Stratégies AP de confiance sur un contrôleur de réseau local sans fil

Contenu

Introduction

Ce document décrit les stratégies de protection sans fil des *points d'accès approuvés* sur un contrôleur de réseau local sans fil (WLC), définit les stratégies de points d'accès approuvés et fournit une brève description de toutes les stratégies de points d'accès approuvés.

Conditions préalables

Conditions requises

Assurez-vous d'avoir une compréhension de base des paramètres de sécurité du LAN sans fil (tels que le SSID, le chiffrement, l'authentification, etc.).

Conventions

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

Stratégies de points d'accès fiables

Les politiques de points d'accès fiables sont une fonctionnalité de sécurité du contrôleur qui est conçue pour être utilisée dans des scénarios où les clients ont un réseau AP autonome parallèle avec le contrôleur. Dans ce scénario, l'AP autonome peut être marqué comme l'AP approuvé sur le contrôleur, et l'utilisateur peut définir des stratégies pour ces AP approuvés (qui devraient

utiliser uniquement WEP ou WPA, notre propre SSID, un préambule court, etc.). Si l'un de ces points d'accès ne respecte pas ces stratégies, le contrôleur déclenche une alarme au périphérique de gestion du réseau (Wireless Control System) qui indique qu'un point d'accès approuvé a violé une stratégie configurée.

Qu'est-ce qu'un point d'accès approuvé ?

Les AP approuvés sont des AP qui ne font pas partie d'une organisation. Cependant, elles ne constituent pas une menace pour la sécurité du réseau. Ces points d'accès sont également appelés points d'accès conviviaux. Il existe plusieurs scénarios dans lesquels vous pouvez vouloir configurer un AP comme un AP approuvé.

Par exemple, vous pouvez avoir différentes catégories de points d'accès dans votre réseau, telles que :

- **AP que vous possédez qui n'exécutent pas LWAPP (peut-être qu'ils exécutent IOS ou VxWorks)**
- AP LWAPP que les employés apportent (avec la connaissance de l'administrateur)
- AP LWAPP utilisés pour tester le réseau existant
- AP LWAPP dont les voisins sont propriétaires

Normalement, les AP approuvés sont des AP qui appartiennent à **la catégorie 1**, qui sont des AP que vous possédez et qui n'exécutent pas LWAPP. Il peut s'agir d'anciens AP qui exécutent VxWorks ou IOS. Afin de s'assurer que ces points d'accès n'endommagent pas le réseau, certaines fonctionnalités peuvent être appliquées, telles que les SSID corrects et les types d'authentification. Configurez les stratégies AP approuvées sur le WLC, et assurez-vous que les AP approuvés respectent ces stratégies. Si ce n'est pas le cas, vous pouvez configurer le contrôleur pour qu'il prenne plusieurs actions, par exemple déclencher une alarme sur le périphérique de gestion du réseau (WCS).

Les AP connus qui appartiennent aux voisins peuvent être configurés en tant qu'AP approuvés.

Normalement, MFP (Management Frame Protection) doit empêcher les AP qui ne sont pas des AP LWAPP légitimes de rejoindre le WLC. Si les cartes NIC prennent en charge la fonction MFP, elles ne sont pas autorisées à accepter les déauthentifications d'autres périphériques que les points d'accès réels. Référez-vous à Exemple de configuration de MFP (Infrastructure Management Frame Protection) avec WLC et LAP pour plus d'informations sur MFP.

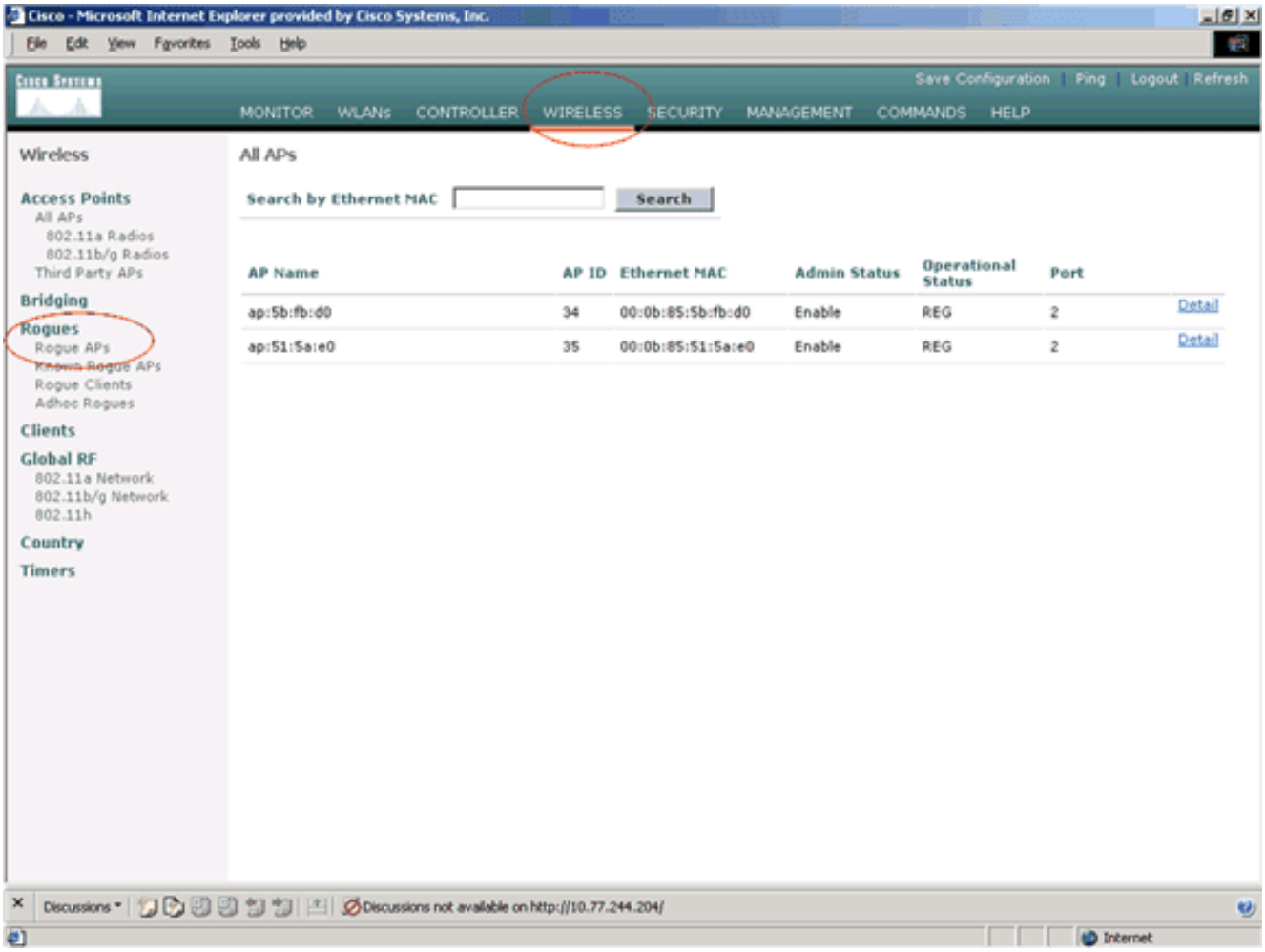
Si vous avez des points d'accès qui exécutent VxWorks ou IOS (comme dans la catégorie 1), ils ne se joindront jamais au groupe LWAPP ou font MFP, mais vous pouvez vouloir appliquer les stratégies répertoriées sur cette page. Dans de tels cas, les stratégies AP fiables doivent être configurées sur le contrôleur pour les AP concernés.

