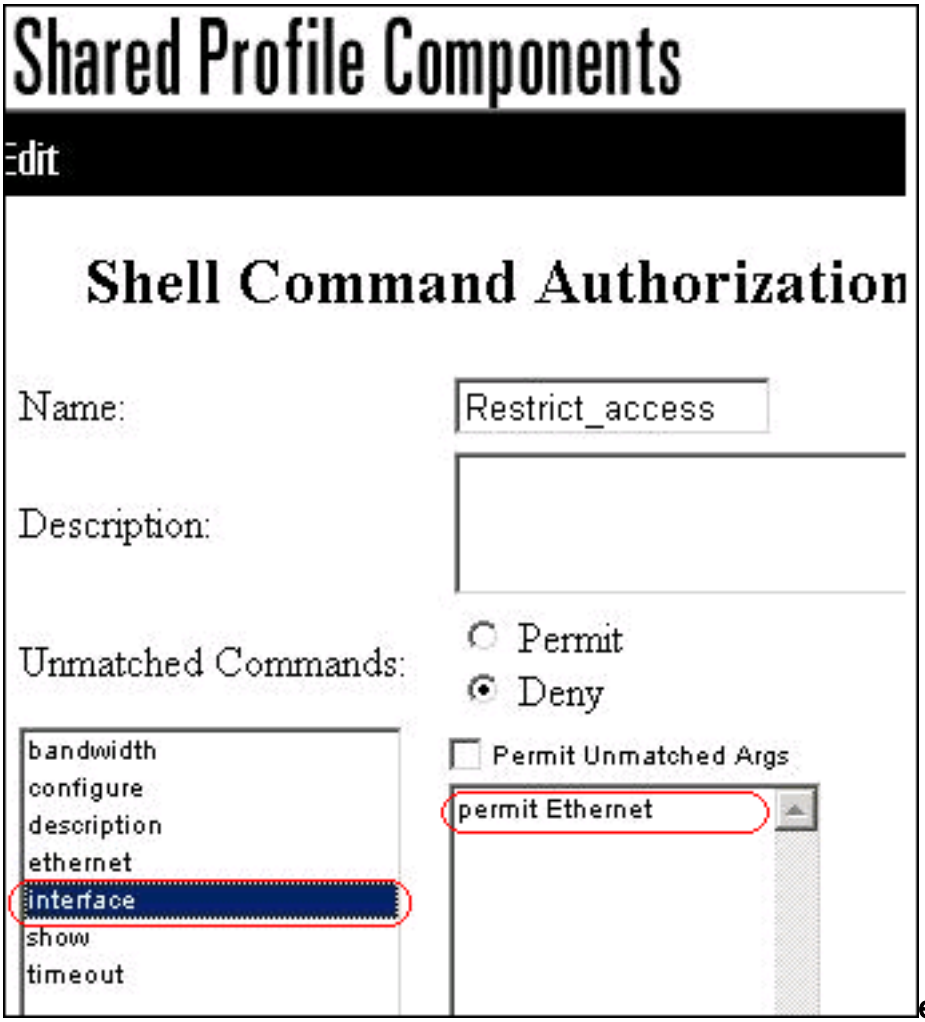
1. [Name] フィールドに、コマンド許可セット名として **Restrict_access** と入力します。
2. [Deny] オプション ボタンをクリックします。
3. AAA クライアントで許可するコマンドを入力します。[Add Command] ボタンの上にあるフィールドに **show** コマンドを入力し、[Add Command] をクリックします。



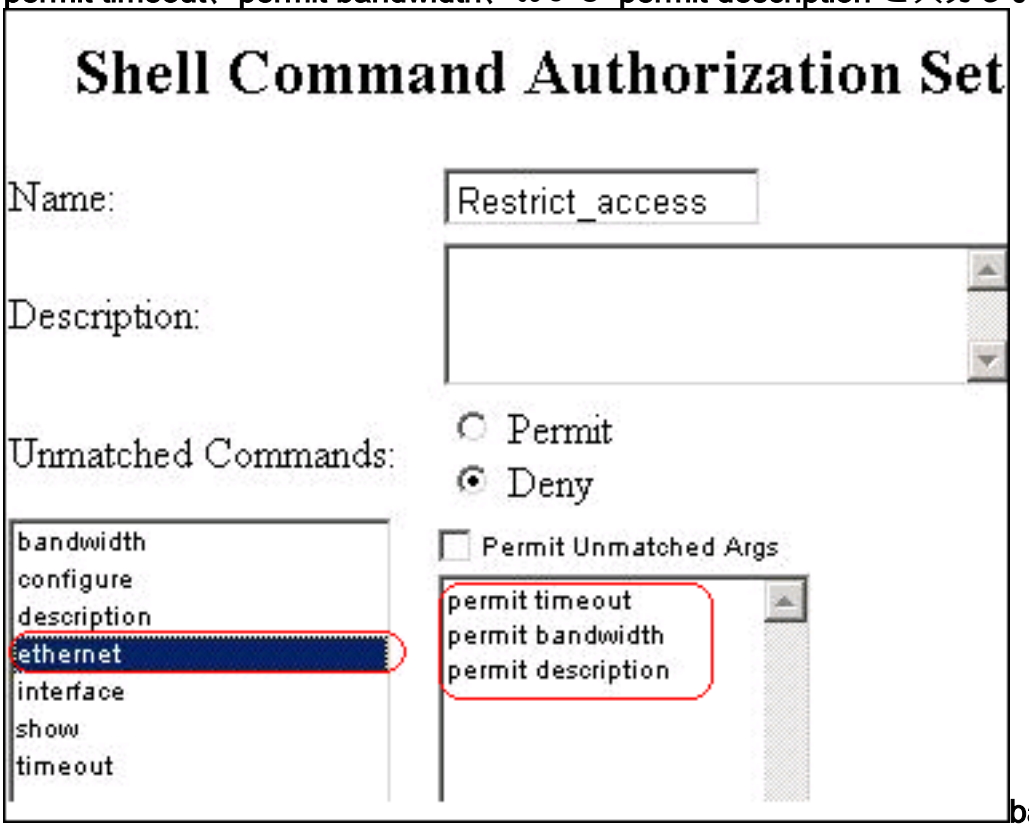
configure コマンドを入力し、[Add Command] をクリックします。**configure** コマンドを選択し、右側のフィールドに **permit terminal** と入力します。



