

# Configurar el VPN 3000 concentrator PPTP con la autenticación de RADIUS del Cisco Secure ACS for Windows

## Contenido

[Introducción](#)

[Antes de comenzar](#)

[Convenciones](#)

[prerrequisitos](#)

[Componentes Utilizados](#)

[Diagrama de la red](#)

[Configuración del concentrador VPN 3000](#)

[Agregando y configurando el Cisco Secure ACS for Windows](#)

[Agregar MPPE \(Cifrado\)](#)

[Incorporación de contabilidad](#)

[Verificación](#)

[Troubleshooting](#)

[Habilitar el debugging](#)

[Debugs - Buena autenticación](#)

[Errores posibles](#)

[Información Relacionada](#)

## [Introducción](#)

El Cisco VPN 3000 Concentrator soporta el método de tunelización del Point-to-Point Tunnel Protocol (PPTP) para los clientes de las ventanas nativas. Los concentradores soporta 40-bit y cifrado del 128-bit para una conexión confiable asegurada. Este documento describe cómo configurar el PPTP en un concentrador VPN 3000 con el Cisco Secure ACS for Windows para la autenticación de RADIUS.

Refiera a [configurar el Cisco Secure PIX Firewall para utilizar el PPTP](#) para configurar las conexiones PPTP al PIX.

Refiera a [configurar la autenticación PPTP del router del Cisco Secure ACS for Windows](#) para configurar una conexión de PC al router; esto proporciona la autenticación de usuario al Cisco Secure Access Control System (ACS) 3.2 para el Servidor Windows antes de que usted permita al usuario en la red.

## [Antes de comenzar](#)

## Convenciones

Para obtener más información sobre las convenciones del documento, consulte [Convenciones de Consejos Técnicos de Cisco](#).

## prerrequisitos

Este documento asume que la autenticación local de PPTP está trabajando antes de agregar la autenticación de RADIUS del Cisco Secure ACS for Windows. Vea por favor [cómo configurar el VPN 3000 concentrator PPTP con la autenticación local](#) para más información sobre la autenticación local de PPTP. ¿Para una lista completa de requisitos y de restricciones, refiérase por favor [cuando es la encriptación PPTP soportada en un Cisco VPN 3000 Concentrator?](#)

## Componentes Utilizados

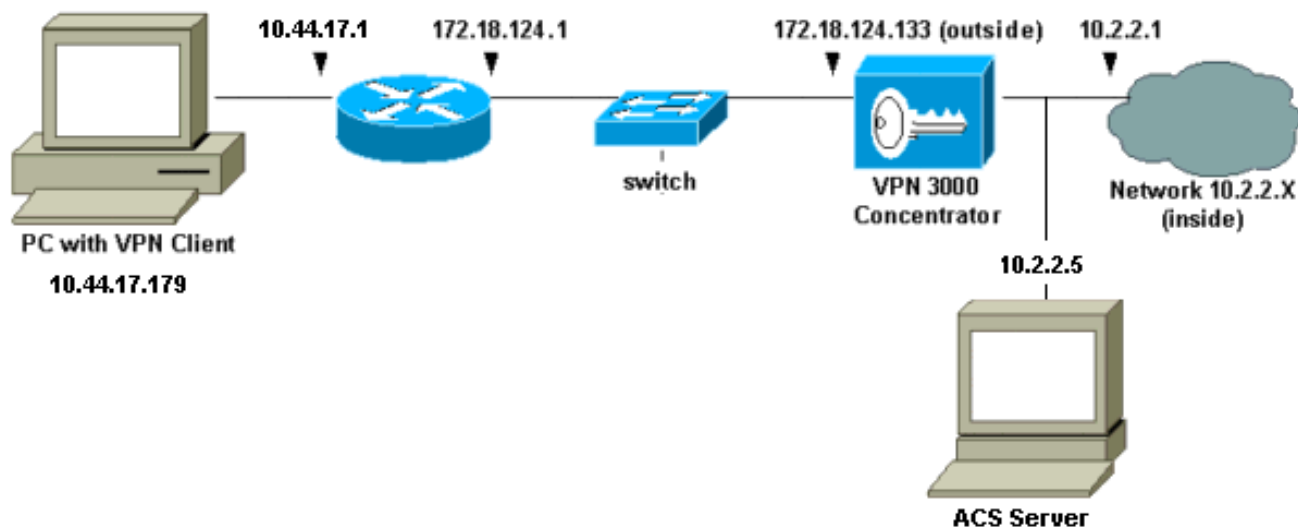
La información que contiene este documento se basa en las versiones de software y hardware indicadas a continuación.

