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

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）が表示されていました。 不正の状態が異なっていても、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 が見つかり、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**.

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

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

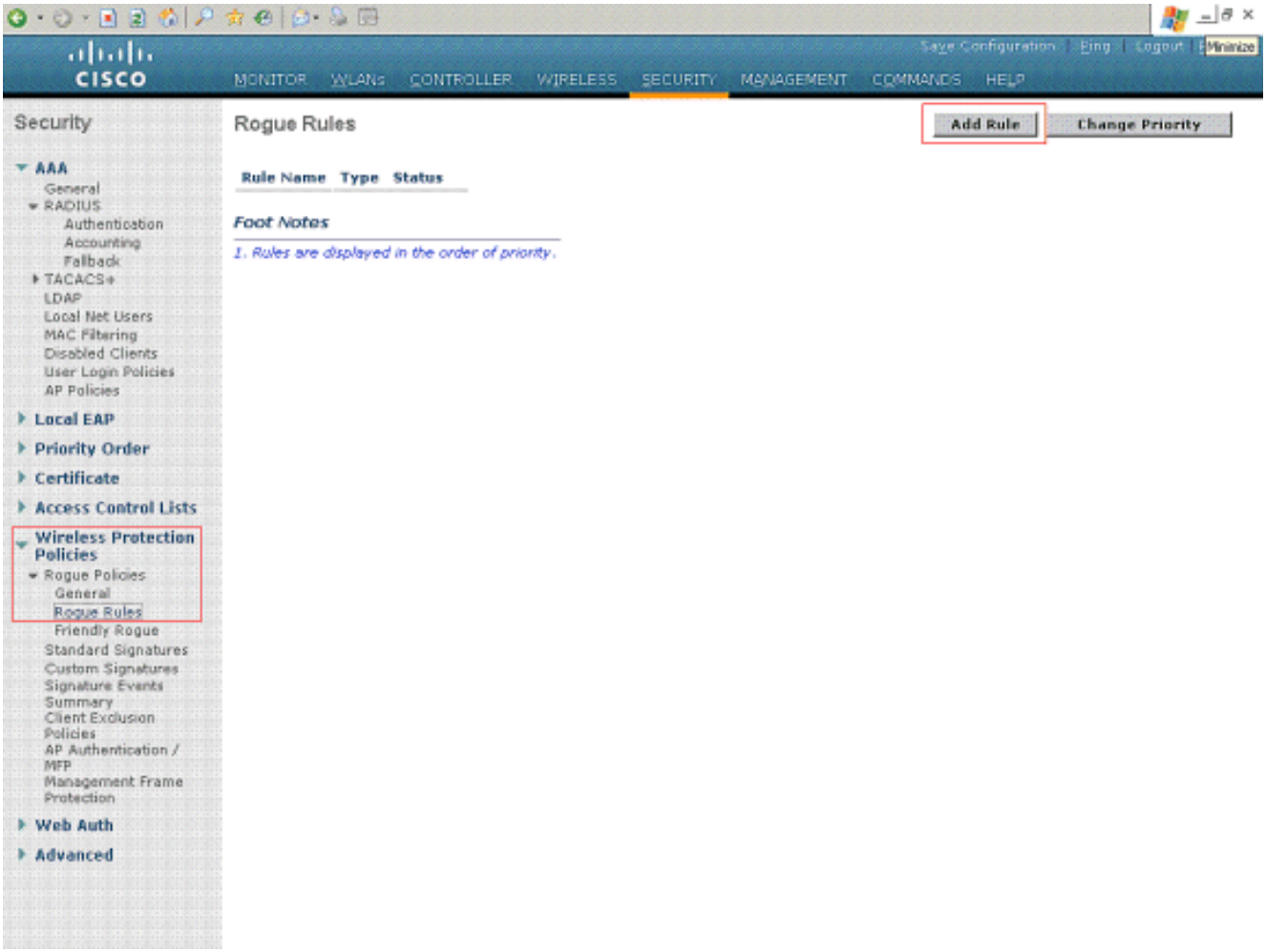
不正の状態の説明

- **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。

