



Point d'accès Cisco WAP125 bibande sans fil AC/N avec PoE

Première publication: 12 Octobre 2016

Dernière modification: 13 Juin 2018

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

LES SPÉCIFICATIONS ET INFORMATIONS SUR LES PRODUITS PRÉSENTÉS DANS CE MANUEL PEUVENT ÊTRE MODIFIÉES SANS PRÉAVIS. TOUTES LES DÉCLARATIONS, INFORMATIONS ET RECOMMANDATIONS PRÉSENTÉES DANS CE MANUEL SONT PRÉSUMÉES EXACTES, MAIS SONT OFFERTES SANS GARANTIE D'AUCUNE SORTE, EXPRESSE OU IMPLICITE. LES UTILISATEURS ASSUMENT LA PLEINE RESPONSABILITÉ DE L'UTILISATION QU'ILS FONT DE CES PRODUITS.

LA LICENCE LOGICIELLE ET LA LIMITATION DE GARANTIE APPLICABLES AU PRODUIT FAISANT L'OBJET DE CE MANUEL SONT EXPOSÉES DANS LA DOCUMENTATION LIVRÉE AVEC LE PRODUIT ET INTÉGRÉES À CE DOCUMENT SOUS CETTE RÉFÉRENCE. SI VOUS NE TROUVEZ PAS LA LICENCE LOGICIELLE OU LA LIMITATION DE GARANTIE, DEMANDEZ-EN UN EXEMPLAIRE À VOTRE REPRÉSENTANT CISCO.

La mise en œuvre Cisco de la compression d'en-tête TCP est l'adaptation d'un programme développé par l'Université de Californie, Berkeley (UCB) dans le cadre de la mise au point, par l'UCB, d'une version gratuite du système d'exploitation UNIX. Tous droits réservés. Copyright © 1981, Regents of the University of California.

NONOBTANT TOUTE AUTRE GARANTIE CONTENUE DANS LES PRÉSENTES, TOUS LES DOSSIERS DE DOCUMENTATION ET LES LOGICIELS PROVENANT DE CES FOURNISSEURS SONT FOURNIS « EN L'ÉTAT », TOUS DÉFAUTS INCLUS. CISCO ET LES FOURNISSEURS MENTIONNÉS CI-DESSUS DÉCLINENT TOUTE GARANTIE EXPLICITE OU IMPLICITE Y COMPRIS, MAIS SANS S'Y LIMITER, TOUTE GARANTIE DE QUALITÉ MARCHANDE, D'ADÉQUATION À UN USAGE PARTICULIER, D'ABSENCE DE CONTREFAÇON OU TOUTE AUTRE GARANTIE DÉCOULANT DE PRATIQUES OU DE RÈGLES COMMERCIALES.

CISCO OU SES FOURNISSEURS NE SERONT EN AUCUN CAS TENUS RESPONSABLES DES DOMMAGES INDIRECTS, PARTICULIERS, CONSÉCUTIFS OU ACCESSOIRES INCLUANT, SANS RESTRICTIONS, LES PERTES DE PROFITS, LA PERTE OU LA DÉTÉRIORATION DE DONNÉES RÉSULTANT DE L'UTILISATION OU DE L'IMPOSSIBILITÉ D'UTILISER CE MANUEL, MÊME SI CISCO OU SES FOURNISSEURS ONT ÉTÉ AVISÉS DE LA POSSIBILITÉ DE TELS DOMMAGES.

Les adresses IP (Internet Protocol) et les numéros de téléphone utilisés dans ce document sont fictifs. Tous les exemples, résultats d'affichage de commandes, schémas de topologie réseau et autres figures compris dans ce document sont donnés à titre d'exemple uniquement. L'utilisation d'adresses IP ou de numéros de téléphone réels à titre d'exemple est non intentionnelle et fortuite.

Cisco et le logo Cisco sont des marques ou des marques déposées de Cisco et/ou de ses filiales aux États-Unis et dans d'autres pays. Pour afficher la liste des marques Cisco, rendez-vous à l'adresse : <https://www.cisco.com/go/trademarks>. Les autres marques commerciales mentionnées dans le présent document sont la propriété de leurs détenteurs respectifs. L'utilisation du mot « partenaire » n'implique nullement une relation de partenariat entre Cisco et toute autre entreprise. (1721R)

© 2018 Cisco Systems, Inc. Tous droits réservés.



Le logo Java est une marque commerciale ou déposée de Sun Microsystems, Inc. aux États-Unis ou dans d'autres pays.

© 2018 Cisco Systems, Inc. Tous droits réservés.



TABLE DES MATIÈRES

CHAPITRE 1

Mise en route 1

- Configuration 1
- Utilisation de l'assistant d'installation de point d'accès 3
 - Utiliser l'assistant d'installation de point d'accès sur un appareil mobile 4
- Modification du mot de passe 5
- Service TCP/UDP 6
- État du système 7
- Configuration du démarrage rapide 7
- Navigation dans les fenêtres 8
 - Volet Navigation 9
 - Boutons de gestion 9

CHAPITRE 2

Configuration du système 11

- Réseau local 11
 - Configuration IPv4 11
 - Paramètres de configuration automatique DHCP 12
 - Configuration IPv6 13
 - Table des paramètres de port 14
 - Protocole STP (Spanning Tree Protocol) 15
 - Paramétrage des VLAN 15
 - Détection des appareils voisins 15
 - LLDP 16
 - Tunnel IPv6 16
- Heure 17
 - Acquisition automatique des paramètres d'heure via NTP 18
 - Configuration manuelle des paramètres d'heure 18

Notification	19
Affichage DEL	19
Paramètres des journaux	19
Serveur de journalisation distant	20
Afficher le journal système	21
Configuration des alertes par e-mail/du serveur de messagerie/des messages	21
Exemples d'alertes par e-mail	23
Comptes d'utilisateur	24
Ajout d'un utilisateur	24
Modification d'un mot de passe utilisateur	24
Gestion	25
Paramètres de la session de connexion/Tâche de service HTTP/HTTPS	25
Statut du fichier de certificats SSL	26
Paramètres SNMP/SNMPv2c	27
Vues SNMPv3	29
Groupes SNMPv3	30
Utilisateurs SNMPv3	31
Cibles SNMPv3	32
Sécurité	33
Serveur RADIUS	33
Demandeur 802.1x	34
Détection de point d'accès non autorisé	35
Affichage de la liste des points d'accès non autorisés	35
Enregistrement de la liste des points d'accès autorisés	37
Importation d'une liste des points d'accès autorisés	37
Configurer la complexité des mots de passe	38
Configurer la complexité WAP-PSK	38

CHAPITRE 3
Technologie sans fil 41

Radio	41
Réseaux	46
Configuration des VAP	47
Configuration des paramètres de sécurité	49
Filtre de client	54

	Configuration d'une liste de filtres de client stockée localement sur l'appareil WAP	55
	Configuration de l'authentification MAC sur le serveur Radius	55
	Planificateur	56
	Configuration du profil du planificateur	56
	Configuration de la règle de profil	56
	QoS	57
<hr/>		
CHAPITRE 4	Pont sans fil	61
	Pont sans fil	61
	Configuration du pont WDS	62
	WEP sur les liaisons WDS	63
	WPA/PSK sur les liaisons WDS	63
	Pont de groupe de travail	63
<hr/>		
CHAPITRE 5	Itinérance rapide	67
	Itinérance rapide	67
	Configuration de l'itinérance rapide	67
	Configuration des profils de la liste de supports de clé distants	68
<hr/>		
CHAPITRE 6	Contrôle d'accès	71
	ACL	71
	ACL IPv4 et IPv6	71
	Procédure de configuration des ACL	72
	Configurer les ACL IPv4	72
	Configurer les ACL IPv6	75
	Configurer les ACL MAC	77
	QoS des clients	79
	Configuration des classes de trafic IPv4	79
	Configuration des classes de trafic IPv6	82
	Configuration des classes de trafic MAC	84
	Stratégie de QoS	85
	Association de la QoS	86
	Accès invité	87
	Table des instances d'accès invité	87

Table des groupes Invité	90
Compte utilisateur Invité	90
Personnalisation du portail web	91

CHAPITRE 7 **Umbrella** **95**

Cisco Umbrella	95
----------------	----

CHAPITRE 8 **Moniteur** **97**

Tableau de bord	97
Statut du réseau local	98
Statut du réseau sans fil	99
Statistiques de trafic	100
Clients	101
Invités	102

CHAPITRE 9 **Administration** **105**

Microprogramme	105
Permutation de l'image du microprogramme	105
Mise à niveau HTTP/HTTPS	106
Mise à niveau TFTP	106
Fichiers de configuration	107
Sauvegarde des fichiers de configuration	107
Téléchargement des fichiers de configuration	108
Copie des fichiers de configuration	109
Suppression des fichiers de configuration	109
Redémarrage	109
Programmer le redémarrage	110

CHAPITRE 10 **Résolution des problèmes** **111**

Capture de paquets	111
Capture de paquets locale	112
Capture de paquets distante	113
Envoyer vers un hôte distant	113
Envoyer vers CloudShark	113

Wireshark 114

Téléchargement du fichier de capture de paquets 116

Utilisation de HTTP 117

Informations relatives au support 117

Télécharger les données du processeur/de la mémoire RAM 117

ANNEXE A :

Codes des motifs des messages de désauthentification 119

Codes des motifs des messages de désauthentification 119

Tableau des codes des motifs de désauthentification 119

ANNEXE B :

Pour en savoir plus 121

Pour en savoir plus 121



CHAPITRE 1

Mise en route

Ce chapitre contient les sections suivantes :

- [Configuration](#), à la page 1
- [Utilisation de l'assistant d'installation de point d'accès](#), à la page 3
- [Modification du mot de passe](#), à la page 5
- [Service TCP/UDP](#), à la page 6
- [État du système](#), à la page 7
- [Configuration du démarrage rapide](#), à la page 7
- [Navigation dans les fenêtres](#), à la page 8

Configuration

Cette section décrit la configuration système requise, ainsi que la manière d'accéder à l'utilitaire de configuration Web.

Navigateurs pris en charge

Avant de commencer à utiliser l'utilitaire de configuration, vérifiez que vous disposez d'un ordinateur doté d'Internet Explorer 9 ou d'une version ultérieure, de Firefox 46 ou d'une version ultérieure, de Chrome 49 ou d'une version ultérieure, ou de Safari 5.0 ou d'une version ultérieure.

Restrictions s'appliquant aux navigateurs

- Si vous utilisez Internet Explorer 9, configurez les paramètres de sécurité suivants :
 - Sélectionnez **Outils, Options Internet**, puis sélectionnez l'onglet **Sécurité**.
 - Sélectionnez **Intranet local**, puis **Sites**.
 - Sélectionnez **Avancé**, puis **Ajouter**. Ajoutez l'adresse Intranet de l'appareil WAP `http://<adresse-ip>` dans la zone Intranet local. L'adresse IP peut également être spécifiée en tant qu'adresse IP du sous-réseau, afin que toutes les adresses du sous-réseau soient ajoutées à la zone Intranet local.
- Si vous disposez de plusieurs interfaces IPv6 sur votre station de gestion, utilisez l'adresse globale IPv6 au lieu de l'adresse locale IPv6 pour accéder à l'appareil WAP à partir de votre navigateur.

Lancement de l'utilitaire de configuration Web

Procédez comme suit pour accéder à l'utilitaire de configuration à partir de votre ordinateur et configurer l'appareil WAP :

1. Connectez l'appareil WAP au réseau (sous-réseau IP) auquel votre ordinateur est relié. Le paramètre par défaut pour la configuration de l'adresse IP de l'appareil WAP est DHCP. Assurez-vous que votre serveur DHCP fonctionne et est accessible.
2. Localisez l'adresse IP de l'appareil WAP.
 1. Pour accéder à l'appareil WAP et le gérer, vous pouvez utiliser l'utilitaire de détection de réseaux FindIT Cisco. Cet utilitaire vous permet de détecter automatiquement tous les appareils Cisco pris en charge dans le même segment de réseau local que votre ordinateur. Vous pouvez obtenir une vue instantanée de chaque appareil ou lancer l'utilitaire de configuration du produit pour afficher et configurer les paramètres. Pour obtenir plus d'informations, reportez-vous à la section <http://www.cisco.com/go/findit>.
 2. L'appareil WAP est équipé de la fonction Bonjour. Il émet automatiquement ses services et écoute les services publiés par d'autres appareils dotés de la fonction Bonjour. Si vous disposez d'un navigateur compatible avec la fonction Bonjour, tel que Microsoft Internet Explorer avec un composant logiciel enfichable Bonjour ou le navigateur Apple Mac Safari, vous pouvez rechercher l'appareil WAP sur votre réseau local sans connaître son adresse IP.

Vous pouvez télécharger la version complète de Bonjour pour Internet Explorer à partir du site Web d'Apple : <http://www.apple.com/bonjour/>.
3. Lancez un navigateur Web tel que Microsoft Internet Explorer.
4. Saisissez l'adresse DHCP par défaut dans la barre d'adresse, puis appuyez sur **Entrée**.
5. Saisissez le nom d'utilisateur et le mot de passe par défaut : `cisco` dans les champs **Nom d'utilisateur** et **Mot de passe**.
6. Cliquez sur **Se connecter**. L'**Assistant Installation du point d'accès sans fil** apparaît.

Suivez les instructions de l'assistant d'installation pour terminer l'installation. Nous vous recommandons d'utiliser l'Assistant d'installation pour la première installation. Pour plus d'informations, reportez-vous à la section [Utilisation de l'assistant d'installation de point d'accès, à la page 3](#).

Pour lancer l'utilitaire de configuration Web sur un appareil portable tel qu'un smartphone ou une tablette, suivez les étapes décrites précédemment dans cette section. Une fois que vous êtes connecté à votre appareil portable, l'Assistant d'installation de point d'accès pour les appareils mobiles s'affiche. Pour plus d'informations, consultez la section [Utiliser l'assistant d'installation de point d'accès sur un appareil mobile, à la page 4](#).

Déconnexion

Par défaut, l'utilitaire de configuration se déconnecte au bout de 10 minutes d'inactivité. Consultez la section [Gestion, à la page 25](#) pour obtenir des instructions sur la modification du délai d'expiration par défaut.

Pour vous déconnecter, cliquez sur **Se déconnecter** dans l'angle supérieur droit de l'utilitaire de configuration.

Utilisation de l'assistant d'installation de point d'accès

La première fois que vous vous connectez au point d'accès (ou après une réinitialisation aux paramètres d'usine par défaut), l'assistant d'installation de point d'accès apparaît afin de vous aider à effectuer les configurations initiales. Procédez comme suit pour exécuter l'assistant :



Remarque Si vous cliquez sur **Annuler** pour ignorer l'assistant, la page **Modifier le mot de passe** s'affiche. Vous pouvez alors modifier le nom d'utilisateur et le mot de passe de connexion par défaut. Pour plus d'informations, consultez la section [Modification du mot de passe](#).

Vous devrez vous reconnecter après avoir modifié votre mot de passe :

- Étape 1** Cliquez sur **Suivant** sur la page d'accueil de l'assistant. La fenêtre **Mise à niveau du firmware** apparaît.
- Étape 2** Cliquez sur **Mettre à niveau** pour mettre à niveau le microprogramme.
Remarque une fois le microprogramme mis à niveau, l'appareil redémarre automatiquement et revient à la page de connexion.
- Étape 3** Cliquez sur **Ignorer**. La fenêtre **Restaurer la configuration** s'affiche.
- Étape 4** Choisissez le fichier de configuration à appliquer à l'appareil, puis cliquez sur **Enregistrer**.
Remarque cliquez sur **Enregistrer**. L'appareil applique la configuration choisie, puis redémarre automatiquement et revient à la page de connexion.
- Étape 5** Cliquez sur **Ignorer**. La fenêtre **Configurer l'appareil - Adresse IP** s'affiche.
- Étape 6** Cliquez sur **Adresse IP dynamique (DHCP)** (recommandé) pour recevoir une adresse IP via un serveur DHCP ou cliquez sur **Adresse IP statique** pour configurer l'adresse IP manuellement. Pour obtenir une description de ces champs, reportez-vous à [Configuration IPv4, à la page 11](#).
- Étape 7** Cliquez sur **Suivant**. La fenêtre Configurer l'appareil - Définir la date et l'heure du système s'affiche.
- Étape 8** Sélectionnez votre fuseau horaire, puis réglez l'heure du système automatiquement à partir d'un serveur NTP ou manuellement. Pour obtenir une description de ces options, reportez-vous à [Heure, à la page 17](#).
- Étape 9** Cliquez sur **Suivant**. La fenêtre Configurer l'appareil - Définir le mot de passe s'affiche.
- Étape 10** Saisissez un **Nouveau mot de passe** et saisissez-le à nouveau dans le champ **Confirmer le mot de passe**.
Remarque Décochez la case **Complexité des mots de passe** pour désactiver les règles de sécurité des mots de passe. Nous vous recommandons toutefois fortement de conserver les règles de sécurité de mot de passe activées. Pour obtenir plus d'informations sur les mots de passe, reportez-vous à [Sécurité, à la page 33](#).
- Étape 11** Cliquez sur **Suivant**. La fenêtre Configurer la radio 1 (2.4 GHz) - Attribuez un nom à votre réseau sans fil apparaît.
- Étape 12** Saisissez un **Nom de réseau**. Ce nom fait office de SSID pour le réseau sans fil par défaut.
- Étape 13** Cliquez sur **Suivant**. La fenêtre Configurer la radio 1 (2.4 GHz) - Sécurisez votre réseau sans fil apparaît.
- Étape 14** Choisissez un type de cryptage de sécurité et saisissez une clé de sécurité. Pour obtenir une description de ces options, reportez-vous à [Configuration des paramètres de sécurité, à la page 49](#).
- Étape 15** Cliquez sur **Suivant**. La fenêtre Configurer la radio 1 (2.4 GHz) - Attribuez l'ID de VLAN à votre réseau sans fil apparaît.

- Étape 16** Sélectionnez l'**ID de VLAN** pour le trafic reçu sur le réseau sans fil.
- Nous vous recommandons d'affecter un ID de VLAN différent de celui par défaut (1) vers le trafic sans fil, afin de le séparer du trafic de gestion sur le VLAN 1.
- Étape 17** Cliquez sur **Suivant**. Répétez les étapes 12 à 16 pour configurer les paramètres de l'interface Radio 2 (5GHz).
- Étape 18** Cliquez sur **Suivant**. La fenêtre Activer le portail captif - Créez votre réseau invité s'affiche.
- Étape 19** Sélectionnez si vous voulez configurer ou non une méthode d'authentification pour les invités sur votre réseau, puis cliquez sur **Suivant**.
- Si vous cliquez sur **Non**, passez à l'étape 27.
- Si vous cliquez sur **Oui**, l'assistant affiche la fenêtre Activer le portail captif - Attribuez un nom à votre réseau invité.
- Étape 20** Spécifiez le **Nom du réseau invité**.
- Étape 21** Cliquez sur **Suivant**. La fenêtre Activer le portail captif - Sécurisez votre réseau invité s'affiche.
- Étape 22** Choisissez un type de cryptage de sécurité pour le réseau invité et entrez une clé de sécurité. Pour obtenir une description de ces options, reportez-vous à la section Configuration des paramètres de sécurité.
- Étape 23** Cliquez sur **Suivant**. La fenêtre Activer le portail captif - Attribuez l'ID de VLAN s'affiche.
- Étape 24** Spécifiez un ID de VLAN pour le réseau invité. L'ID de VLAN du réseau invité doit être différent de l'ID de VLAN de gestion.
- Étape 25** Cliquez sur **Suivant**. La fenêtre Activer le portail captif - Activer l'URL de redirection s'affiche.
- Étape 26** Cochez la case **Activer l'URL de redirection** et spécifiez un nom de domaine complet (FQDN) ou une adresse IP dans le champ **URL de redirection** (y compris http://). S'ils sont spécifiés, les utilisateurs du réseau invité sont redirigés vers l'URL spécifiée après leur authentification.
- Étape 27** Cliquez sur **Suivant**. La fenêtre Récapitulatif - Confirmez vos paramètres s'affiche.
- Étape 28** Vérifiez les paramètres que vous avez configurés. Cliquez sur **Précédent** pour reconfigurer un ou plusieurs paramètres. Si vous cliquez sur **Annuler**, tous les paramètres sont rétablis aux valeurs précédentes ou par défaut.
- Étape 29** S'ils sont corrects, cliquez sur **Submit**. Vos paramètres de configuration sont enregistrés et une fenêtre de confirmation apparaît.
- Étape 30** Cliquez sur **Finish**.
- L'appareil WAP est configuré. Vous êtes invité à vous reconnecter avec le nouveau mot de passe.

