

Classificação desonesto baseada regra nos controladores do Wireless LAN (WLC) e no sistema de controle sem fio (WCS)

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenções](#)

[Classificação desonesto baseada regra](#)

[Terminologias desonestos baseadas regra da classificação](#)

[Regras desonestos da classificação](#)

[Classificação desonesto e estado fora da lei](#)

[Estado fora da lei explicados](#)

[Como configurar regras desonestos em WLC](#)

[Como configurar regras desonestos no WCS](#)

[Informações Relacionadas](#)

[Introdução](#)

Na liberação 5.0 sem fio do sistema de controle (WCS), o WCS aumentou a funcionalidade de gerenciamento desonesto para tipos diferentes AP do rogue e desde que regras definidas pelo utilizador para classificar automaticamente o rogue APs. O WCS aplicou regras desonestos da classificação AP aos controladores. Este original explica a funcionalidade de gerenciamento desonesto aumentada e as etapas necessárias configurar esta funcionalidade no controlador do Wireless LAN (WLC) e no WCS.

[Pré-requisitos](#)

[Requisitos](#)

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Conhecimento do protocolo de pouco peso do Access point (LWAPP)
- Conhecimento de soluções da Segurança do controlador do Wireless LAN

[Componentes Utilizados](#)

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco 4400 Series WLC que executa o firmware 5.2
- Lightweight Access Points do Cisco Aironet série 1130 AG (regaços)
- Versão 5.2 do Sistema de controle sem fio da Cisco

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

Consulte as [Convenções de Dicas Técnicas da Cisco](#) para obter mais informações sobre convenções de documentos.

Ordene a classificação desonesto baseada

Em versões WCS antes da liberação 5.0, o WCS indicou Access point desonestos demais (APs) na **página de sumário da Segurança**. Mesmo que os estado fora da lei difiram, todos aparecem em uma página, classificada pelo MAC address BSSID/do rogue.

Na liberação WCS 5.0, o WCS aumentou a funcionalidade de gerenciamento desonesto e introduziu terminologias novas (não classificado, malicioso, e amigável) para tipos diferentes AP do rogue e desde que regras definidas pelo utilizador para classificar automaticamente o rogue APs. O WCS aplicou regras desonestos da classificação AP aos controladores.

O WCS aumentou a função de gerenciamento do estado fora da lei para manter o estado fora da lei como *externo* uma vez que o estado de rogue foi mudado manualmente a *externo*. O WCS igualmente atualiza o estado *externo* para os outros controladores quando o WCS puxa ou segura o mensagem de armadilha dos outros controladores.

A fim apoiar esta característica, WLC e o WCS devem executar a liberação 5.0.

Terminologias desonestos baseadas regra da classificação

Com esta funcionalidade nova, estes tipos novos AP do rogue são introduzidos:

- **AP malicioso:** Um AP detectado que combine regras maliciosas definidas pelo utilizador ou fosse movido manualmente dos APs amigáveis.
- **AP amigável:** Existir conhecida, reconhece, e os estado fora da lei faltantes da confiança são classificados como amigáveis. Além, os APs detectados que combinam regras amigáveis definidas pelo utilizador são classificados como amigáveis. Os APs amigáveis não podem ser contidos.
- **AP não classificado:** Um AP detectado que não combinasse as regras maliciosas ou amigáveis. Um AP não classificado pode ser contido. Um AP não classificado pode manualmente ser movido para amigável pelo usuário. As regras definidas pelo utilizador para mover automaticamente AP não classificado para amigável ou malicioso, por exemplo, na detecção, o SSID estão vazias. No relatório desonesto seguinte, um SSID é encontrado, e despeja ser um configurado pelo usuário SSID.

Regras desonestos da classificação

Estas são regras da classificação aplicáveis a cada um dos tipos AP do rogue:

- Regras maliciosas Os fósforos controlaram o SSID Combina o configurado pelo usuário SSID No encryption em um SSID Mínimo RSSI Duração do tempo Número de clientes associados
- Regras amigáveis SSID controlado Configurado pelo usuário SSID
- Regras não classificadas Não combina regras maliciosas ou amigáveis

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 .

¹The 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.