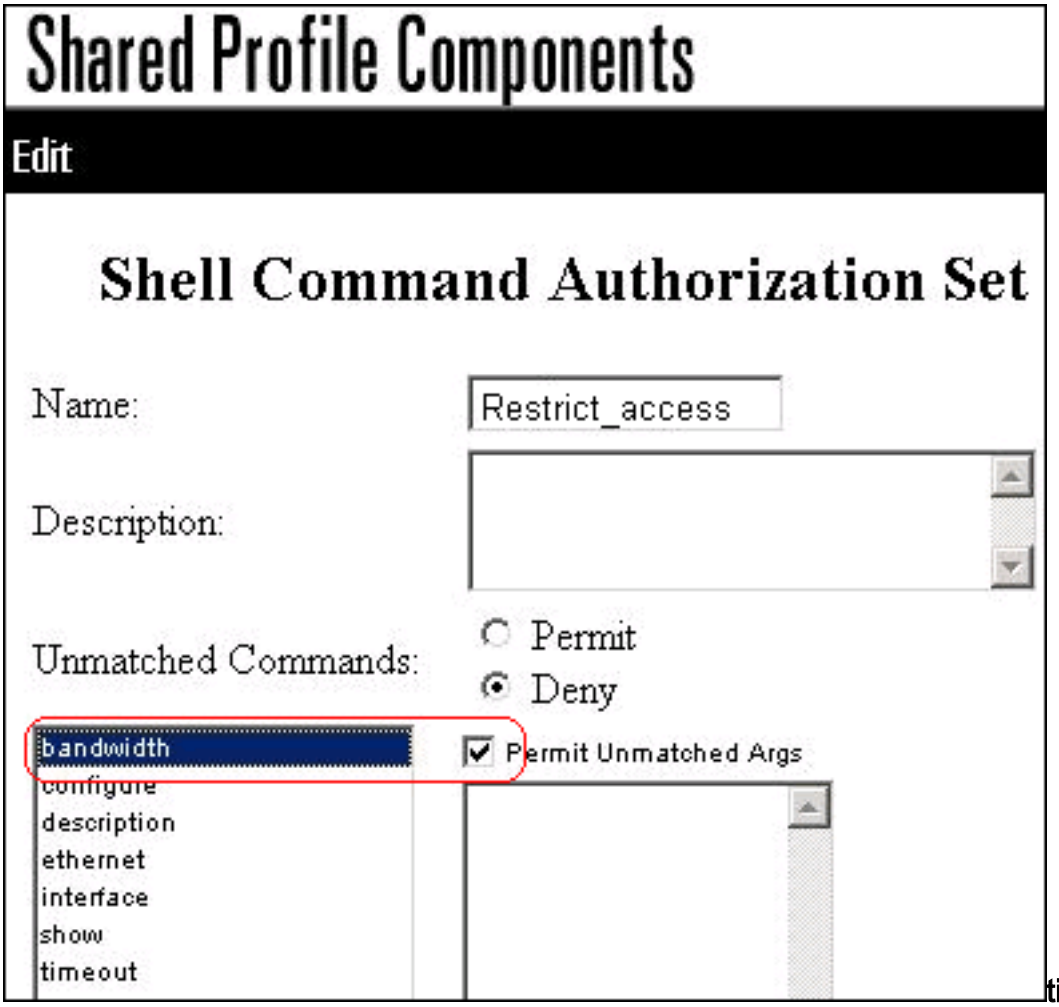
interface コマンドを入力し、[Add Command] をクリックします。**interface** コマンドを選択し、右側のフィールドに **permit Ethernet** と入力します。



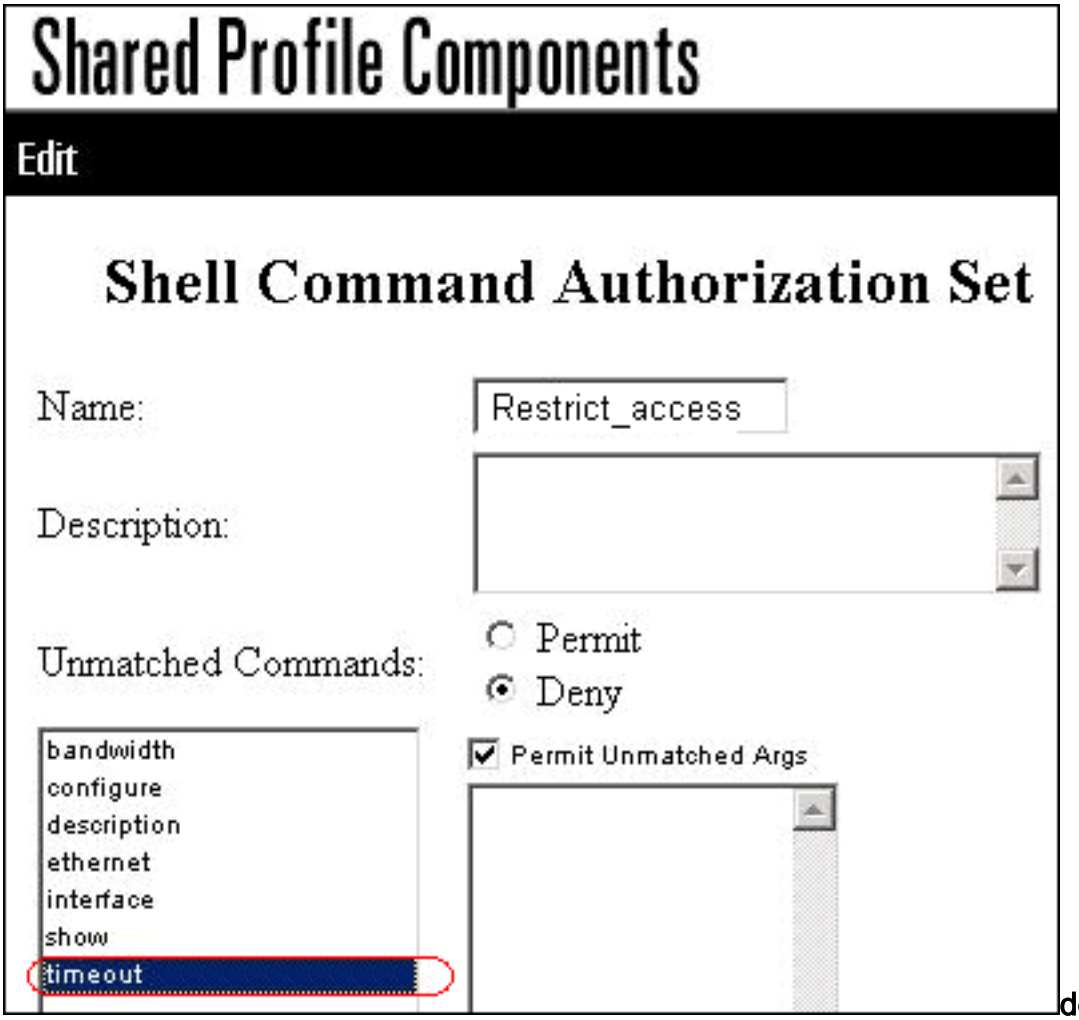
ethernet コマンドを入力し、[Add Command] をクリックします。interface コマンドを選択し、右側のフィールドに permit timeout、permit bandwidth、および permit description と入力します。



