Contenu

Introduction

Ce document décrit les stratégies *de confiance de* protection sans fil *AP* sur un contrôleur LAN Sans fil (WLC), définit des stratégies de confiance AP, et fournit une brève description de toutes les stratégies de confiance AP.

Conditions préalables

Conditions requises

Assurez-vous que vous avez une compréhension de base des paramètres de Sécurité LAN Sans fil (tels que le SSID, cryptage, authentification, et ainsi de suite).

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Stratégies de confiance AP

Les stratégies de confiance AP est une fonctionnalité de sécurité dans le contrôleur qui est conçu pour être utilisé dans les scénarios où les clients ont un réseau autonome parallèle AP avec le contrôleur. Dans ce scénario, AP autonome peut être marqué comme AP de confiance sur le contrôleur, et l'utilisateur peut définir des stratégies pour ces derniers aps de confiance (qui devraient utiliser seulement le WEP ou le WPA, notre propre SSID, préambule court, et ainsi de suite). Si l'un de ces échouer AP pour rencontrer ces stratégies, le contrôleur donne une alarme au périphérique de Gestion de réseau (système de contrôle sans fil) ce des états AP de confiance a violé une stratégie configurée.

Quel est AP de confiance ?

Les aps de confiance sont les aps qui ne sont pas une partie d'une organisation. Cependant, ils

n'entraînent pas une menace de Sécurité pour le réseau. Ces aps s'appellent également les aps amicaux. Plusieurs scénarios existent où vous pourriez vouloir configurer AP comme AP de confiance.

Par exemple, vous pourriez avoir des catégories différentes d'aps dans votre réseau comme :

- **Aps que vous possédez qui n'exécutent pas LWAPP (peut-être ils exécutent l'IOS ou le VxWorks)**
- LWAPP aps lequel les employés apportent (avec la connaissance de l'administrateur)
- LWAPP aps utilisé pour tester le réseau existant
- LWAPP aps ces des voisins possèdent

Normalement, les aps de confiance sont les aps qui se rangent dans la **catégorie 1**, qui sont les aps que vous possédez qui n'exécutent pas LWAPP. Ils pourraient être les vieux aps qui exécutent VxWorks ou IOS. Afin de s'assurer que ces aps n'endommagent pas le réseau, certaines caractéristiques peuvent être imposées, comme le SSID correct et les authentications-type. Configurez les stratégies de confiance AP sur le WLC, et assurez-vous que les aps de confiance rencontrent ces stratégies. Sinon, vous pouvez configurer le contrôleur pour prendre plusieurs mesures, telles que l'augmenter une alarme au périphérique de Gestion de réseau (WCS).

Des aps connus qui appartiennent aux voisins peuvent être configurés en tant qu'aps de confiance.

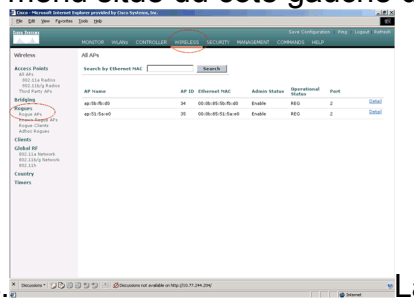
Normalement, MFP (Management Frame Protection) devrait empêcher les aps qui ne sont pas LWAPP légitimes aps de joindre le WLC. Si les cartes NIC prennent en charge MFP, on ne leur permet pas pour recevoir des deauthentications des périphériques autres que les vrais aps. Référez-vous au Management Frame Protection d'infrastructure (MFP) avec WLC et ENROULEZ l'exemple de configuration pour plus d'informations sur MFP.

Si vous avez les aps qui exécutent VxWorks ou IOS (comme dans catégorie 1), ils ne joindront jamais le groupe LWAPP ou feront MFP, mais vous pourraient vouloir imposer les stratégies répertoriées à cette page. En pareil cas, des stratégies de confiance AP doit être configurées sur le contrôleur pour les aps d'intérêt.

Généralement si vous savez un escroc AP et identifiez que ce n'est pas une menace pour votre réseau, vous pouvez identifier qu'AP comme AP de confiance connu.

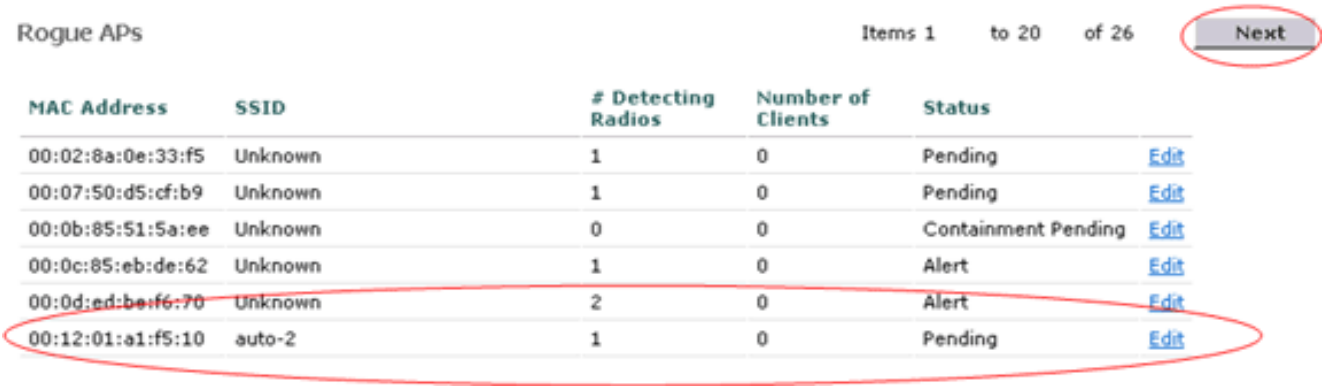
Comment configurer AP comme AP de confiance du GUI WLC ?