O usuário pode escolher combinar **todas as**, ou **algumas** condições da regra sob cada regra:

- **Todos os** meios combinam todas as condições configuradas para a regra.
- **Alguns** meios combinam algumas das condições configuradas para a regra.
- **Alguns** meios combinam poucas das condições configuradas para a regra

Por exemplo, sob *regras maliciosas*, o usuário configura *SSID controlado* e *mínimo RSSI*. Então, o usuário tem a escolha para combinar **todas as** ou **algumas** duas circunstâncias, ou combine apenas a condição do *mínimo RSSI*.

Quando o controlador recebe o relatório desonesto, faz este:

- Verifica se o AP detectado está na lista do configurado pelo usuário MAC. Em caso afirmativo, classifique o AP como um tipo amigável.
- Se o AP detectado não está na lista, começa aplicar as regras.
- Primeiramente, aplica *regras maliciosas*. Se as *regras maliciosas* combinam, está classificado

como o tipo malicioso. Se o detector RLDP/rogue determina que este rogue está na rede, marca o estado fora da lei como uma **ameaça**. O usuário pode manualmente conter o AP que muda o estado fora da lei ao **contido**. Se o AP não está na rede, marca o estado fora da lei como o **alerta**, e o usuário pode contê-lo manualmente.

- Se as *regras maliciosas* não combinam, aplique *regras amigáveis*. Se as *regras amigáveis* combinam, a seguir classifique-o como um tipo amigável.
- Se as *regras amigáveis* não combinam, classifique este AP como não classificado. Se o detector RLDP/rogue determina que este rogue está na rede, marque o estado fora da lei como uma **ameaça** e classifique-o como um tipo malicioso. O usuário pode manualmente conter o AP que muda o estado fora da lei ao **contido**. Se o AP não está na rede, marque o estado fora da lei como o **alerta**, e o usuário pode contê-lo manualmente.
- O usuário pode manualmente mover o AP para um tipo diferente da classificação.

Classificação desonesto e estado fora da lei

Esta tabela mostra as classificações diferentes dos rogues e os estado fora da lei para cada classificação.

Tipo baseado em regras da classificação	Estado fora da lei
AP malicioso	A ameaça alerta contida conteve durante removido
AP não classificado	O alerta contido conteve durante removido
AP amigável	(Sabido atualmente) (reconheça atualmente) (alerta faltante interno externo interno dos desaparecidos da confiança)

Estado fora da lei explicados

- **Durante** — Na primeira detecção, o AP detectado é posto no estado pendente por 3 minutos. Esta vez é suficiente para que os APs controlados determinem se o AP detectado é um vizinho AP.
- **Alerta** — Após o intervalo 3-minute, o AP detectado está movido **para alertar** se não está na lista vizinha ou na lista amigável do configurado pelo usuário MAC.
- **Ameaça** — O AP detectado é encontrado na rede.
- **Contido** — O AP detectado é contido.
- **Contido durante** — O AP detectado é marcado conteve, mas a ação da retenção é atrasada devido aos recursos não disponíveis.
- **Interno** — O AP detectado é dentro da rede, e o usuário configurar-la manualmente como **amigável, interno**, por exemplo, os APs em uma rede de laboratório.
- **Externo** — O AP detectado é fora da rede, e o usuário configurar-la manualmente como **amigável, externo**, por exemplo, os APs que pertencem a uma rede vizinha.
- **Desaparecidos confiados** — Se o configurado pelo usuário MAC amigável foi detectado e não é ouvido para a duração do confiança-intervalo, o estado fora da lei do AP amigável é

