Содержание

Введение

Этот документ объясняет, как генерировать Запрос подписи сертификата (CSR) для получения стороннего сертификата с Wireless Control System (WCS) и как загрузить сертификат на WCS.

Предварительные условия

Требования

Убедитесь, что вы обеспечили выполнение следующих требований, прежде чем попробовать эту конфигурацию:

- Знание того, как установить и настроить WCS для главной операции
- Знание самоподписанных и цифровых сертификатов и других механизмов обеспечения безопасности отнеслось к Инфраструктуре открытых ключей (PKI)

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Версия 4.1.91.0 WCS**Примечание:** Генерация CSR, которая использует WCS, только поддерживается начиная с версии 4.1.91.0 WCS.

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 Условные обозначения технических терминов Cisco.

Запрос подписи сертификата (CSR)

Сертификат является электронным документом, который вы используете для определения сервера, компании или некоторого другого объекта и привязать ту идентичность к открытому ключу.

Подписанный сертификат является сертификатом идентификации, который подписан его собственным создателем. Т.е. человек, который создал сертификат также, закончил на его законности.

Сертификаты могут быть самоподписаны или могут быть засвидетельствованы цифровой подписью от центра сертификации (CA).

CAs являются объектами, которые проверяют сертификаты проблемы и личности. Сертификат, что проблемы CA связывают определенный открытый ключ с названием объекта, который сертификат определяет, такие как название сервера или устройства. Только открытый ключ, который сертифицирует сертификат, работает с соответствующим секретным ключом, находившимся в собственности объектом, который определяет сертификат. Сертификаты помогают предотвращать использование поддельных открытых ключей для олицетворения.

CSR является сообщением, что претендент передает к CA для просьбы цифрового сертификата идентификации. Прежде чем CSR создан, претендент сначала генерирует пару ключей, которая держит секретный ключ в секрете. CSR содержит информацию, которая определяет претендента, такого как имя каталога в случае сертификата X.509 и открытый ключ, выбранный претендентом. Соответствующий секретный ключ не включен в CSR, но используется для снабжения цифровой подписью всего запроса.

CSR может сопровождаться другими учетными данными или доказательствами идентичности, требуемой центром сертификации, и центр сертификации может связаться с претендентом на дополнительную информацию. По большей части независимый поставщик CA компания, те, которые Поручают или VeriSign, требует CSR, прежде чем компания сможет создать цифровой сертификат.

Генерация CSR независима от устройства, на котором вы планируете установить внешний сертификат. Поэтому CSR и файл закрытого ключа могут генерироваться на любом отдельном компьютере, который поддерживает генерацию CSR. Генерация CSR не зависима от коммутатора или зависима от устройства в этом случае.

Этот документ объясняет, как генерировать CSR для стороннего сертификата с помощью Cisco WCS.

Генерация CSR Использование WCS

CSR на WCS могут генерироваться с помощью программного средства, доступного в

каталоге установки WCS. Это программное средство называют **keyadmin.bat**.

Примечание: Если WCS установлен на Linux, необходимо будет использовать **keyadmin.sh** программное средство, доступное в**/opt/WCS4.1/bin/**. Данный пример показывает, как генерировать CSR и импортировать подписанный сертификат с помощью WCS, установленного на Microsoft Windows 2003 Server. Пользователь маршрута WCS должен выполнить эту процедуру так, чтобы мог генерироваться сертификат.

Выполните эти шаги для доступа к программному средству:

