

# El resolver problemas inalámbrico del sistema de control

## Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Troubleshooting](#)

[No capaz de instalar el WCS](#)

[Problemas de compatibilidad entre las versiones del WLC y WCS](#)

[El WCS no puede comenzar después de la instalación en un sistema operativo no inglés de Windows 2003](#)

[Caracteres internacionales no soportados en el WCS](#)

[Incapaz de comenzar el WCS debido a los archivos del registro corrompidos](#)

[Marque el estatus del WCS](#)

[Agregue un WLC al WCS](#)

[Configuración de restauración del WLC del WCS](#)

[Firewall entre el WCS y el regulador o el WCS y la interfaz de usuario WCS](#)

[Reajuste un regulador de nuevo a los valores predeterminados de fábrica usando el WCS](#)

[Base de datos de Defragmenting WCS](#)

[Marque si usted tiene la licencia apropiada para el software WCS](#)

[Utilice la página de resumen de la Seguridad para resolver problemas](#)

[Detecte y localice los puntos de acceso no autorizado](#)

[Utilice la característica de la personificación del punto de acceso en el WCS](#)

[Localice a los clientes](#)

[Agujeros de la cobertura en una red WLAN](#)

[Si usted tiene dificultades cuando usted importa las correspondencias](#)

[Haga ping un dispositivo de red de un WLC de Cisco](#)

[Vea el estatus, las configuraciones, y las estadísticas actuales del WLC de Cisco](#)

[Examine la disposición de la ubicación](#)

[Problemas de sincronización con los servidores WCS y de la ubicación](#)

[Problemas de sincronización con el WCS y el WLC](#)

[Configuración DHCP corrompida cuando la plantilla se avanza del WCS a WiSM](#)

[Las correspondencias del calor WCS muestran los agujeros cuadrados incorrectos de la cobertura](#)

[¿Cuándo la plantilla del granuja AP consigue aplicada al WLC?](#)

[Puertos en el servidor WCS](#)

[Verifique los WLAN son permiso fijado de la exclusivo-lista](#)

[Resuelva problemas el permiso de la exclusivo-lista](#)

[Vea y borre a los clientes global discapacitados](#)

[Vea y borre manualmente a los clientes discapacitados por el regulador](#)

[La búsqueda WCS para los clientes por el edificio no trabaja](#)

[Cuentas incorrectas del cliente de los informes WCS asociadas a los AP en el modo H-REAP](#)

[El WCS no comienza si el caracter de subrayado se configura en el servidor/el nombre de host](#)

[El \[location\] del ERROR no pudo crear el mapa del calor para el MAC: xx: xx: xx: xx: xx: xx razón:](#)

[Se falla como la lista RSSI vacío después de la poda del tiempo](#)

[El mensaje de error "la entrada Point Filexp Could del procedimiento no ser situado en visualizaciones de la biblioteca con link dinámico el DFORRT.DLL"](#)

[Instrucciones al synch los tres dispositivos](#)

[La plantilla de la red inalámbrica \(WLAN\) no aplica la configuración correcta del "broadcast SSID" en el WLC](#)

[Las plantillas de la red inalámbrica \(WLAN\) no visualizan la determinación correcta del checkbox de 7920 CAC](#)

[Incapaz de borrar los reguladores offline de la versión 3.2.51.0 WCS](#)

[No puede agregar la plantilla de la autenticación Web con el valor por defecto del tipo interno del WCS](#)

[Información Relacionada](#)

## **Introducción**

Este documento proporciona procedimientos de Troubleshooting para problemas básicos de WCS (Cisco Wireless Control System).

## **prerrequisitos**

### **Requisitos**

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimiento de cómo configurar Cisco WCS
- Conocimiento de cómo configurar un Wireless LAN (red inalámbrica (WLAN)) con los controladores de WLAN (WLCs) y los Puntos de acceso ligeros (revestimientos)

## **Componentes Utilizados**

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

## **Convenciones**

Consulte [Convenciones de Consejos TécnicosCisco](#) para obtener más información sobre las convenciones del documento.

## **Troubleshooting**

## No capaz de instalar el WCS

Si usted experimenta los problemas cuando usted intenta instalar el WCS, en primer lugar controle para ver si el sistema en el cual usted planea instalar el WCS cumple los requisitos mínimos del sistema.

Ésta es la lista de verificación necesaria de antemano a utilizar antes de que usted instale Cisco WCS:

1. Marque si el sistema en el cual usted está a punto de instalar Cisco WCS cumple los requisitos de hardware y de software necesarios para Cisco WCS. Para la información sobre el software mínimo y los requisitos de hardware para la instalación del WCS, refiera a la sección de los [requisitos del sistema de la guía de configuración de Cisco WCS, la versión 4.0](#).
2. Asegúrese de que usted haya puesto al día su sistema con las actualizaciones y los paquetes de servicios críticos necesarios. Refiera a los últimos Release Note para la información sobre los paquetes de servicios y las correcciones requeridos para la operación correcta del WCS. **Nota:** Antes de que usted instale el WCS en Linux, se requiere un lleno instala de Red Hat Linux.
3. Respaldo la base de datos existente WCS. Refiera a [sostener la base de datos para obtener información WCS](#) en cómo realizar un respaldo de Windows.
4. Desinstale la más vieja versión del WCS. Refiera a [desinstalar Cisco WCS](#) para la información sobre cómo realizar una desinstalación.

Una vez que usted se asegura de que usted tenga los requisitos previos, usted puede instalar el WCS. Refiera a [instalar el WCS para Windows](#) para la información sobre cómo instalar Cisco WCS para Windows.

**Nota:** Funcionamientos WCS solamente en Windows de 32 bits; las instalaciones 64-bit del sistema operativo no se soportan.

Refiera a [instalar el WCS para Linux](#) para la información sobre cómo instalar el WCS en Linux.

## Problemas de compatibilidad entre las versiones del WLC y WCS

Cuando usted instala el WCS para manejar el WLCs, asegúrese de que las versiones WCS y del WLC sean compatibles. Esta información está disponible en los Release Note de la versión WCS que usted instala.

Por ejemplo, Cisco WCS 5.1.64.0 soporta la Administración de estos reguladores del Wireless LAN:

- 4.2.61.0
- 4.2.99.0
- 4.2.112.0
- 4.2.130.0
- 5.0.148.0
- 5.1.151.0

Esta información está disponible en este documento: [Release Note para el Cisco Wireless Control System 5.1.64.0 para Windows o Linux](#)

Si usted utiliza las versiones incompatibles del WCS y del WLC, usted no podrá agrega su WLCs al WCS.

## [El WCS no puede comenzar después de la instalación en un sistema operativo no inglés de Windows 2003](#)

Esto ocurre porque el WCS se soporta solamente en Windows 2003 con el inglés o las versiones japonesas. Si usted utiliza los sistemas operativos traducidos a otros lenguajes, hace el WCS fallar después de la instalación. Para evitar esto, utilice el WCS en Windows 2003 inglés o las versiones japonesas.

## [Caracteres internacionales no soportados en el WCS](#)

El WCS y los dispositivos de la ubicación no soportan los caracteres internacionales en general. Si usted utiliza los caracteres no ingleses para los nombres de asignación, la información del activo, el etc., puede generar los errores de la visualización (caracteres incorrectos visualizados) y los errores en las funciones de la búsqueda.

## [Incapaz de comenzar el WCS debido a los archivos del registro corrompidos](#)

No podemos a veces comenzar el WCS y abrir su interfaz Web. Incluso si usted intenta abrir el WCS con el archivo del ".exe" en el WCS \ el compartimiento \ la carpeta, puede fallar. Este mensaje puede visualizar mientras que usted intenta comenzar el WCS.

```
Starting WCS
```

```
Checking for Port 21 availability... OK
```

```
Checking for Port 8456 availability... OK
```

```
Checking for Port 8457 availability... OK
```

```
.....  
.....  
.....  
.....  
.....
```

```
Starting database server ...
```

```
The Nms_Server service is starting..... The Nms_Server service could not be started. The service did not report an error. More help is available by typing NET HELPMSG 3534. Failed to start WCS server.
```

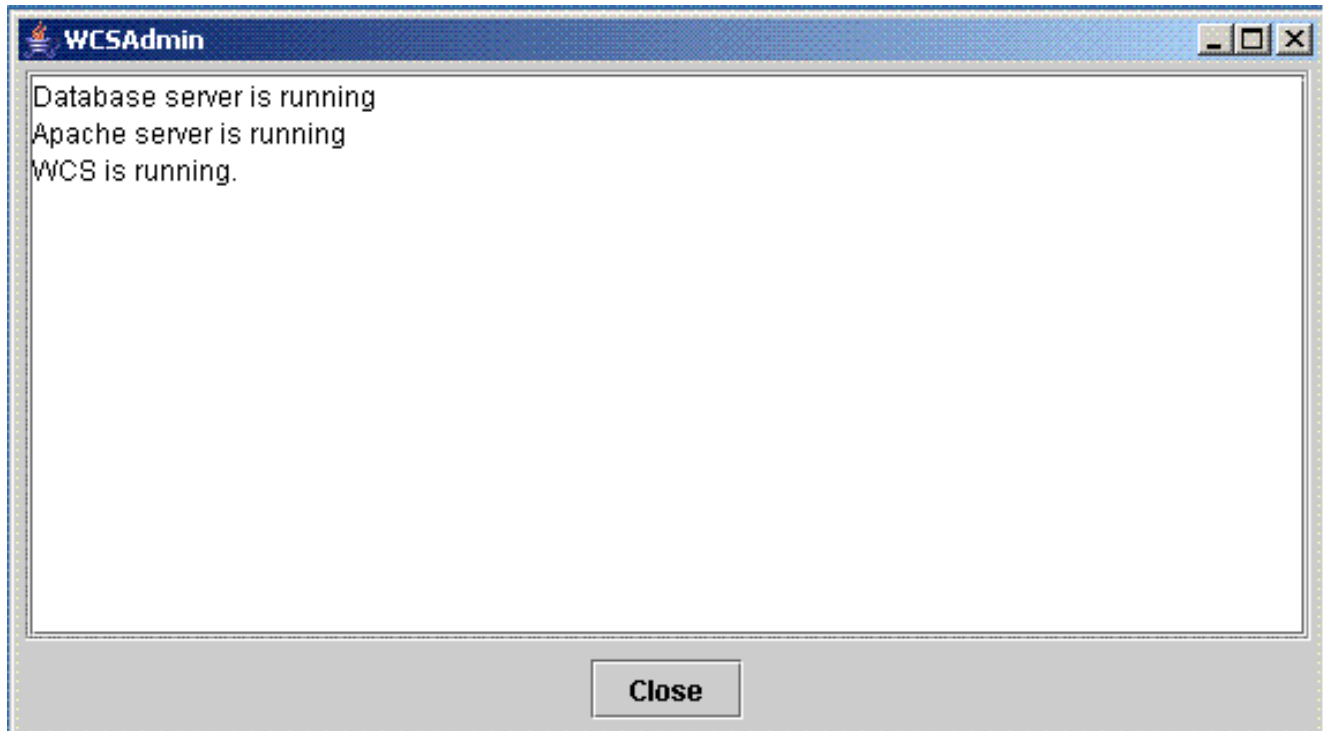
Una razón posible de este problema puede ser el bug [CSCse17963](#) ([clientes registrados solamente](#)).

Según este bug, la base de datos WCS puede no poder comenzar debido a los archivos del registro corrompidos. Para resolver este problema, vaya al sub-directorio **independiente** a través de los **webnms \ eval\_kit de la trayectoria \ independiente** dentro del directorio WCS. En ese sub-directorio, encuentre el **archivo** numerado más alto **sol####.log**, donde está al **####** número de cuatro dígitos. Borrelo y reinicie el servidor. Intente comenzar el WCS. Si el WCS no comienza, relanzar para el archivo siguiente **sol###.log**, y así sucesivamente. Esta solución alternativa resolverá el problema.

## [Marque el estatus del WCS](#)

Si no funciona el WCS como se esperaba, en primer lugar controle el estatus del WCS. Complete estos pasos para marcar el estatus del WCS cuando está instalado como servicio de la aplicación de Windows o de Windows. Usted puede marcar el estatus en cualquier momento.

1. Registro en el sistema como administrador.
2. Realice una de estas acciones: Van al menú Start (Inicio) de Windows y eligen los **programas > el sistema de control inalámbrico > WCSStatus**. Del comando prompt, navegue al directorio de instalación WCS (C:\Program Files\WCS32\bin) y ingrese el **estatus de WCSAdmin**. La ventana de WCSAdmin aparece y visualiza los mensajes que indican el estatus del WCS:



3. Tecleo **cercano** para cerrar la ventana de WCSAdmin.

Si el WCS está instalado en un sistema Linux, complete estos pasos para marcar el estatus del WCS:

1. Registro en el sistema como raíz.
2. Utilice Linux CLI para realizar una de estas tareas: Navegue al directorio de **/opt/WCS32** (o al directorio elegido durante la instalación) y ingrese **./WCSStatus**. Navegue al directorio de **/opt/WCS32/bin** y ingrese el **estatus de WCSAdmin**. El CLI visualiza los mensajes que indican el estatus del WCS.

## [Agregue un WLC al WCS](#)

Cuando un nuevo WLC se agrega al WCS, asegúrese de que la versión de SNMP configurada en el regulador haga juego con la versión de SNMP en el WCS. Si las versiones no hacen juego, el WCS no detecta el regulador y este error aparece en el WCS.

