Políticas de AP confiáveis em um controlador de LAN sem fio

Contents

Introduction Prerequisites Requirements Conventions Políticas de AP confiáveis O que é um AP confiável? Como configurar um AP como um AP confiável a partir da GUI do WLC? Entendendo as configurações de política de AP confiável Como configurar políticas de AP confiáveis na WLC? Mensagem de alerta de violação de política de AP confiável Informações Relacionadas

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 <u>Convenções de Dicas Técnicas da Cisco para obter mais informações sobre</u> <u>convenções de documentos.</u>

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 <u>Infrastructure Management Frame Protection (MFP) com WLC</u> <u>e Exemplo de Configuração de LAP</u> 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**.

| Cisco - Microsoft Internet Exp | plorer provided by Cisco S Tools Help | ystems, Inc. | | <u> 1999</u> | | | | @_X |
|---|--|---------------------------|-------------------|--|----------------------------------|-------------------------------------|----------------|------------------|
| Circa Serritor | MONITOR WLANS | CONTROLLER | WIRELES! | S SECURITY MAN | IAGEMENT COM | Sava Configurat IMANDS HELP | ion Ping | Logout Refresh |
| Wireless ACCess Points All APS B02.11a Radios B02.11b/g Radios Third Party APS Bridging Rogue Rogue APS Rogue APS Rogue Clients Adhoc Rogues Clients Global RF 802.11a Network 802.11b/g Network 802.11b/ Timers | MONITOR WLANS All APS Search by Ethernet AP Name ap:5b:fb:d0 ap:51:5a:e0 | | AP ID 34 35 | Search Ethernet MAC 00:0b:85:5b:fb:d0 00:0b:85:51:5a:e0 | Admin Status Enable Enable | Operational Status REG REG | Port 2 2 | Detail Detail |
| × Discussions • 1 💭 🖓 🗐 |) 1 1 🖉 Ødecus | ions not available on htt | p://10.77.2 | 44.204/ | | | | Ø |
| อา | | | | | | | i in | ternet |

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.

| Rogue APs | | | Item | s 1 to 20 of 26 | Next |
|-------------------|---------|-----------------------|----------------------|---------------------|------|
| MAC Address | SSID | # Detecting Radios | Number of Clients | Status | |
| 00:02:8a:0e:33:f5 | Unknown | 1 | 0 | Pending | Edit |
| 00:07:50:d5:cf:b9 | Unknown | 1 | 0 | Pending | Edit |
| 00:0b:85:51:5a:ee | Unknown | 0 | 0 | Containment Pending | Edit |
| 00:0c:85:eb:de:62 | Unknown | 1 | 0 | Alert | Edit |
| 00:0d:ed:beif6:70 | Unknown | 2 | 0 | Alert | Edit |
| 00:12:01:a1:f5:10 | auto-2 | 1 | 0 | Pending | Edit |
| | | | | | |

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

| Des For Dess (Buckles | Trong Clash | | | | | | | | | | 1110 |
|---|----------------------|---------|--------------|------------|---|----------------------------|---------------|------------|--------------|---------------|-----------------|
| aca Srateme | | | | | | | | iave Confi | guration P | ing Logo | ut Refre |
| A. A. | MONITOR WL | Ws | CONTROLLER | WIRELESS | SECURITY | MANAGEMEN | т соми | IANDS | HELP | | ويرجو المحافظين |
| Vireless | Rogue AP Deta | i i | | | | | | | < Back | | pply |
| All APs | MAC Address | | | | 00:12:01:a1:f | 5:10 | | | | | |
| 802.11a Radios 802.11b/g Radios Third Party APs | Туре | | | | AP | | | | | | |
| sridging | Is Rogue On W | fired N | Vetwork? | | No | | | | | | |
| togues Rogue APs Known Rogue APs | First Time Rep On | orted | | | Wed Dec 12 1 | 2:27:28 2007 | | | | | |
| Rogue Clients Adhoc Rogues | Last Time Rep On | orted | | | Wed Dec 12 1 | 3:13:09 2007 | | | | | |
| lients | Current Statu | | | | Known | | | | | | |
| 802.11a Network 802.11b/g Network 802.11h | Update Status | | | | Choose I | Vew Status] Iew Status | 3 | | | | |
| ountry limers | | | | | Contain Rogu Alert Unknown Known Intern | e al | | | | | |
| | APs that deter | ted t | his Rogue | | Acknowledge | External | | | | | |
| | Base Radio M | 1AC | AP Name | \$\$1 | D | Channel | Radio Type | WEP | WPA | Pre- Amble | RSSI |
| | 00:0b:85:51:5 | ia:e0 | ap:51:5a:e0 | auto | -2 | 1 | 802.119 | Enabled | Enabled | Short | -71 |
| | Clients associ | ated t | o this Roque | AP | | | | | | | |
| | MAC Address | | Last | Time Heard | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| | 4 | | | | | | | | | | |

