Генерируйте CSR для сторонних сертификатов и загрузите цепочечные сертификаты к WLC

Содержание

Введение
Предварительные условия
Требования
Используемые компоненты
Цепочечные сертификаты
Поддержка цепочечного сертификата
Уровни сертификата
Шаг 1. Генерируйте CSR
Вариант A. CSR с OpenSSL
Вариант B. CSR, генерируемый WLC
Шаг 2. Подпишите сертификат
Вариант A: Получите Файл Final.pem из своего Предприятия CA
Вариант B: Получите файл Final.pem из независимого поставщика CA
CLI шага 3. Загрузите сторонний сертификат к WLC с CLI
GUI шага 3. Загрузите сторонний сертификат к WLC с GUI
Устранение неполадок
Дополнительные сведения

Введение

Этот документ описывает, как генерировать Запрос подписи сертификата (CSR) для получения стороннего сертификата и как загрузить цепочечный сертификат к Беспроводной локальной сети (WLAN) контроллер (WLC).

Предварительные условия

Требования

Перед попыткой этой конфигурации необходимо ознакомиться с этими темами:

- Как настроить WLC, Облегченную точку доступа (LAP) и клиентскую беспроводную карту для главной операции
- Как использовать приложение OpenSSL
- Инфраструктура открытых ключей и цифровые сертификаты

Используемые компоненты

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

- WLC Cisco 5508, который выполняет версию микропрограммы 8.3.102
- Приложение OpenSSL для Microsoft Windows
- Программное средство регистрации, которое является определенным для стороннего Центра сертификации (CA)

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.

Цепочечные сертификаты

Цепочка сертификатов является последовательностью сертификатов, где каждый сертификат в цепочке подписан последующим сертификатом. Цель цепочки сертификатов состоит в том, чтобы установить цепочку доверия от сертификата однорангового узла до доверяемого сертификата CA. CA ручается за идентичность в сертификате однорангового узла, когда это подписывает его. Если CA является тем, которому вы доверяете, который обозначен присутствием копии сертификата CA в вашем каталоге корневого сертификата, это подразумевает, что можно доверять сертификату однорангового узла со знаком также.

Часто, клиенты не принимают сертификаты, потому что они не были созданы известным CA., клиент, как правило, сообщает, что не может быть проверена законность сертификата. Дело обстоит так, когда сертификат подписан промежуточным звеном CA, которое не известно клиентскому браузеру. В таких случаях необходимо использовать цепочечный сертификат SSL или группу сертификата.

Поддержка цепочечного сертификата

Контроллер обеспечивает сертификат устройства, который будет загружен как цепочечный сертификат для web-аутентификации.

Уровни сертификата

- Уровень 0 - Использование только серверного сертификата на WLC
- Уровень 1 - Использование серверного сертификата на WLC и корневом сертификате CA
- Уровень 2 - Использование серверного сертификата на WLC, одном одиночном промежуточном сертификате CA и корневом сертификате CA
- Уровень 3 - Использование серверного сертификата на WLC, двух промежуточных сертификатах CA и корневом сертификате CA

WLC не поддерживает объединенные в цепочку сертификаты больше чем 10 КБ в размере на WLC. Однако это ограничение было удалено в Версии 7.0.230.0 WLC и позже.

> **Примечание:** Цепочечные сертификаты поддерживаются для web-аутентификации только; они не поддерживаются для сертификата управления.

Сертификаты web-аутентификации могут быть любым из них:

- Цепочечный
- Освобожденный
- Автоматически генерируемый

Примечание: В Версии 7.6 WLC и позже, только цепочечные сертификаты поддерживаются в WLC для web-аутентификации.

Для получения информации о том, как использовать освобожденные сертификаты на WLC, обратитесь для Генерации CSR для Сторонних Сертификатов и Загрузки Освобожденные Сертификаты к WLC.

Этот документ обсуждает, как должным образом установить цепочечный сертификат Протокола SSL к WLC.

Шаг 1. Генерируйте CSR

Существует два способа генерировать CSR. Любой вручную с OpenSSL (единственный путь, возможный в пред8.3 программных обеспечениях WLC) или использование самого WLC для генерации CSR (Доступный после 8.3.102).

