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 employer afin d'ajouter manuellement les Certificats auto-signés (SSCs) à un contrôleur Sans fil du RÉSEAU LOCAL de Cisco (WLAN) (WLC).

SSC d'un Point d'accès (AP) devrait exister sur tout le WLCs dans le réseau auquel AP a l'autorisation de s'enregistrer. En règle générale, appliquez-vous SSC à tout le WLCs au même groupe de mobilité. Quand l'ajout de SSC au WLC ne se produit pas par l'utilitaire de mise à jour, vous devez manuellement ajouter SSC au WLC avec le recours à la procédure dans ce document. Vous avez besoin également de cette procédure quand AP est déplacé à un réseau différent ou quand WLCs supplémentaire sont ajoutés au réseau existant.

Vous pouvez identifier ce problème quand AP léger Protocol (LWAPP) - AP converti ne s'associe pas au WLC. Quand vous dépannez le problème d'association, vous voyez que ces sorties quand vous émettez ces derniers met au point :

- Quand vous émettez la commande d'**enable de PKI de debug pm**, 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.
```

- Quand 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 SSC que l'utilitaire de mise à jour a généré.
- Les aps contiennent SSC.
- Le telnet est activé sur le WLC et l'AP.
- La version minimum de code logiciel de Cisco IOS® de pre-LWAPP est sur AP à mettre à jour.

Composants utilisés

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

- Cisco 2006 WLC qui exécute le micrologiciel 3.2.116.21 sans SSC a installé
- Gamme 1230 AP de Cisco Aironet avec un SSC

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

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

Informations générales

ÀCisco l'architecture centralisée WLAN, des aps fonctionnent en mode léger. Les aps s'associent à un Cisco WLC 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 des exécutions d'installation et d'authentification et de délai d'exécution de chemin. LWAPP définit également le mécanisme de transmission tunnel pour le trafic de données.

AP léger (RECOUVREMENT) découvre un WLC avec l'utilisation des mécanismes de LWAPP discovery. Le RECOUVREMENT envoie alors au WLC une demande de jonction LWAPP. Le WLC envoie au RECOUVREMENT une réponse de jonction LWAPP qui laisse le RECOUVREMENT pour joindre le WLC. Quand le RECOUVREMENT est joint au WLC, le RECOUVREMENT télécharge le logiciel WLC si les révisions sur le RECOUVREMENT et le WLC ne s'assortissent pas. Ultérieurement, le RECOUVREMENT est complètement sous le contrôle du WLC.

LWAPP sécurise la transmission de contrôle entre AP et le WLC au moyen d'une distribution de clé sécurisée. La distribution de clé sécurisée exige les Certificats numériques X.509 déjà provisioned sur le RECOUVREMENT et le WLC. Des certificats d'origine sont référencés avec le terme « MIC » (certificat installé en usine). L'Aironet aps qui a expédié avant juillet 18, 2005, n'ont pas MICs. Ainsi ces aps créent SSC quand ils sont convertis pour fonctionner en mode léger. Les contrôleurs sont programmés pour accepter les SSC pour l'authentification d'AP spécifiques.

C'est le processus de mise à niveau :

1. L'utilisateur exécute un utilitaire de mise à jour qui reçoit un fichier d'entrée avec une liste d'aps et de leurs adresses IP, en plus de leurs qualifications de procédure de connexion.
2. L'utilitaire établit des sessions de telnet avec les aps et envoie une gamme de commandes de logiciel de Cisco IOS dans le fichier d'entrée afin de préparer AP pour la mise à jour. Ces commandes incluent les commandes de créer le SSCs. En outre, l'utilitaire établit une session de telnet avec le WLC afin de programmer le périphérique pour permettre l'autorisation de SSC spécifique aps.
3. L'utilitaire charge alors la version du logiciel Cisco IOS 12.3(7)JX sur AP de sorte qu'AP puisse joindre le WLC.
4. Après qu'AP joigne le WLC, AP télécharge une version de logiciel complète de Cisco IOS du WLC. L'utilitaire de mise à jour génère un fichier de sortie qui inclut la liste d'aps et de valeurs de clé-informations parasites correspondantes de SSC qui peuvent être importés dans le logiciel de gestion du système de contrôle sans fil (WCS).
5. Le WCS peut alors envoyer ces informations à l'autre WLCs sur le réseau.

Après qu'AP joigne un WLC, vous pouvez réaffecter AP à n'importe quel WLC sur votre réseau, s'il y a lieu.

