Добавление вручную самоподписанных сертификатов к контроллеру точек доступа, преобразованных в LWAPP

Содержание

Введение

Этот документ объясняет методы, которые можно использовать для ручного добавления подписанных сертификатов (SSCs) к беспроводной сети LAN Cisco (WLAN) Контроллер (WLC).

SSC точки доступа (AP) должен существовать на всех WLC в сети, к которой AP имеет разрешения для регистрации. Как правило примените SSC ко всем WLC в той же группе мобильности. Когда добавление SSC к WLC не происходит через утилиту обновления, необходимо вручную добавить SSC к WLC с использованием процедуры в этом документе. Вам также нужна эта процедура, когда AP перемещен в другую сеть или когда дополнительные WLC добавлены к существующей сети.

Когда Протокол Lightweight AP Protocol (LWAPP) - преобразованный AP не связывается к WLC, можно распознать эту проблему. При устранении проблем проблемы сопоставления вы видите эти выходные данные при запуске этих отладок:

- При запуске **команды debug pm pki enable** вы видите:`(Cisco Controller) >`**`debug pm pki enable`** `Thu Jan 26 20:22:50 2006: sshpmGetIssuerHandles: locking ca cert table Thu Jan 26 20:22:50 2006: sshpmGetIssuerHandles: calling x509_alloc() for user cert Thu Jan 26 20:22:50 2006: sshpmGetIssuerHandles: calling x509_decode() Thu Jan 26 20:22:50 2006: sshpmGetIssuerHandles: <subject> L=San Jose, ST= California, C=US, O=Cisco Systems,`

```
MAILTO=support@cisco.com, CN=C1130-00146a1b3744 Thu Jan 26 20:22:50 2006:
sshpmGetIssuerHandles: <issuer> L=San Jose, ST= California, C=US, O=Cisco Systems,
MAILTO=support@cisco.com, CN=C1130-00146a1b3744 Thu Jan 26 20:22:50 2006:
sshpmGetIssuerHandles: Mac Address in subject is 00:XX:XX:XX:XX Thu Jan 26 20:22:50 2006:
sshpmGetIssuerHandles: Cert is issued by Cisco Systems. Thu Jan 26 20:22:50 2006:
sshpmGetIssuerHandles: SSC is not allowed by config; bailing... Thu Jan 26 20:22:50 2006:
sshpmFreePublicKeyHandle: called with (nil) Thu Jan 26 20:22:50 2006:
sshpmFreePublicKeyHandle: NULL argument.
```

- При запуске **команды debug lwapp events enable** вы видите:`(Cisco Controller) >`**`debug lwapp errors enable`** `.... Thu Jan 26 20:23:27 2006: Received LWAPP DISCOVERY REQUEST from AP 00:13:5f:f8:c3:70 to ff:ff:ff:ff:ff:ff on port '1' Thu Jan 26 20:23:27 2006: Successful transmission of LWAPP Discovery-Response to AP 00:13:5f:f8:c3:70 on Port 1 Thu Jan 26 20:23:27 2006: Received LWAPP JOIN REQUEST from AP 00:13:5f:f9:dc:b0 to 06:0a:10:10:00:00 on port '1' Thu Jan 26 20:23:27 2006: sshpmGetIssuerHandles: locking ca cert table Thu Jan 26 20:23:27 2006: sshpmGetIssuerHandles: calling x509_alloc() for user cert Thu Jan 26 20:23:27 2006: sshpmGetIssuerHandles: calling x509_decode() Thu Jan 26 20:23:27 2006: sshpmGetIssuerHandles: <subject> L=San Jose, ST= California, C=US, O=Cisco Systems, MAILTO=support@cisco.com, CN=C1130-00146a1b321a Thu Jan 26 20:23:27 2006: sshpmGetIssuerHandles: <issuer> L=San Jose, ST= California, C=US, O=Cisco Systems, MAILTO=support@cisco.com, CN=C1130-00146a1b321a Thu Jan 26 20:23:27 2006: sshpmGetIssuerHandles: Mac Address in subject is 00:14:6a:1b:32:1a`` **`Thu Jan 26 20:23:27 2006: sshpmGetIssuerHandles: Cert is issued by Cisco Systems. Thu Jan 26 20:23:27 2006: sshpmGetIssuerHandles: SSC is not allowed by config; bailing... Thu Jan 26 20:23:27 2006: LWAPP Join-Request does not include valid certificate in CERTIFICATE_PAYLOAD from AP 00:13:5f:f9:dc:b0. Thu Jan 26 20:23:27 2006: sshpmFreePublicKeyHandle: called with (nil) Thu Jan 26 20:23:27 2006: sshpmFreePublicKeyHandle: NULL argument. Thu Jan 26 20:23:27 2006: Unable to free public key for AP 00:13:5F:F9:DC:B0 Thu Jan 26 20:23:27 2006: spamDeleteLCB: stats timer not initialized for AP 00:13:5f:f9:dc:b0 Thu Jan 26 20:23:27 2006: spamProcessJoinRequest : spamDecodeJoinReq failed`**

