

À lire en priorité



Remarque

Si vous avez acheté un point d'accès 1242G, le présent guide de démarrage rapide peut quelquefois se rapporter à la radio 802.11a. Cependant, votre point d'accès 1242G ne contient pas de radio 802.11a. Il contient uniquement une radio 802.11b ou 802.11g. Veuillez donc ignorer les sections du guide de démarrage rapide se rapportant spécifiquement à une radio 802.11a.

Reportez-vous au tableau suivant et aux instructions pour ouvrir le capot supérieur. Le tableau contient des informations indispensables à la bonne configuration de votre point d'accès.

Paramètre	Valeur par défaut
Login	<i>Cisco</i> (sensible à la casse)
Password	<i>Cisco</i> (sensible à la casse)
IP address	Adresse IP déterminée par le serveur DHCP.
SSID (Service Set Identifier)	Reportez-vous à la section « Configuration radio et de l'adresse IP » à la page 2.

DEL d'indication d'état	Description de l'état
Bleu	Conditions de fonctionnement normales ; au moins un périphérique client sans fil est associé au point d'accès.
Vert clair	Conditions de fonctionnement normales ; aucun périphérique client sans fil n'est associé au point d'accès.
Orange ou rouge	Erreur. Reportez-vous à la section « Vérification des DEL du point d'accès » à la page 45.

Configuration radio et de l'adresse IP

Le point d'accès est fourni avec sa radio désactivée et sans adresse IP ou identifiant SSID attribué. Lorsque vous configurez le point d'accès pour la première fois, vous devez les activer. Aucune adresse IP n'est désormais attribuée au point d'accès. Il est configuré de façon à obtenir une adresse IP attribuée par un serveur DHCP. Si votre réseau n'utilise pas de serveur DHCP, vous devez vous connecter au port de console du point d'accès et lui attribuer une adresse IP statique (reportez-vous à la section « [Attribution d'une adresse IP via l'interface de ligne de commande](#) » à la page 21).

Avant de commencer

Avant d'installer le point d'accès, assurez-vous que l'ordinateur utilisé est connecté au même réseau que le point d'accès. Récupérez auprès de votre administrateur réseau les informations suivantes :

- Le nom d'hôte du point d'accès.
- L'identifiant SSID sensible à la casse pour vos réseaux radio 802.11g et 802.11a.
- Un nom de communauté SNMP (Simple Network Management Protocol) et un attribut de fichier SNMP (si le protocole SNMP est utilisé).
- L'adresse MAC (Media Access Control) indiquée sur l'étiquette située sous le point d'accès (par exemple, 0016462584c), en cas d'emploi de l'utilitaire de configuration IP Cisco pour déterminer l'adresse IP du point d'accès.
- Si vous n'êtes connecté à aucun serveur DHCP, vous pouvez attribuer une adresse IP au point d'accès à l'aide de l'interface de ligne de commande. Dans ce cas, obtenez une adresse IP unique pour le point d'accès, une passerelle par défaut et un masque de sous-réseau auprès de votre administrateur réseau.

Informations de sécurité

Grâce au dossier ET Docket 96-8, la FCC a adopté une norme de sécurité relative à l'exposition humaine à l'énergie électromagnétique des fréquences radio (RF) émise par les équipements certifiés par la FCC. Lorsqu'ils sont utilisés avec des antennes Cisco Aironet approuvées, les produits Cisco Aironet sont conformes aux limites pour un environnement non contrôlé énoncées dans les normes OET-65 et ANSI C95.1, 1991.

L'installation correcte des composants radio, selon les instructions fournies dans ce manuel, entraîne une exposition de l'utilisateur nettement inférieure aux limites recommandées par la FCC.

- Ne manipulez pas de composants radio et faites en sorte d'éloigner les antennes de toute partie du corps, notamment du visage ou des yeux, pendant la transmission.
- L'utilisation d'appareils sans fil dans des endroits dangereux est soumise aux contraintes imposées par les directives de sécurité relatives à de tels environnements.

