



## **GUIDE DE DÉMARRAGE**



### **Points d'accès autonomes de la gamme Cisco Aironet 1140**

- 1** À propos du présent guide
- 2** Consignes de sécurité
- 3** Présentation générale
- 4** Obtention et attribution d'une adresse IP
- 5** Installation du point d'accès
- 6** Configuration des paramètres de base
- 7** Dépannage
- 8** Caractéristiques du point d'accès
- 9** Obtenir de la documentation et envoyer une demande de service
- 10** Déclarations de conformité et informations réglementaires

**Remarque**

Pour consulter les documents en français (y compris les nouveautés), identifiez-vous : [www.cisco.com/cisco/web/CA/fr/support/index.html](http://www.cisco.com/cisco/web/CA/fr/support/index.html)

# 1 À propos du présent guide

Ce guide vous explique comment installer et configurer votre Points d'accès autonomes de la gamme Cisco Aironet 1140. Ce guide présente également les instructions de montage et certaines procédures de dépannage.

# 2 Consignes de sécurité

Les mises en garde traduites sont regroupées dans un document livré avec votre point d'accès. Elles figurent également dans les *mises en garde traduites pour les points d'accès Cisco Aironet*, lesquelles peuvent être consultées sur le CD de documentation et sur Cisco.com.

**Attention****CONSIGNES DE SÉCURITÉ IMPORTANTES**

**Ce symbole de mise en garde signale un danger. Vous vous trouvez dans une situation pouvant entraîner des blessures ou des dommages corporels. Avant de travailler sur un équipement donné, tenez compte des risques relatifs aux circuits électriques et familiarisez-vous avec les procédures couramment utilisées pour éviter les accidents. Utilisez le numéro d'énoncé indiqué à la fin de chaque mise en garde pour retrouver sa traduction parmi les mises en garde relatives à la sécurité fournies avec ce périphérique.** Énoncé 1071

**CONSERVEZ CES INSTRUCTIONS****Attention**

**Avant de brancher le système sur la source d'alimentation, consultez les instructions d'installation.** Énoncé 1004

**Attention**

**Ce produit doit être connecté à une source électrique PoE (Power over Ethernet) conforme à la norme IEEE 802.3af ou à une source électrique limitée conforme à la norme IEC60950.** Énoncé 353

**Attention**

**Cet équipement doit être mis à la terre en externe à l'aide d'un câble de mise à la terre fourni par l'utilisateur, avant la mise sous tension. En cas de doute sur l'adéquation de la mise à la terre disponible, adressez-vous à l'organisme responsable de la sécurité électrique ou à un électricien.** Énoncé 366

**Attention**

**L'installation de l'équipement doit être conforme aux réglementations électriques locales et nationales en vigueur.** Énoncé 1074

**Attention**

**Un système de protection contre les courts-circuits (surintensité) doit être installé dans le bâtiment où ce produit est utilisé. Assurez-vous que l'intensité nominale du dispositif de protection n'est pas supérieure à : 20 A.** Énoncé 1005

**Attention**

**À moins de l'avoir préalablement modifié pour le rendre propre à cet usage, n'utilisez pas votre périphérique réseau sans fil près d'amorces non protégées ni dans un environnement présentant des risques d'explosion.** Énoncé 245B

**Attention**

**Pour respecter les limites FCC d'exposition aux fréquences radio (RF), les antennes doivent être placées à 20 cm (7,9 po) au moins de toute personne.** Énoncé 332

**Avertissement**

Lorsque vous montez le point d'accès sur un mur ou un plafond, veillez à utiliser des fixations appropriées. Celles-ci doivent supporter une force de traction minimale de 9 kg (20 livres) et doivent utiliser les 4 orifices du support de montage extra-plat.

**Avertissement**

Conformément à la définition de l'Environnement A de la norme IEEE 802.af, ce produit et tous les équipements interconnectés, y compris les connexions LAN associées, doivent être installés à l'intérieur d'un même bâtiment.



---

**Remarque**

Le point d'accès est adapté à une utilisation dans un espace de ventilation, conformément à la section 300.22.C du National Electrical Code et aux sections 2-128, 12-010(3) et 12-100 du Code canadien de l'électricité, partie 1, C22.1. N'installez pas le module d'alimentation ni l'injecteur de puissance dans des espaces de ventilation.

---



---

**Remarque**

Utilisez uniquement avec l'équipement ITE référencé.

---

## 3 Présentation générale

Cette section explique les tâches à accomplir avant d'installer le point d'accès 1140.

### Vérification des composants livrés

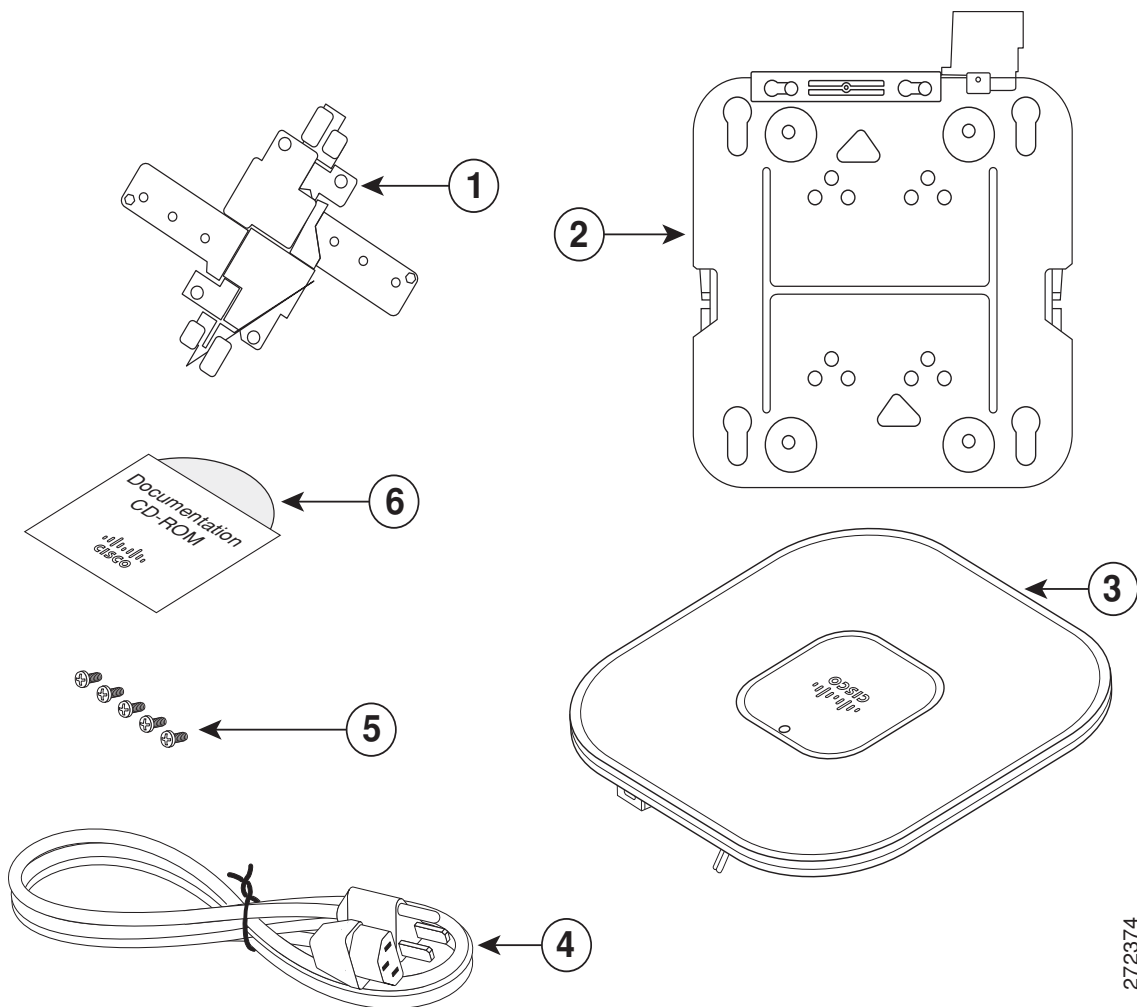
Déballez et vérifiez le contenu du point d'accès 1140 et du kit d'accessoires, comme suit :

- 
- Étape 1** Déballez et retirez le point d'accès et le kit d'accessoires du carton d'expédition.
  - Étape 2** Remettez l'emballage dans le conteneur d'expédition et conservez-le pour une utilisation ultérieure.
  - Étape 3** Vérifiez que vous avez reçu les éléments présentés à la Figure 1. Si des éléments sont manquants ou endommagés, contactez votre représentant ou revendeur Cisco, pour connaître la marche à suivre.
- 

### Ports et composants principaux

Avant de poursuivre l'installation, familiarisez-vous avec le point d'accès. La Figure 2 montre les composants principaux du point d'accès.

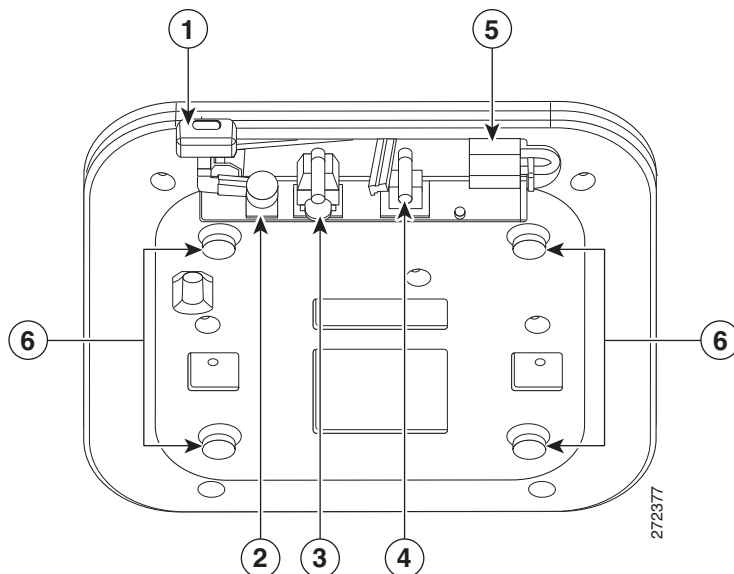
**Figure 1 Contenu de la boîte d'expédition**



272374

<b>1</b>	Attache standard ajustable pour rail en T sur plafond	<b>5</b>	Vis à tête plate 0,63 cm (6,32 x 1/4 po)
<b>2</b>	Support de montage extra-plat	<b>6</b>	CD-ROM de documentation
<b>3</b>	Point d'accès 1140		Alimentation CC (non illustrée, en option)
<b>4</b>	Cordon d'alimentation CA (en option)		

**Figure 2** Ports et connexions du point d'accès



<b>1</b>	Logement pour verrou Kensington	<b>4</b>	Port de console
<b>2</b>	Connexion de l'alimentation	<b>5</b>	Cadenas et loquet de sécurité
<b>3</b>	Port Ethernet	<b>6</b>	Broches du support de montage extra-plat (pieds pour montage sur bureau ou plateau)

## Réalisation d'une étude de site

Avant le montage et le déploiement de votre point d'accès, nous vous recommandons de réaliser une étude de site (ou d'utiliser un outil de planification de site), afin de déterminer le meilleur emplacement pour l'installation de votre point d'accès.

