# Руководство по настройке Wired Dot1x Version 1.05

## Содержание


Введение
Предварительные условия
Требования
Используемые компоненты
Условные обозначения
Установка служб Microsoft Certificate
Установите Microsoft Certificate (CA) сервер
ACS для Windows Certificate Setup
Создайте серверный сертификат
Создайте новый шаблон сертификата
Утвердите сертификат от CA
Загрузите серверный сертификат к серверу ACS
Установите сертификат CA на сервере ACS
Установите ACS для Использования серверного сертификата
Настройка сертификата прибора ACS
Создайте и установите подписанный сертификат
Создайте серверный сертификат Использование CSR
Загрузите сертификат CA к серверу FTP
Установите сертификат CA на устройстве
Настройте параметры настройки глобальной аутентификации
Установите ACS для разрешения аутентификации компьютера
Установите AP на ACS
Настройте коммутатор для Dot1x
Конфигурация таймеров dot1x
Установите клиента для PEAP с аутентификацией компьютера
Динамическое назначение сетей VLAN для 802.1x и ACS
Проверка
Подведенный для создания 'CertificateAuthority. Запрос' объектное сообщение об ошибках
Устранение неполадок
Проблема
Решение
Дополнительные сведения


## Введение

Этот документ предоставляет пример конфигурации для проводной версии 1.05 dot1x.

Это руководство покрывает сертификаты, созданные Microsoft CA и саморегистрируемыми сертификатами, которые поддерживаются с Access Control Server (ACS) 3.3. Использование саморегистрируемого сертификата оптимизировало начальную установку PEAP значительно, так как не требуется никакой внешний CA. В это время период истечения по умолчанию саморегистрируемого сертификата составляет только один год и не может быть изменен. Это довольно стандартно когда дело доходит до серверных сертификатов, но так как подписанный сертификат также действует как корневой сертификат CA, это может означать устанавливать новый сертификат на каждом клиенте, каждый год при использовании Microsoft supplicant (пока вы не выбираете опцию “Validate Server Certificate”). Это, рекомендуют использовать саморегистрируемые сертификаты только как временное измерение, пока не может использоваться традиционный CA. Если вы хотите использовать саморегистрируемый сертификат, посмотрите раздел.

802.1x был разработан для аутентификации хостов на проводной сети вместо реальных пользователей. Попытка аутентифицировать пользователей через 802.1x на проводной сети может привести к нежелательному поведению, такому как проверенный пользователь 802.1x, не вышедший из системы сеть, пока плата NIC не освобождает порт.

# Предварительные условия

## Требования

Прежде чем использовать эту конфигурацию, убедитесь, что выполняются эти требования:

- переключает рабочий релиз 12.1 программного обеспечения Cisco IOS (12c) EA1 и позже (только EI) или CatOS 6.2 и позже
- ACS 3.2
- Windows 2000 SP3 (с заплатой), SP4 или SP1 XP

## Используемые компоненты

Настоящий документ не имеет жесткой привязки к каким-либо конкретным версиям программного обеспечения и оборудования.

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

## Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Технические рекомендации Cisco. Условные обозначения.

# Установка служб Microsoft Certificate

В этом разделе содержатся сведения о настройке функций, описанных в этом документе.

**Примечание:** Информационный сервер интернета (IIS) должен быть установлен перед

установкой CA., Избегают давать CA то же название как сервер ACS; выполнение так может заставить клиентов PEAP отказывать аутентификацию, потому что они запутываются, когда корневой сертификат CA найден с тем же названием как серверный сертификат. Эта проблема не уникальна для клиентов Cisco.

### Установите Microsoft Certificate (CA) сервер

Выполните следующие действия:

1. **Выберите Start > Settings > Control Panel.**
2. В Панели управления откройте **Добавления/удаления программы**.
3. В Добавлениях/удалениях программы выберите **Add/Remove Windows Components**.
4. Выберите **Certificate Services**.
5. **Нажмите кнопку Next.**
6. Нажмите **Yes** к сообщению IIS.
7. Выберите автономное (или Предприятие) узел CA.
8. **Нажмите кнопку Next.**
9. Назовите CA.**Примечание:** Все другие коробки являются дополнительными.**Примечание:** Избегите давать CA то же название как сервер ACS. Это может заставить клиентов PEAP отказывать аутентификацию, потому что они становятся смущенными, когда корневой сертификат CA найден с тем же названием как серверный сертификат. Эта проблема не уникальна для клиентов Cisco. Конечно, если вы не планируете использование PEAP, это не применяется.
10. **Нажмите кнопку Next.**
11. По умолчанию базы данных корректен.
12. **Нажмите кнопку Next.**IIS должен быть установлен перед установкой CA.

