

# Configurer les points d'accès Cisco Clean-Air sur Mobility Express

## Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Informations générales](#)

[Configuration](#)

[Activer l'air pur](#)

[Spécifier les périphériques d'interférence à détecter](#)

[Activer les alarmes Clean-Air](#)

[Gestion des ressources radio pilotées par les événements \(EDRRM\)](#)

[Vérification](#)

[Dépannage](#)

## Introduction

Ce document décrit les étapes à suivre pour configurer Cisco Clean-Air sur les points d'accès express Cisco Mobility.

## Conditions préalables

### Conditions requises

Cisco recommande que vous connaissiez Cisco Mobility Express qui exécute le code 8.3 et supérieur.

### Components Used

Les informations de ce document sont basées sur le point d'accès Cisco 2802 qui exécute le logiciel Mobility Express version 8.5.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

## Informations générales

Les systèmes LAN sans fil fonctionnent dans des bandes ISM (industriel, scientifique et médical) 2,4 et 5 GHz sans licence. De nombreux périphériques tels que les fours à micro-ondes, les téléphones sans fil et les périphériques Bluetooth fonctionnent également dans ces bandes et

peuvent affecter négativement les opérations Wi-Fi. Cisco CleanAir est une solution d'intelligence spectrale capable de détecter les sources d'interférence non Wi-Fi dans votre réseau. Elle vous permet également, vous ou votre réseau, d'agir sur ces informations.

Par exemple, vous pouvez supprimer manuellement le périphérique qui interfère, ou le système peut modifier automatiquement le canal à partir de l'interférence. CleanAir assure la gestion du spectre et la visibilité des radiofréquences (RF).

Les points d'accès Clean-Air collectent des informations sur tous les périphériques qui fonctionnent dans les bandes ISM, identifient et évaluent les informations comme source d'interférence potentielle, et les transmettent au WLC Cisco. Pour chaque périphérique qui fonctionne dans la bande sans licence, Cisco CleanAir vous indique ce qu'il est, où il se trouve et comment il affecte votre réseau sans fil.

Pour plus d'informations sur la fonction Clean-Air, reportez-vous à ce livre blanc.

[https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/cleanair-technology/white\\_paper\\_c11-599260.html](https://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/cleanair-technology/white_paper_c11-599260.html)

## Configuration

### Activer l'air pur

Clean-Air peut être activé au niveau du réseau ou à un niveau spécifique du point d'accès. Afin de l'activer globalement, exécutez la commande **config {802.11a | 802.11b} cleanair enable network**.

For ex:

```
(Cisco Controller) >config 802.11a cleanair enable network
```

Il peut également être activé au niveau du point d'accès avec la commande **config{802.11a | 802.11b}cleanair enable ap\_name**.

For ex:

```
(Cisco Controller) >config 802.11a cleanair enable AP-3702
```

### Spécifier les périphériques d'interférence à détecter

Les points d'accès associés au WLC Cisco envoient des rapports d'interférence uniquement pour les types d'interférence qui ont été activés. Cette fonctionnalité vous permet de filtrer les interférences qui peuvent inonder le réseau et causer des problèmes de performances. Afin de configurer la détection des interférences et de spécifier les sources d'interférence qui doivent être détectées, exécutez la commande **config {802.11a | 802.11b} dispositif cleanair {enable | disable} device\_type**.

For example:

```
(Cisco Controller) >config 802.11a cleanair device enable all
```

### Activer les alarmes Clean-Air

La technologie Cisco CleanAir fournit de nombreuses informations détaillées sur les sources d'interférence détectées. Mais pour faciliter une compréhension instantanée de l'impact des problèmes d'interférence sur le réseau, il regroupe les informations détaillées dans une métrique de haut niveau, facile à comprendre, appelée qualité de l'air (AQ). Une valeur de 100 signifie que la qualité de l'air est la plus élevée et une valeur de 1 représente la pire qualité de l'air. Clean-Air peut être configuré pour envoyer des alarmes lorsque la qualité de l'air d'un point d'accès particulier tombe sous un seuil particulier. Afin de configurer les déclencheurs des alarmes de qualité de l'air, exécutez la commande **config {802.11a | 802.11b} cleanair alarme air-qualité {enable | disable}**. La valeur par défaut est activée.

- L'utilisateur peut spécifier le seuil auquel les alarmes de qualité de l'air doivent être déclenchées. Pour cela exécutez la commande **config {802.11a | 802.11b} seuil de qualité de l'air d'alarme cleanair**. où threshold est une valeur comprise entre 1 et 100 (inclus). Lorsque la qualité de l'air est inférieure au seuil, l'alarme est déclenchée.
- Vous pouvez activer les déclencheurs d'une alarme d'interférence. Exécutez la commande **config {802.11a | 802.11b} dispositif d'alarme cleanair {enable | disable}**. La valeur par défaut est enable.
- Afin de spécifier les sources d'interférence qui déclenchent des alarmes, exécutez la **commande config {802.11a | 802.11b} type de périphérique d'alarme cleanair {enable | disable}**.

