

# Управляйте базирующейся посторонней классификацией в контроллерах беспроводной локальной сети (WLC) и Wireless Control System (WCS)

## Содержание

[Введение](#)

[Предварительные условия](#)

[Требования](#)

[Используемые компоненты](#)

[Условные обозначения](#)

[Управляйте базирующейся посторонней классификацией](#)

[Управляйте базирующейся посторонней терминологией классификации](#)

[Посторонние правила классификации](#)

[Посторонняя классификация и страны-изгои](#)

[Объясненные страны-изгои](#)

[Как настроить посторонние правила в WLC](#)

[Как настроить посторонние правила в WCS](#)

[Дополнительные сведения](#)

## **Введение**

В Wireless Control System (WCS) 5.0 выпусков WCS улучшил Посторонние Функциональные возможности управления для других посторонних типов AP и предоставил определяемые пользователем правила автоматически классифицировать посторонние AP. WCS применил посторонние правила классификации AP к контроллерам. Этот документ объясняет расширенные Посторонние Функциональные возможности управления и шаги, необходимые для настройки этой функциональности на Контроллере беспроводной локальной сети (WLC) и WCS.

## **Предварительные условия**

### **Требования**

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Знание протокола LWAPP
- Знание решений по обеспечению безопасности контроллера беспроводной локальной сети

## Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Cisco WLC серии 4400, который выполняет микропрограммное обеспечение 5.2
- Облегченные точки доступа Cisco Aironet серии 1130 AG (LAP)
- Версия 5.2 Cisco Wireless Control System

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

## Условные обозначения

[Дополнительные сведения об условных обозначениях см. в документе Условные обозначения технических терминов Cisco.](#)

## Управляйте базирующейся посторонней классификацией

В версиях WCS до выпуска 5.0 WCS отобразил слишком много неавторизованных точек доступа (AP) в **Сводной странице Безопасности**. Даже при том, что страны-изгои отличаются, они все появляются на одной странице, сортированной адресом BSSID/MAC жулика.

В выпуске WCS 5.0 WCS улучшил Посторонние Функциональные возможности управления и представил новую терминологию (Несекретный, Злонамеренный, и Дружественный) для других посторонних типов AP и предоставил определяемые пользователем правила автоматически классифицировать посторонние AP. WCS применил посторонние правила классификации AP к контроллерам.

WCS улучшил функцию управления страны-изгоя для хранения страны-изгоя как *Внешней*, как только состояние жулика было вручную изменено на *Внешний*. Когда получения по запросу WCS или обрабатывают сообщение прерывания от других контроллеров, WCS также обновляет *Внешнее* состояние для других контроллеров.

Чтобы поддерживать эту функцию, и WLC и WCS должны выполнять 5.0 выпусков.

## Управляйте базирующейся посторонней терминологией классификации

С этой новой функциональностью представлены эти новые посторонние типы AP:

- **Злонамеренный AP:** обнаруженный AP, который совпадает с определяемыми пользователем Злонамеренными правилами или был вручную перемещен от Дружественных AP.
- **Дружественный AP:** Существующий известный, Подтвердите, и Трастовые Недостающие страны-изгои классифицированы как Дружественные. Кроме того,

обнаруженные AP, которые совпадают с определяемыми пользователем Дружественными правилами, классифицированы как Дружественные. Дружественные AP не могут содержаться.

- **Несекретный AP:** обнаруженный AP, который не совпадал со Злонамеренными или Дружественными правилами. Может содержаться Несекретный AP. Несекретный AP может быть вручную перемещен в Дружественный пользователем. Определяемые пользователем правила автоматически переместить Несекретный AP в Дружественный или Злонамеренное, например, на обнаружении, SSID пуст. На следующем постороннем отчете найден SSID, и это, оказывается, настраиваемый SSID.

## Посторонние правила классификации

Это правила классификации, применимые к каждому из посторонних типов AP:

- Злонамеренные правила Соответствия управляли SSID Совпадает с SSID настройки пользователя Никакое шифрование на SSID Минимальный RSSI Продолжительность времени Количество клиентов связалось
- Дружественные правила Управляемый SSID Настраиваемый SSID
- Несекретные правила Не совпадает со Злонамеренными или Дружественными правилами

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.

Пользователь может принять решение совпасть со всеми, любым или некоторыми условиями правила по каждому правилу:

- **Все** средства совпадают со всеми настроенными условиями для правила.

- **Любые** средства совпадают с любым из настроенных условий для правила.