Terminez-vous ces étapes afin de configurer AP comme AP de confiance :

1. Connectez-vous dans le GUI du WLC par le HTTP ou les https ouvrent une session.
2. Du menu principal de contrôleur, **radio de** clic.
3. Dans le menu situé du côté gauche de la page theWireless, clic **aps escrocs.**  La page de l'escroc aps répertorie tous les aps qui sont

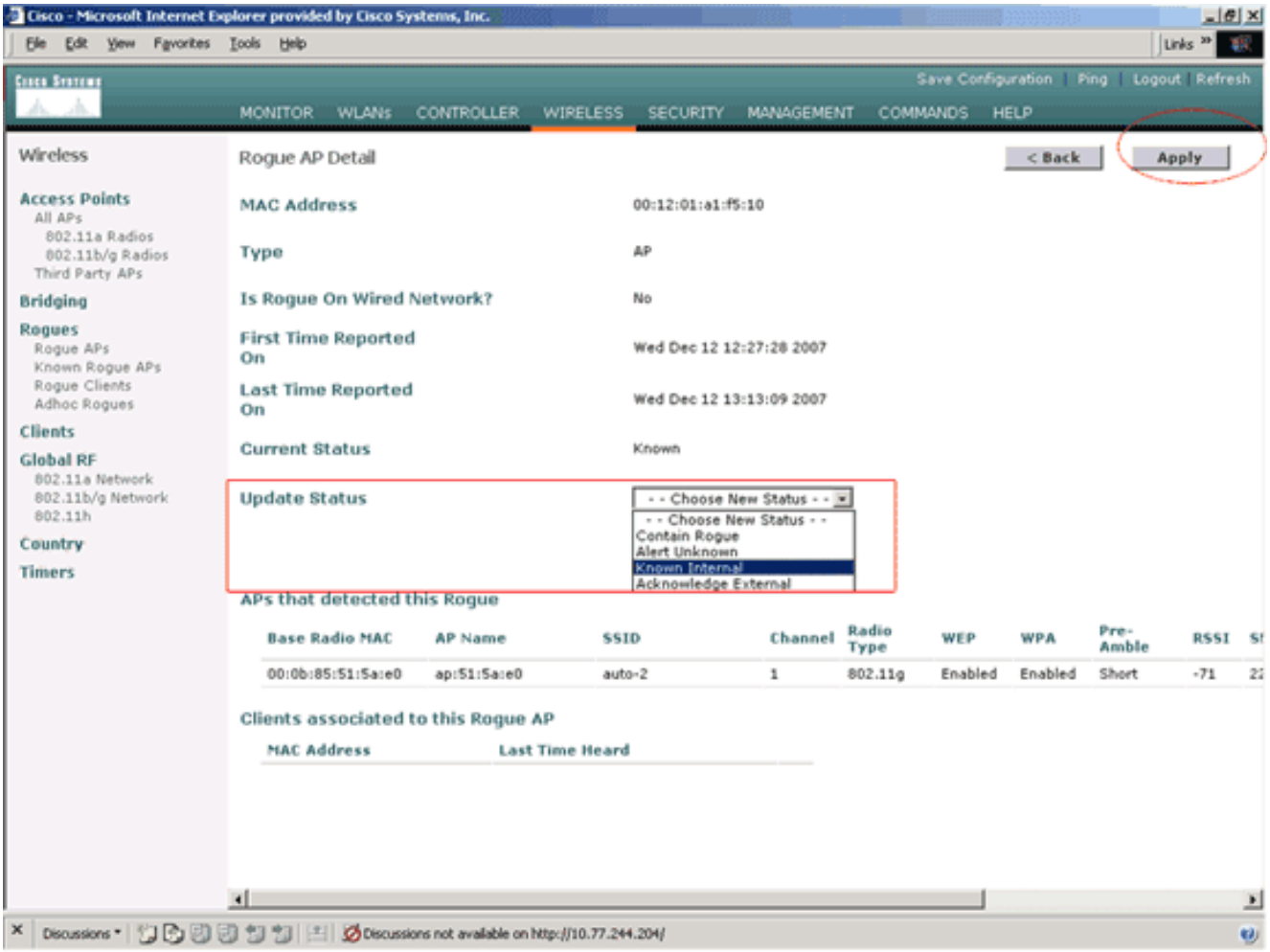
détectés comme escroc aps sur le réseau.

4. De cette liste de l'escroc aps, localisez AP que vous voulez configuré en tant qu'AP de confiance qui tombe sous la catégorie 1 (comme expliqué dans la section précédente).Vous pouvez localiser les aps avec les adresses MAC répertoriées sur la page escroc aps. Si AP désiré n'est pas en cette page, cliquez sur Next afin d'identifier AP de la page suivante.
5. Une fois qu'AP désiré se trouve de la liste de l'escroc AP, cliquez sur le bouton d'**éditer** qui correspond à AP, qui vous porte à la page de détail d'AP.



Dans les petits groupes page de l'escroc AP, vous pouvez trouver les informations détaillées au sujet de cet AP (comme si cet AP connecté au réseau câblé, aussi bien que l'état actuel d'AP et ainsi de suite).

6. Afin de configurer cet AP comme AP de confiance, sélectionnez **interne connu de la** liste déroulante d'état de mise à jour, et cliquez sur Apply.Quand vous mettez à jour l'état AP à *interne connu*, cet AP est configuré comme AP de confiance de ce réseau.

