无线局域网控制器的可信AP策略

目录

简介

本文档介绍无*线LAN控*制器(WLC)上的受信任AP无线保护策略，定义受信任AP策略，并提供所有受信任AP策略的简要说明。

先决条件

要求

确保您基本了解无线LAN安全参数（如SSID、加密、身份验证等）。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

受信任AP策略

受信任AP策略是控制器中的一项安全功能，旨在用于客户拥有并行自治AP网络和控制器的场景。在该场景中，自治AP可以标记为控制器上的受信任AP，用户可以为这些受信任AP定义策略（应仅使用WEP或WPA、我们自己的SSID、短前导码等）。 如果这些AP中的任何一个未能满足这些策略，控制器会向网络管理设备（无线控制系统）发出警报，该设备声明受信任AP违反了配置的策略。

什么是受信任AP?

受信任AP是不属于组织的AP。但是，它们不会对网络造成安全威胁。这些AP也称为友好AP。在几种情况下，您可能希望将AP配置为受信任AP。

例如，您的网络中可能有不同类别的AP，例如：

- **您拥有的不运行LWAPP的AP（可能它们运行IOS或VxWorks）**
- 员工引入的LWAPP AP（在管理员知情的情况下）
- 用于测试现有网络的LWAPP AP
- 邻居拥有的LWAPP AP

通常，受信任AP是属于1类的AP，**即您**拥有的不运行LWAPP的AP。它们可能是运行VxWorks或IOS的旧AP。为了确保这些AP不会损坏网络，可以实施某些功能，例如正确的SSID和身份验证类型。在WLC上配置受信任AP策略，并确保受信任AP满足这些策略。否则，您可以配置控制器以执行多项操作，例如向网络管理设备(WCS)发出警报。

属于邻居的已知AP可以配置为受信任AP。

通常，MFP（管理帧保护）应防止非合法LWAPP AP的AP加入WLC。如果NIC卡支持MFP，则不允许它们接受来自除实际AP之外的设备的解身份验证。有关MFP的详细信息，请参阅使用WLC和LAP的基础设施管理帧保护(MFP)配置示例。

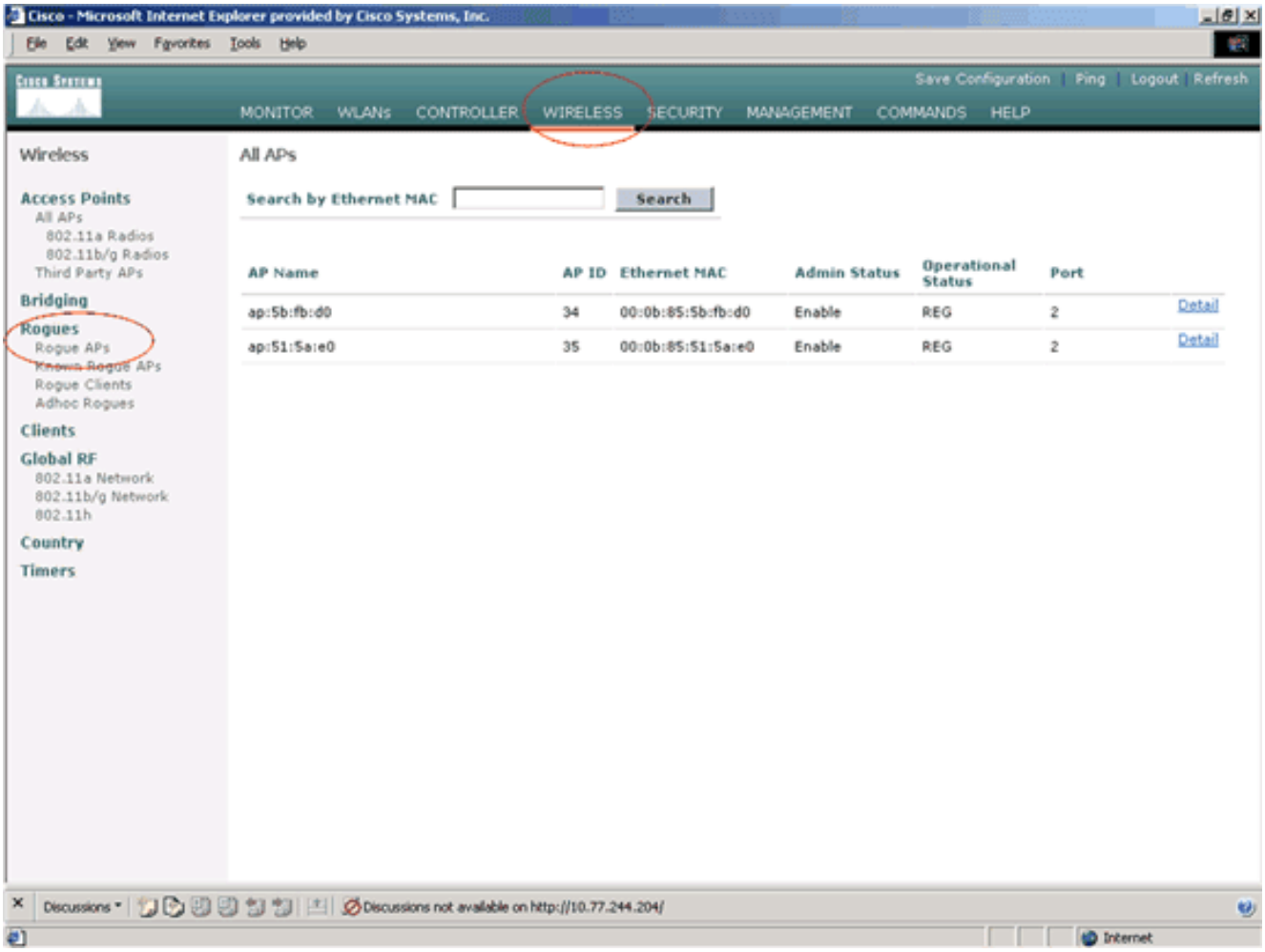
如果您有运行VxWorks或IOS的AP（如第1类），它们将永远不会加入LWAPP组或执行MFP，但您可能希望实施该页面上列出的策略。在这种情况下，需要在控制器上为感兴趣的AP配置受信任AP策略。

通常，如果您知道欺诈AP并确定它不是对网络的威胁，则可以将该AP标识为已知的受信任AP。

如何从WLC GUI将AP配置为受信任AP?