- **Некоторые** средства совпадают с немногими настроенными условиями для правила

Например, по *Злонамеренным Правилам*, пользователь настраивает *Управляемый SSID* и *Минимальный RSSI*. Затем у пользователя есть выбор, чтобы совпасть **со всеми** или **любым** из этих двух условий, или совпасть просто с *Минимальным* условием *RSSI*.

Когда контроллер получает посторонний отчет, он делает это:

- Проверки, если обнаруженный AP находится в настраиваемом списке MAC. Если так, классифицируйте AP как Дружественный тип.
- Если обнаруженный AP не находится в списке, он начинает применять правила.
- Во-первых, это применяет *Злонамеренные Правила*. Если *Злонамеренные Правила* совпадают, это классифицировано как Злонамеренный тип. Если детектор RLDP/rogue решает, что этот жулик находится в сети, он отмечает страну-изгой как **Угрозу**. Пользователь может вручную содержать AP, который изменяет страну-изгой на **Содержавший**. Если AP не находится в сети, он отмечает страну-изгой как **Предупреждение**, и пользователь может содержать его вручную.
- Если *Злонамеренные Правила* не совпадают, применяют *Дружественные Правила*. Если *Дружественные Правила* совпадают, то классифицируют его как Дружественный тип.
- Если *Дружественные Правила* не совпадают, классифицируйте этот AP как Несекретный. Если детектор RLDP/rogue решает, что этот жулик находится в сети, отметьте страну-изгой как **Угрозу** и классифицируйте ее как Злонамеренный тип. Пользователь может вручную содержать AP, который изменяет страну-изгой на **Содержавший**. Если AP не находится в сети, отметьте страну-изгой как **Предупреждение**, и пользователь может содержать его вручную.
- Пользователь может вручную переместить AP в другой тип классификации.

## Посторонняя классификация и страны-изгой

Эта таблица показывает другие классификации жуликов и стран-изгоев для каждой классификации.

Основанный на правилах тип классификации	Страны-изгой
Злонамеренный AP	Аварийная угроза содержащее удаленное ожидание
Несекретный AP	Аварийное содержащее удаленное ожидание
Дружественный AP	Внутренний (Известный в настоящее время) Внешний (В настоящее время подтверждают), Внутренние Пропавшие без вести (Пропавшие без вести Доверия) Предупреждение

