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

Contenido

[Introducción](#)
[Prerequisites](#)
[Requirements](#)
[Componentes Utilizados](#)
[Convenciones](#)
[Antecedentes](#)
[Localice el hash de la clave SHA1](#)
[Agregar el SSC al WLC](#)
[Tarea](#)
[Configuración de la interfaz gráfica para el usuario](#)
[Configuración de CLI](#)
[Verificación](#)
[Troubleshoot](#)
[Información Relacionada](#)

Introducción

Este documento explica los métodos que puede utilizar para agregar manualmente certificados autofirmados (SSC) a un controlador Cisco Wireless LAN (WLAN) Controller (WLC).

El SSC de un punto de acceso (AP) debe existir en todos los WLC en la red a la que el AP tiene permiso para registrarse. Como regla general, aplique el SSC a todos los WLC en el mismo grupo de movilidad. Cuando la adición del SSC al WLC no ocurre a través de la utilidad de upgrade, debe agregar manualmente el SSC al WLC con el uso del procedimiento en este documento. También necesita este procedimiento cuando un AP se mueve a una red diferente o cuando se agregan WLC adicionales a la red existente.

Puede reconocer este problema cuando un AP convertido en protocolo ligero de punto de acceso (LWAPP) no se asocia al WLC. Cuando resuelve el problema de asociación, verá estos resultados cuando ejecute estos debugs:

- Cuando ejecuta el comando **debug pm pki enable**, 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 ejecuta el comando **debug lwapp events enable**, puede ver:

```
(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
```

Prerequisites

Requirements

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- El WLC no contiene el SSC que generó la utilidad de upgrade.
- Los AP contienen un SSC.
- Telnet está habilitado en el WLC y el AP.
- La versión mínima del código de software Cisco IOS® previo al LWAPP se encuentra en el AP que se va a actualizar.

Componentes Utilizados

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

- Cisco 2006 WLC que ejecuta firmware 3.2.116.21 sin SSC instalado
- Cisco Aironet 1230 Series AP con 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.

Convenciones

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

Antecedentes

En la arquitectura WLAN centralizada de Cisco, los AP funcionan en modo ligero. Los AP se asocian a un WLC de Cisco con el 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 (LAP) detecta un WLC con el uso de mecanismos de detección de LWAPP. El LAP entonces envía al WLC una solicitud de unión LWAPP. El WLC envía al LAP una respuesta de unión LWAPP que permite al LAP unirse al WLC. Cuando el LAP se une al WLC, el LAP descarga el software WLC si las revisiones en el LAP y el WLC no coinciden. Posteriormente, el LAP está completamente bajo el control del WLC.

El LWAPP asegura la comunicación de control entre el AP y el WLC mediante una distribución de clave segura. La distribución de clave segura requiere certificados digitales X.509 ya suministrados en el LAP 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). Los AP Aironet que se enviaron antes del 18 de julio de 2005, no tienen MIC. Estos AP crean un SSC cuando se convierten para funcionar en modo ligero. Los controladores se programan para aceptar SSC para la autenticación de AP específicos.

Este es el proceso de actualización:

1. El usuario ejecuta una utilidad de actualización que acepta un archivo de entrada con una lista de AP y sus direcciones IP, además de sus credenciales de inicio de sesión.
2. La utilidad establece sesiones Telnet con los AP y envía una serie de comandos de Cisco IOS Software en el archivo de entrada para preparar el AP para la actualización. Estos comandos incluyen los comandos para crear los SSC. Además, la utilidad establece una sesión Telnet con el WLC para programar el dispositivo para permitir la autorización de APs SSC específicos.
3. La utilidad luego carga el Cisco IOS Software Release 12.3(7)JX en el AP para que el AP pueda unirse al WLC.
4. Después de que el AP se une al WLC, el AP descarga una versión completa del Cisco IOS Software del WLC. La utilidad de actualización genera un archivo de salida que incluye la lista de puntos de acceso y los valores hash de clave SSC correspondientes que se pueden importar al software de administración de Wireless Control System (WCS).
5. El WCS luego puede enviar esta información a otros WLC en la red.

Después de que un AP se une a un WLC, puede reasignar el AP a cualquier WLC en su red, si es necesario.

