Manuelles Hinzufügen von selbstsignierten Zertifikaten zum Controller für LWAPP-konvertierte APs

Inhalt

Einführung

In diesem Dokument werden die Methoden erläutert, mit denen Sie einem Cisco Wireless LAN (WLAN) Controller (WLC) manuell selbstsignierte Zertifikate (SSCs) hinzufügen können.

Der SSC eines Access Points (AP) sollte auf allen WLCs im Netzwerk vorhanden sein, für die der Access Point die Berechtigung zur Registrierung besitzt. Wenden Sie den SSC in der Regel auf alle WLCs in derselben Mobilitätsgruppe an. Wenn das Hinzufügen des SSC zum WLC nicht über das Upgrade-Dienstprogramm erfolgt, müssen Sie den SSC manuell zum WLC hinzufügen, wobei die in diesem Dokument beschriebenen Verfahren verwendet werden. Sie benötigen dieses Verfahren auch, wenn ein Access Point in ein anderes Netzwerk verschoben wird oder wenn dem vorhandenen Netzwerk zusätzliche WLCs hinzugefügt werden.

Sie können dieses Problem erkennen, wenn ein aus LWAPP (Lightweight AP Protocol) umgewandelter AP nicht mit dem WLC verknüpft ist. Wenn Sie das Zuordnungsproblem beheben, sehen Sie diese Ausgaben, wenn Sie diese Debuggen ausführen:

- Wenn Sie den Befehl **debug pm pki enable** ausgeben, sehen Sie:

```
(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.
```

- Wenn Sie den Befehl **debug lwapp events enable** ausgeben, sehen Sie:

```
(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
```

Voraussetzungen

Anforderungen

Stellen Sie sicher, dass Sie diese Anforderungen erfüllen, bevor Sie versuchen, diese Konfiguration durchzuführen:

- Der WLC enthält nicht den SSC, den das Aktualisierungs-Dienstprogramm erstellt hat.
- Die APs enthalten ein SSC.
- Telnet ist auf dem WLC und dem AP aktiviert.
- Die Mindestversion des Cisco IOS® Software-Codes vor der LWAPP-Implementierung befindet sich auf dem zu aktualisierenden Access Point.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco 2006 WLC, der Firmware 3.2.116.21 ohne installierte SSC ausführt
- Cisco Aironet AP der Serie 1230 mit SSC

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Hintergrundinformationen

In der zentralen WLAN-Architektur von Cisco werden APs im Lightweight-Modus betrieben. Die APs werden mit einem Cisco WLC verbunden, wenn der LWAPP verwendet wird. LWAPP ist ein IETF-Entwurfsprotokoll (Internet Engineering Task Force), das das Steuerungs-Messaging für die Einrichtung, die Pfadauthentifizierung und Laufzeitoperationen definiert. LWAPP definiert außerdem den Tunneling-Mechanismus für Datenverkehr.

Ein Lightweight AP (LAP) erkennt einen WLC mithilfe von LWAPP-Erkennungsmechanismen. Die LAP sendet dann die WLC- und LWAPP-Join-Anforderung. Der WLC sendet die LAP- und LWAPP-Join-Antwort, sodass die LAP dem WLC beitreten kann. Wenn die LAP mit dem WLC verbunden ist, lädt die LAP die WLC-Software herunter, wenn die Revisionen auf der LAP und dem WLC nicht übereinstimmen. Anschließend steht die LAP vollständig unter der Kontrolle des WLC.

LWAPP sichert die Steuerungskommunikation zwischen dem Access Point und dem WLC über eine sichere Schlüsselverteilung. Für die sichere Schlüsselverteilung sind auf der LAP und dem WLC bereits bereitgestellte digitale X.509-Zertifikate erforderlich. Auf werkseitig installierte Zertifikate wird der Begriff "MIC" verwiesen, ein Akronym für das Zertifikat, das in der Fertigung installiert wurde. Aironet APs, die vor dem 18. Juli 2005 ausgeliefert wurden, verfügen nicht über MICs. Diese APs erstellen also ein SSC, wenn sie konvertiert werden, um im Lightweight-Modus zu arbeiten. Controller sind so programmiert, dass sie SSCs für die Authentifizierung bestimmter APs akzeptieren.