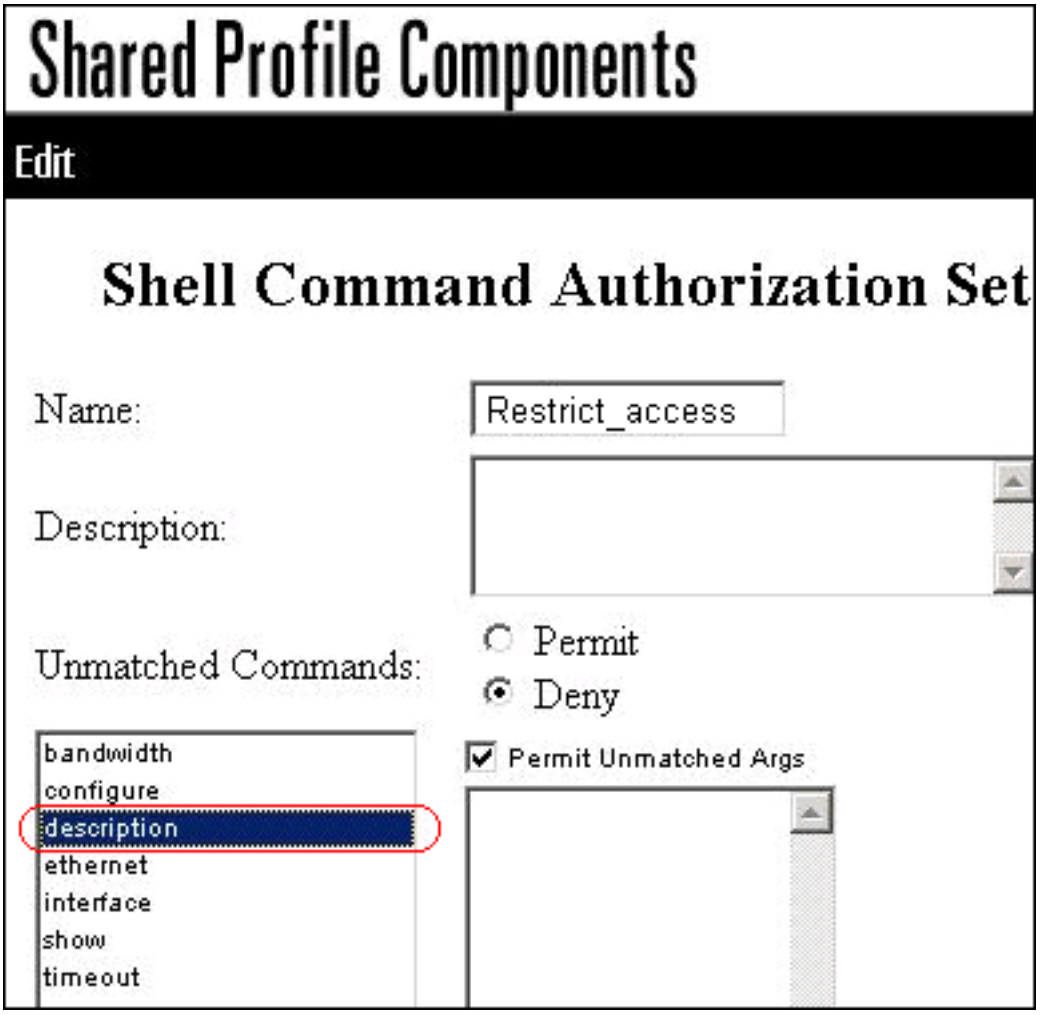
bandwidth コマンドを入力し、[Add Command] をクリックします。



