

Windows RADIUS 인증을 위한 Cisco Secure ACS를 사용하여 VPN 3000 Concentrator PPTP 구성

목차

[소개](#)

[시작하기 전에](#)

[표기 규칙](#)

[사전 요구 사항](#)

[사용되는 구성 요소](#)

[네트워크 다이어그램](#)

[VPN 3000 Concentrator 구성](#)

[Windows용 Cisco Secure ACS 추가 및 구성](#)

[MPPE 추가\(압호화\)](#)

[계정 추가](#)

[다음을 확인합니다.](#)

[문제 해결](#)

[디버깅 활성화](#)

[디버깅 - 정상 인증](#)

[가능한 오류](#)

[관련 정보](#)

소개

Cisco VPN 3000 Concentrator는 네이티브 Windows 클라이언트에 대한 PPTP(Point-to-Point Tunnel Protocol) 터널링 방법을 지원합니다. Concentrator는 안정적인 보안 연결을 위해 40비트 및 128비트 압호화를 지원합니다. 이 문서에서는 RADIUS 인증을 위해 Windows용 Cisco Secure ACS를 사용하여 VPN 3000 Concentrator에서 PPTP를 구성하는 방법에 대해 설명합니다.

PPTP를 [사용하여 PIX에 대한 PPTP 연결을 구성하려면 Cisco Secure PIX Firewall 구성](#)을 참조하십시오.

라우터에 [대한](#) PC 연결을 설정하려면 [Windows 라우터 PPTP 인증을 위한 Cisco Secure ACS 구성](#)을 참조하십시오. 사용자가 네트워크에 접속하도록 허용하기 전에 Windows용 Cisco ACS(Secure Access Control System) 3.2에 대한 사용자 인증을 제공합니다.

시작하기 전에

표기 규칙

문서 규칙에 대한 자세한 내용은 [Cisco 기술 팁 표기 규칙](#)을 참조하십시오.

사전 요구 사항

이 문서에서는 Windows RADIUS용 Cisco Secure ACS 인증을 추가하기 전에 로컬 PPTP 인증이 작동 중이라고 가정합니다. 로컬 PPTP 인증에 대한 자세한 내용은 [How to Configure the VPN 3000 Concentrator PPTP with Local Authentication\(로컬 인증으로 VPN 3000 Concentrator PPTP를 구성하는 방법\)](#)을 참조하십시오. 요구 사항 및 제한 사항의 전체 목록은 [Cisco VPN 3000 Concentrator에서 PPTP 암호화가 지원되는 시기](#)를 참조하십시오.

사용되는 구성 요소

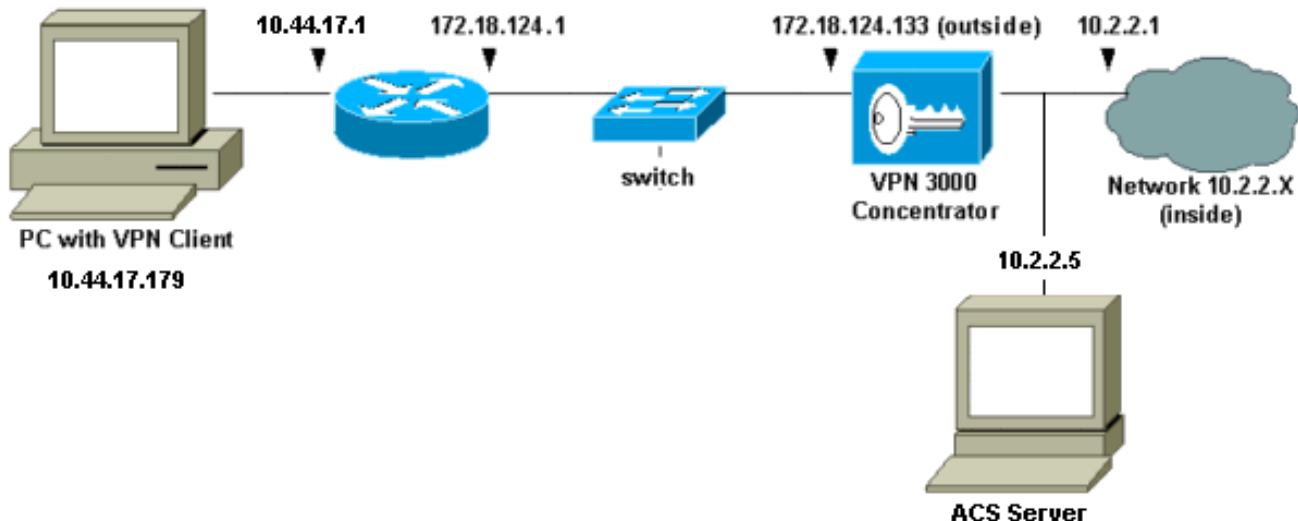
이 문서의 정보는 아래 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco Secure ACS for Windows 버전 2.5 이상
- VPN 3000 Concentrator 버전 2.5.2.C 이상(이 구성은 버전 4.0.x에서 확인됨)