Localice el hash de la clave SHA1

Si el equipo que realizó la conversión de AP está disponible, puede obtener el hash de la clave del algoritmo hash seguro 1 (SHA1) del archivo .csv que se encuentra en el directorio de la herramienta de actualización de Cisco. Si el archivo .csv no está disponible, puede ejecutar un comando **debug** en el WLC para recuperar el hash de la clave SHA1.

Complete estos pasos:

1. Encienda el AP y conéctelo a la red.
2. Habilite la depuración en la interfaz de línea de comandos (CLI) del WLC.El comando es **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
```

Agregar el SSC al WLC

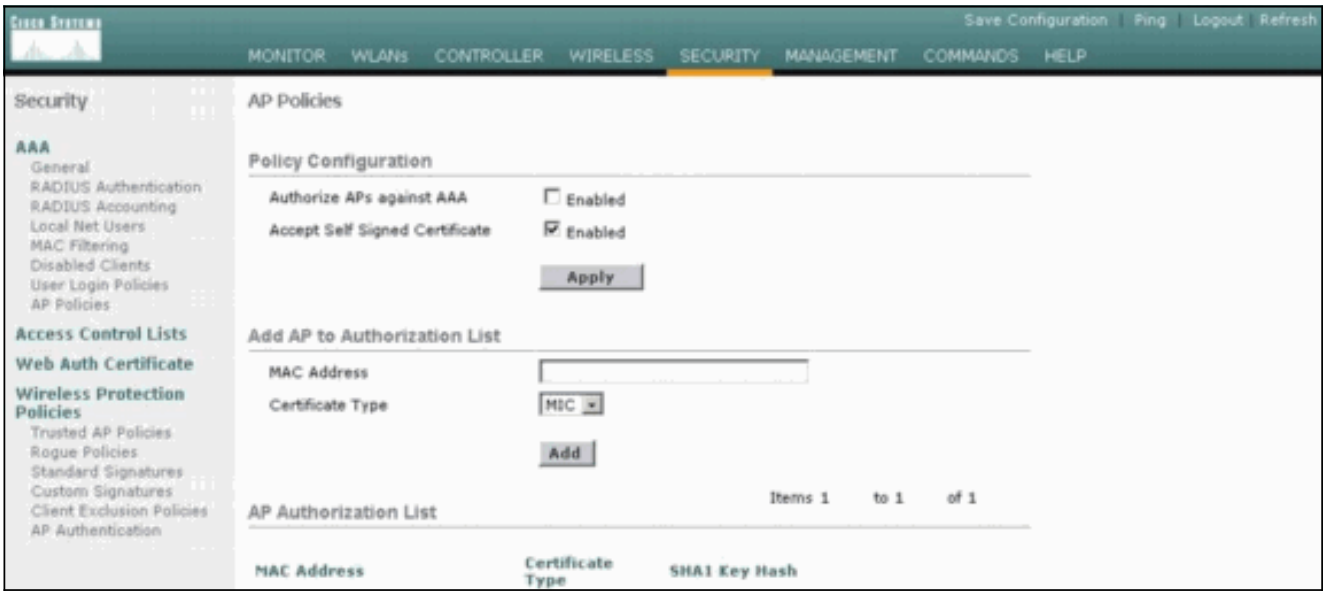
Tarea

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

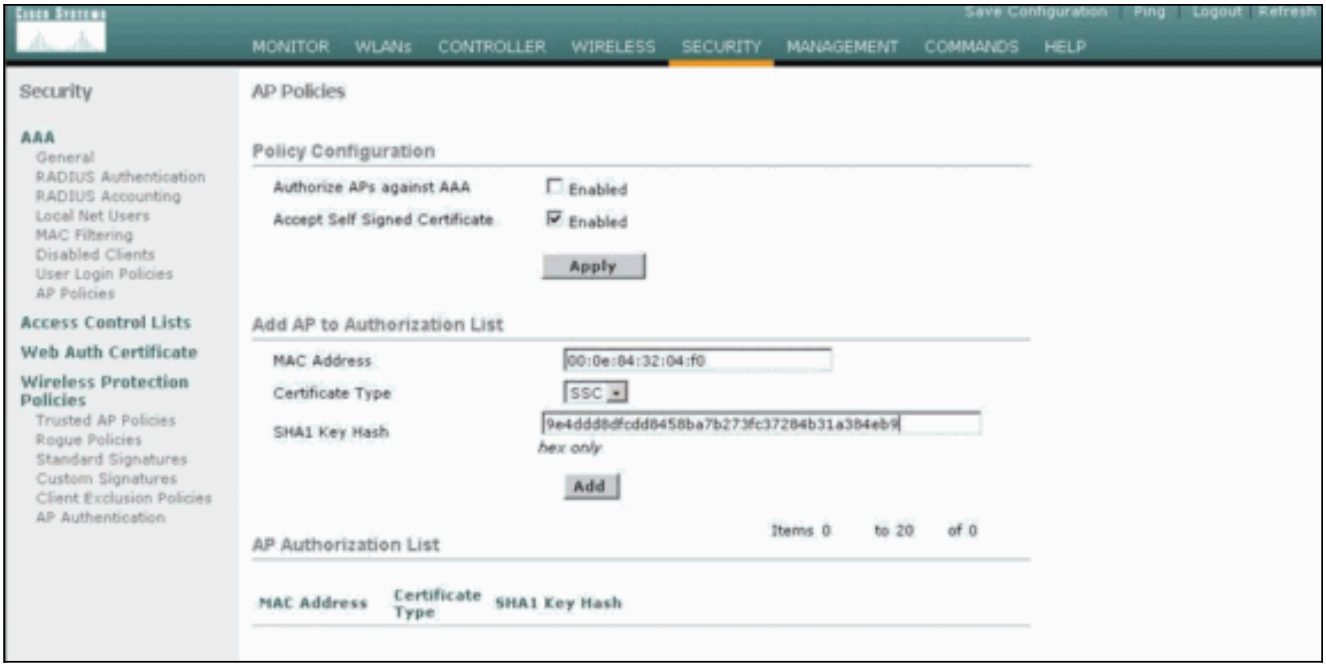
Configuración de la interfaz gráfica para el usuario

Complete estos pasos desde la GUI:

1. Elija **Security > AP Policies** y haga clic en **Enabled** junto a Accept Self Signed Certificate.



2. Seleccione **SSC** en el menú desplegable Tipo de certificado.



3. Ingrese la dirección MAC del AP y la llave hash, y haga clic en **Agregar**.

Configuración de CLI

Complete estos pasos desde la CLI:

1. Habilite Accept Self Signed Certificate en el WLC.El comando es **config auth-list ap-policy ssc enable**.
```
(Cisco Controller) >config auth-list ap-policy ssc enable
```

2. Agregue la dirección MAC del AP y la llave hash a la lista de autorización.El comando es **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.
```

