ワイヤレス LAN コントローラの信頼された AP ポリシー

内容

概要

このドキュメントでは、ワイヤレスLANコントローラ(WLC)上の信頼できるAPワイヤレス保護ポリシーについて説明し、信頼できるAPポリシーを定義し、すべての信頼できるAPポリシーについて簡単に説明します。

前提条件

要件

ワイヤレスLANセキュリティパラメータ（SSID、暗号化、認証など）に関する基本的な知識があることを確認します。

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。

信頼できるAPポリシー

信頼できるAPポリシーは、コントローラとともにパラレル自律APネットワークを使用するシナリオで使用するように設計された、コントローラのセキュリティ機能です。このシナリオでは、Autonomous APをコントローラ上の信頼できるAPとしてマークし、ユーザがこれらの信頼できるAPのポリシー（WEPまたはWPA、独自のSSID、ショートプリアンブルなどを使用する必要があります）を定義できます。 これらのAPのいずれかが、これらのポリシーを満たしていない場合

、コントローラは、信頼できるAPが設定済みのポリシーに違反したことを示すアラームをネットワーク管理デバイス(Wireless Control System)に送信します。

信頼できるAPとは何ですか。

信頼できるAPは、組織に属していないAPです。ただし、ネットワークにセキュリティ上の脅威は発生しません。これらのAPは、フレンドリーAPとも呼ばれます。APを信頼できるAPとして設定する場合は、いくつかのシナリオがあります。

たとえば、ネットワーク内に次のような異なるカテゴリのAPがあるとします。

- **LWAPPを実行していないAP（おそらくIOSまたはVxWorksを実行している）**
- 従業員が持ち込むLWAPP AP（管理者の知識を使用）
- 既存のネットワークのテストに使用されるLWAPP AP
- ネイバーが所有するLWAPP AP

通常、信頼できるAPはカテゴリ1に分類されるAPですが、**LWAPPを実行**していないユーザが所有するAPです。VxWorksまたはIOSが稼働する古いAPである可能性があります。これらのAPがネットワークを損傷しないようにするため、正しいSSIDや認証タイプなどの特定の機能を適用できます。WLCで信頼できるAPポリシーを設定し、信頼できるAPがこれらのポリシーを満たしていることを確認します。そうでない場合は、ネットワーク管理デバイス(WCS)へのアラームの発生など、いくつかのアクションを実行するようにコントローラを設定できます。

ネイバーに属する既知のAPは、信頼できるAPとして設定できます。

通常、MFP(Management Frame Protection)は、正当なLWAPP APではないAPがWLCに加入することを防止する必要があります。NICカードがMFPをサポートしている場合、実際のAP以外のデバイスからの認証解除は許可されません。MFPについての詳細は、『WLCとLAPを使用したインフラストラクチャ管理フレーム保護(MFP)の設定例』を参照してください。

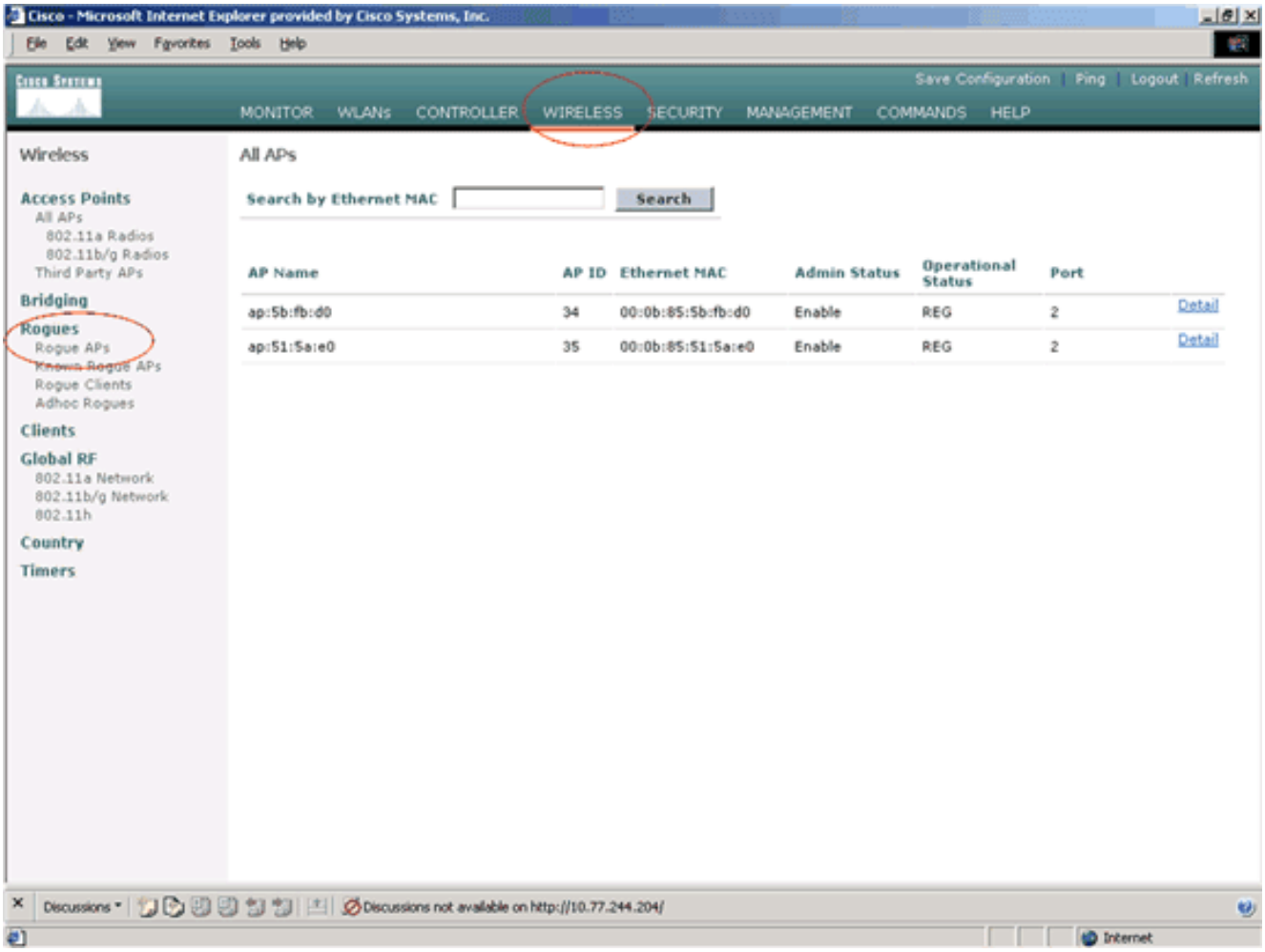
VxWorksまたはIOS（カテゴリ1など）が稼働するAPがある場合、それらはLWAPPグループに参加したり、MFPを実行したりしませんが、そのページにリストされているポリシーを適用する必要がある場合があります。このような場合、信頼できるAPポリシーは、対象のAPのコントローラで設定する必要があります。

