

# Clasificación rogue basada en las reglas en los reguladores del Wireless LAN (WLC) y el sistema de control inalámbrico (WCS)

## Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Clasificación rogue basada en las reglas](#)

[Terminologías rogue basadas en las reglas de la clasificación](#)

[Reglas rogue de la clasificación](#)

[Clasificación rogue y estados agresores](#)

[Estados agresores explicados](#)

[Cómo configurar las reglas rogue en el WLC](#)

[Cómo configurar las reglas rogue en el WCS](#)

[Información Relacionada](#)

## Introducción

En la versión inalámbrica 5.0 del sistema de control (WCS), el WCS aumentó la funcionalidad de administración rogue para diversos tipos del granuja AP y con tal que las reglas definidas por el usuario para clasificar automáticamente al granuja AP. El WCS aplicó las reglas rogue de la clasificación AP a los reguladores. Este documento explica la funcionalidad de administración rogue aumentada y los pasos necesarios configurar estas funciones en el regulador del Wireless LAN (WLC) y el WCS.

## prerrequisitos

### Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Conocimiento del protocolo del Lightweight Access Point (LWAPP)
- Conocimiento de las soluciones acerca de la seguridad del regulador del Wireless LAN

## Componentes Utilizados

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

hardware.

- WLC de las Cisco 4400 Series que funciona con el firmware 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 rogue basada en las reglas](#)

En las versiones WCS antes de la versión 5.0, el WCS visualizó demasiado (APS) de los puntos de acceso no autorizado 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 rogue 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 usuario para clasificar automáticamente al granuja AP. El WCS aplicó las reglas rogue 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 soportar esta característica, el WLC y el WCS deben funcionar con la versión 5.0.

## [Terminologías rogue basadas en las reglas de la clasificación](#)

Con estas nuevas funciones, presentan a estos nuevos tipos del granuja AP:

- **AP malévolo:** Un AP detectado que hace juego las reglas malévolas definidas por el usuario o se ha movido manualmente desde los AP cómodos.
- **AP cómodo:** La existencia sabida, reconoce, y clasifican a los estados agresores que falta de la confianza como cómodos. Además, los AP detectados que hacen juego las reglas cómodas definidas por el usuario se clasifican como cómodos. Los AP 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 usuario para mover automáticamente el AP sin clasificar a cómodo o a malévolo, por ejemplo, en la detección, el SSID están vacías. En el informe rogue siguiente, se encuentra un SSID, y resulta ser usuario configurado SSID.

## Reglas rogue de la clasificación

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

- Reglas malévolas Las coincidencias manejan el SSID Hace juego al usuario configurado SSID No encryption en un SSID Mínimo RSSI Duración del tiempo Número de clientes asociados
- Reglas cómodas SSID manejado Usuario configurado SSID
- Reglas sin clasificar No 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.  <b>Note</b> WCS refers to this option as "Open Authentication."
Managed SSID <sup>1</sup>	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 <sup>1</sup>	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 <b>Add SSID</b> . You can add multiple SSIDs.  To remove an SSID, select the SSID and click <b>Remove</b> .

<sup>1</sup>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 rogue, hace esto:

- Marca 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 el estado rogue 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 clasifíquelo 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 el estado rogue como **amenaza** y clasifíquelo 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 rogue 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 AP 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** — El AP detectado es haber contenido marcado, 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 AP 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 AP que pertenecen a una red vecina.
- **Desaparecidos de confianza** — Si detectaron y no se oye al usuario configurado MAC



