Пример конфигурации локальных сертификатов на контроллерах беспроводных LAN

Содержание

Введение

Этот документ объясняет, как настроить Контроллер беспроводной локальной сети (WLC) и Облегченные точки доступа (LAP) для использования Локально Значительной функции Сертификата. Эта функция введена в версии 5.2 контроллера беспроводных локальных сетей. С этой функцией, если вы принимаете решение управлять инфраструктурой открытых ключей (PKI), можно генерировать локально значительные сертификаты (LSC) на точках доступа и контроллерах. Эти сертификаты могут тогда использоваться для взаимной аутентификации WLC и LAP.

Предварительные условия

Требования

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

- Знание того, как настроить WLC, LAP и клиентскую беспроводную карту для главной операции
- Знание того, как настроить и использовать Microsoft Windows 2003 CA сервер
- Знание Инфраструктуры открытых ключей и цифровых сертификатов

Используемые компоненты

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

- Cisco WLC серии 4400, который выполняет микропрограммное обеспечение 5.2
- Облегченная точка доступа (LAP) Cisco Aironet серии 1130 AG
- Microsoft Windows 2003 Server, настроенный как контроллер домена, и как сервер Центра сертификации.
- Клиентский адаптер a/b/g 802.11 Cisco Aironet, который выполняет релиз микропрограммы 4.2
- Утилита Cisco Aironet Desktop Utility (ADU), которая выполняет версию микропрограммы 4.2

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.

Локально значительные сертификаты

Если точки доступа установили производством сертификаты (MIC), в выпусках ПО контроллера ранее, чем 5.2.157.0, контроллер может или использовать подписанные сертификаты (SSCs), чтобы аутентифицировать точки доступа или передать сведения авторизации к серверу RADIUS. В выпуске ПО контроллера 5.2.157.0, можно настроить контроллер для использования локального значительного сертификата (LSC). Можно использовать LSC, если вы хотите, чтобы ваша собственная инфраструктура открытых ключей (PKI) предоставила лучшую безопасность; иметь контроль над вашим центром сертификации (CA) и определить политику, ограничения и использования на генерируемых сертификатах.

Новые сертификаты LSC должны быть настроены на Контроллере сначала и затем LAP от Сервера Центра сертификации (CA).

LAP связывается с Контроллером (WLC) с протоколом CAPWAP. Любые запросы подписать сертификат и выполнить сертификаты CA для LAP и для самого WLC, должен инициироваться от WLC. LAP не связывается непосредственно с Сервером CA. WLC ведет себя как прокси CA к AP LWAPP. Подробные данные Сервера CA должны быть настроены на WLC и это должно быть достижимый.

Контроллер использует Протокол SCEP (SCEP) для передачи certReqs, генерируемого на устройствах к CA, и использует SCEP снова для получения подписанных сертификатов от CA.

SCEP является протоколом управления сертификатами что клиенты Инфраструктуры открытых ключей (PKI) и использование серверов Центра сертификации для поддержки хранилища сертификатов и аннулирования. Это широко используется в Cisco и поддерживается многими Серверами CA. В Протоколе SCEP HTTP используется в качестве транспортного протокола для сообщений PKI. Первичная цель SCEP является безопасным выпуском сертификатов к сетевым устройствам. SCEP способен ко многим операциям, но для этого проекта и выпуска, SCEP используется для этих операций.

- CA и распределение открытого ключа RA
- Хранилище сертификатов

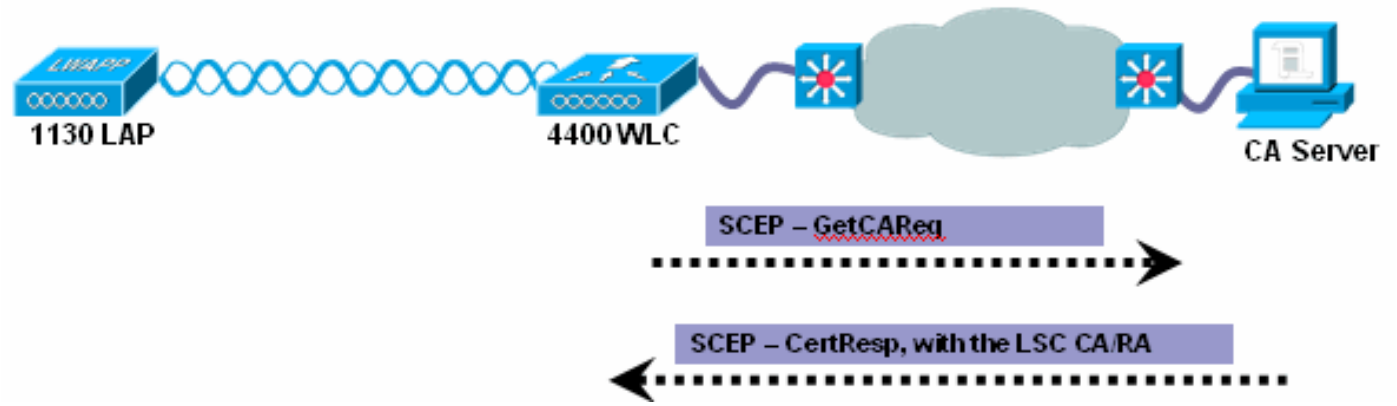
Все транзакции SCEP происходят в автоматическом режиме. Аннулирование сертификата не поддерживается.

Примечание: LSC не поддерживаются на точках доступа, которые настроены для мостового режима.

Инициализация сертификата на контроллерах беспроводной локальной сети (WLC)

Новые сертификаты LSC, и CA и Сертификаты устройства должны быть установлены на Контроллере.

С Протоколом SCEP сертификаты CA получены от Сервера CA. С тех пор на этом этапе, нет никакого подарка сертификатов на контроллере, эта операция является ясным, Получают Операцию. Они установлены на Контроллере. Когда AP настроены с LSC, эти те же сертификаты CA также выдвинуты к AP.



