

À lire en priorité



Remarque

Pour consulter les documents en français (y compris les nouveautés), identifiez-vous :

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



Remarque

Si vous avez acheté un point d'accès 1130G, ce guide de démarrage rapide fait parfois référence à une radio 802.11a. Cependant, votre point d'accès 1130G 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	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. Pour plus d'informations, reportez-vous à la section « Obtention d'une adresse IP » à la page 19.
SSID (Service Set Identifier)	Aucun attribué
DEL d'indication d'état	Description de l'état
Bleu	Conditions de fonctionnement normales ; au moins un périphérique client est associé au point d'accès.
Vert clair	Conditions de fonctionnement normales ; aucun périphérique client n'est associé.
Orange ou rouge	Erreur. Reportez-vous à la section « Vérification des DEL du point d'accès » à la page 43.

Configuration radio et de l'adresse IP

Le point d'accès est livré avec sa radio désactivée. Vous devez l'activer lorsque vous configurez le point d'accès pour la première fois. De plus, aucune adresse IP n'est désormais attribuée au point d'accès. Il est configuré de façon à obtenir une adresse IP à l'aide d'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 20).

Ouverture du capot supérieur

Le capot supérieur permet d'accéder au câble et aux connexions d'alimentation.



Avertissement

N'ouvrez pas le capot supérieur du point d'accès comme une trappe ou une porte. Vous risqueriez de l'endommager. Une étiquette comportant des instructions est fixée sur le point d'accès. Prenez le temps de lire cette étiquette avant d'ouvrir le capot du point d'accès.

Une fois que vous avez pris connaissance de la procédure d'ouverture, nous vous recommandons de retirer l'étiquette et de la placer en lieu sûr, à l'intérieur de la couverture du présent guide, par exemple.

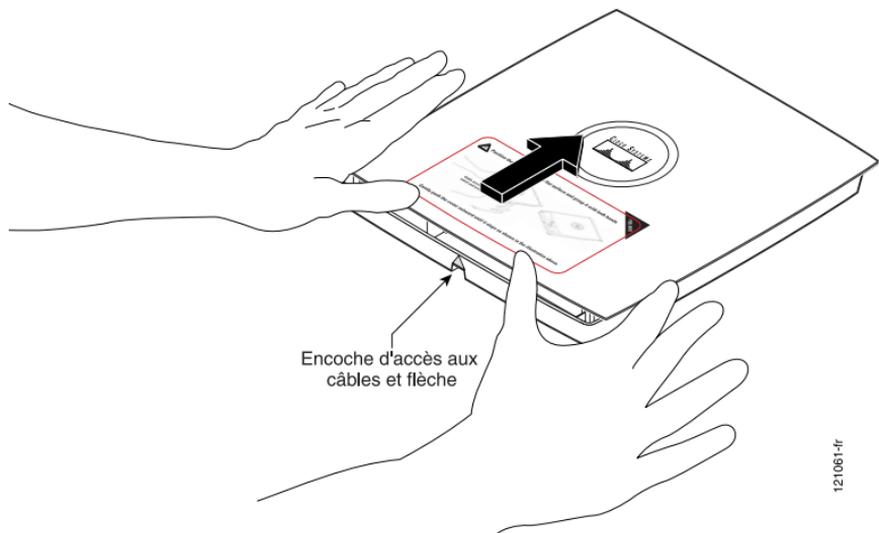


Remarque

Les indications des DEL d'état ne sont pas visibles lorsque le capot supérieur est ouvert.

