

Configuring the VPN 3000 Concentrator and PPTP with Cisco Secure ACS for Windows RADIUS Authentication

Document ID: 13829

Introduction

Before You Begin

- Conventions
- Prerequisites
- Components Used
- Network Diagram

Configuring the VPN 3000 Concentrator

- Adding and Configuring Cisco Secure ACS for Windows
- Adding MPPE (Encryption)
- Adding Accounting

Verify

Troubleshoot

- Enabling Debugging
- Debugs – Good Authentication
- Possible Errors

Related Information

Introduction

The Cisco VPN 3000 Concentrator supports the Point-to-Point Tunnel Protocol (PPTP) tunneling method for native Windows clients. The concentrator supports 40-bit and 128-bit encryption for a secured reliable connection. This document describes how to configure PPTP on a VPN 3000 Concentrator with Cisco Secure ACS for Windows for RADIUS authentication.

Refer to [Configuring the Cisco Secure PIX Firewall to Use PPTP](#) to configure PPTP connections to the PIX.

Refer to [Configuring Cisco Secure ACS for Windows Router PPTP Authentication](#) to set up a PC connection to the router; this provides user authentication to the Cisco Secure Access Control System (ACS) 3.2 for Windows server before you allow the user into the network.

Before You Begin

Conventions

For more information on document conventions, see the [Cisco Technical Tips Conventions](#).

Prerequisites

This document assumes that local PPTP authentication is working before adding Cisco Secure ACS for Windows RADIUS authentication. Please see [How to Configure the VPN 3000 Concentrator PPTP with Local Authentication](#) for more information on local PPTP authentication. For a complete list of requirements and restrictions, please refer to [When Is PPTP Encryption Supported on a Cisco VPN 3000 Concentrator?](#)

Components Used

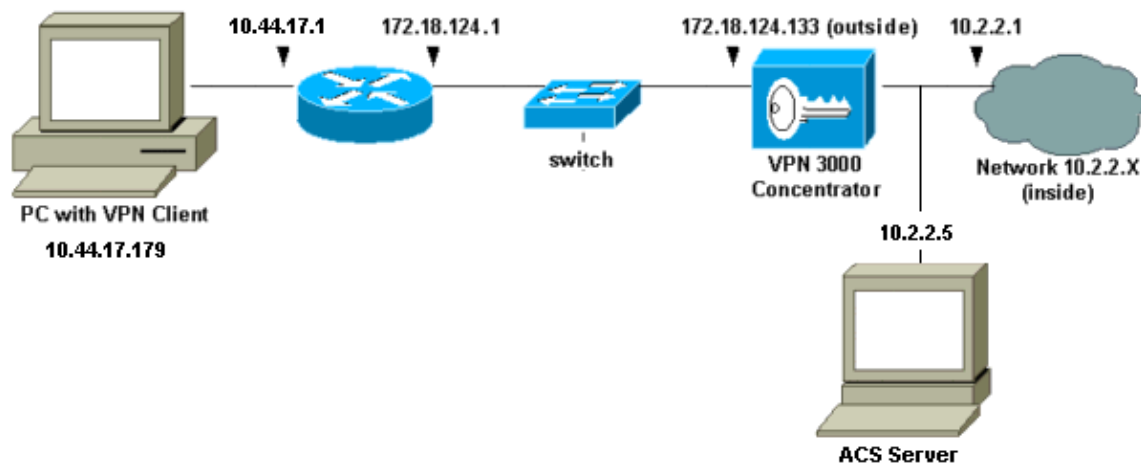
The information in this document is based on the software and hardware versions below.

- Cisco Secure ACS for Windows versions 2.5 and later
- VPN 3000 Concentrator versions 2.5.2.C and later (This configuration has been verified with version 4.0.x.)

The information presented in this document was created from devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If you are working in a live network, ensure that you understand the potential impact of any command before using it.

Network Diagram

This document uses the network setup shown in the diagram below.



Configuring the VPN 3000 Concentrator

Adding and Configuring Cisco Secure ACS for Windows

Follow these steps to configure the VPN Concentrator to use Cisco Secure ACS for Windows.

1. On the VPN 3000 Concentrator, go to **Configuration > System > Servers > Authentication Servers** and add the Cisco Secure ACS for Windows server and key ("cisco123" in this example).

Configuration | System | Servers | Authentication | Add

Configure and add a user authentication server.

Server Type: **RADIUS** Selecting *Internal Server* will let you add users to the internal user database.

Authentication Server: Enter IP address or hostname.