No response from device, check SNMP.

También asegúrese de que el privilegio de acceso de escritura SNMP esté habilitado en el regulador. Si usted ingresa acceso de sólo lectura los parámetros entonces el regulador se agrega al WCS, pero el WCS no puede modificar la configuración en el regulador.

En resumen, marque estos elementos si hay un problema que agrega el regulador al WCS:

- La dirección IP del puerto del servicio del regulador se pudo fijar incorrectamente. Marque la configuración de puerto del servicio en el regulador.
- El WCS no pudo poder entrar en contacto el regulador. Asegurese que usted puede hacer ping el regulador del servidor WCS.
- Las configuraciones SNMP en el regulador no pudieron corresponder con las configuraciones SNMP que usted ingresó en el WCS. Asegurese que las configuraciones SNMP configuradas en el regulador corresponden con las configuraciones que usted ingresó en el WCS.
- Cuando usted actualiza el WCS a la última versión, usted necesita una licencia de Cisco. Si su WCS no se autoriza, usted no puede agregar un nuevo WLC. Para obtener una licencia, usted necesita llamar el soporte a TAC.

**Nota:** Si usted realiza cualesquiera cambios en el WCS, después asegurese le remitir los cambios a sus reguladores. Entonces restaure las configuraciones del regulador para hacerlo actualizado. Vea la [configuración de restauración del WLC de la](#) sección [WCS de](#) este documento para saber restaurar el WLC del WCS.

## [Configuración de restauración del WLC del WCS](#)

Realice estos pasos en el WCS en esta orden para restaurar la configuración de controlador del WCS.

1. Elija la **configuración > los reguladores**.
2. Los reguladores paginan las listas todo el WLCs agregado. De la lista de WLCs, elija el WLC que se restaurará.
3. En la página resultante del regulador, del **selecto un** menú desplegable del **comando**, elige la **configuración de la salvaguardia para contellear** y el tecleo **va**.
4. Después de que la configuración se guarde en el Flash, usted recibe un mensaje acertado en la pantalla. Después de que aparezca la pantalla acertada, elija al mismo regulador cuya configuración fue guardada para contellear y, en el **selecto un comando**, elegir **restaura los config del regulador**.
5. Esto le indica a que conserve o borre la antigua configuración. Elija la **cancelación** y presione **OK**.

## [Firewall entre el WCS y el regulador o el WCS y la interfaz de usuario WCS](#)

Cuando un servidor WCS y una interfaz de usuario WCS están en los lados diferentes de un Firewall, no pueden comunicar a menos que estos puertos en el Firewall estén abiertos al tráfico de dos sentidos:

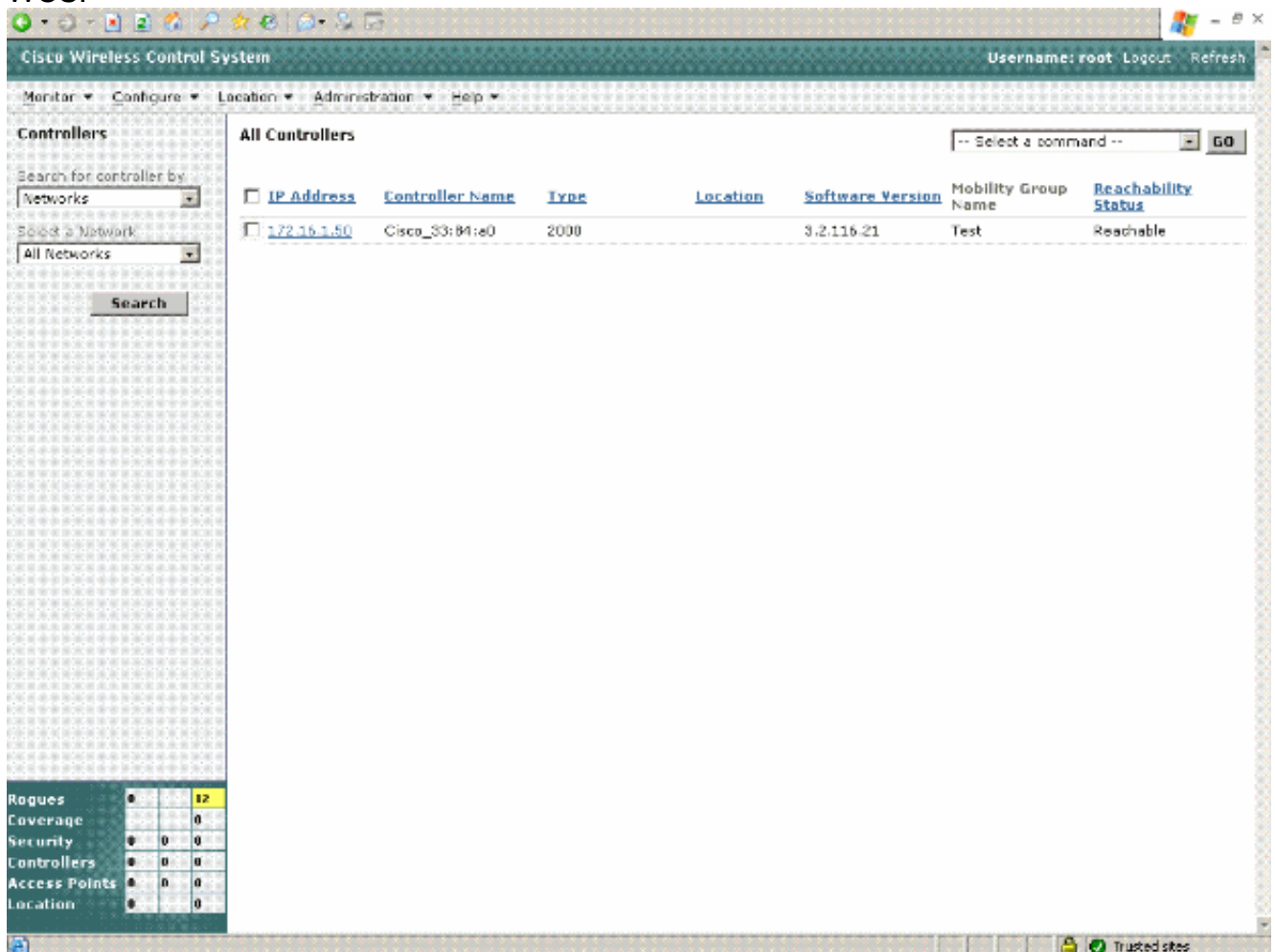
- 80 (para el HTTP inicial)
- 69 (tftp)
- 162 (puerto del desvío)
- 443 (https)

Abra estos puertos para configurar su Firewall para permitir las comunicaciones entre un servidor WCS y una interfaz de usuario WCS.

## [Reajuste un regulador de nuevo a los valores predeterminados de fábrica usando el WCS](#)

Complete estos pasos para reajustar el regulador a los valores predeterminados de fábrica usando el WCS:

1. Elija la **configuración > los reguladores** para visualizar toda la página de los reguladores. Esta página enumera todos los reguladores que sean descubiertos por el WCS.



2. Haga clic en el IP Address del regulador que usted quiere reajustar a los valores predeterminados de fábrica. La ventana de pPropiedades del regulador aparece.
3. Del menú del lado izquierdo, elija el **sistema > los comandos**.La ventana de los comandos controller

Cisco Wireless Control System

Monitor ▾ Configure ▾ Location ▾ Administration ▾ Help ▾

**Controllers**

**Properties**

**System** ▾

- General
- Commands
- Interfaces
- Mobility Groups
- Network Time Protocol
- QoS Profiles
- DHCP Scopes

**WLANs** ▸

**Security** ▸

**Access Points** ▸

**802.11** ▸

**802.11a** ▸

**802.11b/g** ▸

**Known Rogues**

**Ports**

**Management** ▸

**172.16.1.50 > Controller Commands**

**Administrative Commands**

-- Select a command -- ▾ **GO**

- Select a command --
- Reboot
- Save Config To Flash
- Reset To Factory Default**
- Ping From Controller

-- Select a command -- ▾ **GO**

**Upload/Download Commands**

-- Select a command -- ▾ **GO**

**RRM Commands**

-- Select a command -- ▾ **GO**

<b>Rogues</b>	0		<b>12</b>
<b>Coverage</b>			0
<b>Security</b>	0	0	0
<b>Controllers</b>	0	0	0
<b>Access Points</b>	0	0	0
<b>Location</b>	0		0

aparece.

4. Bajo órdenes administrativos seleccione **para reajustar al valor predeterminado de fábrica** y el tecleo **va**.
5. Elija la **reinicialización de los** comandos menu administrativos para reiniciar el regulador sin guardar la configuración en el regulador. Esto reajusta el regulador a los valores predeterminados de fábrica.**Nota:** Una vez que el regulador se reajusta a los valores predeterminados de fábrica, el WCS no puede descubrir el regulador a menos que se configure con el IP Address de administración. Para esto, usted necesita configurar el regulador que usa el comienzo encima del asistente de configuración en el regulador.



## Base de datos de Defragmenting WCS

Todas las operaciones regulares WCS, tales como la cancelación de las alarmas, de los eventos, de agregar/que borra los reguladores, del etc. implican las operaciones SQL internamente con la base de datos WCS (DB). Tales operaciones SQL internas aumentan naturalmente el tamaño de la base de datos, que, a su vez, tienen un impacto en el funcionamiento del WCS.

Por ejemplo, una operación de eliminación en el WCS deja el espacio vacío en las porciones borradas de la base de datos. Esto puede dar lugar a la ubicación discontinuas de los datos en la base de datos, que, a su vez, afecta al funcionamiento WCS. Base de datos de Defragment WCS para superar este problema.

El Defragmentation hace todo el haber utilizado y espacio sin usar contiguos. El inusitado/el espacio sin usar contiguos mejora el funcionamiento. Si usted defragment la base de datos, usted puede reclamar el espacio en disco afectado un aparato pero inusitado. Un defragmentation de la base de datos puede ser beneficioso si el espacio libre en disco en el sistema ejecuta bajo debido a un tamaño de la base de datos grande o si el tiempo de respuesta de la aplicación WCS es perceptiblemente más lento cuando los datos se preguntan ellos.

Para realizar el defragmentation manualmente en el WCS, pare la aplicación WCS. Para hacer esto, haga clic **Start > Programs > sistema de control inalámbrico > la parada WCS**. Entonces abra un cuadro de la línea de comando, cambian a **C:\Program Files\WCS4.0\bin** el directorio (el directorio predeterminado donde el WCS está instalado), y ejecutan el **defrag de DBAdmin** del comando. Esto inicia el proceso del defragmentation. Una vez que se completa el proceso, recomience el WCS con **Start > Programs > operación de la Tecnología inalámbrica > del sistema de control > del comienzo WCS**.

**Nota:** El Defragmentation trabaja automáticamente después de que los restores de la base de datos. No obstante, el defragmentation manual se hace en algunos casos para liberar para arriba un cierto espacio en disco. Un defrag manual no es realmente necesario. Ese espacio se recupera probablemente dentro de algunos días en que el WCS comienza a crear y a borrar las alarmas.

## Marque si usted tiene la licencia apropiada para el software WCS

La versión de software de red del Cisco Unified Wireless 4.0 aplica la autorización basada en software. Se indica a los clientes que ingresen los Certificados de la licencia por todas las nuevas familias de Cisco WCS SKU (excepto la licencia de la demostración de Cisco WCS). Autorizando afectan a los clientes actuales que emigran para liberar 4.0 también. La aplicación de la autorización de Cisco WCS se ata a estos parámetros:

- **Nombre del host** — El nombre del host del servidor de Cisco WCS ahora se requiere durante el proceso de inscripción. Las licencias publicadas se atan al nombre del host original señalado durante el proceso de inscripción.
- **Opción de la característica** — La opción de la característica de Cisco WCS comprada, baja o la ubicación, ahora es seguida por el sistema de autorización de Cisco WCS.
- **Puntos de acceso** — Los números de punto de acceso soportados en los incrementos del conjunto de 50, 100, 500, 1000, o 2500 ahora son seguidos por el sistema de autorización de Cisco WCS.
- **Licencia de la demostración** — Esta licencia libre, ubicación-habilitada de la demostración de Cisco WCS soporta 10 Puntos de acceso por hasta 30 días.

Refiera a [Cisco guía de autorización y que ordena WCS](#) para información más detallada sobre la licencia de Cisco WCS y los diversos tipos de licencias disponibles.

Seleccione la licencia correcta basada en su situación del despliegue, los números de punto de acceso que se soportarán, y las opciones de Cisco WCS (base o ubicación). Todo el SKUs dentro de una familia de SKU se puede combinar con los niveles equivalentes de la opción tales como Base-a-base o Ubicación-a-ubicación. Los niveles desiguales de la opción (base y ubicación) no pueden ser mezclados. Solamente un tipo de licencia puede ser utilizado en el WCS al mismo tiempo.

Por ejemplo, si su ordenador tiene una licencia de ubicación, usted no puede agregar una licencia baja. Usted puede agregar a la licencia actual comprando una licencia de aumentar la cuenta del Punto de acceso. Por ejemplo, si usted tiene una licencia de ubicación con una cuenta del Punto de acceso de 50 y en un año usted necesita agregar más Puntos de acceso, usted puede comprar otra licencia de ubicación con una cuenta del Punto de acceso de 100, aplicarla al WCS, y tener un WCS con una licencia de ubicación para 150 Puntos de acceso. Usted puede agregar una licencia de aumentar los números de punto de acceso en incrementos de 50, de 100, de 500, de 1000, de 2500, o de ilimitado.

