

Настройка PPTP концентратора VPN 3000 с Cisco Secure ACS Iкz аутентификации Windows RADIUS

Содержание

[Введение](#)

[Перед началом работы](#)

[Условные обозначения](#)

[Предварительные условия](#)

[Используемые компоненты](#)

[Схема сети](#)

[Настройка концентратора VPN 3000](#)

[Добавление и Cisco Secure ACS Настройки для Windows](#)

[Добавление протокола MPPE \(шифрование\)](#)

[Добавление автоматического учета](#)

[Проверка](#)

[Устранение неполадок](#)

[Включение отладку](#)

[Отладки - успешная проверка подлинности](#)

[Возможные ошибки](#)

[Дополнительные сведения](#)

[Введение](#)

Cisco VPN 3000 Concentrator поддерживает метод туннелирования PPTP для Windows-клиентов. Поддержки концентратора 40-разрядное и 128-разрядное шифрование для защищенного надежного соединения. Этот документ описывает, как настроить PPTP на VPN 3000 Concentrator с Cisco Secure ACS для Windows для Проверки подлинности RADIUS.

См. [Настройку межсетевой экран Cisco Secure PIX для Использования PPTP](#) для настройки подключений PPTP к PIX.

См. [Cisco Secure ACS Настройки для Аутентификации PPTP маршрутизатора Windows](#) для устанавливания Подключения ПК к маршрутизатору; это предоставляет проверку подлинности пользователя системе управления доступом Cisco Secure Access Control System (ACS) 3.2 для Windows Server, прежде чем вы позволите пользователю в сеть.

[Перед началом работы](#)

[Условные обозначения](#)

[Дополнительные сведения об условных обозначениях см. в документе Технические рекомендации Cisco. Условные обозначения.](#)

[Предварительные условия](#)

Этот документ предполагает, что локальная аутентификация PPTP работает перед добавляющим Cisco Secure ACS для аутентификации Windows RADIUS. Посмотрите, [Как Настроить PPTP концентратора VPN 3000 с Локальной проверкой подлинности](#) для получения дополнительной информации о локальной аутентификации PPTP. Для полного списка требований и ограничений, см. то, [Когда Шифрование PPTP Поддерживается на Cisco VPN 3000 Concentrator?](#)

[Используемые компоненты](#)

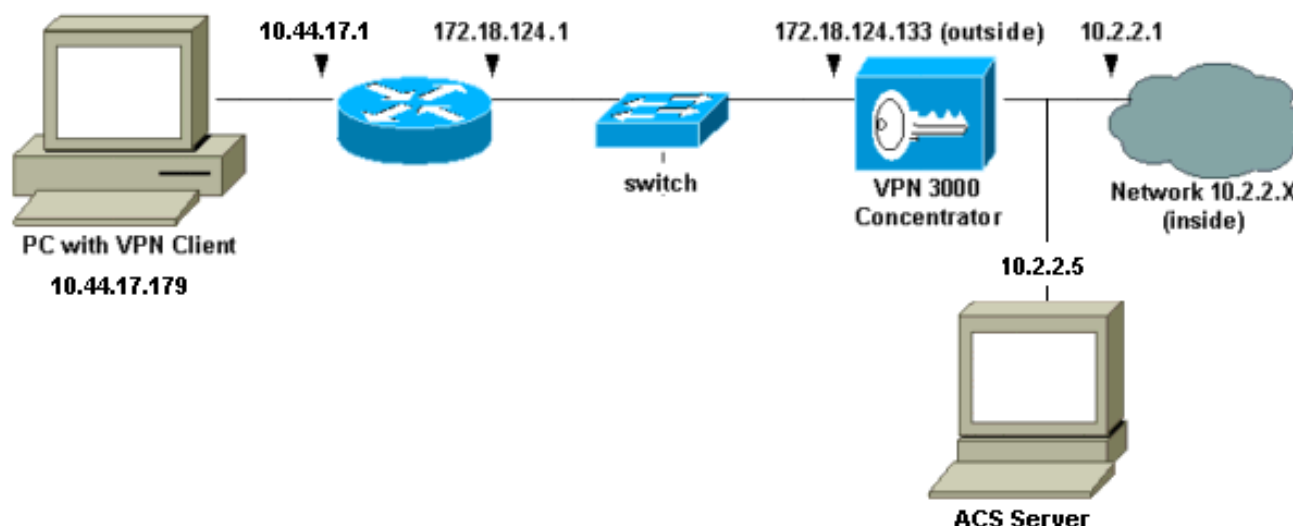
Сведения в этом документе основаны на версиях оборудования и программного обеспечения, указанных ниже.