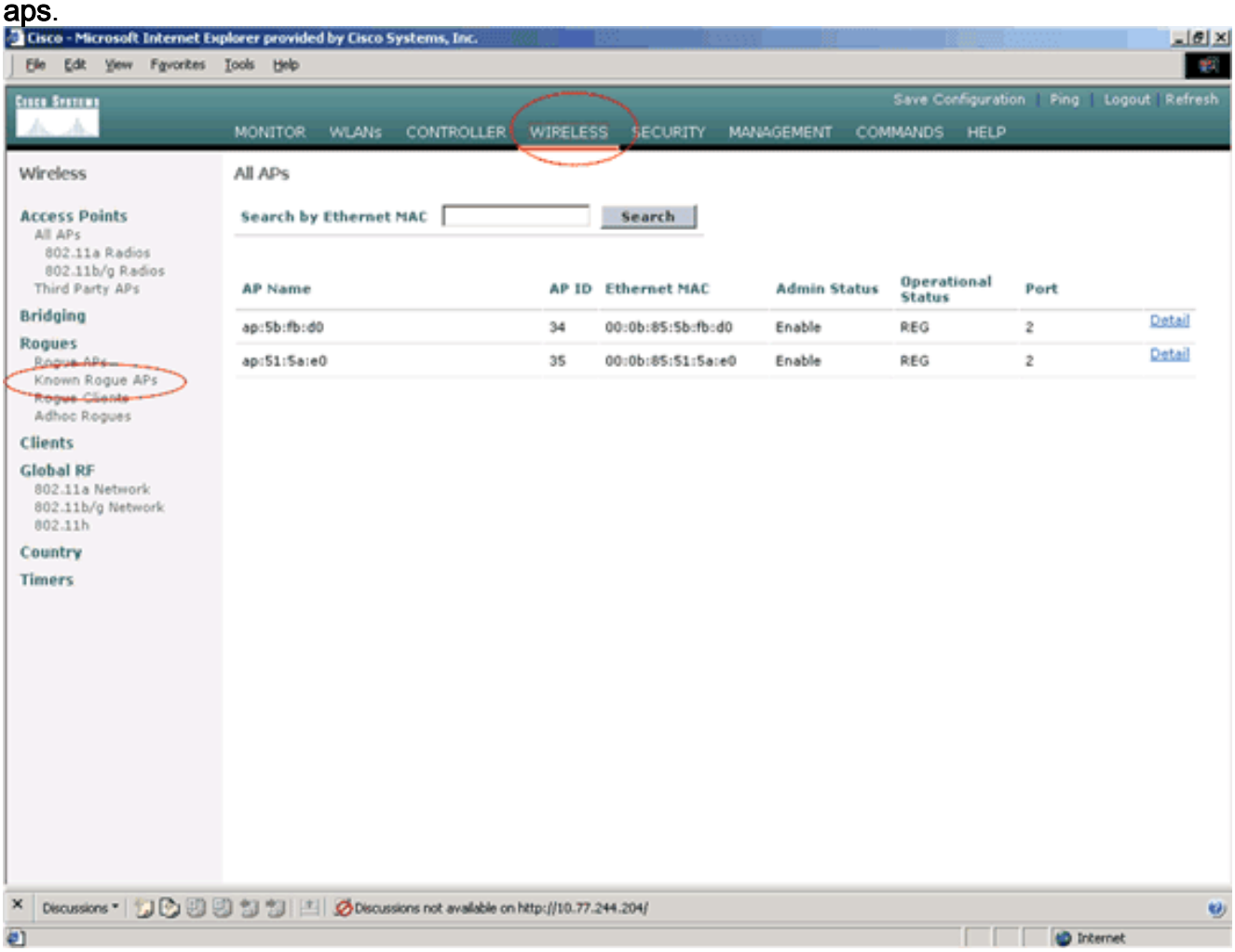


7. Répétez ces étapes pour tous les aps que vous voulez configurer en tant qu'aps de confiance.

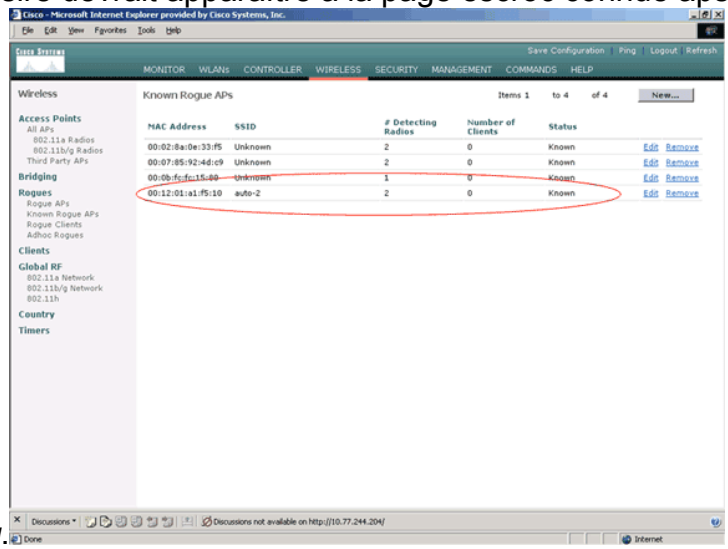
Vérifiez la configuration de confiance AP

Terminez-vous ces étapes afin de vérifier qu'AP est correctement configuré en tant qu'AP de confiance du GUI de contrôleur :

1. **Radio de** clic.
2. Dans le menu situé du côté gauche de la page theWireless, **escroc connu par** clic **aps**.



AP désiré devrait apparaître à la page escroc connue aps avec l'état répertorié comme *connu*.