Si usted tiene una licencia baja y quiere actualizar a una ubicación, usted necesita comprar un actualizar licencia de ubicación. Usted necesita comprar un actualizar licencia de ubicación equivalente al número total de Puntos de acceso con una licencia baja. Por ejemplo, si usted tiene tres licencias bajas con el soporte para 50, 100, y 200 Puntos de acceso (para un total de 350 Puntos de acceso), usted debe comprar un solo actualizar licencia de ubicación con el soporte para 350 Puntos de acceso.

Todo el Cisco WCS SKUs requiere un certificado del PAK registrar la licencia de Cisco WCS. El PAK es un certificado de papel enviado vía el correo E.E.U.U. de Cisco Systems sobre la compra de la licencia de Cisco WCS. El certificado del PAK permite que los clientes reciban una licencia de Cisco WCS. Se utiliza para registrar Cisco WCS y para generar los archivos de licencia. Todos los clientes deben ir al sitio del registro del PAK enumerado en su certificado del PAK para completar su registro de Cisco WCS. El certificado del PAK proporciona las instrucciones claras en cómo completar el Proceso de obtención de licencia de Cisco WCS.

Todos los clientes que compran Cisco WCS del cisco.com vía la descarga o el CD deben activar su licencia de Cisco WCS registrándose en el sitio del PAK. Los clientes recibirán el PAK vía el correo E.E.U.U. Cisco WCS no se activa hasta que se complete el proceso de inscripción del PAK. Refiera a las [licencias WCS](#) para la información sobre cómo instalar y manejar una licencia WCS.

### [Utilice la página de resumen de la Seguridad para resolver problemas](#)

La página de resumen de la Seguridad proporciona al usuario con la información sobre todos los eventos relacionados con la seguridad. Esta página proporciona la información sobre los puntos de acceso no autorizado, la información sobre los ataques de la firma, la información en los ataques en los Puntos de acceso, y relacionado con la información a la Seguridad del cliente.

Esta página es una herramienta del Troubleshooting eficaz específicamente si el problema se relaciona con las amenazas de seguridad. Esta página también proporciona la información sobre las alertas de seguridad más recientes.

Aquí está un ejemplo de la página de resumen de la Seguridad:

The screenshot displays the Cisco WCS Security Summary interface. It is divided into several sections:

- Summary:** Includes links for Rogue APs and Rogue Clients.
- Rogue AP Details:** A table showing the status of rogue access points.
 

Alert	Last Hour	24 Hours	Total Active
Alert	5	5	5
Contained	0	0	0
Threat	0	0	0
Contained Pending	0	0	0
Known Contained	0	0	0
Trusted Missing	0	0	0
802.11a	4	5	3
802.11b/g	9	10	2
On Network	0	0	0
Off Network	13	15	5
Adhoc	0	0	0
- Signature Attacks:** A list of detected attacks with their respective counts for the last hour, 24 hours, and total active instances.
 

Signature Attacks	Last Hour	24 Hours	Total Active
Custom	0	0	0
Assoc flood	0	0	0
Boast deauth	0	0	0
Broadcast Probe flood	0	0	0
Deauth flood	0	0	0
Disassoc flood	0	0	0
EAPOL flood	0	0	0
NULL probe resp 1	0	0	0
NULL probe resp 2	0	0	0
NetStumbler 3.2.0	0	0	0
NetStumbler 3.2.3	0	0	0
NetStumbler 3.3.0	0	0	0
NetStumbler generic	0	0	0
Reassoc flood	0	0	0
Res mgmt 6 & 7	0	0	0
Res mgmt D	0	0	0
Res mgmt E & F	0	0	0
Wellenreiter	0	0	0
- AP Threats/Attacks:** A list of specific threats and attacks.
 

AP Threats/Attacks	Last Hour	24 Hours	Total Active
Fake AP Attack	0	0	0
AP Missing	0	0	0
AP Impersonation	0	0	0
AP Invalid SSID	0	0	0
AP Invalid Preamble	0	0	0
AP Invalid Encryption	0	0	0
AP Invalid Radio Policy	0	0	0
Denial of Service (NAV related)	0	0	0
- Client Security Related:** A list of client-related security events.
 

Client Security Related	Last Hour	24 Hours	Total Active
Excluded Client Events	0	0	0
WEP Decrypt Errors	0	0	0
WPA MIC Errors	0	0	0
- IPSEC Failures:** A list of IPSEC-related failures.
 

IPSEC Failures	Last Hour	24 Hours	Total Active
	0	0	0
- Most Recent Security Alerts:** A section indicating that there are no security alerts in the system.
- Most Recent Rogue APs:** A table showing the most recent detected rogue access points.
 

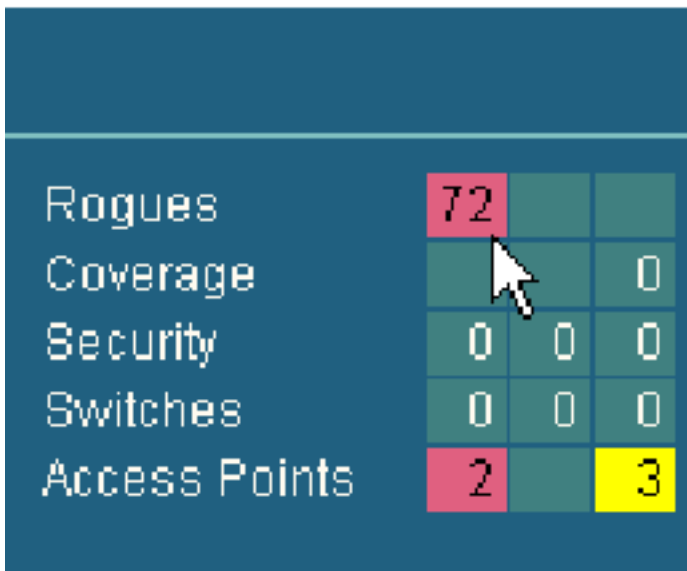
MAC Address	SSID	Type	State	Date/Time
00:0e:83:8b:fa:b0	ssid13	AP	Alert	7/19/06 5:32 AM
00:0c:bc:0d:04:26		AP	Alert	7/19/06 5:32 AM

The interface also includes a sidebar on the left with navigation options like 'Rogues Coverage', 'Security Controllers', 'Access Points', and 'Location'. A status bar at the bottom indicates the page was refreshed on Wed Jul 19 06:28:59 UTC+0530 2006.

## [Detecte y localice los puntos de acceso no autorizado](#)

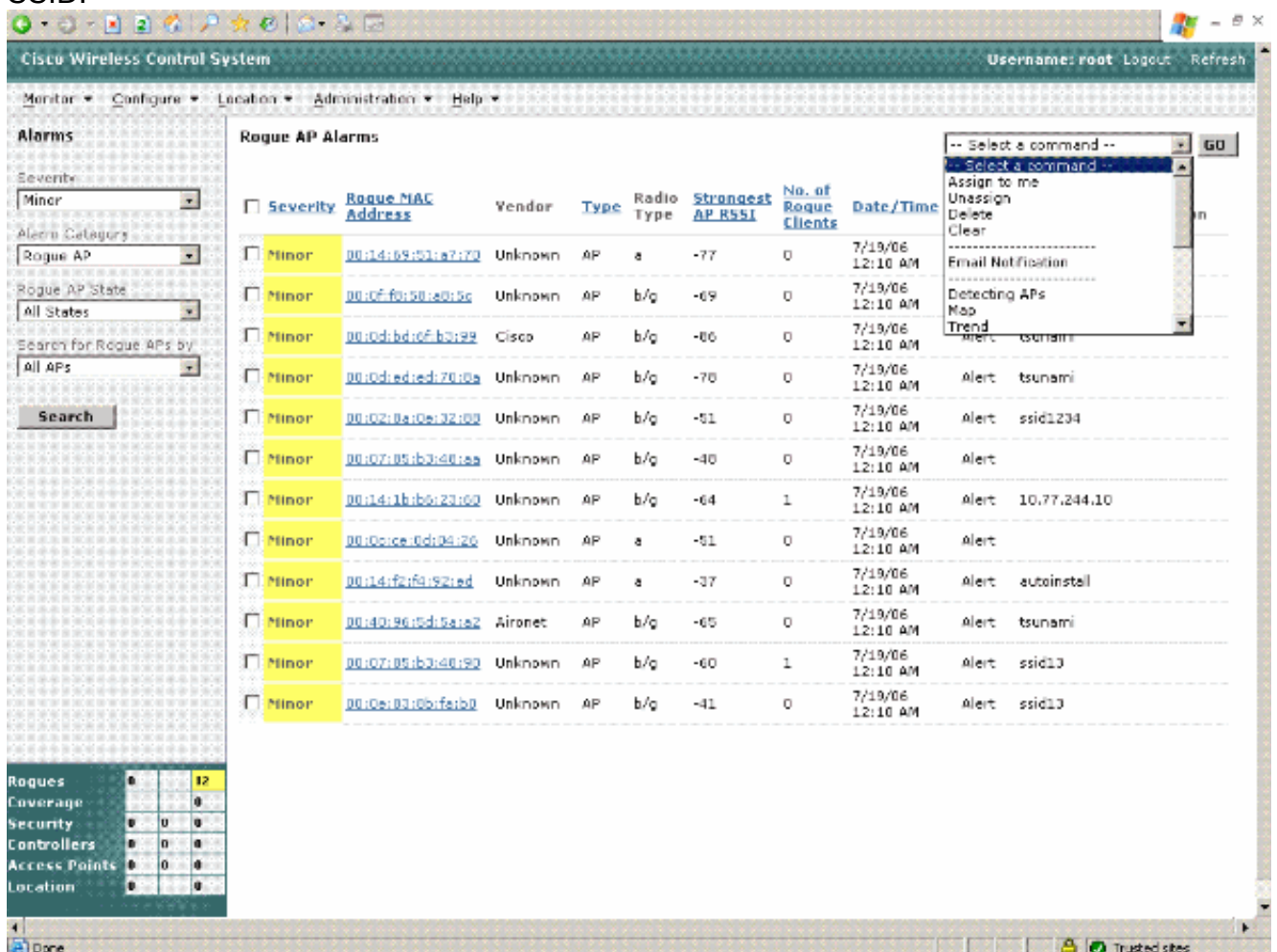
Cuando los revestimientos de Cisco se accionan para arriba y se asocian al WLCs de Cisco, Cisco WCS se incorporó al sistema operativo comienza inmediatamente a estar atentos los puntos de acceso no autorizado. Cuando un WLC de Cisco detecta un punto de acceso no autorizado, notifica inmediatamente Cisco WCS, que crea una alarma del punto de acceso no autorizado. El WCS considera cualquier Punto de acceso que no sea parte de su red inalámbrica como punto de acceso no autorizado.

Cuando Cisco WCS recibe un mensaje del punto de acceso no autorizado de un WLC de Cisco, Cisco WCS genera una alarma, con un indicador visible en la esquina de izquierda inferior de todas las páginas de la interfaz de usuario de Cisco WCS. Este ejemplo muestra 72 alarmas del punto de acceso no autorizado de Cisco WCS.



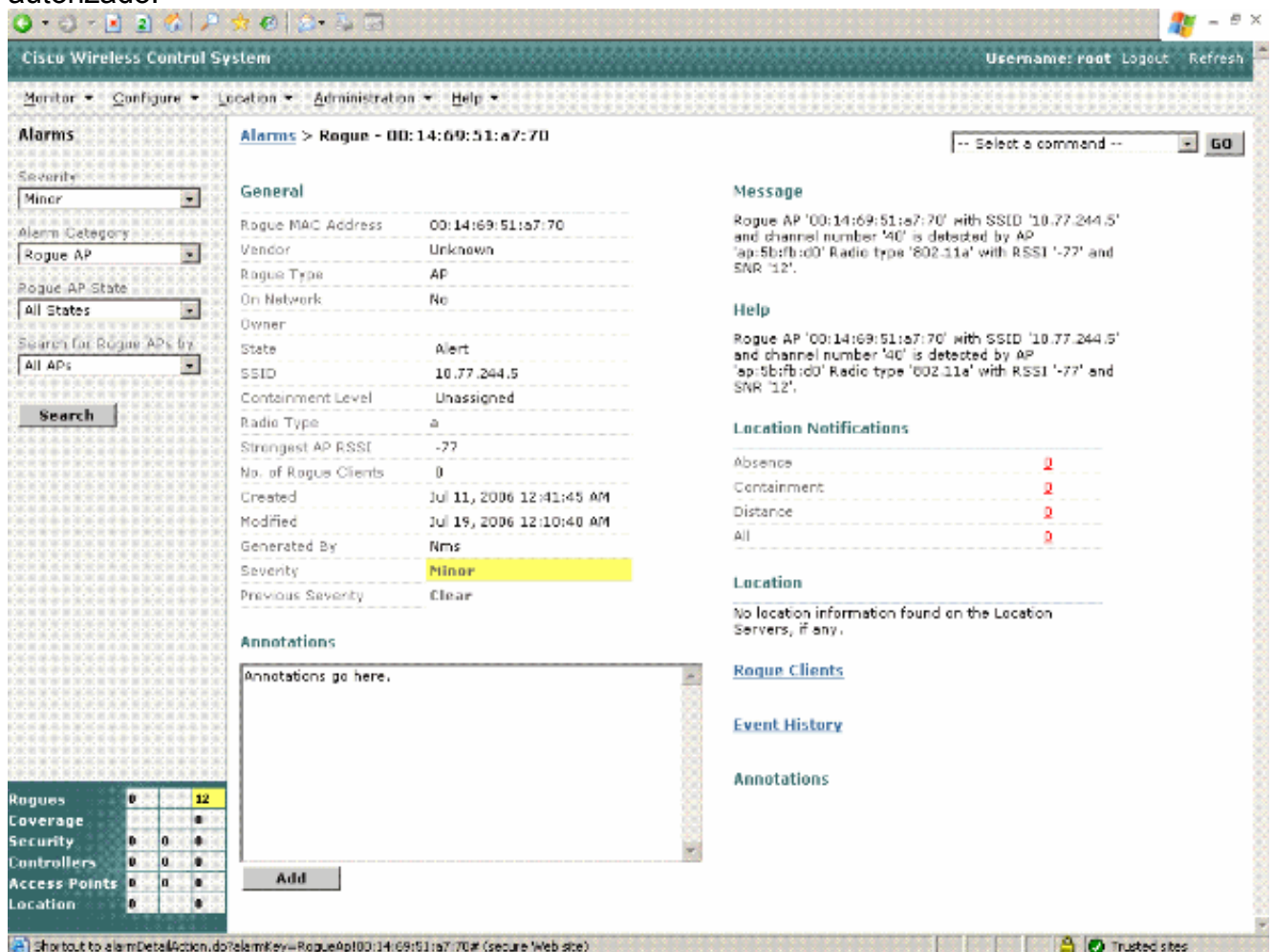
Complete estos pasos para detectar y localizar los puntos de acceso no autorizado:

1. Haga clic el indicador de los **granujas** para visualizar la página de las alarmas del granuja AP. Esta página enumera la gravedad de la alarma, las direcciones MAC del punto de acceso no autorizado, los tipos del punto de acceso no autorizado, la fecha y hora cuando los puntos de acceso no autorizado primero fueron detectados, y sus SSID.