Mises en garde

Les versions traduites des mises en garde suivantes figurent dans l'annexe A du guide *Cisco Aironet 1240AG Series Access Point Hardware Installation Guide*.



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

Un système de protection contre les courts-circuits (surintensité) doit être installé dans le bâtiment. 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 au moins 20 cm (7,9 po) de toute personne. Énoncé 332



Attention

Ne travaillez pas sur le système et ne touchez pas aux câbles pendant un orage. Énoncé 1001

Présentation générale

Ce guide a pour objectif de vous faciliter la configuration de base d'un point d'accès Cisco Aironet 1240AG via son interface graphique d'utilisateur, dans votre navigateur Internet. L'interface graphique constitue le principal outil de configuration. Vous pouvez également procéder via l'interface de ligne de commande. Pour obtenir des instructions concernant l'utilisation de l'interface de ligne de commande, reportez-vous au guide *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points*.



Remarque

La configuration du point d'accès à l'aide du réseau SWAN (Structured Wireless-Aware Network) de Cisco ou du moteur de solution LAN sans fil (WLSE) de Cisco n'est pas abordée dans ce guide. Pour plus d'informations relatives à la configuration, reportez-vous aux documents appropriés concernant le SWAN ou le WLSE. Ces documents sont également disponibles sur Cisco.com.

Ce tableau répertorie les documents liés aux points d'accès de la gamme 1240AG.

Sujet	Document
Configuration avancée	<i>Cisco IOS Software Configuration Guide for Cisco Aironet Access Points</i> <i>Cisco Aironet Command Reference for Cisco Aironet Access Points and Bridges</i>
Montage du point d'accès	<i>Cisco Aironet 1240AG Series Access Point Hardware Installation Guide</i>
Configuration système requise, remarques importantes, limitations et mises à jour de dernière minute	<i>Release Notes for Cisco Aironet 1240AG Series Access Points for Cisco IOS Release 12.3(7)JA</i> (ou version ultérieure)

Ces documents sont disponibles sur Cisco.com via l'URL suivante :

www.cisco.com/en/US/products/ps6521/tsd_products_support_series_home.html

Déballage du point d'accès

Pour déballer le point d'accès, procédez comme suit :

1. Ouvrez l'emballage et retirez son contenu avec soin.
2. Remplacez tous les matériaux d'emballage dans le conteneur et conservez-le.
3. Assurez-vous que tous les éléments indiqués dans la section Contenu du coffret sont bien présents. Vérifiez qu'aucun élément n'est endommagé. Si un élément est endommagé ou absent, contactez votre représentant commercial Cisco agréé.

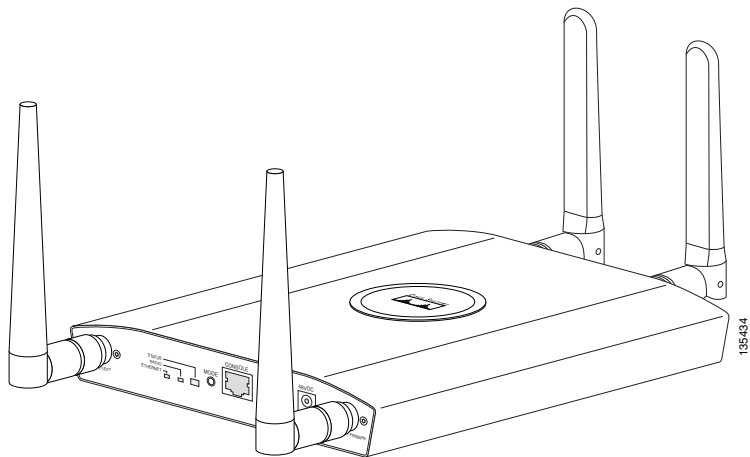
Contenu du coffret

Chaque coffret du point d'accès contient les éléments suivants :

- point d'accès Cisco Aironet 1240AG ;
- module d'alimentation Cisco Aironet 1240AG (module d'alimentation universel), en option ;
- kit et matériel de montage ;

