Генерирование CSR для сторонних сертификатов и загрузка связанных сертификатов в WLC

Содержание

Введение

В этом документе описана процедура формирования запроса на подписание сертификата (CSR) для получения стороннего сертификата, а также загрузки цепочечного сертификата на контроллер беспроводной локальной сети (WLAN) (WLC).

Предварительные условия

Требования

Для выполнения этой настройки требуются знания следующих предметов:

- Как настроить WLC, легкую точку доступа (LAP) и плату беспроводной связи клиента для обеспечения базовой работы
- Как использовать приложение OpenSSL
- Инфраструктура открытых ключей и цифровые сертификаты

Используемые компоненты

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

- Контроллер беспроводной локальной сети Cisco 5508 со встроенным ПО версии 8.3.102
- Приложение OpenSSL для Microsoft Windows
- Программное средство регистрации, предназначенное 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.

Связанные сертификаты

Цепочка сертификатов — это последовательность сертификатов, в которой каждый сертификат подписывается последующим сертификатом. Цель цепочки сертификатов состоит в том, чтобы установить цепочку доверия от сертификата узла до сертификата доверенного CA. Подписывая сертификат, CA ручается за подлинность приведенных в нем данных. Если CA является доверенным, на что указывает наличие копии сертификата CA в каталоге корневых сертификатов, подразумевается, что также можно доверять и подписанному сертификату узла.

Часто клиенты не принимают сертификаты, потому что они не были созданы известным CA. Клиент, как правило, сообщает, что проверить действительность сертификата невозможно. Так обстоит дело, когда сертификат подписан промежуточным CA, который неизвестен браузеру клиента. В таких случаях необходимо использовать связанный сертификат SSL или группу сертификатов.

Поддержка связанного сертификата

Контроллер позволяет загрузить сертификат устройства в качестве связанного сертификата и использовать его для веб-аутентификации.

Уровни сертификатов

- Уровень 0 — использование только серверного сертификата на WLC
- Уровень 1 — использование серверного сертификата на WLC и корневого сертификата CA
- Уровень 2 — использование серверного сертификата на WLC, одного сертификата промежуточного CA и корневого сертификата CA
- Уровень 3 — использование серверного сертификата на WLC, двух сертификатов промежуточных CA и корневого сертификата CA

WLC не поддерживает связанные сертификаты размером больше 10 КБ на WLC. Однако это ограничение было убрано в WLC, начиная с версии 7.0.230.0.

Примечание: Цепочечные сертификаты поддерживаются и на самом деле требуемый

для web-аутентификации и веба - администратора

Примечание. Подстановочные сертификаты полностью поддерживаются для локального EAP, управления или веб-аутентификации

В качестве сертификатов для веб-аутентификации можно использовать любые из следующих сертификатов:

- Связанный
- Несвязанный
- Формируемые автоматически

Примечание: В Версии 7.6 WLC и позже, только цепочечные сертификаты поддерживаются (и поэтому требуемый)

Если вам необходимо сформировать несвязанный сертификат для управления, можно следовать приведенным в этом документе инструкциям, пропуская те его части, в которых сертификат объединяется с сертификатом CA.

В этом документе рассказывается о том, как правильно установить связанный сертификат SSL на WLC.

Шаг 1. Формирование CSR

Существует два способа сформировать CSR. Либо вручную с помощью OpenSSL (это единственно возможный способ при использовании программного обеспечения WLC версии до 8.3), либо с помощью самого WLC (этот способ доступен, начиная с версии 8.3.102).

Вариант A. CSR с помощью OpenSSL»

Примечание. Браузер Chrome, начиная с версии 58, не доверяет одному общему имени сертификата и требует наличия еще и альтернативного имени субъекта. В следующем разделе рассказывается, как добавить поля SAN в CSR, формируемый с помощью OpenSSL, что является новым требованием для этого браузера.

Для того чтобы сформировать CSR с помощью OpenSSL, выполните следующие действия:

1. Установите и откройте OpenSSL.