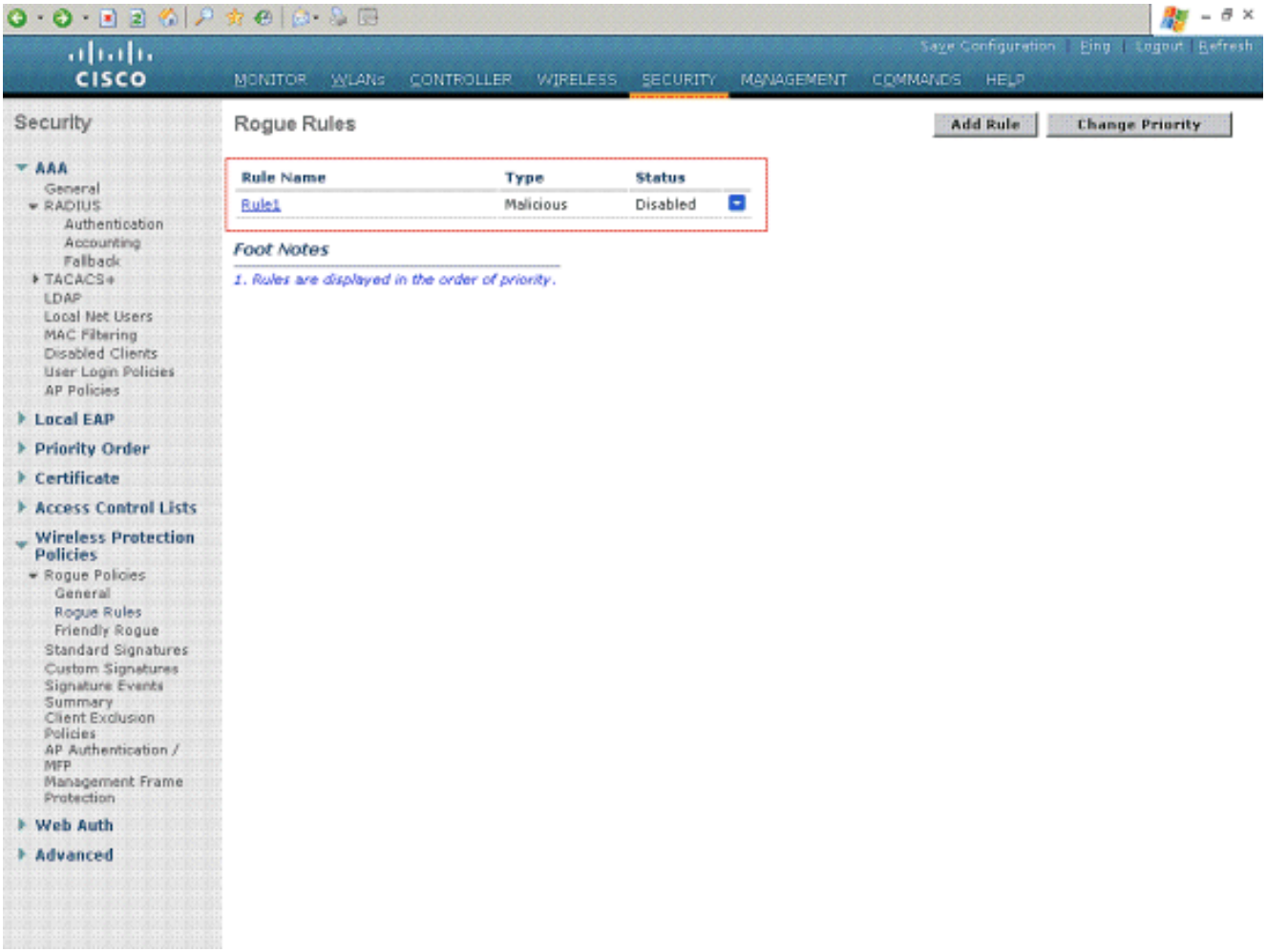
WLC で不正ルールを設定する方法

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。

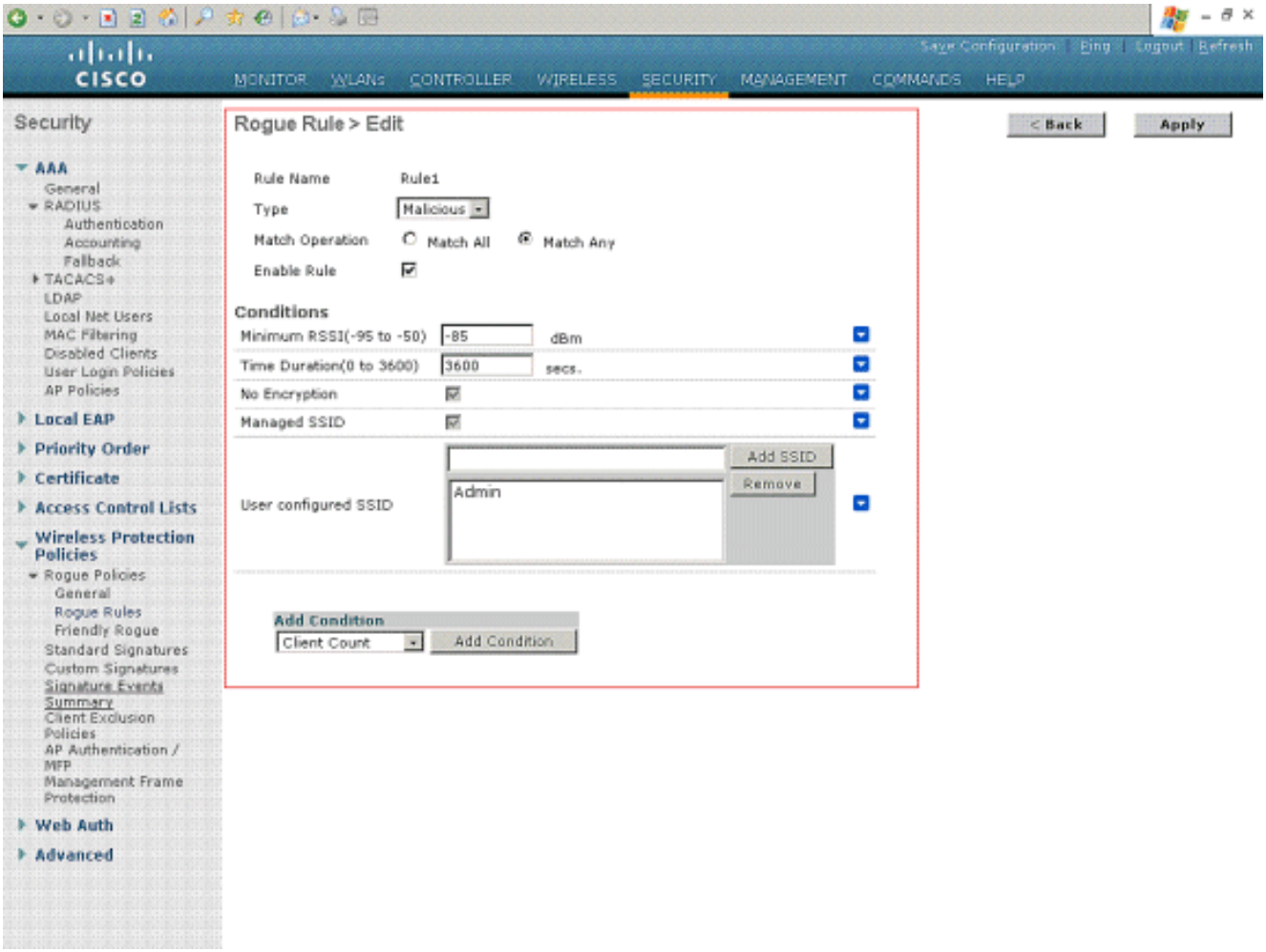
1. 不正ルールは、[Security] > [Wireless Protection Policies] > [Rogue Policies] > [Rogue Rules] のページから WLC で作成できます。



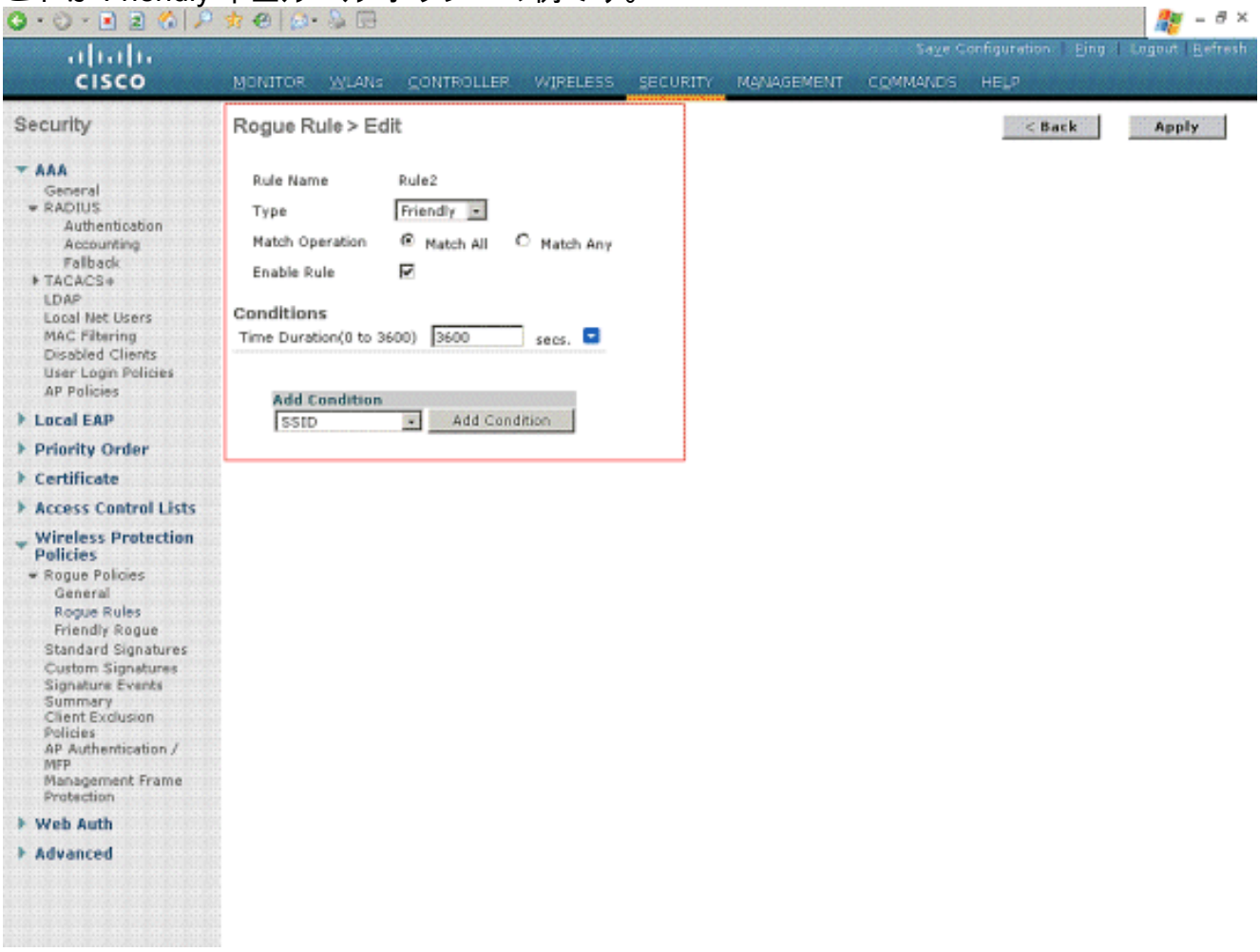
2. 新しい不正ポリシーを作成するには、[Add Rule] ボタンをクリックします。 [Rogue Rules] ウィンドウが表示されます。 ルールの名前を入力します。 この例では Rule1 を使用しています。 ルールのタイプを選択します。 これは、Malicious ルールの例です。 [Add] をクリックします。 Rule1 が作成されます。