2. Haga clic cualquier link rogue de la dirección MAC para visualizar las alarmas > al granuja asociados - página de la dirección MAC AP. Esta página muestra la información detallada sobre la alarma del punto de acceso no

autorizado.



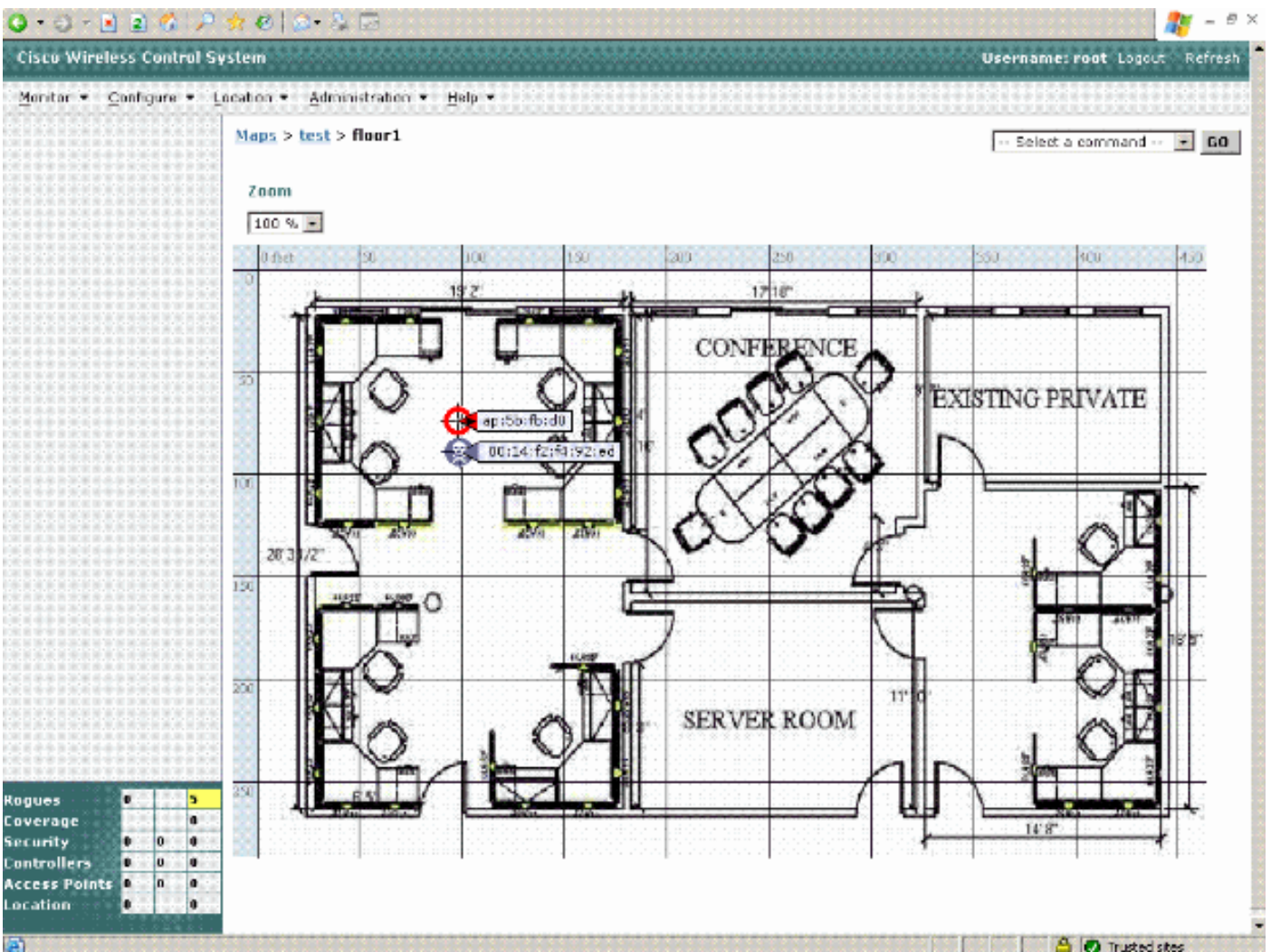
3. Elija uno de estos comandos del selecto un comando menu y el tecleo **VA** para modificar la alarma. **Asígneme** — Asigna la alarma seleccionada al Usuario usuario actual. **Unassign** — Unassigns la alarma seleccionada. **Cancelación** — Borra la alarma seleccionada. **Claro** — Borra la alarma seleccionada. **Historial de eventos** — Le permite para ver los eventos para las alarmas rogue. **Detectando los AP** (con la banda de radio, la ubicación, el SSID, el número de canal, el preámbulo del estado del Wired Equivalent Privacy (WEP), corto o largo, reciben el indicador de la potencia de la señal (RSSI), y el SNR) — le permite para ver los Puntos de acceso que detectan actualmente el punto de acceso no autorizado. **Cientes rogue** — Le permite para ver a los clientes asociados a este punto de acceso no autorizado. **Fije el estado al “desconocido - Alerta”** — Marca el punto de acceso no autorizado con etiqueta como la amenaza más baja, continúa monitoreando el punto de acceso no autorizado, y apaga la contención. **Fije el estado a “sabido - Interno”** — Marca el punto de acceso no autorizado con etiqueta como interno, lo agrega a los puntos de acceso no autorizado sabidos enumeran, y apagan la contención. **Fije el estado a “sabido - Externo”** — Marca el punto de acceso no autorizado con etiqueta como externo, lo agrega a los puntos de acceso no autorizado sabidos enumeran, y apagan la contención. **1 contención AP con la contención de 4 AP** — cuando usted selecciona la contención del nivel 1, un Punto de acceso cerca de la unidad rogue envía el deauthenticate y desasocia los mensajes a los dispositivos del cliente que se asocian a la unidad rogue. Cuando usted selecciona la contención del nivel 2, dos Puntos de acceso cerca de la unidad rogue envían el deauthenticate y desasocian los mensajes a los clientes del granuja y así sucesivamente hasta el nivel 4. es decir, que el Punto de acceso elegido para la contención evita que los clientes comuniquen al punto de acceso no autorizado. Esto neutraliza con eficacia la

función del punto de acceso no autorizado.

4. Va al selecto un menú desplegable del comando, elige el **mapa (de alta resolución)** y el tecleo **VA** para visualizar la corriente calculaba la ubicación del punto de acceso no autorizado en las correspondencias > la página del nombre del suelo del name> del edificio.

Si usted utiliza la ubicación WCS, el WCS compara la potencia de la señal RSSI a partir de dos o más Puntos de acceso para encontrar la ubicación más probable del punto de acceso no autorizado y coloca un pequeño indicador de la cráneo-y-bandera pirata en su ubicación más probable. En el caso de una red bajo-desplegada para la ubicación con solamente un Punto de acceso y una antena del omni, la ubicación más probable está en alguna parte en un timbre alrededor del Punto de acceso, pero el centro de la probabilidad está en el Punto de acceso.

Aquí está un ejemplo que muestra un punto de acceso no autorizado en una correspondencia:



Si usted utiliza la base WCS, el WCS confía en la potencia de la señal RSSI del punto de acceso no autorizado y coloca un pequeño indicador de la cráneo-y-bandera pirata al lado del Punto de acceso que recibe la señal más fuerte RSSI de la unidad rogue.

Con el dispositivo de la ubicación, los granujas pueden ser seguidos, se muestran en el menú desplegable del **monitor > del mapa**, y tienen el granuja AP de la demostración y muestran las opciones de clientes rogue. Sin el dispositivo de la ubicación, estas opciones no están presentes, y usted puede ver solamente la ubicación de los granujas cuando usted va a la alarma rogue y selecciona el comando **(de alta resolución) del MAPA** del menú desplegable.

En la base WCS, muestran el granuja al lado del AP de detección (no el más cercano), sin la

información sobre la ubicación. Para información más detallada sobre las características que se soportan en la base WCS y la ubicación WCS, refiera a la [comparación de la base WCS y de la ubicación WCS](#).

**Nota:** La versión de firmware 4.0 tiene bug Cisco ID [CSCse96812](#) ([clientes registrados solamente](#)) y [CSCsf17545](#) ([clientes registrados solamente](#)) las cuentas rogue de ese cliente de la demostración en ponen a cero siempre adentro la lista del punto de acceso no autorizado. La solución alternativa para este problema es considerar el punto de acceso no autorizado enumerar directamente en el regulador para las cuentas correctas.

## [Utilice la característica de la personificación del punto de acceso en el WCS](#)

La característica de la personificación AP mejora la detección del granuja AP que intenta personificar los revestimientos válidos de las Cisco 1000 Series. Esta característica crea a un grupo de red del Radiofrecuencia (RF), y los revestimientos de las Cisco 1000 Series en el mismo grupo distribuyen los paquetes vecinos del Administración de recursos de radio (RRM) el uno al otro. Si un REVESTIMIENTO de las Cisco 1000 Series oye los paquetes de otro REVESTIMIENTO de las Cisco 1000 Series del cual no ha recibido ninguna paquetes RRM vecina, después el REVESTIMIENTO de las Cisco 1000 Series puede asumir que el nuevo AP está personificando las Cisco 1000 Series TRASLAPA y por lo tanto lo señala como granuja AP.

Cuando el WCS encuentra un AP que intente personificar otro AP en la red inalámbrica (WLAN), usted ve esta alerta en el servidor WCS:

```
AP Impersonation with MAC '00:14:1b:62:4e:42' is detected by authenticated
AP '00:14:1b:62:4e:40' on '802.11b/g' radio and Slot ID '0'
```

En el regulador, este mensaje del registro del desvío muestra el MAC Address de origen que causa el problema:

```
Apr 10 11:21:16 <SomeIPAddress> [WARNING] apf_rogue.c 1890: Possible AP
impersonation of 00:14:1b:62:4e:42, using source
address of 00:90:4b:8a:de:c3, detected by 00:14:1b:62:4e:40 on slot 0.
```

Refiera al Id. de bug Cisco [CSCsb90622](#) ([clientes registrados solamente](#)) para más información sobre los registros de error relacionados personificación AP WCS.

La personificación AP es señalada por el IDS cuando usted ve un AP que haga publicidad de una dirección MAC de Cisco que no comunique con el protocolo del Lightweight Access Point (LWAPP) o el Control Protocol del contexto del Wireless LAN (WLCCP). En el modelo del LWAPP, el WCS puede asociar una ubicación aproximada de un granuja AP de la interpretación del regulador de todas las lecturas AP.

## [Localice a los clientes](#)

Cisco WCS permite que los operadores del sistema localicen a los clientes en la empresa. Complete estos pasos:

1. Elija el **monitor > los dispositivos > a los clientes** para navegar a la página de resumen de los clientes.

The screenshot displays the Cisco WCS interface. On the left sidebar, there are several status indicators:

Rogues	0	0	5
Coverage	0	0	0
Security	0	0	0
Controllers	0	0	0
Access Points	0	0	0
Location	0	0	0

The main content area is titled "Clients Summary". It includes a search section on the left with filters for "All Clients", "WCS Controllers", and "All States". The "Most Recent Excluded Clients" section shows "No Excluded clients found." The "Manually Disabled Clients" section is empty. The "Top 5 APs" section contains the following table:

AP Name	Map Location	a Clients	b/o Clients	Total
ap-5b:f:d0	test > floor1	1	1	2

The "Clients Detected by Location Servers (in last 15 minutes)" section is empty. On the right, the "Clients" section features a line graph titled "Associated Clients vs. Time". The graph shows a client count of 0 until approximately 4:30 AM on 07/19, where it spikes to 2 and remains constant until 6:00 AM.

