LWAPP 변환 AP용 컨트롤러에 자체 서명 인증서 수동 추가

목차

소개

이 문서에서는 WLC(Cisco Wireless LAN) 컨트롤러(WLAN)에 자체 서명 인증서(SSC)를 수동으로 추가하기 위해 사용할 수 있는 방법에 대해 설명합니다.

AP(액세스 포인트)의 SSC는 AP에 등록할 권한이 있는 네트워크의 모든 WLC에 있어야 합니다. 일반적으로 SSC를 동일한 모빌리티 그룹의 모든 WLC에 적용합니다. 업그레이드 유틸리티를 통해 WLC에 SSC를 추가하지 않는 경우 이 문서의 절차를 사용하여 WLC에 SSC를 수동으로 추가해야 합니다. 다른 AP를 이동할 때 이 절차가 필요합니다. 또는 기존 네트워크에 추가 WLC를 추가할 때

LWAPP(Lightweight AP Protocol) 변환 AP가 WLC에 연결되지 않은 경우 이 문제를 인식할 수 있습니다.연결 문제를 해결할 때 다음 디버그를 실행하면 다음 출력이 표시됩니다.

- debug pm pki enable 명령을 실행하면 다음이 표시됩니다.

```
(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.
```

- debug lwapp **events enable** 명령**을 실행하면** 다음을 볼 수 있습니다.

```
(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
```

사전 요구 사항

요구 사항

이 구성을 시도하기 전에 다음 요구 사항을 충족해야 합니다.

- WLC에는 업그레이드 유틸리티가 생성한 SSC가 없습니다.
- AP에 SSC가 포함되어 있습니다.
- 텔넷은 WLC 및 AP에서 활성화됩니다.
- LWAPP 이전 Cisco IOS® 소프트웨어 코드의 최소 버전은 업그레이드할 AP에 있습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- SSC가 설치되지 않은 펌웨어 3.2.116.21을 실행하는 Cisco 2006 WLC
- Cisco Aironet 1230 Series AP(SSC 포함)

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 규칙을 참조하십시오.

배경 정보

Cisco 중앙 집중식 WLAN 아키텍처에서 AP는 경량 모드로 작동합니다.LWAPP를 사용하여 Cisco WLC에 연결된 AP입니다.LWAPP는 설정 및 경로 인증 및 런타임 작업을 위한 제어 메시징을 정의하는 IETF(Internet Engineering Task Force) 초안 프로토콜입니다.LWAPP는 데이터 트래픽에 대한 터널링 메커니즘도 정의합니다.

경량 AP(LAP)는 LWAPP 검색 메커니즘을 사용하여 WLC를 검색합니다.그런 다음 LAP가 WLC와 LWAPP 가입 요청을 보냅니다.WLC는 LAP가 WLC에 참여할 수 있도록 LAP와 LWAPP 조인 응답을 보냅니다.LAP가 WLC에 조인되면 LAP는 LAP의 수정 버전과 WLC가 일치하지 않으면 WLC 소프트웨어를 다운로드합니다.그런 다음 LAP는 WLC의 제어에 완전히 속합니다.

LWAPP는 보안 키 배포를 통해 AP와 WLC 간의 제어 통신을 보호합니다.보안 키 배포에는 LAP 및 WLC 모두에서 이미 프로비저닝된 X.509 디지털 인증서가 필요합니다.공장 출하 시 설치된 인증서는 Manufacturing Installed Certificate의 약어인 "MIC"에서 참조됩니다.2005년 7월 18일 이전에 배송된 Aironet AP에는 MIC가 없습니다.따라서 이러한 AP는 경량 모드에서 작동하도록 변환될 때 SSC를 생성합니다.컨트롤러는 특정 AP의 인증을 위해 SSC를 허용하도록 프로그래밍됩니다.

다음은 업그레이드 프로세스입니다.

