

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

Contenu

[Introduction](#)

[Avant de commencer](#)

[Conventions](#)

[Conditions préalables](#)

[Components Used](#)

[Diagramme du réseau](#)

[Configuration du concentrateur VPN 3000](#)

[Ajout et configuration de Cisco Secure ACS pour Windows](#)

[Ajout de MPPE \(Cryptage\)](#)

[Ajout de comptabilité](#)

[Vérification](#)

[Dépannage](#)

[Activation du débogage](#)

[Débogues - Authentification correcte](#)

[Erreurs possibles](#)

[Informations connexes](#)

[Introduction](#)

Le concentrateur Cisco VPN 3000 prend en charge la méthode de tunnellation PPTP (Point-to-Point Tunnel Protocol) pour les clients Windows natifs. Le concentrateur prend en charge le cryptage 40 bits et 128 bits pour une connexion sécurisée et fiable. Ce document décrit comment configurer PPTP sur un concentrateur VPN 3000 avec Cisco Secure ACS pour l'authentification RADIUS pour Windows.

Reportez-vous à [Configuration du pare-feu Cisco Secure PIX Firewall pour utiliser PPTP](#) pour configurer les connexions PPTP au PIX.

Référez-vous à [Configuration de Cisco Secure ACS pour l'authentification PPTP du routeur Windows](#) pour configurer une connexion PC au routeur ; ceci fournit l'authentification utilisateur au système de contrôle d'accès sécurisé Cisco (ACS) 3.2 pour le serveur Windows avant d'autoriser l'utilisateur à accéder au 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 PPTP locale fonctionne avant d'ajouter l'authentification Cisco Secure ACS pour Windows RADIUS. Consultez [Comment configurer le concentrateur VPN 3000 PPTP avec l'authentification locale](#) pour plus d'informations sur l'authentification PPTP locale. Pour obtenir une liste complète des exigences et restrictions, consultez [Quand le chiffrement PPTP est-il pris en charge sur un concentrateur VPN Cisco 3000 ?](#)

[Components Used](#)

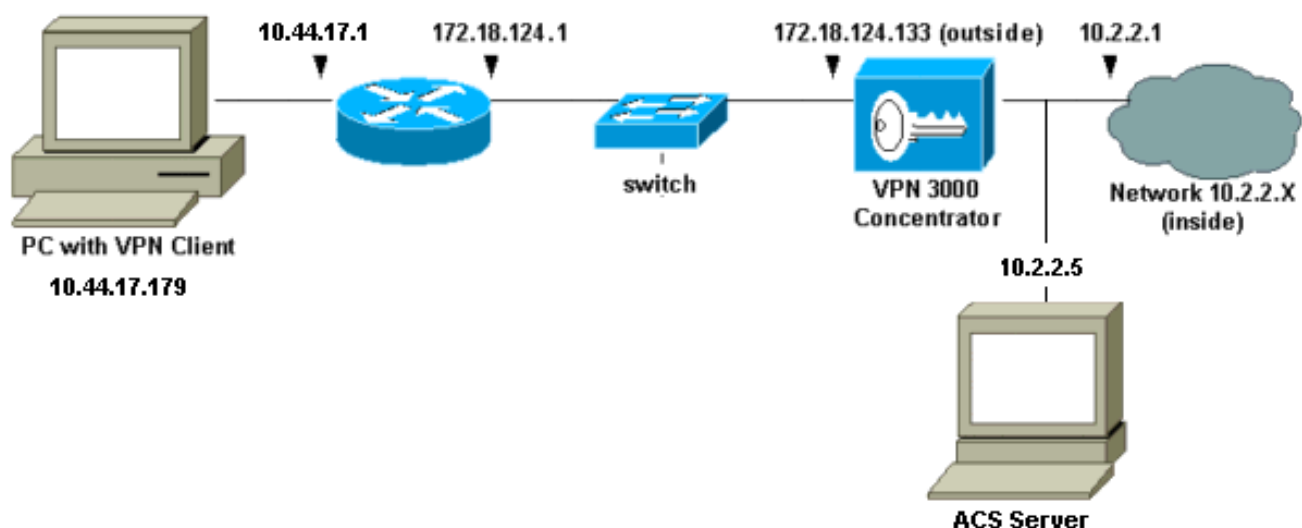
Les informations dans ce document sont basées sur les versions de logiciel et de matériel ci-dessous.

- Cisco Secure ACS pour Windows versions 2.5 et ultérieures
- VPN 3000 Concentrator versions 2.5.2.C et ultérieures (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. All of the devices used in this document started with a cleared (default) configuration. 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](#)

[Ajout et configuration de Cisco Secure ACS pour Windows](#)

Procédez comme suit pour configurer le concentrateur VPN afin qu'il utilise Cisco Secure ACS pour Windows.

1. Sur le concentrateur VPN 3000, accédez à **Configuration > System > Servers > Authentication Servers** et ajoutez le serveur et la clé Cisco Secure ACS pour Windows (« cisco123 » dans cet exemple).