- Cisco Secure ACS для Версий Windows 2.5 и позже
- Версии 2.5.2. С VPN 3000 Concentrator и позже (Эта конфигурация была проверена с версией 4.0. x.)

Сведения, содержащиеся в данном документе, были получены с устройств в специальной лабораторной среде. Все устройства, описанные в данном документе, были запущены с конфигурацией по умолчанию. При работе с реальной сетью необходимо полностью осознавать возможные результаты использования всех команд.

[Схема сети](#)

В данном документе используется сетевая установка, показанная на следующей схеме.



[Настройка концентратора VPN 3000](#)

[Добавление и Cisco Secure ACS Настройки для Windows](#)

Выполните эти действия для настройки Концентратора VPN для использования Cisco Secure ACS для Windows.

1. На VPN 3000 Concentrator перейдите к **Configuration > System > Servers > Authentication Servers** и добавьте Cisco Secure ACS для Windows Server и ключа ("cisco123" в данном примере).

The screenshot shows the configuration page for adding a user authentication server. The breadcrumb navigation at the top reads "Configuration | System | Servers | Authentication | Add". Below the navigation is the instruction "Configure and add a user authentication server." The form includes the following fields and options:

- Server Type:** A dropdown menu currently 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 input field containing "10.2.2.5" with the instruction "Enter IP address or hostname."
- Server Port:** A text input field containing "0" with the instruction "Enter 0 for default port (1645)."
- Timeout:** A text input field containing "4" with the instruction "Enter the timeout for this server (seconds)."
- Retries:** A text input field containing "2" with the instruction "Enter the number of retries for this server."
- Server Secret:** A password input field with masked characters and the instruction "Enter the RADIUS server secret."
- Verify:** A second password input field with masked characters and the instruction "Re-enter the secret."

At the bottom of the form are two buttons: "Add" and "Cancel". A mouse cursor is pointing at the "Add" button.

2. В Cisco Secure ACS для Windows добавьте Концентратор VPN к Конфигурации сети сервера ACS и определите тип