Vous devez disposer des informations suivantes au sujet de votre réseau sans fil :

- Emplacements du point d'accès.
- Options de montage du point d'accès : sous un faux-plafond, sur une surface horizontale plane ou sur un bureau.



### Remarque

Vous pouvez installer le point d'accès au-dessus d'un faux plafond, mais procurez-vous, pour ce faire, du matériel de montage supplémentaire : reportez-vous à la section « Installation du point d'accès » à la page 9, pour obtenir des informations complémentaires.

- Options d'alimentation du point d'accès : l'électricité est fournie par une alimentation CC, par le PoE d'un périphérique du réseau ou par un injecteur de puissance/concentrateur PoE (généralement placé dans une armoire de répartition).



### Remarque

Pour respecter la réglementation applicable en matière de sécurité, faites en sorte que les points d'accès montés dans l'espace de ventilation environnemental d'un bâtiment sont alimentés par un PoE.

Cisco vous recommande d'établir un plan du site montrant les emplacements des points d'accès, afin de pouvoir enregistrer les adresses MAC des périphériques de chaque emplacement et de les transmettre au responsable de la planification ou de la gestion de votre réseau sans fil.

## 4 Obtention et attribution d'une adresse IP

Pour accéder à la page Express Setup du point d'accès, vous devez obtenir une adresse IP pour le point d'accès ou lui en attribuer une, en appliquant l'une des méthodes suivantes :



### Remarque

Le point d'accès ne possède pas d'adresse IP par défaut.

- Attribuez une adresse IP statique au point d'accès en vous connectant à son port de console et en ouvrant son interface de ligne de commande.
- Utilisez un serveur DHCP (si disponible) pour attribuer automatiquement une adresse IP au point d'accès. Pour déterminer l'adresse IP attribuée par le serveur DHCP, utilisez l'une des méthodes suivantes :
  - Pour afficher l'adresse IP, connectez-vous au port de console du point d'accès et utilisez une commande Cisco IOS telle que **show interface bvi1**.
  - Fournissez l'adresse MAC de votre point d'accès à l'administrateur réseau de votre entreprise. Ce dernier va interroger le serveur DHCP à l'aide de l'adresse MAC, pour identifier l'adresse IP. L'adresse MAC se trouve sur une étiquette située sur la partie inférieure du point d'accès.
  - Pour identifier l'adresse IP attribuée, utilisez l'interface de ligne de commande et le port série.

## Connexion locale au point d'accès

Pour configurer localement le point d'accès (sans le connecter à un réseau local câblé), vous pouvez connecter un ordinateur à son port de console, à l'aide d'un câble série DB-9 vers RJ-45.



### Avertissement

Soyez prudent lorsque vous manipulez le point d'accès : la plaque inférieure peut être brûlante.

Pour ouvrir l'interface de ligne de commande en vous connectant au port de console du point d'accès, procédez comme suit :

**Étape 1** Connectez une extrémité du câble série femelle à neuf broches DB-9 vers RJ-45 au port de console RJ-45 du point d'accès et l'autre extrémité, au port COM de l'ordinateur.



### Remarque

La référence Cisco du câble série est AIR-CONCAB1200.

**Étape 2** Configurez un émulateur de terminal sur l'ordinateur pour qu'il communique avec le point d'accès. Utilisez les paramètres suivants pour établir la connexion d'émulation de terminal : 9 600 bauds, 8 bits de données, aucune parité, 1 bit d'arrêt et aucun contrôle de flux.

## Attribuez l'adresse IP à l'interface BVI

Si vous attribuez une adresse IP au point d'accès à l'aide de l'interface de ligne de commande, vous devez également l'attribuer à l'interface BVI. En mode EXEC privilégié, procédez comme suit pour attribuer une adresse IP à l'interface BVI du point d'accès, à l'aide du port de console.

	Commande	Objectif
Étape 1	<code>configure terminal</code>	Passer en mode de configuration globale
Étape 2	<code>interface bvi1</code>	Passer en mode de configuration de l'interface BVI
Étape 3	<code>ip address <i>adresse_ip masque_de_sous-réseau</i></code>	Attribuer une adresse IP et une adresse de masque de sous-réseau à l'interface BVI.

## Attribution d'une adresse IP via l'interface de ligne de commande

Suivez les étapes ci-dessous pour accéder à l'interface de ligne de commande via une session Telnet. Ces étapes sont destinées à un PC fonctionnant sous Microsoft Windows et disposant d'une application de terminal Telnet. Pour plus d'informations, reportez-vous à la documentation de votre PC.

---

**Étape 1** Sélectionnez **Démarrer > Programmes > Accessoires > Telnet**.

Si Telnet n'apparaît pas dans le menu Accessoires, sélectionnez **Démarrer > Exécuter**, saisissez **Telnet** dans le champ textuel et appuyez sur **Entrée**.

**Étape 2** Lorsque la fenêtre Telnet s'affiche, cliquez sur **Connect** et sélectionnez **Remote System**.

**Étape 3** Dans le champ Host Name, saisissez l'adresse IP du point d'accès et cliquez sur **Connect**.



### Remarque

---

Si vous êtes connecté au point d'accès via une session Telnet, vous perdez cette connexion lorsque vous attribuez une nouvelle adresse IP à l'interface BVI. Si vous devez poursuivre la configuration du point d'accès via Telnet, utilisez la nouvelle adresse IP pour ouvrir une autre session Telnet vers le point d'accès.

---

## 5 Installation du point d'accès

Cette section décrit comment monter, relier à la terre et fixer le point d'accès.

### Montage du point d'accès

Cette section décrit comment monter le point d'accès à l'aide du matériel de montage fourni. Pour monter le point d'accès sur toute surface horizontale plane ou sous un faux plafond encastré ou standard, utilisez le support de montage extra-plat fourni (reportez-vous à la Figure 3). Si vous montez le point d'accès sur une table ou un bureau, le support de montage extra-plat n'est pas nécessaire.



### Remarque

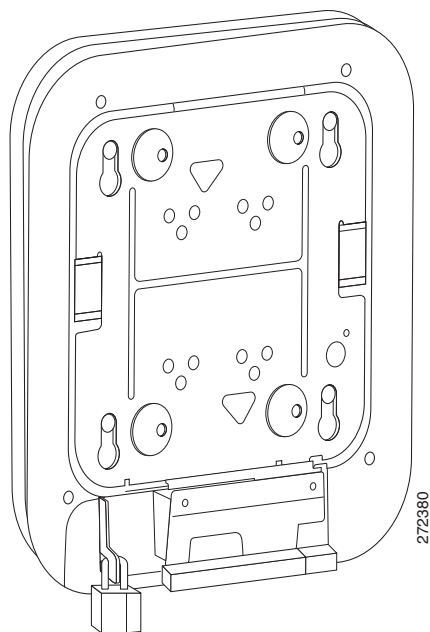
La configuration avec antenne intégrée du point d'accès 1140 est conçue pour des surfaces horizontales (plateau et plafond). Lorsque le point d'accès est monté sur ces surfaces, le modèle de rayonnement des antennes intégrées est optimal. Si vous utilisez les fonctionnalités avancées telles que le trafic voix, la localisation et la détection des points d'accès indésirables, nous vous recommandons vivement le montage au plafond. En revanche, lorsque le client requiert principalement la couverture des données et ne nécessite pas de fonctionnalités avancées, dans des zones plus petites comme les salles de conférence, les kiosques, le transport et les points chauds par exemple, le montage mural avec des fixations à cheville en plastique et des vis numéro 8 est possible.



### Avertissement

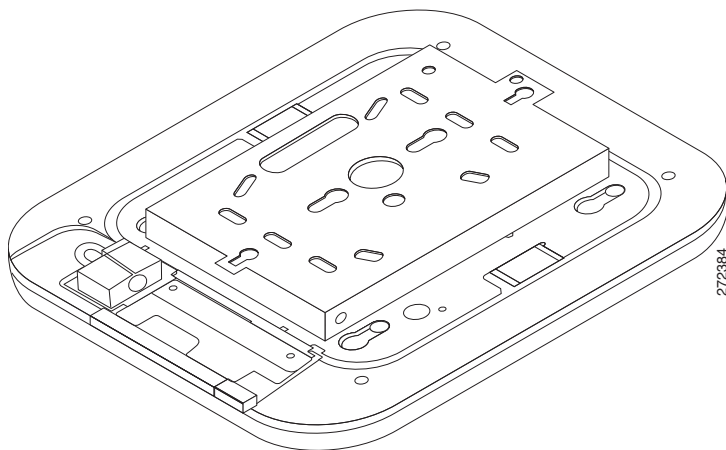
Lorsque vous montez le point d'accès sur un mur ou un plafond, veillez à utiliser des fixations appropriées. Celles-ci doivent supporter une force de traction minimale de 9 kg (20 livres) et doivent utiliser les 4 orifices du support de montage extra-plat.

**Figure 3** Support de montage extra-plat installé sur le point d'accès 1140



Vous pouvez également monter le point d'accès au-dessus d'un faux plafond ou sur une boîte de raccordement, à l'aide du support adaptateur en option. La Figure 4 montre le support adaptateur en option installé sur le point d'accès 1140.

**Figure 4** Support adaptateur en option installé sur le point d'accès 1140.



#### Remarque

Le support adaptateur en option permet également de monter le point d'accès sur un faux-plafond à l'aide du matériel de montage existant, pour les points d'accès 1100, 1130, 1200 ou 1240.

Reportez-vous au document *Cisco Aironet 1140 Series Access Point Alternate and Upgrade Mounting Instructions* pour savoir comment monter un point d'accès 1140 à l'aide du matériel de montage au plafond pour points d'accès 1100, 1130, 1200 ou 1240. Ce document est livré avec la plaque adaptatrice en option et est disponible sur Cisco.com.

## Matériel de montage

Le point d'accès est livré avec le matériel de montage suivant (reportez-vous à la Figure 1) :

- 1 support de montage extra-plat ;
- 1 attache standard ajustable pour rail en T sur plafond ;
- 4 vis à tête plate 0,63 cm (6,32 x 1/4 po).

Le matériel de montage ci-dessous peut être commandé en option :

- Plaque adaptatrice pour les scénarios de montage suivants :
  - au-dessus d'un faux-plafond ;
  - sur une boîte de raccordement ;
  - sur un matériel de montage 1100, 1130, 1200 ou 1240 existant.

## Montage du point d'accès sur une surface horizontale

Utilisez le support de montage extra-plat fourni pour monter le point d'accès sur des surfaces planes et horizontales telles qu'un plafond. Si vous montez le point d'accès sur une boîte de raccordement, utilisez la plaque adaptatrice en option.



### Remarque

Le fonctionnement des antennes intégrées du point d'accès est optimal lorsque le point d'accès est monté sur des surfaces horizontales telles qu'un plateau ou un plafond. Si vous utilisez les fonctionnalités avancées telles que le trafic voix, la localisation et la détection des points d'accès indésirables, nous vous recommandons vivement le montage au plafond. Cependant, pour les espaces plus petits tels que les salles de conférence, les bornes, les transports, ainsi que dans des points d'accès public où la couverture des données est la préoccupation principale, le dispositif peut être monté au mur à l'aide des fixations à cheville plastique fournies et des attaches appropriées.

La procédure ci-dessous décrit les étapes nécessaires pour monter le point d'accès sur un plafond composé de contre-plaqué de 19,05 mm d'épaisseur (3/4 po) ou plus, à l'aide des attaches fournies par l'utilisateur. Les procédures concernant les autres équipements peuvent être différentes et vous devrez peut-être fournir des attaches appropriées supplémentaires.

