

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](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[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](#)

[TACACS+サーバでのユーザアカウントの追加](#)

[TACACS+サーバのグループの編集](#)

[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](#)

[TACACS+認証用のVPNコンセントレータのAdminアカウントの変更](#)

[確認](#)

[トラブルシューティング](#)

[関連情報](#)

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で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](#)

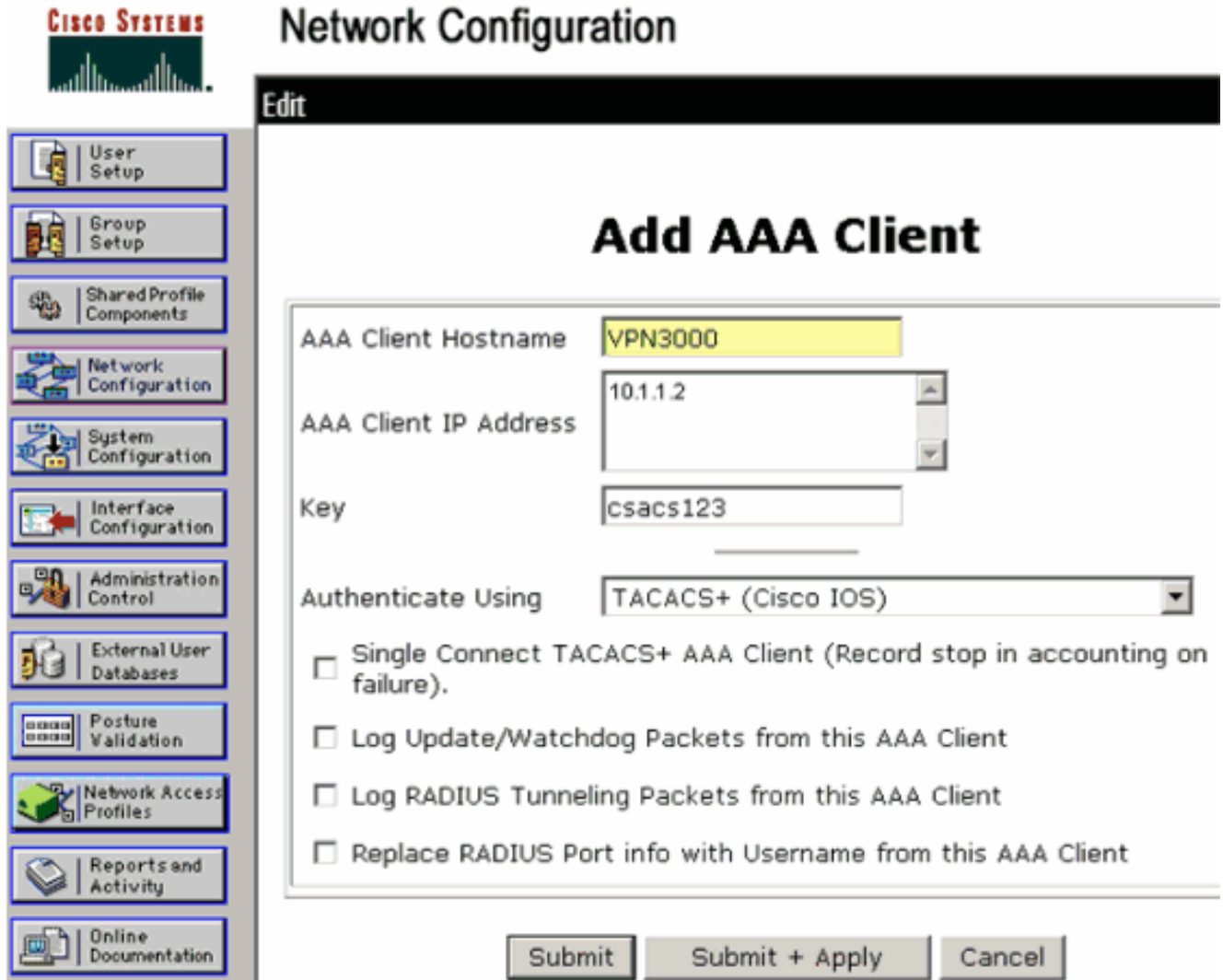
ドキュメント表記の詳細は、『[シスコテクニカルティップスの表記法](#)』を参照してください。

[TACACS+サーバの設定](#)

[TACACS+サーバでのVPN 3000コンソントレータのエントリの追加](#)

VPN 3000コンソ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コンソントレータを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= VPN3000AAAクライアントIPアドレス= 10.1.1.2キー= csacs123TACACS+(Cisco IOS)を使用した認証[Submit + Restart] をクリックします。



The screenshot shows the Cisco Systems Network Configuration interface. The left sidebar contains various configuration options, with 'Network Configuration' selected. The main window is titled 'Add AAA Client' and contains the following fields and options:

- AAA Client Hostname: VPN3000
- AAA Client IP Address: 10.1.1.2
- Key: csacs123
- Authenticate Using: TACACS+ (Cisco IOS)
- Single Connect TACACS+ AAA Client (Record stop in accounting on failure):
- Log Update/Watchdog Packets from this AAA Client:
- Log RADIUS Tunneling Packets from this AAA Client:
- Replace RADIUS Port info with Username from this AAA Client:

At the bottom of the form are three buttons: 'Submit', 'Submit + Apply', and 'Cancel'.