## ACS для Windows Certificate Setup

### Создайте серверный сертификат

Выполните следующие действия:

1. От вашего сервера ACS перейдите к CA (http://IP_of_CA_server/certsrv/).
2. Проверьте **Запрос** коробка **сертификата**.
3. **Нажмите кнопку Next.**
4. Выберите **Расширенный запрос**.
5. **Нажмите кнопку Next.**
6. Выберите **Подтверждение запроса о сертификате в данный центр сертификации с использованием формы**.
7. **Нажмите кнопку Next.**
8. Введите имя на название (CN) коробка.
9. Для Намеченной Цели выберите **Server Authentication Certificate**.**Примечание:** При использовании Предприятие CA, выбираете **Web Server** из первого выпадающего списка.
10. Выберите их под Ключевой Опцией для создания нового шаблона:**CSP — v1.0 Microsoft Base Cryptographic ProviderРазмер ключа — 1024Примечание:** Сертификаты, созданные с размером ключа, больше, чем 1024, могут работать для HTTPS, но не

будут работать для PEAP.**Примечание:** Windows 2003 Enterprise CA позволяет размеры ключа, больше, чем 1024, но использование ключа, больше, чем 1024, не работает с PEAP. Аутентификация, могло бы казаться, прошла бы в ACS, но клиент просто "зависнет" при попытке аутентификации.**Ключи как экспортныеПримечание:** Microsoft изменила Шаблон веб-сервера с выпуском Windows 2003 Enterprise CA. With это изменение шаблона, ключи больше не являются экспортными, и опция отображается серым. Нет никаких других шаблонов сертификата, предоставленных сервисами сертификации, которые являются для проверки подлинности сервера, или которые дают способность отметить ключи как экспортные в раскрывающемся меню. Для создания нового шаблона, который делает так, видит Создавание Нового раздела Шаблона сертификата.**Используйте память локального компьютераПримечание:** Все другие выборы нужно оставить как по умолчанию.

11. **Нажмите кнопку Submit (Отправить).**
12. Необходимо получить это сообщение: Ваш запрос сертификата был получен.

## Создайте новый шаблон сертификата

Выполните следующие действия:

1. Выберите **Start> Run> certmpl.msc**.
2. Щелкните правой кнопкой мыши **Шаблон веб-сервера**.
3. Выберите **Duplicate Template**.
4. Дайте шаблону название, такое как ACS.
5. Нажмите вкладку **Request Handling**.
6. Выберите **секретный ключ Allow, который будет экспортироваться**.
7. Нажмите кнопку **CSP**.
8. Выберите **v1.0 Microsoft Base Cryptographic Provider**.
9. **Нажмите кнопку OK.Примечание:** Все другие опции нужно оставить как по умолчанию.
10. **Щелкните "Применить".**
11. **Нажмите кнопку OK.**
12. Откройте моментальный снимок MMC CA - в.
13. Щелкните правой кнопкой мыши **шаблоны сертификата**.
14. Выберите **New> Certificate Template to Issue**.
15. Выберите новый шаблон, который вы создали.
16. **Нажмите кнопку OK.**
17. Перезапустите CA.Новый шаблон включен в выпадающий список Шаблона сертификата.

## Утвердите сертификат от CA

Выполните следующие действия:

1. Выберите **Start> Programs> Administrative Tools> Certificate Authority**.
2. На левом оконном стекле разверните сертификат.
3. Выберите **Pending Requests**.
4. Щелкните правой кнопкой мыши на сертификате.
5. Выберите **все задачи**.

6. Выберите **Issue**.

