Políticas de AP confiáveis em um controlador de LAN sem fio

Contents

Introduction

Este documento descreve as políticas de proteção sem fio *de AP* confiável em um Wireless LAN Controller (WLC), define as políticas de AP confiáveis e fornece uma breve descrição de todas as políticas de AP confiáveis.

Prerequisites

Requirements

Assegure-se de que você tenha uma compreensão básica dos parâmetros de segurança da LAN sem fio (como SSID, criptografia, autenticação, etc.).

Conventions

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Políticas de AP confiáveis

As políticas de AP confiáveis são um recurso de segurança no controlador projetado para ser usado em cenários em que os clientes têm uma rede de AP autônomo paralela junto com o controlador. Nesse cenário, o AP autônomo pode ser marcado como o AP confiável no controlador, e o usuário pode definir políticas para esses APs confiáveis (que devem usar

somente WEP ou WPA, nosso próprio SSID, preâmbulo curto e assim por diante). Se algum desses AP não atender a essas políticas, o controlador acionará um alarme para o dispositivo de gerenciamento de rede (Wireless Control System) que afirma que um AP confiável violou uma política configurada.

O que é um AP confiável?

Os APs confiáveis são APs que não fazem parte de uma organização. No entanto, eles não causam uma ameaça à segurança da rede. Esses APs também são chamados de APs amigáveis. Existem vários cenários em que você pode querer configurar um AP como um AP confiável.

Por exemplo, você pode ter diferentes categorias de APs em sua rede, como:

- **APs que você possui que não executam LWAPP (talvez executem IOS ou VxWorks)**
- APs LWAPP que os funcionários trazem (com o conhecimento do administrador)
- APs LWAPP usados para testar a rede existente
- APs LWAPP que os vizinhos possuem

Normalmente, os APs confiáveis são APs que se enquadram na **categoria 1**, que são APs que você possui que não executam o LWAPP. Eles podem ser APs antigos que executam VxWorks ou IOS. Para garantir que esses APs não danificem a rede, determinados recursos podem ser aplicados, como SSIDs e tipos de autenticação corretos. Configure as políticas de AP confiáveis na WLC e verifique se os APs confiáveis atendem a essas políticas. Caso contrário, você pode configurar o controlador para tomar várias ações, como disparar um alarme para o dispositivo de gerenciamento de rede (WCS).

Os APs conhecidos que pertencem aos vizinhos podem ser configurados como APs confiáveis.

Normalmente, o MFP (Management Frame Protection, Proteção de Quadro de Gerenciamento) deve impedir que APs que não são APs LWAPP legítimos se juntem ao WLC. Se as placas de rede suportam MFP, elas não têm permissão para aceitar desautenticações de dispositivos diferentes dos APs reais. Consulte Infrastructure Management Frame Protection (MFP) com WLC e Exemplo de Configuração de LAP para obter mais informações sobre MFP.

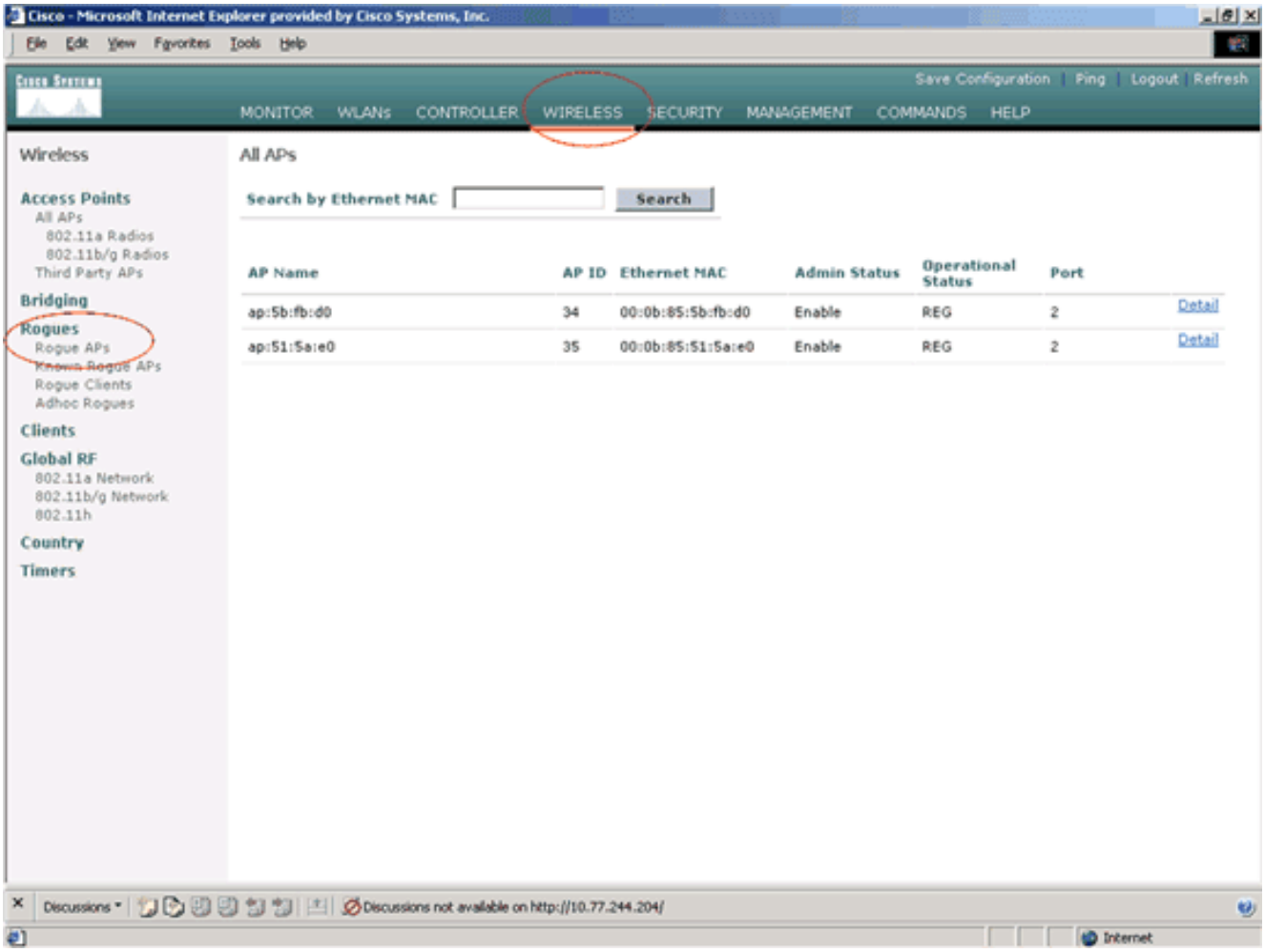
Se você tiver APs que executam VxWorks ou IOS (como na categoria 1), eles nunca se juntarão ao grupo do LWAPP ou ao MFP, mas talvez você queira aplicar as políticas listadas nessa página. Nesses casos, as políticas de AP confiáveis precisam ser configuradas no controlador para os APs de interesse.