一般に、不正なAPについて知っていて、ネットワークに対する脅威ではないことを確認した場合、そのAPを既知の信頼できるAPとして識別できます。

WLC GUIから信頼できるAPとしてAPを設定する方法

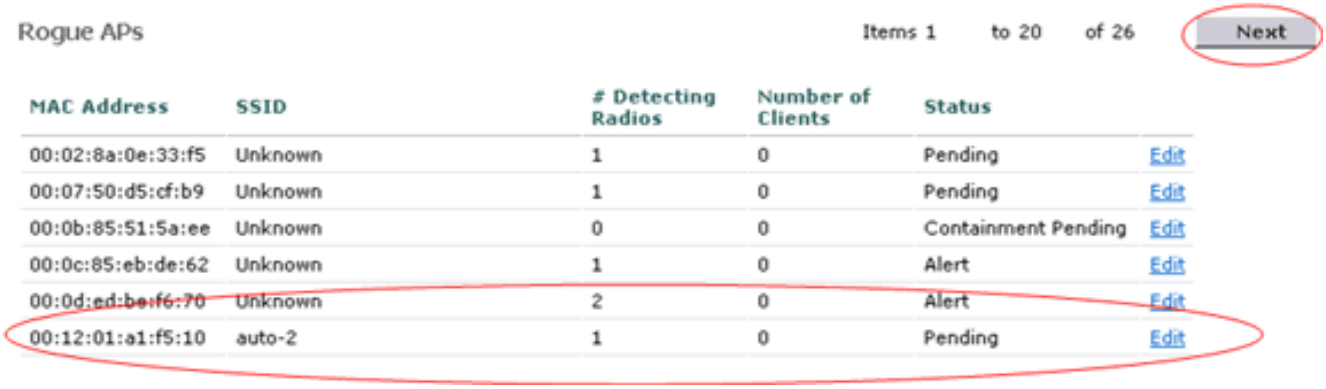
APを信頼できるAPとして設定するには、次の手順を実行します。

1. HTTPまたはhttpsログインを使用して、WLCのGUIにログインします。
2. コントローラのメインメニューで、[ワイヤレス]をクリックします。
3. [Wireless]ページの左側にあるメニューで、[Rogue APs]をクリックします。



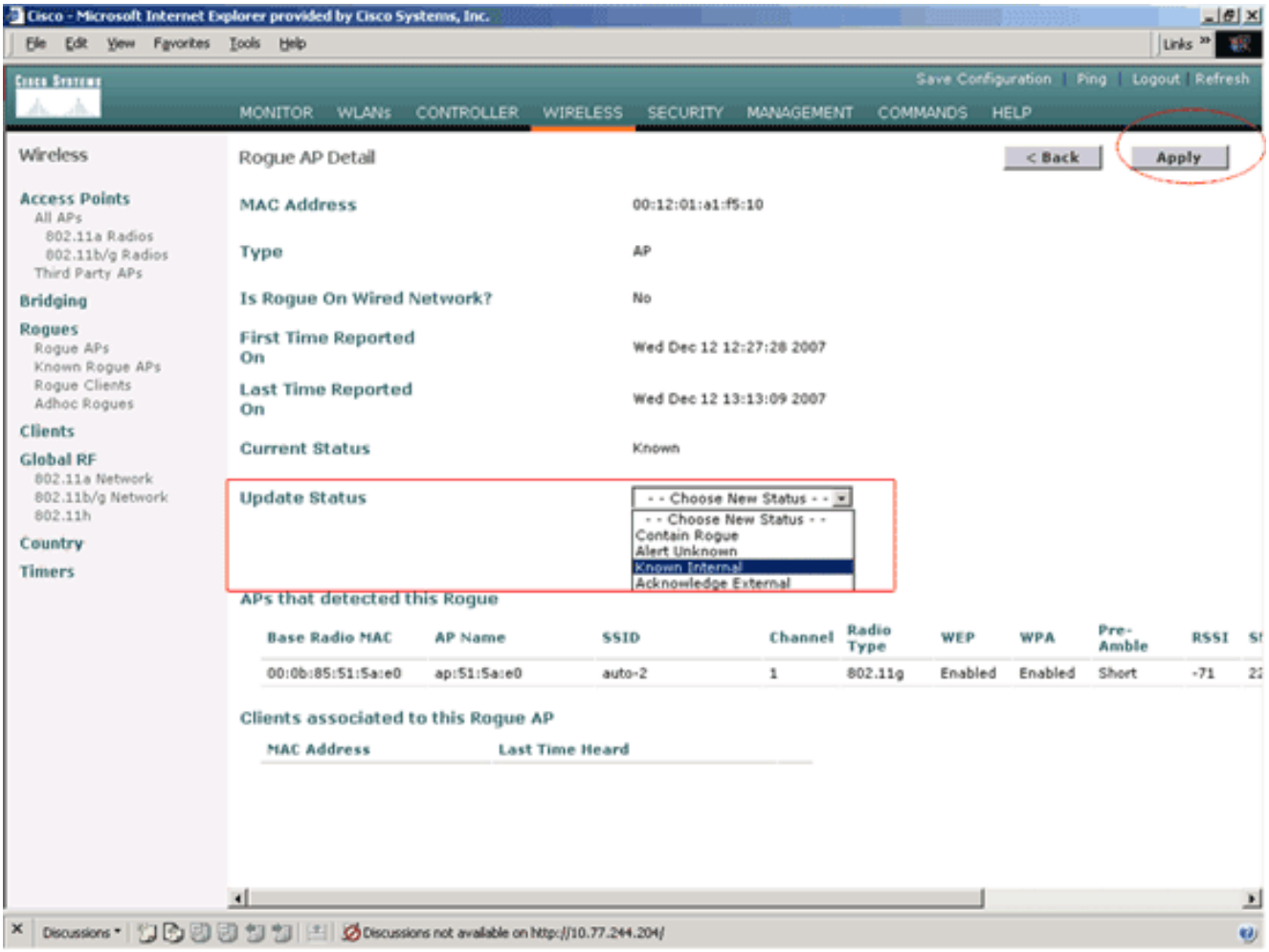
[Rogue APs]ページには、ネットワーク上の不正APとして検出されたすべてのAPがリストされます。

4. この不正APのリストから、カテゴリ1（前のセクションで説明）に該当する信頼できるAPとして設定するAPを見つけます。[Rogue APs]ページにリストされているMACアドレスでAPを特定できます。目的のAPがこのページにない場合は、[**Next**]をクリックして、次のページからAPを識別します。
5. [Rogue AP]リストから目的のAPが見つかったら、そのAPに対応する[Edit] ボタンをクリックします。これにより、APの詳細ページが表示されます。



[Rogue AP details]ページでは、このAPに関する詳細情報（そのAPが有線ネットワークに接続されているかどうか、APの現在のステータスなど）を確認できます。

6. このAPを信頼できるAPとして設定するには、[Update Status]ドロップダウンリストから[**Known Internal**]を選択し、[**Apply**]をクリックします。APのステータスを[Known Internal] に更新すると、このAPはこのネットワークの信頼できるAPとして設定されます。

