Clasificación no fiable basada en las reglas en los reguladores inalámbricos LAN (WLC) y el sistema de control inalámbrico (WCS)

Contenido

Introducción

En la versión inalámbrica 5.0 del sistema de control (WCS), el WCS aumentó la funcionalidad de administración no fiable para diversos tipos del granuja AP y con tal que las reglas definidas por el usario para clasificar automáticamente al granuja APs. El WCS aplicó las reglas no fiables de la clasificación AP a los reguladores. Este documento explica la funcionalidad de administración no fiable aumentada y los pasos necesarios configurar estas funciones en el regulador LAN de la Tecnología inalámbrica (WLC) y el WCS.

prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimiento del protocolo ligero del Punto de acceso (LWAPP)
- Conocimiento de las soluciones inalámbricas de la Seguridad del regulador LAN

Componentes Utilizados

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

hardware.

- Cisco 4400 Series WLC que funciona con los firmwares 5.2
- Puntos de acceso ligeros del Cisco Aironet de la serie 1130 AG (revestimientos)
- Versión 5.2 del Cisco Wireless Control System

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 TécnicosCisco para obtener más información sobre las convenciones del documento.

Clasificación no fiable basada en las reglas

En las versiones WCS antes de la versión 5.0, el WCS visualizó demasiados puntos de acceso no autorizado (APs) en la **página de resumen de la Seguridad**. Aunque diferencian los estados agresores, todos aparecen en una página, clasificada por la dirección MAC BSSID/del granuja.

En la versión WCS 5.0, el WCS aumentó la funcionalidad de administración no fiable e introdujo las nuevas terminologías (sin clasificar, malévolo, y cómodo) para diversos tipos del granuja AP y con tal que las reglas definidas por el usario para clasificar automáticamente al granuja APs. El WCS aplicó las reglas no fiables de la clasificación AP a los reguladores.

El WCS aumentó la función de administración del estado agresor para guardar al estado agresor como *externo* una vez que el estado del granuja se ha cambiado manualmente al *externo*. El WCS también pone al día el estado *externo* para los otros reguladores cuando el WCS tira o maneja del mensaje trampa de los otros reguladores.

Para utilizar esta característica, WLC y el WCS deben funcionar con la versión 5.0.

Terminologías no fiables basadas en las reglas de la clasificación

Con estas nuevas funciones, se introducen estos nuevos tipos del granuja AP:

- **AP malévolo:** Un AP detectado que hace juego las reglas malévolas definidas por el usario o se ha movido manualmente desde los APs cómodos.
- **AP cómodo:** La existencia sabida, reconoce, y clasifican a los estados agresores que falta de la confianza como cómodos. Además, los APs detectados que hacen juego las reglas cómodas definidas por el usario se clasifican como cómodos. Los APs cómodos no pueden ser contenidos.
- **AP sin clasificar:** Un AP detectado que no hizo juego las reglas malévolas o cómodas. Un AP sin clasificar puede ser contenido. Un AP sin clasificar se puede mover manualmente a cómodo por el usuario. Las reglas definidas por el usario para mover automáticamente el AP sin clasificar a cómodo o a malévolo, por ejemplo, en la detección, el SSID están vacías. En el informe no fiable siguiente, se encuentra un SSID, y resulta ser usuario configurado SSID.

Reglas no fiables de la clasificación

Éstas son reglas de la clasificación aplicables a cada uno de los tipos del granuja AP:

- Reglas malévolasLas coincidencias manejaron el SSIDHace juego al usuario configurado SSIDNingún cifrado en un SSIDMínimo RSSIDuración del tiempoNúmero de clientes asociados
- Reglas cómodasSSID manejadoUsuario configurado SSID
- Reglas sin clasificarNo hace juego las reglas malévolas o cómodas

Parameter	Description
Time Duration (0 to 3600)	Requires that the rogue access point be detected for a minimum period of time. If you choose this option, enter a value for the minimum detection period in the Time Duration field. The valid range is 0 to 3600 seconds (inclusive), and the default value is 0 seconds.
Minimum RSSI (-95 to -50)	Requires that the rogue access point have a minimum received signal strength indication (RSSI) value. For example, if the rogue access point has an RSSI that is greater than the configured value, then the access point could be classified as malicious. If you choose this option, enter the minimum RSSI value in the Minimum RSSI field. The valid range is -95 to -50 dBm (inclusive), and the default value is 0 dBm.
Minimum number of Rogue client (1-10)	Requires that a minimum number of clients be associated to the rogue access point. For example, if the number of clients associated to the rogue access point is greater than or equal to the configured value, then the access point could be classified as malicious. If you choose this option, enter the minimum number of clients to be associated to the rogue access point in the Minimum Number of Rogue Clients field. The valid range is 1 to 10 (inclusive), and the default value is 0.
No Encryption	Requires that the rogue access point's advertised WLAN does not have encryption enabled. If a rogue access point has encryption disabled, it is likely that more clients will try to associate to it. No further configuration is required for this option. **Note** WCS refers to this option as "Open Authentication."
Managed SSID[1]	Requires that the rogue access point's managed SSID (the SSID configured for the WLAN) be known to the controller. No further configuration is required for this option.
User configured SSID[1]	Requires that the rogue access point have a specific user-configured SSID. If you choose this option, enter the SSID in the User Configured SSID field, and click **Add SSID**. You can add multiple SSIDs. To remove an SSID, select the SSID and click **Remove**.

[1]The SSID and Managed SSID conditions cannot be used with the Match All operation as these two SSID lists are mutually exclusive. If you define a rule with Match All and have these two conditions configured, the rogue access points are never classified as friendly or malicious because one of the conditions can never be met.

El usuario puede elegir hacer juego **todas las,** o **algunas** condiciones de la regla bajo cada regla:

- **Todos los** medios hacen juego todas las condiciones configuradas para la regla.
- **Cualquier** medio hace juego las condiciones configuradas unas de los para la regla.
- **Algunos** medios hacen juego pocas de las condiciones configuradas para la regla

Por ejemplo, bajo *reglas malévolas*, el usuario configura *SSID manejado* y el *mínimo RSSI*. Entonces, el usuario tiene la opción para hacer juego **todos** o las dos condiciones **unas de los**, o haga juego apenas la condición del *mínimo RSSI*.

Cuando el regulador recibe el informe no fiable, hace esto:

- Controla si el AP detectado está en la lista del usuario configurado MAC. Si es así clasifique el AP como tipo cómodo.
- Si el AP detectado no está en la lista, comienza a aplicar las reglas.
- Primero, aplica las *reglas malévolas*. Si las *reglas malévolas* hacen juego, se clasifica como

el tipo malévolo. Si el detector RLDP/rogue determina que este granuja está en la red, marca al estado agresor como **amenaza**. El usuario puede contener manualmente el AP que cambia al estado agresor a **contenido**. Si el AP no está en la red, marca al estado agresor como **alerta**, y el usuario puede contenerla manualmente.
- Si las *reglas malévolas* no hacen juego, aplique las *reglas cómodas*. Si las *reglas cómodas* hacen juego, después clasifiqúelo como tipo cómodo.
- Si las *reglas cómodas* no hacen juego, clasifique este AP como sin clasificar. Si el detector RLDP/rogue determina que este granuja está en la red, marque al estado agresor como **amenaza** y clasifiqúelo como tipo malévolo. El usuario puede contener manualmente el AP que cambia al estado agresor a **contenido**. Si el AP no está en la red, marque al estado agresor como **alerta**, y el usuario puede contenerla manualmente.
- El usuario puede mover manualmente el AP a un diverso tipo de la clasificación.

Clasificación no fiable y estados agresores

Esta tabla muestra las diversas clasificaciones de los granujas y de los estados agresores para cada clasificación.

Tipo basado en las reglas de la clasificación	Estados agresores
AP malévolo	La amenaza alerta contenida contuvo pendiente quitado
AP sin clasificar	La alerta contenida contuvo pendiente quitado
AP cómodo	(Sabido actualmente) (reconozca actualmente) los desaparecidos internos externos internos (desaparecidos de la confianza) alertan

Estados agresores explicados

- **Pendiente —** En la primera detección, el AP detectado se pone en el estado pendiente por 3 minutos. Esta vez es suficiente para que los APs manejados determinen si el AP detectado es un vecino AP.
- **Alerta —** Después del descanso 3-minute, el AP detectado se mueve **para alertar** si no está en la lista vecina o la lista cómoda del usuario configurado MAC.
- **Amenaza —** El AP detectado se encuentra en la red.
- **Contenido —** Se contiene El AP detectado.
- **Contenido pendiente —** Se marca El AP detectado contuvo, pero la acción de la contención se retrasa debido a los recursos no disponibles.
- **Interno —** El AP detectado está dentro de la red, y el usuario la configura manualmente como **cómoda, interno**, por ejemplo, los APs en una red de laboratorio.
- **Externo —** El AP detectado está fuera de la red, y el usuario la configura manualmente como **cómoda, externo**, por ejemplo, los APs que pertenecen a una red vecina.
- **Desaparecidos de confianza —** Si detectaron y no se oye al usuario configurado MAC