- 1 plaque de montage ;
 - support de protection du câble ;
 - 2 attaches pour rail en T sur faux-plafond (rails en T standard et encastrés pris en charge) ;
 - 1 loquet de sécurité ;
 - 4 vis à métaux Phillips à tête cylindrique large 6 x 32 x ½ po ;
 - 1 vis à tôle Phillips à tête cylindrique large 8 x 18 x ¾ po ;
 - 2 fixations à cheville en plastique n° 8 ;
 - 1 écrou 10 x 24 (pour goujon de mise à la terre sur support de montage) ;
 - 4 protections de pied en caoutchouc ;
 - 2 attaches autobloquantes pour câbles ;
- *Guide de démarrage rapide des points d'accès de la gamme Cisco Aironet 1240AG ;*
- *mises en garde pour les points d'accès Cisco Aironet 1240AG ;*
- cartes d'enregistrement de produit Cisco et de commentaires sur la documentation Cisco.

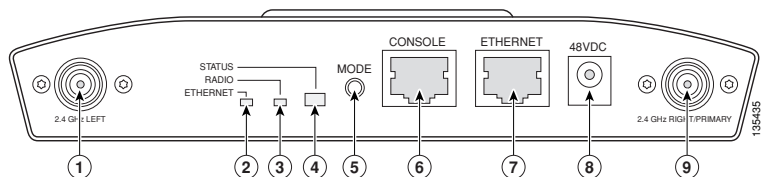
Les illustrations suivantes représentent le point d'accès avec ses antennes externes connectées.



Remarque

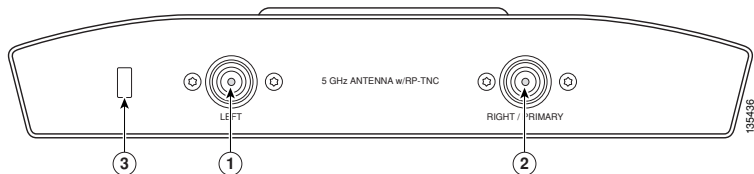
Les antennes 2,4 GHz et 5 GHz de cet exemple ne sont pas fournies avec le point d'accès. Les antennes doivent faire l'objet d'une commande distincte.

Cette illustration représente les connexions et les composants à l'arrière du point d'accès 2,4 GHz.



1	Connecteur d'antenne 2,4 GHz (gauche)	6	Port de console
2	DEL d'indication d'état Ethernet	7	Port Ethernet
3	DEL d'indication d'état Radio	8	Port d'alimentation 48 VCC
4	DEL d'indication d'état	9	Connecteur d'antenne 2,4 GHz (droit/principal)
5	Commutateur de mode		

Cette illustration représente les connexions et les composants à l'arrière du point d'accès 5 GHz.



1	Connecteur d'antenne 5 GHz (gauche)	3	Encoche de verrouillage de sécurité
2	Connecteur d'antenne 5 GHz (droit/principal)		

Résumé de l'installation

L'installation du point d'accès comprend les étapes suivantes :

- Montage du point d'accès
- Connexion à l'alimentation
- Obtention et attribution d'une adresse IP
- Configuration de l'alimentation
- Configuration des paramètres de base
- Activation des interfaces radio
- Configuration des paramètres de sécurité

Montage du point d'accès

Vous trouverez des instructions de montage détaillées dans le guide *Cisco Aironet 1240AG Series Access Point Hardware Installation Guide*. Ce document est disponible sur Cisco.com à l'URL suivante :

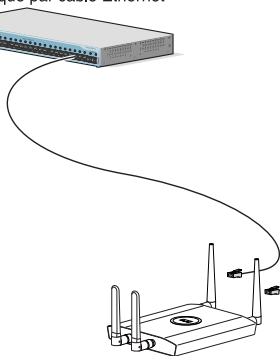
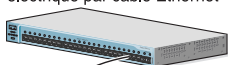
www.cisco.com/en/US/docs/wireless/access_point/1240/installation/guide/1240hig5.html

Connexion à l'alimentation

Le point d'accès peut être alimenté localement à l'aide du module d'alimentation CA ou via l'Ethernet à l'aide d'un équipement d'alimentation. L'illustration suivante présente les différentes options d'alimentation pour le point d'accès.