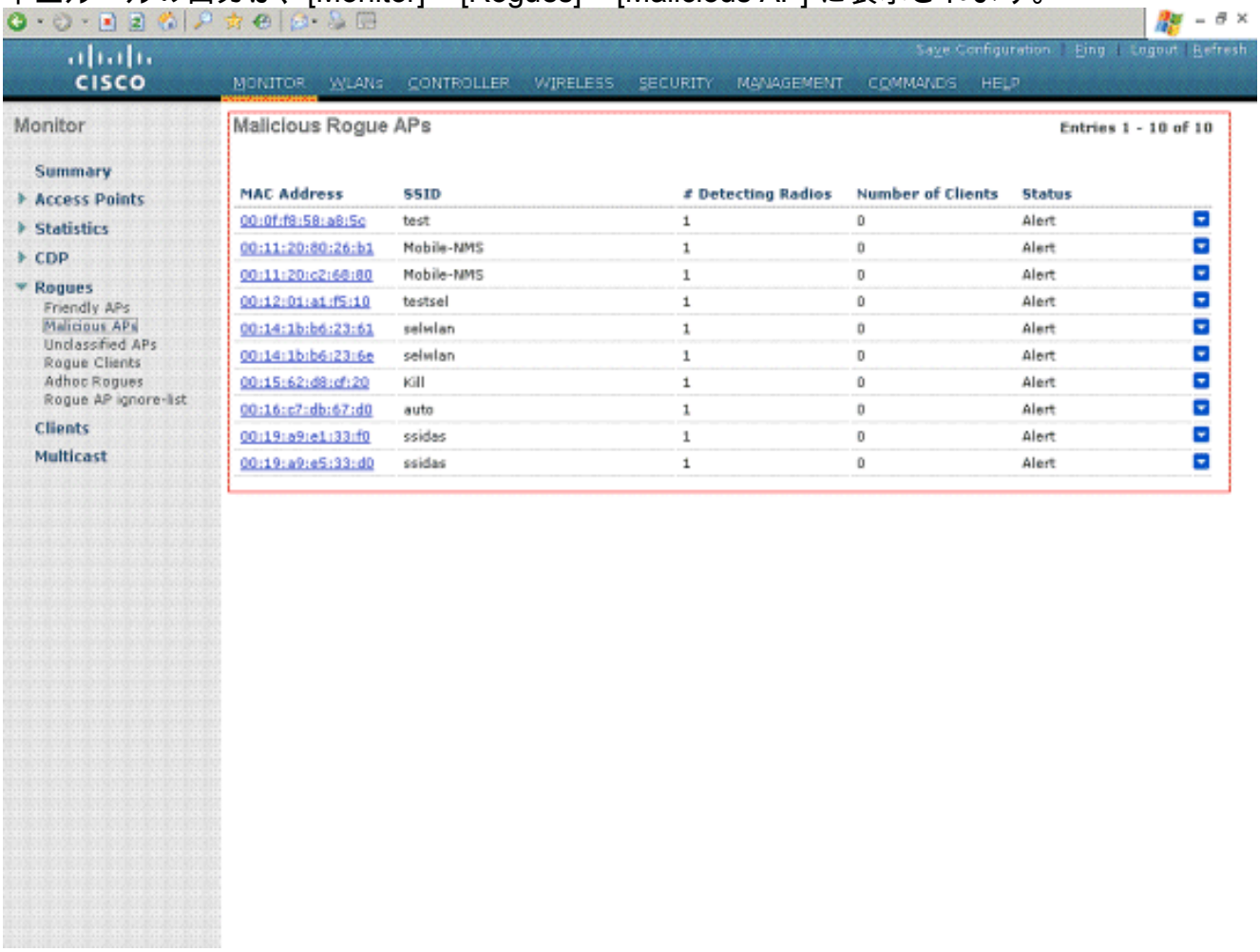
3. このルールを編集するには、作成されたルールをクリックします。 [Rogue Rule > Edit] ページが表示されます。 このページで、ルールをアクティブにするには、[Enable Rule] チェックボックスをオンにします。 次の例のように、要件に基づいて [Match Operation] のタイプやその他の条件を選択します。



4. これは Friendly 不正ルール ポリシーの例です。



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

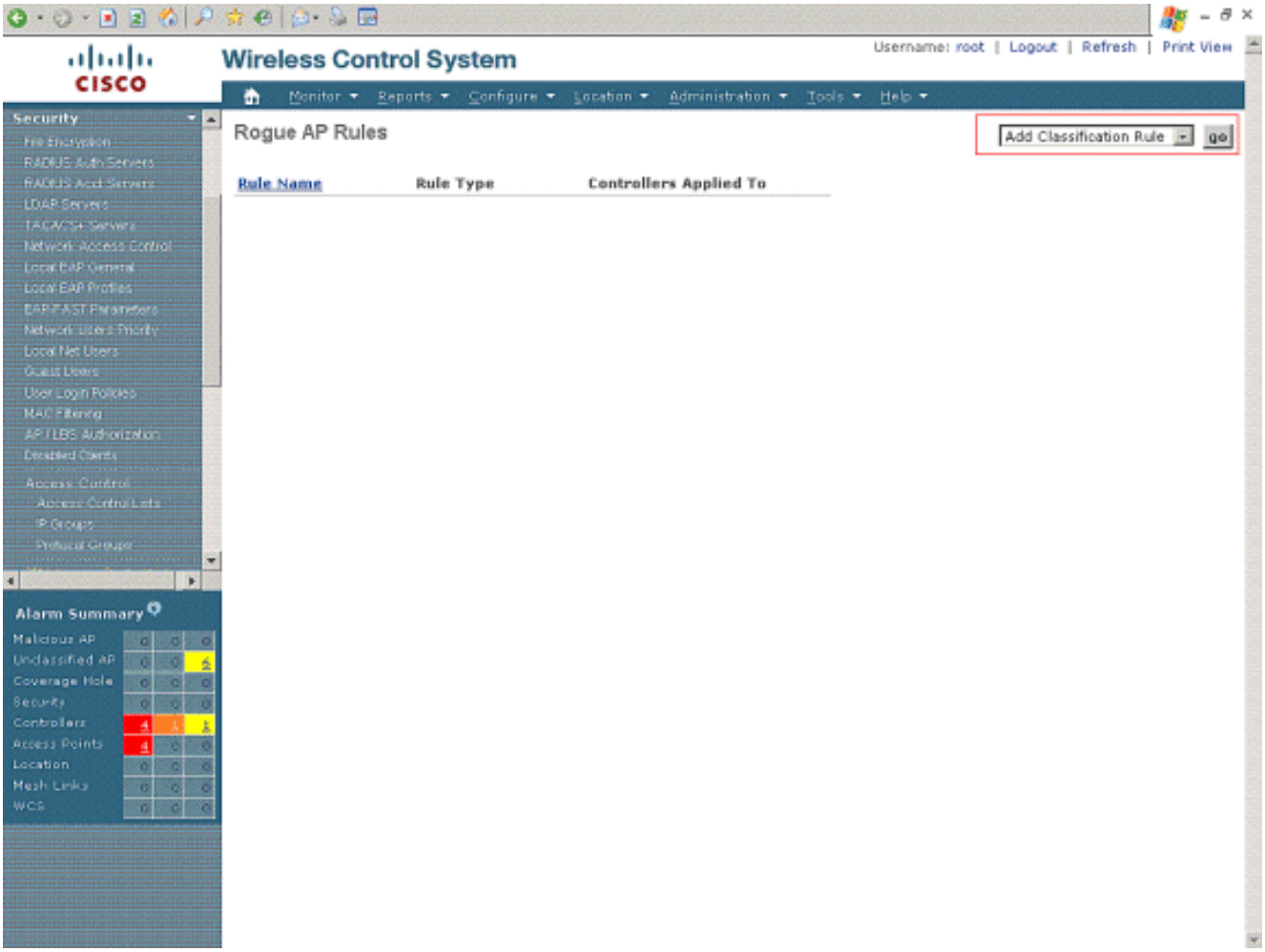


6. 同様に、*Friendly Rules* と *Unclassified Rules* の出力は、それぞれ [Monitor] > [Rogues] > [Unclassified AP] および [Monitor] > [Rogues] > [Friendly AP] のページで確認できます。

