Zelfgetekende certificaathandleiding voor de controller voor LWAPP-geconverteerde AP's

Inhoud

Inleiding

Dit document verklaart de methoden die u kunt gebruiken om zelf ondertekende certificaten (SSC's) aan een Cisco Wireless LAN (WLAN) controller (WLC) toe te voegen.

Het SSC van een toegangspunt (AP) dient te bestaan op alle WLC's in het netwerk waaraan AP toestemming heeft om te registreren. In het algemeen dient de SSC op alle WLC's in dezelfde mobiliteitsgroep van toepassing te zijn. Wanneer toevoeging van de SSC aan de WLC niet via de upgrade plaatsvindt, moet u de SSC handmatig aan de WLC toevoegen met behulp van de procedure in dit document. U heeft deze procedure ook nodig wanneer een AP wordt verplaatst naar een ander netwerk of wanneer extra WLCs aan het bestaande netwerk worden toegevoegd.

U kunt dit probleem herkennen wanneer een lichtgewicht AP Protocol (LWAPP)-geconverteerd AP niet aan WLC associeert. Wanneer u een probleem met betrekking tot de associatie oplossen, ziet u deze uitgangen bij het uitgeven van deze debugs:

- Wanneer u de **debug pm** geeft**, schakelt u** opdracht in:

```
(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.
```

- Wanneer u de **debug lwapp gebeurtenissen** geeft, **kunt u** opdracht geven:

```
(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
```

Voorwaarden

Vereisten

Zorg ervoor dat u aan deze vereisten voldoet voordat u deze configuratie probeert:

- De WLC bevat niet de SSC die het opgegenereerde upgradehulpprogramma bevat.
- De AP's bevatten een SSC.
- Telnet is geactiveerd op de WLC en de AP.
- De minimale versie van pre-LWAPP Cisco IOS® Software code is op de AP die om wordt bijgewerkt.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco WLC van 2006 die firmware 3.2.16.21 zonder SSC geïnstalleerd

- Cisco Aironet 1230 Series AP met een CSC

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg de Cisco Technical Tips Convention voor meer informatie over documentconventies.

Achtergrondinformatie

In de Cisco Gecentraliseerde WLAN-architectuur werken AP's in lichtgewicht modus. APs associeert aan een WLC van Cisco met gebruik van LWAPP. LWAPP is een IETF-ontwerpprotocol (Internet Engineering Task Force) dat het controlebericht definieert voor installatie en routeverificatie en doorlooptijd-bewerkingen. LWAPP definieert ook het tunneling-mechanisme voor gegevensverkeer.

Een lichtgewicht AP (LAP) ontdekt een WLC met gebruik van de ontdekkingsmechanismen van het LWAPP. De LAP stuurt de WLC vervolgens een LWAPP-aanvraag. De WLC stuurt de LAP en de LWAPP doen mee met een reactie waardoor de LAP zich bij de WLC kan aansluiten. Wanneer de LAP is aangesloten op de WLC, downloads de WLC-software als de herzieningen op de LAP en de WLC niet overeenkomen. Vervolgens is de LAP volledig onder controle van de WLC.

LWAPP waarborgt de communicatie tussen het AP en de WLC door middel van een veilige sleutelverdeling. Voor de beveiligde belangrijke distributie zijn al bevoorraden X.509 digitale certificaten nodig op zowel de LAP als de WLC. In de fabriek geïnstalleerde certificaten worden gerefereerd aan de term "MIC", wat een acroniem is voor een industrieel geïnstalleerd certificaat. Aironet APs die verscheept werden vóór 18 juli 2005, hebben geen MICs. Deze AP's creëren dus een SSC wanneer ze worden geconverteerd om in lichtgewicht modus te werken. Controllers zijn geprogrammeerd om SSC's te aanvaarden voor de authenticatie van specifieke AP's.