Utiliser l'assistant d'installation de point d'accès sur un appareil mobile

La première fois que vous vous connectez au point d'accès avec votre appareil portable (ou après une réinitialisation des paramètres d'usine par défaut), l'assistant d'installation de point d'accès pour les appareils mobiles s'affiche afin de vous aider à effectuer les configurations initiales. Pour configurer le point d'accès à l'aide de l'assistant, procédez comme suit :



Remarque

Le SSID par défaut dans le mode d'usine par défaut est **CiscoSB-Setup**. Associez votre terminal mobile au point d'accès avec ce SSID et la clé prépartagée, **cisco123**. Ouvrez un navigateur et saisissez une adresse IP arbitraire ou un nom de domaine. Une page Web avec des champs pour les identifiants de connexion s'affiche. Saisissez le nom d'utilisateur et le mot de passe par défaut : **cisco**. Cliquez sur **Connexion**. **L'assistant Installation du point d'accès** s'affiche.

-
- Étape 1** Cliquez sur **Suivant** sur la page d'**Accueil** de l'assistant. La fenêtre **Configurer l'adresse IP** s'affiche.
- Étape 2** L'option Dynamique (DHCP) (recommandée) est sélectionnée par défaut pour recevoir une adresse IP via un serveur DHCP. Pour configurer l'adresse IP manuellement, cliquez sur **Statique**. Pour obtenir une description de ces champs, reportez-vous à [Configuration IPv4](#).
- Étape 3** Cliquez sur **Suivant**. La fenêtre **Configurer l'appareil - Définir le mot de passe** s'affiche.
- Étape 4** Saisissez un nouveau mot de passe et saisissez-le à nouveau dans le champ **Confirmer le mot de passe**.
- Étape 5** Cliquez sur **Suivant**. La fenêtre **Configurer votre réseau sans fil** s'affiche.
- Saisissez un nom de réseau faisant office de SSID pour le réseau sans fil par défaut.
 - Saisissez une clé de sécurité (type de sécurité, WPA2-Personal - AES par défaut).
 - Saisissez un ID de VLAN pour le trafic reçu sur le réseau sans fil.
- Remarque** Cochez la case pour appliquer la même configuration à la 2e radio (5 GHz) ou basculez vers un autre onglet de radio et répétez l'étape 5 pour réeffectuer la configuration.
- Étape 6** Cliquez sur **Suivant**. La fenêtre **Configurer le portail captif** s'affiche.
- Étape 7** Cliquez sur **Ignorer**. Passez à l'étape 10.
- Étape 8** Cliquez sur **Oui**. La fenêtre **Configuration du portail captif** s'affiche.
- Étape 9** Sélectionnez **Radio 1 (2.4 GHz)** ou **Radio 2 (5 GHz)**.
- Indiquez le Nom du réseau invité.
 - Saisissez une clé de sécurité (type de sécurité, WPA2-Personal - AES par défaut).
 - Indiquez un ID de VLAN pour le réseau invité.
 - Vous pouvez aussi indiquer une URL de redirection avec un nom de domaine complet (FQDN) afin de rediriger les utilisateurs vers l'URL indiquée après leur authentification.
- Étape 10** Cliquez sur **Suivant**. La fenêtre **Récapitulatif** s'affiche.
- Étape 11** Vérifiez les paramètres de configuration. Cliquez sur **Précédent** pour reconfigurer un ou plusieurs paramètres.
- Étape 12** Vérifiez que vos données sont correctes, puis cliquez sur **Envoyer** pour enregistrer.
- Étape 13** L'appareil WAP est configuré. Vous êtes invité à vous reconnecter avec un nouveau mot de passe.
-

Modification du mot de passe

Pour des raisons de sécurité, vous êtes invité à modifier le mot de passe d'administration à intervalles réguliers. Vous devrez accéder à cette page si l'option Délai d'expiration du mot de passe est activée.

L'option obligeant à créer des mots de passe complexes est activée par défaut. Les exigences minimales en termes de complexité des mots de passe sont affichées sur la page Modifier le mot de passe. Le nouveau mot de passe doit respecter les règles de complexité par défaut. Il peut également être temporairement désactivé en désactivant l'option **Complexité des mots de passe**. Pour plus d'informations, reportez-vous à la section [Sécurité, à la page 33](#).

Pour modifier le mot de passe par défaut, configurez les paramètres suivants :

- **Nom d'utilisateur** : saisissez un nouveau nom d'utilisateur. Le nom par défaut est cisco.
- **Ancien mot de passe** : saisissez le mot de passe actuel (par défaut, cisco).

- **Nouveau mot de passe** : saisissez le nouveau mot de passe.
- **Confirmer le mot de passe** : saisissez une nouvelle fois le nouveau le mot de passe pour le confirmer.
- **Mesure de la fiabilité du mot de passe** : le niveau de sécurité du nouveau mot de passe s'affiche.
- **Complexité des mots de passe** : la complexité des mots de passe est activée par défaut ; le nouveau mot de passe doit respecter les paramètres de complexité suivants :
 - Il doit différer du nom d'utilisateur.
 - Il doit différer du mot de passe actuel.
 - Il doit comporter huit caractères minimum.
 - Il doit comporter trois des quatre classes de caractères suivantes : lettres majuscules, lettres minuscules, chiffres et caractères spéciaux disponibles sur un clavier standard.



Remarque

Cochez la case **Désactiver** pour désactiver les règles de complexité des mots de passe. Il est toutefois fortement recommandé de conserver les règles de complexité des mots de passe activées.

Service TCP/UDP

Le tableau des services TCP/UDP affiche des informations sur les protocoles et les services fonctionnant sur l'appareil WAP.

- **Service** : nom du service.
- **Protocole** : protocole de transport sous-jacent utilisé par le service (TCP ou UDP).
- **Adresse IP locale** : adresse IP locale de l'appareil connecté. La valeur Toute indique que toute adresse IP sur l'appareil peut utiliser ce service.
- **Port local** : numéro de port local.
- **Adresse IP distante** : adresse IP d'un hôte distant qui utilise ce service. La valeur Tous indique que le service est disponible pour l'ensemble des hôtes distants qui accèdent au système.
- **Port distant** : numéro de port de tout appareil distant qui communique avec ce service.
- **État de la connexion** : état du service. Pour les services UDP, seules les connexions dont l'état est Active ou Established apparaissent dans la table. Les états TCP suivants sont disponibles :
 - **À l'écoute** : le service est à l'écoute des demandes de connexion.
 - **Active** : une session de connexion est établie et les paquets sont transmis et reçus.
 - **Établie** : une session de connexion est établie entre l'appareil WAP et un serveur ou un client.
 - **Temps d'attente** : la séquence de fermeture a été initiée et l'appareil WAP attend l'expiration d'un délai défini par le système (généralement 60 secondes) avant de fermer la connexion.



Remarque

Vous pouvez modifier l'ordre sur le tableau des services TCP/UDP. Cliquez sur **Actualiser** pour actualiser l'écran et afficher les informations les plus récentes.

Vous pouvez aussi définir les paramètres liés au service, au protocole et à d'autres détails de façon à filtrer les services TCP/UDP affichés.

Cliquez sur **Retour** pour revenir à la page **Mise en route**.

État du système

La page État du système contient une description du modèle de l'appareil et indique la version du logiciel et divers paramètres de configuration, à savoir :

- **PID VID** : modèle et version de l'appareil WAP.
- **Numéro de série** : numéro de série de l'appareil WAP.
- **Nom d'hôte** : nom d'hôte affecté à l'appareil WAP.
- **Adresse MAC** : adresse MAC de l'appareil WAP.
- **Adresse IPv4** : adresse IP de l'appareil WAP.
- **Adresse IPv6** : adresse IPv6 de l'appareil WAP.
- **Port LAN** : état de l'interface Ethernet.
- **Radio 1 (2,4 GHz)** : le mode 2,4 GHz est activé ou désactivé pour l'interface Radio 1.
- **Radio 2 (5 GHz)** : le mode 5 GHz est activé ou désactivé pour l'interface Radio 2.
- **Source d'alimentation** : le système peut être alimenté par un adaptateur secteur ou fonctionner en tant que port PSE (Power Sourcing Equipment, équipement source d'alimentation) PoE (Power-over-Ethernet).
- **Temps utilisation système** : temps qui s'est écoulé depuis le dernier redémarrage.
- **Heure système** : heure système actuelle.
- **Version du micrologiciel (image active)** : numéro de version du micrologiciel de l'image active.
- **Somme de contrôle MD5 du micrologiciel (image active)** : somme de contrôle de l'image active.
- **Version du micrologiciel (non active)** : numéro de version du micrologiciel de l'image de sauvegarde.
- **Somme de contrôle MD5 du micrologiciel (non active)** : somme de contrôle de l'image de sauvegarde.

Configuration du démarrage rapide

Afin de simplifier la configuration de l'appareil grâce à une navigation rapide, la page **Mise en route** contient des liens permettant d'effectuer des tâches courantes. La page **Mise en route** s'affiche par défaut au démarrage.

Catégorie	Nom du lien (sur la page)	Page correspondante
-----------	---------------------------	---------------------

Accès rapide	Assistant d'installation	Utilisation de l'assistant d'installation de point d'accès, à la page 3
	Modifier le mot de passe du compte	Ajout d'un utilisateur, à la page 24
	Sauvegarder/Restaurer la configuration	Fichiers de configuration, à la page 107
	Mettre à niveau le microprogramme de l'appareil	Microprogramme, à la page 105
Configuration avancée	Paramètres sans fil	Radio, à la page 41
	Paramètre de gestion	Gestion, à la page 25
	Paramètre LAN	Configuration IPv4, à la page 11
	Accès invité	Accès invité, à la page 87
En savoir plus	Tableau de bord	Tableau de bord, à la page 97
	Service TCP/UDP	Service TCP/UDP, à la page 6
	Afficher le journal système	Affichage DEL, à la page 19
	Statistiques de trafic	Statistiques de trafic, à la page 100

Pour plus d'informations sur l'appareil, vous pouvez accéder à la page dédiée à la prise en charge des produits ou à la communauté d'assistance Cisco :

- Cliquez sur **Assistance** pour accéder à la page dédiée à la prise en charge des produits.
- Cliquez sur **Forums** pour accéder à la page de la communauté d'assistance Cisco.
- Cliquez sur **Plus d'informations sur FindIT** pour avoir plus d'informations sur l'utilitaire FindIT.
- Cliquez sur **Télécharger FindIT** pour télécharger l'utilitaire FindIT.




Navigation dans les fenêtres

Utilisez les boutons de navigation pour parcourir l'interface utilisateur graphique de l'appareil WAP.

En-tête de l'utilitaire de configuration

L'en-tête de l'utilitaire de configuration contient des informations standard et apparaît en haut de chaque page. Il dispose des boutons suivants :

Nom du bouton	Description
(Utilisateur)	Nom du compte (Administrateur ou Invité) de l'utilisateur connecté à l'appareil WAP. Le nom d'utilisateur par défaut est cisco .
(Langue)	Placez le pointeur de la souris sur le bouton, puis sélectionnez une langue. La langue par défaut est l'anglais.

	Cliquez sur ce bouton pour vous déconnecter de l'utilitaire de configuration.
	Cliquez sur ce bouton pour afficher le type d'appareil WAP, ainsi que son numéro de version.
	Cliquez sur ce bouton pour afficher l'aide contextuelle en ligne. L'aide en ligne est conçue pour être affichée à l'aide de navigateurs utilisant le codage UTF-8. Si l'aide en ligne affiche des caractères errants, vérifiez que les paramètres de codage de votre navigateur sont définis à UTF-8.

Volet Navigation

Un volet de navigation, ou menu principal, est présent sur le côté gauche de chaque page. Le volet de navigation contient la liste des fonctionnalités de niveau supérieur de l'appareil WAP. Si un élément du menu principal est précédé d'une flèche, choisissez de développer et d'afficher le sous-menu de chaque groupe. Vous pouvez ensuite sélectionner l'élément de sous-menu souhaité pour ouvrir la page associée.

Boutons de gestion

Le tableau suivant décrit les boutons couramment utilisés qui s'affichent sur diverses pages du système :

Nom du bouton	Description
Ajouter	Ajoute une nouvelle entrée à une table ou une base de données.
Annuler	Annule la modification apportée à la page.
Effacer tout	Efface toutes les entrées dans une table de journaux.
Supprimer	Supprime une entrée dans une table.
Modifier	Modifie une entrée.
Actualiser	Actualise la page en cours avec les dernières données.
Enregistrer	Enregistre les paramètres ou la configuration.
Mettre à jour	Met à jour la configuration initiale avec les nouvelles informations.



CHAPITRE 2

Configuration du système

Ce chapitre explique comment configurer les paramètres système globaux et effectuer des diagnostics. Il contient les rubriques suivantes :

- Réseau local, à la page 11
- Heure, à la page 17
- Notification, à la page 19
- Comptes d'utilisateur, à la page 24
- Gestion, à la page 25
- Sécurité, à la page 33

Réseau local

Cette section explique comment configurer les paramètres Port, Réseau VLAN, LLDP, IPv4 et IPv6 sur l'appareil WAP.

Configuration IPv4

Utilisez la page Paramètres IPv4 pour configurer l'adresse IPv4.

Étape 1 Sélectionnez **LAN > Configuration IPv4**.

Étape 2 Définissez les paramètres IPv4 suivants :

- **Type de connexion** : par défaut, le client DHCP sur l'appareil WAP diffuse automatiquement les demandes d'informations de réseau. Si vous voulez utiliser une adresse IP statique, vous devez désactiver le client DHCP et configurer manuellement l'adresse IP ainsi que les autres informations de réseau.

Sélectionnez l'une des options suivantes :

- **DHCP** : l'appareil WAP acquiert son adresse IP d'un serveur DHCP sur le réseau local.
 - **IP statique** : configurez manuellement l'adresse IPv4. La forme de l'adresse IPv4 doit être similaire à celle-ci : xxx.xxx.xxx.xxx (172.17.144.170).
- **Adresse IP statique, Masque de sous-réseau et Passerelle par défaut** : saisissez l'adresse IP statique, le masque de sous-réseau et la passerelle par défaut.

- **Serveurs de noms de domaine** : sélectionnez l'une des options suivantes :
 - **Dynamique** : l'appareil WAP acquiert les adresses de serveur DNS d'un serveur DHCP sur le réseau local.
 - **Manuel** : saisissez jusqu'à deux adresses IP dans les champs prévus à cet effet.

Étape 3 Cliquez sur **Enregistrer** pour enregistrer les modifications.

Paramètres de configuration automatique DHCP

- **Options de configuration automatique DHCP** : cette option est activée par défaut. Lorsque le point d'accès est livré avec les paramètres d'usine, il se configure automatiquement à l'aide des options DHCP.

Lors de la configuration automatique :

- Le point d'accès démarre. Seule l'interface Ethernet est activée ; les interfaces WLAN sont inactives.
- Aucun service n'est disponible à l'utilisateur (hormis les interfaces utilisateur).
- Les « Options de configuration automatique DHCP » sont automatiquement désactivées après l'« Intervalle d'attente » ou le chargement TFTP du fichier de configuration, l'échéance la plus proche étant retenue.
- La désactivation du client DHCP (notamment la configuration via une adresse IP statique) ou la désactivation des « Options de configuration automatique DHCP » annule immédiatement la configuration automatique.

Le client DHCP diffuse automatiquement les demandes d'options DHCP 66 et 67. Si les options « DHCP » et « Options de configuration automatique DHCP » sont activées, le point d'accès est configuré automatiquement lors du prochain démarrage en tenant compte des informations concernant les demandes DHCP reçues du serveur DHCP.



Remarque

L'opération de chargement de la configuration de la part de l'utilisateur/Cisco remplace la configuration automatique de façon à ce que le fichier de configuration choisi soit privilégié. Dans tous les autres cas de redémarrage du point d'accès (mise à jour du micrologiciel/opérations de redémarrage, etc.), le paramètre de configuration automatique actuel est activé.

- **Adresse IPv4/Nom d'hôte du serveur TFTP de secours** : si vous configurez l'adresse du serveur TFTP, elle est utilisée s'il est impossible de récupérer le fichier auprès des autres serveurs TFTP spécifiés par le serveur DHCP lors de la configuration automatique. Saisissez l'adresse IPv4 ou le nom d'hôte. Si le format sélectionné est le nom d'hôte, le serveur DNS doit être disponible pour traduire le nom d'hôte en adresse IP.

Cette valeur est utilisée lors de la procédure de configuration automatique au prochain démarrage.

- **Nom du fichier de configuration** : si vous spécifiez le nom du fichier de configuration, il est récupéré auprès du serveur TFTP lors de la configuration automatique du point d'accès si le serveur DHCP n'envoie pas le nom du fichier d'amorçage. L'absence de cette valeur indique le fichier config.xml à utiliser. Ce fichier doit posséder une extension .xml, le cas échéant.

Cette valeur est utilisée lors de la procédure de configuration automatique au prochain démarrage.

- **Intervalle d'attente** : si ce paramètre est configuré, le point d'accès adopte la configuration locale et met les services activés à disposition de l'utilisateur à l'issue de l'intervalle d'attente défini. Le point d'accès abandonne la configuration automatique si la transaction TFTP n'est pas lancée dans l'intervalle spécifié.

Cette valeur est utilisée lors de la procédure de configuration automatique au prochain démarrage.

- **Journal d'état** : ce champ indique la raison de l'exécution ou de l'abandon de la configuration automatique.

Configuration IPv6

Utilisez la page Paramètres IPv6 pour configurer l'adresse IPv6 en procédant comme suit :

Étape 1 Sélectionnez LAN > **Configuration IPv6**.

Étape 2 Configurez les paramètres suivants :

- **Type de connexion IPv6** : sélectionnez l'une des options suivantes :
 - **DHCPv6** : l'adresse IPv6 est affectée par un serveur DHCPv6.
 - **IPv6 statique** : configurez manuellement l'adresse IPv6. Le format de l'adresse IPv6 doit être similaire à celui-ci : xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx (2001:DB8:CAD5:7D91).
- **Mode d'administration des adresses IPv6** : cochez la case **Activer** pour activer le mode d'administration des adresses IPv6.
- **Mode d'administration de la configuration automatique des adresses IPv6** : cochez la case **Activer** pour activer la configuration automatique des adresses IPv6.

Lorsque la configuration automatique des adresses IPv6 est activée, l'appareil WAP détecte ses adresses IPv6 et sa passerelle en traitant les annonces de routeur reçues sur le port LAN. L'appareil WAP peut posséder plusieurs adresses IPv6 configurées automatiquement.
- **Adresse IPv6 statique** : saisissez l'adresse IPv6 statique. l'appareil WAP peut posséder une adresse IPv6 statique, même si des adresses ont déjà été configurées automatiquement.
- **Longueur du préfixe de l'adresse IPv6 statique** : indiquez la longueur de préfixe de l'adresse statique, à savoir un entier compris entre 0 et 128. La valeur par défaut est 0.
- **Statut de l'adresse IPv6 statique** : sélectionnez l'une des options suivantes :
 - **Opérationnel** : l'adresse IP a été vérifiée comme étant unique et elle est utilisable sur l'interface du réseau local.
 - **Provisoire** : l'appareil WAP initie automatiquement un processus de détection des adresses en double (DAD, Duplicate Address Detection) lors de l'affectation d'une adresse IP statique. Cette adresse IPv6 est provisoire, car elle est en cours de vérification sur le réseau et ne peut pas être utilisée pour transmettre ou recevoir le trafic.
 - **Vide (pas de valeur)** : aucune adresse IP n'est affectée.
- **Adresses globales IPv6 autoconfigurées** : répertorie les adresses IPv6 automatiquement attribuées à l'appareil.

- **Adresse IPv6 de liaison locale** : adresse IPv6 utilisée par la liaison physique locale. L'adresse locale de liaison n'est pas configurable et elle est affectée à l'aide du processus de détection de voisinage IPv6.
- **Passerelle IPv6 par défaut** : passerelle IPv6 par défaut configurée de manière statique.
- **Serveurs de noms de domaine IPv6** : sélectionnez l'une des options suivantes :
 - **Dynamique** : les serveurs DNS sont détectés de manière dynamique via DHCPv6.
 - **Manuel** : vous pouvez spécifier manuellement jusqu'à deux serveurs DNS IPv6.

Table des paramètres de port

Utilisez la table des paramètres de port pour afficher et configurer les paramètres du port qui connecte l'appareil WAP à un réseau local.

Étape 1 Sélectionnez Réseau local > Table des paramètres de port.