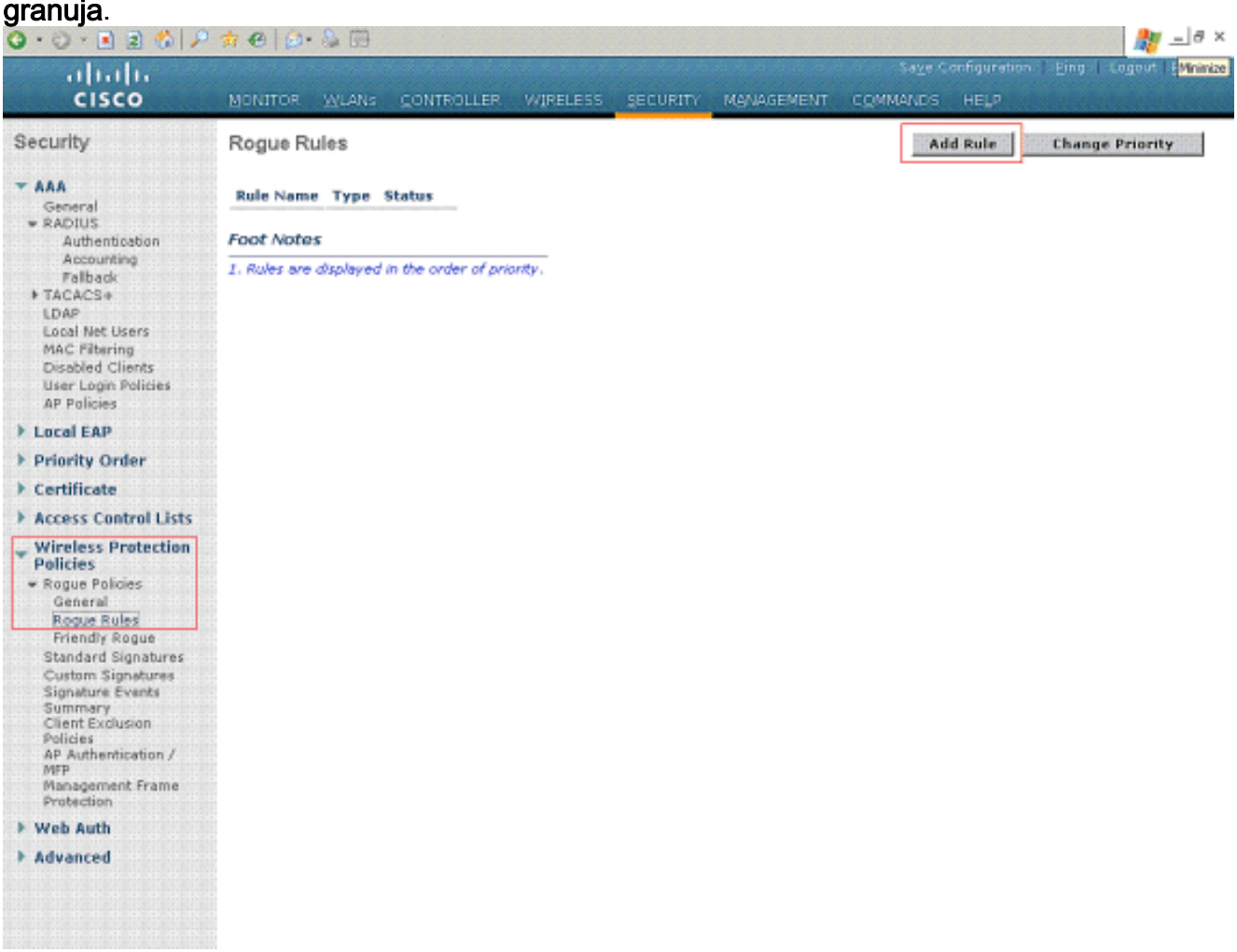
cómodo para la duración del confianza-descanso, marcan al estado agresor del AP cómodo como desaparecidos de confianza.

- **Quitado —** Si el AP malévolo o sin clasificar no se oye de todos los reguladores para la duración del granuja-descanso, marcan al estado agresor del AP como **quitado**.

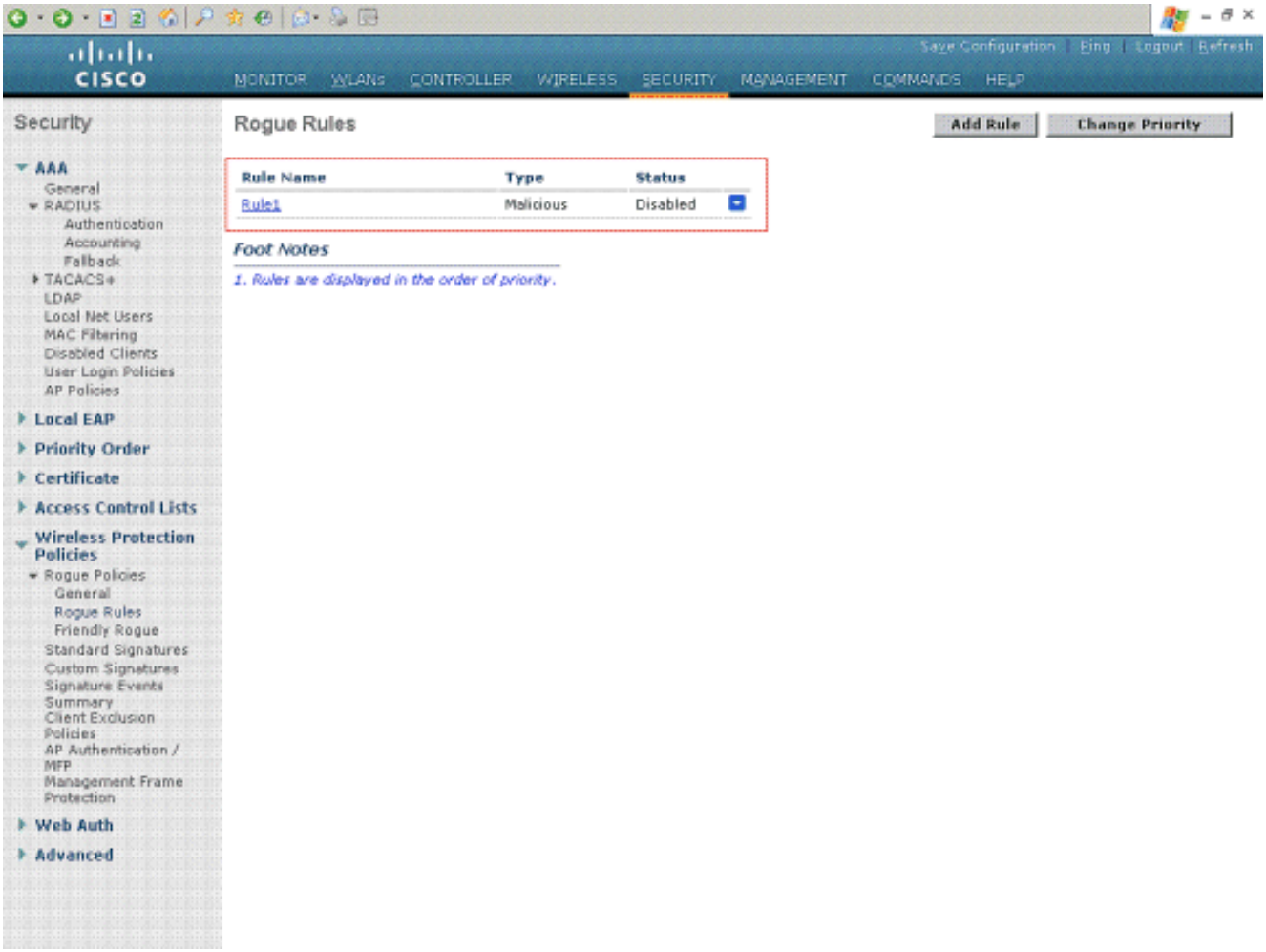
Cómo configurar las reglas no fiables en WLC

Para configurar las reglas no fiables en el regulador LAN de la Tecnología inalámbrica, complete estos pasos.