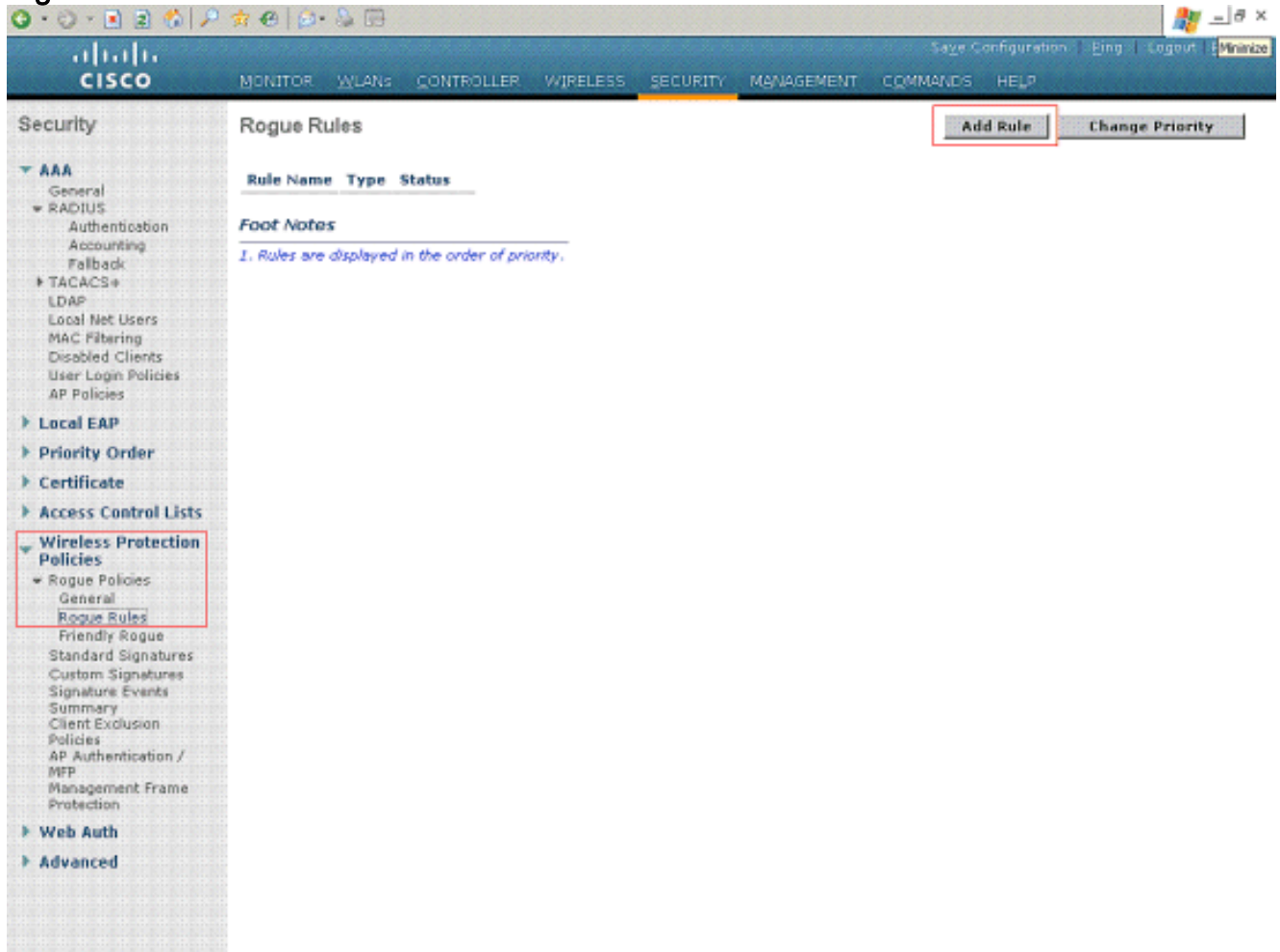
marcado como desaparecidos confiados.

- **Removido** — Se o AP malicioso ou não classificado não é ouvido de todos os controladores para a duração do rogue-intervalo, o estado fora da lei do AP está marcado como **removido**.

Como configurar regras desonestos em WLC

A fim configurar regras desonestos no controlador do Wireless LAN, termine estas etapas.

1. As regras desonestos podem ser criadas do WLC da **Segurança > página sem fio das políticas da proteção > das políticas do rogue > das regras do rogue**.



2. A fim criar uma política desonesto nova, clique o botão da **regra adicionar**. O indicador das **regras do rogue** aparece. Dê entrada com um nome para a regra. Este exemplo usa Rule1. Escolha o tipo de regra. Este é um exemplo de uma regra maliciosa. Clique em Add. Rule1 é criado.

The screenshot shows the Cisco Security configuration interface. The main content area is titled "Rogue Rules" and contains a table with the following data:

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

Below the table, there is a "Foot Notes" section with the following text:

1. Rules are displayed in the order of priority.

On the left side, there is a navigation menu under "Security" with various categories like AAA, RADIUS, TACACS+, Local EAP, Priority Order, Certificate, Access Control Lists, Wireless Protection Policies, Web Auth, and Advanced. The "Wireless Protection Policies" category is expanded to show "Rogue Policies" with sub-items like General, Rogue Rules, Friendly Rogue, Standard Signatures, Custom Signatures, Signature Events, Summary, Client Exclusion, Policies, AP Authentication / MFP, Management Frame Protection.