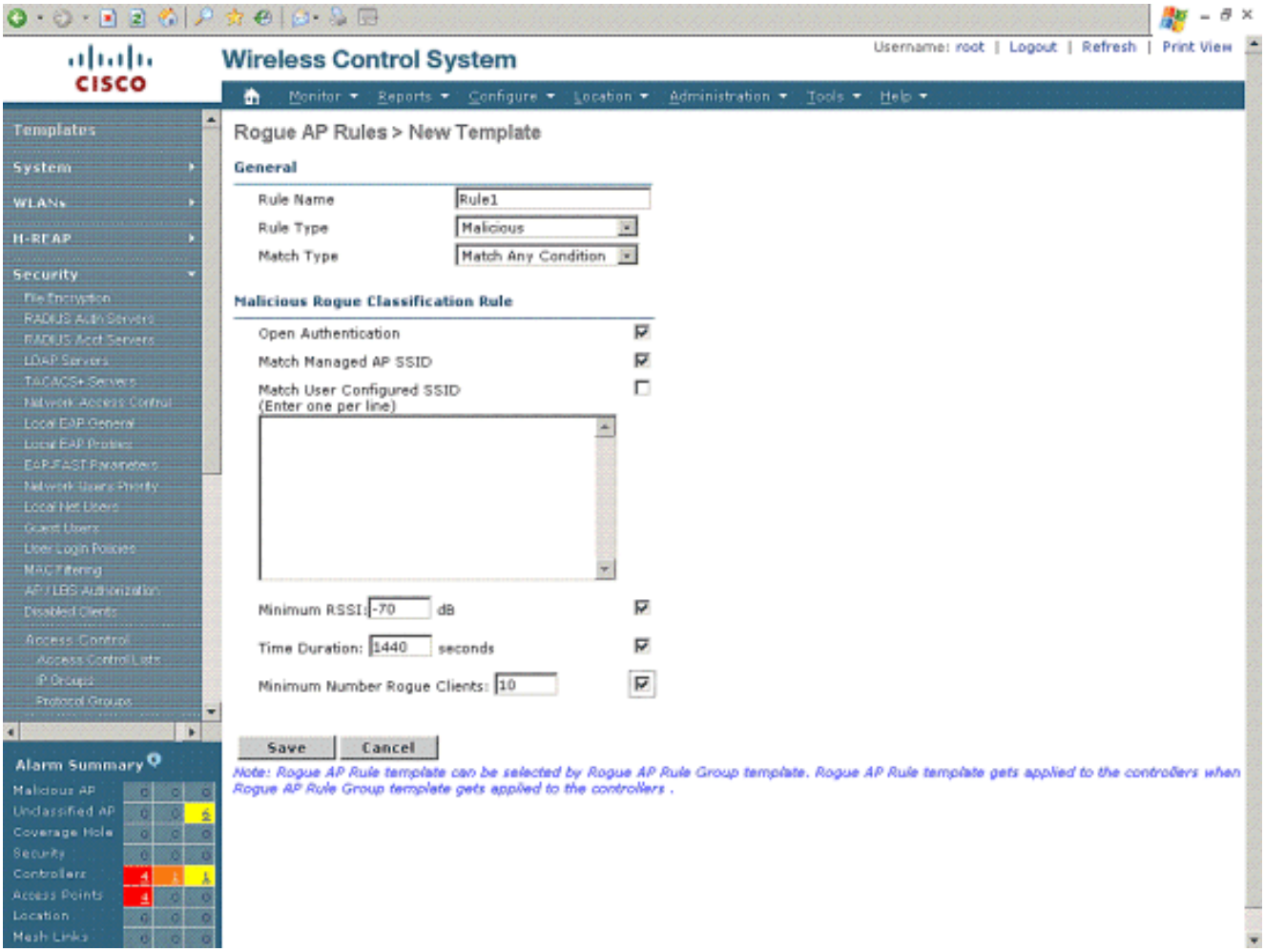
WCS で不正ルールを設定する方法

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。

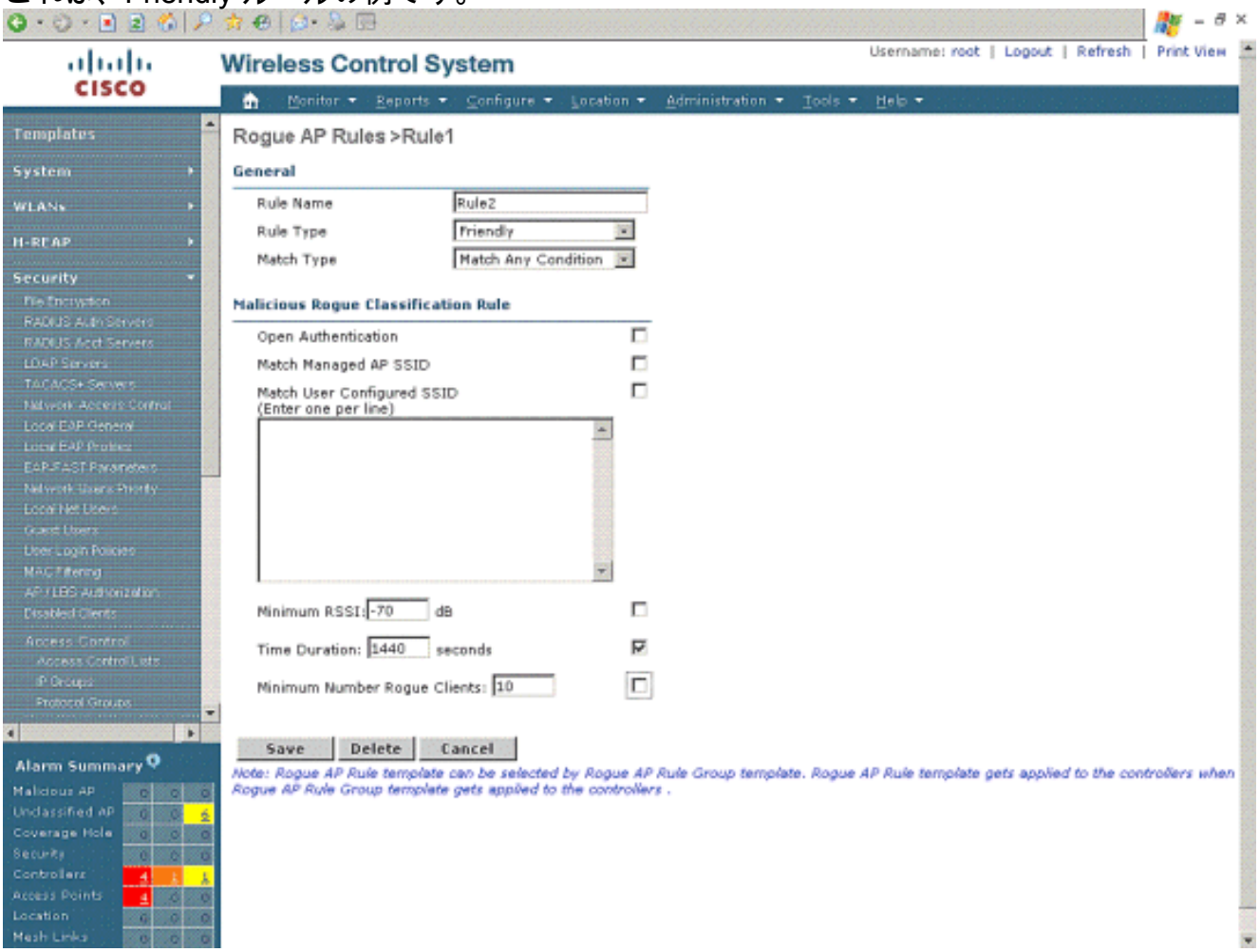
1. [Configure] > [Controller Template] を選択し、[Security] > [Rogue AP Rules] をクリックし、[Rogue AP Rules] のリストのページにアクセスします。
2. 新しい分類ルールを追加するには、右上のドロップダウン メニューから[Add Classification Rule] をクリックします。