Localisez les informations parasites de la clé SHA1

Si l'ordinateur qui a exécuté la conversion AP est disponible, vous pouvez obtenir les informations parasites de clé du Secure Hash Algorithm 1 (SHA1) à partir du fichier .csv qui est dans le répertoire d'outil de mise à jour de Cisco. Si le fichier .csv est indisponible, vous pouvez émettre une commande de **débogage** sur le WLC afin de récupérer les informations parasites de la clé SHA1.

Procédez comme suit :

1. Activez AP et connectez-le au réseau.
2. Activez l'élimination des imperfections sur l'interface de ligne de commande WLC (CLI).La commande est **enable de PKI de debug pm**.`(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`**

Ajoutez SSC au WLC

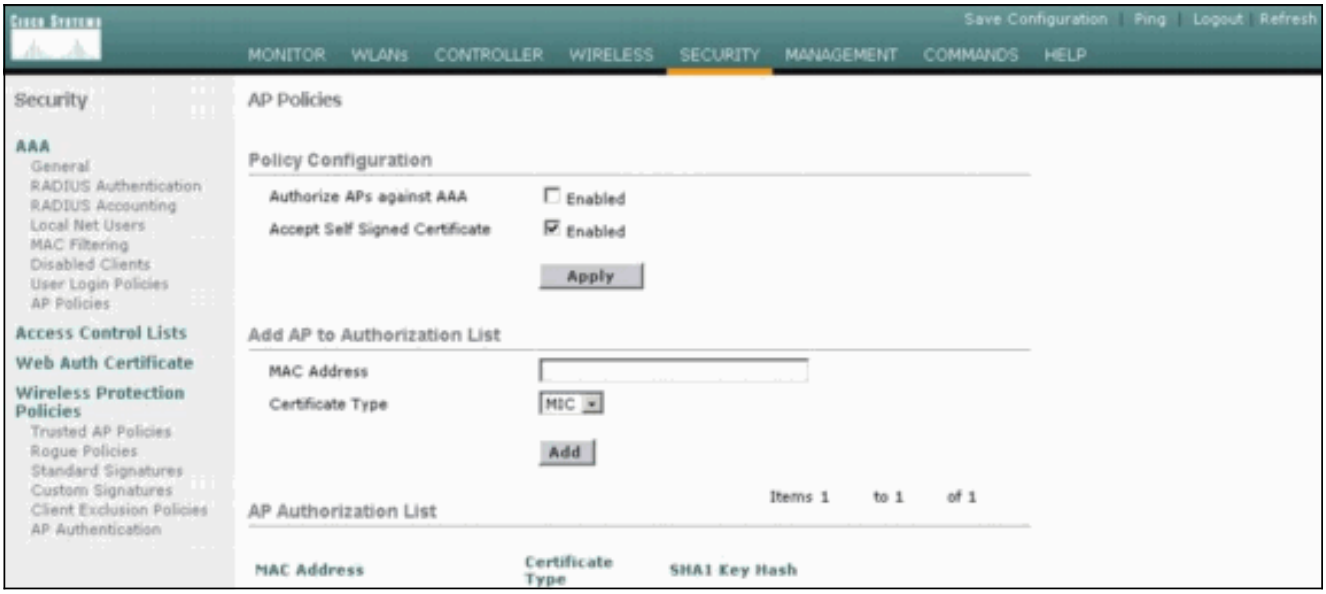
Tâche