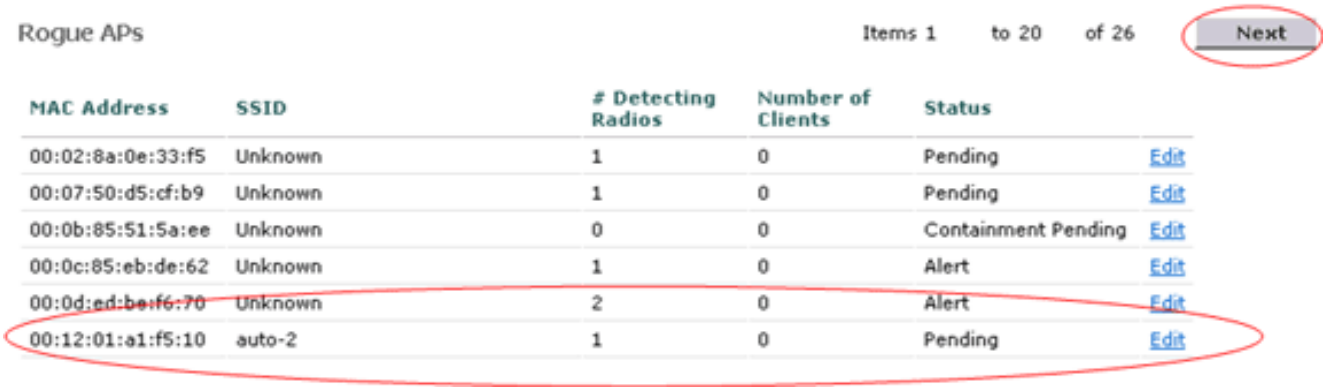
要将AP配置为受信任AP，请完成以下步骤：

1. 通过HTTP或https登录登录WLC的GUI。
2. 在控制器主菜单中，单击**Wireless**。
3. 在Wireless页面左侧的菜单中，单击**Rogue APs**。



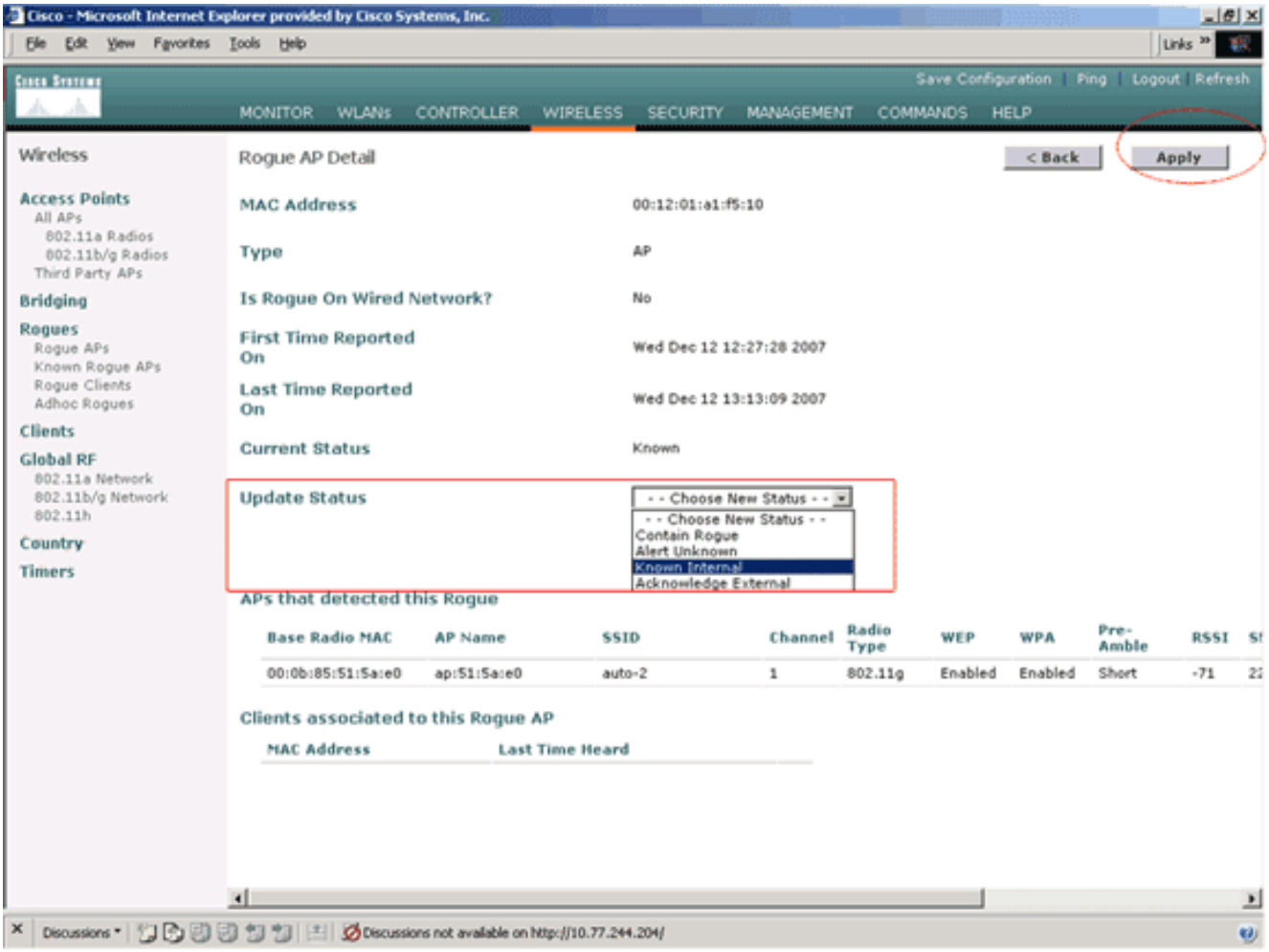
Rogue APs页面列出网络上检测为欺诈AP的所有AP。

4. 从此恶意AP列表中，找到要配置为属于1类（如上一节所述）的受信任AP的AP。您可以找到MAC地址列在Rogue APs页面上的AP。如果所需的AP不在此页中，请单击**Next**以从下一页识别AP。
5. 从Rogue AP列表找到所需的AP后，点击与AP对应的**Edit**按钮，该按钮将带您进入AP的详细信息页面。



在Rogue AP详细信息页面中，您可以找到有关此AP的详细信息（例如该AP是否连接到有线网络以及AP的当前状态等）。

6. 要将此AP配置为受信任AP，请从Update Status下拉列**表中选**择Known Internal，然后单击**Apply**。当您将AP状态更新为Known *Internal*时，此AP将配置为此网络的受信任AP。