Вариант A. CSR с OpenSSL

Примечание: Версия 58 Chrome и позже не доверяет Общему имени одного только сертификата и требует, чтобы также присутствовало Подчиненное Альтернативное название. Следующий раздел объяснит, как добавить поля SAN к CSR OpenSSL, который является новым требованием для этого браузера.

Выполните эти шаги для генерации CSR с OpenSSL:

1. Установите и откройте OpenSSL .

   В Microsoft Windows, по умолчанию, openssl.exe расположен в **C:\> openssl> bin**.

   Примечание: Версия 0.9.8 OpenSSL является рекомендуемой версией для старых версий WLC; однако, с Версии 7.5, поддержка Версии 1.0 OpenSSL была также добавлена (обратитесь к идентификатору ошибки Cisco, CSCti65315 - Нуждаются в поддержке для сертификатов, генерируемых с помощью v1.0 OpenSSL), и рекомендуемая версия для использования. Работы OpenSSL 1.1 были также протестированы и работают отлично на 8.x и более поздние версии WLC.
2. Найдите свой файл config OpenSSL и сделайте копию из него для редактирования его для этого CSR. Отредактируйте копию для добавления следующих разделов:
3. ```
   [req]
   req_extensions = v3_req

   [ v3_req ]
   ```
   ```

```
# Extensions to add to a certificate request

basicConstraints = CA:FALSE
keyUsage = nonRepudiation, digitalSignature, keyEncipherment
subjectAltName = @alt_names

[alt_names]
DNS.1 = server1.example.com
DNS.2 = mail.example.com
DNS.3 = www.example.com
DNS.4 = www.sub.example.com
DNS.5 = mx.example.com
DNS.6 = support.example.com
```

Линии полужирным выше не присутствовали или были прокомментированы в нашей лабораторной работе openSSL версия, она может варьироваться значительно в зависимости от операционной системы и openssl версии. Мы сохраняем эту измененную версию config как **openssl-san.cnf** для данного примера.

4. Выполните эту команду для генерации нового CSR:

```
OpenSSL>req -new -newkey rsa:1024 -nodes -keyout mykey.pem -out myreq.pem -config openssl-san.cnf
```

Примечание: WLC поддерживают максимальный размер ключа 2,048 битов.

5. После выдачи команды существует приглашение для некоторой информации: название страны, состояние, город, и т.д. Предоставьте необходимую информацию.

Примечание: Важно, чтобы вы предоставили корректное Общее имя. Гарантируйте, что имя хоста, которое используется для создания сертификата (Общее имя), совпадает с записью имени хоста Системы доменных имен (DNS) для IP-адреса виртуального интерфейса на WLC и что название существует в DNS также. Кроме того, после внесения изменения в Виртуальное IP (VIP) интерфейс необходимо перезагрузить систему для этого изменения для вступления в силу.
Например:

```
OpenSSL>req -new -newkey rsa:1024 -nodes -keyout mykey.pem -out myreq.pem -config openssl-san.cnf
Loading 'screen' into random state - done
Generating a 1024 bit RSA private key
.....................................................................++++++
.....................................................++++++
writing new private key to 'mykey.pem'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:CA
Locality Name (eg, city) []:San Jose
Organization Name (eg, company) [Internet Widgits Pty Ltd]:ABC
Organizational Unit Name (eg, section) []:CDE
Common Name (eg, YOUR name) []:XYZ.ABC
Email Address []:Test@abc.com

Please enter the following 'extra' attributes
to be sent with your certificate request
```

```
A challenge password []:Test123
An optional company name []:OpenSSL>
```

6. Можно проверить CSR (специально для SAN присутствия атрибутов) с **openssl req - текстом-noout - в csrfilename**
7. После обеспечения всей требуемой подробной информации два файла генерируются:

   новый секретный ключ, который включает название **mykey.pem**CSR, который включает название **myreq.pem**

Вариант B. CSR, генерируемый WLC

Если ваш WLC работает под управлением ПО версии 8.3.102 или позже, более безопасная опция (и самый легкий также) должна использовать WLC для генерации CSR. Преимущество состоит в том, что ключ генерируется на WLC и никогда не оставляет WLC; таким образом никогда не представляется во внешнем мире.

На данный момент этот метод не позволяет настраивать SAN в CSR, который мог бы привести к проблемам с определенными браузерами, который требует присутствия SAN атрибута. Немного CA позволяют вставлять поля SAN при подписании времени, таким образом, это - хорошая идея свериться с вашим CA.

