无线局域网控制器的可信AP策略

目录

简介

本文描述在无线局域网控制器(WLC)的*委托AP*无线保护策略，定义了委托AP策略，并且提供所有委托AP策略简要描述。

先决条件

要求

保证您有无线LAN安全参数基本的了解(例如SSID、加密，验证，等等)。

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

委托AP策略

委托AP策略是在方案设计使用客户有并行自治AP网络与控制器一起的控制器的一个安全功能。在该方案中，自治AP可以被标记作为在控制器的委托AP，并且用户能定义这些的策略委托应该使用WEP或WPA的AP (、仅我们自己的SSID，短的前导，等等)。如果满足这些策略的这些AP失败中的任一，控制器发出报警到该的网络管理设备(无线控制系统)状态委托AP违犯了一项已配置的策略。

什么是委托AP ？

委托AP是不作为组织的部分的AP。然而，他们不导致对网络的一个安全威胁。这些AP也呼叫友好AP。几个方案存在您也许要配置AP作为委托AP的地方。

例如，您也许有AP不同的类别在您的网络的例如：

- **或许您拥有不运行LWAPP的AP (他们运行IOS或VxWorks)**
- 员工带来的LWAPP AP (与管理员的知识)
- AP用于的LWAPP测试现有的网络
- 该的LWAPP AP邻居拥有

通常，委托AP是归入**类别1**，是AP您拥有不运行LWAPP的AP。他们也许是旧有AP运行VxWorks或IOS。为了保证这些AP不损坏网络，某些功能可以被强制执行，例如正确Ssid和验证类型。配置在WLC的委托AP策略，并且确保委托AP满足这些策略。否则，您能配置控制器采取数次行动，例如发出报警到网络管理设备(WCS)。

已知AP属于的邻居可以配置作为委托AP。

通常， MFP (管理帧保护)应该防止不是从加入WLC的合法LWAPP AP的AP。如果NIC卡支持MFP，除实时AP之外，他们没有允许接受从设备的解除验证。参考的基础设施管理帧保护(MFP)与关于MFP的更多信息WLC和LAP配置示例。

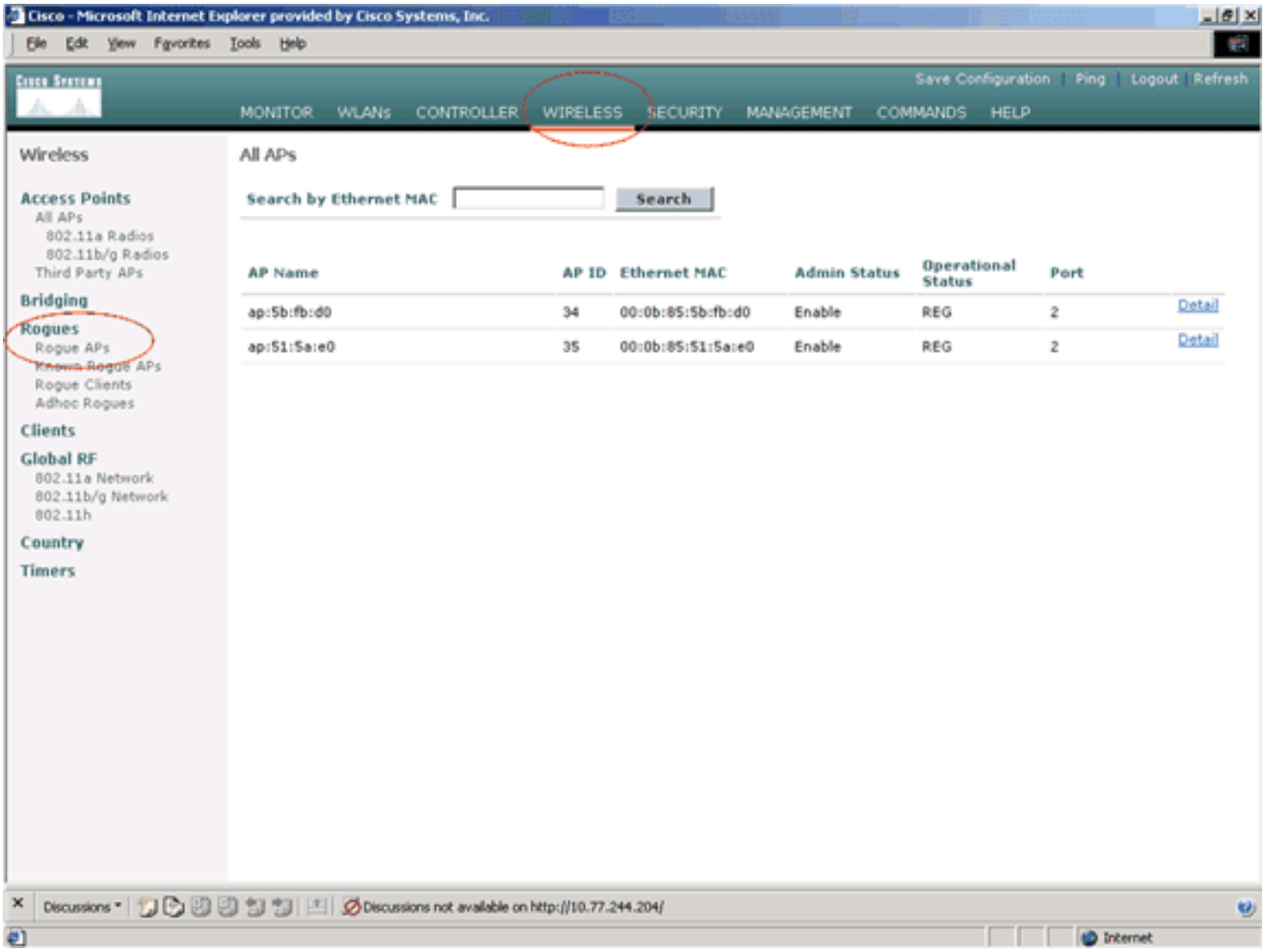
如果有AP运行VxWorks或IOS (正如在类别1)，他们不会加入LWAPP组或执行MFP，但是您也许要强制执行在该页列出的策略。在这类情况下，委托AP策略在AP的控制器需要配置利益。

