

Come configurare VPN 3000 Concentrator PPTP con autenticazione locale

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Esempio di rete](#)

[Convenzioni](#)

[Configurazione di VPN 3000 Concentrator con autenticazione locale](#)

[Configurazione client PPTP Microsoft](#)

[Windows 98 - Installazione e configurazione della funzionalità PPTP](#)

[Windows 2000 - Configurazione della funzionalità PPTP](#)

[Windows NT](#)

[Windows Vista](#)

[Aggiungi MPPE \(crittografia\)](#)

[Verifica](#)

[Verifica di VPN Concentrator](#)

[Verifica il PC](#)

[Debug](#)

[Debug VPN 3000 - Buona autenticazione](#)

[Risoluzione dei problemi](#)

[Possibili problemi Microsoft da risolvere](#)

[Informazioni correlate](#)

[Introduzione](#)

Cisco VPN 3000 Concentrator supporta il metodo di tunneling PPTP (Point-to-Point Tunnel Protocol) per client Windows nativi. Su questi concentratori VPN è disponibile il supporto della crittografia a 40 bit e a 128 bit per una connessione sicura e affidabile.

Per configurare il concentratore VPN per utenti PPTP con autenticazione estesa, fare riferimento alla sezione [Configurazione del concentratore VPN 3000](#) con [Cisco Secure ACS per l'autenticazione RADIUS di Windows](#) (ACS).

[Prerequisiti](#)

[Requisiti](#)

Verificare che siano soddisfatti i prerequisiti indicati in [Quando la crittografia PPTP è supportata su un concentratore Cisco VPN 3000?](#) prima di provare la configurazione.

Componenti usati

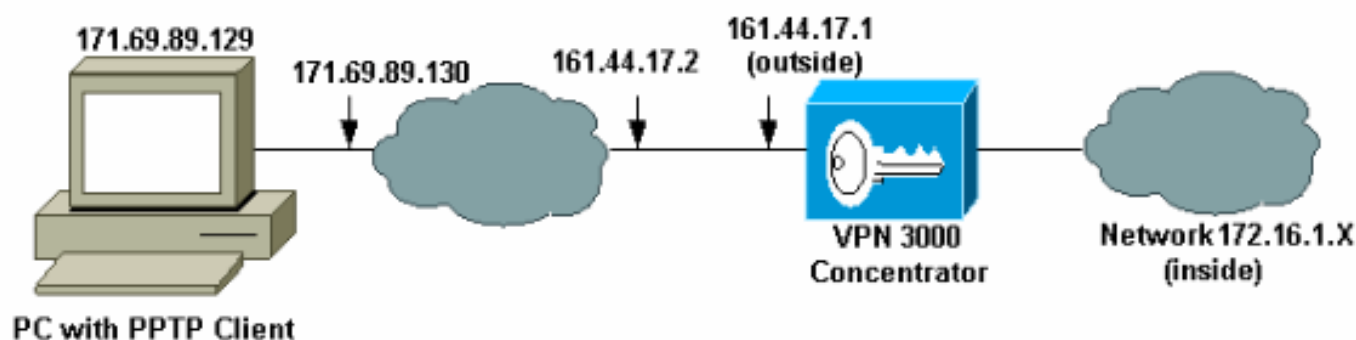
Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- VPN 3015 Concentrator con versione 4.0.4.A
- PC Windows con client PPTP

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Esempio di rete

Nel documento viene usata questa impostazione di rete:



Convenzioni

Fare riferimento a [Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti.](#)


Configurazione di VPN 3000 Concentrator con autenticazione locale

Completare la procedura seguente per configurare VPN 3000 Concentrator con autenticazione locale.

1. Configurare i rispettivi indirizzi IP in VPN Concentrator e verificare la presenza di connettività.
2. Verificare che l'**autenticazione PAP** sia selezionata nella scheda **Configurazione > Gestione utente > Gruppo di base PPTP/L2TP**.

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 <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.
PPTP Compression	<input type="checkbox"/>	Check to enable MPPC compression for PPTP connections for this group.

3. Selezionare **Configurazione > Sistema > Protocolli di tunneling > PPTP** e verificare che **Abilitato** sia selezionato.