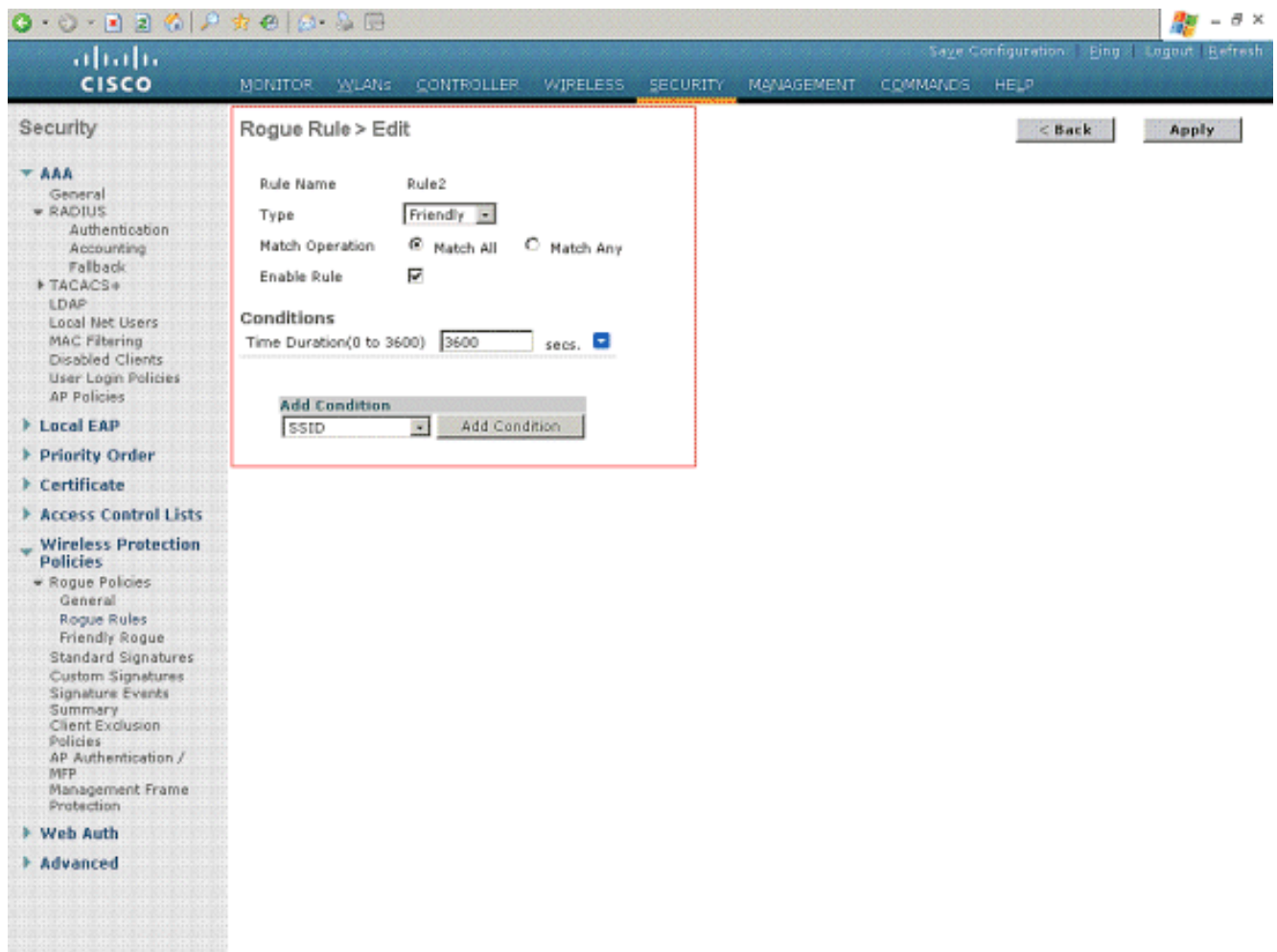
3. A fim editar esta regra, clique a regra que foi criada. **A regra desonesto > edita a página** aparece. Nesta página, verifique a caixa de verificação da **regra da possibilidade** para ativar a regra. Escolha o tipo de operação do fósforo e outras circunstâncias baseados na exigência como neste exemplo.