Dit is het upgradeproces:

1. De gebruiker voert een upgrade-hulpprogramma uit waarmee een invoerbestand met een lijst van AP's en hun IP-adressen wordt geaccepteerd, bovenop hun inlogreferenties.
2. Het nutsbedrijf voert Telnet-sessies met AP's in en stuurt een reeks Cisco IOS-softwarecoopdrachten in het invoerbestand om AP voor de upgrade voor te bereiden. Deze opdrachten bevatten de opdrachten om de SSC's te maken. Het hulpprogramma stelt ook een Telnet-sessie met de WLC op om het apparaat te programmeren om toestemming te geven voor specifieke SSC AP's.
3. Het hulpprogramma laadt vervolgens Cisco IOS-softwarerelease 12.3(7)JX op de AP zodat AP zich bij de WLC kan aansluiten.
4. Nadat AP zich bij de WLC aansluit, installeert AP een volledige Cisco IOS softwareversie van de WLC. Het upgradehulpprogramma genereert een uitvoerbestand dat de lijst van AP's en corresponderende SSC-hoofdwaswaarden bevat die in de beheersoftware van het Wireless Control System (WCS) kunnen worden geïmporteerd.
5. De WCS kan deze informatie dan naar andere WLC's op het netwerk sturen.

Nadat een AP zich bij een WLC aansluit, kunt u AP aan om het even welke WLC op uw netwerk

indien nodig opnieuw toewijzen.

De SHA1-toets lokaliseren

Als de computer die de AP-conversie heeft uitgevoerd beschikbaar is, kunt u de Secure Hash Algorithm 1 (SHA1) Key Hash van het .csv-bestand verkrijgen dat in de map Cisco Upgrade Tool is. Als het .csv-bestand niet beschikbaar is, kunt u een **debug**-opdracht in het WLC geven om de SHA1-Key Hash terug te halen.

Voer de volgende stappen uit:

1. Zet de AP aan en sluit het aan op het netwerk.
2. Schakel het debuggen op de WLC opdrachtregel interface (CLI) in.De opdracht is **debug pm, pki-instelling**.

```
(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
```