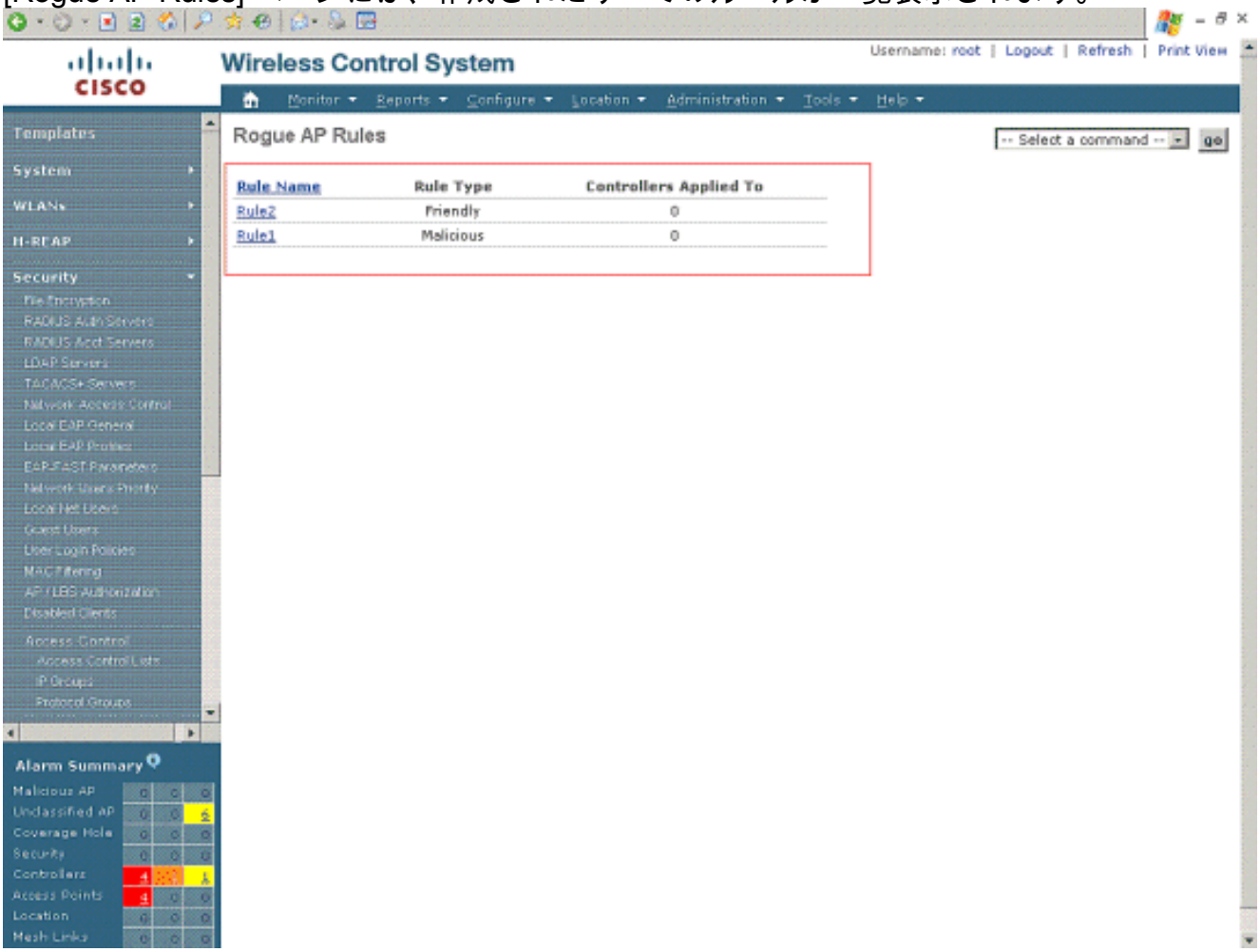
3. 不正ルールを編集するためにテンプレート名をクリックします。 このルールの詳細ページでは、不正 AP ルールの編集やアップデート、または削除を行えます。**不正 AP ルールの設定パラメータ：** このページでは、ユーザは次の条件のいずれか、またはすべてを連結するためにチェックボックスをチェックすることによって条件をイネーブルにできます。暗号化なし管理対象 AP と一致ユーザ設定の SSID と一致最小構成の RSSIコール時間最小数の不正クライアントこれは、Malicious ルールの例です。



