

Configuration du PPTP du concentrateur VPN 3000 avec Cisco Secure ACS pour Windows pour authentification RADIUS

Contenu

[Introduction](#)

[Avant de commencer](#)

[Conventions](#)

[Conditions préalables](#)

[Composants utilisés](#)

[Diagramme du réseau](#)

[Configuration du concentrateur VPN 3000](#)

[Ajoutant et configurant le Cisco Secure ACS pour Windows](#)

[Ajoutant MPPE \(cryptage\)](#)

[Ajout de la comptabilité](#)

[Vérifiez](#)

[Dépannez](#)

[Activation de l'élimination des imperfections](#)

[Debugs - Bonne authentification](#)

[Erreurs possibles](#)

[Informations connexes](#)

[Introduction](#)

Le concentrateur de Cisco VPN 3000 prend en charge la méthode point par point de perçage d'un tunnel de Protocol de tunnel (PPTP) pour les clients Windows indigènes. Le concentrateur prend en charge le cryptage 40-bit et 128-bit pour une connexion fiable sécurisée. Ce document décrit comment configurer PPTP sur un concentrateur VPN 3000 avec le Cisco Secure ACS pour Windows pour l'authentification de RAYON.

Référez-vous à [configurer le pare-feu Cisco Secure PIX pour employer PPTP](#) pour configurer des connexions PPTP au PIX.

Référez-vous à [configurer le Cisco Secure ACS pour que l'authentification du routeur PPTP de Windows](#) installe une connexion par PC au routeur ; ceci fournit l'authentification de l'utilisateur au Système de contrôle d'accès sécurisé Cisco (ACS) 3.2 pour des Windows Server avant que vous permettiez l'utilisateur dans le réseau.

[Avant de commencer](#)

Conventions

Pour plus d'informations sur les conventions des documents, référez-vous aux [Conventions utilisées pour les conseils techniques de Cisco](#).

Conditions préalables

Ce document suppose que l'authentification locale PPTP fonctionne avant d'ajouter le Cisco Secure ACS pour l'authentification de RAYON de Windows. Veuillez voir [comment configurer le concentrateur VPN 3000 PPTP avec l'authentification locale](#) pour plus d'informations sur l'authentification locale PPTP. Pour une liste complète de conditions requises et de restrictions, référez-vous s'il vous plaît [quand est le cryptage PPTP pris en charge sur un concentrateur de Cisco VPN 3000 ?](#)

Composants utilisés

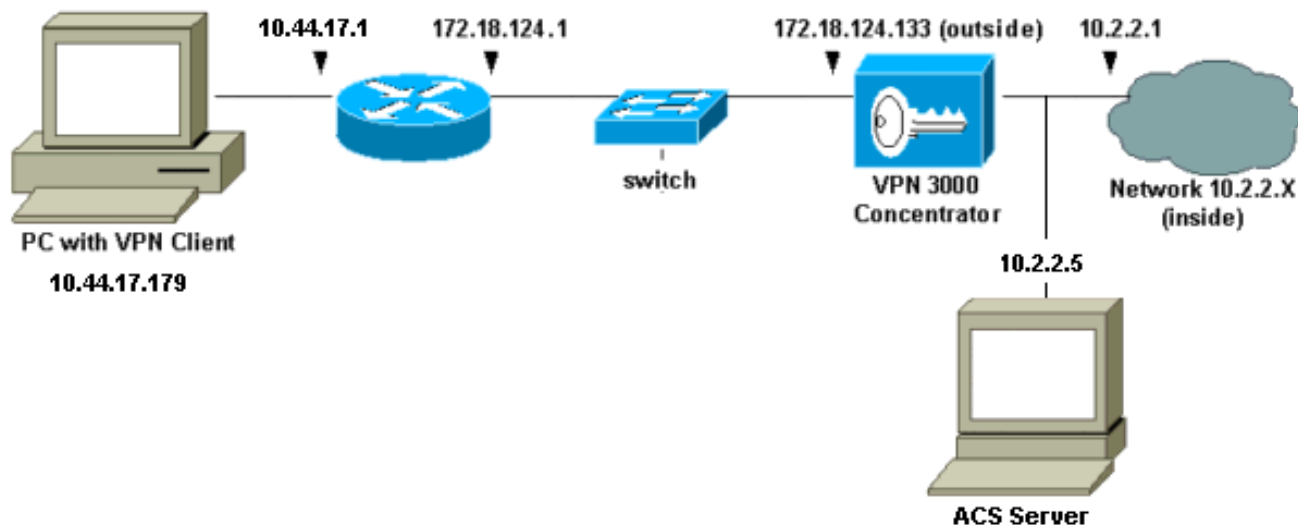
Les informations dans ce document sont basées sur les versions de logiciel et de matériel ci-dessous.