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 라이브 네트워크에서 작업하는 경우, 사용하기 전에 모든 명령의 잠재적인 영향을 이해해야 합니다.

네트워크 다이어그램

이 문서에서는 아래 다이어그램에 표시된 네트워크 설정을 사용합니다.



VPN 3000 Concentrator 구성

Windows용 Cisco Secure ACS 추가 및 구성

Windows용 Cisco Secure ACS를 사용하도록 VPN Concentrator를 구성하려면 다음 단계를 수행합니다.

1. VPN 3000 Concentrator에서 Configuration(컨피그레이션) > System(시스템) > Servers(서버) > Authentication Servers(인증 서버)로 이동하여 Windows용 Cisco Secure ACS 서버 및 키

("cisco123" 이 예에서)를 추가합니다

The screenshot shows the 'Add' configuration page for a user authentication server in Cisco Secure ACS for Windows. The breadcrumb trail at the top is 'Configuration | System | Servers | Authentication | Add'. The main heading is 'Configure and add a user authentication server.' Below this, there are several configuration fields:

- Server Type:** A dropdown menu is set to 'RADIUS'. A tooltip points to it, stating: 'Selecting *Internal Server* will let you add users to the internal user database.'
- Authentication Server:** A text box contains '10.2.2.5'. The instruction is 'Enter IP address or hostname.'
- Server Port:** A text box contains '0'. The instruction is 'Enter 0 for default port (1645).'
- Timeout:** A text box contains '4'. The instruction is 'Enter the timeout for this server (seconds).'
- Retries:** A text box contains '2'. The instruction is 'Enter the number of retries for this server.'
- Server Secret:** A text box contains masked characters. The instruction is 'Enter the RADIUS server secret.'
- Verify:** A text box contains masked characters. The instruction is 'Re-enter the secret.'

At the bottom left, there are two buttons: 'Add' and 'Cancel'. A mouse cursor is pointing at the 'Add' button.