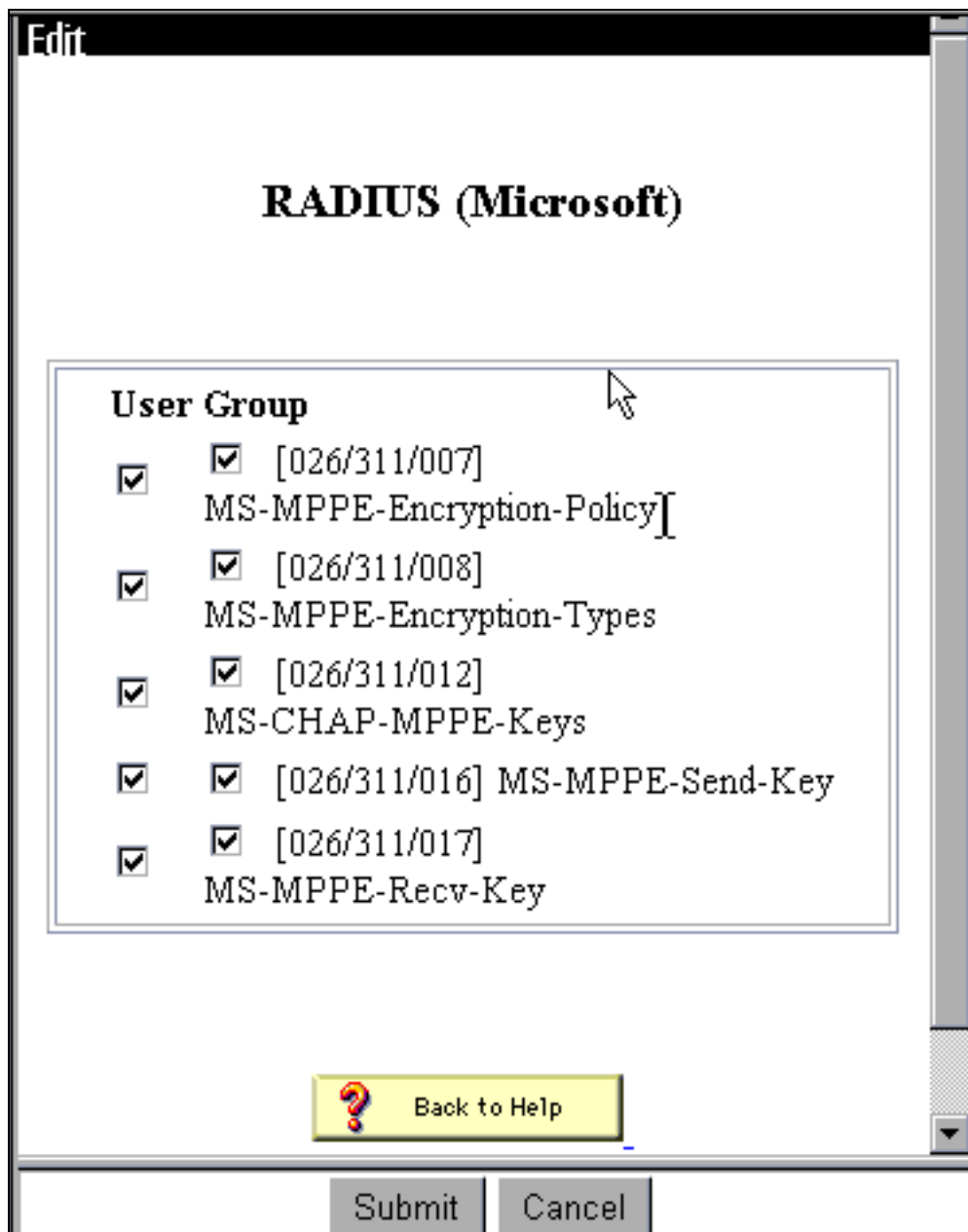
Access Server Setup For VPN3000

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

словаря.

3. В Cisco Secure ACS для Windows перейдите к **Interface Configuration> Radius (Microsoft)** и проверьте атрибуты Средств шифрования Microsoft точка-точка (MPPE) так, чтобы атрибуты появились в групповом



интерфейсе.

4. В Cisco Secure ACS для Windows добавьте пользователя. В группе пользователя добавьте MPPE (Microsoft RADIUS) атрибуты, в случае, если вы требуете шифрования в более позднее

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

время.

- На VPN 3000 Concentrator перейдите к **Configuration> System> Servers> Authentication Servers**. Выберите сервер проверки подлинности из списка, и затем выберите **Test**. Тестовая аутентификация от Концентратора VPN до Cisco Secure ACS для Windows Server путем ввода имени пользователя и пароля. На успешной проверке подлинности Концентратор VPN должен показать Сообщение "authentication successful". Сбои в Cisco Secure ACS для Windows зарегистрированы в **Отчётах и Действии> Неудачные попытки**. В установке по умолчанию эти отчёты сохранены на диске в C:\Program Files\CiscoSecure ACS v2.5\Logs\Failed Attempts.

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

6. Так как вы теперь проверили, что аутентификация от ПК до Концентратора VPN работает и от концентратора до Cisco Secure ACS для Windows Server, можно реконфигурировать Концентратор VPN, чтобы передать пользователям PPTP к Cisco Secure ACS для Windows RADIUS путем перемещения Cisco Secure ACS для Windows Server к вершине списка серверов. Чтобы сделать это на Концентраторе VPN, перейдите к **Configuration> System> Servers> Authentication Servers**.