Предварительные условия

Требования

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

- WLC не содержит SSC, который генерировала утилита обновления.
- AP содержат SSC.
- Telnet включена на WLC и AP.
- Минимальный номер версии кода программного обеспечения Cisco IOS предLWAPP находится на AP, который будет обновлен.

Используемые компоненты

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

- 2006 WLC Cisco, который выполняет микропрограммное обеспечение 3.2.116.21 без установленного SSC
- Cisco Aironet AP серии 1230 с SSC

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

Более подробную информацию о применяемых в документе обозначениях см. в описании условных обозначений, используемых в технической документации Cisco.

Общие сведения

В Cisco Централизованная архитектура WLAN AP работают в облегченном режиме. AP связываются к WLC Cisco с использованием LWAPP. LWAPP является протоколом проекта инженерной группы по развитию Интернета (IETF), который определяет контроль, обменивающийся сообщениями для настройки и аутентификации пути и операций во время выполнения. Протокол LWAPP также определяет механизм туннелирования потока данных.

Легковесный AP (LAP) обнаруживает WLC с использованием механизмов обнаружения LWAPP. LAP тогда передает WLC Запрос на присоединение LWAPP. WLC передает LAP ответ соединения LWAPP, который позволяет LAP присоединяться к WLC. Когда LAP соединен с WLC, LAP загружает программное обеспечение WLC, если не совпадают пересмотры на LAP и WLC. Впоследствии, LAP полностью находится под контролем WLC.

LWAPP защищает связь контроля между AP и WLC посредством безопасного распределения ключей. Безопасное распределение ключей уже требует настроенных цифровых сертификатов X.509 и на LAP и на WLC. Установленные при производстве сертификаты обозначаются термином "MIC", что представляет собой сокращение термина "Сертификат, установленный при производстве" (англ.: Manufacturing Installed Certificate). AP Aironet, которые поставили до 18 июля 2005, не имеют MIC. Таким образом, эти AP создают SSC, когда они преобразованы для работы в облегченном режиме. Контроллеры запрограммированы на принятие SSC для аутентификации определенных AP.

Это - процесс обновления:

1. Пользователь выполняет утилиту обновления, которая принимает входной файл со списком AP и их IP-адресов, в дополнение к их учетным данным входа в систему.
2. Утилита устанавливает сеансы Telnet с AP и передает серию Программных команд Cisco IOS во входном файле для подготовки AP к обновлению. Эти команды включают команды для создания SSCs. Кроме того, утилита устанавливает сеанс Telnet с WLC для программирования устройства для разрешения авторизации определенных AP SSC.
3. Утилита тогда загружает программное обеспечение Cisco IOS версии 12.3 (7) JX на AP так, чтобы AP мог присоединиться к WLC.
4. После того, как AP присоединяется к WLC, AP загружает завершенную версию программного обеспечения Cisco IOS от WLC. Утилита обновления генерирует выходной файл, который включает список AP и соответствующих значений хэша - ключа SSC, которые могут быть импортированы в программное обеспечение для управления Wireless Control System (WCS).
5. WCS может тогда передать эту информацию к другим WLC в сети.

После того, как AP присоединяется к WLC, вы можете reassign AP к любому WLC в вашей сети, при необходимости.