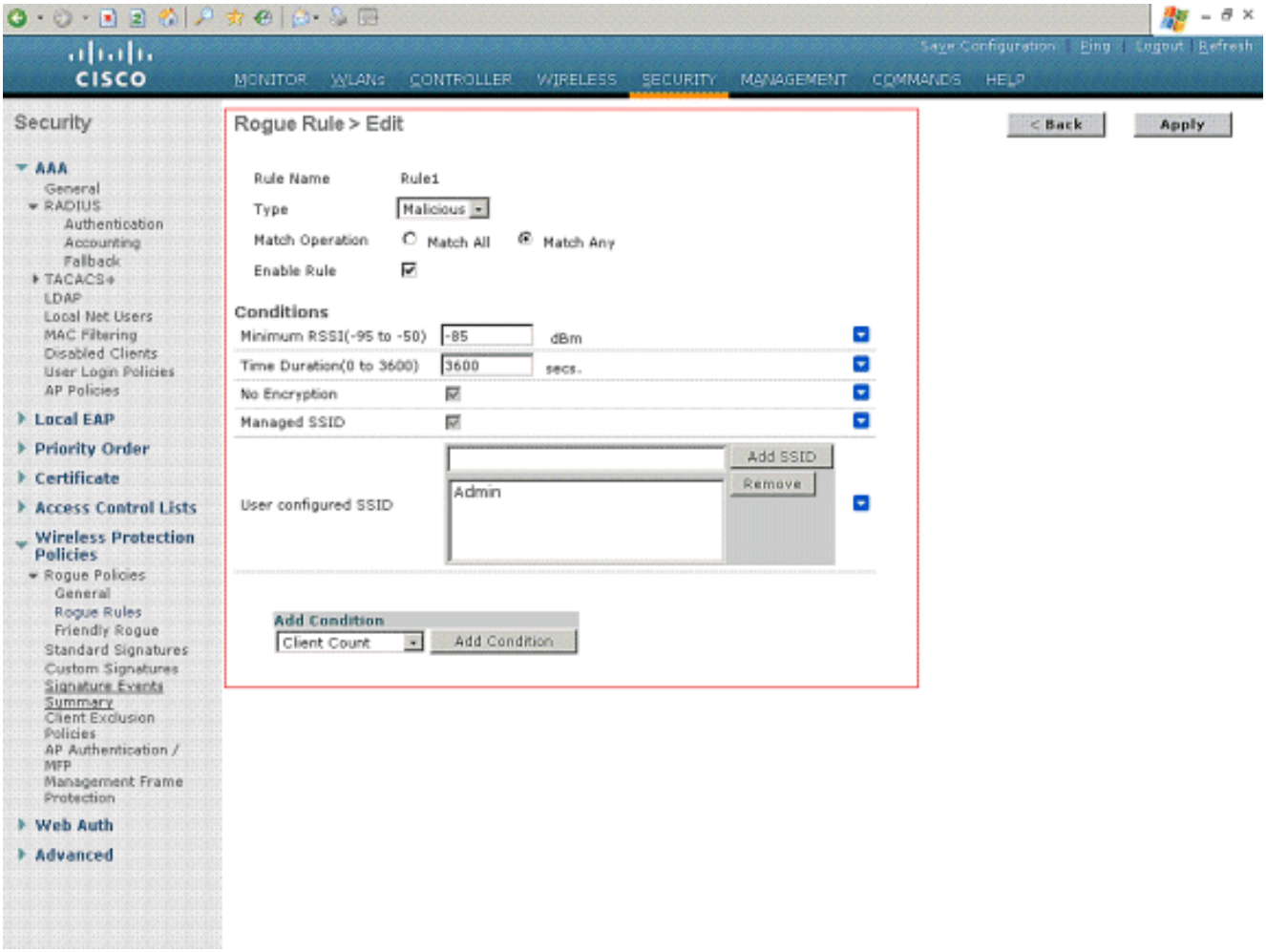
1. Las reglas no fiables se pueden crear del WLC de la **Seguridad >** página **inalámbrica de las directivas de la protección > de las directivas del granuja > de las reglas del granuja**.



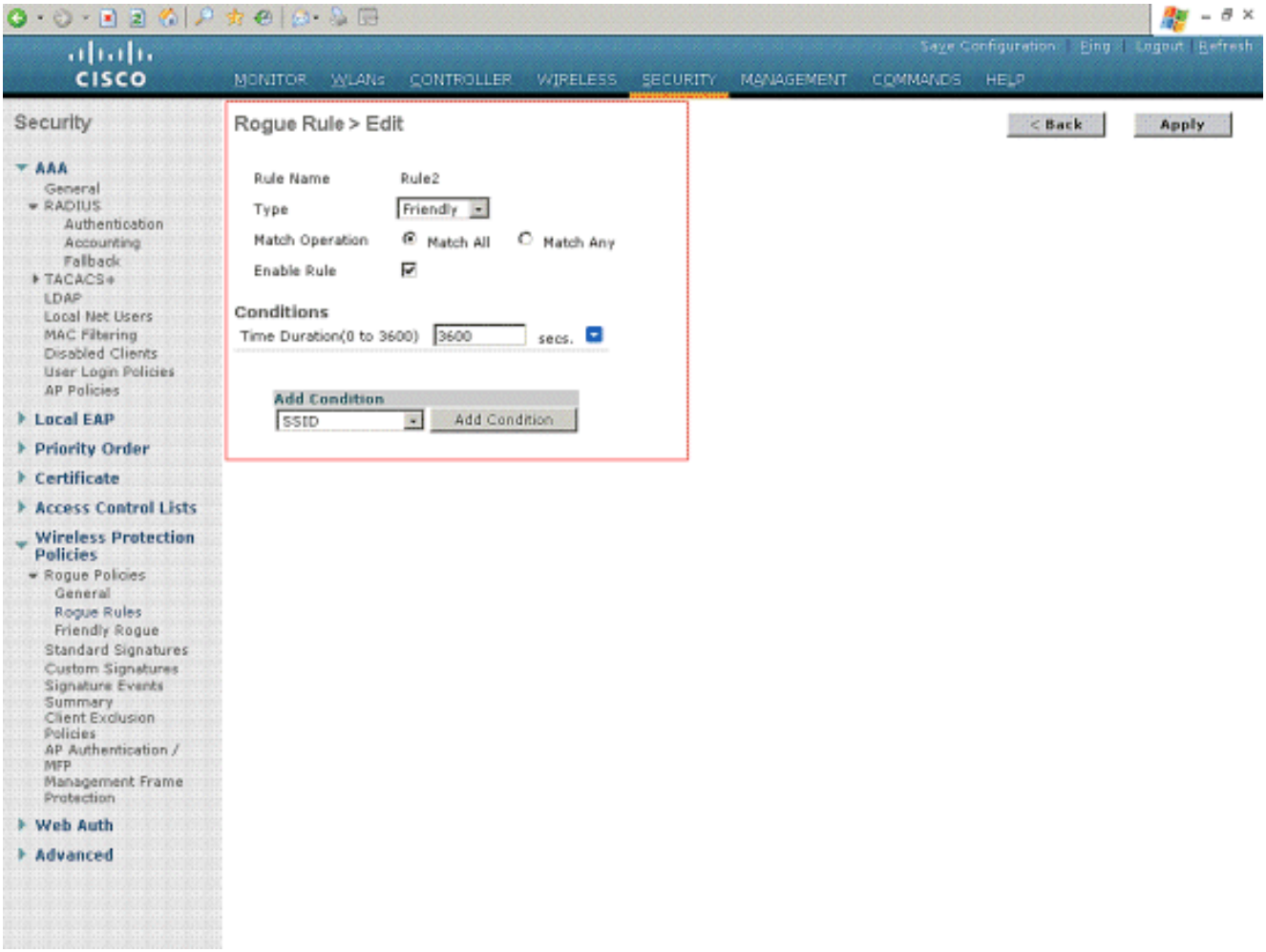
2. Para crear una nueva directiva no fiable, haga clic el botón de la **regla del agregar**. La ventana de las **reglas del granuja** aparece. Ingrese un nombre para la regla. Este ejemplo utiliza Rule1. Elija el tipo de regla. Éste es un ejemplo de una regla malévola. Haga clic en Add (Agregar). Se crea
Rule1.



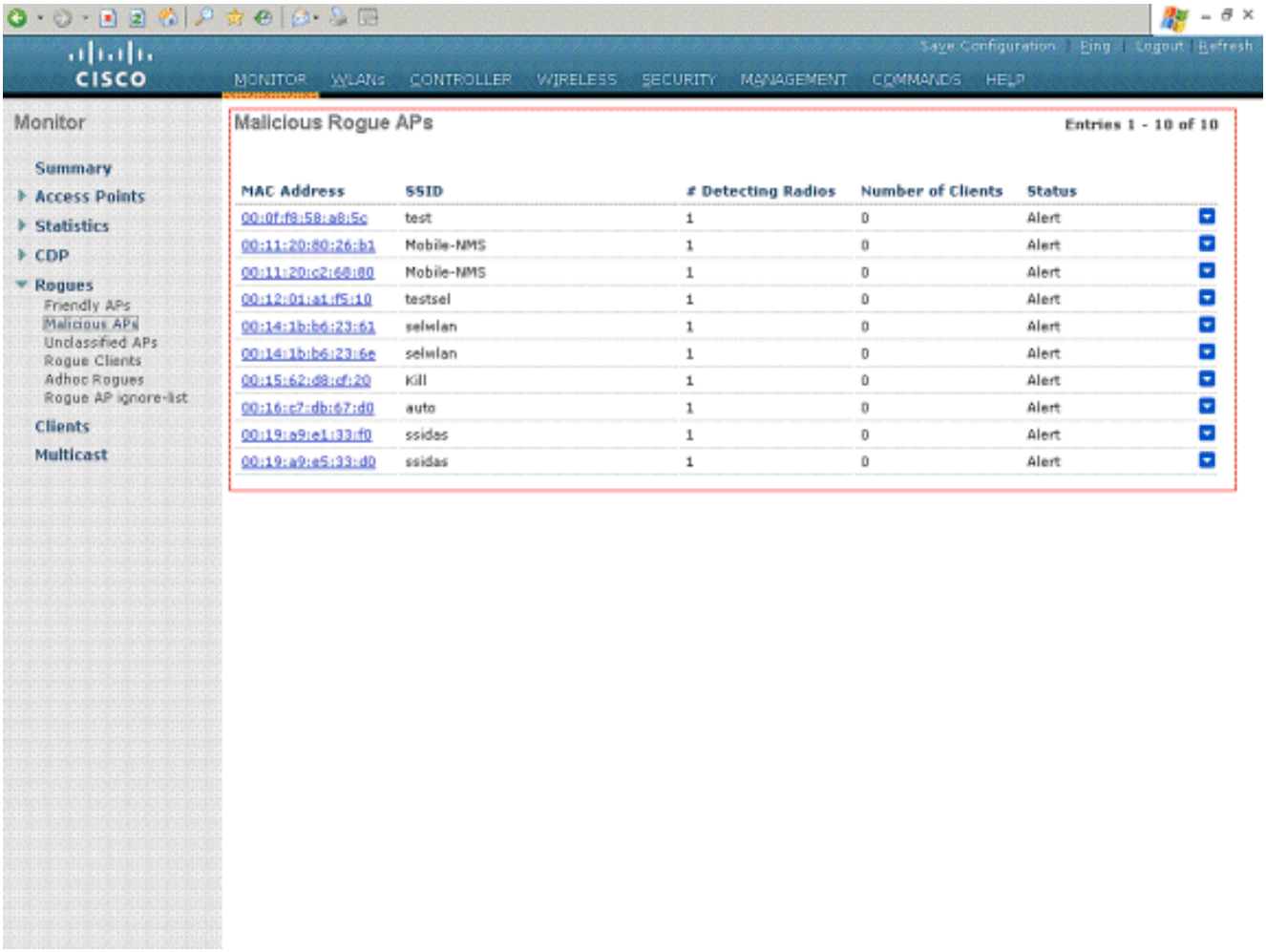
3. Para corregir esta regla, haga clic la regla que fue creada. **La regla no fiable > corrige la** página aparece. En esta página, controle la casilla de verificación de la **regla del permiso** para activar la regla. Elija el tipo de operación de la coincidencia y otras condiciones basados en el requisito como en este ejemplo.



