管理アカウントの TACACS+ 認証をサポートするための Cisco VPN 3000 コンセントレータの設定方法

内容

概要

このドキュメントでは、管理アカウントの TACACS+ 認証をサポートするための Cisco VPN 3000 シリーズ コンセントレータの設定方法を手順を追って説明します。

TACACS+サーバがVPN 3000コンセントレータに設定されるとすぐに、ローカルに設定されたアカウント名とパスワード（admin、config、ispなど）は使用されなくなります。VPN 3000コンセントレータへのすべてのログインは、ユーザとパスワードの確認のために、設定された外部TACACS+サーバに送信されます。

TACACS+サーバ上の各ユーザの特権レベルの定義は、各TACACS+ユーザ名に対するVPN 3000コンセントレータの権限を決定します。次に、VPN 3000コンセントレータでローカルに設定されたユーザ名の下で定義されたAAAアクセスレベルと一致させます。TACACS+サーバが定義されるとすぐに、VPN 3000コンセントレータでローカルに設定されたユーザ名が無効になるため、これは重要なポイントです。ただし、TACACS+サーバから返される特権レベルと、そのローカルユーザの下のAAAアクセスレベルを照合するためだけに使用されます。その後、TACACS+ユーザ名には、ローカルに設定されたVPN 3000コンセントレータユーザがそのプロファイルで定義した権限が割り当てられます。

たとえば、設定セクションで詳しく説明されているように、TACACS+ユーザ/グループは

TACACS+特権レベル15を返すように設定されます。VPN 3000コンセントレータのAdministratorsセクションでは、adminユーザのAAA Access Levelも15に設定されています。TACACS+特権レベルとAAAアクセスレベルが一致するため、TACACS+ユーザにはVPN 3000コンセントレータでそれらの権限が与えられます。

例として、ユーザが設定を変更できる必要があるが、ファイルの読み取り/書き込み*は行わない場合*は、TACACS+サーバで特権レベル12を割り当てます。1 ~ 15の任意の番号を選択できます。次に、VPN 3000コンセントレータで、ローカルに設定された他の管理者の1つを選択します。次に、AAA Access Levelを12に設定し、このユーザの権限を設定して、設定を変更できるようにしますが、ファイルの読み取り/書き込みは行いません。権限/アクセスレベルが一致するため、ユーザはログイン時にこれらの権限を取得します。

VPN 3000コンセントレータでローカルに設定されたユーザ名は使用されなくなりました。ただし、ログイン時に特定のTACACS+ユーザが取得する権限を定義するために、これらの各ユーザの下のAccess RightsとAAA Access Levelsが使用されます。

前提条件

要件

この設定を行う前に、次の要件が満たされていることを確認します。

- VPN 3000コンセントレータからTACACS+サーバにIP接続できることを確認します。TACACS+サーバがパブリックインターフェイスに向いている場合は、パブリックフィルタ（TCPポート49）でTACACS+（TCPポート49）を開くことを忘れないでください。
- コンソール経由のバックアップアクセスが動作していることを確認します。この設定を初めて行う際に、誤ってすべてのユーザを設定から外してしまうのは簡単です。アクセスを回復する唯一の方法は、ローカルに設定されたユーザ名とパスワードを使用するコンソールを使用することです。

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いています。

- Cisco VPN 3000コンセントレータソフトウェアリリース4.7.2.B（または、3.0以降のOSソフトウェアの任意のリリースで動作）
- Cisco Secure Access Control Server for Windows Serversリリース4.0（または、2.4以降のソフトウェアリリースでも動作します）

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ました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