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.

| Image: State State: Save Configuration: Pipe: Cogod: Refresh Wireless MONITOR: WLANS: CONTROLLER: WIRELESS: SECURITY: MANAGEMENT: COMMONDS: HELP Wireless Access Points: All Aris: 00:02:64:00:33:15: Unknown 00:02:64:00:33:15: Unknown 2 0 Diddios 00:02:64:00:33:15: Unknown 2 0 Rogan Aris: 00:02:64:00:33:15: Unknown 2 0 Known Diddios 00:02:64:00:33:15: Unknown 2 0 Known Edd: Bemoxe Rogan Aris: Adros Rogan 2 0 Known Edd: Bemoxe Oi:02:64:06:33:15: Unknown 2 0 Known Edd: Bemoxe Oi:02:64:06:33:15: Unknown 2 0 Known Edd: Bemoxe Oi:02:16:10:15:10: unknown 2 0 Known Edd: Bemoxe Oi:12:10:10:11:15:10: unknown 2 0 Known Edd: Bemoxe Oi:21:10:10:11:15:10: unknown 2 0 Known Edd: Bemoxe Oi:21:10:10:11:15:10: unknown 2 0 Known Edd: Bemoxe Oi:21:10:10:11:15:10: unknoor 0 0 | Eisco - Microsoft Internet E | oplorer provided by Cisco | Systems, Inc. | | | | | @_× |
|---|--|---------------------------|-------------------------|------------------|-----------------------|----------------------|------------------|---------------------|
| Consent Bit Status Control Refresh Minices MONITOR WLANS CONTROLLER WIPELES SECURITY MANAGEMENT COMMANDS HELP Wireless Known Rogue APs Items 1 to 4 of 4 New | Bie Edit Vew Favorites | Toole Reb | | | | | | |
| Monitor WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP Wreckss Access Points All Afs Bodding Radios Radios Radios Status B02.118.16 Addies SED # Detecting Number of Status Edd Remove B02.118.16 Addies SSD # Detecting Number of Status Edd Remove Bridging Mayor Afs 00:00:16:15:12:44:00 Unknown 2 0 Known Edd Remove Rogue AFs Adhoe Rogues AFs 00:00:16:15:10 wdo-2 2 0 Known Edd Remove 00:2:10:10:11:15:10 wdo-2 2 0 Known Edd Remove 00:2:11/9 Network 00:2:11/9:10:11:15:10 wdo-2 0 Known Edd Remove 00:2:11/9 Network 00:2:11/9:10:11:15:10 wdo-2 0 Known Edd Remove 00:2:11/9 Network 00:2:11/9:10:11:15:10 wdo-2 0 Nown Edd Remove 00:2:11/9 Network 00:2:11/9:10:10:11:15:10 wdo-2 0 Nown Edd Remove 00 | Cinca Systems | | | | | | ve Configuration | Ping Logout Refresh |
| Wirders Ares Points Mig Solita Ratios Bage Ratios Rope Ratis <th><u>A. A.</u></th> <th>MONITOR WLANS</th> <th>CONTROLLER</th> <th>WIRELESS</th> <th>SECURITY MAN</th> <th>AGEMENT COMMA</th> <th>NDS HELP</th> <th></th> | <u>A. A.</u> | MONITOR WLANS | CONTROLLER | WIRELESS | SECURITY MAN | AGEMENT COMMA | NDS HELP | |
| Arcs SiD Potecting Number of Status 00:118 Radios 00:01:8:00:315 Unknown 2 0 Known Edd Radios Dridgers Rogue APs 00:01:8:10:13:50 Unknown 1 0 Known Edd Radios Rogue APs Rogue APs Nach Address SID # Order 0 Known Edd Radios Ol:11:01:15:10 unknown 2 0 Known Edd Radios Ol:21:02:13:15:10 unknown 2 0 Known Edd Radios Ol:21:02:13:16:15:10 unknown 2 0 Known Edd Radios Ol:21:02:13:16:15:10 unknown Unknown Edd Radios Unknown Edd Radios Vol:02:13:16:15:10 unknown Unknown Unknown Unknown Edd Radios Unknown | Wireless | Known Rogue AP | 5 | | | Items 1 | to 4 of 4 | New |
