

ワイヤレス LAN コントローラ (WLC) および Wireless Control System (WCS) でのルールベ ースの不正分類 (英語)

目次

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[ルールベースの不正分類](#)

[ルールベースの不正分類の用語](#)

[不正分類ルール](#)

[不正分類と不正の状態](#)

[不正の状態の説明](#)

[WLC で不正ルールを設定する方法](#)

[WCS で不正ルールを設定する方法](#)

[関連情報](#)

概要

Wireless Control System (WCS) 5.0 リリースで、WCS はさまざまな不正 AP タイプの不正管理機能を強化し、不正 AP を自動的に分類するユーザ定義のルールを提供しています。WCS はコントローラに不正 AP の分類ルールを適用します。このドキュメントでは、拡張された不正管理機能、ワイヤレス LAN コントローラ (WLC) および WCS でこの機能を設定する必要な手順について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Lightweight アクセス ポイント プロトコル (LWAPP) に関する知識
- ワイヤレス LAN コントローラのセキュリティ ソリューションについての知識

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- ファームウェア 5.2 が稼働している Cisco 4400 シリーズ WLC
- Cisco Aironet 1130 AG シリーズ Lightweight アクセス ポイント (LAP)
- Cisco Wireless Control System バージョン 5.2

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、クリアな (デフォルト) 設定で作業を開始しています。ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、『[シスコテクニカルティップスの表記法](#)』を参照してください。

ルールベースの不正分類

リリース 5.0 よりも前の WCS バージョンでは、WCS の [Security Summary] ページに多数の不正アクセス ポイント (AP) が表示されてきました。不正の状態が異なっても、これらはすべて不正の BSSID/MAC アドレス順に 1 ページで表示されます。

WCS リリース 5.0 で、WCS は不正管理機能を拡張し、さまざまな不正 AP タイプに向けた新しい用語 (Unclassified、Malicious、および Friendly) を導入し、不正 AP を自動的に分類するユーザ定義のルールを提供しています。WCS はコントローラに不正 AP の分類ルールを適用します。

WCS は不正の状態が手動で *External* に変更されたら、不正の状態を *External* として保持するように不正の状態の管理機能を拡張しました。また、WCS が他のコントローラからのトラップメッセージを取得または処理する場合、WCS は他のコントローラの *External* の状態も更新します。

この機能をサポートするには、WLC と WCS の両方が 5.0 リリースを実行している必要があります。

ルールベースの不正分類の用語

この新機能により、次の新しい不正 AP タイプが導入されました。

- **Malicious AP** : ユーザ定義の悪意のあるルールに一致する検出された AP、または Friendly AP から手動で移動された AP
- **Friendly AP** : 既存の Known、Acknowledge、Trust Missing の不正の状態は、Friendly として分類されます。また、ユーザ定義の Friendly ルールに一致する検出された AP も Friendly として分類されます。Friendly AP は制限できません。
- **Unclassified AP** : Malicious または Friendly ルールに一致しない検出された AP。Unclassified AP は制限できます。Unclassified AP はユーザによって Friendly に手動で移動できます。Unclassified AP を Friendly または Malicious に自動的に移動するユーザ定義のルールは、次のようなものです。たとえば、検出時に SSID は空でした。次の不正レポートで、SSID が見付き、ユーザ設定の SSID であることがわかりました。

不正分類ルール

以下は、それぞれの不正 AP タイプに適用できる分類ルールです。

- Malicious ルール管理対象 SSID と一致ユーザ設定の SSID と一致SSID の暗号化なし最小構成の RSSI期間関連付けられたクライアントの数
- Friendly ルール管理対象 SSIDユーザ設定の SSID
- Unclassified ルールMalicious または Friendly ルールに一致しない

| 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.

ユーザは、ルールごとにルール条件の **all**、**any**、または **some** に一致することを選択できます。

- **All** は、ルールに設定された条件すべてに一致することを意味します。
- **Any** は、ルールに設定された条件のいずれかに一致することを意味します。
- **Some** は、ルールに設定された条件のいくつかに一致することを意味します。

たとえば、*Malicious Rules* でユーザが *Managed SSID* と *Minimum RSSI* を設定したとします。次に、ユーザは 2 つの条件の **all** または **any** に一致させるか、*Minimum RSSI* 条件のみに一致させることを選択できます。