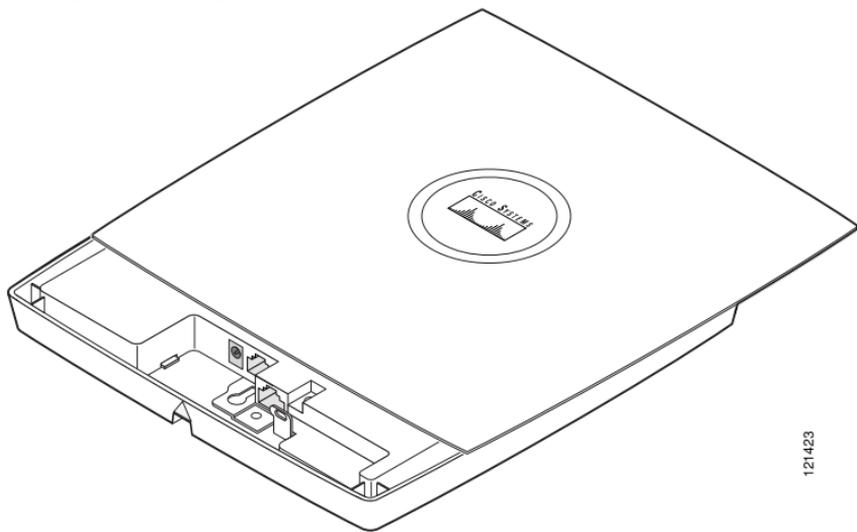
Pour ouvrir le capot supérieur, procédez comme suit :

1. Placez le point d'accès sur une surface plane et saisissez-le des deux mains, comme illustré.



121061-fr

2. Poussez doucement le capot en l'éloignant de vous jusqu'en butée, comme illustré.



3. Retirez l'étiquette comportant les instructions d'ouverture du capot supérieur.



Remarque

Nous vous recommandons de conserver cette étiquette pour pouvoir vous y reporter ultérieurement.

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. Une utilisation appropriée de cet appareil radio, selon les instructions fournies dans le présent document et dans le guide d'installation et de configuration, 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 gardes

Des versions traduites de ces mises en garde sont fournies dans le guide *Cisco Aironet 1130AG Series Access Point Hardware Installation Guide*.



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.



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.



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.



Attention

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



Attention

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



Attention

Un système de protection contre les courts-circuits (surintensité) doit être installé dans le bâtiment. Assurez-vous que la puissance nominale du dispositif de protection n'est pas supérieure à 20 A.

Présentation

Ce guide est conçu pour vous aider à effectuer la configuration de base d'un point d'accès Cisco Aironet 1130AG 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 guide offre une présentation générale du point d'accès, mais il ne décrit pas la procédure de montage. Ces instructions sont fournies dans le guide *Cisco Aironet 1130AG Series Access Point Hardware Installation Guide*, disponible sur Cisco.com.



Remarque

N'essayez pas de connecter un câble doté d'une gaine de protection au port Ethernet ou au port de console du point d'accès. En raison de l'espace restreint dans la zone de connexion, les connecteurs à gaine ne rentrent pas.

Ce tableau répertorie les documents liés aux points d'accès de la gamme 1130AG.

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 1130AG 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 1130AG Series Access Points for Cisco IOS Release 12.3(2)JA</i> (ou version ultérieure)

Ces documents sont disponibles sur Cisco.com via le lien suivant :

www.cisco.com/en/US/products/ps6087/tsd_products_support_series_home.html

Déballage du point d'accès

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

- Point d'accès Cisco Aironet 1130AG ;
- en option : Module d'alimentation Cisco Aironet 1130AG (alimentation universelle)
- kit matériel de montage :
 - 1 plaque de montage ;
 - 1 attache pour rail en T réglable sur plafond suspendu ;
 - 1 adaptateur pour loquet de sécurité ;
 - 4 vis à métaux Phillips à tête plate 6 x 32 x ¼ po ;
 - 1 vis à métaux Phillips à tête cylindrique 8 x 32 x 3/16 po ;
 - 2 fixations à cheville en plastique n° 8 ;
- le présent guide ;
- cartes d'enregistrement de produit Cisco et de commentaires sur la documentation Cisco.

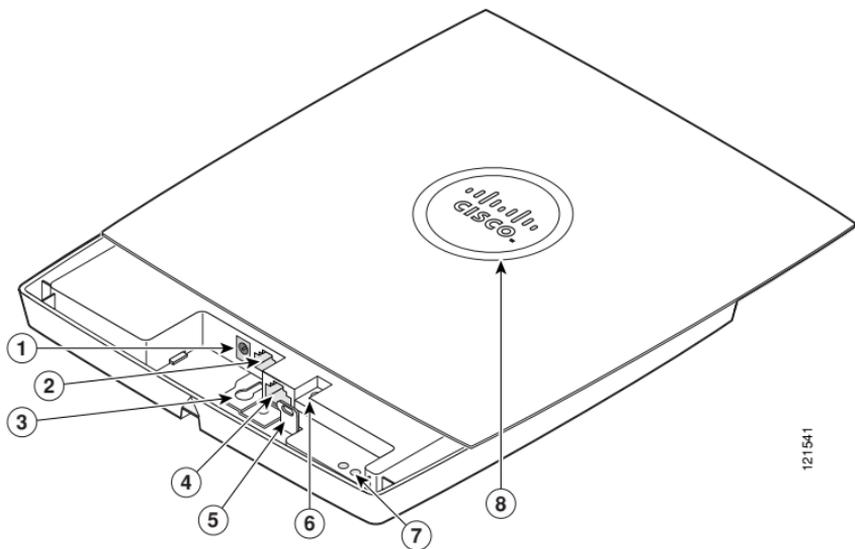
Procédez comme suit pour préparer l'installation.