Voeg SSC aan WLC toe

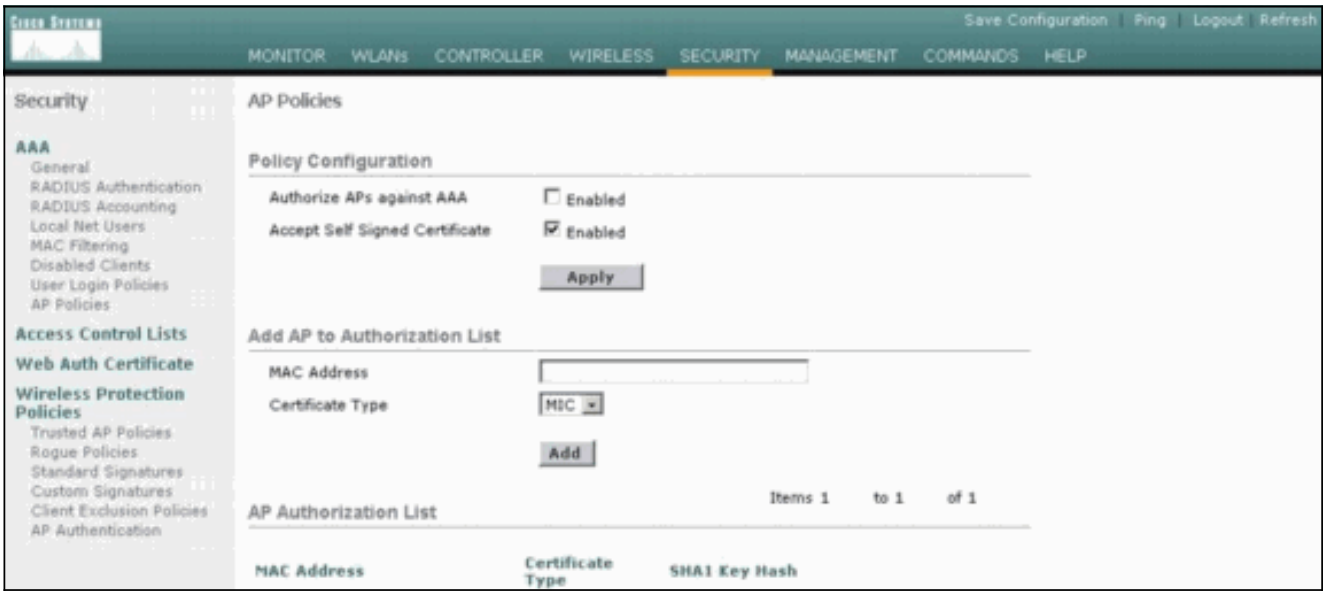
Taak

Deze sectie bevat informatie over het configureren van de functies die in dit document worden beschreven.

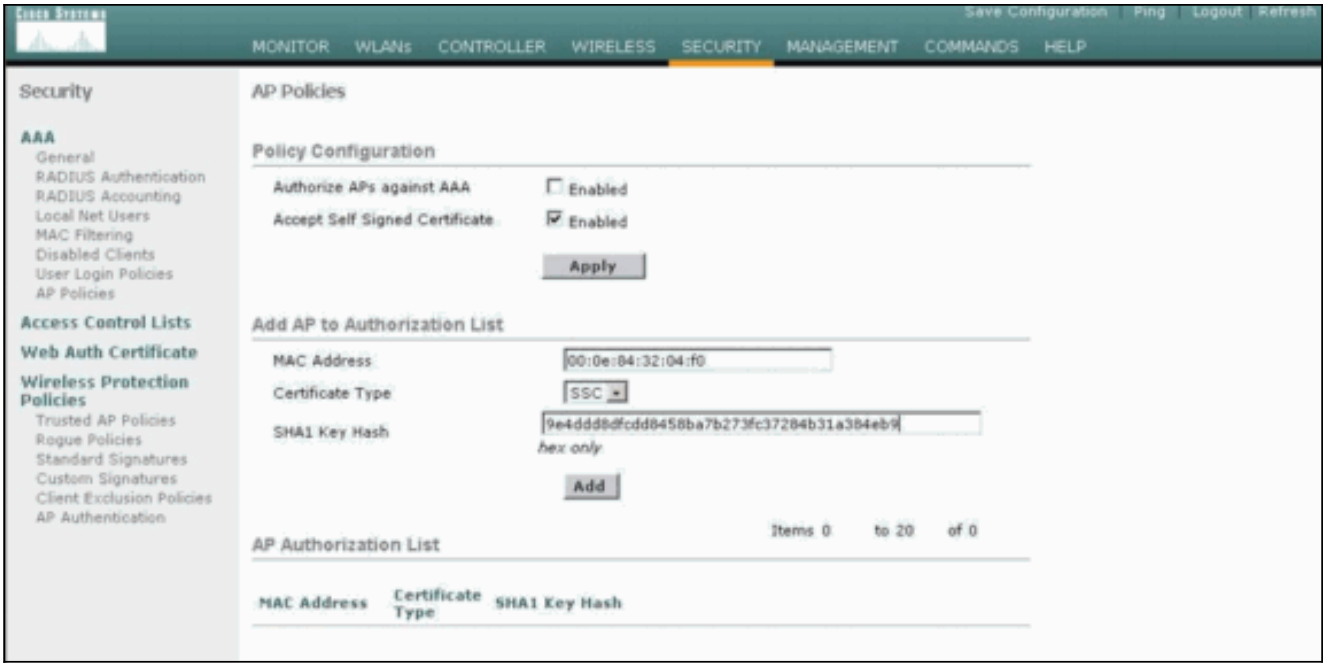
GUI-configuratie

Volg deze stappen vanuit de GUI:

1. Kies **Beveiliging > AP-beleid** en klik op **Ingeschakeld** naast Aanvaardbaar certificaat.



2. Selecteer **SSC** in het vervolgkeuzemenu certificaattype.



3. Voer het MAC-adres van het AP en de hashtoets in en klik op **Add**.

CLI-configuratie

Volg deze stappen van de CLI:

1. Accepteer een zelfondertekend certificaat op de WLC.Het commando is **fungeren als sc**.
   ```
   (Cisco Controller) >config auth-list ap-policy ssc enable
   ```

2. Voeg het AP MAC adres en de haassleutel aan de vergunningslijst toe.Het commando is **configuratie auth-list voegt ssc *AP_MAC AP_key toe*.**
   ```
   (Cisco Controller) >config auth-list add ssc 00:0e:84:32:04:f0
   9e4ddd8dfcdd8458ba7b273fc37284b31a384eb9
   !--- This command should be on one line.
   ```

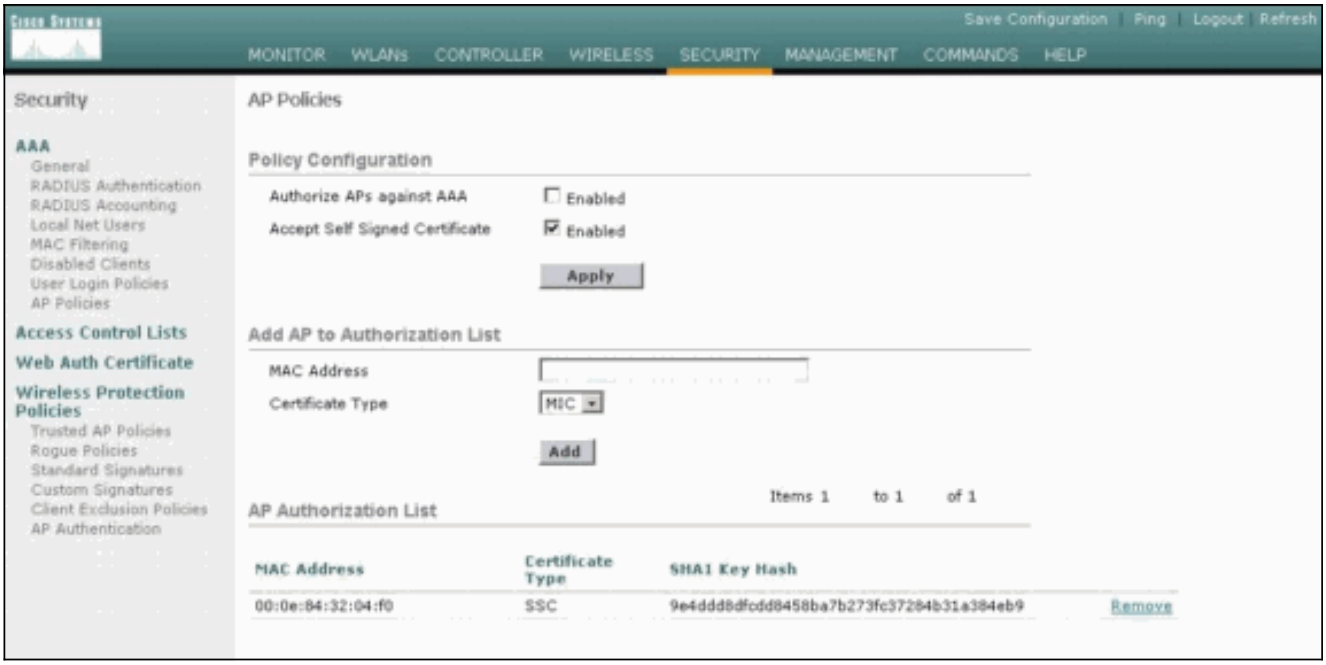
Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

