How to Configure the VPN 3000 Concentrator PPTP with Local Authentication

Document ID: 14101

Contents

Introduction

The Cisco VPN 3000 Concentrator supports the Point−to−Point Tunnel Protocol (PPTP) tunneling method for native Windows clients. There is 40−bit and 128−bit encryption support available on these VPN Concentrators for a secured reliable connection.

Refer to Configuring the VPN 3000 Concentrator PPTP With Cisco Secure ACS for Windows RADIUS Authentication in order to configure the VPN Concentrator for PPTP users with extended authentication using the Cisco Secure Access Control Server (ACS).

Prerequisites

Requirements

Ensure that you meet the prerequisites mentioned in When is PPTP Encryption Supported on a Cisco VPN 3000 Concentrator? before you attempt this configuration.

Components Used

The information in this document is based on these software and hardware versions:

- VPN 3015 Concentrator with version 4.0.4.A
- Windows PC with PPTP client

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Network Diagram

This document uses this network setup:
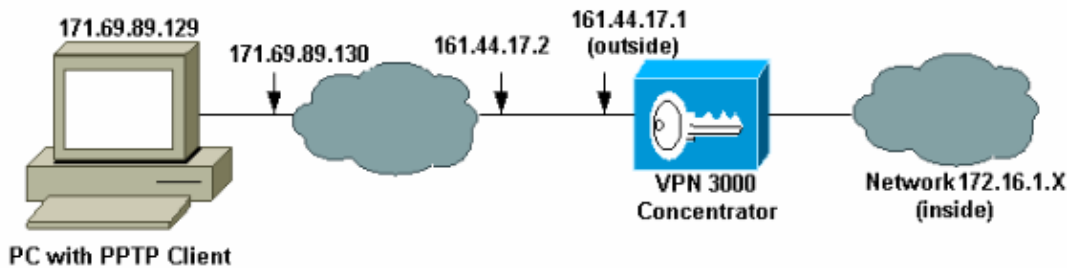
Conventions

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

Configure the VPN 3000 Concentrator with Local Authentication

Complete these steps to configure the VPN 3000 Concentrator with Local Authentication.

1. Configure the respective IP addresses in the VPN Concentrator and ensure that you have connectivity.
2. Ensure that **PAP authentication** is selected in the **Configuration > User Management > Base Group** PPTP/L2TP tab.

3. Select **Configuration > System > Tunneling Protocols > PPTP** and ensure that **Enabled** is checked.

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 [5] seconds

Packet Window Size [16] packets

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

Max. Tunnels [0] Enter 0 for unlimited tunnels.

Max. Sessions/Tunnel [0] Enter 0 for unlimited sessions.

Packet Processing Delay [1] 10^{ths} of seconds

Acknowledgement Delay [500] milliseconds

Acknowledgement Timeout [3] seconds

Apply   Cancel

4. Select **Configuration > User Management > Groups > Add**, and configure a PPTP group. In this example, the group name is "pptpgroup" and the password (and verify password) is "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	pptpgroup	Enter a unique name for the group.
Password	********	Enter the password for the group.
Verify	********	Verify the group's password.
Type	Internal ▾	*External* groups are configured on an external authentication server (e.g. RADIUS). *Internal* groups are configured on the VPN 3000 Concentrator's Internal Database.

Add   Cancel

5. Under the group's General tab, make certain that the **PPTP** option is enabled in authentication protocols.

General | IPSec | Client Config | Client FW | HW Client | PPTP/L2TP

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	☑	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	☑ SEP 1 ☑ SEP 2 ☑ SEP 3 ☑ SEP 4	Select the SEP cards this group can be on.
Tunneling Protocols	☑ PPTP ☑ L2TP ☑ IPSec ☐ L2TP over IPSec	Select the tunneling protocols this group can connect with.
Strip Realm	☐	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. Under the PPTP/L2TP tab, enable **PAP** authentication, and disable **encryption** (encryption can be enabled at any time in the future).

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	☐	☑	Check to accept and use an IP address received from the client.
PPTP Authentication Protocols	☑ PAP ☑ CHAP ☑ MSCHAPv1 ☐ MSCHAPv2 ☐ EAP Proxy	☑	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	☐ Required ☐ Require Stateless ☐ 40-bit ☐ 128-bit	☐	Select the allowed encryption methods for PPTP connections for this group.
PPTP Compression	☐	☑	Check to enable compression for PPTP connections for this group.