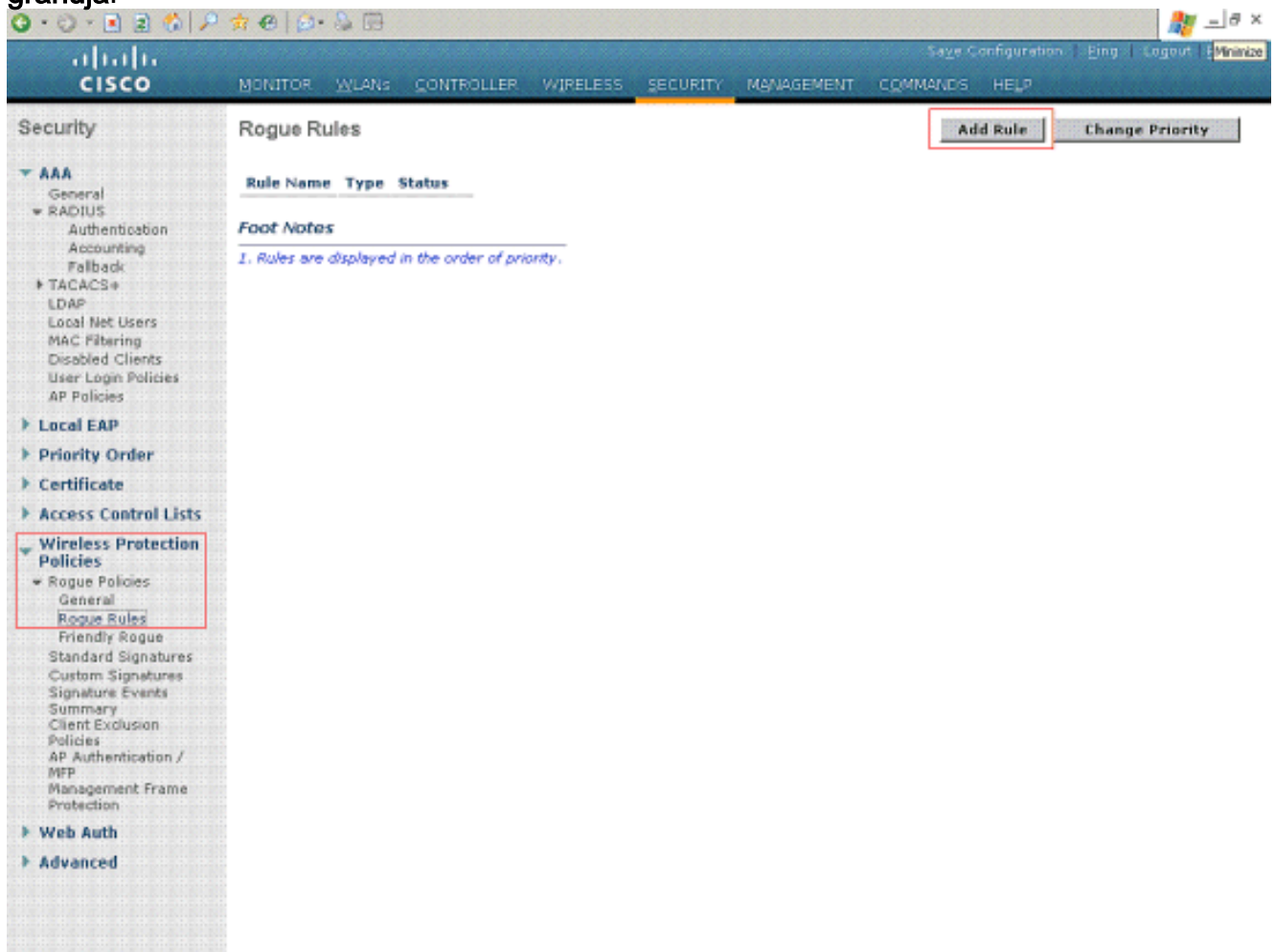
cómo para la duración del confianza-descanso, marcan al estado agresor del AP cómo como desaparecidos de confianza.

- **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 rogue en el WLC

Para configurar las reglas rogue en el regulador del Wireless LAN, complete estos pasos.

1. Las reglas rogue 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 rogue, 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.

The screenshot shows the Cisco Security configuration page for Rogue Rules. The navigation menu on the left includes sections like AAA, RADIUS, TACACS+, Local EAP, Priority Order, Certificate, Access Control Lists, Wireless Protection Policies, and Web Auth. The main content area displays a table of rules:

Rule Name	Type	Status
<a href="#">Rule1</a>	Malicious	Disabled <input type="checkbox"/>

Below the table, there is a 'Foot Notes' section with the following note:

1. Rules are displayed in the order of priority.

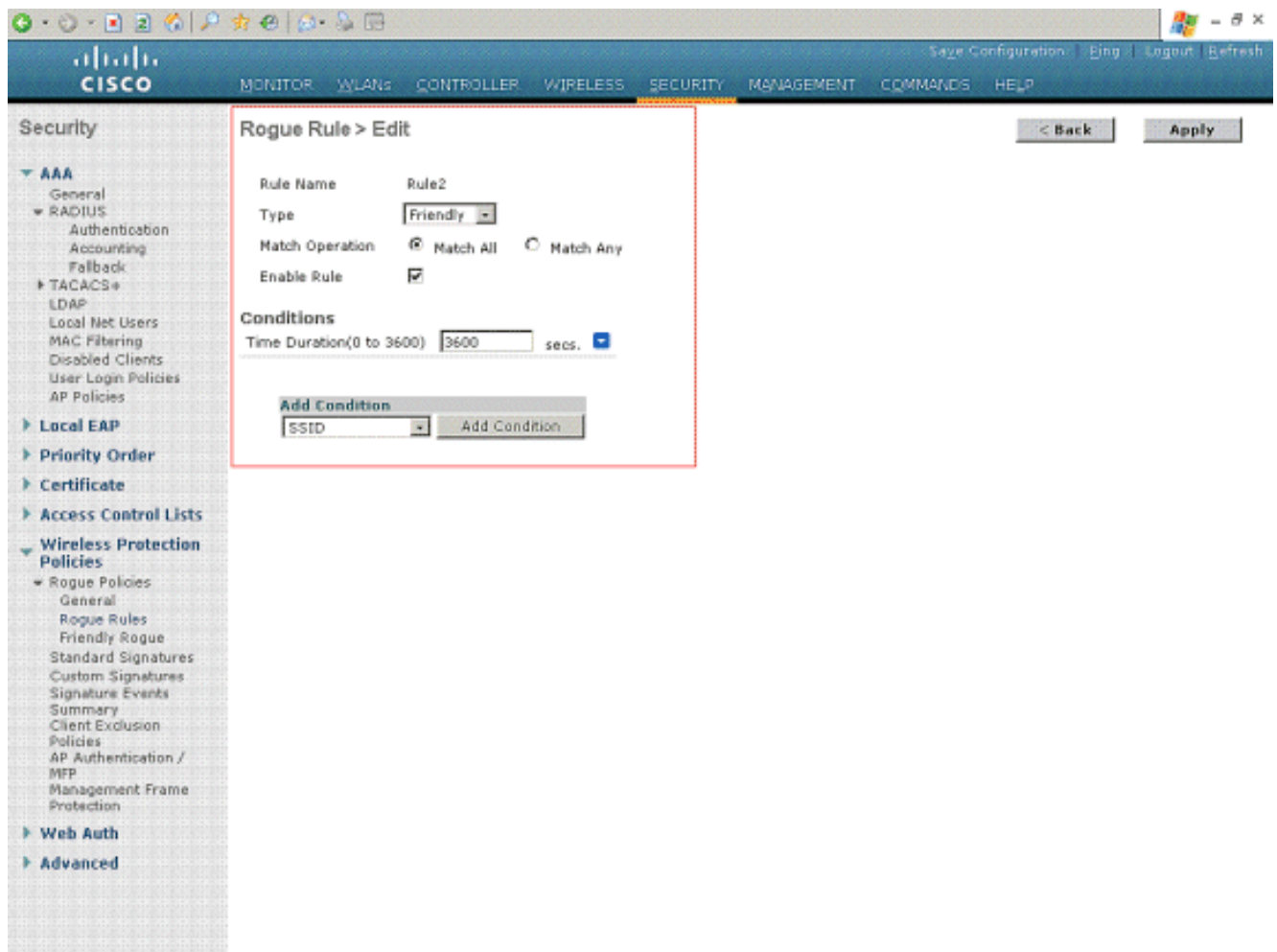
3. Para editar esta regla, haga clic la regla que fue creada. **La regla rogue > edita la página** aparece. En esta página, marque la casilla de verificación de la **regla del permiso** para activar la regla. Elija el tipo de operación de la coincidencia y otras condiciones basados en el requisito como en este ejemplo.

The screenshot displays the Cisco Security configuration interface. The top navigation bar includes 'MONITOR', 'WLAN', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', and 'HELP'. The 'SECURITY' tab is active. On the left, a sidebar menu shows 'Security' expanded, with 'Wireless Protection Policies' selected. Under 'Wireless Protection Policies', 'Rogue Policies' is expanded, and 'Rogue Rules' is selected. The main content area is titled 'Rogue Rule > Edit'. It contains the following fields and options:

- Rule Name:** Rule1
- Type:** Malicious
- Match Operation:** Match All (radio button), Match Any (radio button, selected)
- Enable Rule:**
- Conditions:**
  - Minimum RSSI(-95 to -50): -85 dBm
  - Time Duration(0 to 3600): 3600 secs.
  - No Encryption:
  - Managed SSID:
  - User configured SSID: Admin
- Add Condition:** Client Count

Buttons for '< Back' and 'Apply' are located at the top right of the configuration area.