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 <input checked="" type="checkbox"/>	
Maximum Tunnel Idle Time	<input type="text" value="5"/> seconds
Packet Window Size	<input type="text" value="16"/> packets
Limit Transmit to Window	<input type="checkbox"/> Check to limit the transmitted packets based on the peer's receive window.
Max. Tunnels	<input type="text" value="0"/> Enter 0 for unlimited tunnels.
Max. Sessions/Tunnel	<input type="text" value="0"/> Enter 0 for unlimited sessions.
Packet Processing Delay	<input type="text" value="1"/> 10 ^{ths} of seconds
Acknowledgement Delay	<input type="text" value="500"/> milliseconds
Acknowledgement Timeout	<input type="text" value="3"/> seconds
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>	

4. Selezionare **Configurazione > Gestione utente > Gruppi > Aggiungi** e configurare un gruppo PPTP. Nell'esempio, il nome del gruppo è "pptpgroup" e la password (e la password di verifica) è "cisco123".

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 Parameters

Attribute	Value	Description
Group Name	<input type="text" value="pptpgroup"/>	Enter a unique name for the group.
Password	<input type="password" value="*****"/>	Enter the password for the group.
Verify	<input type="password" 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.

Add

Cancel

5. Nella scheda Generale del gruppo verificare che l'opzione **PPTP** sia attivata nei protocolli di autenticazione.

General Parameters

Attribute	Value	Description
Access Hours	<input type="text" value="-No Restrictions-"/>	Select the access hours for this group.
Simultaneous Logins	<input type="text" value="3"/>	Enter the number of simultaneous logins for users in this group.
Minimum Password Length	<input type="text" value="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	<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.
Strip Realm	<input type="checkbox"/>	Check to remove the realm qualifier of the username during authentication.
DHCP Network Scope	<input type="text"/>	Enter the IP sub-network to which users within this group will be assigned when using the concentrator as a DHCP Proxy.
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>		

6. Nella scheda PPTP/L2TP, abilitare l'autenticazione **PAP** e disabilitare la **crittografia** (la crittografia può essere abilitata in qualsiasi momento in futuro).

Configuration | User Management | Groups | Modify pptpgroup

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 all options means that no 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. Selezionare **Configurazione > Gestione utente > Utenti > Aggiungi**, quindi configurare un utente locale (denominato "pptpuser") con la password **cisco123** per l'autenticazione PPTP. Inserire l'utente nel "pptpgroup" definito in precedenza:

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	pptpuser	Enter a unique user name.
Password	*****	Enter the user's password. The password must satisfy the group password requirements.
Verify	*****	Verify the user's password.
Group	pptpgroup	Enter the group to which this user belongs.
IP Address		Enter the IP address assigned to this user.
Subnet Mask		Enter the subnet mask assigned to this user.

Add

Cancel

8. Nella scheda Generale relativa all'utente, verificare che l'opzione **PPTP** sia abilitata nei protocolli di tunneling.