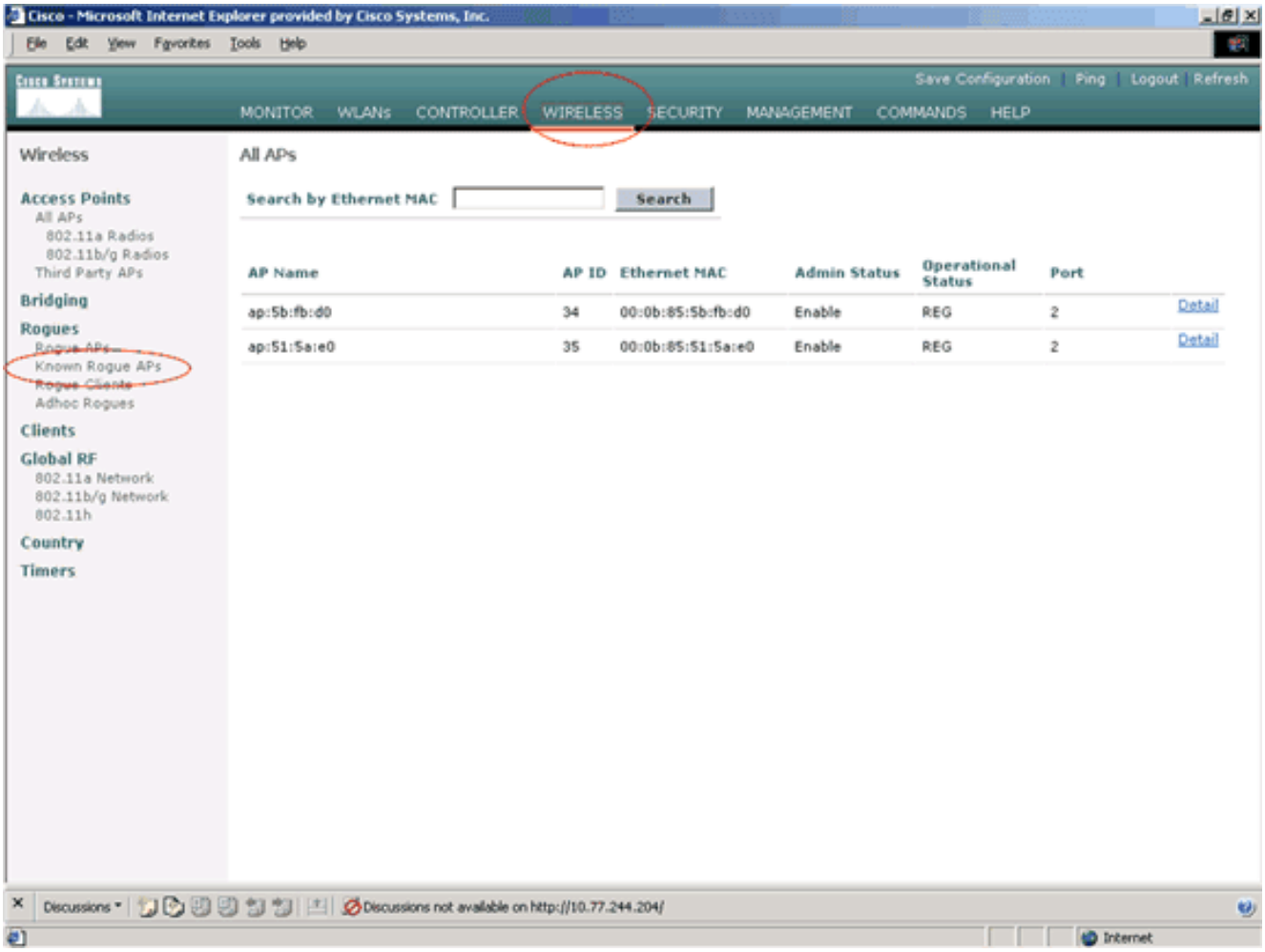


7. 信頼できるAPとして設定するすべてのAPに対して、これらの手順を繰り返します。

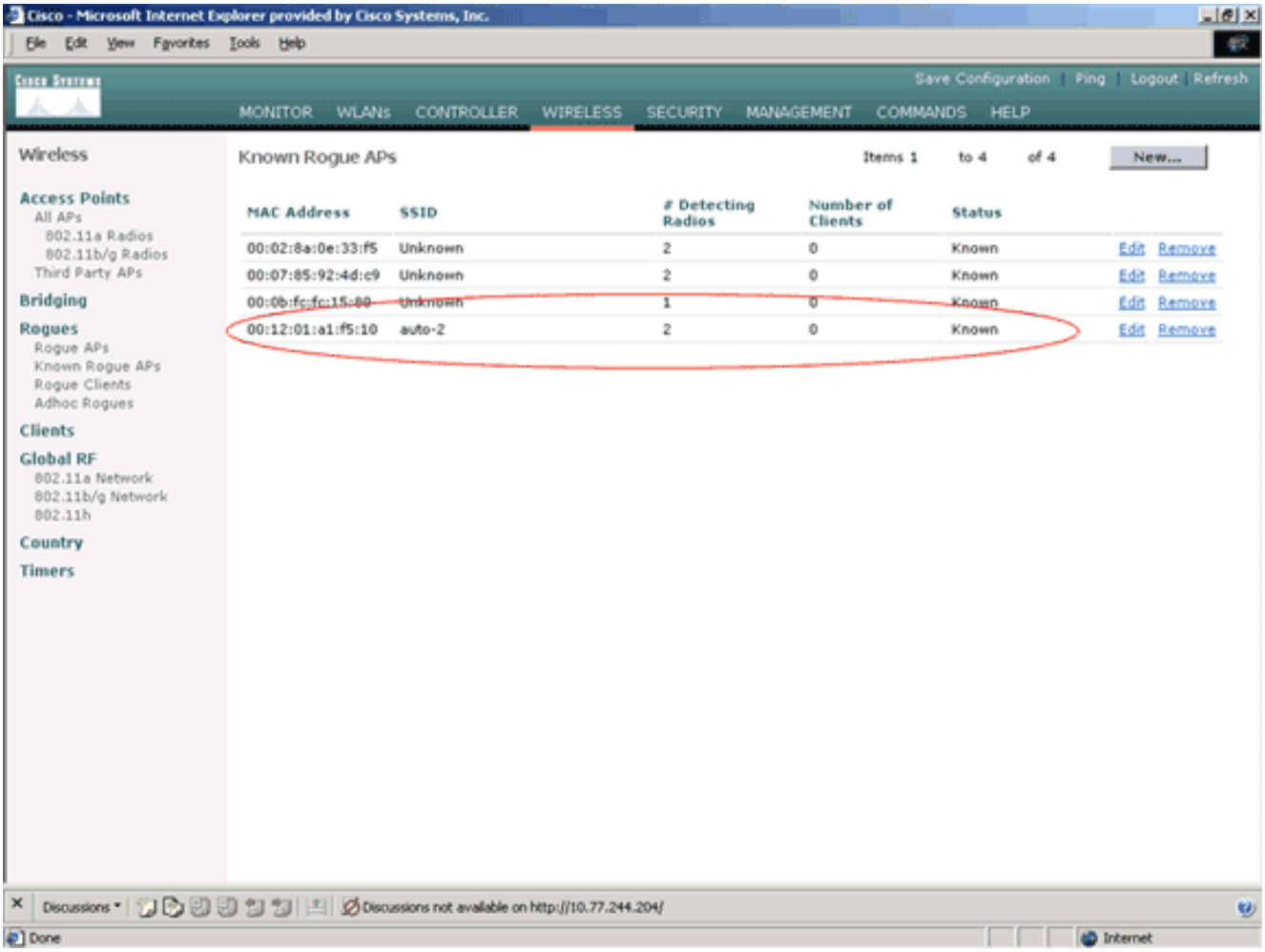
信頼できるAP設定の確認

コントローラのGUIから、APが信頼できるAPとして正しく設定されていることを確認するには、次の手順を実行します。

1. [Wireless]をクリックします。
2. [Wireless]ページの左側にあるメニューで、[Known Rogue APs]をクリックします。



目的のAPが[Known Rogue APs]ページに表示され、ステータスが[*Known*]にリストされます。



信頼できるAPポリシー設定について

WLCには次の信頼できるAPポリシーがあります。

- 暗号化ポリシーの適用
- プリアンブルポリシーの適用
- 強制無線タイプポリシー
- SSIDの検証
- 信頼できるAPがない場合のアラート
- 信頼できるAPエントリの有効期限タイムアウト（秒）

暗号化ポリシーの適用

このポリシーは、信頼できるAPが使用する暗号化タイプを定義するために使用されます。[Enforced encryption policy]では、次の暗号化タイプを設定できます。

- なし
- 開く
- WEP
- WPA/802.11i

WLCは、信頼できるAPに設定されている暗号化タイプが、[Enforced encryption policy] 設定に設定されている暗号化タイプと一致するかどうかを確認します。信頼できるAPが指定された暗号化タイプを使用しない場合、WLCは適切なアクションを実行するために管理システムにアラームを発行します。

プリアンブルポリシーの適用

無線プリアンブル（ヘッダーとも呼ばれる）は、ワイヤレスデバイスがパケットを送受信するときに必要な情報を含むパケットの先頭のデータのセクションです。**ショートプリア**ンブルはスループットパフォーマンスを向上するため、デフォルトで有効になっています。一方、SpectraLink NetLink 電話機のようないくつかの無線デバイスでは、ロング プリアンブルが必要です。[Enforced preamble policy]で次のプリアンブルオプションを設定できます。