コントローラは不正レポートを受信すると、次を実行します。

- 検出された AP がユーザ設定の MAC リストにあるかどうかをチェックします。リストにある場合は、Friendly タイプとして AP を分類します。
- 検出された AP がリストにない場合は、ルールの適用を開始します。
- まず、*Malicious Rules* を適用します。*Malicious Rules* に一致する場合は、Malicious タイプとして分類されます。RLDP/Rogue Detector によって不正がネットワーク上にあると判断されると、不正の状態は **Threat** としてマークされます。ユーザは AP を手動で制限できます。これにより、不正の状態は **Contained** に変更されます。AP がネットワークにない場合、不正の状態は **Alert** としてマークされ、ユーザは AP を手動で制限できます。

- *Malicious Rules* に一致しない場合は、*Friendly Rules* を適用します。*Friendly Rules* に一致する場合は、Friendly タイプとして分類されます。
- *Friendly Rules* に一致しない場合は、この AP Unclassified として分類されます。
RLDP/Rogue Detector によって不正がネットワーク上にあると判断されると、不正の状態は **Threat** としてマークされ、Malicious タイプとして分類されます。ユーザは AP を手動で制限できます。これにより、不正の状態は **Contained** に変更されます。AP がネットワークにない場合、不正の状態は **Alert** としてマークされ、ユーザは AP を手動で制限できます。
- ユーザは AP を別の分類タイプに手動で移動できます。

不正分類と不正の状態

この表に、さまざまな不正の分類と、それぞれの分類の不正の状態を示します。

| ルールベースの分類タイプ | 不正の状態 |
|-----------------|--|
| Malicious AP | Alert Threat Contained Contained Pending Removed |
| Unclassified AP | Alert Contained Contained Pending Removed |
| Friendly AP | Internal (Known currently) External (Acknowledge currently) Internal Missing (Trust Missing) Alert |