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. Перейдите к **Configuration > User Management > Base Group** и выберите вкладку **PPTP/L2TP**. В базовой группе Концентратора VPN гарантируйте, что включены опции для PAP и MSCHAPv1.

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. Выберите **Вкладку Общие** и гарантируйте, что PPTP разрешен в разделе Протоколов туннелирования.

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.

9. Тестовая аутентификация PPTP с пользователем в Cisco Secure ACS для Сервера Windows Radius. Если это не работает, посмотрите [Раздел отладки](#).

[Добавление протокола MPPE \(шифрование\)](#)

Если Cisco Secure ACS для аутентификации PPTP Windows RADIUS работает без шифрования, можно добавить MPPE к VPN 3000 Concentrator.

1. На Концентраторе VPN перейдите к **Configuration> User Management> Base Group**.
2. Под разделом для Шифрования PPTP проверьте опции для **Требуемого, 40-разрядного, и 128-разрядный**. С тех пор не все PC поддерживают и 40-разрядное и 128-разрядное шифрование, проверяют обе опции для учета согласования.
3. Под разделом для Протоколов Аутентификации PPTP проверьте опцию для **MSCHAPv1**. (Вы уже настроили Cisco Secure ACS для атрибутов пользователя Windows 2.5 для шифрования в более раннем шаге.)

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.

Примечание: Клиент PPTP должен быть распознан за оптимальный или обязательное шифрование данных и MSCHAPv1 (если опция).

Добавление автоматического учета

После установления аутентификации можно добавить учет к Концентратору VPN. Перейдите к **Configuration > System > Servers > Accounting Servers** и добавьте Cisco Secure ACS для Windows Server.

В Cisco Secure ACS для Windows учетные записи появляются следующим образом.

```
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
```

Проверка

В настоящее время для этой конфигурации нет процедуры проверки.

Устранение неполадок

В этом разделе описывается процесс устранения неполадок конфигурации.

[Включение отладки](#)

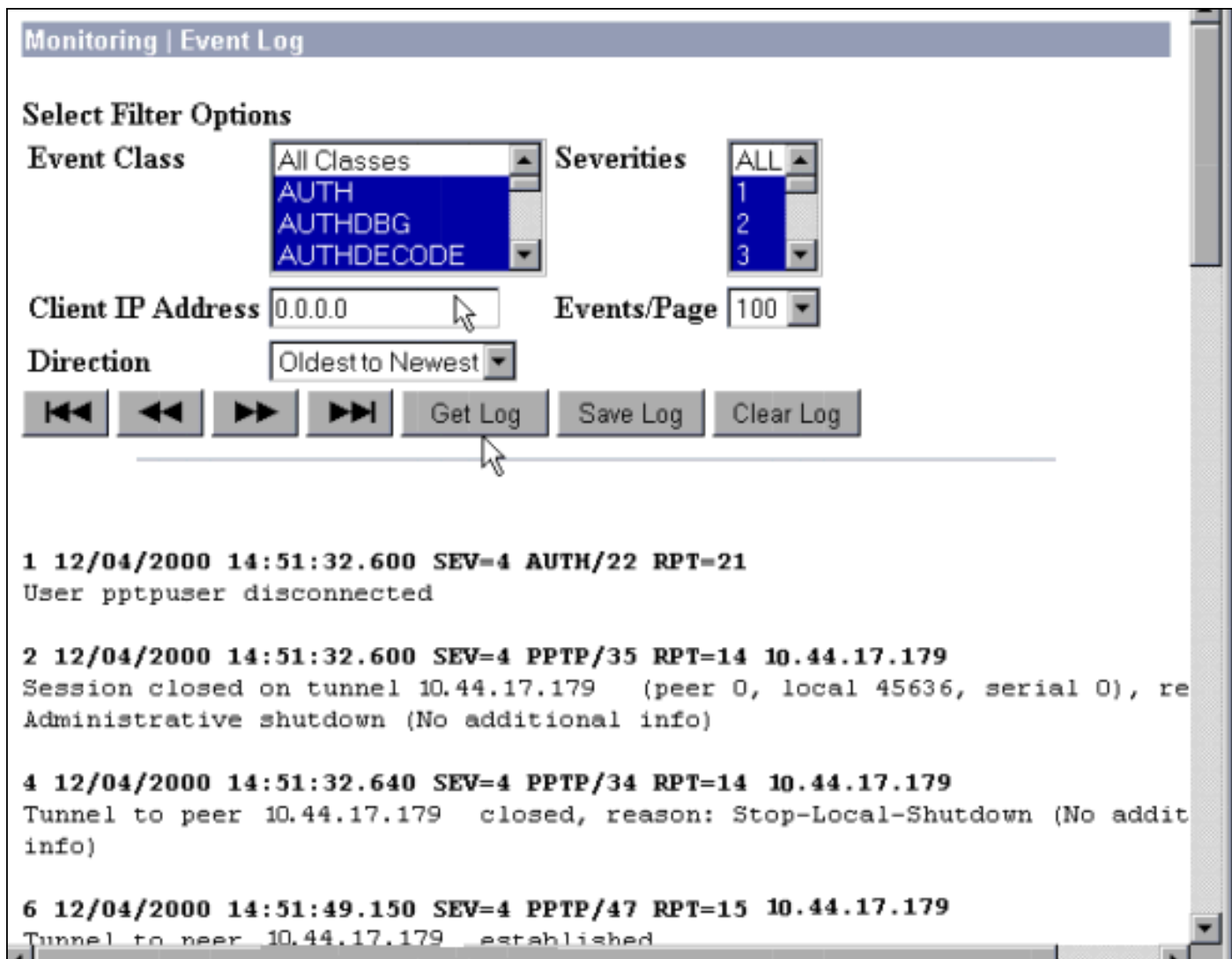
Если соединения не работают, можно добавить PPTP, и Параметры Auth Event Class к Концентратору VPN тем, чтобы переходить **Configuration> System> Events> Classes> Modify**. Можно также добавить PPTPDBG, PPTPDECODE, AUTHDBG и Классы события authdecode, но эти опции могут предоставить слишком много информации.