1. 사용자는 로그인 자격 증명 외에도 AP 및 IP 주소 목록이 포함된 입력 파일을 수락하는 업그레이드 유틸리티를 실행합니다.
2. 이 유틸리티는 AP를 업그레이드하기 위해 준비하기 위해 AP와 텔넷 세션을 설정하고 일련의 Cisco IOS Software 명령을 입력 파일에 전송합니다.이러한 명령에는 SSC를 생성하는 명령이 포함되어 있습니다.또한 이 유틸리티는 특정 SSC AP의 권한 부여를 허용하도록 디바이스를 프로그래밍하기 위해 WLC와 텔넷 세션을 설정합니다.
3. 그런 다음 이 유틸리티는 AP가 WLC에 조인할 수 있도록 Cisco IOS 소프트웨어 릴리스 12.3(7)JX를 AP에 로드합니다.
4. AP가 WLC에 가입하면 AP는 WLC에서 완전한 Cisco IOS 소프트웨어 버전을 다운로드합니다.업그레이드 유틸리티는 WCS(Wireless Control System) 관리 소프트웨어로 가져올 수 있는 AP 목록 및 해당 SSC 키 해시 값을 포함하는 출력 파일을 생성합니다.
5. 그런 다음 WCS는 이 정보를 네트워크의 다른 WLC에 보낼 수 있습니다.

AP가 WLC에 가입한 후 필요한 경우 네트워크의 모든 WLC에 AP를 재할당할 수 있습니다.

SHA1 키 해시 찾기

AP 변환을 수행한 컴퓨터를 사용할 수 있는 경우 Cisco 업그레이드 도구 디렉터리에 있는 .csv 파일에서 SHA1(Secure Hash Algorithm 1) 키 해시를 가져올 수 있습니다. .csv 파일을 사용할 수 없는 경우 SHA1 키 해시를 검색하기 위해 WLC에서 **debug** 명령을 실행할 수 있습니다.

다음 단계를 완료하십시오.

1. AP를 켜고 네트워크에 연결합니다.
2. WLC CLI(Command Line Interface)에서 디버깅을 활성화합니다.명령은 debug pm pki enable**입니다**.

(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

WLC에 SSC 추가

작업

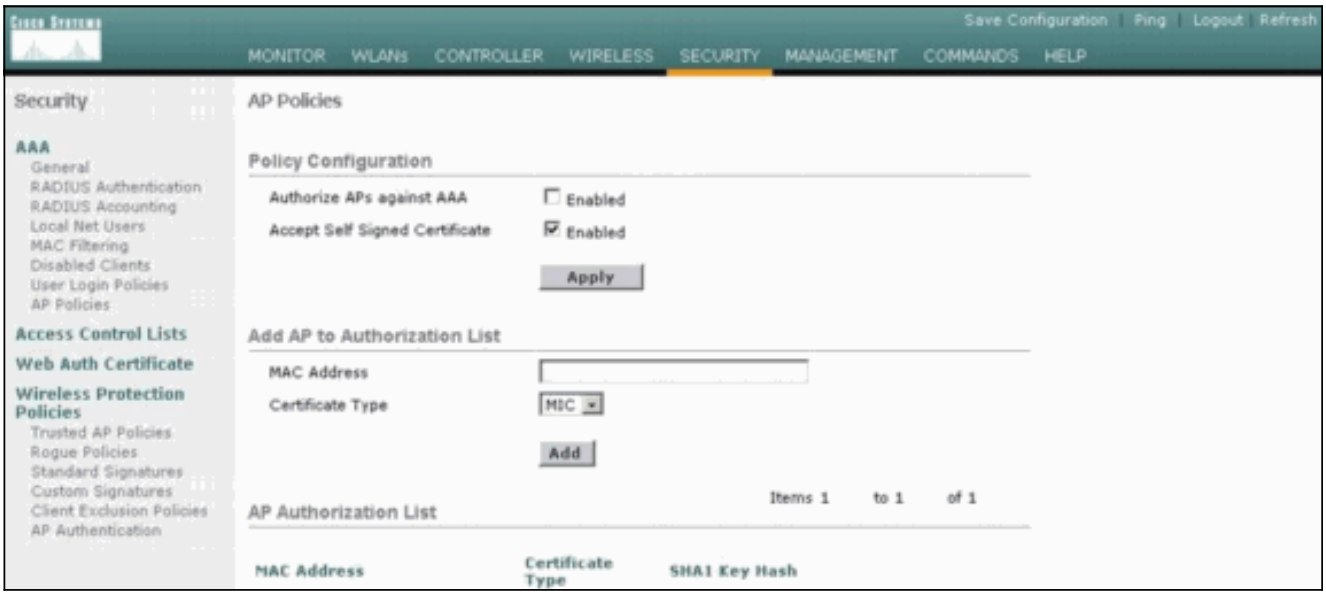
이 섹션에는 이 문서에서 설명하는 기능을 구성하기 위한 정보가 표시됩니다.

