

# Konfigurieren des VPN 3000 Concentrator PPTP mit Cisco Secure ACS für die Windows RADIUS-Authentifizierung

## Inhalt

[Einführung](#)

[Bevor Sie beginnen](#)

[Konventionen](#)

[Voraussetzungen](#)

[Verwendete Komponenten](#)

[Netzwerkdiagramm](#)

[Konfigurieren des VPN 3000-Konzentrators](#)

[Hinzufügen und Konfigurieren von Cisco Secure ACS für Windows](#)

[MPPE \(Verschlüsselung\) hinzufügen](#)

[Hinzufügen von Buchhaltung](#)

[Überprüfen](#)

[Fehlerbehebung](#)

[Aktivieren des Debuggens](#)

[Debugger - Gute Authentifizierung](#)

[Mögliche Fehler](#)

[Zugehörige Informationen](#)

## [Einführung](#)

Der Cisco VPN 3000 Concentrator unterstützt die PPTP-Tunneling-Methode (Point-to-Point Tunnel Protocol) für native Windows-Clients. Der Konzentrator unterstützt 40-Bit- und 128-Bit-Verschlüsselung für eine sichere und zuverlässige Verbindung. In diesem Dokument wird beschrieben, wie PPTP auf einem VPN 300-Konzentrator mit Cisco Secure ACS für Windows für die RADIUS-Authentifizierung konfiguriert wird.

Weitere Informationen finden Sie unter [Konfigurieren der Cisco Secure PIX Firewall zum Verwenden von PPTP](#) zum Konfigurieren von PPTP-Verbindungen zum PIX.

Informationen zum Einrichten einer PC-Verbindung mit dem Router finden Sie unter [Konfigurieren der sicheren Cisco ACS für die PPTP-Authentifizierung des Windows-Routers](#). Diese stellt eine Benutzerauthentifizierung für den Cisco Secure Access Control System (ACS) 3.2 für Windows-Server bereit, bevor Sie den Benutzer in das Netzwerk einbinden.

## [Bevor Sie beginnen](#)

## Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den [Cisco Technical Tips Conventions](#).

## Voraussetzungen

In diesem Dokument wird davon ausgegangen, dass die lokale PPTP-Authentifizierung funktioniert, bevor Cisco Secure ACS für die Windows RADIUS-Authentifizierung hinzugefügt wird. Weitere Informationen zur [lokalen PPTP-Authentifizierung](#) finden Sie unter [Konfigurieren des VPN 3000 Concentrator PPTP mit lokaler Authentifizierung](#). Eine vollständige Liste der Anforderungen und Einschränkungen finden Sie unter [Wann wird PPTP-Verschlüsselung von einem Cisco VPN 3000-Concentrator unterstützt?](#)

## Verwendete Komponenten

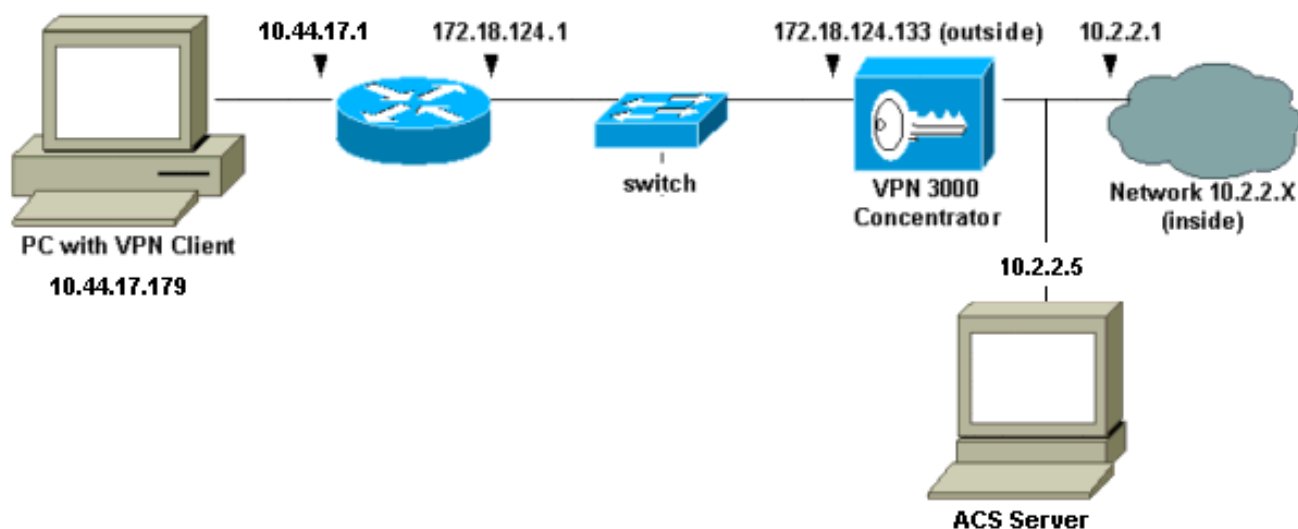
Die Informationen in diesem Dokument basieren auf den unten stehenden Software- und Hardwareversionen.