- Cisco Secure ACS pour des versions 2.5 et ultérieures de Windows
- Versions 2.5.2.C et ultérieures de concentrateur VPN 3000 (cette configuration a été vérifiée avec la version 4.0.x.)

Les informations présentées dans ce document ont été créées à partir de périphériques dans un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si vous travaillez dans un réseau opérationnel, assurez-vous de bien comprendre l'impact potentiel de toute commande avant de l'utiliser.

Diagramme du réseau

Ce document utilise la configuration réseau indiquée dans le diagramme suivant :

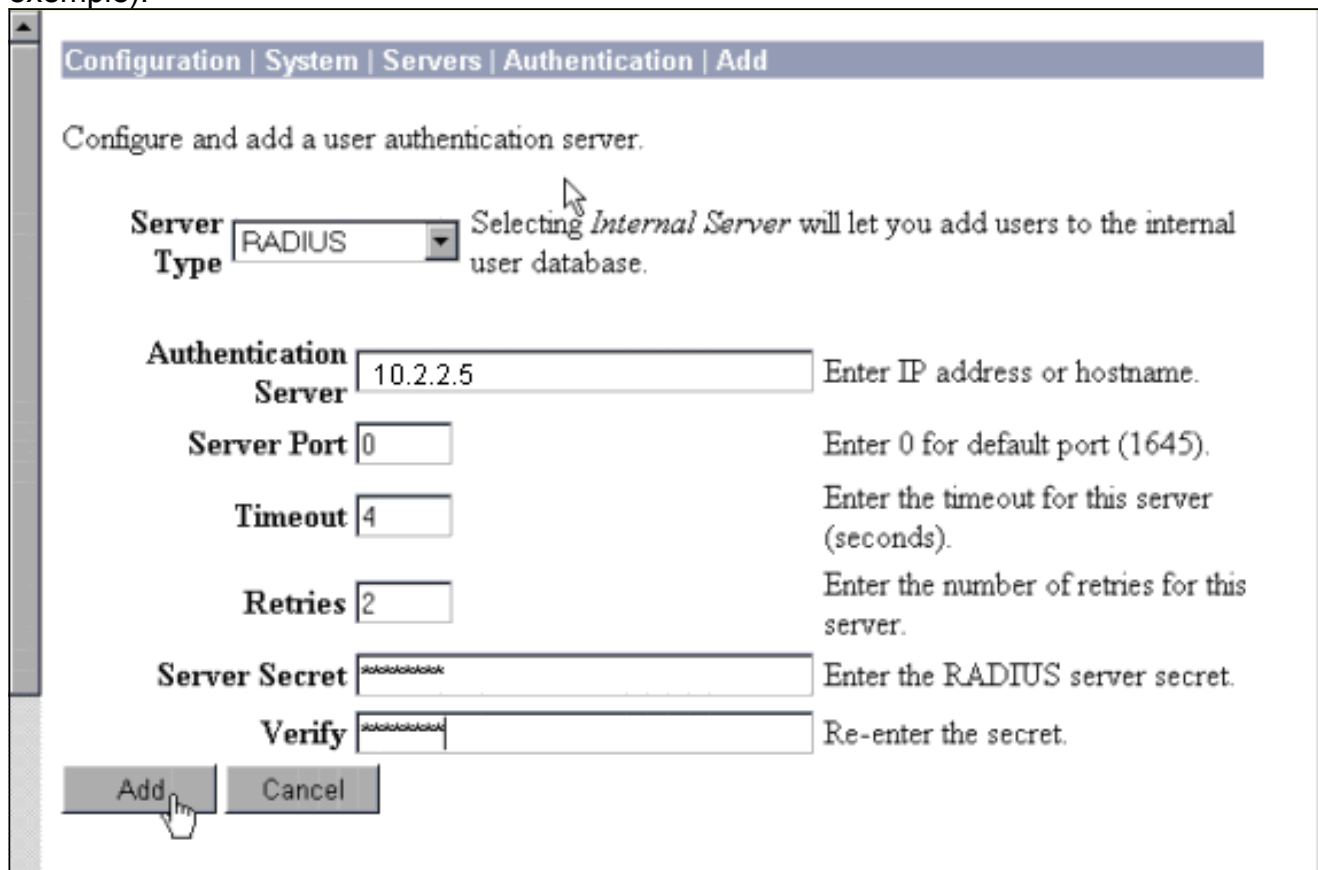


Configuration du concentrateur VPN 3000

[Ajoutant et configurant le Cisco Secure ACS pour Windows](#)

Suivez ces étapes pour configurer le concentrateur VPN pour utiliser le Cisco Secure ACS pour Windows.

1. Sur le concentrateur VPN 3000, allez à la **configuration > au système > aux serveurs > aux serveurs d'authentification** et ajoutez le Cisco Secure ACS pour des Windows Server et l'introduisez ("cisco123" dans cet exemple).