GUI 컨피그레이션

GUI에서 다음 단계를 완료합니다.

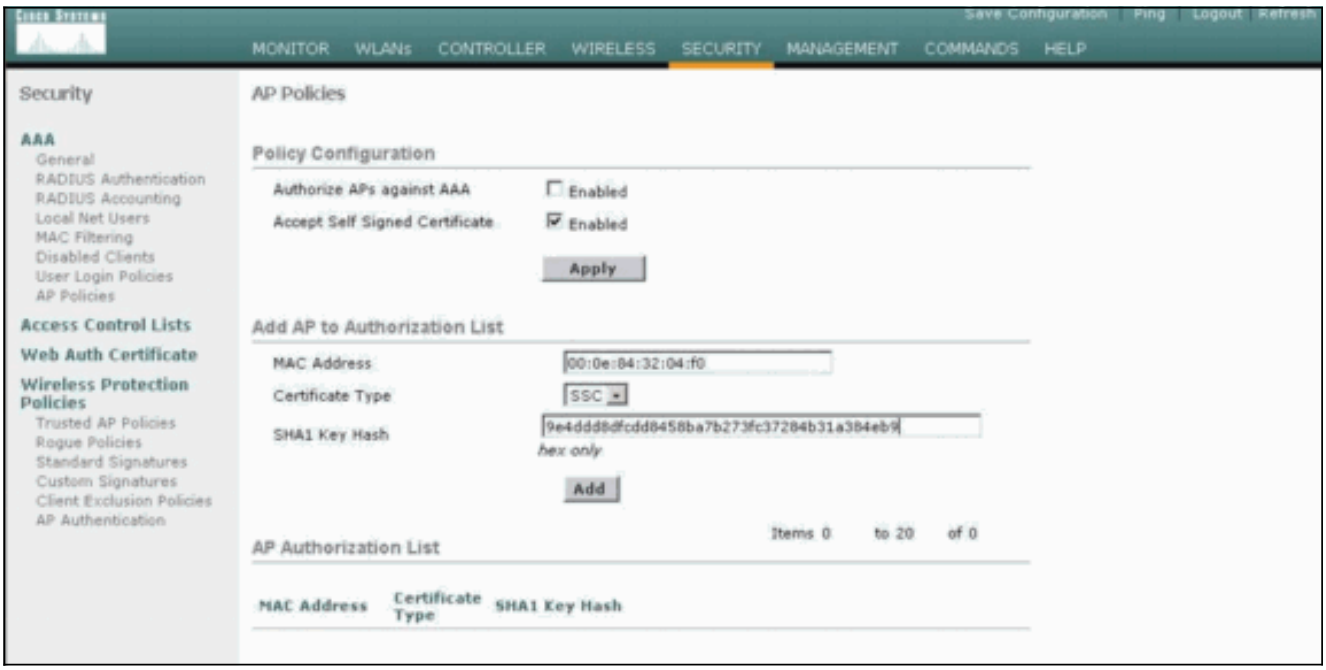
1. Security(**보안) > AP Policies(AP 정책)를** 선택하고 Accept Self Signed Certificate(자체 서명 인증서 수락) 옆의 Enabled(활성화됨)를 클릭합니다

.