Pour monter le point d'accès sur un plafond en contre-plaqué, procédez comme suit.

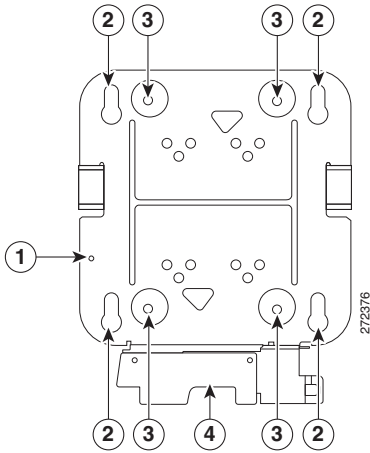
**Étape 1** Utilisez le support de montage extra-plat comme modèle pour noter les emplacements des quatre orifices de montage prévus. Reportez-vous au point 3 de la Figure 5.



### Avertissement

Veillez à noter les quatre emplacements. Pour garantir la sécurité de l'installation, veillez à utiliser les fixations appropriées et montez le point d'accès avec les quatre fixations.

**Figure 5 Description du support de montage extra-plat**



<b>1</b>	Borne de mise à terre	<b>3</b>	Orifices de montage
<b>2</b>	Lumières de montage du point d'accès	<b>4</b>	Capot d'accès aux câbles

**Étape 2** Utilisez un foret de taille appropriée pour percer un trou d'implémentation au niveau des emplacements des orifices de montage que vous avez marqués.



**Remarque**

La taille du trou d'implémentation varie en fonction du matériau et de l'épaisseur de l'installation. Cisco vous recommande de tester le matériau afin de déterminer la taille de trou parfaitement adaptée à votre montage.

**Étape 3** (Facultatif) Percez ou effectuez un orifice d'accès aux câbles à proximité et au-dessous de l'emplacement du capot d'accès aux câbles de la plaque de montage extra-plat. Il doit être suffisamment grand pour le câble Ethernet, le câble de mise à la terre du bâtiment et les câbles d'alimentation.

**Étape 4** Si vous avez exécuté l'étape 4, tirez les câbles à travers le trou d'accès jusqu'à ce qu'environ 30,4 cm (1 pied) de câble ressorte du trou.

**Étape 5** Reliez la ligne de terre du bâtiment à la borne de mise à la terre du support de montage extra-plat. Reportez-vous à la section « Mise à la terre du point d'accès » à la page 17 pour prendre connaissance des instructions générales de mise à la terre.

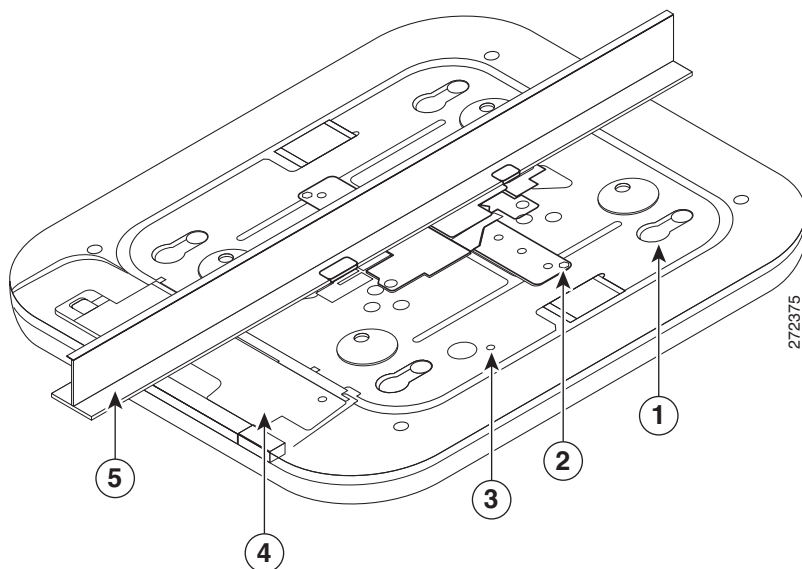
**Étape 6** Positionnez les orifices de montage de la plaque de montage extra-plat (renforcements vers le bas) sur les trous d'implémentation.

- Étape 7** Insérez une attache à tête fendue ou Phillips appropriée dans chaque orifice de montage, puis serrez.
- Étape 8** Alignez les pieds du point d'accès sur la partie large des encoches de montage de la plaque de montage extra-plate. Lorsque la position est correcte, le capot d'accès aux câbles s'insère dans la baie du connecteur du point d'accès.
- Étape 9** Faites glisser délicatement le point d'accès sur les encoches du support de montage extra-plat, jusqu'à ce qu'il s'enclenche.
- Étape 10** Installez les câbles Ethernet et d'alimentation.

## Montage du point d'accès au-dessous d'un faux-plafond

Pour monter le point d'accès au-dessous d'un faux-plafond standard ou encastré, procédez comme suit. Reportez-vous à la Figure 6.

**Figure 6** Détails du montage sur faux-plafond

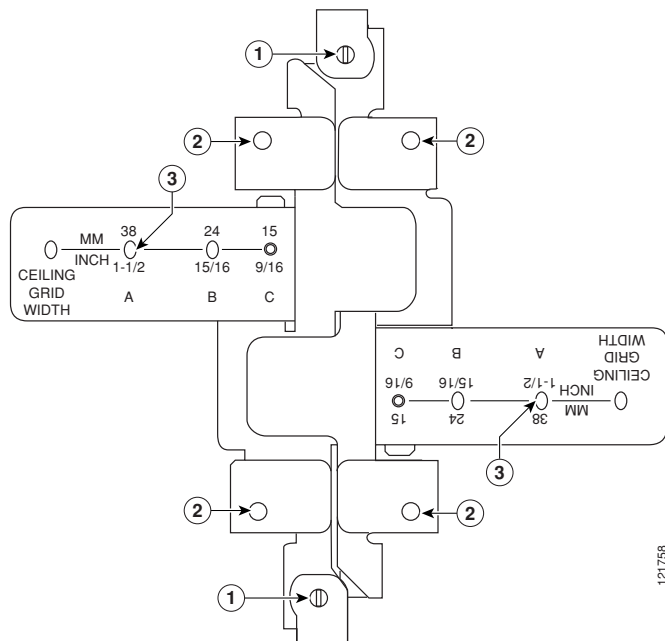


<b>1</b>	Encoche de montage du point d'accès	<b>4</b>	Capot d'accès aux câbles du point d'accès
<b>2</b>	Attache ajustable pour rail en T	<b>5</b>	Rail en T pour plafond
<b>3</b>	Point de mise à la terre		

Pour monter le point d'accès au-dessous d'un faux-plafond, procédez comme suit.

- Étape 1** Choisissez l'emplacement de montage du point d'accès sur votre faux-plafond.
- Étape 2** Sélectionnez l'attache pour rail en T appropriée à votre faux-plafond, puis ouvrez complètement l'attache. Reportez-vous à la Figure 7.

**Figure 7 Attache ajustable pour rail en T**

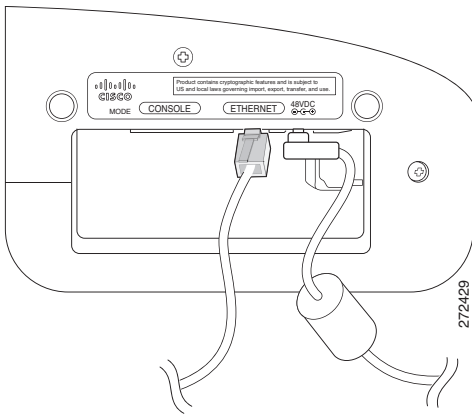


<b>1</b>	Vis de blocage pour rail en T	<b>3</b>	Crans correspondants à la largeur du rail en T (A, B ou C)
<b>2</b>	Trous de vis de la plaque de montage		

- Étape 3** Placez l'attache pour rail en T sur le rail en T, puis refermez-la au niveau du cran approprié (A, B ou C).
- Étape 4** Utilisez un tournevis pour serrer les deux vis de blocage du rail en T et empêcher ainsi l'attache pour rail en T de glisser le long du rail.
- Étape 5** Prenez note de la lettre de cran (A, B ou C) correspondant à la largeur du rail en T.

- Étape 6** Aligned les orifices correspondants (A, B ou C) de la plaque de montage extra-plate sur les orifices de la plaque de montage du rail en T.
- Étape 7** Tenez le support de montage extra-plat, puis insérez une vis à tête plate 0,63 cm (6,32 x 1/4 po) dans chacun des quatre orifices correspondants (A, B ou C) et serrez.
- Étape 8** Si nécessaire, percez ou découpez un trou d'accès aux câbles dans la plaque de plafond. Ce trou doit être suffisamment large pour faire passer les câbles Ethernet et d'alimentation. Tirez les câbles à travers le trou d'accès jusqu'à ce que 30 cm (1 pied) de câble ressortent du trou.
- Étape 9** Reliez le point d'accès à une prise de terre du bâtiment appropriée. Reportez-vous à la section « Mise à la terre du point d'accès » à la page 17 pour prendre connaissance des instructions générales de mise à la terre.
- Étape 10** Installez les câbles Ethernet et d'alimentation. Veillez à faire courir le câble d'alimentation à travers le manchon de contrainte, comme illustré dans la Figure 8.

**Figure 8 Acheminement du câble d'alimentation**



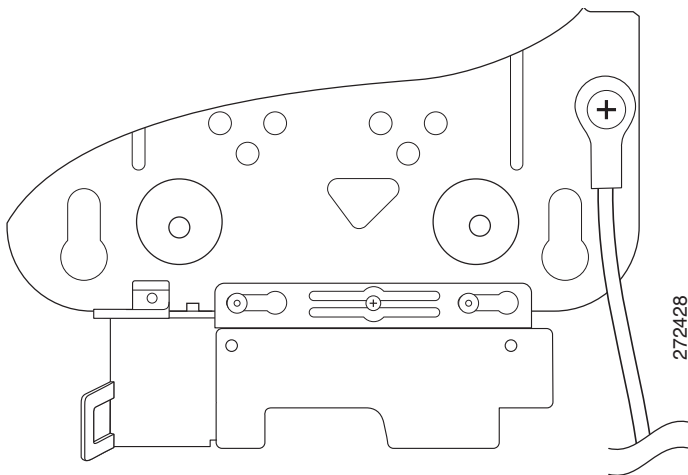
- Étape 11** Aligned les pieds du point d'accès sur les encoches de montage de la plaque de montage extra-plate. Si vous avez percé un trou pour les câbles, positionnez le point d'accès de sorte que les câbles atteignent leurs ports respectifs.
- Étape 12** Faites glisser délicatement le point d'accès sur le montage extra-plat, jusqu'à ce qu'il s'enclenche.

## Mise à la terre du point d'accès

La mise à la terre n'est généralement pas obligatoire dans des installations situées à l'intérieur, car le point d'accès de la gamme 1140 est classé en tant qu'appareil basse tension et il ne contient pas d'alimentation interne ni d'antennes extérieures. Cisco vous recommande toutefois de vérifier vos normes électriques locales et nationales afin de savoir si la mise à la terre est exigée. Si la mise à la terre est requise dans votre région ou si vous souhaitez relier votre point d'accès à la terre, procédez comme suit.