Option 1

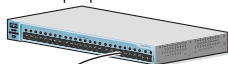
Commutateur avec alimentation électrique par câble Ethernet



Point d'accès

Option 2

Commutateur sans alimentation électrique par câble Ethernet



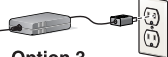
Injecteur de puissance



Cordon d'alimentation



Alimentation universelle



Option 3

135476-fr



Attention

Ce produit doit être connecté à une source d'alimentation PoE conforme à la norme IEEE 802.3af ou à une source d'alimentation limitée conforme à la norme IEC60950.

Énoncé 353

Les différentes options d'alimentation du point d'accès sont les suivantes :

- Option 1 : commutateurs avec alimentation électrique par câble Ethernet suffisante :
 - commutateur avec alimentation électrique par câble Ethernet, comme Catalyst 3550 PWR XL, 3560-48PS, 3750-48PS, 4500 avec module PoE 802.3af ou 6500 avec module PoE 802.3af
 - autre commutateur avec alimentation électrique par câble Ethernet prenant en charge la norme IEEE 802.af
- Option 2 : les commutateurs avec alimentation électrique par câble Ethernet insuffisante peuvent utiliser l'injecteur de puissance :
 - injecteur de puissance Cisco Aironet (AIR-PWRINJ3 ou AIR-PWRINJ-FIB)
- Option 3 : alimentation locale à l'aide d'un module d'alimentation



Remarque

Il est possible que certains commutateurs et tableaux de répartition plus anciens ne fournissent pas assez de puissance pour faire fonctionner le point d'accès. Au moment de la mise sous tension, si le point d'accès ne peut pas déterminer que la source d'alimentation lui fournit une puissance suffisante, il désactive automatiquement les deux radios pour éviter la surintensité. Le point d'accès active également la DEL d'indication d'état qui signale une erreur correspondant à une faible alimentation et crée une entrée dans le journal des erreurs. Pour plus d'informations, reportez-vous au guide *Cisco Aironet 1240AG Series Access Point Hardware Installation Guide*.

Lorsque le point d'accès est sous tension, il lance une séquence de démarrage de routine que vous pouvez suivre en observant les trois DEL à l'arrière du point d'accès 2,4 GHz. Lorsque les trois DEL deviennent vertes pour indiquer le démarrage du système d'exploitation Cisco IOS, la DEL d'indication d'état clignote en vert ; cela signifie que Cisco IOS est opérationnel. Dans cet état, la DEL Ethernet est vert fixe en l'absence de trafic et éteinte en cas de transmission en cours. La durée de la séquence est d'environ 1 minute. Pour obtenir une description des DEL, reportez-vous à la section « [Vérification des DEL du point d'accès](#) » à la page 45.

À la fin de la séquence, vous pouvez obtenir l'adresse IP du point d'accès et effectuer une configuration initiale. Pour obtenir des instructions sur la définition de paramètres de base pour le point d'accès, reportez-vous à la section « [Configuration des paramètres de base](#) » à la page 27.



Remarque

Si votre point d'accès est alimenté par câble Ethernet, ne connectez pas le module d'alimentation au point d'accès. L'utilisation de deux sources d'alimentation peut entraîner l'arrêt du point d'accès pour protéger les composants internes ainsi que l'arrêt du port auquel le point d'accès est connecté par le commutateur. Si le point d'accès est arrêté, vous devez retirer toutes les sources d'alimentation et n'en reconnecter qu'une seule.

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. Vous pouvez connaître l'adresse IP attribuée par le serveur DHCP en utilisant 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. Celui-ci 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 chaude.

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

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



Remarque

La référence Cisco du câble série est AIR-CONCAB1200.

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.

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

Lorsque vous attribuez une adresse IP au point d'accès via 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	configure terminal	Passer en mode de configuration globale
Étape 2	Interface bvi1	Passer en mode de configuration de l'interface BVI
Étape 3	ip address <i>adresse de masque</i>	Attribuer une adresse IP et une adresse de masque de sous-réseau à l'interface BVI



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.