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

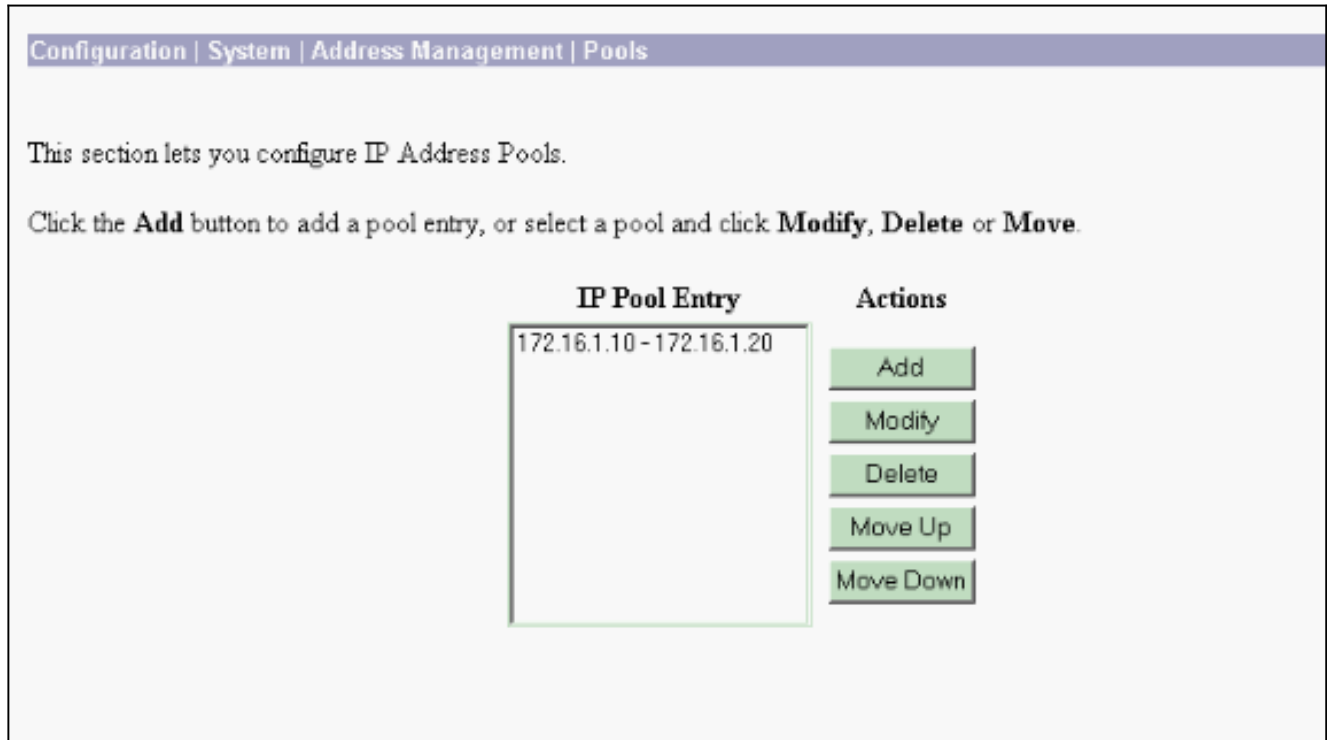
General Parameters

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.

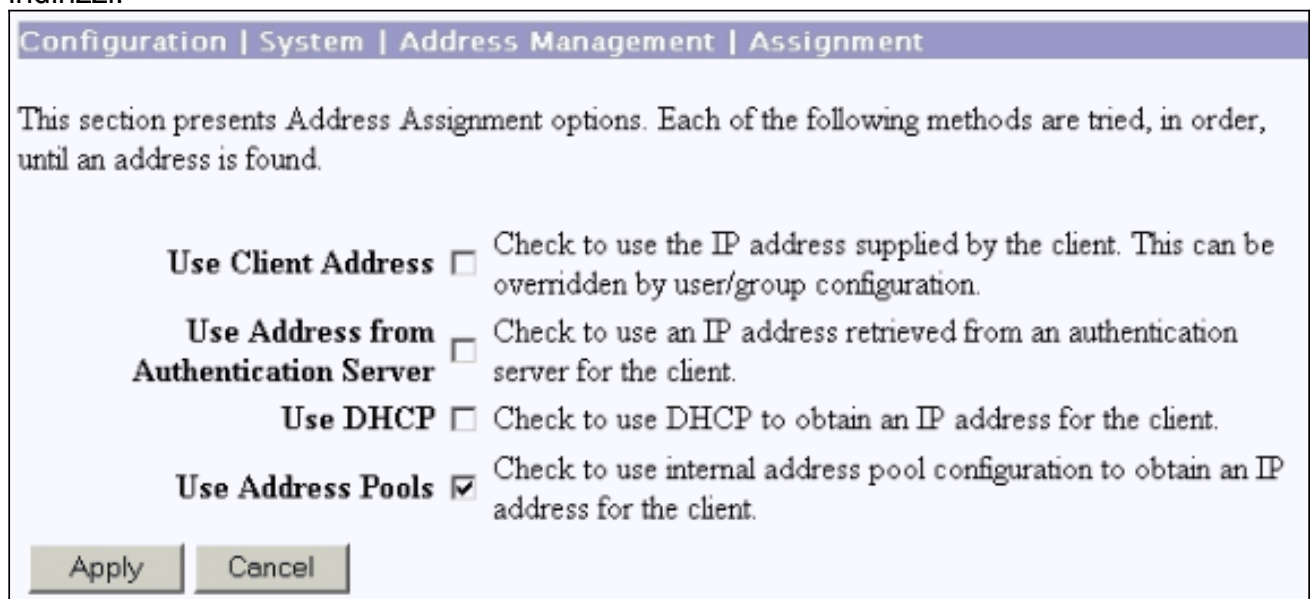
Apply

Cancel

9. Selezionare **Configurazione > Sistema > Gestione indirizzi > Pool** per definire un pool di indirizzi per la gestione degli indirizzi.



