

# Dépannage du système de contrôle sans fil

## Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Conventions](#)

[Dépannez](#)

[Non capable installer WCS](#)

[Problème de compatibilité entre les versions WLC et WCS](#)

[WCS ne commence pas après installation dans un système d'exploitation Non-anglais de Windows 2003](#)

[Caractères internationaux non pris en charge sur WCS](#)

[Incapable de commencer WCS dû aux fichiers journal corrompus](#)

[Vérifiez l'état du WCS](#)

[Ajoutez un WLC au WCS](#)

[Configuration régénératrice WLC de WCS](#)

[Pare-feu entre le WCS et le contrôleur ou le WCS et l'interface utilisateur WCS](#)

[Remettez à l'état initial un contrôleur de nouveau à Factory Defaults utilisant le WCS](#)

[Défragmenter la base de données WCS](#)

[Vérifiez si vous avez le permis approprié pour le logiciel WCS](#)

[Utilisez la page récapitulative de Sécurité pour le dépannage](#)

[Déterminez et placez les points d'accès non autorisés](#)

[Utilisez la caractéristique de personnalisation du Point d'accès \(AP\) sur le WCS](#)

[Localisez les clients](#)

[Trous de couverture dans un réseau WLAN](#)

[Si vous avez des difficultés quand vous importez une carte](#)

[Cliquez sur un périphérique de réseau d'un Cisco WLC](#)

[État en cours, configurations, et statistiques de Cisco WLC de vue](#)

[Examinez la préparation d'emplacement](#)

[Questions de synchronisation avec les serveurs WCS et d'emplacement](#)

[Questions de synchronisation avec le WCS et le WLC](#)

[Configuration DHCP corrompue quand le modèle est poussé de WCS à WiSM](#)

[Les cartes de la chaleur WCS affichent les trous carrés incorrects de couverture](#)

[Quand le modèle de l'escroc AP obtient-il appliqué au WLC ?](#)

[Ports sur le serveur WCS](#)

[Vérifiez les WLAN sont-ils configurés pour l'exclusivité-liste](#)

[Dépannez l'enable d'exclusivité-liste](#)

[Clients globalement handicapés de vue et d'effacement](#)

[Clients handicapés de vue et d'effacement manuellement par contrôleur](#)

[WCS recherchent des clients par bâtiment ne fonctionnent pas](#)  
[Comptes incorrects de client d'états WCS associés aux aps en mode H-REAP](#)  
[WCS ne commence pas si le trait de soulignement est configuré dans le serveur/adresse Internet](#)  
[L'ERREUR \[emplacement\] n'a pas créé la carte de la chaleur pour le MAC : xx : xx : xx : xx : xx : xx raison : Manqué car la liste RSSI est vide après élagage de temps](#)  
[Le message d'erreur « que l'entrée Point Fillexp Could de procédure pas se trouvent dans des affichages de la bibliothèque de liens dynamiques le DFORRT.DLL »](#)  
[Instructions à la synchronisation les trois périphériques](#)  
[Le modèle WLAN n'applique pas la configuration correcte de « Broadcast SSID » dans le WLC](#)  
[Les modèles WLAN n'affichent pas la configuration correcte de case à cocher de 7920 CAC](#)  
[Incapable de supprimer les contrôleurs hors ligne de la version 3.2.51.0 WCS](#)  
[Ne peut pas ajouter le modèle d'authentification Web avec le par défaut de type interne de WCS](#)  
[Informations connexes](#)

## **Introduction**

Il fournit des procédures de dépannage pour des problèmes de fond liés au Système de contrôle sans fil (WCS) Cisco.

## **Conditions préalables**

### **Conditions requises**

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- La connaissance de la façon configurer le Cisco WCS
- La connaissance de la façon configurer un RÉSEAU LOCAL Sans fil (WLAN) avec les contrôleurs WLAN (WLCs) et le Point d'accès léger (recouvrements)

### **Composants utilisés**

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

### **Conventions**

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

## **Dépannez**

### **Non capable installer WCS**

Si vous rencontrez des problèmes quand vous essayez d'installer WCS, premier contrôle pour voir si le système sur lequel vous prévoyez d'installer WCS répond aux configurations système minimales.

C'est la liste de contrôle nécessaire à l'utiliser avant que vous installiez le Cisco WCS :

1. Vérifiez si le système sur lequel vous êtes sur le point d'installer le Cisco WCS répond au matériel et aux logiciels nécessaires nécessaires pour le Cisco WCS. Pour les informations sur le logiciel minimum et des configurations matérielles requises pour l'installation du WCS, référez-vous à la section de [configurations système requises du guide de configuration de Cisco WCS, version 4.0](#).
2. Assurez-vous que vous avez mis à jour votre système avec les mises à jour et les packs de services essentiels nécessaires. Référez-vous aux dernières notes de mise à jour pour les informations sur les packs de services et les correctifs requis pour l'exécution correcte du WCS. **Remarque:** Avant que vous installiez le WCS sur le Linux, un plein installé de Red Hat Linux est exigé.
3. Sauvegarde la base de données existante WCS. Référez-vous à [sauvegarder la base de données WCS](#) pour les informations sur la façon dont exécuter une sauvegarde de Windows.
4. Désinstallez la version plus ancienne du WCS. Référez-vous à [désinstaller le Cisco WCS](#) pour les informations sur la façon dont exécuter un désinstaller.

Une fois que vous vous assurez que vous avez les conditions préalables, vous pouvez installer le WCS. Référez-vous à [installer WCS pour Windows](#) pour les informations sur la façon dont installer le Cisco WCS pour Windows.

**Remarque:** Passages WCS seulement sur Windows de 32 bits ; des installations du système d'exploitation 64-bit ne sont pas prises en charge.

Référez-vous à [installer WCS pour le Linux](#) pour les informations sur la façon dont installer le WCS sur le Linux.

## [Problème de compatibilité entre les versions WLC et WCS](#)

Quand vous installez WCS pour gérer le WLCs, assurez-vous que les versions WCS et WLC sont compatibles. Ces informations sont disponibles dans les notes de mise à jour de la version WCS que vous installez.

Par exemple, le Cisco WCS 5.1.64.0 prend en charge la Gestion de ces contrôleurs LAN Sans fil :

- 4.2.61.0
- 4.2.99.0
- 4.2.112.0
- 4.2.130.0
- 5.0.148.0
- 5.1.151.0

Ces informations sont disponibles dans ce document : [Notes de mise à jour pour le Système de contrôle sans fil Cisco 5.1.64.0 pour Windows ou Linux](#)

Si vous utilisez des versions incompatibles de WCS et de WLC, vous ne pourrez pas ajoutez votre WLCs au WCS.

## [WCS ne commence pas après installation dans un système d'exploitation Non-anglais de Windows 2003](#)

Ceci se produit parce que WCS est pris en charge seulement dans Windows 2003 avec l'anglais ou des versions japonaises. Si vous utilisez des systèmes d'exploitation traduits à d'autres langages, il fait échouer WCS après installation. Afin d'éviter ceci, l'utilisation WCS sur Windows 2003 anglais ou les versions japonaises.

## Caractères internationaux non pris en charge sur WCS

WCS et appliances d'emplacement ne prennent en charge pas les caractères internationaux en général. Si vous utilisez les caractères non-anglais pour des map name, des informations de ressource, etc., il peut générer des erreurs d'affichage (caractères faux affichés) et des erreurs sur des fonctions de recherche.

## Incapable de commencer WCS dû aux fichiers journal corrompus

Parfois nous ne pouvons pas commencer WCS et ouvrir son interface web. Même si vous essayez d'ouvrir WCS avec le fichier « .exe » dans le WCS \ coffre \ répertoire, il peut échouer. Ce message peut afficher tandis que vous essayez de commencer WCS.

```
Starting WCS
```

```
Checking for Port 21 availability... OK
```

```
Checking for Port 8456 availability... OK
```

```
Checking for Port 8457 availability... OK
```

```
.....  
.....  
.....  
.....  
.....
```

```
Starting database server ...
```

```
The Nms_Server service is starting..... The Nms_Server service could not be started. The service did not report an error. More help is available by typing NET HELPMMSG 3534. Failed to start WCS server.
```

Un possible raison pour cette question peut être la bogue [CSCse17963](#) (clients [enregistrés](#) seulement).