## Загрузите серверный сертификат к серверу ACS

Выполните следующие действия:

1. От вашего сервера ACS перейдите к CA (http://IP_of_CA_server/certsrv/).
2. Выберите **проверяют сертификат в состоянии ожидания**.
3. **Нажмите кнопку Next.**
4. Выберите сертификат.
5. **Нажмите кнопку Next.**
6. **Нажмите кнопку Install (Установить).**

## Установите сертификат CA на сервере ACS

**Примечание:** Если ACS и CA установлены на том же сервере, эти шаги не требуются.

1. Выполните следующие действия:

2. От вашего сервера ACS перейдите к CA (http://IP_of_CA_server/certsrv/).
3. Выберите **Retrieve the CA certificate или список отозванных сертификатов**.
4. **Нажмите кнопку Next.**
5. Выберите **закодированный Base 64**.
6. Нажмите **Download CA certificate**.
7. **Нажмите кнопку Open.**
8. **Нажмите кнопку Install Certificate (Установить сертификат).**
9. **Нажмите кнопку Next.**
10. Выберите **Place все сертификаты в следующем хранилище**.
11. **Нажмите кнопку Browse.**
12. Установите флажок **хранилищ Show physical**.
13. На левом оконном стекле разверните **Доверенные корневые центры сертификации**.
14. Выберите **Local Computer**.
15. **Нажмите кнопку OK.**
16. **Нажмите кнопку Next.**
17. **Нажмите кнопку Finish.**
18. Нажмите **OK** на импорте был успешной коробкой.

## Установите ACS для Использования серверного сертификата

Выполните следующие действия:

1. На сервере ACS выберите **System Configuration**.
2. Выберите **ACS Certificate Setup**.
3. Выберите **сертификат Install ACS**.
4. Выберите **сертификат Use из хранилища**.
5. Введите на название CN (то же название, которое использовалось в Шаге 8 Создавания раздела Серверного сертификата).
6. **Нажмите кнопку Submit (Отправить).**

7. На сервере ACS нажмите **конфигурацию системы**.
8. Выберите **ACS Certificate Setup**.
9. Выберите **Edit Certificate Trust List**.
10. Установите флажок для CA.
11. **Нажмите кнопку Submit (Отправить).**

# Настройка сертификата прибора ACS

## Создайте и установите подписанный сертификат

**Примечание:** Если вы не используете внешнего CA., этот раздел только применяется

Выполните следующие действия:

1. На сервере ACS нажмите **System Configuration**.
2. Нажмите **ACS Certificate Setup**.
3. Нажмите **Generate Self-signed Certificate**.
4. Введите предмет сертификата в форме cn=XXXX. В данном примере используется cn=ACS33. Для большего количества параметров конфигурации подписанного сертификата обратитесь к Конфигурации системы: Проверка подлинности и сертификаты.
5. Введите полный путь и название сертификата, который будет создан в коробке Файла сертификата. Например, `c:\acscerts\acs33.cer`.
6. Введите полный путь и название файла закрытого ключа, который будет создан в коробке Файла закрытого ключа. Например, `c:\acscerts\acs33.pvk`.
7. Введите и подтвердите пароль с закрытым ключом.
8. Выберите **1024** из выпадающего списка длины ключа.**Примечание:** В то время как ACS может генерировать размеры ключа, больше, чем 1024, использование ключа, больше, чем 1024, не работает с PEAP. Аутентификация, могло бы казаться, прошла бы в ACS, но клиент "зависает" при попытке аутентификации.
9. Из Дайджеста для подписания со списком выберите дайджест хэша, который будет использоваться для шифрования ключа. В данном примере используется дайджест для подписания с в SHA1.
10. Проверьте**, что Установка генерировала сертификат**.
11. **Нажмите кнопку Submit (Отправить).**

## Создайте серверный сертификат Использование CSR

Выполните следующие действия:

1. От вашего сервера FTP перейдите к CA (http://IP_of_CA_server/certsrv/).
2. Выберите **Request сертификат**.
3. **Нажмите кнопку Next.**
4. Выберите **Расширенный запрос**.
5. **Нажмите кнопку Next.**
6. Выберите **Submit запрос сертификата с помощью base64 кодированные PKC #10 файл или запрос на обновление с помощью base64 кодированные PKC #7 файл**.

7. Вставьте выходные данные от Шага 6 в поле **Base64 Encoded Certificate Request**.
8. **Нажмите кнопку Submit (Отправить).**
9. Нажмите **Download CA certificate**.
10. **Нажмите Save.**
11. Назовите сертификат.
12. Сохраните сертификат к своему каталогу FTP

## Загрузите сертификат CA к серверу FTP

Выполните следующие действия:

1. От вашего сервера FTP перейдите к CA (http://IP_of_CA_server/certsrv/).
2. Выберите **Retrieve the CA certificate или список отозванных сертификатов**.
3. **Нажмите кнопку Next.**
4. Выберите **закодированный Base 64**.
5. Нажмите **Download CA certificate**.
6. **Нажмите Save.**
7. Назовите сертификат.
8. Сохраните сертификат к своему каталогу FTP