一般来说，如果知道关于非法AP并且识别它不是对您的网络的一个威胁，您能识别该AP作为已知委托AP。

如何配置AP作为从WLC GUI的委托AP ？

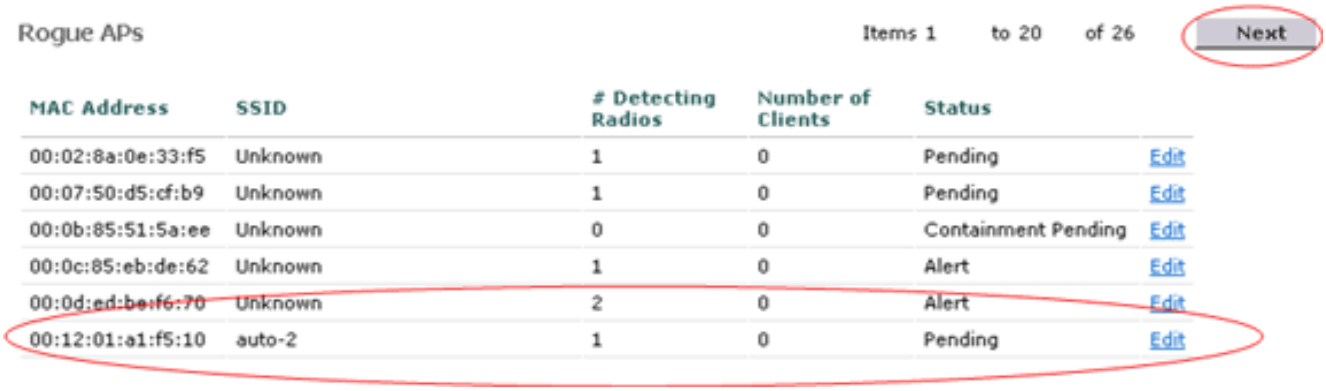
完成这些步骤为了配置AP作为委托AP ：

1. 通过HTTP或https登录WLC的GUI登陆。
2. 从控制器主菜单，请点击**无线**。
3. 在theWireless页的左边查找的菜单，请点击**恶意AP**。



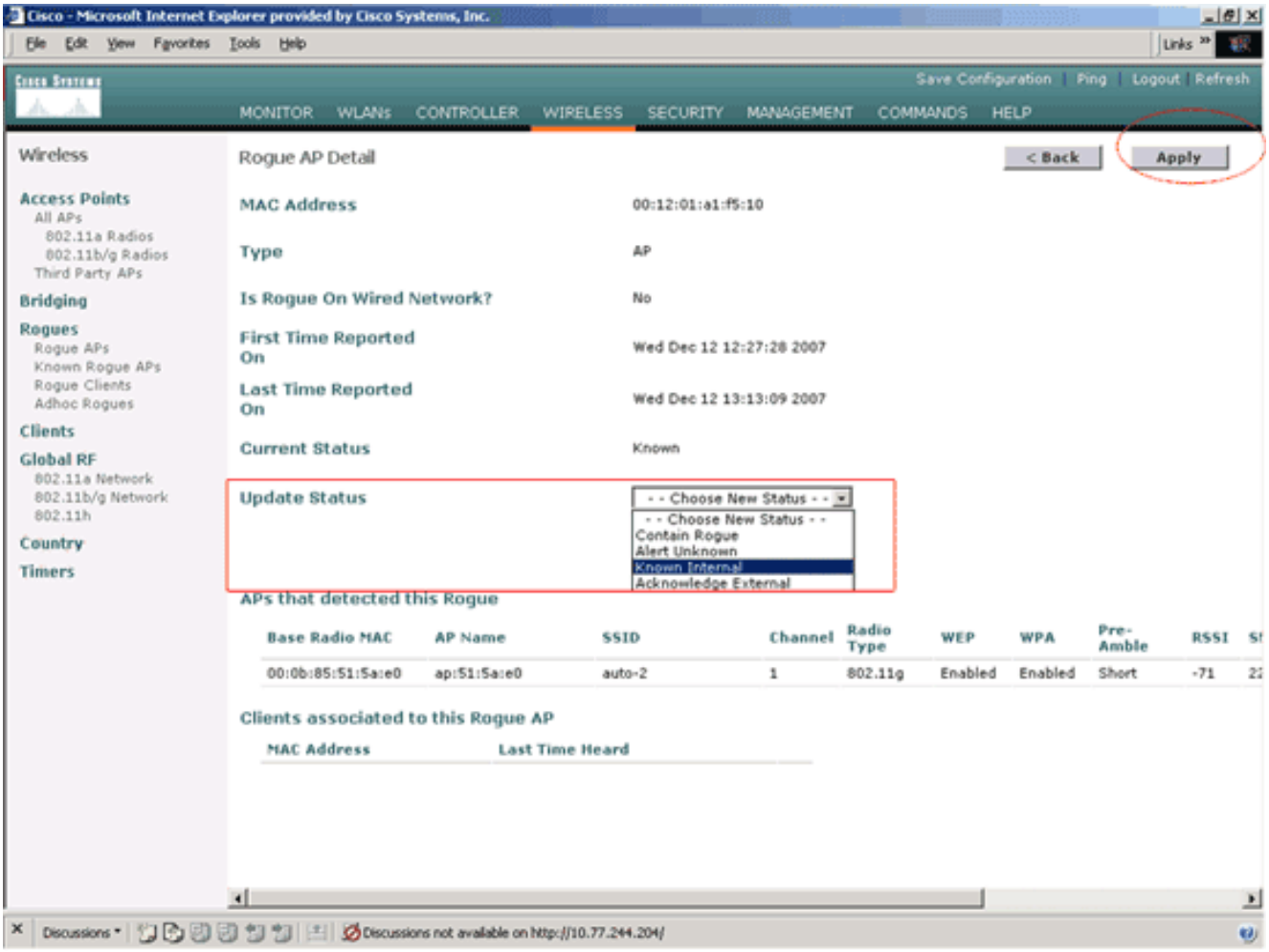
恶意AP页列出检测作为在网络的恶意AP的所有AP。

4. 从恶意AP此列表，请找出您想要配置作为委托AP属于类别1的AP (按照前面部分说明)。您能找出与在恶意AP页列出的MAC地址的AP。如果希望的AP不在此页，**其次请**单击为了识别从Next页的AP。
5. 一旦希望的AP从对应于AP，把您带对AP的详细信息页的非法AP列表查找，请点击**编辑按钮**。