- En la página de resumen de los clientes, en la barra lateral izquierda, búsqueda para **todos los clientes** para tener visualización de Cisco WCS que los clientes paginan.



The screenshot shows the Cisco Wireless Control System (WCS) interface. The main content area displays a table of clients. The table has the following columns: User, Vendor, IP Addr, MAC Addr, AP, Controller, Port, 802.11 State, SSID, Authenticated, and Protocol. Two clients are listed:

User	Vendor	IP Addr	MAC Addr	AP	Controller	Port	802.11 State	SSID	Authenticated	Protocol
<none>	Unknown	0.0.0.0	00:0f:f8:4f:5a:a8	ap:5b:fb:d0	172.16.1.50	1	Associated	CCC	No	802.11b
<none>	Aironet	172.16.1.87	00:40:96:ac:dd:05	ap:5b:fb:d0	172.16.1.50	1	Associated	CCC	Yes	802.11a

On the left side, there are search filters: 'Search for clients by' set to 'All Clients', 'Search in' set to 'WCS Controllers', and 'Client States' set to 'Associated'. There is also an 'Include Disassociated' checkbox which is unchecked. A 'Search' button is located below these filters. At the bottom left, there is a dashboard with various metrics: Rogues (0), Coverage (0), Security (0), Controllers (0), Access Points (0), and Location (0).

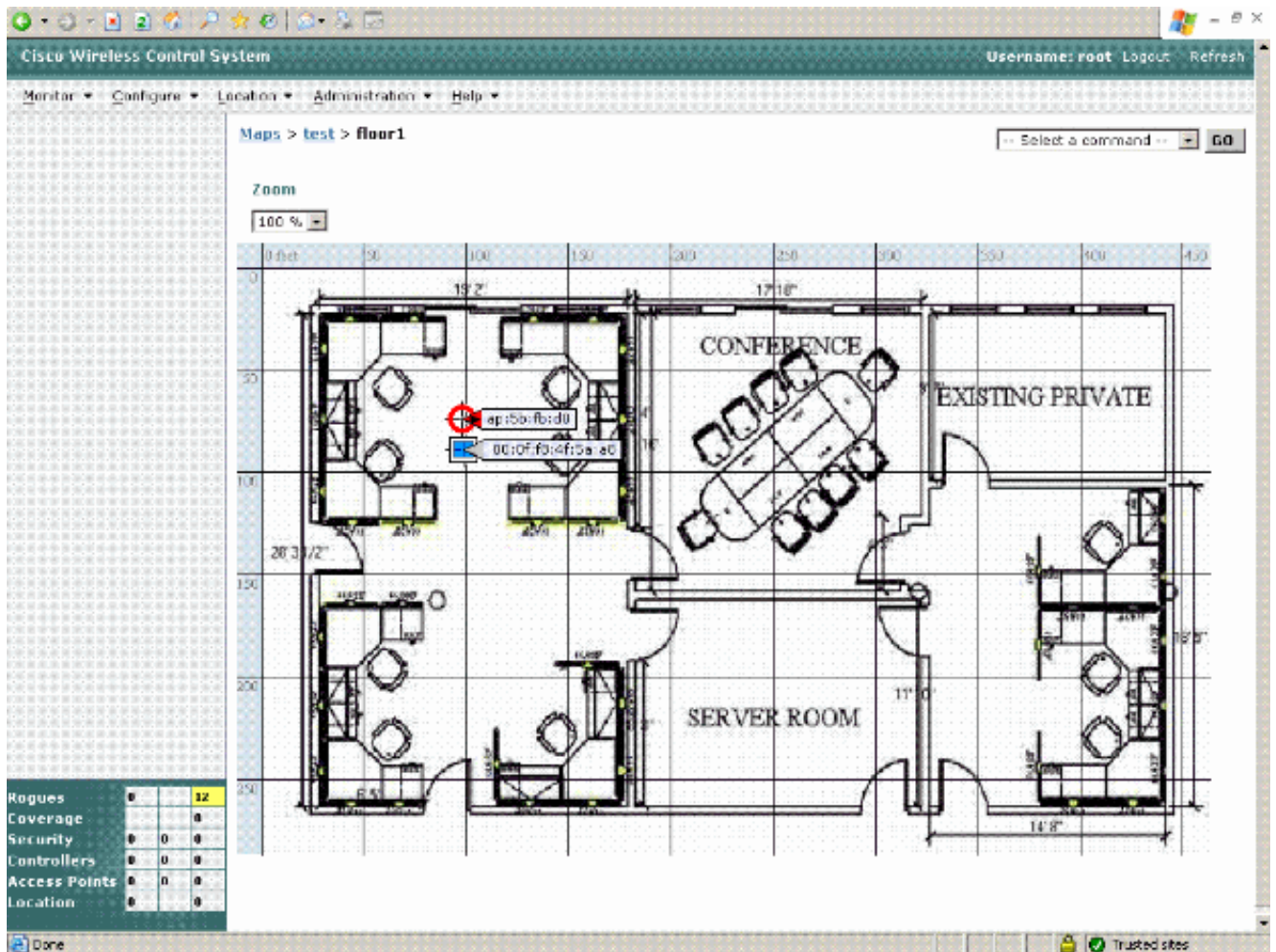
- De la página de los clientes, haga clic el Nombre de usuario del cliente que usted quiere localizar. Cisco WCS visualiza la página <client correspondiente del name> de los clientes.

The screenshot displays the Cisco WCS interface for a specific client. The client is identified as 'unknown' - Aironet: ac:dd:05. The interface is divided into several sections:

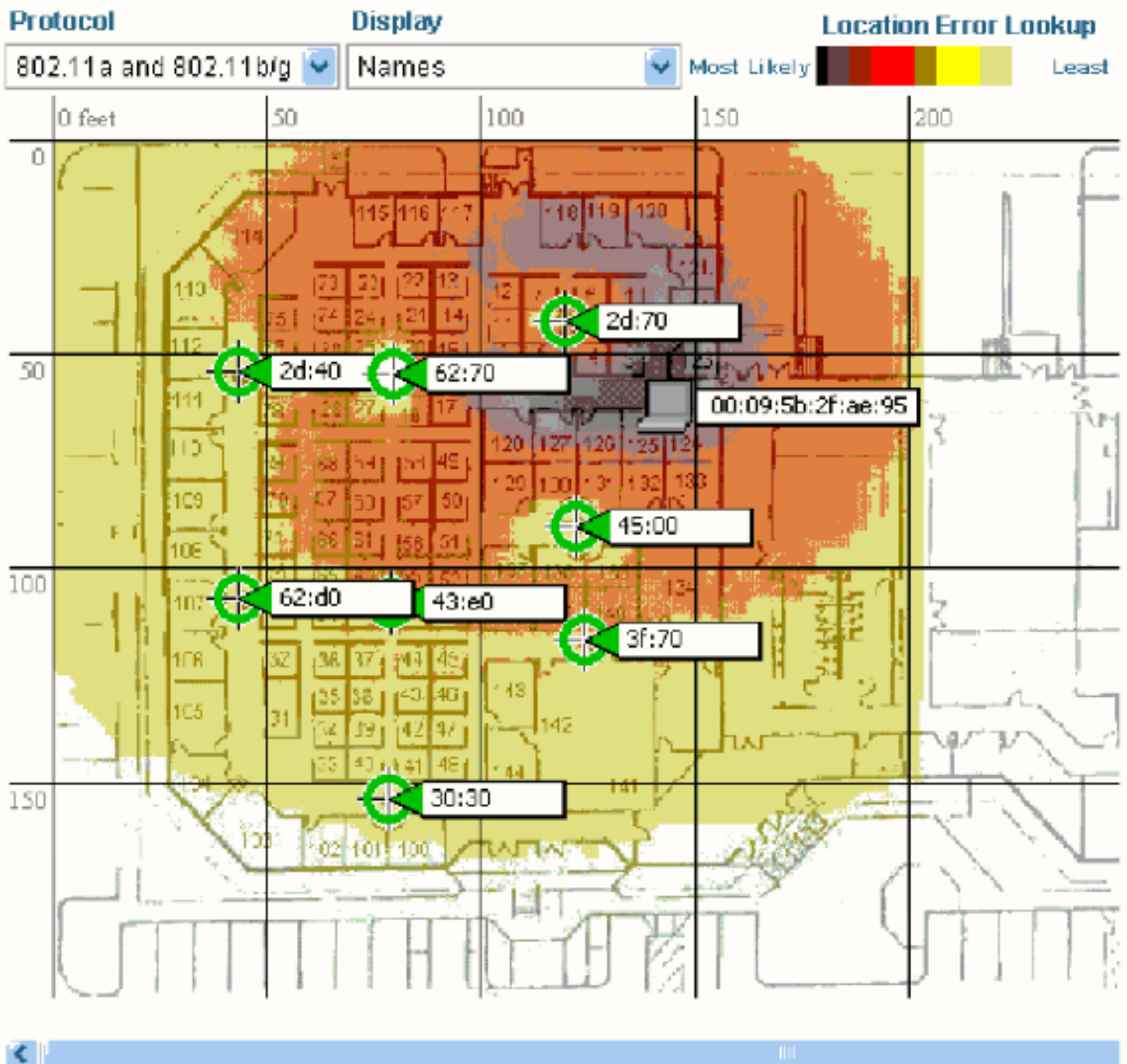
- Client Properties:**
  - Client User Name: (empty)
  - Client IP Address: 172.16.1.87
  - Client MAC Address: 00:40:96:ac:dd:05
  - Client Vendor: Aironet
  - Controller: 172.16.1.50
  - Port: 1
  - Interface: management
  - VLAN ID: 0
  - 802.11 State: Associated
  - Mobility Role: Unassociated
  - Policy Manager State: RUN
  - Anchor Address: 0.0.0.0
- Client Location:**
  - No Location Information. Client is not detected by any Location Server.
- Client Statistics:**
  - Bytes received: 1036116
  - Bytes sent: 13955162
  - Packets received: 11016
  - Packets sent: 13286
  - Policy errors: 0
  - RSSI: -61 dBm
  - SNR: 29
  - Sample Time: (empty)
  - Excessive Retries: 0
  - Retries: 0
  - TX Filtered: 0
- Asset Info:**
  - No Information. Client is not detected by any Location Server.
- AP Properties:**
  - AP Name: ap:5b:fb:d0
  - AP Type: Cisco AP
  - AP Base Radio MAC: 00:0b:85:5b:fb:d0
  - Protocol: 802.11a
  - AP Mode: local
  - SSID: CCC
  - Association Id: 1
  - Reason Code: None
  - 802.11 Authentication: OPENSYSYSTEM
  - Status Code: 0
  - CF Pollable: Not Implemented
  - CF Poll Request: Not Implemented
  - Short Preamble: Not Implemented
  - PBCC: Not Implemented
  - Channel Agility: Not Implemented
  - Timeout: 0
  - WEP State: ENABLE
- Location Notifications:**
  - Absence: 0
  - Containment: 0
  - Distance: 0
  - All: 0
- Security Information:** (empty)

On the left sidebar, there is a search filter set to 'Associated' and a 'Search' button. At the bottom left, there is a 'Rogues' table with columns for Coverage, Security, Controllers, Access Points, and Location, all showing 0 counts.

4. De la página <client del name> de los clientes, usted tiene dos opciones para localizar al cliente: En el menú desplegable, seleccione el **mapa reciente** (resolución alta-baja) para localizar al cliente sin la desasociación de él. En el menú desplegable, seleccione el **actual mapa** (resolución alta-baja) para desasociar y después localizar al cliente después de la reasociación. Si usted toma esta decisión, Cisco WCS visualiza un mensaje de advertencia y pide que usted confirme que usted quiera continuar. Aquí tiene un ejemplo:



Refiera a este ejemplo para un mapa del calor que muestre las ubicaciones del cliente.



**Nota:** La ubicación de Cisco WCS compara la potencia de la señal RSSI a partir de dos o más Cisco 1000 Series traslapa para encontrar la ubicación más probable del cliente, y pone un pequeño icono de la laptop en su ubicación más probable. La base de Cisco WCS compara la potencia de la señal RSSI del cliente, y pone un pequeño icono de la laptop al lado de las Cisco 1000 Series TRASLAPA que reciba la señal más fuerte RSSI del cliente.

**Nota:** Generalmente, cuando usted apaga su laptop, tarda un tiempo prolongado (en los minutos) antes de que el WLC o el WCS quite al cliente de la lista de los clientes. Continúa mostrando que “se asoció”. Esto es porque hay dos temporizadores que controlan el tiempo de inactividad y el tiempo de espera de la sesión llamados información de la asociación de los usuarios. Ambos temporizadores pueden ser cambiados. Éstos son los temporizadores predeterminados:

- Tiempo de inactividad — (300 segundos)
- Tiempo de espera de la sesión — (1800 segundos)

## [Agujeros de la cobertura en una red WLAN](#)

Los agujeros de la cobertura son las áreas donde los clientes no pueden recibir una señal de la red inalámbrica. El Administración de recursos de radio (RRM) del sistema operativo identifica estas áreas del agujero de la cobertura y las señala a Cisco WCS. Esto permite que el administrador TIC llene los agujeros basados en la demanda del usuario.