En général, si vous connaissez un point d'accès non autorisé et que vous identifiez qu'il ne représente pas une menace pour votre réseau, vous pouvez identifier ce point d'accès en tant que point d'accès de confiance connu.

Comment configurer un AP en tant qu'AP de confiance à partir de l'interface graphique du WLC ?

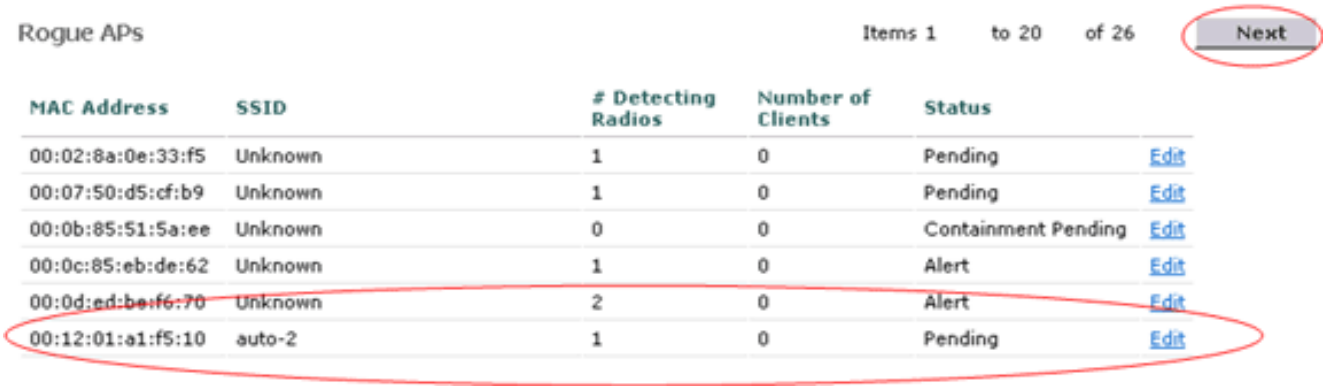
Complétez ces étapes afin de configurer un point d'accès comme point d'accès de confiance :

1. Connectez-vous à l'interface utilisateur graphique du WLC via HTTP ou https login.
2. Dans le menu principal du contrôleur, cliquez sur **Sans fil**.
3. Dans le menu situé à gauche de la page Wireless, cliquez sur **Rogue APs**.



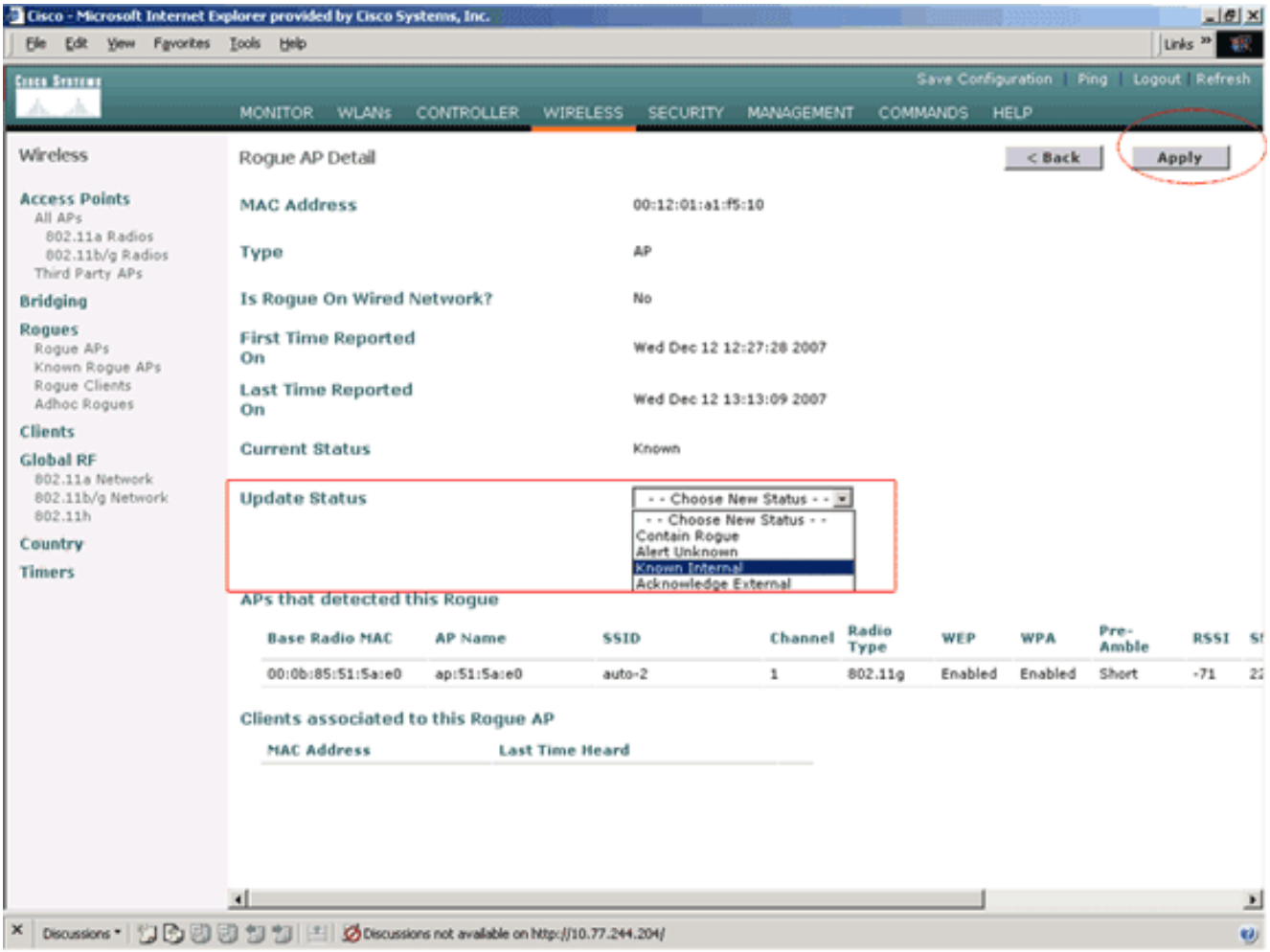
La page Rogue APs répertorie tous les AP qui sont détectés comme AP non autorisés sur le réseau.

4. Àpartir de cette liste de points d'accès non autorisés, localisez le point d'accès que vous voulez configurer comme point d'accès approuvé qui tombe dans la catégorie 1 (comme expliqué dans la section précédente).Vous pouvez localiser les points d'accès avec les adresses MAC répertoriées sur la page des points d'accès indésirables. Si le point d'accès souhaité ne figure pas dans cette page, cliquez sur **Suivant** afin d'identifier le point d'accès de la page suivante.
5. Une fois que le point d'accès souhaité est situé à partir de la liste des points d'accès indésirables, cliquez sur le bouton **Modifier** qui correspond au point d'accès, qui vous amène à la page de détails du point d'accès.