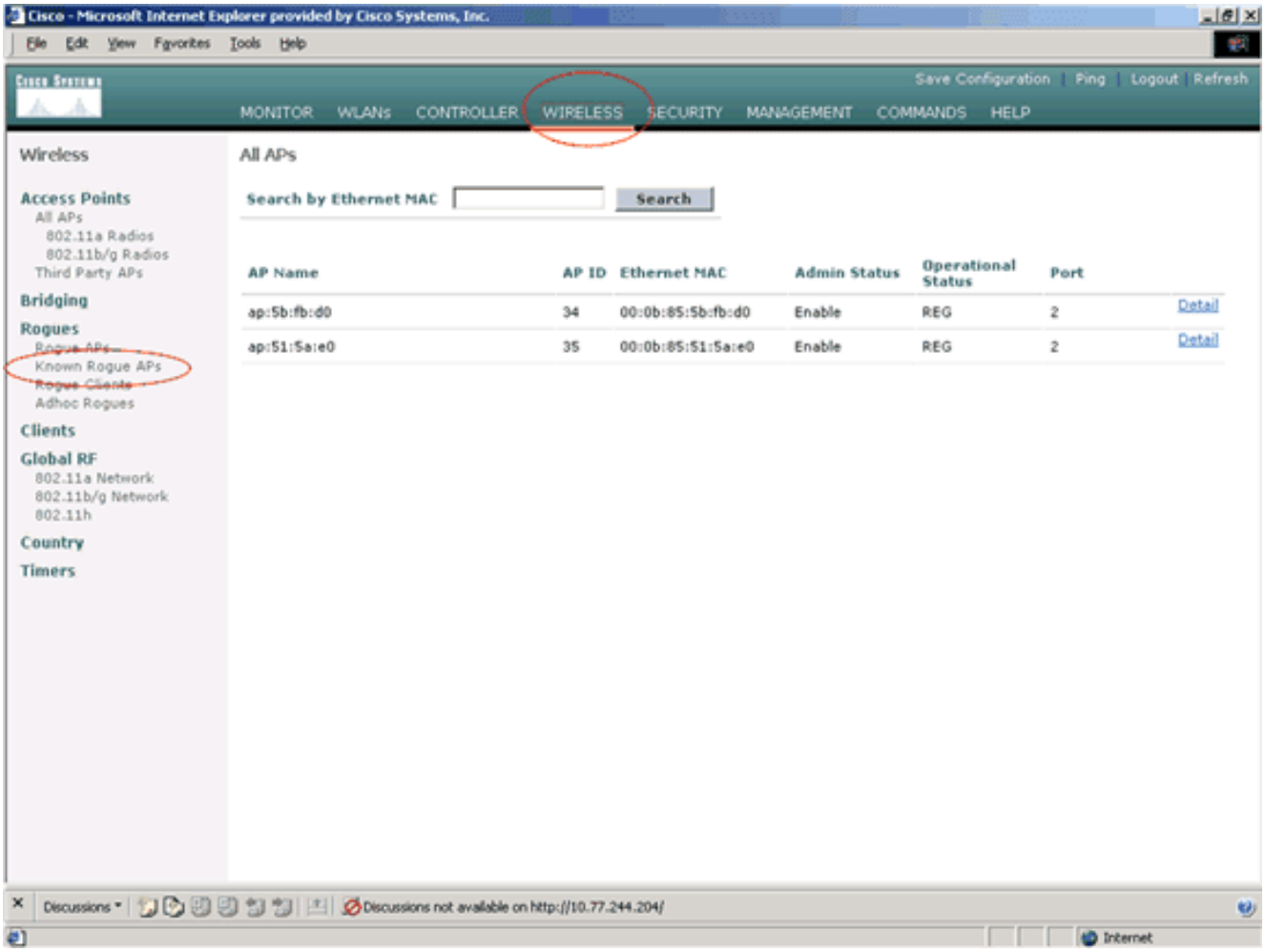


7. 对要配置为受信任AP的所有AP重复这些步骤。

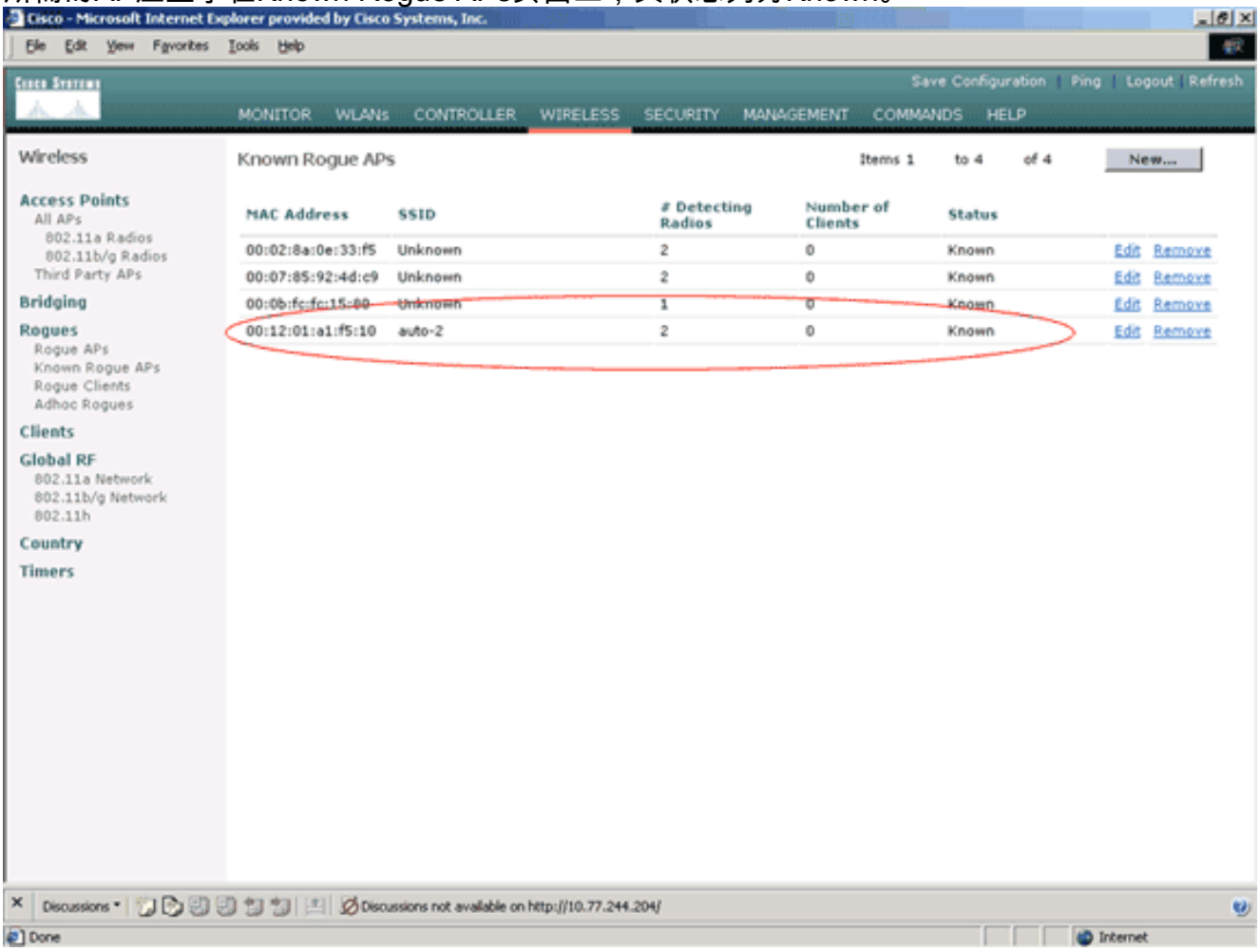
验证受信任AP配置

完成以下步骤，以验证AP是否已从控制器GUI正确配置为受信任AP:

1. 单击**Wireless**。
2. 在Wireless页面左侧的菜单中，单击**Known Rogue APs**。



所需的AP应显示在Known Rogue APs页面上，其状态列为*Known*。



了解受信任AP策略设置

WLC具有以下受信任AP策略：

- 强制加密策略
- 强制前导码策略
- 强制无线电类型策略
- 验证SSID
- 如果受信任AP丢失，则发出警报
- 受信任AP条目的过期超时（秒）

强制加密策略

此策略用于定义受信任AP应使用的加密类型。您可以在“强制加密”策略下配置以下任何加密类型：

- 无
- Open（未解决）
- WEP
- WPA/802.11i

WLC验证在受信任AP上配置的加密类型是否与在“强制加密策略”设置上**配置的加**密类型匹配。如果受信任AP未使用指定的加密类型，WLC会向管理系统发出警报，以便采取适当的操作。

强制前导码策略

无线电前导码（有时称为报头）是数据包头部的数据部分，包含无线设备发送和接收数据包时需要的信息。**短报**头可提高吞吐量性能，因此默认情况下启用它们。但是，某些无线设备（如SpectraLink NetLink电话）需要长**的前**导码。您可以在Enforced preamble策略下配置以下任何前导码选项：