Compréhension des paramètres de la stratégie de confiance AP

Le WLC a ces stratégies de confiance AP :

- Stratégie de chiffrement imposée
- Stratégie imposée de préambule
- Stratégie par radio imposée de type
- Validez le SSID
- Alerte si AP de confiance manque
- Délai d'attente d'expiration pour les entrées de confiance AP (secondes)

Stratégie de chiffrement imposée

Cette stratégie est utilisée pour définir le type de cryptage qu'AP de confiance devrait utiliser. Vous pouvez configurer l'un de ces types de cryptage dans le cadre de la stratégie de chiffrement imposée :

- Aucun
- Ouvrez-vous
- WEP
- WPA/802.11i

Le WLC vérifie si le type de cryptage configuré sur AP de confiance apparie le type de cryptage configuré sur la configuration « de **stratégie de chiffrement imposée** ». Si AP de confiance n'utilise pas le type indiqué de cryptage, le WLC donne une alarme au système de gestion afin d'agir des mesures appropriées.

Stratégie imposée de préambule

Le préambule par radio (parfois appelé une en-tête) est une section de données à la tête d'un paquet qui contient les informations dont les périphériques sans fil ont besoin quand ils envoient et reçoivent des paquets. Les préambules **courts** améliorent la représentation de débit, ainsi ils sont activés par défaut. Cependant, quelques périphériques sans fil, tels que des téléphones de SpectraLink NetLink, exigent de **longs** préambules. Vous pouvez configurer l'un de ces options de préambule dans le cadre de la stratégie imposée de préambule :

- Aucun
- Short
- Long

Le WLC vérifie si le type de préambule configuré sur AP de confiance apparie le type de préambule configuré sur la configuration « de **stratégie imposée de préambule** ». Si AP de confiance n'utilise pas le type spécifié de préambule, le WLC donne une alarme au système de gestion afin d'agir des mesures appropriées.

Stratégie par radio imposée de type

Cette stratégie est utilisée pour définir le type par radio qu'AP de confiance devrait utiliser. Vous pouvez configurer l'un de ces types de radio dans le cadre de la stratégie par radio imposée de type :

- Aucun
- 802.11b seulement
- 802.11a seulement
- 802.11b/g seulement

Le WLC vérifie si le type par radio configuré sur AP de confiance apparie le type par radio configuré sur la configuration « de **stratégie par radio imposée de type** ». Si l'utilisation de confiance d'APdoes pas les radios spécifiées, le WLC donne une alarme au système de gestion afin d'agir des mesures appropriées.

Validez le SSID

Vous pouvez configurer le contrôleur pour valider aps de confiance SSID contre le SSID configuré sur le contrôleur. Si les aps de confiance SSID apparie un du contrôleur SSID, le contrôleur donne une alarme.

Alerte si AP de confiance manque

Si cette stratégie est activée, le WLC alerte le système de gestion si AP de confiance manque de la liste connue de l'escroc aps.

Délai d'attente d'expiration pour les entrées de confiance AP (secondes)

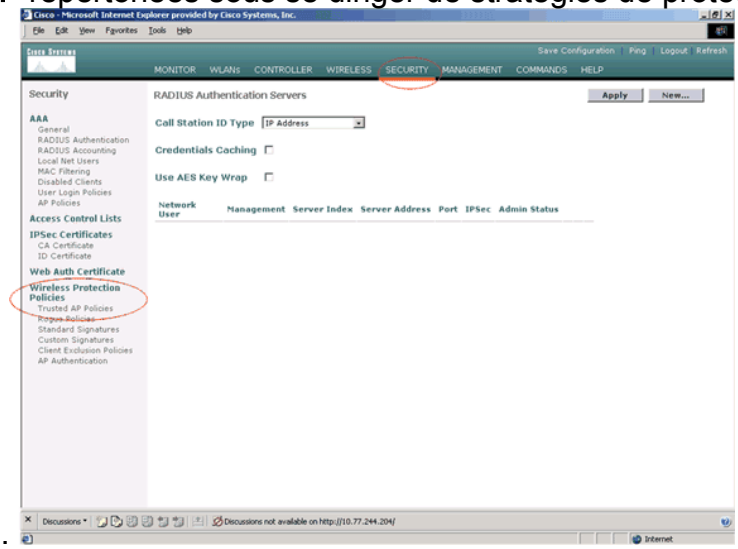
Cette valeur du dépassement de durée d'expiration spécifie le nombre de secondes avant AP de confiance est considérée expiré et vidé de l'entrée WLC. Vous pouvez spécifier cette valeur du dépassement de durée en quelques secondes (120 - 3600 secondes).

Comment configurer a fait confiance à des stratégies AP sur le WLC ?