7. Select **Configuration > User Management > Users > Add**, and configure a local user (called "pptpuser") with the password **cisco123** for PPTP authentication. Put the user in the previously defined "pptpgroup":

Configuration | User Management | Users | Add

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. Under the General tab for the user, make sure that the **PPTP** option is enabled in tunneling protocols.

Configuration | User Management | Users | Modify pptpuser

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-	☑	Select the access hours assigned to this user.
Simultaneous Logins	3	☑	Enter the number of simultaneous logins for this user.
Idle Timeout	30	☑	(minutes) Enter the idle timeout for this user.
Maximum Connect Time	0	☑	(minutes) Enter the maximum connect time for this user.
Filter	--None--	☑	Enter the filter assigned to this user.
Tunneling Protocols	☑ PPTP ☑ L2TP ☑ IPSec ☐ L2TP over IPSec	☑	Select the tunneling protocols this user can connect with.

[Apply] [Cancel]

9. Select **Configuration > System > Address Management > Pools** to define an address pool for address management.

Configuration | System | Address Management | Pools

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	Actions
172.16.1.10 – 172.16.1.20	[Add] [Modify] [Delete] [Move Up] [Move Down]

10. Select **Configuration > System > Address Management > Assignment** and direct the VPN Concentrator to use the address pool.
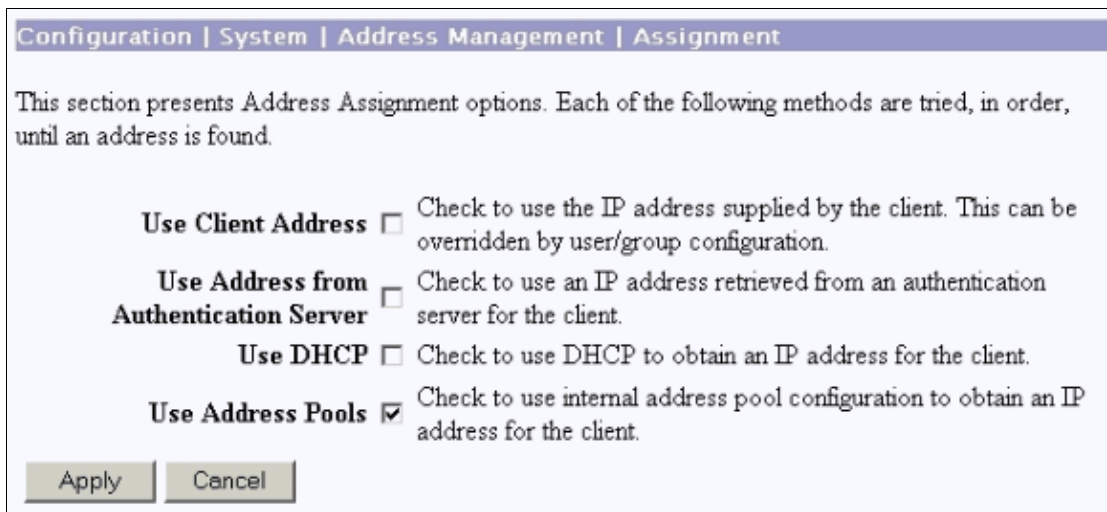
Microsoft PPTP Client Configuration

Note: None of the information available here on configuring Microsoft software comes with any warranty or support for Microsoft software. Support for Microsoft software is available from Microsoft 🗗 .

Windows 98 – Install and Configure the PPTP Feature

Install

Complete these steps to install the PPTP feature.

1. Select **Start > Settings > Control Panel > Add New Hardware (Next) > Select from List > Network Adapter (Next)**.
2. Select **Microsoft** in the left panel and **Microsoft VPN Adapter** on the right panel.

Configure

Complete these steps to configure the PPTP feature.

1. Select **Start > Programs > Accessories > Communications > Dial Up Networking > Make new connection**.
2. Connect using the Microsoft VPN Adapter at the Select a device prompt. The VPN Server IP is the 3000 tunnel endpoint.