The screenshot displays the Cisco Security configuration page for a Rogue Rule. The interface includes a top navigation bar with tabs for MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, COMMANDS, and HELP. The left sidebar shows a tree view under Security, with Wireless Protection Policies expanded to Rogue Policies. The main content area is titled "Rogue Rule > Edit" and contains the following configuration fields:

- Rule Name:** Rule1
- Type:** Malicious
- Match Operation:** Match Any (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. Este é um exemplo da política desonesto amigável da regra.



5. A saída das regras desonestos pode ser considerada no **monitor > nos rogues > AP malicioso**.

The screenshot shows the Cisco WCS interface with the 'Monitor' tab selected. The left sidebar contains a navigation menu with 'Rogues' expanded to 'Malicious APs'. The main content area displays a table titled 'Malicious Rogue APs' with 10 entries. The table columns are: MAC Address, SSID, # Detecting Radios, Number of Clients, and Status. All entries have a status of 'Alert' and 0 clients.

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

6. Similarmente, a saída das *regras amigáveis* e de *regras não classificadas* pode ser vista no monitor > nos rogues > AP não classificado e o monitor > os rogues > páginas amigáveis AP, respectivamente.

Como configurar regras desonestos no WCS

Lista desonesto da regra: O WCS fornece o ajuste desonesto da regra do nível de sistema. A fim configurar regras desonestos no WCS, termine estas etapas.

1. Escolha **configuram > molde do controlador**, e clicam então as **regras AP da Segurança > do rogue** para alcançar a página da lista das regras AP do rogue.
2. O clique **adiciona a regra da classificação** no menu suspenso superior direito para adicionar uma regra nova da classificação.

The screenshot shows the Cisco Wireless Control System (WCS) interface. The top navigation bar includes 'Monitor', 'Reports', 'Configure', 'Location', 'Administration', 'Tools', and 'Help'. The main content area is titled 'Rogue AP Rules' and features a table with columns for 'Rule Name', 'Rule Type', and 'Controllers Applied To'. A red box highlights the 'Add Classification Rule' button in the top right corner. On the left, there is a navigation menu with categories like 'Security' and 'Alarm Summary'.

3. Clique o nome de molde para editar a regra desonesto. Esta página do detalhe da regra permite-o de editar, atualizar a regra AP do rogue, ou de suprimir da regra. **Parâmetros desonestos do ajuste da regra AP:** Nesta página, os usuários podem permitir toda a circunstância quando verificam a caixa de verificação para concatenar algumas ou todas estas circunstâncias: No encryption AP controlado fósforo Configurado pelo usuário SSID do fósforo Mínimo RSSID Duração Cliente desonesto do número mínimo Este é um exemplo de uma regra maliciosa:

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

Este é um exemplo de uma regra amigável:

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

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

Rogue AP Rules > Rule1

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

4. O rogue AP ordena a página alista todas as regras criadas.

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
Rule2	Friendly	0
Rule1	Malicious	0

The left sidebar shows the navigation menu with "Security" expanded. The top right corner shows the user is logged in as "root".

5. A próxima etapa é configurar um grupo da regra e aplicar estas regras aos controladores. Isto, usa os **grupos da regra AP do rogue que ajustam-se no WCS**.
6. A fim criar um grupo novo da regra, escolha **configuram > molde do controlador**, e clicam então **grupos da regra AP da Segurança > do rogue do WCS GUI**.

The screenshot shows the Cisco Wireless Control System (WCS) interface. The main content area is titled 'Rogue AP Rule Groups' and contains a table with the following columns: 'Rule Group Name' and 'No of Controllers Applied To'. The table is currently empty. To the right of the table is a button labeled 'Add Rogue Rule Group' and a 'go' button. The left sidebar contains a navigation menu with categories like Templates, System, WLANs, H-REAP, Security, and Access Control. At the bottom left, there is an 'Alarm Summary' widget showing various system metrics with status indicators.