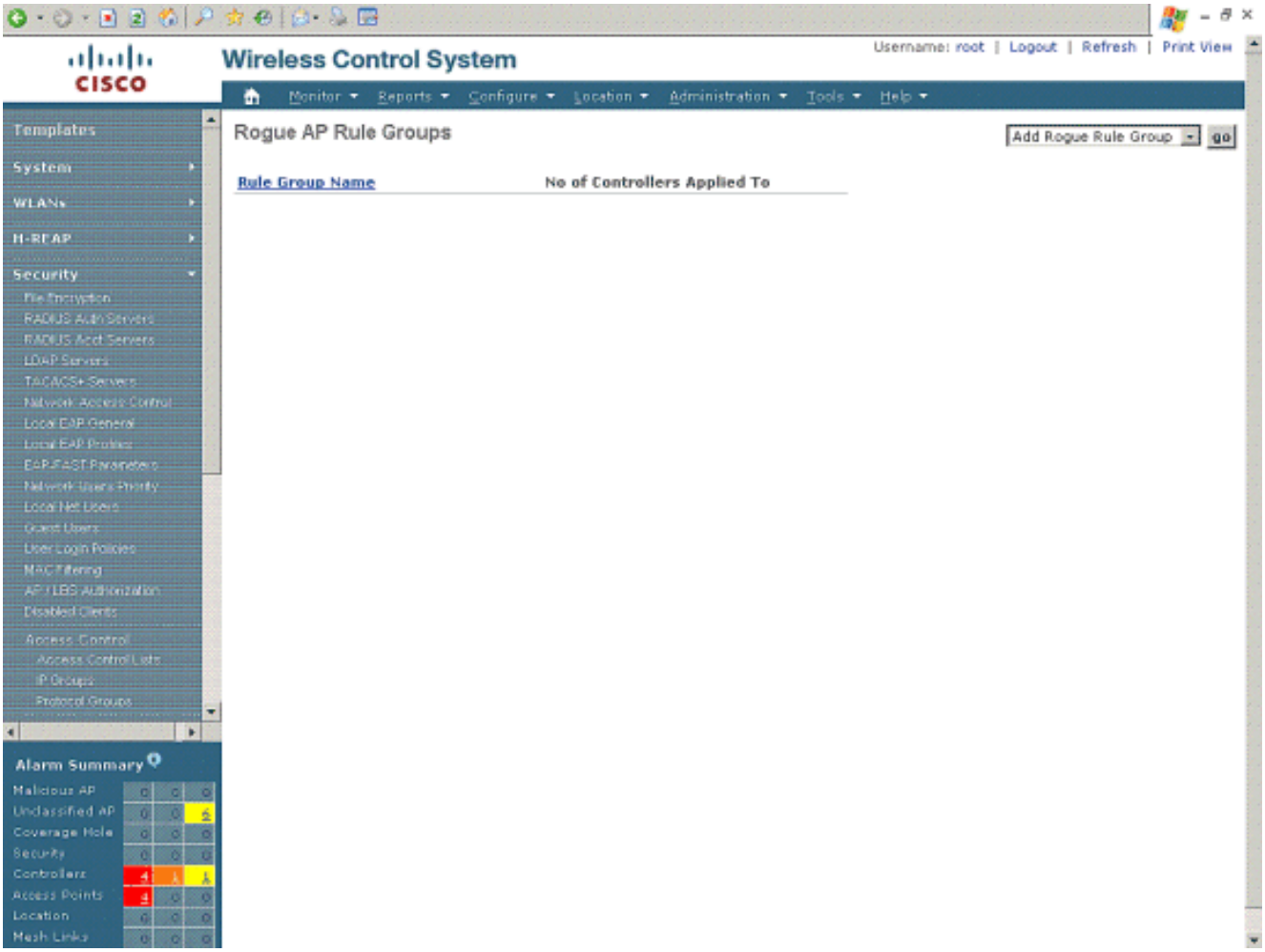
これは、Friendly ルールの例です。



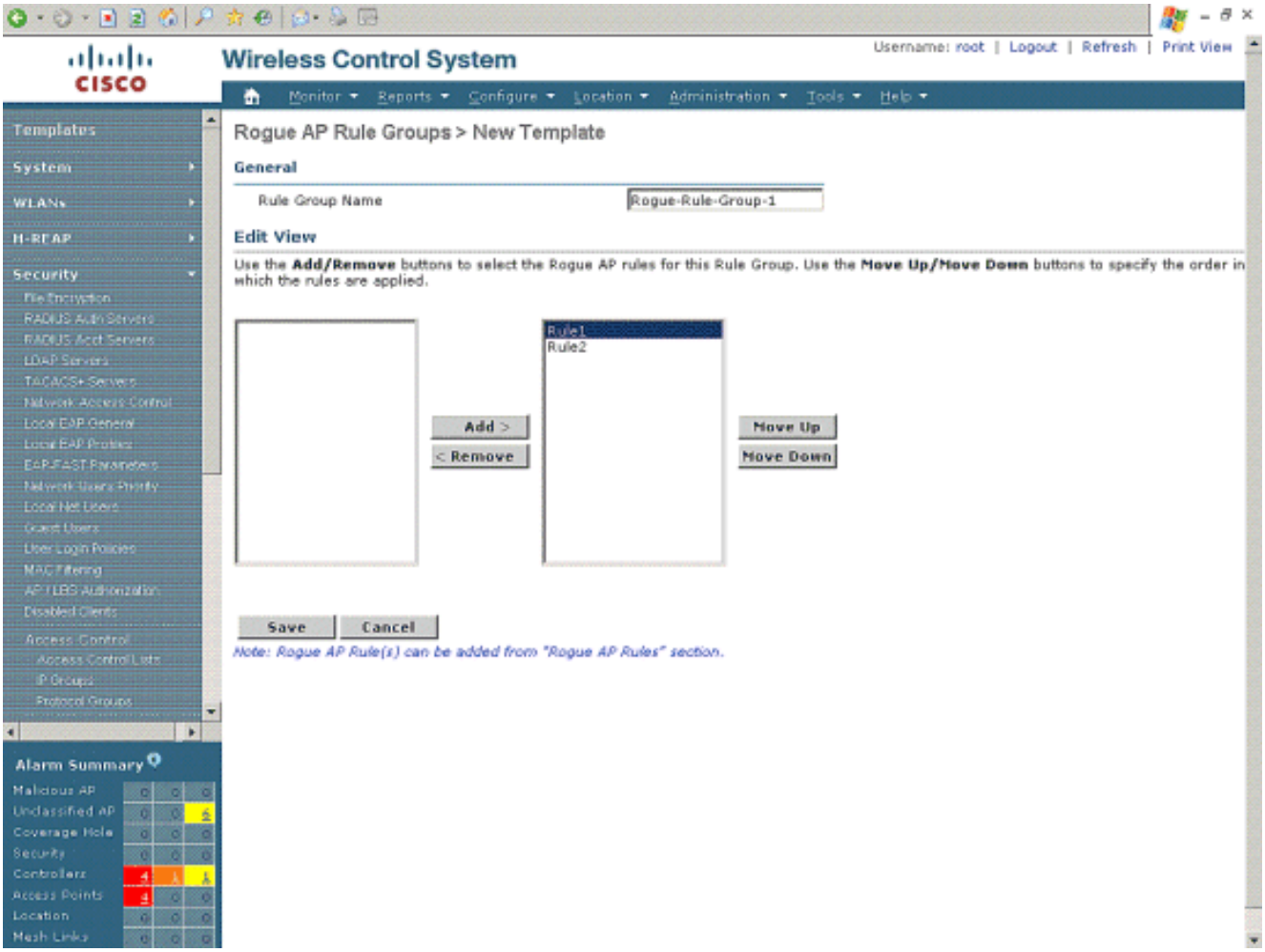
4. [Rogue AP Rules] ページには、作成されたすべてのルールが一覧表示されます。



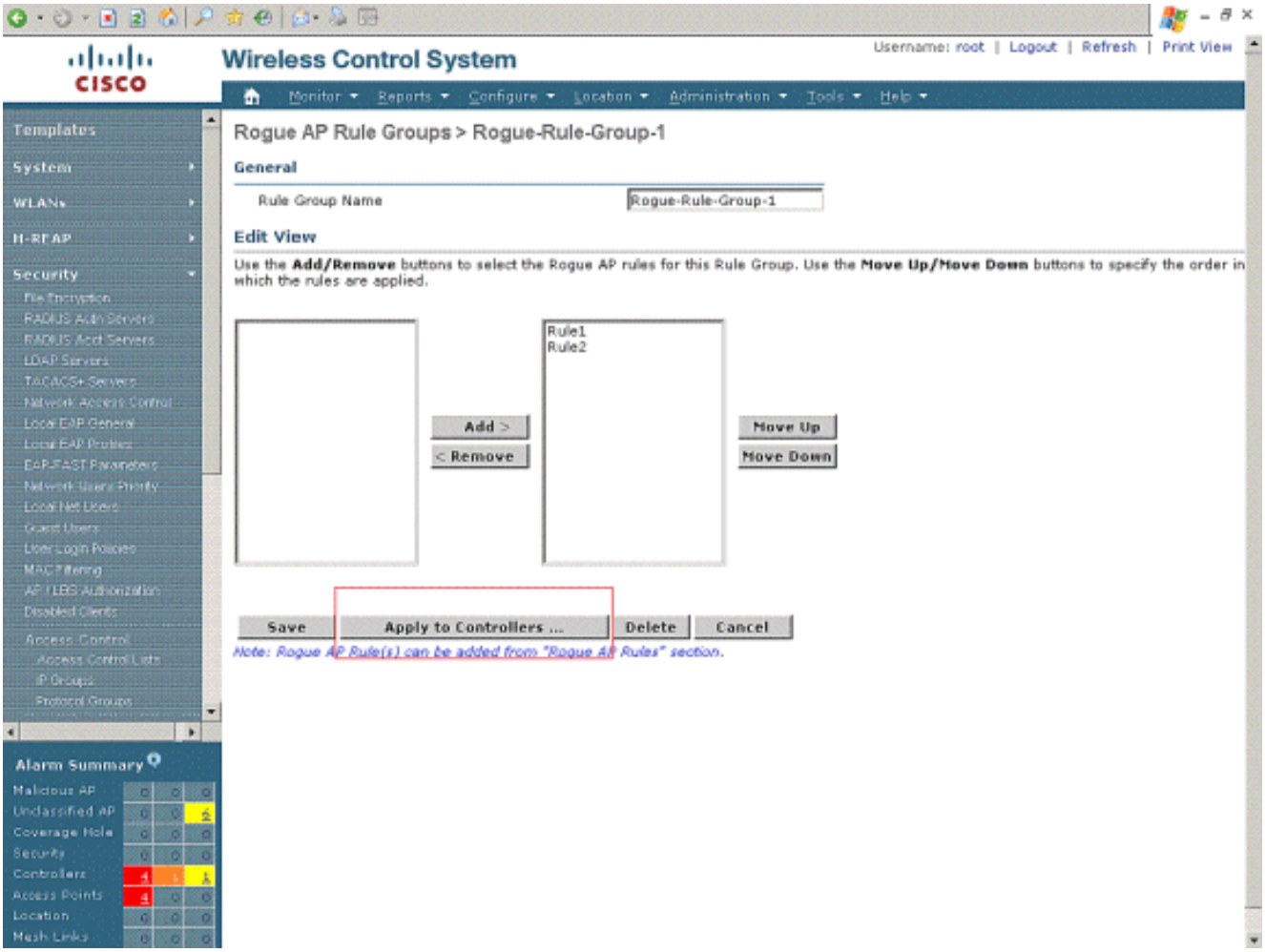
5. 次の手順では、ルール グループを設定し、これらのルールをコントローラに適用します。これには、WCS の [Rogue AP Rule Groups] 設定を使用します。
6. 新しいルール グループを作成するには、[Configure] > [Controller Template] を選択し、WCS GUI から [Security] > [Rogue AP Rule Groups] をクリックします。