Найдите хэш ключа SHA1

Если компьютер, который выполнил преобразование AP, доступен, можно получить Хэш Ключа Защищенного алгоритма хэширования 1 (SHA1) из файла .csv, который находится в каталоге Cisco Upgrade Tool. Если файл .csv недоступен, можно выполнить **команду отладки** на WLC для получения Хэша Ключа SHA1.

Выполните следующие действия:

1. Включите AP и подключите его с сетью.
2. Включите отладку на интерфейсе командной строки (CLI) WLC.Команда является **pki debug pm, включают**.(Cisco Controller) >**debug pm pki enable** Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: getting (old) aes ID cert handle... Mon May 22 06:34:10 2006: sshpmGetCID: called to evaluate <bsnOldDefaultIdCert> Mon May 22 06:34:10 2006: sshpmGetCID: comparing to row 0, CA cert >bsnOldDefaultCaCert< Mon May 22 06:34:10 2006: sshpmGetCID: comparing to row 1, CA cert >bsnDefaultRootCaCert< Mon May 22 06:34:10 2006: sshpmGetCID: comparing to row 2, CA cert >bsnDefaultCaCert< Mon May 22 06:34:10 2006: sshpmGetCID: comparing to row 3, CA cert >bsnDefaultBuildCert< Mon May 22 06:34:10 2006: sshpmGetCID: comparing to row 4, CA cert >cscoDefaultNewRootCaCert< Mon May 22 06:34:10 2006: sshpmGetCID: comparing to row 5, CA cert >cscoDefaultMfgCaCert< Mon May 22 06:34:10 2006: sshpmGetCID: comparing to row 0, ID cert >bsnOldDefaultIdCert< Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Calculate SHA1 hash on Public Key Data Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data 30820122 300d0609 2a864886 f70d0101 Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data 01050003 82010f00 3082010a 02820101 Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data 00c805cd 7d406ea0 cad8df69 b366fd4c Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data 82fc0df0 39f2bff7 ad425fa7 face8f15 Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data f356a6b3 9b876251 43b95a34 49292e11 Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data 038181eb 058c782e 56f0ad91 2d61a389 Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data f81fa6ce cd1f400b b5cf7cef 06ba4375 Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data dde0648e c4d63259 774ce74e 9e2fde19 Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data 0f463f9e c77b79ea 65d8639b d63aa0e3 Mon May 22 06:34:10 2006: sshpmGetIssuerHandles: Key Data 7dd485db 251e2e07 9cd31041 b0734a55 Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data 463fbacc 1a61502d c54e75f2 6d28fc6b Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data 82315490 881e3e31 02d37140 7c9c865a Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data 9ef3311b d514795f 7a9bac00 d13ff85f Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data 97e1a693 f9f6c5cb 88053e8b 7fae6d67 Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data ca364f6f 76cf78bc bc1acc13 0d334aa6 Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data 031fb2a3 b5e572df 2c831e7e f765b7e5 Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data fe64641f de2a6fe3 23311756 8302b8b8 Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data 1bfae1a8 eb076940 280cbed1 49b2d50f Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: Key Data f7020301 0001 Mon May 22 06:34:14 2006: sshpmGetIssuerHandles: **SSC Key Hash is 9e4ddd8dfcdd8458ba7b273fc37284b31a384eb9** Mon May 22 06:34:14 2006: LWAPP Join-Request MTU path from AP 00:0e:84:32:04:f0 is 1500, remote debug mode is 0 Mon May 22 06:34:14 2006: spamRadiusProcessResponse: AP Authorization failure for **00:0e:84:32:04:f0**