Dans la page Détails des points d'accès indésirables, vous pouvez trouver des informations détaillées sur ce point d'accès (par exemple si ce point d'accès est connecté au réseau câblé, ainsi que l'état actuel du point d'accès, etc.).

6. Afin de configurer ce point d'accès en tant qu'AP approuvé, sélectionnez **Interne connu** dans la liste déroulante État de mise à jour, puis cliquez sur **Appliquer**.Lorsque vous mettez à jour l'état du point d'accès sur *Interne connu*, ce point d'accès est configuré comme point d'accès de confiance de ce
réseau.

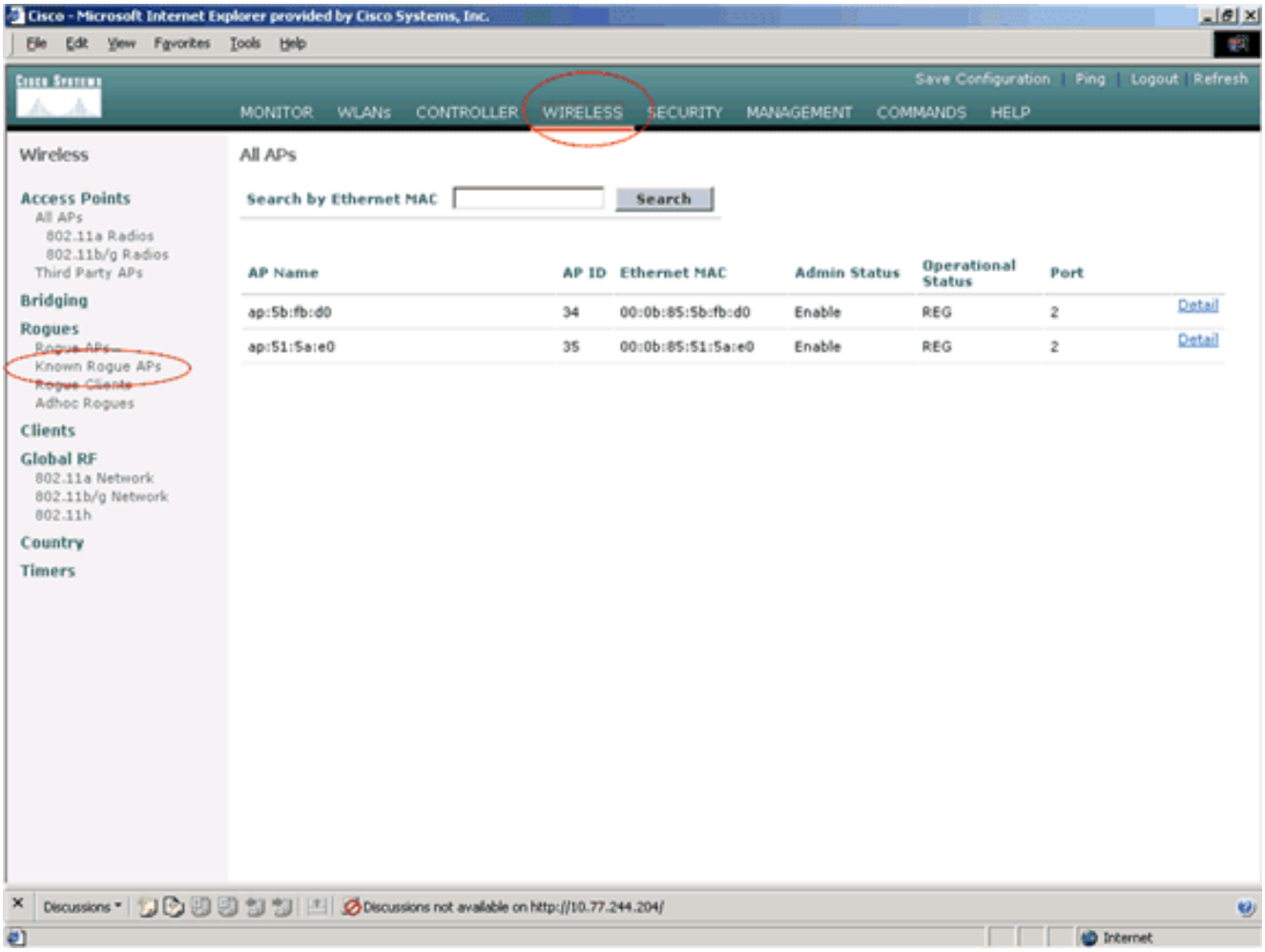


7. Répétez ces étapes pour tous les AP que vous voulez configurer en tant que AP approuvés.

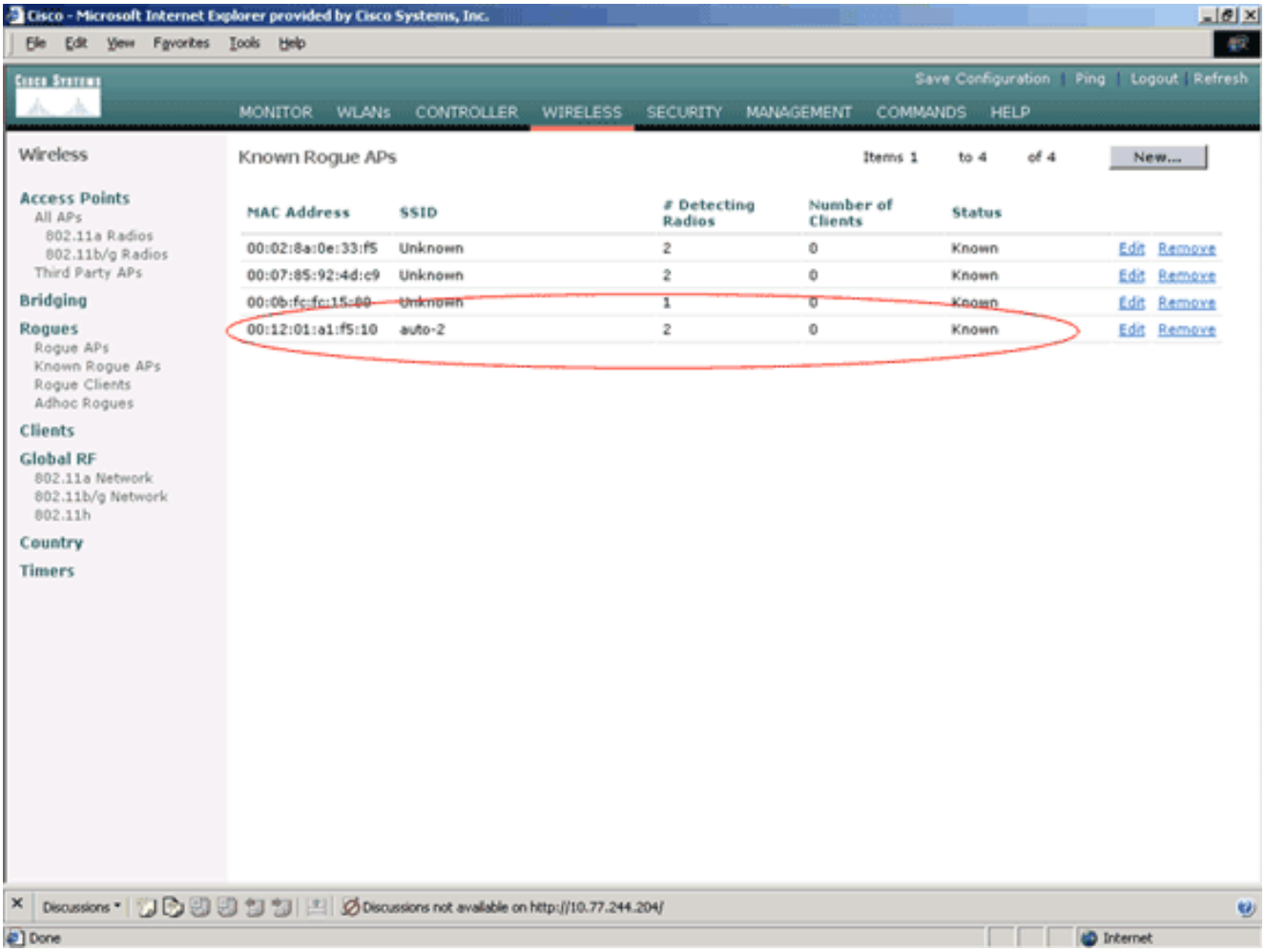
Vérifier la configuration du point d'accès approuvé