Selon cette bogue, la base de données WCS peut pour commencer en raison des fichiers journal corrompus. Afin de résoudre ce problème, allez au sous-répertoire **autonome** par les **webnms de** chemin **\ eval\_kit \ autonome** dans le répertoire WCS. Dans ce sous-répertoire, trouvez le **fichier sol####.log** numéroté le plus élevé, où le **####** est un nombre à quatre chiffres. Supprimez-le et redémarrez le serveur. Tentative de commencer WCS. Si WCS ne commence pas, répéter pour le prochain fichier **sol###.log**, et ainsi de suite. Ce contournement résoudra le problème.

## Vérifiez l'état du WCS

Si le WCS ne fonctionne pas comme prévu, vérifiez d'abord l'état du WCS. Terminez-vous ces étapes afin de vérifier l'état du WCS quand il est installé en tant qu'une application Windows ou service windows. Vous pouvez vérifier l'état à tout moment.

1. Connectez-vous dans le système comme administrateur.
2. Exécutez l'une de ces actions:Allez à Windows le menu de démarrage et choisissez les

**programmes > le système de contrôle sans fil > le WCSStatus.** De l'invite de commande, naviguez vers le répertoire d'installation WCS (C:\Program Files\WCS32\bin) et écrivez l'**état de WCSAdmin**. La fenêtre de WCSAdmin apparaît et affiche les messages qui indiquent l'état du WCS :

3. Clic **étroit** afin de fermer la fenêtre de WCSAdmin.

Si le WCS est installé sur un système Linux, terminez-vous ces étapes afin de vérifier l'état du WCS :

1. Connectez-vous dans le système comme racine.
2. Employez le Linux CLI afin d'effectuer une de ces tâches : Naviguez vers le répertoire de `/opt/WCS32` (ou le répertoire choisi pendant l'installation) et entrez dans `./WCSStatus`. Naviguez vers le répertoire de `/opt/WCS32/bin` et écrivez l'**état de WCSAdmin**. Le CLI affiche les messages qui indiquent l'état du WCS.

## [Ajoutez un WLC au WCS](#)

Quand un nouveau WLC est ajouté au WCS, assurez-vous que la version SNMP configurée sur le contrôleur s'assortit avec la version SNMP sur le WCS. Si les versions ne s'assortissent pas, le WCS ne détecte pas le contrôleur et cette erreur apparaît sur le WCS.

`No response from device, check SNMP.`

Assurez-vous également que le SNMP écriture le privilège d'accès est activé sur le contrôleur. Si vous entrez des paramètres d'accès en lecture seule puis le contrôleur est ajouté au WCS, mais le WCS ne peut pas modifier la configuration sur le contrôleur.

En résumé, vérifiez ces éléments s'il y a un problème ajoutant le contrôleur au WCS :

- L'adresse IP de port de service de contrôleur pourrait être placée inexactement. Vérifiez la configuration de port de service sur le contrôleur.
- Le WCS ne pourrait pas pouvoir entrer en contact avec le contrôleur. Assurez-vous que vous pouvez cingler le contrôleur du serveur WCS.
- Les configurations SNMP sur le contrôleur ne pourraient pas appairer les configurations SNMP que vous avez écrites dans le WCS. Assurez-vous que les configurations SNMP configurées sur le contrôleur appairer les configurations que vous avez écrites dans le WCS.
- Quand vous améliorez le WCS à la dernière version, vous avez besoin d'un permis de Cisco. Si votre WCS n'est pas autorisé, vous ne pouvez pas ajouter un nouveau WLC. Afin d'obtenir un permis, vous devez appeler le support TAC.

**Remarque:** Si vous apportez n'importe quelles modifications sur le WCS, alors veillez-vous pour expédier les modifications à vos contrôleurs. Régénérez alors les configurations du contrôleur afin de le rendre à jour. Voyez la [configuration régénératrice WLC de la](#) section [WCS de](#) ce document pour savoir régénérer WLC du WCS.

## [Configuration régénératrice WLC de WCS](#)

Exécutez ces étapes dans le WCS dans cette commande pour régénérer la configuration de contrôleur de WCS.

1. Choisissez le **Configure > Controllers**.
2. La page de contrôleurs répertorie tout le WLCs ajouté. De la liste de WLCs, choisissez le

WLC à régénérer.

3. Dans la page résultante de contrôleur, du **choisi un** menu déroulant de **commande**, choisissez la **save configuration pour flasher** et cliquer sur Go.
4. Après que la configuration soit enregistrée dans l'éclair, vous recevez un message réussi sur l'écran. Après que l'écran réussi apparaisse, choisissez le même contrôleur dont la configuration a été enregistrée pour flasher et, sur le **choisi une commande**, choisir **régénèrent le config du contrôleur**.
5. Ceci vous incite à retenir ou supprimer la configuration ancienne. Choisissez l'**effacement** et l'appuyez sur **CORRECT**.

## [Pare-feu entre le WCS et le contrôleur ou le WCS et l'interface utilisateur WCS](#)

Quand un serveur WCS et une interface utilisateur WCS sont de différents côtés d'un Pare-feu, ils ne peuvent pas communiquer à moins que ces ports sur le Pare-feu soient ouverts de trafic bi-directionnel :

- 80 (pour le HTTP initial)
- 69 (tftp)
- 162 (port de déROUTement)
- 443 (https)

Ouvrez ces ports afin de configurer votre Pare-feu pour permettre des transmissions entre un serveur WCS et une interface utilisateur WCS.

## [Remettez à l'état initial un contrôleur de nouveau à Factory Defaults utilisant le WCS](#)

Terminez-vous ces étapes pour remettre à l'état initial le contrôleur aux par défaut d'usine utilisant le WCS :

1. Choisissez le **Configure > Controllers** afin d'afficher la toute la page de contrôleurs. Cette page répertorie tous les contrôleurs qui sont découverts par le WCS.
2. Cliquez sur en fonction l'adresse IP du contrôleur que vous voulez remettre à l'état initial aux par défaut d'usine. La fenêtre de Properties de contrôleur apparaît.
3. Du menu de côté gauche, choisissez le **système > les commandes**. La fenêtre de commandes de contrôleur apparaît.
4. Sous des commandes d'administration sélectionnez la **remise au par défaut d'usine** et cliquez sur Go.
5. Choisissez la **réinitialisation du** menu de commandes d'administration afin de redémarrer le contrôleur sans enregistrer la configuration sur le contrôleur. Ceci remet à l'état initial le contrôleur aux par défaut d'usine. **Remarque:** Une fois que le contrôleur est remis à l'état initial aux par défaut d'usine, le WCS ne peut pas découvrir le contrôleur à moins qu'il soit configuré avec l'adresse IP de Gestion. Pour ceci, vous devez configurer le contrôleur utilisant le début vers le haut de l'assistant de configuration sur le contrôleur.

## [Défragmenter la base de données WCS](#)

Toutes les exécutions du militaire de carrière WCS, telles que la suppression des alarmes, des événements, d'ajouter/supprimant des contrôleurs, etc. comportent des exécutions SQL

intérieurement avec la base de données WCS (DB). De telles exécutions internes SQL augmentent naturellement la taille de la base de données, qui, à leur tour, ont une incidence sur la représentation de WCS.

Par exemple, une exécution d'effacement dans WCS laisse l'espace vide dans les parties supprimées de la base de données. Ceci peut avoir comme conséquence l'emplacement discontinu des données dans la base de données, qui, consécutivement, affecte la représentation WCS. Défragmentez la base de données WCS pour surmonter cette question.