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

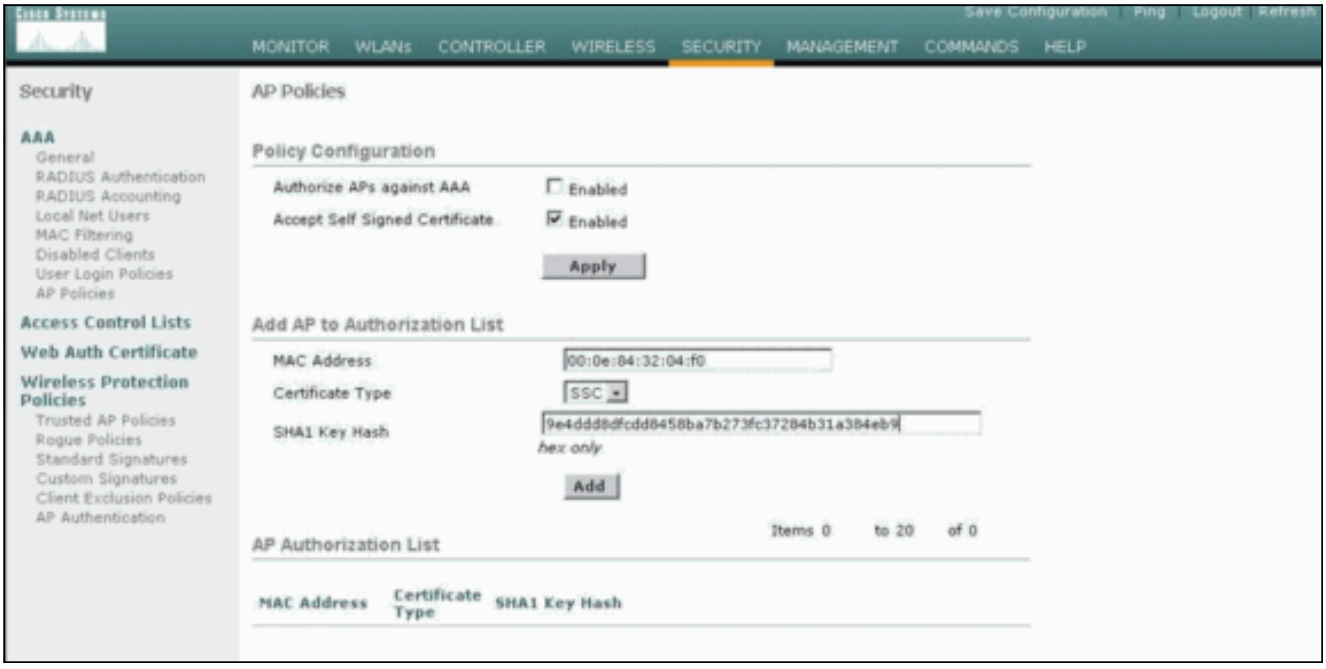
Configuration de la GUI

Terminez-vous ces étapes du GUI :

1. Choisissez le **Security > AP Policies** et le clic **activés** près de l'Accept Self Signed Certificate.



2. **SSC** choisi du menu déroulant de type de certificat.



3. Écrivez l'adresse MAC d'AP et de la clé d'informations parasites, et cliquez sur Add.

Configuration CLI

Terminez-vous ces étapes du CLI :

1. Accept Self Signed Certificate d'enable sur le WLC.La commande est **enable de ssc de config auth-list ap-policy**.`(Cisco Controller) >config auth-list ap-policy ssc enable`
2. Ajoutez l'adresse MAC AP et la clé d'informations parasites à la liste d'autorisation.La commande est le **ssc** *AP_MAC AP_key de* **config auth-list add**.