- Cisco Secure ACS für Windows 2.5 und höher
- VPN 300 Concentrator, Versionen 2.5.2.C und höher (Diese Konfiguration wurde mit Version 4.0.x verifiziert.)

Die in diesem Dokument enthaltenen Informationen wurden aus Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Sie in einem Live-Netzwerk arbeiten, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen, bevor Sie es verwenden.

## Netzwerkdigramm

In diesem Dokument wird die im Diagramm unten dargestellte Netzwerkeinrichtung verwendet.



## Konfigurieren des VPN 3000-Konzentrators

## Hinzufügen und Konfigurieren von Cisco Secure ACS für Windows

Führen Sie diese Schritte aus, um den VPN-Konzentrator für die Verwendung von Cisco Secure ACS für Windows zu konfigurieren.

1. Gehen Sie im VPN 300-Konzentrator zu **Configuration > System > Servers > Authentication Servers** und fügen Sie Cisco Secure ACS für Windows-Server und -Schlüssel hinzu ("cisco123" in diesem Beispiel).

The screenshot shows the configuration page for adding a user authentication server. The breadcrumb navigation at the top reads "Configuration | System | Servers | Authentication | Add". Below the navigation bar, the instruction "Configure and add a user authentication server." is displayed. The form includes the following fields and options:

- Server Type:** A dropdown menu currently set to "RADIUS". A tooltip indicates that selecting "Internal Server" would allow adding users to the internal user database.
- Authentication Server:** A text input field containing "10.2.2.5". The instruction is "Enter IP address or hostname."
- Server Port:** A text input field containing "0". The instruction is "Enter 0 for default port (1645)."
- Timeout:** A text input field containing "4". The instruction is "Enter the timeout for this server (seconds)."
- Retries:** A text input field containing "2". The instruction is "Enter the number of retries for this server."
- Server Secret:** A text input field with masked characters. The instruction is "Enter the RADIUS server secret."
- Verify:** A text input field with masked characters. The instruction is "Re-enter the secret."

At the bottom of the form, there are two buttons: "Add" and "Cancel". A mouse cursor is pointing at the "Add" button.

2. Fügen Sie in Cisco Secure ACS für Windows den VPN-Konzentrator zur ACS-Server-Netzwerkkonfiguration hinzu, und identifizieren Sie den