Em geral, se você souber sobre um AP invasor e identificar que ele não é uma ameaça à sua rede, poderá identificar esse AP como um AP confiável conhecido.

Como configurar um AP como um AP confiável a partir da GUI do WLC?

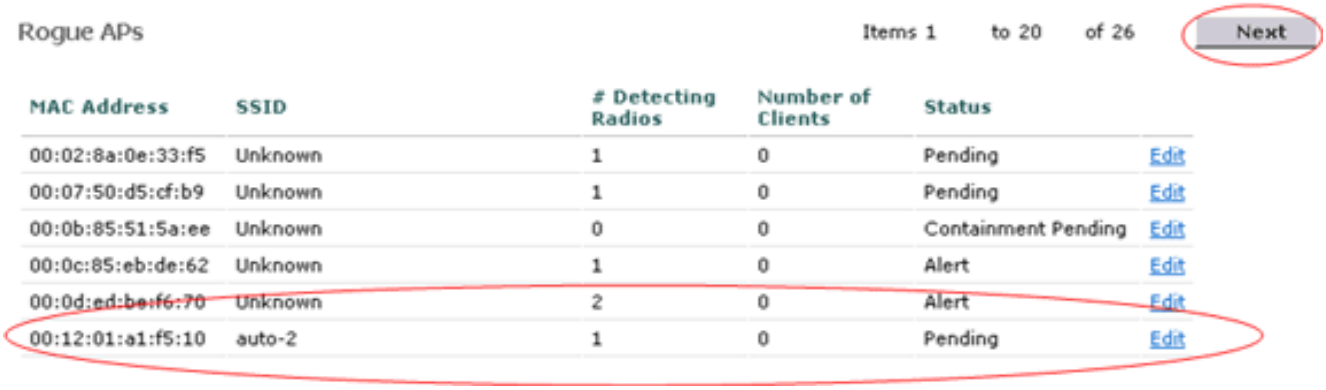
Conclua estes passos para configurar um AP como um AP confiável:

1. Efetue login na GUI do WLC por meio do login HTTP ou https.
2. No menu principal do controlador, clique em **Wireless**.
3. No menu localizado no lado esquerdo da página Wireless, clique em **Rogue APs**.



A página APs não autorizados lista todos os APs detectados como APs não autorizados na rede.

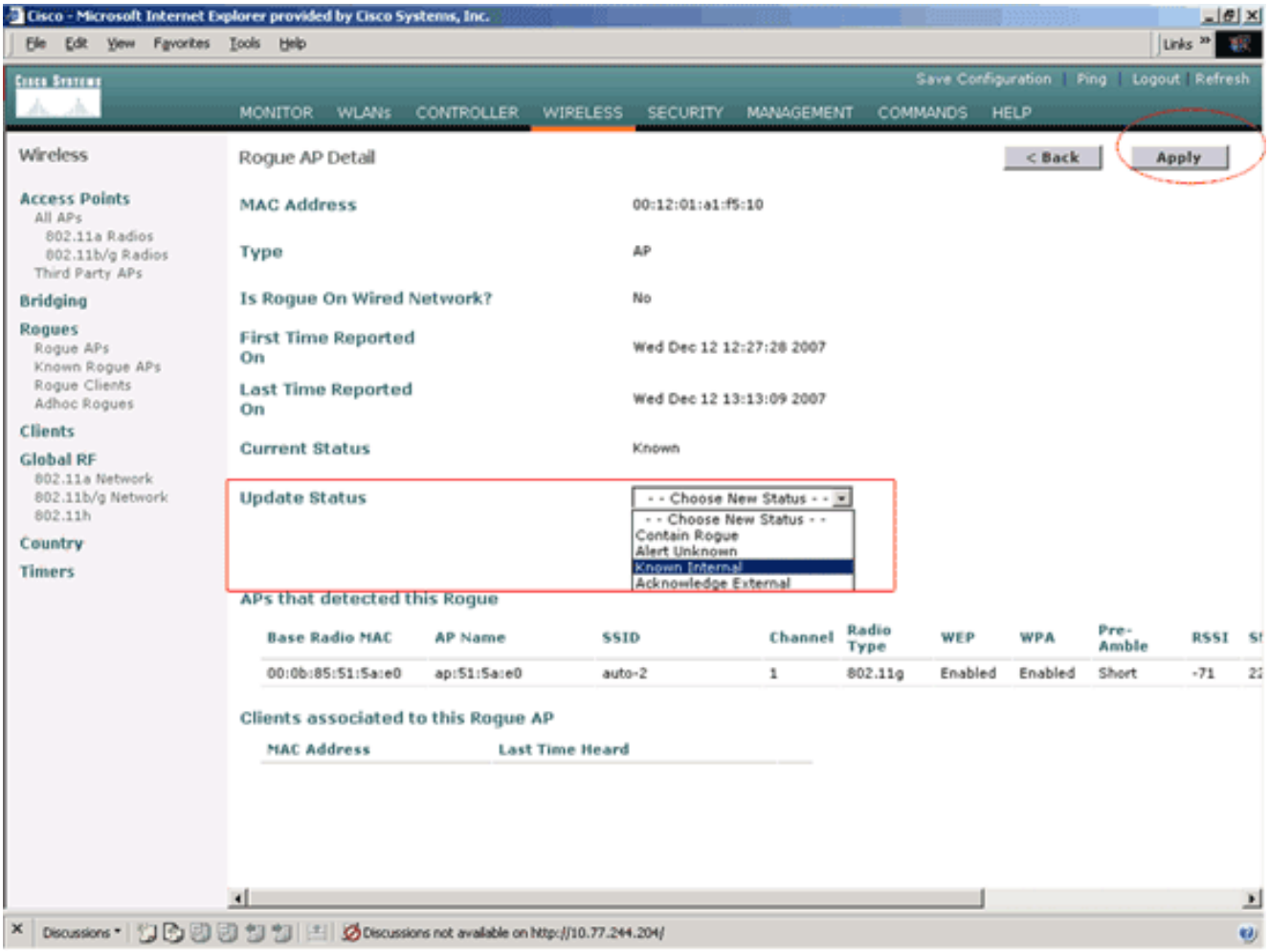
4. Nessa lista de APs não autorizados, localize o AP que deseja configurar como AP confiável que se enquadra na categoria 1 (como explicado na seção anterior).Você pode localizar os APs com os endereços MAC listados na página APs não autorizados. Se o AP desejado não estiver nesta página, clique em **Next** para identificar o AP da próxima página.
5. Quando o AP desejado estiver localizado na lista de APs não autorizados, clique no botão **Editar** que corresponde ao AP, que o leva até a página de detalhes do AP.



Na página de detalhes do Rogue AP, você pode encontrar informações detalhadas sobre esse AP (como se o AP se conectou à rede com fio, bem como o status atual do AP e assim por diante).

6. Para configurar esse AP como um AP confiável, selecione **Interno conhecido** na lista suspensa Status da atualização e clique em **Aplicar**.Quando você atualiza o status do AP para *Interno Conhecido*, esse AP é configurado como o AP confiável desta

rede.