表記法

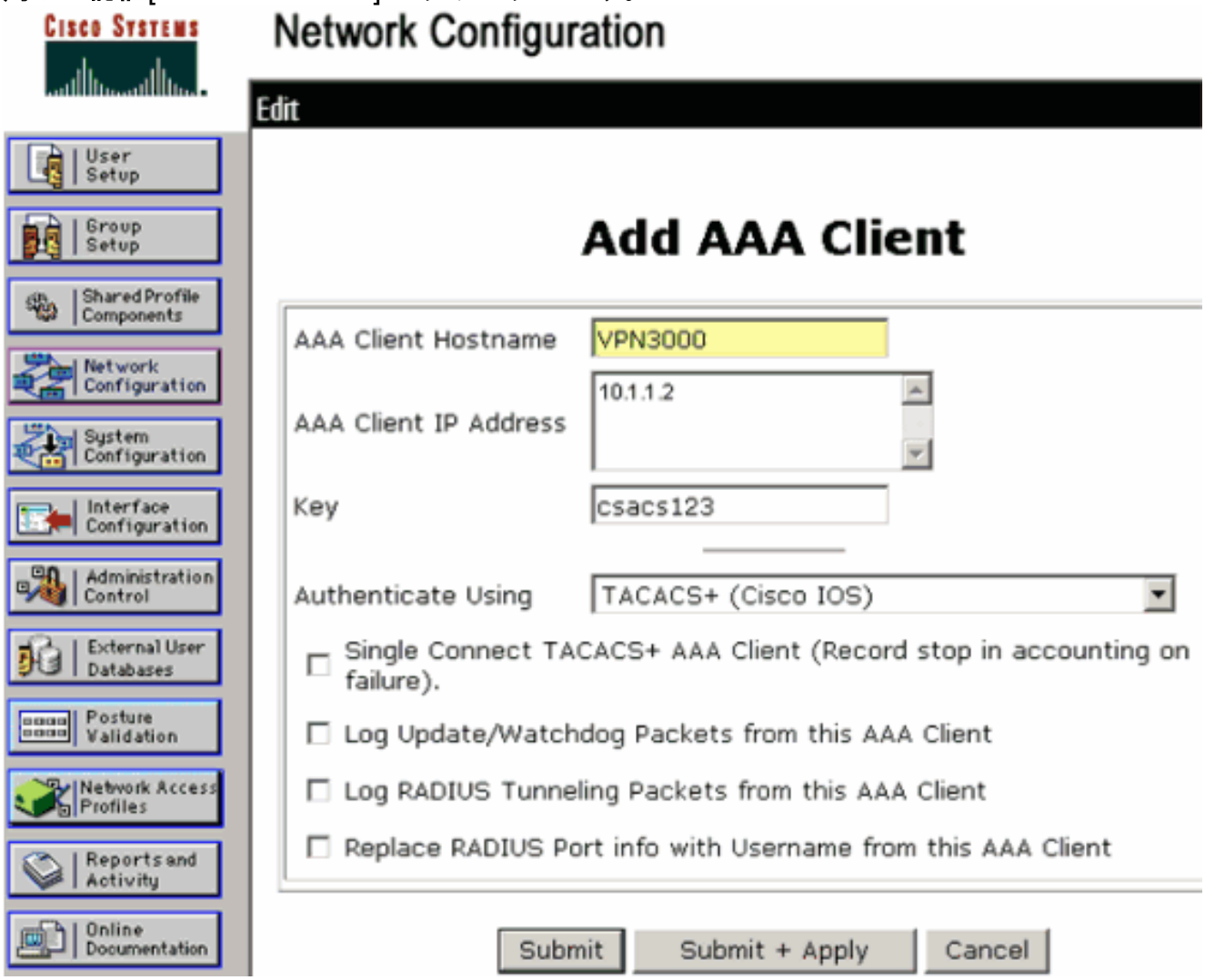
ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

TACACS+サーバの設定

TACACS+サーバでのVPN 3000コンセントレータのエントリの追加

VPN 3000コンセントレータのエントリをTACACS+サーバに追加するには、次の手順を実行します。

1. 左側のパネルの**[Network Configuration]**をクリックします。AAA Clients の下で **[Add Entry]** をクリックします。
2. 次のウィンドウで、フォームに入力して、VPNコンセントレータをTACACS+クライアントとして追加します。この例では次の設定を使用しています。AAAクライアントホスト名= **VPN3000**AAAクライアントIPアドレス= **10.1.1.2**キー= **csacs123**TACACS+(**Cisco IOS)を使用した認証**[Submit + Restart] をクリックします。