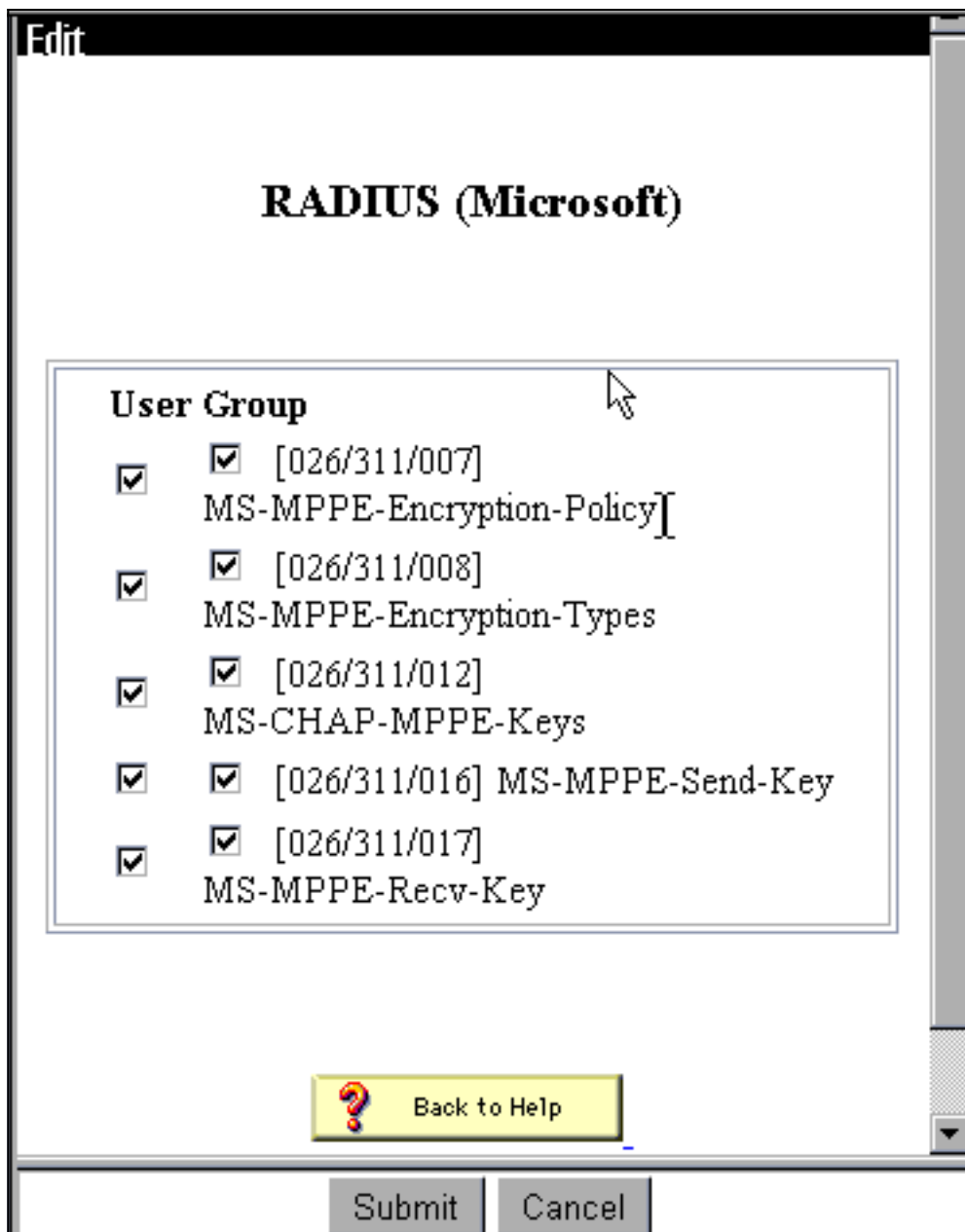
## Access Server Setup For VPN3000

Network Access Server IP Address	<input type="text" value="10.2.2.1"/>
Key	<input type="text" value="cisco123"/>
Network Device Group	<input type="text" value="(Not Assigned)"/>
Authenticate Using	<input type="text" value="RADIUS (Cisco VPN 3000)"/>

- Single Connect TACACS+ NAS (Record stop in accounting on failure).
- Log Update/Watchdog Packets from this Access Server
- Log Radius Tunneling Packets from this Access Server

Wörterbuchtyp.

3. Gehen Sie in Cisco Secure ACS für Windows zu **Schnittstellenkonfiguration > RADIUS (Microsoft)** und überprüfen Sie die Microsoft Point-to-Point Encryption (MPPE)-Attribute, sodass die Attribute in der Gruppenschnittstelle angezeigt



werden.

4. Fügen Sie in Cisco Secure ACS für Windows einen Benutzer hinzu. Fügen Sie in der Benutzergruppe die MPPE-Attribute (Microsoft RADIUS) hinzu, falls Sie zu einem späteren Zeitpunkt eine Verschlüsselung

Access Restrictions	Token Cards	Password Aging
IP Address Assignment	IETF Radius	Cisco VPN3000 Radius
MS MPPE Radius		

**Microsoft RADIUS Attributes** ?

[311\007] MS-MPPE-Encryption-Policy  
Encryption Allowed

[311\008] MS-MPPE-Encryption-Types  
40-bit

[311\012] MS-CHAP-MPPE-Keys

[311\016] MS-MPPE-Send-Key

[311\017] MS-MPPE-Recv-Key

benötigen.