The screenshot shows a configuration window titled "Configuration | System | Servers | Authentication | Add". The main instruction is "Configure and add a user authentication server." The form includes the following fields and options:

- Server Type:** A dropdown menu set to "RADIUS". A tooltip indicates: "Selecting *Internal Server* will let you add users to the internal user database."
- Authentication Server:** A text box containing "10.2.2.5" with the instruction "Enter IP address or hostname."
- Server Port:** A text box containing "0" with the instruction "Enter 0 for default port (1645)."
- Timeout:** A text box containing "4" with the instruction "Enter the timeout for this server (seconds)."
- Retries:** A text box containing "2" with the instruction "Enter the number of retries for this server."
- Server Secret:** A masked text box with the instruction "Enter the RADIUS server secret."
- Verify:** A masked text box with the instruction "Re-enter the secret."

At the bottom, there are two buttons: "Add" (with a mouse cursor over it) and "Cancel".

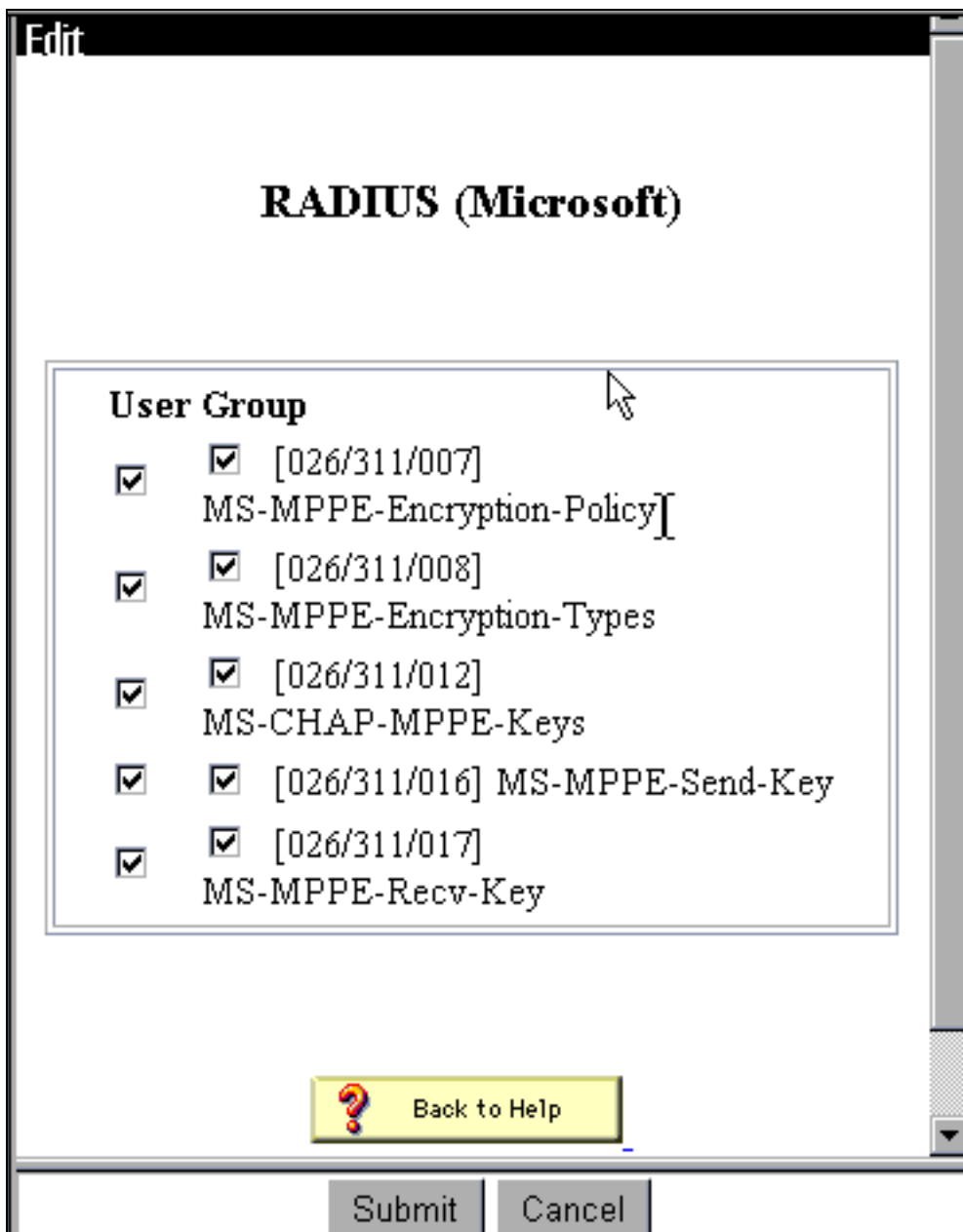
2. Dans le Cisco Secure ACS pour Windows, ajoutez le concentrateur VPN à la configuration réseau de serveur ACS, et identifiez le type de