Операция регистрации сертификата устройства

И для LAP и для Контроллера, который запрашивает подписанный сертификат CA, передается certRequest, поскольку PKCS#10 обменивается сообщениями. certRequest содержит Имя субъекта, PublicKey и другие атрибуты, которые будут включены в сертификат X.509 и снабжены цифровой подписью PrivateKey Запрашивающей стороны. Они должны быть переданы CA, который преобразовывает certRequest в сертификат X.509.

CA, который получает PKCS#10 certRequest, запрашивает дополнительную информацию,

чтобы аутентифицировать идентичность запрашивающей стороны и проверить, что запрос неизменен. Много раз PKCS#10 объединялся с другими подходами, такими как PKCS#7, чтобы передать и получить Req/Resp Свидетельства.

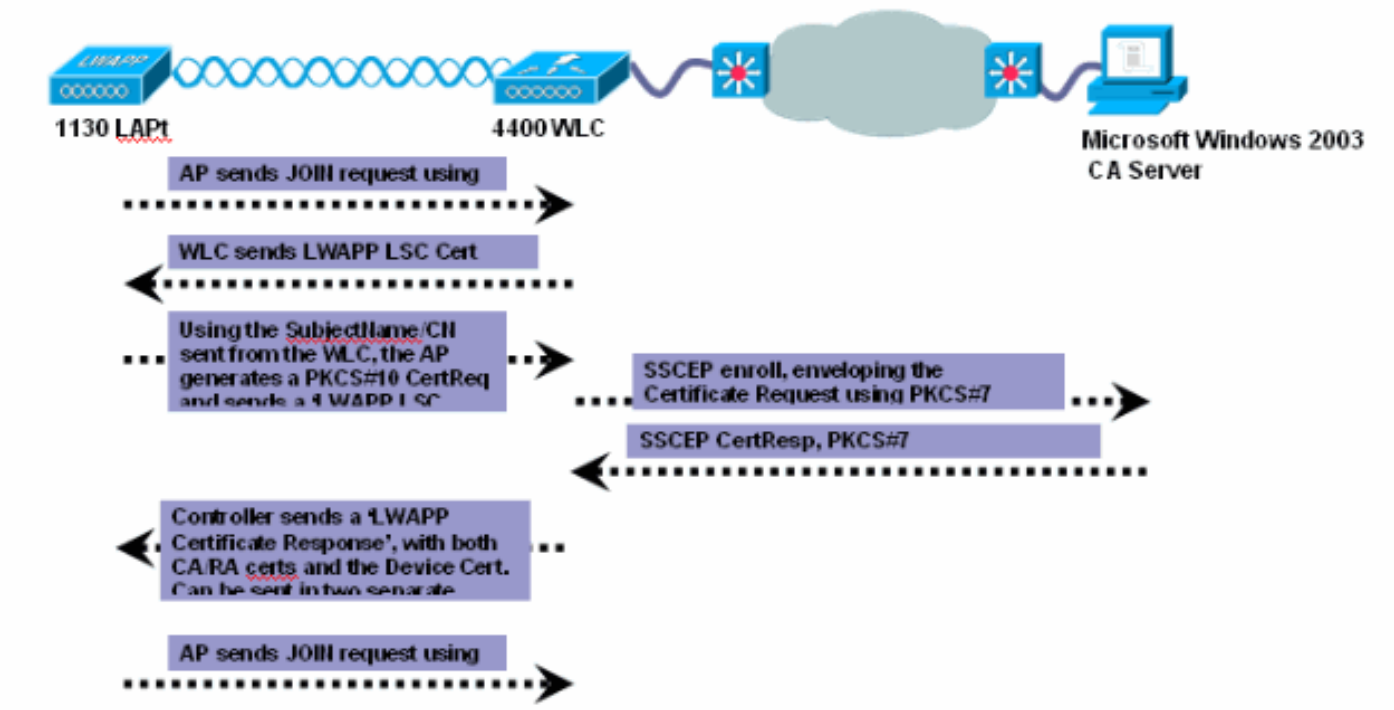
Здесь, PKCS#10 обернут в тип сообщения PKCS#7 SignedData. В то время как сообщение PKCSReq передается Контроллеру, это поддерживается как часть функциональности клиента SCEP.

После успешной операции регистрации и сертификат CA и Сертификат устройства теперь присутствуют на Контроллере.

Инициализация сертификата на AP LWAPP

Для нового Сертификата, который будет настроен на LAP, в то время как в режиме CAPWAP LAP должен быть в состоянии получить новый сертификат X.509 со знаком. Чтобы сделать это, это передает certRequest к Контроллеру, который действует как прокси CA и помогает получать certRequest, подписанный CA для LAP.

certReq и certResponses передаются LAP с информационными наполнениями LWAPP. Эта схема показывает поток для LAP для инициализации LSC.



Вот шаги подробно:

1. Инициализация LAP с более новыми LSC происходит, как только LAP находится в Работоспособном состоянии, после того, как это ПРИСОЕДИНИЛОСЬ к WLC со своим текущим MIC/SSC. В фазе Инициализации LSC, даже при том, что AP находится в Работоспособном состоянии, насильственно закрыты радио.
2. Использование и условие LSC должны быть включены на WLC. Этот процесс включает, чтобы включить LSC, добавить CA Сервер и настроить другие Параметры. Запрос Команды Параметров Сертификата LSC отправлен от Контроллера до LAP, с subject-name, Время Законности и набор Размера ключа в информационном наполнении. Когда certRequest создан, эти поля используются LAP. Информационное

наполнение также указывает, что LAP должен создать certRequest и передать его обратно в Контроллер.
3. LAP генерирует настроенную пару общественности/секретного ключа RSA размера ключа. После генерации пары ключей генерируется certRequest после того, как SubjectName, полученный от Контроллера, настроен. CN автоматически сгенерирован с существующим форматом SSC/MIC, “Cxxxx-EtherMacAddr”. LAP генерирует PKCS#10 CertReq и передает его как информационное наполнение, Запрос сертификата LSC, к Контроллеру.
4. Контроллер тогда создает SSCEP PKCSReq сообщение, форматированное сообщение PKCS#7, и передает его к CA от имени: LAP, для подписывания запроса сертификата настроенным CA. установленный CA/RA certs используется для шифрования certReq.
5. Если CA в состоянии утвердить Запрос сертификата, сообщение CertRep с Status=SUCCESS передают обратно клиенту SSCEP (контроллер) в формате PKCS#7. Ответ Свидетельства записан локально в файл как сертификат формата PEM.
6. Так как этот CertResp для LAP, WLC передает сертификат к LAP с информационным наполнением ‘Ответ Сертификата’. Свидетельство CA передается сначала с тем же информационным наполнением, тогда Сертификат устройства передается в отдельном информационном наполнении.