- なし
- Short
- Long

WLCは、信頼できるAPに設定されているプリアンブルタイプが、[Enforced preamble policy] 設定で設定されているプリアンブルタイプと一致するかどうかを確認します。信頼できるAPが指定されたプリアンブルタイプを使用しない場合、WLCは適切なアクションを実行するために管理システムにアラームを発生させます。

強制無線タイプポリシー

このポリシーは、信頼できるAPが使用する無線タイプを定義するために使用されます。[Enforced radio type policy]で、次のいずれかの無線タイプを設定できます。

- なし
- 802.11bのみ
- 802.11aのみ
- 802.11b/gのみ

WLCは、信頼できるAPに設定されている無線タイプが、[Enforced radio type policy] 設定に設定されている無線タイプと一致するかどうかを確認します。信頼できるAPが指定された無線を使用しない場合、WLCは適切なアクションを実行するために管理システムにアラームを発生させます。

SSIDの検証

コントローラで設定したSSIDに対して、信頼できるAP SSIDを検証するようにコントローラを設定できます。信頼できるAPのSSIDがコントローラのSSIDのいずれかに一致すると、コントローラはアラームを発生します。

信頼できるAPがない場合のアラート

このポリシーが有効になっている場合、信頼できるAPが既知の不正APリストに存在しない場合、WLCは管理システムに警告します。

信頼できるAPエントリの有効期限タイムアウト（秒）

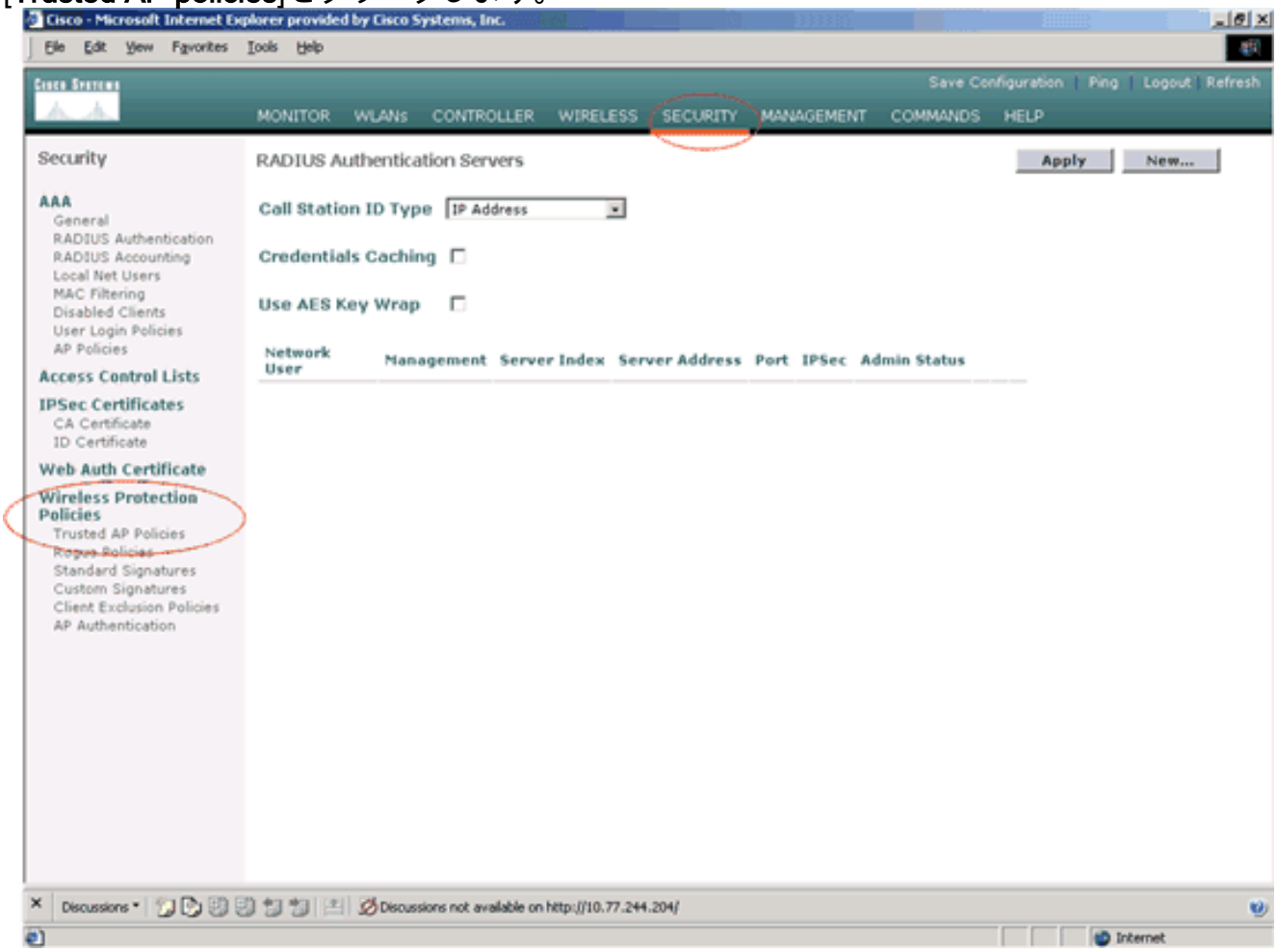
この[Expiration Timeout]値は、信頼できるAPが期限切れとしてWLCエントリからフラッシュされるまでの秒数を指定します。このタイムアウト値は、秒（120 ~ 3600秒）で指定できます。