在Details页的非法AP，您能找到关于此AP的详细信息(例如是否该AP连接对有线网络，以及AP的当前状态等)。

6. 为了配置此AP作为委托AP，选择**已知内部**从更新状态下拉列表，和单击**应用**。当您更新AP状态对*已知内部时*，此AP配置作为此网络委托AP。

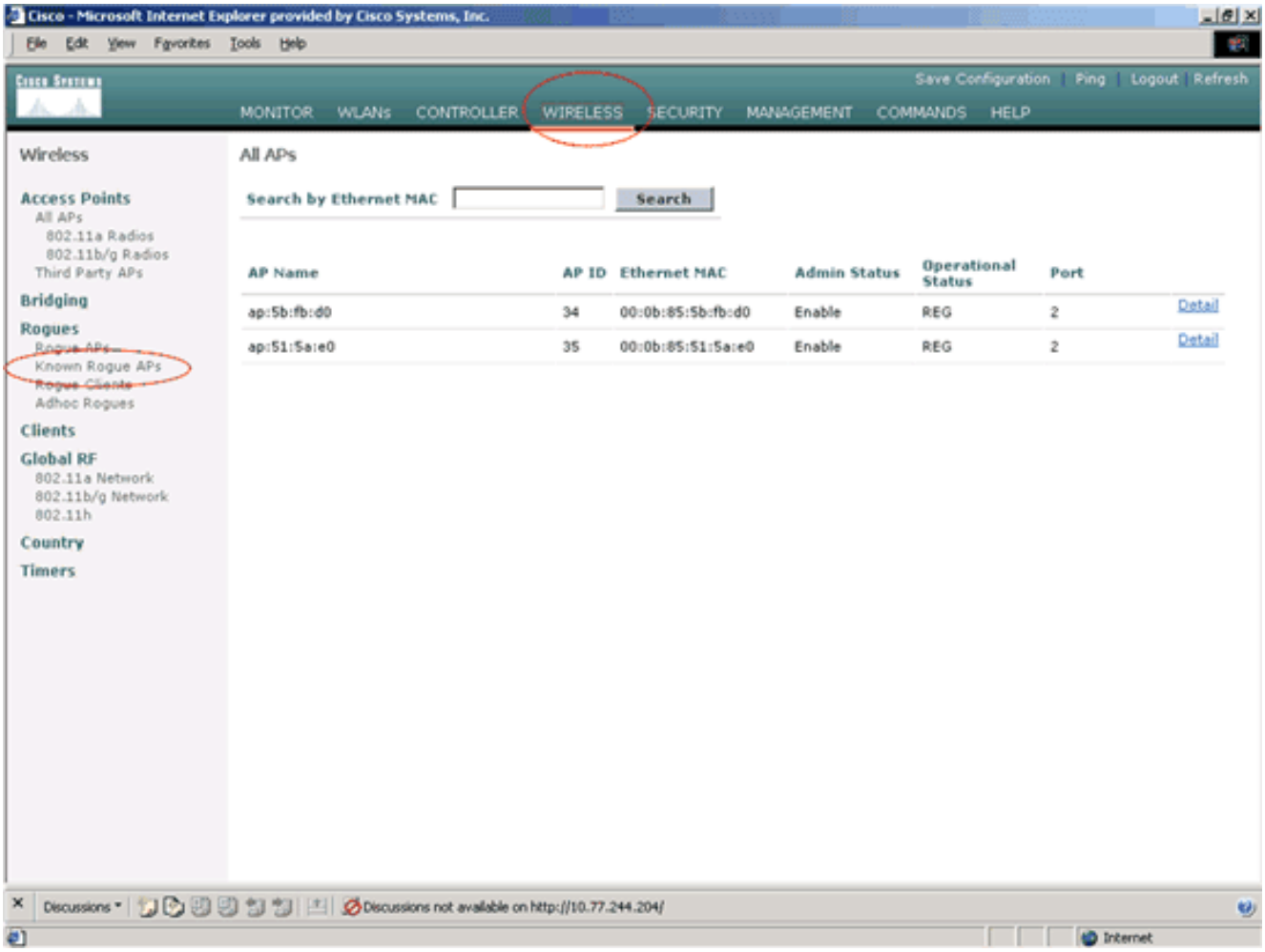


7. 重复您要配置作为委托AP的所有AP的这些步骤。

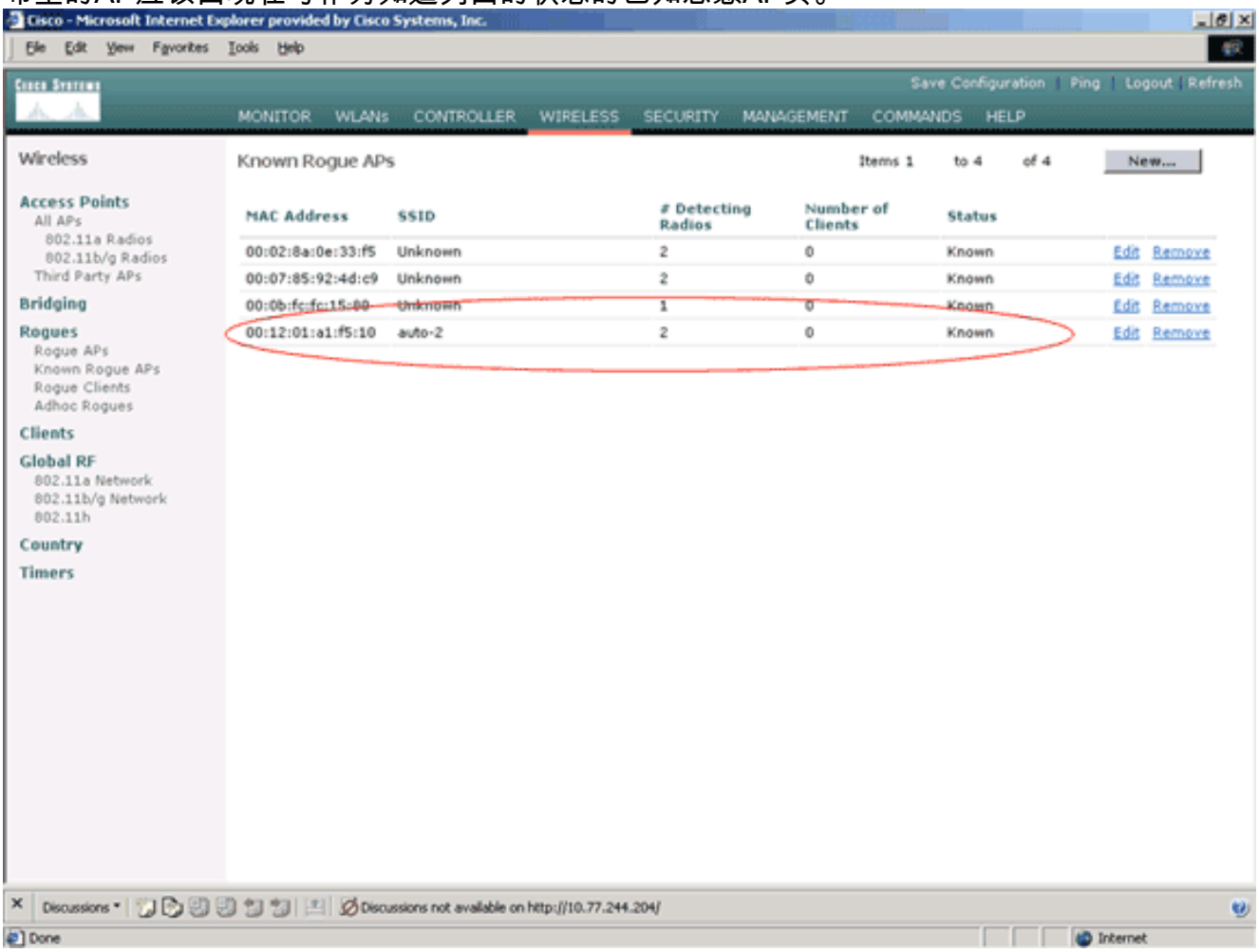
验证委托AP配置

完成这些步骤为了验证AP正确地配置作为从控制器GUI的委托AP ：

1. 点击**无线**。
2. 在theWireless页的左边查找的菜单，请点击**已知恶意AP**。



希望的AP应该出现在与作为*知道*列出的状态的已知恶意AP页。



了解委托AP策略设置

WLC有这些委托AP策略：

- 被强制执行的加密策略
- 被强制执行的前导策略
- 被强制执行的无线电类型策略
- 验证SSID
- 警报，如果委托AP缺失
- 委托AP条目的(秒钟)有效期超时

被强制执行的加密策略

此策略用于定义委托AP应该使用的加密类型。您能根据被强制执行的加密策略配置这些加密类型中的任一种：

- 无
- 打开
- WEP
- WPA/802.11i

WLC验证在委托AP配置的加密类型是否匹配在“**被强制执行的加密策略**”设置配置的加密类型。如果委托AP不使用指定加密类型， WLC发出报警到管理系统为了采取适当行为。

被强制执行的前导策略