La table des paramètres de port répertorie les configurations et les statuts suivants pour l'interface LAN :

- **Statut de la liaison** : affiche le statut actuel de la liaison du port.
- **Débit du port** : en mode de vérification, ce champ indique le débit actuel du port. En mode de modification et lorsque l'option Négociation automatique est désactivée, sélectionnez un débit de port, par exemple 100 Mbit/s ou 10 Mbit/s. 1 000 Mbit/s est le seul débit pris en charge lorsque la négociation automatique est activée.
- **Mode duplex** : en mode de vérification, ce champ indique le mode duplex du port actuel. En mode de modification et lorsque l'option Négociation automatique est désactivée, sélectionnez le mode duplex **Semi** ou **Intégral**.
- **Négociation automatique** : lorsque cette option est activée, le port négocie avec son partenaire de liaison afin de définir le débit de liaison le plus rapide et le mode duplex disponible. Si cette option est désactivée, vous pouvez configurer manuellement le débit du port et le mode duplex.
- **Green Ethernet** : le mode Green Ethernet prend en charge le mode de mise hors tension automatique et le mode EEE (Energy Efficient Ethernet, IEEE 802.3az). Le mode Green Ethernet fonctionne uniquement lorsque la négociation automatique est activée sur le port. Le mode de mise hors tension automatique réduit la consommation du processeur en l'absence de signal provenant d'un partenaire de liaison. L'appareil WAP passe automatiquement en mode basse consommation en cas de perte d'énergie sur la ligne et reprend un fonctionnement normal lorsqu'il détecte de l'énergie. Le mode EEE prend en charge les périodes de pause lors d'une faible utilisation de la liaison, ce qui permet aux deux extrémités de la liaison de désactiver les portions du circuit de fonctionnement de chaque PHY et d'économiser de l'énergie.

Étape 2 Cliquez sur Enregistrer.

Protocole STP (Spanning Tree Protocol)

En mode Spanning Tree Protocol, cochez la case **Activer** pour activer le mode STP sur l'appareil WAP Cisco. Une fois l'activation effectuée, STP empêche les boucles de basculement. STP est recommandé si vous configurez des liaisons WDS.

Paramétrage des VLAN

Utilisez la page Configuration du VLAN pour afficher et configurer les paramètres du VLAN.

Étape 1 Sélectionnez **Réseau local > Plus > Table des paramètres du VLAN**.

Étape 2 Définissez les paramètres suivants :

- **ID de VLAN non balisé** : spécifiez un nombre compris entre 1 et 4 094 pour l'ID de VLAN non balisé. La valeur par défaut est 1. Le trafic sur le VLAN que vous spécifiez dans ce champ n'est pas balisé avec un ID de VLAN lorsqu'il est transféré au réseau.
- **Description** : description du VLAN associé.
- **VLAN de gestion** : le VLAN de gestion est utilisé pour accéder à l'appareil WAP via Telnet ou l'interface utilisateur graphique (GUI) web. Seul un VLAN de gestion est autorisé. Si aucune interface (filaire ou sans fil) n'est affectée au VLAN de gestion, l'utilisateur ne dispose d'aucune interface pour accéder à l'utilitaire de configuration.
- **VLAN** : sélectionnez le VLAN (**Non balisé ou Balisé**) dans la liste déroulante.

Par défaut, la totalité du trafic sur l'appareil WAP utilise le VLAN 1, à savoir le VLAN non balisé par défaut. Cela signifie que l'ensemble du trafic est non balisé jusqu'à la désactivation du VLAN non balisé, la modification de l'ID de VLAN du trafic non balisé ou la modification de l'ID de VLAN d'un point d'accès virtuel (VAP) ou d'un client utilisant un serveur RADIUS.

Étape 3 Cliquez sur **Enregistrer**. Les modifications sont enregistrées dans la configuration de démarrage.

Détection des appareils voisins

Bonjour permet à l'appareil WAP et à ses services d'être détectés via le protocole mDNS (Multicast DNS). Bonjour annonce ses services au réseau et répond aux questions concernant les types de service pris en charge, ce qui simplifie la configuration du réseau dans vos environnements.

L'appareil WAP annonce les types de service suivants :

- **Description d'appareils spécifiques à Cisco (cisco-sb)** : ce service permet aux clients de détecter les appareils WAP Cisco et d'autres produits déployés sur vos réseaux.
- **Interfaces utilisateur de gestion** : ce service identifie les interfaces de gestion disponibles sur l'appareil WAP (HTTP et SNMP).

Lorsqu'un appareil WAP compatible avec Bonjour est connecté à un réseau, tout client Bonjour peut détecter l'utilitaire de configuration et y accéder sans configuration préalable.

Un administrateur système peut utiliser un module d'extension Internet Explorer installé pour détecter l'appareil WAP. L'utilitaire de configuration web apparaît sous forme d'onglet dans le navigateur.

**Remarque**

L'administrateur système peut afficher l'appareil WAP compatible avec Bonjour à l'aide du dernier module d'extension Internet Explorer (outil Cisco FindIT). Tous les appareils WAP présents dans un cluster apparaissent sous le nom du cluster après le processus de détection Bonjour. L'administrateur doit s'assurer que le nom du cluster est unique sur un réseau.

Bonjour fonctionne sur les réseaux IPv4 et IPv6.

Pour activer la détection de l'appareil WAP via Bonjour, procédez comme suit :

Étape 1

Sélectionnez **Réseau local > Détection des appareils voisins**.

Étape 2

Cochez la case **Activer** pour activer Bonjour.

Étape 3

Cliquez sur **Enregistrer**. Les modifications sont enregistrées dans la configuration de démarrage.

LLDP

Le protocole LLDP (Link Layer Discovery Protocol) est défini par le standard IEEE 802.1AB et permet au VAP d'annoncer le nom système, les fonctions système et les exigences en termes d'alimentation. Ces informations peuvent vous aider à identifier la topologie du système et à détecter des erreurs de configurations sur le LAN. Le point d'accès prend également en charge le protocole LLDP-MED (Link Layer Discovery Protocol for Media Endpoint Devices), qui standardise des éléments d'informations supplémentaires que les appareils peuvent se transmettre en vue d'améliorer la gestion du réseau.

Étape 1

Pour configurer les paramètres LLDP, sélectionnez **LAN > LLDP**.

Étape 2

Configurez les paramètres suivants :

- **Mode LLDP** : cochez la case **Activer** pour activer ce mode. Une fois ce mode activé, le point d'accès transmet les unités de données du protocole LLDP aux appareils voisins.
- **Intervalle de transmission** : nombre de secondes entre les transmissions des messages LLDP. La plage valide va de 5 à 32768 secondes. La valeur par défaut est 30 secondes.
- **Priorité PoE** : sélectionnez le niveau de priorité dans le menu déroulant (**Critique, Élevé, Faible ou Inconnu**). Le paramètre Priorité PoE permet à un appareil PSE (Power Sourcing Equipment) de déterminer à quels appareils alimentés il doit donner la priorité en matière d'affectation de l'alimentation lorsque le PSE n'est pas capable d'alimenter l'ensemble des appareils connectés.

Étape 3

Cliquez sur **Enregistrer**.

Tunnel IPv6

les appareils WAP prennent en charge le protocole ISATAP (Intra-Site Automatic Tunnel Addressing Protocol). Le protocole ISATAP permet à l'appareil WAP de transmettre des paquets IPv6 encapsulés dans des paquets

IPv4 sur le réseau local. Grâce à ce protocole, l'appareil WAP peut communiquer avec des hôtes compatibles IPv6 distants, même si le réseau local qui les connecte ne prend pas en charge IPv6.

l'appareil WAP agit en tant que client ISATAP. Un hôte ou un routeur prenant en charge le protocole ISATAP doit résider sur le réseau local. L'adresse IP ou le nom d'hôte du routeur est configuré sur l'appareil WAP (par défaut, il s'agit d'ISATAP). S'il est configuré en tant que nom d'hôte, l'appareil WAP communique avec un serveur DNS pour résoudre le nom en une ou plusieurs adresses de routeur ISATAP. l'appareil WAP envoie ensuite des messages de sollicitation aux routeurs. Lorsqu'un routeur prenant en charge le protocole ISATAP répond par le biais d'un message d'annonce, l'appareil WAP et le routeur établissent le tunnel. Une adresse lien-local et une adresse IPv6 globale sont affectées à l'interface de tunnel et font office d'interfaces IPv6 virtuelles sur le réseau IPv4.

Lorsque des hôtes IPv6 initient une communication avec l'appareil WAP connecté par l'intermédiaire du routeur ISATAP, les paquets IPv6 sont encapsulés dans des paquets IPv4 par le routeur ISATAP.

- **Statut ISATAP** : cochez la case **Activer** pour activer ISATAP sur l'appareil.
- **Hôte compatible ISATAP** : saisissez l'adresse IP ou le nom DNS du routeur ISATAP. La valeur par défaut est isatap.
- **Intervalle des requêtes ISATAP** : indiquez la fréquence à laquelle l'appareil WAP doit envoyer des requêtes au serveur DNS pour tenter de résoudre le nom d'hôte ISATAP en une adresse IP. La plage valide va de 120 à 3600 secondes. La valeur par défaut est 120 secondes.
- **Intervalle de sollicitation ISATAP** : indiquez la fréquence à laquelle l'appareil WAP doit envoyer les messages de sollicitation de routeur aux routeurs ISATAP. l'appareil WAP n'envoie des messages de sollicitation de routeur que lorsqu'il n'y a pas de routeur ISATAP actif. La plage valide va de 120 à 3600 secondes. La valeur par défaut est 120 secondes.
- **ISATAP IPv6 Link Local Address** : adresse IPv6 utilisée par la liaison physique locale. L'adresse locale de liaison n'est pas configurable et elle est affectée à l'aide du processus de détection de voisinage IPv6.
- **ISATAP IPv6 Autoconfigured Global Addresses** : si une ou plusieurs adresses IPv6 ont été affectées automatiquement au périphérique WAP, ces adresses sont répertoriées ici.



Remarque

Lorsque le tunnel a été établi, les valeurs Adresse IPv6 de liaison locale ISATAP et Adresse IPv6 globale ISATAP s'affichent sur la page. Il s'agit des adresses des interfaces IPv6 virtuelles.

Cliquez sur **Enregistrer**.

Heure

Une horloge système fournit un service d'horodatage synchronisé sur le réseau pour les journaux de messages. Vous pouvez configurer l'horloge système manuellement ou configurer l'appareil WAP en tant que client NTP (Network Time Protocol) qui obtient les données d'horloge d'un serveur.

Utilisez la page Paramètres d'heure pour définir l'heure système manuellement ou à partir d'un serveur NTP préconfiguré. Par défaut, l'appareil WAP est configuré de manière à obtenir l'heure à partir d'une liste prédéfinie de serveurs NTP.

L'heure système actuelle apparaît en haut de la page avec l'option **Source d'horloge système**.

Acquisition automatique des paramètres d'heure via NTP

Pour acquérir automatiquement les paramètres d'heure auprès d'un serveur NTP, procédez comme suit :

-
- Étape 1** Sélectionnez **Configuration système > Heure**.
- Étape 2** Dans la zone Source d'horloge système, cliquez sur **NTP (Network Time Protocol)**.
- Étape 3** Configurez les paramètres suivants :
- **du serveur NTP (1 à 4)** : spécifiez l'adresse IPv4, l'adresse IPv6 ou le nom d'hôte d'un serveur NTP. Un serveur NTP par défaut est répertorié.
Un nom d'hôte peut être constitué d'un ou de plusieurs libellés, qui sont des ensembles pouvant contenir jusqu'à 63 caractères alphanumériques. Si un nom d'hôte inclut plusieurs libellés, ceux-ci sont séparés par un point (.). La série complète de libellés et de points peut contenir jusqu'à 253 caractères.
 - **Fuseau horaire** : sélectionnez votre fuseau horaire.
 - **Prendre en compte l'heure d'été** : sélectionnez cette option pour l'activer et configurer les champs suivants :
 - **Début** : sélectionnez le jour, la semaine, le mois et l'heure du passage à l'heure d'été.
 - **Fin** : sélectionnez le jour, la semaine, le mois et l'heure du passage à l'heure d'hiver.
 - **Décalage dû à l'heure d'été** : indiquez de combien de minutes vous devez avancer l'horloge lors du passage à l'heure d'été et de combien vous devez la reculer lors du passage à l'heure d'hiver.
- Étape 4** Cliquez sur **Enregistrer**. Les modifications sont enregistrées dans la configuration de démarrage.
-

Configuration manuelle des paramètres d'heure

Pour configurer manuellement les paramètres d'heure, procédez comme suit :

-
- Étape 1** Sélectionnez **Configuration système > Heure**.
- Étape 2** Dans la zone Source d'horloge système, sélectionnez **Manuellement**.
- Étape 3** Cliquez sur **Synchroniser l'heure avec l'ordinateur** pour appliquer la même heure sur le système que celle de votre ordinateur local.
- Étape 4** Vous pouvez également configurer les champs suivants :
- **Date système** : sélectionnez le jour, le mois et l'année dans les listes déroulantes.
 - **Heure système** : sélectionnez l'heure et les minutes au format 24 heures.
 - **Fuseau horaire** : sélectionnez votre fuseau horaire.
 - **Prendre en compte l'heure d'été** : si votre fuseau horaire prend en compte l'heure d'été, activez cette option et configurez les champs suivants :
 - **Début** : sélectionnez l'heure, le jour, la semaine et le mois du passage à l'heure d'été.
 - **Fin** : sélectionnez l'heure, le jour, la semaine et le mois du passage à l'heure d'hiver.

- **Décalage dû à l'heure d'été** : indiquez de combien de minutes vous devez avancer l'horloge lors du passage à l'heure d'été et de combien vous devez la reculer lors du passage à l'heure d'hiver.

Étape 5 Cliquez sur **Enregistrer**. Les modifications sont enregistrées dans la configuration de démarrage.

Remarque Cliquez sur **Synchroniser l'heure avec l'ordinateur** pour que l'heure de l'appareil soit identique à l'heure de l'ordinateur.

Notification

Cette section décrit la procédure d'activation et de configuration des notifications du point d'accès.

Affichage DEL

L'appareil WAP dispose de deux types de voyants : voyants système et voyants Ethernet. Utilisez la page Affichage DEL pour configurer tous les voyants.

Pour configurer l'affichage DEL, procédez comme suit :

Étape 1 Sélectionnez **Notification > Affichage DEL**.

Étape 2 Sélectionnez **Activer** pour activer les voyants. Sélectionnez **Désactiver** pour désactiver les voyants. Sélectionnez **Associer un planificateur** et passez à l'étape 3.

Étape 3 Sélectionnez un nom de profil dans la liste déroulante pour associer un planificateur à l'affichage DEL. Par défaut, aucun profil n'est associé aux voyants. La liste déroulante contient les noms de profil de planificateur configurés sur la page **Réseau sans fil > Planificateur**.

Lorsque le voyant est associé à un profil de planificateur, cette colonne indique le statut en fonction de la présence ou de l'absence d'une règle de profil active à ce moment de la journée.

Étape 4 Cliquez sur **Enregistrer**.

Paramètres des journaux

Vous pouvez utiliser la page Paramètres des journaux pour permettre l'enregistrement des messages de journal dans la mémoire permanente. Vous pouvez également envoyer des journaux à un hôte distant.

Si le système redémarre de manière inattendue, les messages de journal peuvent être utiles pour en diagnostiquer la cause. Toutefois, les messages de journal sont effacés au redémarrage du système sauf si vous activez la journalisation persistante.



Avertissement

L'activation de la journalisation persistante peut épuiser la mémoire flash (non volatile) et dégrader les performances réseau. Activez uniquement la journalisation persistante pour déboguer un problème. Veillez à désactiver la journalisation persistante une fois que vous avez débogué le problème.

Configuration du journal persistant

Étape 1 Sélectionnez **Notification > Paramètres des journaux**.

Étape 2 Définissez les paramètres suivants :

- **Persistance** : cochez la case **Activer** pour enregistrer les journaux système dans la mémoire non volatile afin de permettre la conservation des journaux au redémarrage de l'appareil WAP. Vous pouvez enregistrer jusqu'à 1 000 messages de journal. Lorsque la limite de 1000 est atteinte, le message le plus ancien du journal est remplacé par le nouveau message. Effacez le contenu de ce champ si vous souhaitez enregistrer les journaux système dans la mémoire volatile. Les journaux présents dans la mémoire volatile sont supprimés au redémarrage du système.
- **Gravité** : dans la liste déroulante, sélectionnez la gravité (**Urgence, Alerte, Critique, Erreur, Avertissement, Notification, Info ou Débogage**) utilisée pour filtrer les messages d'événement qui seront enregistrés dans la mémoire non volatile. Tous les autres messages seront enregistrés dans la mémoire volatile.
- **Profondeur** : saisissez le nombre maximal de messages (jusqu'à 1 000) pouvant être stockés dans la mémoire volatile. Lorsque le nombre défini dans ce champ est atteint, l'événement le plus ancien du journal est remplacé par le nouvel événement.

Étape 3 Cliquez sur **Enregistrer**.

Serveur de journalisation distant

Le journal du noyau est une liste complète d'événements système (présentée dans le journal système) et de messages du noyau.

Vous ne pouvez pas consulter les messages de journal du noyau directement à partir de l'utilitaire de configuration. Vous devez d'abord configurer un serveur de journalisation distant qui recevra et capturera les journaux. Vous pouvez ensuite configurer l'appareil WAP à journaliser sur le serveur de journalisation distant. L'appareil WAP prend en charge jusqu'à deux serveurs de journalisation distants.

La collecte du serveur de journalisation distant pour les messages syslog offre les fonctions suivantes :

- Elle permet l'agrégation des messages syslog depuis plusieurs points d'accès.
- Elle stocke un historique des messages plus long que celui conservé sur un seul appareil WAP.
- Elle déclenche des opérations de gestion scriptées et des alertes.

Pour spécifier un hôte de votre réseau en tant que serveur de journalisation distant :

Étape 1 Sélectionnez **Notification > Paramètres des journaux**.

Étape 2 Dans la Table de serveurs de journalisation distants, configurez les paramètres suivants :

- **Nom/adresse IPv4/IPv6 du serveur** : saisissez l'adresse IPv4 ou IPv6, ou le nom d'hôte du serveur de journalisation distant.

Un nom d'hôte peut être constitué d'un ou de plusieurs libellés, qui sont des ensembles pouvant contenir jusqu'à 63 caractères alphanumériques. Si un nom d'hôte inclut plusieurs libellés, ceux-ci sont séparés par un point (.). La série complète de libellés et de points peut contenir jusqu'à 253 caractères.

- **Activer** : cochez cette case pour activer le serveur de journalisation distant. Définissez ensuite le niveau de gravité du journal et le port UDP.
- **Niveau de gravité du journal** : définissez le niveau de gravité d'un événement pour que celui-ci soit envoyé au serveur de journalisation distant.
- **Port UDP** : saisissez le numéro de port logique pour le processus syslog sur l'hôte distant. La plage valide est de 1 à 65535. La valeur par défaut est 514.

Il est recommandé d'utiliser le port par défaut. Si vous reconfigurez le port du journal, vérifiez que le numéro de port que vous attribuez à syslog est disponible.

Étape 3

Cliquez sur **Enregistrer**. Les modifications sont enregistrées dans la configuration de démarrage.

Remarque Si vous activez un serveur de journalisation distant et que vous cliquez sur **Enregistrer**, vous activez alors la journalisation distante. L'appareil WAP envoie ses messages du noyau en temps réel afin qu'ils soient affichés sur le moniteur du serveur de journalisation distant, un fichier journal du noyau spécifié ou un autre système de stockage, selon votre configuration.

Si vous désactivez un serveur de journalisation distant et que vous cliquez sur **Enregistrer**, vous désactivez alors la journalisation distante.

Afficher le journal système

La page Afficher le journal système affiche la liste des événements système qui se produisent sur l'appareil. Le contenu du journal est effacé lors d'un redémarrage et il peut également l'être par un administrateur. Le journal peut afficher un maximum de 1000 événements. Lorsque cela s'avère nécessaire, les entrées les plus anciennes sont supprimées de la liste, afin de créer de la place pour les nouveaux événements.

Pour afficher les journaux système, sélectionnez **Notification > Afficher le journal système**.

Les informations suivantes s'affichent :

- **Horodatage** : heure système de l'occurrence de l'événement.
- **Gravité** : niveau de gravité de l'événement.
- **Service** : service associé à l'événement.
- **Description** : description de l'événement.

Vous pouvez filtrer ou classer les paramètres sur la page Afficher le journal système.

Cliquez sur **Actualiser** pour actualiser l'écran et afficher les informations les plus récentes.

Cliquez sur **Effacer tout** pour effacer toutes les entrées du journal.

Cliquez sur **Télécharger** pour télécharger toutes les entrées du journal.