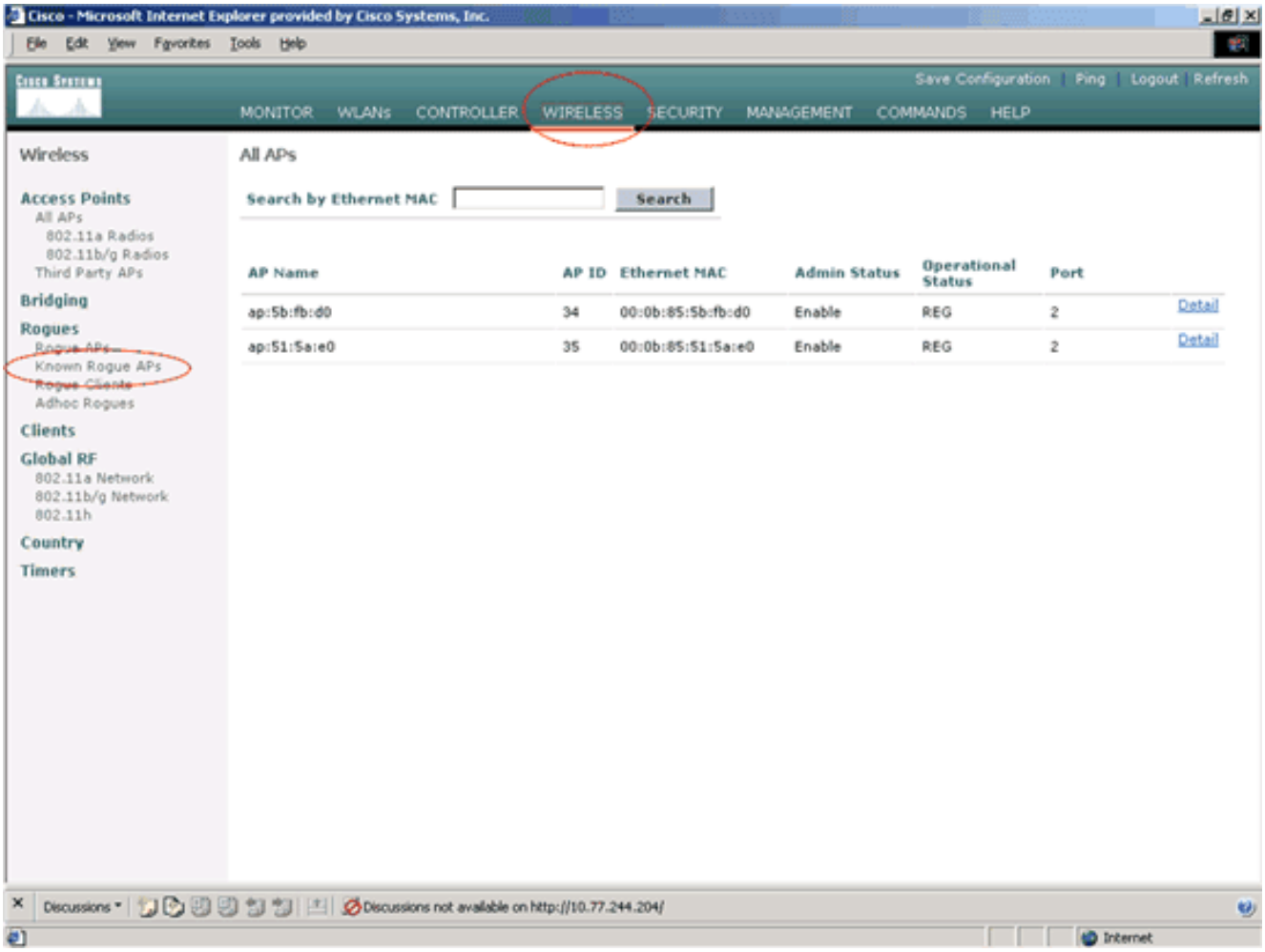


7. Repita essas etapas para todos os APs que deseja configurar como APs confiáveis.

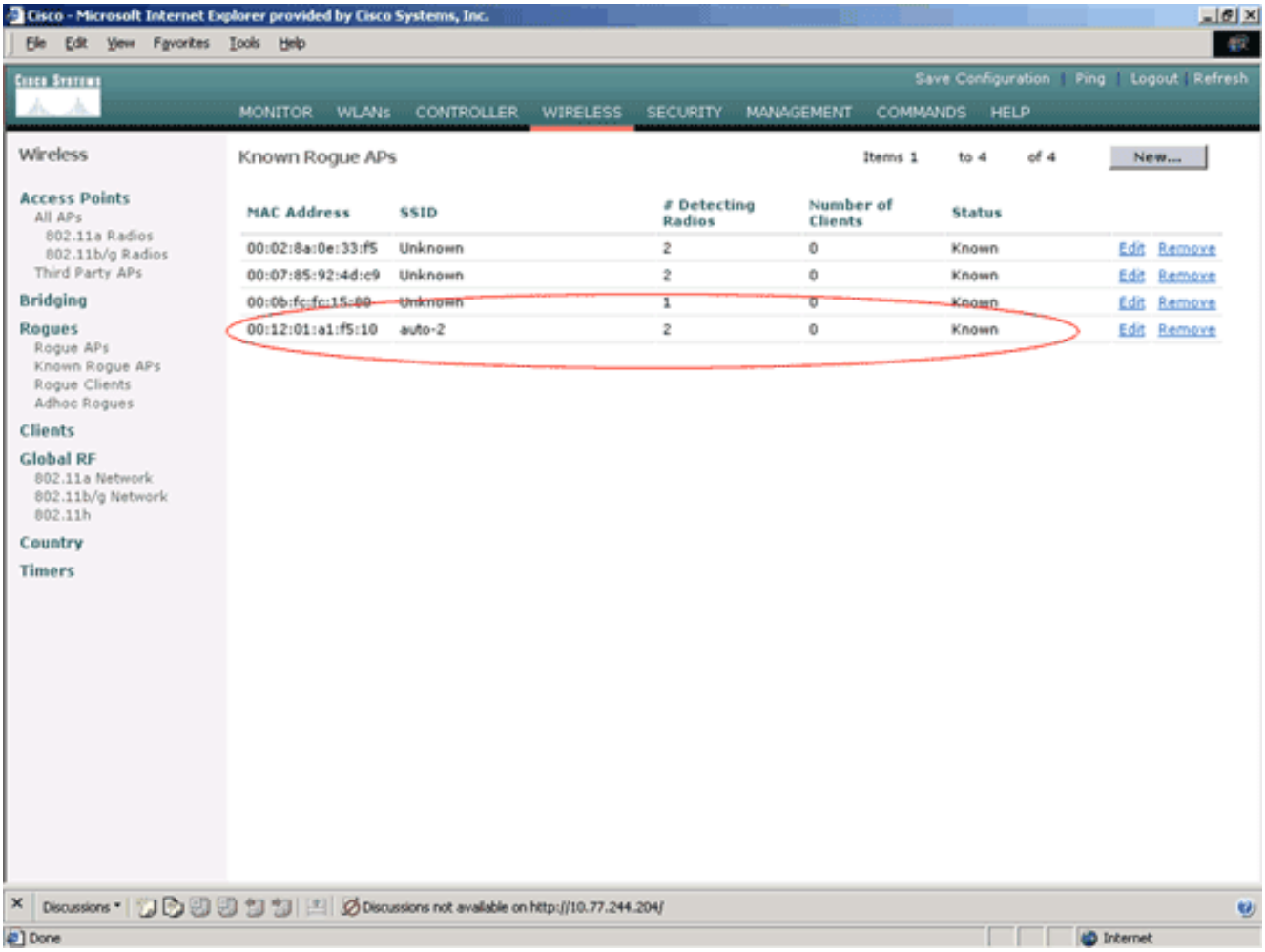
Verifique a configuração de AP confiável