4. Éste es un ejemplo de la directiva rogue cómoda de la regla.



5. La salida de las reglas rogue se puede considerar en el monitor > los granujas > AP malévolo.



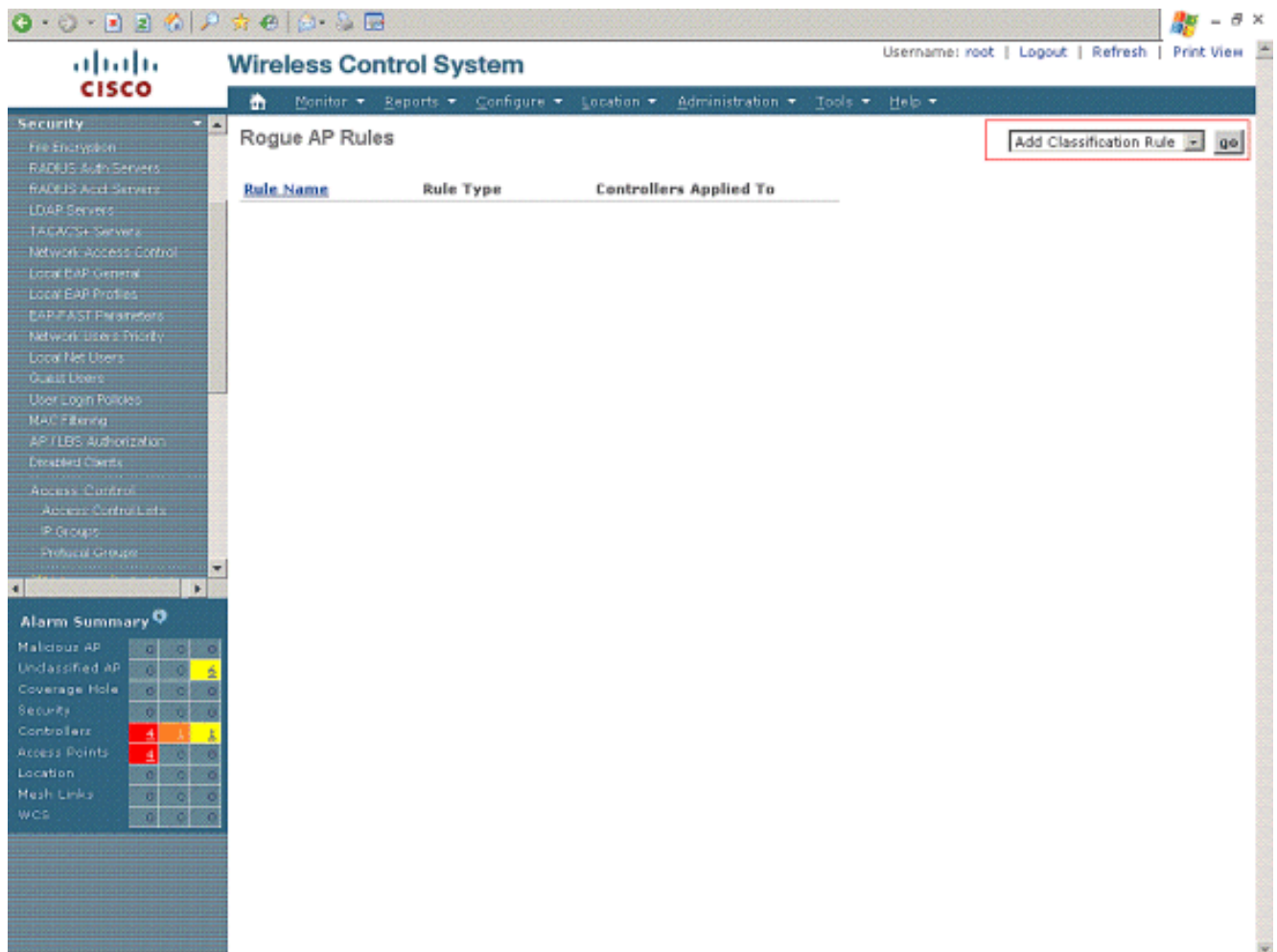
MAC Address	SSID	# Detecting Radios	Number of Clients	Status
<a href="#">00:0f:f8:58:a8:5c</a>	test	1	0	Alert
<a href="#">00:11:20:80:26:b1</a>	Mobile-NMS	1	0	Alert
<a href="#">00:11:20:c2:68:80</a>	Mobile-NMS	1	0	Alert
<a href="#">00:12:01:a1:f5:10</a>	testsel	1	0	Alert
<a href="#">00:14:1b:b6:23:61</a>	selwlan	1	0	Alert
<a href="#">00:14:1b:b6:23:6e</a>	selwlan	1	0	Alert
<a href="#">00:15:62:d8:cf:20</a>	Kill	1	0	Alert
<a href="#">00:16:e7:db:d7:d0</a>	auto	1	0	Alert
<a href="#">00:19:a9:e1:33:f0</a>	ssidas	1	0	Alert
<a href="#">00:19:a9:e5:33:d0</a>	ssidas	1	0	Alert