Rule Group Name	No of Controllers Applied To

7. Os grupos da regra AP do rogue > página nova do molde permitem-no de adicionar, atualizar o grupo da regra AP do rogue, de suprimir da regra, e de aplicar o grupo da regra ao controlador. Use adicionar/botões Remove Button para escolher as regras AP do rogue para este grupo da regra. Use os botões Up/Down para especificar a ordem em que as regras são aplicadas. Este é um exemplo. Uma vez que o grupo das regras é configurado, **salvaguada do clique.**

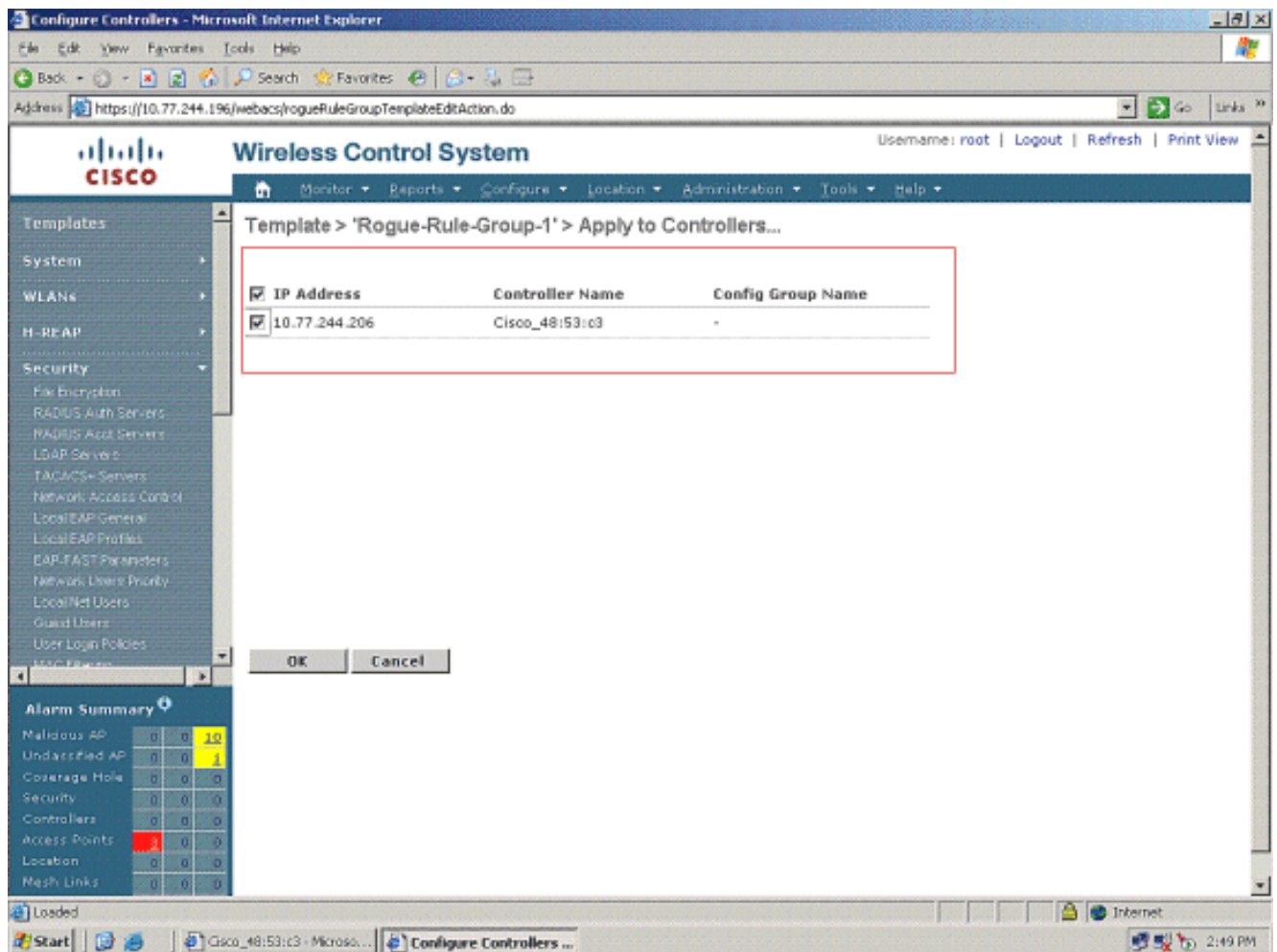
The screenshot displays the Cisco Wireless Control System (WCS) interface. The top navigation bar includes 'Monitor', 'Reports', 'Configure', 'Location', 'Administration', 'Tools', and 'Help'. The left sidebar contains a tree view with categories like 'Templates', 'System', 'WLANs', 'H-REAP', 'Security', 'Access Control', and 'Alarm Summary'. The main content area is titled 'Rogue AP Rule Groups > New Template'. It features a 'General' section with a 'Rule Group Name' field containing 'Rogue-Rule-Group-1'. Below this is an 'Edit View' section with 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.' The 'Edit View' section contains two empty boxes for rule selection, with 'Add >' and '< Remove' buttons between them, and 'Move Up' and 'Move Down' buttons to the right. At the bottom of the 'Edit View' section are 'Save' and 'Cancel' buttons. A note at the bottom reads: 'Note: Rogue AP Rule(s) can be added from "Rogue AP Rules" section.'