无线电前导(有时呼叫报头)是数据的部分在包含信息无线设备需要数据包的题头，当他们发送并且收到数据包时。**短的**前导改进吞吐量性能，默认情况下，因此他们启用。然而，一些无线设备，例如SpectraLink NetLink电话，要求**长**前导。您能根据被强制执行的前导策略配置这些前导选项中的任一个：

- 无
- 肖特
- 龙牌

WLC验证在委托AP配置的前导类型是否匹配在“**被强制执行的前导策略**”设置配置的前导类型。如果委托AP不使用指定的前导类型， WLC发出报警到管理系统为了采取适当行为。

被强制执行的无线电类型策略

此策略用于定义委托AP应该使用的无线电类型。您能根据被强制执行的无线电类型策略配置这些无线电类型中的任一个：

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

WLC验证在委托AP配置的无线电类型是否匹配在“**被强制执行的无线电类型策略**”设置配置的无线电类型。如果不是委托APdoes使用指定的无线电， WLC发出报警到管理系统为了采取适当行为。

验证SSID

您能配置控制器验证委托AP SSID在控制器配置的Ssid。如果委托AP SSID匹配其中一控制器Ssid，控制器发出报警。

警报，如果委托AP缺失

如果此策略启用， WLC警告管理系统，如果委托AP从已知恶意AP列表未命中。

委托AP条目的(秒钟)有效期超时

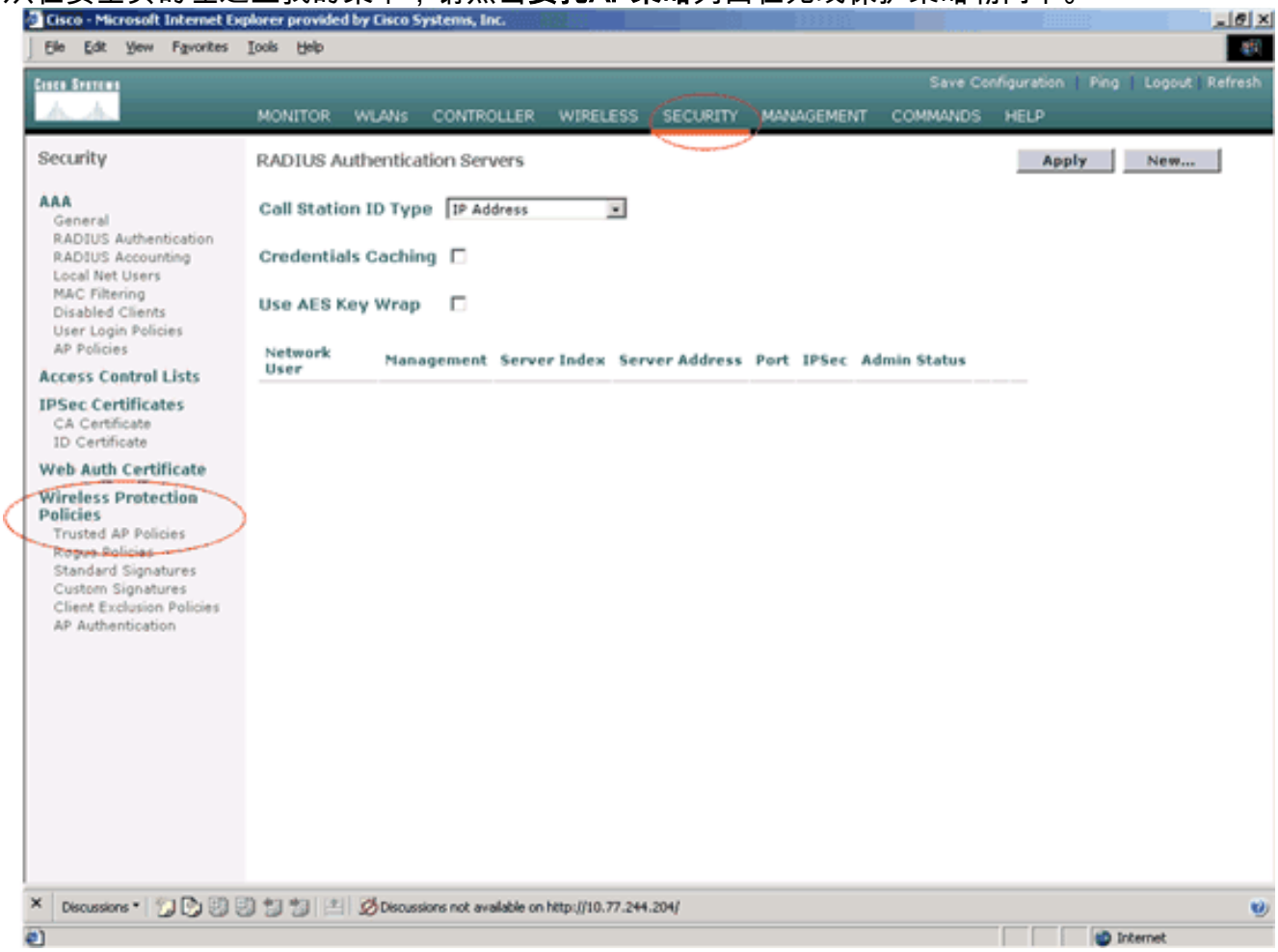
在委托AP被认为超时和被冲洗从WLC条目前，此有效期超时值指定秒钟数量。您能指定此超时值以秒钟(120 - 3600秒)。

