

# Konfigurieren des Cisco VPN 3000 Concentrator zur Unterstützung der TACACS+-Authentifizierung für Managementkonten

## Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konventionen](#)

[Konfigurieren des TACACS+-Servers](#)

[Hinzufügen eines Eintrags für den VPN 300-Konzentrator im TACACS+-Server](#)

[Hinzufügen eines Benutzerkontos im TACACS+-Server](#)

[Bearbeiten der Gruppe auf dem TACACS+-Server](#)

[Konfigurieren des VPN 3000-Konzentrators](#)

[Hinzufügen eines Eintrags für den TACACS+-Server im VPN 300-Konzentrator](#)

[Ändern Sie das Administratorkonto im VPN-Konzentrator für die TACACS+-Authentifizierung.](#)

[Überprüfen](#)

[Fehlerbehebung](#)

[Zugehörige Informationen](#)

## **[Einführung](#)**

Dieses Dokument enthält schrittweise Anweisungen zur Konfiguration der Cisco VPN Concentrators der Serie 3000 zur Unterstützung der TACACS+-Authentifizierung für Managementkonten.

Sobald ein TACACS+-Server im VPN 3000-Konzentrator konfiguriert ist, werden die lokal konfigurierten Kontennamen und Kennwörter wie admin, config, isp usw. nicht mehr verwendet. Alle Anmeldungen beim VPN 300 Concentrator werden zur Benutzer- und Kennwortverifizierung an den konfigurierten externen TACACS+-Server gesendet.

Die Definition einer Berechtigungsstufe für jeden Benutzer auf dem TACACS+-Server legt die Berechtigungen für den VPN 3000-Konzentrator für jeden TACACS+-Benutzernamen fest. Ordnen Sie dies dann der AAA-Zugriffsstufe zu, die unter dem lokal konfigurierten Benutzernamen im VPN 3000-Concentrator definiert ist. Dies ist ein wichtiger Punkt, denn sobald ein TACACS+-Server definiert ist, sind die lokal konfigurierten Benutzernamen im VPN 3000 Concentrator nicht mehr gültig. Sie werden jedoch weiterhin nur verwendet, um die vom TACACS+-Server zurückgegebene Berechtigungsebene mit der AAA-Zugriffsebene unter diesem lokalen Benutzer abzustimmen. Dem TACACS+-Benutzernamen werden dann die Berechtigungen zugewiesen, die der lokal konfigurierte VPN 3000 Concentrator-Benutzer unter seinem Profil definiert hat.

Beispielsweise wird ein TACACS+-Benutzer bzw. eine TACACS+-Gruppe, der bzw. die eine TACACS+-Berechtigungsstufe von 15 zurückgibt, ausführlich in den Konfigurationsabschnitten beschrieben. Im Abschnitt "Administratoren" des VPN 300-Konzentrators ist für den Administrator-Benutzer der AAA-Zugriffsgrad ebenfalls auf 15 festgelegt. Dieser Benutzer kann die Konfiguration in allen Abschnitten ändern und Dateien lesen und schreiben. Da TACACS+-Berechtigungen und die AAA-Zugriffsstufe übereinstimmen, erhält der TACACS+-Benutzer diese Berechtigungen für den VPN 3000-Konzentrator.

Wenn Sie beispielsweise beschließen, dass ein Benutzer die Konfiguration ändern kann, aber *keine* Lese-/Schreibdateien benötigt, weisen Sie ihnen auf dem TACACS+-Server die Berechtigungsstufe 12 zu. Sie können eine beliebige Zahl zwischen 1 und 15 wählen. Wählen Sie anschließend im VPN 3000 Concentrator einen der anderen lokal konfigurierten Administratoren aus. Legen Sie als Nächstes die AAA-Zugriffsstufe auf 12 fest, und legen Sie die Berechtigungen für diesen Benutzer fest, damit die Konfiguration geändert werden kann, jedoch nicht Lese-/Schreibdateien. Aufgrund der entsprechenden Berechtigungen/Zugriffsebene erhält der Benutzer diese Berechtigungen bei der Anmeldung.