- Uma vez que você salvar o grupo da regra, pode ser aplicado aos controladores. A fim aplicar o grupo da regra ao controlador, edite o grupo da regra. Clique o nome do grupo da regra.

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 of the right-hand box. At the bottom, a row of buttons includes "Save", "Apply to Controllers ..." (highlighted with a red box), "Delete", and "Cancel". A note below the buttons states: "Note: Rogue AP Rule(s) can be added from 'Rogue AP Rules' section." In the bottom left corner, 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

O clique **aplica-se aos controladores**. Na página seguinte, escolha os controladores a que esta regra é aplicada. Este é um exemplo.



9. Uma vez que as regras são aplicadas aos controladores, você vê um **mensagem de sucesso** no 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 is a representation of the data shown in the screenshot.

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

The 'Alarm Summary' section at the bottom left of the interface shows the following counts:

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

10. Os detalhes sobre os APs classificados podem ser vistos na **página de sumário da Segurança**. Este é um exemplo.

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
	Last Hour	24 Hours	Total Active	Auth flood	0	0	0		Last Hour	24 Hours	Total Active
Friendly Rogue APs				NetStumbler 3.2.3	0	0	0	Client Security Related			
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
	Last Hour	24 Hours	Total Active	Reserved mgmt 7	0	0	0				
Unclassified Rogue APs				Assoc flood	0	0	0				
Alert	0	0	1	NULL probe resp 2	0	0	0				
Contained	0	0	0								
Contained Pending	0	0	0								
802.11a/n5.0	0	0	0								
802.11b/g/n2.4	0	0	1								

11. Os detalhes sobre os APs classificados, APs especificamente maliciosos, amigáveis, e não classificados, podem ser vistos quando você clica a classificação apropriada da página de sumário da Segurança. Este é um exemplo para os APs maliciosos.

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

Monitor Reports Configure Location Administration Tools Help

Quick Search: [IP, Name, SSID] Go

Search Alarms: [New Search...] Saved Searches: [--Select Search--]

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	00:14:1b:b6:23:61	Cisco	Malicious	b, g	-61	0		4/21/09 2:48:01 PM	Alert	selwan	No	
<input type="checkbox"/>	Minor	00:12:01:a1:f5:10	Cisco	Malicious	b, g	-59	0		4/21/09 2:48:01 PM	Alert	testsel	No	
<input type="checkbox"/>	Minor	00:19:a9:e1:33:f0	Cisco	Malicious	b, g	-60	0		4/21/09 2:48:01 PM	Alert	ssidas	No	
<input type="checkbox"/>	Minor	00:16:e7:db:67:d0	Cisco	Malicious	b, g	-54	0		4/21/09 2:48:01 PM	Alert	auto	No	
<input type="checkbox"/>	Minor	00:0f:f0:58:a0:5c	Cisco	Malicious	b	-62	0		4/21/09 2:48:01 PM	Alert	test	No	
<input type="checkbox"/>	Minor	00:14:1b:b6:23:6a	Cisco	Malicious	a	-72	0		4/21/09 2:48:01 PM	Alert	selwan	No	
<input type="checkbox"/>	Minor	00:15:67:d0:0f:20	Cisco	Malicious	a	-75	0		4/21/09 2:48:01 PM	Alert	Kil	No	
<input type="checkbox"/>	Minor	00:11:20:80:26:b1	Cisco	Malicious	a	-91	0		4/21/09 2:48:01 PM	Alert	Mobile-NMS	No	
<input type="checkbox"/>	Minor	00:11:20:c2:68:80	Cisco	Malicious	g	-78	0		4/21/09 2:48:01 PM	Alert	Mobile-NMS	No	
<input type="checkbox"/>	Minor	00:19:a9:e5:33:d0	Cisco	Malicious	a	-72	0		4/21/09 2:48:01 PM	Alert	ssidas	No	

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

Informações Relacionadas

- [Detecção desonesto sob redes Wireless unificadas](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)