И LSC CA и Сертификаты устройства LAP установлены в LAP и системные самоперезагрузки. В следующий раз это подходит, так как это настроено для использования LSC, AP передает Сертификат устройства LSC к Контроллеру как часть ПРИСОЕДИНИТЬСЯ Запроса. Как часть ПРИСОЕДИНИТЬСЯ Ответа, контроллер передает свой новый Сертификат устройства и также проверяет входящий сертификат LAP с новым Корневым сертификатом CA.

Примечание: LSC не поддерживаются на точках доступа, которые настроены для мостового режима.

Поддержка LSC на контроллерах беспроводной локальной сети (WLC) и облегченные точки доступа (LAP)

LSC поддерживается на этих Платформах WLC:

- Контроллеры беспроводных LAN серии Cisco 4400
- Cisco 2100 Series Wireless LAN Controllers
- Cisco Catalyst 6500 Series Wireless Services Module (WiSM)
- Cisco Catalyst 3750G интегрированный контроллер беспроводной локальной сети
- Cisco Wireless LAN Controller Module

LSC поддерживается на Cisco Aironet C1130, C1140, C1240, точки доступа C1252 и любые новые точки доступа.

LSC не поддерживается на AP СЕТКИ (1510, 1522), AP Мостового режима.

Этот документ объясняет с примером конфигурации, как включить и аутентифицировать LAP с Локально Значительными Сертификатами.

Настройка

Примечание: Локально Значительная опция Сертификата может быть активирована через GUI или CLI на контроллере.

Примечание: Функция LSC на контроллере не берет запрос на ввод пароля. Поэтому для LSC для работы необходимо отключить запрос на ввод пароля на сервере CA. Кроме того, вы не можете использовать Microsoft Windows server 2008 в качестве сервера CA, потому что не возможно отключить запрос на ввод пароля на нем.

Настройка сети

В данном примере вы настраиваете 4400 Контроллеров беспроводной локальной сети и Облегченную точку доступа серии 1130 для использования локально значительных сертификатов (LSC). Для выполнения этого необходимо настроить Контроллер беспроводной локальной сети и LAP с LSC от сервера Центра сертификации (CA).

Этот документ использует Microsoft Windows 2003 Server в качестве сервера CA.

CA и процесс установки SCEP

Документ предполагает, что существует конфигурация сервера CA на Microsoft Windows 2003 Server. Вот сводка шагов для процесса установки SCEP и CA:

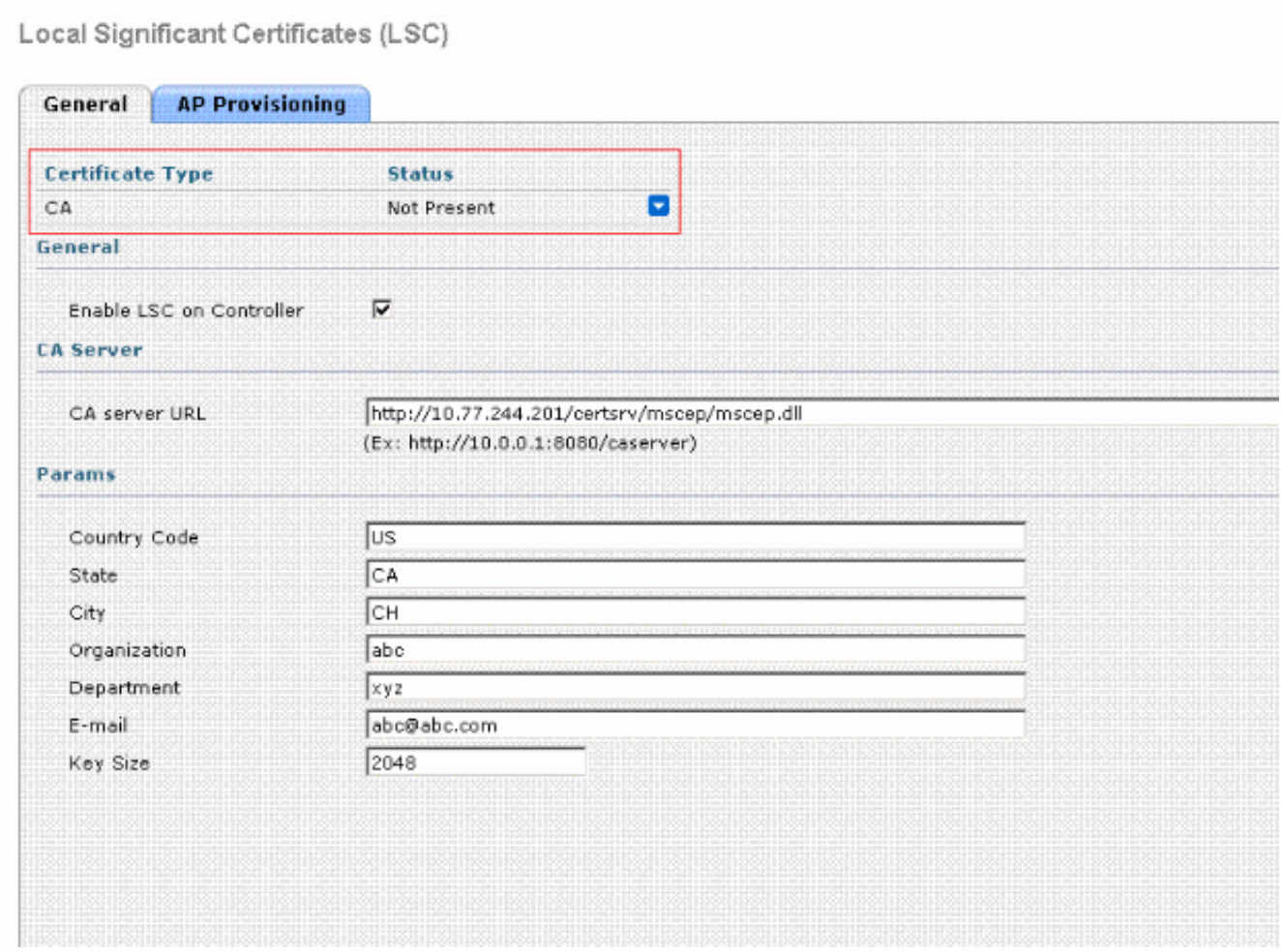
1. Установите Windows 2003 и CA сервер, удостоверьтесь, что работают *http://ca-server/certsrv*
2. Загрузите *cepsetup.exe* от узла Веб-узла Microsoft
3. Установите cepsetup.exe, снимите флажок, "*Требуют Фразы проблемы SCEP*", так как WLC не мог поддержать проблему, регистрируют режим теперь.
4. Предоставьте Название, электронную почту, страну, город и другие подробные данные.
5. Гарантируйте*, что http://ca-server/certsrv/mscep/mscep.dll* работает как ожидалось.