Le Defragmentation fait tout l'espace utilisé et inutilisé contigu. Espace inutilisé/inutilisé contigu améliore la représentation. Si vous défragmentez la base de données, vous pouvez reprendre l'espace disque alloué mais inutilisé. Un defragmentation de base de données peut être salutaire si l'espace disque libre sur le système exécute le bas dû à une grande taille de la base de données ou si le temps de réponse de l'application WCS est sensiblement plus lent quand des données sont demandées à elles.

Afin d'exécuter le defragmentation manuellement dans WCS, arrêtez l'application WCS. Afin de faire ceci, le **début de clic > programme > système de contrôle sans fil > arrêt WCS**. Ouvrez alors une ligne de commande case, modification au répertoire de **C:\Program Files\WCS4.0\bin** (le répertoire par défaut où WCS est installé), et exécutez le **defrag de DBAdmin** de commande. Ceci initie le procédé de defragmentation. Une fois que le processus est terminé, redémarrez WCS avec l'exécution de **début > de programmes > de radio > de Control System > de début WCS**.

**Remarque:** Le Defragmentation fonctionne automatiquement après que les restaurations de base de données. Encore, dans certains cas, le defragmentation manuel est fait pour libérer un certain espace disque. Un defrag manuel n'est pas vraiment nécessaire. Cet espace vraisemblablement est regagné dans quelques jours où des débuts WCS pour créer et supprimer des alarmes.

## [Vérifiez si vous avez le permis approprié pour le logiciel WCS](#)

La version de logiciel 4.0 de réseau sans fil unifié Cisco impose l'autorisation articulée autour d'un logiciel. Des clients sont incités à entrer dans des Certificats de permis par toutes les nouvelles familles du Cisco WCS UGS (excepté le permis de démonstration de Cisco WCS). Des clients en cours qui migrent vers la version 4.0 sont également affectés par l'autorisation. L'application d'autorisation de Cisco WCS est attachée à ces paramètres :

- **Nom d'hôte** — Le nom d'hôte du serveur de Cisco WCS est maintenant exigé pendant la procédure d'enregistrement. Des permis émis sont attachés au nom d'hôte d'origine indiqué pendant la procédure d'enregistrement.
- **Option de caractéristique** — L'option de caractéristique de Cisco WCS achetée, de base ou l'emplacement, est maintenant dépistée par le système des licences de Cisco WCS.
- **Points d'accès** — Le nombre de Points d'accès pris en charge dans des incréments de positionnement de 50, de 100, de 500, de 1000, ou de 2500 est maintenant dépisté par le système des licences de Cisco WCS.
- **Permis de démonstration** — Ce permis libre et emplacement-activé de démonstration de Cisco WCS prend en charge 10 Points d'accès pendant jusqu'à 30 jours.

Référez-vous au [guide de autorisation et de commande de Cisco WCS](#) pour plus d'informations détaillées sur le permis de Cisco WCS et aux différents types de permis disponibles.

Sélectionnez le permis correct basé sur votre situation de déploiement, le nombre de Points d'accès à prendre en charge, et des options de Cisco WCS (base ou emplacement). Tous les

UGS dans une famille UGS peuvent être combinés avec les niveaux équivalents d'option tels que la Base-à-base ou l'Emplacement-à-emplacement. Les niveaux inégaux d'option (base et emplacement) ne peuvent pas être mélangés. Seulement un type de permis peut être utilisé sur le WCS en même temps.

Par exemple, si votre ordinateur a un permis d'emplacement, vous ne pouvez pas ajouter un permis de base. Vous pouvez ajouter au permis en cours en achetant un permis d'augmenter le compte de Point d'accès. Par exemple, si vous avez un permis d'emplacement avec un compte de Point d'accès de 50 et pendant une année vous devez ajouter plus de Points d'accès, vous pouvez acheter un autre permis d'emplacement avec un compte de Point d'accès de 100, l'appliquer au WCS, et avoir un WCS avec un permis d'emplacement pour 150 Points d'accès. Vous pouvez ajouter un permis d'augmenter le nombre de Points d'accès par paliers de 50, de 100, de 500, de 1000, de 2500, ou d'illimité.

Si vous avez un permis de base et voulez améliorer à un emplacement, vous devez acheter un permis de mise à jour d'emplacement. Vous devez acheter un permis de mise à jour d'emplacement équivalent au nombre total de Points d'accès avec un permis de base. Par exemple, si vous avez trois permis de base avec le soutien de 50, 100, et 200 Points d'accès (pour un total de 350 Points d'accès), vous devez acheter un permis simple de mise à jour d'emplacement avec le soutien de 350 Points d'accès.

Tout le Cisco WCS UGS exigent d'un certificat PAK d'enregistrer le permis de Cisco WCS. Le PAK est un certificat de papier envoyé par l'intermédiaire de la messagerie des États-Unis de Cisco Systems sur l'achat du permis de Cisco WCS. Le certificat PAK permet à des clients pour recevoir un permis de Cisco WCS. Il est utilisé pour enregistrer le Cisco WCS et pour générer des fichiers de licence. Tous les clients doivent aller au site indiqué d'enregistrement PAK sur leur certificat PAK pour se terminer leur enregistrement de Cisco WCS. Le certificat PAK fournit des instructions claires sur la façon dont compléter la procédure d'autorisation de Cisco WCS.

Tous les clients qui achètent le Cisco WCS de Cisco.com par l'intermédiaire du téléchargement ou du CD doivent lancer leur permis de Cisco WCS par l'enregistrement au site PAK. Les clients recevront le PAK par l'intermédiaire de la messagerie des États-Unis. Le Cisco WCS n'est pas lancé jusqu'à ce que la procédure d'enregistrement PAK soit terminée. Référez-vous aux [permis WCS](#) pour les informations sur la façon dont installer et gérer un permis WCS.

## [Utilisez la page récapitulative de Sécurité pour le dépannage](#)

La page récapitulative de Sécurité fournit à l'utilisateur des informations sur tous les événements liés à la sécurité. Cette page fournit des informations sur des points d'accès non autorisés, des informations sur des attaques de signature, des informations sur des attaques sur les Points d'accès, et relatif à l'information à la Sécurité de client.

Cette page est un outil efficace de dépannage spécifiquement si le problème est lié aux menaces de Sécurité. Cette page fournit également des informations sur les alertes sécurité les plus récentes.

Voici un exemple de la page récapitulative de Sécurité :

## [Déterminez et placez les points d'accès non autorisés](#)

Quand les recouvrements de Cisco sont mis et associés sous tension avec des Cisco WLC, le Cisco WCS a construit dans les débuts de système d'exploitation immédiatement pour écouter



des points d'accès non autorisé. Quand un Cisco WLC détecte un point d'accès non autorisé, il informe immédiatement le Cisco WCS, qui crée une alarme de point d'accès non autorisé. WCS considère n'importe quel Point d'accès qui n'est pas une partie de son réseau Sans fil comme point d'accès non autorisé.

Quand le Cisco WCS reçoit un message de point d'accès non autorisé d'un Cisco WLC, le Cisco WCS génère une alarme, avec un indicateur visible dans le coin inférieur gauche de toutes les pages d'interface utilisateur de Cisco WCS. Cet exemple affiche 72 alarmes de point d'accès non autorisé de Cisco WCS.