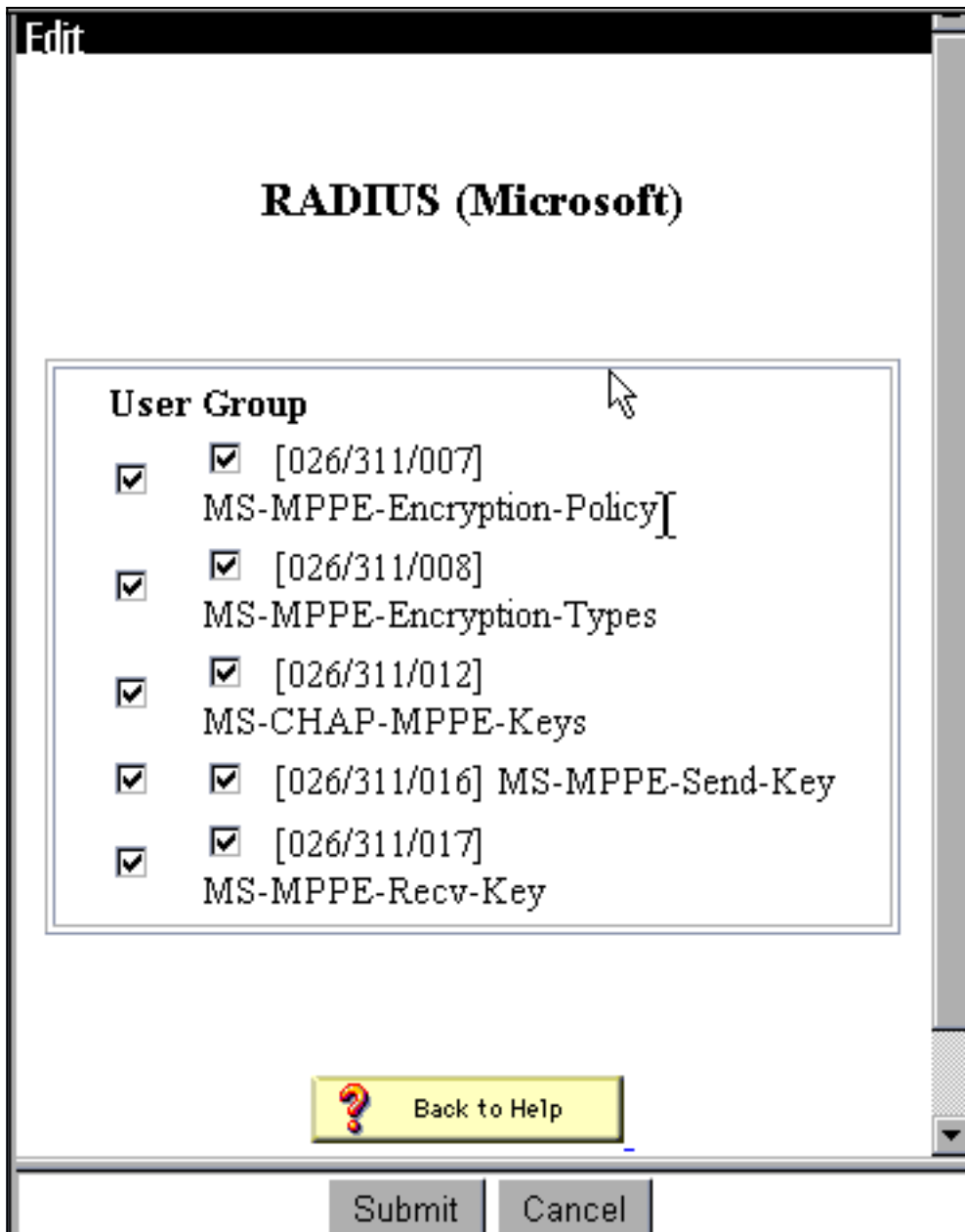
2. Cisco Secure ACS for Windows에서 ACS 서버 네트워크 구성에 VPN Concentrator를 추가하고 사전 유형을 식별합니다

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)"/>

- 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

3. Windows용 Cisco Secure ACS에서 **Interface Configuration(인터페이스 컨피그레이션) > RADIUS(Microsoft)**로 이동하여 Microsoft MPPE(Point-to-Point Encryption) 특성을 확인하여 특성이 그룹 인터페이스에 나타나도록 합니다



4. Cisco Secure ACS for Windows에서 사용자를 추가합니다. 나중에 암호화가 필요할 경우 사용자 그룹에서 MPPE(Microsoft RADIUS) 특성을 추가합니다

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

5. VPN 3000 Concentrator에서 Configuration(컨피그레이션) > System(시스템) > Servers(서버) > **Authentication Servers(인증 서버)로 이동합니다.** 목록에서 인증 서버를 선택한 다음 **테스트**를 선택합니다. 사용자 이름과 비밀번호를 입력하여 VPN Concentrator에서 Cisco Secure ACS for Windows 서버로의 인증을 테스트합니다.올바른 인증에서 VPN Concentrator는 "Authentication Successful(인증 성공)" 메시지를 표시해야 합니다. Windows용 Cisco Secure ACS의 실패는 **Reports and Activity(보고서 및 활동) > Failed Attempts(실패 시도)에 기록됩니다.** 기본 설치에서 이러한 보고서는 C:\Program Files\CiscoSecure ACS v2.5\Logs\Failed Attempts의 디스크에 저장됩니다

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

- 이제 PC에서 VPN Concentrator로의 인증을 확인했으므로 Concentrator에서 Cisco Secure ACS for Windows 서버로의 인증을 확인했으므로 Cisco Secure ACS for Windows RADIUS로 PPTP 사용자를 전송하도록 VPN Concentrator를 재구성할 수 있습니다. Windows용 Cisco Secure ACS 서버를 서버 목록의 맨 위로 이동하면 됩니다. VPN Concentrator에서 이 작업을 수행하려면 Configuration(컨피그레이션) > System(시스템) > **Servers(서버)** > **Authentication Servers(인증 서버)**로 이동합니다

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. Configuration(컨피그레이션) > User Management(사용자 관리) > Base Group(기본 그룹)으로 이동하고 PPTP/L2TP 탭을 선택합니다. VPN Concentrator 기본 그룹에서 PAP 및 MSCHAPv1에 대한 옵션이 활성화되었는지 확인합니다

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. General(일반) 탭을 선택하고 Tunneling Protocols(터널링 프로토콜) 섹션에서 PPTP가 허용되는지 확인합니다

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. Windows RADIUS용 Cisco Secure ACS 서버의 사용자와 PPTP 인증을 테스트합니다. 이 방법이 작동하지 않으면 [디버깅](#) 섹션을 참조하십시오.