10. Selezionare **Configurazione > Sistema > Gestione indirizzi > Assegnazione** e indicare al concentratore VPN di utilizzare il pool di indirizzi.



[Configurazione client PPTP Microsoft](#)

Nota: nessuna delle informazioni disponibili qui sulla configurazione del software Microsoft è fornita con alcuna garanzia o supporto per il software Microsoft. Il supporto per il software Microsoft è disponibile presso [Microsoft](#) .

[Windows 98 - Installazione e configurazione della funzionalità PPTP](#)

[Install](#)

Completare la procedura seguente per installare la funzionalità PPTP.

1. Selezionare **Start > Impostazioni > Pannello di controllo > Nuovo hardware (Avanti) > Seleziona dall'elenco > Scheda di rete (Avanti)**.
2. Selezionare **Microsoft** nel pannello sinistro e **Microsoft VPN Adapter** nel pannello destro.

Configurazione

Completare la procedura seguente per configurare la funzionalità PPTP.

1. Selezionare **Start > Programmi > Accessori > Comunicazioni > Accesso remoto > Crea nuova connessione**.
2. Connettersi utilizzando Microsoft VPN Adapter al prompt Select a device (Seleziona un dispositivo). L'IP del server VPN è l'endpoint del tunnel 3000.

L'autenticazione predefinita di Windows 98 utilizza la crittografia della password, ad esempio CHAP o MSCHAP. Per disabilitare inizialmente la crittografia, selezionare **Proprietà > Tipi di server** e deselezionare le caselle **Password crittografata** e **Richiedi crittografia dati**.

Windows 2000 - Configurazione della funzionalità PPTP

Completare la procedura seguente per configurare la funzionalità PPTP.

1. Selezionare **Start > Programmi > Accessori > Comunicazioni > Connessioni di rete e remote > Crea nuova connessione**.
2. Fare clic su **Avanti** e selezionare **Connetti a una rete privata tramite Internet > Componi una connessione prima** (non selezionare questa opzione se si utilizza una rete LAN).
3. Fare di nuovo clic su **Avanti** e immettere il nome host o l'IP dell'endpoint del tunnel, che è l'interfaccia esterna di VPN 3000 Concentrator. Nell'esempio, l'indirizzo IP è 161.44.17.1.

Selezionare **Proprietà > Protezione per la connessione > Avanzate** per aggiungere un tipo di password come PAP. Il valore predefinito è MSCHAP e MSCHAPv2, non CHAP o PAP.

In quest'area è possibile configurare la crittografia dei dati. Inizialmente è possibile disattivarla.

Windows NT

È possibile accedere alle informazioni sulla configurazione dei client Windows NT per PPTP sul [sito Web Microsoft](#).

Windows Vista

Completare la procedura seguente per configurare la funzionalità PPTP.

1. Dal pulsante **Start**, scegliere **Connetti a**.
2. Scegliere **Configura connessione o rete**.
3. Scegliere **Connetti a una rete aziendale** e fare clic su **Avanti**.
4. Scegliere **Usa connessione Internet (VPN)**. **Nota:** se viene richiesto se si desidera utilizzare una connessione già esistente, scegliere **No, creare una nuova connessione** e fare clic su **Avanti**.