WLCでの信頼できるAPポリシーの設定方法

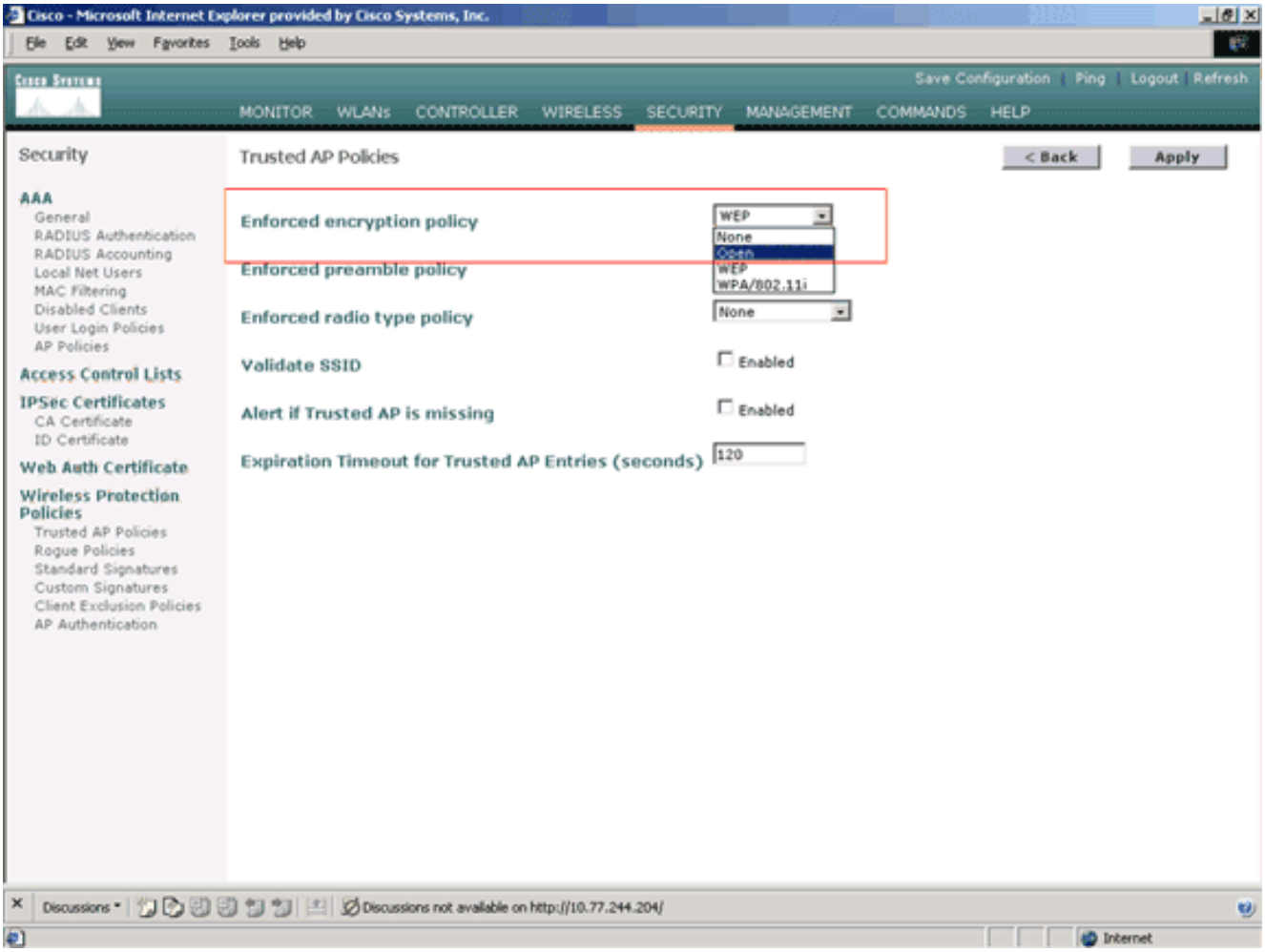
GUIを使用してWLCで信頼できるAPポリシーを設定するには、次の手順を実行します。

注：信頼できるAPポリシーはすべて、同じWLCページにあります。

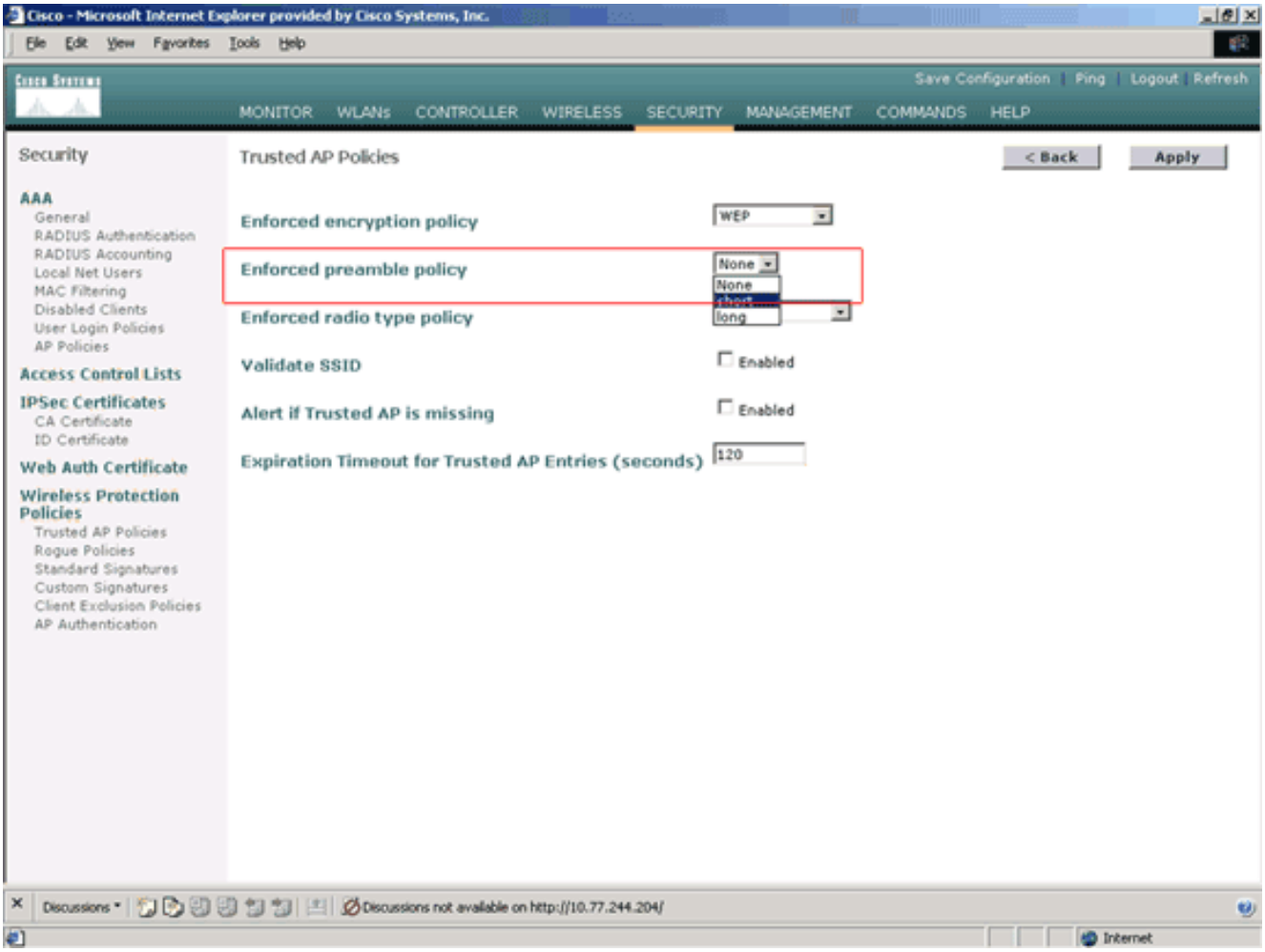
1. WLC GUIのメインメニューで、[**Security**]をクリックします。
2. [Security]ページの左側にあるメニューから、[Wireless Protection Policies]の下に表示される[**Trusted AP policies**]をクリックします。