Conclua estes passos para verificar se o AP está configurado corretamente como um AP confiável da GUI do controlador:

1. Clique em **Sem fio**.
2. No menu localizado no lado esquerdo da página Wireless, clique em **Known Rogue APs**.



O AP desejado deve aparecer na página APs conhecidos invasores com o status listado como
conhecido.



Entendendo as configurações de política de AP confiável

A WLC tem estas políticas de AP confiáveis:

- Política de criptografia forçada
- Política de preâmbulo forçada
- Política de tipo de rádio aplicada
- Validar SSID
- Alertar se o AP confiável está ausente
- Tempo limite de expiração para entradas de AP confiáveis (segundos)

Política de criptografia forçada

Essa política é usada para definir o tipo de criptografia que o AP confiável deve usar. Você pode configurar qualquer um destes tipos de criptografia em Diretiva de criptografia forçada:

- Nenhum
- Abrir
- WEP
- WPA/802.11i

A WLC verifica se o tipo de criptografia configurado no AP confiável corresponde ao tipo de criptografia configurado na configuração "**Diretiva de criptografia forçada**". Se o AP confiável não usar o tipo de criptografia designado, a WLC disparará um alarme ao sistema de gerenciamento para tomar as ações apropriadas.

Política de preâmbulo forçada

O preâmbulo do rádio (às vezes chamado de cabeçalho) é uma seção de dados à frente de um pacote que contém informações que os dispositivos sem fio precisam quando enviam e recebem pacotes. **Os** preâmbulos **curtos** melhoram o desempenho da taxa de transferência, para que sejam ativados por padrão. No entanto, alguns dispositivos sem fio, como os telefones SpectraLink NetLink, exigem **longos** preâmbulos. Você pode configurar qualquer uma destas opções de preâmbulo na política de preâmbulo forçado:

- Nenhum
- Curto
- Longo

A WLC verifica se o tipo de Preâmbulo configurado no AP confiável corresponde ao tipo de preâmbulo configurado na configuração "**Política de preâmbulo forçada**". Se o AP confiável não usar o tipo de preâmbulo especificado, a WLC disparará um alarme ao sistema de gerenciamento para tomar as ações apropriadas.

Política de tipo de rádio aplicada

Essa política é usada para definir o tipo de rádio que o AP confiável deve usar. Você pode configurar qualquer um destes tipos de rádio em Diretiva de tipo de rádio aplicada:

- Nenhum
- Somente 802.11b
- Somente 802.11a
- Somente 802.11b/g

A WLC verifica se o tipo de rádio configurado no AP confiável corresponde ao tipo de rádio configurado na configuração "**Diretiva de tipo de rádio forçada**". Se o AP confiável não usar os rádios especificados, a WLC disparará um alarme ao sistema de gerenciamento para tomar as ações apropriadas.

Validar SSID

Você pode configurar o controlador para validar um SSID de APs confiáveis em relação aos SSIDs configurados no controlador. Se o SSID de APs confiáveis corresponder a um dos SSIDs da controladora, a controladora disparará um alarme.

Alertar se o AP confiável está ausente

Se essa política estiver habilitada, a WLC alertará o sistema de gerenciamento se o AP confiável estiver ausente na lista de APs não autorizados conhecidos.

Tempo limite de expiração para entradas de AP confiáveis (segundos)

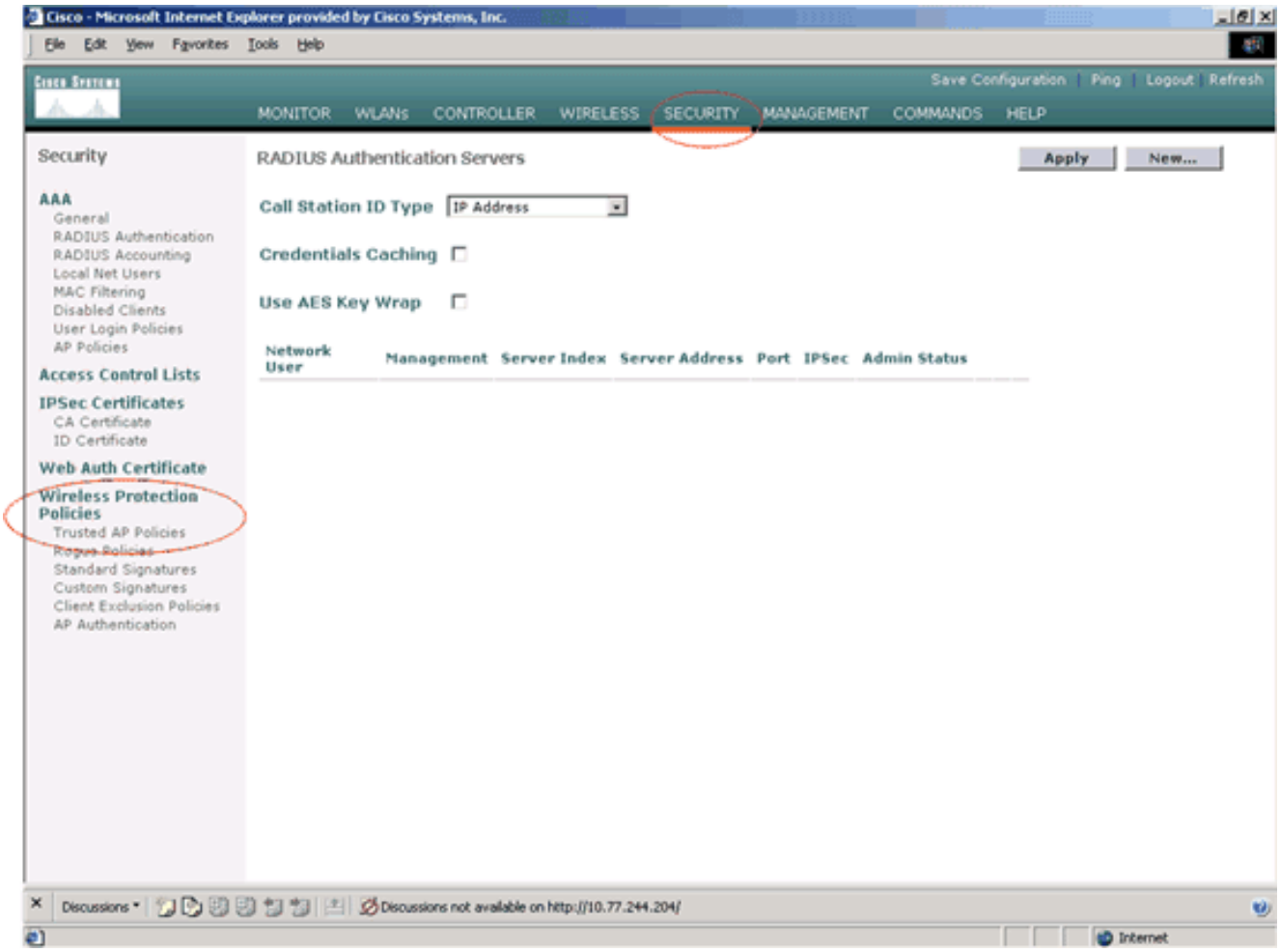
Este valor de Tempo Limite de Expiração especifica o número de segundos antes do AP confiável ser considerado expirado e liberado da entrada da WLC. Você pode especificar esse valor de tempo limite em segundos (120 a 3600 segundos).