Die lokal konfigurierten Benutzernamen des VPN 3000-Konzentrators werden nicht mehr verwendet. Die Zugriffsrechte und die AAA-Zugriffsebenen unter jedem dieser Benutzer werden jedoch verwendet, um die Berechtigungen festzulegen, die ein bestimmter TACACS+-Benutzer bei der Anmeldung erhält.

## Voraussetzungen

### Anforderungen

Stellen Sie sicher, dass Sie diese Anforderungen erfüllen, bevor Sie versuchen, diese Konfiguration durchzuführen:

- Stellen Sie sicher, dass Sie über den VPN 300 Concentrator eine IP-Verbindung zum TACACS+-Server haben. Wenn sich Ihr TACACS+-Server in Richtung der öffentlichen Schnittstelle befindet, vergessen Sie nicht, TACACS+ (TCP-Port 49) auf dem öffentlichen Filter zu öffnen.
- Stellen Sie sicher, dass der Backup-Zugriff über die Konsole betriebsbereit ist. Es ist einfach, alle Benutzer bei der ersten Einrichtung aus der Konfiguration zu entfernen. Die einzige Möglichkeit, den Zugriff wiederherzustellen, ist die Konsole, die weiterhin die lokal konfigurierten Benutzernamen und Kennwörter verwendet.

### Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco VPN 3000 Concentrator Software, Version 4.7.2.B (Alternativ dazu funktioniert jede Version der Betriebssystemsoftware 3.0 oder höher.)
- Cisco Secure Access Control Server für Windows-Server Version 4.0 (Alternativ funktioniert jede Version von 2.4 oder neuer Software.)

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie

die potenziellen Auswirkungen eines Befehls verstehen.

## Konventionen

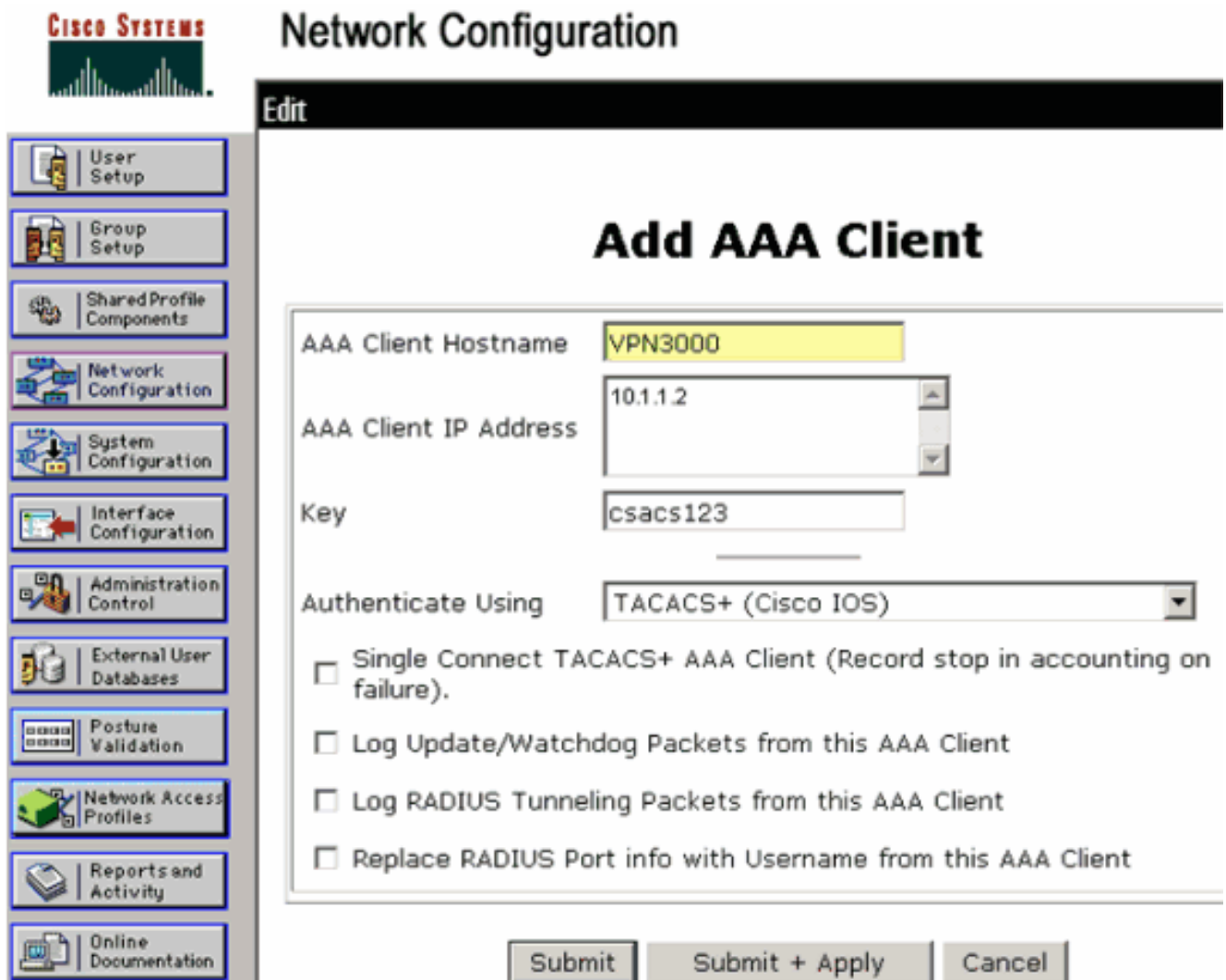
Weitere Informationen zu Dokumentkonventionen finden Sie unter [Cisco Technical Tips Conventions](#) (Technische Tipps zu Konventionen von Cisco).