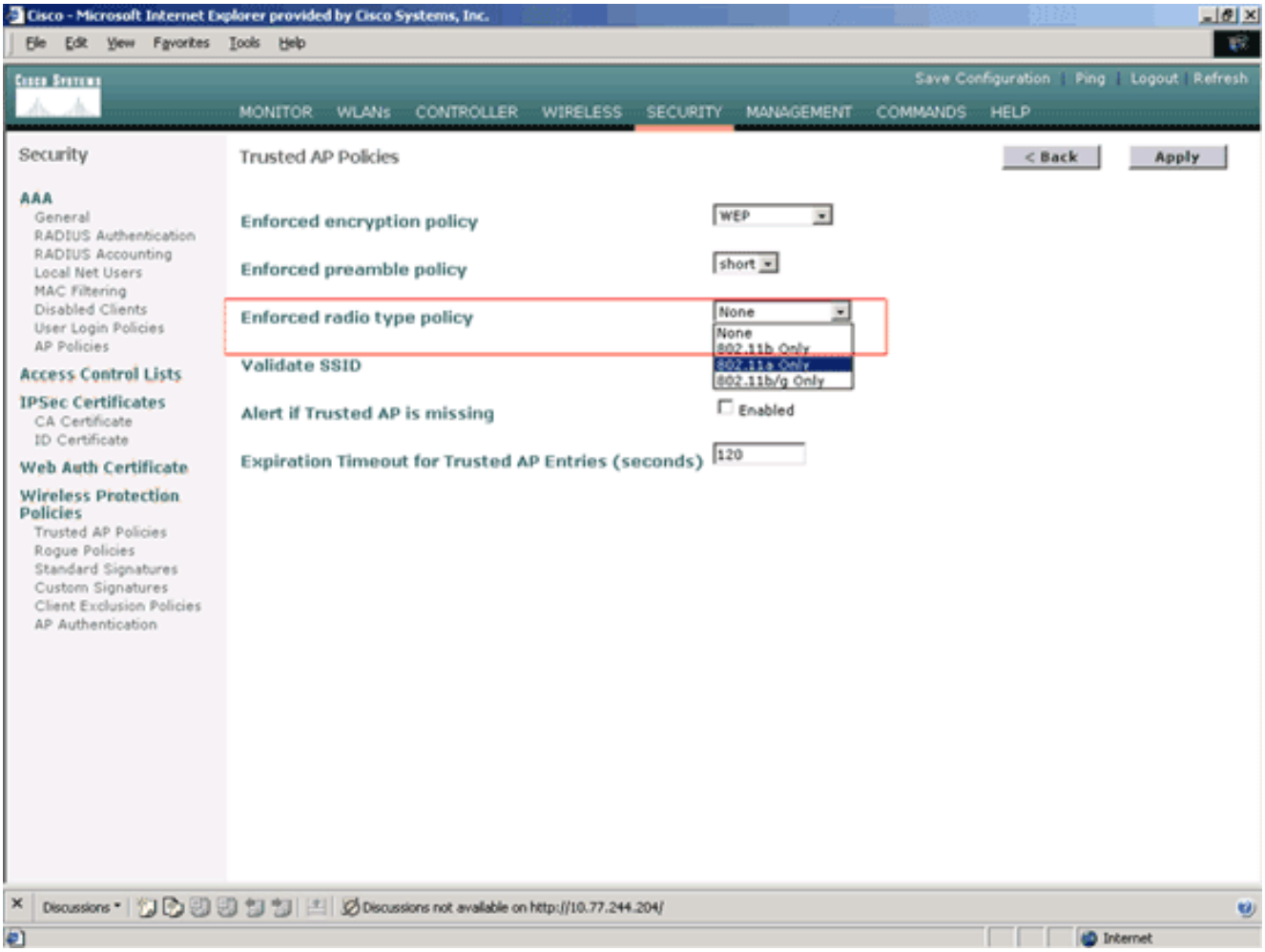
3. [Trusted AP policies]ページで、[Enforced encryption policy]ドロップダウンリストから目的の暗号化タイプ([None]、[Open]、[WEP]、[WPA/802.11i])を選択します。