如何配置委托在WLC的AP策略？

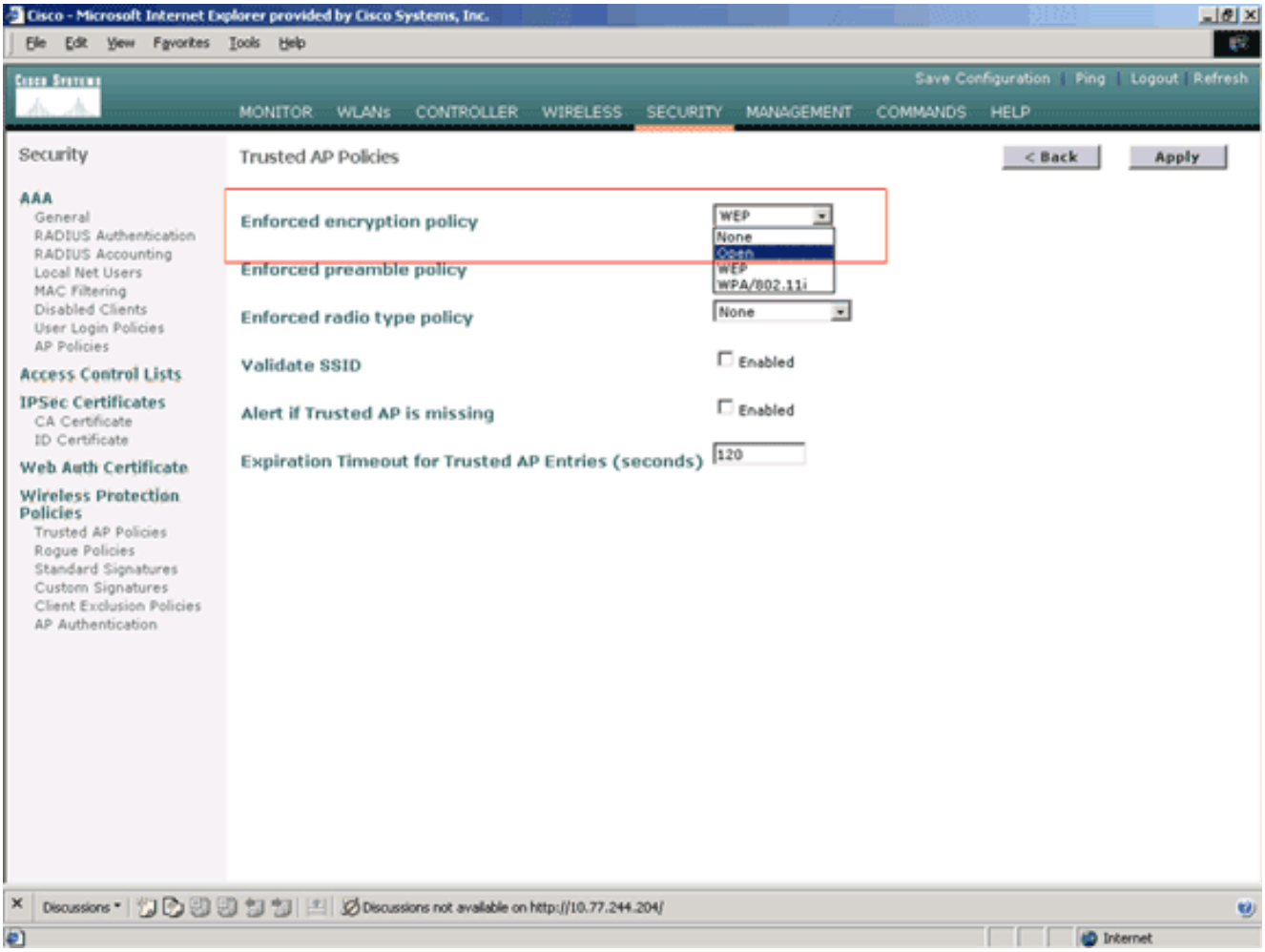
完成这些步骤为了通过GUI配置委托在WLC的AP策略：

注意： 所有委托AP策略在同一个WLC页驻留。

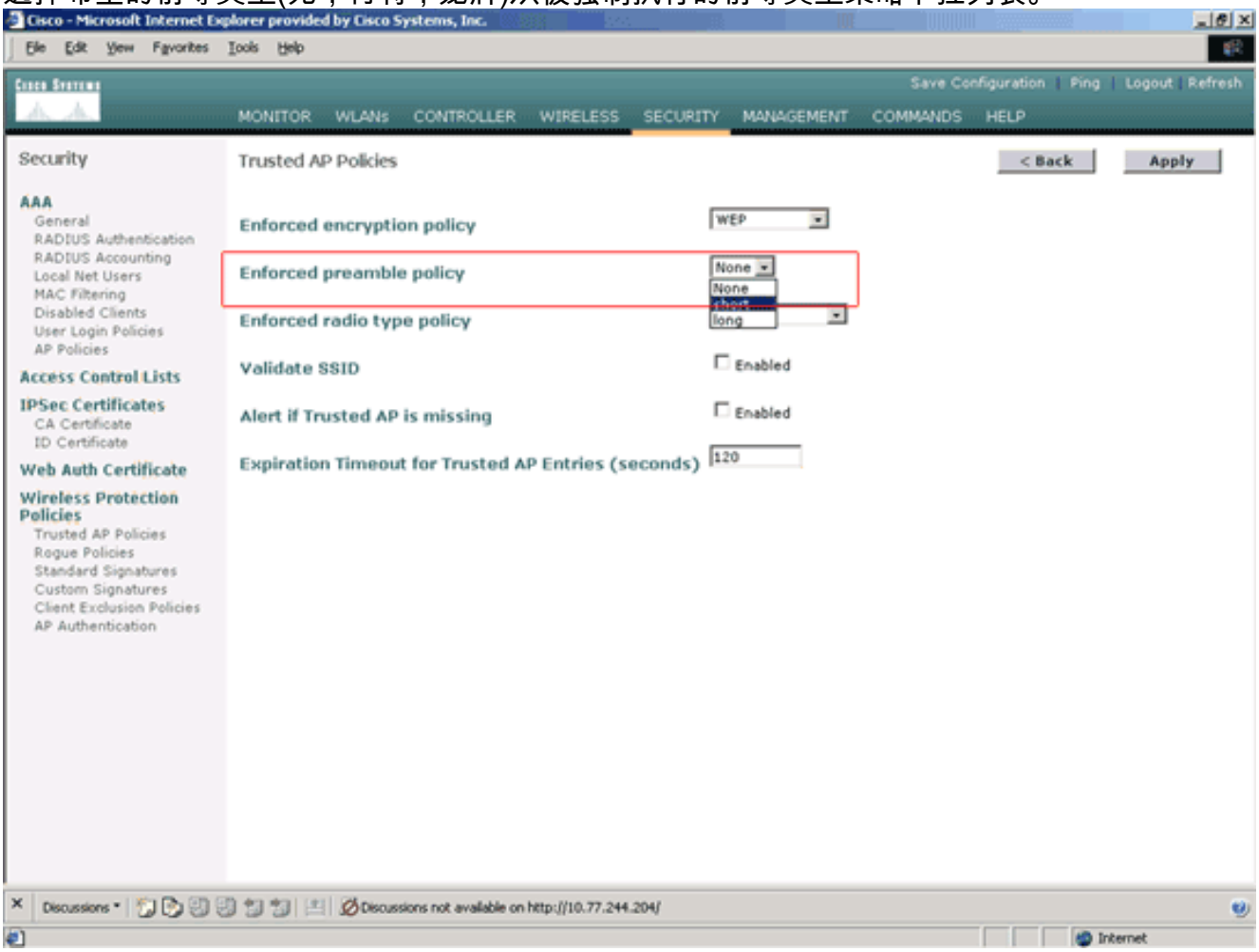
1. 从WLC GUI主菜单，请点击**安全**。