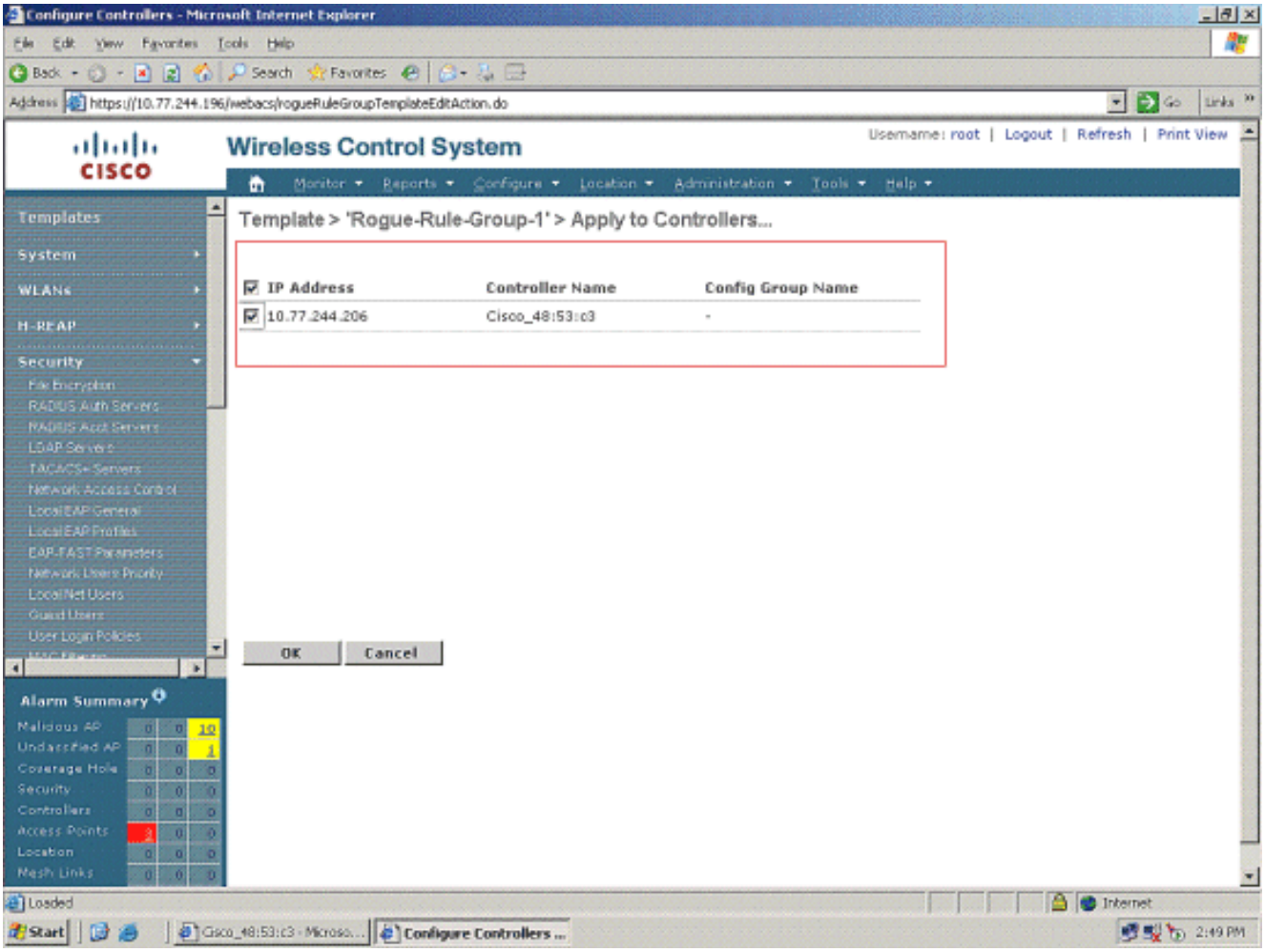
7. [Rogue AP Rule Groups > New Template] ページでは、不正 AP ルール グループの追加とアップデート、ルールの削除、コントローラへのルール グループの適用を実行することができます。 このルール グループの不正 AP ルールを選択するには、[Add]/[Remove] ボタンを使用します。 [Up]/[Down] ボタンをクリックして、ルールが適用される順序を指定します。 次に例を示します。 ルール グループが設定されたら、[Save] をクリックします。



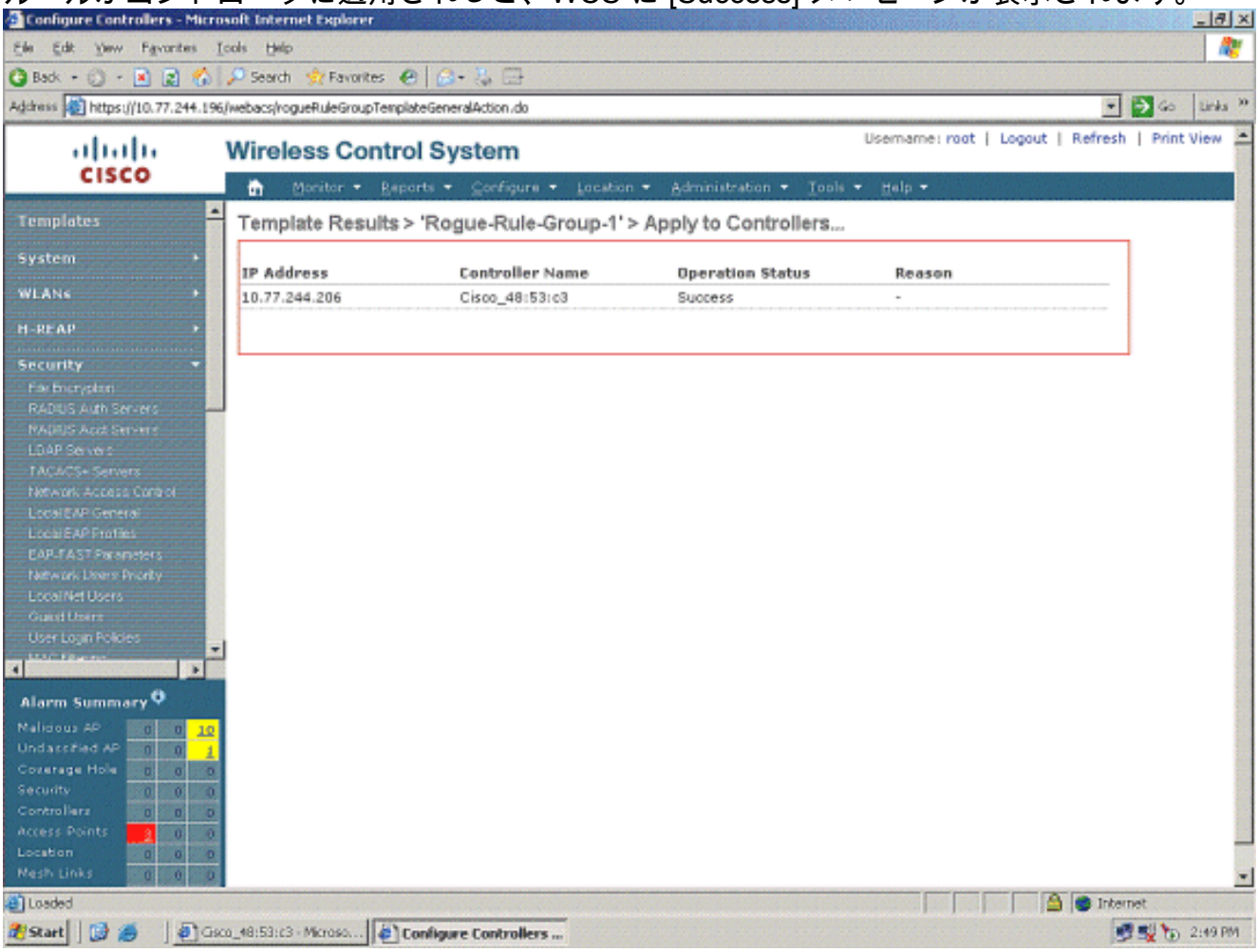
8. ルール グループを保存したら、これをコントローラに適用できます。 コントローラにルール グループを適用するには、ルール グループを編集します。 ルール グループ名をクリックします。