## Установите сертификат CA на устройстве

Выполните следующие действия:

1. Выберите **System Configuration> ACS Certificate Setup> ACS Certification Authority Setup**.
2. Нажмите **файл Download CA certificate**.
3. В поле FTP Server введите IP-адрес или имя хоста сервера FTP
4. В поле Login введите допустимое имя пользователя, которое Cisco Secure ACS может использовать для доступа к серверу FTP.
5. Iin Поле Password, введите пароль пользователя.
6. В поле Remote FTP Directory введите относительный путь от корневого каталога сервера FTP до каталога, содержащего файл сертификата CA.
7. В поле Remote FTP File Name введите имя файла сертификата CA.
8. **Нажмите кнопку Submit (Отправить).**
9. Проверьте имя файла в поле.
10. **Нажмите кнопку Submit (Отправить).**
11. Выберите **System Configuration> Service Control** для перезапуска сервисов ACS.

## Настройте параметры настройки глобальной аутентификации

Выполните следующие действия:

1. На сервере ACS нажмите **System Configuration**.
2. Нажмите **Global Authentication Setup**.

Выполните эти шаги для v3.2 ACS и позже:

1. Проверьте **Позволять EAP-MSCHAPv2 при использовании** коробки **Microsoft PEAP**.
2. Проверьте **Позволять EAP-GTC при использовании** коробки **PEAP Cisco**.

3. Установите **Позволять** флажок **Аутентификации Версии MS-CHAP 1**.
4. Установите **Позволять** флажок **Аутентификации Версии MS-CHAP 2**.
5. **Нажмите кнопку Submit (Отправить).**

Выполните эти шаги для v3 1 ACS и позже:

1. Установите **Позволять** флажок **PEAP**.
2. Установите **Позволять** флажок **Аутентификации Версии MS-CHAP 1**.
3. Установите **Позволять** флажок **Аутентификации Версии MS-CHAP 2**.
4. **Нажмите кнопку Submit (Отправить).**

## Установите ACS для разрешения аутентификации компьютера

Выполните следующие действия:

1. Выберите **External User Databases> Database Configuration**.
2. **Выберите Windows Database (База данных Windows).**
3. **Нажмите кнопку Configure (Настроить).**
4. Установите флажок **аутентификации компьютера PEAP Разрешения**.
5. **Нажмите кнопку Submit (Отправить).**

## Установите AP на ACS

Выполните эти шаги для устанавливания AP на ACS:

1. На сервере ACS нажмите **Network Configuration** слева.
2. Для добавления клиента AAA **нажмите Add Запись**.
3. Введите эти значения в коробки:IP-адрес клиента AAA — IP_of_your_APКлюч — Составляет ключ (удостоверьтесь, что ключ совпадает с общим секретным ключом AP),Используемая аутентификация — RADIUS (Cisco Aironet)
4. **Нажмите кнопку Submit (Отправить).**
5. Перезапуск.

## Настройте коммутатор для Dot1x

См. эти документы для конфигурации dot1x:

- Catalyst 2950
- Catalyst 3550
- Catalyst 4500
- Catalyst 6500

## Конфигурация таймеров dot1x

Выполните эти шаги для настройки таймеров dot1x как пар A/V RADIUS:

- Настройте атрибут RADIUS Session-Timeout (Атрибут [27]), который задает время, после которого происходит переаутентификация.
- Настройте атрибут RADIUS Действия Завершения (Атрибут [29]), который задает

действие для исполнения во время переаутентификации. Когда значение атрибута установлено в По умолчанию, концы сеанса IEEE 802.1X, и подключение потеряно во время переаутентификации. Когда значение атрибута установлено в RADIUS-Request, на сеанс не влияют во время переаутентификации.

**Примечание:** Значения для атрибутов 27 и 29 могут быть назначены на каждой группе по отдельности под RADIUS (IETF) раздел. Атрибут набора 27 к переопознавательному периоду, и 29 к Запросу RADIUS.