- Gehen Sie im VPN 300-Konzentrator zu **Configuration > System > Servers > Authentication Servers**. Wählen Sie einen Authentifizierungsserver aus der Liste aus, und wählen Sie dann **Test** aus. Testen Sie die Authentifizierung vom VPN Concentrator zum Cisco Secure ACS für Windows-Server, indem Sie einen Benutzernamen und ein Kennwort eingeben. Bei einer guten Authentifizierung sollte der VPN Concentrator die Meldung "Authentication Successful" (Authentifizierung erfolgreich) anzeigen. Fehler in Cisco Secure ACS für Windows werden in **Berichten und Aktivitäten** protokolliert > **Fehlgeschlagene Versuche**. Bei einer Standardinstallation werden diese Berichte auf der Festplatte unter C:\Program Files\CiscoSecure ACS v2.5\Logs\Failed Attempts gespeichert.

Configuration | System | Servers | Authentication | Test

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

User Name

Password


OK Cancel

6. Da Sie nun überprüft haben, ob die Authentifizierung vom PC zum VPN-Concentrator funktioniert und vom Konzentrator zum Cisco Secure ACS für Windows-Server, können Sie den VPN-Concentrator neu konfigurieren, um PPTP-Benutzer an Cisco Secure ACS für Windows RADIUS zu senden, indem Sie die Cisco Secure ACS für Windows-Server an die oberste Stelle der Serverliste verschieben. Gehen Sie dazu im VPN Concentrator zu **Configuration > System > Servers > Authentication Servers**.

This section lets you configure parameters for servers that authenticate users.

You should have a properly configured RADIUS, NT Domain, or SDI server to access, or you can configure the internal server and [add users to the internal database](#).

Click the **Add** button to add a server, or select a server and click **Modify**, **Delete**, **Move**, or **Test**.

Authentication Servers	Actions
10.2.2.5 (Radius) 	Add
Internal (Internal)	Modify
	Delete
	Move Up
	Move Down
	Test

7. Gehen Sie zu **Konfiguration > Benutzerverwaltung > Basisgruppe**, und wählen Sie die Registerkarte **PPTP/L2TP** aus. Stellen Sie in der VPN Concentrator-Basisgruppe sicher, dass die Optionen für PAP und MSCHAPv1 aktiviert sind.



Configuration   User Management   Base Group		
General   IPsec   <b>PPTP/L2TP</b>		
<b>PPTP/L2TP Parameters</b>		
Attribute	Value	Description
<b>Use Client Address</b>	<input type="checkbox"/>	Check to accept and use an IP address received from the client.
<b>PPTP Authentication Protocols</b>	<input checked="" type="checkbox"/> PAP <input type="checkbox"/> CHAP <input type="checkbox"/> EAP <input type="text" value="-MD5"/> <input checked="" type="checkbox"/> MSCHAPv1 <input type="checkbox"/> MSCHAPv2	Select the authentication protocols allowed by the device. <b>Unchecking <i>all</i> options means that <i>no</i> authentication is required.</b>
<b>PPTP Encryption</b>	<input type="checkbox"/> Required <input type="checkbox"/> Require Stateless <input checked="" type="checkbox"/> 40-bit <input checked="" type="checkbox"/> 128-bit	Select the allowed encryption methods for PPTP connections for this group.
<b>L2TP Authentication Protocols</b>	<input type="checkbox"/> PAP <input checked="" type="checkbox"/> CHAP <input type="checkbox"/> EAP <input type="text" value="-MD5"/> <input checked="" type="checkbox"/> MSCHAPv1 <input type="checkbox"/> MSCHAPv2	Select the authentication protocols allowed by the device. <b>Unchecking <i>all</i> options means that <i>no</i> authentication is required.</b>
<b>L2TP Encryption</b>	<input type="checkbox"/> Required <input type="checkbox"/> Require Stateless <input type="checkbox"/> 40-bit <input type="checkbox"/> 128-bit	Select the allowed encryption methods for L2TP connections for this group.

8. Wählen Sie die Registerkarte **Allgemein**, und stellen Sie sicher, dass PPTP im Abschnitt Tunneling Protocols (Tunneling-Protokolle) zugelassen ist.