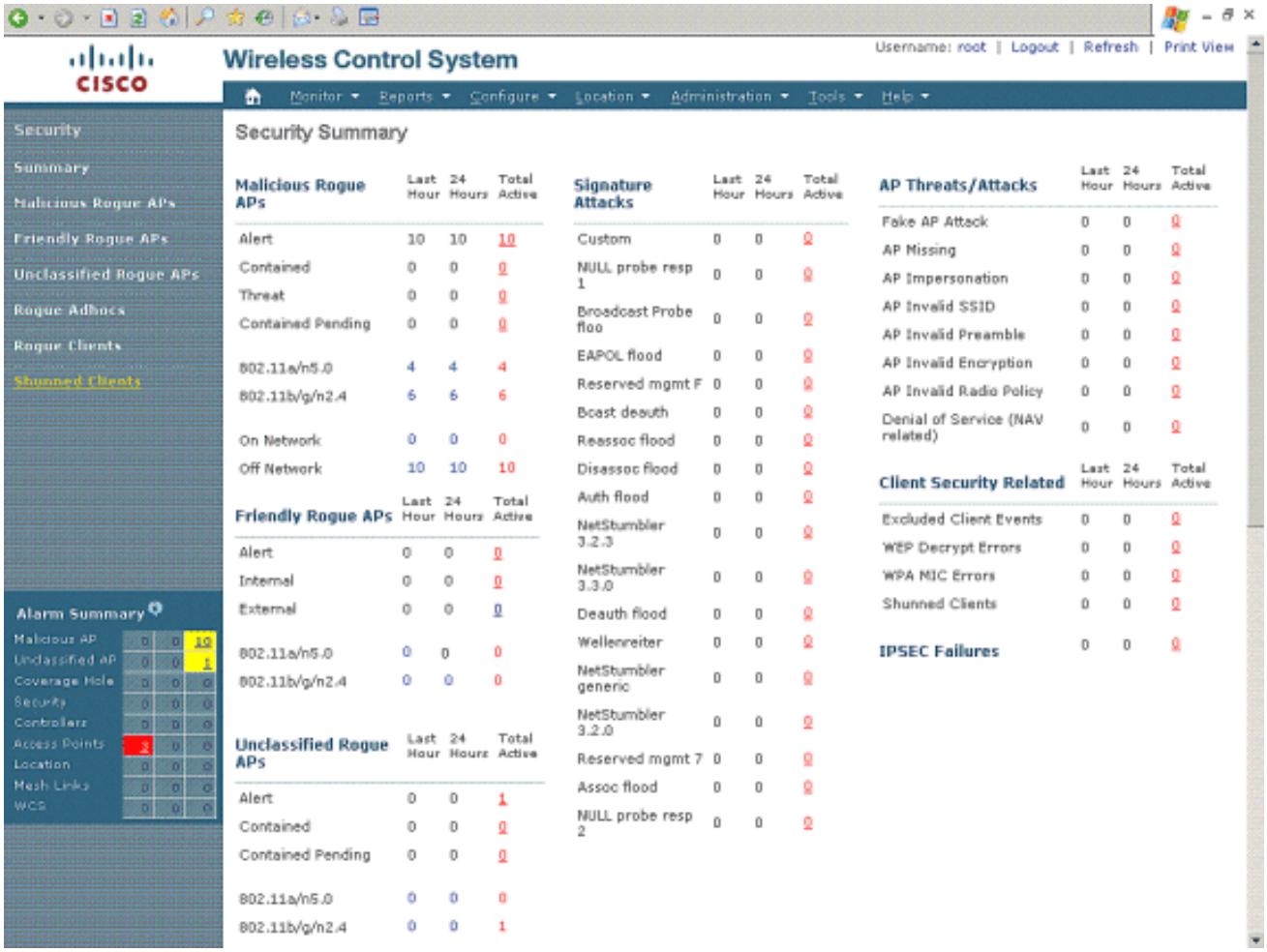
[Apply to Controllers] をクリックします。 次のページで、このルールを適用するコントローラを選択します。 次に例を示します。



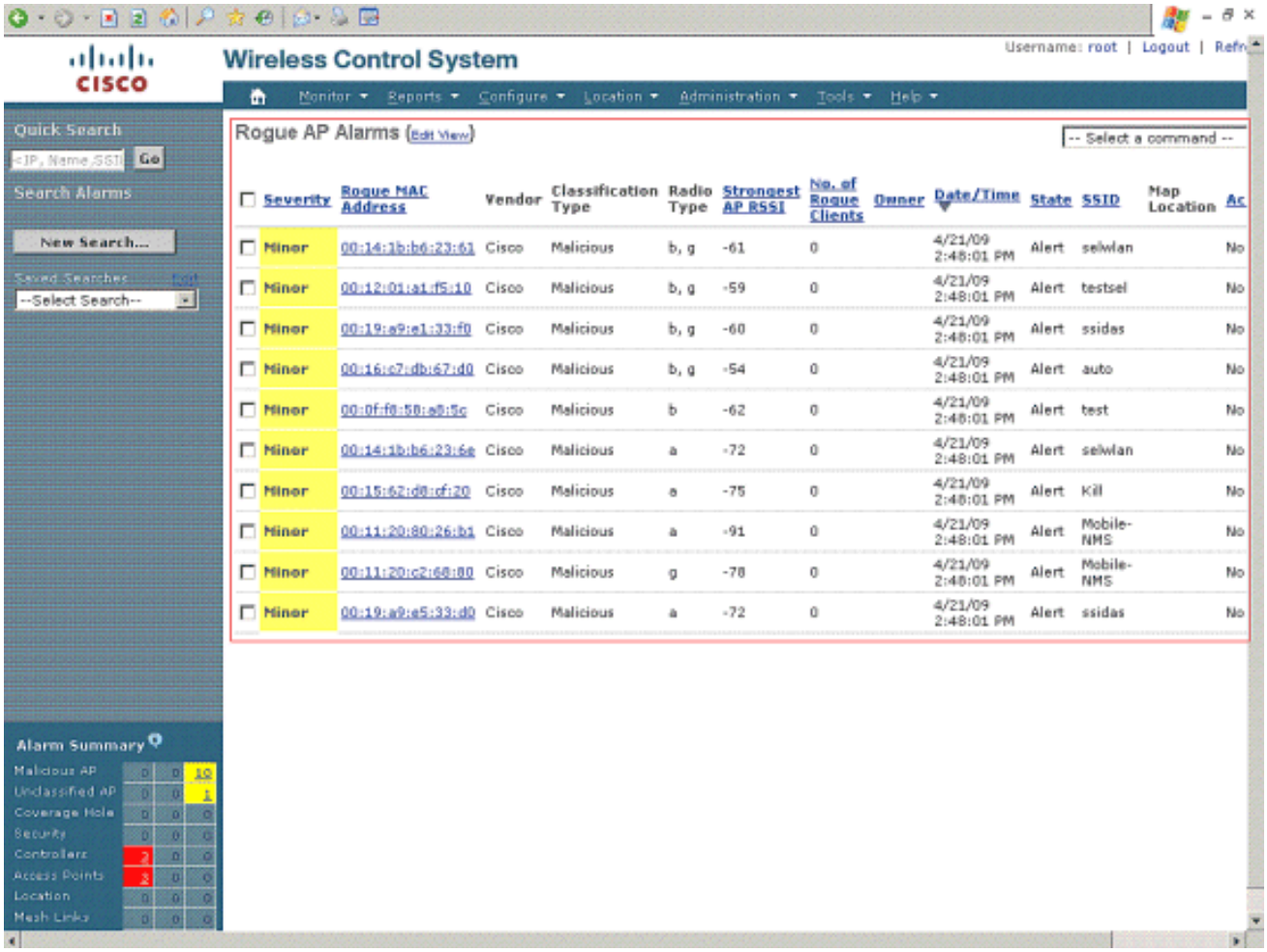
9. ルールがコントローラに適用されると、WCS に [Success] メッセージが表示されます。



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。



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。



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