> **Примечание:** Если вы выполните csr команду генерации и еще не установите получающийся сертификат, то ваш WLC будет абсолютно недостижим на HTTPS в следующей перезагрузке, поскольку WLC будет использовать недавно генерируемый ключ CSR после перезагрузки, но не имеет сертификата, который идет с ним.

Для генерации CSR для web-аутентификации введите эту команду:

(WLC)**> config certificate генерирует csr-webauth BR BE Брюссельский Центр технической поддержки Cisco mywebauthportal.wireless.com tac@cisco.com**

```
-----НАЧНИТЕ ЗАПРОС СЕРТИФИКАТА-----
MIICqjCCAZICAQAwZTELMAkGA1UECAwCQllxETAPBgNVBAcMCEJydXNzZWxzMQ4w
DAYDVQQKDAVDaXNjbzEMMAoGA1UECwwDVEFDMSUwIwYDVQQDDBxteXdlYmF1dGhw
b3J0YWwud2lyZWxlc3MuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKC
AQEAnssc0BxlJ2ULa3xgJH5lAUtbd9CuQVqqf2nflh+V1tu82rzTvz38bjF3g+MX
JiaBbKMA27VJH1J2K2ycDMlhjyYpH9N59T4fXvZr3JNGVfmHIRuYDnCSdil0ookK
FU4sDwXyOxR6gfB6m+Uv5SCOuzfBsTz5bfQ1NlZqg1hNemnhqVgbXEd90sgJmaF2
0tsL0jUhbLosdwMLUbZ5LUa34mvufoI3VAKA0cmWZh2WzMJiaI2JpbO0afRO3kSg
x3XDkZiR7Z9a8rK6Xd8rwDlx0TcMFWdWVcKMDgh7Tw+Ba1cUjjIMzKT6OOjFGOGu
yNkgYefrrBN+WkDdc6c55bxErwIDAQABoAAwDQYJKoZIhvcNAQELBQADggEBAB0K
ZvEpAafoovphlcXIElL2DSwVzjlbd9u7T5JRGgqri1l9/0wzxFjTymQofga427mj
5dNqlCWxRFmKhAmO0fGQkUoP1YhJRxidu+0T8O46s/stbhj9nuInmoTgPaA0s3YH
tDdWgjmV2ASnroUV9oBNu3wR6RQtKDX/CnTSRG5YufTWOVf9IRnL9LkU6pzA69Xd
YHPLnD2ygR1Q+3Is4+5Jw6ZQAaqlPWyVQccvGyFacscA7L+nZK3SSITzGt9B2HAa
PQ8DQOaCwnqt2efYmaezGiHOR8XHOaWcNoJQCFOnb4KK6/1aF/7eOS4LMA+jSzt4
Wkc/wH4DyYdH7x5jzHc =
-----КОНЕЧНЫЙ ЗАПРОС СЕРТИФИКАТА-----
```

Для генерации CSR для webadmin команда только изменяется:

(WLC)> **config certificate генерирует csr-webadmin BR BE Брюссельский Центр технической поддержки Cisco mywebauthportal.wireless.com tac@cisco.com**

> **Примечание:** CSR распечатан на терминале после ввода команды. Нет никаких других способов получить его; не возможно загрузить его от WLC, и при этом не возможно сохранить его. Вы должны скопировать/вставить он к файлу на вашем компьютере после ввода команды. Генерируемый ключ остается на WLC, пока следующий CSR не генерируется (ключ таким образом перезаписан). Если когда-нибудь необходимо изменять аппаратные средства WLC позже (RMA), вы не будете в состоянии повторно установить тот же сертификат как новый ключ, и CSR должен будет генерироваться на новом WLC.