Dies ist der Upgrade-Prozess:

1. Der Benutzer führt ein Upgrade-Dienstprogramm aus, das zusätzlich zu seinen Anmeldeinformationen eine Eingabedatei mit einer Liste von APs und ihren IP-Adressen akzeptiert.
2. Das Dienstprogramm richtet Telnet-Sitzungen mit den APs ein und sendet eine Reihe von Cisco IOS Software-Befehlen in der Eingabedatei, um den Access Point auf das Upgrade vorzubereiten. Diese Befehle enthalten die Befehle zum Erstellen der SSCs. Außerdem richtet das Dienstprogramm eine Telnet-Sitzung mit dem WLC ein, um das Gerät so zu programmieren, dass die Autorisierung bestimmter SSC-APs möglich ist.
3. Das Dienstprogramm lädt dann die Cisco IOS Software, Version 12.3(7)JX, auf den AP,

damit der Access Point dem WLC beitreten kann.

4. Wenn der AP dem WLC beitritt, lädt der AP eine vollständige Cisco IOS Software-Version vom WLC herunter. Das Aktualisierungsprogramm generiert eine Ausgabedatei, die eine Liste der APs und die zugehörigen SSC-Schlüssel-Hash-Werte enthält, die in die Verwaltungssoftware des Wireless Control System (WCS) importiert werden können.
5. Das WCS kann diese Informationen dann an andere WLCs im Netzwerk senden.

Wenn ein Access Point einem WLC beitritt, können Sie den Access Point einem beliebigen WLC im Netzwerk zuweisen, falls erforderlich.

Suchen Sie den SHA1-Schlüssel-Hash.

Wenn der Computer, der die AP-Konvertierung durchgeführt hat, verfügbar ist, können Sie den Schlüssel-Hash-Algorithmus 1 (SHA1) aus der CSV-Datei im Cisco Upgrade Tool-Verzeichnis abrufen. Wenn die CSV-Datei nicht verfügbar ist, können Sie einen **Debug-**Befehl auf dem WLC ausführen, um den SHA1-Schlüssel-Hash abzurufen.

Gehen Sie wie folgt vor:

1. Schalten Sie den Access Point ein, und schließen Sie ihn an das Netzwerk an.
2. Aktivieren Sie das Debuggen auf der WLC-Befehlszeilenschnittstelle (CLI).Der Befehl lautet **debug pm pki enable**.

```
(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
```