- 无
- 短
- 长

WLC验证在受信任AP上配置的前导码类型是否与在“强制前导码策略”设置上**配置的前导**码类型匹配。如果受信任AP未使用指定的前导码类型，WLC会向管理系统发出警报以采取适当的操作。

强制无线电类型策略

此策略用于定义受信任AP应使用的无线电类型。您可以在Enforced radio type policy（强制无线电类型策略）下配置以下任何无线电类型：

- 无
- 仅802.11b
- 仅802.11a
- 仅802.11b/g

WLC验证在受信任AP上配置的无线电类型是否与在“Enforced radio type policy”设置上配置的无线电类型匹配。如果受信任AP不使用指定的无线电，WLC会向管理系统发出警报，以便采取适当的操作。

验证SSID

您可以配置控制器，以根据控制器上配置的SSID验证受信任AP SSID。如果受信任AP SSID与其中一个控制器SSID匹配，则控制器会发出警报。

如果受信任AP丢失，则发出警报

如果启用此策略，则如果已知欺诈AP列表中缺少受信任AP，WLC会向管理系统发出警报。

受信任AP条目的过期超时（秒）

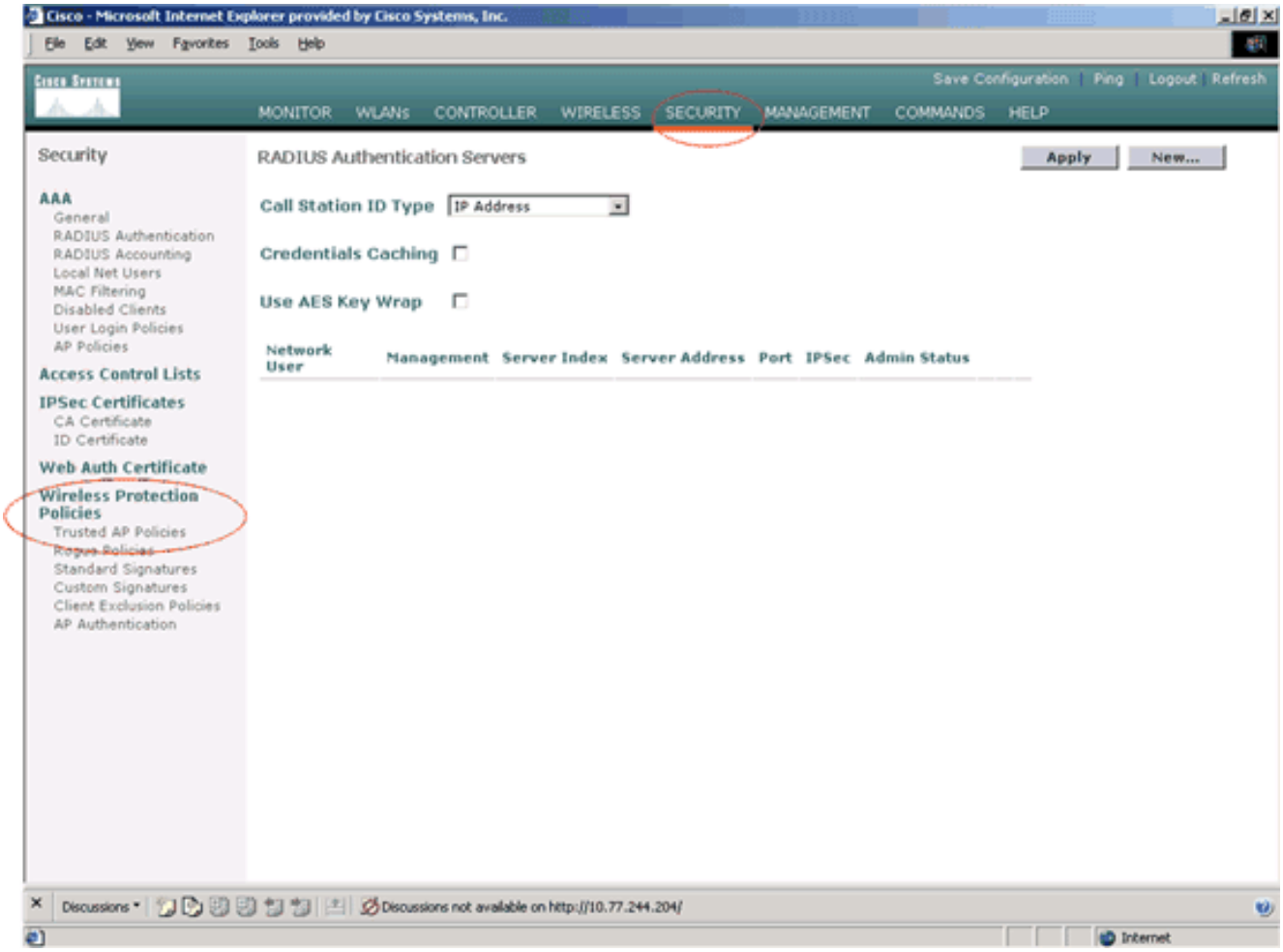
此Expiration Timeout值指定在受信任AP被视为已过期并从WLC条目刷新之前的秒数。可以以秒（120 - 3600秒）指定此超时值。