1. Déballez soigneusement et retirez le point d'accès et le kit matériel du carton d'expédition.
2. Remplacez tous les matériaux d'emballage dans le conteneur et conservez-le.
3. Vérifiez que le contenu de l'emballage est complet et qu'aucun élément n'est endommagé. Si des éléments sont manquants ou endommagés, contactez votre représentant Cisco pour obtenir de l'aide.
4. Pour obtenir les instructions de montage, téléchargez le guide *Cisco Aironet 1130AG Series Access Point Hardware Installation Guide* sur le site Cisco.com.
5. Familiarisez-vous avec le point d'accès et ses caractéristiques, identifiées dans l'illustration.



Avertissement

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



121541

1	Connecteur d'alimentation	5	Languette de verrouillage
2	Port Ethernet	6	Bouton Mode
3	Encoche en trou de serrure	7	DEL Ethernet (E) et radio (R)
4	Port de console	8	DEL d'indication d'état

Résumé de l'installation

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

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

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 :

- un nom système ;
- l'identifiant SSID sans fil sensible à la casse pour votre réseau radio ;
- un nom de communauté SNMP (Simple Network Management Protocol) et l'attribut de fichier SNMP (si le protocole SNMP est utilisé).

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.

Montage du point d'accès

Le point d'accès est doté d'une plaque de montage universelle détachable qui permet de le monter sur des surfaces horizontales planes, telles qu'un plafond. La plaque de montage universelle est également utilisée pour monter le point d'accès sur une boîte de raccordement électrique ou réseau, ou sur les attaches pour rail fournies pour un montage sur faux-plafond.



Avertissement

Évitez de monter le point d'accès sur un mur ou une surface verticale. En effet, la plaque métallique de l'unité, conçue pour dissiper la chaleur, agit comme un réflecteur, ce qui entraîne la propagation directionnelle de l'antenne intégrée au point d'accès. Cette propagation directionnelle est susceptible de nuire aux performances, surtout lorsque vous avez recours à des fonctions avancées, telles que les applications vocales ou de localisation.

Le processus de montage est simple et nécessite des outils courants. Comme la plaque de montage universelle est détachable, vous pouvez l'utiliser afin de repérer la position des trous de montage pour votre installation. Il vous suffit ensuite d'installer le support de montage universel sur la surface et de fixer le point d'accès lorsque vous êtes prêt.

Une fois que vous avez monté le point d'accès, la languette de verrouillage vous permet de protéger le port Ethernet, les câbles d'alimentation et le bouton Mode, et également de fermer le point d'accès avec un cadenas.

Vous trouverez des instructions de montage détaillées dans le guide *Cisco Aironet 1130AG Series Access Point Hardware Configuration Guide*. Ce document est disponible sur Cisco.com.

Connexion à l'alimentation

Connectez le point d'accès 1130AG à une source électrique. Le point d'accès peut être alimenté localement à l'aide d'un module d'alimentation CA ou via l'Ethernet à l'aide d'un équipement d'alimentation. Quelle que soit la méthode choisie, la source électrique doit être conforme à la norme IEC60950 pour une source électrique limitée. Les périphériques IEC60950 comprennent les éléments suivants :

- un module d'alimentation CA branché sur le connecteur d'alimentation du point d'accès
- les périphériques PoE suivants :
 - une source d'alimentation conforme à la norme IEEE 802.3af ;
 - un commutateur d'alimentation électrique par câble Ethernet Cisco conforme ;
 - un injecteur de puissance Cisco avec un module d'alimentation CA conforme.