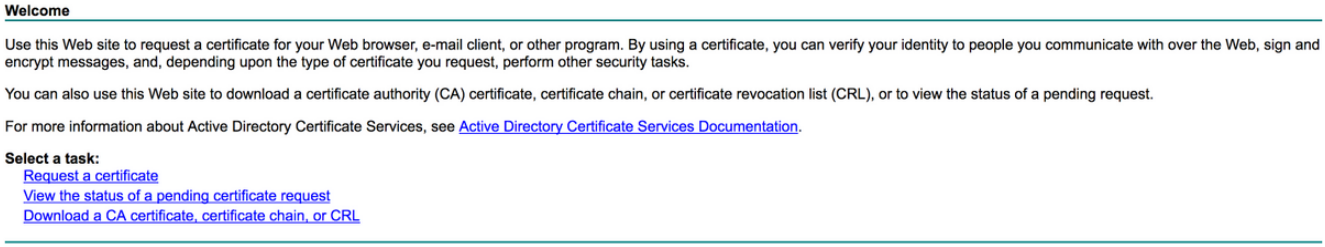
Тогда необходимо передать этот CSR сторонним полномочиям подписания или инфраструктуре открытых ключей (PKI) предприятия.

Шаг 2. Подпишите сертификат

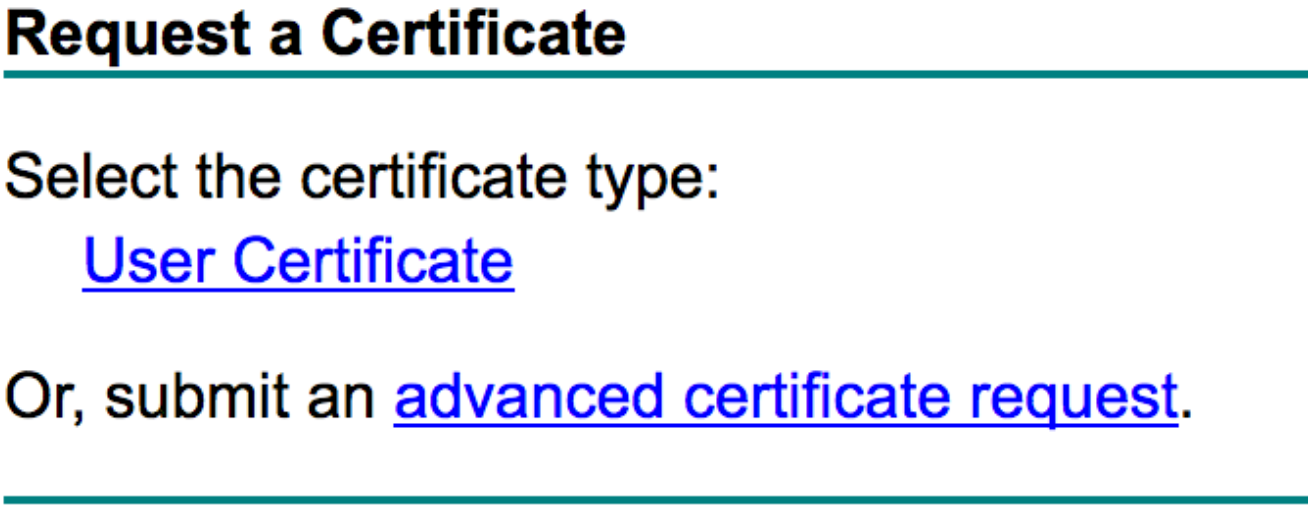
Вариант A: Получите Файл Final.pem из своего Предприятия CA

Данный пример только демонстрирует существующее предприятие CA (Windows Server 2012 в данном примере) и не покрывает шаги для устанавливания Windows Server CA с нуля.