Configuration des alertes par e-mail/du serveur de messagerie/des messages

La fonction d'alerte par e-mail prend en charge la configuration du serveur de messagerie, la configuration de la gravité des messages et la configuration de trois adresses e-mail maximum pour l'envoi par e-mail des

alertes urgentes et non urgentes. Utilisez la fonction d'alerte par e-mail pour envoyer des messages aux adresses e-mail configurées lorsque des événements système spécifiques se produisent.



Conseil N'utilisez pas d'adresses e-mail personnelles, car vous risquez d'exposer inutilement vos informations de connexion. Utilisez plutôt un compte de messagerie distinct. Notez également que de nombreux comptes de messagerie conservent par défaut une copie de tous les messages envoyés. Toutes les personnes ayant accès à ce compte de messagerie ont accès aux messages envoyés. Vérifiez les paramètres de messagerie afin de vous assurer qu'ils respectent votre politique de confidentialité.

Pour configurer l'appareil WAP afin qu'il envoie des alertes par e-mail :

Étape 1 Sélectionnez **Notification > Alerte par e-mail**.

Étape 2 Dans la zone Configuration globale, définissez les paramètres suivants :

- **Mode d'administration** : cochez la case **Activer** pour activer la fonction d'alerte par e-mail.
- **Adresse e-mail de l'expéditeur** : saisissez l'adresse e-mail à afficher en tant qu'expéditeur de l'e-mail. L'adresse est une chaîne de 255 caractères imprimables. Aucune adresse n'est configurée par défaut.
- **Durée du journal** : choisissez la fréquence à laquelle les messages planifiés sont envoyés. La plage valide va de 30 à 1440 minutes. La valeur par défaut est 30 minutes.
- **Gravité des messages planifiés** : dans la liste déroulante, sélectionnez la gravité (**Urgence, Alerte, Critique, Erreur** ou **Avertissement**) pour qu'un événement soit envoyé à l'adresse e-mail de configuration à la fréquence spécifiée par le paramètre Durée du journal. La gravité par défaut est **Avertissement**.
- **Gravité des messages urgents** : dans la liste déroulante, sélectionnez la gravité (**Urgence, Alerte, Critique, Erreur, Avertissement, Notification, Info** ou **Débogage**) pour qu'un événement soit immédiatement envoyé à l'adresse e-mail configurée. La gravité par défaut est **Alerte**.

Étape 3 Dans la zone Mail Server Configuration, définissez les paramètres suivants :

- **Nom/adresse IPv4 du serveur** : saisissez l'adresse IP ou le nom d'hôte du serveur SMTP sortant. L'adresse du serveur doit être une adresse IPv4 ou un nom d'hôte valides. La forme de l'adresse IPv4 doit être similaire à celle-ci : xxx.xxx.xxx.xxx (192.0.2.10).
Un nom d'hôte peut être constitué d'un ou de plusieurs libellés, qui sont des ensembles pouvant contenir jusqu'à 63 caractères alphanumériques. Si un nom d'hôte inclut plusieurs libellés, ceux-ci sont séparés par un point (.). La série complète de libellés et de points peut contenir jusqu'à 253 caractères.
- **Cryptage de données** : sélectionnez le mode de sécurité dans la liste déroulante (**Ouvert** ou **TLSv1**) pour l'alerte par e-mail sortante. L'utilisation du protocole TLSv1 sécurisé empêche l'espionnage électronique et la falsification lors des communications via le réseau public.
- **Port** : saisissez le numéro de port SMTP à utiliser pour les e-mails sortants. La valeur est un numéro de port valide compris entre 0 et 65535. La valeur par défaut est 465.
- **Nom d'utilisateur** : saisissez le nom d'utilisateur du compte de messagerie qui sera utilisé pour envoyer ces e-mails. Généralement (pas systématiquement), le nom d'utilisateur correspond à l'adresse e-mail complète incluant le domaine (par exemple, Nom@exemple.com). Le compte spécifié sera utilisé en tant qu'adresse e-mail de l'expéditeur. Le nom d'utilisateur peut être constitué de 1 à 64 caractères alphanumériques.

- **Mot de passe** : saisissez le mot de passe du compte de messagerie qui sera utilisé pour l'envoi de ces e-mails. Le mot de passe peut être constitué de 1 à 64 caractères.

Étape 4 Dans la zone Configuration des messages, spécifiez les adresses e-mail et la ligne d'objet :

- **Adresse e-mail du destinataire 1/2/3** : saisissez au maximum trois adresses de réception des alertes par e-mail. Chaque adresse e-mail doit être valide.
- **Objet du courrier électronique** : saisissez le texte qui s'affichera dans la ligne d'objet de l'e-mail. Il peut s'agir d'une chaîne alphanumérique de 255 caractères maximum.

Étape 5 Cliquez sur **Enregistrer**.

Exemples d'alertes par e-mail

L'exemple suivant indique comment renseigner les paramètres de la zone Configuration du serveur de messagerie :

```
Gmail
Server IPv4 Address/Name = smtp.gmail.com
Data Encryption = TLSv1
Port = 465
Username = Your full email address you can use to login to your email account
associated with the above server
Password = xxxxxxxx is a valid password of your valid email account
To Email Address 1 = myemail@gmail.com
```

```
Windows Live Hotmail
Windows Live Hotmail recommends the following settings: Data Encryption: TLSv1
SMTP Server: smtp.live.com
SMTP Port: 587
Username: Your full email address, such as myName@hotmail.com or
myName@myDomain.com
Password: Your Windows Live account password
```

```
Yahoo! Mail
Yahoo requires using a paid account for this type of service. Yahoo
recommends the following settings:
Data Encryption: TLSv1
SMTP Server: plus.smtp.mail.yahoo.com
SMTP Port: 465 or 587
Username: Your email address, without the domain name such as myName (without
@yahoo.com)
Password: Your Yahoo account password
```

L'exemple suivant présente la mise en forme d'un e-mail de journal général :

```
From: AP-192.168.2.10@mailserver.com
Sent: Wednesday, September 09, 2009 11:16 AM
To: administrator@mailserver.com
Subject: log message from AP

TIME          Priority > Process Id > > > Message
Sep 8 03:48:25 info >> login[1457]> > > root login on tty0
Sep 8 03:48:26 info >> mini_http-ssl[1175]>Max concurrent connections of 20
reached
```

Comptes d'utilisateur

Par défaut, un utilisateur de gestion est configuré sur l'appareil WAP :

- Nom d'utilisateur : **cisco**
- Mot de passe : **cisco**

Utilisez la page Comptes d'utilisateur pour configurer un maximum de quatre utilisateurs supplémentaires et modifier le mot de passe d'un utilisateur.

Ajout d'un utilisateur

Configurez les paramètres suivants pour ajouter un nouvel utilisateur :

Étape 1 Cliquez sur **Configuration système > Comptes d'utilisateur**.

La table des comptes d'utilisateur affiche les utilisateurs actuellement configurés. L'utilisateur cisco est préconfiguré dans le système et dispose de privilèges de lecture/écriture.

Tous les autres utilisateurs peuvent disposer d'un accès en lecture seule, mais pas d'un accès en lecture/écriture.

Étape 2 Cliquez sur pour ajouter une nouvelle ligne.

Étape 3 Cochez la case en regard du nouvel utilisateur et donnez-lui un nom.

Étape 4 Saisissez le nouveau mot de passe constitué de 0 à 127 caractères, puis saisissez le même mot de passe dans le champ Confirmer le nouveau mot de passe.

Le champ Mesure de la fiabilité du mot de passe indique la fiabilité du mot de passe, comme suit :

- **Rouge** : le mot de passe ne répond pas aux exigences minimales en termes de complexité.
- **Orange** : le mot de passe répond aux exigences minimales en termes de complexité, mais offre une faible sécurité.
- **Vert** : le mot de passe offre un niveau de fiabilité élevé.

Étape 5 Cliquez sur **Enregistrer**.

Remarque Pour supprimer un utilisateur, sélectionnez-le, puis cliquez sur **Supprimer**. Pour modifier un utilisateur, sélectionnez-le, puis cliquez sur **Modifier** ; cliquez ensuite sur **Enregistrer** pour enregistrer toutes les modifications apportées aux configurations.

Modification d'un mot de passe utilisateur

Pour modifier un mot de passe utilisateur :

Étape 1 Cliquez sur **Configuration système > Comptes d'utilisateur**.

La table des comptes d'utilisateur affiche les utilisateurs actuellement configurés. L'utilisateur cisco est préconfiguré dans le système pour avoir les privilèges de lecture/écriture. Le mot de passe de l'utilisateur cisco peut être modifié.

Étape 2 Sélectionnez l'utilisateur à configurer et cliquez sur **Modifier**.

Étape 3 Saisissez le **Nouveau mot de passe** constitué de 0 à 127 caractères, puis saisissez le même mot de passe dans le champ **Confirmer le nouveau mot de passe**.

Le champ Mesure de la fiabilité du mot de passe indique la fiabilité du mot de passe, comme suit :

- **Rouge** : le mot de passe ne répond pas aux exigences minimales en termes de complexité.
- **Orange** : le mot de passe répond aux exigences minimales en termes de complexité, mais offre une faible sécurité.
- **Vert** : le mot de passe offre un niveau de fiabilité élevé.

Étape 4 Cliquez sur **Enregistrer**. Les modifications sont enregistrées dans la configuration de démarrage.

Remarque Si vous modifiez votre mot de passe, vous devez vous reconnecter au système.

Gestion

La page Paramètres système vous permet de configurer les informations qui identifient l'appareil WAP sur le réseau.

Pour définir les paramètres système :

Étape 1 Sélectionnez **Configuration système > Gestion**.

Étape 2 Définissez les paramètres suivants :

- **Nom d'hôte** : saisissez le nom d'hôte de l'appareil WAP. Par défaut, il s'agit du nom de domaine complet (FQDN) du nœud. Le nom d'hôte par défaut est wap concaténé avec les 6 derniers chiffres hexadécimaux de l'adresse MAC de l'appareil WAP. Le nom d'hôte ne peut comporter que des lettres, des chiffres et des tirets. Il ne peut pas être précédé ou suivi d'un tiret. Les autres symboles, les signes de ponctuation et les espaces ne sont pas autorisés. Le nom d'hôte peut comporter de 1 à 63 caractères.
- **Contact système** : spécifiez la personne à contacter pour l'appareil WAP. Le contact système peut comporter de 0 à 255 caractères et peut inclure des espaces et des caractères spéciaux.
- **Emplacement du système** : spécifiez l'emplacement physique de l'appareil WAP. L'emplacement système peut comporter de 0 à 255 caractères et peut inclure des espaces et des caractères spéciaux.

Étape 3 Cliquez sur **Enregistrer**. Les modifications sont enregistrées dans la configuration de démarrage.

Paramètres de la session de connexion/Tâche de service HTTP/HTTPS

Utilisez la page Service HTTP/HTTPS pour activer et configurer des connexions de gestion web. Si HTTPS est utilisé pour sécuriser les sessions de gestion, vous pouvez aussi utiliser cette page pour gérer les certificats SSL requis.

Pour configurer les services HTTP et HTTPS :

Étape 1 Sélectionnez **Configuration système > Gestion**.

Étape 2 Dans la zone Paramètres globaux, définissez les paramètres suivants :

- **Nombre maximal de sessions** : saisissez le nombre de sessions web, y compris HTTP et HTTPS, pouvant être utilisées simultanément.

Lorsqu'un utilisateur se connecte à l'utilitaire de configuration de l'appareil WAP, une session est créée. Cette session reste active jusqu'à ce que l'utilisateur se déconnecte ou jusqu'à la fin du délai d'expiration de la session. La plage est comprise entre 1 et 10 sessions. La valeur par défaut est 5. Si le nombre maximal de sessions est atteint, le prochain utilisateur qui tente de se connecter à l'utilitaire de configuration reçoit un message d'erreur relatif à la limite de session.

- **Délai d'expiration de la session** : saisissez le délai maximal, en minutes, pendant lequel un utilisateur inactif reste connecté. Lorsque le délai d'expiration est atteint, l'utilisateur est automatiquement déconnecté. La plage valide va de 2 à 60 minutes. La valeur par défaut est 10 minutes.

Étape 3 Configurez les services HTTP et HTTPS :

- **Service HTTP** : activez ou désactivez l'accès par HTTP. L'accès HTTP est activé par défaut. Si vous le désactivez, toutes les connexions actives qui utilisent ce protocole sont déconnectées.

- **Port HTTP** : saisissez le numéro de port logique à utiliser pour les connexions HTTP, compris entre 1025 et 65535. Le numéro de port par défaut pour les connexions HTTP est le numéro de port IANA connu 80.

- **Rediriger HTTP vers HTTPS** : redirige les tentatives d'accès HTTP de gestion sur le port HTTP vers le port HTTPS. Ce champ est uniquement disponible lorsque l'accès HTTP est désactivé.

- **Service HTTPS** : activez ou désactivez l'accès par HTTP sécurisé (HTTPS). L'accès HTTPS est activé par défaut. Si vous le désactivez, toutes les connexions actives qui utilisent ce protocole sont déconnectées.

- **Port HTTPS** : saisissez le numéro de port logique à utiliser pour les connexions HTTPS, compris entre 1025 et 65535. Le numéro de port par défaut pour les connexions HTTPS est le numéro de port IANA connu 443.

- **Mode de l'ACL de gestion** : si la liste de contrôle d'accès de gestion est activée, l'accès via le web et SNMP est limité aux hôtes IP spécifiés. Si cette fonction est désactivée, tout le monde peut accéder à l'utilitaire de configuration depuis n'importe quel client réseau en fournissant le nom d'utilisateur et le mot de passe corrects à l'appareil WAP.

Remarque Vérifiez chaque adresse IP que vous saisissez. Si vous saisissez une adresse IP qui ne correspond pas à votre ordinateur d'administration, vous n'aurez plus accès à l'interface de configuration. Il est recommandé d'attribuer une adresse IP statique à l'ordinateur d'administration afin que cette adresse reste toujours la même.

Étape 4 Cliquez sur **Enregistrer**.

Statut du fichier de certificats SSL

Pour utiliser les services HTTPS, l'appareil WAP doit posséder un certificat SSL valide. L'appareil WAP peut générer un certificat ou vous pouvez le télécharger depuis votre réseau ou un serveur TFTP.

Dans la zone Générer le certificat SSL, cliquez sur **Paramètres SSL**, puis cliquez sur **Générer** pour générer le certificat de l'appareil WAP. Cette procédure doit être effectuée une fois que l'appareil WAP a obtenu une adresse IP afin de garantir que le nom commun du certificat correspond à l'adresse IP de l'appareil WAP. La génération d'un nouveau certificat SSL entraîne le redémarrage du serveur web sécurisé. La connexion sécurisée ne fonctionne pas tant que le nouveau certificat n'est pas accepté par le navigateur.

Dans la zone Statut du fichier de certificats SSL, vous pouvez afficher le certificat actuel sur l'appareil WAP. Les paramètres suivants s'affichent :

- Fichier de certificat présent
- Date d'expiration du certificat
- Nom de l'émetteur du certificat

S'il existe un certificat SSL (portant l'extension .pem) sur l'appareil WAP, vous pouvez le télécharger vers votre ordinateur en tant que sauvegarde. Dans la zone **Transférer le certificat SSL depuis** (appareil vers ordinateur), sélectionnez l'option de téléchargement **HTTP/HTTPS** ou **TFTP**, puis cliquez sur **Transférer**.

- Si vous sélectionnez **HTTP/HTTPS**, vous devez confirmer le téléchargement, puis accéder à l'emplacement d'enregistrement du fichier sur votre réseau.
- Si vous sélectionnez **TFTP**, saisissez le nom de fichier à attribuer au fichier téléchargé, puis saisissez l'adresse IPv4 du serveur TFTP où le fichier sera téléchargé.

Vous pouvez également télécharger un fichier de certificat (portant une extension .pem) depuis votre ordinateur vers l'appareil WAP. Dans la zone **Transférer le certificat SSL depuis** (ordinateur vers appareil), sélectionnez l'option de téléchargement **HTTP/HTTPS** ou **TFTP**, puis cliquez sur **Transférer**.

- Pour **HTTP/HTTPS**, accédez à l'emplacement réseau, sélectionnez le fichier, puis cliquez sur **Transférer**.
- Pour **TFTP**, saisissez le nom de fichier et l'adresse IPv4 du serveur TFTP, puis cliquez sur **Transférer**.
Le nom de fichier ne peut pas contenir les caractères suivants : espaces, <, >, |, \, :, (,), &, ;, #, ? aszxaa, *, ainsi que deux points successifs ou plus.

Un message de confirmation s'affiche lorsque le chargement a été correctement effectué.

Paramètres SNMP/SNMPv2c

Le protocole SNMP définit une norme pour l'enregistrement, le stockage et le partage d'informations relatives à des appareils réseau. Il permet également de faciliter la gestion, le dépannage et la maintenance des réseaux. L'appareil WAP prend en charge SNMP et peut fonctionner en tant qu'appareil SNMP géré pour une intégration transparente dans des systèmes de gestion de réseau.

Utilisez la page Paramètres SNMP/SNMPv2c pour activer SNMP et configurer les paramètres de protocole de base.

Pour configurer les paramètres SNMP généraux :

-
- Étape 1** Sélectionnez **Gestion > Paramètres SNMP**.
- Étape 2** Cochez la case **Activer** pour activer SNMP.
- Étape 3** Spécifiez le port UDP pour le trafic SNMP. La valeur par défaut est 161. Vous pouvez néanmoins le configurer de façon à ce que l'agent écoute les demandes sur un port différent. La plage valide est comprise entre 1025 et 65535.

Étape 4 Dans la zone Paramètres SNMPv2c, configurez les paramètres SNMPv2c :

- **Communauté en lecture seule** : saisissez un nom de communauté en lecture seule pour l'accès SNMPv2. La plage valide va de 1 à 256 caractères alphanumériques et caractères spéciaux.
Le nom de communauté agit en tant que fonctionnalité d'authentification simple visant à limiter le nombre d'appareils sur le réseau pouvant demander des données à l'agent SNMP. Ce nom fonctionne comme un mot de passe et la demande est supposée être authentique si son émetteur connaît le mot de passe.
- **Communauté en lecture-écriture** : saisissez un nom de communauté en lecture-écriture, utilisé pour les demandes de configuration SNMP. La plage valide va de 1 à 256 caractères alphanumériques et caractères spéciaux. La définition d'un nom de communauté est similaire à celle d'un mot de passe. Seules les demandes émanant des ordinateurs qui s'identifient avec ce nom de communauté sont acceptées.
- **Poste de gestion** : détermine les postes qui peuvent accéder à l'appareil WAP par le biais du protocole SNMP. Sélectionnez l'une des options suivantes :
 - **Tous** : tous les postes peuvent accéder à l'appareil WAP par le biais du protocole SNMP.
 - **Défini par l'utilisateur** : l'ensemble des demandes SNMP définies par l'utilisateur qui sont autorisées.
- **Nom/adresse IPv4 du système de gestion de réseau** : saisissez l'adresse IP IPv4, le nom d'hôte DNS ou le sous-réseau du système de gestion de réseau.

Un nom d'hôte DNS peut être constitué d'un ou de plusieurs libellés, qui sont des ensembles pouvant contenir jusqu'à 63 caractères alphanumériques. Si un nom d'hôte inclut plusieurs libellés, ceux-ci sont séparés par un point (.). La série complète de libellés et de points peut contenir jusqu'à 253 caractères.

Comme dans le cas des noms de communauté, ce paramètre assure un certain niveau de sécurité sur les paramètres SNMP. L'agent SNMP accepte uniquement les demandes émanant de l'adresse IP, du nom d'hôte ou du sous-réseau spécifiés ici.

Pour spécifier un sous-réseau, saisissez une ou plusieurs plages d'adresses de sous-réseau sous la forme adresse/longueur du masque, où « adresse » est une adresse IP et « longueur du masque » est le nombre de bits du masque. Les deux formats adresse/masque et adresse/longueur du masque sont pris en charge. Par exemple, si vous entrez la plage 192.168.1.0/24, cela signifie que l'adresse du sous-réseau est 192.168.1.0 et que le masque du sous-réseau est 255.255.255.0.

- **Nom/adresse IPv6 du système de gestion du réseau** : adresse IP IPv6, nom d'hôte DNS ou sous-réseau des appareils pouvant exécuter des demandes d'obtention et de configuration vers les appareils gérés. Le format de l'adresse IPv6 doit être similaire à celui-ci : xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx (2001:DB8:CAD5:7D91).

Remarque Un nom d'hôte peut être constitué d'un ou de plusieurs libellés, qui sont des ensembles pouvant contenir jusqu'à 63 caractères alphanumériques. Si un nom d'hôte inclut plusieurs libellés, ceux-ci sont séparés par un point (.). La série complète de libellés et de points peut contenir jusqu'à 253 caractères.

