Cómo Agregar Manualmente el Certificado Autofirmado al Controlador para los AP Convertidos en LWAPP

Contenido

Introducción

Este documento explica los métodos que usted puede utilizar para agregar manualmente los certificados autofirmados (SSCs) a un regulador de la tecnología inalámbrica de Cisco LAN (red inalámbrica (WLAN)) (WLC).

SSC de un punto de acceso debe existir en todo el WLCs en la red a la cual el AP tiene permiso para registrarse. Como regla general, aplique SSC a todo el WLCs en el mismo grupo de la movilidad. Cuando la adición de SSC al WLC no ocurre con la utilidad de la actualización, usted debe agregar manualmente SSC al WLC con el uso del procedimiento en este documento. Usted también necesita este procedimiento cuando un AP se mueve a una diversa red o cuando el WLCs adicional se agrega a la red existente.

Usted puede reconocer este problema cuando un protocolo ligero AP (LWAPP) - AP convertido no se asocia al WLC. Cuando usted resuelve problemas el problema de asociación, usted ve estas salidas cuando usted publica estos debugs:

- Cuando usted publica el **comando debug pm pki enable**, usted ve:`(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.
```

- Cuando usted publica el **comando debug lwapp events enable**, usted ve:

```
(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
```

prerrequisitos

Requisitos

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- El WLC no contiene SSC que la utilidad de la actualización generó.
- Los AP contienen SSC.
- Telnet se habilita en el WLC y el AP.
- La versión mínima del código del software de Cisco IOS® del PRE-LWAPP está en el AP que se actualizará.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- El WLC de Cisco 2006 que funciona con el firmware 3.2.116.21 sin SSC instaló
- 1230 Series AP del Cisco Aironet con SSC

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

Antecedentes

En Cisco la arquitectura de WLAN centralizada, los AP actúa en el modo ligero. Los AP asocian a Cisco un WLC al uso del LWAPP. El LWAPP es un proyecto de protocolo de la Internet Engineering Task Force (IETF) que define la mensajería del control para las operaciones de la disposición y de la autenticación y operaciones en tiempo de ejecución. El LWAPP también define el mecanismo de tunelización para el tráfico de datos.

Un AP ligero (REVESTIMIENTO) descubre un WLC con el uso de los mecanismos de la detección de LWAPP. El REVESTIMIENTO entonces envía el WLC que un LWAPP se une a la petición. El WLC envía el REVESTIMIENTO que un LWAPP se une a la respuesta que permite que el REVESTIMIENTO se una al WLC. Cuando el REVESTIMIENTO se une a al WLC, el REVESTIMIENTO descarga el software WLC si las revisiones en el REVESTIMIENTO y el WLC no hacen juego. Posteriormente, el REVESTIMIENTO está totalmente bajo el control del WLC.

El LWAPP asegura la comunicación del control entre el AP y el WLC mediante una distribución de claves segura. La distribución de claves segura requiere ya los Certificados digitales del aprovisionado X.509 en el REVESTIMIENTO y el WLC. Los certificados instalados en fábrica se denominan con el término “MIC”, que son las siglas de Manufacturing Installed Certificate (Certificado de Instalación de Fábrica). El Aironet AP que envió antes de julio 18, 2005, no tiene MIC. Estos AP crean tan SSC cuando se convierten para actuar en el modo ligero. Los controladores se programan para aceptar SSC para la autenticación de AP específicos.

Éste es el proceso de actualización:

1. El usuario funciona con una utilidad de la actualización que valide un archivo de entrada con una lista de AP y de sus IP Addresses, además de sus credenciales del login.
2. La utilidad establece a las sesiones telnets con los AP y envía a una serie de comandos del Cisco IOS Software en el archivo de entrada para preparar el AP para la actualización. Estos comandos include los comandos de crear el SSCs. También, la utilidad establece a una sesión telnet con el WLC para programar el dispositivo para permitir la autorización de SSC específico AP.
3. La utilidad entonces carga el Cisco IOS Software Release 12.3(7)JX sobre el AP de modo que el AP pueda unirse al WLC.
4. Después de que el AP se una al WLC, el AP descarga una versión del Cisco IOS Software completa del WLC. La utilidad de la actualización genera un archivo saliente que incluya la lista de AP y de valores de clave-hash correspondientes de SSC que se puedan importar en el software de administración inalámbrico del sistema de control (WCS).
5. El WCS puede entonces enviar esta información al otro WLCs en la red.

Después de que un AP se una a un WLC, usted puede reasignar el AP a cualquier WLC en su red, en caso necesario.

Localice el hash de la clave SHA1

Si el ordenador que realizó la conversión AP está disponible, usted puede obtener el hash de la clave del algoritmo de troceo seguro 1 (SHA1) del archivo del .csv que está en el directorio de la herramienta de actualización de Cisco. Si el archivo del .csv es inasequible, usted puede publicar un **comando debug** en el WLC para extraer el hash de la clave SHA1.

Complete estos pasos:

1. Gire el AP y conéctelo con la red.
2. Habilite el debugging en el comando line interface(cli) del WLC.El comando es **permiso del pki del debug P.M.**