Avertissement

Si le point d'accès est alimenté en électricité via un périphérique PoE, le courant de sortie de l'équipement d'alimentation ne peut pas dépasser 400 mA ou 154 000 V/port, selon la limite la moins élevée. La source électrique doit être conforme à la norme IEC60950. Les équipements d'alimentation conformes à la norme IEEE 802.3af sont conformes à la norme IEC60950.

Lorsque le point d'accès est alimenté en électricité, une séquence de mise sous tension de routine commence. Vous pouvez la surveiller en observant la DEL d'indication d'état du point d'accès. Pendant la séquence de mise sous tension, la DEL s'allume dans différentes couleurs successivement. Une fois la séquence de mise sous tension terminée, la DEL s'allume en vert clair pour

indiquer que le point d'accès est prêt à fonctionner. Lorsqu'un client est associé au point d'accès, la DEL d'indication d'état passe au bleu. La DEL s'allume en orange pour indiquer un problème, comme l'impossibilité pour le point d'accès de vérifier que l'équipement d'alimentation fournit un courant suffisant, par exemple. Reportez-vous à la section « [Configuration de l'alimentation](#) » à la page 23.

Obtention d'une adresse IP

Pour fonctionner, votre point d'accès a besoin d'une adresse IP. Le point d'accès n'est plus livré avec une adresse IP par défaut. Il obtient une adresse IP à partir du serveur DHCP de votre réseau lorsque vous le connectez au réseau. Si votre réseau ne comporte pas de serveur DHCP, le point d'accès continue à demander une adresse IP jusqu'à ce que vous lui en attribuez une. Par conséquent, vous devez configurer l'adresse IP en ouvrant l'interface de ligne de commande à partir d'une session de terminal via le port de console du point d'accès. Reportez-vous à la section « [Attribution d'une adresse IP via l'interface de ligne de commande](#) » à la page 20.

Vous devez connaître l'adresse IP de votre point d'accès pour pouvoir utiliser l'interface graphique de gestion en ligne. Si votre point d'accès a obtenu son adresse IP à partir du serveur DHCP de votre réseau, vous ou votre administrateur réseau pouvez la trouver en interrogeant le serveur DHCP à

l'aide de l'adresse MAC du point d'accès. Vous pouvez également connaître l'adresse IP du point d'accès à l'aide de l'utilitaire de configuration IP de Cisco. Vous pouvez télécharger cet utilitaire sur le site Cisco.com.

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

Lorsque vous connectez le point d'accès au réseau local câblé, il se connecte au réseau via une interface de pont virtuelle (BVI) qu'il crée automatiquement. Au lieu de suivre des adresses IP indépendantes pour les ports radio et Ethernet du point d'accès, le réseau utilise l'interface BVI.

Pour accéder à l'interface de ligne de commande, vous pouvez connecter un PC au port de console à l'aide d'un câble série DB-9 à RJ-45 (AIR-CONCAB1200).



Remarque

Pour commander ce câble, consultez le site www.cisco.com/go/marketplace.

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.

Lorsque vous attribuez une adresse IP au point d'accès à l'aide de l'interface de ligne de commande, vous devez aussi 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 :

	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>address mask</i>	Attribuer une adresse IP et une adresse de masque de sous-réseau à l'interface BVI.



Remarque

Lorsque vous avez fini d'utiliser le port de console, vous devez retirer le câble série du 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**.

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 devrez configurer des paramètres sur le point d'accès ou le commutateur pour identifier la source électrique.

Identifiez la source électrique et l'état du commutateur, puis vérifiez que vos périphériques sont configurés comme indiqué dans le tableau à la page 20.

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-C3624-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 vérifier l'état du commutateur, 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. Veuillez consulter 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 d'une adresse IP](#) » à la page 19.

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.