Cuando Cisco WCS visualiza los 5 agujeros superiores de la cobertura, haga clic el indicador de la **cobertura** en el extremo inferior izquierdo de la página de la interfaz de usuario de Cisco WCS (o elija los **>Alarms del monitor** y después busque para la **categoría de la alarma - cobertura**) para tener visualización de Cisco WCS que las alarmas del agujero de la cobertura paginan. En las alarmas del agujero de la cobertura pagine, elija el **monitor > las correspondencias** y después busque para los Puntos de acceso por el nombre de los revestimientos de las Cisco 1000 Series (esta Herramienta de búsqueda es con diferenciación entre mayúsculas y minúsculas). Cisco WCS visualiza la página de las correspondencias > de los resultados de la búsqueda, que enumera el suelo o el área al aire libre donde se localiza el REVESTIMIENTO de las Cisco 1000 Series. Haga clic el link para visualizar las correspondencias relacionadas > name> > página <building del <floorname>.

En las correspondencias > el name> > la página <building del name> del <floor, buscan las áreas de la potencia de la señal baja cerca de las Cisco 1000 Series TRASLAPAN que señalado el agujero de la cobertura. Ésas son las ubicaciones más probable de los agujeros de la cobertura. Si no aparecen ser ninguna áreas de la potencia de la señal débil, aseegurese que la correspondencia del plan de piso es exacta. También, si usted ha utilizado el editor del plan de piso para crear los archivos .FPE, que usted no ha dejado hacia fuera ninguna obstrucciones del metal, tales como paredes, ejes de elevador, escaleras, o estantes para libros. Si es así agreguelos al archivo del plan de piso .FPE y substituya el viejo plan de piso por el nuevo plan de piso.

## [Si usted tiene dificultades cuando usted importa las correspondencias](#)

Cisco WCS permite al usuario para ver la red WLAN manejada en el campus, el edificio, y las correspondencias realistas del plan de piso. Usted puede importar el suelo, el campus, o el plan del edificio a Cisco WCS mientras que un archivo de imagen y usted pueden agregar los dispositivos en las ubicaciones apropiadas. Cisco WCS apoya estos tipos de imagen:

- Formato del .PNG
- Formato .JPG
- Formato .JPEG
- Formato .GIF

Si usted hace frente a un problema cuando usted importa las correspondencias a Cisco WCS, podría ser debido a un formato sin apoyo de la imagen. Para resolver este problema, abrir la imagen con la pintura de Microsoft y salvar el archivo como **<filename>.GIF**. Entonces intento para importar la imagen otra vez.

A veces, el archivo de imagen importado puede visualizar en el WCS con mismo la baja calidad, aunque el archivo de imagen original está de alta calidad. Una razón posible de este problema está con la imagen sí mismo. El WCS incorpora el espacio blanco que rodea la imagen bajo suposición que es parte de la correspondencia; esto puede llevar a la calidad de la visualización de los pobres en el editor de la correspondencia WCS. Intente cosechar el archivo de imagen para quitar el espacio blanco y después para importar la nueva imagen en el WCS.

Refiera a [agregar y a usar las correspondencias](#) para información detallada sobre agregar las correspondencias a Cisco WCS.

## [Haga ping un dispositivo de red de un WLC de Cisco](#)

Complete estos pasos para hacer ping los otros dispositivos de un WLC de Cisco:

1. Elija la **configuración > los reguladores** y haga clic una dirección IP bajo la columna de la dirección IP para tener visualización de Cisco WCS <ipaddress> > las propiedades del regulador paginan.
2. En <ipaddress> > el regulador que las propiedades paginan, que van a la barra lateral izquierda y que eligen el **sistema > los comandos** tener visualización de Cisco WCS <ipaddress> > los comandos controller pagina.
3. En <ipaddress> > los comandos controller paginan, eligen los **órdenes administrativos > el ping del Switch** y el tecleo **VA**.
4. En el ingresar un IP Address (x.x.x.x) hacer ping la ventana, ingrese el IP Address del dispositivo de red que el WLC de Cisco es hacer ping, y hace clic la **AUTORIZACIÓN**.
5. Cisco WCS visualiza la ventana de resultados del ping que muestra los paquetes enviados y recibidos. Haga clic el **reinicio** para hacer ping el dispositivo de red otra vez, o haga clic **cerca** para parar el hacer ping del dispositivo de red y cerrar la ventana de resultados del ping.

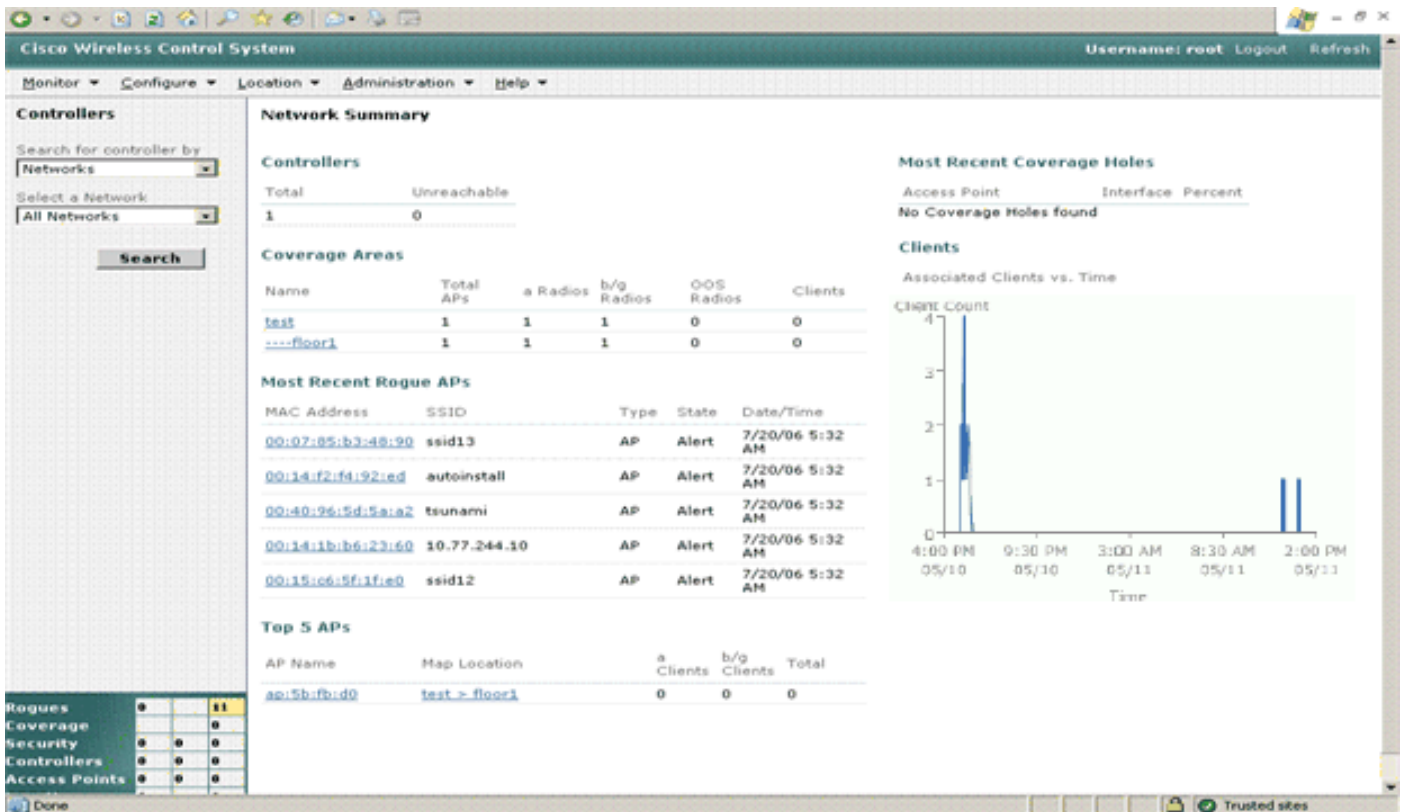
## [Vea el estatus, las configuraciones, y las estadísticas actuales del WLC de Cisco](#)

Después de que usted agregue el WLCs de Cisco y las Cisco 1000 Series IEEE 802.11a/b/g traslapan a Cisco WCS la base de datos, usted puede ver el estatus de la solución de Cisco WLAN.

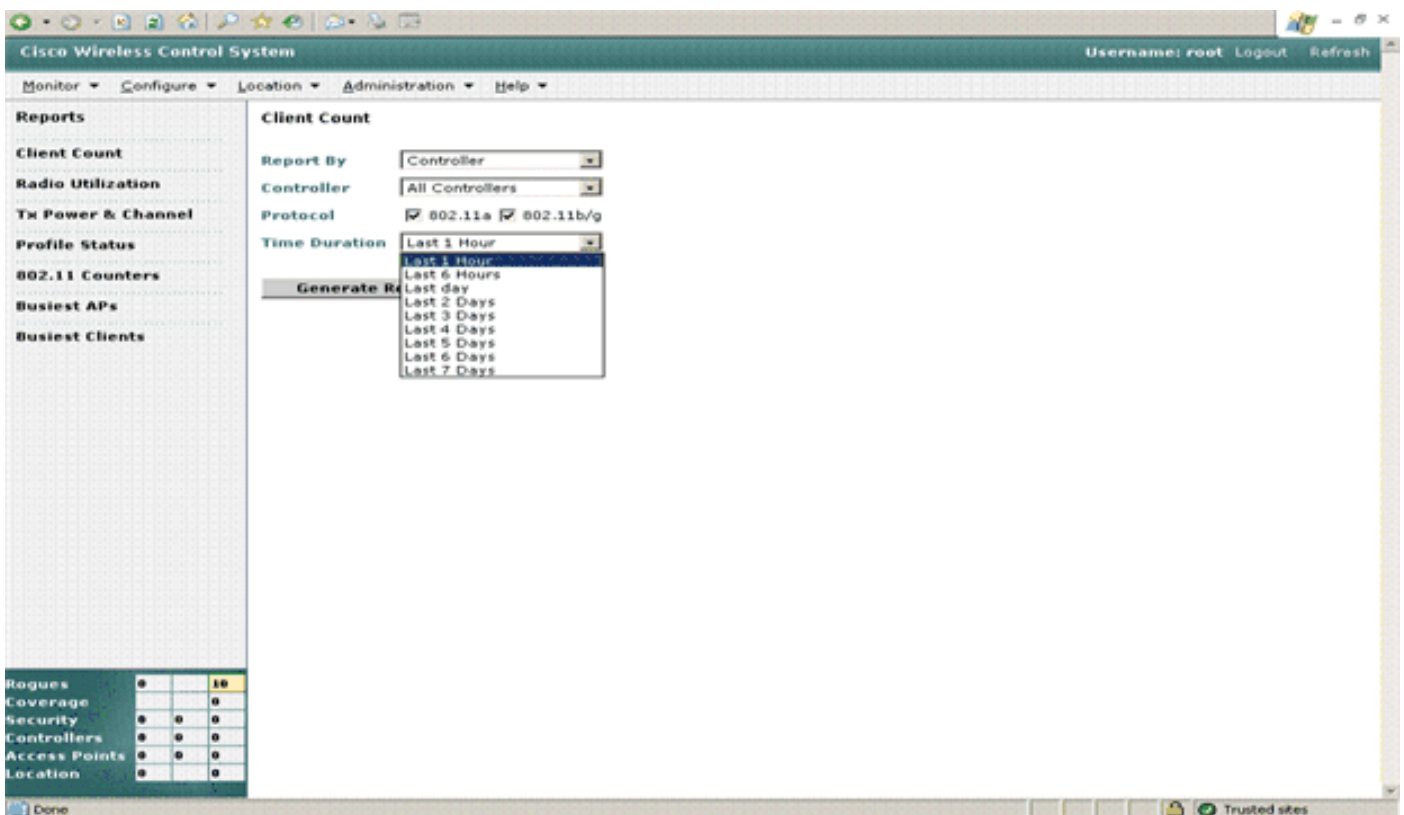
**Nota:** Cuando usted busca para los clientes o las etiquetas sin un dispositivo de la ubicación, usted necesita especificar los reguladores del WLC en la base de datos WCS. Esto es porque el WCS omite siempre los “servidores de la ubicación”.

**Nota:** La aplicación WCS debe ser parada manualmente apaga antes de que usted realice cualquier cambio al dirección IP del servidor. Si usted reinicia el servidor sin la detención de la aplicación, después hay las ocasiones que la base de datos pudo conseguir corrompida.