```
(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
```

Agregue SSC al WLC

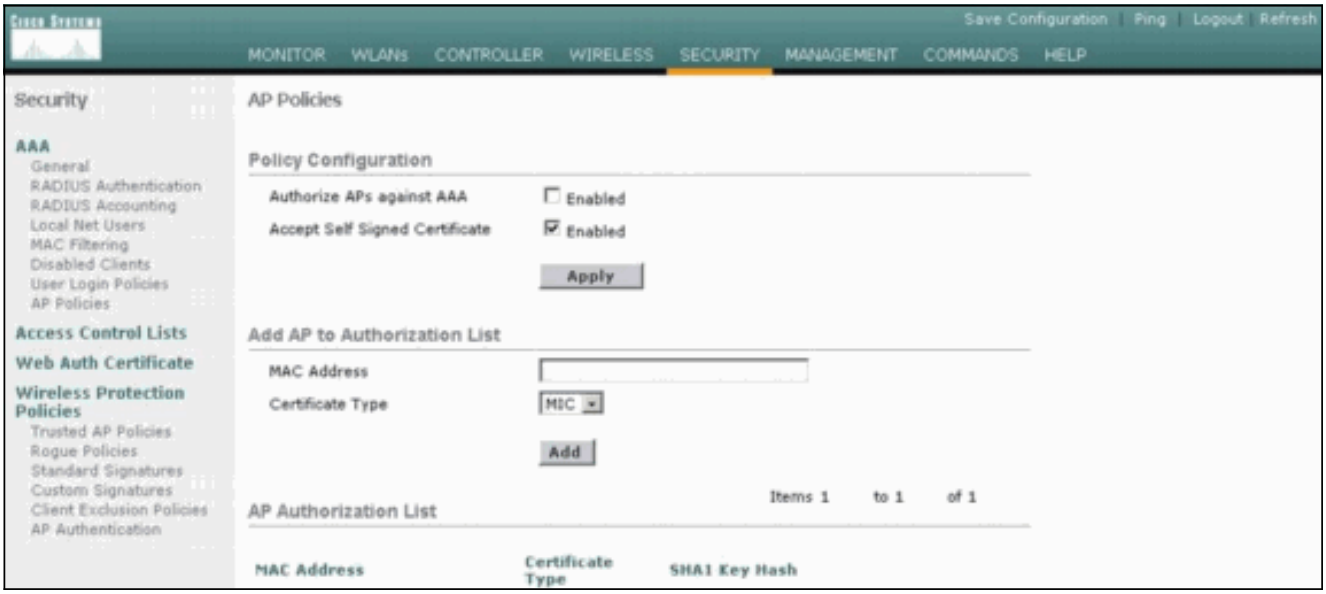
Tarea

En esta sección encontrará la información para configurar las funciones descritas en este documento.

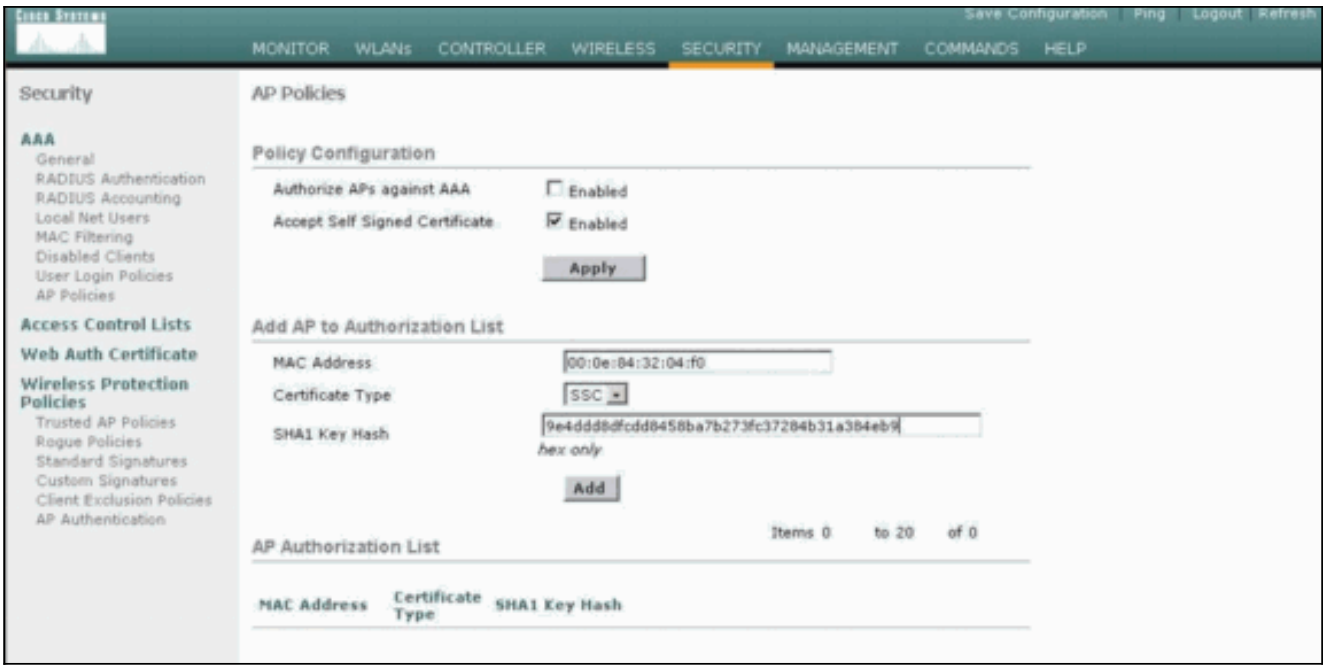
Configuración de la interfaz gráfica para el usuario

Complete estos pasos del GUI:

1. Elija la **Seguridad > las directivas AP** y haga clic **habilitado** por otra parte validan el certificado firmado del uno mismo.



2. Seleccione **SSC del** menú desplegable del tipo de certificado.



3. Ingrese el MAC address del AP y de la clave del hash, y el haga click en Add

Configuración de CLI

Complete estos pasos del CLI:

1. El permiso valida el certificado firmado del uno mismo en el WLC.El comando es **permiso del ssc de la ap-directiva de la auténtico-lista de los config**.`(Cisco Controller) >`**`config auth-list ap-policy ssc enable`**
2. Agregue la dirección MAC AP y la clave del hash a la lista de la autorización.El comando es auténtico-**lista de los config agrega el 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.`*

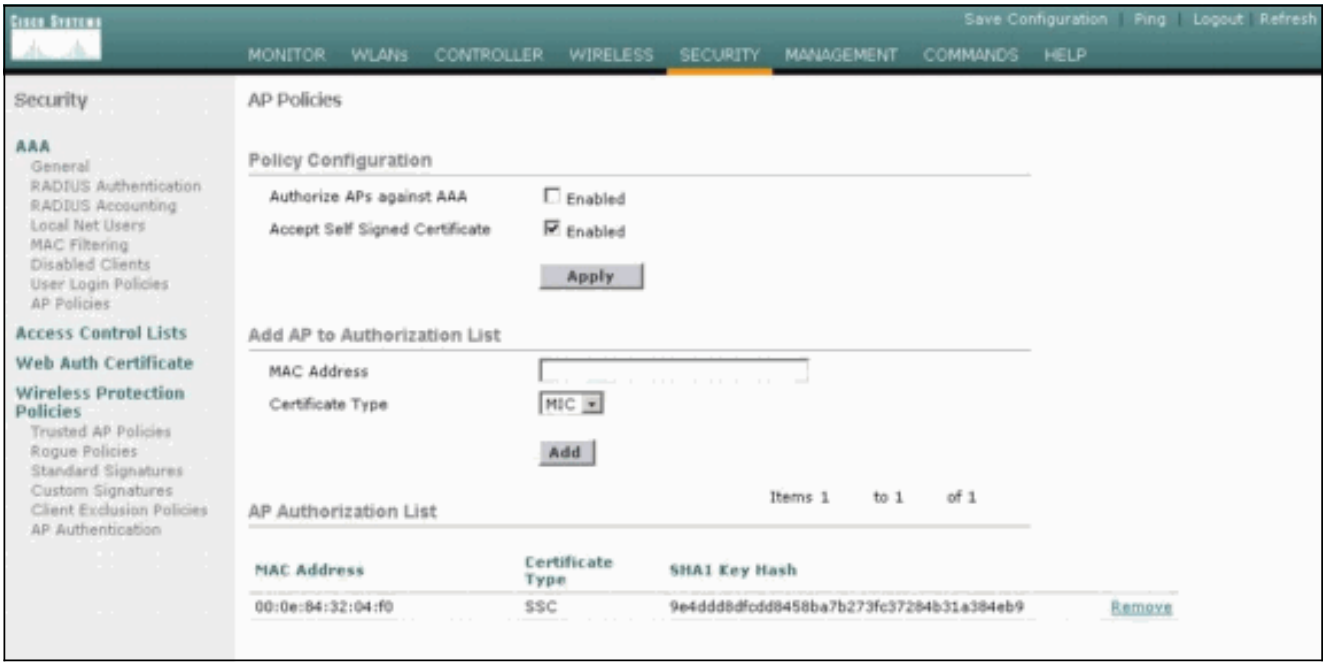
Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

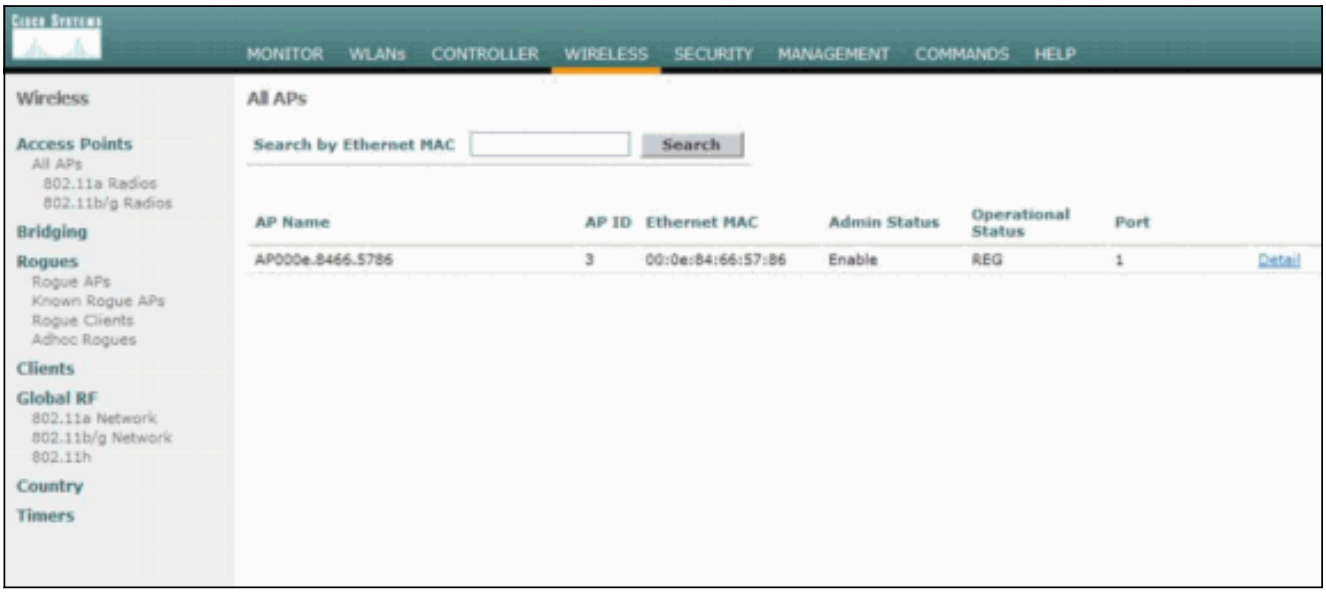
Verificación GUI

Complete estos pasos:

1. En la ventana Policies (Políticas) AP, verifique que la dirección MAC AP y el hash dominante SHA1 aparezcan en el área de la lista de la autorización AP.



2. En toda la ventana APs, verifique que todos los AP estén registrados con el WLC.



Verificación CLI

La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

- **auténtico-lista de la demostración** — Visualiza la lista de la autorización AP.
- **muestre el resumen ap** — Visualiza un resumen de todos los AP conectados.

Troubleshooting

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

Información Relacionada

- Preguntas Frecuentes sobre el Troubleshooting de los Controladores de WAN Inalámbricos (WLC)
- Guía de Configuración de Cisco Wireless LAN Controller , Release 3.2
- Ejemplo de la configuración básica del controlador y del Lightweight Access Point del Wireless LAN
- Soporte Técnico y Documentación - Cisco Systems