

如何使用本地身份驗證配置VPN 3000集中器 PPTP

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[網路圖表](#)

[慣例](#)

[使用本地身份驗證配置VPN 3000集中器](#)

[Microsoft PPTP客戶端配置](#)

[Windows 98 — 安裝和配置PPTP功能](#)

[Windows 2000 — 配置PPTP功能](#)

[Windows NT](#)

[Windows Vista](#)

[新增MPPE \(加密 \)](#)

[驗證](#)

[驗證VPN集中器](#)

[檢驗PC](#)

[調試](#)

[VPN 3000偵錯 — 良好驗證](#)

[疑難排解](#)

[須排解的Microsoft可能問題](#)

[相關資訊](#)

簡介

Cisco VPN 3000集中器支援本地Windows客戶端的點對點隧道協定(PPTP)隧道方法。這些VPN集中器提供40位和128位加密支援，以實現安全的可靠連線。

請參閱[使用適用於Windows RADIUS身份驗證的Cisco Secure ACS配置VPN 3000集中器PPTP](#)，以使用思科安全訪問控制伺服器(ACS)為使用擴展身份驗證的PPTP使用者配置VPN集中器。

必要條件

需求

確保滿足[Cisco VPN 3000集中器何時支援PPTP加密？](#)，然後再嘗試此配置。

採用元件

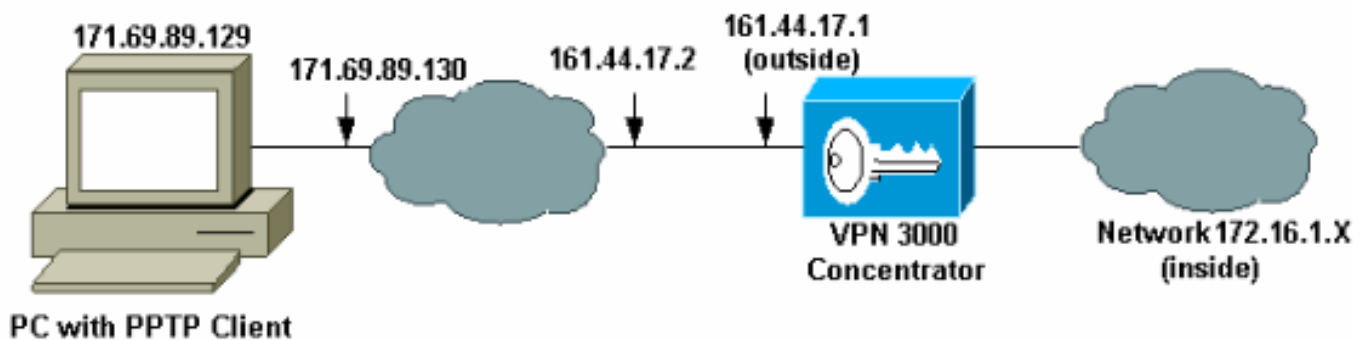
本文中的資訊係根據以下軟體和硬體版本：

- 4.0.4.A版的VPN 3015集中器
- 帶PPTP客戶端的Windows PC

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

網路圖表

本檔案會使用以下網路設定：



慣例

請參閱[思科技術提示慣例](#)以瞭解更多有關文件慣例的資訊。

使用本地身份驗證配置VPN 3000集中器

完成以下步驟，使用本地身份驗證配置VPN 3000集中器。


1. 在VPN集中器中配置各自的IP地址，並確保您已建立連線。
2. 確保在Configuration > User Management > Base Group PPTP/L2TP頁籤中選擇PAP身份驗證。

Configuration User Management Base Group		
General IPSec Client Config Client FW HW Client 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 checked="" type="checkbox"/> CHAP <input checked="" type="checkbox"/> MSCHAPv1 <input type="checkbox"/> MSCHAPv2 <input type="checkbox"/> EAP Proxy	Check the authentication protocols allowed. Refer to the online help for authentication protocol dependencies. Unchecking all options means that no 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.
PPTP Compression	<input type="checkbox"/>	Check to enable MPPC compression for PPTP connections for this group.