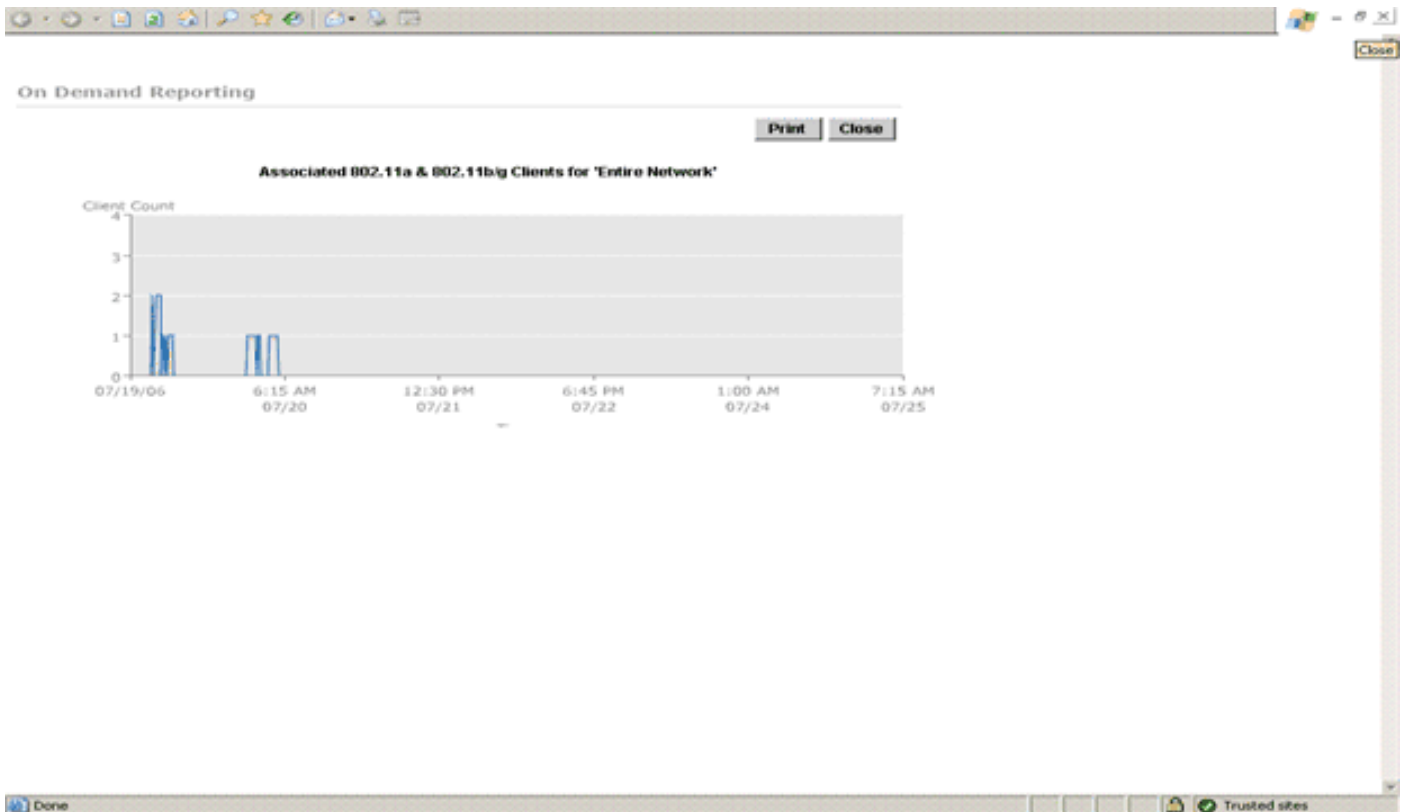
En la interfaz de usuario de Cisco WCS, elija el **monitor > la red** para visualizar el resumen de la red del monitor. Aquí tiene un ejemplo:



Cisco WCS recoge periódicamente las estadísticas, tales como RSSI, SNR, los errores del perfil, el cliente cuenta, el punto de acceso no autorizado tiende, y los clientes ocupados, y las ordena en los informes. Utilice las ventanas del **monitor > de los informes** para ver estos informes.



Aquí está un ejemplo del informe de la cuenta del cliente para los clientes 802.11a/b/g para los siete días más pasados:



Estos informes se pueden también utilizar como herramienta del Troubleshooting eficaz.

## [Examine la disposición de la ubicación](#)

El examen de la disposición de la ubicación es una característica introducida en la versión 2.1.34.0 del dispositivo de la ubicación. Con esta característica, el WCS puede verificar la capacidad del despliegue existente del Punto de acceso de estimar la ubicación verdadera de un elemento a 10 contadores por lo menos de 90% del tiempo. El cálculo de la disposición de la ubicación se basa en el número y la colocación de los Puntos de acceso.

Para examinar la disposición de la ubicación del WCS, elija **examinan la disposición de la ubicación del** menú encontrado en la página del **monitor > de las correspondencias**. Una correspondencia con código de color aparece que muestra esas áreas que lo hagan (sí) y (no) no resuelvan los 10 contadores, especificación de la ubicación del 90%.

## [Problemas de sincronización con los servidores WCS y de la ubicación](#)

A veces pudo haber problemas con el WCS que conseguía sincronizado con el dispositivo de la ubicación. El diagrama de la red en el WCS no pudo sincronizar con el dispositivo de la ubicación. Hay muy algunas razones por este problema de sincronización.

- El tamaño del diseño de red pudo haber excedido el límite máximo de 30 Mb. El Id. de bug Cisco [CSCse60657](#) ([clientes registrados solamente](#)) aborda este problema más claramente. Por lo tanto, mientras que usted intenta sincronizar un diagrama del campus cuyo tamaño total, incluyendo el número de interior de los edificios que el campus y el número de suelos en cada edificio, en un conjunto pudieron haber excedido el límite máximo de 30 Mb, este proceso de la sincronización falla. Este problema puede ser verificado más a fondo cuando usted ve los registros del dispositivo de la ubicación para este mensaje. `TRACE[ com.aes ]  
THROW com.aes.server.cmn.AesServerException:`



Server Exception: Message sizeexceeded: 37176782 Esta limitación de tamaño se supera en la versión próxima WCS.

- Otra razón posible es que la resolución de la imagen cargada en el WCS es demasiado alta, y excede probablemente la resolución aceptable de 1024x768. Mientras que intenta sincronizar tal imagen con el dispositivo de la ubicación, el proceso de la sincronización falla. En estos casos, reduzca la resolución para ayudar a este problema.
- Asegúrese de que usted funcione con la última versión en su servidor WCS y de la ubicación. También asegúrese de que la coincidencia de la Fecha y hora exactamente en todos los dispositivos. Esto puede ser verificada cuando usted mira estas salidas. Salida del comando de la **fecha y hora** en el WCS Salida de la **fecha** en el locserver Salida del **comando show time** en el WLC
- Otro remedio posible es parar el ubicación-servidor, y quita la base de datos usando este comando en la consola del servidor de la ubicación: **rm - rf /opt/locserver/db/linux/server-eng.db** donde está el directorio **/opt/locserver/db/linux/server-eng.db** para el DB del ubicación-servidor. Recomience el servidor de la ubicación con el **reinicio de /etc/rc.d/init.d/locserver** del comando. Entonces intente resincronizar los dispositivos.

## Problemas de sincronización con el WCS y el WLC

Los problemas de sincronización pudieron ocurrir entre el WCS y el WLC. Debido a este problema, el número de clientes activos pudo ser diferente en el WLC y el WCS. Para sincronizar los reguladores y el WCS, complete estos pasos:

1. Elija la **configuración > los reguladores**, y haga clic la casilla de verificación en la cima de la lista de IP Address para elegir todos los reguladores.
2. Del selecto una lista desplegable del comando, elige los **Config de la salvaguardia para contellear**.
3. Haga clic en OK. Esto es una prueba básica a verificar que el SNMP trabaja correctamente, y los reguladores harán como el WCS les dice.
4. Elija la **configuración > los reguladores**, y haga clic la casilla de verificación en la cima de la lista de IP Address para elegir todos los reguladores.
5. Del selecto una lista desplegable del comando, elige **restaura los Config de los reguladores**.
6. Haga clic en OK. Esta acción dice el WCS creer que la nueva información de los reguladores sobre cualquier cosa que había sabido previamente.

## Configuración DHCP corrompida cuando la plantilla se avanza del WCS a WiSM

Cuando una plantilla general se avanza del WCS al módulo de Servicios inalámbricos (WiSM), la configuración del Protocolo de configuración dinámica de host (DHCP) en el regulador se corrompe. La plantilla puede tener exactamente las mismas opciones que están presentes en el WiSM.

El efecto principal es que los mensajes de la oferta de DHCP están caídos, así que los clientes no reciben un DHCP Address. Este mensaje se abre una sesión el regulador:

```
Thu Jul 13 05:05:07 2006 [VERBOSE] dhcpd.c 164: Dropping packet from  
192.168.80.23 (unable to match to a dhcp scope)
```

Este problema es debido al Id. de bug Cisco [CSCse98623](#) ([clientes registrados solamente](#)). No utilice las plantillas generales en el WCS. La configuración tiene que ser restablecida

manualmente para recuperar el envío del DHCP. Este bug se repara en la versión de firmware 4.0.87.0 WCS y posterior.

## [Las correspondencias del calor WCS muestran los agujeros cuadrados incorrectos de la cobertura](#)

Las correspondencias del calor WCS muestran los agujeros cuadrados incorrectos de la cobertura. Los agujeros de la cobertura deben nunca ser cuadrados o rectángulo. El patrón de radiación de la correspondencia del calor es circular. Este problema es una perforación rectangular específica en la correspondencia, que no debe ser posible. No se ha realizado el ningún editar de la traza en la correspondencia. Con el uso de una herramienta del topógrafo del sitio, se verifica que existe ningún agujero de la cobertura. La conexión es muy fuerte en estas áreas.

Esto se relaciona con el Id. de bug Cisco [CSCsf19291](#) ([clientes registrados solamente](#)). Elija la **predicción del recálculo de la** opción del menú desplegable y recalcula la predicción. La correspondencia del calor se convierte en circular y ningunos agujeros cuadrados de la cobertura existen. Este problema se repara en la versión 4.0, pero si usted emigra de la versión 3.0 entonces el problema pudo existir para los suelos tamaño pequeño.

## [¿Cuándo la plantilla del granuja AP consigue aplicada al WLC?](#)

La plantilla del punto de acceso no autorizado (AP) consigue aplicada al regulador solamente si estas dos condiciones son verdades:

- El AP en ese regulador ha descubierto al granuja AP.
- Se completa la tarea del horario del granuja AP.

## [Puertos en el servidor WCS](#)

Cuando usted ejecuta un Firewall en el servidor adonde la aplicación WCS se ejecuta, usted necesita abrir algunos puertos para comunicar con el WLC. Hay algunos servicios que se ejecutan en los servidores WCS tales como Apache.exe, JavaService.exe, y Solid.exe. En TCPView, la salida aparece similar a esta salida:

```
Apache.exe:1712 TCP 0.0.0.0:443 0.0.0.0:0 LISTENING
JavaService.exe:1680 TCP 0.0.0.0:21 0.0.0.0:0 LISTENING
solid.exe:2672 TCP 0.0.0.0:1315 0.0.0.0:0 LISTENING
```

```
Apache.exe:208 TCP 127.0.0.1:1268 127.0.0.1:8009 ESTABLISHED
JavaService.exe:1680 TCP 127.0.0.1:1067 127.0.0.1:1315 ESTABLISHED
JavaService.exe:1680 TCP 127.0.0.1:1068 127.0.0.1:1315 ESTABLISHED
solid.exe:2672 TCP 127.0.0.1:1315 127.0.0.1:1083 ESTABLISHED
solid.exe:2672 TCP 127.0.0.1:1315 127.0.0.1:1082 ESTABLISHED
```

Para trabajar con el WLC, abra solamente algunos puertos como el (SNMP) UDP 161, UDP 162 (SNMP trap), y TCP 443 (HTTPS). Esta tabla muestra una lista de puertos cuál pudo ser útil si algo del tráfico se bloquea.

Servicio	Puertos	Números de puerto
SNMP	UDP	161
SNMP trap	UDP	162

HTTPS	TCP	443
Red del advenimiento	TCP	2000
Base de datos	TCP	1315
FTP	TCP	21
Conector HTTP	TCP	8457
El conector HTTP reorienta	TCP	8457
HTTP	TCP	80
RMI	TCP	1299
TFTP	UDP	69
Envase de la red	TCP	8009

### [Verifique los WLAN son permiso fijado de la exclusivo-lista](#)

Complete estos pasos para verificar que los WLAN son **permiso** fijado de la exclusivo-lista.

1. Elija la **configuración > el regulador**.
2. Haga clic en un IP Address bajo la columna del IP Address.
3. Haga clic la **red inalámbrica (WLAN)** a la izquierda.
4. Haga clic en cada ID DE WLAN para verificar que no está fijado a **marcado**.

### [Resuelva problemas el permiso de la exclusivo-lista](#)

Complete estos pasos para resolver problemas el **permiso de la exclusivo-lista**.

1. Siga al cliente.
2. Verifique la red inalámbrica (WLAN) para el cliente de la exclusión.
3. Seleccione al cliente exclusivo **borrar**.
4. Borre a los clientes de la exclusivo-lista bajo el regulador especificado.

### [Vea y borre a los clientes global discapacitados](#)

Complete estos pasos para ver y borrar a los clientes global discapacitados.

1. Elija el **monitor > los dispositivos > a los clientes**.
2. Haga clic **manualmente a los clientes discapacitados**.
3. Seleccione la dirección MAC para acceder esta página.
4. Haga clic la **cancelación**.

### [Vea y borre manualmente a los clientes discapacitados por el regulador](#)

Por motivos de seguridad y varias otras razones, ciertos clientes pueden ser puestos como "clientes manualmente discapacitados".

Complete estos pasos para ver manualmente a los clientes discapacitados individualmente en cada regulador agregado al WCS:

1. Vaya al WCS GUI.
2. Elija la **configuración > los reguladores**.
3. Haga clic en el IP Address bajo la columna del IP Address para el regulador al cual los clientes discapacitados necesitan manualmente ser vistos.
4. En la página que aparece, elija la **Seguridad** y haga clic **manualmente a los clientes discapacitados** para visualizar la lista de clientes manualmente discapacitados para este regulador determinado.

Del menú desplegable a la izquierda, elija a los **clientes discapacitados de la cancelación manualmente** para borrar manualmente a los clientes discapacitados.