The Windows 98 default authentication uses password encryption (for example, CHAP or MSCHAP). In order to initially disable this encryption, select **Properties > Server types**, and uncheck the **Encrypted Password** and **Require Data Encryption** boxes.

Windows 2000 – Configuring the PPTP Feature

Complete these steps to configure the PPTP feature.

1. Select **Start > Programs > Accessories > Communications > Network and Dialup connections > Make new connection**.
2. Click **Next**, and select **Connect to a private network through the Internet > Dial a connection prior** (do not select this if you use a LAN).
3. Click **Next** again, and enter the Hostname or IP of the tunnel endpoint, which is the outside interface of the VPN 3000 Concentrator. In this example the IP address is 161.44.17.1.

Select **Properties > Security for the connection > Advanced** to add a password type as PAP. The default is MSCHAP and MSCHAPv2, not CHAP or PAP.

Data encryption is configurable in this area. You can disable it initially.

Windows NT

You can access information about setting up Windows NT clients for PPTP at Microsoft's website ⬚ .

Windows Vista

Complete these steps to configure the PPTP feature.

1. From the **Start** button, choose **Connect To**.
2. Choose **Set up a connection or network**.
3. Choose **Connect to a workplace** and click **Next**.
4. Choose **Use my Internet Connection (VPN)**.

   Note: If prompted for "Do you want to use a connection that you already have," choose **No, create a new connection** and click **Next**.
5. In the **Internet Address** field, type **pptp.vpn.univ.edu**, for example.
6. In the **Destination Name** field, type **UNIVVPN**, for example.
7. In the **User Name** field, type your UNIV Logon ID. Your UNIV Logon ID is the part of your email address before **@univ.edu**.
8. In the **Password** field, type your UNIV Logon ID password.
9. Click the **Create** button and then click the **Close** button.
10. In order to connect to the VPN server after you create the VPN connection, click Start, and then **Connect to**.
11. Choose the VPN connection in the window and click **Connect**.

Add MPPE (Encryption)

Make sure that the PPTP connection works without encryption before you add encryption. For example, click the **Connect** button on the PPTP client to make sure that the connection completes. If you decide to require encryption, MSCHAP authentication must be used. On the VPN 3000, select **Configuration > User Management > Groups**. Then, under the PPTP/L2TP tab for the group, uncheck **PAP**, check **MSCHAPv1**, and check **Required for PPTP Encryption**.

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	☐	☑	Check to accept and use an IP address received from the client.
PPTP Authentication Protocols	☐ PAP ☐ CHAP ☑ MSCHAPv1 ☐ MSCHAPv2 ☐ EAP Proxy	☐	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	☑ Required ☐ Require Stateless ☑ 40-bit ☑ 128-bit	☐	Select the allowed encryption methods for PPTP connections for this group.
PPTP Compression	☐	☑	Check to enable compression for PPTP connections for this group.

The PPTP client should be reconfigured for optional or required data encrytption and MSCHAPv1 (if it is an option).

Verify

This section provides information you can use to confirm your configuration is working properly.

Verify the VPN Concentrator

You can start the PPTP session by dialing form the PPTP client created earlier in the Microsoft PPTP Client Configuration section.

Use the Administration >Administer Sessions window on the VPN Concentrator to view the parameters and statistics for all active PPTP sessions.

Verify the PC

Issue the **ipconfig** command in the command mode of the PC to see that the PC has two IP addresses. One is its own IP address and the other is assigned by the VPN Concentrator from the pool of IP address. In this example the IP address 172.16.1.10 is the IP address assigned by the VPN Concentrator.

```
C:\WINNT\system32\cmd.exe                                              _ |□| X
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

If the connection does not work, the PPTP event class debug can be added to the VPN Concentrator. Select **Configuration > System > Events > Classes > Modify** or **Add** (shown here). PPTPDBG and PPTPDECODE event classes are also available, but might provide too much information.

The event log can be retrieved from **Monitoring > Filterable Event Log**.

VPN 3000 Debug – Good Authentication