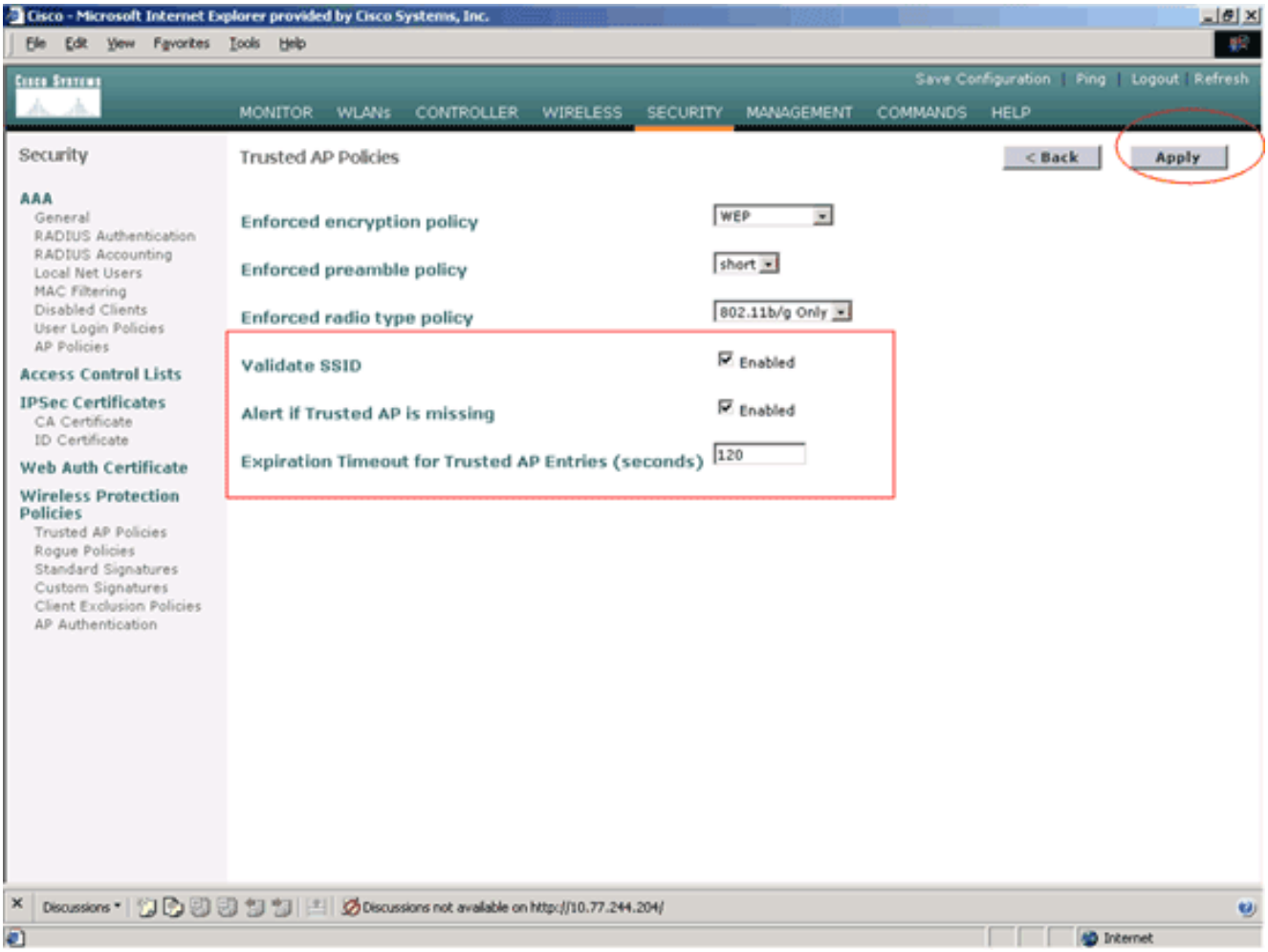
4. [Enforced preamble type policy]ドロップダウンリストから、目的のプリアンブルタイプ([None]、[Short]、[Long])を選択します。



5. [強制無線タイプポリシー(Enforced radio type policy)]ドロップダウンリストから、必要な無線タイプ([なし(None)]、[802.11bのみ（802.11aのみ）]、[802.11b/gのみ（802.11b/gのみ）])を選択します。



6. [Validate SSID Enabled]チェックボックスをオンまたはオフにして、Validate SSID設定を有効または無効にします。
7. [Alert if **trusted AP is missing Enabled]チェックボックスをオンまたはオフに**して、Trusted AP is missing設定を有効または無効にします。
8. [Expiration Timeout for **Trusted AP entries**]オプションに値（秒）を入力します。



9. [Apply] をクリックします。

注：WLC CLIからこれらの設定を行うには、適切なポリシーオプションを指定してconfig wps trusted-ap**コマンドを使用できます。**

```
Cisco Controller) >config wps trusted-ap ?

encryption      Configures the trusted AP encryption policy to be enforced.
missing-ap      Configures alert of missing trusted AP.
preamble        Configures the trusted AP preamble policy to be enforced.
radio           Configures the trusted AP radio policy to be enforced.
timeout         Configures the expiration time for trusted APs, in seconds.
```