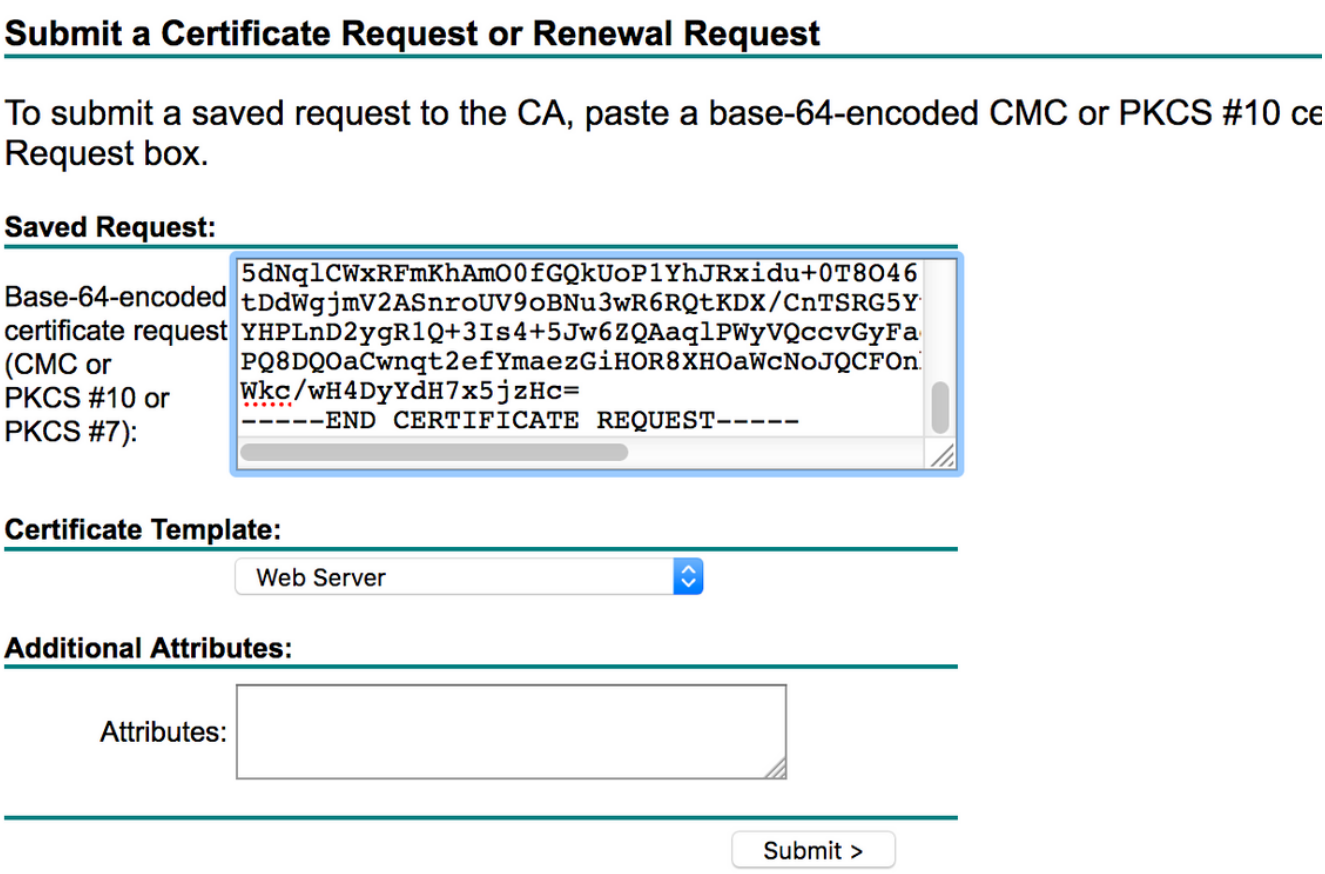
1. Перейдите к своему предприятию страница CA в браузере (обычно https://<ip CA>/certsrv) и нажмите **Request сертификат**.



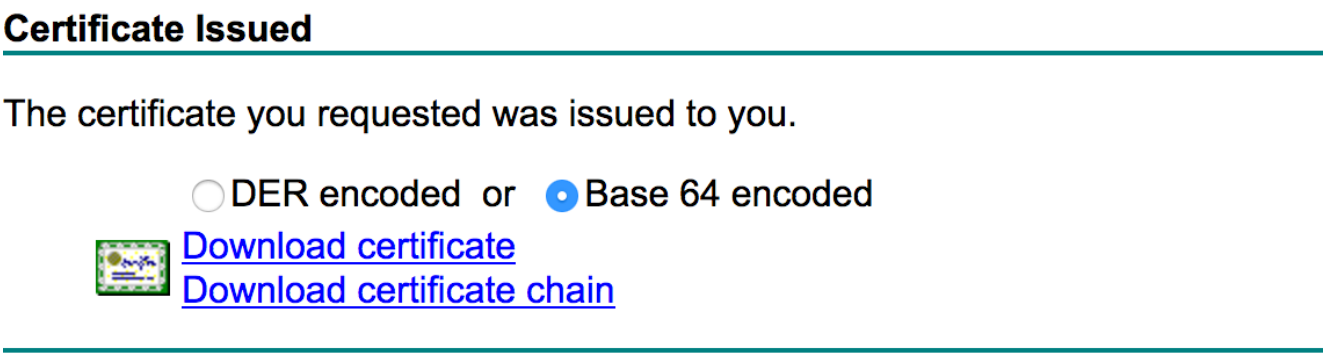
2. Нажмите **усовершенствованный запрос сертификата**.