TACACS+サーバでのユーザアカウントの追加

TACACS+サーバにユーザアカウントを追加するには、次の手順を実行します。

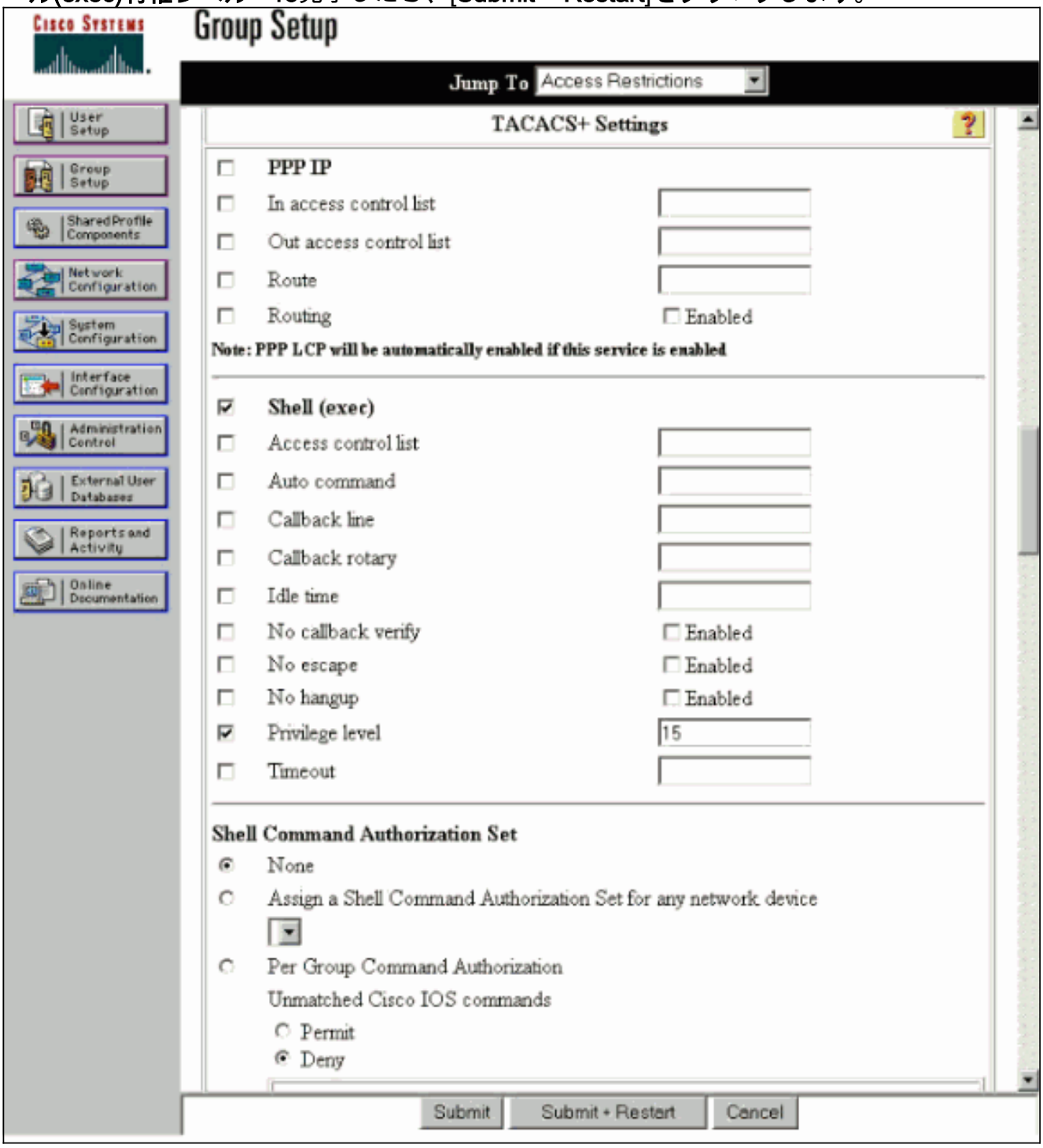
1. 後でTACACS+認証に使用できるユーザアカウントをTACACS+サーバに作成します。これを行**うには、**左側のパネルで[User Setup]をクリックし、ユーザ「johnsmith」を追加し、**[Add/Edit]**をクリックします。
2. このユーザのパスワードを追加し、他のVPN 3000コンセントレータの管理者を含むACSグループにユーザを割り当てます。**注：この例**では、この特定のユーザACSグループプロファイルの下に特権レベルを定義しています。ユーザ単位で行う場合は、**Interface Configuration > TACACS+ (Cisco IOS)の順に選択し、Shell(exec)サービスのUser**ボックスにチェックマー