Como configurar políticas de AP confiáveis na WLC?

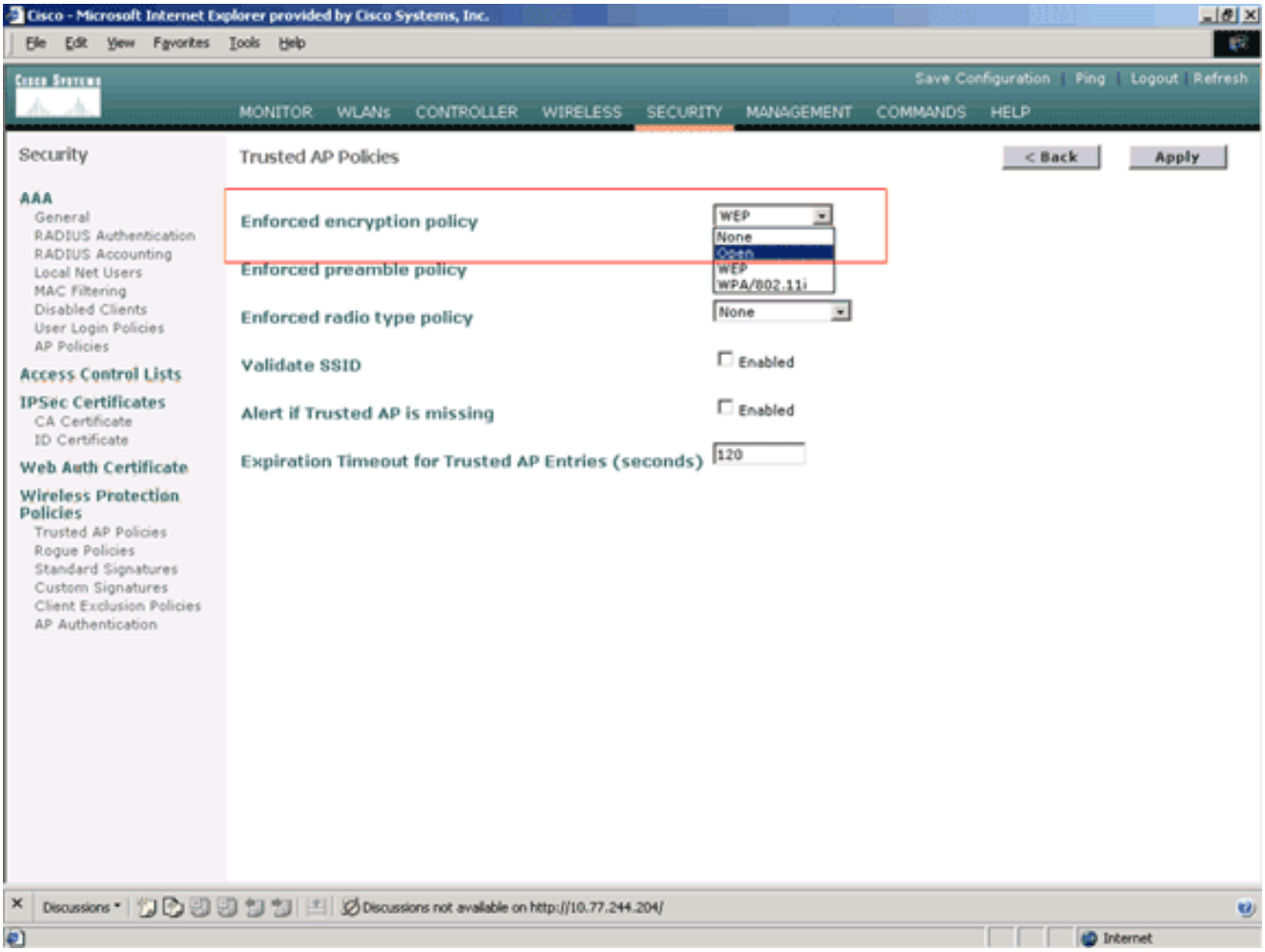
Conclua estes passos para configurar políticas de AP confiáveis na WLC através da GUI:

Observação: todas as políticas de AP confiáveis residem na mesma página da WLC.