- Étape 1** Déterminez un point de mise à la terre adapté du bâtiment qui soit le plus proche possible du point d'accès.
- Étape 2** Connectez un câble de mise à la terre fourni par l'utilisateur au point de mise à la terre du bâtiment. Il doit s'agir au minimum d'un câble 14AWG pouvant assurer une longueur de circuit de 7,62 m (25 pieds). Pour plus d'informations, reportez-vous aux normes électriques locales.
- Étape 3** Faites courir le câble de mise à la terre jusqu'au point d'accès.
- Étape 4** Utilisez un tournevis Phillips pour retirer la vis de la borne de mise à la terre du support de montage extra-plat.
- Étape 5** Reliez le câble à une cosse circulaire de mise à la terre appropriée.
- Étape 6** Sertissez ou soudez le câble à la cosse.
- Étape 7** Insérez la vis de la borne de mise à la terre dans la cosse, puis refixez-la sur la plaque de montage extra-plate, comme illustré à la Figure 9.

**Figure 9** Fixation de la vis de la borne de mise à la terre



**Étape 8** Utilisez un tournevis Phillips pour serrer la vis de la borne de mise à la terre.

**Étape 9** Une fois que le point d'accès est correctement monté et mis à la terre, il peut être raccordé à une source d'alimentation et mis sous tension.

---

## Fixation du point d'accès

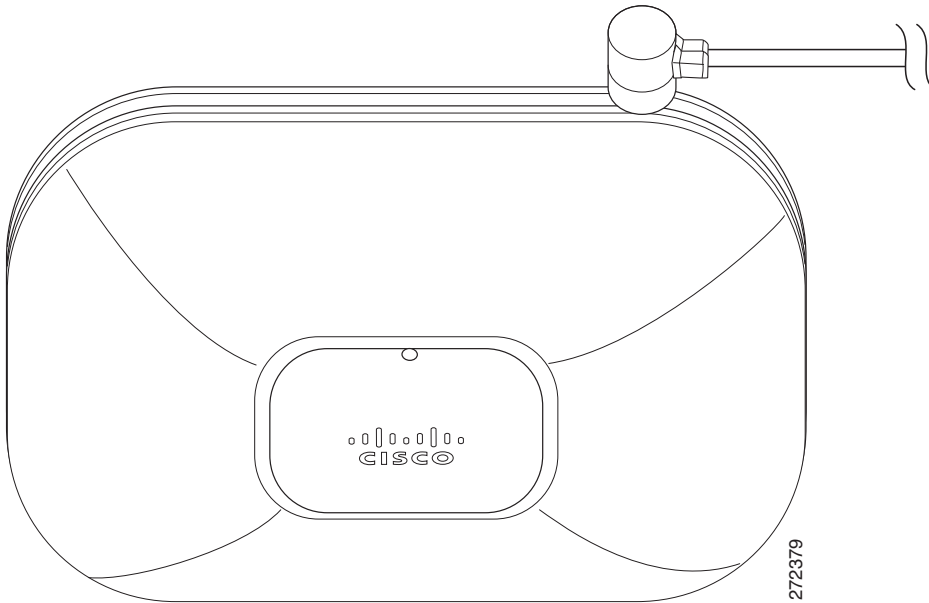
Il existe deux méthodes pour fixer votre point d'accès :

- Vous pouvez l'attacher à un objet fixe, à l'aide d'un câble de sécurité.
- Vous pouvez le verrouiller à la plaque de montage, à l'aide d'un cadenas.

### Fixation du point d'accès à l'aide d'un câble de sécurité

Vous pouvez fixer votre point d'accès en installant un câble de sécurité standard (tel que Kensington Notebook MicroSaver, référence 64068) dans l'emplacement réservé du point d'accès, comme illustré dans la Figure 10.

**Figure 10** Détails du câble de sécurité



Le câble de sécurité peut être utilisé avec n'importe laquelle des méthodes de montage décrites dans ce guide.

Pour installer le câble de sécurité, procédez comme suit.

---

**Étape 1** Enroulez le câble de sécurité autour d'un objet fixe situé à proximité.

**Étape 2** Insérez la clé dans le verrou du câble de sécurité.

**Étape 3** Insérez le loquet du câble de sécurité dans l'encoche du point d'accès prévue à cet effet.



**Remarque**

---

Faites pivoter la clé à gauche ou à droite pour immobiliser le verrou du câble de sécurité sur le point d'accès.

---

**Étape 4** Retirez la clé.

---

## Fixation du point d'accès à la plaque de montage

Utilisez le loquet de sécurité sur le capot d'accès aux câbles de l'adaptateur extra-plat et un cadenas (que vous devez vous procurer), pour fixer votre point d'accès à la plaque de montage. Les cadenas compatibles sont les modèles Master Lock 120T et 121T. Le capot d'accès aux câbles situé sur la plaque de montage extra-plat recouvre la baie de câblage (notamment le port d'alimentation, le port Ethernet, le port de console et le bouton de mode) pour empêcher l'installation ou le retrait des câbles ou l'activation du bouton de mode.

Pour installer le cadenas, procédez comme suit :

---

**Étape 1** Une fois que le point d'accès est installé sur le support de montage extra-plat, insérez un cadenas dans le loquet de sécurité.



**Remarque**

---

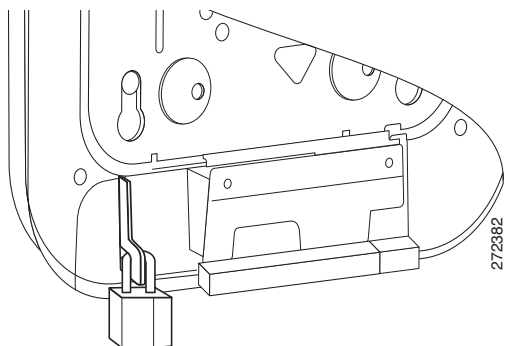
Si votre point d'accès est monté sur un plafond en dur, l'espace entre le support de montage extra-plat et le plafond est mince. Procédez lentement en utilisant vos deux mains afin de positionner et de fixer le verrou dans le loquet du support de montage.

---

**Étape 2** Tournez le verrou dans le sens des aiguilles d'une montre, puis alignez le crochet de fixation sur le corps du verrou.

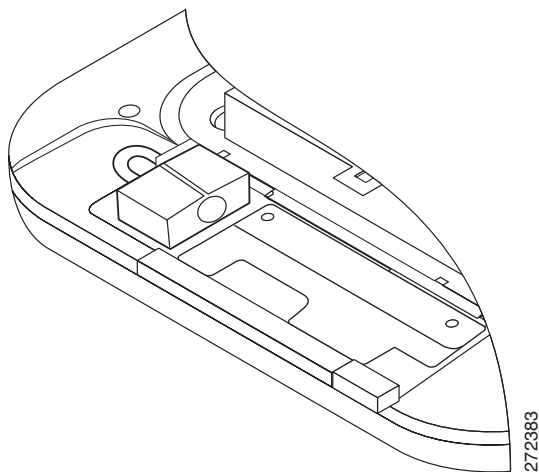
**Étape 3** Saisissez le verrou et insérez-le dans le crochet, afin de le verrouiller. Reportez-vous à la Figure 11.

**Figure 11** *Insertion du cadenas dans le loquet de sécurité*



**Étape 4** Faites tourner le cadenas dans la zone de verrouillage. Reportez-vous à la Figure 12.

**Figure 12** *Rotation du cadenas dans la zone de verrouillage*



## 6 Configuration des paramètres de base

Pour configurer les paramètres de base, vous devez donner au point d'accès et à votre PC une adresse IP. Reportez-vous à la section « Obtention et attribution d'une adresse IP » à la page 7.

Pour configurer les paramètres de base du point d'accès à l'aide de la page Express Setup de l'interface graphique d'utilisateur, procédez comme suit :

- Étape 1** Ouvrez votre navigateur et saisissez l'adresse IP du point d'accès dans la barre d'adresse. Un écran contenant les champs Username et Password s'affiche.
- Étape 2** Saisissez le nom d'utilisateur Cisco et le mot de passe Cisco. Le nom d'utilisateur et le mot de passe respectent la casse.
- Étape 3** Appuyez sur Entrée. La page Summary Status s'affiche.

The screenshot shows the configuration page for a Cisco Aironet 1140 Series Access Point. The page title is "Cisco Aironet 1140 Series Access Point" and the hostname is "ap". The page is titled "Home: Summary Status".

**Association**

Clients: 0	Repeaters: 0
------------	--------------

**Network Identity**

IP Address	10.91.107.17
MAC Address	0022.9090.8f4d

**Network Interfaces**

Interface	MAC Address	Transmission Rate
GigabitEthernet0	0022.9090.8f4d	100Mbps
Radio0-802.11n@40MHz	0022.9092.9970	Mcs Index 15
Radio1-802.11n@80MHz	0022.9093.99b0	Mcs Index 15

**Event Log**

Time	Severity	Description
Mar 1 00:27:48.007	◆Notification	Line protocol on interface Dot11Radio1, changed state to down
Mar 1 00:27:48.007	◆Notification	Line protocol on interface Dot11Radio0, changed state to down
Mar 1 00:27:47.850	◆Notification	Line protocol on interface BV11, changed state to up
Mar 1 00:27:47.700	◆Notification	Line protocol on interface GigabitEthernet0, changed state to up
Mar 1 00:27:47.010	⚠Warning	Full power- AC_ADAPTOR inline power source
Mar 1 00:27:47.008	◆Notification	Interface Dot11Radio1, changed state to administratively down
Mar 1 00:27:47.008	◆Notification	Interface Dot11Radio0, changed state to administratively down
Mar 1 00:00:09.991	◆Notification	SNMP agent on host ap is undergoing a cold start
Mar 1 00:00:09.990	◆Notification	System restarted --
Mar 1 00:00:09.988	◆Notification	Configured from memory by console

Refresh 2058653

- Étape 4** Si nécessaire, configurez les paramètres d'alimentation comme décrit à la section précédente. Autrement, cliquez sur Express Setup. La page Express Setup apparaît.

HOME Hostname ap ap uptime is 3 minutes

EXPRESS SET-UP

EXPRESS SECURITY

NETWORK MAP

ASSOCIATION

NETWORK INTERFACES

SECURITY

SERVICES

WIRELESS SERVICES

SYSTEM SOFTWARE

EVENT LOG

---

**Express Set-Up**

**Host Name:**

**MAC Address:** 0022.9090.8f4d

**Configuration Server Protocol:**  DHCP  Static IP

**IP Address:**

**IP Subnet Mask:**

**Default Gateway:**

**SNMP Community:**

Read-Only  Read-Write

---

**Radio0.802.11N<sup>2.4GHz</sup>**

**Role in Radio Network:**  Access Point  Repeater  
 Root Bridge  Non-Root Bridge  
 Workgroup Bridge  Universal Workgroup Bridge Client MAC:   
 Scanner

**Optimize Radio Network for:**  Throughput  Range  Default  Custom

**Aironet Extensions:**  Enable  Disable

---

**Radio1.802.11N<sup>5GHz</sup>**

**Role in Radio Network:**  Access Point  Repeater  
 Root Bridge  Non-Root Bridge  
 Workgroup Bridge  Universal Workgroup Bridge Client MAC:   
 Scanner

**Optimize Radio Network for:**  Throughput  Range  Default  Custom

**Aironet Extensions:**  Enable  Disable

## Étape 5 Configurer les paramètres en vous aidant des sections suivantes.

- **Host Name :** le nom d'hôte (ou nom système) est un nom qui identifie le point d'accès sur votre réseau. Le nom système s'affiche dans le titre des pages du système de gestion.
- **Configuration Server Protocol :** spécifie comment le point d'accès obtient une adresse IP.
  - DHCP : l'adresse IP est automatiquement attribuée par le serveur DHCP du réseau.
  - Static IP : le point d'accès utilise l'adresse IP statique que vous avez saisie dans le champ IP Address.
- **IP Address :** ce paramètre attribue son adresse IP au point d'accès ou la modifie, s'il en possède déjà une. Si l'option DHCP est activée, le point d'accès obtient son adresse IP à partir du serveur DHCP de votre réseau. Vous pouvez attribuer une adresse IP statique dans ce champ.
- **IP Subnet Mask :** le masque de sous-réseau IP identifie le sous-réseau sur lequel réside le point d'accès. Ce sous-réseau est fourni par votre administrateur réseau. Si l'option DHCP est activée, laissez ce champ vide.