クを付けます。このドキュメントで説明されているTACACS+オプションは、各ユーザプロファイルで使用できます。

TACACS+サーバのグループの編集

TACACS+サーバでグループを編集するには、次の手順を実行します。

1. 左側のパネルで**[グループ**設定]をクリックします。
2. ドロップダウンメニューから、[Add a User Account in the TACACS+ Server]セクション（この例ではグループ1）でユーザが追加されたグループを選択し、**[Edit Settings]をクリックします。**
3. 次のウィンドウで、[TACACS+ Settings]で次の属性が選択されていることを確認します。**シェル(exec)特権レベル= 15**完了したら、**[Submit + Restart]をクリックします。**

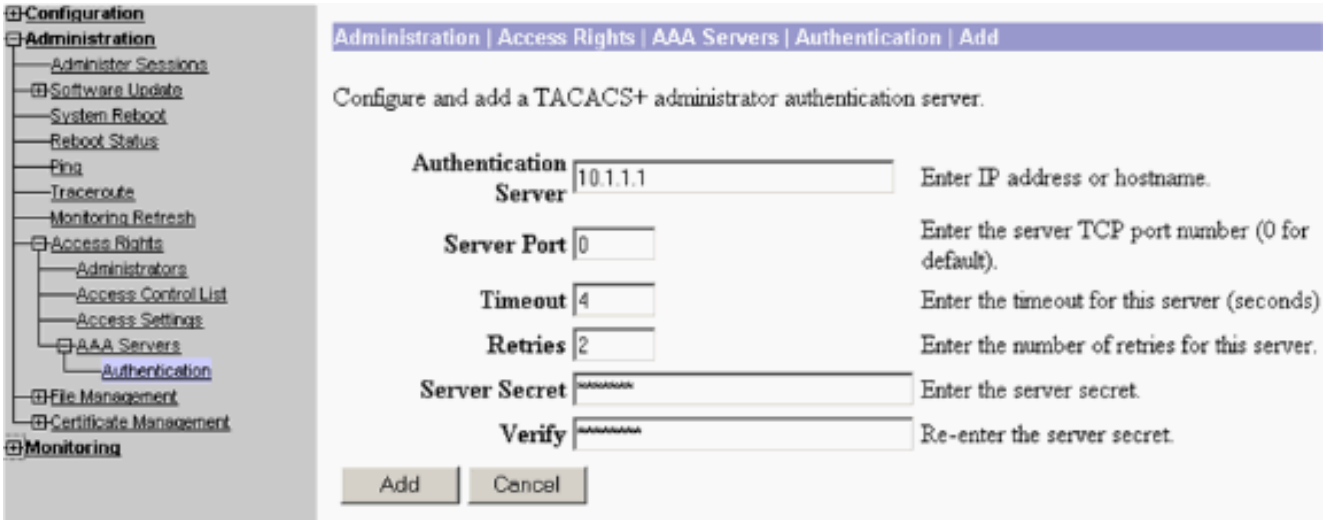


VPN 3000 コンセントレータの設定

VPN 3000コンセントレータでのTACACS+サーバのエントリの追加

VPN 3000コンセントレータにTACACS+サーバのエントリを追加するには、次の手順を実行します。

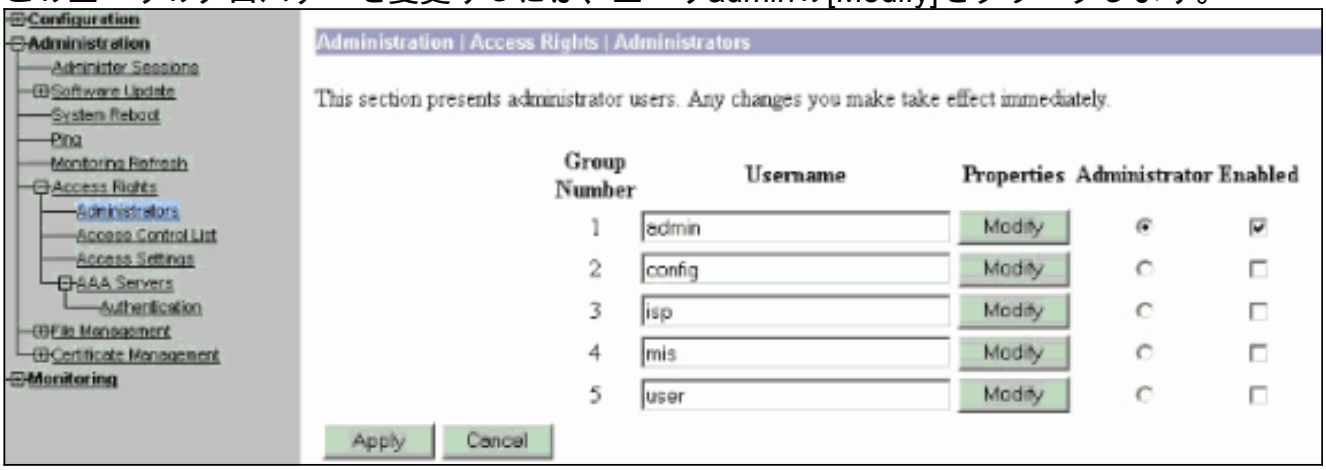
1. 左側のパネルのナビゲーションツリーで[Administration] > [Access Rights] > [AAA Servers] > [Authentication]の順に選択し、右側のパネルで[Add]をクリックします。このサーバを追加するために[Add] をクリックするとすぐに、VPN 3000コンセントレータでローカルに設定されたユーザ名/パスワードは使用されなくなります。ロックアウトが発生した場合は、コンソール経由のバックアップアクセスが機能することを確認します。
2. 次のウィンドウで、次に示すフォームに入力します。認証サーバ= 10.1.1.1 (TACACS+サーバのIPアドレス) サーバポート= 0(デフォルト)Timeout = 4再試行= 2サーバシークレット= csacs123確認= csacs123