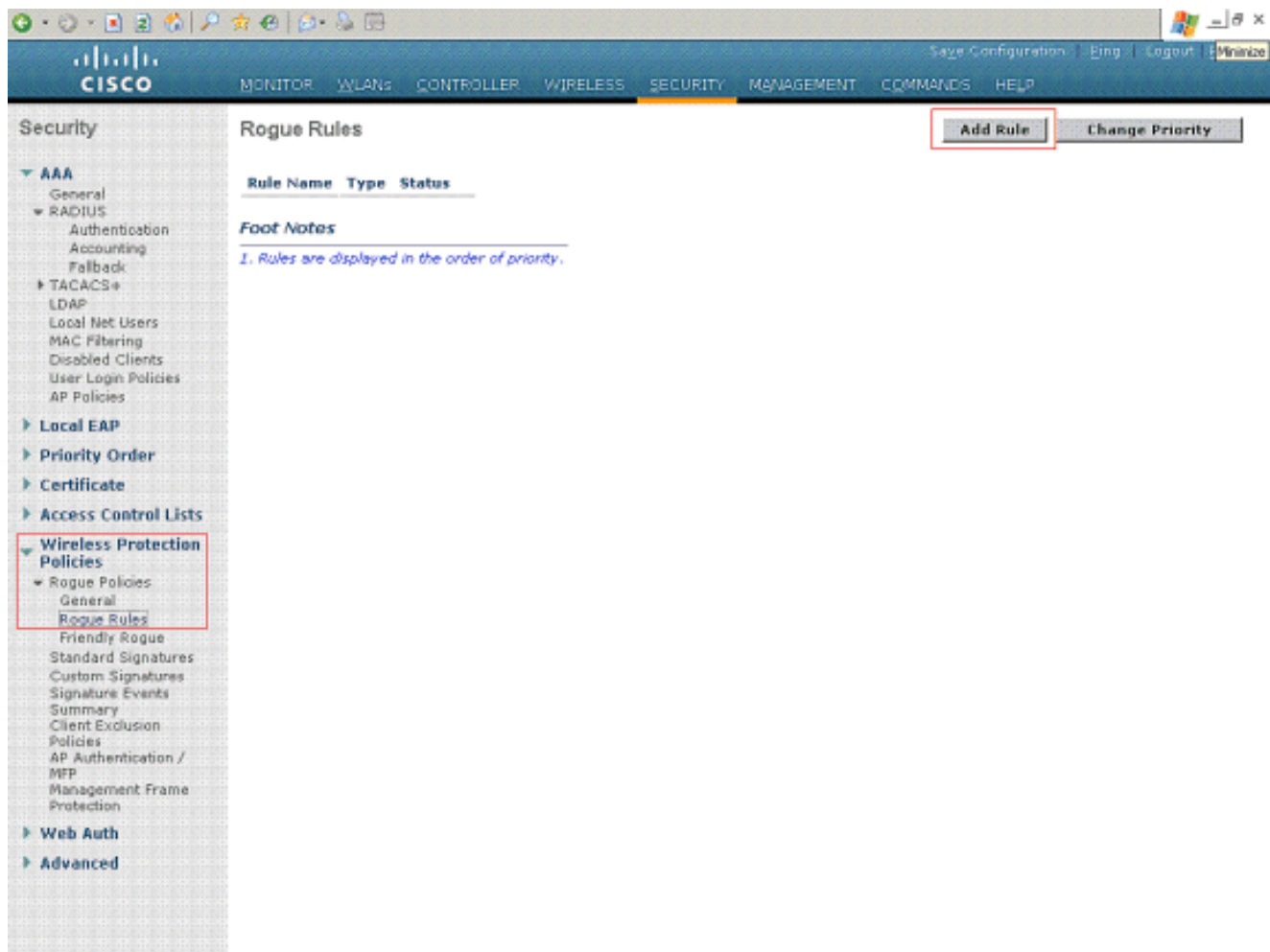
## Объясненные страны-изгой

- **Ожидая** — На первом обнаружении, обнаруженный AP помещен в состояние в состоянии ожидания в течение 3 минут. На этот раз достаточно для управляемых AP, чтобы определить, является ли обнаруженный AP соседним AP.
- **Предупреждение** — После 3-минутного таймаута, обнаруженный AP перемещен в **Предупреждение**, если это не находится в соседнем списке или настраиваемом Дружественном списке MAC.
- **Угроза** — обнаруженный AP найден в сети.
- **Содержавший** — обнаруженный AP содержится.
- **Содержавшее Ожидание** — обнаруженный AP отмечен содержащий, но действие включения задержано из-за ней имеющихся в наличии ресурс.
- **Внутренний** — обнаруженный AP в сети, и пользователь вручную настраивает его как **Дружественный, Внутренний**, например, AP в лабораторной сети.
- **Внешний** — обнаруженный AP вне сети, и пользователь вручную настраивает его как **Дружественный, Внешний**, например, AP, которые принадлежат соседней сети.
- **Доверяемое Отсутствие** — Если настраиваемый Дружественный MAC обнаружили и не слышат на время трастового таймаута, страну-изгой Дружественного AP, отмечено как Доверяемые Пропавшие без вести.
- **Удаленный** — Если Злонамеренный или Несекретный AP не слышат от всех контроллеров на время постороннего таймаута, страна-изгой AP отмечена как **Удаленная**.