timeout コマンドを入力し、[Add Command] をクリックします。



description コマンドを入力し、[Add Command] をクリックします。



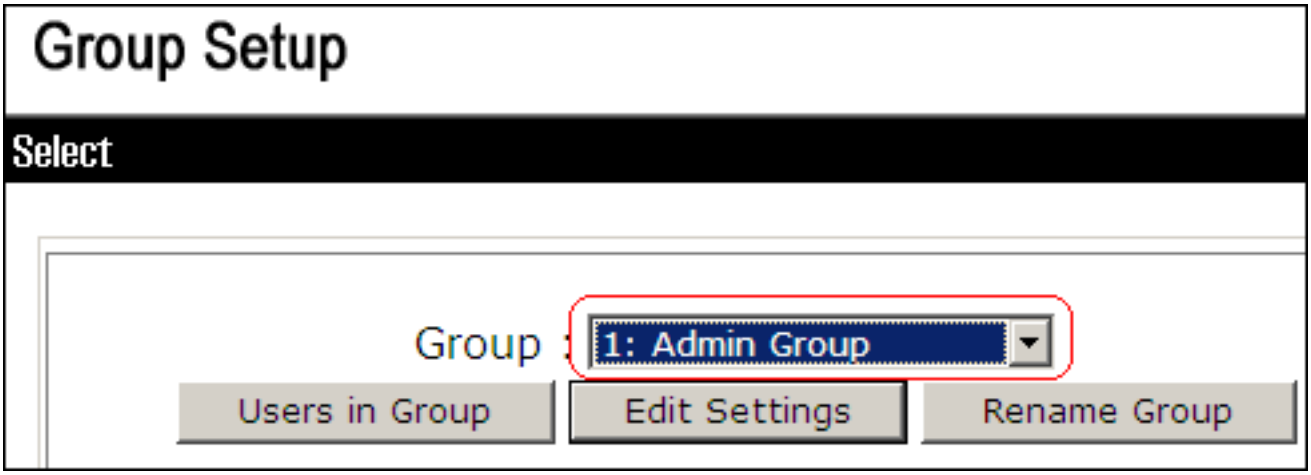
4. [Submit] をクリックします。

ユーザ グループへのシェル コマンド許可セットの関連付け

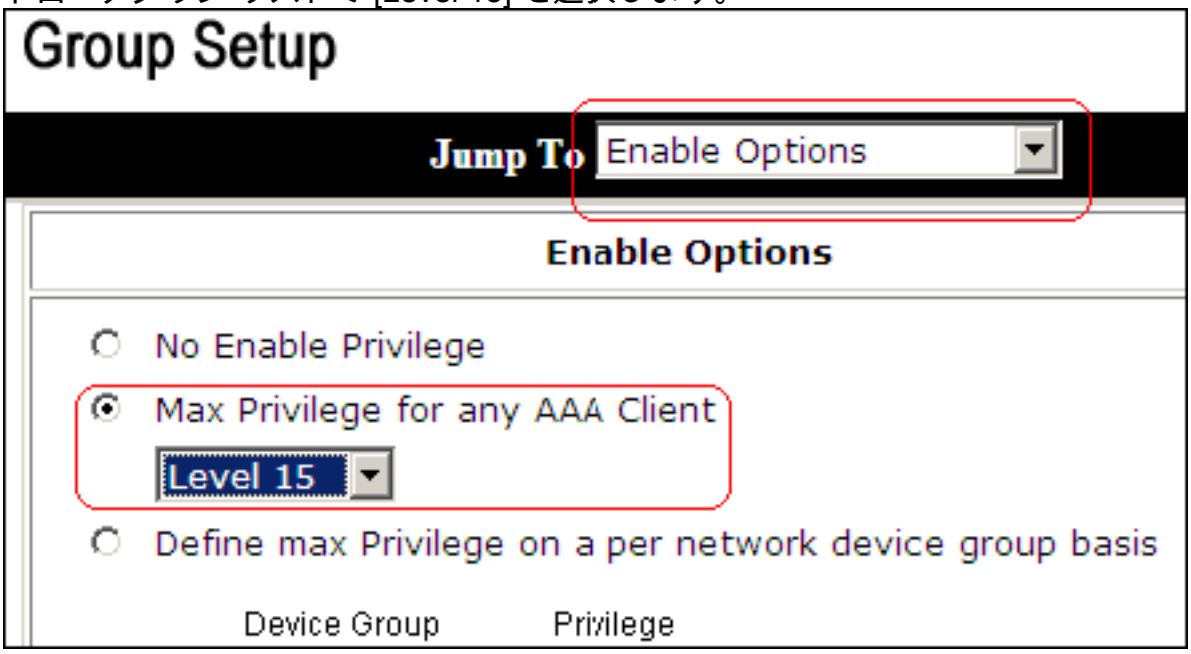
ユーザ グループのシェル コマンド許可セットの設定方法に関する情報については、『Cisco Secure Access Control Server 4.1 ユーザ ガイド』の「ユーザ グループのシェル コマンド許可セットの設定」セクションを参照してください。

ユーザ グループ（管理グループ）へのシェル コマンド許可セット（読み取り/書き込みアクセス）の関連付け

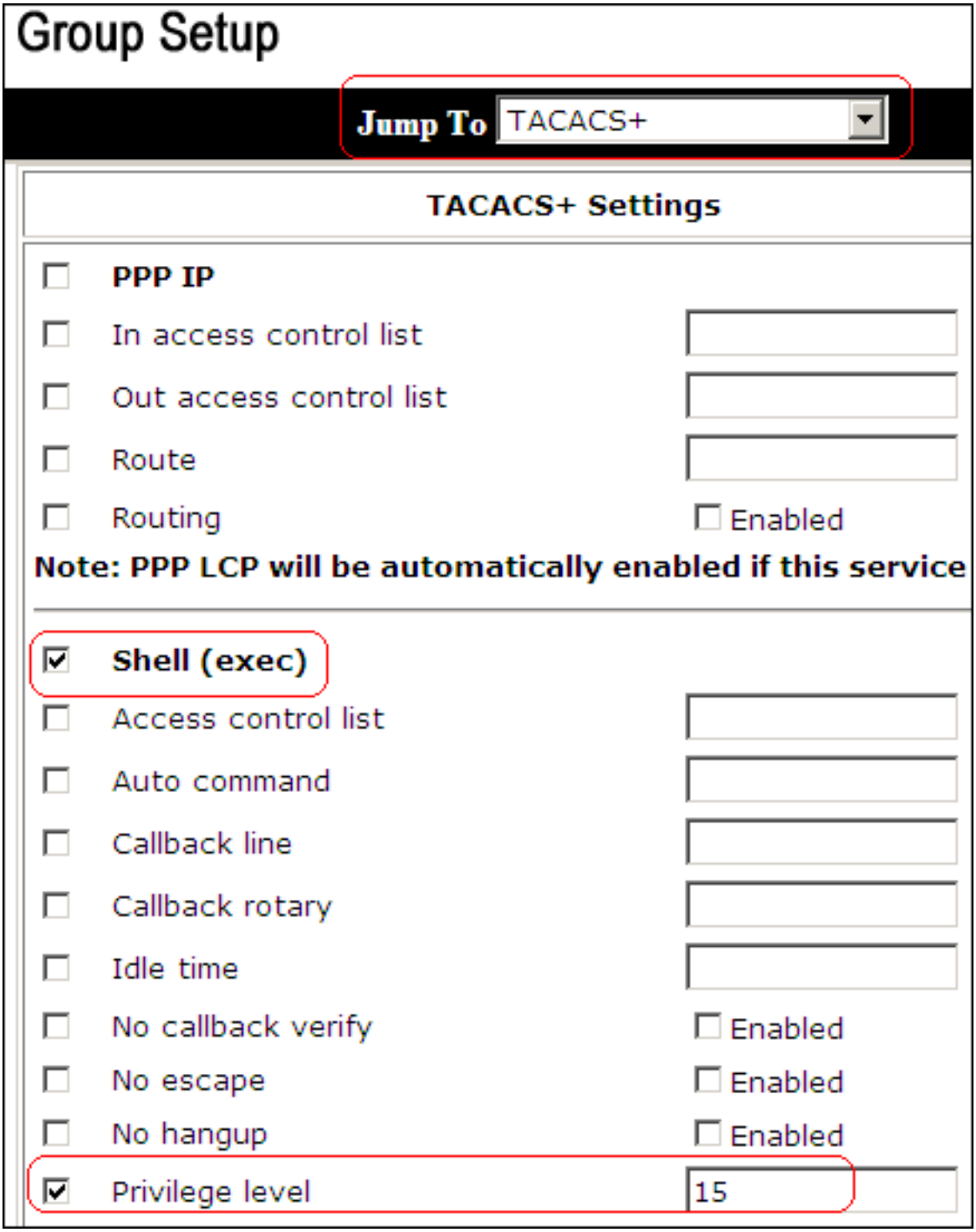
1. [ACS] ウィンドウで [Group Setup] をクリックし、[Group] ドロップダウン リストから [Admin Group] を選択します。