Примечание: Необходимо будет создать учетную запись пользователя, назначить ее Рид и Зарегистрировать разрешения на IPSec (Офлайновый Запрос) шаблон и сделать ее участником IIS_WPG Group. Поскольку завершенные подробные данные обращаются к Веб-узлу Microsoft для SCEP Установки и настройки

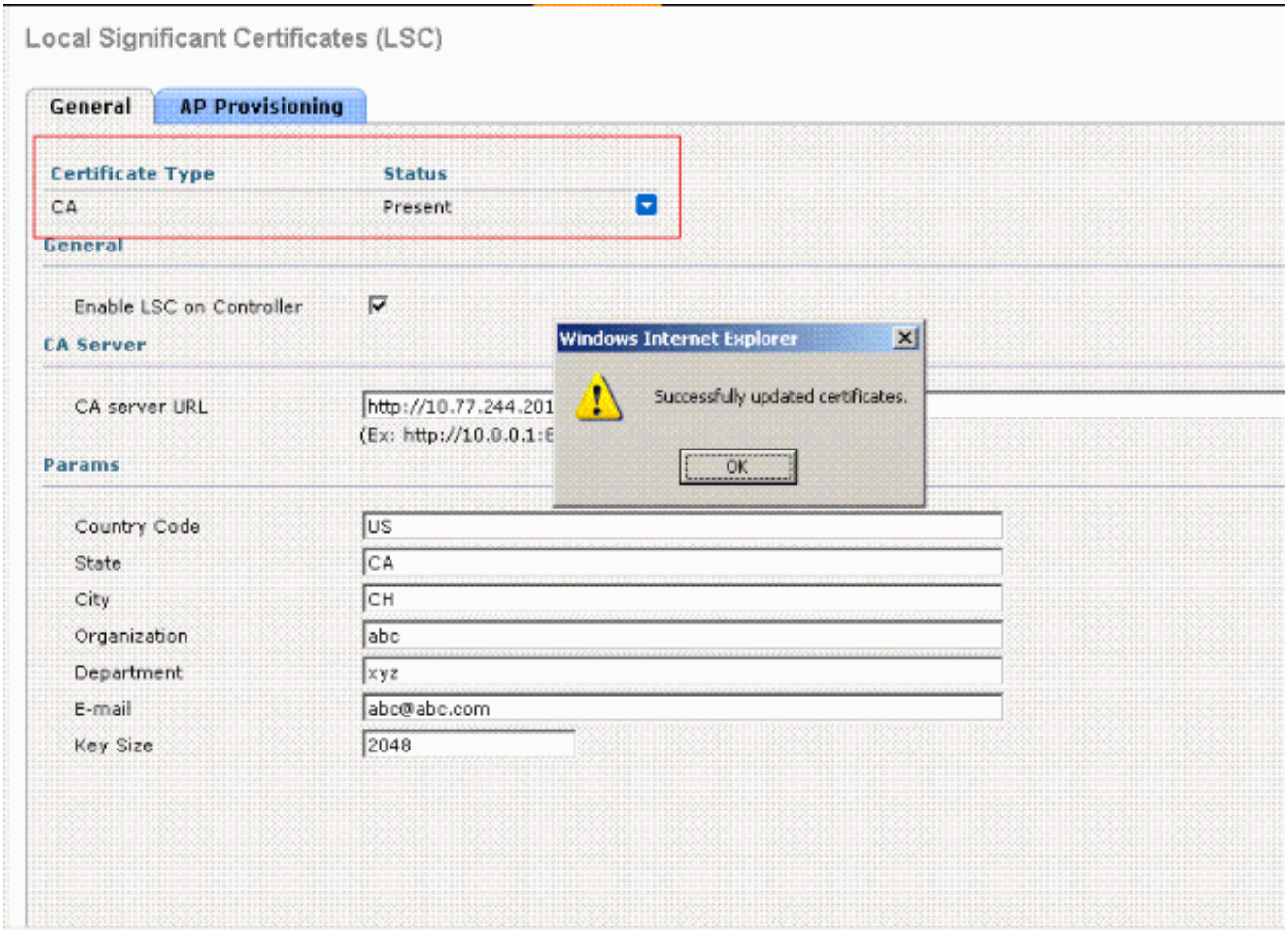
Настройте контроллер беспроводной локальной сети через GUI

Выполните следующие действия:

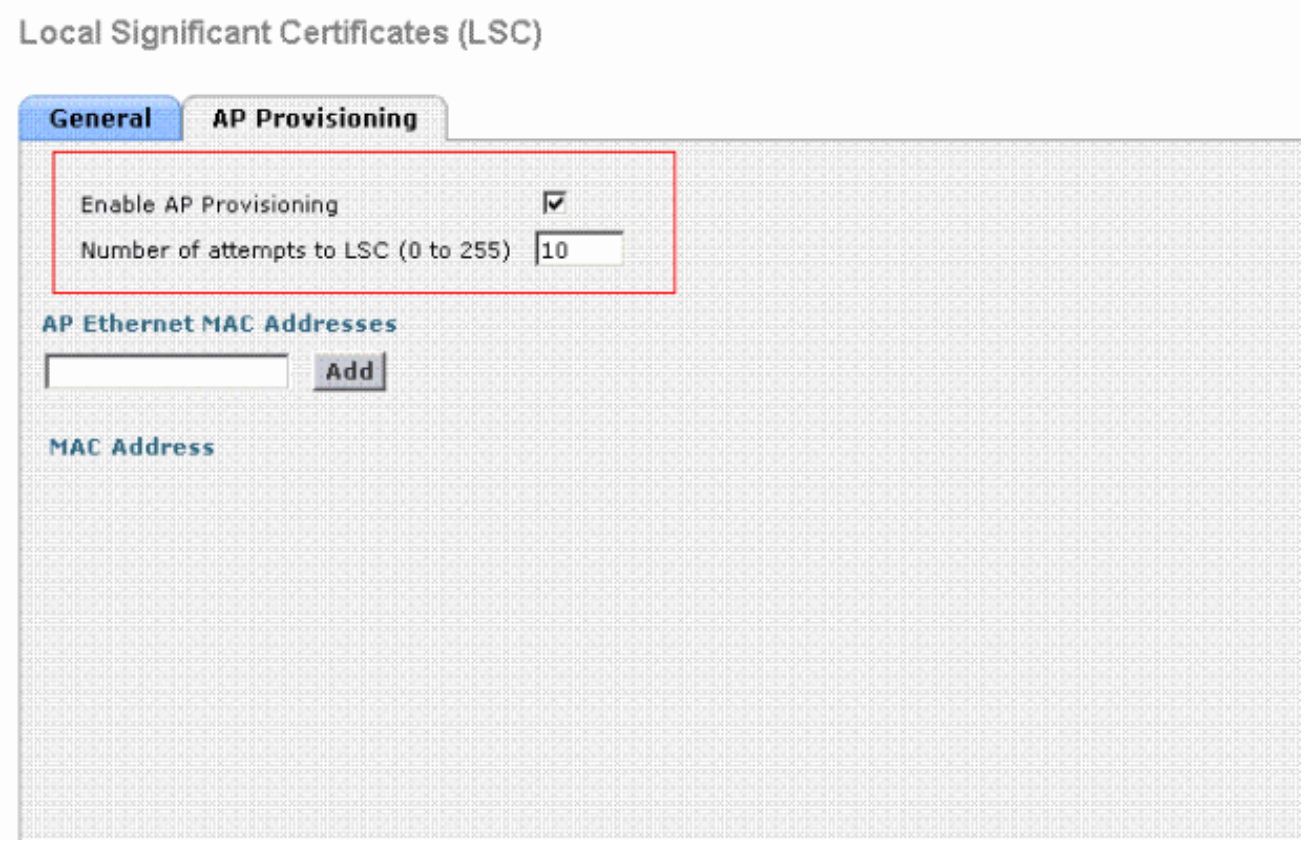
1. От GUI Контроллера беспроводной локальной сети нажмите **Security> Certificate> LSC** для открытия страницы Local Significant Certificates (LSC).
2. Нажмите **Вкладку Общие**.
3. Для включения LSC в системе проверьте **Разрешать LSC на флажке Controller**.
4. В поле CA Server URL введите URL в сервер CA. Можно ввести или доменное имя или IP-адрес.
5. В полях Params введите параметры для сертификата устройства. Размер ключа является значением от 384 до 2048 (в битах), и значение по умолчанию является 2048.
6. Нажмите **Apply** для фиксации изменений.



7. Для добавления сертификата CA в базу данных сертификата CA контроллера, нависают курсор над синей стрелкой выпадающего списка для Типа сертификата, и для выбора **Add**.
   Например.



8. Для инициализации LSC на точке доступа нажмите вкладку **AP Provisioning** и проверьте флажок **Enable AP Provisioning**.
9. Для добавления точек доступа к списку условия введите MAC-адрес точки доступа в поле AP Ethernet MAC Addresses и **нажмите Add**. Для удаления точки доступа из списка условия, нависают курсор над синей стрелкой выпадающего списка для точки доступа, и для выбора **Remove**.При настройке списка условия точки доступа только точки доступа в списке условия настроены при включении инициализации AP. Если вы не настраиваете список условия точки доступа, все точки доступа с MIC или сертификатом SSC, которые присоединяются к контроллеру, являются настроенным LSC.
10. Нажмите **Apply** для фиксации изменений.