5. Nel campo **Indirizzo Internet**, digitare **pptp.vpn.univ.edu**, ad esempio.
6. Nel campo **Nome destinazione**, digitare **UNIVVPN**, ad esempio.
7. Nel campo **User Name** (Nome utente), digitare l'ID di accesso UNIV. L'ID di accesso UNIV è la parte dell'indirizzo e-mail precedente a **@univ.edu**.
8. Nel campo **Password**, digitare la password dell'ID di accesso UNIV.
9. Fare clic sul pulsante **Crea**, quindi sul pulsante **Chiudi**.
10. Per connettersi al server VPN dopo aver creato la connessione VPN, fare clic su **Start** e quindi su **Connetti a**.
11. Scegliere la connessione VPN nella finestra e fare clic su **Connetti**.

Aggiungi MPPE (crittografia)

Prima di aggiungere la crittografia, verificare che la connessione PPTP funzioni senza crittografia. Ad esempio, fare clic sul pulsante **Connect** (Connetti) sul client PPTP per assicurarsi che la connessione sia stata completata. Se si decide di richiedere la crittografia, è necessario utilizzare l'autenticazione MSCHAP. Sulla VPN 3000, selezionare **Configurazione > Gestione utente > Gruppi**. Quindi, nella scheda PPTP/L2TP del gruppo, deselezionare **PAP**, selezionare **MSCHAPv1** e selezionare **Obbligatorio per crittografia PPTP**.

Configuration | User Management | Groups | Modify pptpgroup

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 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	<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.

Il client PPTP deve essere riconfigurato per la crittografia dei dati facoltativa o obbligatoria e per MSCHAPv1 (se è un'opzione).

Verifica

Le informazioni contenute in questa sezione permettono di verificare che la configurazione funzioni correttamente.

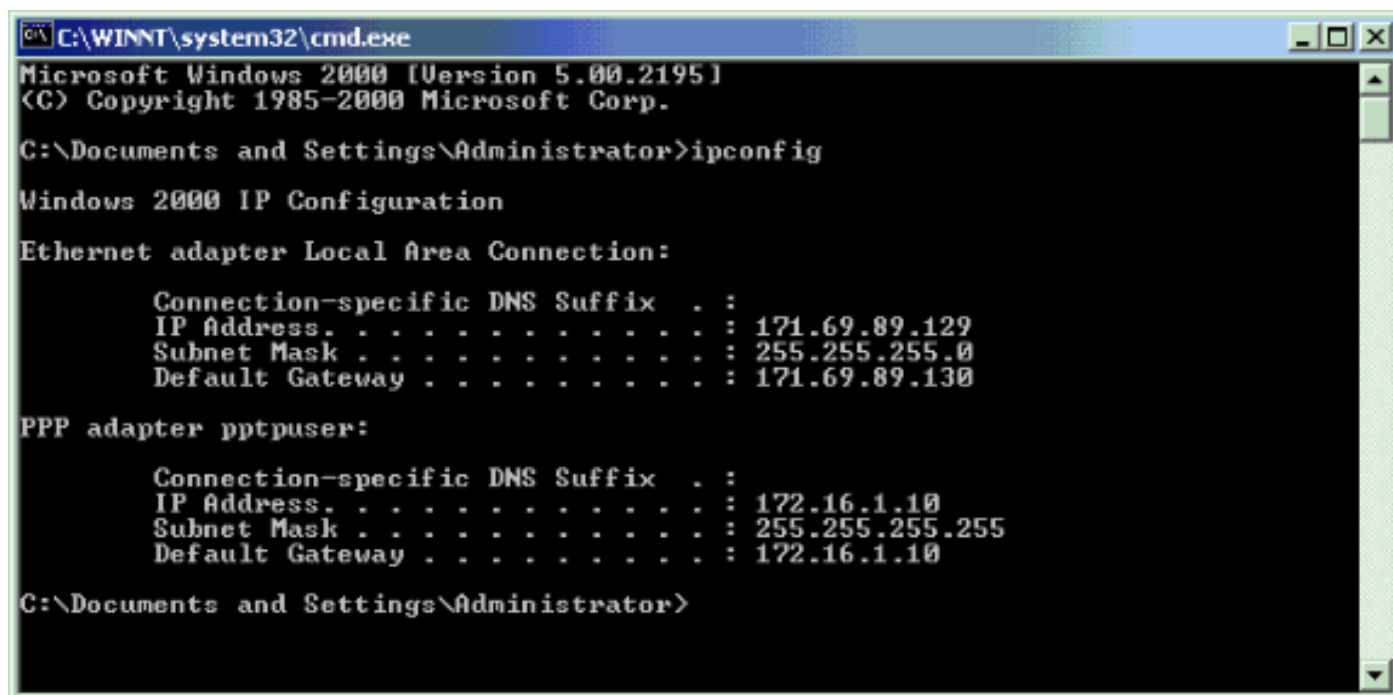
Verifica di VPN Concentrator

È possibile avviare la sessione PPTP chiamando il client PPTP creato in precedenza nella sezione [Configurazione client PPTP Microsoft](#).