Terminez-vous ces étapes afin de détecter et placer des points d'accès non autorisé :

1. Cliquez sur l'indicateur d'**escrocs** afin d'afficher la page d'alarmes de l'escroc AP. Cette page répertorie la sévérité des alarmes, les adresses MAC de point d'accès non autorisé, les types de point d'accès non autorisé, la date et le moment où les points d'accès non autorisé ont été détectés la première fois, et leur SSID.
2. Cliquez sur n'importe quel lien escroc d'adresse MAC afin d'afficher les alarmes > l'escroc associés - page d'adresse MAC AP. Cette page affiche les informations détaillées au sujet de l'alarme de point d'accès non autorisé.
3. Choisissez une de ces commandes du choisi un menu de commande et cliquez sur Go afin de modifier l'alarme.**Assignez-moi** — Assigne l'alarme sélectionnée à l'utilisateur courant.**Unassign** — Unassigns l'alarme sélectionnée.**Effacement** — Supprime l'alarme sélectionnée.**Espace libre** — Efface l'alarme sélectionnée.**Historique d'événement** — Te permet de visualiser des événements pour les alarmes escrocs.**Détectant des aps** (avec la bande radio, l'emplacement, le SSID, le numéro de canal, l'état de Confidentialité équivalente aux transmissions par fil (WEP), le short ou le long préambule, reçoivent l'indicateur de force du signal (RSSI), et le SNR) — te permet de visualiser les Points d'accès qui détectent actuellement le point d'accès non autorisé.**Clients escrocs** — Te permet de visualiser les clients associés avec ce point d'accès non autorisé.**Placez l'état au « inconnu - Alerte »** — Étiquette le point d'accès non autorisé comme plus basse menace, continue à surveiller le point d'accès non autorisé, et arrête la retenue.**Placez l'état à « connaître - Interne »** — Étiquette le point d'accès non autorisé comme interne, l'ajoute aux points d'accès non autorisé connus répertorient, et arrêtent la retenue.**Placez l'état à « connaître - Externe »** — Étiquette le point d'accès non autorisé comme externe, l'ajoute aux points d'accès non autorisé connus répertorient, et arrêtent la retenue.**1 retenue AP par la retenue de 4 AP** — quand vous sélectionnez la retenue du niveau 1, un Point d'accès à proximité de l'unité escroc envoie désauthentifie et dissocient des messages aux périphériques de client qui sont associés à l'unité escroc. Quand vous sélectionnez la retenue du niveau 2, deux Points d'accès à proximité de l'unité escroc envoient désauthentifie et les messages dissociés aux clients de l'escroc et ainsi de suite jusqu'au niveau 4. c'est-à-dire, le Point d'accès choisi pour la retenue empêche des clients de communiquer au point d'accès non autorisé. Ceci neutralise efficacement la fonction du point d'accès non autorisé.
4. Allez au choisi un menu déroulant de commande, choisissez la **carte (de haute résolution)** et cliquez sur Go afin d'afficher le courant a calculé l'emplacement de point d'accès non autorisé sur les cartes > la page de nom de bâtiment > de nom de plancher.

Si vous utilisez l'emplacement WCS, WCS compare la force du signal RSSI de deux Points d'accès ou plus afin de trouver l'emplacement le plus probable du point d'accès non autorisé et place un petit indicateur de crâne-et-os croisés à son emplacement le plus susceptible. Dans le cas d'un réseau sous-déployé pour l'emplacement avec seulement un Point d'accès et une

antenne d'omni, l'emplacement le plus susceptible est quelque part sur un anneau autour du Point d'accès, mais le centre de la probabilité est au Point d'accès.

Voici un exemple qui affiche un point d'accès non autorisé sur une carte :

Si vous utilisez WCS de base, WCS se fonde sur la force du signal RSSI du point d'accès non autorisé et place un petit indicateur de crâne-et-os croisés à côté du Point d'accès qui reçoit le signal RSSI le plus fort à partir de l'unité escroc.

Avec l'appliance d'emplacement, des escrocs peuvent être dépistés, sont affichés dans le menu déroulant de **moniteur > de carte**, et ont l'escroc AP d'exposition et affichent aux clients escrocs des options. Sans appliance d'emplacement, ces options ne sont pas présentes, et vous pouvez seulement voir l'emplacement des escrocs quand vous allez à l'alarme escroc et sélectionnez la commande (**de haute résolution**) de **MAP** du menu déroulant.

Sur la base WCS, l'escroc est affiché à côté d'AP le détectant (pas le plus étroit), sans information d'emplacement. Pour plus d'informations détaillées sur les caractéristiques qui sont prises en charge dans la base WCS et l'emplacement WCS, référez-vous à la [comparaison de la base WCS et de l'emplacement WCS](#).

**Remarque:** La version de microprogramme 4.0 a les id [CSCse96812](#) (clients [enregistrés de](#) bogues Cisco seulement) et [CSCsf17545](#) (clients [enregistrés](#) seulement) des comptes de ce toujours client débarrassés des plants peu vigoureux par exposition à mettent dedans la liste à zéro de point d'accès non autorisé. Le contournement pour ce problème est de voir le point d'accès non autorisé le répertoire directement sur le contrôleur pour des comptes corrects.

## [Utilisez la caractéristique de personnalisation du Point d'accès \(AP\) sur le WCS](#)

La caractéristique de personnalisation AP améliore la détection de l'escroc aps qui tentent de personnaliser les recouvrements valides de gamme Cisco 1000. Cette caractéristique crée un groupe de réseau de Radiofréquence (RF), et les recouvrements de gamme Cisco 1000 dans le même groupe distribuent les paquets voisins de Gestion des ressources radio (RRM) entre eux. Si un RECOUVREMENT de gamme Cisco 1000 entend des paquets d'un autre RECOUVREMENT de gamme Cisco 1000 duquel il n'a reçu aucun paquet voisin RRM, alors le RECOUVREMENT de gamme Cisco 1000 peut supposer que nouvel AP personnalifie une gamme Cisco 1000 ENROULENT et le signale donc en tant qu'escroc AP.

Quand le WCS trouve AP qui tente de personnalifier un autre AP sur le WLAN, vous voyez cette alerte sur le serveur WCS :

```
AP Impersonation with MAC '00:14:1b:62:4e:42' is detected by authenticated
AP '00:14:1b:62:4e:40' on '802.11b/g' radio and Slot ID '0'
```

Sur le contrôleur, ce message de log de déROUTement affiche l'adresse MAC source qui entraîne la question :

```
Apr 10 11:21:16 <SomeIPAddress> [WARNING] apf_rogue.c 1890: Possible AP
impersonation of 00:14:1b:62:4e:42, using source
address of 00:90:4b:8a:de:c3, detected by 00:14:1b:62:4e:40 on slot 0.
```

Référez-vous à l'ID de bogue Cisco [CSCsb90622](#) (clients [enregistrés](#) seulement) pour plus d'informations sur les journaux des erreurs associés par personnalisation AP WCS.

La personnalisation AP est signalée par des ID quand vous voyez AP qui annonce une adresse MAC de Cisco qui ne communique pas par le point d'accès léger Protocol (LWAPP) ou le Control

Protocol Sans fil de contexte de RÉSEAU LOCAL (WLCCP). Dans le modèle LWAPP, WCS peut tracer un emplacement approximatif d'un escroc AP de la traduction de contrôleur de toutes les lectures AP.

## [Localisez les clients](#)

Le Cisco WCS permet à des opérateurs du système pour localiser des clients à l'entreprise. Procédez comme suit :

1. Choisissez le **moniteur > les périphériques > les clients** afin de naviguer vers la page récapitulative de clients.
2. À la page récapitulative de clients, dans la barre latérale gauche, recherchez **tous les clients** afin d'avoir l'affichage de Cisco WCS que les clients paginent.
3. Des clients paginez, cliquez sur le nom d'utilisateur du client que vous voulez localiser. Le Cisco WCS affiche la page <client correspondante de name> de clients.
4. De la page <client de name> de clients, vous avez deux choix pour localiser le client : Dans le menu déroulant, **carte récente** choisie (résolution haute-basse) afin de localiser le client sans la dissocier. Dans le menu déroulant, la **carte actuelle** choisie (résolution haute-basse) afin de dissocier et puis localiser le client après reassociation. Si vous faites ce choix, le Cisco WCS affiche un message d'avertissement et te demande de confirmer que vous voulez continuer. Voici un exemple :

Référez-vous à cette illustration pour une carte de la chaleur qui affiche des emplacements de client.

**Remarque:** L'emplacement de Cisco WCS compare le point fort de signal RSSI de deux gammes Cisco 1000 ou plus enrôle afin de trouver l'emplacement le plus probable du client, et place un petit graphisme d'ordinateur portable à son emplacement le plus susceptible. La base de Cisco WCS compare le point fort de signal RSSI du client, et place un petit graphisme d'ordinateur portable à côté de la gamme Cisco 1000 ENROULENT qui reçoit le signal RSSI le plus fort du client.