## Konfigurieren des TACACS+-Servers

### Hinzufügen eines Eintrags für den VPN 300-Konzentrator im TACACS+-Server

Gehen Sie wie folgt vor, um im TACACS+-Server einen Eintrag für den VPN 3000-Konzentrator hinzuzufügen.

1. Klicken Sie im linken Bereich auf **Netzwerkconfiguration**. Klicken Sie unter AAA-Clients auf **Eintrag hinzufügen**.
2. Füllen Sie im nächsten Fenster das Formular aus, um den VPN Concentrator als TACACS+-Client hinzuzufügen. In diesem Beispiel wird Folgendes verwendet: AAA-Client-Hostname = VPN3000 IP-Adresse des AAA-Clients = 10.1.1.2 Key = csacs123 Authentifizierung mit = TACACS+ (Cisco IOS) Klicken Sie auf **Senden + Neu starten**.



The screenshot shows the Cisco Systems Network Configuration interface. The left sidebar contains a navigation menu with the following items: User Setup, Group Setup, Shared Profile Components, Network Configuration (highlighted), System Configuration, Interface Configuration, Administration Control, External User Databases, Posture Validation, Network Access Profiles, Reports and Activity, and Online Documentation. The main content area is titled 'Network Configuration' and 'Edit'. The 'Add AAA Client' form is displayed with 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, there are three buttons: Submit, Submit + Apply, and Cancel.

## [Hinzufügen eines Benutzerkontos im TACACS+-Server](#)

Führen Sie diese Schritte aus, um dem TACACS+-Server ein Benutzerkonto hinzuzufügen.

1. Erstellen Sie im TACACS+-Server ein Benutzerkonto, das später für die TACACS+-Authentifizierung verwendet werden kann. Klicken Sie im linken Bereich auf **User Setup (Benutzereinrichtung)**, fügen Sie den Benutzer "johnsmith" hinzu, und klicken Sie dazu auf **Hinzufügen/Bearbeiten**.
2. Fügen Sie ein Kennwort für diesen Benutzer hinzu, und weisen Sie den Benutzer einer ACS-Gruppe zu, die die anderen VPN 3000 Concentrator-Administratoren enthält. **Hinweis:** In diesem Beispiel wird die Berechtigungsebene unter diesem bestimmten Benutzer-ACS-Gruppenprofil definiert. Wenn dies auf Benutzerbasis erfolgen soll, wählen Sie **Interface Configuration > TACACS+ (Cisco IOS)** und aktivieren das **User**-Kontrollkästchen für den Shell (exec)-Dienst. Nur dann sind die in diesem Dokument beschriebenen TACACS+-Optionen unter jedem Benutzerprofil verfügbar.