TACACS+認証用のVPNコンセントレータのAdminアカウントの変更

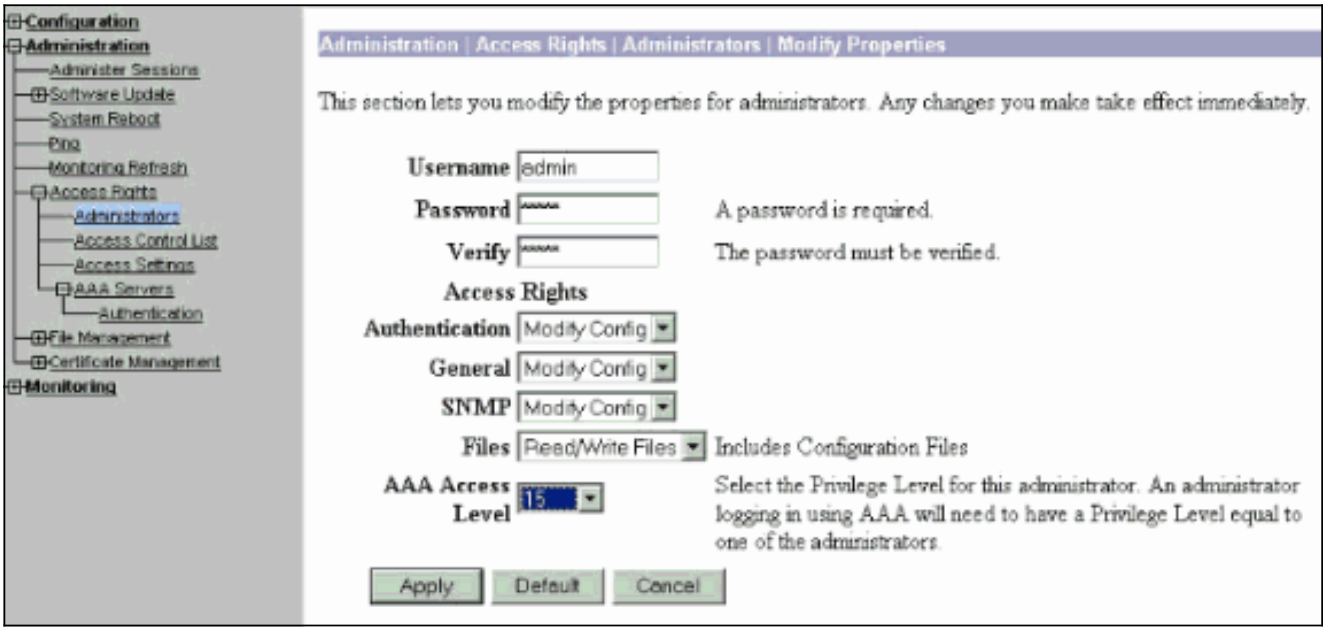
TACACS+認証用にVPNコンセントレータの管理者アカウントを変更するには、次の手順を実行します。