2. 从在安全页的左边查找的菜单，请点击**委托AP策略**列出在无线保护策略朝向下。



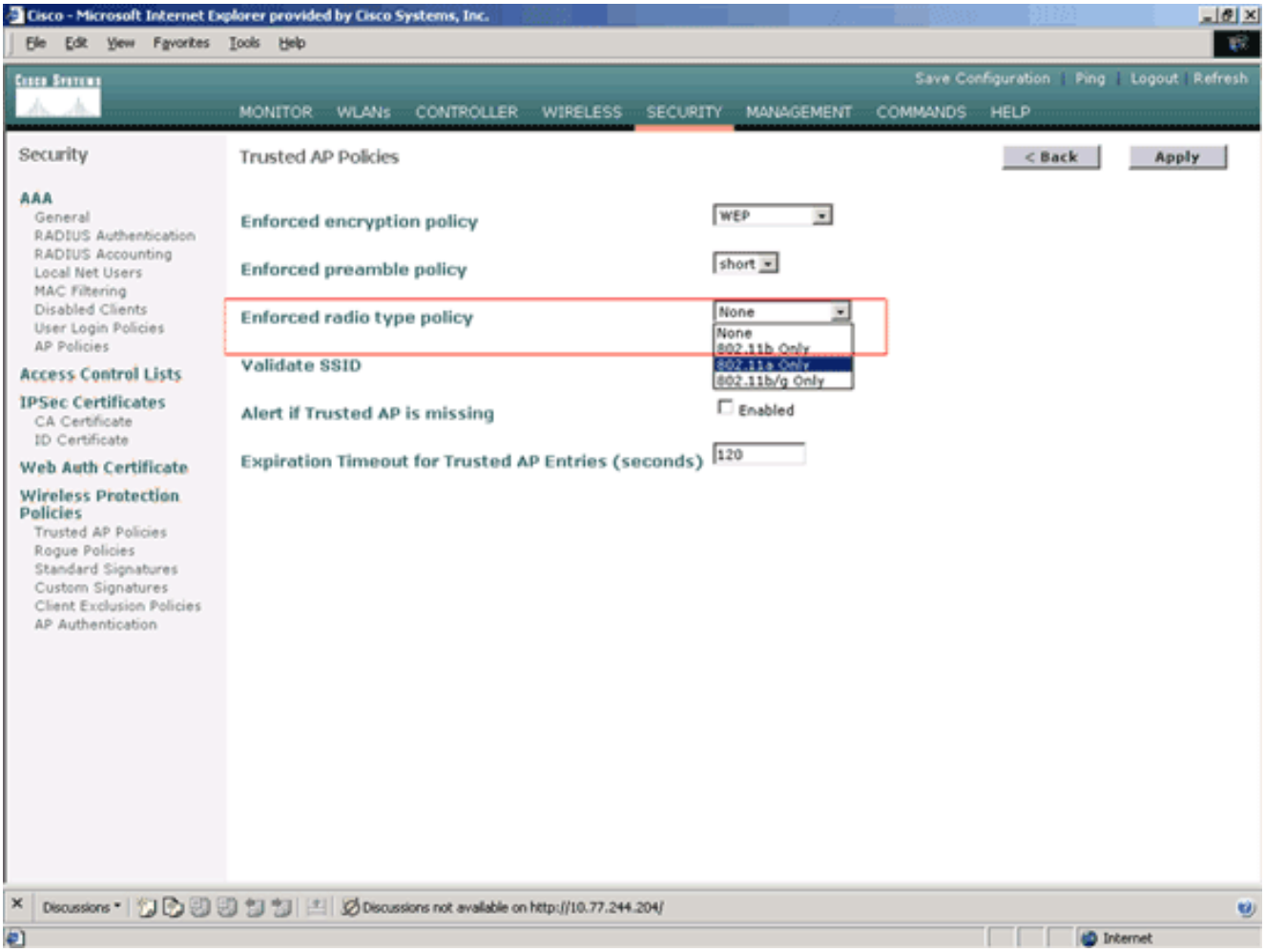
3. 在Policies页委托的AP，请选择希望的加密类型(什么都，不打开， WEP， WPA/802.11i)从被强制执行的加密策略下拉列表。