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 rogue en el WCS

**Lista rogue de la regla:** El WCS proporciona el nivel del sistema configuración rogue de la regla. Para configurar las reglas rogue en el WCS, complete estos pasos.

1. Elija la configuración > la plantilla del regulador, y después haga clic las reglas de la Seguridad > del granuja AP para acceder 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 editar la regla rogue. Esta página del detalle de la regla le permite para editar, para poner al día la regla del granuja AP, o para borrar la regla. **Parámetros rogue de la configuración de la regla AP:** En esta página, los usuarios pueden habilitar cualquier condición cuando marcan la casilla de verificación para concatenar el cualquiera o todo el de estas condiciones: No encryption AP manejado coincidencia Usuario configurado SSID de la coincidencia Mínimo RSSIDuración Cliente rogue del número mínimo Éste es un ejemplo de una regla malévola:

Wireless Control System Username: root | Logout | Refresh | Print View

Monitor | Reports | Configure | Location | Administration | Tools | Help

### Rogue AP Rules > New Template

**General**

Rule Name:   
 Rule Type:   
 Match Type:

**Malicious Rogue Classification Rule**

Open Authentication:   
 Match Managed AP SSID:   
 Match User Configured SSID:   
 (Enter one per line)

Minimum RSSI:  dB   
 Time Duration:  seconds   
 Minimum Number Rogue Clients:

Note: Rogue AP Rule template can be selected by Rogue AP Rule Group template. Rogue AP Rule template gets applied to the controllers when Rogue AP Rule Group template gets applied to the controllers.

**Alarm Summary**

Malicious AP	0	0	0
Unclassified AP	0	0	0
Coverage Hole	0	0	0
Security	0	0	0
Controllers	4	1	1
Access Points	4	0	0
Location	0	0	0
Mesh Links	0	0	0

Éste es un ejemplo de una regla cómoda:

The screenshot displays the Cisco Wireless Control System (WCS) interface. The main configuration area is titled "Rogue AP Rules > Rule1". Under the "General" section, the following fields are visible:

- Rule Name: Rule2
- Rule Type: Friendly
- Match Type: Match Any Condition

Under the "Malicious Rogue Classification Rule" section, the following options are visible:

- Open Authentication:
- Match Managed AP SSID:
- Match User Configured SSID (Enter one per line): [Empty text area]
- Minimum RSSI: -70 dB
- Time Duration: 1440 seconds
- Minimum Number Rogue Clients: 10

At the bottom of the configuration area, there are "Save", "Delete", and "Cancel" buttons. A note below the buttons states: "Note: Rogue AP Rule template can be selected by Rogue AP Rule Group template. Rogue AP Rule template gets applied to the controllers when Rogue AP Rule Group template gets applied to the controllers."

On the left side, there is an "Alarm Summary" table:

Alarm Summary	0	0	0
Malicious AP	0	0	0
Unclassified AP	0	0	0
Coverage Hole	0	0	0
Security	0	0	0
Controllers	4	1	1
Access Points	4	0	0
Location	0	0	0
Mesh Links	0	0	0

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

The screenshot shows the Cisco Wireless Control System (WCS) interface. The main content area is titled "Rogue AP Rules" and contains a table with the following data:

Rule Name	Rule Type	Controllers Applied To
<a href="#">Rule2</a>	Friendly	0
<a href="#">Rule1</a>	Malicious	0

The left sidebar shows the navigation menu with "Security" expanded to "Rogue AP Rules". An "Alarm Summary" widget at the bottom left shows various system metrics:

Alarm Summary	Count	Color
Malicious AP	0	Green
Unclassified AP	0	Yellow
Coverage Hole	0	Green
Security	0	Green
Controllers	4	Yellow
Access Points	1	Red
Location	0	Green
Mesh Links	0	Green

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 la **configuración > la plantilla del regulador**, y después haga clic a los **grupos de reglas de la Seguridad > del granuja AP** del WCS GUI.