- Default Gateway : la passerelle par défaut identifie l'adresse que le point d'accès utilise pour accéder à un autre réseau. Cette passerelle est fournie par votre administrateur réseau. Si l'option DHCP est activée, laissez ce champ vide.
- Web Server : ce paramètre spécifie le type de protocole HTTP utilisé pour accéder au point d'accès à l'aide d'un navigateur Internet.
  - Standard (HTTP) : protocole standard utilisé pour transférer du contenu HTML à l'aide de trafic non crypté, entre des navigateurs Internet.
  - Secure (HTTPS) : protocole utilisé pour transférer des données sécurisées à l'aide de trafic crypté vers et en provenance de l'utilisateur, au moyen du protocole SSL (Secure Socket Layer).
- SNMP Community : le paramètre SNMP Community identifie et définit les attributs du protocole SNMP (Simple Network Management Protocol) utilisé pour gérer le réseau sur lequel réside le point d'accès.
  - Read-Only : le point d'accès n'autorise qu'un accès SNMP en lecture.
  - Read-Write : le point d'accès autorise un accès en lecture et en écriture.

## Configuration des radios

Votre point d'accès 1140 inclut deux radios internes, qui doivent être configurées individuellement via la fonction de configuration rapide. Sélectionnez le rôle, le paramètre d'optimisation et les possibilités d'extension de la Radio0 (802.11N<sup>2.4GHz</sup>) et de la Radio1 (802.11N<sup>5GHz</sup>).


- Role in Radio Network : permet de déterminer la fonction de chaque radio du point d'accès, dans le réseau sans fil.
  - Access Point : indique que l'unité fonctionne en tant que point d'accès connecté au réseau LAN Ethernet principal. Dans ce mode, les clients sans fil s'associent au point d'accès.
  - Repeater : indique que l'unité fonctionne en tant que point d'accès répéteur non connecté à un réseau LAN Ethernet. Dans ce mode, les clients sans fil s'associent au point d'accès.
  - Root Bridge : indique que l'unité fonctionne en tant que pont racine et se connecte directement au réseau LAN Ethernet principal. Dans ce mode, l'unité accepte les associations provenant d'autres ponts non racine et d'autres périphériques client sans fil Cisco Aironet.
  - Workgroup Bridge : indique que l'unité fonctionne en tant que pont de groupe de travail et qu'elle est connectée à un petit réseau LAN Ethernet câblé via un commutateur ou un concentrateur Ethernet. Le pont de groupe de travail doit s'associer à un pont ou point d'accès Cisco Aironet.
  - Scanner : indique que l'unité est configurée par le WLSE Cisco, fonctionne comme un scanner et communique le trafic du réseau au WLSE Cisco.

- Optimize Radio Network For : permet d'optimiser les performances radio du point d'accès dans le réseau sans fil, en ajustant les débits de données. Il doit correspondre au paramètre défini sur les clients.
  - Throughput : permet de maximiser le volume de données traitées par le point d'accès mais risque de réduire sa portée.
  - Range : permet de maximiser la portée du point d'accès mais risque de réduire son débit.
  - Default : le point d'accès utilise les paramètres de débit de données par défaut pour la radio sélectionnée.
  - Custom : le point d'accès utilise les paramètres que vous saisissez sur la page Radio Settings. Pour accéder à cette page, cliquez sur **Custom**.
- Aironet Extensions : par défaut, le point d'accès utilise des extensions Cisco Aironet 802.11 pour détecter les caractéristiques des périphériques clients Cisco Aironet et prendre en charge les fonctions qui nécessitent une interaction spécifique entre le point d'accès et les périphériques clients associés. Les extensions Aironet doivent être activées pour prendre en charge les fonctions telles que l'équilibrage de charge, Message Integrity Check (MIC), Temporal Key Integrity Protocol (TKIP), le mode répéteur et le mode international. La désactivation des extensions Aironet désactive les fonctions susmentionnées mais cela permet parfois d'associer plus facilement des périphériques clients non Cisco au point d'accès.

## Paramètres par défaut de la page Express Setup

Le Tableau 1 liste les paramètres par défaut de la page Express Setup.

**Tableau 1** Paramètres par défaut de la configuration rapide

Paramètre	Valeur par défaut
System Name	ap
Configuration Server Protocol	DHCP
IP Address	Affectée par DHCP
	 <b>Remarque</b> Le point d'accès ne possède pas d'adresse IP par défaut.
IP Subnet Mask	Affectée par DHCP
Default Gateway	Affectée par DHCP

**Tableau 1 Paramètres par défaut de la configuration rapide (suite)**

Paramètre	Valeur par défaut
Role in Radio Network	Access point
Web Server	Standard (HTTP)
SNMP Community	default Community
Optimize Radio Network for	Throughput
Aironet Extensions	Enable



**Remarque**

Pour restaurer les paramètres d'usine du point d'accès, débranchez puis rebranchez la prise d'alimentation tout en appuyant sur le bouton **Mode**, jusqu'à ce que la DEL Ethernet passe à l'orange (environ 2 à 3 secondes).

## Activation des interfaces radio

Les radios du point d'accès sont désactivées par défaut et il n'y a pas d'identifiant SSID par défaut. Vous devez créer un identifiant SSID et activer les interfaces radio pour que le point d'accès autorise les associations avec d'autres périphériques sans fil. Pour obtenir des instructions sur la configuration du SSID, reportez-vous à la section « Configuration des paramètres de sécurité de base » à la page 26.

Pour activer les interfaces radio, procédez comme suit :

- Étape 1** Accédez à votre point d'accès.
- Étape 2** Lorsque la page Summary Status s'affiche, cliquez sur 802.11N<sup>2.4GHz</sup>. La page de statut de la radio 2.4 GHz s'affiche.
- Étape 3** Cliquez sur l'onglet **Settings**, en haut de la page. La page Radio Settings s'affiche.
- Étape 4** Cliquez sur **Enable** dans le champ Enable Radio.
- Étape 5** Cliquez sur **Apply**.
- Étape 6** Revenez à la page Summary Status, puis cliquez sur 802.11N<sup>5GHz</sup>. La page de statut de la radio 5 GHz s'affiche.
- Étape 7** Répétez les étapes 3 à 5.
- Étape 8** Fermez le navigateur Internet.

# Configuration des paramètres de sécurité

Après les paramètres de base de votre point d'accès, vous devez configurer ses paramètres de sécurité, pour empêcher l'accès non autorisé à votre réseau. Le point d'accès étant un appareil radio, il peut communiquer au-delà des limites physiques de votre site de travail.

De même que la page Express Setup permet de définir les paramètres de base, vous pouvez utiliser la page Express Security pour créer des identifiants SSID uniques et leur attribuer l'un des quatre types de sécurité disponibles. Pour plus d'informations sur la sécurité, reportez-vous au *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points*.

## Configuration des paramètres de sécurité de base

La page Express Security permet de créer des identifiants SSID uniques et de leur attribuer l'un des quatre types de sécurité disponibles. La page Express Security est illustrée ci-dessous.

Hostname AP1140 AP1140 uptime is 4 minutes

### Express Security Set-Up

#### SSID Configuration

1. SSID   Broadcast SSID in Beacon

2. VLAN

No VLAN  Enable VLAN ID:  (1-4094)  Native VLAN

3. Security

No Security

Static WEP Key

Key 1   128 bit

EAP Authentication

RADIUS Server:  (Hostname or IP Address)

RADIUS Server Secret:

RADIUS Server:  (Hostname or IP Address)

RADIUS Server Secret:

#### SSID Table

SSID	VLAN	Encryption	Authentication	Key Management	Native VLAN	Broadcast SSID

205851

## Présentation de la configuration rapide de la sécurité

Lorsque le point d'accès est configuré par défaut, le premier identifiant SSID que vous créez sur la page Express Security remplace celui qui existe par défaut et qui ne dispose d'aucun paramètre de sécurité. Les identifiants SSID que vous créez apparaissent dans le tableau des identifiants SSID situé en bas de la page. Vous pouvez créer jusqu'à 16 identifiants SSID sur le point d'accès.

## Utilisation des réseaux locaux virtuels

Si vous utilisez des réseaux locaux virtuels sur votre réseau local sans fil et que vous leur attribuez des identifiants SSID, vous pouvez créer plusieurs identifiants SSID à l'aide de l'un des quatre paramètres de sécurité disponibles sur la page Express Security. Cependant, si vous n'utilisez pas de réseau local virtuel sur votre réseau local sans fil, les options de sécurité que vous pouvez attribuer aux identifiants SSID sont limitées en raison des options de cryptage restreintes de la page Express Security. Sans réseau local virtuel, les paramètres de cryptage (WEP et chiffrement) s'appliquent à une interface, comme l'interface radio, et vous ne pouvez pas utiliser plus d'un paramètre de cryptage par interface. Par exemple, lorsque vous créez un identifiant SSID avec un WEP statique et que les réseaux locaux virtuels sont désactivés, vous ne pouvez pas créer d'identifiant SSID supplémentaires disposant d'une authentification WPA, car ils utilisent des paramètres de cryptage différents. Si le paramètre de sécurité d'un identifiant SSID entre en conflit avec un autre identifiant SSID, vous pouvez supprimer un ou plusieurs identifiants SSID, pour éliminer ce conflit.

Si des réseaux locaux virtuels sont définis sur le point d'accès, le port de ligne réseau sur le commutateur doit être limité pour autoriser uniquement les réseaux locaux virtuels définis sur le point d'accès.

## Types de sécurité rapides

Vous pouvez attribuer quatre types de sécurité différents à un identifiant SSID :

- **No security** : option la moins sûre. Choisissez cette option pour les identifiants SSID utilisés dans un espace public uniquement et attribuez-la à un réseau local virtuel qui restreint l'accès à votre réseau.
- **Static WEP Key** : option plus sûre que No Security. Les clés WEP statiques sont vulnérables aux attaques. Les clés WEP peuvent avoir deux longueurs : 40 bits et 128 bits (caractères hexadécimaux ou ASCII). Les points d'accès Cisco utilisent des caractères hexadécimaux. Les adaptateurs clients peuvent utiliser l'un ou l'autre type de caractère, selon la configuration choisie par le fournisseur.
- **EAP Authentication** : active l'authentification 802.1x. Nécessite une adresse IP et un secret partagé d'un serveur d'authentification sur votre réseau (port d'authentification 1645 du serveur). Vous n'avez pas besoin de saisir une clé WEP.