3. 選擇 Configuration > System > Tunneling Protocols > PPTP，並確保選中 Enabled。

Configuration | System | Tunneling Protocols | PPTP

This section lets you configure system-wide PPTP (Point-to-Point Tunneling Protocol) options.

 Disabling PPTP will terminate any active PPTP sessions.

Enabled

Maximum Tunnel Idle Time seconds

Packet Window Size packets

Limit Transmit to Window Check to limit the transmitted packets based on the peer's receive window.

Max. Tunnels Enter 0 for unlimited tunnels.

Max. Sessions/Tunnel Enter 0 for unlimited sessions.

Packet Processing Delay 10^{ths} of seconds

Acknowledgement Delay milliseconds

Acknowledgement Timeout seconds

4. 選擇 Configuration > User Management > Groups > Add，然後配置 PPTP 組。在本例中，組名為「pptpgroup」，密碼（和驗證密碼）為「cisco123」。

Configuration | User Management | Groups | Add

This section lets you add a group. Check the **Inherit?** box to set a field that you want to default to the base group value. Uncheck the **Inherit?** box and enter a new value to override base group values.

Identity | General | IPsec | Mode Config | Client FW | HW Client | PPTP/L2TP

Identity Parameters

Attribute	Value	Description
Group Name	<input type="text" value="pptpgroup"/>	Enter a unique name for the group.
Password	<input type="text" value="*****"/>	Enter the password for the group.
Verify	<input type="text" value="*****"/>	Verify the group's password.
Type	<input type="text" value="Internal"/>	<i>External</i> groups are configured on an external authentication server (e.g. RADIUS). <i>Internal</i> groups are configured on the VPN 3000 Concentrator's Internal Database.

5. 在組的 General 頁籤下，確保在身份驗證協定中啟用 PPTP 選項。

General Parameters

Attribute	Value	Description
Access Hours	-No Restrictions-	Select the access hours for this group.
Simultaneous Logins	3	Enter the number of simultaneous logins for users in this group.
Minimum Password Length	8	Enter the minimum password length for users in this group.
Allow Alphabetic-Only Passwords	<input checked="" type="checkbox"/>	Enter whether to allow users with alphabetic-only passwords to be added to this group.
Idle Timeout	30	(minutes) Enter the idle timeout for this group.
Maximum Connect time	0	(minutes) Enter the maximum connect time for this group.
Filter	-None-	Select the filter assigned to this group.
Primary DNS		Enter the IP address of the primary DNS server for this group.
Secondary DNS		Enter the IP address of the secondary DNS server.
Primary WINS		Enter the IP address of the primary WINS server for this group.
Secondary WINS		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.
Strip Realm	<input type="checkbox"/>	Check to remove the realm qualifier of the username during authentication.
DHCP Network Scope		Enter the IP sub-network to which users within this group will be assigned when using the concentrator as a DHCP Proxy.

Apply Cancel

6. 在PPTP/L2TP頁籤下，啟用PAP身份驗證並禁用加密（加密可以在將來任何時間啟用）。

Check the **Inherit?** box to set a field that you want to default to the base group value. Uncheck the **Inherit?** box and enter a new value to override base group values.

Identity General IPsec Client Config Client FW HW Client PPTP/L2TP

PPTP/L2TP Parameters			
Attribute	Value	Inherit?	Description
Use Client Address	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Check to accept and use an IP address received from the client.
PPTP Authentication Protocols	<input checked="" type="checkbox"/> PAP <input checked="" type="checkbox"/> CHAP <input checked="" type="checkbox"/> MSCHAPv1 <input type="checkbox"/> MSCHAPv2 <input type="checkbox"/> EAP Proxy	<input checked="" type="checkbox"/>	Check the authentication protocols allowed by this group. The choices available are determined by base group settings. Refer to the online help for authentication protocol dependencies. 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 type="checkbox"/> 40-bit <input type="checkbox"/> 128-bit	<input type="checkbox"/>	Select the allowed encryption methods for PPTP connections for this group.
PPTP Compression	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Check to enable compression for PPTP connections for this group.