В Microsoft Windows файл openssl.exe по умолчанию расположен в каталоге C:\> openssl> bin.

Примечание. Для старых выпусков WLC рекомендуется использовать OpenSSL версии 0.9.8; начиная с версии 7.5, также появилась поддержка OpenSSL версии 1.0 (см. описание ошибки Cisco с идентификатором CSCti65315 — нужна поддержка для сертификатов, сформированных с помощью OpenSSL 1.0), которую и рекомендуется использовать. Работа OpenSSL 1.1 также была протестирована и подтверждена в

выпусках WLC, начиная с 8.x.

2. Найдите файл конфигурации OpenSSL и сделайте его копию, а затем отредактируйте этот файл для данного CSR. Отредактируйте копию и добавьте в нее следующие разделы:
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
```

Строки, начинающиеся с DNS.1 и DNS.2 и так далее, должны содержать все альтернативные имена, которые будут иметь сертификаты. Затем можно будет ввести любой возможный URL-адрес, который будет использоваться для WLC. Строки, выделенные выше полужирным шрифтом, отсутствовали или были закомментированы в версии openSSL, которая использовалась в нашей лабораторной работе. Они могут сильно отличаться в зависимости от операционной системы и версии openssl. **В данном примере эта измененная версия файла конфигурации имеет имя openssl-san.cnf.**

4. Для того чтобы сформировать новый CSR, выполните следующую команду:

```
OpenSSL>req -new -newkey rsa:3072 -nodes -keyout mykey.pem -out myreq.pem -config openssl-san.cnf
```

Примечание. Начиная с версии программного обеспечения 8.5, контроллеры WLC поддерживают ключи размером не более 4096 бит

5. После ввода этой команды выдается запрос определенной информации: название страны, регион, город и т. д. Предоставьте необходимую информацию.

Примечание. Важно указать правильное общее имя. Убедитесь, что имя узла, которое используется для создания сертификата (общее имя), совпадает с записью имени узла в системе доменных имен (DNS) для IP-адреса виртуального интерфейса на WLC, а также в том, что это имя также существует и в DNS. Кроме того, после изменения виртуального интерфейса IP (VIP) необходимо перезагрузить систему, чтобы это изменение вступило в силу.
Например:

```
OpenSSL>req -new -newkey rsa:3072 -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. **CSR можно проверить (особенно на наличие атрибутов SAN) с помощью команды openssl req -text -noout -in csrfilename**
7. После того как будут предоставлены все необходимые сведения, формируется два файла:

   новый закрытый ключ с именем mykey.pemcSR с именем myreq.pem

Вариант B. CSR, формируемый WLC

Если в вашем контроллере WLC используется программное обеспечение версии 8.3.102 или выше, более безопасным (и самым простым) вариантом является формирование CSR с помощью WLC. Преимущество состоит в том, что ключ формируется на WLC и никогда не покидает контроллер беспроводной локальной сети Cisco; таким образом, он никогда не вступает в контакт с внешним миром.

На данный момент этот метод не позволяет настраивать SAN в CSR, что может стать причиной проблем в некоторых браузерах, которые требуют наличия атрибута SAN. Некоторые CA позволяют вставлять поля SAN во время подписания, поэтому рекомендуется узнать о такой возможности в вашем CA..

При формировании CSR с помощью WLC используется ключ размером 2048 бит, а размер ключа ecdsa составит 256 бит.

> **Примечание. Если подать команду формирования csr и не установить итоговый сертификат, к контроллеру WLC будет абсолютно невозможно подключиться по HTTPS после следующей перезагрузки, поскольку после перезагрузки WLC будет использовать только что сформированный ключ CSR, а сертификат для него будет отсутствовать.**

Для того чтобы сформировать CSR для веб-аутентификации, введите следующую команду:

(WLC) >config certificate generate csr-webauth BE BR Brussels Cisco TAC mywebauthportal.wireless.com tac@cisco.com

-----BEGIN CERTIFICATE REQUEST-----
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 =
-----END CERTIFICATE REQUEST-----