3. Введите CSR, который вы получили из WLC или OpenSSL. В выпадающем списке Шаблона сертификата выберите **Web Server**.



4. Нажмите **Ядро 64 закодированных** кнопки с зависимой фиксацией.



5. Если загруженный сертификат имеет тип PKCS7 .p(7b), то необходимо преобразовать его в PEM (в ниже примера, мы загрузили цепочку сертификатов как "все-certs.p7b" имя файла):

openssl pkcs7-print_certs - во все-certs.p7b - все-certs.pem

6. Объедините цепочку сертификатов (в данном примере, это называют "все-certs.pem"), сертификаты с секретным ключом, который вы генерировали наряду с CSR (секретный ключ сертификата устройства, который является mykey.pem в данном примере), если вы пошли с опцией A (т.е. вы использовали OpenSSL для генерации CSR), и сохраните файл как **final.pem**. При генерации CSR непосредственно от WLC (опция B), можно пропустить этот шаг.

Выполните эти команды в приложении OpenSSL для создания все-certs.pem и final.pem

файлов:

```
openssl>pkcs12 -export -in All-certs.pem -inkey mykey.pem
-out All-certs.p12 -clcerts -passin pass:check123
-passout pass:check123

openssl>pkcs12 -in All-certs.p12 -out final.pem
-passin pass:check123 -passout pass:check123
```

> **Примечание:** В этой команде необходимо ввести пароль для параметров **-passin** и **-passout**. Пароль, который настроен для **-passout** параметра, должен совпасть с **certpassword** параметром, который настроен на WLC. В данном примере пароль, который настроен и для **-passin** и для **-passout** параметров, является **check123**.

Final.pem является файлом, который необходимо загрузить к WLC, если бы вы придерживались “Опции A. CSR с OpenSSL”. Если вы придерживались “Опции B. CSR, генерируемый самим WLC”, тогда все-certs.pem файл, который необходимо загрузить к WLC. Следующий шаг должен загрузить этот файл к WLC.

> **Примечание:** Если загрузка сертификата к сбоям WLC, может случиться так, что у вас нет целой цепочки в pem файле. См. шаг 2 опции B (получают final.pem из третьей стороны CA), ниже, чтобы видеть, как это должно быть похожим. Если вы только видите один сертификат в файле, то необходимо вручную загрузить все промежуточное звено и файлы корневого сертификата CA и добавить их (вставкой простой копии) к файлу для создания цепочки.

Вариант B: Получите файл Final.pem из независимого поставщика CA

1. Скопируйте и вставьте информацию о CSR в любое программное средство регистрации CA.

   После отправки CSR независимому поставщику CA независимый поставщик CA снабжает цифровой подписью сертификат и передает цепочку подписанного сертификата обратно через электронную почту. В случае цепочечных сертификатов вы получаете всю цепочку сертификатов от CA., Если у вас только есть один промежуточный сертификат как в данном примере, вы получаете эти три сертификата от CA:

   Root certificate.pemПромежуточное звено certificate.pemУстройство certificate.pem**Примечание:** Удостоверьтесь, что сертификат совместим с Apache с шифрованием Защищенного алгоритма хэширования 1 (SHA1).
2. Как только вы имеете все три сертификата, копируете и вставляете содержание каждого файла .pem в другой файл в этом заказе:

   ```
   openssl>pkcs12 -export -in All-certs.pem -inkey mykey.pem
   -out All-certs.p12 -clcerts -passin pass:check123
   ```

```
-passout pass:check123

openssl>pkcs12 -in All-certs.p12 -out final.pem
-passin pass:check123 -passout pass:check123
```

3. Сохраните файл как **все-certs.pem**.

4. Объедините все-certs.pem сертификат с секретным ключом, который вы генерировали наряду с CSR (секретный ключ сертификата устройства, который является mykey.pem в данном примере), если вы пошли с опцией A (т.е. вы использовали OpenSSL для генерации CSR), и сохраните файл как **final.pem**. При генерации CSR непосредственно от WLC (опция B), можно пропустить этот шаг.