Hinzufügen des SSC zum WLC

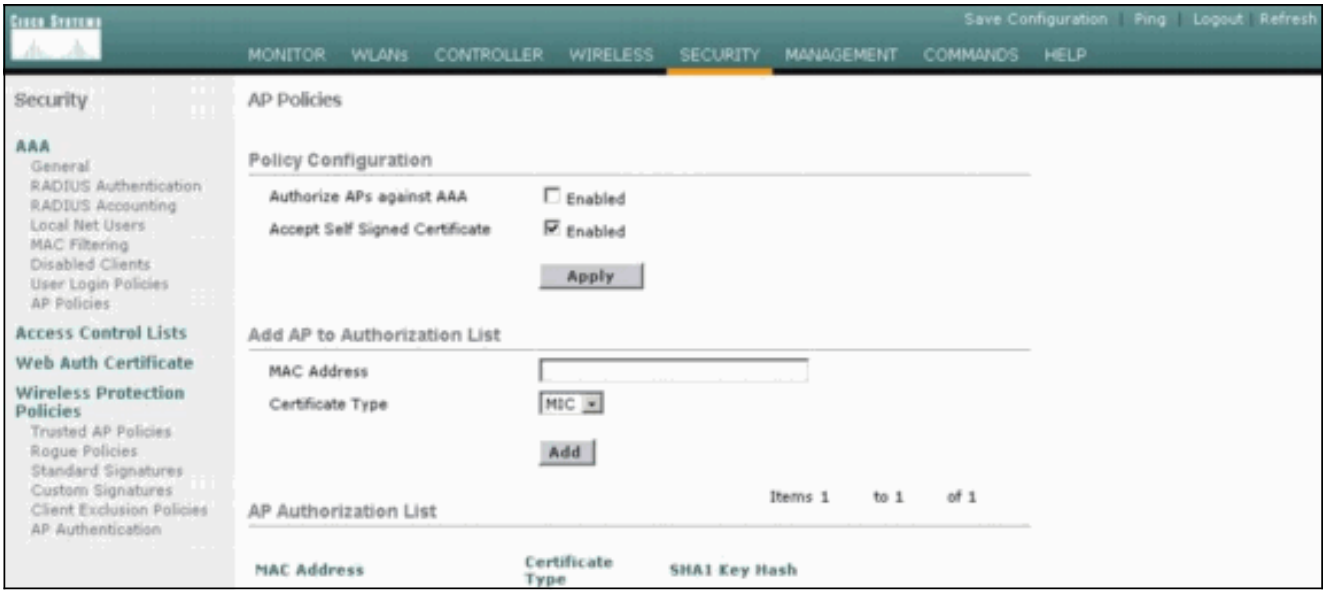
Aufgabe

In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

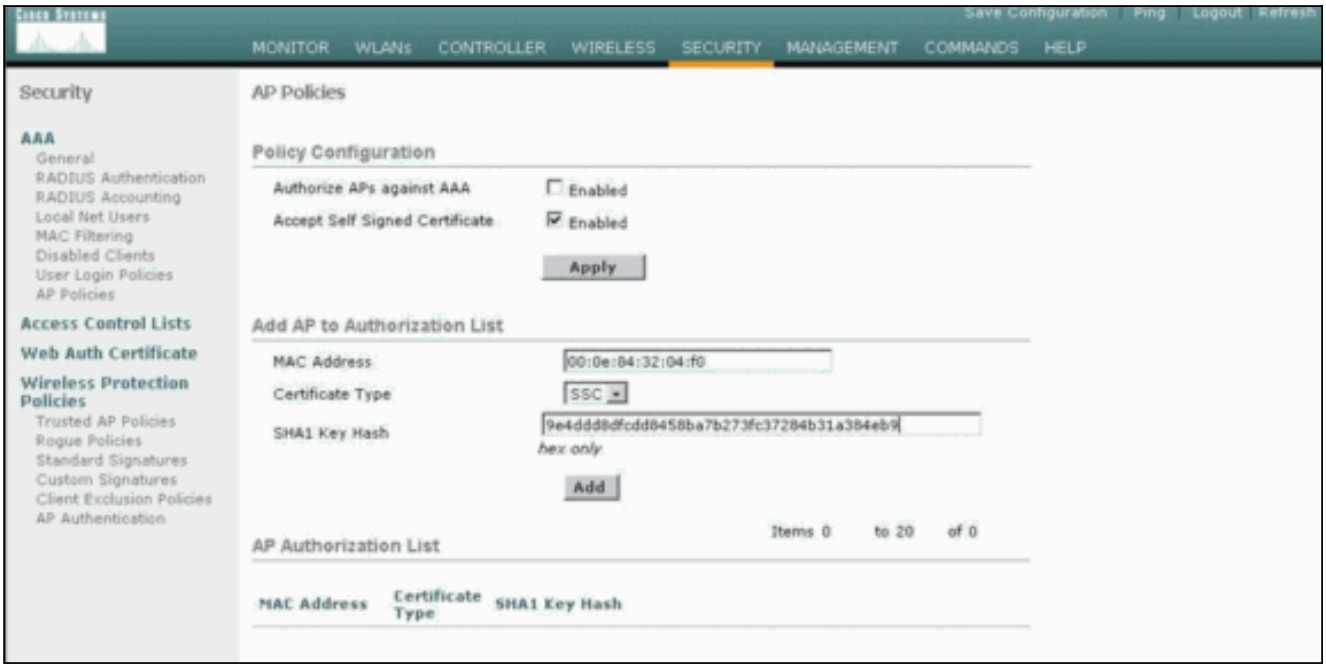
GUI-Konfiguration

Führen Sie die folgenden Schritte über die Benutzeroberfläche aus:

1. Wählen Sie **Security > AP Policies (Sicherheit > AP-Richtlinien) aus,** und klicken Sie neben Accept Self Signed Certificate (Selbstsigniertes Zertifikat akzeptieren) auf **Enabled (Aktiviert)**.