Utilisation d'une session Telnet pour accéder à 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.

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**.

2. Lorsque la fenêtre Telnet s'affiche, cliquez sur **Connect** et sélectionnez **Remote System**.
3. Dans le champ Host Name, saisissez l'adresse IP du point d'accès et cliquez sur **Connect**.

Configuration de l'alimentation

Une fois le point d'accès 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 un courant suffisant. Dans ce cas, vous devez configurer les paramètres sur le point d'accès ou le commutateur afin d'identifier votre source d'alimentation.

Identifiez la source électrique et l'état du commutateur, puis vérifiez que vos périphériques sont configurés comme indiqué dans le tableau à la page 21.

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

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.
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.
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.
4. Faites-la défiler vers le bas jusqu'à la section System Power Settings, comme illustré ci-dessous.

System Power Settings

Power State: WARNING ALL RADIOS DISABLED

Power Source: LOW_POWER_CLASSIC (WS-C3524-PWR-XL on port 0009.7c05.200e)

Power Settings: Power Negotiation Pre-standard Compatibility

Power Injector: Installed on Port with MAC Address: (HHHH.HHHH.HHHH)

121707

5. Définissez les paramètres Power Settings et Power Injector. Vérifiez que l'état du commutateur est celui indiqué dans le tableau des paramètres d'alimentation.



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.

Source d'alimentation	Paramètres d'alimentation du système	État du commutateur
Équipements d'alimentation Cisco prenant en charge la technologie Cisco Intelligent Power Management ¹	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 ¹	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 ¹	Power Settings : option Power Negotiation sélectionnée Power Injector : non sélectionné	power inline never

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 ¹	Power Settings : option Power Negotiation sélectionnée Power Injector : sélectionné Adresse MAC ²	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.

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.

Configuration des paramètres de base

Pour que vous puissiez configurer les paramètres de base, le point d'accès et votre PC doivent avoir une adresse IP. Reportez-vous à la section « [Obtention et attribution d'une adresse IP](#) » à la page 18.

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 :

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.
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.
3. Appuyez sur **Entrée**. La page Summary Status s'affiche.

Home: Summary Status

Association

Clients_0 [Repeater_0](#)

Network Identity

IP Address 10.91.107.16

MAC Address 000b.fcff.b04e

Network Interfaces

Interface	MAC Address	Transmission Rate
FastEthernet	000b.fcff.b04e	100Mb/s
Radio0-802.11G	000b.fcff.b24e	54.0Mb/s
Radio1-802.11A	000b.fcff.b44e	54.0Mb/s

Event Log

Time	Severity	Description
Mar 1 00:00:10.803	◆ Notification	Line protocol on Interface BV11, changed state to up
Mar 1 00:00:10.754	◆ Notification	Line protocol on Interface Dot11Radio1, changed state to down
Mar 1 00:00:10.730	◆ Notification	Line protocol on Interface Dot11Radio0, changed state to down
Mar 1 00:00:10.593	◆ Notification	Line protocol on Interface FastEthernet0, changed state to up
Mar 1 00:00:10.082	⚠ Warning	Full power - AC_ADAPTOR inline power source
Mar 1 00:00:10.075	◆ Notification	SNMP agent on host AP1242AG is undergoing a cold start
Mar 1 00:00:10.075	◆ Notification	System restarted --
Mar 1 00:00:10.075	◆ Notification	Configured from memory by console
Mar 1 00:00:09.754	◆ Notification	Interface Dot11Radio1, changed state to administratively down
Mar 1 00:00:09.730	◆ Notification	Interface Dot11Radio0, changed state to administratively down

Refresh

230145

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
EXPRESS SET UP
EXPRESS SECURITY
NETWORK MAP +
ASSOCIATION +
NETWORK +
INTERFACES +
SECURITY +
SERVICES +
WIRELESS SERVICES +
SYSTEM SOFTWARE +
EVENT LOG +