## [Bearbeiten der Gruppe auf dem TACACS+-Server](#)

Gehen Sie wie folgt vor, um die Gruppe auf dem TACACS+-Server zu bearbeiten.

1. Klicken Sie im linken Bereich auf **Gruppeneinrichtung**.
2. Wählen Sie aus dem Dropdown-Menü die Gruppe aus, der der Benutzer im Abschnitt [TACACS+ Server \(TACACS+-Server\) ein Benutzerkonto hinzufügen](#) hinzugefügt wurde (in diesem Beispiel Gruppe 1), und klicken Sie auf **Edit Settings (Einstellungen bearbeiten)**.
3. Vergewissern Sie sich im nächsten Fenster, dass diese Attribute unter TACACS+ Settings (TACACS+-Einstellungen) ausgewählt sind: **Shell (exec) Berechtigungsstufe = 15** Klicken Sie abschließend auf **Senden + Neu starten**.

**CISCO SYSTEMS** Group Setup

Jump To **Access Restrictions**

**TACACS+ Settings**

**PPP IP**

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)**

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

Per Group Command Authorization

Unmatched Cisco IOS commands

Permit

Deny

Submit Submit + Restart Cancel

## [Konfigurieren des VPN 3000-Konzentrators](#)

### [Hinzufügen eines Eintrags für den TACACS+-Server im VPN 300-Konzentrator](#)

Gehen Sie wie folgt vor, um im VPN 300 Concentrator einen Eintrag für den TACACS+-Server hinzuzufügen.

1. Wählen Sie im Navigationsbaum im linken Bereich **Administration > Access Rights > AAA Servers > Authentication (Verwaltung > Zugriffsrechte > AAA-Server > Authentifizierung)** aus, und klicken Sie dann im rechten Bereich auf **Add (Hinzufügen)**. Sobald Sie auf **Hinzufügen** klicken, um diesen Server hinzuzufügen, werden die lokal konfigurierten Benutzernamen/Kennwörter im VPN 3000-Concentrator nicht mehr verwendet. Stellen Sie

sicher, dass der Backup-Zugriff über die Konsole bei einem Sperren funktioniert.

2. Füllen Sie das Formular im nächsten Fenster wie folgt aus: Authentifizierungsserver = 10.1.1.1 (IP-Adresse des TACACS+-Servers) Server-Port = 0 (Standard) Timeout = 4 Wiederholungen = 2 Server Secret = csacs123 Verify = csacs123

Administration | Access Rights | AAA Servers | Authentication | Add

Configure and add a TACACS+ administrator authentication server.

|                       |          |   |
|-----------------------|----------|---|
| 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.                       |

Add Cancel

## Ändern Sie das Administratorkonto im VPN-Konzentrator für die TACACS+-Authentifizierung.

Gehen Sie wie folgt vor, um das Administratorkonto im VPN Concentrator für die TACACS+-Authentifizierung zu ändern.

1. Klicken Sie auf **Ändern** für den Benutzeradministrator, um die Eigenschaften dieses Benutzers zu ändern.

Administration | Access Rights | Administrators

This section presents administrator users. Any changes you make take effect immediately.

| 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"/>            |

Apply Cancel

2. Wählen Sie als AAA-Zugriffsstufe **15 aus**. Dieser Wert kann eine beliebige Zahl zwischen 1 und 15 sein. Beachten Sie, dass sie der im Benutzer-/Gruppenprofil auf dem TACACS+-Server definierten TACACS+-Berechtigungsebene entsprechen muss. Der TACACS+-Benutzer übernimmt dann die Berechtigungen, die unter diesem VPN 3000 Concentrator-Benutzer definiert wurden, für die Änderung der Konfiguration, das Lesen/Schreiben von Dateien usw.





