

De VPN 3000 Concentrator PPTP configureren met Cisco Secure ACS voor Windows RADIUS-verificatie

Inhoud

[Inleiding](#)

[Voordat u begint](#)

[Conventies](#)

[Voorwaarden](#)

[Gebruikte componenten](#)

[Netwerkdigram](#)

[De VPN-concentratie configureren 3000](#)

[Cisco Secure ACS toevoegen en configureren voor Windows](#)

[MPPE toevoegen \(encryptie\)](#)

[Boekhouding toevoegen](#)

[Verifiëren](#)

[Problemen oplossen](#)

[Debuggen inschakelen](#)

[Debugs - goede verificatie](#)

[Mogelijke fouten](#)

[Gerelateerde informatie](#)

Inleiding

Cisco VPN 3000 Concentrator ondersteunt de Point-to-Point Tunnel Protocol (PPTP)-tunnelmethode voor native Windows-clients. De concentrator ondersteunt 40-bits en 128-bits codering voor een beveiligde betrouwbare verbinding. Dit document beschrijft hoe u PPTP op een VPN 3000 Concentrator met Cisco Secure ACS voor Windows voor RADIUS-verificatie kunt configureren.

Raadpleeg [de Cisco Secure PIX-firewall configureren om PPTP te gebruiken](#) om PPTP-verbindingen naar de PIX te configureren.

Raadpleeg [Cisco Secure ACS voor Windows-routerverificatie configureren](#) om een pc-verbinding met de router in te stellen; Dit biedt gebruikersverificatie naar het Cisco Secure Access Control System (ACS) 3.2 voor Windows-server voordat u de gebruiker in het netwerk toestaat.

[Voordat u begint](#)

[Conventies](#)

Zie de [Cisco Technical Tips Convention](#) voor meer informatie over documentconventies.

Voorwaarden

Dit document gaat ervan uit dat de lokale PPTP-verificatie werkt voordat Cisco Secure ACS voor Windows RADIUS-verificatie wordt toegevoegd. Zie [Hoe u VPN 3000 Concentrator PPTP met Lokale verificatie configureren](#) voor meer informatie over lokale PPTP-verificatie. Raadpleeg voor een compleet overzicht van vereisten en beperkingen [wanneer wordt PPTP-encryptie ondersteund op een Cisco VPN 3000 Concentrator?](#)

Gebruikte componenten

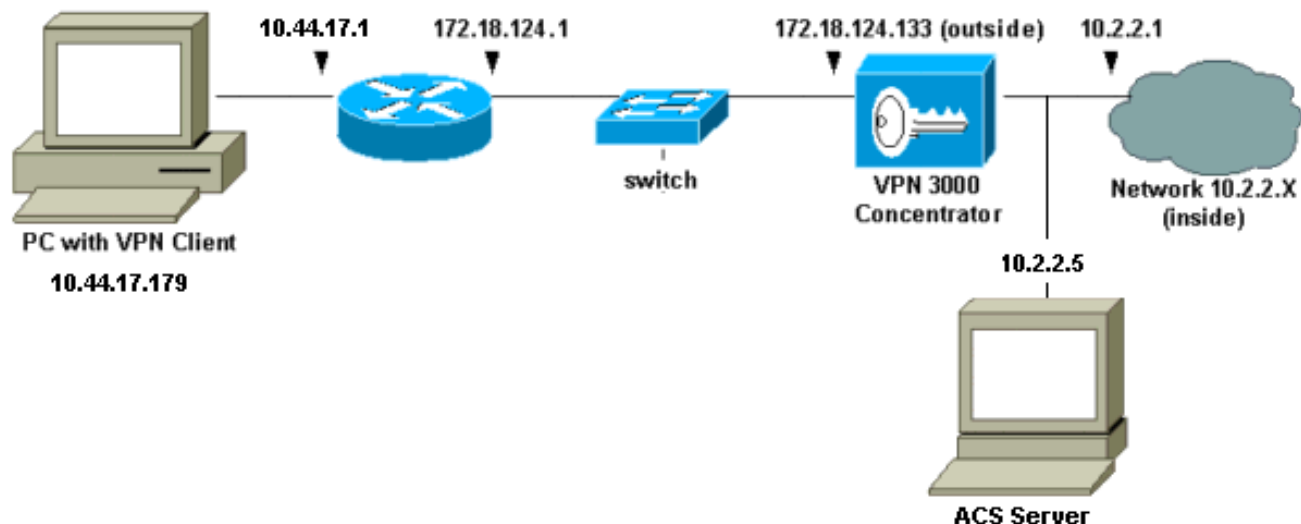
De informatie in dit document is gebaseerd op de onderstaande software- en hardwareversies.

- Cisco Secure ACS voor Windows versies 2.5 en hoger
- VPN 3000 Concentrator versies 2.5.2.C en hoger (Deze configuratie is geverifieerd met versie 4.0.x.)

De informatie in dit document is gebaseerd op apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als u in een levend netwerk werkt, zorg er dan voor dat u de potentiële impact van om het even welke opdracht begrijpt alvorens het te gebruiken.