<b>Idle Timeout</b>	<input type="text" value="30"/>	(minutes) Enter the idle timeout for this group.
<b>Maximum Connect time</b>	<input type="text" value="0"/>	(minutes) Enter the maximum connect time for this group.
<b>Filter</b>	<input type="text" value="-None-"/>	Select the filter assigned to this group.
<b>Primary DNS</b>	<input type="text"/>	Enter the IP address of the primary DNS server for this group.
<b>Secondary DNS</b>	<input type="text"/>	Enter the IP address of the secondary DNS server.
<b>Primary WINS</b>	<input type="text"/>	Enter the IP address of the primary WINS server for this group.
<b>Secondary WINS</b>	<input type="text"/>	Enter the IP address of the secondary WINS server.
<b>SEP Card Assignment</b>	<input checked="" type="checkbox"/> SEP 1 <input checked="" type="checkbox"/> SEP 2 <input checked="" type="checkbox"/> SEP 3 <input checked="" type="checkbox"/> SEP 4	Select the SEP cards this group can be on.
<b>Tunneling Protocols</b>	<input checked="" type="checkbox"/> PPTP <input checked="" type="checkbox"/> L2TP <input checked="" type="checkbox"/> IPsec <input type="checkbox"/> L2TP over IPsec	Select the tunneling protocols this group can connect with.

9. Testen Sie die PPTP-Authentifizierung mit dem Benutzer im Cisco Secure ACS für Windows RADIUS-Server. Wenn dies nicht funktioniert, lesen Sie den Abschnitt [Debuggen](#).

### [MPPE \(Verschlüsselung\) hinzufügen](#)

Wenn die Cisco Secure ACS für die Windows RADIUS PPTP-Authentifizierung ohne Verschlüsselung funktioniert, können Sie dem VPN 3000 Concentrator MPPE hinzufügen.

1. Gehen Sie im VPN Concentrator zu **Configuration > User Management > Base Group**.
2. Aktivieren Sie im Abschnitt für die PPTP-Verschlüsselung die Optionen **Required**, **40-bit** und **128-bit**. Da nicht alle PCs sowohl die 40-Bit- als auch die 128-Bit-Verschlüsselung unterstützen, überprüfen Sie beide Optionen, um Verhandlungen zuzulassen.
3. Aktivieren Sie im Abschnitt für PPTP-Authentifizierungsprotokolle die Option für **MSCHAPv1**. (Sie haben die Benutzerattribute für Cisco Secure ACS für Windows 2.5 zur Verschlüsselung bereits zuvor konfiguriert.)

PPTP/L2TP Parameters		
Attribute	Value	Description
Use Client Address	<input type="checkbox"/>	Check to accept and use an IP address received from the client.
PPTP Authentication Protocols	<input type="checkbox"/> PAP <input type="checkbox"/> CHAP <input type="checkbox"/> EAP [-MD5] <input checked="" type="checkbox"/> MSCHAPv1 <input type="checkbox"/> MSCHAPv2	Select the authentication protocols allowed by the device. <b>Unchecking all options means that no authentication is required.</b>
PPTP Encryption	<input checked="" type="checkbox"/> Required <input type="checkbox"/> Require Stateless <input checked="" type="checkbox"/> 40-bit <input checked="" type="checkbox"/> 128-bit	Select the allowed encryption methods for PPTP connections for this group.
L2TP Authentication Protocols	<input type="checkbox"/> PAP <input checked="" type="checkbox"/> CHAP <input checked="" type="checkbox"/> EAP [-MD5] <input checked="" type="checkbox"/> MSCHAPv1 <input type="checkbox"/> MSCHAPv2	Select the authentication protocols allowed by the device. <b>Unchecking all options means that no authentication is required.</b>
L2TP Encryption	<input type="checkbox"/> Required <input type="checkbox"/> Require Stateless <input type="checkbox"/> 40-bit <input type="checkbox"/> 128-bit	Select the allowed encryption methods for L2TP connections for this group.

**Hinweis:** Der PPTP-Client sollte für eine optimale oder erforderliche Datenverschlüsselung und MSCHAPv1 (falls eine Option verfügbar ist) erkannt werden.

## [Hinzufügen von Buchhaltung](#)

Nachdem Sie die Authentifizierung eingerichtet haben, können Sie dem VPN Concentrator Accounting hinzufügen. Gehen Sie zu **Configuration > System > Servers > Accounting Servers**, und fügen Sie den Cisco Secure ACS für Windows-Server hinzu.