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)"/>
<input type="checkbox"/>	Single Connect TACACS+ NAS (Record stop in accounting on failure).
<input type="checkbox"/>	Log Update/Watchdog Packets from this Access Server
<input type="checkbox"/>	Log Radius Tunneling Packets from this Access Server

dictionnaire.

3. Dans le Cisco Secure ACS pour Windows, allez à la **configuration d'interface** > au **RAYON (Microsoft)** et vérifiez les attributs point par point du cryptage de Microsoft (MPPE) de sorte que les attributs apparaissent dans l'interface de



groupe.

4. Dans le Cisco Secure ACS pour Windows, ajoutez un utilisateur. Dans le Groupe d'utilisateurs, ajoutez les attributs MPPE (RAYON de Microsoft), au cas où vous auriez besoin du cryptage à une date

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

ultérieure.

5. Sur le concentrateur VPN 3000, allez à la **configuration > au système > aux serveurs > aux serveurs d'authentification**. Sélectionnez un serveur d'authentification de la liste, et puis sélectionnez le **test**. Test d'authentification du concentrateur VPN au Cisco Secure ACS pour des Windows Server en écrivant un nom d'utilisateur et mot de passe. Sur une bonne authentification, le concentrateur VPN devrait afficher à une « authentification » le message réussi. Les pannes dans le Cisco Secure ACS pour Windows sont des **états et activité > des essais ratés** ouverts une session. Dans un par défaut installez, ces états sont enregistrés sur le disque dans des tentatives 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. Puisque vous avez maintenant vérifié l'authentification du PC aux travaux de concentrateur VPN et du concentrateur au Cisco Secure ACS pour des Windows Server, vous pouvez modifier le concentrateur VPN pour envoyer des utilisateurs PPTP au Cisco Secure ACS pour le RAYON de Windows en déplaçant le Cisco Secure ACS pour des Windows Server au dessus de la liste de serveur. Pour faire ceci sur le concentrateur VPN, allez à la **configuration > au système > aux serveurs > aux serveurs d'authentification.**

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. Allez au **Configuration > User Management > groupe de base** et sélectionnez l'onglet **PPTP/L2TP**. Dans le groupe de base de concentrateur VPN, assurez-vous que les options pour le PAP et le MSCHAPv1 sont activées.

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. Sélectionnez l'onglet **Général** et assurez-vous qu'on permet PPTP dans la section de protocoles de Tunnellisation.