The screenshot shows the configuration page for adding a user authentication server. The breadcrumb trail at the top is "Configuration | System | Servers | Authentication | Add". The page title is "Configure and add a user authentication server." 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." Below this, there are several input fields with their respective labels and instructions:

- Authentication Server:** 10.2.2.5 (Instruction: Enter IP address or hostname.)
- Server Port:** 0 (Instruction: Enter 0 for default port (1645).)
- Timeout:** 4 (Instruction: Enter the timeout for this server (seconds).)
- Retries:** 2 (Instruction: Enter the number of retries for this server.)
- Server Secret:** [masked] (Instruction: Enter the RADIUS server secret.)
- Verify:** [masked] (Instruction: Re-enter the secret.)

At the bottom, there are two buttons: "Add" and "Cancel". A mouse cursor is hovering over the "Add" button.

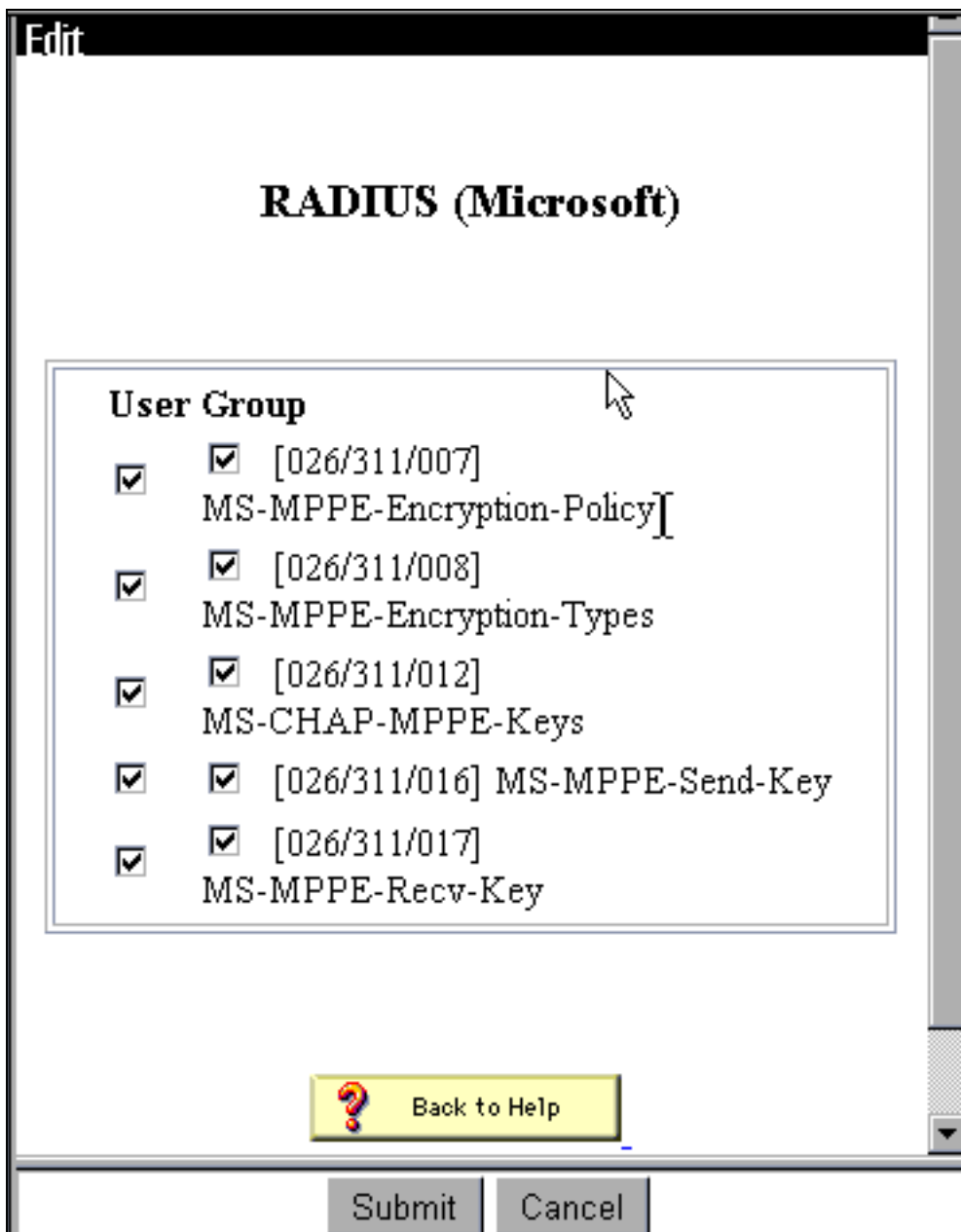
2. Dans Cisco Secure ACS pour Windows, ajoutez le concentrateur VPN à la configuration réseau du serveur ACS et identifiez le type de

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 Cisco Secure ACS pour Windows, accédez à **Configuration d'interface > RADIUS (Microsoft)** et vérifiez les attributs MPPE (Microsoft Point-to-Point Encryption) de sorte que les attributs apparaissent dans l'interface de



groupe.