- WPA : l'accès protégé Wi-Fi (WPA, pour Wi-Fi Protected Access) octroie un accès sans fil aux utilisateurs authentifiés sur une base de données via un serveur d'authentification. Ensuite, le WPA crypte leur trafic IP avec des algorithmes plus puissants que ceux utilisés avec la clé WEP. Comme avec l'authentification EAP, vous devez saisir l'adresse IP et le secret partagé pour un serveur d'authentification sur votre réseau (port d'authentification 1645 du serveur).

## Configuration de la sécurité pour la norme 802.11n

Pour atteindre les débits 802.11n, vous devez configurer le point d'accès sans cryptage ou avec un cryptage WPA2/AES. Tout autre paramètre bloque les fonctionnalités 802.11n de la configuration.

## Limites de la configuration rapide de la sécurité

Puisque la page Express Security est conçue pour une simple configuration de la sécurité de base, les options disponibles ne représentent qu'une partie des fonctionnalités de sécurité du point d'accès. Tenez compte des limites suivantes lorsque vous utilisez la page Express Security :

- Vous ne pouvez pas modifier les identifiants SSID, mais vous pouvez les supprimer et les recréer.
- Vous ne pouvez pas attribuer d'identifiants SSID à des interfaces radio spécifiques. Les identifiants SSID que vous créez sont activés sur toutes les interfaces radio. Pour attribuer des identifiants SSID à des interfaces radio spécifiques, sélectionnez **Security > SSID Manager**.
- Vous ne pouvez pas configurer plusieurs serveurs d'authentification. Pour configurer plusieurs serveurs d'authentification, cliquez sur **Security > Server Manager**.
- Vous ne pouvez pas configurer plusieurs clés WEP. Pour configurer plusieurs clés WEP, cliquez sur **Security > Encryption Manager**.
- Vous ne pouvez pas attribuer un identifiant SSID à un réseau local virtuel qui est déjà configuré sur le point d'accès. Pour attribuer un identifiant SSID à un réseau local virtuel existant, sélectionnez **Security > SSID Manager**.
- Vous ne pouvez pas configurer des combinaisons de types d'authentification sur le même identifiant SSID (comme une authentification par adresse MAC et une authentification EAP). Pour configurer des combinaisons de types d'authentification, sélectionnez **Security > SSID Manager**.

## Utilisation de la page Express Security

Pour créer un identifiant SSID sur la page Express Security, procédez comme suit :

---

**Étape 1** Saisissez l'identifiant SSID dans le champ de saisie SSID. Il peut comporter jusqu'à 32 caractères alphanumériques.



---

**Remarque**

Les caractères suivants ne sont pas autorisés dans l'identifiant SSID : +, ], /, “, tabulation et espace à la fin.

---

**Étape 2** Pour diffuser l'identifiant SSID dans la balise du point d'accès, cochez la case Broadcast SSID in Beacon.



**Remarque**

---

Lorsque vous diffusez l'identifiant SSID, les périphériques qui n'en spécifient aucun peuvent s'associer au point d'accès. Cette option est utile pour un identifiant SSID utilisé par des périphériques invités ou clients dans un lieu public. Si vous ne diffusez pas l'identifiant SSID, les périphériques clients ne peuvent s'associer au point d'accès que si leur identifiant SSID correspond à celui défini sur le point d'accès. Par conséquent, la balise du point d'accès ne peut inclure qu'un identifiant SSID.

---

**Étape 3** (Facultatif) Cochez la case Enable VLAN ID, puis saisissez un numéro de réseau local virtuel (entre 1 et 4095) pour attribuer l'identifiant SSID à un réseau local virtuel. Vous ne pouvez pas attribuer d'identifiant SSID à un réseau local virtuel existant.

**Étape 4** (Facultatif) Cochez la case Native VLAN pour identifier le réseau comme étant le réseau local virtuel natif.

**Étape 5** Sélectionnez le paramètre de sécurité de l'identifiant SSID. Les paramètres sont listés selon leur fiabilité, de No Security à WPA, le paramètre le plus sûr.

- a. Si vous sélectionnez l'option Static WEP Key, indiquez le numéro de la clé et la taille de cryptage, puis saisissez la clé de cryptage (10 caractères hexadécimaux pour les clés 40 bits ou 26 caractères hexadécimaux, pour les clés 128 bits).
- b. Si vous sélectionnez l'option EAP Authentication ou WPA, saisissez l'adresse IP et le secret partagé du serveur d'authentification sur votre réseau.
- c. Votre configuration de sécurité 802.11n doit être : no encryption (pas de cryptage) ou WPA2/AES. Toute autre configuration empêche les débits de données rapides fournis par la norme 802.11n.



**Remarque**

---

Si vous n'utilisez pas de réseau local virtuel sur votre réseau local sans fil, les options de sécurité que vous pouvez attribuer aux divers identifiants SSID sont limitées. Pour plus d'informations sur les réseaux locaux virtuels, reportez-vous au *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points*.

---

1. Cliquez sur **Apply**. L'identifiant SSID apparaît dans le tableau des identifiants SSID situé en bas de la page.
-

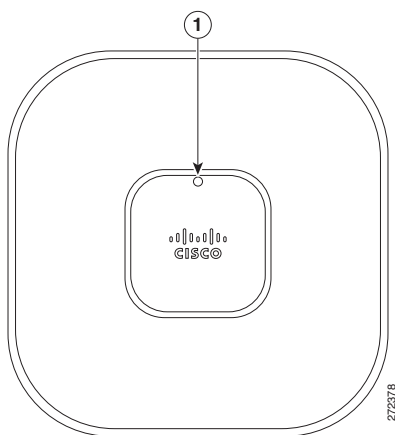
## 7 Dépannage

Cette section contient des suggestions de diagnostic et de configuration qui vous aideront à résoudre les problèmes rencontrés avec votre point d'accès.

### Vérification des DEL du point d'accès

La Figure 13 montre l'emplacement de la DEL d'indication d'état du point d'accès.

**Figure 13** Emplacement de la DEL du point d'accès



<b>1</b>	DEL d'indication d'état
----------	-------------------------

Le Tableau 2 indique le diagnostic de la DEL du point d'accès dans différentes situations.

**Tableau 2 Messages de diagnostic de la DEL du point d'accès**

<b>Type de message</b>	<b>DEL d'indication d'état</b>	<b>Signification du message</b>
Séquence d'état du programme d'amorçage	Vert, clignotant	Test mémoire DRAM en cours
		Test mémoire DRAM OK
		Initialisation de la carte en cours
		Initialisation du système de fichiers FLASH
		Test mémoire FLASH OK
		Initialisation Ethernet
		Ethernet OK
		Lancement de Cisco IOS
Etat des associations	Vert	Conditions de fonctionnement normales ; aucun client sans fil associé
	Bleu	Conditions de fonctionnement normales ; au moins un client sans fil associé
Etat de fonctionnement	Bleu, clignotant	Mise à jour du logiciel en cours
	Succession rapide et alternant entre le bleu, le vert, le rouge et le blanc	Exécution de la commande Access point location
	Rouge, clignotant	Liaison Ethernet non opérationnelle
Mises en garde du programme d'amorçage	Bleu, clignotant	Récupération de la configuration en cours (pression du bouton MODE pendant 2 à 3 secondes)
	Rouge	Échec de la liaison Ethernet ou récupération des images (pression du bouton MODE pendant 20 à 30 secondes)
	Vert, clignotant	Récupération des images en cours (relâchement du bouton MODE)

**Tableau 2 Messages de diagnostic de la DEL du point d'accès (suite)**

Type de message	DEL d'indication d'état	Signification du message	
Erreurs du programme d'amorçage	Rouge	Échec du test mémoire DRAM	
	Rouge et bleu, clignotant	Échec du système de fichiers FLASH	
	Rouge clignotant et éteint		Échec des variables d'environnement
			Adresse MAC incorrecte
			Échec de la liaison Ethernet pendant la récupération des images
			Échec de l'environnement d'amorçage
Aucun fichier image Cisco			
Échec de l'amorçage			
Erreurs Cisco IOS	Rouge	Échec du logiciel : essayez de déconnecter puis de reconnecter l'alimentation.	
	Bleu, vert, rouge et éteint en alternance	Mise en garde générale : alimentation électrique par câble insuffisante	

## Configuration des paramètres d'alimentation du système

Une fois que le point d'accès est connecté à une source électrique, sa DEL d'indication d'état peut s'allumer en orange pour indiquer que le point d'accès ne peut pas vérifier si l'équipement d'alimentation fournit suffisamment de courant. Dans ce cas, vous devez configurer les paramètres sur le point d'accès ou le commutateur afin d'identifier votre source d'alimentation.

Identifiez l'état de la source d'alimentation et du commutateur, puis assurez-vous que vos périphériques sont configurés avec une adresse IP.

Pour configurer les paramètres d'alimentation du système à l'aide de l'interface graphique d'utilisateur, procédez comme suit :

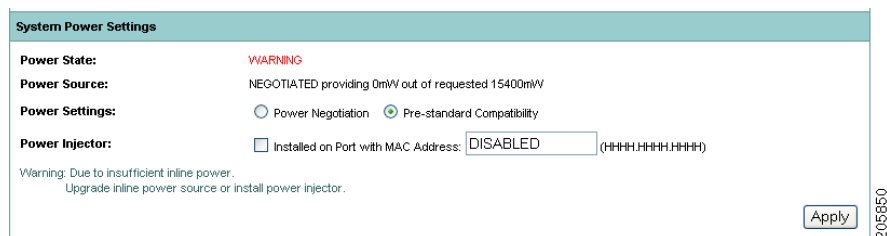
**Étape 1** Ouvrez votre navigateur et saisissez l'adresse IP du point d'accès dans la barre d'adresse. Un écran contenant les champs Login et Password s'affiche.

**Étape 2** Saisissez le nom d'utilisateur **Cisco** et le mot de passe **Cisco**. Le nom d'utilisateur et le mot de passe respectent la casse.

**Étape 3** Lorsque le point d'accès ne reçoit pas une puissance suffisante pour effectuer des opérations complètes, il fonctionne en mode basse puissance. Dans ce cas, un message d'avertissement s'affiche pour indiquer que toutes les radios sont désactivées en raison d'une puissance insuffisante. Cliquez sur **OK** pour continuer. La page System Configuration apparaît.

**Étape 4** Faites-la défiler vers le bas jusqu'à la section System Power Settings, comme illustré dans la Figure 14.

**Figure 14** Mise en garde : mode basse puissance



**Étape 5** Définissez les valeurs des options Power Settings et Power Injector, puis vérifiez l'état de votre commutateur, comme illustré dans la Tableau 3.



**Remarque**

Pour ce faire, vous devez utiliser l'interface de ligne de commande du commutateur. Reportez-vous au guide de configuration du logiciel Cisco IOS pour votre commutateur.