2. Certificate Type 드롭다운 메뉴에서 SSC를 선택합니다

.



3. AP의 MAC 주소와 해시 키를 입력하고 Add(추가)를 **클릭합니다**.

CLI 컨피그레이션

CLI에서 다음 단계를 완료합니다.

1. WLC에서 Accept Self Signed Certificate를 활성화합니다.이 명령은 **config auth-list ap-policy ssc enable입니다**.
```
(Cisco Controller) >config auth-list ap-policy ssc enable
```

2. 권한 부여 목록에 AP MAC 주소 및 해시 키를 추가합니다.이 명령은 **config auth-list add ssc *AP_MAC AP_key입니다***.
```
(Cisco Controller) >config auth-list add ssc 00:0e:84:32:04:f0
9e4ddd8dfcdd8458ba7b273fc37284b31a384eb9
!--- This command should be on one line.
```

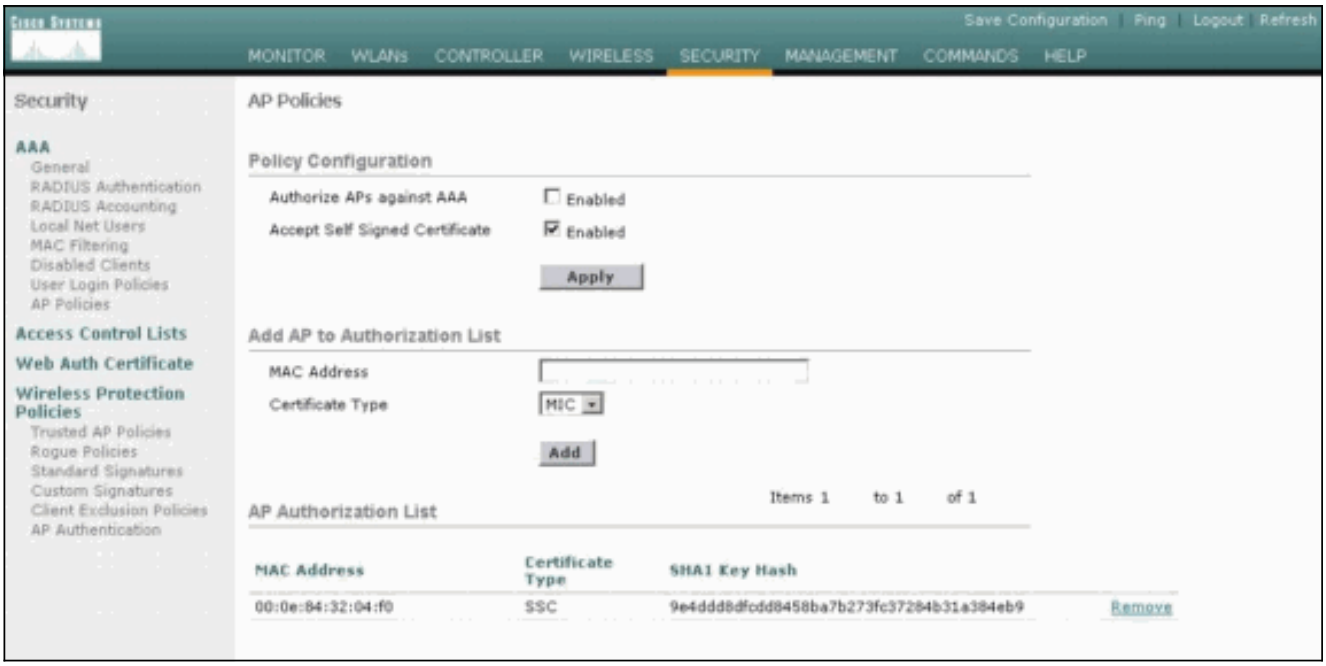
다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