`(Cisco Controller) >config auth-list add ssc 00:0e:84:32:04:f0 9e4ddd8dfcdd8458ba7b273fc37284b31a384eb9 !--- This command should be on one line.`

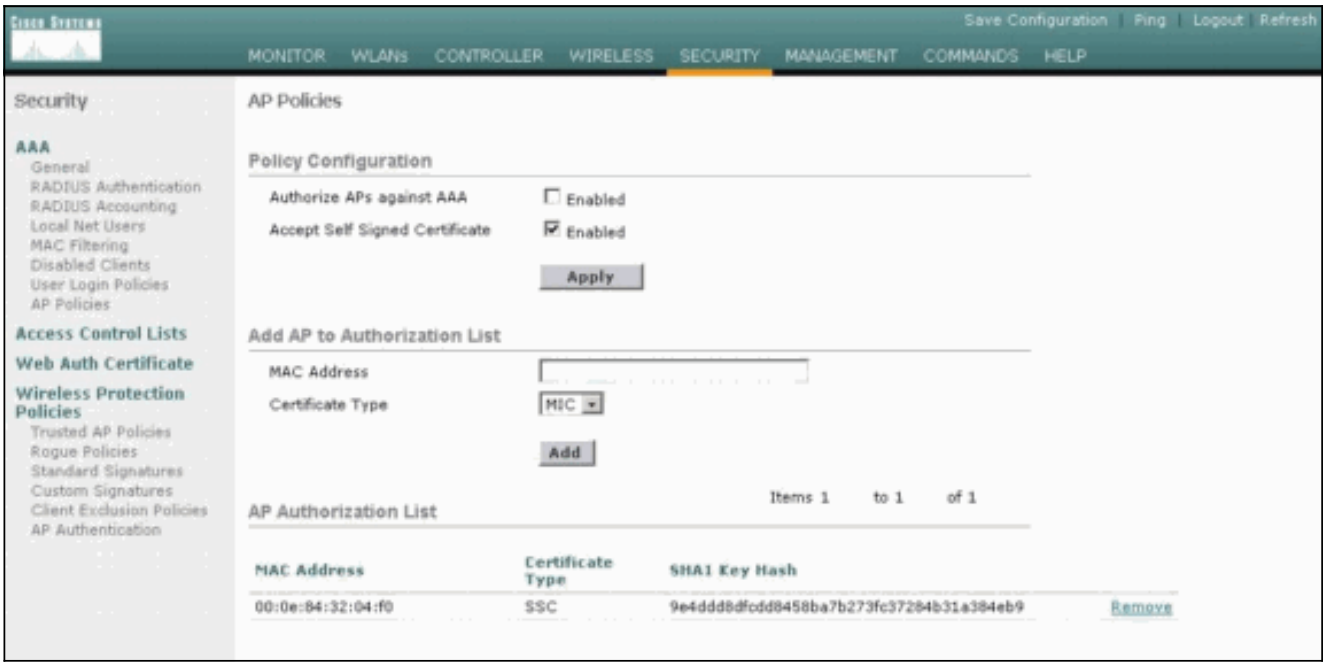
Vérifiez

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

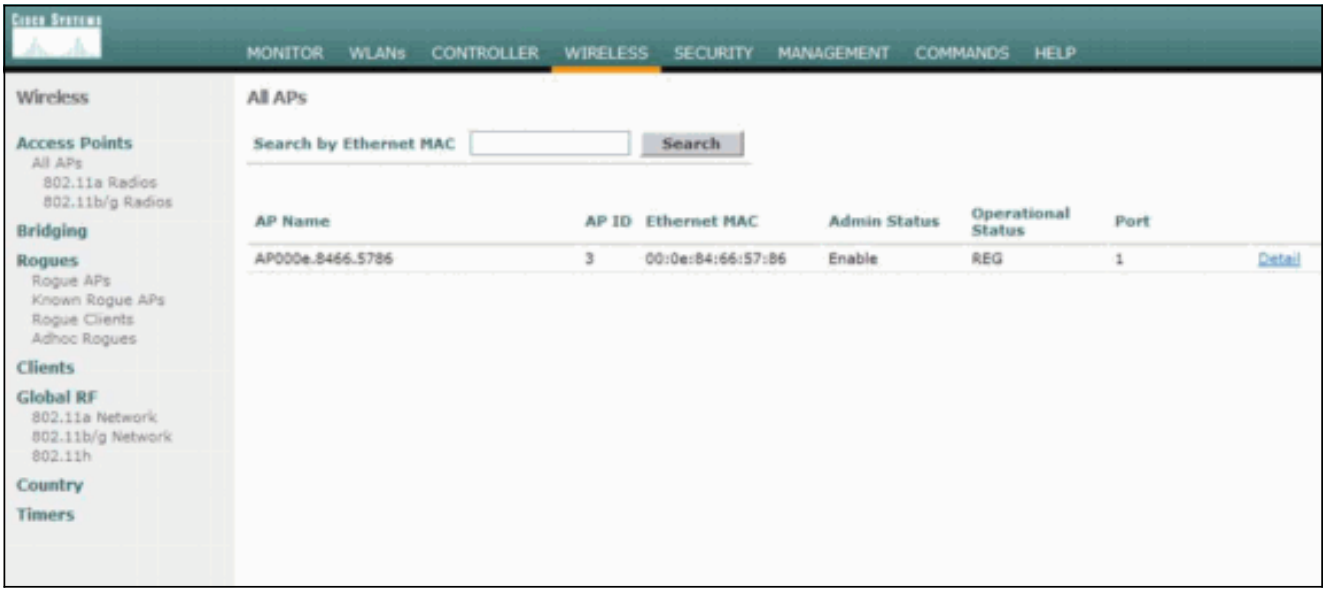
Vérification GUI

Procédez comme suit :

1. Dans la fenêtre de stratégies AP, vérifiez que l'adresse MAC AP et les informations parasites SHA1 principales apparaissent dans la région de liste d'autorisation AP.



2. Dans la toute la fenêtre aps, vérifiez que tous les aps sont inscrits au 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'autorisation AP.
- **show ap summary** — Affiche un résumé de tous les aps connectés.

Dépannez

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