Complétez ces étapes afin de vérifier que le point d'accès est correctement configuré comme point d'accès approuvé à partir de l'interface graphique du contrôleur :

1. Cliquez sur **Sans fil**.
2. Dans le menu situé à gauche de la page Wireless, cliquez sur **Known Rogue APs**.



Le point d'accès souhaité doit apparaître sur la page des points d'accès non fiables connus avec l'état
Connu.



Présentation des paramètres de stratégie de point d'accès approuvé

Le WLC a ces stratégies AP approuvées :

- Stratégie de chiffrement appliquée
- Stratégie de préambule appliquée
- Stratégie de type de radio appliquée
- Valider le SSID
- Alerte si le point d'accès approuvé est manquant
- Expiration du délai d'expiration des entrées de point d'accès approuvé (secondes)

Stratégie de chiffrement appliquée

Cette stratégie est utilisée pour définir le type de chiffrement que le point d'accès approuvé doit utiliser. Vous pouvez configurer l'un de ces types de chiffrement sous Stratégie de chiffrement appliquée :

- Aucune
- Open (ouvert)
- WEP
- WPA/802.11i

Le WLC vérifie si le type de chiffrement configuré sur le point d'accès approuvé correspond au type de chiffrement configuré sur le paramètre **Stratégie de chiffrement appliquée**. Si le point d'accès approuvé n'utilise pas le type de chiffrement désigné, le WLC déclenche une alarme au

système de gestion afin d'entreprendre les actions appropriées.

Stratégie de préambule appliquée

Le préambule radio (parfois appelé en-tête) est une section de données située en tête d'un paquet qui contient les informations dont les périphériques sans fil ont besoin lorsqu'ils envoient et reçoivent des paquets. **Les** préambules **courts** améliorent les performances de débit, de sorte qu'ils sont activés par défaut. Cependant, certains périphériques sans fil, tels que les téléphones SpectraLink NetLink, nécessitent des préambules **longs**. Vous pouvez configurer l'une des options de préambule suivantes sous Stratégie de préambule appliquée :

- Aucune
- court
- Long

Le WLC vérifie si le type de préambule configuré sur le point d'accès approuvé correspond au type de préambule configuré sur le paramètre de **stratégie de préambule appliqué**. Si le point d'accès approuvé n'utilise pas le type de préambule spécifié, le WLC déclenche une alarme au système de gestion afin d'entreprendre les actions appropriées.

Stratégie de type de radio appliquée

Cette stratégie est utilisée pour définir le type de radio que le point d'accès approuvé doit utiliser. Vous pouvez configurer l'un de ces types de radio sous Stratégie de type de radio appliquée :

- Aucune
- 802.11b uniquement
- 802.11a uniquement
- 802.11b/g uniquement

Le WLC vérifie si le type de radio configuré sur le point d'accès approuvé correspond au type de radio configuré sur le paramètre **Stratégie de type de radio appliquée**. Si le point d'accès approuvé n'utilise pas les radios spécifiées, le WLC déclenche une alarme au système de gestion afin d'entreprendre les actions appropriées.

Valider le SSID

Vous pouvez configurer le contrôleur pour valider un SSID AP approuvé par rapport aux SSID configurés sur le contrôleur. Si le SSID des AP approuvés correspond à l'un des SSID du contrôleur, le contrôleur déclenche une alarme.

Alerte si le point d'accès approuvé est manquant

Si cette stratégie est activée, le WLC alerte le système de gestion si le point d'accès approuvé est absent de la liste des points d'accès non autorisés connus.

Expiration du délai d'attente pour les entrées de point d'accès fiables (secondes)