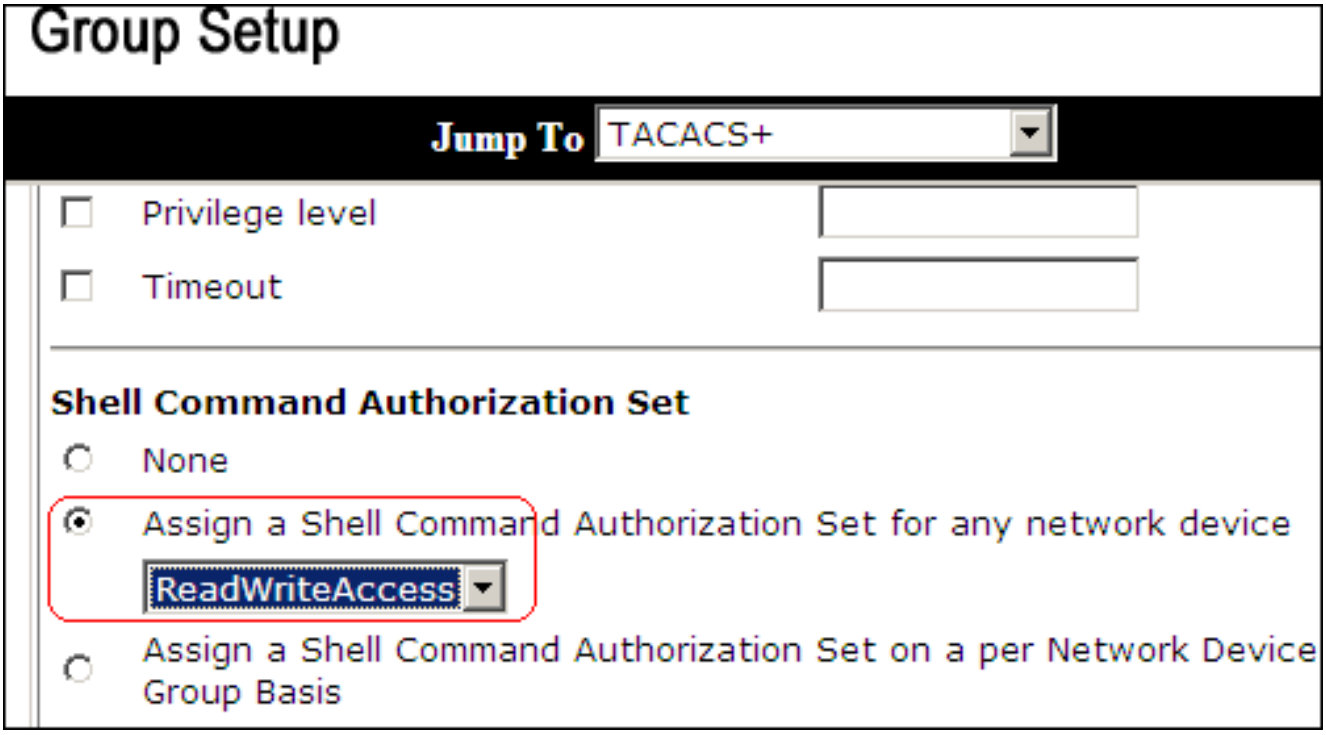
2. Edit Settings をクリックします。
3. [Jump To] ドロップダウン リストで [Enable Options] を選択します。
4. [Enable Options] 領域で [Max privilege for any AAA client] オプション ボタンをクリックし、ドロップダウン リストで [Level 15] を選択します。



5. [Jump To] ドロップダウン リストで [TACACS+] を選択します。
6. [TACACS+ Settings] 領域で [Shell (exec)] チェックボックスと [Privilege level] チェックボックスをオンにし、[Privilege level] フィールドに **15** と入力します。



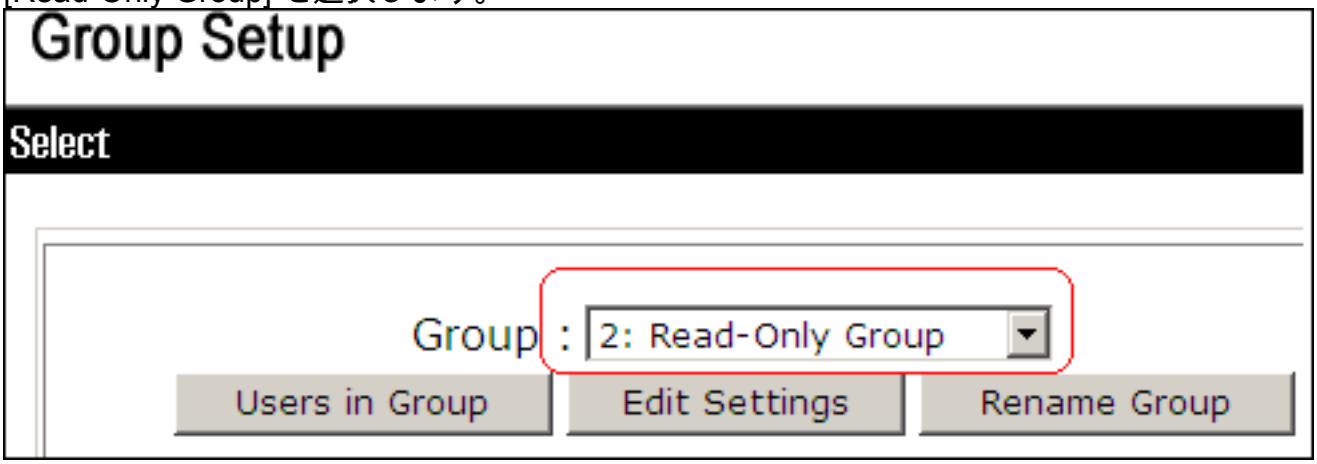
7. [Shell Command Authorization Set] 領域で [Assign a Shell Command Authorization Set for any network device] オプション ボタンをクリックし、ドロップダウン リストで [ReadWriteAccess] を選択します。