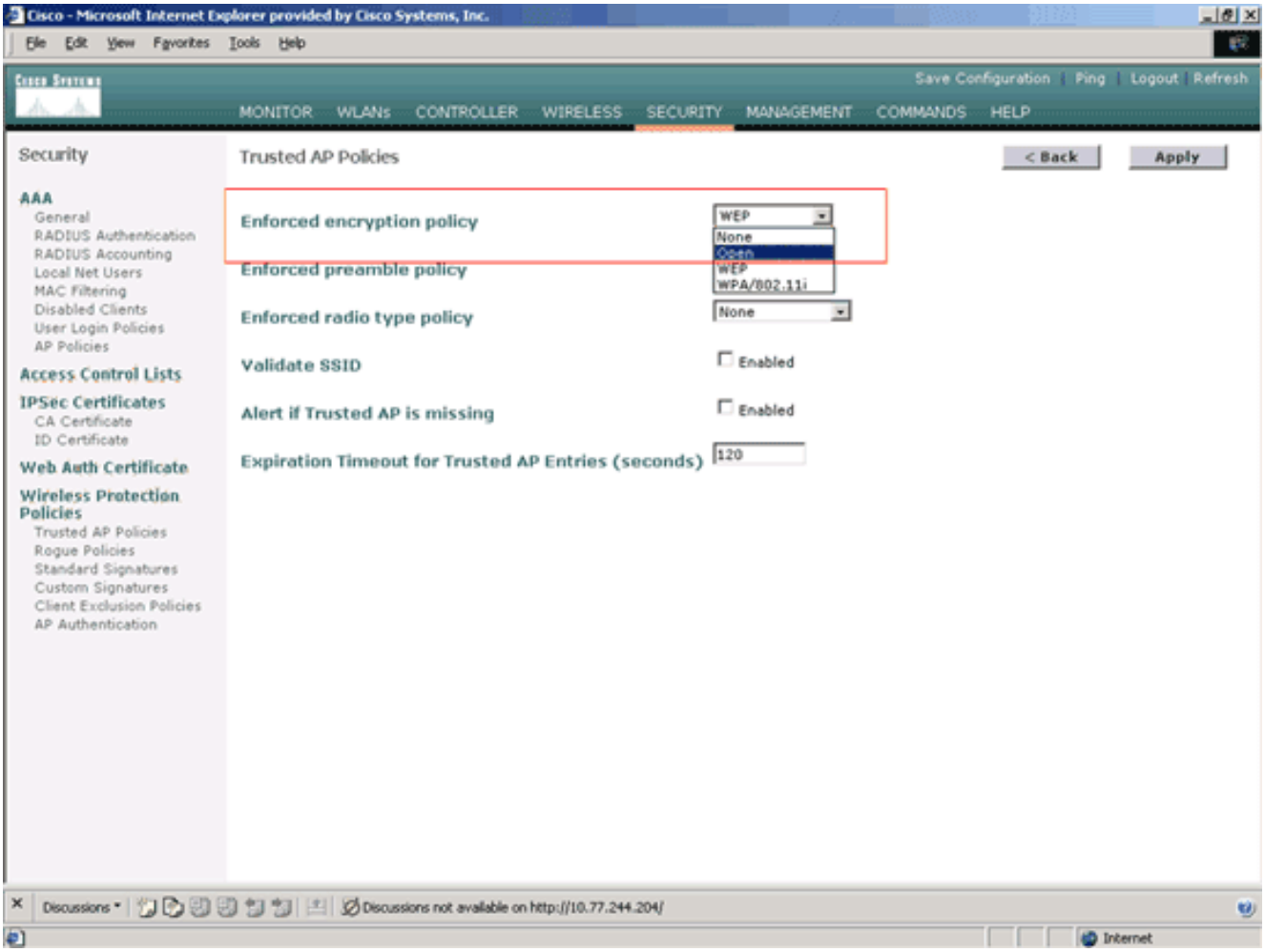
Terminez-vous ces étapes afin de configurer des stratégies de confiance AP sur le WLC par le GUI :

Remarque: Toutes les stratégies de confiance AP résident à la même page WLC.

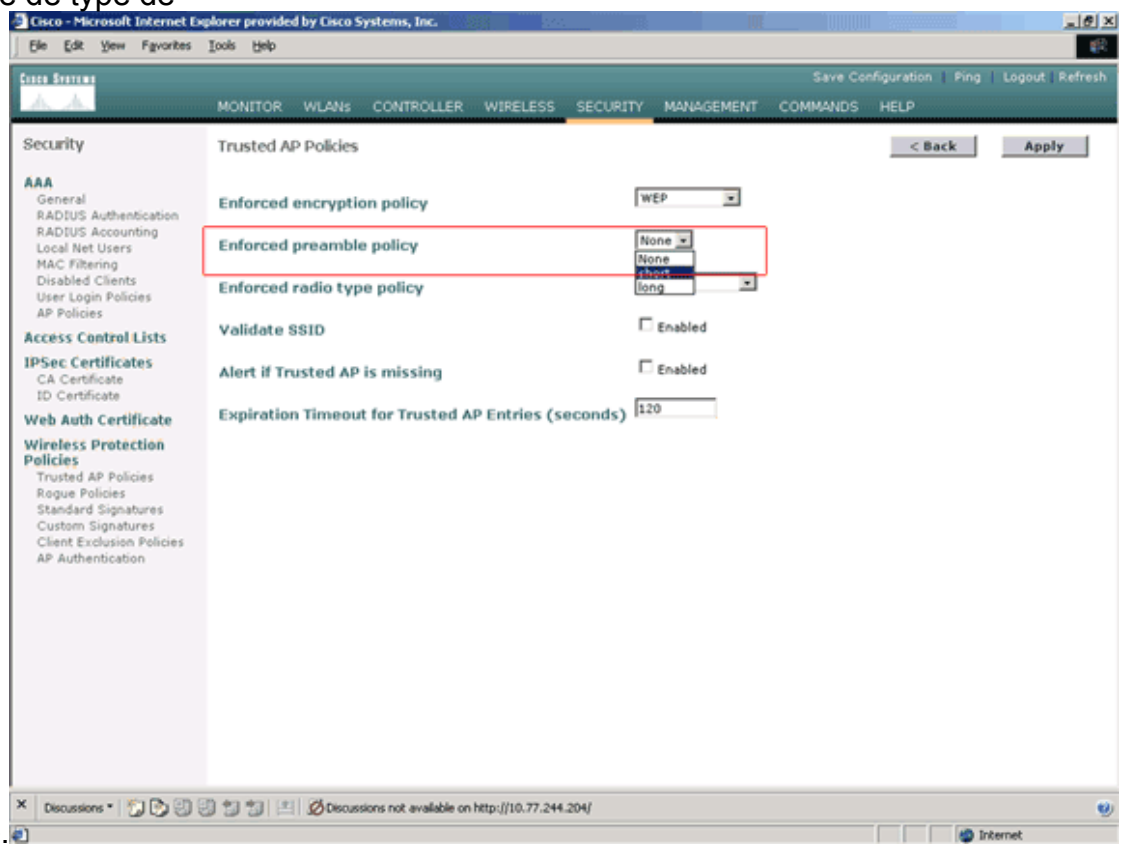
1. Du menu principal GUI WLC, cliquez sur Security.
2. Du menu situé du côté gauche de la page de Sécurité, le clic **a fait confiance à des stratégies AP** répertoriées sous se diriger de stratégies de protection sans fil.