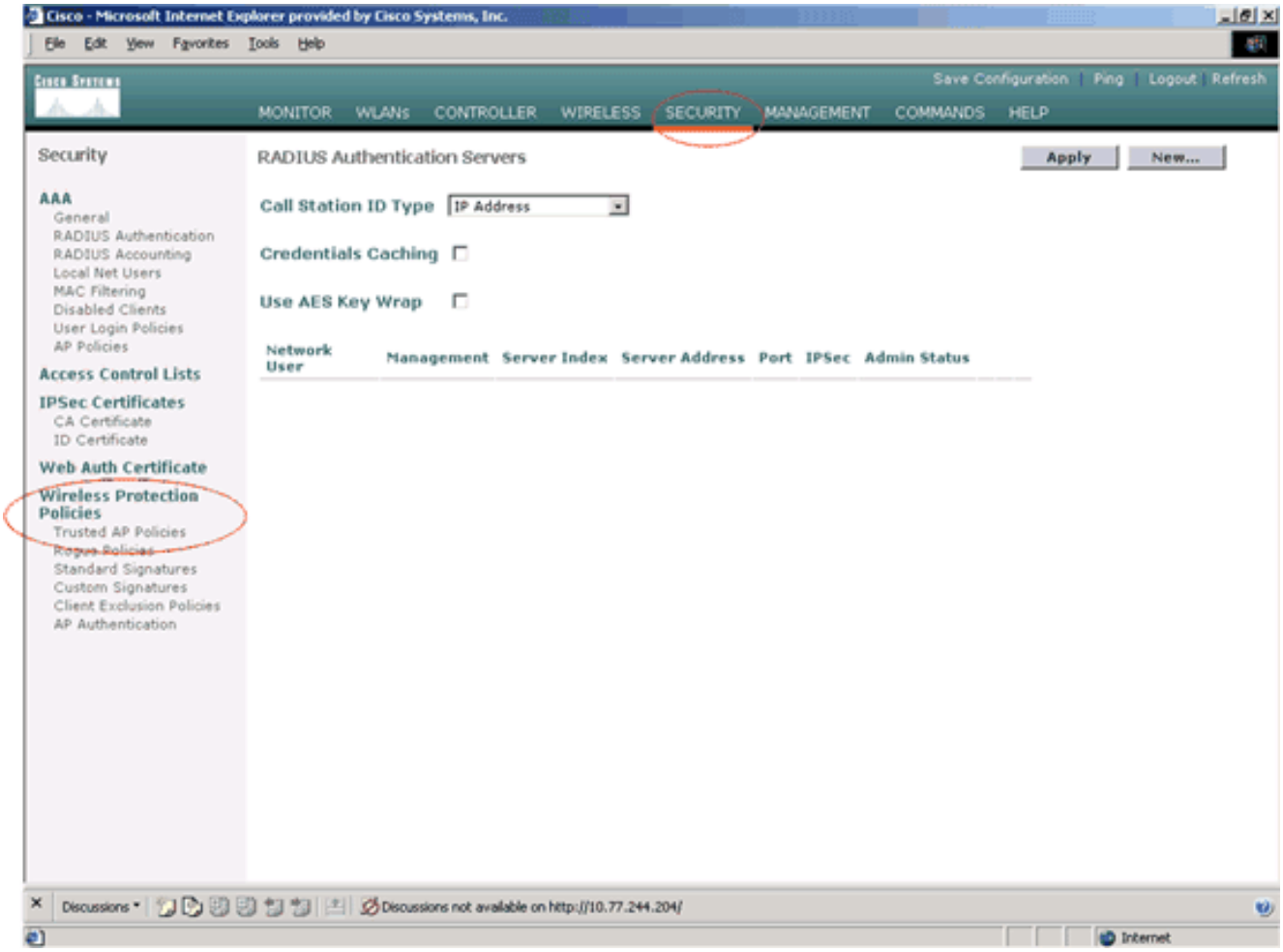
Cette valeur de délai d'expiration spécifie le nombre de secondes avant que le point d'accès approuvé soit considéré comme expiré et vidé de l'entrée du WLC. Vous pouvez spécifier cette valeur de délai d'attente en secondes (120 à 3 600 secondes).

Comment configurer les stratégies de points d'accès de confiance sur le WLC ?

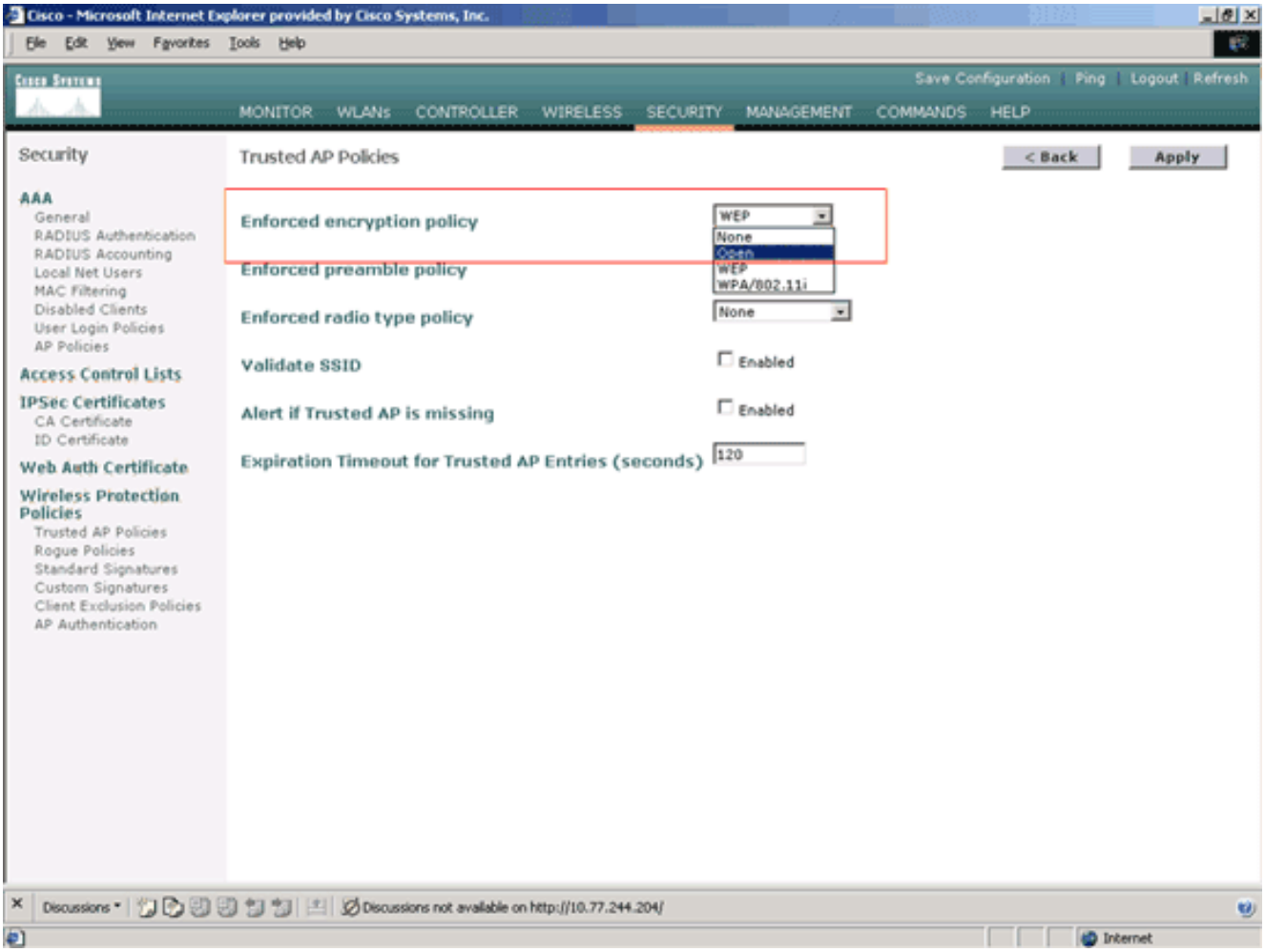
Complétez ces étapes afin de configurer des stratégies AP fiables sur le WLC via l'interface utilisateur graphique :

Remarque : Toutes les stratégies AP approuvées résident sur la même page WLC.