Utilizzare la finestra Amministrazione > Amministra sessioni di VPN Concentrator per visualizzare i parametri e le statistiche per tutte le sessioni PPTP attive.

Verifica il PC

Eseguire il comando **ipconfig** nella modalità di comando del PC per verificare che disponga di due indirizzi IP. Uno è il proprio indirizzo IP e l'altro è assegnato dal concentratore VPN dal pool di indirizzi IP. Nell'esempio, l'indirizzo IP 172.16.1.10 è l'indirizzo IP assegnato dal concentratore VPN.



```
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>
```

Debug

Se la connessione non funziona, è possibile aggiungere il debug della classe di evento PPTP a VPN Concentrator. Selezionare **Configurazione > Sistema > Eventi > Classi > Modifica o Aggiungi** (qui). Sono inoltre disponibili le classi di eventi PPTPDBG e PPTPDECODE, ma potrebbero fornire troppe informazioni.

This screen lets you add and configure an event class for special handling.

Class Name	<input type="text" value="PPTP"/>	Select the event class to configure.
Enable	<input checked="" type="checkbox"/>	Check to enable special handling of this class.
Severity to Log	<input type="text" value="1-13"/>	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.

Il registro eventi può essere recuperato da **Monitoraggio > Registro eventi filtrabili**.

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
    
```

[Debug VPN 3000 - Buona autenticazione](#)

1 09/28/2004 21:36:52.800 SEV=4 PPTP/47 RPT=29 171.69.89.129

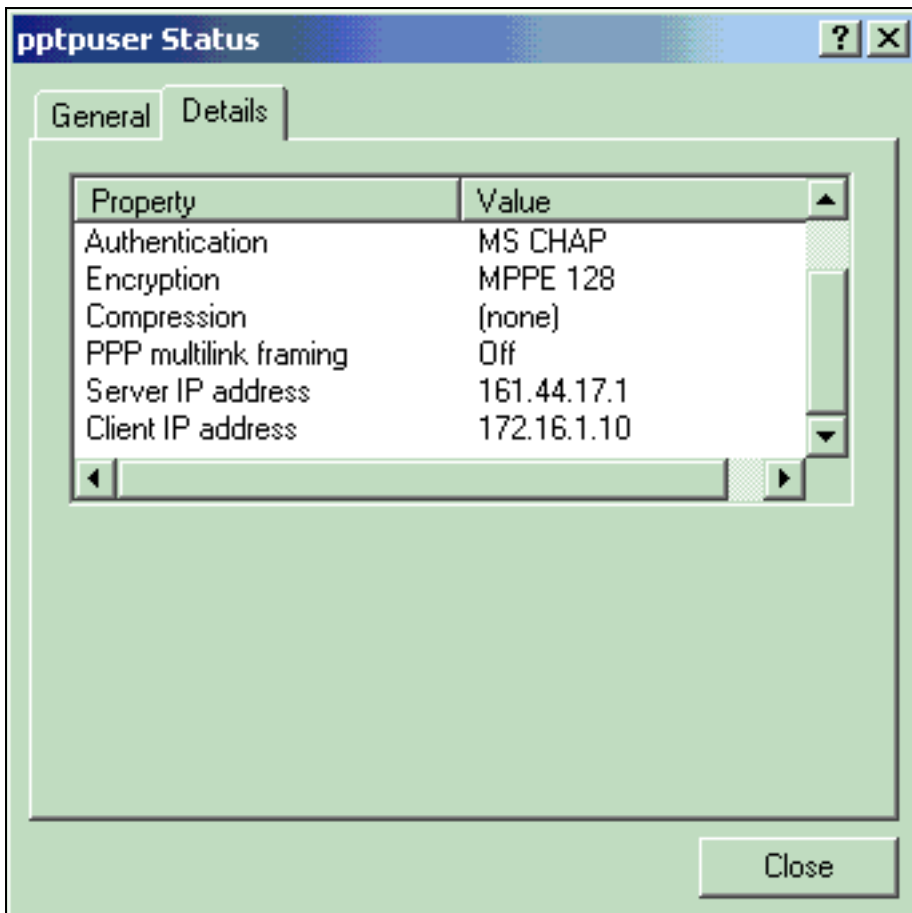
Tunnel to peer 171.69.89.129 established

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

Fare clic sulla finestra **Dettagli** stato utente PPTP per controllare i parametri sul PC Windows.



Risoluzione dei problemi

Di seguito sono riportati i possibili errori che è possibile rilevare:

- **Nome utente o password non validi** Output di debug VPN 3000 Concentrator:

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)
```