Для того чтобы сформировать CSR для webadmin, команду необходимо немного изменить:

(WLC) >config certificate generate csr-webadmin BE BR Brussels Cisco TAC mywebauthportal.wireless.com tac@cisco.com

> **Примечание. После ввода этой команды CSR выводится на терминал.** Никаких других способов получить его нет; выгрузить его с WLC или сохранить невозможно. После ввода команды сертификат необходимо скопировать и вставить в файл на компьютере. Сформированный ключ остается на контроллере беспроводной локальной сети Cisco, пока не будет сформирован следующий CSR (ключ при этом перезаписывается). Если когда-либо в будущем вам придется заменить оборудование WLC (RMA), повторно установить тот же сертификат как новый ключ не получится. CSR необходимо будет сформировать заново на новом WLC.

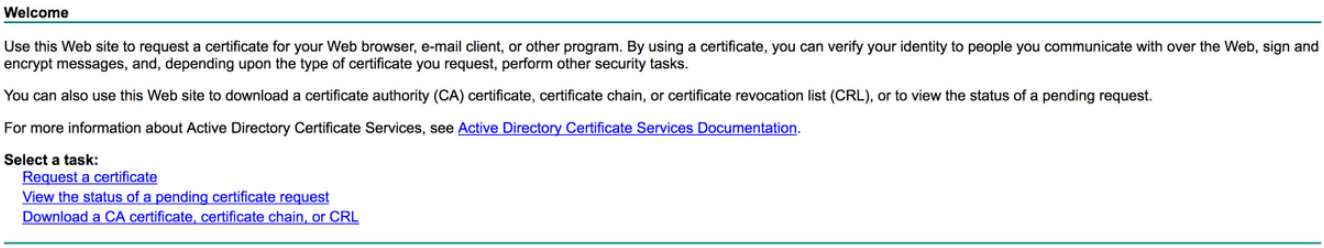
Затем этот CSR необходимо будет передать стороннему органу, выполняющему подписание, или в инфраструктуру открытых ключей (PKI) предприятия.

Шаг 2. Подписание сертификата

Вариант A: Получение файла Final.pem от корпоративного CA

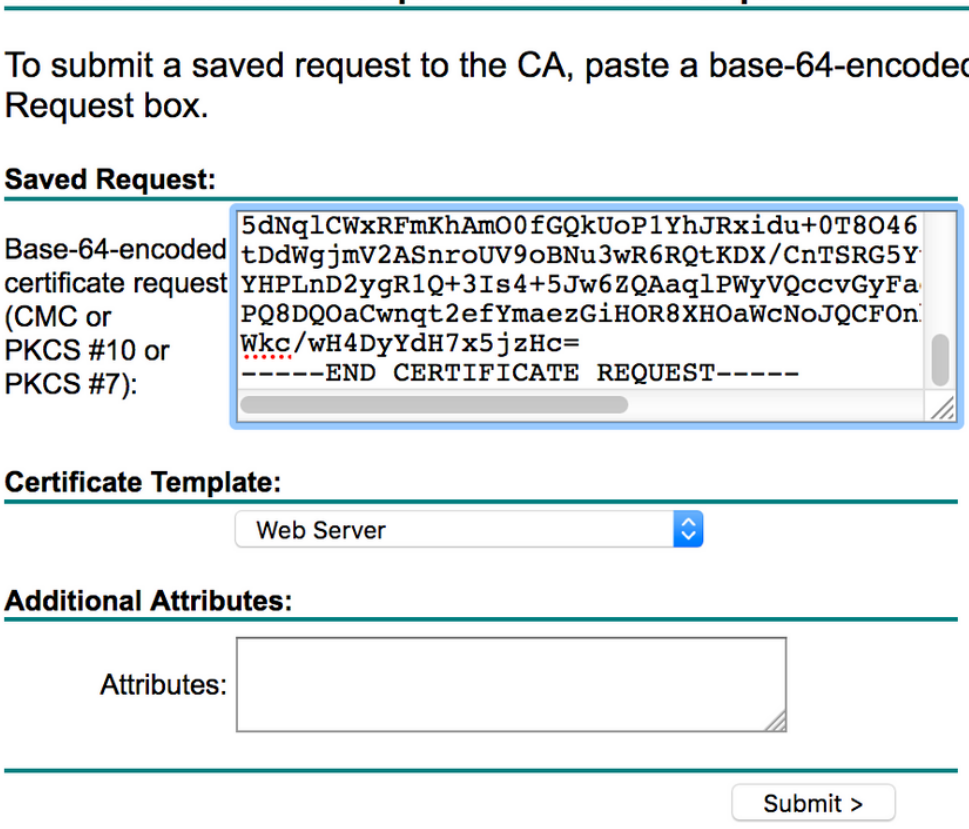
В данном примере рассматривается ситуация, когда CA предприятия уже существует (здесь это Windows Server 2012). В нем не приводятся действия по настройке Windows Server CA с нуля.