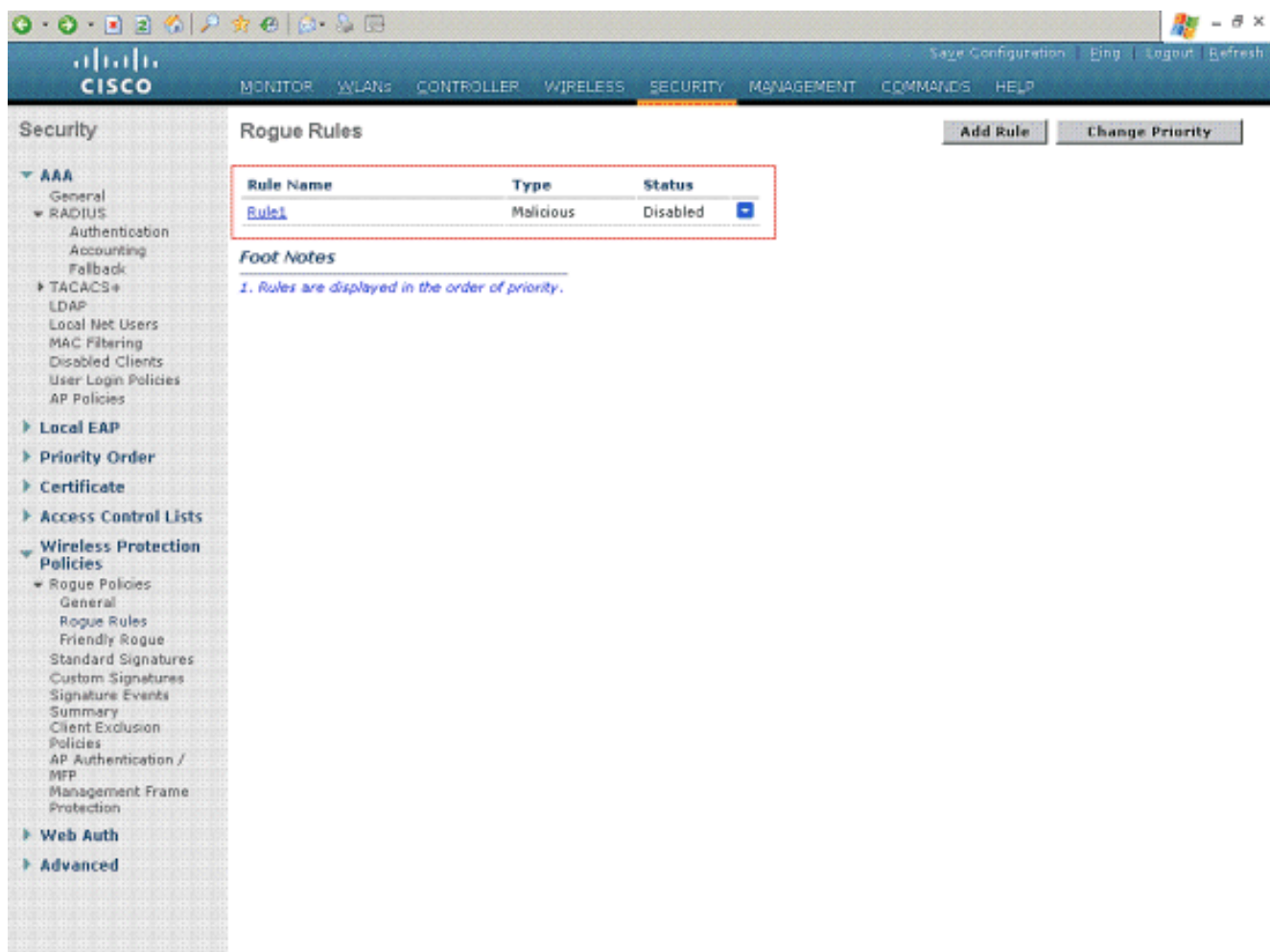
## Как настроить посторонние правила в WLC

Для настройки посторонних правил о Контроллере беспроводной локальной сети выполните эти шаги.

1. Посторонние правила могут быть созданы от WLC от страницы **Security> Wireless Protection Policies> Rogue Policies> Rogue Rules**.



2. Для создания новой посторонней политики нажмите кнопку **Add Rule**. Окно **Rogue Rules** появляется. Введите имя для правила. Данный пример использует Rule1. Выберите тип правила. Это - пример Злонамеренного правила. **Нажмите Add**. Rule1 создан.



Security

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP

Save Configuration | Ping | Logout | Refresh

**Rogue Rules** Add Rule Change Priority

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

**Foot Notes**

1. Rules are displayed in the order of priority.

- AAA
  - General
  - RADIUS
    - Authentication
    - Accounting
    - Fallback
  - TACACS+
  - LDAP
  - Local Net Users
  - MAC Filtering
  - Disabled Clients
  - User Login Policies
  - AP Policies
- Local EAP
- Priority Order
- Certificate
- Access Control Lists
- Wireless Protection Policies
  - Rogue Policies
    - General
    - Rogue Rules
    - Friendly Rogue
    - Standard Signatures
    - Custom Signatures
    - Signature Events
    - Summary
    - Client Exclusion
    - Policies
    - AP Authentication / MFP
    - Management Frame Protection
- Web Auth
- Advanced

3. Для редактирования этого правила нажмите правило, которое было создано. **Постороннее Правило** > страница **Edit** появляется. На этой странице проверьте флажок **Enable Rule** для активации правила. Выберите Match Operation type и другие условия на основе требования как в данном примере.