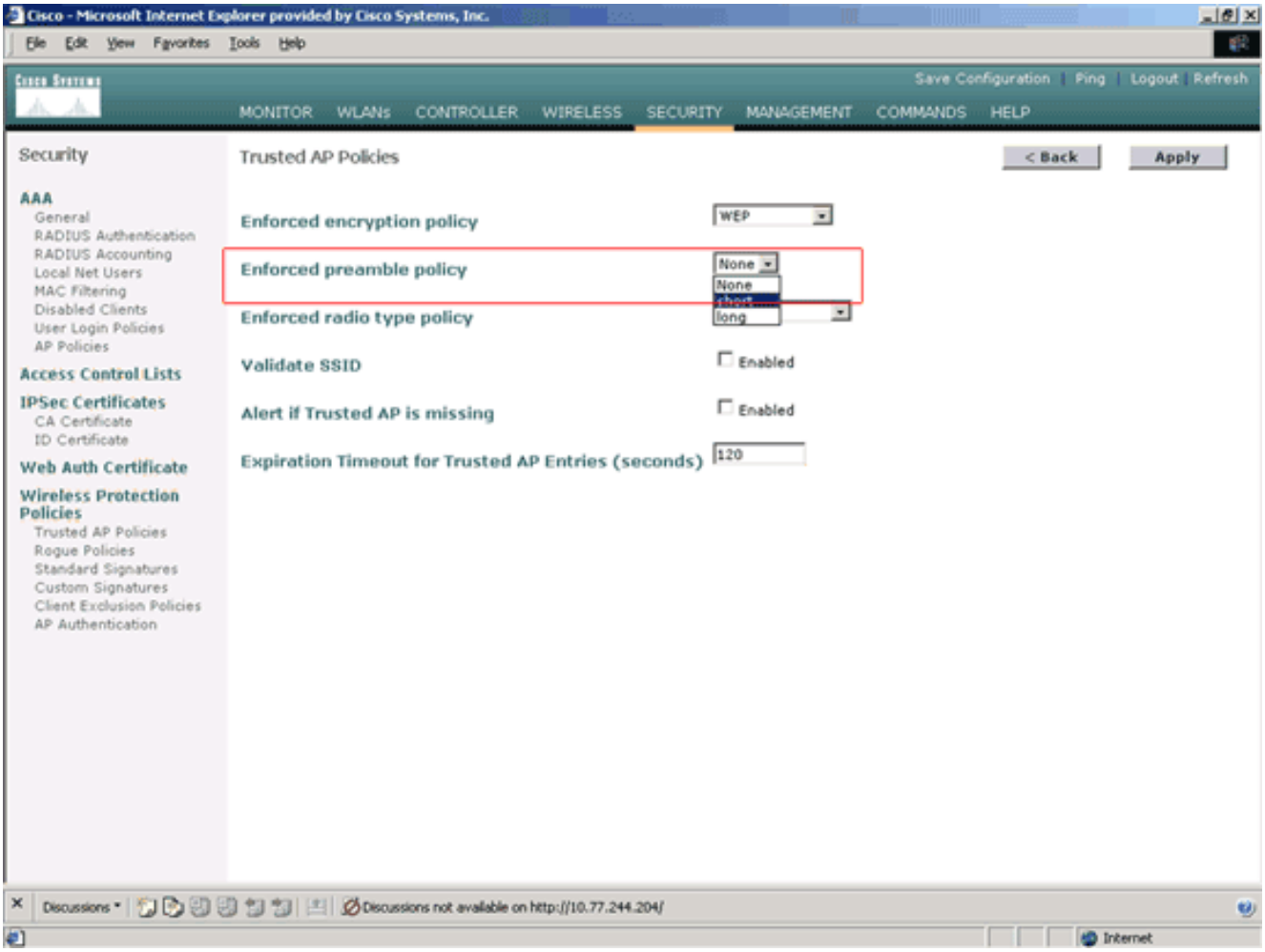
1. Dans le menu principal de l'interface utilisateur graphique du WLC, cliquez sur **Sécurité**.
2. Dans le menu situé sur le côté gauche de la page Sécurité, cliquez sur **Stratégies d'AP de confiance** répertoriées sous l'en-tête Stratégies de protection sans fil.



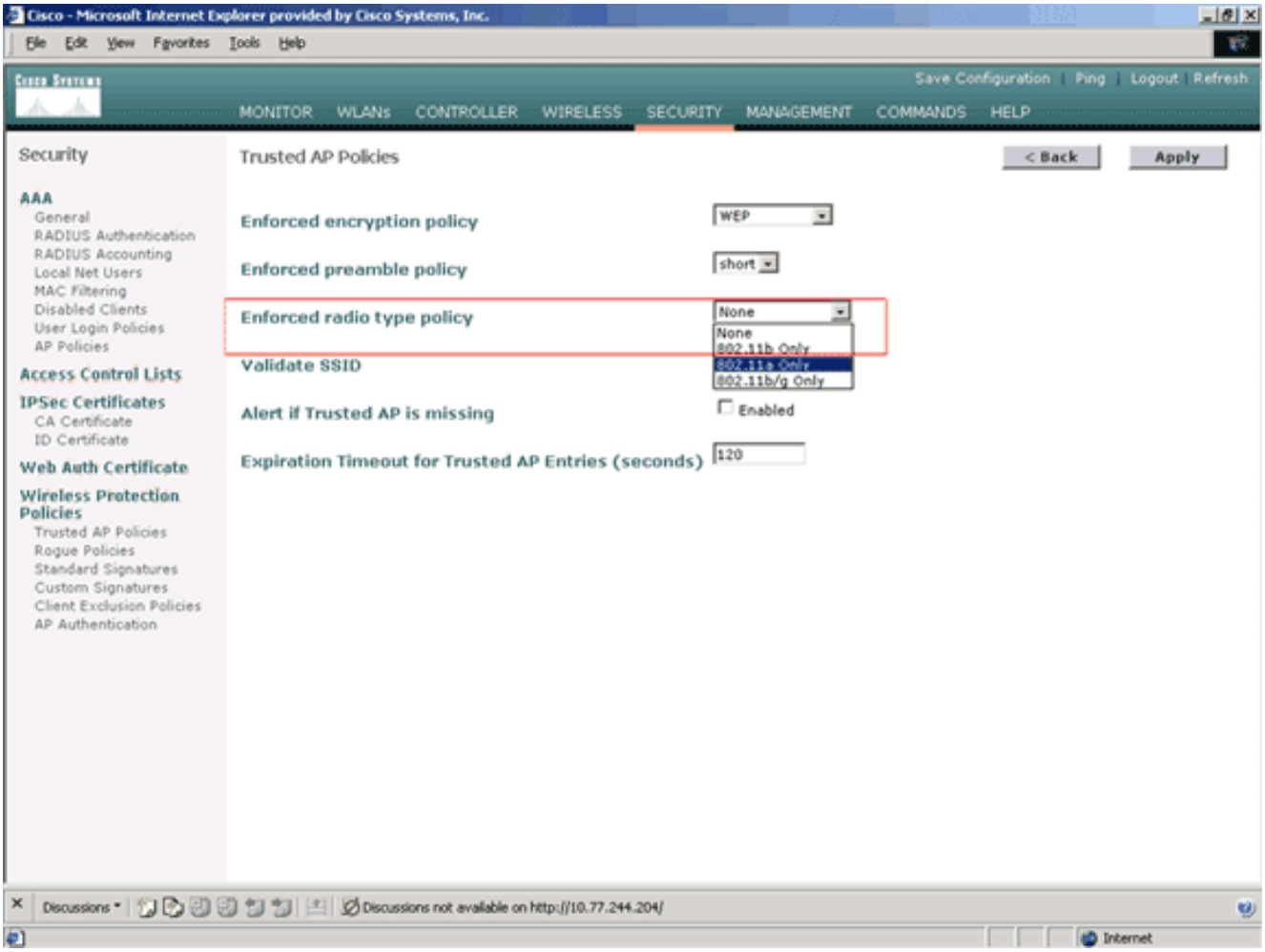
3. Sur la page Stratégies d'AP approuvé, sélectionnez le type de chiffrement souhaité (Aucun, Ouvrir, WEP, WPA/802.11i) dans la liste déroulante Stratégie de chiffrement appliquée.