Добавьте SSC к WLC

Задача

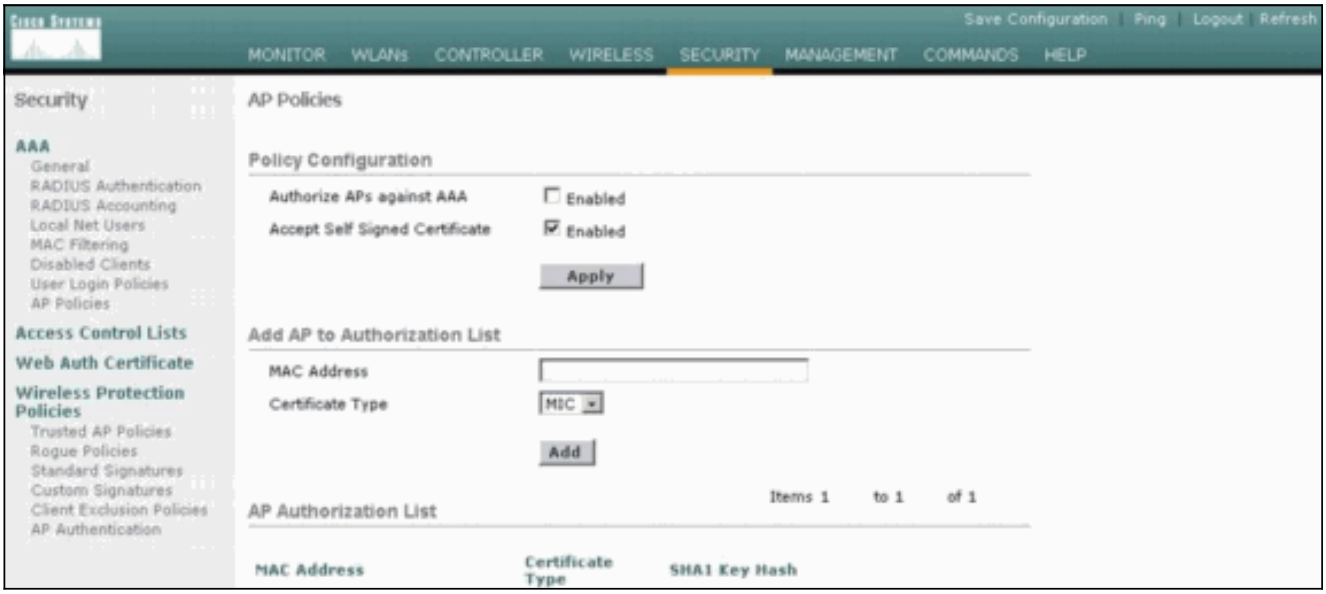
В этом разделе содержатся сведения о настройке функций, описанных в этом документе.

Конфигурация графического интерфейса пользователя (GUI)

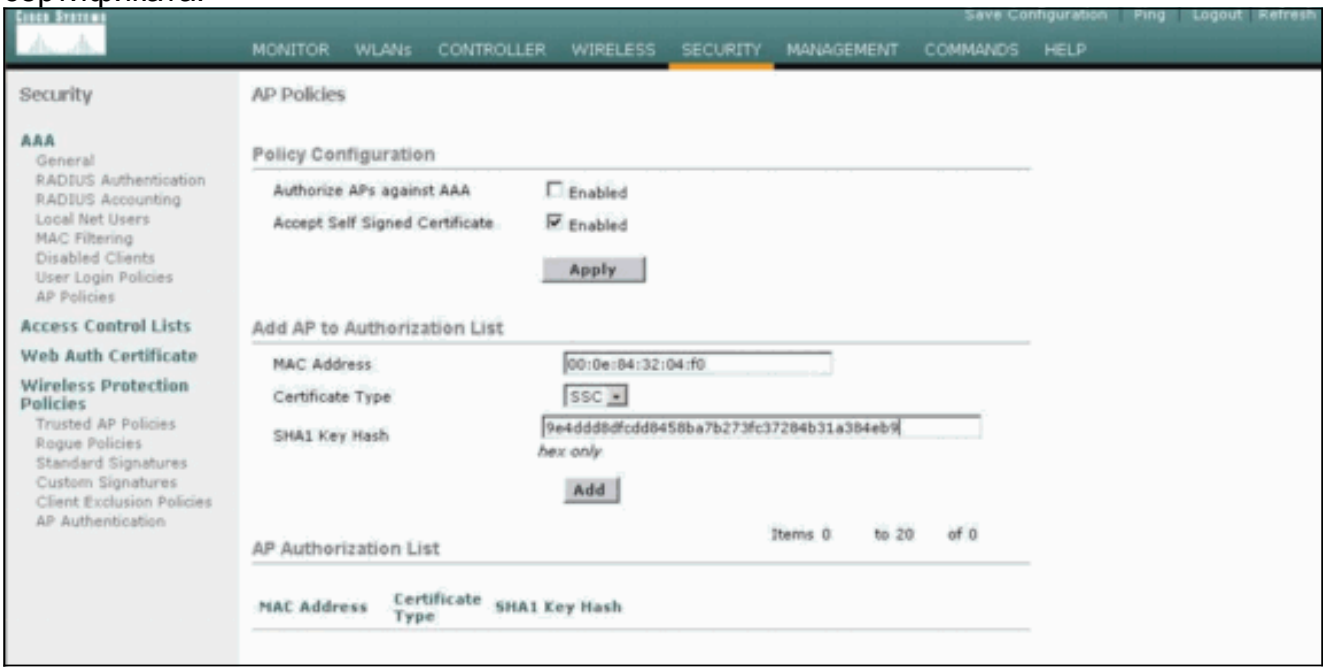
Выполните эти шаги от GUI:

1. Выберите **Security> AP Policies** и нажмите **Enabled beside Accept Self Signed**

Certificate.



2. Выберите **SSC** от раскрывающегося меню Типа сертификата.



3. Введите MAC-адрес AP и ключа хэша, и **нажмите Add**.

Конфигурация интерфейса командой строки CLI

Выполните эти шаги от CLI:

1. Включите принимают сам подписанный сертификат на WLC.Команда является **config auth-list ap-policy ssc, включают**.`(Cisco Controller) >config auth-list ap-policy ssc enable`
2. Добавьте MAC-адрес AP и ключ хэша к списку авторизации.Команда является **config auth-list add ssc** *AP_MAC AP_key*.`(Cisco Controller) >config auth-list add ssc 00:0e:84:32:04:f0 9e4ddd8dfcdd8458ba7b273fc37284b31a384eb9 !--- This command should be on one line.`

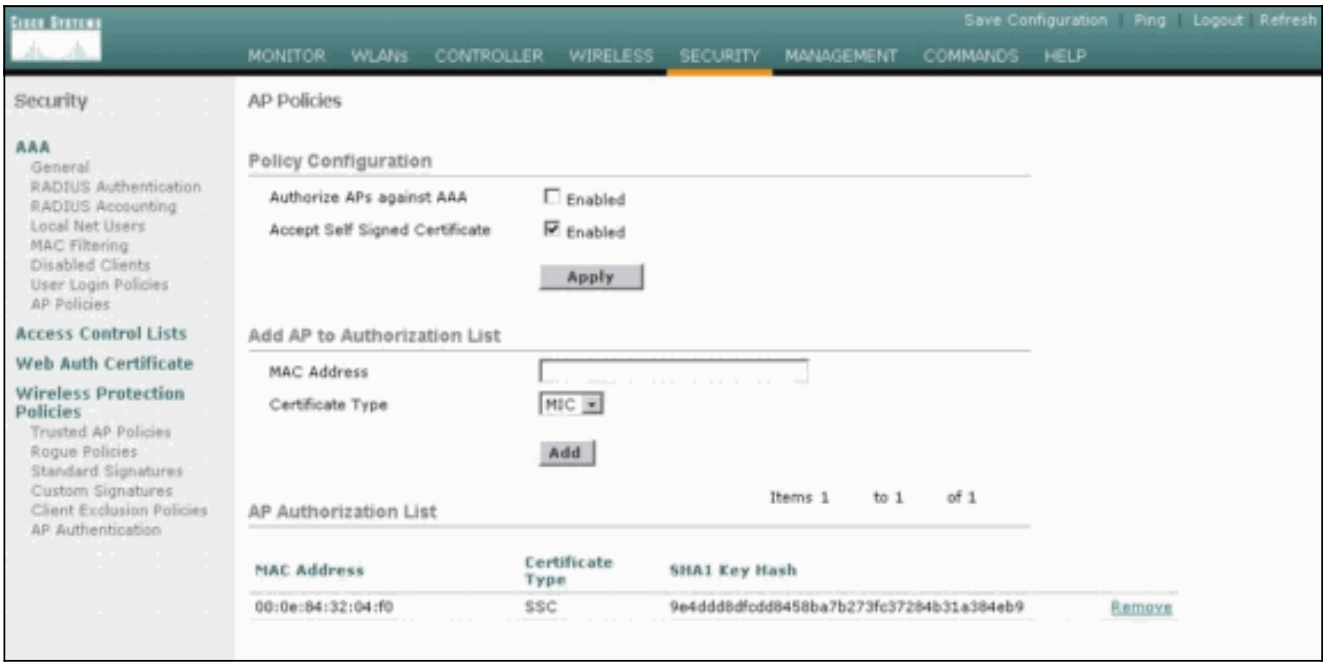
Проверка

Этот раздел позволяет убедиться, что конфигурация работает правильно.