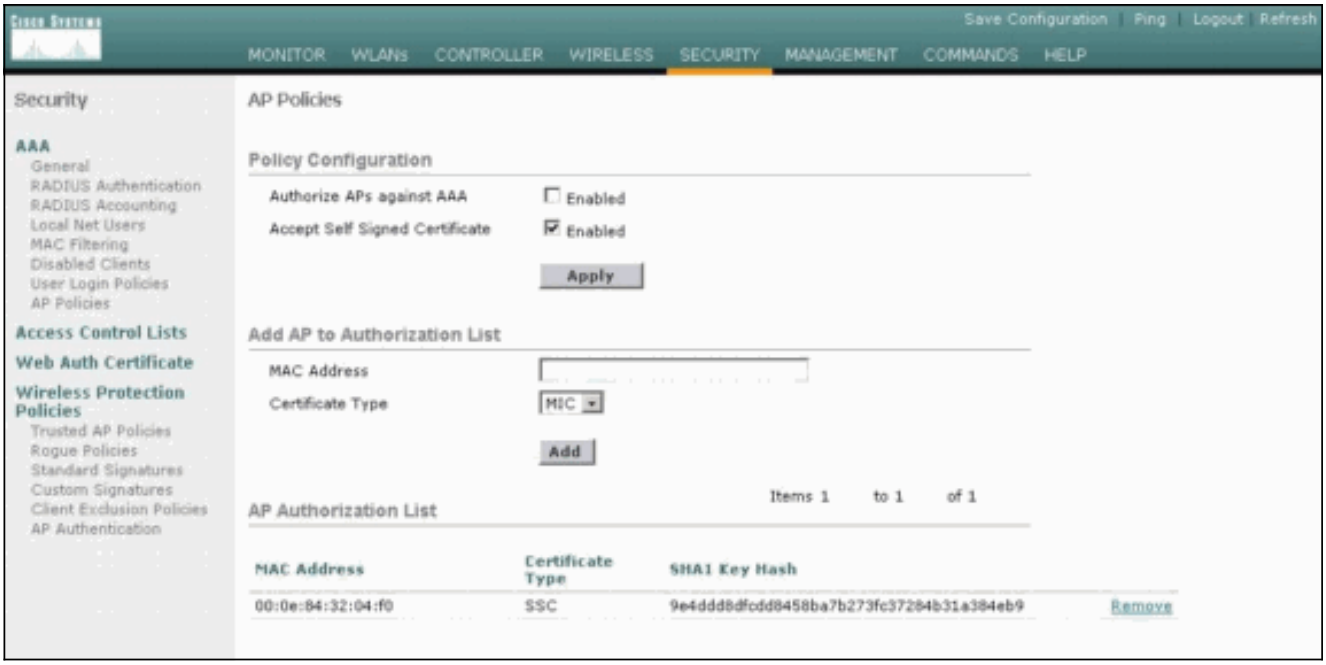
Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