1. このユーザのプロパティを変更するには、ユーザadminの[Modify]をクリックします。



2. [AAA Access Level]に[15]を選択します。この値は1 ~ 15の任意の数値で指定できます。

TACACS+サーバのユーザ/グループプロファイルで定義されているTACACS+特権レベルと一致する必要があります。TACACS+ユーザは、このVPN 3000コンセントレータユーザで定義されている権限を取得して、設定の変更、ファイルの読み取り/書き込みなどを行います。



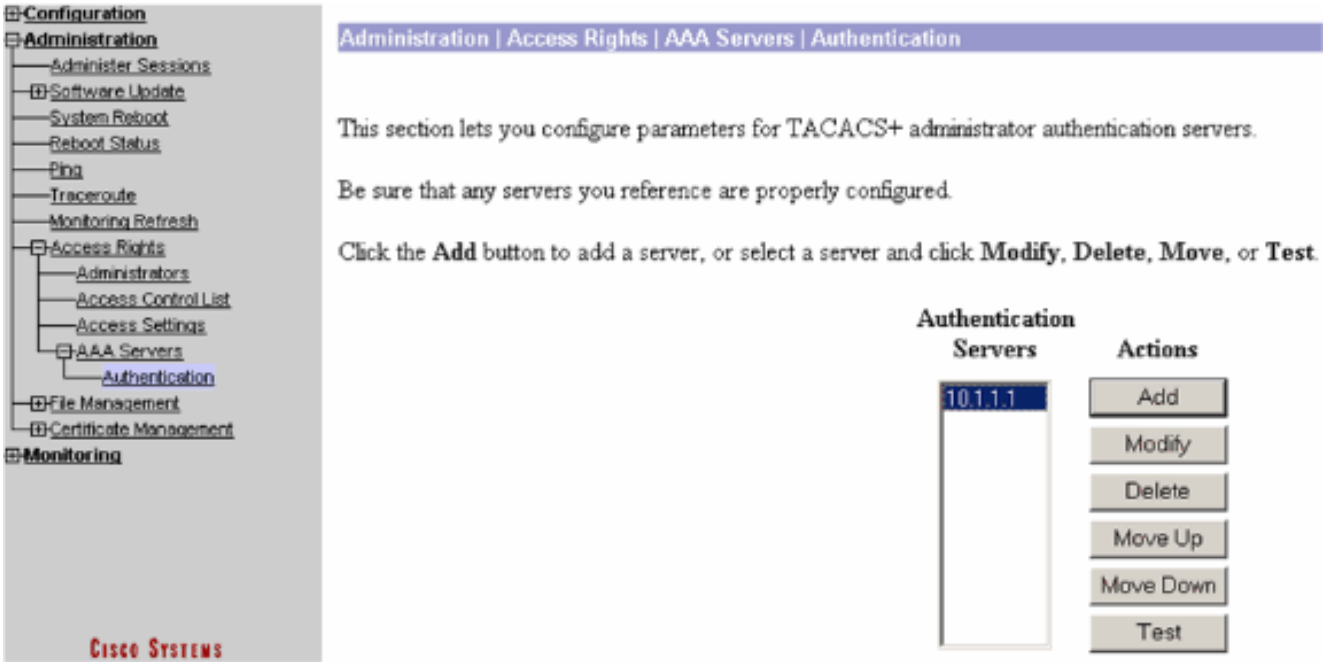
確認

現在、この設定に使用できる確認手順はありません。

トラブルシュート

設定をトラブルシューティングするには、次の手順を実行します。

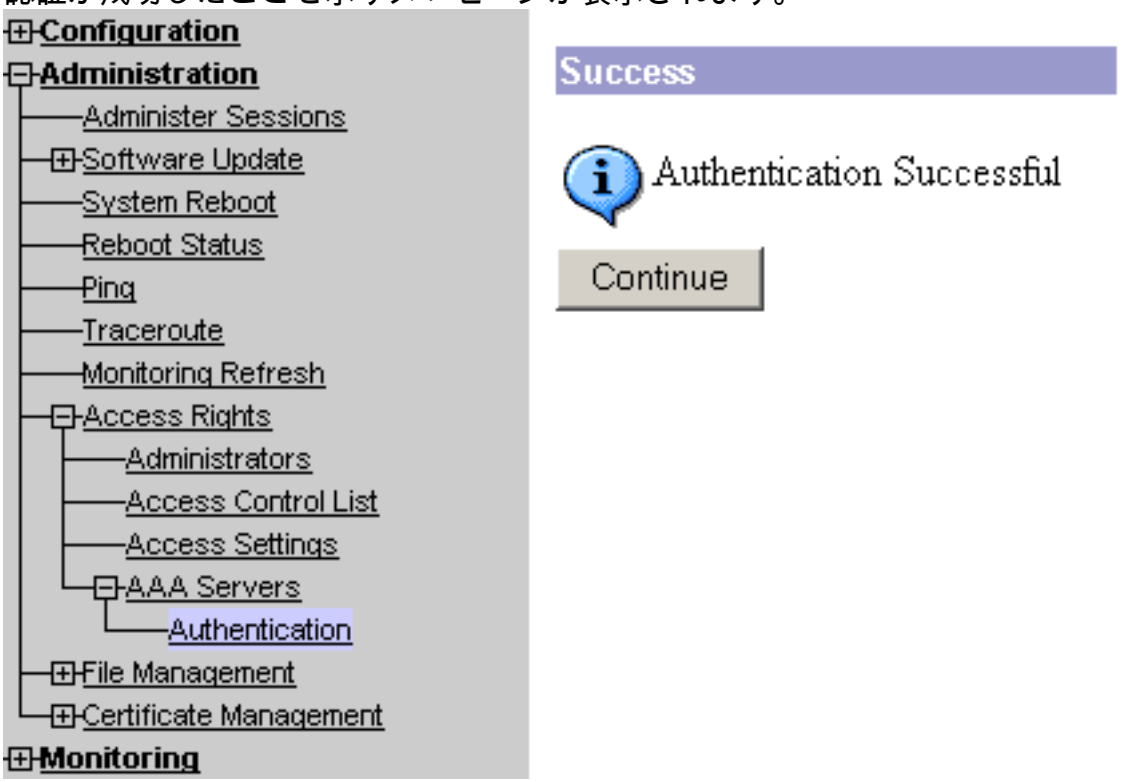
1. 認証をテストするには：TACACS+サーバの場合**[Administration] > [Access Rights] > [AAA Servers] > [Authentication]を選択します。**[サーバ]を選択してから **[Test]** をクリックします。



注：TACACS+サーバが[Administration]タブで設定されている場合、VPN 3000ローカルデー

タベースでユーザを認証するように設定する方法はありません。フォールバックできるのは、別の外部データベースまたはTACACSサーバを使用する場合だけです。TACACS+ユーザ名とパスワードを入力し、[OK]をクリックします。

認証が成功したことを示すメッセージが表示されます。