Настройте контроллер беспроводной локальной сети через CLI

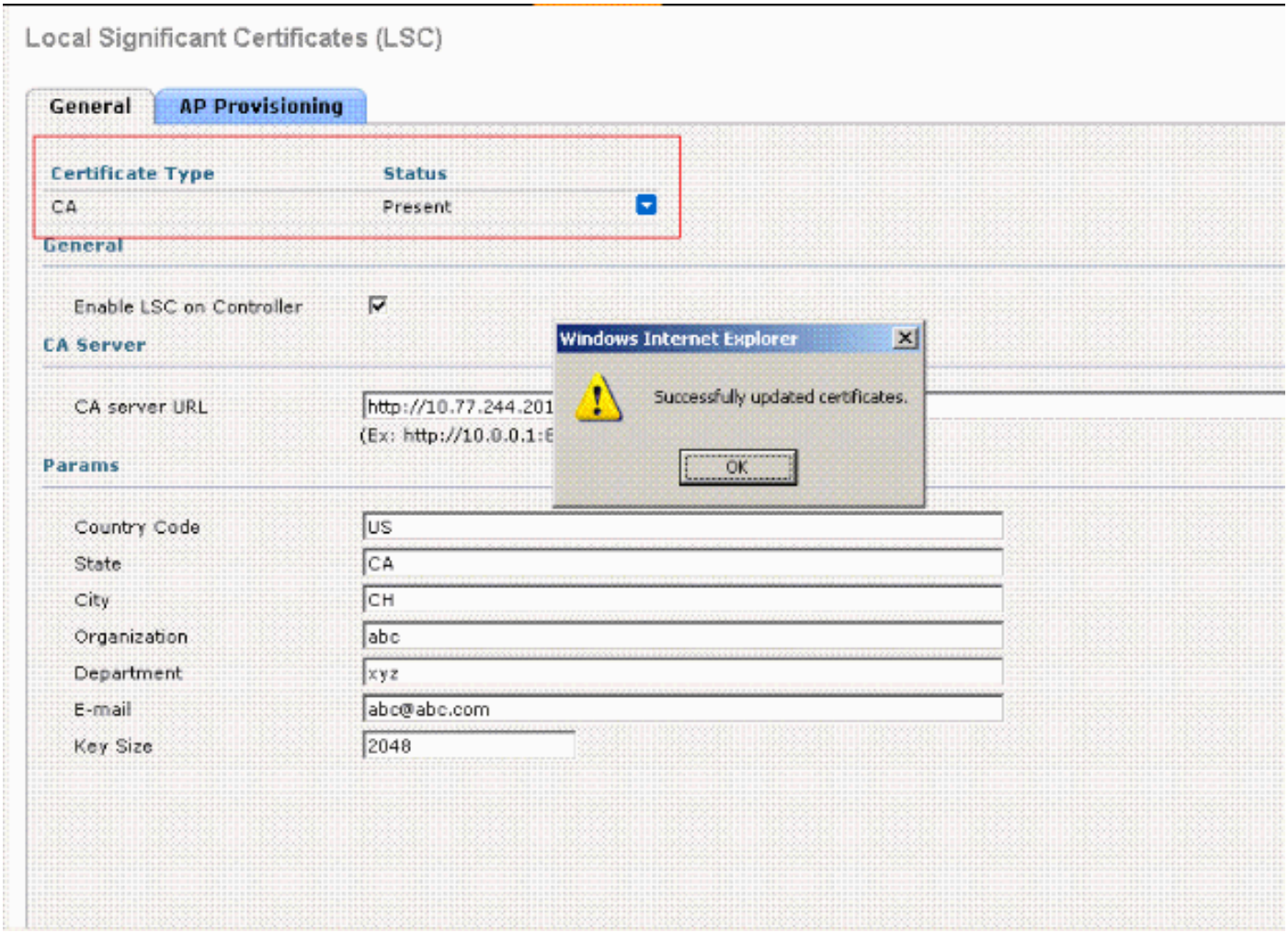
См. Использование CLI для Настройки раздела LSC руководства по конфигурированию контроллера Cisco Wireless LAN, Выпуска 5.2 для получения информации о процедуре для включения опции логически значимого сертификата (LSC) от CLI на контроллере.

Проверка

Этот раздел позволяет убедиться, что конфигурация работает правильно.

Средство Output Interpreter (OIT) (только для зарегистрированных клиентов) поддерживает определенные команды show. **Посредством OIT можно анализировать выходные данные команд show.**

Как только Контроллер беспроводной локальной сети настроен, и сервер CA существует, Контроллер беспроводной локальной сети использует Протокол SCEP, чтобы связаться с сервером CA и получить сертификат LSC. Вот снимок экрана WLC, как только установлен сертификат.



Когда LAP подходит, LAP обнаруживает WLC с механизмами обнаружения Уровня 3 Уровня 2/и отправляет Соединению Запросы к контроллеру с сертификатом MIC.

Контроллер беспроводной локальной сети тогда передает запрос параметра сертификата LSC к LAP.

С SubjectName/CN, передаваемым от WLC, AP генерирует PKCS #10 CertReq и передает ‘Запрос сертификата LSC LWAPP’ к WLC.

Этот запрос в свою очередь передан WLC к серверу CA. Сервер CA передает сертификат LSC LAP к контроллеру. Контроллер тогда передает LSC к LAP.

Это сообщение появляется на CLI AP.

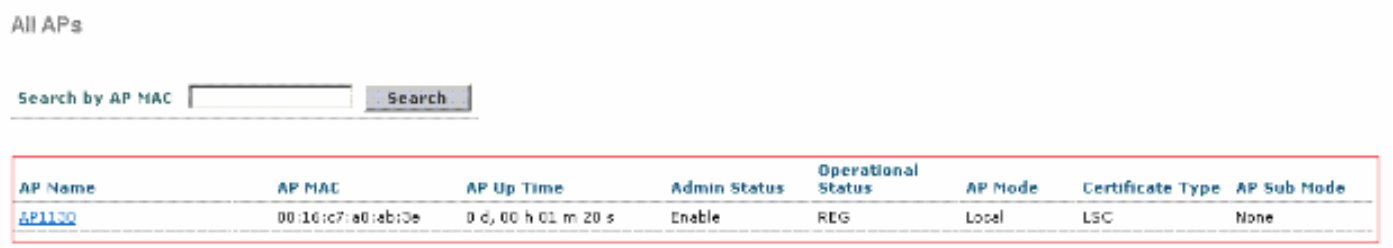
```
The name for the keys will be: Cisco_IOS_LSC_Keys

% The key modulus size is 2048 bits
% Generating 2048 bit RSA keys, keys will be non-exportable...[OK]
LSC CA cert successfully imported
LSC device cert successfully imported
```

Наконец, LAP отправляет запрос соединения с LSC.

Выполните **команду debug capwap events enable** для просмотра этой последовательности событий.

Как только LAP регистрируется в WLC с LSC, можно подтвердить это на GUI WLC.