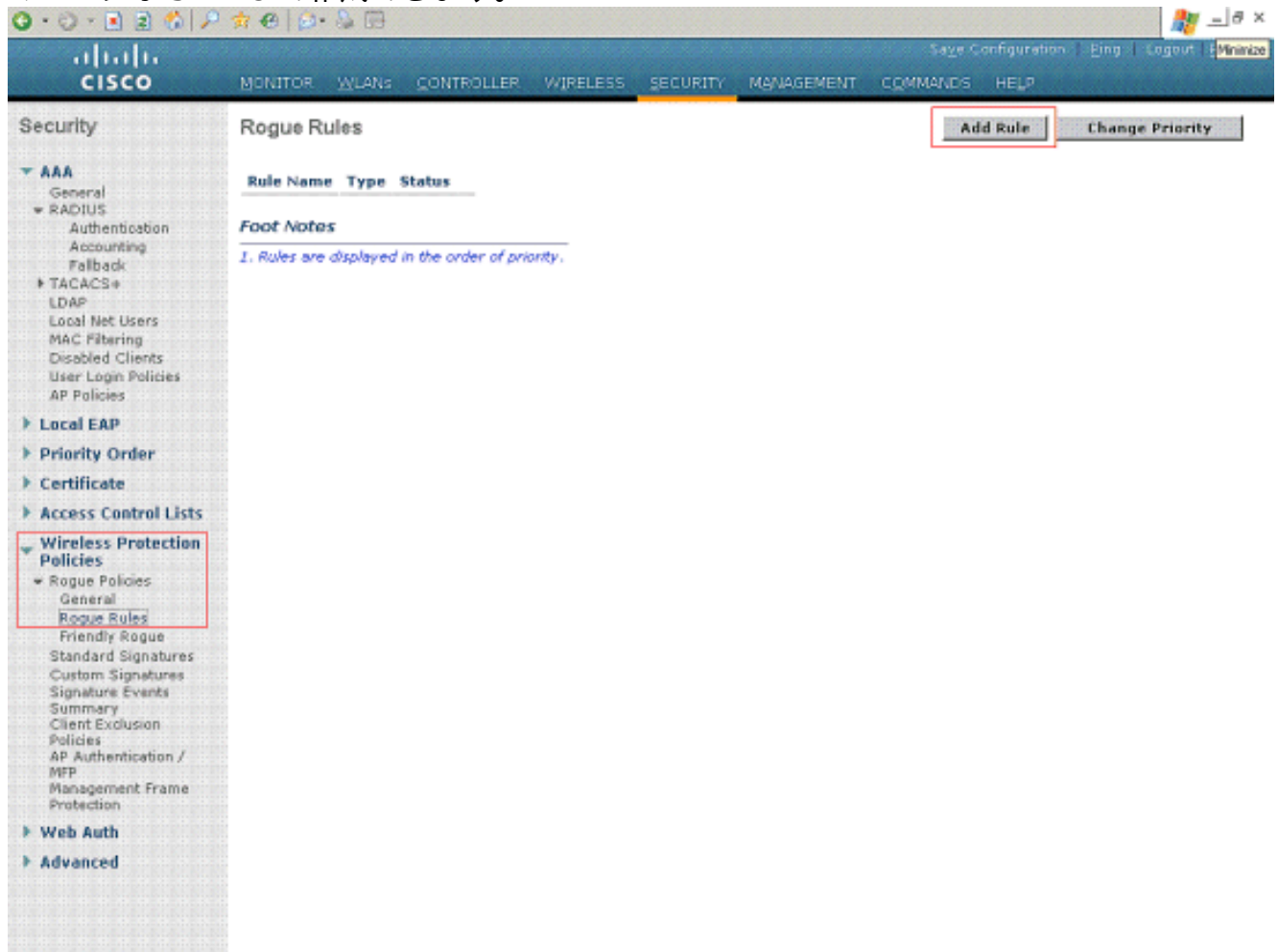
不正の状態の説明

- **Pending** : 最初の検出で、検出された AP は 3 分間 Pending 状態に置かれます。この時間は、検出された AP がネイバー AP かどうかを管理対象 AP が判断するのに十分です。
- **Alert** : 3 分のタイムアウト後に、ネイバー リストまたはユーザ設定の Friendly MAC リストに含まれない場合は検出された AP は **Alert** に移動されます。
- **Threat** : 検出された AP はネットワーク上にあります。
- **Contained** : 検出された AP は抑止されています。
- **Contained Pending** : 検出された AP は Contained としてマークされていますが、リソースが使用できないため抑止のアクションが遅延されています。
- **Internal** : たとえばラボ ネットワーク内の AP など、検出された AP はネットワークの内部にあります。この AP をユーザは手動で **Friendly, Internal** として設定します。
- **External** : たとえばネイバー ネットワークに属している AP など、検出された AP はネットワークの外部にあります。この AP をユーザは手動で **Friendly, External** として設定します。
- **Trusted Missing** : ユーザ設定の Friendly MAC が検出されたが、信頼タイムアウトの期間中に受信がなかった場合は、Friendly AP の不正の状態は Trusted Missing としてマークされます。
- **Removed** : Malicious AP または Unclassified AP が不正タイムアウト期間中にすべてのコントローラから受信がなかった場合は、AP の不正の状態は **Removed** としてマークされます。

WLC で不正ルールを設定する方法

ワイヤレス LAN コントローラの不正ルールを設定するには、次の手順を実行します。

1. 不正ルールは、[Security] > [Wireless Protection Policies] > [Rogue Policies] > [Rogue Rules] のページから WLC で作成できます。



2. 新しい不正ポリシーを作成するには、[Add Rule] ボタンをクリックします。[Rogue Rules] ウィンドウが表示されます。ルールの名前を入力します。この例では Rule1 を使用しています。ルールのタイプを選択します。これは、Malicious ルールの例です。[Add] をクリックします。Rule1 が作成されます。

The screenshot shows the Cisco Security configuration page for Rogue Rules. The interface includes a top navigation bar with tabs for MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY (selected), MANAGEMENT, COMMANDS, and HELP. A left sidebar lists various security categories like AAA, RADIUS, TACACS+, Local EAP, Priority Order, Certificate, Access Control Lists, Wireless Protection Policies, Web Auth, and Advanced. 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 text: '1. Rules are displayed in the order of priority.' Buttons for 'Add Rule' and 'Change Priority' are located at the top right of the table area.

3. このルールを編集するには、作成されたルールをクリックします。[Rogue Rule > Edit] ページが表示されます。このページで、ルールをアクティブにするには、[Enable Rule] チェックボックスをオンにします。次の例のように、要件に基づいて [Match Operation] のタイプやその他の条件を選択します。

The screenshot shows the Cisco Wireless LAN Controller configuration interface. The left sidebar is expanded to 'Wireless Protection Policies' > 'Rogue Policies' > 'Rogue Rules'. The main content area is titled 'Rogue Rule > Edit' and contains the following configuration:

- 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 visible in the top right corner.