## [La búsqueda WCS para los clientes por el edificio no trabaja](#)

Este problema puede ser debido al Id. de bug Cisco [CSCse97619](#) ([clientes registrados solamente](#)). Una búsqueda WCS para los clientes en un suelo en un edificio trabaja correctamente, pero una búsqueda para los clientes en todos los suelos en un edificio no trabaja. El arreglo para este bug está disponible con la versión 4.0.87.0 WCS. Si usted utiliza las versiones WCS anterior que 4.0.87.0, la solución alternativa es buscar para los clientes en una superficie cubierta.

## [Cuentas incorrectas del cliente de los informes WCS asociadas a los AP en el modo H-REAP](#)

Este problema es debido al Id. de bug Cisco [CSCsg48059](#) ([clientes registrados solamente](#)). El WCS señala las cuentas del cliente que son demasiado altas cuando H-REAP se habilita en el regulador. La solución alternativa para descubrir asociar a cuántos clientes a los AP o el regulador dado es utilizar el monitor > a los clientes característica, la búsqueda por el AP o el regulador WCS, que son limitados por el tipo de radio para evitar los duplicados, y utiliza el número total de elementos encontrados como su número de población verdadero. La tabla del bsnMobileStation también tiene el número de hilera correcto para el número de clientes. Usted puede también utilizar el WLC para encontrar la cuenta correcta del cliente.

## [El WCS no comienza si el caracter de subrayado se configura en el servidor/el nombre de host](#)

Los caracteres “\_” del caracter de subrayado no se soportan en el WCS Nombre del servidor. Si usted utiliza un caracter de subrayado en el servidor/el nombre de host en una instalación WCS, el WCS no puede comenzar. La instalación del software no señala ninguna problemas y lo instala como normal, sino los estados del RFC-952 que el caracter de subrayado es un carácter sin apoyo, que es porqué éste hace el software WCS fallar.

## [El \[location\] del ERROR no pudo crear el mapa del calor para el MAC: xx: xx: xx: xx: xx: xx razón: Se falla como la lista RSSI vacío después de la poda del tiempo](#)

Es esencial que los reguladores, los servidores de la ubicación, y el WCS todo el Network Time Protocol (NTP) del uso asegurar la hora local exacta. El servidor de la ubicación cae cualquier fecha del regulador que está fuera de su ventana de 15 minutos.

El regulador guarda solamente una vez internamente pero la modifica para la visualización si se especifica un desplazamiento. Si usted especifica un desplazamiento, usted dice a regulador que el tiempo cuál fue ingresado era [local time for London, UK] del tiempo UTC y que usted quisiera

que el regulador visualizara su hora local con la adición del desplazamiento. El NTP es siempre en la hora UTC, y se requiere un desplazamiento si usted quisiera que el regulador lo visualizara en su hora local. Por ejemplo, el EST tiene un desplazamiento de -5. Si usted hace el NTP configurar, el regulador consigue la hora UTC pero agrega el desplazamiento para conseguir la hora local para los grupos fecha/hora en los registros.

El regulador, el servidor de la ubicación, y el WCS **deben** todo ser dentro de tiempo interno de 15 minutos (no [internal time with offset] de la hora local), o el servidor de la ubicación no visualiza ni sigue a los clientes; en lugar muestra este mensaje de error en el registro del servidor de la ubicación:

```
3/08/07 00:46:59 ERROR[location] Failed to create heat map for MAC: xx:xx:xx:xx:xx:xx Reason: Failed as the RSSI list is empty after time pruning
```

El servidor de la ubicación tiene solamente bastante almacenamiento en tiempo real para el último 15 minutos de los datos almacenados. Recuerde que el servidor de la ubicación sigue a los clientes en el tiempo real, mientras que el WCS archiva los datos durante períodos de tiempo más largos. El WCS puede seguir los clientes pero las actualizaciones solamente cada pocos minutos - no en tiempo real. Si los relojes están apagado entre los dispositivos, no hay datos del cliente después de que el servidor de la ubicación quite los que está fuera del intervalo de tiempo especificado en la petición. De hecho, si el servidor de la ubicación recibe los datos del regulador con la hora interna más de 15 minutos fuera de su tiempo interno, lanza los datos en el bloque de memoria de bits.

Usted debe girar el NTP para que el WLC, el WCS, y el servidor de la ubicación sincronicen automáticamente el tiempo interno al UTC.

### [El mensaje de error “la entrada Point\\_FIIifexp\\_Could del procedimiento no ser situado en visualizaciones de la biblioteca con link dinámico el DFORRT.DLL”](#)

Si el WCS utiliza una aplicación de terceros, tal como compilador MATLAB, y MATLAB utiliza una versión específica de la biblioteca DFORRT.dll, cuando una aplicación ha instalado ya la biblioteca DFORRT.dll en c:\windows\system32, el WCS no está instalado correctamente. Como consecuencia, cuando usted comienza el WCS, visualizaciones de este mensaje de error:

```
The procedure entry point _FIIifexp_ could not be located in the dynamic link library DFORRT.DLL
```

Para corregir el problema, quite el archivo DFORRT.dll en c:\windows\system32 y reinstale el WCS.

### [Instrucciones al synch los tres dispositivos](#)

**Para el servidor de la ubicación:** Refiera a la [guía de instalación y configuración](#) para la información dentro de la configuración inicial.

Después de que se comience el dispositivo, usted debe parar el servidor de la ubicación antes de que usted pueda cambiar la fecha, mide el tiempo, o huso horario. Siga estos pasos:

1. Para cambiar el huso horario del dispositivo de la ubicación, copie el archivo de zona del momento apropiado a /etc/localtime:# `cp /usr/share/zoneinfo/<your country>/<your timezone>/etc/localtime`
2. Verifique que el archivo /etc/sysconfig/clock esté definido como esté esto sin ninguna ZONA especificada:# `more /etc/sysconfig/clock`

```
UTC=true  
ARC=false
```

3. Verifique la fecha y hora con el **comando date** en el servidor CLI de la ubicación. # `date`
4. Recomience el servidor de la ubicación con las instrucciones disponibles en [http://www.cisco.com/en/US/products/ps6386/products\\_qanda\\_item09186a008078ece3.shtml#qa13](http://www.cisco.com/en/US/products/ps6386/products_qanda_item09186a008078ece3.shtml#qa13)

**Nota:** Si usted quiere utilizar al servidor NTP para el dispositivo de la ubicación, refiera a [configurar al servidor NTP](#).

**Para el WCS:** El WCS confía en Windows por la hora correcta. Marca el OS (Sistema operativo) Windows una vez cada 24 horas por el Tiempo del sistema. No sabe inmediatamente sobre los cambios del Tiempo del sistema a menos que usted pare y recomience el servidor WCS. Haga clic con el botón derecho del ratón el reloj y elija la hora del cambio/la fecha. Utilice una fuente horaria NTP para fijar el reloj y para fijar manualmente el desplazamiento para su timezone. Esto se fija típicamente ya.

**Para el regulador:** En el regulador, utilice el **reloj de la demostración del** comando CLI para verificar el tiempo y el desplazamiento. Usted puede hacer esto con el GUI, también. Desmarque el checkbox del DST o utilice la **neutralización -8 del timezone del tiempo del** comando `config 0 -8 0`.

Después de que usted acabe la sincronización horaria entre los dispositivos, usted necesita sincronizar el servidor de la ubicación con el WCS (bajo el ubicación-**servidor > sincronice**). Se hace esto de modo que tengan los mismos datos con los mismos grupos fecha/hora.

Note que el WCS, el regulador, y el software de la ubicación están liberados en la misma fecha.

### [La plantilla de la red inalámbrica \(WLAN\) no aplica la configuración correcta del "broadcast SSID" en el WLC](#)

Después de que usted cree las plantillas de la red inalámbrica (WLAN) y las cargue en el WLC con el WCS, los restos del campo del "broadcast SSID" llegaron a la pantalla de configuración individual de la red inalámbrica (WLAN) del regulador, sin importar la configuración en la plantilla de la red inalámbrica (WLAN) WCS. Esto transmite siempre la información de la red inalámbrica (WLAN) SSID.

Para inhabilitar el broadcast SSID en la plantilla actual de la red inalámbrica (WLAN) con el WCS, realice estos pasos en el WCS con las versiones anterior de 4.1.83.

**Nota:** Si usted actualiza el WCS a la versión 4.1.83, también resuelve este problema. También, tales problemas ocurren principalmente cuando el regulador y el WCS están fuera de sincronizan. En estos casos, sincronice el WLC y el WCS.

1. En la plantilla de la red inalámbrica (WLAN) WCS, inhabilite o desmarque el cuadro del **estado del administrador** y asegúrese que **transmitir el SSID** está desmarcado.
2. Salve la plantilla.
3. Aplique la plantilla al regulador.
4. Vuelva a permitir el cuadro admin de esta red inalámbrica (WLAN).
5. Salve la plantilla
6. Aplique la plantilla al regulador otra vez.

Ahora, usted puede encontrar el campo del "broadcast SSID" según lo apagado en la

configuración individual de la red inalámbrica (WLAN) del regulador.

## [Las plantillas de la red inalámbrica \(WLAN\) no visualizan la determinación correcta del checkbox de 7920 CAC](#)

Cuando usted crea las plantillas de la red inalámbrica (WLAN) para avanzar los WLAN a los reguladores, marque los 7920 checkbox CAC para habilitar esa característica y para salvarla y para red desplegarla que la misma red inalámbrica (WLAN). La plantilla muestra según lo desmarcado aunque se marca realmente y habilita esa característica en el regulador cuando está avanzada a ella.

Esto debe introducir errores de funcionamiento [CSCsi77521](#), que se asocia a este problema.

Actualice el WCS a la versión 4.1 para resolver este problema.

## [Incapaz de borrar los reguladores offline de la versión 3.2.51.0 WCS](#)

En ciertos casos, los usuarios no pueden borrar el WLCs que son no se utilizan más del WCS. Esto está debido a los problemas con la estructura de la base de datos del WCS en la versión 3.2.51.0; como consecuencia, el WCS tiende a bloquear para arriba los recursos. La base de datos entera fue reestructurada en la versión 4.0 y ha aumentado el nivel de rendimiento.

Hay dos soluciones alternativas para este problema:

- Borre los informes de auditoría y después borre el regulador o
- Actualización a WCS 4.0.87.0 y posterior

Con la primera opción, para borrar los reguladores offline, haga esto:

1. Cuando el WCS monitorea un pool muy grande de los reguladores, la mejor cosa está a primero borra los informes de auditoría de esos reguladores, uno por uno, y después intenta borrar esos reguladores. Para borrar los informes de auditoría, siga los siguientes pasos: Vaya al **regulador de la configuración**. Marque el cuadro del regulador deseado. Se permite solamente un en un momento del regulador. Elija los **informes de auditoría del comando view** de la casilla desplegable. Haga clic el botón del **ir**. Borre los informes de auditoría. Entonces intente borrar los reguladores.
2. Intente este procedimiento en el resto de los reguladores. Asegurese que las cuentas de usuario que usted utiliza para realizar estas tareas son parte del grupo del superusuario. De vez en cuando, borra algunos de los informes de auditoría pero de no todos los informes para un regulador específico.
3. Los informes de auditoría que tienen el estado de sincronización **lo mismo en el WCS y el regulador** pueden ser borrados con éxito, solamente los informes de auditoría con el estado de sincronización de **diferente en el WCS y el regulador** no pueden ser borrados.
4. Usted puede ver este mensaje de error cuando usted intenta borrar los informes de auditoría con el estatus de **diferente en el WCS y el regulador**. `The resource you are trying to delete seems to be busy`
5. En este caso, el regulador no puede ser borrado. Este mensaje de error significa que la base de datos ha bloqueado el recurso. Esto puede suceder si el usuario golpeó el botón Delete Button, no esperó bastante tiempo, y después golpeó la *parte posterior* para ir a la página previa. Esto era un problema en la versión 3.2; apenas espere y vea si el recurso libera para

arriba.

Alternativamente, usted puede utilizar la segunda opción para actualizar el WCS a 4.0.87.0 o arriba, que tiene grandes mejoras en el rendimiento a partir del 3.2 debido a una reestructuración de la base de datos WCS.

## [No puede agregar la plantilla de la autenticación Web con el valor por defecto del tipo interno del WCS](#)

En un intento por avanzar la plantilla, el **funcionamiento de SNMP del mensaje de error al dispositivo fallado** aparece.

Esto está debido al bug CSCsh89306. El WCS da el error de SNMP cuando avanza una plantilla de la autenticación Web a un regulador que funcione con la versión 4.0.206.0.

La solución alternativa es configurar una autenticación Web directamente en el regulador.

1. Navegue a la página de la plantilla del arreglo para requisitos particulares de la autenticación Web.
2. Elija el tipo de la autenticación Web como **externo**.
3. Ingrese un poco de texto simulado URL.
4. Cambie el tipo de la autenticación Web **para omitir interno**.
5. Ingrese una aduana reorientan el URL.
6. Salve y aplique la plantilla.

Básicamente, el externo y la aduana reorientan el URL no se deben ir en blanco en la página incluso si no son relevantes a la autenticación Web actual Application type (Tipo de aplicación).

## [Información Relacionada](#)

- [Preguntas Más Frecuentes de Troubleshooting de Wireless Control System \(WCS\)](#)
- [Guía de configuración del Cisco Wireless Control System, versión 4.0](#)
- [Cisco Wireless Control System](#)
- [Página de Soporte de Red Inalámbrica](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)