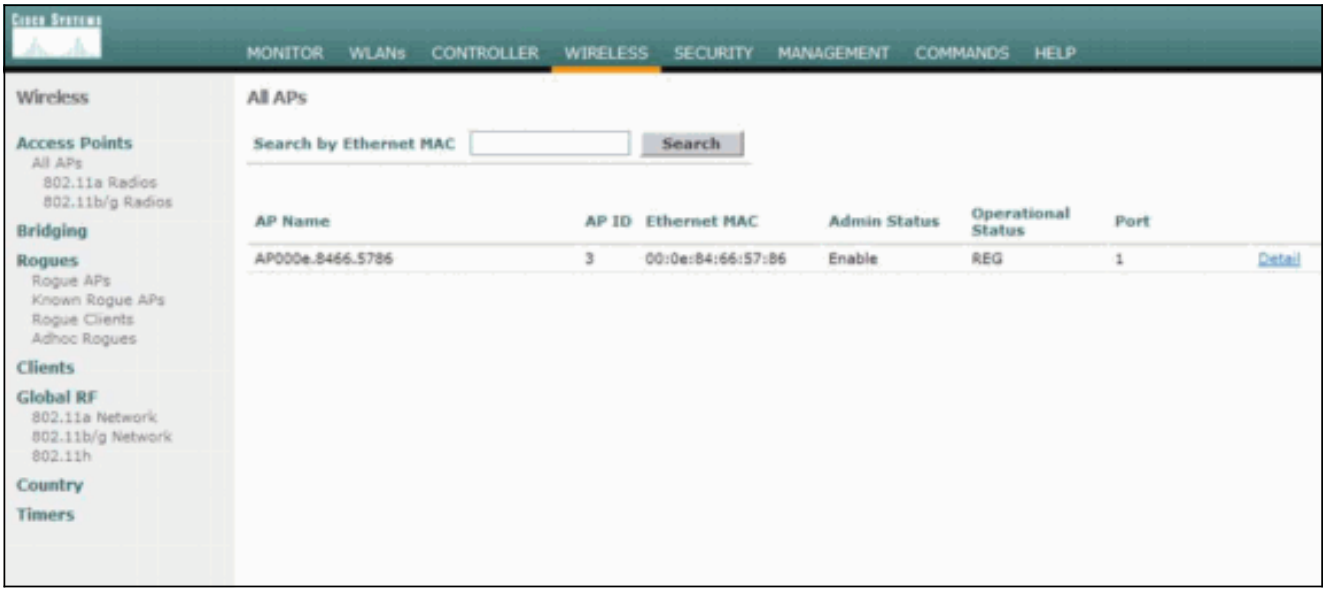
Verificación de GUI

Complete estos pasos:

1. En la ventana AP Policies , verifique que la dirección MAC del AP y el hash de la clave SHA1 aparezcan en el área AP Authorization List
.



2. En la ventana All APs , verifique que todos los APs 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.

- **show auth-list**—Muestra la lista de autorización AP.
- **show ap summary**—Muestra un resumen de todos los AP conectados.

Troubleshoot

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