7. 選擇 Configuration > User Management > Users > Add，然後使用口令 cisco123 for PPTP 身份驗證配置本地使用者（稱為「pptpuser」）。將使用者置於先前定義的「pptpgroup」中：

This section lets you add a user. Uncheck the **Inherit?** box and enter a new value to override group values.

Identity General IPsec PPTP/L2TP

Identity Parameters		
Attribute	Value	Description
User Name	<input type="text" value="pptpuser"/>	Enter a unique user name.
Password	<input type="password" value="*****"/>	Enter the user's password. The password must satisfy the group password requirements.
Verify	<input type="password" value="*****"/>	Verify the user's password.
Group	<input type="text" value="pptpgroup"/> ▼	Enter the group to which this user belongs.
IP Address	<input type="text"/>	Enter the IP address assigned to this user.
Subnet Mask	<input type="text"/>	Enter the subnet mask assigned to this user.

8. 在使用者的 General 頁籤下，確保在隧道協定中啟用 PPTP 選項。

Check the **Inherit?** box to set a field that you want to default to the group value. Uncheck the **Inherit?** box and enter a new value to override group values.

Identity General IPsec PPTP/L2TP

General Parameters

Attribute	Value	Inherit?	Description
Access Hours	-No Restrictions-	<input checked="" type="checkbox"/>	Select the access hours assigned to this user.
Simultaneous Logins	3	<input checked="" type="checkbox"/>	Enter the number of simultaneous logins for this user.
Idle Timeout	30	<input checked="" type="checkbox"/>	(minutes) Enter the idle timeout for this user.
Maximum Connect Time	0	<input checked="" type="checkbox"/>	(minutes) Enter the maximum connect time for this user.
Filter	-None-	<input checked="" type="checkbox"/>	Enter the filter assigned to this user.
Tunneling Protocols	<input checked="" type="checkbox"/> PPTP <input checked="" type="checkbox"/> L2TP <input checked="" type="checkbox"/> IPsec <input type="checkbox"/> L2TP over IPsec	<input checked="" type="checkbox"/>	Select the tunneling protocols this user can connect with.

Apply

Cancel

9. 選擇 Configuration > System > Address Management > Pools 以定義地址管理的地址池。

This section lets you configure IP Address Pools.

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

IP Pool Entry

172.16.1.10 - 172.16.1.20

Actions

Add

Modify

Delete

Move Up

Move Down

10. 選擇 Configuration > System > Address Management > Assignment，並指示VPN集中器使用地址池。

This section presents Address Assignment options. Each of the following methods are tried, in order, until an address is found.

- Use Client Address** Check to use the IP address supplied by the client. This can be overridden by user/group configuration.
- Use Address from Authentication Server** Check to use an IP address retrieved from an authentication server for the client.
- Use DHCP** Check to use DHCP to obtain an IP address for the client.
- Use Address Pools** Check to use internal address pool configuration to obtain an IP address for the client.

Apply

Cancel

Microsoft PPTP客戶端配置

注意：此處提供的有關配置Microsoft軟體的任何資訊均未提供Microsoft軟體的任何保修或支援。
[Microsoft](#) 支援Microsoft軟體。

Windows 98 — 安裝和配置PPTP功能

安裝

完成以下步驟以安裝PPTP功能。

1. 選擇**開始>設定>控制面板>新增新硬體 (下一步)>從清單中選擇>網路介面卡 (下一步)**。
2. 在左側面板中選擇**Microsoft**，在右側面板中選擇**Microsoft VPN Adapter**。