4. Dans Cisco Secure ACS pour Windows, ajoutez un utilisateur. Dans le groupe de l'utilisateur, ajoutez les attributs MPPE (Microsoft RADIUS), au cas où vous auriez besoin d'un cryptage

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

ultérieur.

5. Sur le concentrateur VPN 3000, accédez à **Configuration > System > Servers > Authentication Servers**. Sélectionnez un serveur d'authentification dans la liste, puis sélectionnez **Test**. Testez l'authentification du concentrateur VPN vers le serveur Cisco Secure ACS pour Windows en entrant un nom d'utilisateur et un mot de passe. Sur une bonne authentification, le concentrateur VPN doit afficher un message « Authentication Success ». Les échecs de Cisco Secure ACS pour Windows sont consignés dans **Rapports et activité > Tentatives échouées**. Dans une installation par défaut, ces rapports sont stockés sur le disque dans 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. Puisque vous avez maintenant vérifié l'authentification du PC au concentrateur VPN fonctionne et du concentrateur au serveur Cisco Secure ACS pour Windows, vous pouvez reconfigurer le concentrateur VPN pour envoyer des utilisateurs PPTP à Cisco Secure ACS pour Windows RADIUS en plaçant le serveur Cisco Secure ACS pour Windows en haut de la liste des serveurs. Pour ce faire sur le concentrateur VPN, accédez à **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)  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. Accédez à **Configuration > User Management > Base Group** et sélectionnez l'onglet **PPTP/L2TP**. Dans le groupe de base du concentrateur VPN, assurez-vous que les options pour PAP et MSCHAPv1 sont activées.

Configuration | User Management | Base Group

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 que PPTP est autorisé dans la section 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. Testez l'authentification PPTP avec l'utilisateur dans le serveur Cisco Secure ACS pour Windows RADIUS. Si cela ne fonctionne pas, consultez la section [Débogage](#).

[Ajout de MPPE \(Cryptage\)](#)

Si l'authentification PPTP Cisco Secure ACS pour Windows RADIUS fonctionne sans chiffrement, vous pouvez ajouter MPPE au concentrateur VPN 3000.

1. Sur le concentrateur VPN, accédez à **Configuration > User Management > Base Group**.
2. Dans la section relative au cryptage PPTP, cochez les options **Required**, **40-bit** et **128-bit**. Comme tous les PC ne prennent pas en charge le cryptage 40 bits et 128 bits, cochez les deux options pour autoriser la négociation.
3. Sous la section Protocoles d'authentification PPTP, cochez l'option pour **MSCHAPv1**. (Vous avez déjà configuré les attributs utilisateur de Cisco Secure ACS pour Windows 2.5 pour le chiffrement à une étape antérieure.)

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 doit être reconnu pour le chiffrement optimal ou obligatoire des données et MSCHAPv1 (si une option est disponible).

Ajout de comptabilité

Une fois l'authentification établie, vous pouvez ajouter la comptabilité au concentrateur VPN. Accédez à **Configuration > System > Servers > Accounting Servers** et ajoutez le serveur Cisco Secure ACS pour Windows.

Dans Cisco Secure ACS pour Windows, les enregistrements comptables 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
```

Vérification

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

Dépannage

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

[Activation du débogage](#)

Si les connexions ne fonctionnent pas, vous pouvez ajouter des classes d'événements PPTP et AUTH au concentrateur VPN en accédant à **Configuration > System > Events > Classes > Modify**. Vous pouvez également ajouter des classes d'événements 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 des événements en accédant à **Surveillance > Journal des 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

```

[Débugues - Authentification correcte](#)

Les bons débugages sur le concentrateur VPN ressembleront aux suivants.

```

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](#)

Il se peut que vous rencontriez des erreurs, comme indiqué ci-dessous.

[Nom d'utilisateur ou mot de passe incorrect sur le serveur Cisco Secure ACS pour Windows RADIUS](#)

- Sortie de débogage du concentrateur VPN 3000

```
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
```

- Sortie du journal Cisco Secure ACS pour Windows

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

- Message que l'utilisateur voit (depuis 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.
```

« Cryptage MPPE requis » est sélectionné sur le concentrateur, mais le serveur Cisco Secure ACS pour Windows n'est pas configuré pour MS-CHAP-MPPE-Keys et MS-CHAP-MPPE-Types

- Sortie de débogage du concentrateur VPN 3000Si AUTHDECODE (1-13 Severity) et PPTP debug (1-9 Severity) sont activés, le journal indique que le serveur Cisco Secure ACS pour Windows n'envoie pas l'attribut 26 (0x1A) spécifique au fournisseur dans le access-accept du serveur (journal partiel).

```
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 sortie du journal Cisco Secure ACS pour Windows ne montre aucune défaillance.
- 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](#)