**Remarque:** Habituellement, quand vous arrêtez votre ordinateur portable, cela prend un longtemps (en quelques minutes) avant que le WLC ou le WCS retire le client de la liste de clients. Il continue à afficher que « a associé ». C'est parce qu'il y a des infidèles qui contrôlent le délai d'attente et la Session Timeout de veille appelés par informations d'association d'utilisateurs. Chacun des deux temporisateurs peuvent être changés. Ce sont les minuteurs par défaut :

- **Délai d'attente de veille** — (300 secondes)
- **Session Timeout** — (1800 secondes)

## [Trous de couverture dans un réseau WLAN](#)

Les trous de couverture sont des zones où les clients ne peuvent pas recevoir un signal du réseau Sans fil. Le Gestion des ressources radio (RRM) du système d'exploitation identifie ces zones de trou de couverture et les signale au Cisco WCS. Ceci permet au directeur des technologies de l'information pour remplir trous basés sur la demande d'utilisateur.

Quand le Cisco WCS affiche les 5 trous principaux de couverture, cliquez sur l'indicateur de **couverture** sur en bas à gauche de la page d'interface utilisateur de Cisco WCS (ou choisissez les **>Alarms de moniteur** et puis recherchez la **catégorie d'alarme - couverture**) afin d'avoir l'affichage

de Cisco WCS que le trou de couverture alarme la page. Sur le trou de couverture les alarmes paginent, choisissent le **moniteur > les cartes** et puis recherchent des Points d'accès par le nom de recouvrements de gamme Cisco 1000 (cet outil de recherche distingue les majuscules et minuscules). Le Cisco WCS affiche la page de cartes > de résultats de la recherche, qui répertorie le plancher ou la zone extérieure où le RECOUVREMENT de gamme Cisco 1000 se trouve. Cliquez sur le lien pour afficher les cartes relatives > page <building de name> > de <floorname>.

Sur les cartes > la page <building de name> > de name> de <floor, recherchent des zones de bas point fort de signal près de la gamme Cisco 1000 ENROULENT que signalé le trou de couverture. Tels sont les emplacements le plus susceptibles des trous de couverture. S'il ne semblent pas y avoir aucune zone de la force du signal faible, assurez-vous que la carte de plan d'étage est précise. En outre, si vous avez utilisé l'éditeur de plan d'étage pour créer des fichiers .FPE, que vous n'avez laissé aucun obstacle en métal, tel que des murs, des axes d'argumentaire, des cages d'escalier, ou des bibliothèques. Si oui, ajoutez-les au fichier de plan d'étage .FPE et remplacez le vieux plan d'étage par le nouveau plan d'étage.

### [Si vous avez des difficultés quand vous des import map](#)

Le Cisco WCS permet à l'utilisateur de visualiser le réseau WLAN géré sur le campus, le bâtiment, et les cartes réalistes de plan d'étage. Vous pouvez importer le plancher, le campus, ou le plan de bâtiment au Cisco WCS pendant qu'un fichier d'image et vous pouvez ajouter des périphériques aux localisations adaptées. Le Cisco WCS prend en charge ces types d'image :

- Format .PNG
- Format .JPG
- Format .JPEG
- Format .GIF

Si vous faites face à une question quand vous des import map au Cisco WCS, il pourriez être dû à un format sans support d'image. Afin de résoudre ce problème, ouvrir l'image avec le paint de Microsoft et sauvegarder le fichier comme <filename>.GIF. Puis essayez pour importer l'image de nouveau.

Parfois, le fichier d'image importé peut afficher dans WCS avec très la mauvaise qualité, quoique le fichier d'image originale soit de haute qualité. Un possible raison pour ce problème est avec l'image elle-même. WCS incorpore l'espace blanc qui entoure l'image dans la supposition que ce fait partie de la carte ; ceci peut mener à la qualité d'affichage de pauvres dans l'éditeur de carte WCS. Essayez de cultiver le fichier d'image pour enlever l'espace blanc et puis pour importer la nouvelle image dans WCS.

Référez-vous à [ajouter et à utiliser des cartes](#) pour des informations détaillées sur ajouter des cartes au Cisco WCS.

### [Cinglez un périphérique de réseau d'un Cisco WLC](#)

Terminez-vous ces étapes afin de cingler d'autres périphériques d'un Cisco WLC :

1. Choisissez le **Configure > Controllers** et cliquez sur une adresse IP sous la colonne d'adresse IP pour avoir l'affichage de Cisco WCS la page de Propriétés de <IPaddress> > de contrôleur.
2. À la page de Propriétés de <IPaddress> > de contrôleur, allez à la barre latérale gauche et choisissez le **système > les commandes** d'avoir l'affichage de Cisco WCS les commandes de

<IPAddress> > de contrôleur paginent.

3. Sur le <IPAddress> > le contrôleur que les commandes paginent, choisissent les **commandes d'administration > le ping** du commutateur et cliquent sur Go.
4. Dans l'entrer une adresse IP (x.x.x.x) pour cingler la fenêtre, écrivez l'adresse IP du périphérique de réseau que le Cisco WLC est de cingler, et cliquez sur OK.
5. Le Cisco WCS affiche la fenêtre de résultats Ping qui affiche les paquets envoyés et reçus. Cliquez sur la **reprise** afin de cingler le périphérique de réseau de nouveau, ou cliquez sur **étroitement** afin de cesser de cingler le périphérique de réseau et fermer la fenêtre de résultats Ping.

## [État en cours, configurations, et statistiques de Cisco WLC de vue](#)

Après que vous ajoutiez des Cisco WLC et la gamme Cisco 1000 IEEE 802.11a/b/g enroule à la base de données de Cisco WCS, vous pouvez visualiser l'état de solution WLAN de Cisco.

**Remarque:** Quand vous recherchez des clients ou des pré-mod. une appliance d'emplacement, vous devez spécifier des contrôleurs WLC dans la base de données WCS. C'est parce que le WCS se transfère toujours sur des « serveurs d'emplacement ».

**Remarque:** L'application WCS doit être arrêté manuellement arrêté avant que vous apportiez toutes les modifications à l'adresse IP du serveur. Si vous redémarrez le serveur sans arrêter l'application, alors il y a des occasions que la base de données pourrait obtenir corrompu.

Dans l'interface utilisateur de Cisco WCS, choisissez le **moniteur > le réseau** afin d'afficher le résumé de réseau de moniteur. Voici un exemple :

Le Cisco WCS recueille périodiquement des statistiques, telles que RSSI, SNR, des pannes de profil, le client compte, le point d'accès non autorisé tend, et les clients occupés, et les organise en états. Utilisez les fenêtres de **moniteur > d'états** afin de visualiser ces états.

Voici un exemple de l'état de compte de client pour les clients 802.11a/b/g pour les sept derniers jours :

Ces états peuvent également être utilisés comme outil efficace de dépannage.

## [Examinez la préparation d'emplacement](#)

L'inspection de la préparation d'emplacement est une fonctionnalité introduite dans la version 2.1.34.0 d'appareils d'emplacement. Avec cette configuration, WCS peut vérifier la capacité du déploiement existant de Point d'accès d'estimer l'emplacement vrai d'un élément à moins de 10 mètres au moins de 90% du temps. Le calcul de préparation d'emplacement est basé sur le nombre et le placement de Points d'accès.

Afin d'examiner la préparation d'emplacement de WCS, choisissez **examinent la préparation d'emplacement** du menu trouvé à la page de **moniteur > de cartes**. Une carte de code à couleurs apparaît qui affiche ces zones qui font (oui) et (non) ne rencontrent pas les 10 mètres, spécification d'emplacement de 90%.