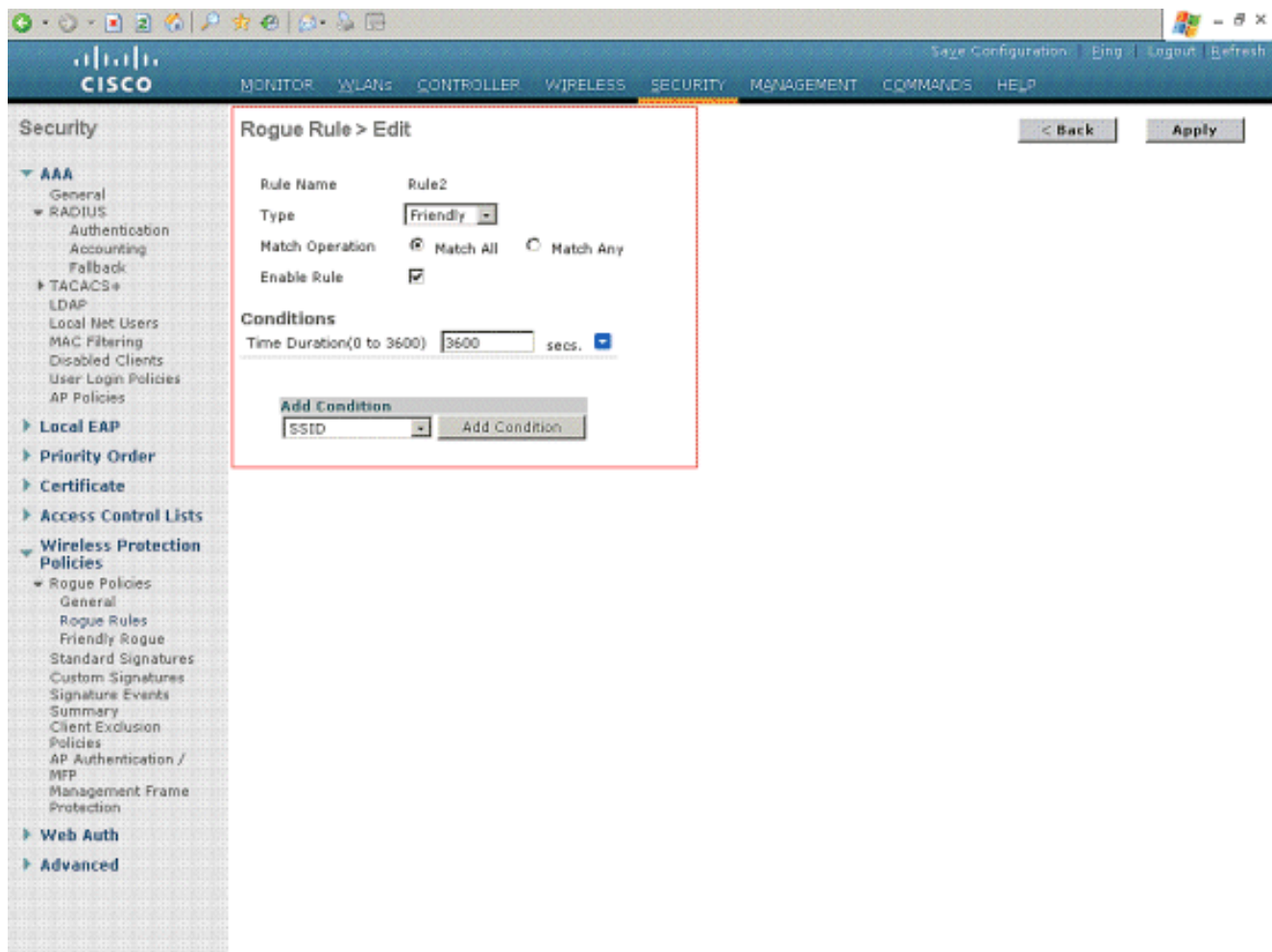
The screenshot displays the Cisco Security configuration page for a Rogue Rule. The interface includes a top navigation bar with tabs for MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, COMMANDS, and HELP. The left sidebar shows a tree view under Security, with 'Wireless Protection Policies' expanded to 'Rogue Policies' and 'Rogue Rules' selected. 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. Это - пример Дружественной посторонней политики правила.





5. Выходные данные посторонних правил могут быть замечены в **Мониторе > Жулики > Злонамеренный AP**.