[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コンソ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。

The screenshot shows the Cisco Systems Group Setup interface. The left sidebar contains navigation options: User Setup, Group Setup, Shared Profile Components, Network Configuration, System Configuration, Interface Configuration, Administration Control, External User Databases, Reports and Activity, and Online Documentation. The main content area is titled "Group Setup" and "TACACS+ Settings". A "Jump To" dropdown menu is set to "Access Restrictions". The settings are organized into sections:

- PPP IP** (disabled):
 - In access control list
 - Out access control list
 - Route
 - Routing Enabled

Note: PPP LCP will be automatically enabled if this service is enabled
- Shell (exec)** (checked):
 - Access control list
 - Auto command
 - Callback line
 - Callback rotary
 - Idle time
 - No callback verify Enabled
 - No escape Enabled
 - No hangup Enabled
 - Privilege level: 15
 - Timeout
- Shell Command Authorization Set**:
 - None
 - Assign a Shell Command Authorization Set for any network device (dropdown menu)
 - Per Group Command Authorization
 - Unmatched Cisco IOS commands
 - Permit
 - Deny

At the bottom, there are three buttons: "Submit", "Submit + Restart", and "Cancel".

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

The screenshot shows the configuration window for adding a TACACS+ administrator authentication server. The left sidebar shows the navigation tree with 'AAA Servers' > 'Authentication' selected. The main window has the following fields:

Field	Value	Description
Authentication Server	10.1.1.1	Enter IP address or hostname.
Server Port	0	Enter the server TCP port number (0 for default).
Timeout	4	Enter the timeout for this server (seconds)
Retries	2	Enter the number of retries for this server.
Server Secret	csacs123	Enter the server secret.
Verify	csacs123	Re-enter the server secret.

Buttons: Add, Cancel

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。

The screenshot shows the 'Administrators' configuration window. The left sidebar shows the navigation tree with 'Access Rights' > 'Administrators' selected. The main window displays a table of administrator users:

Group Number	Username	Properties	Administrator	Enabled
1	admin	Modify	<input checked="" type="radio"/>	<input checked="" type="checkbox"/>
2	config	Modify	<input type="radio"/>	<input type="checkbox"/>
3	isp	Modify	<input type="radio"/>	<input type="checkbox"/>
4	mis	Modify	<input type="radio"/>	<input type="checkbox"/>
5	user	Modify	<input type="radio"/>	<input type="checkbox"/>

Buttons: Apply, Cancel

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。



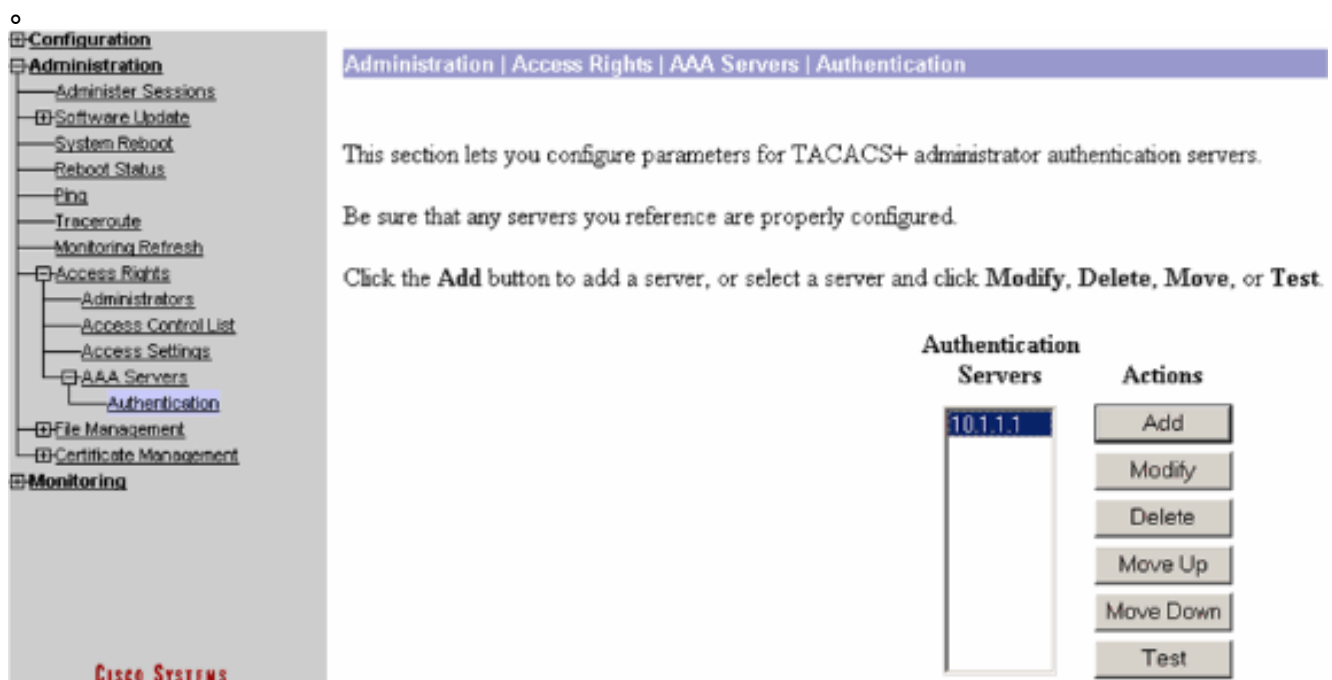
確認

現在、この設定に使用できる確認手順はありません。

トラブルシューティング

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

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。

Administration | Access Rights | AAA Servers | Authentication | Test

Enter a username and password with which to test. Please wait for the operation to complete or timeout.

Username

Password

認証が成功したことを示すメッセージが表示されます。

The image shows a configuration tree on the left and a success message dialog on the right. The tree is expanded to 'Authentication' under 'AAA Servers'. The dialog has a purple header 'Success', an information icon, the text 'Authentication Successful', and a 'Continue' button.

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](#)