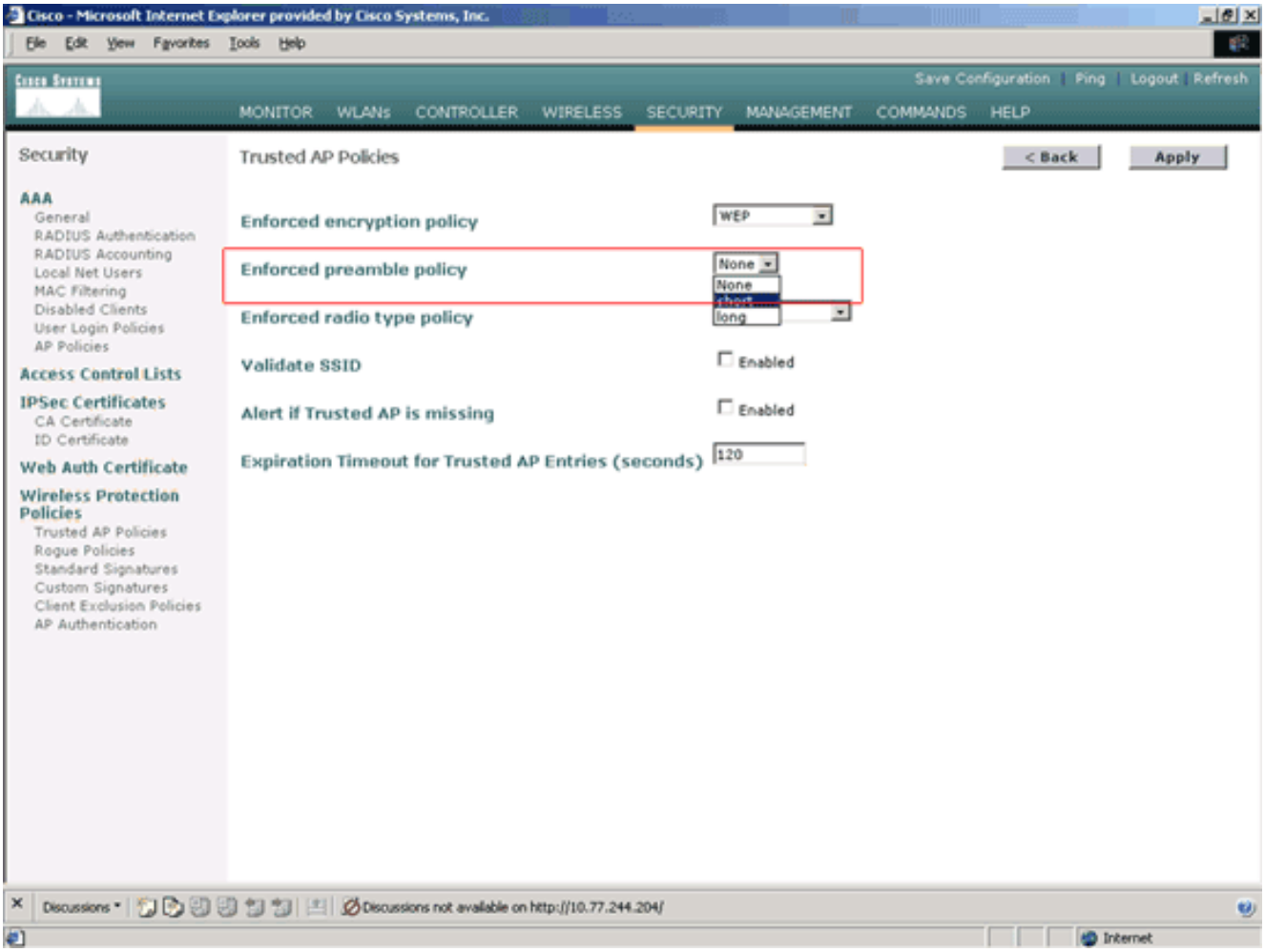
1. No menu principal da GUI da WLC, clique em **Segurança**.
2. No menu localizado no lado esquerdo da página Segurança, clique em **Políticas de APs Confiáveis** listadas no cabeçalho Políticas de proteção sem fio.



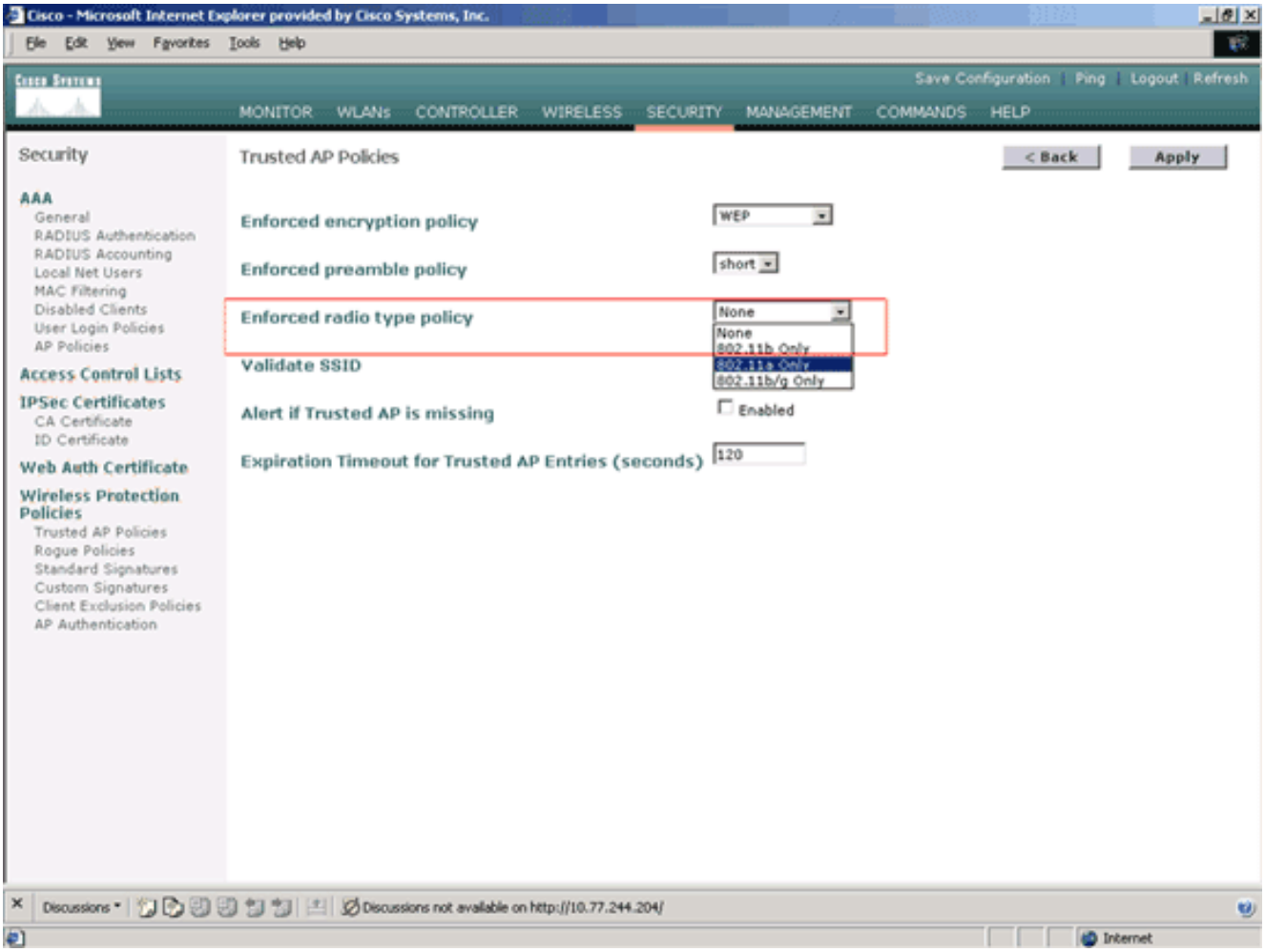
3. Na página de Políticas de AP confiável, selecione o tipo de criptografia desejado (None, Open, WEP, WPA/802.11i) na lista suspensa Diretiva de criptografia forçada.