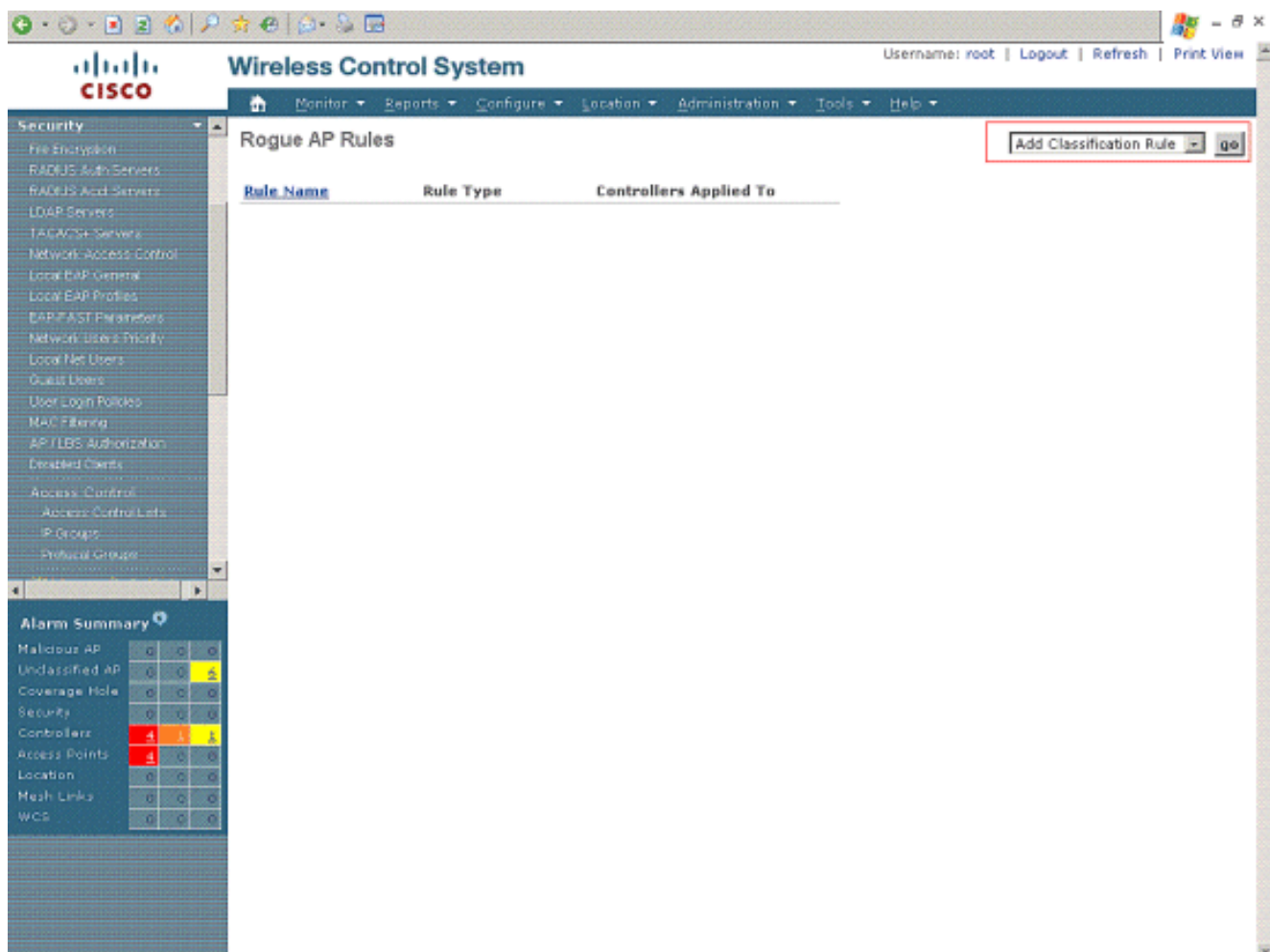
MAC Address	SSID	# Detecting Radios	Number of Clients	Status
<a href="#">00:0f:f8:58:a8:5c</a>	test	1	0	Alert
<a href="#">00:11:20:80:26:b1</a>	Mobile-NMS	1	0	Alert
<a href="#">00:11:20:c2:68:80</a>	Mobile-NMS	1	0	Alert
<a href="#">00:12:01:a1:f5:10</a>	testsel	1	0	Alert
<a href="#">00:14:1b:b6:23:61</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:c7: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. Точно так же выходные данные *Дружественных Правил* и *Несекретных Правил* могут быть просмотрены в страницах **Monitor> Rogues> Unclassified AP** и **Monitor> Rogues> Friendly AP**, соответственно.