**Tableau 3** Paramètres d'alimentation du système

Source d'alimentation	Paramètres d'alimentation du système	État du commutateur
Équipements d'alimentation Cisco prenant en charge la technologie Cisco Intelligent Power Management <sup>1</sup>	Power Settings : option Power Negotiation sélectionnée Power Injector : non sélectionné	power inline auto
Équipements d'alimentation Cisco ne prenant pas en charge la technologie Cisco Intelligent Power Management <sup>1</sup>	Power Settings : option Pre-standard Compatibility sélectionnée Power Injector : non sélectionné	power inline auto
Injecteur de puissance Cisco Aironet avec un équipement d'alimentation Cisco prenant en charge la technologie Cisco Intelligent Power Management <sup>1</sup>	Power Settings : option Power Negotiation sélectionnée Power Injector : non sélectionné	power inline never

**Tableau 3 Paramètres d'alimentation du système (suite)**

Source d'alimentation	Paramètres d'alimentation du système	État du commutateur
Injecteur de puissance Cisco Aironet avec un équipement d'alimentation Cisco ne prenant pas en charge la technologie Cisco Intelligent Power Management <sup>1</sup>	Power Settings : option Power Negotiation sélectionnée Power Injector : sélectionné Adresse MAC <sup>2</sup>	power inline never
Injecteur de puissance Cisco Aironet avec un commutateur non Cisco	Pas de configuration requise	
Commutateur conforme 802.3af ne prenant pas en charge l'alimentation électrique par câble Ethernet (commutateur non Cisco)	Pas de configuration requise	
Adaptateur secteur	Pas de configuration requise	

1. Consultez les notes de version applicables à votre équipement d'alimentation pour déterminer quelle version de Cisco IOS prend en charge la technologie Cisco Intelligent Power Management. Il se peut que certains équipements d'alimentation ne prennent pas encore en charge cette technologie.
2. L'adresse MAC est l'adresse hexadécimale à 12 caractères du port de commutateur auquel le point d'accès est connecté. Le format de l'adresse MAC est HHHH.HHHH.HHHH.

**Étape 6** Cliquez sur **Apply**. Lors du redémarrage, le point d'accès est configuré selon les paramètres d'alimentation que vous avez spécifiés.



**Remarque**

Vous devrez peut-être actualiser l'écran de votre navigateur pour vérifier que les radios du point d'accès sont activées.

## Plus d'aide pour résoudre les problèmes

Si votre problème n'est toujours pas résolu et avant de contacter Cisco, recherchez une solution dans ce guide ou dans le chapitre consacré au dépannage du guide d'installation matérielle qui correspond au point d'accès utilisé. Ces guides, ainsi que d'autres documents, sont disponibles sur Cisco.com. Pour accéder à ces documents et les télécharger, procédez comme suit :

**Étape 1** Ouvrez votre navigateur Internet, puis connectez-vous à l'adresse [www.cisco.com](http://www.cisco.com).

**Étape 2** Cliquez sur **Products & Services**. Une fenêtre instantanée s'affiche.

- Étape 3** Cliquez sur **Wireless**. La page Wireless Introduction s'affiche.
- Étape 4** Faites défiler jusqu'à la section Product Portfolio.
- Étape 5** Sous Access Points, cliquez sur **Cisco Aironet 1140 Series**. La page Cisco Aironet 1140 Series Introduction s'affiche.
- Étape 6** Faites défiler la fenêtre Support, puis cliquez sur **Install and Upgrade**. La page Cisco Aironet 1140 Series Install and Upgrade s'affiche.
- Étape 7** Cliquez sur **Install and Upgrade Guides**. La page Cisco Aironet 1140 Series Install and Upgrade Guides s'affiche.
- Étape 8** Sélectionnez la section qui répond le mieux à votre problème.

## 8 Caractéristiques du point d'accès

Le Tableau 4 répertorie les caractéristiques techniques du point d'accès autonome 1140.

**Tableau 4** *Caractéristiques du point d'accès*

Catégorie	Caractéristique
Dimensions (LxlxH)	22,04 x 22,04 x 4,67 cm (8,68 x 8,68 x 1,84 pouces)
Poids	0,86 kg (1,9 livre)
Température de fonctionnement	De 0 à 40 degrés C (de 32 à 104 degrés F)
Température de stockage	De -30 à 85 degrés C (de -22 to 185 degrés F)
Humidité	De 10 à 90 % (sans condensation)
Antenne	Intégrée
Conformité	Le point d'accès 1140 respecte la norme UL 2043 relative aux produits installés dans les espaces de ventilation des bâtiments, tels que les faux-plafonds.
Sécurité	UL 60950-1 CAN/CSA C22.2 N° 60950-1 IEC 60950-1 avec les différences spécifiques à chaque pays EN 60950-1 UL 2043

**Tableau 4**      **Caractéristiques du point d'accès (suite)**

<b>Catégorie</b>	<b>Caractéristique</b>
EMI et sensibilité	FCC classe B sections 15.107 et 15.109 ICES-003 classe B (Canada) EN 301.489 EN 55022 classe B, version 2000 EN 55024 AS/NZS 3548 classe B VCCI classe B
Radio	FCC sections 15.247 et 15.407 Canada RSS-210 Japan Telec 33, 66, T71 EN 330.328, EN 301.893 Bulletin 65C OET de la FCC Industrie Canada RSS-102
Paramètres de puissance maximale et des canaux	Puissance maximale et canaux autorisés dans votre domaine réglementaire (reportez-vous au document <i>Channels and Maximum Power Settings for Cisco Aironet Lightweight Access Points.</i> ) Celui-ci est disponible sur Cisco.com.

## 9 Obtenir de la documentation et envoyer une demande de service

Pour plus d'informations sur la façon d'obtenir de la documentation, sur l'envoi d'une demande de service et sur la collecte de renseignements supplémentaires, consultez le bulletin mensuel *What's New in Cisco Product Documentation*, qui présente par ailleurs toute la documentation récente et révisée disponible sur les produits Cisco, à l'adresse suivante :

[www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html](http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html)

Abonnez-vous au flux RSS *What's New in Cisco Product Documentation* et programmez l'envoi direct de contenus vers votre bureau à l'aide d'une application de type lecteur. Le service de flux RSS est gratuit et Cisco prend actuellement en charge la syndication RSS version 2.0.

# 10 Déclarations de conformité et informations réglementaires

Cette section présente les déclarations de conformité et les informations réglementaires relatives aux Points d'accès autonomes de la gamme Cisco Aironet 1140.

## Déclaration de conformité de la Federal Communication Commission pour les fabricants



### Modèles

AIR-AP1141N-A-K9

AIR-AP1142N-A-K9

### Numéros de certification

LDK102069

LDK102070

Fabricant :

Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
États-Unis

Cet équipement est conforme à la section 15 de la réglementation. Son utilisation est sujette aux deux conditions suivantes :

1. Cet appareil ne peut pas causer d'interférences nuisibles.
2. Cet appareil doit accepter toutes les interférences, y compris celles qui sont susceptibles de perturber le fonctionnement de l'appareil.

Cet équipement a été testé et jugé conforme aux limites des appareils numériques de classe B, en vertu de la section 15 de la réglementation de la FCC. Ces limites sont conçues pour fournir une protection raisonnable contre toute interférence nuisible lorsque l'équipement est utilisé dans un environnement résidentiel. Cet équipement génère, utilise et émet de l'énergie radioélectrique. S'il n'est pas installé ni utilisé conformément aux instructions, il peut provoquer des interférences nuisibles. Cependant, rien ne garantit l'absence d'interférences. Si cet équipement provoque des interférences avec la réception de la radio ou de la télévision, lesquelles peuvent être détectées par la mise hors tension puis sous tension de l'équipement, l'utilisateur peut tenter d'y remédier de différentes façons :

- Réorientez ou déplacez l'antenne réceptrice.
- Augmentez la distance entre l'équipement et le récepteur.
- Branchez l'équipement sur la prise d'un circuit autre que celui auquel le récepteur est relié.
- Prenez avis auprès du distributeur ou d'un technicien radio/télévision expérimenté.



---

**Avertissement**

Les dispositifs radio conformes à la section 15 fonctionnent sur une base de non-interférence avec les autres dispositifs opérant à cette fréquence, lors de l'utilisation des antennes intégrées. Toute modification au produit non expressément approuvée par Cisco peut annuler le droit de l'utilisateur de faire usage de ce dispositif.

---



---

**Avertissement**

À l'intérieur d'une bande comprise entre 5,15 et 5,25 GHz (canaux radio 5 GHz de 34 à 48), les appareils UNII sont limités à une utilisation intérieure afin de réduire toute interférence nuisible potentielle avec les opérations du système mobile par satellite (MSS) de même canal.

---

## Déclaration relative à la norme VCCI pour le Japon

### Warning

---

**This is a Class B product based on the standard of the Voluntary Control Council for Interference from Information Technology Equipment (VCCI). If this is used near a radio or television receiver in a domestic environment, it may cause radio interference. Install and use the equipment according to the instruction manual.**

**警告** この装置は、クラスB情報技術装置です。この装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。  
取扱説明書に従って正しい取り扱いをして下さい。

VCCI-B

---

## Instructions relatives à l'utilisation des points d'accès Cisco Aironet au Japon

Cette section contient des instructions permettant d'éviter toute interférence lors de l'utilisation des points d'accès Cisco Aironet au Japon. Ces instructions existent en japonais et en anglais.

## Traduction japonaise

この機器の使用周波数帯では、電子レンジ等の産業・科学・医療用機器のほか工場の製造ライン等で使用されている移動体識別用の構内無線局（免許を要する無線局）及び特定小電力無線局（免許を要しない無線局）が運用されています。

- 1 この機器を使用する前に、近くで移動体識別用の構内無線局及び特定小電力無線局が運用されていないことを確認して下さい。
- 2 万一、この機器から移動体識別用の構内無線局に対して電波干渉の事例が発生した場合には、速やかに使用周波数を変更するか又は電波の発射を停止した上、下記連絡先にご連絡頂き、混信回避のための処置等(例えば、パーティションの設置など)についてご相談して下さい。
- 3 その他、この機器から移動体識別用の特定小電力無線局に対して電波干渉の事例が発生した場合など何かお困りのことが起きたときは、次の連絡先へお問い合わせ下さい。

連絡先 : 03-6434-6500

43768

## Traduction anglaise

This equipment operates in the same frequency bandwidth as industrial, scientific, and medical devices such as microwave ovens and mobile object identification (RF-ID) systems (licensed premises radio stations and unlicensed specified low-power radio stations) used in factory production lines.

1. Before using this equipment, make sure that no premises radio stations or specified low-power radio stations of RF-ID are used in the vicinity.
2. If this equipment causes RF interference to a premises radio station of RF-ID, promptly change the frequency or stop using the device; contact the number below and ask for recommendations on avoiding radio interference, such as setting partitions.
3. If this equipment causes RF interference to a specified low-power radio station of RF-ID, contact the number below.

Contact Number: 03-6434-6500

## Énoncé 371 : Câble d'alimentation et adaptateur CA (au Japon uniquement)

接続ケーブル、電源コード、ACアダプタ、バッテリーなどの部品は、必ず添付品または指定品をご使用ください。添付品・指定品以外の部品をご使用になると故障や動作不良、火災の原因となります。また、電気用品安全法により、当該法の認定（PSEとコードに表記）でなくUL認定（ULまたはCSAマークがコードに表記）の電源ケーブルは弊社が指定する製品以外の電気機器には使用できないためご注意ください。

### Traduction anglaise

When installing the product, please use the provided or designated connection cables/power cables/AC adaptors. Using any other cables/adaptors could cause a malfunction or a fire. Electrical Appliance and Material Safety Law prohibits the use of UL-certified cables (that have the “UL” shown on the code) for any other electrical devices than products designated by CISCO. The use of cables that are certified by Electrical Appliance and Material Safety Law (that have “PSE” shown on the code) is not limited to CISCO-designated products.