| 00:3.13 k Addos Rogues Rogue A/S Rogue Clients Addos Rogue 00:12:10:13:15:10 00:12:10:13:15:10 00:12:10:13:15:10 00:12:10:13:15:10 00:12:10:13:15:10 00:12:10:13:15:10 00:12:10:13:15:10 00:12:10:13:15:10 00:12:10:13:15:10 00:12:10:13:15:10 00:12:10:13:15:10 00:12:10:13:15:10 00:12:10:13:15:10 00:12:10:13:15:10 00:12:10:13:15:10 00:12:10:13:15:10 | Access Points All APs | MAC Address | SSID | | # Detecting Radios | Number of Clients | Status | |
| Third Party APs Bridging Rogue 3 Rogue 4Ps Known Rogue 4Ps Rogue 7 Berder P Bozation Rogue 4Ps Rogue 11/9 Network Bozzi 11/9 Network Notwork Bozzi 11/9 Network Notwork Bozzi 11/9 Network Bozzi 11/9 Network Bozzi 11/9 Network | 802.11a Radios 802.11b/g Radios | 00:02:8a:0e:33:f5 | Unknown | | 2 | 0 | Known | Edit Remove |
| Bridging 00:00:ftg:ftc:15:00 Unknownh 1 0 Kooun Eds Reques Rogue APs 00:12:01:a1:f5:10 #uto-2 2 0 Known Eds Remoure Rogue APs Known Rogue APs Rogue Clients Adhoc Rogues Clients Eds Remoure Clobal RF 00:12:01:a1:f5:10 #uto-2 2 0 Known Eds Remoure Clobal RF 00:12:01:a1:f5:10 #uto-2 2 0 Known Eds Remoure Clobal RF 00:12:01:a1:f5:10 #uto-2 2 0 Known Eds Remoure 00:12:01:a1:F5:10 #uto-2 2 0 Known Eds Remoure Clobal RF 00:12:01:a1:F5:10 #uto-2 Remoure Remoure Remoure Remoure 00:11:16 Note Remoure Remoure Remoure Remoure Remoure Clobal RF 00:12:01:a1:F5:10 #uto-2 Remoure Remoure Remoure Remoure Vocations Remoure Remoure Remoure Remoure <td>Third Party APs</td> <td>00:07:85:92:4d:c9</td> <td>Unknown</td> <td></td> <td>2</td> <td>0</td> <td>Known</td> <td>Edit Remove</td> | Third Party APs | 00:07:85:92:4d:c9 | Unknown | | 2 | 0 | Known | Edit Remove |
| Regues 00:12:01:s1:f5:10 avto-2 2 0 Known Edit Remove Rogues APs Rogues APs Rogues Clients Adhoc Rogues APs Rogues Clients Adhoc Rogues Edit Remove Clients Objection S Objection S Adhoc Rogues Edit Remove Edit Remove Clients Objection S Objection S Adhoc Rogues Edit Remove Edit Remove Objection S Objection S Objection S Edit Remove Edit Remove Edit Remove V Decession S Objection S Edit Remove Edit Remove Edit Remove | Bridging | 00:0b:fc:fc:15:00 | Unknown | | 1 | 0 | Known | Edit Remove |
| Rogue APs Rogue Clients Adhoc Rogues Clients Clobal RF 802.113 Network 802.113 Network 802.113 Network 802.113 Network 802.113 Network 802.116 Network 802.117 Timers | Rogues | 00:12:01:a1:f5:10 | auto-2 | | 2 | 0 | Known | Edit Remove |
| Cleats Global FF 002.11a Network 002.11b Country Timers V Decusions * | Known Rogue APs Rogue Clients Adhoc Rogues | | | | | | | |
| Clobal RF 002.11a Network 002.11b Country Timers × Descussions * D & D & D & D & D & D & D & D & D & D | Clients | | | | | | | |
| Country Timers | Global RF 802.11a Network 802.11b/g Network 802.11b | | | | | | | |
| Timers | Country | | | | | | | |
| × Decussions • 😨 🕃 🗐 🗐 🗐 🖉 🖉 Decussions not evalable on http://10.77.244.204/ | Timers | | | | | | | |
| | × Discussions • 🐘 🔁 🗐 | 3 13 13 18 ØDeo | ssions not available on | http://10.77.244 | 204/ | | | |
| | Doos | | | | | | | all Internet |