Hostname AP1242AG AP1242AG uptime is 1 week, 2 days, 17 hours, 0 minutes

Express Set-Up

Host Name:

MAC Address:

Configuration Server Protocol: DHCP Static IP

IP Address:

IP Subnet Mask:

Default Gateway:

SNMP Community:

Read-Only Read-Write

Radio0.802.11G

Role in Radio Network: Access Point Repeater
 Root Bridge Non-Root Bridge
 Workgroup Bridge Scanner

Optimize Radio Network for: Throughput Range Default Custom

Alronet Extensions: Enable Disable

Radio1.802.11A

Role in Radio Network: Access Point Repeater
 Root Bridge Non-Root Bridge
 Workgroup Bridge Scanner

Optimize Radio Network for: Throughput Range Default Custom

Alronet Extensions: Enable Disable

230144

5. Configurez 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 écriture.



Remarque

Les paramètres radio suivants doivent être appliqués séparément à chaque type de radio : Radio0 - 802.11G et Radio1 - 802.11A.

- Role in Radio Network : permet de déterminer la fonction 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 périphériques client sans fil Cisco Aironet.
- Non-Root Bridge : indique que l'unité fonctionne en tant que pont non racine et qu'elle se connecte à un réseau LAN distant. Dans ce mode, l'unité doit s'associer à un pont racine Cisco Aironet via l'interface sans fil. Le pont non racine prend en charge des périphériques clients sans fil.
- 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 : spécifie 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. Désactiver les 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 suivant énumère les paramètres par défaut de la page Express Setup.

Paramètre	Valeur par défaut
System Name	ap
Configuration Server Protocol	DHCP
IP Address	Affectée par DHCP Remarque Le point d'accès ne possède pas d'adresse IP par défaut.
IP Subnet Mask	Affectée par DHCP
Default Gateway	Affectée par DHCP
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 devienne orange (environ 2 à 3 secondes).

Activation des interfaces radio

Dans la version 12.3(7)JA de Cisco IOS, les radios du point d'accès sont désactivées par défaut et il n'existe 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. Ces modifications de la configuration par défaut renforcent la sécurité des points d'accès récemment installés. Pour obtenir des instructions sur la configuration de l'identifiant SSID, reportez-vous à la section « [Configuration des paramètres de sécurité](#) » à la page 36.

Pour activer les interfaces radio, procédez comme suit :

1. Accédez à votre point d'accès.
2. Lorsque la page Summary Status s'affiche, cliquez sur **Radio0-802.11G**. La page d'état radio 2,4 GHz s'affiche.
3. Cliquez sur l'onglet **Settings** en haut de la page. La page Radio Settings s'affiche.

4. Cliquez sur **Enable** dans le champ Enable Radio.
5. Cliquez sur **Apply**.
6. Cliquez sur **Radio1-802.11A**. La page d'état radio 5 GHz s'affiche.
7. Répétez les étapes 3 à 5.
8. Fermez le navigateur Internet.

Configuration des paramètres de sécurité

Après les paramètres de base de votre point d'accès, vous devez configurer les 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. Pour plus d'informations sur la sécurité, reportez-vous au *guide de configuration du logiciel Cisco IOS pour les points d'accès Cisco Aironet*.

Configuration des paramètres de sécurité de base

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

- HOME
- EXPRESS SET-UP
- EXPRESS SECURITY**
- NETWORK MAP +
- ASSOCIATION +
- NETWORK INTERFACES +
- SECURITY +
- SERVICES +
- WIRELESS SERVICES +
- SYSTEM SOFTWARE +
- EVENT LOG +

Hostname AP1242AG

AP1242AG uptime is 1 week, 3 days, 12 hours, 51 minutes

Express Security Set-Up

SSID Configuration

1. SSID [Broadcast SSID in Beacon](#)

2. VLAN

No VLAN Enable VLAN ID: (1-4095) Native VLAN

3. Security

[No Security](#)

[Static WEP Key](#)

Key 1 128 bit

[EAP Authentication](#)

RADIUS Server: (Hostname or IP Address)

RADIUS Server Secret:

[WPA](#)

RADIUS Server: (Hostname or IP Address)

RADIUS Server Secret:

SSID Table

SSID	VLAN	Encryption	Authentication	Key Management	Native VLAN	Broadcast SSID

Close Window  Copyright (c) 1992-2005 by Cisco Systems, Inc.