- Versiones 2.5 del Cisco Secure ACS for Windows y posterior
- Versiones concentradoras VPN 3000 2.5.2.C y posterior (esta configuración se ha verificado con la versión 4.0.x.)

La información que se presenta en este documento se originó a partir de dispositivos dentro de un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener un comando antes de ejecutarlo.

## Diagrama de la red

Este documento utiliza la instalación de red que se muestra en el siguiente diagrama.

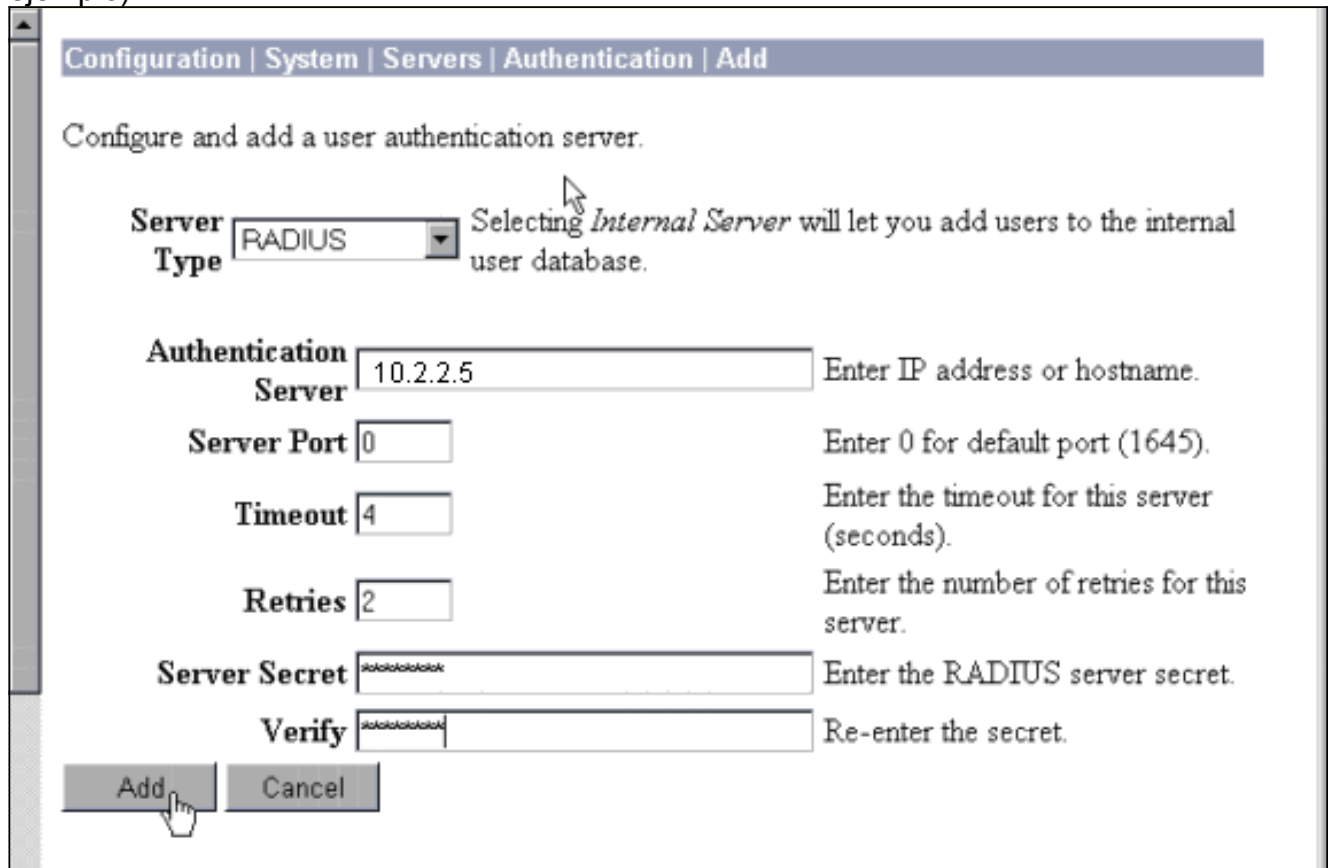


## Configuración del concentrador VPN 3000

## [Agregando y configurando el Cisco Secure ACS for Windows](#)

Siga los siguientes pasos para configurar el concentrador VPN para utilizar el Cisco Secure ACS for Windows.