2. Wählen Sie **SSC** im Dropdown-Menü Zertifikatstyp aus.



3. Geben Sie die MAC-Adresse des Access Points und den Hash-Schlüssel ein, und klicken Sie auf **Hinzufügen**.

CLI-Konfiguration

Gehen Sie wie folgt von der CLI aus:

1. Aktivieren des selbstsignierten Zertifikats akzeptieren auf dem WLC.Der Befehl lautet **config auth-list ap-policy ssc enable**.
```
(Cisco Controller) >config auth-list ap-policy ssc enable
```

2. Fügen Sie die AP-MAC-Adresse und den Hash-Schlüssel zur Autorisierungsliste hinzu.Der Befehl lautet **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.
```

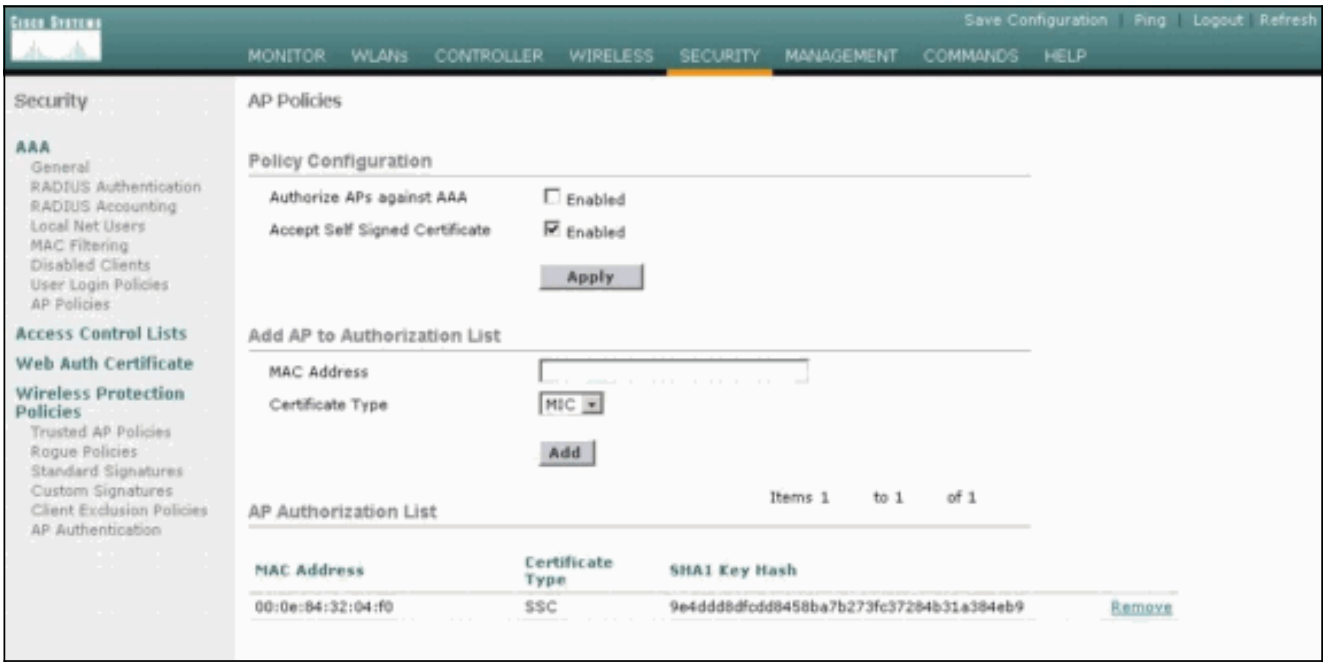
Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

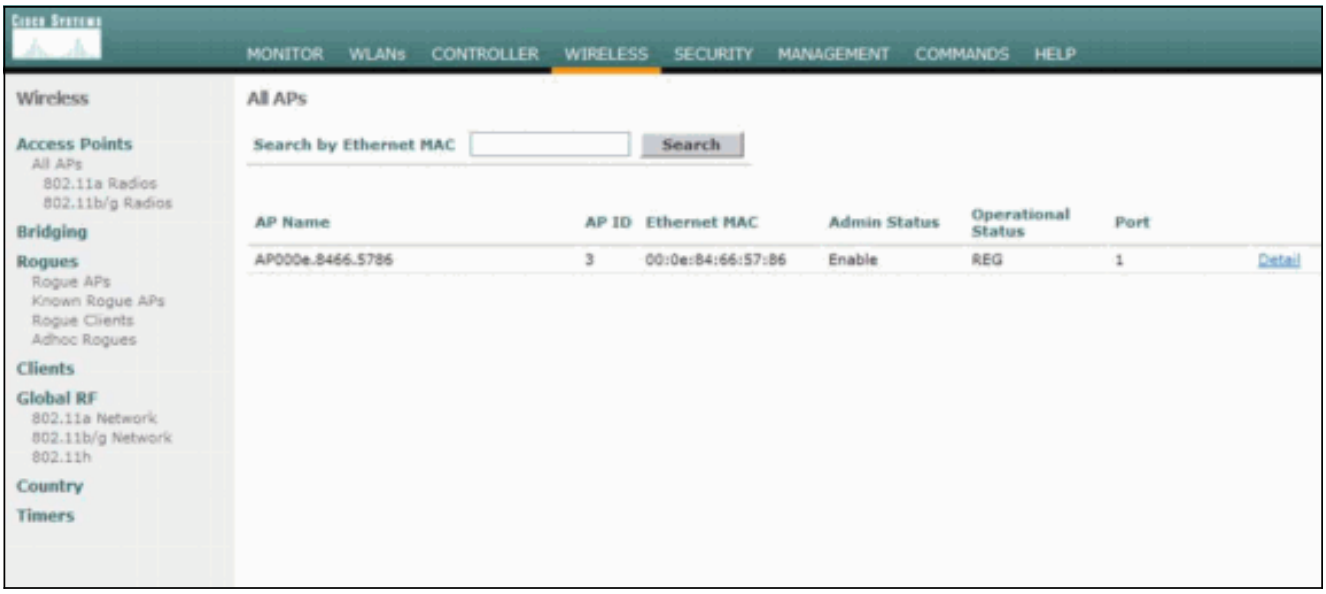
GUI-Verifizierung

Gehen Sie wie folgt vor:

1. Überprüfen Sie im Fenster AP Policies (AP-Richtlinien), ob die MAC-Adresse des Access Points und der SHA1-Schlüssel-Hash im Bereich AP Authorization List (AP-Autorisierungsliste) angezeigt
werden.



2. Überprüfen Sie im Fenster All APs (Alle APs), ob alle APs beim WLC registriert sind.



CLI-Verifizierung

Das Output Interpreter Tool (nur registrierte Kunden) (OIT) unterstützt bestimmte **show**-Befehle.

Verwenden Sie das OIT, um eine Analyse der **Ausgabe des** Befehls **show anzuzeigen**.

- **show auth-list**: Zeigt die AP-Autorisierungsliste an.
- **show ap summary**: Zeigt eine Zusammenfassung aller angeschlossenen APs an.

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

Zugehörige Informationen

- Häufig gestellte Fragen zur Fehlerbehebung für Wireless LAN Controller (WLC)
- Konfigurationsleitfaden für Cisco Wireless LAN Controller, Version 3.2
- Grundlegende Konfigurationsbeispiel für Wireless LAN Controller und Lightweight Access Point
- Technischer Support und Dokumentation - Cisco Systems