設定

完成以下步驟以配置PPTP功能。

1. 選擇**Start > Programs > Accessories > Communications > Dial Up Networking > Make new connection**。
2. 在Select a device提示符下使用Microsoft VPN介面卡連線。VPN伺服器IP是3000隧道端點。Windows 98預設身份驗證使用密碼加密 (例如CHAP或MSCHAP)。要最初禁用此加密，請選擇**Properties > Server types**，然後取消選中**Encrypted Password**和**Require Data Encryption**框。

Windows 2000 — 配置PPTP功能

完成以下步驟以配置PPTP功能。

1. 選擇**Start > Programs > Accessories > Communications > Network and Dialup connections > Make new connection**。
2. 按一下**Next**，然後選擇**Connect to a private network through the Internet > Dial a connection previous (如果使用LAN，則不要選擇此選項)**。

3. 再次按一下**Next**，輸入隧道端點（VPN 3000集中器的外部介面）的主機名或IP。在本示例中，IP地址為161.44.17.1。

選擇**Properties > Security for the connection > Advanced**將密碼型別新增為PAP。預設值為MSCHAP和MSCHAPv2，而不是CHAP或PAP。

資料加密可在此區域中配置。您可以先將其禁用。

Windows NT

您可以在Microsoft的網站上訪問有關為PPTP設定Windows NT [客戶端的資訊](#)。

Windows Vista

完成以下步驟以配置PPTP功能。

1. 在**Start**按鈕中選擇**Connect To**。
2. 選擇**設定連線或網路**。
3. 選擇**連線到工作區**，然後按一下**下一步**。
4. 選擇**Use my Internet Connection(VPN)**。注意：如果系統提示「是否要使用已有的連線」，請選擇**否**，建立一個新連線，然後單擊「**下一步**」。
5. 例如，在「**Internet Address**」欄位中鍵入pptp.vpn.univ.edu。
6. 例如，在**Destination Name**欄位中，鍵入UNIVVPN。
7. 在**User Name**欄位中，鍵入您的UNIV登入ID。您的UNIV登入ID是@univ.edu之前的電子郵件地址的一部分。
8. 在「**Password**」欄位中，輸入您的UNIV登入ID密碼。
9. 按一下**Create**按鈕，然後按一下**Close**按鈕。
10. 要在建立VPN連線後連線到VPN伺服器，請按一下「**開始**」，然後按一下「**連線到**」。
11. 在視窗中選擇VPN連線，然後按一下**Connect**。

新增MPPE (加密)

新增加密之前，請確保PPTP連線在不加密的情況下正常工作。例如，按一下PPTP客戶端上的**Connect**按鈕以確保連線完成。如果您決定要求加密，則必須使用MSCHAP身份驗證。在VPN 3000上，選擇**Configuration > User Management > Groups**。然後，在組的PPTP/L2TP頁籤下，取消選中PAP，選中MSCHAPv1，並選中PPTP加密所需。

Check the **Inherit?** box to set a field that you want to default to the base group value. Uncheck the **Inherit?** box and enter a new value to override base group values.

Identity General IPsec Client Config Client FW HW Client PPTP/L2TP

PPTP/L2TP Parameters

Attribute	Value	Inherit?	Description
Use Client Address	<input type="checkbox"/>	<input checked="" 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 checked="" type="checkbox"/> MSCHAPv1 <input type="checkbox"/> MSCHAPv2 <input type="checkbox"/> EAP Proxy	<input type="checkbox"/>	Check the authentication protocols allowed by this group. The choices available are determined by base group settings. Refer to the online help for authentication protocol dependencies. Unchecking <i>all</i> options means that <i>no</i> 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	<input type="checkbox"/>	Select the allowed encryption methods for PPTP connections for this group.
PPTP Compression	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Check to enable compression for PPTP connections for this group.