4. Éste es un ejemplo de la directiva no fiable cómoda de la regla.



5. La salida de las reglas no fiables se puede considerar en el **monitor > los granujas > AP malévolo**.

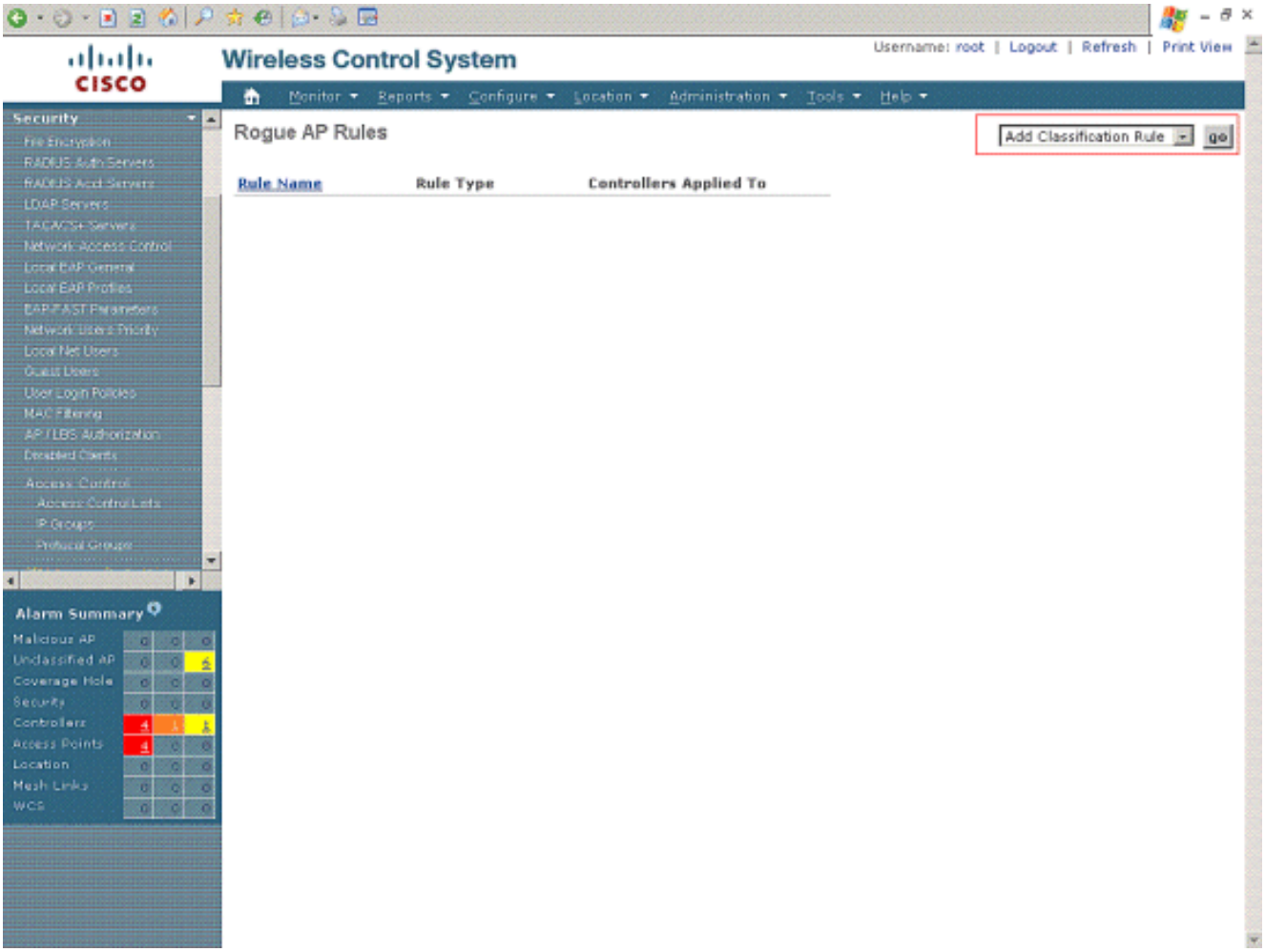


6. Semejantemente, la salida de las *reglas cómodas* y de las *reglas sin clasificar* se puede ver en el **monitor > los granujas > AP sin clasificar** y el **monitor > los granujas > las** páginas **cómodas AP**, respectivamente.

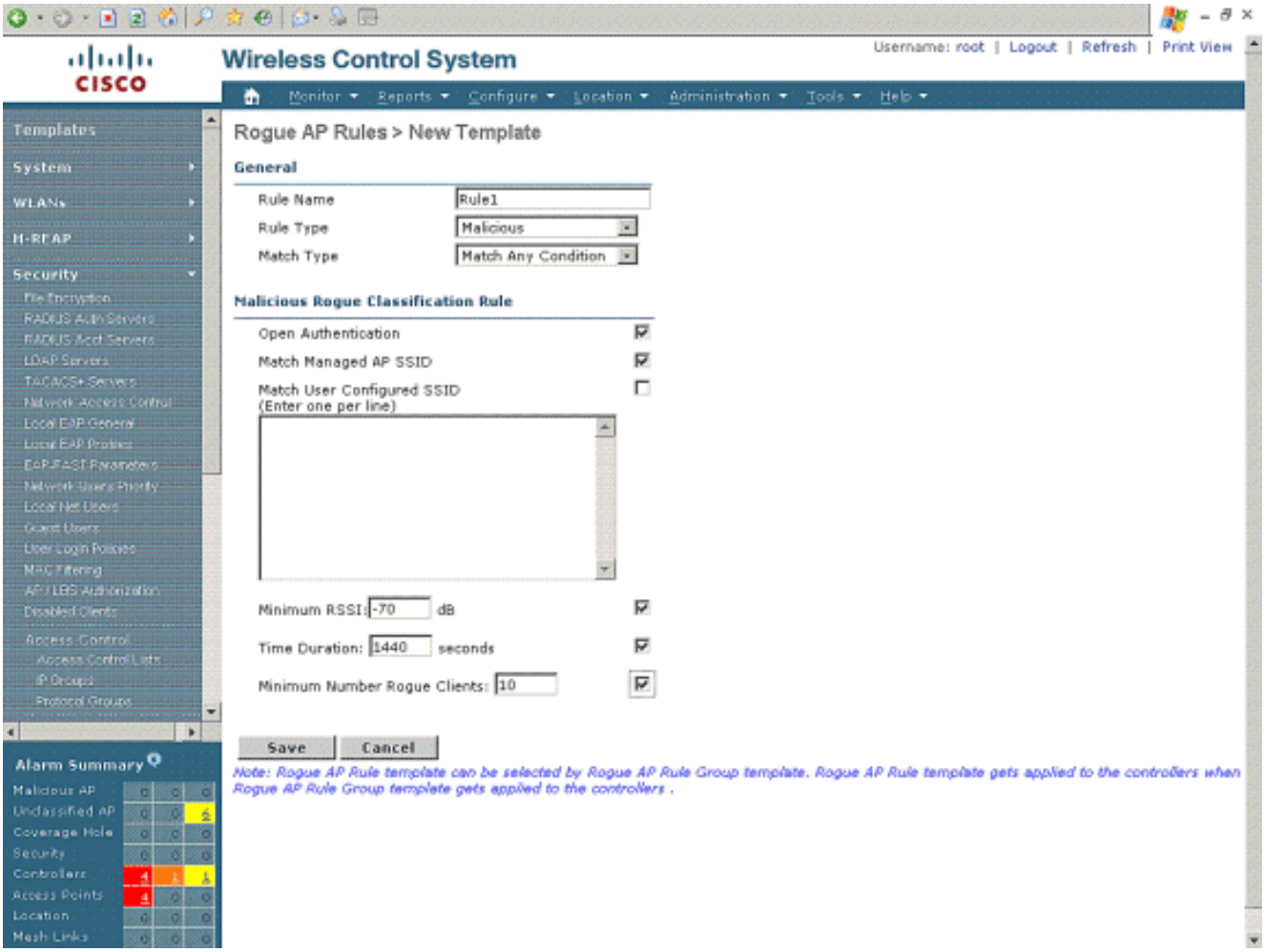
Cómo configurar las reglas no fiables en el WCS

Lista no fiable de la regla: El WCS proporciona a la configuración no fiable de la regla del nivel del sistema. Para configurar las reglas no fiables en el WCS, complete estos pasos.