Netwerkdigram

Dit document gebruikt de netwerkinstellingen die in het onderstaande schema zijn weergegeven.



De VPN-concentratie configureren 3000

Cisco Secure ACS toevoegen en configureren voor Windows

Volg deze stappen om de VPN-Concentrator te configureren om Cisco Secure ACS voor Windows te gebruiken.

1. Ga in de VPN 3000 Concentrator naar **Configuration > System > Server > Verificatieservers** en voeg de Cisco Secure ACS voor Windows server en de toets ("cisco123" in dit voorbeeld) toe.

The screenshot shows a web-based configuration interface for a VPN 3000 Concentrator. The breadcrumb navigation at the top reads "Configuration | System | Servers | Authentication | Add". Below this, the instruction "Configure and add a user authentication server." is displayed. The main configuration area includes several fields: "Server Type" is a dropdown menu set to "RADIUS", with a tooltip that says "Selecting *Internal Server* will let you add users to the internal user database."; "Authentication Server" is a text box containing "10.2.2.5" with the instruction "Enter IP address or hostname."; "Server Port" is a text box containing "0" with the instruction "Enter 0 for default port (1645)."; "Timeout" is a text box containing "4" with the instruction "Enter the timeout for this server (seconds)."; "Retries" is a text box containing "2" with the instruction "Enter the number of retries for this server."; "Server Secret" and "Verify" are password fields, both containing masked characters, with instructions "Enter the RADIUS server secret." and "Re-enter the secret." respectively. At the bottom left, there are two buttons: "Add" and "Cancel". A mouse cursor is pointing at the "Add" button.

2. In Cisco Secure ACS voor Windows, voegt u de VPN-centrator toe aan de ACS-servernetwerkconfiguratie en identificeert u het

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

woordenboektype.


3. In Cisco Secure ACS voor Windows, ga naar **Interface Configuration > RADIUS (Microsoft)** en controleer de Microsoft Point-to-Point Encryption (MPPE)-eigenschappen, zodat de eigenschappen in de groepsinterface

Edit

RADIUS (Microsoft)

User Group

- [026/311/007]
MS-MPPE-Encryption-Policy]
- [026/311/008]
MS-MPPE-Encryption-Types
- [026/311/012]
MS-CHAP-MPPE-Keys
- [026/311/016] MS-MPPE-Send-Key
- [026/311/017]
MS-MPPE-Recv-Key

 Back to Help

verschijnen.

4. Voeg een gebruiker toe in Cisco Secure ACS voor Windows. In de groep van de gebruiker, voeg de MPPE (Microsoft RADIUS) eigenschappen toe, voor het geval u encryptie op een later tijdstip nodig

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

hebt.

- Ga in de VPN 3000 Concentrator naar **Configuration > System > Server > Verificatieservers**. Selecteer een verificatieserver uit de lijst en selecteer vervolgens **Test**. Verificatie vanuit VPN-centrator naar Cisco Secure ACS voor Windows-server door een gebruikersnaam en wachtwoord in te voeren. Bij een goede authenticatie zou de VPN Concentrator een "Verificatie succesvol" bericht moeten laten zien. De mislukkingen in Cisco Secure ACS voor Windows zijn inlogd in **Rapporten en Activiteit > mislukte Pogingen**. Standaard wordt de installatie van deze rapporten op de harde schijf opgeslagen in C:\Program Files\CiscoSecure ACS v2.5\Logs\Failed Attempts.

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. Aangezien u nu verificatie van de verificatie van de PC naar de VPN Concentrator hebt uitgevoerd en u van de concentrator naar de Cisco Secure ACS voor Windows server hebt geverifieerd, kunt u de VPN Concentrator opnieuw configureren om PPTP-gebruikers naar Cisco Secure ACS voor Windows RADIUS te verzenden door de Cisco Secure ACS voor Windows server naar de top van de serverlijst te verplaatsen. Ga om dit op de VPN Concentrator te doen naar **Configuration > System > Server > Verificatieservers**.

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)  Internal (Internal)	<input type="button" value="Add"/>
	<input type="button" value="Modify"/>
	<input type="button" value="Delete"/>
	<input type="button" value="Move Up"/>
	<input type="button" value="Move Down"/>
	<input type="button" value="Test"/>

7. Ga naar **Configuration > User Management > Base Group** en selecteer het **PPTP/L2TP**-tabblad. Zorg ervoor dat de opties voor PAP en MSCHAPv1 in de basisgroep van VPN Concentrator zijn ingeschakeld.

General

IPSec

PPTP/L2TP

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 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. Unchecking <i>all</i> options means that <i>no</i> authentication is required.
PPTP Encryption	<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.
L2TP Authentication Protocols	<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. Unchecking <i>all</i> options means that <i>no</i> authentication is required.
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.