PPTP客戶端應重新配置為可選或必需的資料加密和MSCHAPv1（如果是一個選項）。

驗證

本節提供的資訊可用於確認您的組態是否正常運作。

驗證VPN集中器

您可以從[Microsoft PPTP客戶端配置](#)部分中以前建立的PPTP客戶端撥號，以啟動PPTP會話。

使用VPN集中器上的「管理」>「管理會話」視窗檢視所有活動PPTP會話的引數和統計資訊。

檢驗PC

在PC的命令模式下發出`ipconfig`命令，以檢視PC具有兩個IP地址。一個是自己的IP地址，另一個由VPN集中器從IP地址池中分配。在本示例中，IP地址172.16.1.10是由VPN集中器分配的IP地址。

```
C:\WINNT\system32\cmd.exe
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\Documents and Settings\Administrator>ipconfig

Windows 2000 IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . .               : 171.69.89.129
    Subnet Mask . . . . .             : 255.255.255.0
    Default Gateway . . . . .         : 171.69.89.130

PPP adapter pptpuser:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . .               : 172.16.1.10
    Subnet Mask . . . . .             : 255.255.255.255
    Default Gateway . . . . .         : 172.16.1.10

C:\Documents and Settings\Administrator>
```

調試

如果連線不起作用，則可以將PPTP事件類調試新增到VPN集中器。選擇**Configuration > System > Events > Classes > Modify**或**Add**（如此處所示）。PPTPDBG和PPTPDCODE事件類也可用，但可能提供太多資訊。

The screenshot shows the 'Add' dialog box in the Windows Event Viewer. The title bar reads 'Configuration | System | Events | Classes | Add'. The main text says: 'This screen lets you add and configure an event class for special handling.' Below this, there are several configuration options:

- Class Name:** A dropdown menu with 'PPTP' selected. Description: 'Select the event class to configure.'
- Enable:** A checked checkbox. Description: 'Check to enable special handling of this class.'
- Severity to Log:** A dropdown menu with '1-13' selected. Description: 'Select the range of severity values to enter in the log.'
- Severity to Console:** A dropdown menu with '1-3' selected. Description: 'Select the range of severity values to display on the console.'
- Severity to Syslog:** A dropdown menu with 'None' selected. Description: 'Select the range of severity values to send to a Syslog server.'
- Severity to Email:** A dropdown menu with 'None' selected. Description: 'Select the range of severity values to send via email to the recipient list.'
- Severity to Trap:** A dropdown menu with 'None' selected. Description: 'Select the range of severity values to send to an SNMP system.'

At the bottom of the dialog, there are two buttons: 'Add' and 'Cancel'.

可從**Monitoring > Filterable Event Log**中檢索事件日誌。

Select Filter Options

Event Class	<input type="text" value="All Classes"/> AUTH AUTHDBG AUTHDECODE	Severities	<input type="text" value="ALL"/> 1 2 3
Client IP Address	<input type="text" value="0.0.0.0"/>	Events/Page	<input type="text" value="100"/>
Group	<input type="text" value="-All-"/>	Direction	<input type="text" value="Oldest to Newest"/>

```
1 09/30/2004 09:34:05.550 SEV=4 PPTP/47 RPT=10 171.69.89.129
Tunnel to peer 171.69.89.129 established

2 09/30/2004 09:34:05.550 SEV=4 PPTP/42 RPT=10 171.69.89.129
Session started on tunnel 171.69.89.129

3 09/30/2004 09:34:08.750 SEV=5 PPP/8 RPT=8 171.69.89.129
User [pptpuser]
Authenticated successfully with PAP

4 09/30/2004 09:34:12.590 SEV=4 AUTH/22 RPT=6
User [pptpuser] Group [pptpgroup] connected, Session Type: PPTP
```

[VPN 3000偵錯 — 良好驗證](#)