## [Questions de synchronisation avec les serveurs WCS et d'emplacement](#)

Parfois il pourrait y avoir des problèmes avec obtenir WCS synchronisé avec l'appliance d'emplacement. Le schéma de réseau dans le WCS ne pourrait pas synchroniser avec l'appliance d'emplacement. Il y a tout à fait quelques raisons pour ce problème de synchronisation.

- La taille de la conception de réseaux pourrait avoir dépassé la limite maximum de la mi-bande 30. L'ID de bogue Cisco [CSCse60657](#) (clients [enregistrés](#) seulement) aborde cette question plus clair.Par conséquent, alors que vous tentez de synchroniser un diagramme de campus dont la taille globale, y compris le nombre d'intérieur de bâtiments que le campus et le nombre de planchers sur chaque bâtiment, sur une totalité pourraient avoir dépassé la limite maximum de la mi-bande 30, ce processus de synchronisation échoue.Ce problème peut être encore vérifié quand vous visualisez les logs de l'appliance d'emplacement pour ce message.

```
message.TRACE[com.aes] THROW com.aes.server.cmn.AesServerException:
Server Exception: Message sizeexceeded: 37176782
```

 Cette limite dans la taille est surmontée dans la version prochaine WCS.
- Un autre possible raison est que la résolution de l'image chargée dans le WCS est trop élevée, et dépasse probablement la résolution acceptable de 1024x768. Tout en essayant de synchroniser une telle image avec l'appliance d'emplacement, le processus de synchronisation échoue. En pareil cas, réduisez la résolution afin d'aider cette question.
- Assurez-vous que vous exécutez la dernière version sur votre serveur WCS et d'emplacement. Assurez également à cela la correspondance de date et heure exactement sur tous les périphériques.Ceci peut être vérifié quand vous regardez ces sorties.La sortie de la **date** et de l'**heure** commandent sur le WCSSortie de la **date** sur le locserverSortie de la commande de **show time** sur le WLC
- Une autre solution possible est d'arrêter l'emplacement-serveur, et enlève la base de données utilisant cette commande à la console de serveur d'emplacement :

```
rm -rf /opt/locserver/db/linux/server-eng.db
```

 où `/opt/locserver/db/linux/server-eng.db` est le répertoire pour le DB d'emplacement-serveur.Redémarrez le serveur d'emplacement avec la **reprise de /etc/rc.d/init.d/locserver** de commande.Puis essayez pour resynchroniser les périphériques.

## [Questions de synchronisation avec le WCS et le WLC](#)

Les problèmes de synchronisation pourraient se poser entre le WCS et le WLC. En raison de cette question, le nombre de clients actifs pourrait être différent sur le WLC et le WCS. Afin de synchroniser les contrôleurs et le WCS, terminez-vous ces étapes :

1. Choisissez le **Configure > Controllers**, et cliquez sur la case en haut de la liste d'adresse IP pour choisir tous les contrôleurs.
2. Du choisi une liste déroulante de commande, choisissent la **save config pour flasher**.
3. Cliquez sur **OK**.C'est un test de base à vérifier que le SNMP fonctionne correctement, et les contrôleurs suffiront comme le WCS leur indique.
4. Choisissez le **Configure > Controllers**, et cliquez sur la case en haut de la liste d'adresse IP pour choisir tous les contrôleurs.
5. Du choisi une liste déroulante de commande, choisissent **régénèrent le config des contrôleurs**.
6. Cliquez sur **OK**.Cette action indique le WCS croire que les nouvelles informations des contrôleurs au-dessus de quelque chose qu'il précédemment avait su.

## [Configuration DHCP corrompue quand le modèle est poussé de WCS à WiSM](#)

Quand un modèle général est poussé du WCS au Wireless Services Module (WiSM), la configuration du protocole DHCP (DHCP) dans le contrôleur devient corrompue. Le modèle peut avoir exactement les mêmes options qui sont présentes dans le WiSM.

L'effet principal est que des messages d'offre DHCP sont abandonnés, ainsi les clients ne reçoivent pas une adresse DHCP. Ce message est ouvert une session le contrôleur :

```
Thu Jul 13 05:05:07 2006 [VERBOSE] dhcpd.c 164: Dropping packet from
192.168.80.23 (unable to match to a dhcp scope)
```

Ce problème est dû à l'ID de bogue Cisco [CSCse98623](#) (clients [enregistrés](#) seulement). N'utilisez pas les modèles généraux dans le WCS. La configuration doit être restaurée manuellement afin de récupérer l'expédition DHCP. Cette bogue est réparée dans la version 4.0.87.0 et ultérieures de micrologiciels WCS.

## [Les cartes de la chaleur WCS affichent les trous carrés incorrects de couverture](#)

Les cartes de la chaleur WCS affichent les trous carrés incorrects de couverture. Les trous de couverture devraient ne jamais être à angle droit ou rectangle. Le diagramme de rayonnement de carte de la chaleur est circulaire. Cette question est une perforation rectangulaire spécifique sur la carte, qui ne devrait pas être possible. Aucune retouche de suivi n'a été exécutée sur la carte. Avec l'utilisation d'un outil d'arpenteur de site, on le vérifie qu'aucun trou de couverture n'existe. La connexion est très forte dans ces zones.

Ceci est lié à l'ID de bogue Cisco [CSCsf19291](#) (clients [enregistrés](#) seulement). Choisissez la **prévision de Recompute** d'option du menu déroulant et recompute la prévision. La carte de la chaleur devient circulaire et trou carré de couverture n'existe pas. Cette question est réparée dans la version 4.0, mais si vous migrez de la version 3.0 puis la question pourrait exister pour les planchers de petite taille.

## [Quand le modèle de l'escroc AP obtient-il appliqué au WLC ?](#)

Le modèle du point d'accès non autorisé (AP) obtient appliqué au contrôleur seulement si ces deux conditions sont vraies :

- AP sur ce contrôleur a découvert l'escroc AP.
- La tâche de programme de l'escroc AP est terminée.

## [Ports sur le serveur WCS](#)

Quand vous exécutez un Pare-feu sur le serveur où l'application WCS fonctionne, vous devez ouvrir quelques ports afin de communiquer avec le WLC. Il y a quelques services qui dirigent sur les serveurs WCS tels qu'Apache.exe, JavaService.exe, et Solid.exe. Dans TCPView, la sortie ressemble à cette sortie :

```
Apache.exe:1712 TCP 0.0.0.0:443 0.0.0.0:0 LISTENING
JavaService.exe:1680 TCP 0.0.0.0:21 0.0.0.0:0 LISTENING
solid.exe:2672 TCP 0.0.0.0:1315 0.0.0.0:0 LISTENING
```

```
Apache.exe:208 TCP 127.0.0.1:1268 127.0.0.1:8009 ESTABLISHED
JavaService.exe:1680 TCP 127.0.0.1:1067 127.0.0.1:1315 ESTABLISHED
JavaService.exe:1680 TCP 127.0.0.1:1068 127.0.0.1:1315 ESTABLISHED
solid.exe:2672 TCP 127.0.0.1:1315 127.0.0.1:1083 ESTABLISHED
solid.exe:2672 TCP 127.0.0.1:1315 127.0.0.1:1082 ESTABLISHED
```

Afin de fonctionner avec le WLC, ouvrez seulement quelques ports comme l'UDP 161 (SNMP), l'UDP 162 (déroutement SNMP), et le TCP 443 (HTTPS). Cette table affiche une liste de ports ce qui pourrait être utile si une partie du trafic est bloquée.

Service	Ports	Numéros de port
SNMP	UDP	161
Déroutement SNMP	UDP	162
HTTPS	TCP	443
Net d'apparition	TCP	2000
Base de données	TCP	1315
FTP	TCP	21
Connecteur de HTTP	TCP	8457
Le connecteur de HTTP réorientent	TCP	8457
HTTP	TCP	80
RMI	TCP	1299
TFTP	UDP	69
Conteneur de Web	TCP	8009

## [Vérifiez les WLAN sont enable réglé d'exclusivité-liste](#)

Terminez-vous ces étapes afin de vérifier que les WLAN sont **enable** réglé d'exclusivité-liste.