Messaggio visualizzato dall'utente (da 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.

Messaggio visualizzato dall'utente (da Windows 2000):

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

- **Sul PC è selezionata l'opzione "Crittografia richiesta", ma non sul concentratore**

VPN Messaggio visualizzato dall'utente (da 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.

Messaggio visualizzato dall'utente (da Windows 2000):

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

- **Sul concentratore VPN è selezionata l'opzione "Crittografia richiesta" (128 bit) con un PC che supporta solo la crittografia a 40 bit** Output di debug VPN 3000 Concentrator:

```
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.
```

Messaggio visualizzato dall'utente (da Windows 98):

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

Messaggio visualizzato dall'utente (da 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 Concentrator è configurato per MSCHAPv1 e il PC è configurato per PAP, ma non è possibile accettare un metodo di autenticazione** Output di debug VPN 3000 Concentrator:

```
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.
```

Messaggio visualizzato dall'utente (da Windows 2000):

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

Possibili problemi Microsoft da risolvere

- **Come mantenere attive le connessioni RAS dopo la disconnessione** Quando si esegue la disconnessione da un client di Servizio di accesso remoto Windows (RAS), tutte le connessioni RAS vengono disconnesse automaticamente. Abilitare la chiave **KeepRasConnections** nel Registro di sistema del client RAS in modo che rimanga connessa dopo la disconnessione. Per ulteriori informazioni, fare riferimento all'[articolo della Microsoft Knowledge Base - 158909](#).
- **L'Utente Non Viene Avvisato Quando Accede Con Credenziali Memorizzate Nella Cache** Questo problema si verifica quando si tenta di accedere a un dominio da una workstation basata su Windows o da un server membro e non è possibile individuare un controller di dominio e non viene visualizzato alcun messaggio di errore. È stato invece eseguito l'accesso al computer locale utilizzando le credenziali memorizzate nella cache. Per ulteriori informazioni, fare riferimento all'[articolo della Microsoft Knowledge Base - 242536](#).

- **Come scrivere un file LMHOSTS per la convalida del dominio e altri problemi di risoluzione dei nomi** In alcuni casi si verificano problemi di risoluzione dei nomi sulla rete TCP/IP e è necessario utilizzare i file LMHOSTS per risolvere i nomi NetBIOS. In questo articolo viene descritto il metodo corretto utilizzato per creare un file LMHOSTS che agevoli la risoluzione dei nomi e la convalida del dominio. Per ulteriori informazioni, fare riferimento all'[articolo della Microsoft Knowledge Base - 180094](#) .

Informazioni correlate

- [RFC 2637: Protocollo PPTP \(Point-to-Point Tunneling Protocol\)](#)
- [Pagine di supporto Cisco Secure ACS per Windows](#)
- [Quando la crittografia PPTP è supportata su un concentratore Cisco VPN 3000?](#)
- [Configurazione di VPN 3000 Concentrator e PPTP con Cisco Secure ACS per autenticazione RADIUS Windows](#)
- [Pagine di supporto Cisco VPN 3000 Concentrator](#)
- [Pagine di supporto client Cisco VPN 3000](#)
- [Pagine di supporto dei prodotti IP Security \(IPSec\)](#)
- [Pagine di supporto dei prodotti PPTP](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)