Étape 5 Dans la zone Paramètres de filtre SNMPv2c, configurez les paramètres de filtre SNMPv2c :

- **Communauté de filtre** : saisissez une chaîne de communauté globale associée aux filtres SNMP. Les dérouterments envoyés à partir de l'appareil fournissent cette chaîne en tant que nom de communauté. La plage valide va de 1 à 60 caractères alphanumériques et caractères spéciaux.
- **Table de destination des filtres** : saisissez une liste de trois adresses IP ou noms d'hôtes maximum pouvant recevoir des filtres SNMP. Cochez la case et choisissez un Type d'adresse IP hôte (IPv4 ou IPv6) avant d'ajouter le Nom d'hôte/Adresse IP.

Un exemple de nom d'hôte DNS est `filtressnmp.foo.com`. Les filtres SNMP étant envoyés de manière aléatoire à partir de l'agent SNMP, il est logique de spécifier à quel emplacement exact les filtres doivent être envoyés. Le nombre maximal de noms d'hôte DNS est égal à trois. Vérifiez que vous avez coché la case **Activé** et sélectionnez le Type d'adresse IP hôte approprié.

Étape 6 Cliquez sur **Enregistrer**.

Vues SNMPv3

Une vue MIB SNMP est une famille de sous-arborescences de vues dans la hiérarchie MIB. Une sous-arborescence de vues est identifiée par l'association d'une valeur de sous-arborescence d'ID d'objet (OID) et d'une valeur de masque de chaîne de bits. Chaque vue MIB est définie par deux ensembles de sous-arborescences de vues, inclus dans la vue MIB ou exclus de celle-ci. Vous pouvez créer des vues MIB dans le but de contrôler la plage d'OID à laquelle les utilisateurs SNMPv3 peuvent accéder.

L'appareil WAP prend en charge 16 vues au maximum.

Cette section répertorie les principales informations de configuration des vues SNMPv3. Veuillez lire l'ensemble de ces remarques avant de continuer.



Remarque Une vue MIB appelée « all » est créée par défaut dans le système. Cette vue contient l'ensemble des objets de gestion pris en charge par le système.



Remarque Par défaut, les vues SNMPv3 « view-all » et « view-none » sont créées sur l'appareil WAP. Ces vues ne peuvent pas être supprimées ou modifiées.

Pour ajouter et configurer une vue SNMP, procédez comme suit :

Étape 1 Sélectionnez **Gestion > SNMPv3**.

Étape 2 Cliquez sur pour créer une nouvelle ligne dans le tableau **Vues SNMPv3** ou cochez la case en regard des vues existantes, puis cliquez sur **Modifier**.

- **View Name** : entrez le nom de la vue MIB. Les noms de vue peuvent comporter jusqu'à 32 caractères alphanumériques.
- **Type** : choisissez d'inclure la sous-arborescence de vues ou la famille de sous-arborescences dans la vue MIB ou de l'en exclure.
- **OID** : entrez une chaîne d'OID pour la sous-arborescence à inclure dans la vue ou à exclure de celle-ci. Par exemple, la sous-arborescence système est spécifiée par la chaîne d'OID string.1.3.6.1.2.1.1.
- **Mask** : entrez un masque d'OID. La longueur du masque est de 47 caractères. Le format du masque d'OID est `xx.xx.xx (...)` ou `xx:xx:xx.... (:)` et sa longueur est de 16 octets. Chaque octet se compose de deux caractères hexadécimaux séparés par un point (.) ou par un caractère deux-points (:). Seuls les caractères hexadécimaux sont autorisés dans ce champ. Par exemple, le masque d'OID FA.80 est 11111010.10000000.

Un masque de famille est utilisé pour définir une famille de sous-arborescences de vues. Le masque de famille indique quels sous-identificateurs de la chaîne d'OID de la famille associée sont significatifs pour la définition de la famille. Une famille de sous-arborescences de vues permet un accès de contrôle efficace à une ligne du tableau.

Étape 3 Cliquez sur **Enregistrer**.

Remarque Pour supprimer une vue, sélectionnez-la dans la liste et cliquez sur **Supprimer**.

Groupes SNMPv3

Les groupes SNMPv3 permettent de répartir les utilisateurs en groupes de privilèges d'autorisation et d'accès différents. Chaque groupe est ainsi associé à l'un des trois niveaux de sécurité suivants :

- noAuthNoPriv
- authNoPriv
- authPriv

L'accès aux bases d'informations de gestion (MIB) pour chaque groupe est contrôlé en associant une vue MIB à un groupe pour l'accès en lecture ou en écriture, et ce, de manière séparée.

Par défaut, l'appareil WAP possède deux groupes :

- **LS** : groupe en lecture seule utilisant l'authentification et le cryptage des données. Les utilisateurs de ce groupe utilisent une clé ou un mot de passe SHA pour l'authentification, et une clé DES ou AES128 pour le cryptage. Les clés ou mots de passe SHA, DES et AES128 doivent être définis. Par défaut, les utilisateurs de ce groupe ont un accès en lecture à la vue MIB par défaut « all ».
- **LE** : groupe en lecture-écriture utilisant l'authentification et le cryptage des données. Les utilisateurs de ce groupe utilisent une clé ou un mot de passe SHA pour l'authentification, et une clé DES ou AES128 pour le cryptage. Les clés ou mots de passe SHA, DES et AES128 doivent être définis. Par défaut, les utilisateurs de ce groupe ont un accès en lecture et en écriture à la vue MIB par défaut « all ».



Remarque Les groupes par défaut RO et RW ne peuvent pas être supprimés. L'appareil WAP prend en charge huit groupes au maximum.

Pour ajouter et configurer le groupe SNMP, procédez de la façon suivante :

Étape 1 Sélectionnez **Gestion > SNMPv3**.

Étape 2 Cliquez sur pour ajouter une nouvelle ligne au tableau des groupes SNMPv3.

Étape 3 Cochez la case du nouveau groupe et définissez les paramètres suivants.

- **Nom du groupe** : saisissez le nom du groupe. Les noms de groupe par défaut sont RO et RW. Les noms de groupe peuvent comporter jusqu'à 32 caractères alphanumériques.
- **Niveau de sécurité** : sélectionnez le niveau de sécurité du groupe parmi les options suivantes :
 - **noAuthNoPriv** : pas d'authentification et pas de cryptage des données (aucune sécurité).

- **authNoPriv** : authentification, mais pas de cryptage des données. Avec ce niveau de sécurité, les utilisateurs envoient des messages SNMP qui utilisent une clé ou un mot de passe SHA pour l'authentification, mais pas de clé DES ou AES128 pour le cryptage.
- **authPriv** : authentification et cryptage des données. Avec ce niveau de sécurité, les utilisateurs envoient une clé ou un mot de passe SHA pour l'authentification, et une clé DES ou AES128 pour le cryptage. Pour les groupes qui nécessitent une authentification, un cryptage ou les deux, vous devez définir les clés ou mots de passe SHA, DES et AES128 sur la page Utilisateurs SNMP.
- **Vues en écriture** : sélectionnez l'accès en écriture pour les MIB du groupe parmi les options suivantes :
 - **afficher-tout** : le groupe peut créer, modifier et supprimer des MIB.
 - **afficher-aucun** : le groupe ne peut pas créer, ni modifier, ni supprimer des MIB.
- **Vues en lecture** : sélectionnez l'accès en lecture pour les MIB du groupe parmi les options suivantes :
 - **afficher-tout** : le groupe est autorisé à afficher et à lire l'ensemble des MIB.
 - **afficher-aucun** : le groupe ne peut ni afficher ni lire des MIB.

Étape 4 Cliquez sur **Enregistrer** pour ajouter le groupe à la liste des groupes SNMPv3.

Remarque Pour supprimer un groupe, sélectionnez-le dans la liste et cliquez sur **Supprimer**. Pour modifier un groupe, sélectionnez-le dans la liste et cliquez sur **Modifier**.

Utilisateurs SNMPv3

Utilisez la page Utilisateurs SNMP pour définir des utilisateurs, associer un niveau de sécurité à chaque utilisateur et configurer des clés de sécurité pour chacun d'entre eux.

Chaque utilisateur est mappé sur un groupe SNMPv3, à partir des groupes prédéfinis ou des groupes définis par l'utilisateur, et, éventuellement, est configuré pour l'authentification et le cryptage. Pour l'authentification, seul le type SHA est pris en charge. Pour le cryptage, seuls les types DES et AES128 sont pris en charge. Il n'y a pas d'utilisateur SNMPv3 par défaut sur l'appareil WAP et vous pouvez ajouter jusqu'à huit utilisateurs.

Pour ajouter des utilisateurs SNMP, procédez comme suit :

Étape 1 Sélectionnez **Gestion > SNMPv3**.

Étape 2 Cliquez sur pour ajouter une nouvelle ligne au tableau des utilisateurs SNMPv3.

Étape 3 Cochez la case dans la nouvelle ligne et définissez les paramètres suivants :

- **Nom d'utilisateur** : saisissez le nom qui identifie l'utilisateur SNMPv3. Les noms d'utilisateur peuvent comporter jusqu'à 32 caractères alphanumériques.
- **Groupe** : saisissez le groupe sur lequel l'utilisateur est mappé. Les groupes par défaut sont RW et RO. Vous pouvez définir des groupes supplémentaires à la page SNMP Groups.
- **Type d'authentification** : sélectionnez le type d'authentification à utiliser sur les demandes SNMPv3 émanant de l'utilisateur parmi les options suivantes :

- **SHA** : requiert l'authentification SHA dans le cas des demandes SNMP émanant de l'utilisateur.
- **Aucun(e)** : les demandes SNMPv3 émanant de cet utilisateur ne requièrent pas d'authentification.
- **Phrase secrète d'authentification** : si vous spécifiez SHA en tant que type d'authentification, saisissez la phrase secrète permettant à l'agent SNMP d'authentifier les demandes envoyées par l'utilisateur. La longueur de la phrase secrète doit être comprise entre 8 et 32 caractères.
- **Type de cryptage** : sélectionnez le type de cryptage/confidentialité appliqué aux demandes SNMP de l'utilisateur parmi les options suivantes :
 - **DES** : utilise le cryptage DES dans le cas des demandes SNMPv3 émanant de l'utilisateur.
 - **AES128** : utilise le cryptage AES128 pour les demandes SNMPv3 émanant de l'utilisateur.
 - **None** : les demandes SNMPv3 émanant de cet utilisateur ne requièrent pas de confidentialité.
- **Phrase secrète de cryptage** : si vous spécifiez DES ou AES128 comme type de cryptage, saisissez la phrase secrète utilisée pour crypter les demandes SNMP. La longueur de la phrase secrète doit être comprise entre 8 et 32 caractères.

Étape 4 Cliquez sur **Enregistrer**. L'utilisateur est ajouté à la liste des utilisateurs SNMPv3 et vos modifications sont enregistrées dans la configuration initiale.

Remarque Pour supprimer un utilisateur, sélectionnez-le dans la liste et cliquez sur **Supprimer**. Pour modifier un utilisateur, sélectionnez le dans la liste et cliquez sur **Modifier**.

Cibles SNMPv3

Les cibles SNMPv3 envoient des notifications SNMP à l'aide de messages d'information au gestionnaire SNMP. Dans le cas des cibles SNMPv3, seuls des messages d'information sont envoyés et pas les filtres. Dans le cas des versions 1 et 2 du protocole SNMP, des filtres sont envoyés. Chaque cible est définie avec une adresse IP cible, un port UDP et un nom d'utilisateur SNMPv3.



Remarque La configuration des utilisateurs SNMPv3 (voir la page [Utilisateurs SNMPv3](#)) doit être terminée avant celle des cibles SNMPv3.

L'appareil WAP prend en charge huit cibles au maximum.

Pour ajouter des cibles SNMP, procédez comme suit :

Étape 1 Sélectionnez **Gestion > Cibles SNMPv3**.

Étape 2 Cliquez sur pour ajouter une nouvelle ligne au tableau.

Étape 3 Cochez la case dans la nouvelle ligne et définissez les paramètres suivants :

- **Adresse IP** : saisissez l'adresse IPv4 ou IPv6 du gestionnaire SNMP distant qui doit recevoir la cible.
- **Port UDP** : saisissez le port UDP à utiliser pour l'envoi des cibles SNMPv3.

- **Utilisateurs** : saisissez le nom de l'utilisateur SNMP à associer à la cible. Pour configurer les utilisateurs SNMP, reportez-vous à la page [Utilisateurs SNMPv3](#), à la page 31.

Étape 4 Cliquez sur **Enregistrer**. L'utilisateur est ajouté à la liste des cibles SNMPv3 et vos modifications sont enregistrées dans la configuration initiale.

Remarque Pour supprimer une cible SNMP, sélectionnez l'utilisateur dans la liste et cliquez sur **Supprimer**. Pour modifier une cible SNMP, sélectionnez l'utilisateur dans la liste et cliquez sur **Modifier**.

Sécurité

Cette section explique comment configurer les paramètres de sécurité sur l'appareil WAP.

Serveur RADIUS

Plusieurs fonctionnalités nécessitent une communication avec un serveur d'authentification RADIUS. Par exemple, lorsque vous configurez des points d'accès virtuels (VAP) sur l'appareil WAP, vous pouvez configurer des méthodes de sécurité qui contrôlent l'accès des clients sans fil (voir [Radio](#), à la page 41). La méthode de sécurité WPA entreprise utilise un serveur RADIUS externe pour authentifier les clients. La fonctionnalité de filtrage des adresses MAC, dans laquelle l'accès des clients est limité à une liste, peut également être configurée afin d'utiliser un serveur RADIUS pour le contrôle des accès. La fonctionnalité de portail captif utilise également un serveur RADIUS pour l'authentification des clients.

Utilisez la page Serveur Radius pour configurer les serveurs RADIUS qui seront utilisés par ces fonctionnalités. Vous pouvez configurer jusqu'à quatre serveurs RADIUS IPv4 ou IPv6 disponibles globalement. Vous devez néanmoins indiquer si le client RADIUS fonctionne en mode IPv4 ou IPv6 par rapport aux serveurs globaux. Un des serveurs joue toujours le rôle de serveur principal, tandis que l'autre fait office de serveur de secours.



Remarque En plus d'utiliser les serveurs RADIUS globaux, vous pouvez aussi configurer chaque point d'accès virtuel (VAP) de telle sorte qu'il utilise un ensemble spécifique de serveurs RADIUS. Pour plus d'informations, reportez-vous à la section [Réseaux](#), à la page 46.

Pour configurer les serveurs globaux RADIUS, procédez de la façon suivante :

Étape 1 Sélectionnez **Sécurité > Serveur Radius**.

Étape 2 Définissez les paramètres suivants :

- **Type d'adresse IP du serveur** : sélectionnez la version IP utilisée par le serveur RADIUS. Vous pouvez basculer entre les différents types d'adresse afin de définir les paramètres d'adresse RADIUS globale IPv4 et IPv6, mais l'appareil WAP ne contactera que le ou les serveurs RADIUS correspondant au type d'adresse que vous sélectionnez dans ce champ.
- **Adresse IP du serveur-1 ou Adresse IPv6 du serveur-1** : saisissez l'adresse du serveur RADIUS global principal. Lorsque le premier client sans fil tente de s'authentifier auprès de l'appareil WAP, celui-ci envoie une demande d'authentification au serveur principal. Si le serveur principal répond à la demande d'authentification, l'appareil

WAP continue à utiliser ce serveur RADIUS en guise de serveur principal et les demandes d'authentification sont envoyées à l'adresse spécifiée.

- **Adresse IP du serveur-2 ou Adresse IPv6 du serveur-2** : saisissez les adresses des serveurs RADIUS IPv4 ou IPv6 de secours. Si l'authentification auprès du serveur principal échoue, une tentative est effectuée sur le serveur de secours.
- **Clé-1** : saisissez la clé secrète partagée que l'appareil WAP utilise pour s'authentifier auprès du serveur RADIUS principal. Vous pouvez utiliser de 1 à 64 caractères alphanumériques standard et caractères spéciaux. La clé est sensible à la casse et doit correspondre à la clé configurée sur le serveur RADIUS. Le texte que vous saisissez apparaît sous la forme d'astérisques.
- **Clé-2** : saisissez la clé RADIUS associée aux serveurs RADIUS de sauvegarde configurés. Le serveur sur l'adresse IPv6 du serveur 2 utilise la clé 2.
- **Gestion de comptes RADIUS** : cochez la case **Activer** pour activer le suivi et la mesure des ressources consommées par un utilisateur donné (heure système, volume de données transmises et reçues, etc.). Si vous activez la gestion des comptes RADIUS, cette fonctionnalité est activée à la fois pour le serveur RADIUS principal et pour l'ensemble des serveurs de sauvegarde.

Étape 3 Cliquez sur **Enregistrer**. Les modifications sont enregistrées dans la configuration de démarrage.

Demandeur 802.1x

L'authentification IEEE 802.1X permet à l'appareil WAP d'accéder à un réseau filaire sécurisé. Vous pouvez activer l'appareil WAP en tant que demandeur (client) 802.1X sur le réseau filaire. Il est possible de configurer un nom d'utilisateur et un mot de passe à l'aide de l'algorithme de cryptage MD5 afin d'autoriser l'appareil WAP à effectuer une authentification à l'aide de la technologie 802.1X.

Sur les réseaux qui utilisent le contrôle d'accès réseau basé sur les ports IEEE 802.1X, un demandeur ne peut pas accéder au réseau tant que l'authentificateur 802.1X ne lui en a pas donné l'autorisation. Si votre réseau utilise la technologie 802.1X, vous devez configurer les informations d'authentification 802.1X sur l'appareil WAP, de telle sorte qu'il puisse les transmettre à l'authentificateur.

Pour configurer les paramètres du demandeur 802.1X, procédez de la façon suivante :

Étape 1 Cliquez sur **Sécurité > Demandeur 802.1X**.

Étape 2 Dans la zone Demandeur 802.1x, cochez la case **Activer** pour activer le mode d'administration.

Étape 3 Configurez le statut opérationnel 802.1X et les paramètres de base :

- **Méthode EAP** : sélectionnez l'algorithme à utiliser pour le cryptage des noms d'utilisateur et des mots de passe utilisés lors de l'authentification. Les options disponibles sont les suivantes :
 - **MD5** : fonction de hachage définie dans le standard RFC 3748 et offrant une sécurité de base.
 - **PEAP** : protocole (PEAP, Protected Extensible Authentication Protocol) offrant un niveau de sécurité supérieur à celui de la technologie MD5, grâce à l'encapsulation de celle-ci à l'intérieur d'un tunnel TLS.
 - **TLS** : sécurité de la couche transport (TLS, Transport Layer Security), telle que définie dans le standard RFC 5216, à savoir un standard ouvert offrant un haut niveau de sécurité.
- **Nom d'utilisateur** : saisissez le nom d'utilisateur.

- **Mot de passe** : saisissez le mot de passe.

- Étape 4** La zone Chargement du fichier de certificats permet de charger un fichier de certificat sur l'appareil WAP :
- Sélectionnez **HTTP** ou **TFTP** en guise de méthode de transfert.
 - Si vous avez sélectionné HTTP, cliquez sur **Parcourir** pour sélectionner le fichier. Reportez-vous à la section [Paramètres de la session de connexion/Tâche de service HTTP/HTTPS](#) pour plus d'informations sur la configuration des paramètres du serveur HTTP.
 - Si vous avez sélectionné **TFTP**, saisissez le nom de fichier et l'adresse IPv4 du serveur TFTP.
 - Cliquez sur **Charger**. Une fenêtre de confirmation apparaît, suivie d'une barre de progression indiquant l'état du téléchargement.
- Étape 5** Cliquez sur **Enregistrer**.

Détection de point d'accès non autorisé

Un point d'accès non autorisé est un point d'accès qui a été installé sur un réseau sécurisé sans l'autorisation explicite d'un administrateur système. Un point d'accès non autorisé constitue une menace de sécurité, car toute personne ayant accès aux locaux peut, par ignorance ou par malveillance, installer un appareil WAP sans fil bon marché susceptible de permettre à des personnes non autorisées d'accéder au réseau.

L'appareil WAP effectue une analyse RF sur tous les canaux afin de détecter tous les points d'accès à proximité du réseau. Si des points d'accès non autorisés sont détectés, ils apparaissent sur la page Rogue AP Detection. Si un point d'accès identifié comme non autorisé est en réalité légitime, vous pouvez l'ajouter à la liste des points d'accès connus.



Remarque

La Detected Rogue AP List et la Trusted AP List fournissent des informations. Le point d'accès n'a aucun contrôle sur les points d'accès indiqués dans les listes et ne peut pas appliquer de politiques de sécurité aux points d'accès détectés via l'analyse RF.

Lorsque la détection de point d'accès non autorisé est activée, la radio bascule régulièrement de son canal de fonctionnement pour analyser les autres canaux de la même bande.