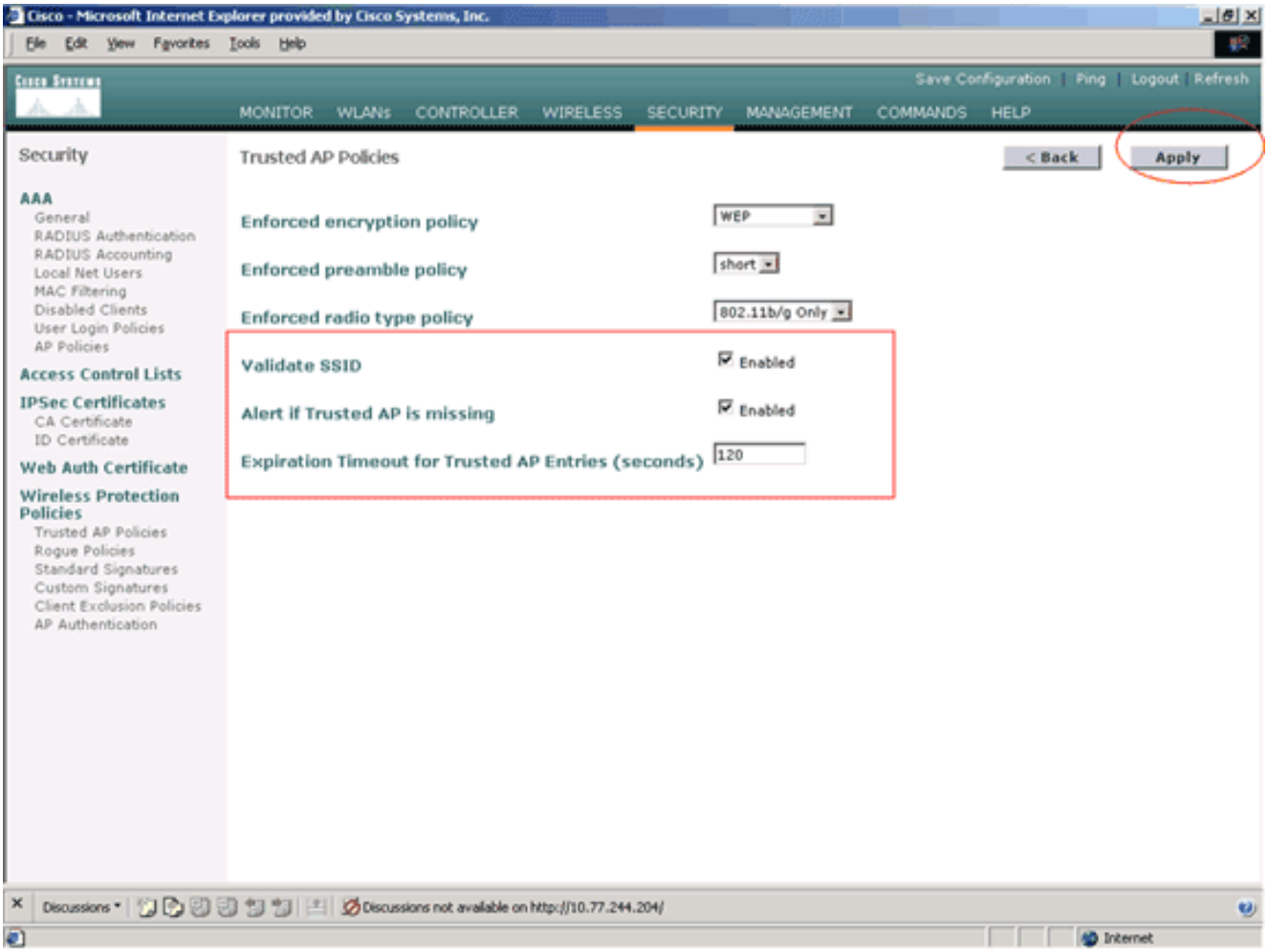
4. Selecione o tipo de preâmbulo desejado (Nenhum, Curto, Longo) na lista suspensa Política de tipo de preâmbulo
forçado.



5. Selecione o tipo de rádio desejado (Nenhum, 802.11b apenas, 802.11a apenas, 802.11b/g somente) na lista suspensa Política de tipo de rádio forçada.



6. Marque ou desmarque a caixa de seleção **Validar SSID habilitado** para habilitar ou desabilitar a configuração Validar SSID.
7. Marque ou desmarque a caixa de seleção **Alert if trust AP is missing Enabled (Alerta se o AP confiável está ausente** Habilitado) para habilitar ou desabilitar o Alerta se o AP confiável estiver faltando.
8. Insira um valor (em segundos) para a opção **Expiration Timeout for Trusted AP entries (Tempo limite de expiração para entradas de AP confiáveis)**.



9. Clique em Apply.

Observação: para definir essas configurações a partir da CLI da WLC, você pode usar o comando **config wps trust-ap** com a opção de política apropriada.

```
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.
```

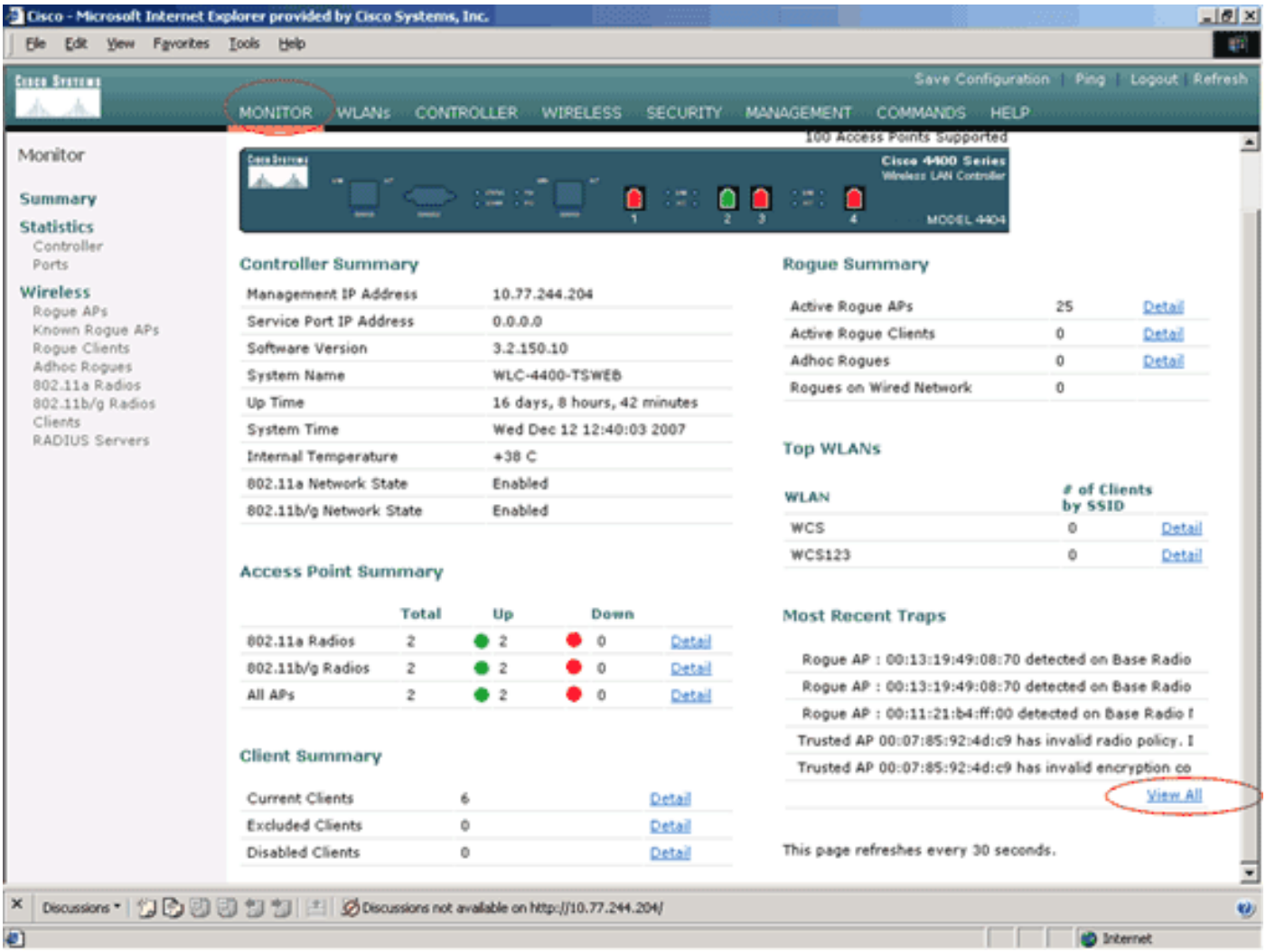
Mensagem de alerta de violação de política de AP confiável