In Cisco Secure ACS für Windows werden die Accounting-Datensätze wie folgt angezeigt.

```
Date, Time, User-Name, Group-Name, Calling-Station-Id, Acct-Status-Type, Acct-Session-Id,
Acct-Session-Time, Service-Type, Framed-Protocol, Acct-Input-Octets, Acct-Output-Octets,
Acct-Input-Packets, Acct-Output-Packets, Framed-IP-Address, NAS-Port, NAS-IP-Address
03/18/2000, 08:16:20, CSNTUSER, Default Group, , Start, 8BD00003, , Framed,
PPP, , , , 1.2.3.4, 1163, 10.2.2.1
03/18/2000, 08:16:50, CSNTUSER, Default Group, , Stop, 8BD00003, 30, Framed,
PPP, 3204, 24, 23, 1, 1.2.3.4, 1163, 10.2.2.1
```

## [Überprüfen](#)

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

## [Fehlerbehebung](#)

Dieser Abschnitt enthält Informationen zur Fehlerbehebung in Ihrer Konfiguration.

## [Aktivieren des Debuggens](#)

Wenn Verbindungen nicht funktionieren, können Sie dem VPN Concentrator PPTP- und AUTH-Ereignisklassen hinzufügen, indem Sie **Configuration > System > Events > Classes > Modify wählen**. Sie können auch PPTPDBG-, PPTPDECODE-, AUTHDBG- und AUTHDECODE-Ereignisklassen hinzufügen, diese Optionen können jedoch zu viele Informationen bereitstellen.

Configuration | System | Events | Classes | Modify

This screen lets you modify an event class configured for special handling.

Class Name	<input type="text" value="PPTP"/>	
Enable	<input checked="" type="checkbox"/>	Check to enable special handling of this class.
Severity to Log	<input type="text" value="1-9"/>	Select the range of severity values to enter in the log.
Severity to Console	<input type="text" value="1-3"/>	Select the range of severity values to display on the console.
Severity to Syslog	<input type="text" value="None"/>	Select the range of severity values to send to a Syslog server.
Severity to Email	<input type="text" value="None"/>	Select the range of severity values to send via email to the recipient list.
Severity to Trap	<input type="text" value="None"/>	Select the range of severity values to send to an SNMP system.

Sie können das Ereignisprotokoll abrufen, indem Sie **Monitoring > Event Log (Überwachung > Ereignisprotokoll)** aufrufen.

Monitoring | Event Log

Select Filter Options

Event Class: All Classes (dropdown menu showing AUTH, AUTHDBG, AUTHDECODE)

Severities: ALL (dropdown menu showing 1, 2, 3)

Client IP Address: 0.0.0.0 (text input)

Events/Page: 100 (dropdown menu)

Direction: Oldest to Newest (dropdown menu)

Navigation buttons: <<<, <<, >>, >>>, Get Log, Save Log, Clear Log

```

1 12/04/2000 14:51:32.600 SEV=4 AUTH/22 RPT=21
User pptpuser disconnected

2 12/04/2000 14:51:32.600 SEV=4 PPTP/35 RPT=14 10.44.17.179
Session closed on tunnel 10.44.17.179 (peer 0, local 45636, serial 0), re
Administrative shutdown (No additional info)

4 12/04/2000 14:51:32.640 SEV=4 PPTP/34 RPT=14 10.44.17.179
Tunnel to peer 10.44.17.179 closed, reason: Stop-Local-Shutdown (No addit
info)

6 12/04/2000 14:51:49.150 SEV=4 PPTP/47 RPT=15 10.44.17.179
Tunnel to peer 10.44.17.179 established

```

## [Debugger - Gute Authentifizierung](#)

Gute Debug-Vorgänge im VPN-Concentrator ähneln dem folgenden Beispiel.

```

1 12/06/2000 09:26:16.390 SEV=4 PPTP/47 RPT=20 10.44.17.179
Tunnel to peer 161.44.17.179 established
2 12/06/2000 09:26:16.390 SEV=4 PPTP/42 RPT=20 10.44.17.179
Session started on tunnel 161.44.17.179
3 12/06/2000 09:26:19.400 SEV=7 AUTH/12 RPT=22
Authentication session opened: handle = 22
4 12/06/2000 09:26:19.510 SEV=6 AUTH/4 RPT=17 10.44.17.179
Authentication successful: handle = 22, server = 10.2.2.5,
user = CSNTUSER
5 12/06/2000 09:26:19.510 SEV=5 PPP/8 RPT=17 10.44.17.179
User [ CSNTUSER ]
Authenticated successfully with MSCHAP-V1
6 12/06/2000 09:26:19.510 SEV=7 AUTH/13 RPT=22
Authentication session closed: handle = 22
7 12/06/2000 09:26:22.560 SEV=4 AUTH/21 RPT=30
User CSNTUSER connected

```

## [Mögliche Fehler](#)

Eventuell treten Fehler wie unten dargestellt auf.