```
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
```

Click on the PPTP user status **Details** window to check the parameters on the Windows PC.
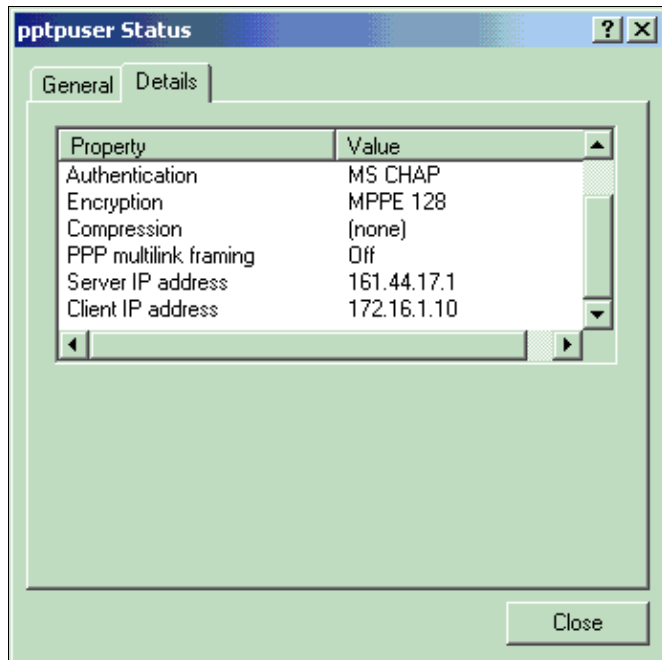
Troubleshoot

These are possible errors you can encounter:

- **Bad username or password**

  VPN 3000 Concentrator debug output:

  ```
  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)
  ```

  The message that the user sees (from 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.
  ```

  The message that the user sees (from Windows 2000):

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

- **"Encryption Required" is selected on the PC, but not on the VPN Concentrator**

  The message that the user sees (from 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.
  ```

  The message that the user sees (from Windows 2000):

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

- **"Encryption Required" (128–bit) is selected on the VPN Concentrator with a PC that only supports 40–bit encryption**

  VPN 3000 Concentrator debug output:

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

  The message that the user sees (from Windows 98):

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

  The message that the user sees (from Windows 2000):

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

- **The VPN 3000 Concentrator is configured for MSCHAPv1 and the PC is configured for PAP, but they cannot agree on an authentication method**

  VPN 3000 Concentrator debug output:

  ```
  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.
  ```

  The message that the user sees (from Windows 2000):

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

Possible Microsoft Issues to Troubleshoot

- **How to Keep RAS Connections Active After Logging Off**

  When you log off from a Windows Remote Access Service (RAS) client, any RAS connections are automatically disconnected. Enable the **KeepRasConnections** key in the registry on the RAS client to remain connected after you log off. Refer to Microsoft Knowledge Base Article – 158909 ⬈ for more information.

- **User Is Not Alerted When Logging On with Cached Credentials**

  The symptoms of this issue are when you attempt to log on to a domain from a Windows–based workstation or member server and a domain controller cannot be located and no error message is displayed. Instead, you are logged on to the local computer using cached credentials. Refer to

Microsoft Knowledge Base Article – 242536 ⬚ for more information.

- **How to Write an LMHOSTS File for Domain Validation and Other Name Resolution Issues**

There can be instances when you experience name resolution issues on your TCP/IP network and you need to use LMHOSTS files to resolve NetBIOS names. This article discusses the proper method used to create an LMHOSTS file to aid in name resolution and domain validation. Refer to Microsoft Knowledge Base Article – 180094 ⬚ for more information.

Related Information

- **RFC 2637: Point−to−Point Tunneling Protocol (PPTP)** ⬚
- **Cisco Secure ACS for Windows Support Pages**
- **When is PPTP Encryption Supported on a Cisco VPN 3000 Concentrator?**
- **Configuring the VPN 3000 Concentrator and PPTP with Cisco Secure ACS for Windows RADIUS Authentication**
- **Cisco VPN 3000 Concentrator Support Pages**
- **Cisco VPN 3000 Client Support Pages**
- **IP Security (IPSec) Product Support Pages**
- **PPTP Product Support Pages**
- **Technical Support & Documentation – Cisco Systems**

Updated: Dec 06, 2006   Document ID: 14101