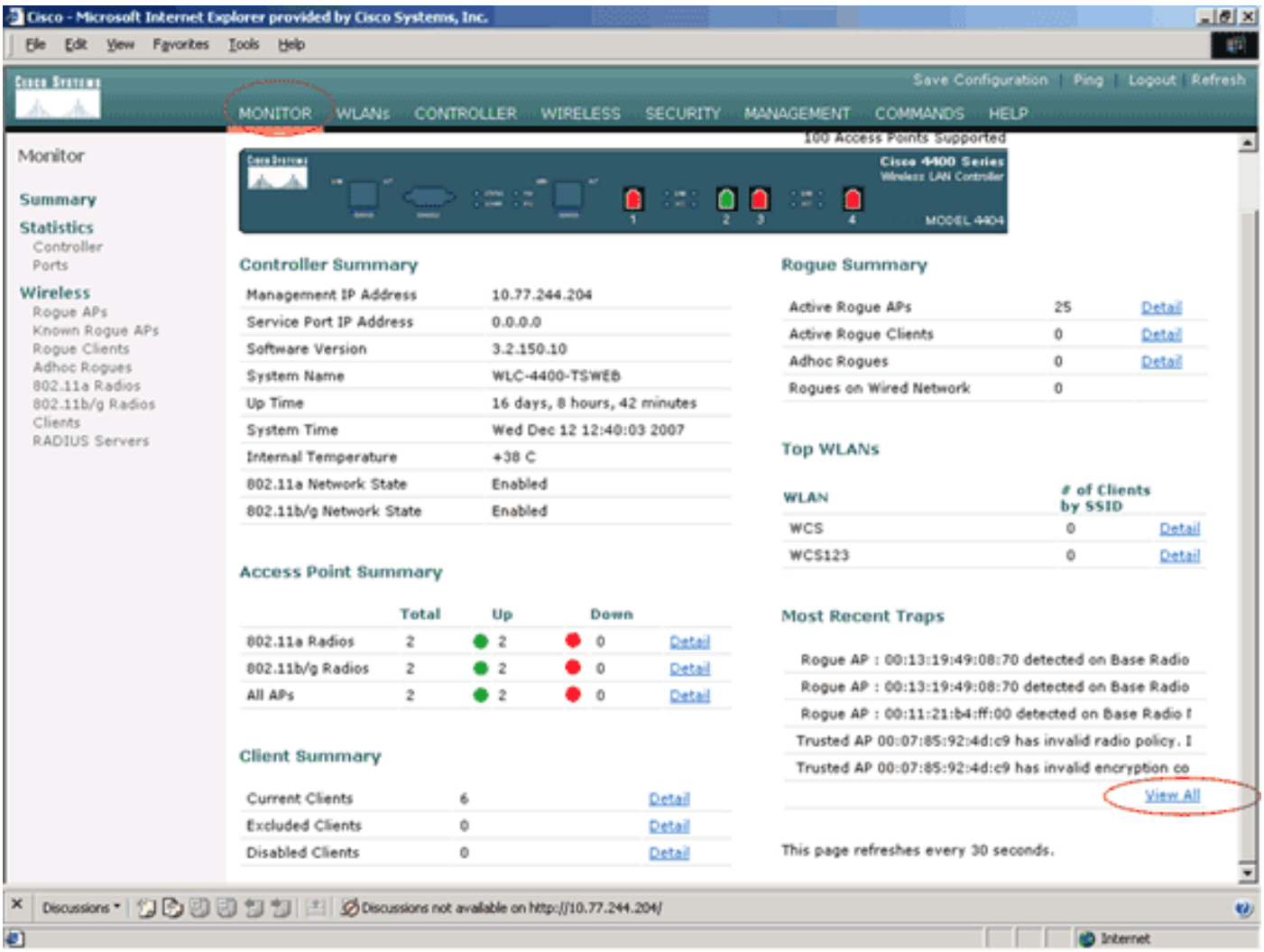
Trusted AP Policy Violationアラートメッセージ

コントローラによって表示される信頼できるAPポリシー違反アラートメッセージの例を次に示します。

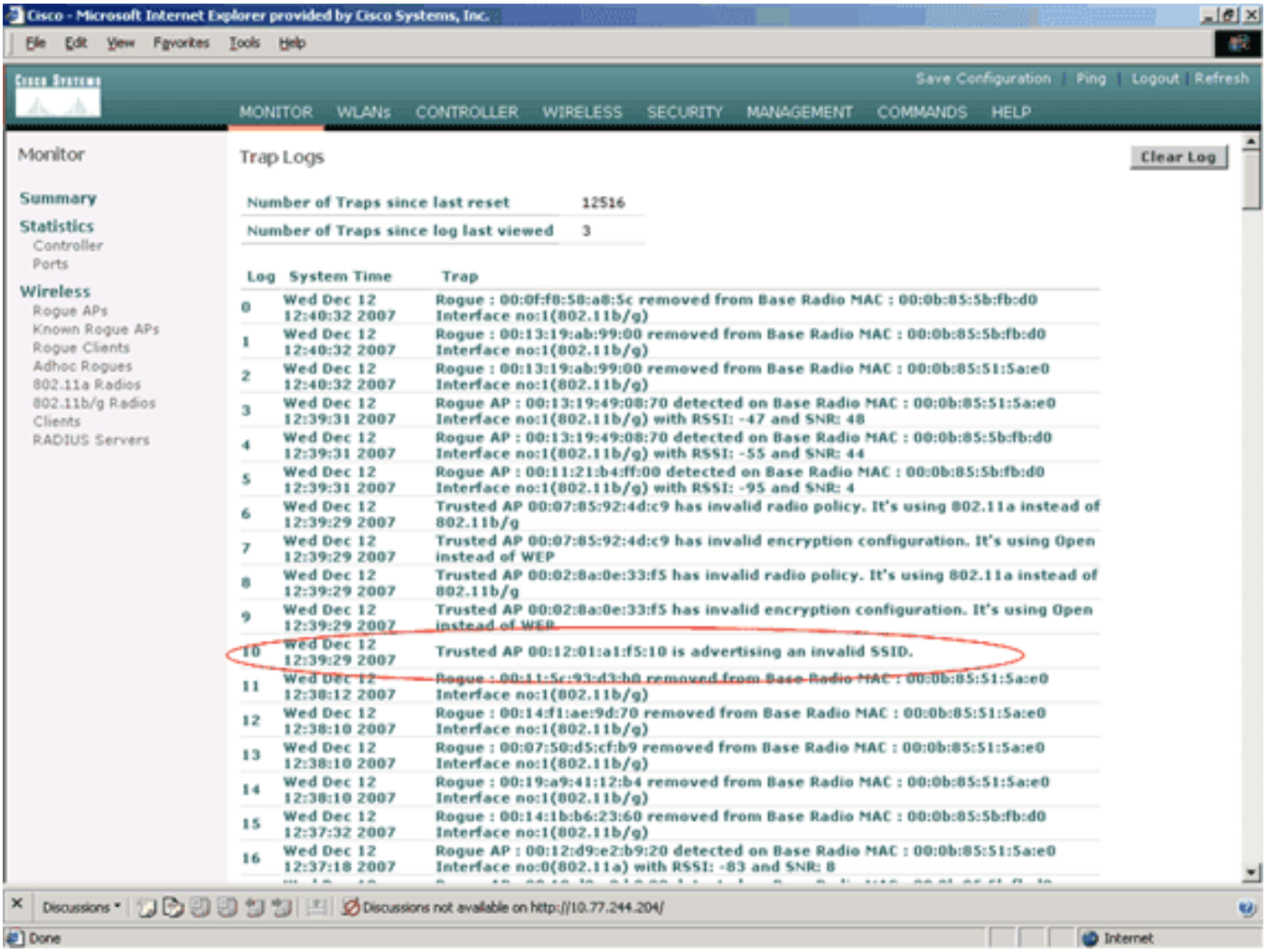
```
Thu Nov 16 12:39:12 2006  [WARNING] apf_rogue.c 1905: Possible AP
impersonation of xx:xx:xx:xx:xx:xx, using source address of
00:16:35:9e:6f:3a, detected by 00:17:df:7d:e1:70 on slot 0
 Thu Nov 16 12:39:12 2006  [SECURITY] apf_rogue.c 1490: Trusted AP Policy
failed for AP xx:xx:xx:xx:xx:xx - invalid SSID 'SSID1'
Thu Nov 16 12:39:12 2006  [SECURITY] apf_rogue.c 1457: Trusted AP Policy
failed for AP xx:xx:xx:xx:xx:xx - invalid encryption type
Thu Nov 16 12:39:12 2006  Previous message occurred 6 times
```

強調表示されたエラーメッセージに注目してください。これらのエラーメッセージは、信頼できるAPに設定されているSSIDと暗号化タイプが、信頼できるAPポリシー設定と一致しないことを示しています。

同じアラートメッセージがWLC GUIから表示されます。このメッセージを表示するには、WLCのGUIメインメニューに移動し、[**Monitor**]をクリックします。[Monitor]ページの[Most Recent Traps]セクションで、[**View All**]をクリックして、WLC上のすべての最近のアラートを表示します。



[Most Recent Traps]ページでは、次の図に示すように、信頼できるAPポリシー違反アラートメッセージを生成するコントローラを特定できます。



関連情報

- Cisco Wireless LAN Controllerコンフィギュレーションガイド、リリース5.2:RFグループでのルータアクセスポイントの検出の有効化
- Cisco Wireless LAN Controller コンフィギュレーション ガイド ソフトウェア リリース 4.0 - セキュリティ ソリューションの設定
- Unified Wireless Network における不正検出
- SpectraLink 電話器の設計および展開ガイド
- 基本的な無線 LAN 接続の設定例
- ワイヤレス LAN ネットワークにおける接続のトラブルシューティング
- ワイヤレス LAN コントローラでの認証の設定例
- テクニカル サポートとドキュメント – Cisco Systems