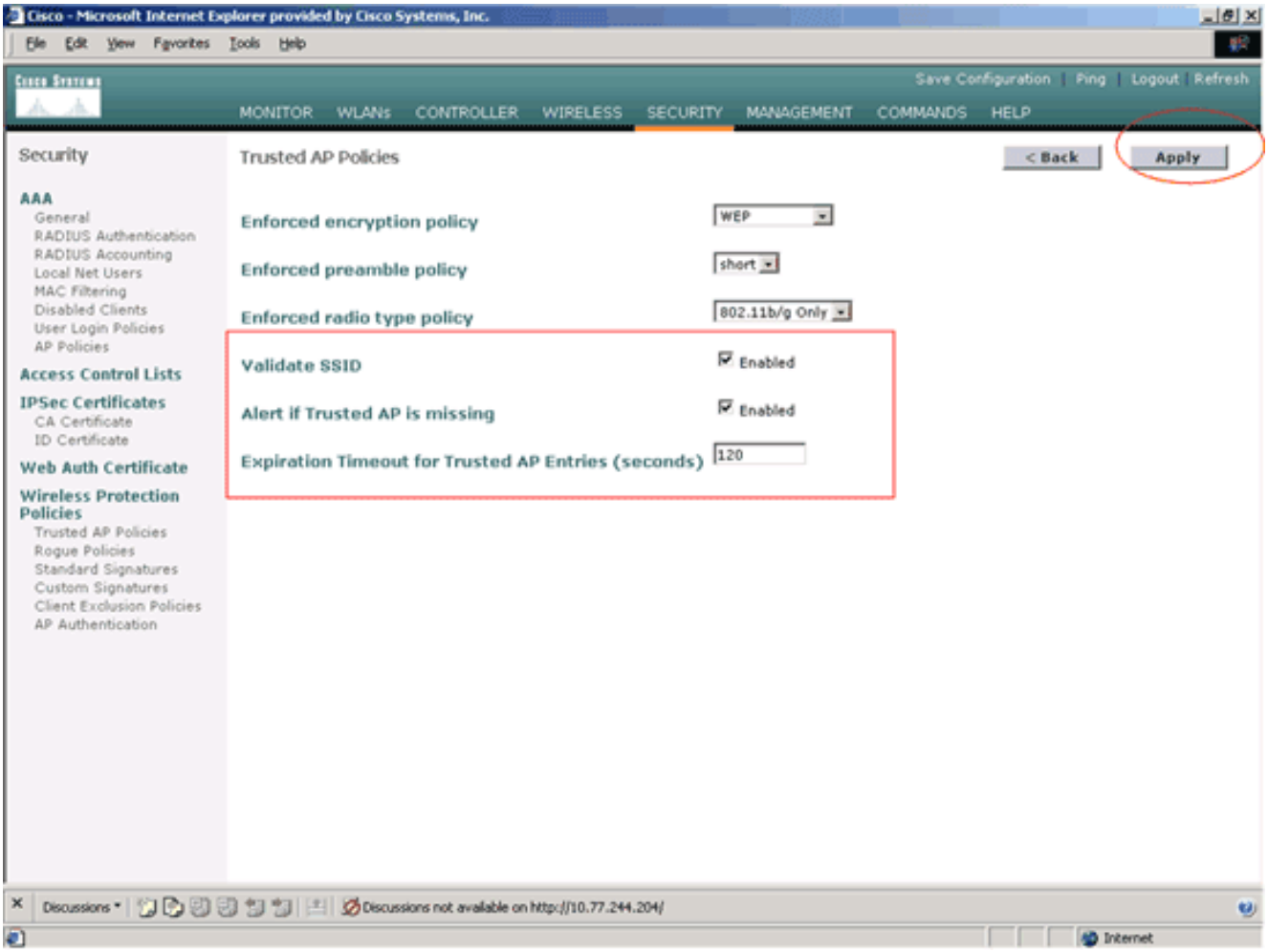
4. Sélectionnez le type de préambule souhaité (Aucun, Court, Long) dans la liste déroulante Stratégie de type de préambule
appliqué.



5. Sélectionnez le type de radio souhaité (Aucun, 802.11b uniquement, 802.11a uniquement, 802.11b/g uniquement) dans la liste déroulante Stratégie de type de radio appliquée.



6. Cochez ou décochez la case **Valider le SSID activé** afin d'activer ou de désactiver le paramètre Valider le SSID.
7. Cochez ou décochez la case **Alerte si le point d'accès approuvé est manquant** pour activer ou désactiver l'alerte si le point d'accès approuvé est manquant.
8. Entrez une valeur (en secondes) pour l'option **Expiration Timeout for Trusted AP entry**.



9. Cliquez sur Apply.

Remarque : afin de configurer ces paramètres à partir de l'interface de ligne de commande du WLC, vous pouvez utiliser la commande **config wps trust-ap** avec l'option de stratégie appropriée.

```
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.
```

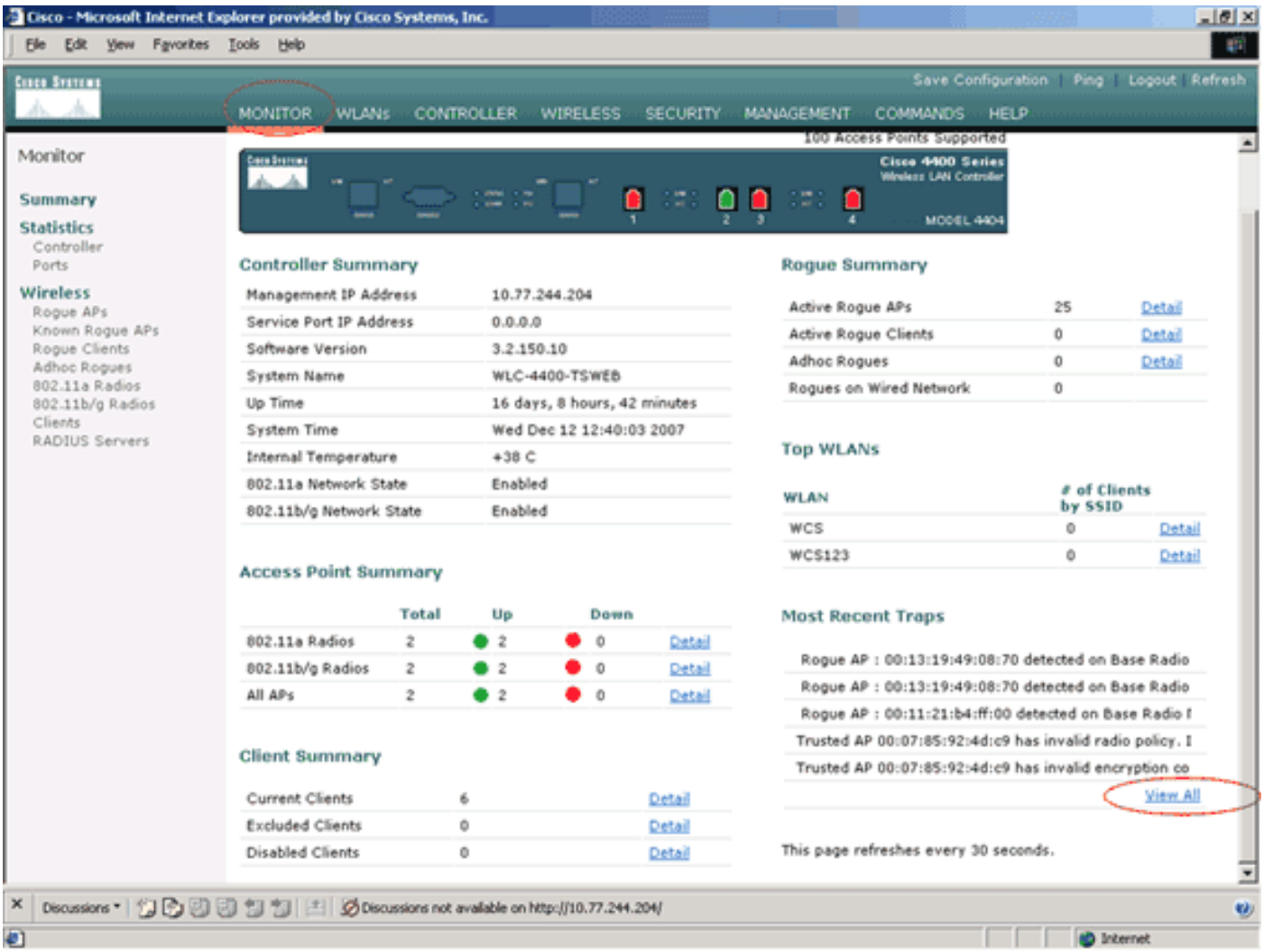
Message d'alerte de violation de stratégie AP de confiance