The screenshot displays the configuration interface for a Cisco Aironet 1130AG Series Access Point. The page title is "Cisco Aironet 1130AG Series Access Point". The status bar shows "ap uptime is 7 minutes". A left-hand navigation menu includes options like HOME, EXPRESS SET-UP, NETWORK SECURITY, NETWORK MAP, ASSOCIATION, NETWORK INTERFACES, SECURITY, SERVICES, WIRELESS SERVICES, SYSTEM SOFTWARE, and EVENT LOG. The main content area is titled "Home: Summary Status" and contains several sections: "Association" (Clients: 0, Repeaters: 0), "Network Identity" (IP Address: 10.0.0.109, MAC Address: 000b.fcfc.1420), "Network Interfaces" (listing FastEthernet, Radio0-802.11G, and Radio1-802.11A with their respective MAC addresses and transmission rates), and "Event Log" (a table with columns for Time, Severity, and Description). A "Refresh" button is located at the bottom right of the main content area. The footer includes "Close Window" and "Copyright (c) 1992-2004 by Cisco Systems, Inc.".

12/7/05

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



Cisco Aironet 1130AG Series Access Point



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

Hostname ap

ap uptime is 7 minutes

Express Set-Up

Host Name:

MAC Address: 000b.fcfb.7d2f

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 Root Repeater Non-Root

Optimize Radio Network for: Throughput Range Default [Custom](#)

Aironet Extensions: Enable Disable

Radio1-802.11A

Role in Radio Network: Access Point Root Repeater Non-Root

Optimize Radio Network for: Throughput Range Default [Custom](#)

Aironet Extensions: Enable Disable

12/1/04

5. Configurez les paramètres en vous aidant des sections suivantes.

Host Name

Le nom système (system name) est un nom qui identifie le point d'accès sur votre réseau.

Valeur par défaut : *ap*

Configuration Server Protocol

Ce paramètre spécifie comment le point d'accès obtient une adresse IP.

Options : DHCP ou Static IP

Valeur par défaut : *DHCP*

Option	Description
DHCP	L'adresse IP est automatiquement attribuée par le serveur DHCP du réseau.
Static IP	Le point d'accès utilise l'adresse IP 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.

Options : Standard (HTTP) ou Secure (HTTPS)

Valeur par défaut : *Standard (HTTP)*

Option	Description
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 l'utilisateur et en provenance de ce dernier 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.

Attribut	Description
Read-Only	Le point d'accès n'autorise qu'un accès SNMP en lecture.
Read-Write	Le point d'accès autorise l'accès en lecture et en écriture.

Sections de configuration Radio 802.11G et 802.11A



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

Ce paramètre détermine la fonction qu'occupe le point d'accès dans le réseau sans fil.

Options : Access Point root ou Repeater non root

Valeur par défaut : *Access Point root*

Option	Description
Access Point root	Le point d'accès se connecte directement au réseau local Ethernet principal et accepte les associations avec des clients sans fil.
Repeater non root	Le point d'accès se connecte à un réseau local distant, accepte les associations avec des clients sans fil et doit s'associer à un point d'accès racine via l'interface sans fil.

Optimize Radio Network For

Ce paramètre optimise 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.

Options : Throughput, Range, Default, Custom

Valeur par défaut : *Default*

Option	Description
Throughput	Maximise le volume de données traité mais peut réduire la portée.
Range	Maximise la portée mais peut réduire le débit.
Default	Conserve les paramètres radio par défaut, qui garantissent à la fois une portée et un débit satisfaisants.
Custom	Utilise les paramètres que vous saisissez sur la page Network Interfaces de l'interface graphique d'utilisateur. Remarque Pour en savoir plus sur ce paramètre, reportez-vous au guide <i>Cisco IOS Software Configuration Guide for Cisco Aironet Access Points</i> ou au document <i>Cisco Aironet Command Reference for Cisco Aironet Access Points and Bridges</i> .

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.

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. La page Express Security est illustrée ci-dessous.



Cisco Aironet 1130AG Series Access Point



- HOME
- EXPRESS SETUP
- EXPRESS SECURITY
- NETWORK MAP +
- ASSOCIATION +
- NETWORK INTERFACES +
- SECURITY +
- SERVICES +
- WIRELESS SERVICES +
- SYSTEM SOFTWARE +
- EVENT LOG +

Hostname ap

ap uptime is 58 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](#)
 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

<input type="button" value="Delete"/>	SSID	VLAN	Encryption	Authentication	Key Management	Native VLAN	Broadcast SSID
<input checked="" type="radio"/>	tsunami	none	none	open	none		<input checked="" type="checkbox"/>

121703

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.