MPPE 추가(암호화)

Windows RADIUS PPTP용 Cisco Secure ACS 인증이 암호화 없이 작동하는 경우 VPN 3000 Concentrator에 MPPE를 추가할 수 있습니다.

- VPN Concentrator에서 Configuration(구성) > User Management(사용자 관리) > Base Group(기본 그룹)으로 이동합니다.
- PPTP Encryption(PPTP 암호화) 섹션에서 Required(필수), 40비트 및 128비트 옵션을 선택합니다. 모든 PC가 40비트 및 128비트 암호화를 모두 지원하는 것은 아니므로 두 옵션을 모두 선택하여 협상을 허용합니다.
- PPTP Authentication Protocols(PPTP 인증 프로토콜) 섹션에서 MSCHAPv1 옵션을 선택합니다. (이전 단계에서 암호화를 위한 Cisco Secure ACS for Windows 2.5 사용자 특성을 이미 구성했습니다.)

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.

참고: PPTP 클라이언트는 최적 또는 필수 데이터 암호화 및 MSCHAPv1(옵션이 있는 경우)에 대해 인식되어야 합니다.

계정 추가

인증을 설정한 후 VPN Concentrator에 어카운팅을 추가할 수 있습니다. Configuration(컨피그레이션) > System(시스템) > Servers(서버) > Accounting Servers(어카운팅 서버)로 이동하여 Cisco Secure ACS for Windows 서버를 추가합니다.

Cisco Secure ACS for Windows에서 회계 레코드는 다음과 같이 표시됩니다.

```
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
```

다음을 확인합니다.

현재 이 구성에 대해 사용 가능한 확인 절차가 없습니다.

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

디버깅 활성화

연결이 작동하지 않으면 Configuration(구성) > System(시스템) > Events(이벤트) > Classes(클래스) > **Modify(수정)**로 이동하여 VPN Concentrator에 PPTP 및 AUTH 이벤트 클래스를 추가할 수 있습니다. PPTPDBG, PPTPDECODE, AUTHDBG 및 AUTHDECODE 이벤트 클래스를 추가할 수도 있지만 이러한 옵션은 너무 많은 정보를 제공할 수 있습니다.

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.

Monitoring(모니터링) > Event Log(이벤트 로그)로 이동하여 이벤트 로그를 검색할 수 있습니다.

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

디버깅 - 정상 인증

VPN Concentrator의 정상 디버그는 다음과 유사합니다.

```

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

```

가능한 오류

아래와 같이 오류가 발생할 수 있습니다.

[Windows RADIUS용 Cisco Secure ACS 서버의 사용자 이름 또는 암호가 잘못되었습니다.](#)

- VPN 3000 Concentrator 디버그 출력

```
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
```

- Windows용 Cisco Secure ACS 로그 출력

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

- 사용자에게 표시되는 메시지(Windows 98에서)

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

Concentrator에서 "MPPE Encryption Required(MPPE 암호화 필요)"가 선택되었지만 Windows용 Cisco Secure ACS가 MS-CHAP-MPPE-Keys 및 MS-CHAP-MPPE-Types에 대해 구성되지 않았습
니다.

- VPN 3000 Concentrator 디버그 출력AUTHDECODE(1-13 Severity) 및 PPTP 디버그(1-9 Severity)가 켜져 있으면 Windows용 Cisco Secure ACS가 서버의 access-accept(부분 로그)에 공급업체별 특성 26(0x1A)을 보내지 않음을 로그에 표시합니다.

```
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.
```

- Windows용 Cisco Secure ACS 로그 출력에 오류가 표시되지 않습니다.

- 사용자에게 표시되는 메시지

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

[관련 정보](#)

- [Cisco VPN 3000 Series Concentrator 지원 페이지](#)
- [Cisco VPN 3000 Series 클라이언트 지원 페이지](#)
- [IPSec 지원 페이지](#)
- [Cisco Secure ACS for Windows 지원 페이지](#)
- [RADIUS 지원 페이지](#)
- [PPTP 지원 페이지](#)

- [RFC 2637: PPTP\(Point-to-Point Tunneling Protocol\)](#)
- [RFC\(Request for Comments\)](#)
- [기술 지원 및 문서 - Cisco Systems](#)