Affichage de la liste des points d'accès non autorisés

Pour activer la détection des points d'accès non autorisés, la radio sans fil doit être activée. Vous devez activer l'interface radio avant d'activer la détection des points d'accès non autorisés sur celle-ci.

Pour autoriser la radio à collecter des informations sur les points d'accès non autorisés :

Étape 1 Sélectionnez **Sécurité > Détection de point d'accès non autorisé**.

Étape 2 Cochez la case **Activer** pour activer la détection des points d'accès pour la Radio 1 et la Radio 2.

Étape 3 Cliquez sur **Enregistrer**.

La table Liste des points d'accès non autorisés détectés affiche tous les points d'accès non autorisés détectés. La Liste des points d'accès approuvés affiche tous les points d'accès approuvés. Les paramètres suivants s'affichent pour chaque liste de points d'accès non autorisés :

- **Adresse MAC** : adresse MAC du point d'accès non autorisé.
- **Intervalle de balise** : intervalle de balise utilisé par le point d'accès non autorisé. Les trames de balise sont transmises par un point d'accès à intervalles réguliers pour annoncer l'existence du réseau sans fil. Le comportement par défaut consiste à envoyer une trame de balise toutes les 100 millisecondes (ou 10 par seconde). Vous pouvez définir l'intervalle de balise sur la page [Radio](#).
- **Type** : type d'appareil. Les options disponibles sont les suivantes :
 - **Point d'accès** : l'appareil non autorisé est un point d'accès qui prend en charge la structure IEEE 802.11 Wireless Networking Framework en mode Infrastructure.
 - **Ad hoc** : station non autorisée fonctionnant en mode Ad hoc. Le mode Ad hoc est une structure IEEE 802.11 Wireless Networking Framework, également appelée mode homologue à homologue ou un IBSS (Independent Basic Service Set).
- **SSID** : SSID (Service Set Identifier) de l'appareil WAP.
- **Confidentialité** : indique si un processus de sécurité est appliqué à l'appareil non autorisé. Les options disponibles sont les suivantes :
 - **Désactivé** : le mode de sécurité est désactivé (pas de sécurité).
 - **Activé** : le mode de sécurité est activé.
- **WPA** : spécifie si la sécurité WPA est activée ou désactivée pour le point d'accès non autorisé.
- **Bande** : mode IEEE 802.11 actuellement utilisé sur le point d'accès non autorisé, notamment IEEE 802.11a, IEEE 802.11b ou IEEE 802.11g.
Le numéro affiché indique le mode :
 - 2,4 indique le mode IEEE 802.11b, 802.11g ou 802.11n (ou une combinaison des modes).
 - 5 indique le mode IEEE 802.11a ou 802.11n (ou les deux modes).
- **Canal** : canal sur lequel le point d'accès non autorisé est en cours de diffusion.
- **Débit** : débit, en mégabits par seconde, auquel le point d'accès non autorisé transmet. Le débit actuel est toujours l'un des débits spécifiés dans le champ Débits pris en charge.
- **Signal** : puissance du signal radio qui émet depuis le point d'accès non autorisé. Si vous passez le pointeur de la souris sur les barres, un nombre représentant la puissance en décibels (dB) apparaît.
- **Balises** : nombre total de balises reçues du point d'accès non autorisé depuis sa première détection.
- **Dernière balise** : date et heure de la dernière balise reçue du point d'accès non autorisé.
- **Débits** : ensemble de débits de base (annoncés) et pris en charge pour le point d'accès non autorisé. Les débits sont affichés en mégabits par seconde (Mbit/s). Tous les débits pris en charge sont répertoriés ; les débits de base apparaissent en gras. Vous pouvez configurer les ensembles de débits sur la page [Radio](#).

Étape 4

Vérifiez la liste des points d'accès, puis cliquez sur **Déplacer vers la liste des points d'accès autorisés** afin de déplacer le point d'accès vers la **Liste des points d'accès autorisés**. Si le point d'accès se trouve dans la **Liste des points d'accès approuvés**, cliquez sur **Liste des points d'accès non autorisés détectés** pour déplacer le point d'accès vers la **Liste des points d'accès non autorisés détectés**.

Étape 5 Cliquez sur **Actualiser** pour actualiser l'écran et afficher les informations les plus récentes.

Enregistrement de la liste des points d'accès autorisés

Pour créer une liste des points d'accès autorisés et l'enregistrer dans un fichier :

- Étape 1** Sélectionnez **Sécurité**, puis cliquez sur **Afficher la liste des points d'accès non autorisés** dans la section **Détection des points d'accès non autorisés**. La page **Détection des points d'accès non autorisés** s'affiche.
- Étape 2** Dans la **Liste des points d'accès non autorisés détectés**, cliquez sur **Déplacer vers la liste des points d'accès approuvés** pour les points d'accès que vous connaissez. Les points d'accès approuvés sont déplacés vers la liste des points d'accès autorisés.
- Étape 3** Dans la zone **Télécharger/Enregistrer la liste des points d'accès approuvés**, cliquez sur **Enregistrer (point d'accès vers ordinateur)**.
- Étape 4** Cliquez sur **Enregistrer**.
- La liste contient les adresses MAC de tous les points d'accès qui ont été ajoutés à la liste des points d'accès connus. Par défaut, le nom du fichier est `Rogue2.cfg`. Vous pouvez utiliser un éditeur de texte ou un navigateur web pour ouvrir le fichier et afficher son contenu.
-

Importation d'une liste des points d'accès autorisés

Vous pouvez importer une liste de points d'accès connus à partir d'une liste enregistrée. Vous pouvez obtenir la liste depuis un autre point d'accès ou la créer à partir d'un fichier texte. Si l'adresse MAC d'un point d'accès apparaît dans la Liste des points d'accès approuvés, elle ne sera plus détectée comme non autorisée.

Pour importer une liste de points d'accès à partir d'un fichier :

- Étape 1** Sélectionnez **Sécurité > Détection de point d'accès non autorisé**.
- Étape 2** Dans la zone **Télécharger/Enregistrer la liste des points d'accès approuvés**, cliquez sur **Télécharger (Ordinateur vers point d'accès)**.
- Étape 3** Dans le champ **Nom du fichier source**, cliquez sur **Parcourir** pour sélectionner le fichier à importer.
- Le fichier importé doit être un fichier texte brut portant une extension `.txt` ou `.cfg`. Les entrées du fichier sont des adresses MAC au format hexadécimal, dont chaque octet est séparé par le signe deux points (par exemple, `00:11:22:33:44:55`). Vous devez séparer les entrées par un espace. Pour que le point d'accès accepte le fichier, il doit uniquement contenir des adresses MAC.
- Étape 4** Dans le champ **Destination de gestion de fichiers**, indiquez si vous souhaitez remplacer la liste des points d'accès approuvés ou ajouter les entrées du fichier importé à cette liste. Les options disponibles sont les suivantes :
- **Remplacer** : importe la liste et remplace le contenu de la liste des points d'accès connus.
 - **Fusionner** : importe la liste et ajoute les points d'accès du fichier importé aux points d'accès déjà présents dans la liste des points d'accès connus.
- Étape 5** Cliquez sur **Enregistrer**.

Une fois l'importation terminée, l'écran s'actualise et les adresses MAC des points d'accès du fichier importé apparaissent dans la liste des points d'accès connus.

Configurer la complexité des mots de passe

La page Complexité des mots de passe permet de modifier les exigences en matière de complexité des mots de passe utilisés pour accéder à l'utilitaire de configuration. Des mots de passe complexes augmentent la sécurité.

Pour configurer les exigences en matière de complexité des mots de passe, procédez de la façon suivante :

Étape 1 Sélectionnez **Sécurité > Configurer la complexité des mots de passe**.

Étape 2 Cochez la case **Activer** pour activer la complexité des mots de passe.

Étape 3 Définissez les paramètres suivants :

- **Nombre minimal de catégories de caractères dans le mot de passe** : saisissez le nombre minimal de catégories de caractères devant être représentées dans la chaîne de mot de passe. Les quatre classes de caractères possibles sont les lettres majuscules, les lettres minuscules, les chiffres et les caractères spéciaux disponibles sur un clavier standard.
- **Mot de passe différent du mot de passe actuel** : sélectionnez cette option afin de permettre aux utilisateurs de saisir un autre mot de passe lorsque leur mot de passe actuel arrive à expiration. Si vous ne sélectionnez pas cette option, les utilisateurs peuvent saisir à nouveau le même mot de passe une fois celui-ci arrivé à expiration.
- **Longueur maximale du mot de passe** : la longueur maximale du mot de passe est comprise entre 64 et 127 caractères. La valeur par défaut est 64.
- **Longueur minimale du mot de passe** : la longueur minimale du mot de passe est comprise entre 0 et 32 caractères. La valeur par défaut est 8.
- **Prise en charge de la durée de vie du mot de passe** : sélectionnez cette option pour que les mots de passe expirent après une période déterminée que vous configurez.
- **Délai d'expiration du mot de passe** : nombre de jours avant qu'un nouveau mot de passe n'expire. Cette valeur est comprise entre 1 et 365. La valeur par défaut est de 180 jours.

Étape 4 Cliquez sur **Enregistrer**. Les modifications sont enregistrées dans la configuration de démarrage.

Remarque Une fois le **Délai d'expiration du mot de passe** dépassé, vous devez accéder à la page [Modification du mot de passe](#).

Configurer la complexité WAP-PSK

Lorsque vous configurez les points d'accès virtuels (VAP) sur l'appareil WAP, vous pouvez sélectionner une méthode d'authentification sécurisée des clients. Si vous sélectionnez le protocole WPA personnel (également connu sous le nom de clé prépartagée WPA ou WPA-PSK) en guise de méthode de sécurité, vous pouvez

configurer la complexité sur la page Complexité WPA-PSK à utiliser dans le processus d'authentification. Des clés plus complexes offrent une sécurité accrue.

Pour configurer la complexité WPA-PSK :

Étape 1 Sélectionnez **Sécurité > Configurer la complexité WPA-PSK**.

Étape 2 Cochez la case **Activer** pour autoriser l'appareil WAP à vérifier que les clés WPA-PSK répondent aux critères configurés. Si vous désactivez cette option, aucun des paramètres configurés n'est utilisé. La complexité WPA-PSK est désactivée par défaut.

Étape 3 Définissez les paramètres suivants :

- **Nombre minimal de classes de caractères WPA-PSK** : nombre minimal de classes de caractères devant être représentées dans la chaîne de clé. Les quatre classes de caractères possibles sont les lettres majuscules, les lettres minuscules, les chiffres et les caractères spéciaux disponibles sur un clavier standard. La valeur par défaut est trois.
- **Clé WPA-PSK différente de la clé actuelle** : cochez la case **Activer** pour autoriser les utilisateurs à configurer une autre clé après l'expiration de leur clé actuelle. Si cette option est désactivée, les utilisateurs peuvent continuer à utiliser leur ancienne clé ou leur clé précédente lorsque leur clé actuelle arrive à expiration.
- **Longueur WPA-PSK maximale** : saisissez une valeur de longueur de clé. La longueur de clé maximale est comprise entre 32 et 63 caractères. La valeur par défaut est 63.
- **Longueur WPA-PSK minimale** : saisissez une valeur de longueur de clé. La longueur de clé minimale est comprise entre 8 et 16 caractères. La valeur par défaut est 8.

Étape 4 Cliquez sur **Enregistrer**.



CHAPITRE 3

Technologie sans fil

Ce chapitre explique comment configurer les propriétés de la radio sans fil. Elle contient les rubriques suivantes :

- [Radio](#), à la page 41
- [Réseaux](#), à la page 46
- [Filtre de client](#), à la page 54
- [Planificateur](#), à la page 56
- [QoS](#), à la page 57

Radio

La radio est la partie physique de l'appareil WAP qui crée un réseau sans fil. Les paramètres de la radio sur l'appareil WAP permettent de contrôler le comportement de la radio et de déterminer le type de signaux sans fil émis par le WAP.

Pour configurer les paramètres de la radio sans fil :

Étape 1 Sélectionnez **Réseau sans fil > Radio**.

Étape 2 Sélectionnez le mode de fonctionnement :

- **2,4 GHz uniquement** : prise en charge de la radio 2,4 GHz avec un mode 2x2 MIMO.
- **5 GHz uniquement** : prise en charge de la radio 5 GHz avec un mode 2x2 MIMO.
- **Bibande** : prise en charge des radios 2,4 GHz et 5 GHz avec deux chaînes 1x1 SISO.

Cette solution à circuit intégré unique permet d'utiliser la radio en mode 2x2 MIMO ou comme deux chaînes 1x1. Cela permet aux utilisateurs d'effectuer différentes tâches dans deux bandes distinctes ou dans les mêmes bandes (avec certaines restrictions) simultanément.

Étape 3 Dans la zone Paramètres de base, configurez les paramètres suivants pour l'interface radio sélectionnée :

Remarque Les réglementations locales peuvent interdire l'utilisation de certains modes radio. Les modes ne sont pas tous disponibles dans la totalité des pays.

- **Radio** : cochez la case **Activer** pour activer l'interface radio.

- **Mode de réseau sans fil** : standard IEEE 802.11 et fréquence utilisés par la radio. La valeur par défaut du mode est 802.11b/g/n pour la Radio 1 et 802.11a/n/ac pour la Radio 2. Pour chaque radio, sélectionnez l'un des modes disponibles.

2,4 GHz prend en charge les modes radio suivants :

- **802.11b/g** : les clients 802.11b et 802.11g peuvent se connecter à l'appareil WAP.
- **802.11b/g/n (par défaut)** : les clients 802.11b, 802.11g et 802.11n fonctionnant à la fréquence 2,4 GHz peuvent se connecter à l'appareil WAP.
- **802.11n 2,4 GHz** : seuls les clients 802.11n fonctionnant à la fréquence 2,4 GHz peuvent se connecter à l'appareil WAP.

5 GHz prend en charge les modes radio suivants :

- **802.11a** : seuls les clients 802.11a peuvent se connecter à l'appareil WAP.
 - **802.11a/n/ac** : les clients 802.11a, 802.11n et 802.11ac fonctionnant dans la fréquence 5 GHz peuvent se connecter à l'appareil WAP.
 - **802.11n/ac** : les clients 802.11n et 802.11ac fonctionnant dans la fréquence 5 GHz peuvent se connecter à l'appareil WAP.
- **Sélection de bande sans fil (modes 802.11n et 802.11ac uniquement)** : la spécification 802.11n autorise une bande coexistante de 20/40 MHz en plus de la bande 20 MHz héritée qui est disponible avec les autres modes. La bande 20/40 MHz offre des débits de données plus élevés, mais laisse moins de bandes à la disposition des autres appareils de 2,4 GHz et 5 GHz.

La spécification 802.11ac permet la présence d'une bande d'une largeur de 80 MHz en plus des bandes de 20 MHz et 40 MHz.

Définissez le champ à 20 MHz afin de restreindre l'utilisation de la bande passante sans fil à une bande de 20 MHz. En ce qui concerne le mode 802.11ac, définissez le champ à 40 MHz afin d'empêcher la radio d'utiliser la bande passante sans fil de 80 MHz.

- **Canal principal (modes 802.11n avec une bande passante de 20/40 MHz uniquement)** : on peut considérer qu'un canal de 40 MHz se compose de deux canaux de 20 MHz qui sont contigus dans le domaine de fréquence. On appelle souvent ces deux canaux de 20 MHz le canal principal et le canal secondaire. Le canal principal est utilisé pour les clients 802.11n qui prennent uniquement en charge une bande passante de canal de 20 MHz et pour les clients hérités.

Sélectionnez l'une des options suivantes :

- **Supérieur** : définit le canal principal en tant que canal de 20 MHz supérieur dans la bande de 40 MHz.
 - **Inférieur** : définit le canal principal en tant que canal de 20 MHz inférieur dans la bande de 40 MHz. Lower est la sélection par défaut.
- **Canal** : partie du spectre radio utilisée par la radio pour la transmission et la réception.

La plage des canaux disponibles est déterminée par le mode de l'interface radio et le paramètre de code de pays. Si vous sélectionnez Auto pour le paramètre de canal, l'appareil WAP recherche les canaux disponibles et sélectionne le canal ayant le moins de trafic.

Chaque mode offre plusieurs canaux en fonction du spectre attribué sous licence par les autorités nationales et internationales, telles que la Federal Communications Commission (FCC) ou la International Telecommunication Union (ITU-R).

- **Planificateur** : pour l'interface radio, sélectionnez le profil dans la liste.

Étape 4 Dans la zone Paramètres avancés, définissez les paramètres suivants :

- **Intervalle de sûreté court pris en charge** : ce champ est uniquement disponible si le mode radio sélectionné inclut 802.11n. L'intervalle de sûreté est le temps mort, en nanosecondes, entre les symboles OFDM. L'intervalle de sûreté empêche les interférences ISI (Inter-Symbol Interference) et ICI (Inter-Carrier Interference). Le mode 802.11n permet dans cet intervalle de sûreté de diminuer la définition a et g de 800 nanosecondes à 400 nanosecondes. La diminution de l'intervalle de sûreté peut entraîner une amélioration de 10 % du débit de données. Le client avec lequel l'appareil WAP communique doit aussi prendre en charge l'intervalle de sûreté court.

Sélectionnez l'une des options suivantes :

- **Oui** : l'appareil WAP transmet les données avec un intervalle de garde de 400 nanosecondes lorsqu'il communique avec des clients qui prennent aussi en charge l'intervalle de sûreté court. Il s'agit de la sélection par défaut.
 - **Non** : l'appareil WAP transmet les données avec un intervalle de sûreté de 800 nanosecondes.
- **Protection** : la fonction de protection contient les règles garantissant que les transmissions 802.11 ne créent pas d'interférences avec les stations ou applications héritées. Par défaut, la protection est activée (Auto). Lorsque la protection est activée, celle-ci est appelée si les appareils hérités se trouvent à portée de l'appareil WAP.

Vous pouvez désactiver la protection ; cependant, les clients hérités ou les appareils WAP à portée peuvent être affectés par les transmissions 802.11n. La protection est également disponible lorsque le mode est 802.11b/g. Si la protection est activée dans ce mode, elle protège les clients 802.11b et les appareils WAP contre les transmissions 802.11g.

Remarque Ce paramètre n'empêche pas le client de s'associer à l'appareil WAP.

- **Intervalle de balise** : intervalle entre la transmission des trames de balise. L'appareil WAP transmet ces trames à intervalles réguliers pour annoncer l'existence du réseau sans fil. Le comportement par défaut consiste à envoyer une trame de balise toutes les 100 millisecondes (ou 10 par seconde). Saisissez un entier compris entre 20 et 2 000 millisecondes. La valeur par défaut est 100 millisecondes.
- **Période DTIM** : période DTIM (Delivery Traffic Information Map). Saisissez un entier compris entre 1 et 255 balises. La valeur par défaut est 2 balises.

Le message DTIM est un élément inclus dans certaines trames de balise. Il indique les stations clientes actuellement en mode faible consommation, qui ont des données mises en mémoire tampon sur l'appareil WAP en attente de sélection.

La période DTIM indique la fréquence à laquelle les clients servis par cet appareil WAP doivent rechercher les données mises en mémoire tampon en attente de sélection.

La mesure s'effectue en balises. Par exemple, si vous définissez ce champ sur 1, les clients recherchent les données mises en mémoire tampon sur l'appareil WAP à chaque balise. Si vous définissez ce champ sur 10, les clients effectuent leur recherche toutes les 10 balises.

- **Seuil de fragmentation** : seuil de la taille de trame, en octets. La valeur doit être un nombre entier pair compris entre 256 et 2 346. La valeur par défaut est 2346.

Le seuil de fragmentation est un moyen de limiter la taille des paquets (trames) transmis sur le réseau. Si un paquet dépasse le seuil de fragmentation défini, la fragmentation est activée et le paquet est envoyé sous forme de plusieurs trames 802.11.

Si le paquet transmis est égal ou inférieur au seuil, la fragmentation n'est pas utilisée. La définition du seuil à la valeur la plus élevée (2 346 octets, qui est la valeur par défaut) désactive effectivement la fragmentation.

Par défaut, la fragmentation est désactivée. Nous vous conseillons de ne pas utiliser la fragmentation, à moins que vous ne suspectiez des interférences radio. Les en-têtes supplémentaires appliqués à chaque fragment augmentent la charge de traitement sur le réseau et peuvent réduire significativement le débit.

- **Seuil RTS** : valeur de seuil Request to Send (RTS). La valeur doit être un nombre entier compris entre 0 et 65 535. La valeur par défaut est 65 535 octets.

Le seuil RTS indique le nombre d'octets dans un MPDU au-dessous duquel aucune liaison RTS/CTS n'est établie.