1. En el concentrador VPN 3000, vaya al **Configuration (Configuración) > System (Sistema) > Servers (Servidores) > Authentication servers (Servidores de autenticación)** y agregue el servidor y la clave (el "cisco123" del Cisco Secure ACS for Windows en este ejemplo).



The screenshot shows the configuration window for adding a user authentication server. The breadcrumb navigation at the top reads "Configuration | System | Servers | Authentication | Add". Below the navigation bar, the text "Configure and add a user authentication server." is displayed. The "Server Type" dropdown menu is set to "RADIUS". A tooltip points to the dropdown, stating: "Selecting *Internal Server* will let you add users to the internal user database." The "Authentication Server" field contains "10.2.2.5" with the instruction "Enter IP address or hostname." The "Server Port" field contains "0" with the instruction "Enter 0 for default port (1645)." The "Timeout" field contains "4" with the instruction "Enter the timeout for this server (seconds)." The "Retries" field contains "2" with the instruction "Enter the number of retries for this server." The "Server Secret" field contains masked characters with the instruction "Enter the RADIUS server secret." The "Verify" field also contains masked characters with the instruction "Re-enter the secret." At the bottom, there are "Add" and "Cancel" buttons, with a mouse cursor clicking on the "Add" button.

2. En el Cisco Secure ACS for Windows, agregue el concentrador VPN a la configuración de red del servidor ACS, e identifique el tipo de

## 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

diccionario.

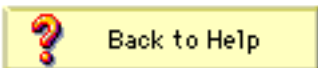
3. En el Cisco Secure ACS for Windows, vaya a **Interface Configuration > Radius (Microsoft)** y marque los atributos del Microsoft Point-to-Point Encryption (MPPE) de modo que los atributos aparezcan en la interfaz de

**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

grupo.

4. En el Cisco Secure ACS for Windows, agregue a un usuario. En el grupo de usuario, agregue los atributos MPPE (Microsoft RADIUS), en caso de que usted requiera el cifrado

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

en otro momento.

- En el concentrador VPN 3000, vaya al **Configuration (Configuración) > System (Sistema) > Servers (Servidores) > Authentication servers (Servidores de autenticación)**. Seleccione a un servidor de autenticación de la lista, y después seleccione la **prueba**. Prueba de la autenticación del concentrador VPN al servidor del Cisco Secure ACS for Windows ingresando un nombre de usuario y contraseña. En una buena autenticación, el concentrador VPN debe mostrar un mensaje "autenticación exitosa". Los errores en el Cisco Secure ACS for Windows son **informes y actividad > intentos fallidos** abiertos una sesión. En un valor por defecto instale, estos informes se salvan en el disco en las tentativas de C:\Program Files\CiscoSecure ACS v2.5\Logs\Failed.

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. Puesto que usted ahora ha verificado la autenticación del PC a los trabajos del concentrador VPN y del concentrador al servidor del Cisco Secure ACS for Windows, usted puede configurar de nuevo el concentrador VPN para enviar a los Usuarios usuarios PPTP al Cisco Secure ACS for Windows RADIUS moviendo el servidor del Cisco Secure ACS for Windows al top de la lista de servidores. Para hacer esto en el concentrador VPN, vaya al **Configuration (Configuración) > System (Sistema) > Servers (Servidores) > Authentication servers (Servidores de autenticación)**.

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. Vaya al **Configuration (Configuración) > User Management (Administración del usuario) > Base Group (Grupo base)** y seleccione la lengüeta **PPTP/L2TP**. En el grupo base del concentrador VPN, asegúrese de que las opciones para el PAP y el MSCHAPv1 estén habilitadas.



Configuration | User Management | Base Group

General IPsec **PPTP/L2TP**

### PPTP/L2TP Parameters

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 <span style="border: 1px solid black; padding: 0 2px;">-MD5</span> <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 <span style="border: 1px solid black; padding: 0 2px;">-MD5</span> <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. Seleccione la **ficha general** y asegúrese de que el PPTP está permitido en la sección de los protocolos de túneles.