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
- <u>Tempo limite de expiração para entradas de AP confiáveis (segundos)</u>

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.

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. Cisco - Microsoft Internet Explorer provided by Cisco Systems, Inc. _ @ × Ele Edit View Favorites Iools Help 41 Save Configuration | Ping | Logout | Refresh Cinco Svoremo MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS Security RADIUS Authentication Servers Apply New... AAA Call Station ID Type IP Address . General **RADIUS** Authentication RADIUS Accounting Credentials Caching Local Net Users MAC Filtering Disabled Clients Use AES Key Wrap **User Login Policies** AP Policies Network Management Server Index Server Address Port IPSec Admin Status User Access Control Lists **IPSec Certificates** CA Certificate ID Certificate Web Auth Certificate Wireless Protection Policies Trusted AP Policies Rogue Policies Standard Signatures Custom Signatures Client Exclusion Policies AP Authentication × Discussions • 🎲 🕃 🕄 🐩 🐮 🖄 Discussions not available on http://10.77.244.204/ ۲ i Internet
- 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.



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



 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.

| Cisco - Microsoft Internet Er | splorer provided by Cisi | to Systems, Inc. | | | / | | 01020 | _ 8 × |
|--|--|--|------------------|----------|------------|----------|--------------------|----------------|
| Ele Edit Yew Favorites | Tools Relb | | | | | | | 10 |
| Cases Searcas | | | | | | Save Co | nfiguration Ping | Logout Refresh |
| A. A. | MONITOR WLAN | Is CONTROLLER | WIRELESS | SECURITY | MANAGEMENT | COMMANDS | HELP | |
| Security | Trusted AP Polic | es | | | | | < Back | Apply |
| AAA General RADIUS Authentication RADIUS Authentication RADIUS Accounting Local Net Users MAC Filtering Disabled Clients User Login Policies AP Policies Access Control Lists IPSec Certificates ID Certificate ID Certificate Web Auth Certificate Wireless Protection Policies Standard Signatures Custom Signatures Client Exclusion Policies AP Authentication | Enforced encry Enforced pream Enforced radio t Validate SSID Alert if Trusted Expiration Time | ption policy able policy type policy AP is missing out for Trusted A | JP Entries (s | econds) | VEP | | | |
| N State State Date | Ob days along 1 (a) 1 and - | | | | | | | - |
| * Discussions * 🕤 🕥 🕄 | 9991 H Ør | cussions not available on | http://10.77.244 | 204/ | | | | 9 |
| ₽ | | | | | | | 1 🔘 Ir | ternet |

- 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.
- 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 Controlle | er) > 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, 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.