The screenshot shows the Cisco Wireless Control System interface. The main content area is titled "Rogue AP Rule Groups" and contains a table with the following structure:

Rule Group Name	No of Controllers Applied To

At the bottom left, there is an "Alarm Summary" widget with the following data:

Alarm Category	Count	Color
Malicious AP	0	Green
Unclassified AP	0	Yellow
Coverage Hole	0	Green
Security	0	Green
Controllers	1	Yellow
Access Points	1	Red
Location	0	Green
Mesh Links	0	Green

7. Los grupos de reglas del granuja AP > nueva página de la plantilla le permiten para agregar, para poner al día el grupo de reglas del granuja AP, para borrar la regla, y para 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** teclado.

The screenshot shows the Cisco Wireless Control System (WCS) interface. The main content area is titled "Rogue AP Rule Groups > New Template". Under the "General" tab, the "Rule Group Name" is set to "Rogue-Rule-Group-1". The "Edit View" section contains instructions: "Use the **Add/Remove** buttons to select the Rogue AP rules for this Rule Group. Use the **Move Up/Move Down** buttons to specify the order in which the rules are applied." Below this, there are two empty boxes representing rule lists, with "Add >" and "< Remove" buttons between them, and "Move Up" and "Move Down" buttons to the right. At the bottom of the main area are "Save" and "Cancel" buttons. A note states: "Note: Rogue AP Rule(s) can be added from 'Rogue AP Rules' section." On the left, a navigation menu lists various system components, and an "Alarm Summary" table is visible at the bottom left.

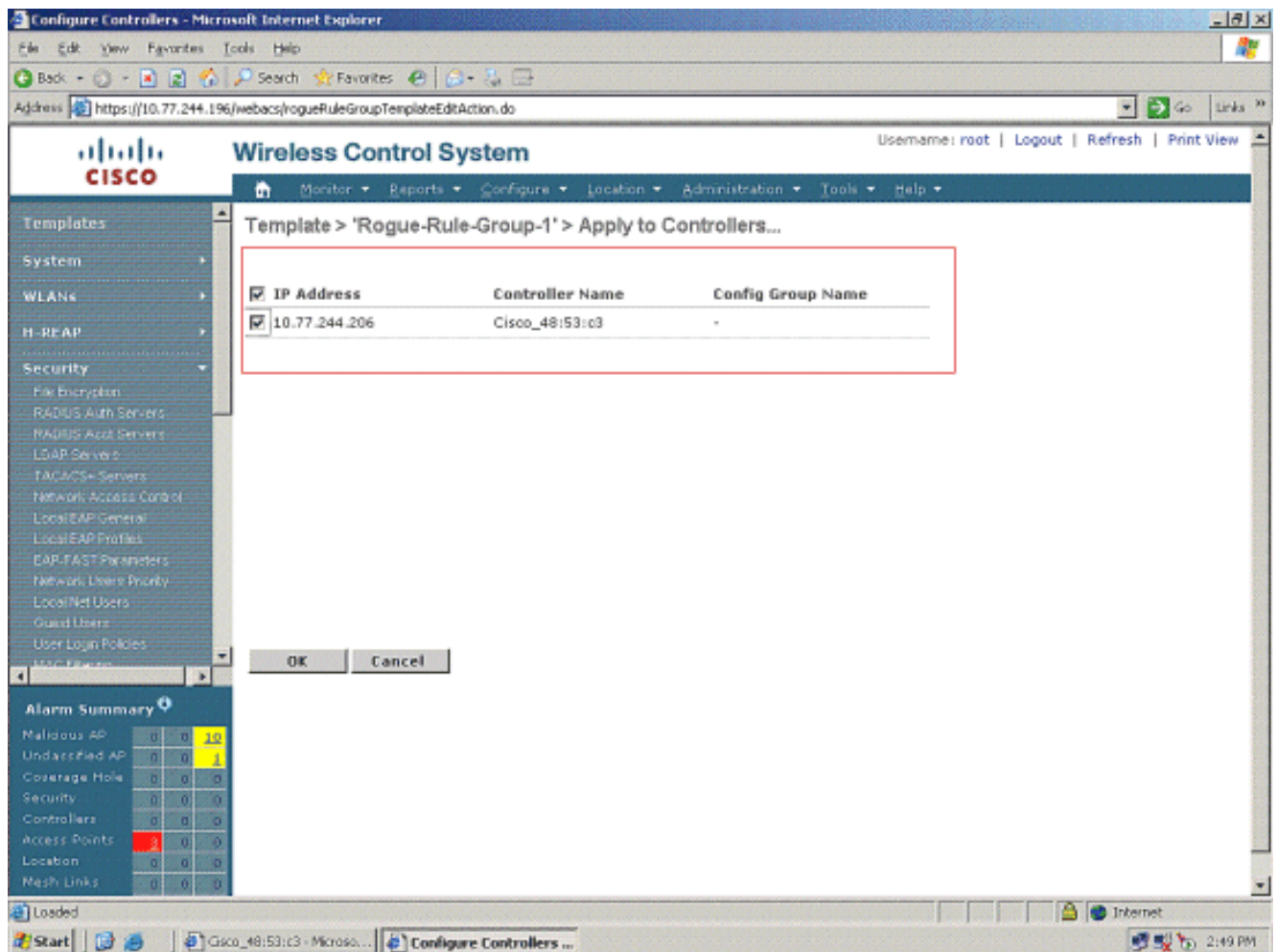
Alarm Summary			
Malicious AP	0	0	0
Unclassified AP	0	0	0
Coverage Hole	0	0	0
Security	0	0	0
Controllers	4	1	1
Access Points	1	0	0
Location	0	0	0
Mesh Links	0	0	0