## Как настроить посторонние правила в WCS

**Постороннее Правило List:WCS** предоставляет значение правила жулика уровня системы. Для настройки посторонних правил о WCS выполните эти шаги.

1. Выберите **Configure> Controller Template**, и затем нажмите **Security> Rogue AP Rules** для доступа к Посторонней странице списка Правил AP.
2. Нажмите **Add Правило Классификации** о правильном главном раскрывающемся меню для добавления нового правила классификации.



3. Нажмите имя шаблона для редактирования постороннего правила. Эта подробная страница правила позволяет вам отредактировать, обновить постороннее правило AP или удалить правило. **Посторонний AP Управляет Устанавливающим Parameters: On** эта страница, пользователи могут включить любое условие, когда они проверяют флажок для конкатенации любых из этих условий: Никакое шифрование Совпадают с управляемым AP Совпадают с SSID настройки пользователя Минимальный RSSI Продолжительность Клиент жулика минимального количества Это - пример Злонамеренного правила:

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

Это - пример Дружественного правила:

**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. Страница Rogue AP Rules перечисляет все созданные правила.

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 is visible at the bottom left, showing various alarm counts and status indicators.

5. Следующий шаг должен настроить группу правила и применить эти правила к контроллерам. Чтобы к этому, используйте значение **Rogue AP Rule Groups** на WCS.
6. Для создания новой группы правила выберите **Configure> Controller Template**, и затем нажмите **Security> Rogue AP Rule Groups** от GUI WCS.

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

Below the table, there is an "Add Rogue Rule Group" button 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" section with a table showing various alarm types and their counts.

Alarm Type	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. Страница Rogue AP Rule Groups> New Template позволяет вам добавить, обновить постороннюю группу правила AP, удалить правило и применить группу правила к контроллеру. Используйте кнопки Add/Remove для выбора посторонних правил AP для этой группы правила. Используйте кнопки Up/Down для определения заказа, в котором применены правила. Ниже представлен пример. Как только группа правил настроена, нажмите **Save**.

The screenshot shows the Cisco Wireless Control System (WCS) interface. The main title is "Wireless Control System" with the Cisco logo. The user is logged in as "root". The navigation menu includes: Monitor, Reports, Configure, Location, Administration, Tools, and Help. The current page is "Rogue AP Rule Groups > New Template".

**General**

Rule Group Name:

**Edit View**

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.

Left List (Empty):

Right List (Contains):

- Rule1
- Rule2

Buttons: Add >, < Remove, Move Up, Move Down

Buttons: Save, Cancel

Note: Rogue AP Rule(s) can be added from "Rogue AP Rules" section.