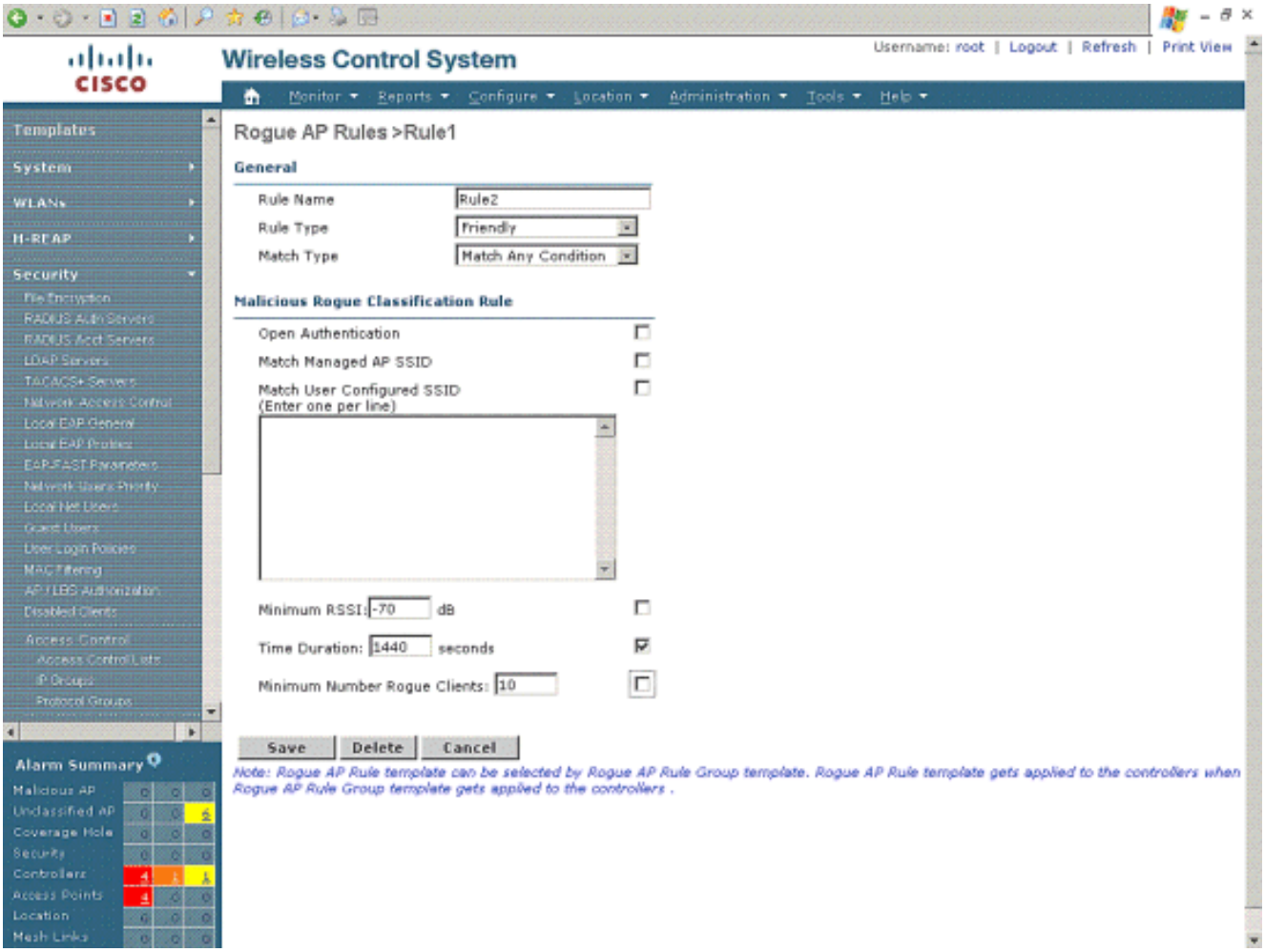
1. Elija **configuran > plantilla del regulador**, y después hacen clic las **reglas de la Seguridad > del granuja AP** para tener acceso al granuja que las reglas AP enumeran la página.
2. El tecleo **agrega la regla de la clasificación** en el menú desplegable superior correcto para agregar una nueva regla de la clasificación.



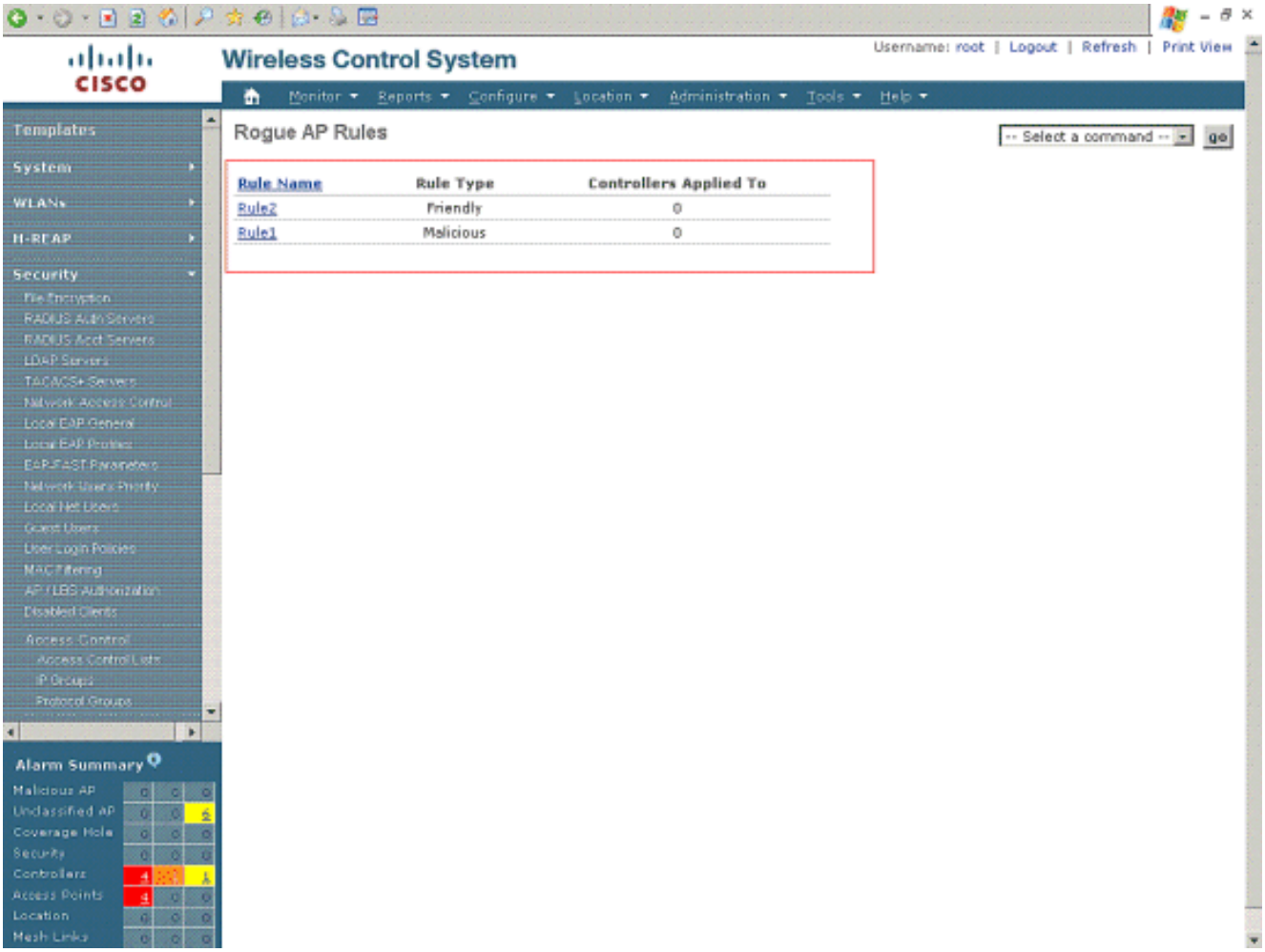
3. Haga clic el nombre de la plantilla para corregir la regla no fiable. Esta página del detalle de la regla le permite corregir, poner al día la regla del granuja AP, o suprimir la regla.**Parámetros no fiables de la configuración de la regla AP:** En esta página, los usuarios pueden activar cualquier condición cuando controlan la casilla de verificación para concatenar el cualquiera o todo el de estas condiciones:Ningún cifradoAP manejado coincidenciaUsuario configurado SSID de la coincidenciaMínimo RSSIDuraciónCliente no fiable del número mínimoÉste es un ejemplo de una regla malévola:



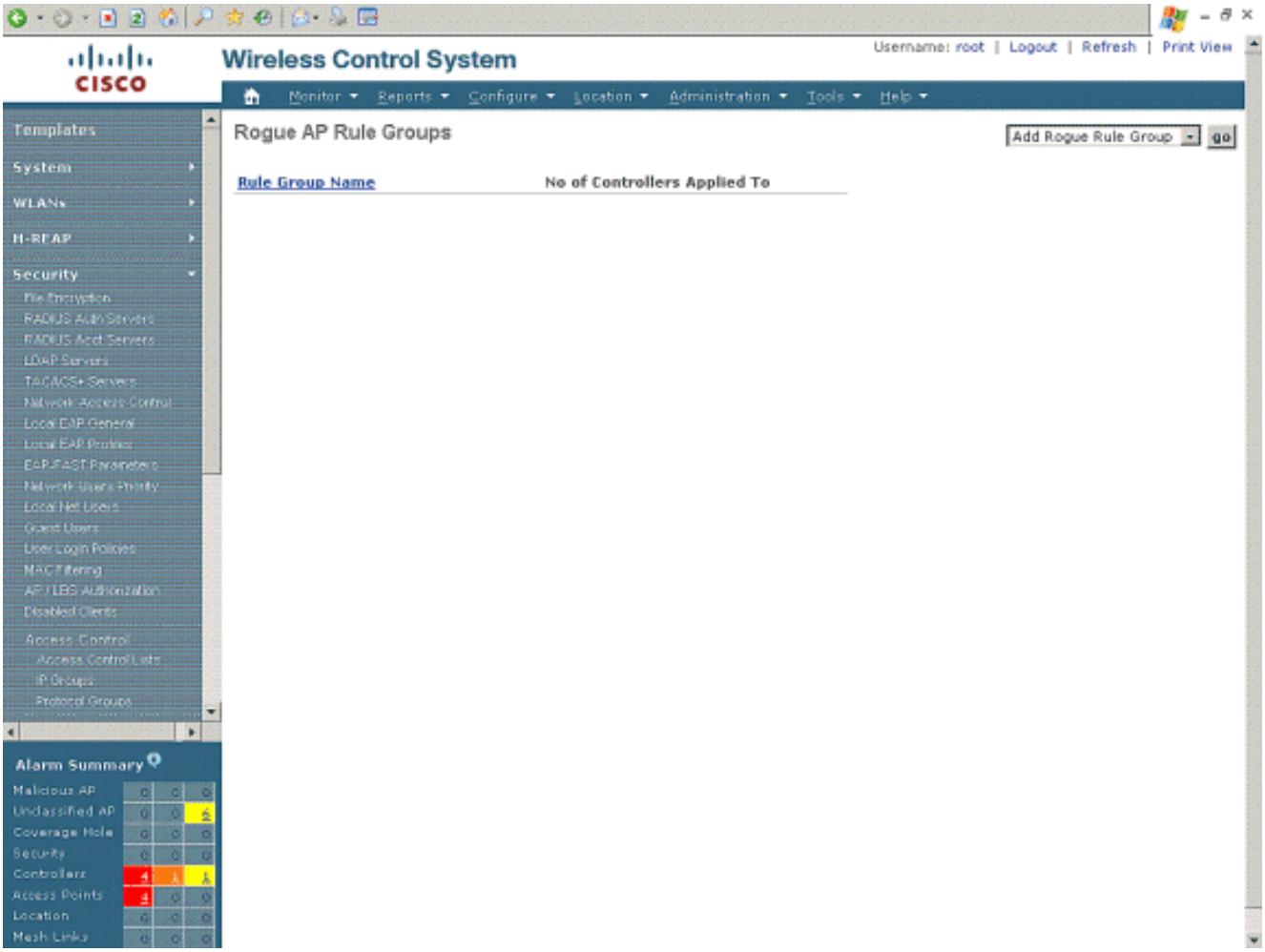
Éste es un ejemplo de una regla cómoda:



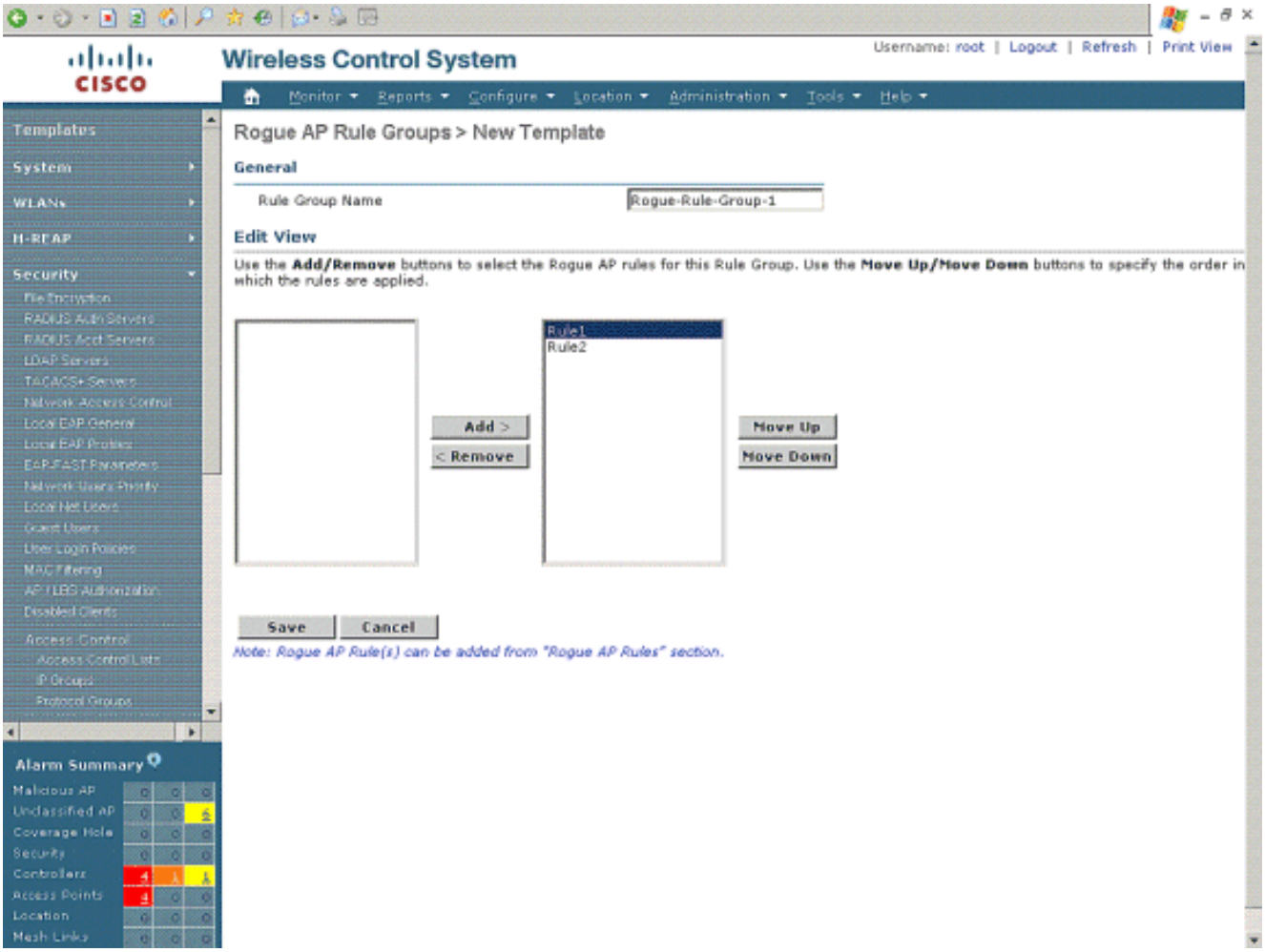
4. Las reglas del granuja AP paginan las listas que todas las reglas crearon.



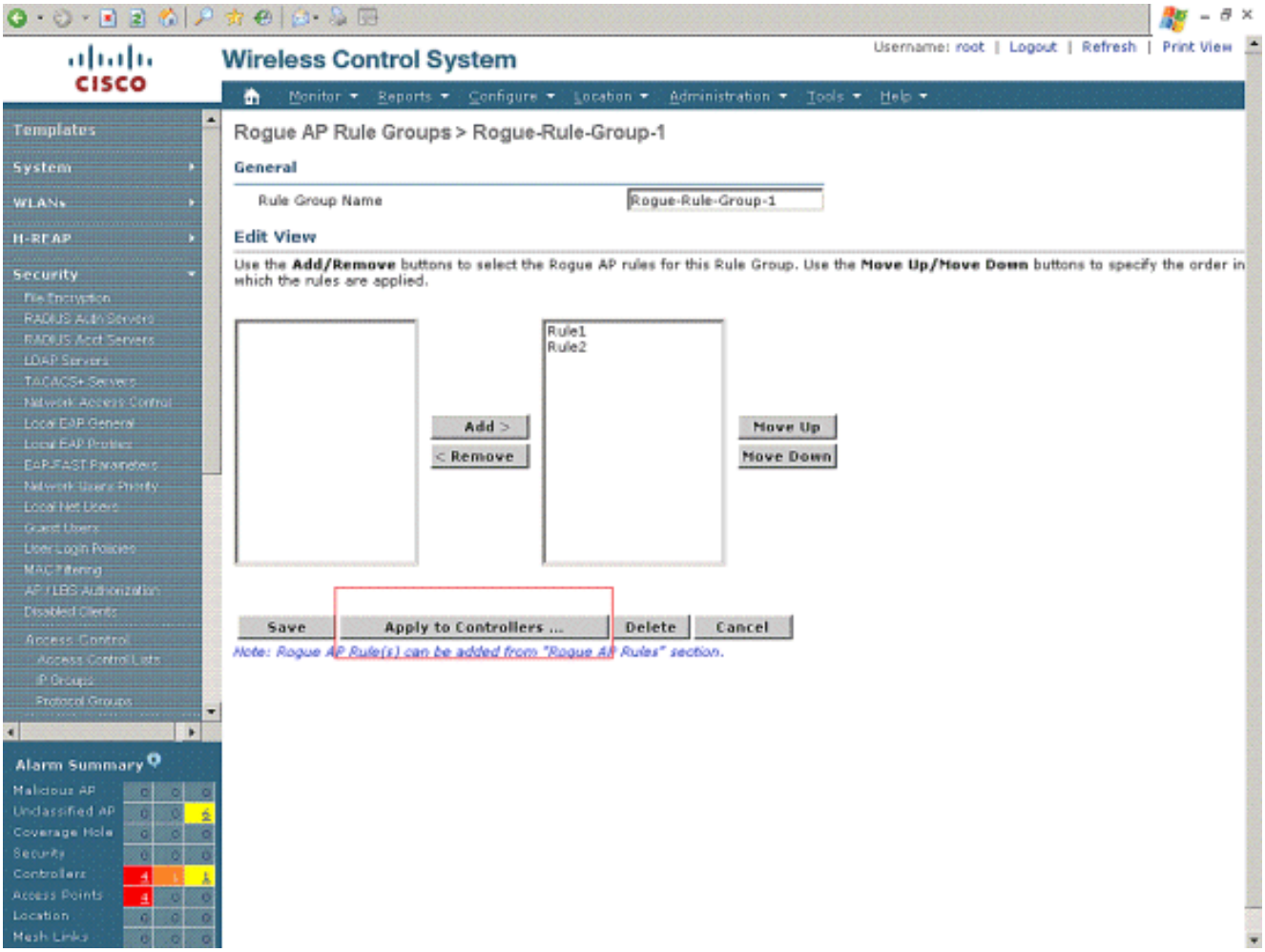
5. El siguiente paso es configurar a un grupo de reglas y aplicar estas reglas a los reguladores. Para esto, utiliza a los **grupos de reglas del granuja AP** que fijan en el WCS.
6. Para crear a un nuevo grupo de reglas, elija **configuran > plantilla del regulador**, y después hacen clic a los **grupos de reglas de la Seguridad > del granuja AP del** GUI WCS.