1. **Перейдите на страницу CA предприятия в браузере (обычно это https://<CA-ip>/certsrv) и нажмите Request a certificate (Запросить сертификат).**

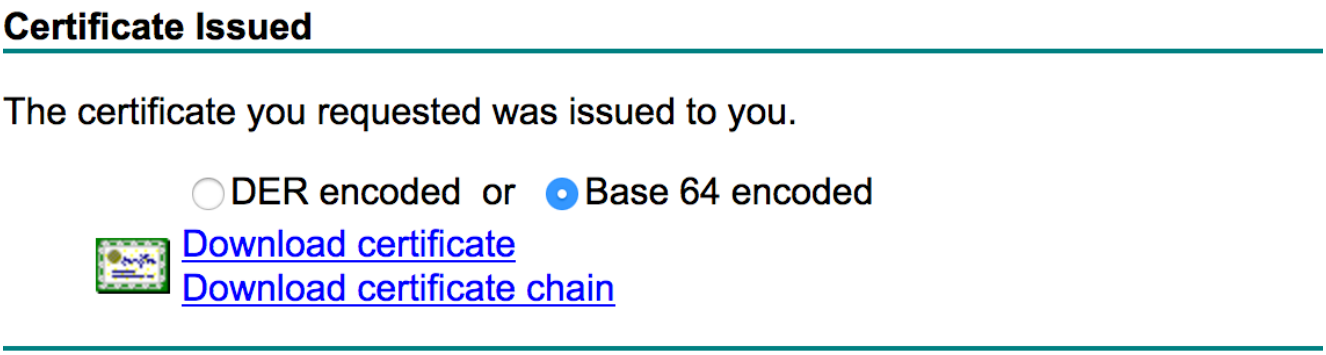


2. Нажмите advanced certificate request (расширенный запрос сертификата).

3. Введите запрос CSR, полученный с помощью WLC или OpenSSL. В раскрывающемся списке Certificate Template (Шаблон сертификата) выберите Web Server (Веб-сервер).



4. Установите переключатель в положение Base 64 encoded (С кодировкой Base64).



5. Если загруженный сертификат имеет тип PKCS7 (.p7b), то его необходимо преобразовать в PEM (в приведенном далее примере мы загрузили цепочку сертификатов в виде файла с именем All-certs.p7b):

openssl pkcs7 -print_certs -in All-certs.p7b -out All-certs.pem

6. Объедините в цепочку сертификатов (в данном примере она называется All-certs.pem) сертификаты с закрытым ключом, который был сформирован вместе с CSR (это закрытый ключ сертификата устройства, которым в данном примере является файл mykey.pem), если вы выбрали вариант A (то есть использовали OpenSSL для формирования CSR), и сохраните файл как final.pem. При генерации CSR непосредственно на WLC (вариант Б) этот шаг можно пропустить.