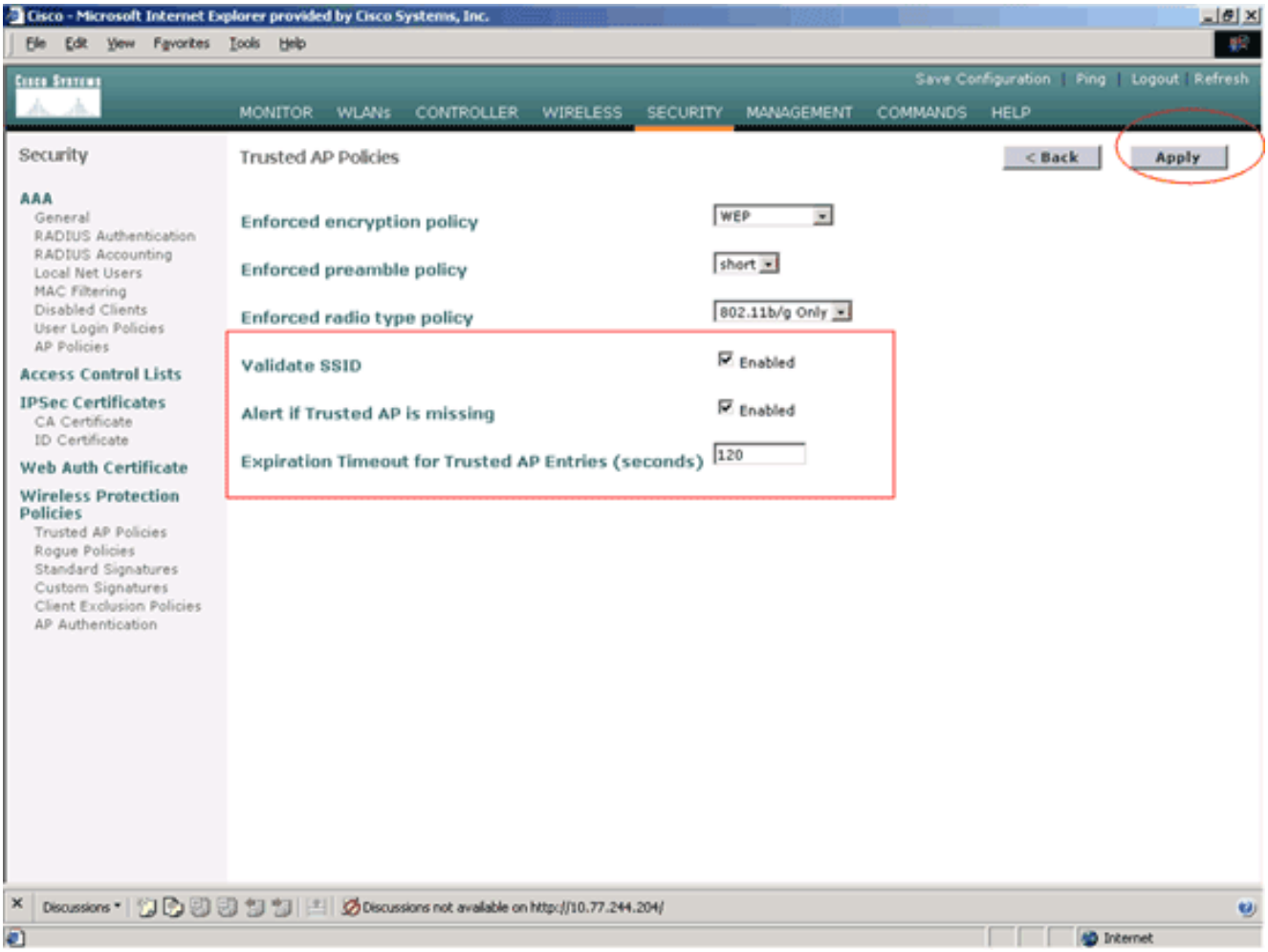
4. 选择希望的前导类型(无，肖特，龙牌)从被强制执行的前导类型策略下拉列表。



5. 选择希望的无线电类型(无，仅802.11b，仅仅802.11a， 802.11b/g)从被强制执行的无线电类型策略下拉列表。



6. 检查或不选定**验证SSID Enabled复选框**为了启用或禁用验证SSID设置。
7. 请检查或不选定**警报，如果委托AP是缺少Enabled复选框**为了启用或禁用警报，如果委托AP是缺少设置。
8. 输入一个值(以秒钟)**委托AP条目**选项的**有效期超时的**。



9. 单击 Apply。

注意： 为了配置从WLC CLI的这些设置，您能以相应的策略选项使用**设置wps委托AP**命令。

```
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.
```