1. Choisissez **configurent > contrôleur**.
2. Cliquez sur en fonction une adresse IP sous la colonne d'adresse IP.
3. Clic **WLAN** du côté gauche.
4. Cliquez sur en fonction chaque ID de WLAN afin de vérifier qu'il n'est pas placé à **vérifié**.

## [Dépannez l'enable d'exclusivité-liste](#)

Terminez-vous ces étapes afin de dépanner l'**enable d'exclusivité-liste**.

1. Dépistez le client.
2. Vérifiez le WLAN pour le client d'exclusion.
3. Sélectionnez le client exclusif **pour supprimer**.
4. Supprimez les clients de l'exclusivité-liste sous le contrôleur spécifié.

## [Clients globalement handicapés de vue et d'effacement](#)

Terminez-vous ces étapes afin de visualiser et supprimer les clients globalement handicapés.

1. Choisissez le **moniteur > les périphériques > les clients**.
2. De clic **clients handicapés manuellement**.
3. Sélectionnez l'adresse MAC pour accéder à cette page.
4. Cliquez sur **Delete**.



## Clients handicapés de vue et d'effacement manuellement par contrôleur

Pour des raisons de sécurité et plusieurs autres raisons, certains clients peuvent être mis sur la liste noire en tant que « clients manuellement handicapés ».

Terminez-vous ces étapes afin de visualiser manuellement les clients handicapés individuellement sur chaque contrôleur ajouté au WCS :

1. Allez au GUI WCS.
2. Choisissez le **Configure > Controllers**.
3. Cliquez sur en fonction l'adresse IP sous la colonne d'adresse IP pour le contrôleur auquel a manuellement désactivé le besoin des clients d'être visualisé.
4. À la page qui paraît, choisissez la **Sécurité** et cliquez sur **manuellement les clients handicapés** afin d'afficher la liste de clients manuellement handicapés pour ce contrôleur particulier.

Du menu déroulant du côté gauche, choisissez les **clients handicapés d'effacement manuellement** afin de supprimer manuellement les clients handicapés.

## WCS recherchent des clients par bâtiment ne fonctionnent pas

Ce problème peut être dû à l'ID de bogue Cisco [CSCse97619](#) (clients [enregistrés](#) seulement). Un WCS recherche des clients sur un plancher sur des travaux d'un bâtiment correctement, mais les clients d'un rechercher sur tous les planchers dans un bâtiment ne travaille pas. La difficulté pour cette bogue est disponible avec la version 4.0.87.0 WCS. Si vous utilisez des versions WCS plus tôt que 4.0.87.0, le contournement est de rechercher des clients dans une surface couverte.

## Comptes incorrects de client d'états WCS associés aux aps en mode H-REAP

Ce problème est dû à l'ID de bogue Cisco [CSCsg48059](#) (clients [enregistrés](#) seulement). WCS signale les comptes de client qui sont trop élevés quand H-REAP est activé sur le contrôleur. Le contournement à découvrir combien de clients sont associés aux aps ou le contrôleur donné est d'utiliser la caractéristique de Monitor > Clients WCS, la recherche par AP ou le contrôleur, qui sont limités par le type par radio pour éviter des doublons, et utilisent le nombre total d'éléments trouvés en tant que votre véritable nombre de population. La table de bsnMobileStation a également le nombre de lignes correct pour le nombre de clients. Vous pouvez également employer le WLC pour trouver le compte correct de client.

## WCS ne commence pas si le trait de soulignement est configuré dans le serveur/adresse Internet

Le «\_des caractères de soulignement » ne sont pas pris en charge dans le nom du serveur WCS. Si vous utilisez un trait de soulignement dans le nom d'hôte de serveur/sur une installation WCS, WCS ne commence pas. L'installation du logiciel ne signale aucune question et l'installe en tant que normale, mais le RFC-952 déclare que le trait de soulignement est un caractère sans support, qui est pourquoi ceci fait échouer le logiciel WCS.

## L'ERREUR [emplacement] n'a pas créé la carte de la chaleur pour le MAC : xx : xx : xx : xx : xx : xx raison : Manqué car la liste RSSI est vide après élagage de temps

Il est essentiel que les contrôleurs, les serveurs d'emplacement, et le WCS tout le Protocole NTP (Network Time Protocol) d'utilisation d'assurer l'heure locale précise. Le serveur d'emplacement relâche n'importe quelle date du contrôleur qui est en dehors de sa fenêtre de 15 minutes.

Le contrôleur garde seulement une fois intérieurement mais la modifie pour l'affichage si un décalage est spécifié. Si vous spécifiez un décalage, vous dites au contrôleur que le temps ce qui a été écrit était le temps UTC [heure locale pour Londres, le R-U] et que vous voulez que le contrôleur affiche votre heure locale en plus du décalage. Le NTP a lieu toujours dans le temps UTC, et un décalage est exigé si vous voulez que le contrôleur l'affiche dans votre heure locale. Par exemple, l'est a un décalage de -5. Si vous faites configurer le NTP, le contrôleur a le temps UTC mais ajoute le décalage pour avoir l'heure locale pour les horodateurs dans les logs.

Le contrôleur, le serveur d'emplacement, et le WCS **doivent** tout être à moins de temps interne de 15 minutes (pas heure locale [temps interne avec le décalage]), ou le serveur d'emplacement n'affiche pas ou dépiste des clients ; au lieu de cela il affiche ce message d'erreur dans le journal du serveur d'emplacement :

```
3/08/07 00:46:59 ERROR[location] Failed to create heat map for MAC: xx:xx:xx:xx:xx:xx Reason:
Failed as the RSSI list is empty after time pruning
```

Le serveur d'emplacement a seulement assez de mémoire en temps réel pour les 15 dernières minutes de données stockées. Souvenez-vous que le serveur d'emplacement dépiste des clients en temps réel, alors que le WCS archive les données au-dessus de plus longues périodes. WCS peut dépister des clients mais des mises à jour seulement toutes les quelques minutes - non en temps réel. Si les horloges sont hors fonction entre les périphériques, il n'y a aucune donnée de client après que le serveur d'emplacement retire ceux extérieur l'intervalle de temps spécifié dans la demande. En fait, si le serveur d'emplacement reçoit des données du contrôleur avec l'horodateur interne plus de 15 minutes en dehors de son temps interne, il jette les données en l'air dans la position de bit.

Vous devez activer le NTP pour que le WLC, le WCS, et le serveur d'emplacement synchronise automatiquement le temps interne à l'UTC.

### [Le message d'erreur « que l'entrée Point Filfexp Could de procédure pas se trouvent dans des affichages de la bibliothèque de liens dynamiques le DFORRT.DLL »](#)

Si WCS utilise une application de tiers, telle que le compilateur MATLAB, et MATLAB utilise une version spécifique de la bibliothèque DFORRT.dll, quand une application a déjà installé la bibliothèque DFORRT.dll dans c:\windows\system32, le WCS n'est pas correctement installé. En conséquence, quand vous commencez WCS, affichages de ce message d'erreur :

```
The procedure entry point _FIIfexp_ could not be located in the dynamic link library DFORRT.DLL
Afin de corriger le problème, retirez le fichier DFORRT.dll dans c:\windows\system32 et réinstallez
WCS.
```

### [Instructions à la synchronisation les trois périphériques](#)

**Pour le serveur d'emplacement :** Référez-vous au [guide d'installation et de configuration](#) pour les informations dans la configuration initiale.