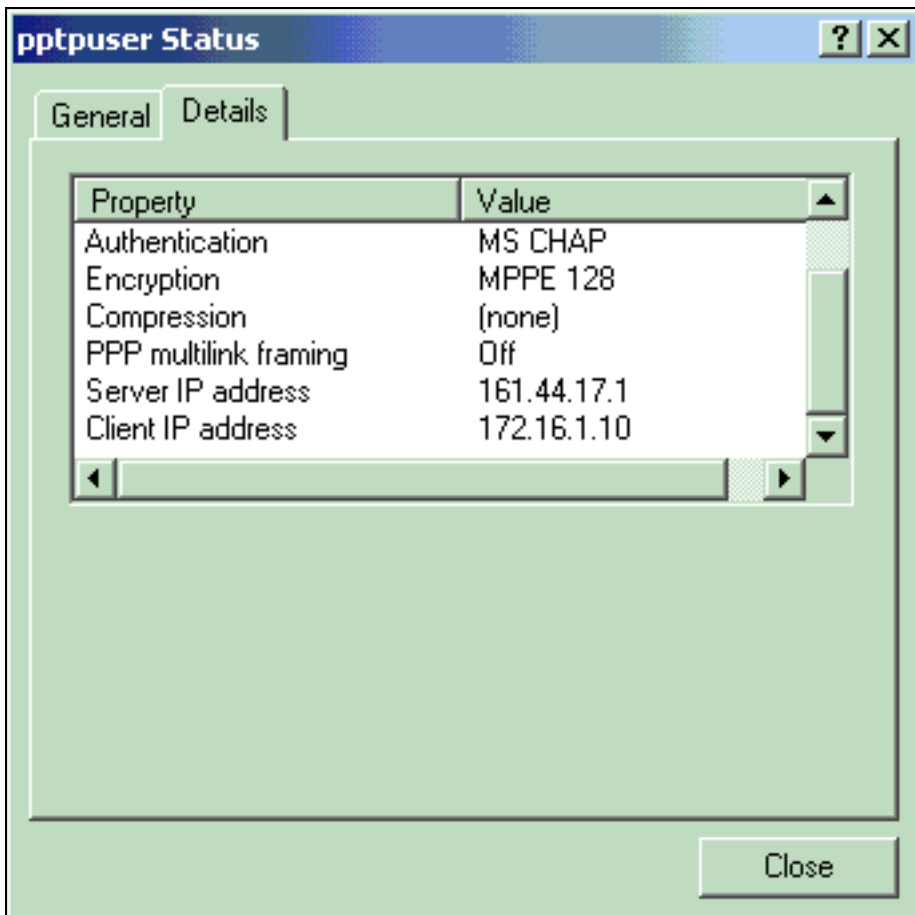
```
1 09/28/2004 21:36:52.800 SEV=4 PPTP/47 RPT=29 171.69.89.129
Tunnel to peer 171.69.89.129 established

2 09/28/2004 21:36:52.800 SEV=4 PPTP/42 RPT=29 171.69.89.129
Session started on tunnel 171.69.89.129

3 09/28/2004 21:36:55.910 SEV=5 PPP/8 RPT=22 171.69.89.129
User [pptpuser]
Authenticated successfully with MSCHAP-V1

4 09/28/2004 21:36:59.840 SEV=4 AUTH/22 RPT=22
User [pptpuser] Group [Base Group] connected, Session Type: PPTP
```

按一下PPTP user status **Details**視窗檢查Windows PC上的引數。



疑難排解

您可能會遇到以下錯誤：

- 使用者名稱或密碼不正確VPN 3000 Concentrator調試輸出：

```

1 09/28/2004 22:08:23.210 SEV=4 PPTP/47 RPT=44 171.69.89.129
  Tunnel to peer 171.69.89.129 established

2 09/28/2004 22:08:23.220 SEV=4 PPTP/42 RPT=44 171.69.89.129
  Session started on tunnel 171.69.89.129

3 09/28/2004 22:08:26.330 SEV=3 AUTH/5 RPT=11 171.69.89.129
  Authentication rejected: Reason = User was not found
  handle = 44, server = (none), user = pptpusers, domain = <not specified>

5 09/28/2004 22:08:26.330 SEV=5 PPP/9 RPT=11 171.69.89.129
  User [pptpusers]
  disconnected.. failed authentication ( MSCHAP-V1 )

6 09/28/2004 22:08:26.340 SEV=4 PPTP/35 RPT=44 171.69.89.129
  Session closed on tunnel 171.69.89.129 (peer 32768, local 22712, serial 40761),
  reason: Error (No additional info)

8 09/28/2004 22:08:26.450 SEV=4 PPTP/34 RPT=44 171.69.89.129
  Tunnel to peer 171.69.89.129 closed, reason: None (No additional info)