如何在WLC上配置受信任AP策略？

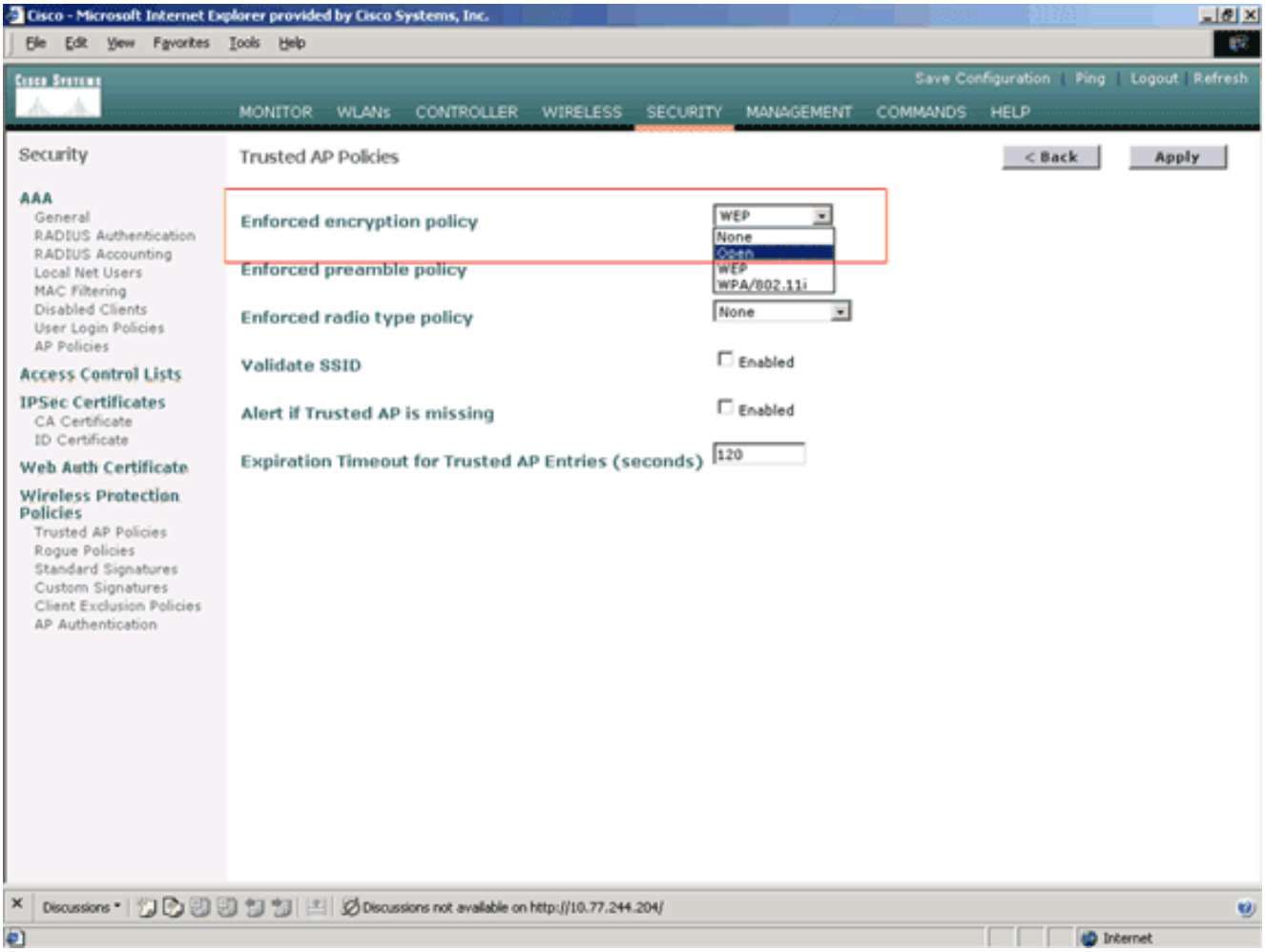
要通过GUI在WLC上配置受信任AP策略，请完成以下步骤：

注意：所有受信任AP策略都位于同一WLC页上。

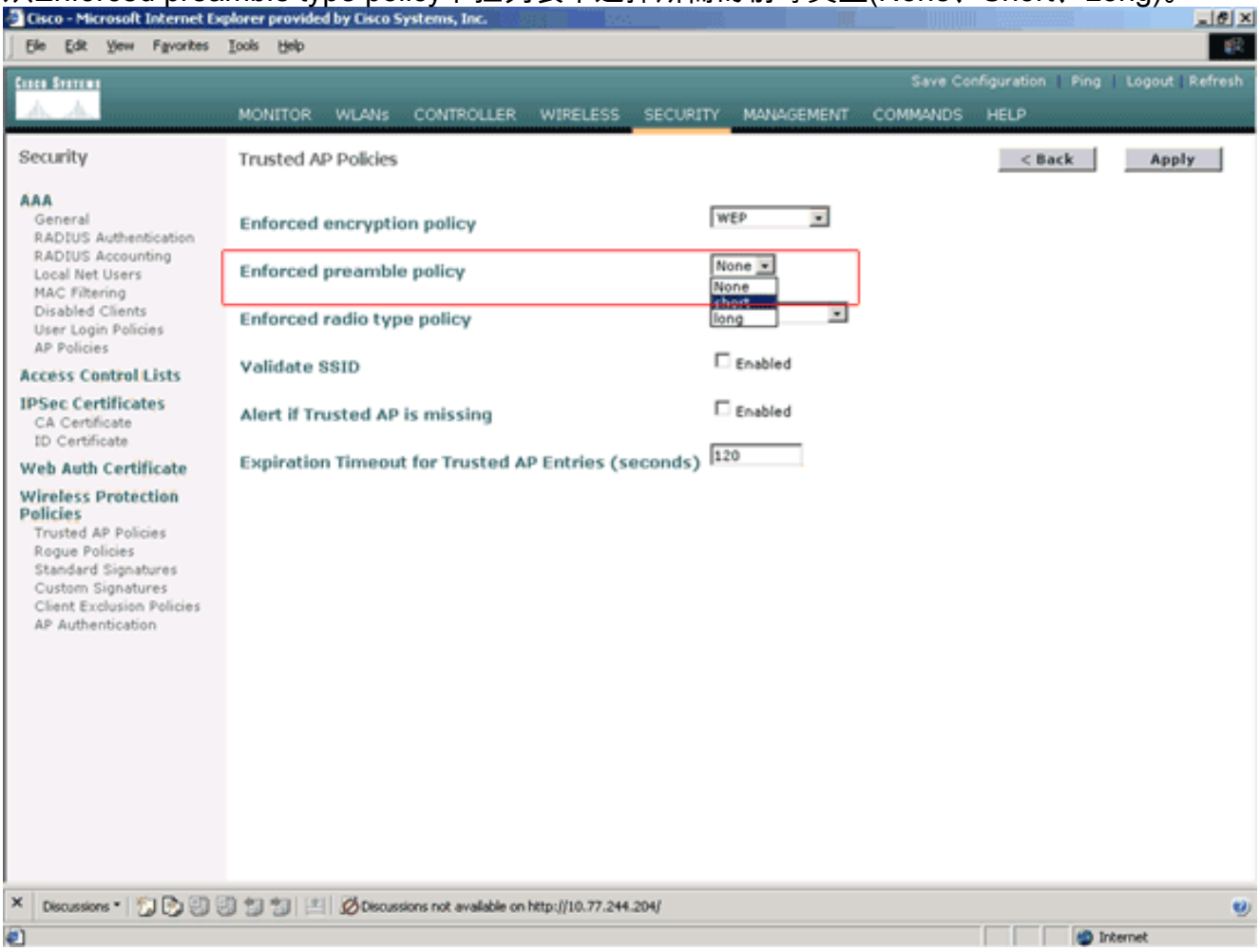
1. 从WLC GUI主菜单中，单击**Security**。