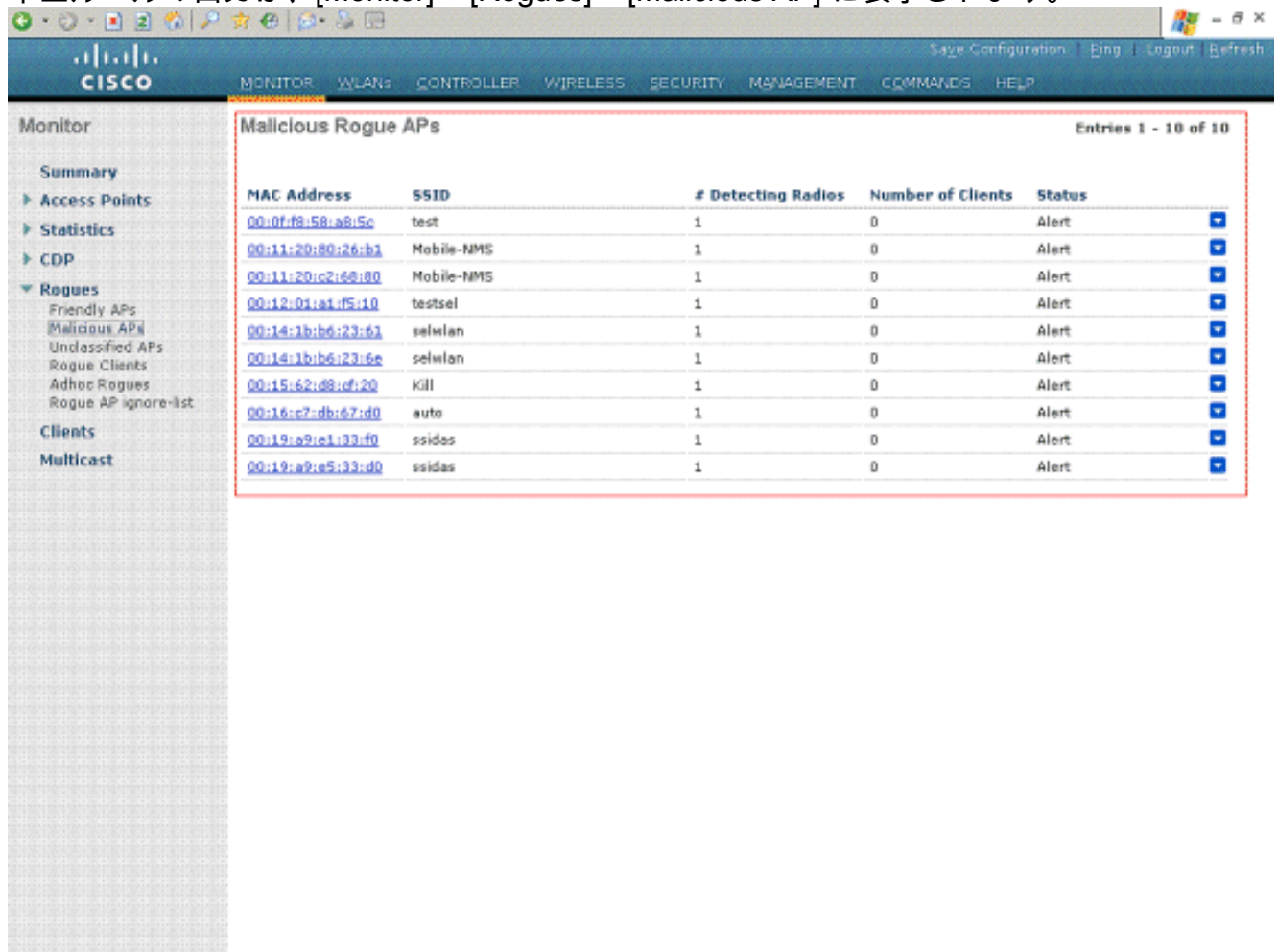
4. これは Friendly 不正ルール ポリシーの例です。

The screenshot shows the Cisco Wireless LAN Controller configuration interface. The left sidebar is expanded to 'Wireless Protection Policies' > 'Rogue Policies' > 'Rogue Rules'. The main content area is titled 'Rogue Rule > Edit' and contains the following configuration:

- Rule Name:** Rule2
- Type:** Friendly
- Match Operation:** Match All (selected)
- Enable Rule:**
- Conditions:**
 - Time Duration(0 to 3600): 3600 secs.
- Add Condition:** SSID

Buttons for '< Back' and 'Apply' are visible in the top right corner.