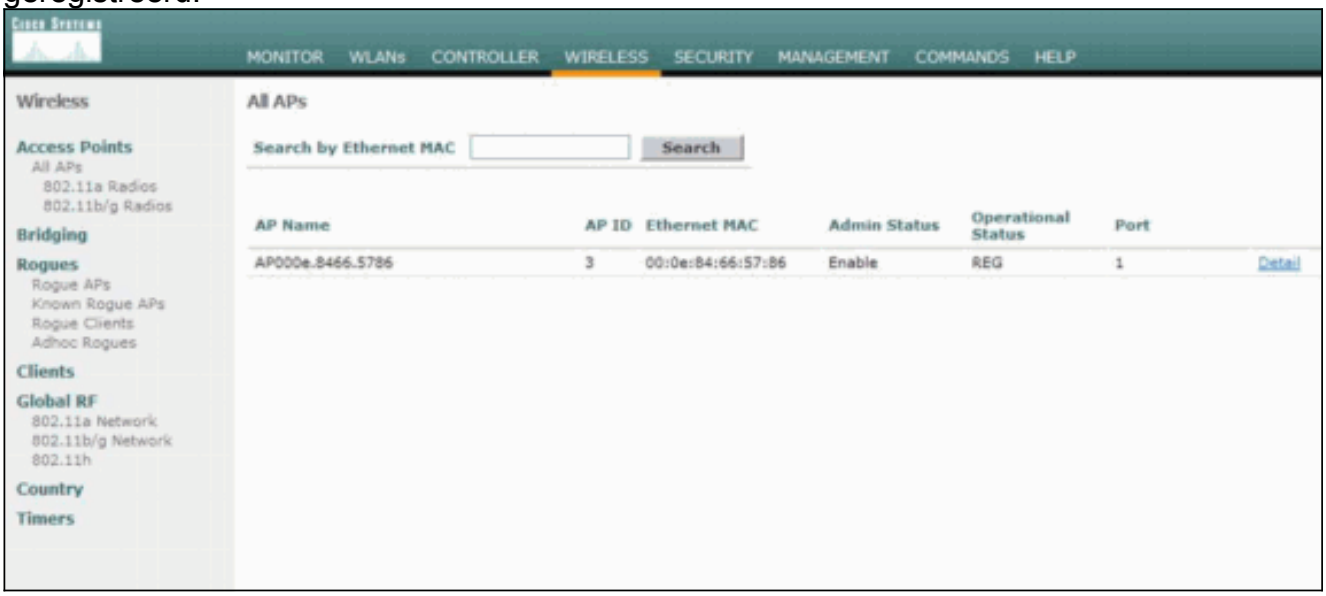
GUI-verificatie

Voer de volgende stappen uit:

1. Controleer in het venster AP Policy of het AP MAC-adres en de SHA1-toets worden weergegeven in het gebied AP Authorization
   List.



2. Controleer in het venster Alle AP's of alle AP's bij de WLC zijn geregistreerd.



CLI-verificatie

Het Uitvoer Tolk (uitsluitend geregistreerde klanten) (OIT) ondersteunt bepaalde **show** opdrachten. Gebruik de OIT om een analyse van **tonen** opdrachtoutput te bekijken.

- **Toon de auth-list**-Toont de AP autorisatie lijst.
- **toon samenvatting**—Hier wordt een samenvatting van alle aangesloten AP's weergegeven.

Problemen oplossen

Er is momenteel geen specifieke troubleshooting-informatie beschikbaar voor deze configuratie.

Gerelateerde informatie

- WLC (Wireless LAN Controller) probleemoplossing in FAQ

- Configuratie-gids voor Cisco draadloze LAN-controllers, release 3.2
- Configuratievoorbeeld voor draadloos LAN-controller en lichtgewicht access point
- Technische ondersteuning en documentatie – Cisco Systems