Server Port: Enter 0 for default port (1645).

Timeout: Enter the timeout for this server (seconds).

Retries: Enter the number of retries for this server.

Server Secret: Enter the RADIUS server secret.

Verify: Re-enter the secret.

- In Cisco Secure ACS for Windows, add the VPN Concentrator to the ACS server Network Configuration, and identify the dictionary type.

Access Server Setup For VPN3000

Network Access Server IP Address:

Key:

Network Device Group:

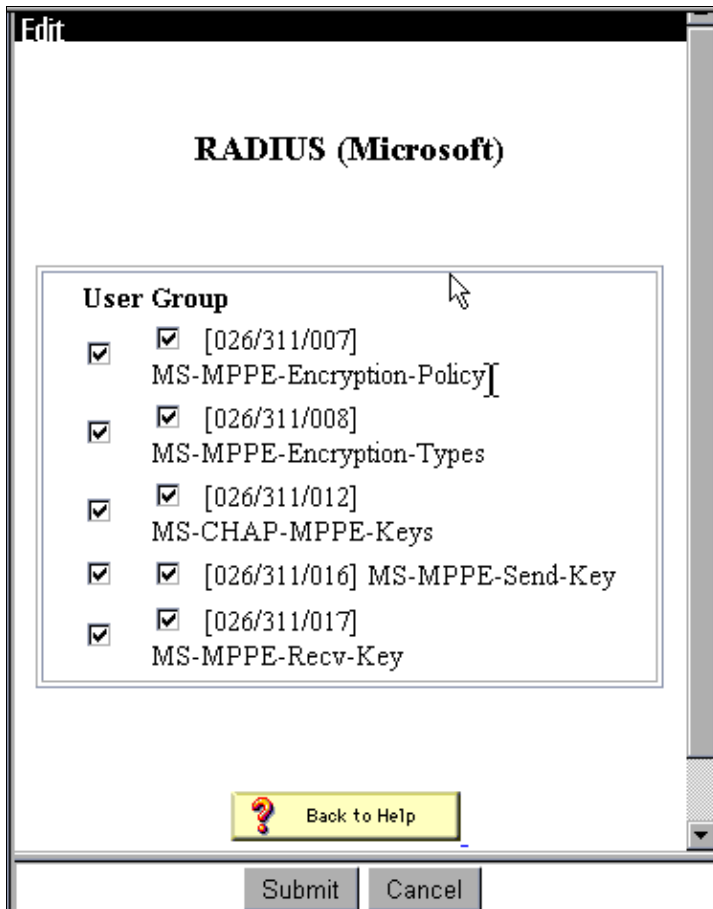
Authenticate Using: **RADIUS (Cisco VPN 3000)**

Single Connect TACACS+ NAS (Record stop in accounting on failure).

Log Update/Watchdog Packets from this Access Server

Log Radius Tunneling Packets from this Access Server

- In Cisco Secure ACS for Windows, go to **Interface Configuration > RADIUS (Microsoft)** and check the Microsoft Point-to-Point Encryption (MPPE) attributes so that the attributes appear in the group interface.



4. In Cisco Secure ACS for Windows, add a user. In the user's group, add the MPPE (Microsoft RADIUS) attributes, in case you require encryption at a later time.