5. 不正ルールの出力は、[Monitor] > [Rogues] > [Malicious AP] に表示されます。



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

| MAC Address | SSID | # Detecting Radios | Number of Clients | Status |
|-----------------------------------|------------|--------------------|-------------------|--------|
| 00:0f:f9:58: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:af:f5:d0 | 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:67:d0 | auto | 1 | 0 | Alert |
| 00:19:a9:e1:33:d0 | ssidas | 1 | 0 | Alert |
| 00:19:a9:e5:33:d0 | ssidas | 1 | 0 | Alert |

6. 同様に、*Friendly Rules* と *Unclassified Rules* の出力は、それぞれ [Monitor] > [Rogues] > [Unclassified AP] および [Monitor] > [Rogues] > [Friendly AP] のページで確認できます。

WCS で不正ルールを設定する方法

不正ルールのリスト：WCS では、システム レベルでの不正ルールの設定が提供されています。WCS で不正ルールを設定するには、次の手順を実行します。

1. [Configure] > [Controller Template] を選択し、[Security] > [Rogue AP Rules] をクリックし、[Rogue AP Rules] のリストのページにアクセスします。
2. 新しい分類ルールを追加するには、右上のドロップダウン メニューから [Add Classification Rule] をクリックします。

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 'Security' menu and an 'Alarm Summary' section with a table of alarm counts.

| Rule Name | Rule Type | Controllers Applied To |
|-----------|-----------|------------------------|
| | | |

| Alarm Type | Count | Severity | Actions |
|-----------------|-------|----------|---------|
| Malicious AP | 0 | 0 | 0 |
| Unclassified AP | 0 | 0 | 0 |
| Coverage Hole | 0 | 0 | 0 |
| Security | 0 | 0 | 0 |
| Controllers | 4 | 1 | 0 |
| Access Points | 4 | 0 | 0 |
| Location | 0 | 0 | 0 |
| Mesh Links | 0 | 0 | 0 |
| WCS | 0 | 0 | 0 |

- 不正ルールを編集するためにテンプレート名をクリックします。このルールの詳細ページでは、不正 AP ルールの編集やアップデート、または削除を行えます。不正 AP ルールの設定パラメータ：このページでは、ユーザは次の条件のいずれか、またはすべてを連結するためにチェックボックスをチェックすることによって条件をイネーブルにできます。暗号化なし管理対象 AP と一致ユーザ設定の SSID と一致最小構成の RSSIコール時間最小数の不正クライアントこれは、Malicious ルールの例です。

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 | 1 | 0 | 0 |
| Location | 0 | 0 | 0 |
| Mesh Links | 0 | 0 | 0 |

これは、Friendly ルールの例です。

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 | 1 | 0 | 0 |
| Location | 0 | 0 | 0 |
| Mesh Links | 0 | 0 | 0 |

4. [Rogue AP Rules] ページには、作成されたすべてのルールが一覧表示されます。

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 interface also features a navigation menu on the left with categories like Templates, System, WLANs, H-REAP, Security, and Alarm Summary. The Alarm Summary section at the bottom shows various metrics with status indicators.

5. 次の手順では、ルールグループを設定し、これらのルールをコントローラに適用します。これには、WCS の [Rogue AP Rule Groups] 設定を使用します。
6. 新しいルールグループを作成するには、[Configure] > [Controller Template] を選択し、WCS GUI から [Security] > [Rogue AP Rule Groups] をクリックします。

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 metrics with colored indicators.

| Rule Group Name | No of Controllers Applied To |
|-----------------|------------------------------|
| | |

7. [Rogue AP Rule Groups > New Template] ページでは、不正 AP ルール グループの追加とアップデート、ルール削除、コントローラへのルールグループの適用を実行することができます。このルールグループの不正 AP ルールを選択するには、[Add]/[Remove] ボタンを使用します。[Up]/[Down] ボタンをクリックして、ルールが適用される順序を指定します。次に例を示します。ルールグループが設定されたら、[Save] をクリックします。

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" section, 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 for rules, with "Add >" and "< Remove" buttons between them, and "Move Up" and "Move Down" buttons to the right. At the bottom of the main content area, there are "Save" and "Cancel" buttons. A note states: "Note: Rogue AP Rule(s) can be added from 'Rogue AP Rules' section." On the left side, there is a navigation menu with categories like Templates, System, WLANs, H-REAP, Security, and Access Control. At the bottom left, there is an "Alarm Summary" table.