Выполните следующие команды в приложении OpenSSL, чтобы создать файлы All-certs.pem и final.pem:

```
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, настроенный для параметра -passout, должен совпадать с параметром certpassword, который задан на WLC. В данном примере для параметров -passin и -passout задан пароль check123.

Final.pem является файлом, который необходимо загрузить на WLC, если был выбран «Вариант A. CSR с помощью OpenSSL». Если был выбран «Вариант Б. CSR, формируемый самим WLC», то на WLC необходимо загрузить файл All-certs.pem. Далее необходимо загрузить этот файл на WLC.

Примечание. Если при выгрузке сертификата на WLC произойдет ошибка, это может

быть связано с тем, что в файле pem собрана не вся цепочка. См. шаг 2 варианта Б (получите файл final.pem от стороннего CA), приведенный ниже, в котором видно, как это должно выглядеть. Если в файле есть только один сертификат, то необходимо вручную загрузить все файлы сертификатов промежуточных и корневого CA и добавить их (простым копированием и вставкой) в файл, чтобы создать эту цепочку.

Вариант B: Получение файла Final.pem от стороннего CA

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

   После отправки CSR независимому CA этот CA снабжает сертификат цифровой подписью и возвращает подписанную цепочку сертификатов по электронной почте. В случае цепочечных сертификатов вы получаете от CA всю цепочку сертификатов. Если у вас только есть один промежуточный сертификат, как в данном примере, вы получите от CA следующие три сертификата:

   Файл .pem корневого сертификатаФайл .pem промежуточного сертификатаФайл .pem сертификата устройства**Примечание. Сертификат должен быть совместим с Apache и использовать шифрование SHA1.**
2. Получив все три сертификата, скопируйте и вставьте содержимое каждого файла .pem в другой файл в следующем порядке:

```
------BEGIN CERTIFICATE------
*Device cert*
------END CERTIFICATE------
------BEGIN CERTIFICATE------
*Intermediate CA cert *
------END CERTIFICATE--------
------BEGIN CERTIFICATE------
*Root CA cert *
------END CERTIFICATE------
```

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

4. **Объедините сертификат All-certs.pem с закрытым ключом, который был сформирован вместе с CSR (закрытый ключ сертификата устройства, в данном примере это mykey.pem), если изначально был выбран вариант A (то есть CSR был сформирован с помощью OpenSSL), и сохраните файл как final.pem.** При генерации CSR непосредственно на WLC (вариант Б) этот шаг можно пропустить.

   Выполните следующие команды в приложении OpenSSL, чтобы создать файлы All-certs.pem и final.pem:

```
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, настроенный для параметра -passout, должен совпадать с параметром certpassword, который задан на WLC. В данном примере для параметров -passin и -passout задан пароль check123. Final.pem является файлом, который необходимо загрузить на WLC, если был выбран «Вариант A. CSR с помощью OpenSSL». Если был выбран «Вариант Б. CSR, формируемый самим WLC», то на WLC необходимо загрузить файл All-certs.pem. Далее необходимо загрузить этот файл на WLC.

Примечание. Шифрование SHA2 также поддерживается. Описание ошибки Cisco с идентификатором CSCuf20725 является запросом о поддержке SHA512.

Шаг 3. Интерфейс командной строки. Загрузка стороннего сертификата на WLC с помощью интерфейса командной строки

Выполните следующие действия, чтобы загрузить связанный сертификат на контроллер беспроводной локальной сети Cisco с помощью интерфейса командной строки:

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

2. В интерфейсе командной строки выполните следующие 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, чтобы операционная система могла расшифровать ключ SSL и сертификат.

```
>transfer download certpassword password
```

Примечание. Параметру certpassword должно быть задано такое же значение, как параметру -passout . Это пароль, который был задан на шаге 4 (или 5), приведенном в разделе Формирование CSR. В данном примере параметру certpassword должно быть задано значение check123. Если изначально был выбран вариант Б (то есть формирование CSR с помощью WLC), можно оставить поле certpassword пустым.

4. **Выполните команду transfer download start, чтобы просмотреть обновленные настройки. Затем при появлении приглашения введите y, чтобы подтвердить текущие настройки загрузки и запустить загрузку сертификата и ключа.** 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, чтобы изменения вступили в силу.