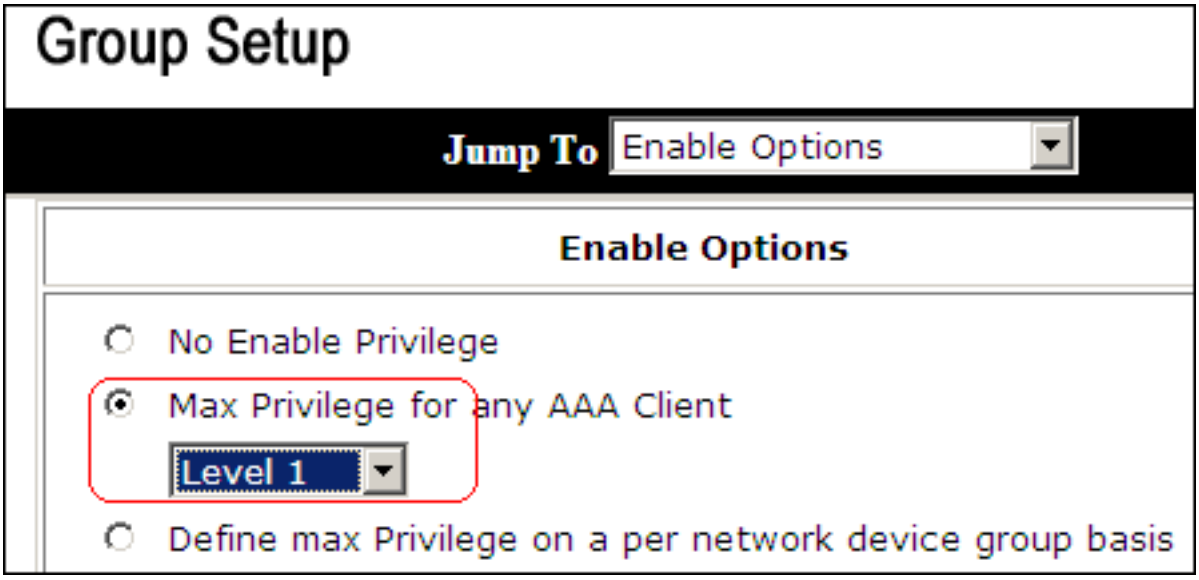
8. [Submit] をクリックします。

ユーザ グループ（読み取り専用グループ）へのシェル コマンド許可セット（読み取り専用アクセス）の関連付け

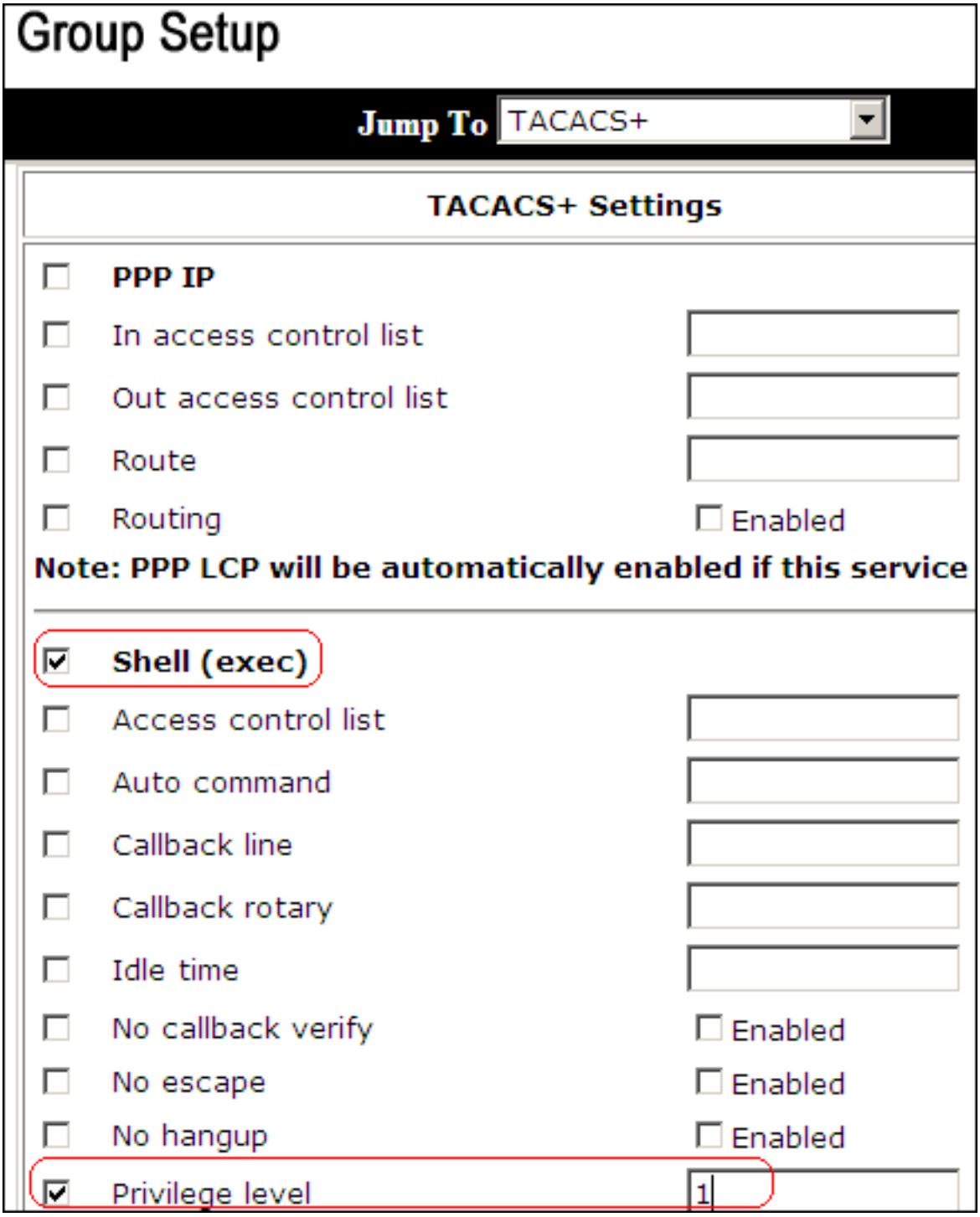
1. [ACS] ウィンドウで [Group Setup] をクリックし、[Group] ドロップダウン リストから [Read-Only Group] を選択します。



2. Edit Settings をクリックします。
3. [Jump To] ドロップダウン リストで [Enable Options] を選択します。
4. [Enable Options] 領域で [Max privilege for any AAA client] オプション ボタンをクリックし、ドロップダウン リストで [Level 1] を選択します。