For example:

```
(Cisco Controller) >config 802.11a cleanair alarm device enable all
```

## Gestion des ressources radio pilotées par les événements (EDRRM)

EDRRM est une fonctionnalité d'air pur qui peut déclencher un changement de canal en fonction de la gravité de la source d'interférence. Par exemple, un téléphone sans fil avec un signal FM continu peut provoquer une panne de plusieurs minutes (tant que le téléphone est actif). Cela peut provoquer une baisse spectaculaire de la qualité de l'air de n'importe quel point d'accès voisin. EDRRM fait en sorte que le système évalue et modifie immédiatement le canal du point d'accès affecté. Si c'est possible, il va de l'avant et change de canal. En raison de l'absence de canaux supplémentaires sur la radio 802.11b, il est recommandé d'activer cette fonctionnalité uniquement sur la bande 802.11a. EDRRM peut être activé avec la commande **config advanced {802.11a | 802.11b} channel cleanair-event {enable | disable}**. Par défaut, cette option est désactivée.

Vous pouvez également spécifier le seuil à partir duquel le RRM doit être déclenché. Lorsque le niveau d'interférence pour le point d'accès monte au-dessus du niveau de seuil, RRM lance une exécution DCA (Dynamic Channel Assignment) locale et modifie le canal de la radio AP affectée si possible pour améliorer les performances du réseau. Faible représente une sensibilité moindre aux changements dans l'environnement, tandis qu'élevée représente une sensibilité accrue. Vous pouvez également définir la sensibilité à un niveau personnalisé de votre choix. La valeur par défaut est medium. **config advanced {802.11a | 802.11b} sensibilité aux événements cleanair du canal {low | moyen | élevé | personnalisé}**

Si vous définissez la sensibilité de seuil comme personnalisée, vous devez définir une valeur de seuil personnalisée. Il est défini par défaut à 35. **config advanced {802.11a | 802.11b} seuil de sensibilité aux événements cleanair-channel**

## Vérification

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

Vous pouvez afficher la configuration de Cisco CleanAir pour le réseau 802.11a/n ou 802.11b/g/n. Exécutez la commande **show {802.11a | 802.11b} cleanair config**. Des informations similaires à celles-ci apparaissent.

```
(Cisco Controller) >show 802.11a cleanair config
Clean Air Solution..... Enabled
Air Quality Settings:
  Air Quality Reporting..... Enabled
  Air Quality Reporting Period (min)..... 15
  Air Quality Alarms..... Enabled
  Air Quality Alarm Threshold..... 35
  Unclassified Interference..... Disabled
  Unclassified Severity Threshold..... 20
Interference Device Settings:
  Interference Device Reporting..... Enabled
Interference Device Types:
  TDD Transmitter..... Enabled
  Jammer..... Enabled
  Continuous Transmitter..... Enabled
Interference Device Alarms..... Enabled
Interference Device Types Triggering Alarms:
  TDD Transmitter..... Disabled
  Jammer..... Enabled
  Continuous Transmitter..... Disabled
Additional Clean Air Settings:
  CleanAir ED-RRM State..... Disabled
  CleanAir ED-RRM Sensitivity..... Medium
  CleanAir ED-RRM Custom Threshold..... 50
  CleanAir Persistent Devices state..... Disabled
  CleanAir Persistent Device Propagation..... Enabled
```

Vous pouvez également afficher la configuration et l'état propres à un point d'accès individuel. Exécutez la commande **show ap config {802.11a | nom\_ap 802.11b}**.

For ex:

```
(Cisco Controller) >show ap config 802.11a AP-3702
CleanAir Management Information
  CleanAir Capable..... Yes
  CleanAir Management Administration St.... Enabled
  CleanAir Management Operation State..... Up
  Rapid Update Mode..... Off
  Spectrum Expert connection..... Enabled
  CleanAir NSI Key..... ED1EF0A5BCD83D2BE7124DCB3D975555
  Spectrum Expert Connections counter.... 0
  CleanAir Sensor State..... Configured
```

Vous pouvez consulter les informations sur la qualité de l'air de tous les points d'accès. Exécutez la commande **show {802.11a | 802.11b} résumé de la qualité de l'air pur**.

For ex:

```
(Cisco Controller) >show 802.11a cleanair air-quality summary
```

AQ = Air Quality

DFS = Dynamic Frequency Selection

```
AP Name          Channel Avg AQ Min AQ Interferers DFS
-----
```

Afin d'afficher des informations détaillées sur les périphériques d'interférence détectés par un point d'accès particulier, exécutez la commande **show {802.11a | 802.11b} cleanair device ap\_name**.

Afin d'afficher des détails sur chaque type de périphérique d'interférence vu, exécutez la commande **show {802.11a | 802.11b} cleanair device type device\_type**.

## Dépannage

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.