Шаг 3. Графический интерфейс пользователя. Загрузка стороннего сертификата на WLC с помощью графического интерфейса пользователя

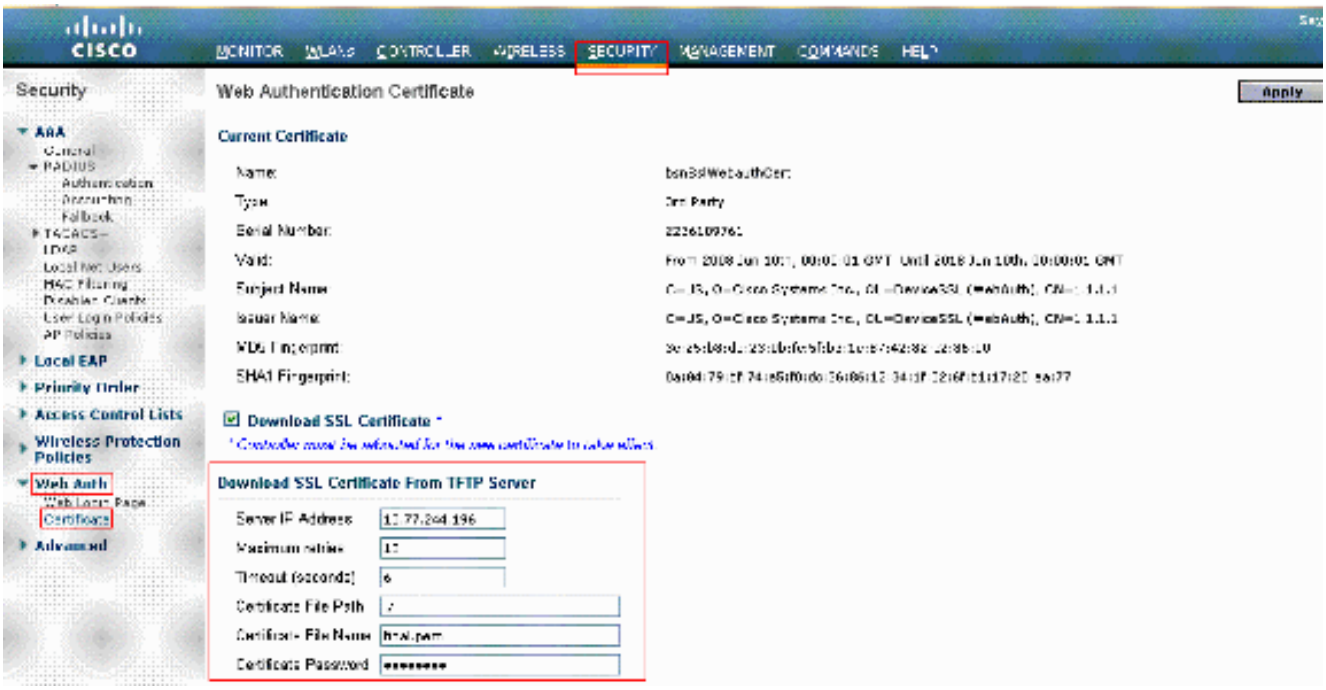
Выполните следующие действия, чтобы загрузить связанный сертификат на контроллер беспроводной локальной сети Cisco с помощью графического интерфейса пользователя:

1. Скопируйте сертификат устройства final.pem в каталог по умолчанию на своем сервере TFTP.

2. **Выберите Security > Web Auth > Cert (Безопасность > Веб-аутентификация > Сертификат), чтобы открыть страницу Web Authentication Certificate (Сертификат для веб-аутентификации).**

3. **Установите флажок Download SSL Certificate (Загрузить сертификат SSL), чтобы открыть параметры Download SSL Certificate From TFTP Server (Загрузка сертификата SSL с сервера TFTP).**

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



5. В поле File Path (Путь к файлу) введите путь к каталогу с сертификатом.

6. В поле File Name (Имя файла) введите имя сертификата.