На коммутаторе выполните эту конфигурацию для коммутатора для принятия значений атрибутов RADIUS от сервера RADIUS:

```
(config-if)#dot1x reauthentication (config-if)#dot1x timeout reauth-period server
```

## Установите клиента для PEAP с аутентификацией компьютера

### Подключитесь к домену

Выполните следующие действия:

**Примечание:** Для выполнения этого шага компьютер должен иметь одно из этих соединений с CA:

- проводное соединение
- беспроводное соединение с отключенной безопасностью 802.1x

1. Войдите к Windows XP с учетной записью, которая имеет администраторские привилегии.
2. Щелкните правой кнопкой мыши на **моем компьютере**.
3. **Выберите Properties.**
4. **Перейдите на вкладку «Имя компьютера».**
5. **Нажмите кнопку «Изменить».**
6. В Поле Имя компьютера введите имя хоста.
7. Выберите **Domain**.
8. Введите имя домена.
9. **Нажмите кнопку ОК.**
10. Диалоговое окно входа в систему отображено. Войдите с учетной записью, которая имеет разрешения для присоединения к домену.
11. Как только компьютер успешно присоединился к домену, перезапустите компьютер. Машина становится участником домена, имеет сертификат для CA, установленного, и пароль для проверки подлинности компьютера автоматически генерируется.

Если клиент присоединился к домену до установки CA, или сертификат CA не был установлен на клиенте, выполните эти шаги:

**Примечание:** Потребность в этом часто обозначается ошибками проверки подлинности (но не всегда) с ошибками, такими как , SSL.

1. От вашего сервера ACS перейдите к CA (http://IP_of_CA_server/certsrv/).
2. Выберите **Retrieve the CA certificate или список отозванных сертификатов**.
3. **Нажмите кнопку Next.**
4. Выберите **закодированный Base 64**.

5. Нажмите **Download CA certificate**.
6. **Нажмите кнопку Open.**
7. **Нажмите кнопку Install Certificate (Установить сертификат).**
8. **Нажмите кнопку Next.**
9. Выберите **Place все сертификаты в следующем хранилище**.
10. **Нажмите кнопку Browse.**
11. Установите флажок **хранилищ Show physical**.
12. На левом оконном стекле разверните сертификат.
13. Выберите **Local Computer**.
14. **Нажмите кнопку OK.**
15. **Нажмите кнопку Next.**
16. **Нажмите кнопку Finish.**
17. Нажмите **OK** на импорте был успешной коробкой.

## Установите SP1 XP для PEAP с аутентификацией компьютера

Выполните следующие действия:

1. **Выбрать Start> Control Panel> Network Connections**.
2. **Выберите Properties.**
3. Нажмите **вкладку Authentication**.
4. Проверьте **разрешать IEEE 802.1x...** коробка.
5. Для типа EAP выберите **Protected EAP**.
6. **Нажмите Properties.**
7. Проверьте **Аутентифицирование как компьютер....** коробка.
8. **Выберите Properties.**
9. Установите флажок для CA
10. **Нажмите кнопку OK.**
11. **Нажмите кнопку OK.**

## Установите Windows 2000 для аутентификации компьютера PEAP

Выполните следующие действия:

1. Если вы выполняете SP3, загружаете и устанавливаете заплату 802.1x: http://support.microsoft.com/default.aspx? kbid=313664. Это не требуется для SP4.
2. Выберите **Start> Settings> Control Panel> Network и Dial-up Connections**.
3. Щелкните правой кнопкой мыши сетевое подключение.
4. **Выберите Properties.**
5. Нажмите **вкладку Authentication**.
6. Выберите **управление доступом к сети Enable с помощью IEEE 802.1x**.
7. Выберите **Protected EAP (PEAP)** от EAP вводят выпадающий список.
8. Проверьте **Аутентифицирование как компьютер...** коробка.
9. **Выберите Properties.**
10. Установите флажок для CA
11. **Нажмите кнопку OK.**
12. **Нажмите кнопку OK.**

**Примечание:** Если нет никакой **вкладки Authentication**, сервис 802.1X установлен в

отключенном состоянии. Для решения этого необходимо включить сервис **Конфигурации беспроводной сети** в списке сервисов.

**Примечание:** Если **вкладка Authentication** присутствует, но недоступна, это указывает, что драйвер сетевого адаптера не поддерживает 802.1x правильно. Проверьте страницу заплаты 802.1x или веб-сайт поставщика для поддерживаемых драйверов.

1. Выполните эти шаги для включения конфигурации беспроводной сети:

2. Щелкните правой кнопкой мыши **мой компьютер**.
3. **Щелкните Manage (Управление).**
4. Нажмите **Services и Applications**.
5. **Нажмите кнопку Services (Службы).**
6. Установите значение запуска для сервиса к Автоматическому.
7. Запустите этот сервис.