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 ▼

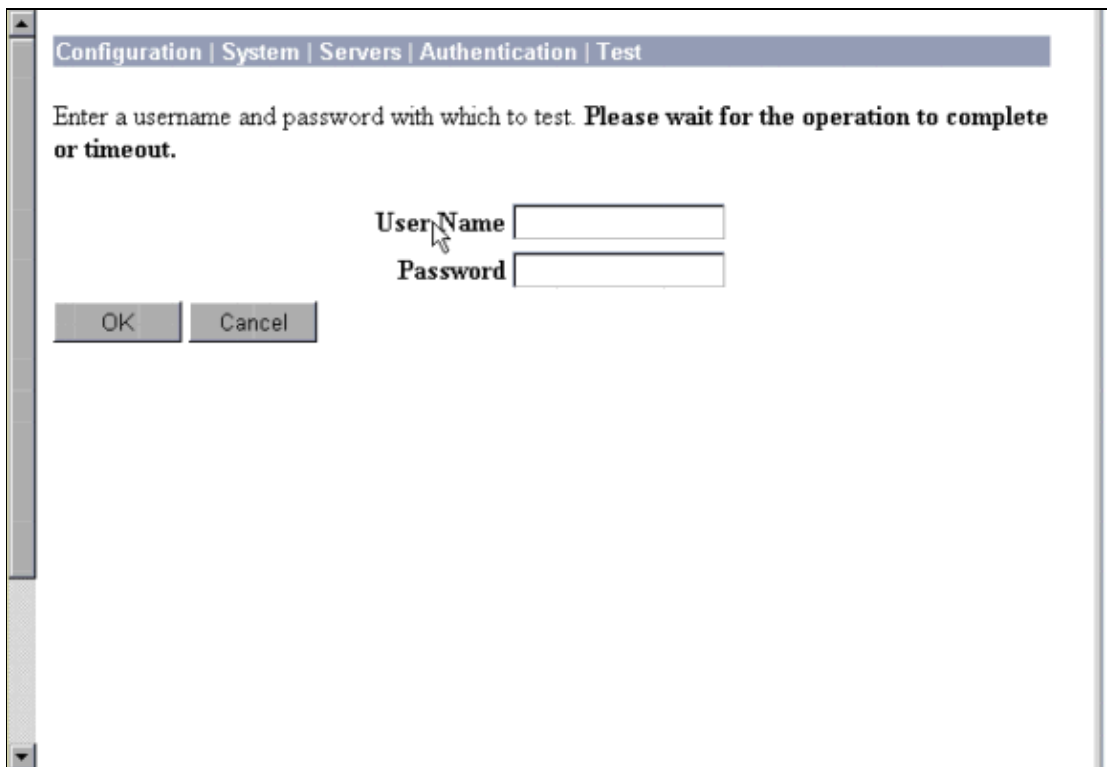
[311\012] MS-CHAP-MPPE-Keys

[311\016] MS-MPPE-Send-Key
[Empty text box]

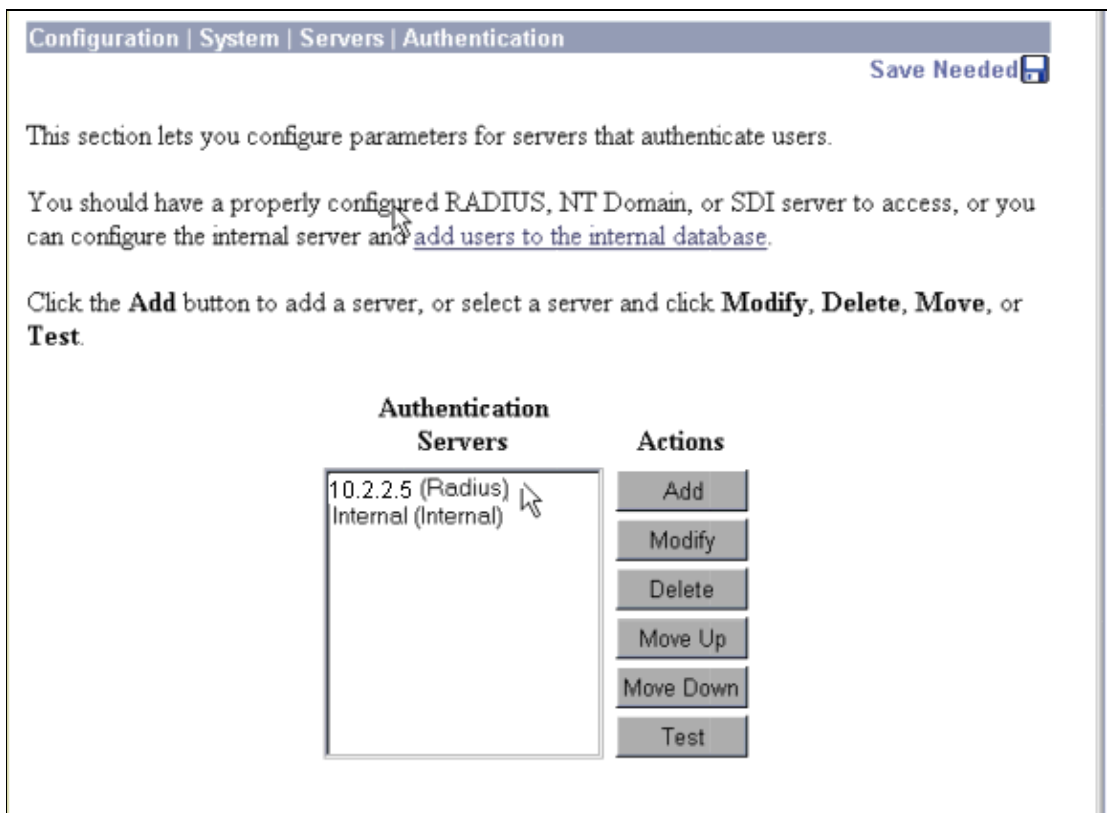
[311\017] MS-MPPE-Recv-Key
[Empty text box]

- On the VPN 3000 Concentrator, go to **Configuration > System > Servers > Authentication Servers**. Select an authentication server from the list, and then select **Test**. Test authentication from the VPN Concentrator to the Cisco Secure ACS for Windows server by entering a username and password.