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

The screenshot shows the Cisco Wireless Control System (WCS) interface. The left sidebar contains a navigation menu with categories like Templates, System, WLANs, H-REAP, and Security. The main content area is titled 'Rogue AP Rule Groups > Rogue-Rule-Group-1'. Under the 'General' tab, the 'Rule Group Name' is set to 'Rogue-Rule-Group-1'. The 'Edit View' section contains two empty boxes for rules, with 'Add >' and '< Remove' buttons between them, and 'Move Up' and 'Move Down' buttons to the right. At the bottom, there are buttons for 'Save', 'Apply to Controllers ...', 'Delete', and 'Cancel'. The 'Apply to Controllers ...' button is highlighted with a red box. A note below the buttons states: 'Note: Rogue AP Rule(s) can be added from "Rogue AP Rules" section.' At the bottom left, there is an 'Alarm Summary' table.

Alarm Summary			
Malicious AP	0	0	0
Unclassified AP	0	0	0
Coverage Hole	0	0	0
Security	0	0	0
Controllers	4	1	1
Access Points	1	0	0
Location	0	0	0
Mesh Links	0	0	0

El teclado **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.

The screenshot shows the Cisco Wireless Control System (WCS) interface. The main content area displays the results of applying a template to controllers. The table below shows the results:

IP Address	Controller Name	Operation Status	Reason
10.77.244.206	Cisco_48:53:c3	Success	-

The interface also includes a navigation menu on the left and an 'Alarm Summary' section at the bottom left, which shows the following data:

Alarm Category	Count
Malicious AP	10
Undesired AP	1
Coverage Hole	0
Security	0
Controllers	0
Access Points	3
Location	0
Mesh Links	0

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



Wireless Control System Username: root | Logout | Refresh | Print View

Monitor Reports Configure Location Administration Tools Help

**Security**

Summary

Malicious Rogue APs

Friendly Rogue APs

Unclassified Rogue APs

Rogue AdHocs

Rogue Clients

Shunned Clients

---

**Alarm Summary**

Malicious AP	0	0	10
Unclassified AP	0	0	1
Coverage Hole	0	0	0
Security	0	0	0
Controllers	0	0	0
Access Points	2	0	0
Location	0	0	0
Mesh Links	0	0	0
WCS	0	0	0