2. 从Security页面左侧的菜单中，单击Wireless Protection Policies标题下列**出的Trusted AP** Policies。



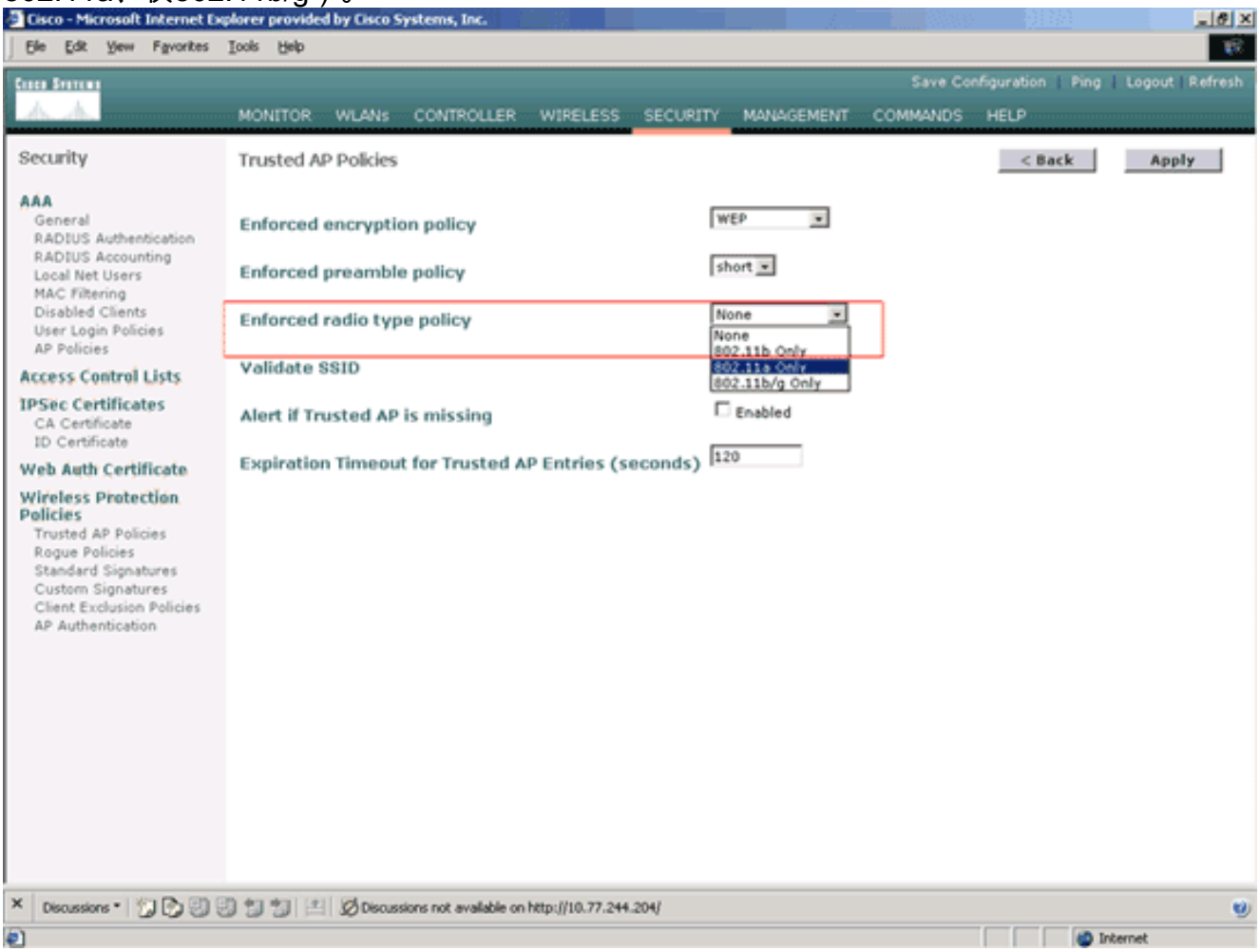
3. 在“受信任AP策略”(Trusted AP policies)页面上，从“强制加密策略”(Enforced encryption policy)下拉列表中选择所需的加密类型（无、打开、WEP、WPA/802.11i）。