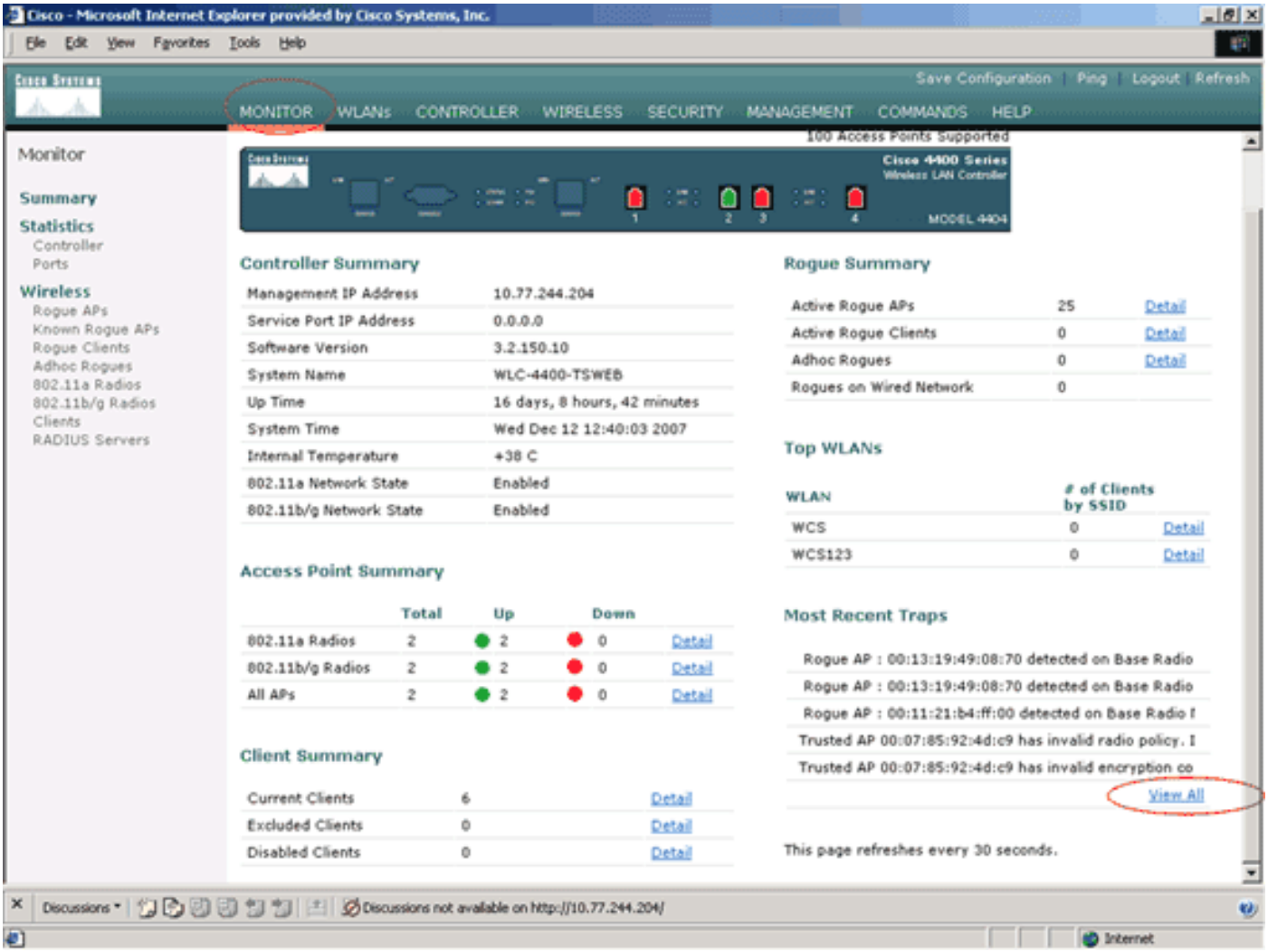
委托AP策略违反警报消息

这是委托AP控制器表示的策略违反警报消息示例。

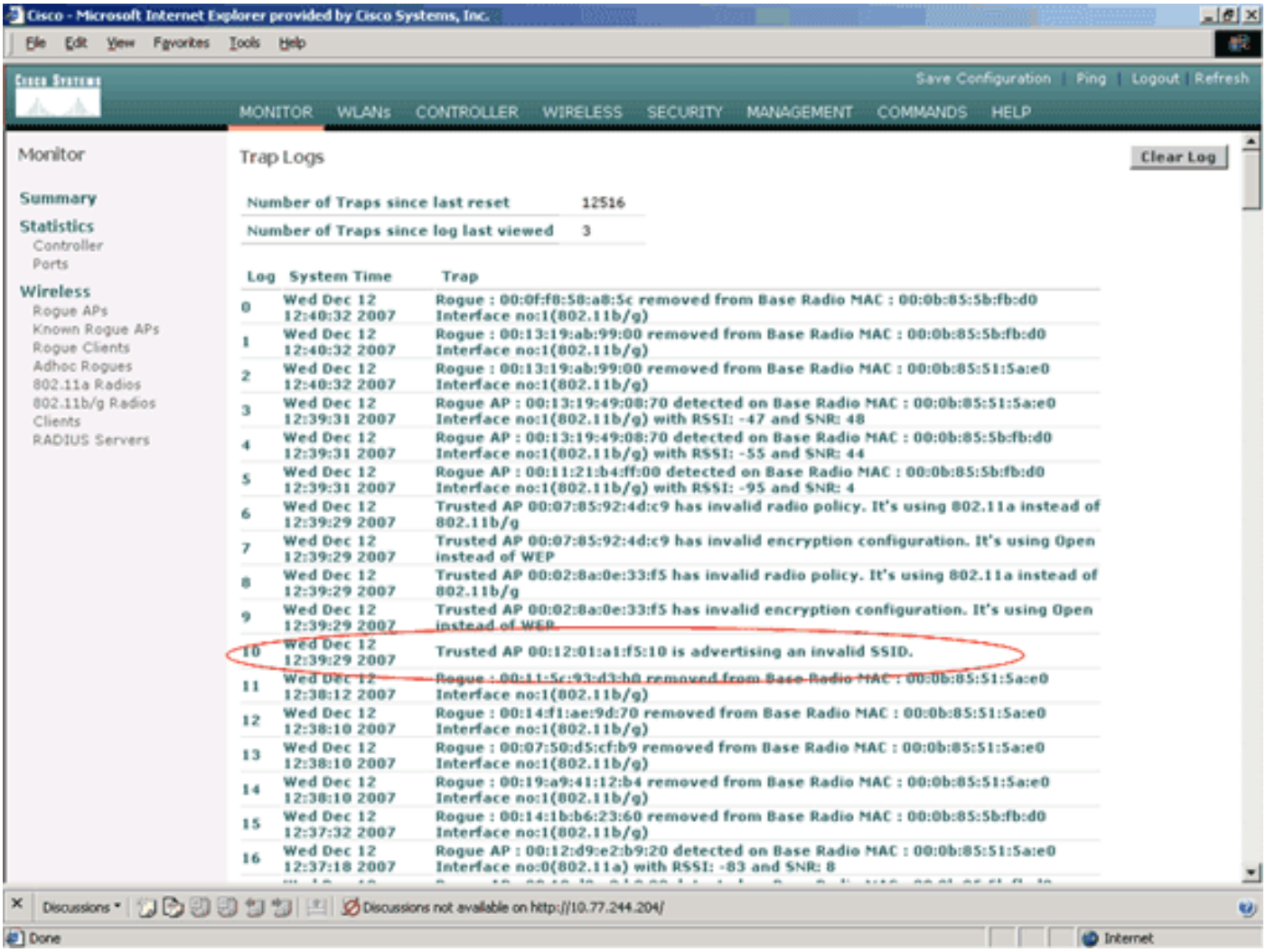
```
Thu Nov 16 12:39:12 2006  [WARNING] apf_rogue.c 1905: Possible AP
impersonation of xx:xx:xx:xx:xx:xx, using source address of
00:16:35:9e:6f:3a, detected by 00:17:df:7d:e1:70 on slot 0
 Thu Nov 16 12:39:12 2006  [SECURITY] apf_rogue.c 1490: Trusted AP Policy failed for AP
xx:xx:xx:xx:xx:xx - invalid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

注意选中项目错误消息此处。这些错误消息表明在委托AP和加密类型配置的SSID不匹配委托AP策略设置。

同一个警报消息能从WLC GUI被看到。为了查看此消息，去WLC GUI主菜单，并且点击**箴言报**。在箴言报页的最最近的陷阱部分，请点击**视图全部**为了查看在WLC的所有最近的警报。



在最最近的陷阱页上，您能识别如此镜像所显示，生成委托AP策略违反警报消息的控制器：



相关信息

- Cisco无线LAN控制器配置指南，版本5.2 -在RF组中启用胭脂接入点检测
- Cisco无线LAN控制器配置指南，版本4.0 -配置安全问题解决方案
- 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