La modification du seuil RTS peut vous aider à contrôler le flux de trafic via l'appareil WAP. Si vous spécifiez une valeur de seuil faible, les paquets RTS sont envoyés plus fréquemment, ce qui consomme davantage de bande passante et réduit le débit du paquet. Cependant, l'envoi d'un plus grand nombre de paquets RTS peut permettre le rétablissement du réseau suite à des interférences ou des collisions susceptibles de se produire sur un réseau chargé ou sur un réseau rencontrant des interférences électromagnétiques.

- **Nombre max. de clients associés** : nombre maximal de stations autorisées à accéder à l'appareil WAP à tout moment. Vous pouvez saisir un nombre entier compris entre 0 et 100. La valeur par défaut est 100 stations.
- **Puissance de transmission** : valeur en pourcentage du niveau de puissance de transmission pour l'appareil WAP.

La valeur par défaut de Maximal - 100 % peut être plus économique qu'un pourcentage inférieur, car elle donne à l'appareil WAP une plage de diffusion maximale et réduit le nombre de points d'accès requis.

Pour accroître la capacité du réseau, rapprochez les appareils WAP les uns des autres et diminuez la valeur de puissance de transmission. Vous réduisez ainsi le chevauchement et les interférences entre les points d'accès. Une puissance de transmission plus basse permet également de sécuriser davantage votre réseau, car des signaux sans fil plus faibles sont moins susceptibles de se propager à l'extérieur de l'emplacement physique de votre réseau.

Certaines combinaisons de plages de canaux et de code de pays ont une puissance de transmission maximale relativement basse. Si vous essayez de définir la puissance de transmission sur des plages plus basses (par exemple, 25 % ou Minimale - 12 %), la baisse de puissance attendue est susceptible de ne pas se produire, car certains amplificateurs de puissance doivent respecter une puissance de transmission minimale.

- **Prise en charge de la rafale de trames** : d'une manière générale, l'activation de la prise en charge des rafales de trames permet d'améliorer les performances radio en aval.
- **Mode Rééquilibrage du temps réseau (Airtime Fairness)** : la fonction ATF (Airtime Fairness) a été mise en place pour résoudre les problèmes de ralentissement des transferts de données, qui limitent les transferts rapides.
- **Seuil d'utilisation maximal** : saisissez le pourcentage d'utilisation de la bande passante réseau autorisé sur la radio avant que l'appareil WAP ne cesse d'accepter de nouvelles associations de clients. La plage de nombres entiers valide est comprise entre 0 et 100 pour cent. La valeur par défaut est 0 pour cent. Si elle est définie sur 0, toutes les nouvelles associations sont autorisées, quel que soit le taux d'utilisation.
- **Taux de multidiffusion fixe** : vitesse de transmission, en Mbit/s, pour les paquets de diffusion et de multidiffusion. Ce paramètre peut être utile dans un environnement offrant une lecture vidéo à multidiffusion sans fil, pourvu que les clients sans fil prennent en charge le débit configuré.

Lorsque vous sélectionnez **Auto**, l'appareil WAP choisit le meilleur débit pour les clients associés. La plage de valeurs valides est déterminée par le mode radio configuré.

- **Ensembles de débits existants** : les débits sont exprimés en mégabits par seconde.

Les ensembles de débits existants indiquent les débits pris en charge par l'appareil WAP. Vous pouvez sélectionner plusieurs débits. L'appareil WAP choisit automatiquement le débit le plus efficace en fonction de facteurs comme les taux d'erreur et la distance à laquelle les stations clientes se trouvent de l'appareil WAP.

Les ensembles de débits de base indiquent les débits annoncés au réseau par l'appareil WAP, de façon à établir la communication avec les autres points d'accès et stations clientes du réseau. Il est généralement plus efficace d'avoir un appareil WAP qui diffuse un sous-ensemble de ses ensembles de débits pris en charge.

- **Limites de débit de diffusion/multidiffusion** : la limite du débit de diffusion et multidiffusion peut augmenter la performance globale du réseau en limitant le nombre de paquets transmis sur le réseau.

Par défaut, cette fonction est désactivée. Tant que vous n'activez pas cette fonction, les champs suivants sont désactivés :

- **Limite de débit** : limite de débit pour le trafic de diffusion et multidiffusion. La limite doit être supérieure à 1, mais inférieure à 50 paquets par seconde. Tout le trafic inférieur à cette limite de débit est conforme et est toujours transmis vers la destination appropriée. Le paramètre de limite de débit par défaut et maximale est de 50 paquets par seconde.
- **Rafale de limite de débit** : volume de trafic, mesuré en octets, autorisé à transiter sous forme de rafale temporaire même s'il dépasse le débit maximal défini. Le paramètre de rafale de limite de débit par défaut et maximale est de 75 paquets par seconde.
- **Fonctionnalités de très haut débit** : l'objectif de cette fonction est d'activer ou de désactiver les extensions propres à Broadcom dans le très haut débit pour les liaisons Broadcom à Broadcom. La fonctionnalité de très haut débit prend en charge les très hauts débits 256 QAM non spécifiés par le standard 802.11 ac. Les débits sont les suivants : mode LDPC très haut débit, MCS 9 Nss 1 20 Mhz, MCS 9 Nss 2 20 Mhz, MCS 6 Nss 3 80 Mhz. La fonctionnalité de très haut débit est prise en charge par PHY 802.11 ac.

Étape 5

Cliquez sur **Configurer TSPEC**, puis définissez les paramètres suivants :

- **Intervalle de violation TSPEC** : dans ce champ, spécifiez la durée, en secondes, pendant laquelle l'appareil WAP doit consigner les clients associés qui ne respectent pas les procédures de contrôle d'admission obligatoires. La consignation s'effectue via le journal système et les déroutements SNMP. Saisissez une durée comprise entre 0 et 900 secondes. La valeur par défaut est de 300 secondes.
- **Mode TSPEC** : régule le mode TSPEC global sur l'appareil WAP. Par défaut, le mode TSPEC est désactivé. Les options disponibles sont les suivantes :
 - **Activé** : l'appareil WAP traite les demandes TSPEC en fonction des paramètres TSPEC définis sur la page Radio.
 - **Désactivé** : l'appareil WAP ignore les demandes TSPEC des stations clientes.
- **Mode ACM voix TSPEC** : régule le contrôle d'admission obligatoire (ACM) pour la catégorie d'accès vocal. Par défaut, le mode TSPEC Voice ACM est désactivé. Les options disponibles sont les suivantes :
 - **Activé** : une station doit envoyer une demande TSPEC de bande passante à l'appareil WAP avant d'envoyer ou de recevoir un flux de trafic vocal. L'appareil WAP répond avec le résultat de la demande, qui inclut le temps moyen alloué si la TSPEC a été autorisée.
 - **Désactivé** : une station peut envoyer et recevoir le trafic vocal prioritaire sans demander une TSPEC autorisée. L'appareil WAP ignore les demandes TSPEC vocales des stations clientes.

- **Limite ACM voix TSPEC** : limite supérieure du volume de trafic que l'appareil WAP tente de transmettre sur le support sans fil via un contrôle d'autorisation vocal pour obtenir l'accès. La limite par défaut est de 20 p% du trafic total.
- **Mode ACM vidéo TSPEC** : régule le contrôle d'admission obligatoire pour la catégorie d'accès vidéo. Par défaut, le mode TSPEC Video ACM est désactivé. Les options disponibles sont les suivantes :
 - **Activé** : une station doit envoyer une demande TSPEC de bande passante à l'appareil WAP avant d'envoyer ou de recevoir un flux de trafic vidéo. L'appareil WAP répond avec le résultat de la demande, qui inclut le temps moyen alloué si la TSPEC a été autorisée.
 - **Désactivé** : une station peut envoyer et recevoir le trafic de priorité vidéo sans nécessiter de TSPEC autorisée ; l'appareil WAP ignore les demandes TSPEC vidéo des stations clientes.
- **Limite ACM vidéo TSPEC** : limite supérieure du volume de trafic que l'appareil WAP tente de transmettre sur le support sans fil via un contrôle d'autorisation vidéo pour obtenir l'accès. La limite par défaut est de 15 p% du trafic total.
- **Délai d'inactivité du point d'accès TSPEC** : durée nécessaire à un appareil WAP pour détecter une spécification inactive de trafic descendant avant de la supprimer. La plage de nombres entiers valides est comprise entre 0 et 120 secondes. La valeur par défaut est 30 secondes.
- **Délai d'inactivité de la station TSPEC** : durée nécessaire à un appareil WAP pour détecter une spécification inactive de trafic montant avant de la supprimer. La plage de nombres entiers valides est comprise entre 0 et 120 secondes. La valeur par défaut est 30 secondes.
- **Mode de mappage de files d'attente WMM TSPEC** : cochez la case Activer pour activer l'interaction du trafic hérité dans les files d'attente fonctionnant comme ACM. Par défaut, ce mode est désactivé.

Étape 6 Cliquez sur **OK**, puis sur **Enregistrer**.

Réseaux

Les points d'accès virtuels (VAP) segmentent le réseau local sans fil en plusieurs domaines de diffusion qui constituent l'équivalent sans fil des VLAN Ethernet. Les VAP simulent plusieurs points d'accès dans un seul appareil WAP physique. Cet appareil WAP Cisco prend en charge un maximum de quatre VAP.

Chaque VAP peut être activé ou désactivé indépendamment, à l'exception du VAP0. Le VAP0 est l'interface radio physique et reste activé tant que la radio est activée. Pour désactiver le VAP0, la radio elle-même doit être désactivée.

Chaque VAP est identifié par un SSID (Service Set Identifier) configuré par l'utilisateur. Plusieurs VAP ne peuvent pas avoir le même nom SSID. Les diffusions SSID peuvent être activées ou désactivées indépendamment sur chaque VAP. La diffusion SSID est activée par défaut.

Conventions d'affectation de noms SSID

Le SSID par défaut de VAP0 est **ciscosb**. Chaque VAP supplémentaire créé a un nom SSID vierge. Les SSID de tous les VAP peuvent être définis sur d'autres valeurs. Le SSID peut être n'importe quelle entrée alphanumérique sensible à la casse constituée de 2 à 32 caractères.

Les caractères autorisés sont les suivants :

- ASCII 0x20 à 0x7E.
- Les espaces au début et à la fin (ASCII 0x20) ne sont pas autorisés.

**Remarque**

Cela signifie que les espaces sont autorisés dans le SSID, mais pas comme premier ou dernier caractère. Le point « . » (ASCII 0x2E) est aussi autorisé.

ID VLAN

Chaque VAP est associé à un VLAN, qui est identifié par un ID de VLAN (VID). Un VID peut avoir n'importe quelle valeur comprise entre 1 et 4 094. Cet appareil WAP Cisco prend en charge neuf VLAN actifs (huit pour le WLAN, plus un VLAN de gestion).

Par défaut, le VID attribué à l'utilitaire de configuration pour l'appareil WAP est 1, qui est aussi le VID non balisé par défaut. Si le VID de gestion est le même que le VID attribué à un VAP, les clients WLAN associés à ce VAP spécifique peuvent administrer l'appareil WAP. Si nécessaire, une liste de contrôle d'accès (ACL) peut être créée pour désactiver l'administration depuis les clients WLAN.

Configuration des VAP

Pour configurer les VAP :

-
- Étape 1** Sélectionnez **Réseau sans fil > Réseaux**.
- Étape 2** Dans le champ Radio, cliquez sur l'interface radio (**Radio 1** ou **Radio 2**) à laquelle les paramètres de configuration du VAP sont appliqués.
- Étape 3** Si VAP0 est le seul VAP configuré sur le système et que vous souhaitez ajouter un VAP, cliquez sur . Sélectionnez ensuite le VAP.
- Étape 4** Configurez les options suivantes :
- **ID de VLAN** : spécifiez l'ID de VLAN du réseau VLAN à associer au VAP.
Veillez à saisir un ID de VLAN correctement configuré sur le réseau. Des problèmes réseau peuvent survenir si le VAP associe des clients sans fil dont le VLAN n'est pas configuré correctement.
Si un client sans fil se connecte à l'appareil WAP par l'intermédiaire de ce VAP, l'appareil WAP balise tout le trafic à partir du client sans fil avec l'ID de VLAN configuré, sauf si vous saisissez l'ID de VLAN du port ou que vous utilisez un serveur RADIUS pour attribuer un client sans fil à un VLAN. La plage de l'ID de VLAN est comprise entre 1 et 4094.
Si vous définissez l'ID de VLAN sur un autre ID que l'ID de VLAN de gestion actuel, les clients WLAN associés à ce VAP spécifique ne pourront pas administrer l'appareil. Vous pouvez vérifier la configuration des ID de VLAN non balisés et de gestion sur la page du réseau local (LAN). Pour plus d'informations, reportez-vous à la section [Configuration IPv4](#), à la page 11.
 - **Nom SSID** : saisissez le nom du réseau sans fil. Le SSID est une chaîne alphanumérique constituée de 32 caractères maximum. Choisissez un SSID unique pour chaque VAP.
Si vous êtes connecté en tant que client sans fil au à l'appareil WAP que vous administrez, la réinitialisation du SSID entraînera une perte de connexion à l'appareil WAP. Vous devrez vous reconnecter au nouveau SSID une fois cette nouvelle configuration enregistrée.

- **Diffusion SSID** : active et désactive la diffusion du SSID.

Indiquez si vous souhaitez autoriser l'appareil WAP à diffuser le SSID dans ses trames de balise. Le paramètre Broadcast SSID est activé par défaut. Lorsque le VAP ne diffuse pas son SSID, le nom réseau n'apparaît pas dans la liste des réseaux disponibles sur une station cliente. Vous devez donc saisir manuellement le nom réseau exact dans l'utilitaire de connexion sans fil sur le client, afin de permettre l'établissement de la connexion.

La désactivation du SSID de diffusion est suffisante pour empêcher les clients de se connecter accidentellement à votre réseau, mais celle-ci n'empêche aucunement la plus simple des tentatives d'un pirate informatique de se connecter ou de surveiller le trafic déchiffré. La suppression de la diffusion SSID offre un niveau de protection très bas sur un réseau autrement exposé (comme un réseau d'invité) où la priorité est de permettre aux clients d'obtenir une connexion et où aucune information sensible n'est disponible.

WMF : le transfert de multidiffusion sans fil est un moyen efficace de transférer le trafic de multidiffusion sur l'appareil sans fil et de résoudre les problèmes de transmission de multidiffusion sur le WLAN à l'aide des trames de monodiffusion ou de multidiffusion répétées.

- **Sécurité** : sélectionnez le type d'authentification requis pour l'accès au VAP. Les options disponibles sont les suivantes :
 - Aucun(e)
 - WEP statique
 - WPA personnel
 - WPA entreprise

Si vous sélectionnez un autre mode de sécurité que Aucun(e), des champs supplémentaires s'affichent. Pour plus d'informations sur la configuration des paramètres de sécurité sans fil, reportez-vous à la section [Configuration des paramètres de sécurité](#).

Nous vous conseillons d'utiliser WPA Personal ou WPA Enterprise comme type d'authentification, car ils offrent une sécurité plus élevée.

Remarque L'option WEP statique peut être utilisée pour les ordinateurs ou appareils sans fil qui ne prennent pas en charge WPA personnel et WPA entreprise. Pour définir la sécurité avec l'option WEP statique, configurez la radio sur le mode 802.11a ou 802.11b/g. Le mode 802.11n restreint l'utilisation du mode de sécurité WEP statique.

- **Filtre de client** : indique si les stations qui peuvent accéder à ce VAP sont limitées à une liste globale configurée d'adresses MAC. Vous pouvez sélectionner l'un des types de filtres de client suivants :
 - **Désactivé** : aucun filtre de client n'est utilisé.
 - **Local** : vous utilisez la liste d'authentification MAC que vous configurez sur la page Filtre de client.
 - **RADIUS** : vous utilisez la liste d'authentification MAC sur un serveur RADIUS externe.
- **Isolation des canaux** : sélectionnez ce paramètre pour activer l'isolation des canaux.

Lorsque ce paramètre est désactivé, les clients sans fil peuvent communiquer entre eux normalement en envoyant le trafic via l'appareil WAP.

Lorsque ce paramètre est activé, l'appareil WAP bloque les communications entre les clients sans fil situés sur le même VAP. L'appareil WAP autorise toujours le trafic de données entre ses clients sans fil et les appareils filaires.

du réseau, via une liaison WDS, et avec les autres clients sans fil associés à un autre VAP, mais pas au sein même des clients sans fil.

- **Guidage de bandes** : sélectionnez ce paramètre pour activer le guidage de bandes lorsque les deux radios sont actives. Cette option utilise de manière efficace la bande de 5 GHz en guidant les clients bibandes pris en charge depuis la bande de 2,4 GHz vers la bande de 5 GHz.
 - Elle est configurée pour chaque VAP et doit être activée sur les deux radios.
 - Elle n'est pas recommandée sur les VAP avec trafic vocal ou vidéo sensible au temps.
 - Elle ne prend pas en considération la bande passante d'ordre n de la radio. Même si la radio 5 GHz utilise la bande passante de 20 MHz, cette option tente de guider les clients vers cette radio.
- **Planificateur** : sélectionnez un profil de planificateur dans la liste ; il est impossible d'associer VAP0 à un profil de planificateur.
- **Instance d'accès invité** : associez une instance de portail captif à un VAP. Les paramètres de l'instance de portail captif associée s'appliquent aux utilisateurs qui tentent de s'authentifier sur le point d'accès virtuel. Sélectionnez le nom d'instance pour chaque point d'accès virtuel auquel vous souhaitez associer une instance.

Remarque Il est possible d'associer un VAP à une instance d'accès invité dans la page **Contrôle d'accès > Accès invité**. Vous devez tout d'abord configurer l'**Instance d'accès invité**.

Étape 5 Cliquez sur **Enregistrer**.

Avertissement Une fois les nouveaux paramètres enregistrés, les processus correspondants peuvent être arrêtés et redémarrés. Si tel est le cas, l'appareil WAP risque d'être privé de connectivité. Il est recommandé de modifier les paramètres de l'appareil WAP à ce moment-là.

Remarque Pour supprimer un VAP, sélectionnez-le, puis cliquez sur **Supprimer**. Pour modifier un VAP, sélectionnez-le, puis cliquez sur **Modifier**. Pour enregistrer vos modifications, cliquez sur **Enregistrer** lorsque vous avez terminé.

Configuration des paramètres de sécurité

Cette section décrit les paramètres de sécurité pouvant être configurés sur l'appareil WAP sur la page Réseaux. Trois paramètres de sécurité sont disponibles : Aucun(e), WPA personnel et WPA entreprise.

Aucun(e)

Si vous sélectionnez **Aucun(e)** en guise de mode de sécurité, il n'est pas nécessaire de définir de paramètres de sécurité supplémentaires sur l'appareil. Ce mode signifie que toutes les données transférées de et vers l'appareil WAP ne sont pas chiffrées. Ce mode de sécurité peut être utile lors de la configuration initiale du réseau pour la résolution des problèmes, mais il n'est pas recommandé pour une utilisation régulière sur le réseau interne, car il n'offre pas la sécurité nécessaire.

WEP statique

Wired Equivalent Privacy (WEP) est un protocole de cryptage de données destiné aux réseaux sans fil 802.11. Tous les points d'accès et stations sans fil du réseau sont configurés avec une clé partagée statique 64 bits (clé

secrète 40 bits + vecteur d'initialisation 24 bits (IV)) ou 128 bits (clé secrète 104 bits + clé partagée 24 bits (IV) pour le cryptage des données.

Static WEP n'est pas le mode offrant le plus de sécurité, mais il fournit davantage de protection que le mode None (Plain-text), puisqu'il empêche un utilisateur externe de facilement détecter le trafic sans fil non chiffré.

WEP chiffre les données transmises sur le réseau sans fil à partir d'une clé statique. L'algorithme de cryptage est un cryptage de flux appelé RC4.