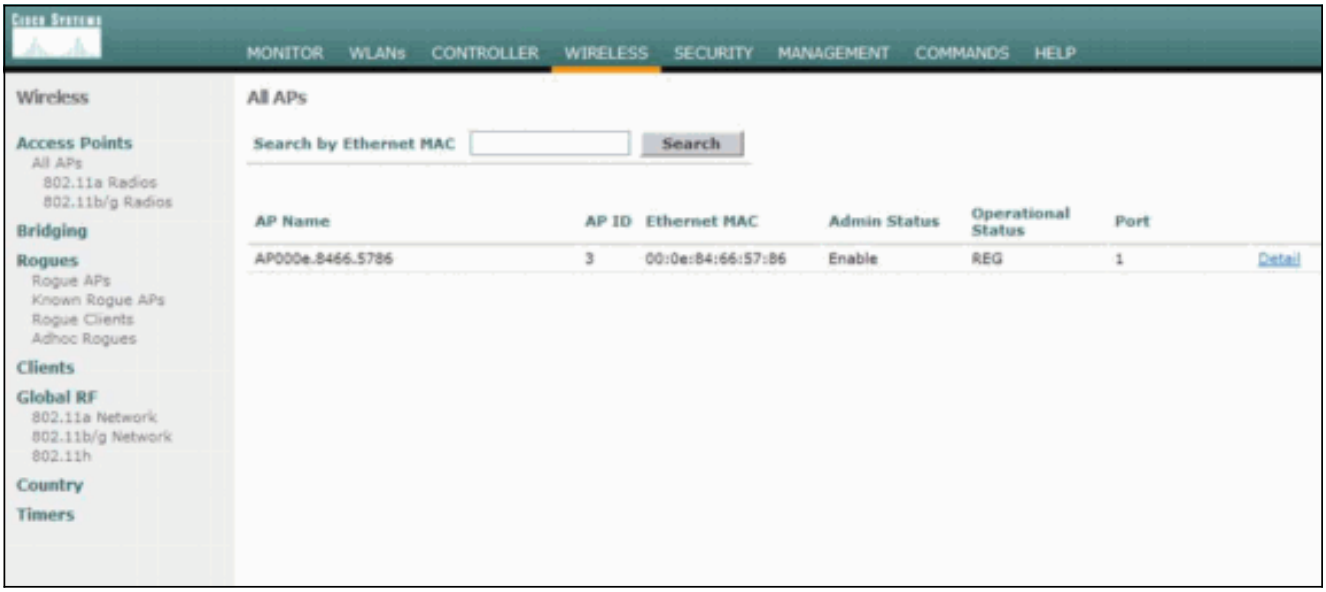
Проверка GUI

Выполните следующие действия:

1. В Окне политик AP проверьте, что MAC-адрес AP и Хэш Ключа SHA1 появляются в области AP Authorization
   List.



2. Во Всем окне Все APs проверьте, что все AP зарегистрированы в
   WLC.



Проверка CLI

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

- **show auth-list** список авторизации AP.

- **show ap summary** — Отображает сводку всех связанных AP.

Устранение неполадок

Для этой конфигурации в настоящее время нет сведений об устранении проблем.

Дополнительные сведения

- Wireless LAN Controller (WLC) Troubleshoot FAQ
- Руководство по настройке контроллеров беспроводной локальной сети Cisco, выпуск 3.2
- Пример базовой конфигурации контроллера беспроводной локальной сети и "облегченной" точки доступа
- Cisco Systems – техническая поддержка и документация