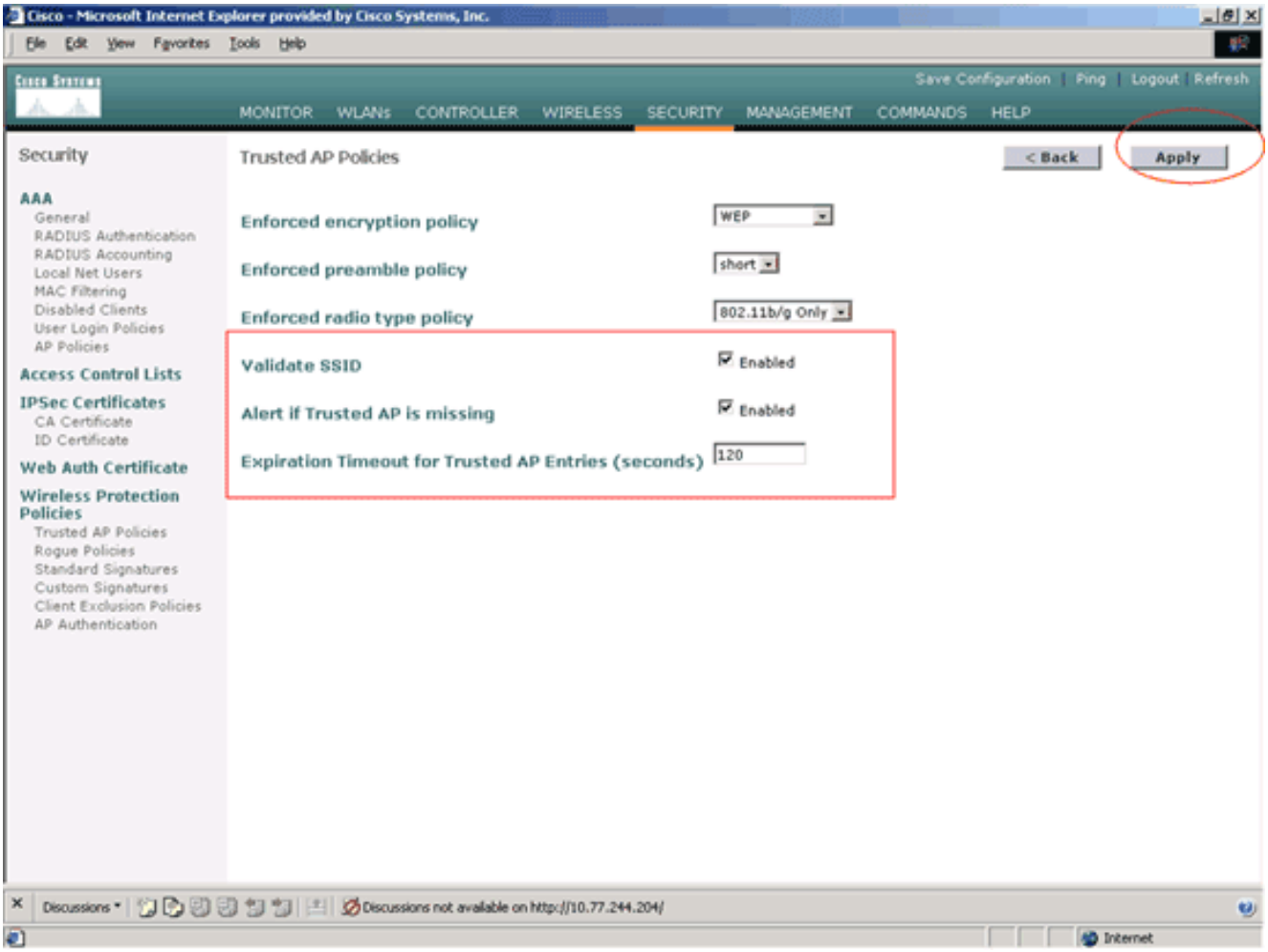
4. 从Enforced preamble type policy下拉列表中选择所需的前导类型(None、Short、Long)。



5. 从Enforced radio type policy下拉列表中选择所需的无线电类型（None、仅802.11b、仅802.11a、仅802.11b/g）。



6. 选中或取消选中**Validate SSID Enabled复选**框，以启用或禁用Validate SSID设置。
7. 选中或取消选中**Alert if trusted AP is missing Enabled复选框，以**启用或禁用Alert if trusted AP is missing设置。
8. 输入值（以秒为单位），以**Expiration Timeout for Trusted AP entries选**项。



9. 单击 Apply。

注意：要从WLC CLI配置这些设置，可以使用配置wps trusted-ap**命令和**适当的策略选项。

```
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.
```

受信任AP策略违规警报消息

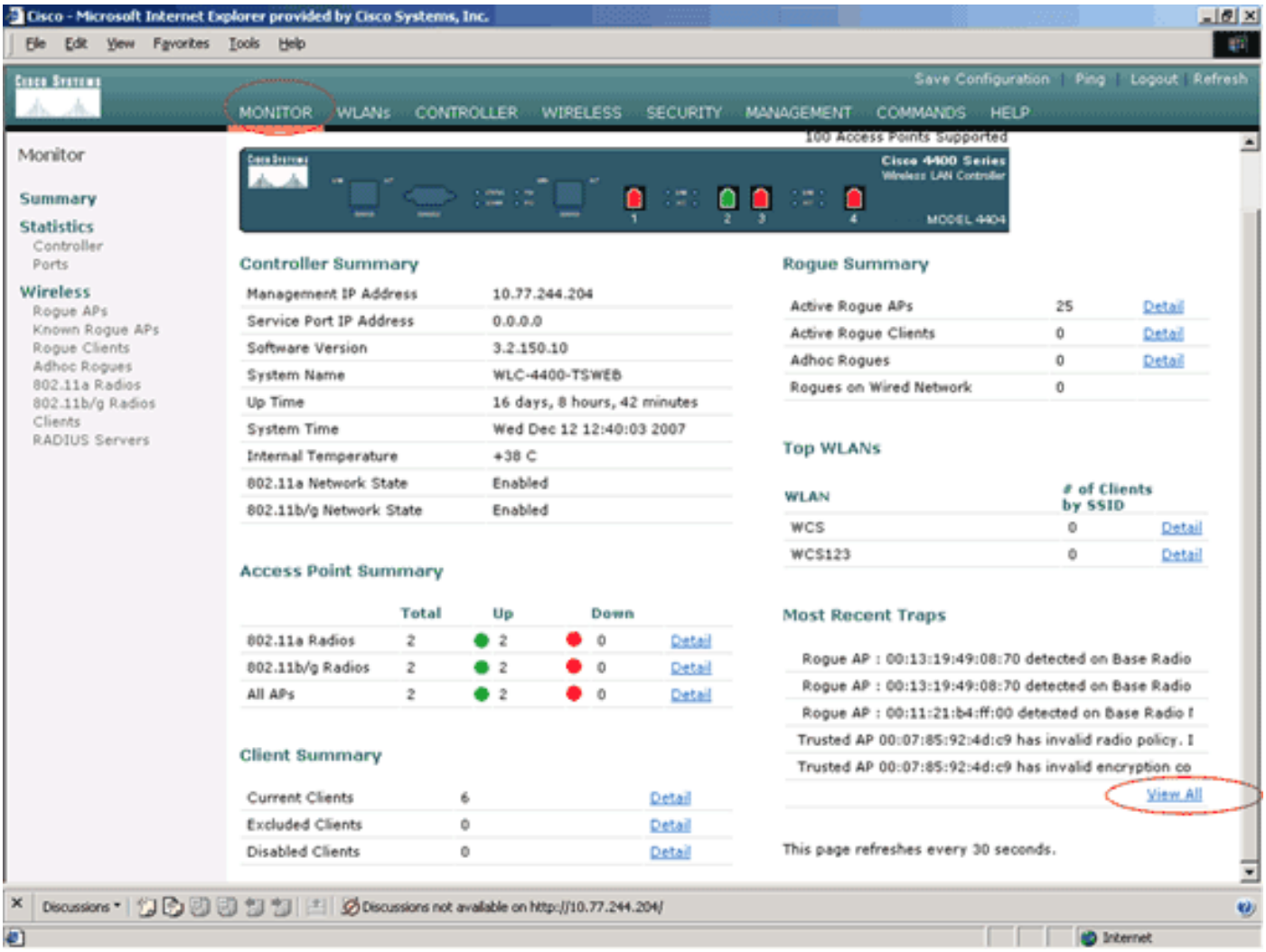
以下是控制器显示的受信任AP策略违规警报消息示例。

```
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
```