## Ungültiger Benutzername oder falsches Kennwort auf dem Cisco Secure ACS für Windows RADIUS-Server

- VPN 3000 Concentrator Debug-Ausgabe

```
6 12/06/2000 09:33:03.910 SEV=4 PPTP/47 RPT=21 10.44.17.179
Tunnel to peer 10.44.17.179 established
```

```
7 12/06/2000 09:33:03.920 SEV=4 PPTP/42 RPT=21 10.44.17.179
Session started on tunnel 10.44.17.179
```

```
8 12/06/2000 09:33:06.930 SEV=7 AUTH/12 RPT=23
Authentication session opened: handle = 23
```

```
9 12/06/2000 09:33:07.050 SEV=3 AUTH/5 RPT=4 10.44.17.179
Authentication rejected: Reason = Unspecified
handle = 23, server = 10.2.2.5, user = baduser
```

```
11 12/06/2000 09:33:07.050 SEV=5 PPP/9 RPT=4 10.44.17.179
User [ baduser ]
disconnected.. failed authentication ( MSCHAP-V1 )
```

```
12 12/06/2000 09:33:07.050 SEV=7 AUTH/13 RPT=23
Authentication session closed: handle = 23
```

- Cisco Secure ACS für Windows-Protokollausgabe

```
03/18/2000,08:02:47,Authen failed, baduser,,,CS user
unknown,,,1155,10.2.2.1
```

- Die vom Benutzer angezeigte Meldung (aus Windows 98)

```
Error 691: The computer you have dialed in to has denied access because
the username and/or password is invalid on the domain.
```

**Im Konzentrator ist "MPPE Encryption Required" (MPPE-Verschlüsselung erforderlich) ausgewählt, der Cisco Secure ACS für Windows-Server ist jedoch nicht für MS-CHAP-MPPE-Keys und MS-CHAP-MPPE-Typen konfiguriert.**

- VPN 3000 Concentrator Debug-Ausgabe Wenn AUTHDECODE (1-13 Schweregrad) und PPTP-Debuggen (1-9 Schweregrad) aktiviert sind, zeigt das Protokoll, dass der Cisco Secure ACS für Windows-Server das anbieterspezifische Attribut 26 (0x1A) im access-accept vom Server (partielles Protokoll) nicht sendet.

```
2221 12/08/2000 10:01:52.360 SEV=13 AUTHDECODE/0 RPT=545
0000: 024E002C 80AE75F6 6C365664 373D33FE .N...u.l6Vd7=3.
0010: 6DF74333 501277B2 129CBC66 85FFB40C m.C3P.w....f....
0020: 16D42FC4 BD020806 FFFFFFFF ..//.....
```

```
2028 12/08/2000 10:00:29.570 SEV=5 PPP/13 RPT=12 10.44.17.179
User [ CSNTUSER ] disconnected. Data encrypt required. Auth server
or auth protocol will not support encrypt.
```

- Die Protokollausgabe von Cisco Secure ACS für Windows zeigt keine Fehler an.

- Die vom Benutzer angezeigte Nachricht

```
Error 691: The computer you have dialed in to has denied access because
the username and/or password is invalid on the domain.
```

## Zugehörige Informationen

- [Support-Seite für Cisco VPN Concentrator der Serie 3000](#)
- [Cisco VPN Client Support-Seite der Serie 3000](#)
- [IPSec-Support-Seite](#)
- [Support-Seite für Cisco Secure ACS für Windows](#)

- [RADIUS-Support-Seite](#)
- [PPTP-Support-Seite](#)
- [RFC 2637: Point-to-Point Tunneling Protocol \(PPTP\)](#)
- [Anforderungen für Kommentare \(RFCs\)](#)
- [Technischer Support und Dokumentation - Cisco Systems](#)