## Überprüfen

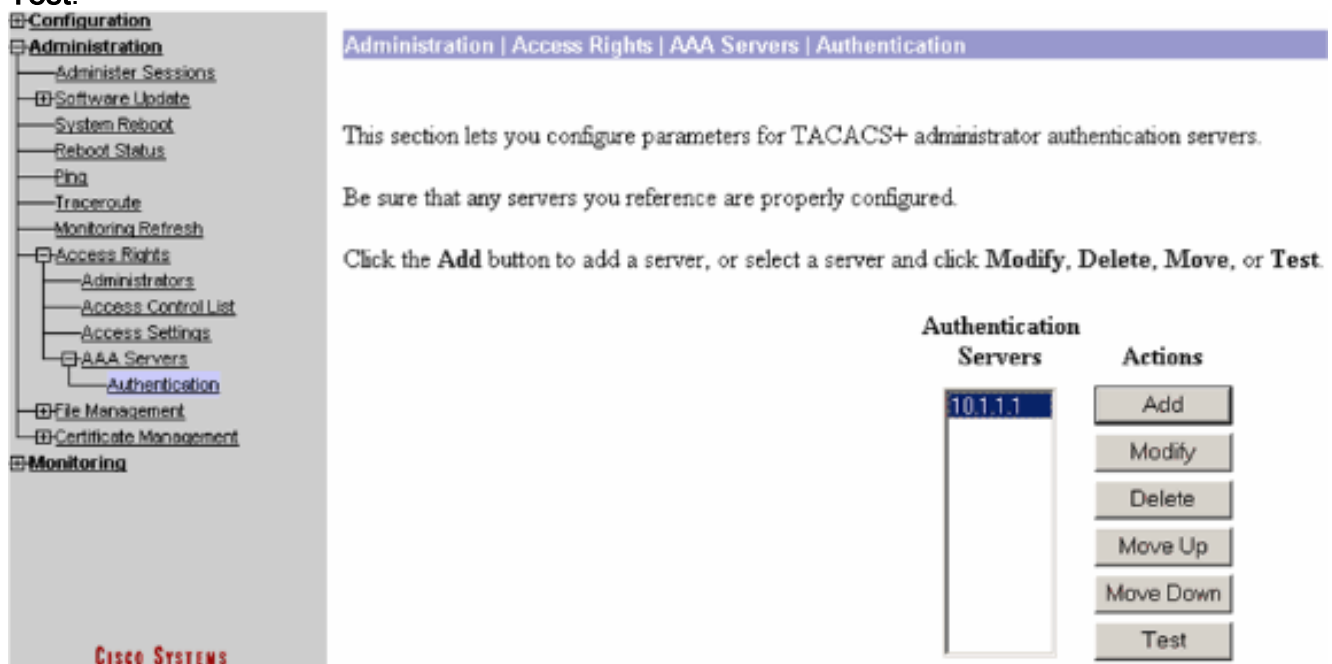
Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

## Fehlerbehebung

Führen Sie die Schritte in diesen Anweisungen aus, um eine Fehlerbehebung für Ihre Konfiguration durchzuführen.

1. So testen Sie die Authentifizierung: Für TACACS+-Server Wählen Sie **Administration > Access Rights > AAA Servers > Authentication** aus. Wählen Sie den Server aus, und klicken Sie dann auf

### Test.



**Hinweis:** Wenn der TACACS+-Server auf der Registerkarte "Administration" (Verwaltung) konfiguriert ist, kann der Benutzer keine Authentifizierung für die lokale VPN 3000-Datenbank einrichten. Sie können Fallback nur mit einer anderen externen Datenbank oder

einem TACACS-Server verwenden. Geben Sie den Benutzernamen und das Kennwort für TACACS+ ein, und klicken Sie auf OK.