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

8. **Нажмите Apply.**

9. **После того как загрузка будет завершена, выберите Commands> Reboot> Reboot (Команды > Перезагрузка > Перезагрузить).**

10. **При появлении запроса на сохранение изменений выберите Save and Reboot (Сохранить и перезагрузить).**

11. **Нажмите OK, чтобы подтвердить решение перезагрузить контроллер.**

Устранение неполадок

То То Чаще всего проблемы возникают при установке сертификата на WLC. **Для того чтобы выполнить поиск и устранить неполадку, откройте командную строку на WLC и введите debug transfer all enable и debug pm pki enable, после чего выполните процедуру загрузки сертификата.**

```
In some cases, the logs will only say that the certificate installation failed:
*TransferTask: Sep 09 08:37:17.415: RESULT_STRING: TFTP receive complete... Installing
Certificate.
*TransferTask: Sep 09 08:37:17.415: RESULT_CODE:13

TFTP receive complete... Installing Certificate.
```

```
*TransferTask: Sep 09 08:37:21.418: Adding cert (1935 bytes) with certificate key password.
*TransferTask: Sep 09 08:37:21.421: RESULT_STRING: Error installing certificate.
```

Затем необходимо будет проверить формат сертификата и цепочку. Напомним, что, начиная с версии 7.6, WLC требуют наличия всей цепочки, поэтому нельзя выгрузить только один сертификат WLC. В файле должна присутствовать цепочка вплоть до корневого CA.

Вот пример данных отладки при наличии неправильного промежуточного CA:

```
*TransferTask: Jan 04 19:08:13.338: Add WebAuth Cert: Adding certificate & private key using
password check123
*TransferTask: Jan 04 19:08:13.338: Add ID Cert: Adding certificate & private key using password
check123
*TransferTask: Jan 04 19:08:13.338: Add Cert to ID Table: Adding certificate (name:
bsnSslWebauthCert) to ID table using password check123
*TransferTask: Jan 04 19:08:13.338: Add Cert to ID Table: Decoding PEM-encoded Certificate
(verify: YES)
*TransferTask: Jan 04 19:08:13.338: Decode & Verify PEM Cert: Cert/Key Length was 0, so taking
string length instead
*TransferTask: Jan 04 19:08:13.338: Decode & Verify PEM Cert: Cert/Key Length 7148 & VERIFY
*TransferTask: Jan 04 19:08:13.342: Decode & Verify PEM Cert: X509 Cert Verification return
code: 0
*TransferTask: Jan 04 19:08:13.342: Decode & Verify PEM Cert: X509 Cert Verification result
text: unable to get local issuer certificate
*TransferTask: Jan 04 19:08:13.342: Decode & Verify PEM Cert: Error in X509 Cert Verification at
0 depth: unable to get local issuer certificate
*TransferTask: Jan 04 19:08:13.343: Add Cert to ID Table: Error decoding (verify: YES) PEM
certificate
*TransferTask: Jan 04 19:08:13.343: Add ID Cert: Error decoding / adding cert to ID cert table
(verifyChain: TRUE)
*TransferTask: Jan 04 19:08:13.343: Add WebAuth Cert: Error adding ID cert
```

Высокая доступность (HA SSO) факторы

Как объяснено в WLC HA руководство по развертыванию SSO, сертификаты не реплицированы от основного до вспомогательного контроллера в сценарии SSO HA. Это означает, что у вас есть к import all сертификаты к вторичному устройству прежде, чем сформировать пару HA. Другое предупреждение состоит в том, что это не будет работать, если вы генерировали CSR (и поэтому создал ключ локально) на основном WLC, поскольку не может быть экспортирован тот ключ. Единственный путь состоит в том, чтобы генерировать CSR для основного WLC с OpenSSL (и поэтому подключите ключ к сертификату), и импортируйте тот сертификат/сочетание клавиш на обоих WLC.

Дополнительные сведения

- Формирование CSR для сторонних сертификатов и загрузка сертификатов без цепочки на 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
- WLC HA руководство SSO