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

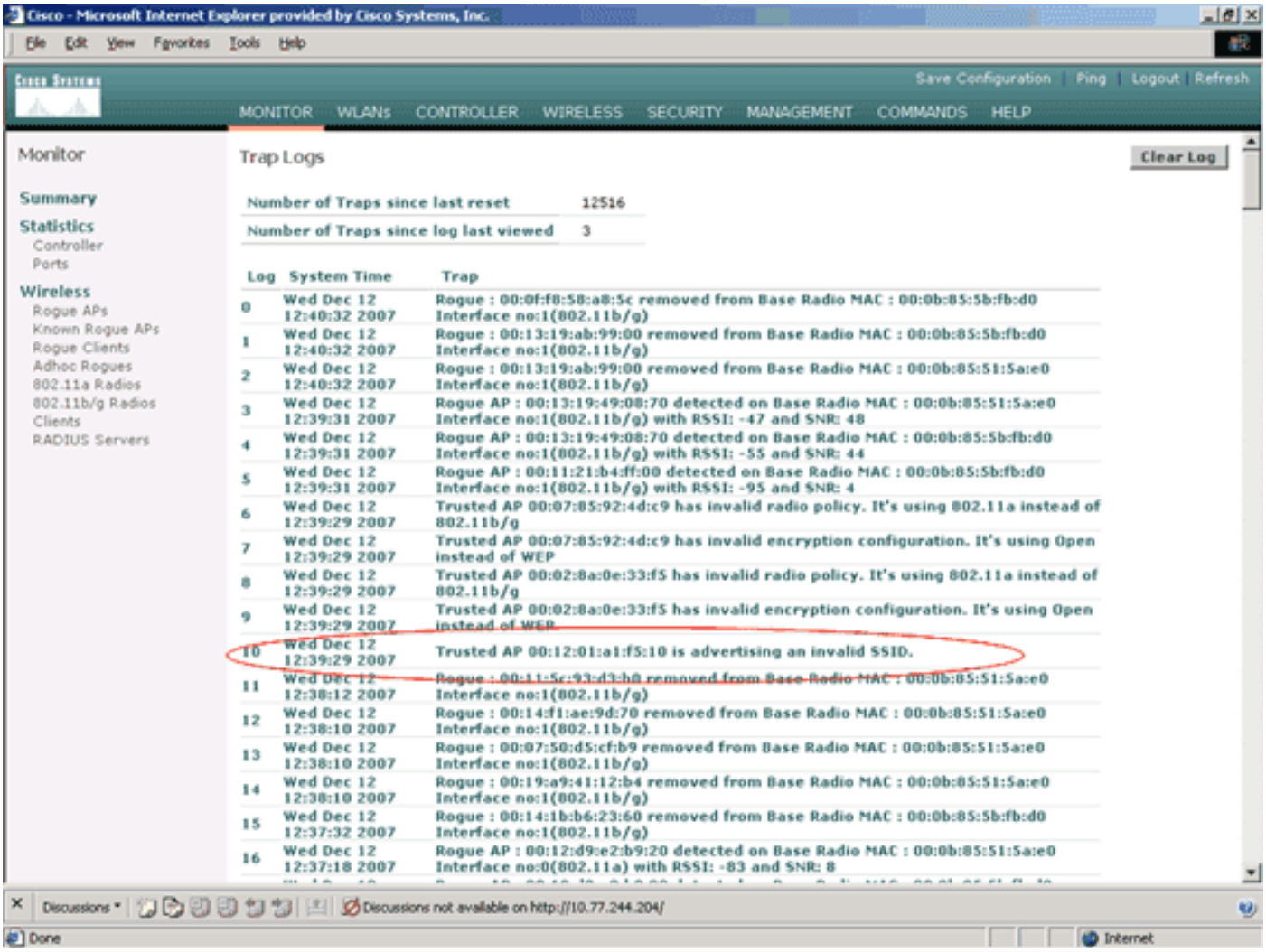
```
Thu Nov 16 12:39:12 2006  [WARNING] apf_rogue.c 1905: Possible AP
impersonation of xx:xx:xx:xx:xx:xx, using source address of
00:16:35:9e:6f:3a, detected by 00:17:df:7d:e1:70 on slot 0
 Thu Nov 16 12:39:12 2006  [SECURITY] apf_rogue.c 1490: Trusted AP Policy
failed for AP xx:xx:xx:xx:xx:xx - invalid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

Notez les messages d'erreur mis en surbrillance ici. Ces messages d'erreur indiquent que le SSID et le type de chiffrement configurés sur le point d'accès approuvé ne correspondent pas au paramètre de stratégie du point d'accès approuvé.

Le même message d'alerte peut être vu à partir de l'interface utilisateur graphique du WLC. Afin d'afficher ce message, accédez au menu principal de l'interface utilisateur graphique du WLC, puis cliquez sur **Monitor**. Dans la section Traps les plus récents de la page Monitor, cliquez sur **View All** afin d'afficher toutes les alertes récentes sur le WLC.



Sur la page Traps les plus récents, vous pouvez identifier le contrôleur qui génère le message d'alerte de violation de stratégie AP approuvé, comme illustré dans cette image :



Informations connexes

- Guide de configuration du contrôleur LAN sans fil Cisco, version 5.2 - Activation de la détection de point d'accès Rouge dans les groupes RF
- Guide de configuration du contrôleur LAN sans fil 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