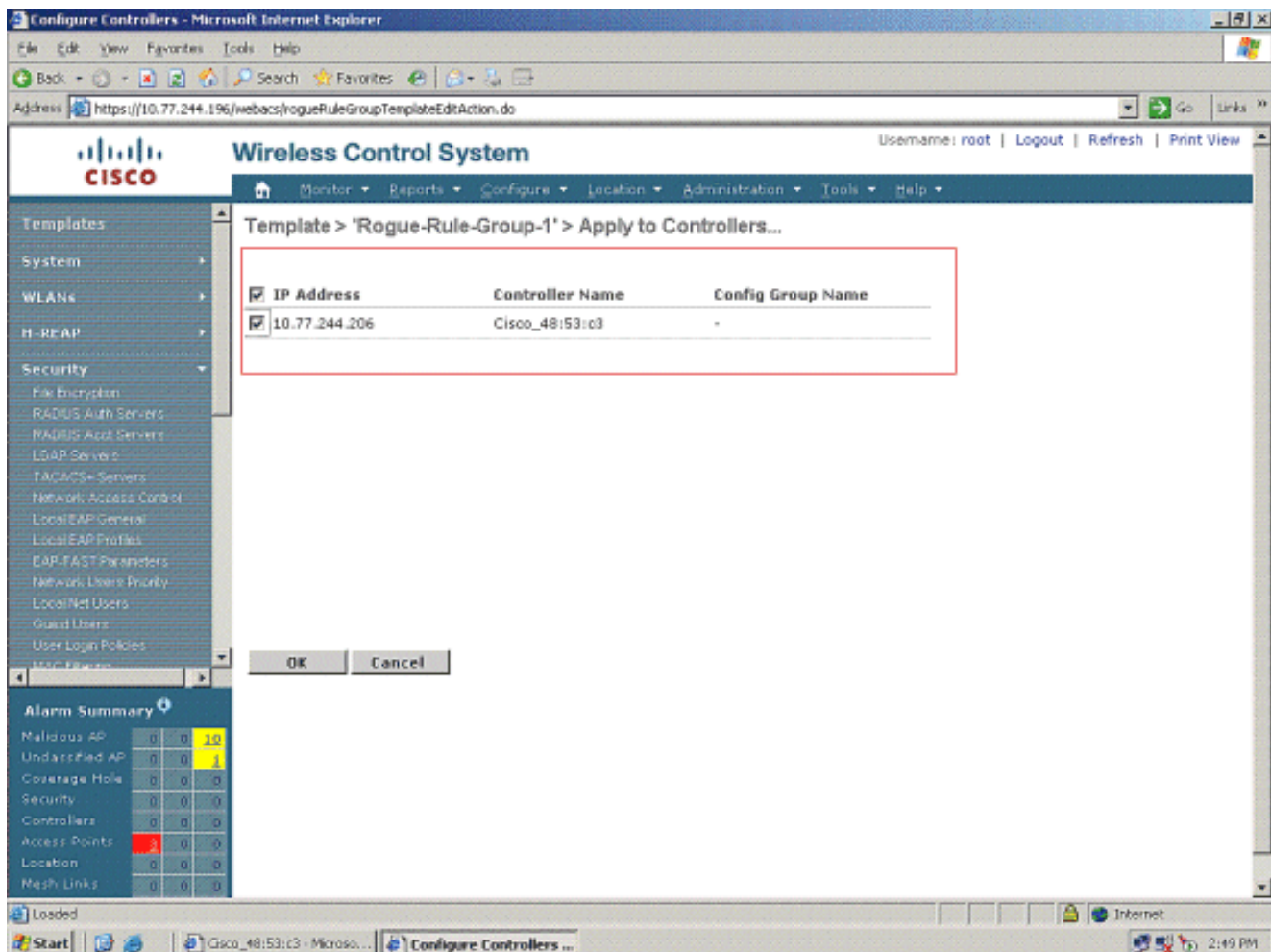
| Alarm Summary | | | |
|-----------------|---|---|---|
| Malicious AP | 0 | 0 | 0 |
| Unclassified AP | 0 | 0 | 0 |
| Coverage Hole | 0 | 0 | 0 |
| Security | 0 | 0 | 0 |
| Controllers | 4 | 1 | 1 |
| Access Points | 1 | 0 | 0 |
| Location | 0 | 0 | 0 |
| Mesh Links | 0 | 0 | 0 |

8. ルールグループを保存したら、これをコントローラに適用できます。コントローラにルールグループを適用するには、ルールグループを編集します。ルールグループ名をクリックします。