<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. Pruebe la autenticación PPTP con el usuario en el servidor de RADIUS del Cisco Secure ACS for Windows. Si esto no trabaja, satisfacer vea la [sección de debugging](#).

### [Agregar MPPE \(Cifrado\)](#)

Si la autenticación PPTP del Cisco Secure ACS for Windows RADIUS trabaja sin el cifrado, usted puede agregar el MPPE al concentrador VPN 3000.

1. En el concentrador VPN, vaya al **Configuration (Configuración) > User Management (Administración del usuario) > Base Group (Grupo base)**.
2. Bajo sección para la encriptación PPTP, marque las opciones para **requerido**, **40-bit**, y **128-bit**. Puesto que no todos los PC soportan 40-bit y el cifrado del 128-bit, marque ambas opciones para tener en cuenta la negociación.
3. Bajo sección para los protocolos de autenticación PPTP, marque la opción para el **MSCHAPv1**. (Usted configuró ya los atributos de usuario del Cisco Secure ACS for Windows 2.5 para el cifrado en un paso anterior.)

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.

**Nota:** El cliente PPTP debe ser reconocido para óptimo o encriptación de datos requeridos y MSCHAPv1 (si una opción).

## Incorporación de contabilidad

Después de que usted haya establecido la autenticación, usted puede agregar las estadísticas al concentrador VPN. Vaya al **Configuration (Configuración) > System (Sistema) > Servers (Servidores) > Accounting Servers (Servidores de contabilidad)** y agregue el servidor del Cisco Secure ACS for Windows.

En el Cisco Secure ACS for Windows, los registros de contabilidad aparecen como sigue.

```
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
```

## Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

## Troubleshooting

En esta sección encontrará información que puede utilizar para solucionar problemas de

configuración.

## Habilitar el debugging

Si las conexiones no trabajan, usted puede agregar las clases de evento PPTP y AUTH al concentrador VPN yendo al **Configuration (Configuración) > System (Sistema) > Events (Eventos) > Classes (Clases) > Modify (Modificar)**. Usted puede también agregar el PPTPDBG, el PPTPDECODE, el AUTHDBG, y las clases de evento authdecode, pero estas opciones pueden proporcionar demasiada información.

**Configuration | System | Events | Classes | Modify**

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

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

Usted puede extraer el registro de acontecimientos yendo al **Monitoring (Monitoreo) > Event Log (Registro de evento)**.

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

```

## [Debugs - Buena autenticación](#)

Los debugs correctos en el concentrador VPN parecerán similares al siguiente.

```

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

```

## [Errores posibles](#)

Usted puede encontrar los errores posibles como se muestra abajo.

[Nombre de usuario incorrecto o contraseña en el servidor de RADIUS del Cisco Secure ACS for](#)

## [Windows](#)

- Salida de los debugs concentradora VPN 30006 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
- Salida del registro del Cisco Secure ACS for Windows03/18/2000,08:02:47,Authen failed, baduser,,,CS user unknown,,,1155,10.2.2.1
- El mensaje que el usuario ve (de 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.

**La “encripción MPPE requerida” se selecciona en el concentrador, pero el servidor del Cisco Secure ACS for Windows no se configura para las MS-GRIETA-MPPE-claves y los MS-GRIETA-MPPE-tipos**

- Salida de los debugs concentradora VPN 3000Si el debug AUTHDECODE (gravedad 1-13) y PPTP (gravedad 1-9) está prendido, el registro muestra que el servidor del Cisco Secure ACS for Windows no está enviando el atributo específico del proveedor 26 (0x1A) en el access-accept del servidor (registro parcial).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.
- La salida del registro del Cisco Secure ACS for Windows no muestra ningún error.
- El mensaje que el usuario veError 691: The computer you have dialed in to has denied access because the username and/or password is invalid on the domain.

## [Información Relacionada](#)

- [Página de soporte del concentrador de la serie Cisco VPN 3000](#)
- [Página de soporte al cliente Serie Cisco VPN 3000](#)
- [Página de soporte de IPSec](#)
- [Página de soporte de Cisco Secure ACS para Windows](#)
- [Página de soporte de RADIUS](#)

- [Página de soporte de PPTP](#)
- [RFC 2637: Protocolo de Tunnelización punto a Punto \(PPTP\)](#)
- [Solicitudes de Comentarios \(RFC\)](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)