5. [TACACS+ Settings] 領域で [Shell (exec)] チェックボックスと [Privilege level] チェックボックスをオンにし、[Privilege level] フィールドに 1 と入力します。



6. [Shell Command Authorization Set] 領域で [Assign a Shell Command Authorization Set for any network device] オプション ボタンをクリックし、ドロップダウン リストで [ReadOnlyAccess] を選択します。

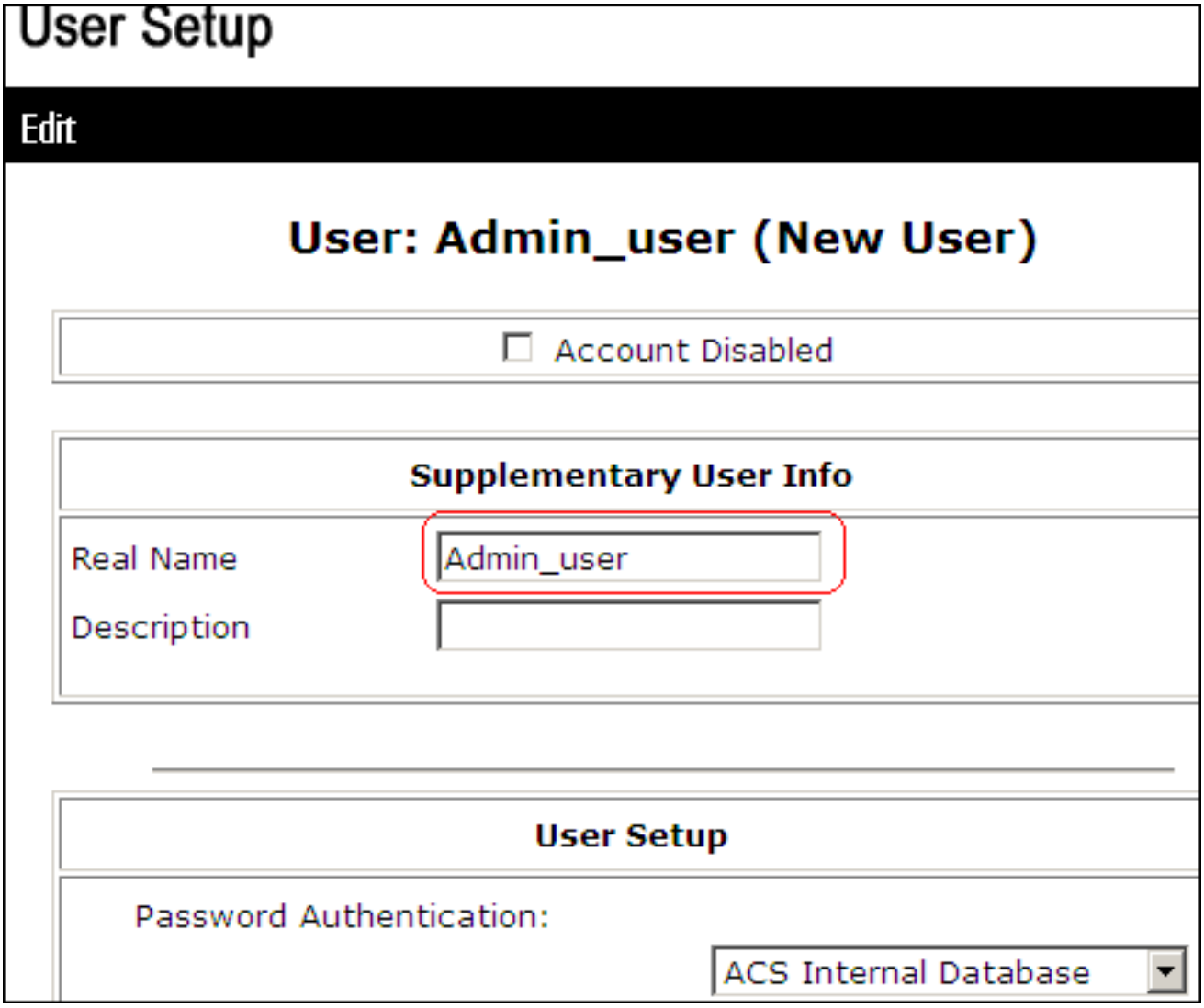
7. [Submit] をクリックします。

ユーザへのシェル コマンド許可セット（制限付きアクセス）の関連付け

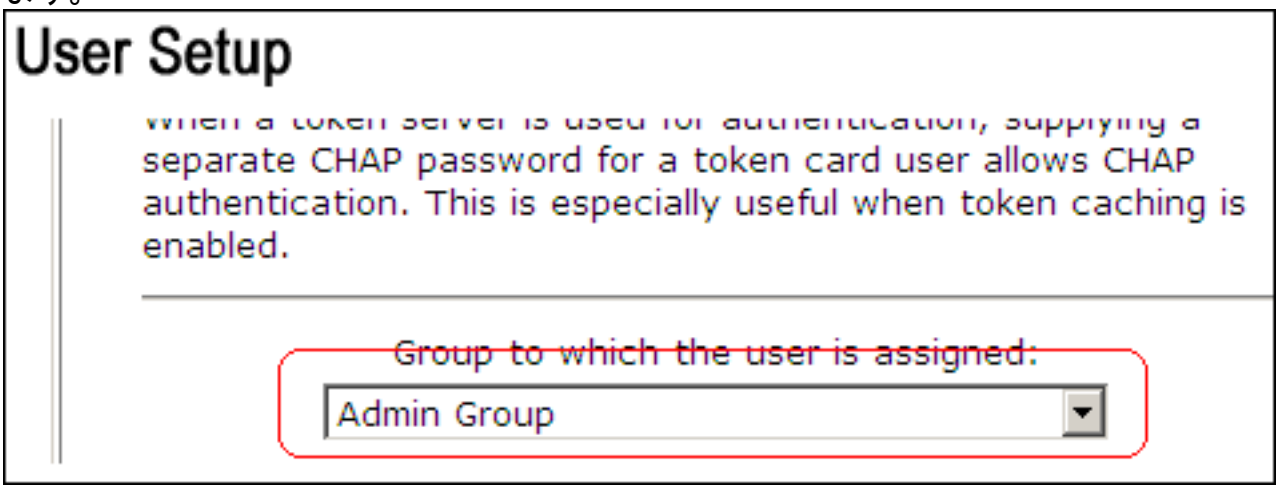
ユーザのシェル コマンド許可セットの設定方法に関する情報については、『Cisco Secure Access Control Server 4.1 ユーザ ガイド』の「ユーザのシェル コマンド許可セットの設定」セクションを参照してください。