   Выполните эти команды в приложении OpenSSL для создания все-certs.pem и final.pem файлов:

```
openssl>pkcs12 -export -in All-certs.pem -inkey mykey.pem
-out All-certs.p12 -clcerts -passin pass:check123
-passout pass:check123

openssl>pkcs12 -in All-certs.p12 -out final.pem
-passin pass:check123 -passout pass:check123
```

   Примечание: В этой команде необходимо ввести пароль для параметров**-passin** и**-passout**. Пароль, который настроен для**-passout** параметра, должен совпасть **с certpassword** параметром, который настроен на WLC. В данном примере пароль, который настроен и для**-passin** и для**-passout** параметров, является **check123**.Final.pem является файлом, который необходимо загрузить к WLC, если бы вы придерживались “Опции A. CSR с OpenSSL”. Если вы придерживались “Опции B. CSR, генерируемый самим WLC”, тогда все-certs.pem файл, который необходимо загрузить к WLC. Следующий шаг должен загрузить этот файл к WLC.

   Примечание: SHA2 также поддерживается. Идентификатор ошибки Cisco CSCuf20725 является запросом о поддержке SHA512.

CLI шага 3. Загрузите сторонний сертификат к WLC с CLI

Выполните эти шаги для загрузки цепочечного сертификата к WLC с CLI:

1. Переместите **final.pem** файл в каталог по умолчанию на вашем сервере TFTP.

2. В CLI выполните эти команды для изменения настроек загрузки:

```
    >transfer download mode tftp
>transfer download datatype webauthcert
>transfer download serverip <TFTP server IP address>
>transfer download path <absolute TFTP server path to the update file>
>transfer download filename final.pem
```

3. Введите пароль для файла .pem так, чтобы операционная система могла дешифровать ключ SSL и сертификат.

```
>transfer download certpassword password
```

Примечание: Убедитесь, что значение для **certpassword** совпадает с**-passout** паролем параметра, который был установлен в Шаге 4 (или 5) Генерирования раздела CSR. В данном примере **certpassword** должен быть **check123**. При выборе опции B (т.е. используйте сам WLC для генерации CSR), можно оставить certpassword незаполненное поле.

4. Выполните **команду transfer download start** для просмотра обновленных настроек. Затем введите **y** в приглашение, чтобы подтвердить текущие параметры настройки загрузки и запустить сертификат и ключевую загрузку. Например:

```
(Cisco Controller) >transfer download start

Mode..................................... TFTP
Data Type................................ Site Cert
TFTP Server IP........................... 10.77.244.196
TFTP Packet Timeout...................... 6
TFTP Max Retries......................... 10
TFTP Path......................................./
TFTP Filename............................ final.pem

This might take some time.
Are you sure you want to start? (y/N) y

TFTP EAP Dev cert transfer starting.

Certificate installed.
Reboot the switch to use new certificate.
```

5. Перезагрузите WLC для изменений для вступления в силу.