## Динамическое назначение сетей VLAN для 802.1x и ACS

Эта опция поддерживается в IOS 12.1 (12c) EA1 (только EI) или 12.1 (14) EA1 или CatOS 7.2 и позже

**Примечание:** 802.1x был разработан для аутентификации хостов на проводной сети вместо реальных пользователей. Попытка аутентифицировать пользователей через 802.1x на проводной сети может привести к нежелательному поведению, такому как динамическое назначение сетей VLAN, назначенное на пользователя, не изменяемого, пока плата NIC не освобождает порт (компьютер перезапущен или powercycled).

Выполните следующие действия:

1. Выберите **Interface Configuration> RADIUS (IETF)**.
2. Проверьте **[064] Tunnel-Type для пользователя/Группового блока**.
3. Проверьте **[065] Туннельный Средний Тип для пользователя/Группового блока**.
4. Проверьте **[081] Tunnel-Private-Group-ID для пользователя/Группового блока**.
5. **Нажмите кнопку Submit (Отправить).**
6. Выберите **пользователя/настройку групп.**
7. Проверьте **[064]** коробка **Tunnel-Type**.
8. Выберите **1** из выпадающего списка Метки.
9. Выберите **VLAN** для Раскрывающегося списка значенего.
10. Выберите **0** для всех последующих выпадающих списков Метки.
11. Проверьте **[065]** коробка **Туннельного Среднего Типа**.
12. Выберите **1** из выпадающего списка Метки.
13. Выберите **802** из Раскрывающегося списка значенего.
14. Выберите **0** для всех последующих выпадающих списков Метки.
15. Проверьте **[081] Tunnel-Private-Group-ID** коробка.
16. Выберите **1** из выпадающего списка Метки.
17. Используйте название VLAN, которая должна быть выдвинута. Это может быть именем по умолчанию и найдено путем запуска **команды show vlan**.
18. Выберите **0** для всех последующих выпадающих списков Метки.
19. **Нажмите кнопку Submit (Отправить).**

# Проверка

## Подведенный для создания 'CertificateAuthority. Запрос' объектное сообщение об ошибках

В этом разделе содержатся сведения, которые помогают убедиться в надлежащей работе конфигурации.

Выполните следующие действия:

1. Выберите **Start> Administrative Tools> IIS**.
2. Выберите **Web Sites> Default Web Site**.
3. Щелкните правой кнопкой мыши **CertSrv**.
4. **Выберите Properties.**
5. Нажмите **кнопку Configuration** в разделе Прикладных режимов вкладки **Virtual Directory**.
6. Нажмите вкладку **Options**.
7. Выберите **состояние сеанса Enable**.**Примечание:** Все другие опции нужно оставить как по умолчанию.
8. **Нажмите кнопку ОК.**
9. **Нажмите кнопку ОК.**
10. Перезапуск IIS.

Если ваши блокировки браузера с сообщением элемента управления ActiveX Загрузки, обратитесь к этой статье относительно Веб-узла Microsoft: Internet Explorer Прекращает Отвечать при "Загрузке элемента управления ActiveX" сообщение Когда Вы Попытка Использовать Сервер сертификатов.

# Устранение неполадок

## Проблема

Когда основной сервер ACS выключается на аутентификации Dot1x, коммутатор не в состоянии связываться с дополнительным сервером ACS; эта ошибка occurs:`"Authen session timed out: Challenge not provided by client."`

### Решение

Эта ошибка происходит, когда таймер простоя не настроен на коммутаторе, который заставляет коммутатор продолжать пробовать основной сервер, который не работает. Это заставляет аутентификацию отказывать. Для решения этой проблемы настройте таймер простоя на коммутаторе так, чтобы контакты переключателя дополнительный сервер ACS после того, как это ждет в течение настроенного времени (в секундах) или количество повторных попыток для достижения основного сервера прежде, полагали, что основной сервер объявлен мертвые или недоступные. Теперь аутентификация успешно выполняется с дополнительным сервером, который активен. Deadtime может быть настроен с этой командой: radius-server dead-criteria [секунды времени [пробует номер] | номер попыток в режиме глобальной конфигурации.

# Дополнительные сведения

- Cisco Secure Access Control Server for Unix
- Cisco Secure Access Control Server for Windows
- Определите - базирующееся руководство по конфигурации сетевых систем
- Cisco Systems – техническая поддержка и документация