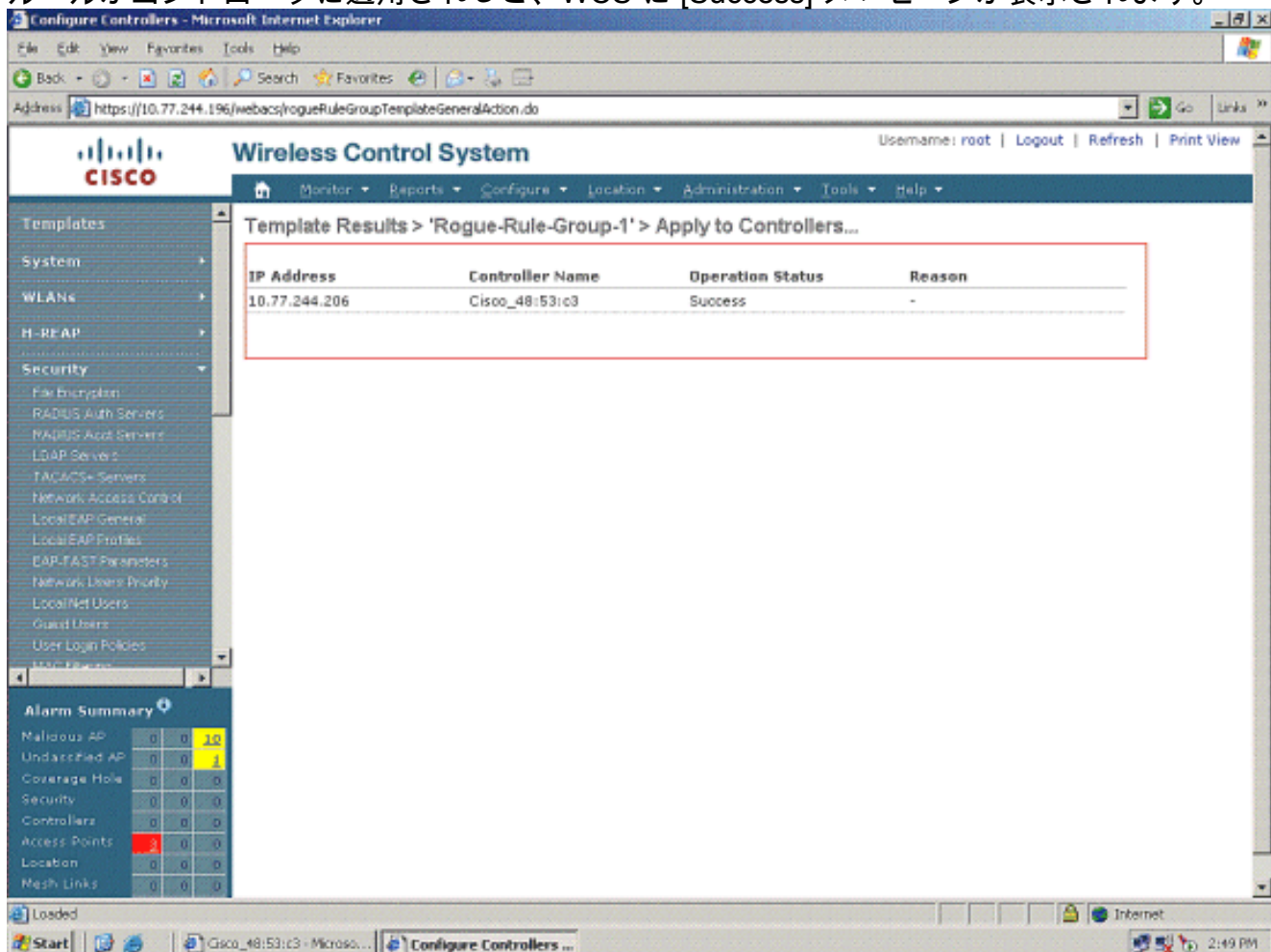
The screenshot shows the Cisco Wireless Control System (WCS) interface. The breadcrumb trail is "Rogue AP Rule Groups > Rogue-Rule-Group-1". The "General" section shows the "Rule Group Name" as "Rogue-Rule-Group-1". The "Edit View" section contains two boxes: an empty one on the left and one on the right containing "Rule1" and "Rule2". Between the boxes are "Add >" and "< Remove" buttons. To the right of the second box are "Move Up" and "Move Down" buttons. At the bottom of the edit view are "Save", "Apply to Controllers ...", "Delete", and "Cancel" buttons. 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." In the bottom left corner, 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 | 1 | 0 | 0 |
| Location | 0 | 0 | 0 |
| Mesh Links | 0 | 0 | 0 |