Можно также использовать эти команды от CLI WLC для проверки этого. Например:

```
show certificate lsc summary Information similar to the following appears: LSC
Enabled..................................... Yes LSC CA-
Server...................................... http://10.77.244.201:8080/caserver LSC AP-
Provisioning................................ Yes Provision-
List.............................. Not Configured LSC Revert Count in AP
reboots................... 3 LSC Params: Country..................................... 4
State....................................... ca
City........................................ ch
Orgn........................................ abc
Dept........................................ xyz
Email....................................... abc@abc.com
KeySize..................................... 2048 LSC Certs: CA
Cert........................................ Not Configured RA
Cert..................................... Not Configured
```

Чтобы посмотреть детали о точках доступа, которые настроены с LSC, вводят эту команду:

```
show certificate lsc ap-provision Information similar to the following appears: LSC AP-
Provisioning.......................... Yes Provision-List.............................
Present Idx Mac Address --- ------------ 1 00:18:74:c7:c0:90
```

Устранение неполадок

Этот раздел объясняет, как устранить неполадки вашей конфигурации. Можно использовать **команду debug pm pki scep enable** для просмотра последовательности событий.

Вот пример успешного журнала отладки:

```
Success log:

WLC

(Cisco Controller) >

scep: waiting for 10 secsmLscScepTask: Nov 23 06:52:21.455:
scep: : Nov 23 06:52:27.519:

===== SCEP_OPERATION_GETCAPS =====
scep: Failed to get SCEP Capabilities from CA. Some CA's do not support this.
scep: Getting CA Certificate(s).
scep: : Nov 23 06:52:27.519:

===== SCEP_OPERATION_GETCA =====
scep: requesting CA certificate

scep: Sent 82 byteseded: Operation now in progress*emWeb: Nov 23 06:52:27.526:
scep: Http response is <HTTP/1.1 200 OK>
scep: Server returned status code 200.
scep: header info: <Connection: close>
```

```
scep: header info: <Date: Wed, 23 Nov 2011 06:52:30 GMT>
scep: header info: <Server: Microsoft-IIS/6.0>
scep: header info: <Content-Length: 3795>
scep: header info: <Content-Type: application/x-x509-ca-ra-cert>
scep: MIME header: application/x-x509-ca-ra-cert
scep: found certificate:
  subject: /DC=com/DC=ccie/CN=AD
  issuer: /DC=com/DC=ccie/CN=AD
  usage: Digital Signature, Certificate Sign, CRL Sign
scep: found certificate:
  subject: /C=CN/ST=BJ/L=BJ/O=Cisco/OU=BN/CN=tls/emailAddress=tls@ccie.com
  issuer: /DC=com/DC=ccie/CN=AD
  usage: Key Encipherment
scep: found certificate:
  subject: /C=CN/ST=BJ/L=BJ/O=Cisco/OU=BN/CN=tls/emailAddress=tls@ccie.com
  issuer: /DC=com/DC=ccie/CN=AD
  usage: Digital Signature
scep: CA cert retrieved with fingerprint 639993FF7FF8FB12EF2FB09DEC7C5BED

scep: waiting for 10 secs 06:52:34.463:

AP
(Cisco Controller) >
scep: waiting for 10 secsmLscScepTask: Nov 23 06:52:47.471:
scep: waiting for 10 secs 06:53:00.479:
scep: AP MAC: 58:bc:27:13:4a:d0 Starting new enrollment request.
scep: creating inner PKCS#7:01.542:
scep: data payload size: 797 bytes:
scep: successfully encrypted payload
scep: envelope size: 1094 bytes545:
scep: Sender Nonce before send: 089AC8C4604FCEB10C1F30E045073B10
scep: creating outer PKCS#7:01.545:
scep: signature added successfully:
scep: adding signed attributes.545:
scep: adding string attribute transId
scep: adding string attribute messageType
scep: adding octet attribute senderNonce
scep: PKCS#7 data written successfully
scep: applying base64 encoding.565:
scep: base64 encoded payload size: 3401 bytes

scep: Sent 3646 bytesed: Operation now in progress*sshpmLscTask: Nov 23 06:53:01.613:
scep: SenderNonce in reply: BF4EE64D4169584D90B2502ECCC0C133
scep: recipientNonce in reply: 089AC8C4604FCEB10C1F30E045073B10
scep: Http response is <HTTP/1.1 200 OK>
scep: Server returned status code 200.:
scep: header info: <Connection: close>:
scep: header info: <Date: Wed, 23 Nov 2011 06:53:02 GMT>
scep: header info: <Server: Microsoft-IIS/6.0>
scep: header info: <Content-Length: 2549>
scep: header info: <Content-Type: application/x-pki-message>
scep: MIME header: application/x-pki-message

scep: reading outer PKCS#706:53:13.488:
scep: PKCS#7 payload size: 2549 bytes8:
scep: PKCS#7 contains 2023 bytes of enveloped data
scep: verifying signature 06:53:13.489:
scep: signature ok Nov 23 06:53:13.490:
scep: finding signed attributes:13.490:
scep: finding attribute transId:13.490:
scep: allocating 32 bytes for attribute.
scep: reply transaction id: A984A2DFE20DA7E0FE702DC8EC307F33
scep: finding attribute messageType490:
scep: allocating 1 bytes for attribute.
```

scep: reply message type is good13.490:
scep: finding attribute senderNonce490:
scep: allocating 16 bytes for attribute.
scep: finding attribute recipientNonce:
scep: allocating 16 bytes for attribute.
scep: finding attribute pkiStatus3.491:
scep: allocating 1 bytes for attribute.
scep: pkistatus: **SUCCESS3** 06:53:13.491: scep: reading inner PKCS#706:53:13.491: scep: decrypting inner PKCS#753:13.492: scep: **found certificate:** subject: /serialNumber= PID:AIR-LAP1262N-A-K9 SN:FTX1433K60R/C=CN/ST=BJ/L=BJ/O=Cisco/OU=BN/CN=AP3G1-f866f267577e/emailAddress= tls@ccie.com issuer: /DC=com/DC=ccie/CN=AD scep: PKCS#7 payload size: 1580 bytes:53:13.518: Digital Signature, Key Encipherment scep: waiting for 10 secs 06:53:13.520:

Это - пример случая, где это отказывает:

Fail log
WLC
(Cisco Controller) >debug pm pki scep detail enable
scep: waiting for 10 secsmLscScepTask: Nov 23 00:57:52.407:
scep: waiting for 10 secs 00:58:05.415:
scep: waiting for 10 secs 00:58:18.423:
scep: waiting for 10 secs 00:58:31.431:
scep: waiting for 10 secs 00:58:44.439:
scep: waiting for 10 secs 00:58:57.447:
scep: waiting for 10 secs 00:59:10.455:
scep: : Nov 23 00:59:22.479:
===== SCEP_OPERATION_GETCAPS =====
scep: Failed to get SCEP Capabilities from CA. Some CA's do not support this.
scep: Getting CA Certificate(s).
scep: : Nov 23 00:59:22.479:
===== SCEP_OPERATION_GETCA =====
scep: requesting CA certificate

scep: Sent 82 byteseded: Operation now in progress*emWeb: Nov 23 00:59:22.486:
scep: Http response is <HTTP/1.1 200 OK>
scep: Server returned status code 200.
scep: header info: <Connection: close>
scep: header info: <Date: Wed, 23 Nov 2011 00:59:22 GMT>
scep: header info: <Server: Microsoft-IIS/6.0>
scep: header info: <Content-Length: 3795>
scep: header info: <Content-Type: application/x-x509-ca-ra-cert>
scep: MIME header: application/x-x509-ca-ra-cert
scep: found certificate:
  subject: /DC=com/DC=ccie/CN=AD
  issuer: /DC=com/DC=ccie/CN=AD
  usage: Digital Signature, Certificate Sign, CRL Sign
scep: found certificate:
  subject: /C=CN/ST=BJ/L=BJ/O=Cisco/OU=BN/CN=tls/emailAddress=tls@ccie.com
  issuer: /DC=com/DC=ccie/CN=AD
  usage: Key Encipherment
scep: found certificate:
  subject: /C=CN/ST=BJ/L=BJ/O=Cisco/OU=BN/CN=tls/emailAddress=tls@ccie.com
  issuer: /DC=com/DC=ccie/CN=AD
  usage: Digital Signature
scep: CA cert retrieved with fingerprint 639993FF7FF8FB12EF2FB09DEC7C5BED

scep: waiting for 10 secs 00:59:23.463:

AP:
(Cisco Controller) >debug pm pki scep detail enable
scep: waiting for 10 secsmLscScepTask: Nov 22 18:06:22.100:
scep: waiting for 10 secs 18:06:35.108:
scep: waiting for 10 secs 18:06:48.116:
scep: waiting for 10 secs 18:07:01.124:

```
scep: AP MAC: 58:bc:27:13:4a:d0 Starting new enrollment request.
scep: creating inner PKCS#7:04.631:
scep: data payload size: 536 bytes:
scep: successfully encrypted payload
scep: envelope size: 838 bytes.633:
scep: Sender Nonce before send: F8BBA9EB06579188A62635A1DFA6510A
scep: creating outer PKCS#7:04.634:
scep: signature added successfully:
scep: adding signed attributes.634:
scep: adding string attribute transId
scep: adding string attribute messageType
scep: adding octet attribute senderNonce
scep: PKCS#7 data written successfully
scep: applying base64 encoding.655:
scep: base64 encoded payload size: 3055 bytes

scep: Sent 3280 bytesed: Operation now in progress*sshpmLscTask: Nov 22 18:07:04.690:
scep: SenderNonce in reply: 69A4BF610ED41746B1066B5BEC4427F0
scep: recipientNonce in reply: F8BBA9EB06579188A62635A1DFA6510A
scep: Http response is <HTTP/1.1 200 OK>
scep: Server returned status code 200.:
scep: header info: <Connection: close>:
scep: header info: <Date: Tue, 22 Nov 2011 18:07:04 GMT>
scep: header info: <Server: Microsoft-IIS/6.0>
scep: header info: <Content-Length: 540>
scep: header info: <Content-Type: application/x-pki-message>
scep: MIME header: application/x-pki-message

scep: reading outer PKCS#718:07:14.133:
scep: PKCS#7 payload size: 540 bytes33:
scep: PKCS#7 contains 1 bytes of enveloped data
scep: verifying signature 18:07:14.134:
scep: signature ok Nov 22 18:07:14.135:
scep: finding signed attributes:14.135:
scep: finding attribute transId:14.135:
scep: allocating 32 bytes for attribute.
scep: reply transaction id: 3DA1646840CD4FFEB1534EA8F1D45F76
scep: finding attribute messageType135:
scep: allocating 1 bytes for attribute.
scep: reply message type is good14.135:
scep: finding attribute senderNonce135:
scep: allocating 16 bytes for attribute.
scep: finding attribute recipientNonce:
scep: allocating 16 bytes for attribute.
scep: finding attribute pkiStatus4.136:
scep: allocating 1 bytes for attribute.
scep: pkistatus: FAILURE2 18:07:14.136:
scep: finding attribute failInfo14.136: scep: allocating 1 bytes for attribute. scep: reason:
Transaction not permitted or supported scep: waiting for 10 secs 18:07:14.136: scep: waiting for
10 secs 18:07:27.144: scep: waiting for 10 secs 18:07:40.152: scep: waiting for 10 secs
18:07:53.160: scep: waiting for 10 secs 18:08:06.168: scep: waiting for 10 secs 18:08:19.176:
scep: waiting for 10 secs 18:08:32.184: scep: waiting for 10 secs 18:08:45.192: scep: waiting
for 10 secs 18:08:58.200: scep: waiting for 10 secs 18:09:11.208:
```

Дополнительные сведения

- Руководство по конфигурированию контроллера Cisco Wireless LAN, выпуск 5.2
- Создание запроса подписи сертификата (CSR) для сертификата от третьей стороны на контроллере WLAN (WLC)
- Создание запроса подписи сертификата для сертификата от третьей и процедура закрузки связанных сертификатов в WLC

- Страница поддержки беспроводных технологий
- Cisco Systems – техническая поддержка и документация