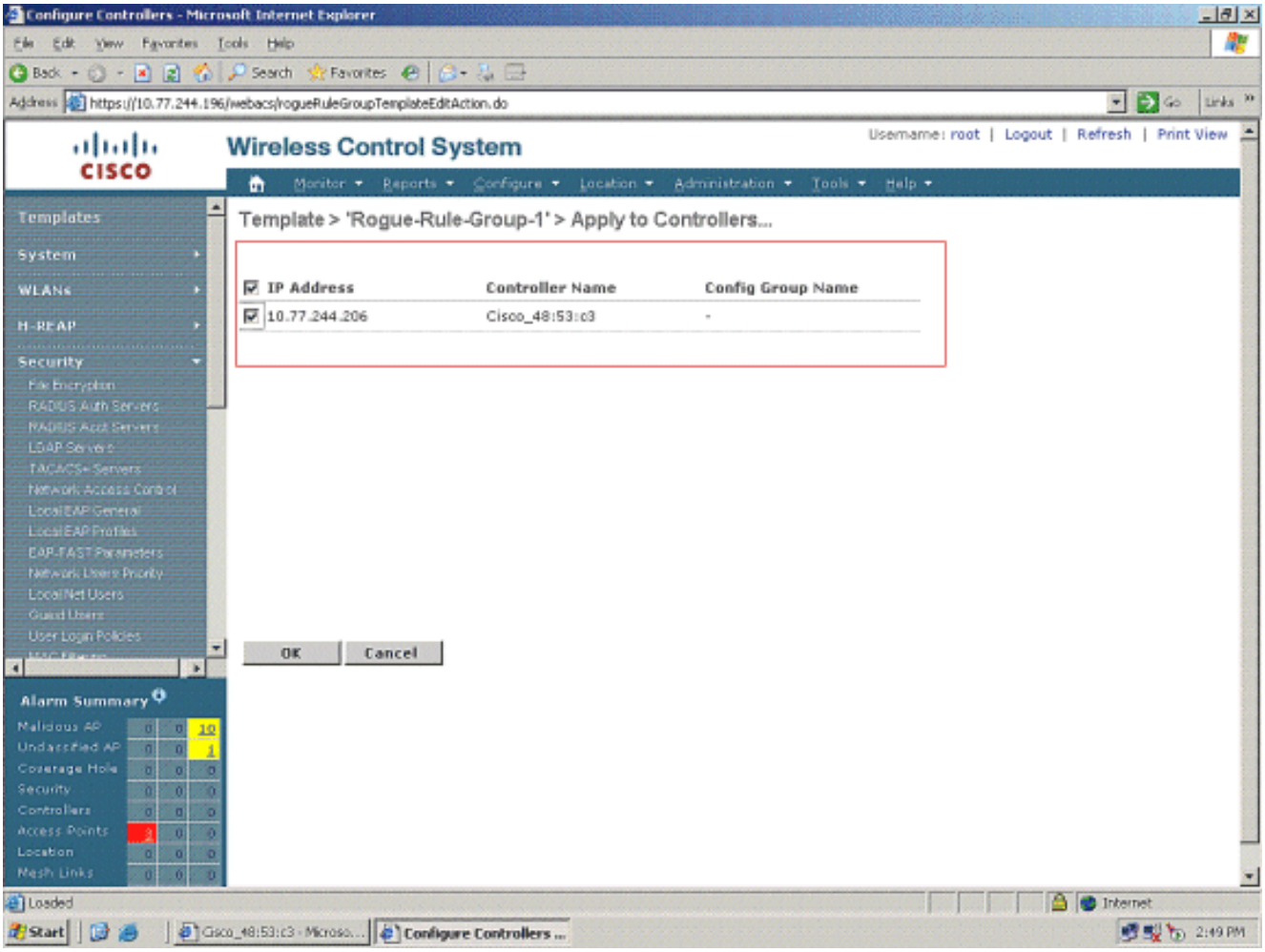
7. Los grupos de reglas del granuja AP > nueva página de la plantilla le permiten agregar, poner al día el grupo de reglas del granuja AP, suprimir la regla, y aplicar al grupo de reglas al regulador. Utilice el agregar/los botones Remove Button para elegir las reglas del granuja AP para este grupo de reglas. Utilice los botones arriba/abajos para especificar la orden en la cual las reglas son aplicadas. Esto es un ejemplo. Una vez que configuran al grupo de las reglas, **salvaguardia del**
tecleo.



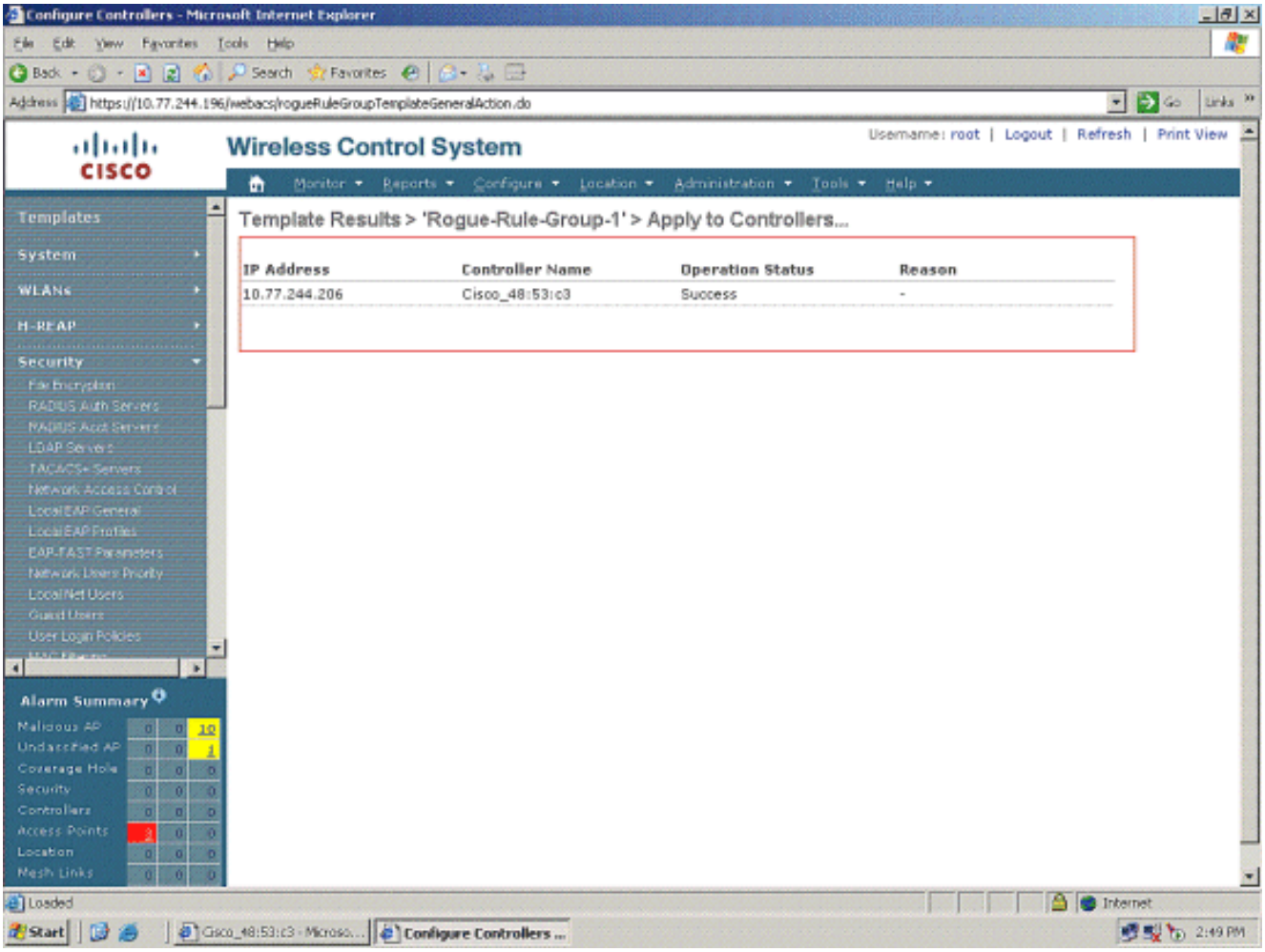
8. Una vez que usted salva al grupo de reglas, puede ser aplicado a los reguladores. Para aplicar al grupo de reglas al regulador, corrija al grupo de reglas. Haga clic el nombre de grupo de
reglas.