## Industrie Canada

### Déclaration de conformité canadienne

AIR-AP1141N-E-K9

2461B-102069

AIR-AP1142N-E-K9

2461B-102070

This Class B Digital apparatus meets all the requirements of the Canadian Interference-Causing Equipment Regulations.

Cet appareil numérique de la classe B respecte les exigences du Règlement sur le matériel brouilleur du Canada.

Cet appareil respecte les Limites d'Industrie Canada concernant les appareils de classe B. Son utilisation est sujette aux deux conditions suivantes :

1. Cet appareil ne peut pas causer d'interférences nuisibles.
2. Cet appareil doit accepter toutes les interférences, y compris celles qui sont susceptibles de perturber le fonctionnement de l'appareil.

Les points d'accès Cisco Aironet sont certifiés conformes à la norme RSS-210. L'utilisation de ce périphérique sur un système fonctionnant partiellement ou entièrement à l'extérieur peut requérir l'obtention d'une licence, par l'utilisateur, pour le système, conformément aux réglementations en vigueur au Canada. Pour plus d'informations, contactez votre agence Industrie Canada locale.

## Communauté européenne, Suisse, Norvège, Islande et Liechtenstein

Modèles :

AIR-AP1141N-E-K9

AIR-AP1142N-E-K9

Les normes suivantes ont été appliquées :

- Radio : EN 300.328-1, EN 300.328-2, EN 301.893
- EN 301.489-1, EN 301.489-17
- Sécurité : EN 60950-1



---

### Remarque

Ce matériel a été conçu pour être utilisé dans tous les pays de l'UE et de l'AELE. Son utilisation à l'extérieur peut faire l'objet de restrictions de fréquences et/ou peut être soumise à l'obtention d'une licence. Pour plus de détails, contactez le service de conformité industrielle de Cisco.

---

La marque CE ci-dessous est apposée sur le point d'accès doté d'une radio 2,4 GHz et d'une radio 5 GHz :



## Déclaration de conformité à la directive européenne 1999/5/CE (R&TTE)

Български [Bulgarian]	Това оборудване отговаря на съществените изисквания и приложими клаузи на Директива 1999/5/EC.
Česky [Czech]:	Toto zařízení je v souladu se základními požadavky a ostatními odpovídajícími ustanoveními Směrnice 1999/5/EC.
Dansk [Danish]:	Dette udstyr er i overensstemmelse med de væsentlige krav og andre relevante bestemmelser i Direktiv 1999/5/EF.
Deutsch [German]:	Dieses Gerät entspricht den grundlegenden Anforderungen und den weiteren entsprechenden Vorgaben der Richtlinie 1999/5/EU.
Eesti [Estonian]:	See seade vastab direktiivi 1999/5/EÜ olulistele nõuetele ja teistele asjakohastele sätetele.
English:	This equipment is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.
Español [Spanish]:	Este equipo cumple con los requisitos esenciales así como con otras disposiciones de la Directiva 1999/5/CE.
Ελληνική [Greek]:	Αυτός ο εξοπλισμός είναι σε συμμόρφωση με τις ουσιώδεις απαιτήσεις και άλλες σχετικές διατάξεις της Οδηγίας 1999/5/EC.
Français [French]:	Cet appareil est conforme aux exigences essentielles et aux autres dispositions pertinentes de la Directive 1999/5/EC.
Íslenska [Icelandic]:	Þetta tæki er samkvæmt grunnkröfum og öðrum viðeigandi ákvæðum Tilskipunar 1999/5/EC.
Italiano [Italian]:	Questo apparato é conforme ai requisiti essenziali ed agli altri principi sanciti dalla Direttiva 1999/5/CE.
Latviešu [Latvian]:	Šī iekārta atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lietuvių [Lithuanian]:	Šis įrenginys tenkina 1999/5/EB Direktyvos esminius reikalavimus ir kitas šios direktyvos nuostatas.

Nederlands [Dutch]:	Dit apparaat voldoet aan de essentiële eisen en andere van toepassing zijnde bepalingen van de Richtlijn 1999/5/EC.
Malti [Maltese]:	Dan l-apparat huwa konformi mal-htigiet essenzjali u l-provedimenti l-oħra rilevanti tad-Direttiva 1999/5/EC.
Magyar [Hungarian]:	Ez a készülék teljesíti az alapvető követelményeket és más 1999/5/EK irányelvben meghatározott vonatkozó rendelkezéseket.
Norsk [Norwegian]:	Denne utstyret er i samsvar med de grunnleggende krav og andre relevante bestemmelser i EU-direktiv 1999/5/EF.
Polski [Polish]:	Urządzenie jest zgodne z ogólnymi wymaganiami oraz szczególnymi warunkami określonymi Dyrektywą UE: 1999/5/EC.
Português [Portuguese]:	Este equipamento está em conformidade com os requisitos essenciais e outras provisões relevantes da Directiva 1999/5/EC.
Română [Romanian]:	Acest echipament este în conformitate cu cerințele esențiale și cu alte prevederi relevante ale Directivei 1999/5/EC.
Slovensko [Slovenian]:	Ta naprava je skladna z bistvenimi zahtevami in ostalimi relevantnimi pogoji Direktive 1999/5/EC.
Slovensky [Slovak]:	Toto zariadenie je v zhode so základnými požiadavkami a inými príslušnými nariadeniami direktív: 1999/5/EC.
Suomi [Finnish]:	Tämä laite täyttää direktiivin 1999/5/EY olennaiset vaatimukset ja on siinä asetettujen muiden laitetta koskevien määräysten mukainen.
Svenska [Swedish]:	Denna utrustning är i överensstämmelse med de väsentliga kraven och andra relevanta bestämmelser i Direktiv 1999/5/EC.

142730

# Déclaration de conformité concernant l'exposition aux radiofréquences

## États-Unis

L'exposition aux radiofréquences émises par ce système a été évaluée conformément aux limites de la norme ANSI C 95.1 (American National Standards Institute). L'évaluation s'est appuyée sur la norme ANSI C 95.1 et sur la norme FCC OET Bulletin 65C rév. 01,01. Cette norme définit à 20 cm (7,9 po) la distance minimale devant séparer l'antenne de toute personne.

## Canada

L'exposition aux radiofréquences émises par ce système a été évaluée conformément aux limites de la norme ANSI C 95.1 (American National Standards Institute). Cette évaluation s'est appuyée sur le document RSS-102 rév. 2. Cette norme définit à 20 cm (7,9 po) la distance minimale devant séparer l'antenne de toute personne.

## Union européenne

L'exposition humaine aux radiofréquences émises par ce système a été évaluée conformément aux limites de l'ICNIRP (International Commission on Non-Ionizing Radiation Protection). Cette évaluation s'est appuyée sur la norme EN 50385, Norme produit pour la démonstration de la conformité des stations de base radio et des stations terminales fixes pour les radio-télécommunications, aux restrictions de base ou aux niveaux de référence relatifs à l'exposition de l'homme aux champs électromagnétiques de radiofréquence compris entre 300 MHz et 40 GHz. Cette norme définit à 20 cm (7,9 po) la distance minimale devant séparer l'antenne de toute personne.

## Australie

L'exposition humaine aux radiofréquences émises par ce système a été évaluée conformément à la norme australienne sur la protection contre les rayonnements et conformément aux limites de l'ICNIRP (International Commission on Non-Ionizing Radiation Protection). Cette norme définit à 20 cm (7,9 po) la distance minimale devant séparer l'antenne de toute personne.

## Normes administratives pour les points d'accès Cisco Aironet à Taïwan

Cette section présente les normes administratives relatives à l'utilisation de points d'accès Cisco Aironet à Taïwan. Les règles s'appliquant à tous les points d'accès sont fournies en chinois et en anglais.

## Traduction chinoise

### 低功率電波輻射性電機管理辦法

第十二條 經型式認證合格之低功率射頻電機，非經許可，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

第十四條 低功率射頻電機之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。

前項合法通信，指依電信法規定作業之無線電信。

低功率射頻電機須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

127048

## Traduction anglaise

### Administrative Rules for Low-power Radio-Frequency Devices

#### Article 12

For those low-power radio-frequency devices that have already received a type-approval, companies, business units or users should not change its frequencies, increase its power or change its original features and functions.

#### Article 14

The operation of the low-power radio-frequency devices is subject to the conditions that no harmful interference is caused to aviation safety and authorized radio station; and if interference is caused, the user must stop operating the device immediately and can't re-operate it until the harmful interference is clear.

The authorized radio station means a radio-communication service operating in accordance with the Communication Act.

The operation of the low-power radio-frequency devices is subject to the interference caused by the operation of an authorized radio station, by another intentional or unintentional radiator, by industrial, scientific and medical (ISM) equipment, or by an incidental radiator.

## Traduction chinoise

### 低功率射頻電機技術規範

#### 4.7 無線資訊傳輸設備

4.7.5 在 5.25-5.35 兆赫頻帶內操作之無線資訊傳輸設備，限於室內使用。

4.7.6 無線資訊傳輸設備須忍受合法通信之干擾且不得干擾合法通信；如造成干擾，應立即停用，俟無干擾之虞，始得繼續使用。

4.7.7 無線資訊傳輸設備的製造廠商應確保頻率穩定性，如依製造廠商使用手冊上所述正常操作，發射的信號應維持於操作頻帶中。

202591

## Utilisation des points d'accès Cisco Aironet au Brésil

Cette section contient des informations propres à l'utilisation des points d'accès Cisco Aironet au Brésil.

### Modèles de points d'accès

AIR-AP1142N-T-K9

AIR-AP1141N-A-K9

## Informations réglementaires

La Figure 15 présente les informations réglementaires brésiliennes concernant les modèles de points d'accès identifiés à la section précédente.

**Figure 15** Informations réglementaires brésiliennes



## Traduction portugaise

Este equipamento opera em caráter secundário, isto é, não tem direito a proteção contra interferência prejudicial, mesmo de estações do mesmo tipo, e não pode causar interferência a sistemas operando em caráter primário.

## Traduction anglaise

This equipment operates on a secondary basis and consequently must accept harmful interference, including interference from stations of the same kind. This equipment may not cause harmful interference to systems operating on a primary basis.





**Siège social aux États-Unis**  
Cisco Systems, Inc.  
San Jose, Californie

**Siège social en Asie**  
Cisco Systems (USA) Pte. Ltd.  
Singapour

**Siège social en Europe**  
Cisco Systems International BV  
Amsterdam, Pays-Bas

**Cisco dispose de plus de 200 agences à travers le monde. Les adresses et les numéros de téléphone et de fax sont répertoriés sur le site Web de Cisco à l'adresse [www.cisco.com/go/offices](http://www.cisco.com/go/offices).**

Cisco et le logo Cisco sont des marques déposées de Cisco Systems, Inc. et/ou de ses filiales aux États-Unis et dans d'autres pays. Vous trouverez une liste des marques commerciales de Cisco sur la page Web [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Les autres marques commerciales mentionnées dans les présentes sont la propriété de leurs détenteurs respectifs. L'utilisation du terme « partenaire » n'implique pas de relation de partenariat entre Cisco et toute autre entreprise. (1005R)

© 2011 Cisco Systems, Inc. Tous droits réservés.

78-20203-01