Aqui está um exemplo de mensagem de alerta de violação de política de AP confiável mostrada pelo controlador.

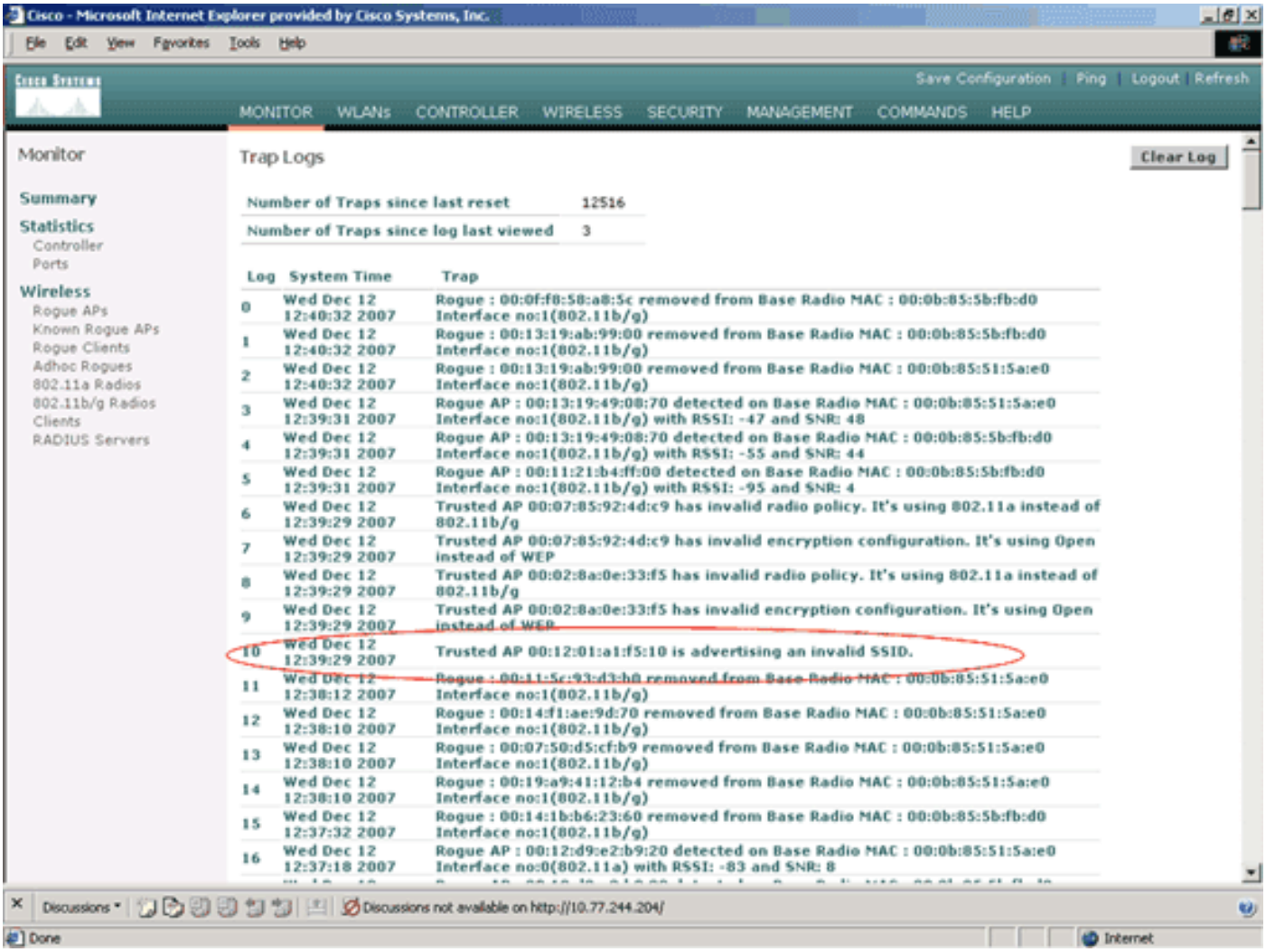
```
Thu Nov 16 12:39:12 2006  [WARNING] apf_rogue.c 1905: Possible AP
impersonation of xx:xx:xx:xx:xx:xx, using source address of
00:16:35:9e:6f:3a, detected by 00:17:df:7d:e1:70 on slot 0
 Thu Nov 16 12:39:12 2006  [SECURITY] apf_rogue.c 1490: Trusted AP Policy
failed for AP xx:xx:xx:xx:xx:xx - invalid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

Observe as mensagens de erro realçadas aqui. Essas mensagens de erro indicam que o SSID e o tipo de criptografia configurados no AP confiável não correspondem à configuração da política de AP confiável.

A mesma mensagem de alerta pode ser vista na GUI do WLC. Para visualizar esta mensagem, vá para o menu principal da GUI da WLC e clique em **Monitor**. Na seção Armadilhas mais recentes da página Monitor, clique em **Exibir tudo** para visualizar todos os alertas recentes na WLC.



Na página Traps mais recentes, você pode identificar o controlador que gera a mensagem de alerta de violação de política de AP confiável, como mostrado nesta imagem:



Informações Relacionadas

- Guia de Configuração do Cisco Wireless LAN Controller, Versão 5.2 - Ativação da Detecção de Ponto de Acesso de Rota em Grupos de RF
- Guia de configuração do Cisco Wireless LAN Controller Release 4.0 - Configurando soluções de segurança
- Detecção de invasores em redes sem fio unificadas
- Guia de projeto e implantação do SpectraLink Phone
- Exemplo de Configuração de Conexão de LAN Wireless Básica
- Conectividade deTroubleshooting em uma Rede Wireless LAN
- Exemplos de configuração de autenticação em controladores de LAN sem fio
- Suporte Técnico e Documentação - Cisco Systems