2. 認証が失敗した場合は、設定に問題があるか、IP 接続に問題があります。ACS サーバの Failed Attempts Log で、この失敗に関連するメッセージがないか確認します。このログにメッセージが表示されない場合は、IP 接続に問題があると考えられます。TACACS+要求がTACACS+サーバに到達しない。適切なVPN 3000コンセントレータインターフェイスに適用されているフィルタで、TACACS+（TCPポート49）パケットの入出力が可能であることを確認します。ログに「service denied」と表示された場合、TACACS+サーバのユーザプロファイルまたはグループプロファイルでシェル(exec)サービスが正しく有効になっていません。
3. テスト認証が成功しても VPN 3000 コンセントレータへのログインが引き続き失敗する場合は、コンソール ポート経由で Filterable Event Log を確認してください。次のようなメッセージが表示される場合：

```
65 02/09/2005 13:14:40.150 SEV=5 AUTH/32 RPT=2
User [ johnsmith ] Protocol [ HTTP ] attempted ADMIN logon.
Status: <REFUSED> authorization failure. NO Admin Rights
```

このメッセージは、TACACS+サーバに割り当てられた特権レベルが、VPN 3000コンセントレータユーザの下で一致するAAAアクセスレベルを持っていないことを示します。たとえば、ユーザjohnsmithのTACACS+特権レベルは7ですが、5人のVPN 3000コンセントレータ管

理者のAAAアクセスレベルは7ではありません。

関連情報

- Cisco VPN 3000 シリーズ コンセントレータに関するサポート ページ
- Cisco VPN 3000 シリーズ クライアントに関するサポート ページ
- IPSec ネゴシエーション/IKE プロトコルに関するサポート ページ
- TACACS/TACACS+ サポート ページ
- IOS での TACACS+ に関するドキュメント
- テクニカル サポートとドキュメント – Cisco Systems