230143

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 par défaut, 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 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 à un identifiant SSID :

- **No security** : option la moins sûre. Choisissez cette option uniquement pour les identifiants SSID utilisés dans un espace public 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).

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 de ces limites lorsque vous utilisez la page Express Security :

- Vous ne pouvez pas modifier les identifiants SSID. Cependant, vous pouvez les supprimer et les créer à nouveau.
- Vous ne pouvez pas attribuer les 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 :

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.

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, seul un identifiant SSID peut être inclus dans la balise du point d'accès.

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

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).

Si vous sélectionnez l'option EAP Authentication ou WPA, saisissez l'adresse IP et le secret partagé du serveur d'authentification sur votre réseau.



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 *guide de configuration du logiciel Cisco IOS pour les points d'accès Cisco Aironet*.

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

En cas de difficulté

Si vous avez suivi les instructions des sections précédentes de ce guide, vous ne devriez pas avoir de difficulté à installer et à faire fonctionner votre point d'accès. Dans le cas contraire, les sections suivantes fournissent des informations de dépannage de base.

Avant de contacter Cisco, cherchez la solution à votre problème dans ce guide ou dans le chapitre de dépannage du guide *Cisco Aironet 1240AG Series Access Point Hardware Installation Guide*.

Cliquez sur le lien suivant pour accéder à l'assistance technique Cisco :

www.cisco.com/cisco/web/support/index.html

Vérification des DEL du point d'accès

Si votre point d'accès ne fonctionne pas correctement, vérifiez la DEL d'indication d'état à l'arrière du point d'accès 2,4 GHz. La couleur des DEL vous permet d'évaluer l'état de l'appareil.

La signification des DEL est décrite dans le tableau suivant.

DEL d'indication d'état	DEL Ethernet	DEL radio	Signification
Bleu	—	—	Conditions de fonctionnement normales ; au moins un périphérique sans fil associé
Vert clair	—	—	Conditions de fonctionnement normales ; aucun périphérique sans fil associé
—	Vert, clignotant	—	Envoi ou réception de paquets Ethernet en cours
—	—	Vert, clignotant	Envoi ou réception de paquets radio en cours
Bleu foncé, clignotant	Vert ou vert clignotant	Vert clignotant ou éteint	Mise à jour du logiciel en cours
Orange	Divers	Divers	Erreurs Cisco IOS
Rouge, clignotant	Divers	Divers	Erreurs du programme d'amorçage

Pour plus d'informations sur ces codes d'état des DEL, reportez-vous au chapitre « Troubleshooting » du guide *Cisco Aironet 1240AG Series Access Point Hardware Installation Guide*.

Vérification des paramètres de base

La non-correspondance des paramètres de base est la cause la plus courante de perte de connectivité avec les clients sans fil. Si le point d'accès ne communique pas avec les périphériques clients, vérifiez les points suivants.

SSID

Les clients sans fil qui tentent de s'associer au point d'accès doivent utiliser le même identifiant SSID que celui-ci. Si l'identifiant SSID d'un périphérique client ne correspond pas à l'identifiant SSID d'un point d'accès dans la portée radio, le périphérique client ne s'associera pas.

Clés WEP

Les clés WEP que vous utilisez pour transmettre les données doivent être configurées exactement de la même manière sur votre point d'accès et sur tout périphérique sans fil auquel il est associé. Par exemple, si vous définissez le paramètre WEP Key 3 de votre adaptateur client sur la valeur 0987654321 et si vous sélectionnez cette clé comme clé de transmission, vous devez également définir la même valeur pour le paramètre WEP Key 3 du point d'accès. Cependant, le point d'accès n'a pas besoin d'utiliser la clé WEP Key 3 comme clé de transmission.

Pour obtenir des instructions sur le paramétrage des clés WEP du point d'accès, reportez-vous au guide *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points*.

