Ajout manuel de certificats auto-signés au contrôleur pour des points d'accès convertis selon le protocole LWAPP

Contenu

Introduction

Ce document explique les méthodes que vous pouvez utiliser pour ajouter manuellement des certificats auto-signés (SSC) à un contrôleur de réseau local sans fil (WLAN) Cisco (WLC).

Le SSC d'un point d'accès (AP) doit exister sur tous les WLC du réseau auquel le point d'accès a l'autorisation de s'enregistrer. En règle générale, appliquez le SSC à tous les WLC du même groupe de mobilité. Lorsque l'ajout du SSC au WLC ne se produit pas par le biais de l'utilitaire de mise à niveau, vous devez ajouter manuellement le SSC au WLC avec l'utilisation de la procédure dans ce document. Vous avez également besoin de cette procédure lorsqu'un point d'accès est déplacé vers un autre réseau ou lorsque des WLC supplémentaires sont ajoutés au réseau existant.

Vous pouvez reconnaître ce problème lorsqu'un AP converti en LWAPP (Lightweight AP Protocol) ne s'associe pas au WLC. Lorsque vous dépannez le problème d'association, vous voyez ces sorties lorsque vous émettez ces débogages :

- Lorsque vous émettez la commande **debug pm pki enable**, vous voyez :

```
(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.
```

- Lorsque vous émettez la commande **debug lwapp events enable**, vous voyez :

```
(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
```

Conditions préalables

Conditions requises

Assurez-vous que vous répondez à ces exigences avant d'essayer cette configuration :

- Le WLC ne contient pas le SSC généré par l'utilitaire de mise à niveau.
- Les points d'accès contiennent un SSC.
- Telnet est activé sur le WLC et l'AP.
- La version minimale du code logiciel Cisco IOS® pré-LWAPP est sur l'AP à mettre à niveau.

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de

logiciel suivantes :

- WLC Cisco 2006 qui exécute le microprogramme 3.2.116.21 sans SSC installé
- Point d'accès de la gamme Cisco Aironet 1230 avec SSC

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Informations générales

Dans l'architecture WLAN centralisée de Cisco, les points d'accès fonctionnent en mode léger. Les points d'accès s'associent à un WLC Cisco avec l'utilisation du LWAPP. LWAPP est un projet de protocole de l'Internet Engineering Task Force (IETF) qui définit la messagerie de contrôle pour la configuration et l'authentification des commandes exécutées et des parcours. LWAPP définit également le mécanisme de transmission tunnel pour le trafic de données.

Un point d'accès léger (LAP) découvre un WLC avec l'utilisation de mécanismes de détection LWAPP. Le LAP envoie ensuite au WLC une demande de jointure LWAPP. Le WLC envoie au LAP une réponse de jointure LWAPP qui permet au LAP de rejoindre le WLC. Lorsque le LAP est joint au WLC, le LAP télécharge le logiciel du WLC si les révisions sur le LAP et le WLC ne correspondent pas. Par la suite, le LAP est complètement sous le contrôle du WLC.

LWAPP sécurise la communication de contrôle entre l'AP et le WLC au moyen d'une distribution de clé sécurisée. La distribution de clé sécurisée nécessite des certificats numériques X.509 déjà provisionnés sur le LAP et le WLC. Des certificats d'origine sont référencés avec le terme « MIC » (certificat installé en usine). Les points d'accès Aironet expédiés avant le 18 juillet 2005 ne possèdent pas de MIC. Ces points d'accès créent un SSC lorsqu'ils sont convertis pour fonctionner en mode léger. Les contrôleurs sont programmés pour accepter les SSC pour l'authentification d'AP spécifiques.

Voici le processus de mise à niveau :

1. L'utilisateur exécute un utilitaire de mise à niveau qui accepte un fichier d'entrée avec une liste de points d'accès et leurs adresses IP, en plus de leurs identifiants de connexion.
2. L'utilitaire établit des sessions Telnet avec les points d'accès et envoie une série de commandes du logiciel Cisco IOS dans le fichier d'entrée afin de préparer l'AP pour la mise à niveau. Ces commandes incluent les commandes permettant de créer les SSC. En outre, l'utilitaire établit une session Telnet avec le WLC afin de programmer le périphérique pour permettre l'autorisation de points d'accès SSC spécifiques.
3. L'utilitaire charge ensuite le logiciel Cisco IOS Version 12.3(7)JX sur l'AP afin que l'AP puisse rejoindre le WLC.
4. Une fois que le point d'accès a rejoint le WLC, le point d'accès télécharge une version complète du logiciel Cisco IOS à partir du WLC. L'utilitaire de mise à niveau génère un fichier de sortie qui inclut la liste des points d'accès et les valeurs de hachage de clé SSC correspondantes qui peuvent être importées dans le logiciel de gestion Wireless Control

System (WCS).