On a good authentication, the VPN Concentrator should show an "Authentication Successful" message. Failures in Cisco Secure ACS for Windows are logged in **Reports and Activity > Failed Attempts**. In a default install, these reports are stored on disk in C:\Program Files\CiscoSecure ACS v2.5\Logs\Failed Attempts.



6. Since you have now verified authentication from the PC to the VPN Concentrator works and from the concentrator to the Cisco Secure ACS for Windows server, you can reconfigure the VPN Concentrator to send PPTP users to Cisco Secure ACS for Windows RADIUS by moving the Cisco Secure ACS for Windows server to the top of the server list. To do this on the VPN Concentrator, go to **Configuration > System > Servers > Authentication Servers**.



7. Go to **Configuration > User Management > Base Group** and select the **PPTP/L2TP** tab. In the VPN Concentrator base group, ensure that the options for PAP and MSCHAPv1 are enabled.

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 [-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 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 [-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.

8. Select the **General** tab and ensure that PPTP is permitted in the Tunneling Protocols section.

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.

Apply Cancel

9. Test PPTP authentication with the user in the Cisco Secure ACS for Windows RADIUS server. If this does not work, please see the Debugging section.

Adding MPPE (Encryption)

If Cisco Secure ACS for Windows RADIUS PPTP authentication works without encryption, you can add MPPE to the VPN 3000 Concentrator.

1. On the VPN Concentrator, go to **Configuration > User Management > Base Group**.
2. Under the section for PPTP Encryption, check the options for **Required**, **40-bit**, and **128-bit**. Since not all PCs support both 40-bit and 128-bit encryption, check both options to allow for negotiation.
3. Under the section for PPTP Authentication Protocols, check the option for **MSCHAPv1**. (You already configured the Cisco Secure ACS for Windows 2.5 user attributes for encryption in an earlier step.)

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.

Note: The PPTP client should be recognized for optimal or required data encryption and MSCHAPv1 (if an option).

Adding Accounting

After you have established authentication, you can add accounting to the VPN Concentrator. Go to **Configuration > System > Servers > Accounting Servers** and add the Cisco Secure ACS for Windows server.

In Cisco Secure ACS for Windows, the accounting records appear as follows.

```
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
```

Verify

There is currently no verification procedure available for this configuration.

Troubleshoot

This section provides information you can use to troubleshoot your configuration.