Paramètres de sécurité

Les périphériques sans fil qui tentent de s'authentifier auprès de votre point d'accès doivent prendre en charge les mêmes options de sécurité que celles configurées sur le point d'accès, comme EAP ou LEAP, l'authentification par adresse MAC, Message Integrity Check (MIC), le hachage de clé WEP et les versions IEEE 802.1X.

Si un client sans fil ne parvient pas à s'authentifier auprès de votre point d'accès, contactez l'administrateur système pour connaître les paramètres de sécurité corrects dans l'adaptateur client ainsi que les versions de microprogramme et de pilote d'adaptateur client compatibles avec les paramètres du point d'accès.

Réinitialisation de la configuration par défaut

Si vous avez oublié le mot de passe permettant de configurer le point d'accès, il se peut que vous deviez réinitialiser entièrement la configuration. Pour ce faire, vous pouvez utiliser le bouton MODE du point d'accès.



Remarque

En suivant ces étapes, vous allez réinitialiser *tous* les paramètres de configuration par défaut, y compris les mots de passe, les clés WEP, l'adresse IP et l'identifiant SSID.

Utilisation du bouton Mode

Pour supprimer la configuration actuelle et restaurer tous les paramètres par défaut du point d'accès à l'aide du bouton MODE, procédez comme suit :

1. Débranchez l'alimentation du point d'accès (prise d'alimentation externe ou câble Ethernet en cas d'alimentation par câble).
2. Appuyez sur le bouton MODE et maintenez-le enfoncé pendant que vous rebranchez l'alimentation.
3. Appuyez sur le bouton MODE jusqu'à ce que la DEL Ethernet devienne orange (environ 2 à 3 secondes). Relâchez ensuite le bouton.
4. Une fois que le point d'accès a redémarré, vous devez le reconfigurer à l'aide de l'interface du navigateur Internet, de l'interface Telnet ou du port de console du point d'accès.

Utilisation de l'interface du navigateur Internet

Pour supprimer la configuration actuelle et restaurer tous les paramètres par défaut du point d'accès à l'aide de l'interface du navigateur Internet, procédez comme suit :

1. Ouvrez votre navigateur Internet. Vous devez utiliser Microsoft Internet Explorer (5.x ou version ultérieure) ou Netscape Navigator (4.x ou version ultérieure).

2. Saisissez l'adresse IP du point d'accès dans la barre d'adresse du navigateur et appuyez sur **Entrée**. L'écran Enter Network Password apparaît.
3. Saisissez le nom d'utilisateur *Cisco* dans le champ User Name.
4. Saisissez le mot de passe *Cisco* dans le champ Password et appuyez sur **Entrée**. La page Summary Status s'affiche.
5. Cliquez sur **System Software**. L'écran System Software apparaît.
6. Cliquez sur **System Configuration**. L'écran System Configuration apparaît.
7. Cliquez sur le bouton **Reset to Defaults**.



Remarque

Si le point d'accès est configuré avec une adresse IP statique, l'adresse IP ne change pas.

Une fois que le point d'accès a redémarré, vous devez le reconfigurer.

Informations relatives à la conformité

Cet équipement a été testé et est conforme à la norme européenne sur les télécommunications ETS 300.328. Cette norme couvre les systèmes de transmission de données large bande auxquels fait référence la recommandation CEPT T/R 10.01.

Cet équipement approuvé est conçu de façon à fournir une protection raisonnable contre les interférences nuisibles lorsqu'il est utilisé dans un environnement commercial. Cet équipement génère, utilise et peut émettre de l'énergie radioélectrique. S'il n'est pas installé conformément aux instructions du manuel, il peut provoquer des interférences nuisibles aux communications radio.

Pour ce produit, vous trouverez les déclarations de conformité correspondant à l'Union européenne et aux autres pays suivant la directive UE 1999/5/CE (directive R&TTE) dans le guide *Cisco Aironet 1240AG Series Access Point Hardware Installation Guide*. Ce guide est disponible sur Cisco.com.