Après que l'appliance soit commencée, vous devez arrêter le serveur d'emplacement avant que vous puissiez changer la date, chronométrez, ou fuseau horaire. Suivez ces étapes :

1. Afin de changer le fuseau horaire d'appareils d'emplacement, copiez le fichier approprié de fuseau horaire sur `/etc/localtime` :# `cp /usr/share/zoneinfo/<your country>/<your timezone>/etc/localtime`
2. Vérifiez que le fichier `/etc/sysconfig/clock` est défini en tant qu'est ceci sans n'importe quelle ZONE spécifiée :# `more /etc/sysconfig/clock`

```
UTC=true  
ARC=false
```

3. Vérifiez la date et l'heure avec la commande de **date** sur le serveur CLI d'emplacement. #  
`date`
4. Redémarrez le serveur d'emplacement avec les instructions disponibles chez [http://www.cisco.com/en/US/products/ps6386/products\\_qanda\\_item09186a008078ece3.shtml#qa13](http://www.cisco.com/en/US/products/ps6386/products_qanda_item09186a008078ece3.shtml#qa13)

**Remarque:** Si vous voulez utiliser le serveur de NTP pour l'appliance d'emplacement, référez-vous à [configurer le serveur de NTP](#).

**Pour le WCS :** WCS se fonde sur Windows pendant le temps correct. Il vérifie le système d'exploitation windows une fois toutes les 24 heures pour l'heure système. Il ne sait pas immédiatement des modifications heure système à moins que vous arrêtiez et redémarriez le serveur WCS. Cliquez avec le bouton droit l'horloge et choisissez l'heure de modification/date. Employez une source temporelle de NTP pour régler l'horloge et pour placer manuellement le décalage pour votre fuseau horaire. Typiquement ceci est déjà placé.

**Pour le contrôleur :** Sur le contrôleur, utilisez le **show clock** de commande CLI pour vérifier le temps et le décalage. Vous pouvez faire ceci par le GUI, aussi bien. Décochez la case à cocher DST ou utilisez le **débronnement -8 de config time timezone** de commande `0 -8 0`.

Après que vous terminiez la synchronisation horaire entre les périphériques, vous devez synchroniser le serveur d'emplacement avec le WCS (sous l'emplacement-serveur > **synchronisez**). Ceci est fait de sorte qu'ils aient les mêmes données avec les mêmes horodateurs.

Notez que les WCS, le contrôleur, et le logiciel d'emplacement sont libérés à la même date.

## [Le modèle WLAN n'applique pas la configuration correcte de « Broadcast SSID » dans le WLC](#)

Après que vous créez des modèles WLAN et les chargiez dans le WLC par WCS, les restes de champ de « Broadcast SSID » ont signé l'écran individuel de configuration du contrôleur WLAN, indépendamment de la configuration dans le modèle WCS WLAN. Ceci annonce toujours les informations WLAN SSID.

Afin de désactiver l'émission SSID sur le modèle du courant WLAN avec WCS, exécutez ces étapes dans WCS avec des versions plus tôt que 4.1.83.

**Remarque:** Si vous améliorez le WCS à la version 4.1.83, elle résout également ce problème. En outre, de tels problèmes se posent principalement quand le contrôleur et les WCS sont hors de sync. En pareil cas, synchronisez le WLC et le WCS.

1. Dans le modèle WCS WLAN, le débronnement ou décochent la case d'état d'**admin** et s'assurent que le **Broadcast SSID** est décoché.
2. Sauvegardez le modèle.
3. Appliquez le modèle au contrôleur.

4. Réactivez la case d'admin de ce WLAN.
5. Sauvegardez le modèle
6. Appliquez le modèle au contrôleur de nouveau.

Maintenant, vous pouvez trouver le champ de « Broadcast SSID » comme arrêté dans la configuration individuelle WLAN du contrôleur.

## [Les modèles WLAN n'affichent pas la configuration correcte de case à cocher de 7920 CAC](#)

Quand vous créez des modèles WLAN pour pousser les WLAN aux contrôleurs, vérifiez la case à cocher de 7920 CAC pour activer cette caractéristique et pour la sauvegarder et l'afficher à nouveau que le même WLAN. Le modèle affiche comme décoché quoiqu'il soit vraiment vérifié et active cette caractéristique sur le contrôleur une fois poussé à lui.

Ce doit introduire des erreurs pour tests [CSCsi77521](#), qui est associé avec cette question.

Améliorez le WCS à la version 4.1 pour résoudre ce problème.

## [Incapable de supprimer les contrôleurs hors ligne de la version 3.2.51.0 WCS](#)

Dans certains cas, les utilisateurs ne peuvent pas supprimer WLCs qui ne sont plus utilisés du WCS. C'est en raison des questions avec la structure de base de données de WCS dans la version 3.2.51.0 ; en conséquence, WCS tend à bloquer des ressources. La base de données entière a été restructurée dans la version 4.0 et a amélioré le niveau des performances.

Il y a deux contournements pour cette question :

- Supprimez les rapports de contrôle et puis supprimez le contrôleur **ou**
- Mise à jour à WCS 4.0.87.0 et plus tard

Avec le premier choix, afin de supprimer les contrôleurs autonomes, faites ceci :

1. Quand WCS surveille un groupe très grand de contrôleurs, la meilleure chose est à d'abord supprimer les rapports de contrôle de ces contrôleurs, un, et puis essayent de supprimer ces contrôleurs. Afin de supprimer les rapports de contrôle, suivez ces étapes :Allez **configurer le contrôleur**.Cochez la case du contrôleur désiré. On permet seulement un contrôleur à la fois.Choisissez les **rapports de contrôle de vue de** commande de la liste déroulante.Cliquez sur le bouton d'**aller**.Supprimez les rapports de contrôle.Puis essayez pour supprimer les contrôleurs.
2. Essayez cette procédure sur tous autres contrôleurs. Assurez-vous que les comptes utilisateurs que vous utilisez pour effectuer ces tâches font partie du groupe de super utilisateur.Occasionnellement, il supprime certains des rapports de contrôle mais de non tous états pour un contrôleur spécifique.
3. Les rapports de contrôle qui ont l'état de synchronisation de **mêmes dans WCS et contrôleur** peuvent être avec succès supprimés, mais des rapports de contrôle avec l'état de synchronisation de **différent dans WCS et le contrôleur** ne peuvent pas être supprimés.
4. Vous pouvez voir ce message d'erreur quand vous essayez de supprimer des rapports de contrôle avec l'état de **différent dans WCS et contrôleur**.The resource you are trying to delete seems to be busy
5. Dans ce cas, le contrôleur ne peut pas être supprimé. Ce message d'erreur signifie que la

base de données a verrouillé la ressource. Ceci peut se produire si l'utilisateur frappait le bouton d'effacement, n'a pas attendu assez longtemps, et a alors frappé le *dos* pour aller à la page précédente. C'était une question dans la version 3.2 ; juste attendez et voyez si la ressource libère.

Alternativement, vous pouvez utiliser la deuxième option d'améliorer WCS à 4.0.87.0 ou en haut, qui a de grandes améliorations des performances de 3.2 dus à une restructuration de la base de données WCS.

## [Ne peut pas ajouter le modèle d'authentification Web avec le par défaut de type interne de WCS](#)

Afin d'essayer de pousser le modèle, l'**exécution SNMP de message d'erreur au périphérique a manqué** apparaît.

C'est en raison de la bogue CSCsh89306. WCS donne l'erreur SNMP quand il pousse un modèle d'authentification Web à un contrôleur qui exécute la version 4.0.206.0.

Le contournement est de configurer une authentification Web directement sur le contrôleur.

1. Naviguez vers la page de modèle de personnalisation d'authentification Web.
2. Choisissez le type d'authentification Web comme **externe**.
3. Entrez dans un certain texte factice URL.
4. Changez le type d'authentification Web **pour transférer interne**.
5. Écrivez une coutume réorientent l'URL.
6. Sauvegardez et appliquez le modèle.

Fondamentalement, l'externe et les faits sur commande réorientent l'URL ne doivent pas être blanc de gauche à la page même si elles ne sont pas appropriées au type d'application en cours d'authentification Web.

## [Informations connexes](#)

- [Dépannage du système de contrôle sans fil \(WCS\) - Forum Aux Questions](#)
- [Guide de configuration de Système de contrôle sans fil Cisco, version 4.0](#)
- [Système de contrôle sans fil Cisco](#)
- [Page de prise en charge du mode sans fil](#)
- [Support et documentation techniques - Cisco Systems](#)