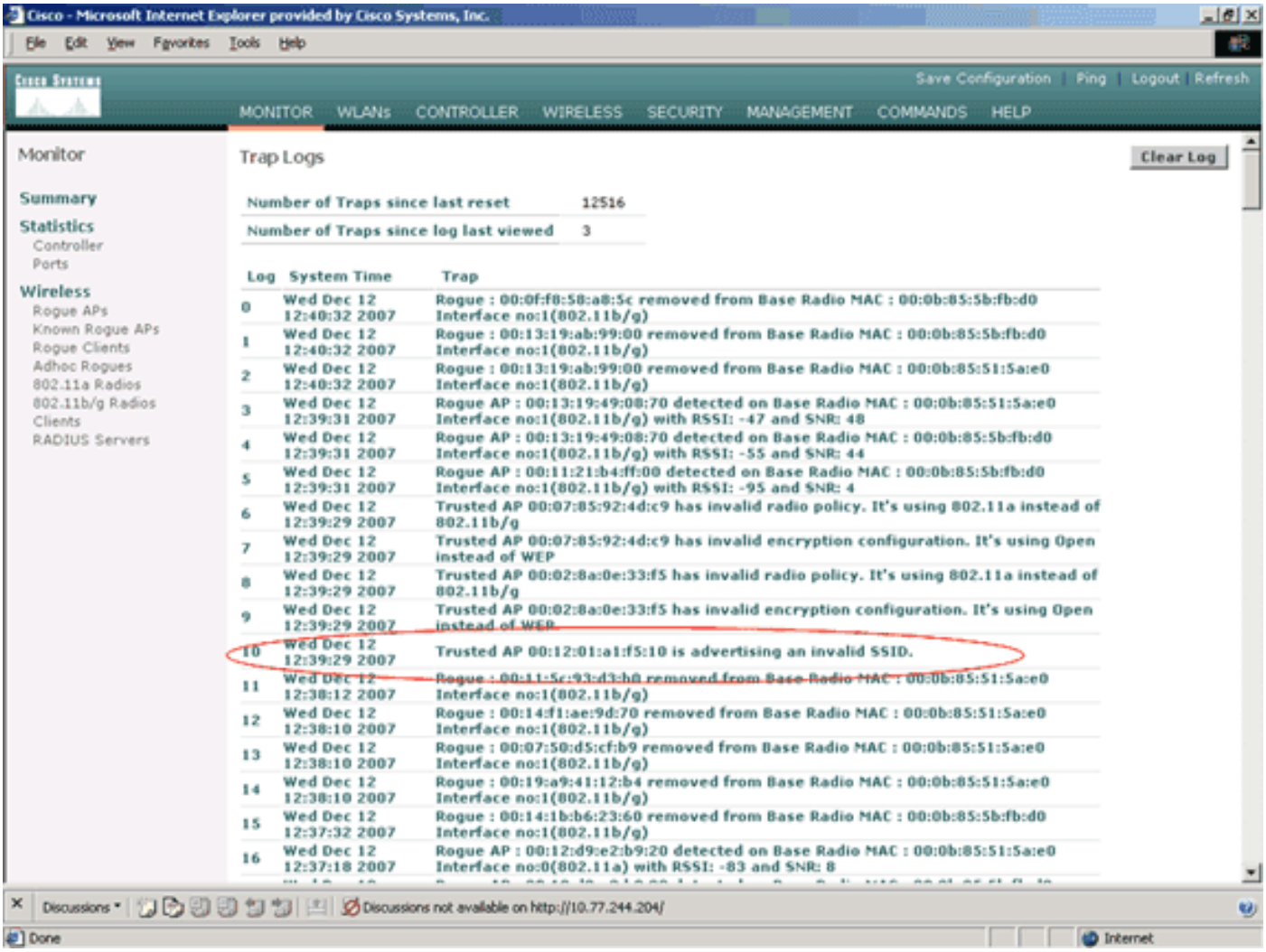
注意此处突出显示的错误消息。这些错误消息表明受信任AP上配置的SSID和加密类型与受信任AP策略设置不匹配。

从WLC GUI中可以看到相同的警报消息。要查看此消息，请转到WLC GUI主菜单，然后单击 **Monitor**。在“监控”(Monitor)页面的“最近陷阱”(Most Recent Traps)部分，单击“**查看全部**”(View

All)以查看WLC上所有最近的警报。



在Most Recent Traps页面上，可以识别生成受信任AP策略违规警报消息的控制器，如下图所示：



相关信息

- 思科无线局域网控制器配置指南，版本5.2 — 在RF组中启用欺诈接入点检测
- 思科无线局域网控制器配置指南，版本4.0 — 配置安全解决方案
- 统一无线网络的恶意检测
- SpectraLink电话设计和部署指南
- 基本的无线局域网连接配置示例
- 无线 LAN 网络中的连通性故障排除
- 无线局域网控制器认证的配置示例
- 技术支持和文档 - Cisco Systems