| | | | | | | | Save Config | uration Ping | Logout | | |
|------------------------------|---------------------|---------------------------------|--------|---------|--------|----------|---|------------------|----------------|--|--|
| A. A. arasanana | MONITOR WLAN: | sCONT | ROLLER | WIREL | ESS. | SECURITY | MANAGEMENT COMMANDS HI | EUP | | | |
| onitor mmary atistics | Continues A. A | - | :# :* | • | - [|) :=: Q | 100 Access Points Supported Cisco 4400 Series Weekss LAN Controller 3 4 MODEL 4404 | | | | |
| Controller Ports | Controller Summ | ary | | | | | Rogue Summary | | | | |
| ireless | Management IP Add | iress | 10.77. | 244.204 | 4 | | Active Roque APs | 25 | Detail | | |
| logue APs Inown Rogue APs | Service Port IP Add | Service Port IP Address 0.0.0.0 | | | | | Active Roque Clients | 0 | Detail | | |
| logue Clients | Software Version | Software Version 3.2.150.10 | | | | | Adhoc Roques | 0 | Detail | | |
| dhoc Rogues 02.11a Radios | System Name | | WLC-4 | 400-TS | WEB | | Roques on Wired Network | 0 | ACX MILE | | |
| 02.11b/g Radios | Up Time | Up Time 16 days, 8 hours, 42 m | | | | | Rogues on miles neovork | 0 | | | |
| lients ADTUS Servers | System Time | | Wed D | ec 12 1 | 2:40:0 | 3 2007 | | | | | |
| AD103 Servers | Internal Temperatur | re | +38 C | | | | Top WLANS | | | | |
| | 802.11a Network St | ate | Enable | d | | | | # of C | lients | | |
| | 802.11b/g Network | State | Enable | d | | | WLAN | by SS | SSID | | |
| | | | | | | | WCS | 0 | Deta | | |
| | Access Point Sur | nmary | | | | WCS123 | 0 | Deta | | | |
| | | Total | Up | | Down | | Most Recent Traps | | | | |
| | 802.11a Radios | 2 | • 2 | ٠ | 0 | Detail | | | | | |
| | 802.11b/g Radios | 2 | • 2 | ٠ | 0 | Detail | Rogue AP : 00:13:19:49:08: | 70 detected on | Base Radio | | |
| | All APs | 2 | • 2 | ٠ | 0 | Detail | Rogue AF : 00:13:19:49:08: | 70 detected on | Base Radio | | |
| | | | | | | | Rogue AP : 00:11:21:64:#:0 | 0 detected on I | Base Radio I | | |
| | Client Summary | | | | | | Trusted AP 00:07:85:92:4d:c | 9 has invalid ra | adio policy. I | | |
| | | | | | | | Trusted AP 00:07:85:92:4d:c9 has invalid encryption co | | | | |
| | Current Clients | | 6 | | | Detail | | | View A | | |
| | Excluded Clients | Excluded Clients 0 | | | | Detail | | | | | |
| | | | | | | Detail | This page refreshes every 30 st | econds. | | | |

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:

| Cisco - Microsoft Internet Ex | plorer provided by Cisco S | ystems, Inc. | <u> Biliyy</u> y | | | | | @_× |
|----------------------------------|--------------------------------|--|--------------------------------|-------------------------------|------------------------------------|------------------|--------------------|----------------------|
| Ele Edit Yew Favorites | Tools Flatb | | | | | | | # R |
| Cases Systems | | | | | | Save Co | nfiguration Ping | g Logout Refresh |
| A.A. | MONITOR WLANS | CONTROLLER | WIRELESS | SECURITY | MANAGEMENT | COMMANDS | HELP | |
| Monitor | Trap Logs | | | | | | | Clear Log |
| Summary | Number of Traps si | nce last reset | 12516 | | | | | |
| Statistics Controller | Number of Traps si | nce log last view | wed 3 | | | | | |
| Ports | Log System Time | Trap | | | | | | |
| Rogue APs | 0 Wed Dec 12 12:40:32 2007 | Rogue : 00: Interface n | 0f:f8:58:a8:5c o:1(802.11b/ | removed fro g) | om Base Radio N | IAC : 00:0b:85: | 5b:fb:d0 | |
| Known Rogue APs Rogue Clients | 1 Wed Dec 12 12:40:32 2007 | Rogue : 00: Interface n | 13:19:ab:99:0 o:1(802.11b/ | 0 removed f 9) | rom Base Radio | MAC : 00:0b:85 | :5b:fb:d0 | |
| Adhoc Rogues 802.11a Radios | 2 Wed Dec 12 12:40:32 2007 | Rogue : 00: Interface n | 13:19:ab:99:0 o:1(802.11b/ | 0 removed f g) | rom Base Radio | MAC : 00:0b:85 | 51:5a:e0 | |
| 802.11b/g Radios Clients | 3 Wed Dec 12 12:39:31 2007 | Rogue AP : Interface n | 00:13:19:49:0 o:1(802.11b/ | 8:70 detecte g) with RSSI: | d on Base Radio -47 and SNR: 44 | MAC:00:0b:8 | 5:51:5a:e0 | |
| RADIUS Servers | 4 Wed Dec 12 12:39:31 2007 | Rogue AP : Interface n | 00:13:19:49:0 o:1(802.11b/ | 8:70 detecte g) with RSSI: | d on Base Radio -55 and SNR: 4 | MAC:00:0b:8 | 5:5b:fb:d0 | |
| | 5 Wed Dec 12 12:39:31 2007 | Rogue AP : Interface n | 00:11:21:b4:ff | :00 detected | on Base Radio | MAC: 00:0b:85 | :Sb:fb:d0 | |
| | 6 Wed Dec 12 12:39:29 2007 | Trusted AP 802.11b/g | 00:07:85:92:4 | d:c9 has inv | alid radio policy | . It's using 80 | 2.11a instead of | |
| | 7 Wed Dec 12 12:39:29 2007 | Trusted AP | 00:07:85:92:4 WEP | d:c9 has inv | alid encryption | configuration. | It's using Open | |
| | 8 Wed Dec 12 12:39:29 2007 | Trusted AP 802.11b/g | 00:02:8a:0e:3 | 3:f5 has inv | alid radio policy | . It's using 802 | .11a instead of | |
| | 9 Wed Dec 12 12:39:29 2007 | Trusted AP | 00:02:8a:0e:3 | 3:f5 has inv | alid encryption (| onfiguration. | It's using Open | |
| | 10 Wed Dec 12 12:39:29 2007 | Trusted AP | 00:12:01:a1:f | 5:10 is adve | rtising an invali | d SSID. | > | |
| | 11 Wed Dec 12 12-38-12 2007 | Wed Dec 12 Regue : 00:11:5r:93:d3:h0 removed from Base Radio MAC : 00:00:85:51:5a:e0 | | | | | | |
| | 12 Wed Dec 12 | Rogue : 00: | 14:f1:ae:9d:70 | removed fr | om Base Radio ! | MAC: 00:0b:85 | 51:5a:e0 | |
| | 12:38:10 2007 Wed Dec 12 | Interface n | 0:1(802.11b/ | g) removed fr | om Base Radio M | AC - 00-05-85 | 51-5a:e0 | |
| | 13 12:38:10 2007 | Interface n | o:1(802.11b/ | g) | om dase nauro i | inc i delabies. | 01100/00 | |
| | 14 Wed Dec 12 12:38:10 2007 | Rogue : 00: Interface n | | | | | | |
| | 15 Wed Dec 12 12:37:32 2007 | Rogue : 00: Interface n | 14:1b:b6:23:6 o:1(802.11b/ | 0 removed f g) | rom Base Radio | MAC : 00:0b:85 | :5b:fb:d0 | |
| | 16 Wed Dec 12 12:37:18 2007 | Rogue AP : Interface n | 00:12:d9:e2:b o:0(802.11a) | 9:20 detecte with RSSI: -8 | d on Base Radio 3 and SNR: 8 | MAC : 00:0b:8 | 5:51:5a:e0 | - |
| × Discussions • 🗇 🔁 🗐 🖗 | 0 10 10 11 ØDiscus | sions not available on | http://10.77.244 | 204/ | | | | 8) |
| Done Done | | | | | | | | Internet |

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
- <u>Guia de configuração do Cisco Wireless LAN Controller Release 4.0 Configurando soluções</u> 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
- <u>Conectividade deTroubleshooting em uma Rede Wireless LAN</u>
- Exemplos de configuração de autenticação em controladores de LAN sem fio
- <u>Suporte Técnico e Documentação Cisco Systems</u>