5. Le WCS peut ensuite envoyer ces informations à d'autres WLC sur le réseau.

Une fois qu'un point d'accès rejoint un WLC, vous pouvez réaffecter le point d'accès à n'importe quel WLC de votre réseau, si nécessaire.

Localiser le hachage de clé SHA1

Si l'ordinateur qui a effectué la conversion AP est disponible, vous pouvez obtenir le hachage de clé SHA1 (Secure Hash Algorithm 1) à partir du fichier .csv qui se trouve dans le répertoire Cisco Upgrade Tool. Si le fichier .csv n'est pas disponible, vous pouvez émettre une commande **debug** sur le WLC afin de récupérer le hachage de clé SHA1.

Procédez comme suit :

1. Activez le point d'accès et connectez-le au réseau.
2. Activez le débogage sur l'interface de ligne de commande (CLI) du WLC.La commande est **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
```

Ajouter le SSC au WLC

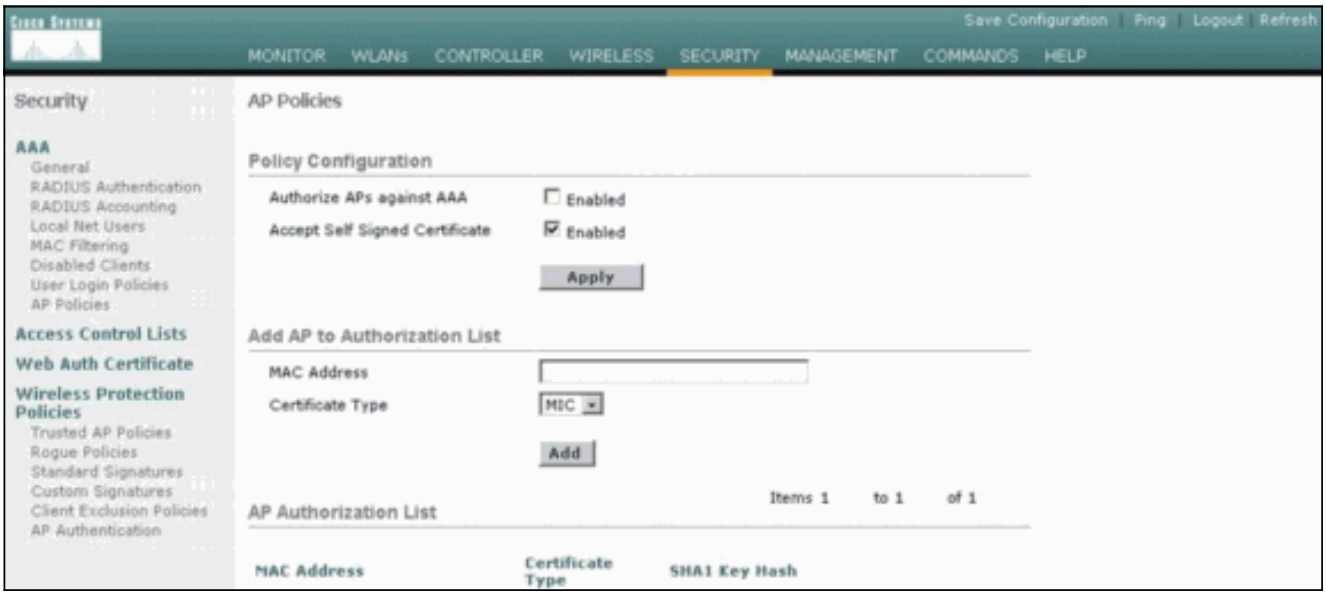
Tâche