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.

Можно получить журнал событий, перейдя к **Monitoring> Event Log**.



[Отладки - успешная проверка подлинности](#)

Хорошие отладки на Концентраторе VPN будут выглядеть подобными следующему.

```

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

```

[Возможные ошибки](#)

Можно встретиться с возможными ошибками как показано ниже.

[Неверное имя пользователя или пароль на Cisco Secure ACS для Сервера Windows Radius](#)

- **Выходные данные отладки VPN 3000 Concentrator** 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 для вывода лога Windows** 03/18/2000,08:02:47,Authen failed,
baduser,,,CS user
unknown,,,1155,10.2.2.1
- **Сообщение, что пользователь видит (от 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.

"Шифрование MPPE, Требуемое", выбрано на концентраторе, но Cisco Secure ACS для Windows Server не настроен для MS-CHAP-MPPE-Keys и MS-CHAP-MPPE-Types

- **Выходные данные отладки VPN 3000 Concentrator**Если AUTHDECODE (Степени серьезности ошибки 1-13) и отладка PPTP (Степени серьезности ошибки 1-9) идет, журнал показывает, что Cisco Secure ACS для Windows Server не передает определяемые производителем характеристика 26 (0x1A) в access-accept от сервера (частичный журнал).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 для вывода лога Windows не показывает сбоя.**
- **Сообщение, что видит пользователь**Error 691: The computer you have dialed in to has
denied access because
the username and/or password is invalid on the domain.

Дополнительные сведения

- [Страница поддержки концентратора Cisco VPN серии 3000](#)
- [Страница поддержки Cisco VPN 3000 Series Client](#)
- [Страница поддержки IPSec](#)
- [Страница поддержки Cisco Secure ACS для Windows](#)
- [Страница поддержки RADIUS](#)
- [Страница поддержки PPTP](#)
- [RFC 2637: Протокол PPTP](#)

- [Запросы комментариев \(RFC\)](#)
- [Cisco Systems – техническая поддержка и документация](#)