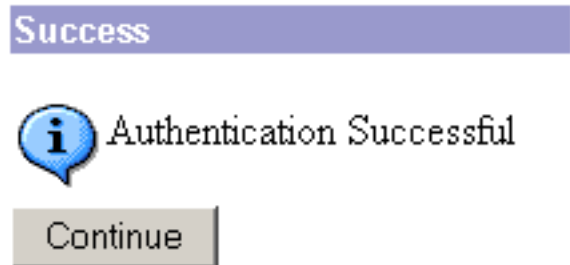
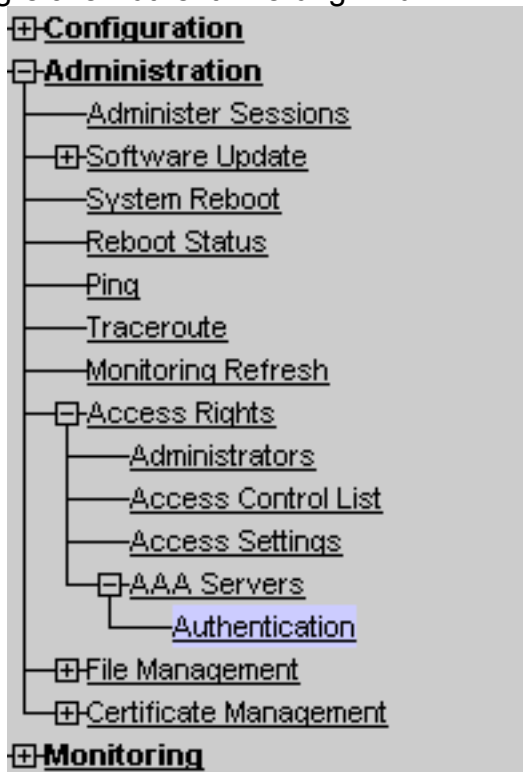
Administration | Access Rights | AAA Servers | Authentication | Test

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

Username

Password

Eine erfolgreiche Authentifizierung wird



angezeigt. **Monitoring**

2. Wenn es fehlschlägt, liegt entweder ein Konfigurationsproblem oder ein IP-Verbindungsproblem vor. Überprüfen Sie, ob im ACS-Server bei fehlgeschlagenen Versuchen Meldungen zu dem Fehler eingehen. Wenn in diesem Protokoll keine Meldungen angezeigt werden, liegt wahrscheinlich ein Problem mit der IP-Verbindung vor. Die TACACS+-Anforderung erreicht den TACACS+-Server nicht. Überprüfen Sie, ob die auf die entsprechende VPN 300 Concentrator-Schnittstelle angewendeten Filter TACACS+-Pakete (TCP-Port 49) ein- und auslassen. Wenn der Fehler im Protokoll als "Dienst verweigert" angezeigt wird, wurde der Shell (exec)-Dienst im Benutzer- oder Gruppenprofil des TACACS+-Servers nicht korrekt aktiviert.
3. Wenn die Testauthentifizierung erfolgreich ist, die Anmeldung beim VPN 3000-Konzentrator jedoch weiterhin fehlschlägt, überprüfen Sie das Filterbare Ereignisprotokoll über den Konsolenport. Wenn eine ähnliche Meldung angezeigt wird:

```
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
```

Diese Meldung weist darauf hin, dass die auf dem TACACS+-Server zugewiesene Berechtigungsebene unter keinem der VPN 3000 Concentrator-Benutzer die



übereinstimmende AAA-Zugriffsebene aufweist. Beispielsweise verfügt User Johnsmith auf dem TACACS+-Server über eine TACACS+-Berechtigungsstufe von 7, aber keiner der fünf VPN 3000 Concentrator-Administratoren verfügt über eine AAA-Zugriffsstufe von 7.

## Zugehörige Informationen

- [Support-Seite für Cisco VPN Concentrator der Serie 3000](#)
- [Cisco VPN Client Support-Seite der Serie 3000](#)
- [Support-Seite für IPSec-Aushandlung/IKE-Protokolle](#)
- [Support-Seite für TACACS/TACACS+](#)
- [TACACS+ in der IOS-Dokumentation](#)
- [Technischer Support und Dokumentation - Cisco Systems](#)