**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

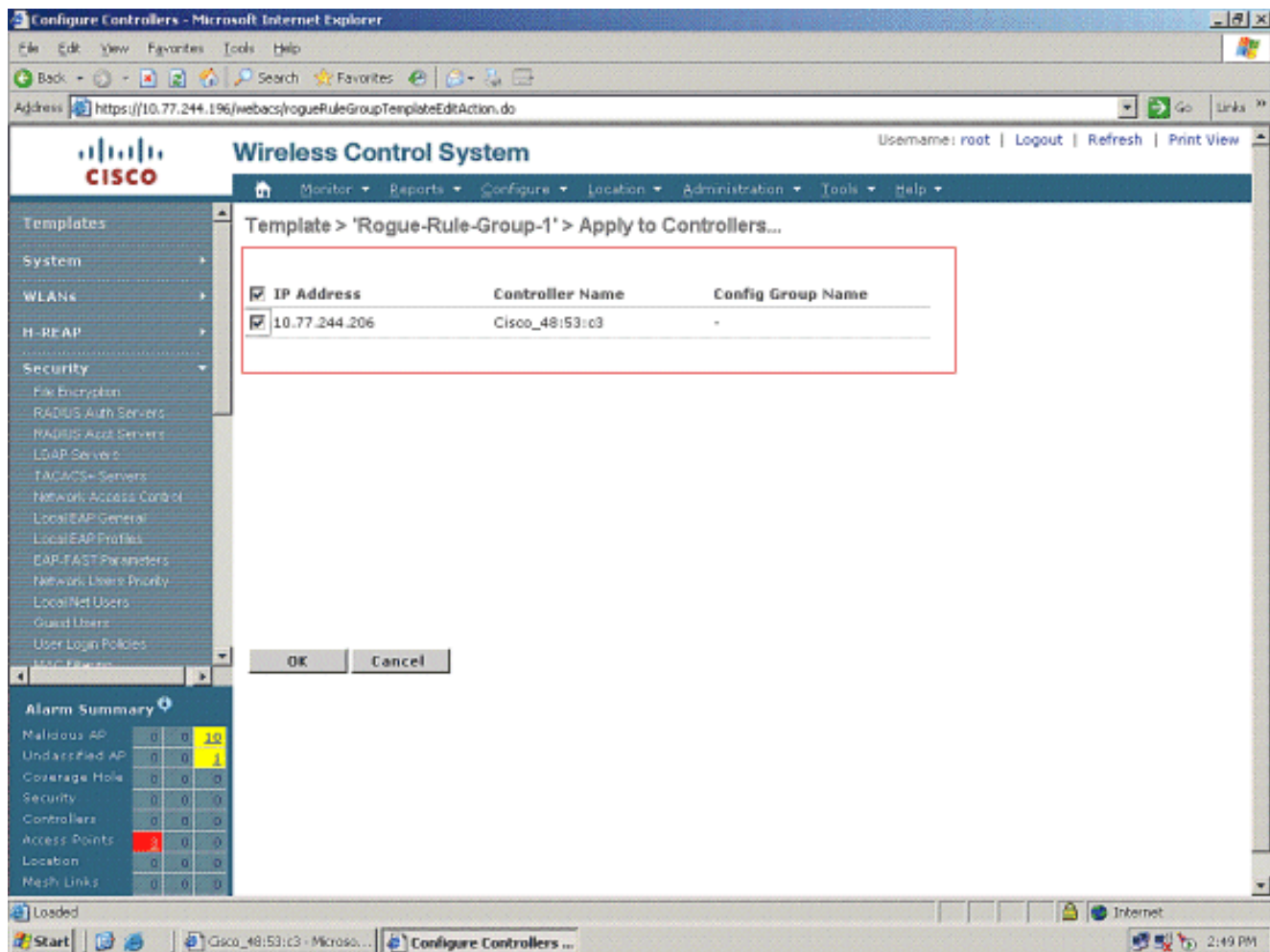
8. Как только вы сохраняете группу правила, она может быть применена к контроллерам. Для применения группы правила к контроллеру отредактируйте группу правила. Нажмите имя группы правила.



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, the "Apply to Controllers ..." button is highlighted with a red box. Below the buttons, a note 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

Нажмите **Apply to Controllers**. На следующей странице выберите контроллеры, к которым применено это правило. Ниже представлен пример.



9. Как только правила применены к контроллерам, вы видите **Сообщение об успешном завершении** на WCS.

The screenshot shows the Cisco Wireless Control System (WCS) interface in a Microsoft Internet Explorer browser. The browser address bar shows the URL: `https://10.77.244.196/webacs/rogueRuleGroupTemplateGeneralAction.do`. The page title is "Wireless Control System" and the user is logged in as "root".

The main content area displays "Template Results > 'Rogue-Rule-Group-1' > Apply to Controllers...". A table with a red border shows the results:

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

On the left side, there is a navigation menu with categories like System, WLANs, H-REAP, Security, and Alarm Summary. The Alarm Summary section shows a table of counts for various security events:

Alarm Category	Count 1	Count 2	Count 3
Malicious AP	0	0	10
Undescribed AP	0	0	1
Coverage Hole	0	0	0
Security	0	0	0
Controllers	0	0	0
Access Points	3	0	0
Location	0	0	0
Mesh Links	0	0	0

The Windows taskbar at the bottom shows the Start button, several open applications including "Cisco\_48:53:c3 - Microso...", and the system clock showing 2:49 PM.

10. Детали о классифицированных AP могут посмотреть на **Сводной странице Безопасности**. Ниже представлен пример.

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 3.2.0	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. Детали о классифицированных AP, в частности Злонамеренных, Дружественных, и Несекретных AP, могут посмотреться при нажатии соответствующей классификации от Сводной страницы Безопасности. Это - пример для Злонамеренных AP.

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	Kill		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

## Дополнительные сведения

- [Обнаружение несанкционированных точек доступа в Unified Wireless Networks](#)
- [Cisco Systems – техническая поддержка и документация](#)