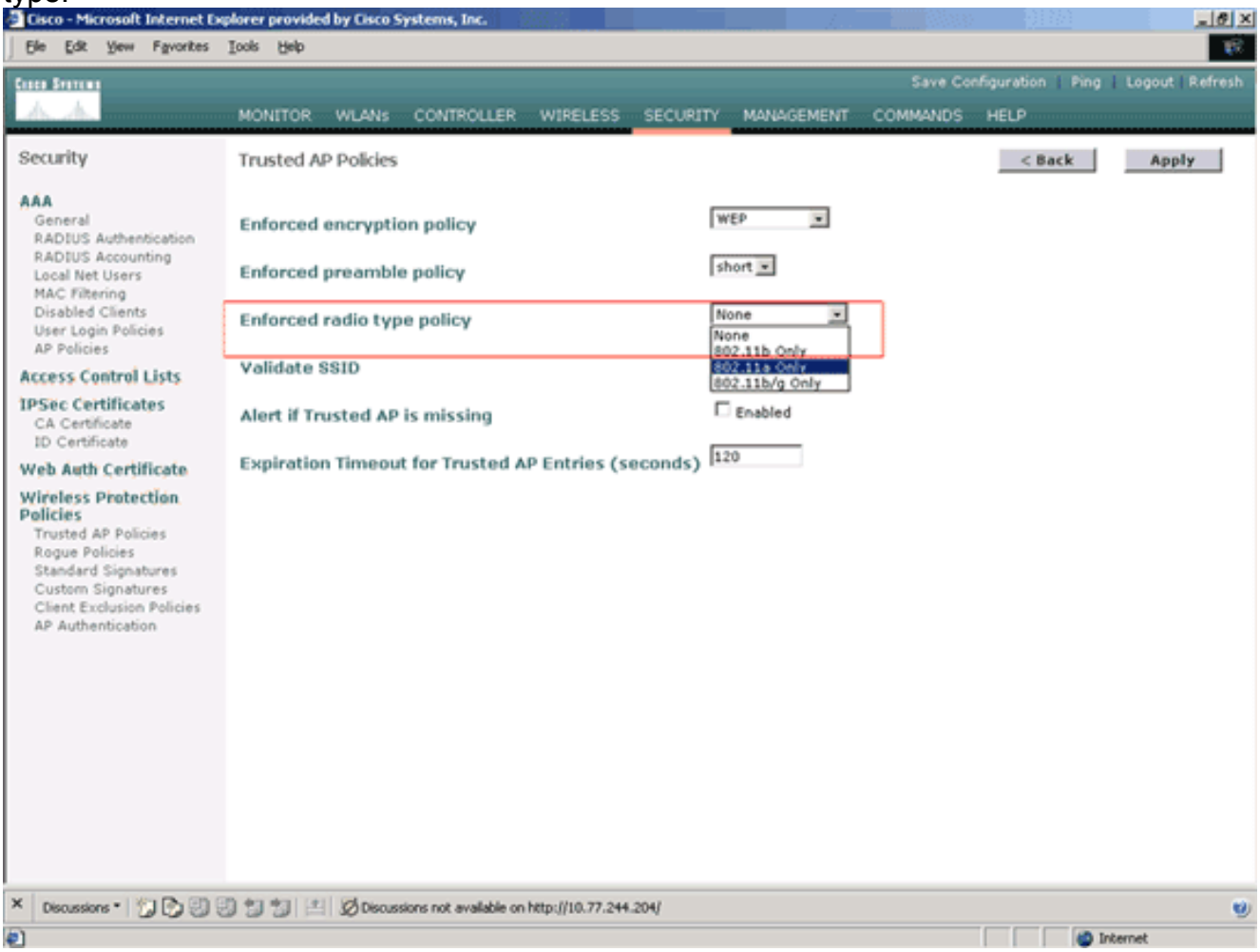
3. Sur AP de confiance les stratégies paginent, sélectionnent le type désiré de cryptage (aucune, ne s'ouvre, WEP, WPA/802.11i) de la liste déroulante imposée de stratégie de chiffrement.



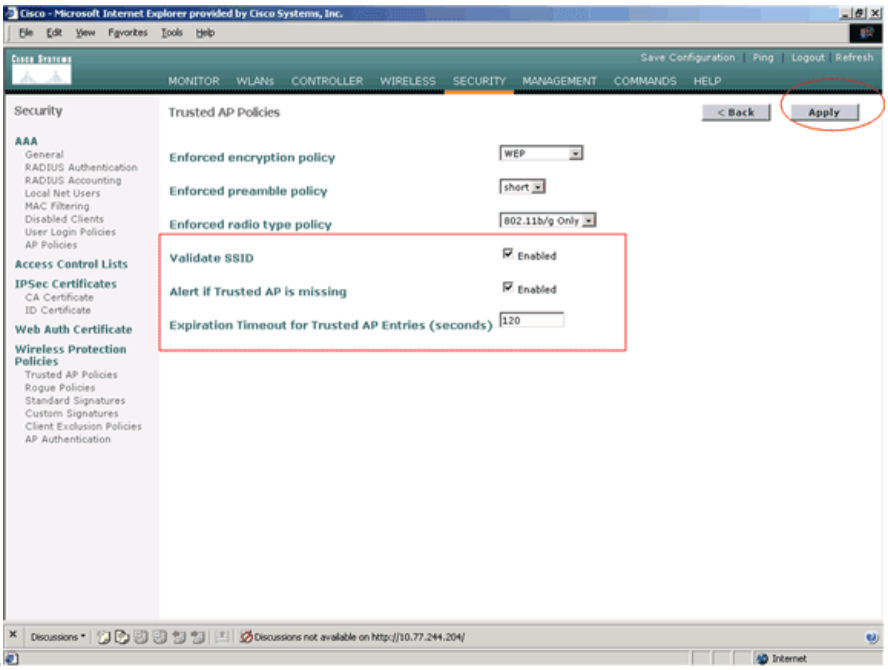
4. Sélectionnez le type désiré de préambule (aucun, court, long) de la liste déroulante imposée de stratégie de type de préambule.