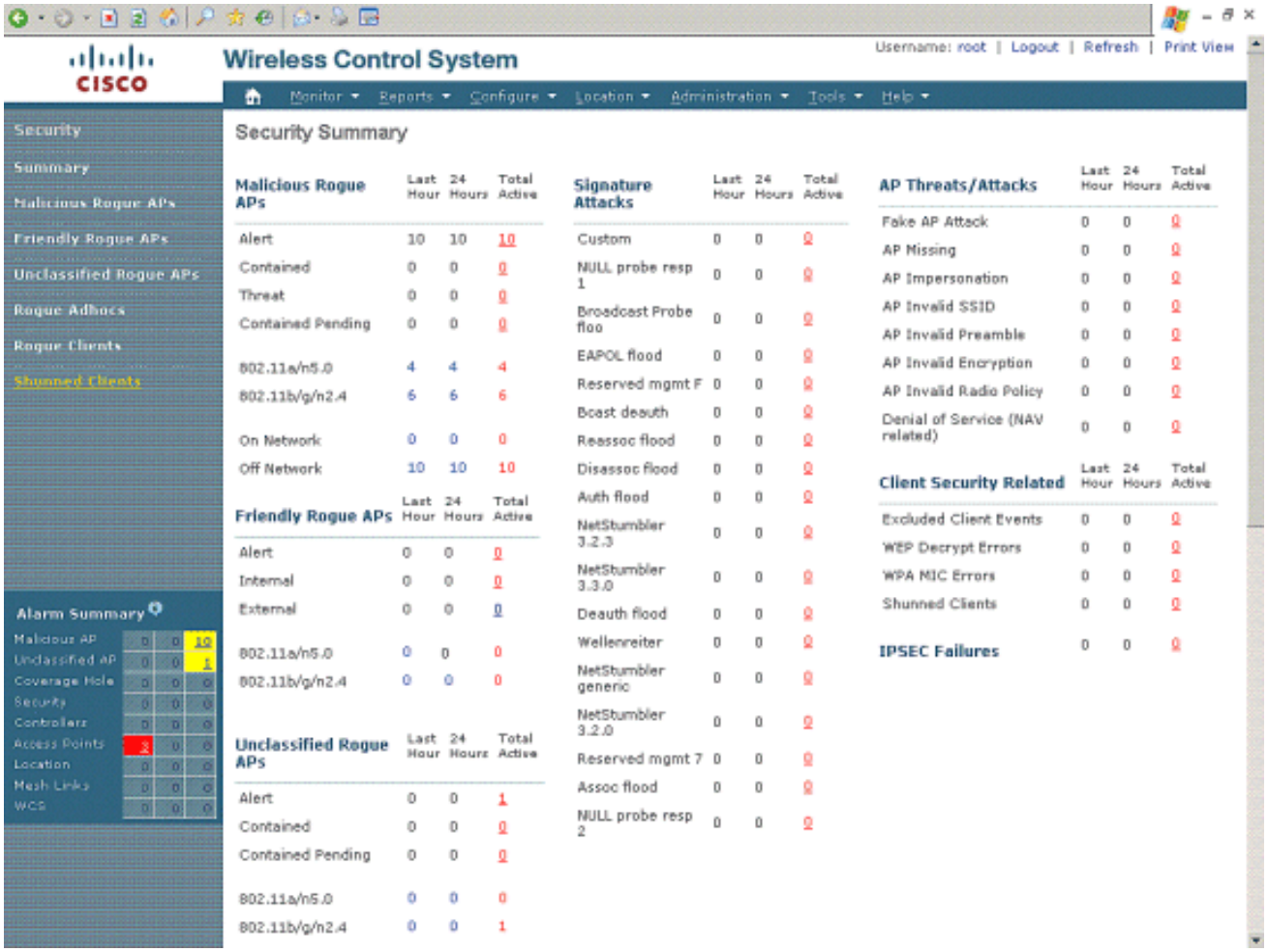
El tecleo **se aplica a los reguladores**. En la página siguiente, elija los reguladores a los cuales esta regla es aplicada. Esto es un ejemplo.



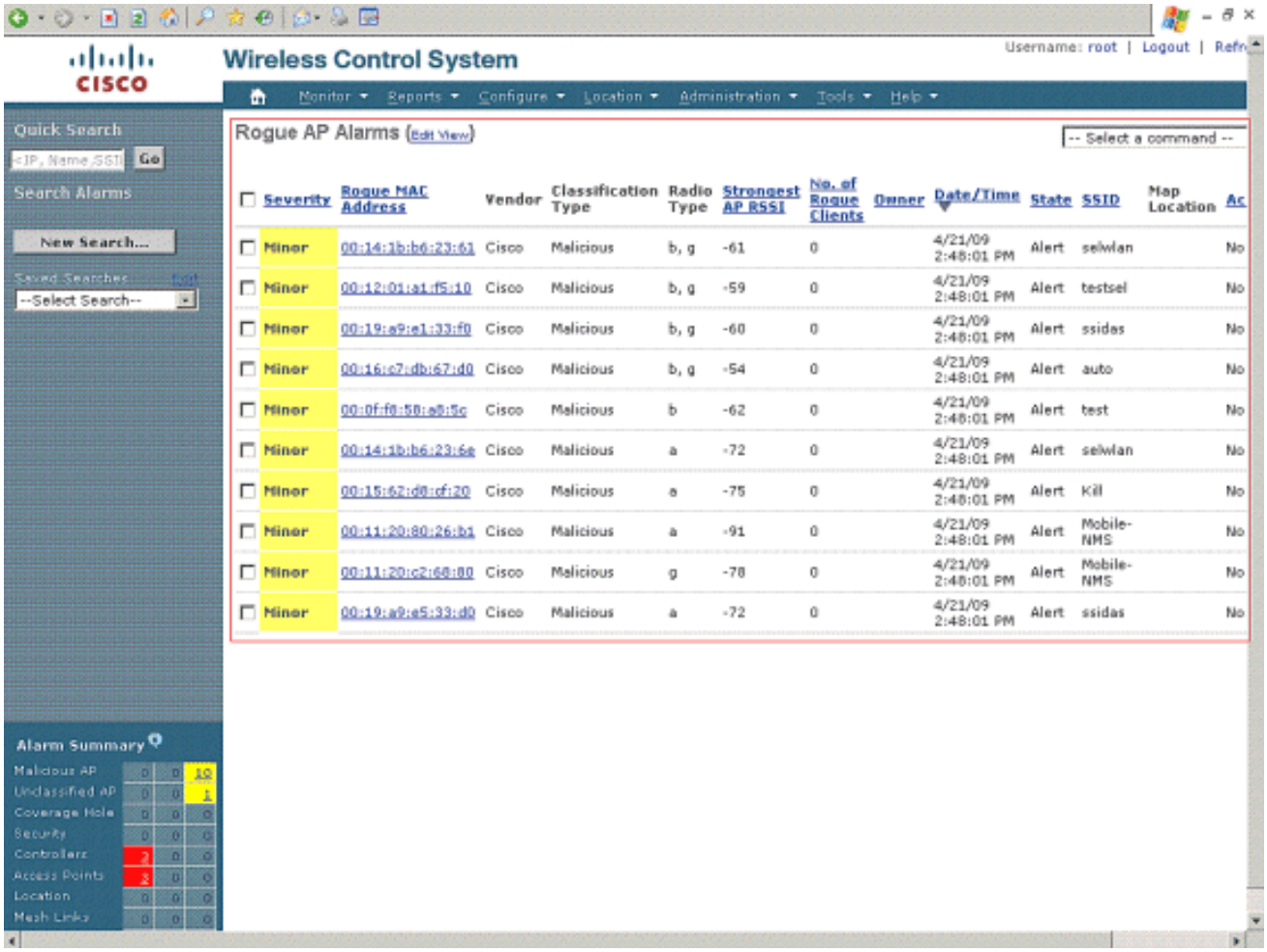
9. Una vez que las reglas se aplican a los reguladores, usted ve un **Mensaje de éxito** en el WCS.



10. Los detalles sobre los APs clasificados se pueden ver en la **página de resumen de la Seguridad**. Esto es un ejemplo.



11. Los detalles sobre los APs clasificados, los APs específicamente malévolos, cómodos, y sin clasificar, pueden ser vistos cuando usted hace clic la clasificación apropiada de la página de resumen de la Seguridad. Esto es un ejemplo para los APs malévolos.



Información Relacionada

- Detección no fiable bajo redes inalámbricas unificadas
- Soporte Técnico y Documentación - Cisco Systems