[Apply to Controllers] をクリックします。次のページで、このルールを適用するコントローラを選択します。次に例を示します。



9. ルールがコントローラに適用されると、WCSに [Success] メッセージが表示されます。



10. 分類された AP についての詳細は、[Security Summary] ページで確認できます。次に例を示します。

The screenshot displays the Cisco Wireless Control System interface. The left sidebar shows the 'Security' menu with 'Summary' selected. The main content area is titled 'Security Summary' and contains several tables:

- Malicious Rogue APs:**

| | Last Hour | 24 Hours | Total Active |
|-------------------|-----------|----------|--------------|
| Alert | 10 | 10 | 10 |
| Contained | 0 | 0 | 0 |
| Threat | 0 | 0 | 0 |
| Contained Pending | 0 | 0 | 0 |
| 802.11a/n5.0 | 4 | 4 | 4 |
| 802.11b/g/n2.4 | 6 | 6 | 6 |
| On Network | 0 | 0 | 0 |
| Off Network | 10 | 10 | 10 |
- Friendly Rogue APs:**

| | Last Hour | 24 Hours | Total Active |
|----------------|-----------|----------|--------------|
| Alert | 0 | 0 | 0 |
| Internal | 0 | 0 | 0 |
| External | 0 | 0 | 0 |
| 802.11a/n5.0 | 0 | 0 | 0 |
| 802.11b/g/n2.4 | 0 | 0 | 0 |
- Unclassified Rogue APs:**

| | Last Hour | 24 Hours | Total Active |
|-------------------|-----------|----------|--------------|
| Alert | 0 | 0 | 1 |
| Contained | 0 | 0 | 0 |
| Contained Pending | 0 | 0 | 0 |
| 802.11a/n5.0 | 0 | 0 | 0 |
| 802.11b/g/n2.4 | 0 | 0 | 1 |
- Signature Attacks:**

| | Last Hour | 24 Hours | Total Active |
|----------------------|-----------|----------|--------------|
| Custom | 0 | 0 | 0 |
| NULL probe resp 1 | 0 | 0 | 0 |
| Broadcast Probe floo | 0 | 0 | 0 |
| EAPOL flood | 0 | 0 | 0 |
| Reserved mgmt F | 0 | 0 | 0 |
| Boast deauth | 0 | 0 | 0 |
| Reassoc flood | 0 | 0 | 0 |
| Disassoc flood | 0 | 0 | 0 |
| Auth flood | 0 | 0 | 0 |
| NetStumbler 3.2.3 | 0 | 0 | 0 |
| NetStumbler 3.3.0 | 0 | 0 | 0 |
| Death flood | 0 | 0 | 0 |
| Wellenreiter | 0 | 0 | 0 |
| NetStumbler generic | 0 | 0 | 0 |
| NetStumbler 3.2.0 | 0 | 0 | 0 |
| Reserved mgmt 7 | 0 | 0 | 0 |
| Assoc flood | 0 | 0 | 0 |
| NULL probe resp 2 | 0 | 0 | 0 |
- AP Threats/Attacks:**

| | Last Hour | 24 Hours | Total Active |
|---------------------------------|-----------|----------|--------------|
| Fake AP Attack | 0 | 0 | 0 |
| AP Missing | 0 | 0 | 0 |
| AP Impersonation | 0 | 0 | 0 |
| AP Invalid SSID | 0 | 0 | 0 |
| AP Invalid Preamble | 0 | 0 | 0 |
| AP Invalid Encryption | 0 | 0 | 0 |
| AP Invalid Radio Policy | 0 | 0 | 0 |
| Denial of Service (NAV related) | 0 | 0 | 0 |
- Client Security Related:**

| | Last Hour | 24 Hours | Total Active |
|------------------------|-----------|----------|--------------|
| Excluded Client Events | 0 | 0 | 0 |
| WEP Decrypt Errors | 0 | 0 | 0 |
| WPA MIC Errors | 0 | 0 | 0 |
| Shunned Clients | 0 | 0 | 0 |
| IPSEC Failures | 0 | 0 | 0 |

11. 分類された AP の詳細、特に Malicious AP、Friendly AP、および Unclassified AP の詳細は、[Security Summary] ページから該当する分類をクリックすると表示されます。これは、Malicious AP の例です。

Wireless Control System

Username: root | Logout | Refr

Monitor Reports Configure Location Administration Tools Help

Quick Search

Search Alarms

New Search...

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 | 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:a8:5c | 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 |

関連情報

- [Unified Wireless Network における不正検出](#)
- [テクニカルサポートとドキュメント - Cisco Systems](#)