5. Sélectionnez le type par radio désiré (aucun, 802.11b seulement, 802.11a seulement, 802.11b/g seulement) de la liste déroulante par radio imposée de stratégie de type.



6. Cochez ou décochez la case **activée par SSID de validation** afin d'activer ou désactiver la configuration de la validation SSID.
7. Cochez ou décochez l'**alerte si AP de confiance est** case **activée manquante** afin d'activer ou désactiver l'alerte si AP de confiance est configuration manquante.
8. Écrivez une valeur (en quelques secondes) pour le **délai d'attente d'expiration pour l'**option **de confiance d'entrées**



AP.

9. Cliquez sur **Apply**.

Remarque: Afin de configurer ces configurations du WLC CLI, vous pouvez utiliser la commande des **wps faire confiance-AP de config** avec l'option appropriée de stratégie.

```
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.
```

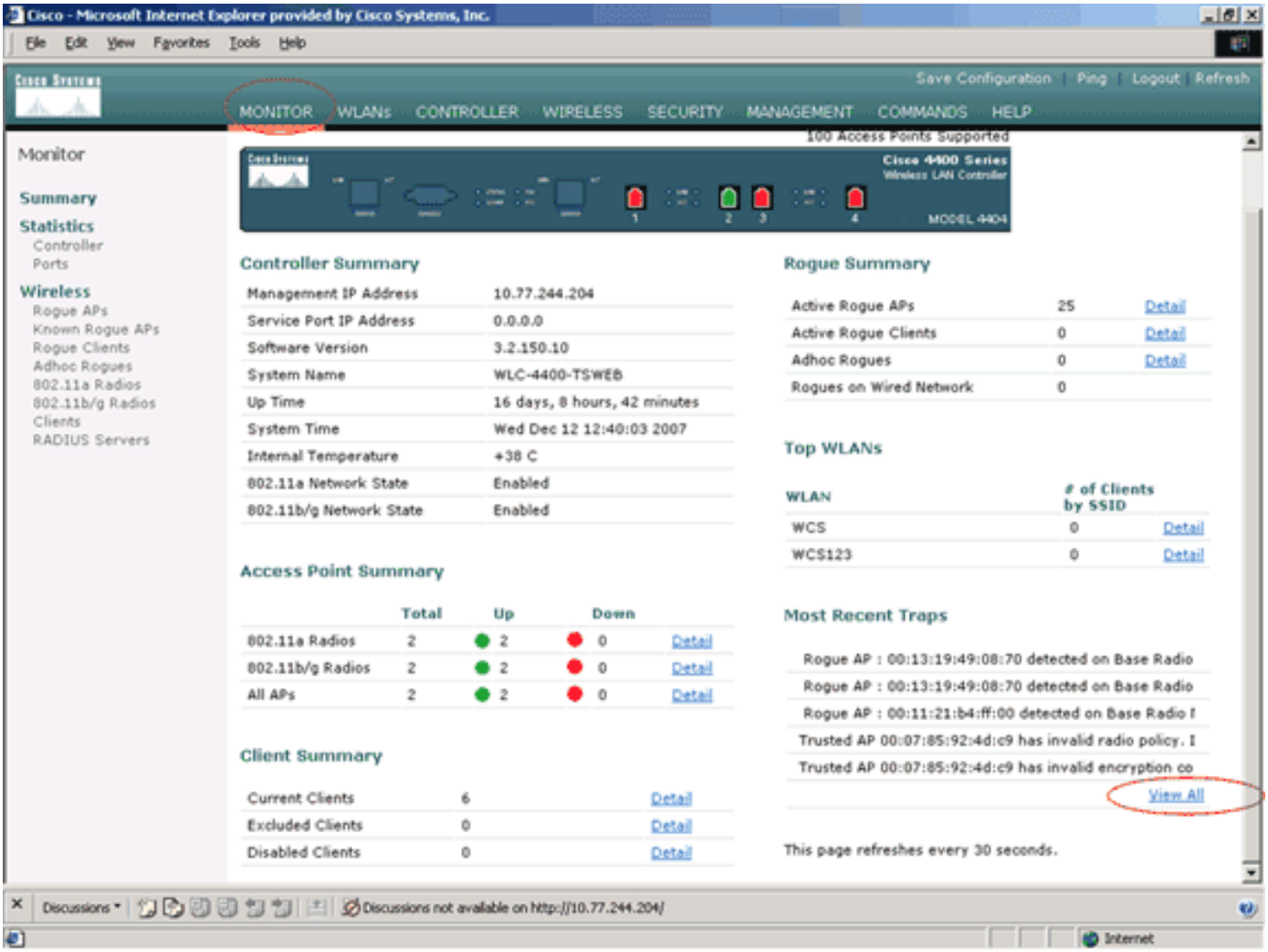
Message d'alerte de confiance de violation de stratégie AP

Voici un exemple du message d'alerte de confiance de violation de stratégie AP affiché par le contrôleur.