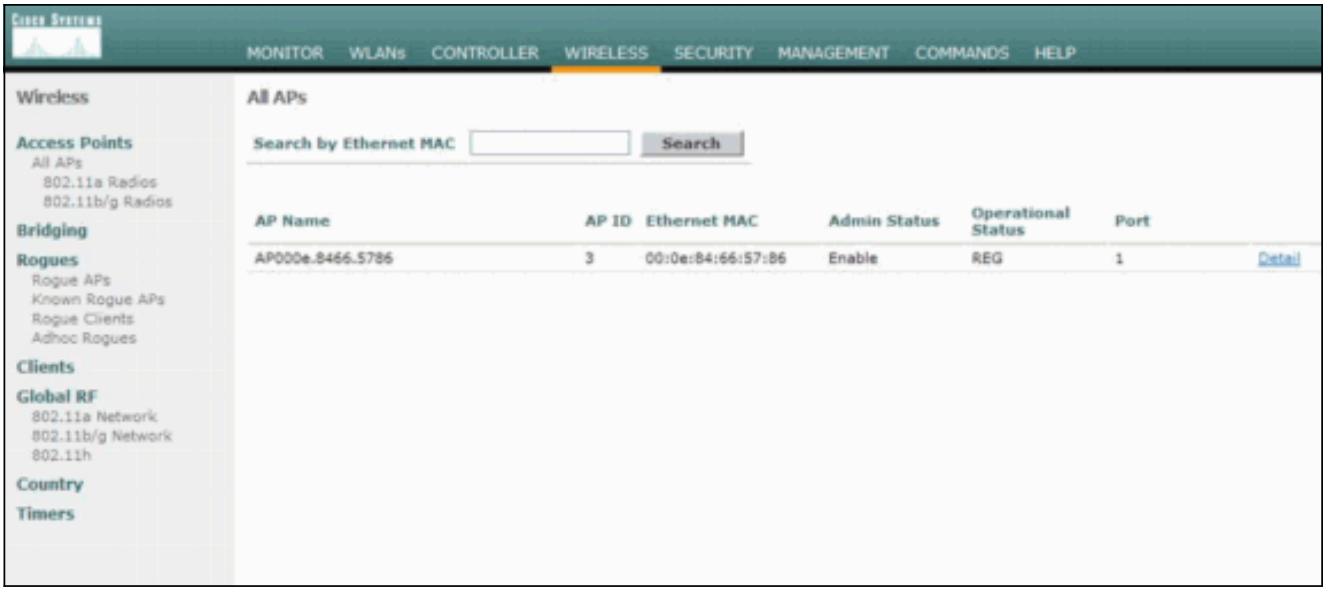
GUI 확인

다음 단계를 완료하십시오.

1. AP Policies(AP 정책) 창에서 AP MAC 주소 및 SHA1 Key Hash가 AP Authorization List(AP 권한 부여 목록) 영역에 나타나는지 확인합니다
.



2. All APs(모든 AP) 창에서 모든 AP가 WLC에 등록되었는지 확인합니다
.



CLI 확인

Output Interpreter 도구(등록된 고객만 해당)(OIT)는 특정 **show** 명령을 지원합니다.OIT를 사용하여 **show** 명령 출력의 분석을 봅니다.

- **show auth-list** - AP 권한 부여 목록을 표시합니다.
- **show ap summary** - 연결된 모든 AP의 요약을 표시합니다.

문제 해결

현재 이 컨피그레이션에 사용할 수 있는 특정 문제 해결 정보가 없습니다.

관련 정보

- WLC(Wireless LAN Controller) 문제 해결 FAQ
- Cisco Wireless LAN Controller 컨피그레이션 가이드, 릴리스 3.2
- 무선 LAN 컨트롤러 및 경량 액세스 포인트 기본 구성 예
- 기술 지원 및 문서 – Cisco Systems