Enabling Debugging

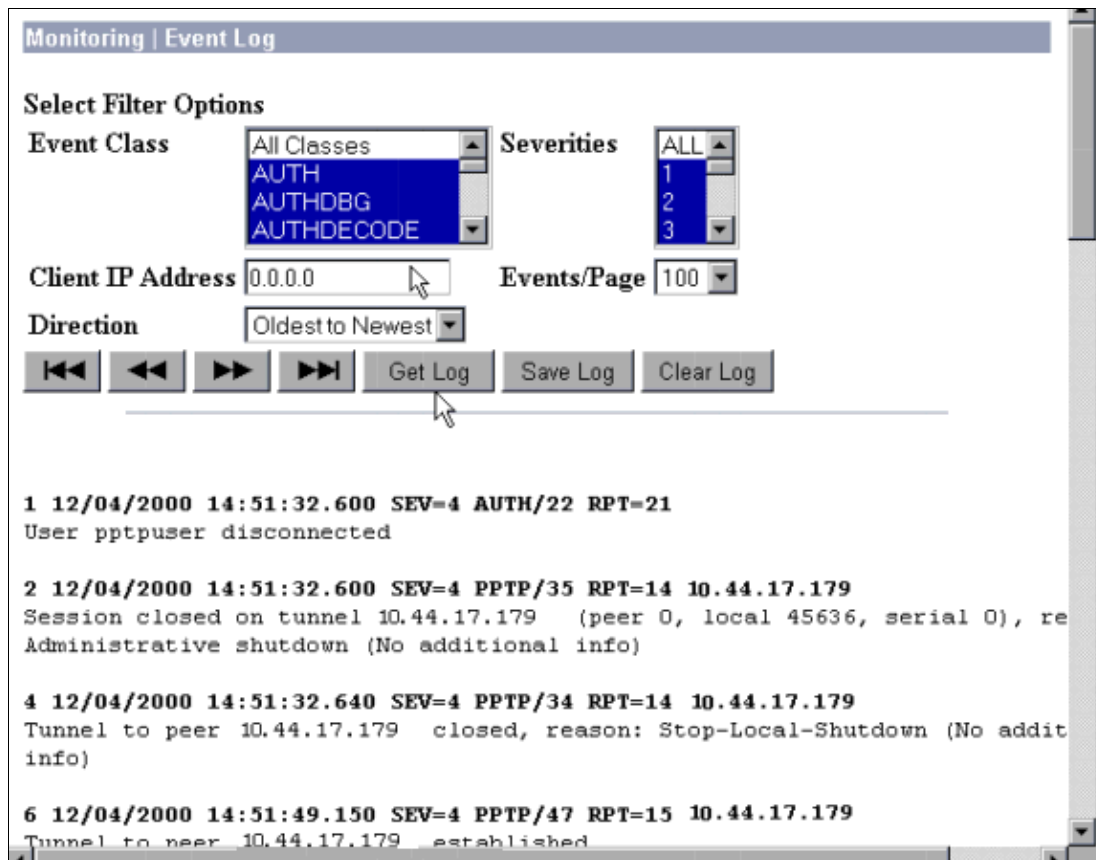
If connections do not work, you can add PPTP and AUTH event classes to the VPN Concentrator by going to **Configuration > System > Events > Classes > Modify**. You can also add PPTPDBG, PPTPDECODE, AUTHDBG, and AUTHDECODE event classes, but these options may provide too much information.

The screenshot shows a web interface for modifying an event class. At the top, a breadcrumb trail reads "Configuration | System | Events | Classes | Modify". Below this, a message states: "This screen lets you modify an event class configured for special handling." The configuration fields are as follows:

- Class Name:** A text input field containing "PPTP".
- Enable:** A checked checkbox.
- Severity to Log:** A dropdown menu set to "1-9".
- Severity to Console:** A dropdown menu set to "1-3".
- Severity to Syslog:** A dropdown menu set to "None".
- Severity to Email:** A dropdown menu set to "None".
- Severity to Trap:** A dropdown menu set to "None".

At the bottom left, there are two buttons: "Apply" and "Cancel". To the right of the "Enable" checkbox and each "Severity" dropdown, there is a mouse cursor icon and a descriptive text box explaining the field's function.

You can retrieve the event log by going to **Monitoring > Event Log**.



Debugs – Good Authentication

Good debugs on the VPN Concentrator will look similar to the following.

```

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

```

Possible Errors

You may encounter possible errors as shown below.

Bad username or password on the Cisco Secure ACS for Windows RADIUS server

- VPN 3000 Concentrator debug output

```

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
```

- Cisco Secure ACS for Windows log output

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

- 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.
```

"MPPE Encryption Required" is selected on the concentrator, but the Cisco Secure ACS for Windows server is not configured for MS-CHAP-MPPE-Keys and MS-CHAP-MPPE-Types

- VPN 3000 Concentrator debug output

If AUTHDECODE (1–13 Severity) and PPTP debug (1–9 Severity) are on, the log shows that the Cisco Secure ACS for Windows server is not sending vendor-specific attribute 26 (0x1A) in the access-accept from the server (partial log).

```
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.
```

- Cisco Secure ACS for Windows log output shows no failures.

- The message that the user sees

```
Error 691: The computer you have dialed in to has denied access because
the username and/or password is invalid on the domain.
```

Related Information

- [Cisco VPN 3000 Series Concentrator Support Page](#)
- [Cisco VPN 3000 Series Client Support Page](#)
- [IPSec Support Page](#)
- [Cisco Secure ACS for Windows Support Page](#)
- [Documentation for Cisco Secure ACS for Windows](#)
- [RADIUS Support Page](#)
- [RADIUS in IOS Documentation](#)
- [PPTP Support Page](#)
- [RFC 2637: Point-to-Point Tunneling Protocol \(PPTP\)](#)

- **Requests for Comments (RFCs)**
 - **Technical Support & Documentation – Cisco Systems**
-

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2007 – 2008 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Jan 15, 2008

Document ID: 13829