8. Selecteer het **tabblad General** en controleer of PPTP is toegestaan in het gedeelte Tunneling Protocols.

Idle Timeout	<input type="text" value="30"/>	(minutes) Enter the idle timeout for this group.
Maximum Connect time	<input type="text" value="0"/>	(minutes) Enter the maximum connect time for this group.
Filter	<input type="text" value="-None-"/>	Select the filter assigned to this group.
Primary DNS	<input type="text"/>	Enter the IP address of the primary DNS server for this group.
Secondary DNS	<input type="text"/>	Enter the IP address of the secondary DNS server.
Primary WINS	<input type="text"/>	Enter the IP address of the primary WINS server for this group.
Secondary WINS	<input type="text"/>	Enter the IP address of the secondary WINS server.
SEP Card Assignment	<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.
Tunneling Protocols	<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. Test PPTP-verificatie met de gebruiker in Cisco Secure ACS voor Windows RADIUS-server. Als dit niet werkt, raadpleegt u het gedeelte [Debugging](#).

[MPPE toevoegen \(encryptie\)](#)

Als Cisco Secure ACS voor Windows RADIUS PPTP-verificatie zonder encryptie werkt, kunt u MPPE aan de VPN 3000 Concentrator toevoegen.

1. Ga in de VPN Concentrator naar **Configuration > User Management > Base Group**.
2. Controleer onder het gedeelte voor PPTP-encryptie de opties voor **verplicht, 40-bits** en **128-bits**. Aangezien niet alle PC's zowel 40-bits als 128-bits codering ondersteunen, controleer beide opties om onderhandeling mogelijk te maken.
3. Controleer onder het kopje voor PPTP-verificatieprotocollen de optie voor **MSCHAPv1**. (U hebt de Cisco Secure ACS voor Windows 2.5-gebruikerseigenschappen voor codering in een eerdere stap al ingesteld.)

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. Unchecking all options means that no authentication is required.
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. Unchecking all options means that no authentication is required.
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.

Opmerking: De PPTP-client moet worden herkend voor optimale of vereiste gegevenscodering en MSCHAPv1 (indien een optie).

[Boekhouding toevoegen](#)

Nadat u verificatie hebt ingesteld, kunt u accounting aan de VPN-centrator toevoegen. Ga naar **Configuration > System > Server > Accounting Server** en voeg Cisco Secure ACS toe voor Windows-server.

In Cisco Secure ACS voor Windows verschijnen de accounting records als volgt.

```
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
```

[Verifiëren](#)

Er is momenteel geen verificatieprocedure beschikbaar voor deze configuratie.

[Problemen oplossen](#)

Deze sectie bevat informatie waarmee u problemen met de configuratie kunt oplossen.

[Debuggen inschakelen](#)

Als de verbindingen niet werken, kunt u PPTP- en AUTH-eventklassen aan de VPN-centrator toevoegen door naar **Configuration > System > Events > Classes > Wijzigen** te gaan. U kunt ook klassen PPTPDBG, PPTPDECODE, AUTHDBG en AUTHDECODE-gebeurtenissen toevoegen, maar deze opties kunnen te veel informatie bieden.

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.

U kunt het logbestand van de gebeurtenis herstellen door naar **Monitoring > Event Log** te gaan.

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)

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

Debugs - goede verificatie

Goede deposito's op de VPN-centrator lijken op het volgende.

```

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

```

Mogelijke fouten

U kunt mogelijke fouten ondervinden zoals hieronder wordt getoond.

Slechte gebruikersnaam of wachtwoord op Cisco Secure ACS voor Windows RADIUS-server

- VPN 3000 Concentrator debug-uitvoer

```
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 voor Windows-loguitvoer

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

- Het bericht dat de gebruiker ziet (vanuit 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.
```

"MPPE-encryptie vereist" is geselecteerd op de concentrator, maar Cisco Secure ACS voor Windows-server is niet geconfigureerd voor MS-CHAP-MPPE-toetsen en MS-CHAP-MPPE-typen

- VPN 3000 Concentrator debug-uitvoerAls AUTHDECODE (1-13 Severity) en PPTP debug (1-9 Severity) zijn ingeschakeld, toont het logbestand aan dat Cisco Secure ACS voor Windows-server geen leverancierspecifieke eigenschap 26 (0x1A) in de access-accepteren vanuit de server (gedeeltelijk logbestand) stuurt.

```
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.
```

- Cisco Secure ACS voor Windows-loguitvoer toont geen tekortkomingen.
- Het bericht dat de gebruiker ziet
Error 691: The computer you have dialed in to has denied access because
the username and/or password is invalid on the domain.

Gerelateerde informatie

- [Ondersteuning van Cisco VPN 3000 Series Concentrator-pagina](#)
- [Cisco VPN 3000 Series clientondersteuningspagina](#)
- [IPsec-ondersteuningspagina](#)
- [Cisco Secure ACS voor Windows-ondersteuningspagina](#)
- [RADIUS-ondersteuningspagina](#)

- [PPTP-ondersteuningspagina](#)
- [RFC 2637: Point-to-Point Tunneling Protocol \(PPTP\)](#)
- [Verzoeken om opmerkingen \(RFC's\)](#)
- [Technische ondersteuning en documentatie – Cisco Systems](#)