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. Testez l'authentification PPTP avec l'utilisateur dans le Cisco Secure ACS pour le serveur de RAYON de Windows. [Si ceci ne fonctionne pas, satisfaire voyez la section de mise au point.](#)

[Ajoutant MPPE \(cryptage\)](#)

Si le Cisco Secure ACS pour l'authentification du RAYON PPTP de Windows fonctionne sans cryptage, vous pouvez ajouter le MPPE au concentrateur VPN 3000.

1. Sur le concentrateur VPN, allez au **Configuration > User Management > groupe de base**.
2. Sous la section pour le cryptage PPTP, vérifiez les options pour **requis, 40-bit, et 128-bit**. Puisque non tous les PC prennent en charge le cryptage 40-bit et 128-bit, vérifiez les deux options de tenir compte de la négociation.
3. Sous la section pour des Protocoles d'authentification PPTP, vérifiez l'option pour **MSCHAPv1**. (Vous avez déjà configuré le Cisco Secure ACS pour Windows 2.5 attributs d'utilisateur pour le cryptage dans une étape plus tôt.)

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.

Remarque: Le client PPTP devrait être identifié pour le chiffrement de données optimal ou prié et le MSCHAPv1 (si une option).

[Ajout de la comptabilité](#)

Après que vous ayez établi l'authentification, vous pouvez ajouter la comptabilité au concentrateur VPN. Allez à la **configuration > au système > aux serveurs > aux serveurs de comptabilité** et ajoutez le Cisco Secure ACS pour des Windows Server.

Dans le Cisco Secure ACS pour Windows, les enregistrements des comptes apparaissent comme suit.

```
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
```

[Vérifiez](#)

Aucune procédure de vérification n'est disponible pour cette configuration.

[Dépannez](#)

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

[Activation de l'élimination des imperfections](#)

Si les connexions ne fonctionnent pas, vous pouvez ajouter PPTP et les classes d'événement AUTHENTIQUES au concentrateur VPN en allant à la **configuration > au système > aux événements > aux classes > modifiant**. Vous pouvez également ajouter des classes d'événement PPTPDBG, PPTPDECODE, AUTHDBG, et AUTHDECODE, mais ces options peuvent fournir trop d'informations.

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.

Vous pouvez récupérer le journal d'événements en allant à la **surveillance > journal d'événements**.

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 - Bonne authentification](#)

Bon met au point sur le concentrateur VPN regardera semblable au suivant.

```

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

```

[Erreurs possibles](#)

Vous pouvez rencontrer des erreurs possibles comme affiché ci-dessous.

[Mauvais nom d'utilisateur ou mot de passe sur le Cisco Secure ACS pour le serveur de RAYON](#)

de Windows

- **Sortie de débogage de concentrateur VPN 3000**
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 pour la sortie de log de Windows**
03/18/2000,08:02:47,Authen failed,
baduser,,,CS user
unknown,,,1155,10.2.2.1
- **Le message que l'utilisateur voit (du 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.

Le « chiffrement MPPE exigé » est sélectionné sur le concentrateur, mais le Cisco Secure ACS pour des Windows Server n'est pas configuré pour des Ms-CHAP-MPPE-clés et des Ms-CHAP-MPPE-types

- **Sortie de débogage de concentrateur VPN 3000**
Si AUTHDECODE (sévérité 1-13) et PPTP
mettent au point (sévérité 1-9) sont allumés, le log prouvent que le Cisco Secure ACS pour
des Windows Server n'envoie pas la constructeur-particularité attribuent 26 (0x1A) dans
l'Access-recevoir du serveur (partie du journal).
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.
- **Le Cisco Secure ACS pour la sortie de log de Windows n'affiche aucune panne.**
- **Le message que l'utilisateur voit**
Error 691: The computer you have dialed in to has denied
access because
the username and/or password is invalid on the domain.

Informations connexes

- [Page d'assistance des concentrateurs VPN Cisco 3000](#)
- [Page d'assistance du Client VPN 3000 Series Cisco](#)
- [Page d'assistance IPsec](#)
- [Cisco Secure ACS pour la page d'assistance de Windows](#)
- [Page d'assistance RADIUS](#)

- [Page de support PPTP](#)
- [RFC 2637 : Protocole de tunnellation point à point \(PPTP\)](#)
- [Demandes de commentaires \(RFC\)](#)
- [Support et documentation techniques - Cisco Systems](#)