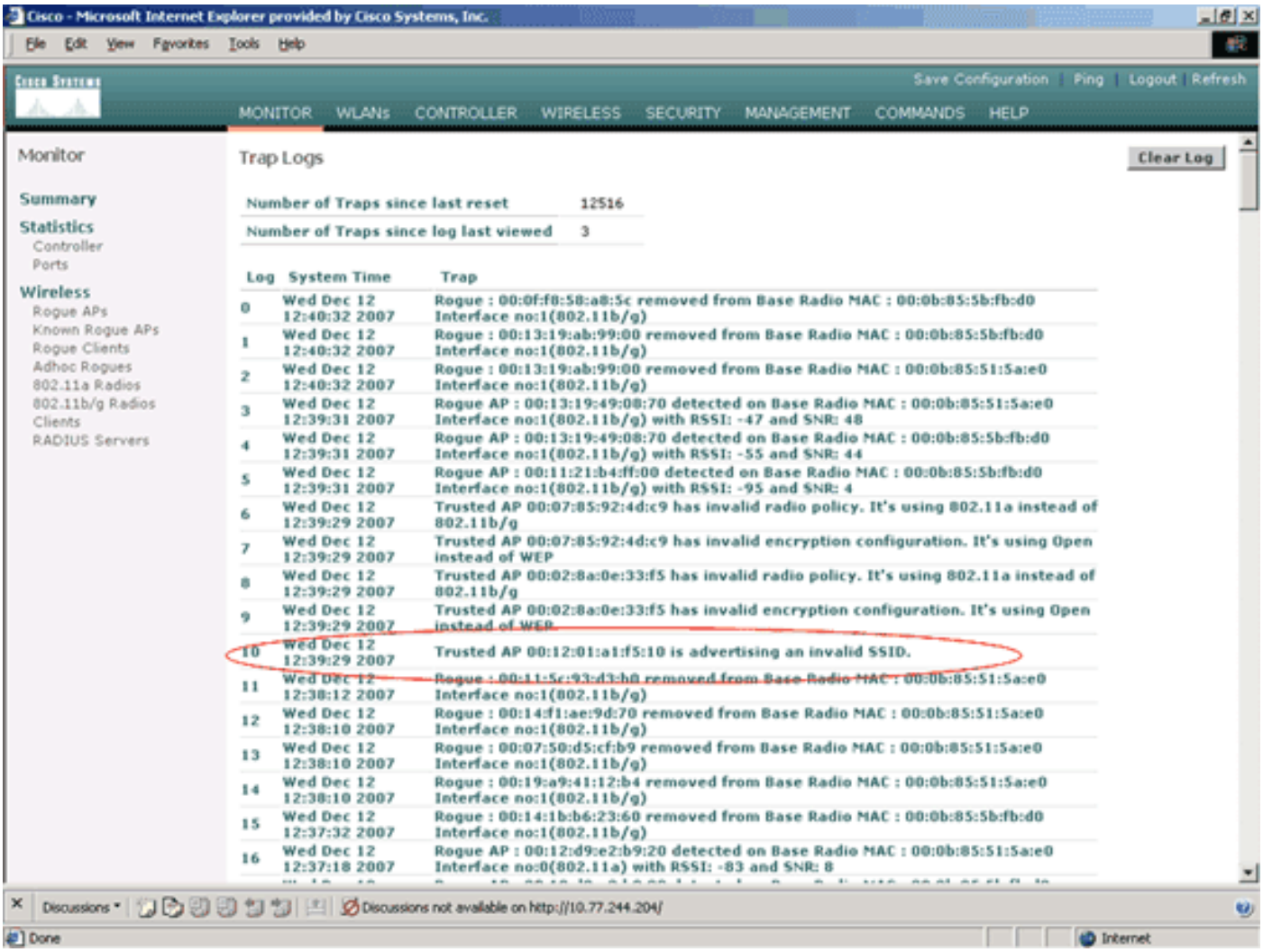
```
Thu Nov 16 12:39:12 2006  [WARNING] apf_rogue.c 1905: Possible APimpersonation of xx:xx:xx:xx:xx:xx, using source address of00:16:35:9e:6f:3a, detected by 00:17:df:7d:e1:70 on slot 0 Thu Nov 16 12:39:12 2006  [SECURITY] apf_rogue.c 1490: Trusted AP Policyfailed for AP xx:xx:xx:xx:xx:xx - invalid SSID 'SSID1'Thu Nov 16 12:39:12 2006  [SECURITY] apf_rogue.c 1457: Trusted AP Policyfailed for AP xx:xx:xx:xx:xx:xx - invalid encryption typeThu Nov 16 12:39:12 2006  Previous message occurred 6 times
```

Notez les messages d'erreur mis en valeur ici. Ces messages d'erreur indiquent que le SSID et le type de cryptage configurés sur AP de confiance n'apparient pas le paramètre de la stratégie de confiance AP.

Le même message d'alerte peut être vu du GUI WLC. Afin de visualiser ce message, allez au menu principal GUI WLC, et to cliquer sur Monitor. Dans la section de déroutements la plus récente de la page de moniteur, **vue toute de** clic afin de visualiser toutes les alertes récentes sur le WLC.



Sur les déroutements les plus récents page, vous pouvez identifier le contrôleur qui génère le message d'alerte de confiance de violation de stratégie AP suivant les indications de cette image :



Informations connexes

- Guide de configuration Sans fil de contrôleur LAN de Cisco, version 5.2 - Activation de la détection de Point d'accès de fard à joues dans des groupes rf
- Guide de configuration Sans fil de contrôleur LAN de Cisco, version 4.0 - Configuration des solutions de sécurité
- Détection de systèmes indésirables sous des réseaux sans fil unifiés
- Guide de conception et de déploiement des téléphones SpectraLink
- Exemple de configuration de connexion LAN sans fil de base
- Résolution des problèmes de connectivité dans un réseau LAN sans fil
- Exemples de configuration de l'authentification sur des contrôleurs de réseau local sans fil
- Support et documentation techniques - Cisco Systems