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

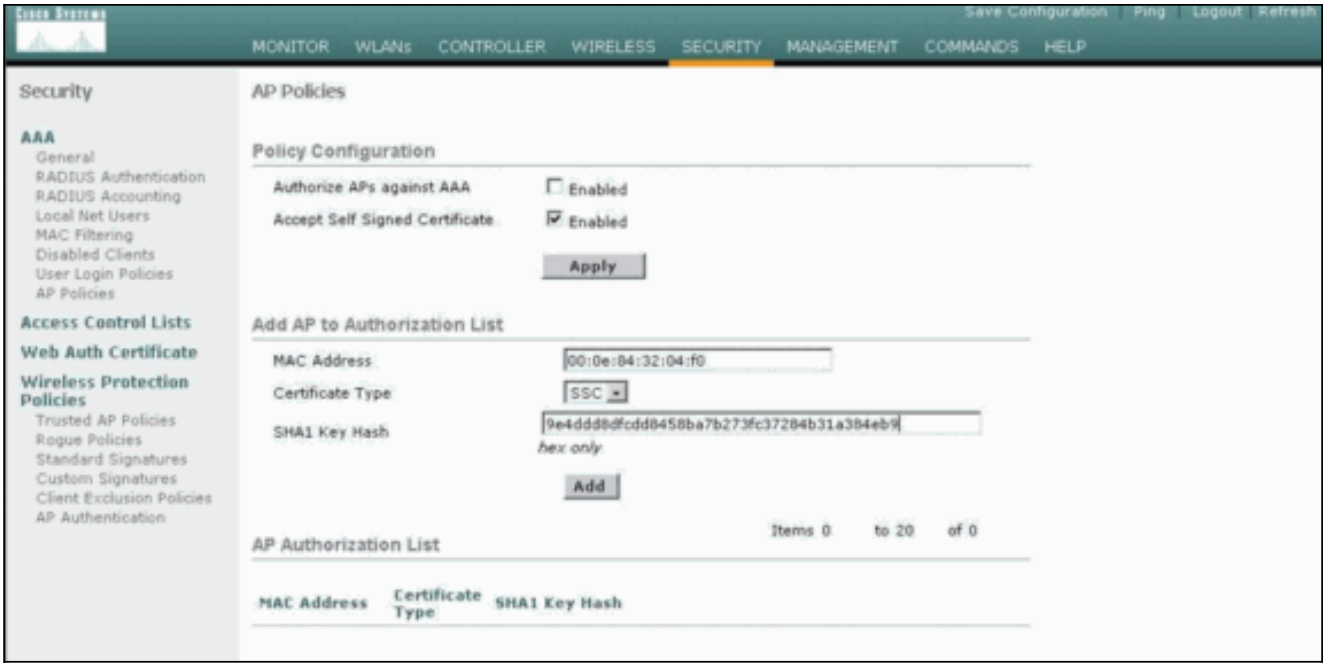
Configuration de la GUI

Effectuez ces étapes à partir de l'interface utilisateur graphique :

1. Choisissez **Security > AP Policies** et cliquez sur **Enabled** en regard de Accept Self Signed Certificate.



2. Sélectionnez **SSC** dans le menu déroulant Type de certificat.



3. Entrez l'adresse MAC du point d'accès et la clé de hachage, puis cliquez sur **Ajouter**.

Configuration CLI

Effectuez ces étapes à partir de l'interface de ligne de commande :

1. Activez Accepter le certificat auto-signé sur le WLC.La commande est **config auth-list ap-policy ssc enable**.
   ```
   (Cisco Controller) >config auth-list ap-policy ssc enable
   ```

2. Ajoutez l'adresse MAC de l'AP et la clé de hachage à la liste d'autorisation.La commande est **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.
   ```