### Security Summary

Malicious Rogue APs	Last Hour	24 Hours	Total Active	Signature Attacks	Last Hour	24 Hours	Total Active	AP Threats/Attacks	Last Hour	24 Hours	Total Active
Alert	10	10	10	Custom	0	0	0	Fake AP Attack	0	0	0
Contained	0	0	0	NULL probe resp 1	0	0	0	AP Missing	0	0	0
Threat	0	0	0	Broadcast Probe flood	0	0	0	AP Impersonation	0	0	0
Contained Pending	0	0	0	EAPOL flood	0	0	0	AP Invalid SSID	0	0	0
802.11a/n5.0	4	4	4	Reserved mgmt F	0	0	0	AP Invalid Preamble	0	0	0
802.11b/g/n2.4	6	6	6	Boast deauth	0	0	0	AP Invalid Encryption	0	0	0
On Network	0	0	0	Reassoc flood	0	0	0	AP Invalid Radio Policy	0	0	0
Off Network	10	10	10	Disassoc flood	0	0	0	Denial of Service (NAV related)	0	0	0
				Auth flood	0	0	0				
Friendly Rogue APs	Last Hour	24 Hours	Total Active	NetStumbler 3.2.3	0	0	0	Client Security Related	Last Hour	24 Hours	Total Active
Alert	0	0	0	NetStumbler 3.3.0	0	0	0	Excluded Client Events	0	0	0
Internal	0	0	0	Deauth flood	0	0	0	WEP Decrypt Errors	0	0	0
External	0	0	0	Wellenreiter	0	0	0	WPA MIC Errors	0	0	0
802.11a/n5.0	0	0	0	NetStumbler generic	0	0	0	Shunned Clients	0	0	0
802.11b/g/n2.4	0	0	0	NetStumbler 3.2.0	0	0	0	IPSEC Failures	0	0	0
Unclassified Rogue APs	Last Hour	24 Hours	Total Active	Reserved mgmt 7	0	0	0				
Alert	0	0	1	Assoc flood	0	0	0				
Contained	0	0	0	NULL probe resp 2	0	0	0				
Contained Pending	0	0	0								
802.11a/n5.0	0	0	0								
802.11b/g/n2.4	0	0	1								

11. Los detalles sobre los AP clasificados, los AP 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 AP malévolos.

Wireless Control System Username: root | Logout | Refr...

Monitor | Reports | Configure | Location | Administration | Tools | Help

Quick Search: [IP, Name, SSID]

Search Alarms:

Saved Searches:

Alarm Summary

Malicious AP	0	0	10
Unclassified AP	0	0	1
Coverage Hole	0	0	0
Security	0	0	0
Controllers	2	0	0
Access Points	2	0	0
Location	0	0	0
Mesh Links	0	0	0

Rogue AP Alarms [Edit View](#) -- Select a command --

<input type="checkbox"/>	Severity	Rogue MAC Address	Vendor	Classification Type	Radio Type	Strongest AP RSSI	No. of Rogue Clients	Owner	Date/Time	State	SSID	Map Location	Ac
<input type="checkbox"/>	Minor	<a href="#">00:14:1b:b6:23:61</a>	Cisco	Malicious	b, g	-61	0		4/21/09 2:48:01 PM	Alert	selwan	No	
<input type="checkbox"/>	Minor	<a href="#">00:12:01:a1:f5:d0</a>	Cisco	Malicious	b, g	-59	0		4/21/09 2:48:01 PM	Alert	testsel	No	
<input type="checkbox"/>	Minor	<a href="#">00:19:a9:e1:33:f0</a>	Cisco	Malicious	b, g	-60	0		4/21/09 2:48:01 PM	Alert	ssidas	No	
<input type="checkbox"/>	Minor	<a href="#">00:16:e7:db:67:d0</a>	Cisco	Malicious	b, g	-54	0		4/21/09 2:48:01 PM	Alert	auto	No	
<input type="checkbox"/>	Minor	<a href="#">00:0f:f0:58:a0:5c</a>	Cisco	Malicious	b	-62	0		4/21/09 2:48:01 PM	Alert	test	No	
<input type="checkbox"/>	Minor	<a href="#">00:14:1b:b6:23:6a</a>	Cisco	Malicious	a	-72	0		4/21/09 2:48:01 PM	Alert	selwan	No	
<input type="checkbox"/>	Minor	<a href="#">00:15:67:d0:0f:20</a>	Cisco	Malicious	a	-75	0		4/21/09 2:48:01 PM	Alert	Kil	No	
<input type="checkbox"/>	Minor	<a href="#">00:11:20:80:26:b1</a>	Cisco	Malicious	a	-91	0		4/21/09 2:48:01 PM	Alert	Mobile-NMS	No	
<input type="checkbox"/>	Minor	<a href="#">00:11:20:c2:68:80</a>	Cisco	Malicious	g	-78	0		4/21/09 2:48:01 PM	Alert	Mobile-NMS	No	
<input type="checkbox"/>	Minor	<a href="#">00:19:a9:e5:33:d0</a>	Cisco	Malicious	a	-72	0		4/21/09 2:48:01 PM	Alert	ssidas	No	

## Información Relacionada

- [Detección rogue bajo redes inalámbricas unificadas](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)