```

使用者看到的消息 (來自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.

使用者看到的消息 (來自Windows 2000)：

Error 691: Access was denied because the username and/or password was invalid on the domain.

- 在PC上選擇「需要加密」，但在VPN集中器上未選擇使用者看到的消息（來自Windows 98）：

Error 742: The computer you're dialing in to does not support the data encryption requirements specified.
Please check your encryption settings in the properties of the connection.
If the problem persists, contact your network administrator.

使用者看到的消息（來自Windows 2000）：

Error 742: The remote computer does not support the required data encryption type

- 在僅支援40位加密的PC的VPN集中器上選擇「需要加密」（128位）VPN 3000 Concentrator調試輸出：

4 12/05/2000 10:02:15.400 SEV=4 PPP/6 RPT=7 171.69.89.129 User [pptpuser] disconnected.
PPTP Encryption configured as REQUIRED.. remote client not supporting it.

使用者看到的消息（來自Windows 98）：

Error 742: The remote computer does not support the required data encryption type.

使用者看到的消息（來自Windows 2000）：

Error 645 Dial-Up Networking could not complete the connection to the server.
Check your configuration and try the connection again.

- VPN 3000集中器配置了MSCHAPv1,PC配置了PAP，但他們無法就身份驗證方法達成一致VPN 3000 Concentrator調試輸出：

8 04/22/2002 14:22:59.190 SEV=5 PPP/12 RPT=1 171.69.89.129

User [pptpuser] disconnected. Authentication protocol not allowed.

使用者看到的消息（來自Windows 2000）：

Error 691: Access was denied because the username and/or password was invalid on the domain.

須排解的Microsoft可能問題

- 如何在註銷後保持RAS連線處於活動狀態從Windows遠端訪問服務(RAS)客戶端註銷時，所有RAS連線都會自動斷開連線。在RAS客戶端上的登錄檔中啟用KeepRasConnections項，以便在註銷後保持連線。有關詳細資訊，請參閱[Microsoft知識庫文章 - 158909。](#)
- 使用快取憑據登入時不會提示使用者此問題的症狀是：當您嘗試從基於Windows的工作站或成員伺服器登入到域時，找不到域控制器，並且未顯示錯誤消息。而是使用快取的憑據登入到本地電腦。有關詳細資訊，請參閱[Microsoft知識庫文章 - 242536。](#)
- 如何針對域驗證和其他名稱解析問題編寫LMHOSTS檔案在某些情況下，您的TCP/IP網路上會遇到名稱解析問題，您需要使用LMHOSTS檔案來解析NetBIOS名稱。本文討論用於建立LMHOSTS檔案以幫助進行名稱解析和域驗證的正確方法。有關詳細資訊，請參閱[Microsoft知識庫文章 - 180094。](#)

相關資訊

- [RFC 2637:點對點通道通訊協定\(PPTP\)](#)
- [適用於Windows的Cisco Secure ACS支援頁面](#)
- [Cisco VPN 3000集中器何時支援PPTP加密？](#)
- [為Windows RADIUS身份驗證配置VPN 3000集中器和PPTP](#)
- [Cisco VPN 3000集中器支援頁](#)
- [Cisco VPN 3000客戶端支援頁](#)
- [IP安全\(IPSec\)產品支援頁面](#)
- [PPTP產品支援頁面](#)

- [技術支援與文件 - Cisco Systems](#)