GUI шага 3. Загрузите сторонний сертификат к WLC с GUI

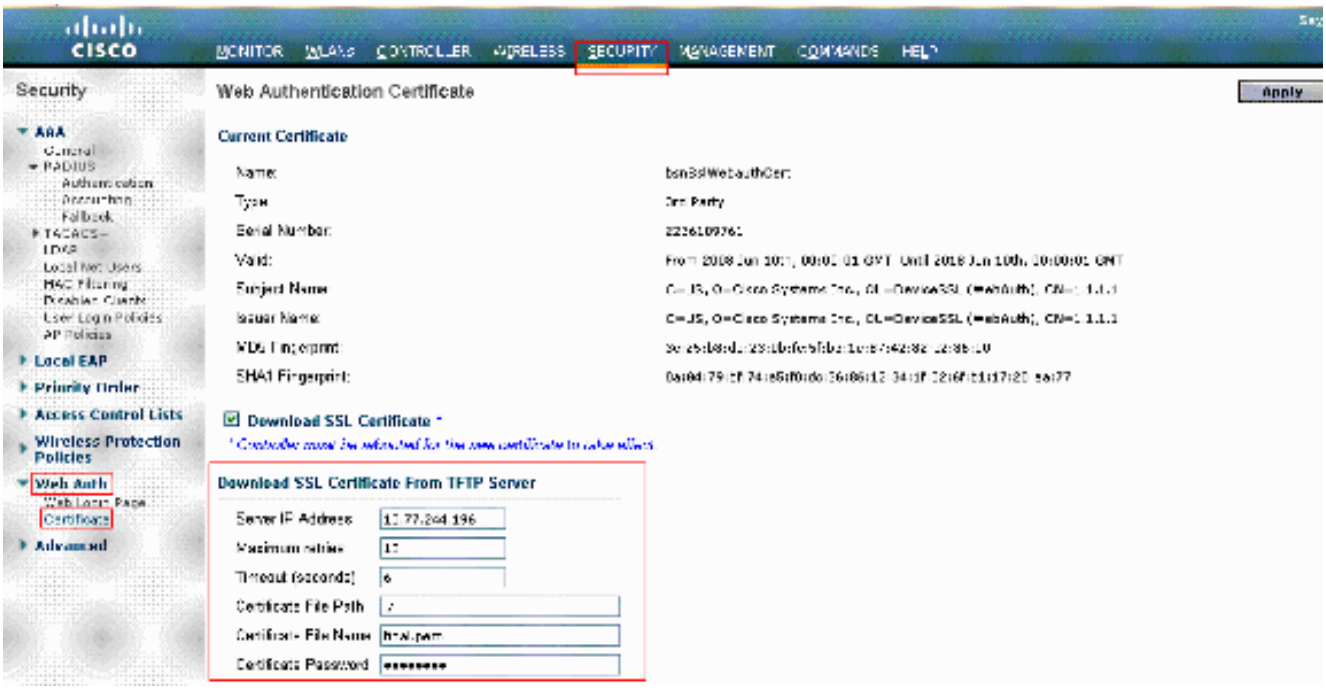
Выполните эти шаги для загрузки цепочечного сертификата к WLC с GUI:

1. Скопируйте сертификат устройства final.pem к каталогу по умолчанию на вашем сервере TFTP.

2. Выберите **Security> Web Auth> Cert** для открытия страницы Web Authentication Certificate.

3. Проверьте флажок **Download SSL Certificate** для просмотра сертификата SSL Загрузки От параметров Сервера TFTP.

4. В поле IP Address введите IP-адрес сервера TFTP.



5. В поле File Path введите путь к каталогу сертификата.

6. В поле File Name введите имя сертификата.

7. В поле Certificate Password введите пароль, который использовался для защиты сертификата.

8. **Щелкните "Применить".**

9. После того, как загрузка завершена, выберите **Commands> Reboot> Reboot**.

10. Если предложено сохранить ваши изменения, нажмите **Save и Reboot**.

11. Нажмите **OK** для подтверждения решения перезагрузить контроллер.

Устранение неполадок

Что будет, скорее всего, позировать, проблемой является установка сертификата на WLC. Для устранения проблем откройте командную строку на WLC и введите **debug transfer, которого все включают** и затем завершают процедуру сертификата загрузки.

```
(Cisco Controller) >transfer download start

Mode..................................... TFTP
Data Type................................ Site Cert
TFTP Server IP........................... 10.77.244.196
TFTP Packet Timeout...................... 6
TFTP Max Retries......................... 10
TFTP Path......................................./
TFTP Filename............................ final.pem

This might take some time.
```

```
Are you sure you want to start? (y/N) y

TFTP EAP Dev cert transfer starting.

Certificate installed.
Reboot the switch to use new certificate.
```

Необходимо проверить формат сертификата и объединяющий в цепочку тогда. Помните, что WLC позже, чем версия 7.6 требуют, чтобы целая цепочка присутствовала, таким образом, можно не только загрузить один только сертификат WLC. Цепочка до узла CA должна присутствовать в файле.

Дополнительные сведения

- Генерируйте CSR для сторонних сертификатов и загрузите освобожденные сертификаты к WLC
- Создание запроса подписи сертификата (CSR) для сертификата от третьей стороны на беспроводной системе управления (WCS)
- Пример конфигурации запроса регистрации сертификата (CSR) системы Wireless Control System (WCS), установленной на сервере Linux
- Cisco Systems – техническая поддержка и документация