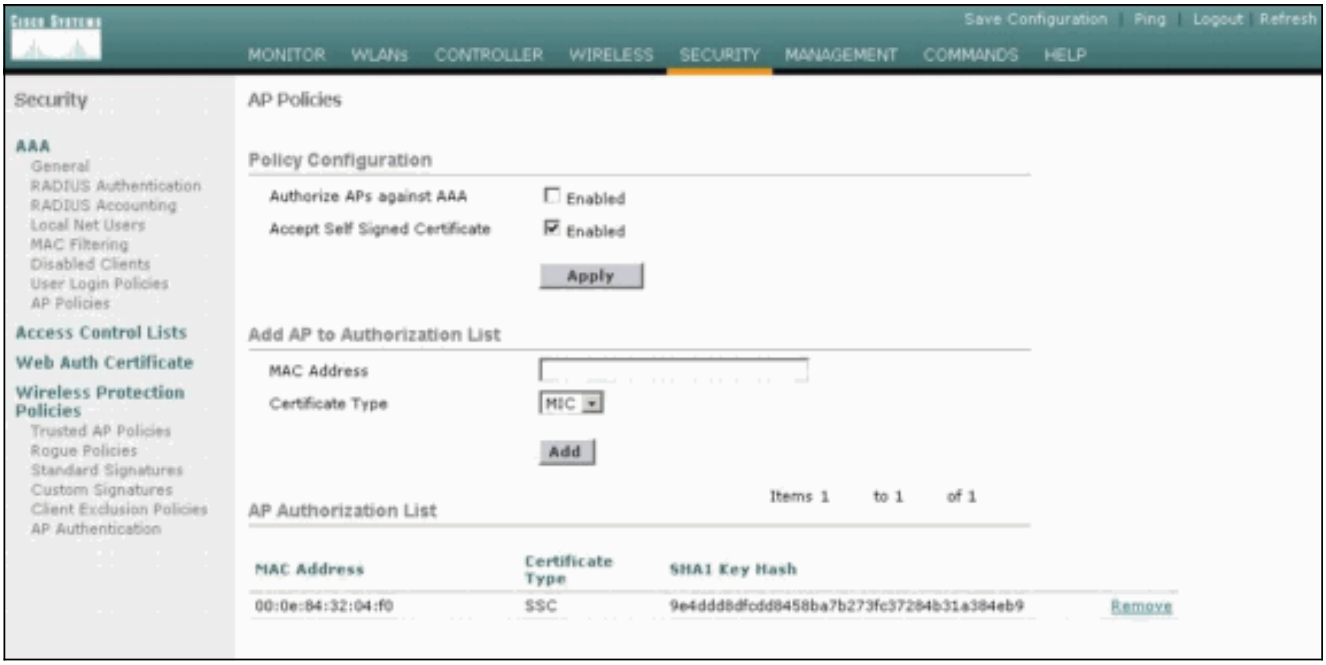
Vérification

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

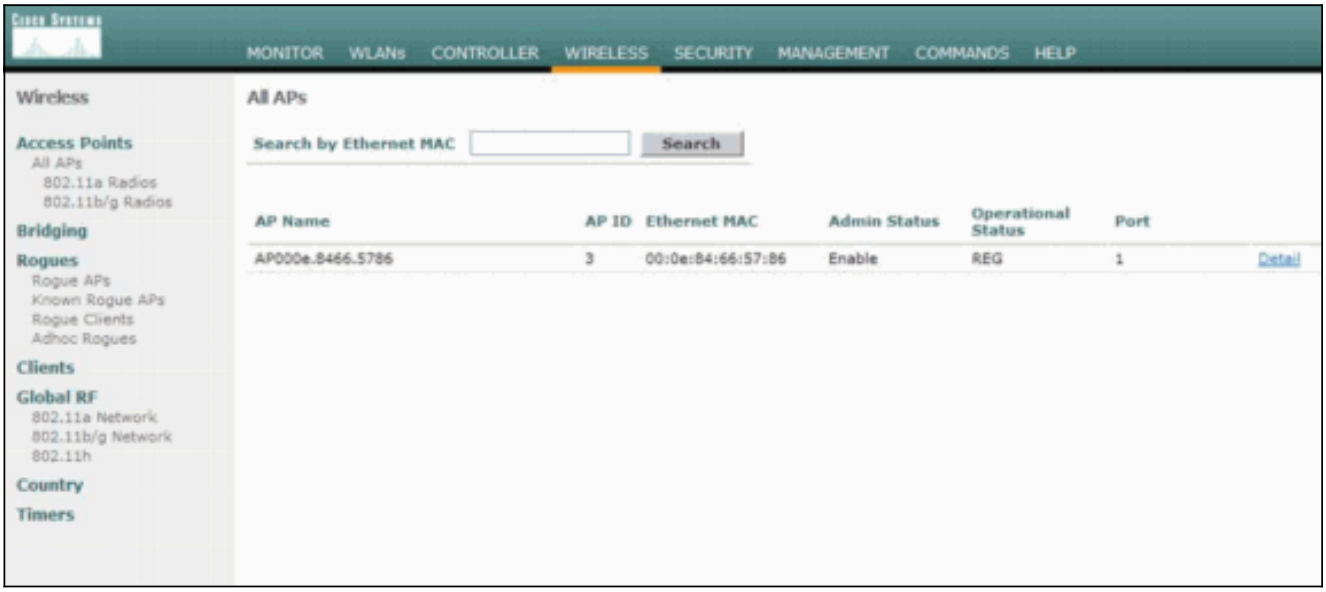
Vérification de l'interface utilisateur

Procédez comme suit :

1. Dans la fenêtre AP Policies, vérifiez que l'adresse MAC AP et le hachage de clé SHA1 apparaissent dans la zone AP Authorization
   List.



2. Dans la fenêtre Tous les AP, vérifiez que tous les AP sont enregistrés auprès du WLC.



Vérification CLI

L'Outil Interpréteur de sortie (clients enregistrés uniquement) (OIT) prend en charge certaines commandes show. Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show .**

- **show auth-list** - Affiche la liste d'autorisations de point d'accès.
- **show ap summary** : affiche un résumé de tous les AP connectés.

Dépannage

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Informations connexes

- Dépannage du contrôleur LAN sans fil (WLC) - FAQ

- Guide de configuration du contrôleur LAN sans fil Cisco, version 3.2
- Exemple de configuration de base d'un contrôleur LAN sans fil et d'un point d'accès léger
- Support et documentation techniques - Cisco Systems