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 car, sur la page Express Security, les paramètres de cryptage et les types d'authentification sont liés. 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.

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**.

Les sections et paramètres configurables de l'écran Express Setup sont identifiés et brièvement décrits ci-dessous.

SSID Configuration

SSID

Le SSID est un identifiant unique que les clients utilisent pour s'associer à un point d'accès. Il permet aux périphériques clients de faire la distinction entre plusieurs réseaux sans fil dans la même zone. Un identifiant SSID peut être tout terme alphanumérique comprenant entre 2 et 32 caractères.

Valeur par défaut : *aucun identifiant SSID attribué*



Remarque

Les caractères suivants ne sont pas autorisés : ?, ", \$, [, \,], et +. D'autre part, l'identifiant SSID ne peut pas commencer par les caractères suivants : !, # et ;.

VLAN

Un réseau local virtuel (VLAN) est un réseau commuté segmenté de manière logique par fonction, équipe de projet ou application plutôt que selon des critères physiques ou géographiques.

Options : No VLAN, Enable VLAN ID (1–4095)

Valeur par défaut : *No VLAN*

Option	Description
No VLAN	Aucun réseau local virtuel n'est activé.
Enable VLAN ID	Active un réseau local virtuel et spécifie son numéro d'identification (1 à 4095).
Native VLAN	<p>Spécifie le réseau local virtuel qui transmet et reçoit normalement les données administratives.</p> <p>Remarque Une fois que vous avez activé un réseau local virtuel et que vous lui avez attribué un numéro d'identification, cochez la case Native VLAN pour le définir en tant que réseau local virtuel natif.</p>

Security

Cette option identifie les paramètres de sécurité disponibles sur la page Express Security Setup.

Options : No Security, Static WEP Key, EAP Authentication, WPA

Valeur par défaut : *No Security*

Option	Description
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. Cependant, 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.

Option	Description
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 et WPA2	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).

**Remarque**

Pour obtenir des informations détaillées sur la sécurité et les paramètres de sécurité, reportez-vous au guide *Cisco IOS Software Configuration Guide for Cisco Aironet Access Points*.

En cas de problèmes

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 1130AG Series Access Point Hardware Installation Guide*.

Le Centre d'assistance technique (TAC) tient à jour une liste des principaux problèmes liés aux technologies sans fil sur Cisco.com. Vous y accédez via le lien suivant :

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

Vérification des DEL du point d'accès

Si votre point d'accès ne fonctionne pas correctement, observez la DEL d'indication d'état sur la partie supérieure ou les DEL Ethernet et Radio dans la zone de la baie de câblage. Vous pouvez utiliser la couleur des voyants pour évaluer l'état de l'appareil.

**Remarque**

Pour voir les DEL Ethernet et Radio, vous devez ouvrir le capot du point d'accès. (Reportez-vous à la section « [Ouverture du capot supérieur](#) » à la page 3).

La signification des DEL est indiquée dans ce tableau.

Partie supérieure de l'unité	Zone de la baie de câblage		Signification
	DEL Ethernet	DEL radio	
DEL d'indication d'état			
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	—	Transmission ou réception de paquets Ethernet en cours

Partie supérieure de l'unité	Zone de la baie de câblage		Signification
DEL d'indication d'état	DEL Ethernet	DEL radio	
—	—	Vert, clignotant	Transmission ou réception de paquets radio
Bleu foncé, clignotant	Vert ou vert clignotant	Vert clignotant ou éteint	Mise à jour du logiciel en cours
Orange	Divers	Divers	Erreurs 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 1130AG 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 du protocole 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 micrologiciel 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. Ouvrez le capot du point d'accès (reportez-vous à la section « [Ouverture du capot supérieur](#) » à la page 3).
2. Débranchez l'alimentation du point d'accès (prise d'alimentation externe ou câble Ethernet en cas d'alimentation par câble).
3. Appuyez sur le bouton MODE et maintenez-le enfoncé pendant que vous rebranchez l'alimentation.
4. Maintenez le bouton MODE enfoncé jusqu'à ce que la DEL Ethernet s'allume en orange (environ 2 à 3 secondes). Relâchez ensuite le bouton.
5. 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.

8. 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 1130AG Series Access Point Hardware Installation Guide*. Ce guide est disponible sur Cisco.com.