注: ユーザ レベル設定は、ACS のグループ レベル設定より優先されます。つまり、ユーザのユーザ レベル設定にシェル コマンド許可セットがある場合は、それがグループ レベル設定より優先されます。

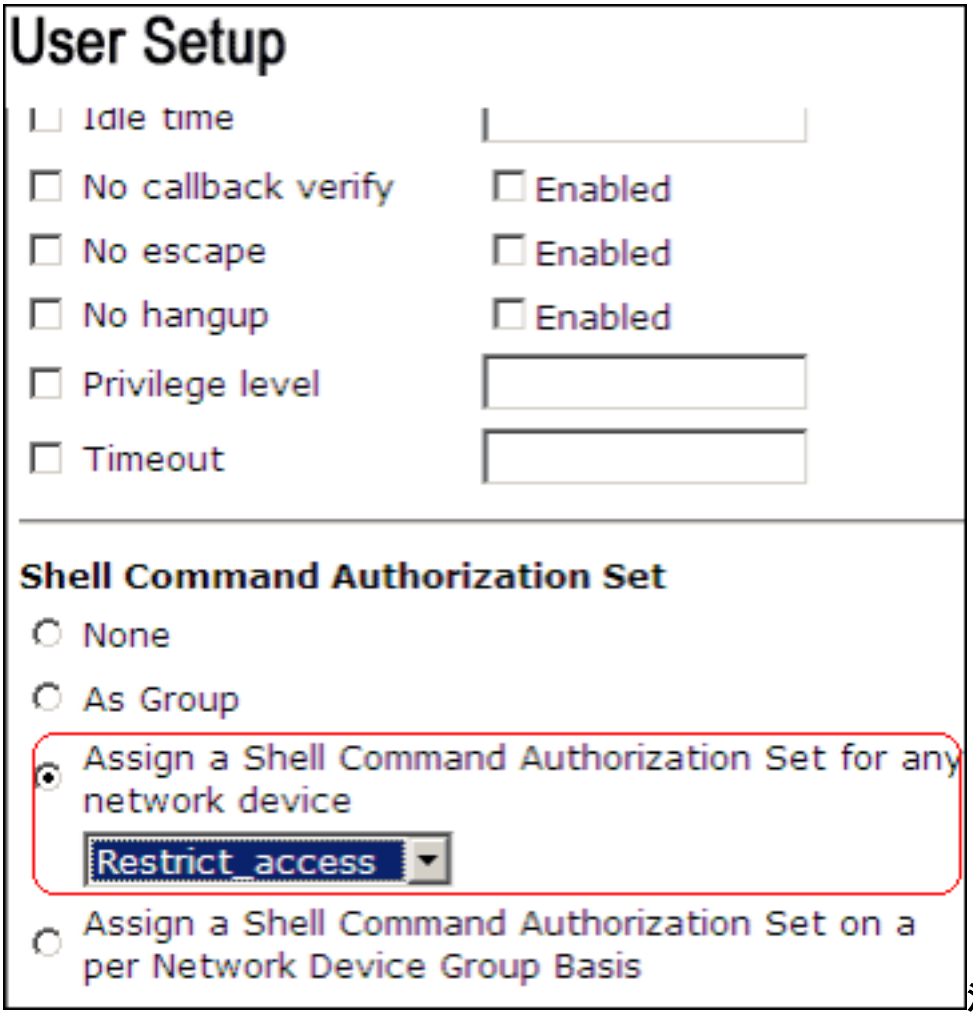
1. [User Setup] > [Add/Edit] をクリックして、「*Admin_user*」という名前の新しいユーザを作成し、管理グループに加えます。



2. ユーザが割り当てられているグループのドロップダウン リストで [Admin Group] を選択します。



3. [Shell Command Authorization Set] 領域で [Assign a Shell Command Authorization Set for any network device] オプション ボタンをクリックし、ドロップダウン リストで [Restrict_access] を選択します。**注:** このシナリオでは、このユーザは管理グループに属しています。 [Restrict_access] シェル許可セットは適用できますが、 [ReadWrite Access] シェル許可セットは適用できません。



注: [Interface Configuration] 領域の [TACACS+ (Cisco)] セクションで、[User] 列の [Shell (exec)] オプションが選択されていることを確認します。

IOS ルータの設定

プリセット設定に加えて、ACS サーバでコマンド許可を実装するために、次のコマンドが IOS ルータまたはスイッチで必要です。

```
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 設定

プリセット設定に加えて、ACS サーバでコマンド許可を実装するために、次のコマンドが ASA/PIX/FWSM で必要です。

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

注: 読み取り専用にするために、RADIUS プロトコルを使用して ASDM へのユーザ アクセスを制限することはできません。 RADIUS パケットには、認証と許可が同時に含まれるため、RADIUS サーバで認証されたすべてのユーザの特権レベルは 15 になります。 これは、コマンド許可セッ

トの実装によって TACACS を介して実現できます。

注: ASA/PIX/FWSM は、コマンド許可の実行に ACS を使用できない場合でも、入力された各コマンドの実行に長い時間がかかります。 ACS が使用不可で、ASA でコマンド許可が設定されている場合でも、ASA は各コマンドについてコマンド許可を要求します。

トラブルシューティング

エラー： command authorization failed

問題

TACACS のロギングを介してファイアウォールにログインした後、コマンドが機能しません。コマンドを入力すると、エラー [command authorization failed] が表示されます。

解決策

この問題を解決するには、次の手順を実行します。

1. 正しいユーザ名が使用されていることと、必要な権限がすべてユーザに割り当てられていることを確認します。
2. ユーザ名と特権が正しい場合は、ASA に ACS との接続性があり、ACS がアクティブであることを確認します。

注: このエラーは、管理者が誤って、ローカルおよび TACACS ユーザのコマンド許可を設定した場合に発生する可能性があります。 この場合は、パスワード回復を実行して問題を解決してください。

関連情報

- Cisco PIX Firewall ソフトウェア
- Cisco Secure PIX ファイアウォール コマンド リファレンス
- セキュリティ製品に関する Field Notice (PIX を含む)
- Requests for Comments (RFC)
- Cisco Secure Control Access Control Server に関するサポート ページ
- テクニカルサポートとドキュメント - Cisco Systems