1. Перейдите **к Командной строке**, доступной с Windows.
2. Пойдите каталог установки WCS, затем к **папке bin**.Например:`c:\CD Program FilesC:\Program Files>CD WCS4.1C:\Program Files\WCS4.1> cd binC:\Program Files\WCS4.1\bin>`Эта папка будет иметь **keyadmin.bat** программное средство, которое используется для генерации CSR.
3. Выполните эти шаги для генерации CSR:Введите эту команду:`keyadmin -newdn -csr genkey [csrFileName]`Это генерирует новую пару ключа/подписанного сертификата и вывело CSR к указанному файлу. Флаг**-newdn** заставляет его вызывать для полей составного имени для сертификата. Важно задать заключительное имя хоста, которое будет использоваться для доступа к WCS в поле CN DN во избежание предупреждений браузера.Например:`c:\Program Files\WCS4.1\bin>keyadmin -newdn -csr genkey C:\TEST\CSR-WCS.PEMThe WCS server is runningChanges will take affect on the next server restartEnter the domain name of the server: TS-WEBEnter the name of your organizational unit: ABCEnter the name of your organization: XYZEnter the name of your city or locality: SanjoseEnter the name of your state or province: CAEnter the two letter code for your country: USGenerating RSA keyConfiguring Apache server for keyWriting certificate signing request to C:\TEST\CSR-WCS.PEM`Как только команда выполняется, информация о CSR генерируется и пишется в файл.Информация о CSR похожа на это:`c:\Program Files\WCS4.1\bin>keyadmin -newdn -csr genkey C:\TEST\CSR-WCS.PEMThe WCS server is runningChanges will take affect on the next server restartEnter the domain name of the server: TS-WEBEnter the name of your organizational unit: ABCEnter the name of your organization: XYZEnter the name of your city or locality: SanjoseEnter the name of your state or province: CAEnter the two letter code for your country: USGenerating RSA keyConfiguring Apache server for keyWriting certificate signing request to C:\TEST\CSR-WCS.PEM`Теперь, когда ваш CSR готов, копия, и вставьте информацию о CSR в любое программное средство регистрации CA.Чтобы скопировать и вставить информацию в регистрационную форму, открывает файл в текстовом редакторе, который не добавляет дополнительные символы. Cisco рекомендует использовать Блокнот Microsoft или UNIX VI. См. веб-сайт независимого поставщика CA для получения дополнительной информации о том, как отправить CSR через программное средство регистрации.После отправки CSR независимому поставщику CA независимый поставщик CA снабжает цифровой подписью сертификат и передает подписанный сертификат обратно по электронной почте.Как только вы возвращаете подписанный сертификат от CA, можно установить его для замены исходного подписанного сертификата путем ввода этой команды:`keyadmin importsignedcert [certFileName]`Сертификат и ключ сохранены в **C:\ProgramFiles\WCS4.1\webnms\apache\conf\ssl.crt**.Сертификат должен быть сертификацией X.509 со знаком в формате PEM, и это должно совпасть с секретным ключом, который первоначально генерировался **командой genkey** (см. шаг 1). Поэтому при генерации ключа снова перед импортом сертификата это отклонит сертификат.

Импортируйте Существующую ранее Пару Ключа/Сертификата к WCS

WCS также имеет условия для импорта существующей ранее пары ключа/сертификата. Для выполнения этого введите эту команду:

keyadmin importkey *[keyFileName] [certFileName]*
Ключ должен быть закодированным PEM закрытым ключом RSA с линией, которая запускается с ЗАКРЫТОГО КЛЮЧА RSA BEGIN, или это может быть закодированный PEM закрытый ключ RSA в формате PKCS8 с линией, которая запускается с СЕКРЕТНОГО КЛЮЧА BEGIN. В любом случае ключ не должен быть защищен паролем.

Сертификат должен быть закодированным PEM сертификатом X.509, который совпадает с ключом.

Импортируйте серверный сертификат с промежуточным CAs

Если сертификат SSL - сервера подписан промежуточным звеном CA, чтобы удостовериться, что WCS пасует назад полную цепочку для ключей CA, необходимо объединить серверный сертификат, промежуточный CAs и корневой сертификат CA в новом сертификате PEM:

keyadmin importkey *[keyFileName] [certFileName]*
Этот новый файл сертификата PEM [certFileName], который будет использоваться с командами:

keyadmin importkey *[keyFileName] [certFileName]*

Проверка

Выполните эти шаги, чтобы проверить, работает ли конфигурация как ожидалось:

1. После того, как вы импортируете подписанный сертификат на WCS, перезапускаете WCS для изменений для вступления в силу.
2. Обратитесь к WCS через web-браузер.Если подписанный сертификат допустим и имеет соответствующее доменное имя, пользователь должен пойти право на страницу входа без проблемы со всплывающим окном сертификата предупреждение диалогового окна.

Устранение неполадок

Программное средство Keyadmin.bat не будет генерировать CSR в каталоге установки

Когда **keyadmin.bat** выполнен в каталоге **WCS\bin** на Windows, эта ошибка появляется:

```
Generating RSA keyConfiguring Apache server for keyWriting certificate signing request toError
generating key java.security.KeyStoreException: Could not create CSRC:\Program Files\WCS4.x\bin>
```
Для решения этого вопроса определите имя файла в некотором другом каталоге помимо каталога установки WCS. Например:

```
C:\Program Files\WCS4.2.81.0\bin>keyadmin -newdn -csr genkey C:\TEST\CSR-WCS.PEMThe WCS server
is runningChanges will take affect on the next server restartEnter the domain name of the
server: ciscoEnter the name of your organizational unit: ciscoEnter the name of your
```

```
organization: ciscoEnter the name of your city or locality: SJEnter the name of your state or
province: CAEnter the two letter code for your country: USGenerating RSA keyConfiguring Apache
server for key\Writing certificate signing request to C:\TEST\CSR-WCS.PEM
```

Дополнительные сведения

- Создание запроса подписи сертификата (CSR) для сертификата от третьей стороны на контроллере WLAN (WLC)
- Устранение неисправностей беспроводной системы управления
- Страница поддержки беспроводных технологий
- Cisco Systems – техническая поддержка и документация