Les paramètres suivants vous permettent de configurer le mode WEP statique :

- **Index de clé de transfert** : saisissez une liste d'index de clé. Les index de clé 1 à 4 sont disponibles. La valeur par défaut est 1. Transfer Key Index indique la clé WEP utilisée par l'appareil WAP pour crypter les données qu'il transmet.
- **Longueur de clé** : sélectionnez une longueur de clé de 64 bits ou de 128 bits.
- **Type de clé** : sélectionnez le type de clé, à savoir ASCII ou Hexa.
- **Clés WEP** : vous pouvez spécifier jusqu'à quatre clés WEP. Dans chaque zone de texte, saisissez une chaîne de caractères pour chaque clé. Les clés que vous saisissez dépendent du type de clé sélectionné :
 - **ASCII** : inclut les lettres majuscules et minuscules, les chiffres, et les caractères spéciaux comme @ et #.
 - **Hexa** : inclut les chiffres 0 à 9 et les lettres A à F.
- Utilisez le même nombre de caractères pour chaque clé, comme spécifié dans le champ **Caractères requis**. Il s'agit des clés WEP RC4 partagées avec les stations par l'intermédiaire de l'appareil WAP. Chaque station cliente doit être configurée pour utiliser l'une de ces mêmes clés WEP, dans le même logement que celui spécifié sur l'appareil WAP.
- **Authentification 802.1X** : l'algorithme d'authentification définit la méthode utilisée pour déterminer si un poste client est autorisé à s'associer à un appareil WAP lorsque le mode de sécurité WEP statique est sélectionné.
- Spécifiez l'algorithme d'authentification que vous souhaitez utiliser en choisissant l'une des options suivantes :
 - Système ouvert permet à n'importe quelle station cliente de s'associer à l'appareil WAP, peu importe si cette station cliente dispose de la clé WEP correcte. Cet algorithme est aussi utilisé en mode texte brut, IEEE802.1X et WPA. Lorsque l'algorithme d'authentification est défini sur Système ouvert, tout client peut s'associer à l'appareil WAP.



Remarque Même si une station cliente est autorisée à s'associer, cela ne signifie pas qu'elle pourra systématiquement échanger des données avec un appareil WAP. Une station doit disposer de la clé WEP correcte pour pouvoir accéder à l'appareil WAP et décrypter ses données, mais aussi pour transmettre des données lisibles à celui-ci.

- Clé partagée nécessite que la station cliente dispose de la clé WEP correcte pour s'associer à l'appareil WAP. Lorsque l'algorithme d'authentification est défini sur Clé partagée, une station ayant une clé WEP incorrecte ne peut pas s'associer à l'appareil WAP.

- Système ouvert et Clé partagée. Si vous sélectionnez les deux algorithmes d'authentification, les stations clientes configurées pour utiliser le WEP en mode Clé partagée doivent disposer d'une clé WEP valide pour s'associer à l'appareil WAP. En outre, les stations clientes configurées pour utiliser le WEP en mode Système ouvert (mode Clé partagée désactivé) peuvent s'associer à l'appareil WAP même si elles ne disposent pas de la clé WEP correcte.

Règles du mode Static WEP

Si vous utilisez WEP statique, les règles suivantes s'appliquent :

- Sur toutes les stations clientes, la sécurité Réseau local sans fil (WLAN) doit être définie sur WEP ; par ailleurs, tous les clients doivent disposer de l'une des clés WEP spécifiées sur l'appareil WAP pour pouvoir décoder les transmissions de données du point d'accès vers la station.
- l'appareil WAP doit disposer de toutes les clés utilisées par les clients pour les transmissions de la station vers le point d'accès, afin de pouvoir décoder les transmissions de la station.
- La même clé doit occuper le même logement sur tous les nœuds (point d'accès et clients). Par exemple, si l'appareil WAP définit la clé abc123 comme clé WEP 3, les stations clientes doivent définir cette même chaîne comme clé WEP 3.
- Les stations clientes peuvent utiliser différentes clés pour transmettre des données au point d'accès. (Elles peuvent aussi toutes utiliser la même clé, mais cela s'avère moins sûr, car cela signifie qu'une station peut décrypter les données envoyées par une autre.)
- Sur certains logiciels de clients sans fil, vous pouvez configurer plusieurs clés WEP et définir un index de clé de transfert de station cliente, puis définir les stations afin de crypter les données qu'elles transmettent par l'intermédiaire de différentes clés. Cela permet de s'assurer que les points d'accès situés à proximité ne pourront pas décoder les transmissions des autres points d'accès.
- Vous ne pouvez pas placer à la fois des clés WEP 64 bits et 128 bits entre le point d'accès et ses stations clientes.

WPA personnel

WPA personnel est un standard IEEE 802.11i Wi-Fi Alliance qui inclut le cryptage AES-CCMP et TKIP. WPA personnel utilise une clé prépartagée (PSK) au lieu de IEEE 802.1X et EAP comme dans le mode de sécurité WPA entreprise. Le PSK est uniquement utilisé pour le contrôle initial des informations d'identification. WPA Personal est également appelé WPA-PSK.

Ce mode de sécurité est rétrocompatible pour les clients sans fil qui prennent en charge le WPA d'origine.

Pour configurer WPA personnel, définissez les paramètres suivants :

- **Versions des points d'accès sans fil** : sélectionnez les types de stations clientes parmi les suivantes :
 - **WPA-TKIP** : ce réseau intègre des stations clientes qui prennent en charge uniquement le WPA d'origine, ainsi que le protocole de sécurité TKIP. Notez qu'il est impossible de sélectionner uniquement WPA-TKIP conformément aux dernières exigences de la Wi-Fi Alliance.
 - **WPA2-AES** : toutes les stations clientes du réseau prennent en charge la version WPA2, ainsi que le protocole de cryptage et de sécurité AES-CCMP. Cette version fournit une sécurité optimale avec le standard IEEE 802.11i. Conformément aux dernières exigences de la Wi-Fi Alliance, le point d'accès doit prendre en charge ce mode en permanence.

Si le réseau intègre un mélange de clients, certains prenant en charge le WPA2 et d'autres prenant uniquement en charge le WPA d'origine, activez ces deux options. Les stations clientes WPA et WPA2 peuvent ainsi s'associer et s'authentifier, mais peuvent aussi utiliser le WPA2 (plus robuste) pour les clients qui le prennent en charge. Cette configuration WPA offre davantage d'interopérabilité et un peu moins de sécurité.

Les clients WPA doivent disposer de l'une des clés ci-dessous pour pouvoir s'associer à l'appareil WAP :

- Une clé TKIP valide
- Une clé AES-CCMP valide

- **PMF (Protection Management Frame)** : assure la sécurité des trames de gestion 802.11 non chiffrées. Lorsque le mode de sécurité est désactivé, l'option PMF est définie sur Pas de PMF et ne peut pas être modifiée (elle est masquée ou grisée). Lorsque le mode de sécurité est défini sur WPA2-xxx, l'option PMF est par défaut définie sur Compatible et peut être modifiée. Vous pouvez ainsi configurer les trois valeurs suivantes.

- **Non requis**
- **Compatible**
- **Obligatoire**



Remarque La Wi-Fi Alliance exige l'activation de l'option PMF, qui doit être définie par défaut sur Compatible. Vous pouvez désactiver cette option lorsque les clients sans fil non conformes sont instables ou présentent des problèmes de connectivité.

- **Clé** : clé secrète partagée pour la sécurité WPA personnel. Saisissez une chaîne de 8 caractères minimum et de 63 caractères maximum. Les caractères acceptés sont les lettres alphabétiques majuscules et minuscules, les chiffres numériques et les symboles spéciaux comme @ et #.
- **Afficher le mot de passe en texte clair** : lorsque cette option est activée, le texte que vous saisissez est visible. Si cette option est désactivée, le texte n'est pas masqué lors de sa saisie.
- **Mesure de la fiabilité de la clé** : l'appareil WAP contrôle la clé sur la base de critères de complexité comme le nombre de types de caractères différents utilisés (lettres alphabétiques majuscules et minuscules, nombres et caractères spéciaux), mais vérifie également la longueur de la clé. Lorsque la fonction de contrôle de la complexité WPA-PSK est activée, la clé n'est pas acceptée si elle ne respecte pas les critères minimaux. Pour obtenir des informations sur la configuration du contrôle de la complexité, reportez-vous à la section [Configurer la complexité WAP-PSK, à la page 38](#).
- **Taux d'actualisation de la clé de diffusion** : intervalle auquel la clé (groupe) de diffusion est actualisée pour les clients associés à ce VAP. La valeur par défaut est 86 400 secondes et la plage valide est comprise entre 0 et 86 400 secondes. La valeur 0 indique que la clé de diffusion n'est pas actualisée.

WPA entreprise

WPA entreprise avec RADIUS est une implémentation de le standard IEEE 802.11i Wi-Fi Alliance, qui inclut le cryptage CCMP (AES) et TKIP. Le mode Entreprise nécessite l'utilisation d'un serveur RADIUS pour l'authentification des utilisateurs.

Ce mode de sécurité est rétrocompatible avec les clients sans fil qui prennent en charge le WPA d'origine.

Activé par défaut, le mode VLAN dynamique permet au serveur d'authentification RADIUS de sélectionner le réseau VLAN utilisé pour les stations.

Les paramètres ci-après permettent de configurer WPA entreprise :

- **Versions des points d'accès sans fil** : sélectionnez les types de stations clientes à prendre en charge. Les options disponibles sont les suivantes :
 - **WPA-TKIP** : le réseau intègre des stations clientes qui prennent en charge uniquement le WPA d'origine, ainsi que le protocole de sécurité TKIP. Notez qu'il est impossible de sélectionner uniquement WPA-TKIP pour le point d'accès conformément aux dernières exigences de la Wi-Fi Alliance.
 - **WPA2-AES** : toutes les stations clientes du réseau prennent en charge la version WPA2, ainsi que le protocole de cryptage et de sécurité AES-CCMP. Cette option fournit une sécurité optimale avec le standard IEEE 802.11i. Conformément aux dernières exigences de la Wi-Fi Alliance, le point d'accès doit prendre en charge ce mode en permanence.
- **Activer la pré-authentification** : si vous sélectionnez uniquement WPA2, ou à la fois WPA et WPA2 pour l'option Versions des points d'accès sans fil, vous pouvez activer la pré-authentification pour les clients WPA2.

Activez cette option si vous souhaitez que les clients sans fil WPA2 puissent envoyer des paquets de pré-authentification. Les informations de pré-authentification sont relayées de l'appareil WAP que le client utilise actuellement vers l'appareil WAP cible. L'activation de cette fonction permet d'accélérer l'authentification pour les clients en itinérance qui se connectent à plusieurs points d'accès.

Cette option ne s'applique pas si vous avez sélectionné WPA pour l'option Versions des points d'accès sans fil, car le WPA d'origine ne prend pas en charge cette fonction.

Les stations clientes configurées pour utiliser WPA avec RADIUS doivent posséder l'une des adresses et clés suivantes :

- Une adresse IP RADIUS TKIP et une clé RADIUS valides
 - Une adresse IP CCMP (AES) et une clé RADIUS valides
- **PMF (Protection Management Frame)** : assure la sécurité des trames de gestion 802.11 non chiffrées. Lorsque le mode de sécurité est défini sur Désactivé ou sur WEP, l'option PMF est définie sur **Pas de PMF** et ne peut pas être modifiée (elle est masquée ou grisée). Lorsque le mode de sécurité est défini sur **WPA2-xxx**, l'option PMF est par défaut définie sur **Compatible** et peut être modifiée. Vous pouvez ainsi configurer les trois valeurs suivantes.
 - **Non requis**
 - **Compatible**
 - **Obligatoire**



Remarque

Les normes Wi-Fi Alliance exigent l'activation de l'option PMF, qui doit être définie par défaut sur **Compatible**. Vous pouvez désactiver cette option lorsque les clients sans fil non compatibles sont instables ou présentent des problèmes de connectivité.

- **Utiliser les paramètres globaux des serveurs RADIUS** : par défaut, chaque VAP utilise les paramètres RADIUS globaux que vous définissez pour l'appareil WAP. Toutefois, vous pouvez configurer chaque VAP de façon à ce qu'il utilise un autre groupe de serveurs RADIUS.

Activez cette option pour utiliser les paramètres RADIUS globaux ; désactivez-la pour utiliser un serveur RADIUS distinct pour le VAP, puis saisissez l'adresse IP et la clé du serveur RADIUS dans les champs appropriés.

- **Type d'adresse IP du serveur** : version IP utilisée par le serveur RADIUS. Vous pouvez basculer entre les différents types d'adresses afin de définir les paramètres d'adresse RADIUS globaux IPv4 et IPv6, mais l'appareil WAP ne contactera que le ou les serveurs RADIUS répondant au type d'adresse que vous sélectionnez dans ce champ.
- **Adresse IP du serveur-1 ou Adresse IPv6 du serveur-1** : adresse du serveur RADIUS principal pour ce VAP.
- **Adresse IP du serveur-2 ou Adresse IPv6 du serveur-2** : jusqu'à trois adresses IPv4 et/ou IPv6 à utiliser comme serveurs RADIUS de sauvegarde pour ce VAP. Si l'authentification auprès du serveur principal échoue, une tentative est effectuée sur chaque serveur de secours configuré.
- **Clé-1** : clé secrète partagée pour le serveur RADIUS global. Vous pouvez utiliser jusqu'à 63 caractères alphanumériques standard et caractères spéciaux. La clé est sensible à la casse. Vous devez en outre configurer la même clé sur l'appareil WAP et sur votre serveur RADIUS. Le texte que vous saisissez s'affiche sous forme d'astérisques pour empêcher d'autres personnes de voir la clé RADIUS pendant que vous la saisissez.
- **Clé-2** : clé RADIUS associée aux serveurs RADIUS de sauvegarde configurés. Le serveur sur l'adresse IPv6 du serveur 2 utilise la clé 2.
- **Activer la gestion de comptes RADIUS** : effectue le suivi et la mesure des ressources qui ont été consommées par un utilisateur donné (heure système, volume de données transmises et reçues, etc.) Si vous activez la gestion des comptes RADIUS, cette fonctionnalité est activée à la fois pour le serveur RADIUS principal et pour l'ensemble des serveurs de sauvegarde.
- **Serveur actif** : permet de sélectionner administrativement le serveur RADIUS actif, ce qui évite à l'appareil WAP de devoir contacter dans l'ordre chaque serveur configuré et de choisir le premier serveur actif.
- **Taux d'actualisation de la clé de diffusion** : intervalle auquel la clé (groupe) de diffusion est actualisée pour les clients associés à ce VAP. La valeur par défaut est de 86400 secondes. La plage valide est comprise entre 0 et 86 400 secondes. La valeur 0 indique que la clé de diffusion n'est pas actualisée.
- **Taux d'actualisation de la clé de session** : intervalle auquel l'appareil WAP actualise les clés de session (monodiffusion) pour chaque client associé au VAP. La plage valide est comprise entre 30 et 86 400 secondes. La valeur 0 indique que la clé de session n'est pas actualisée.

Filtre de client

Vous pouvez utiliser le filtre de client pour autoriser ou refuser l'authentification des stations clientes répertoriées avec l'appareil WAP. L'authentification MAC est configurée à la page [Réseaux](#), à la page 46. Selon la configuration du VAP, l'appareil WAP peut faire référence à une liste de filtres de client stockée sur un serveur RADIUS externe ou stockée localement sur l'appareil WAP.

Configuration d'une liste de filtres de client stockée localement sur l'appareil WAP

L'appareil WAP prend en charge une seule liste de filtres de client. Le filtre peut être configuré pour accorder l'accès uniquement aux adresses MAC spécifiées dans la liste ou pour interdire l'accès uniquement aux adresses spécifiées dans la liste.

Vous pouvez ajouter un maximum de 512 adresses MAC dans la liste de filtrage.

Pour configurer le filtre de client, procédez de la façon suivante :

Étape 1 Sélectionnez **Réseau sans fil > Filtre de client**.

Étape 2 Sélectionnez la façon dont l'appareil WAP utilise la liste de filtrage :

- **Autoriser (Autoriser uniquement les clients de la liste)** : les postes de travail qui ne figurent pas dans la liste se voient interdire l'accès au réseau via l'appareil WAP.
- **Refuser (Refuser tous les clients de la liste)** : seuls les postes de travail qui figurent dans la liste se voient interdire l'accès au réseau via l'appareil WAP. L'accès est autorisé pour toutes les autres stations.

Remarque Le paramètre de filtre s'applique également à la liste de filtres de client stockée sur le serveur RADIUS, s'il en existe une.

Étape 3 Continuez à saisir des adresses MAC jusqu'à ce que la liste soit terminée. Cliquez sur la flèche en regard de l'option **Clients associés**. La liste des clients associés s'affiche. Choisissez l'une des adresses MAC et cliquez sur **Ajouter**. Une règle s'ajoute au tableau des adresses MAC. La liste des clients associés :

- **Adresse MAC** : l'adresse MAC du client sans fil associé.
- **Nom d'hôte** : le nom d'hôte du client sans fil associé.
- **Adresse IP** : l'adresse IP du client sans fil associé.
- **Réseau (SSID)** : SSID (Service Set Identifier) de l'appareil WAP. Le SSID est une chaîne alphanumérique de 32 caractères maximum qui identifie de manière unique un réseau local sans fil. Il est également appelé « nom du réseau ».

Étape 4 Cliquez sur **Enregistrer**.

Configuration de l'authentification MAC sur le serveur Radius

Si un ou plusieurs VAP sont configurés pour utiliser un filtre de client, vous devez configurer la liste des stations sur le serveur RADIUS. Le format de la liste est décrit dans le tableau ci-dessous :

Attribut du serveur RADIUS	Description	Valeur
User-Name (1)	Adresse MAC de la station cliente.	Adresse MAC Ethernet valide.

User-Password (2)	Mot de passe global fixe utilisé pour rechercher une entrée MAC de client.	NOPASSWORD
-------------------	--	------------

Planificateur

Le planificateur de radio et VAP vous permet de configurer une règle avec un intervalle de temps spécifique pour que les VAP ou radios soient opérationnels.

Vous pouvez utiliser cette fonction pour planifier la radio afin qu'elle fonctionne ou autorise l'accès aux VAP uniquement pendant les heures de bureau, de façon à bénéficier de la sécurité adéquate et à réduire la consommation électrique.

L'appareil WAP peut prendre en charge un maximum de 16 profils. Seules les règles valides sont ajoutées au profil. Vous pouvez regrouper 16 règles maximum pour former un profil de planification. Les entrées de période appartenant au même profil ne peuvent pas se chevaucher.

Configuration du profil du planificateur

Vous pouvez créer jusqu'à 16 noms de profil de planificateur. Par défaut, aucun profil n'est créé.

Pour afficher le statut du planificateur et ajouter un profil de planificateur :

Étape 1 Sélectionnez **Réseau sans fil > Planificateur**.

Étape 2 Cochez la case **Activer** pour activer le mode d'administration. Il est désactivé par défaut.

La zone Statut opérationnel du planificateur indique l'état de fonctionnement en cours du planificateur :

- **Statut** : statut opérationnel du planificateur (activé ou désactivé). Le paramètre par défaut est Désactivé.
- **Raison** : raison du statut opérationnel du planificateur. Les valeurs possibles sont les suivantes :
 - **Est actif** : le planificateur est administrativement activé.
 - **Le mode d'administration est désactivé** : le mode d'administration du planificateur est désactivé.
 - **L'heure du système est obsolète** : l'heure du système est obsolète.
 - **Mode géré** : le planificateur est en mode géré.

Étape 3 Pour ajouter un profil, saisissez un nom de profil dans la zone de texte Configuration du profil du planificateur, puis cliquez sur **Ajouter**. Le nom de profil peut comporter jusqu'à 32 caractères alphanumériques.

Configuration de la règle de profil

Vous pouvez configurer un maximum de 16 règles par profil. Chaque règle spécifie l'heure de début, l'heure de fin, ainsi que le ou les jours de la semaine pendant lesquels la radio ou le VAP peut fonctionner. Les règles sont périodiques et se répètent chaque semaine. Une règle valide doit contenir tous les paramètres suivants (jours de la semaine, heure et minute) relatifs à l'heure de début et à l'heure de fin. Il ne doit y avoir aucun conflit de règles. Par exemple, vous pouvez configurer une règle commençant chaque jour ouvrable de la

semaine et une autre commençant chaque jour du week-end, mais vous ne pouvez pas configurer une règle commençant quotidiennement et une autre commençant le week-end.

Pour configurer une règle de profil :

Étape 1 Sélectionnez le profil dans la liste **Sélectionner un nom de profil**.

Étape 2 Cliquez sur .

La nouvelle règle s'affiche dans la **Table des règles de profil**.

Étape 3 Cochez la case en regard du **Nom de profil**, puis cliquez sur **Modifier**.

Étape 4 Dans le menu **Jour de la semaine**, sélectionnez le planning de répétition de la règle. Vous pouvez configurer la règle pour qu'elle s'exécute quotidiennement, chaque jour ouvrable de la semaine, chaque jour du week-end (samedi et dimanche) ou n'importe quel jour de la semaine.

Étape 5 Définissez les heures de début et de fin :

- **Heure de début** : heure à laquelle le VAP ou la radio est activé(e). L'heure est au format 24 heures hh:mm. La plage est comprise entre <00-23>:<00-59>. La valeur par défaut est 00:00.
- **Heure de fin** : heure à laquelle le VAP ou la radio est désactivé(e). L'heure est au format 24 heures hh:mm. La plage est comprise entre <00-23>:<00-59>. La valeur par défaut est 00:00.

Étape 6 Cliquez sur **Enregistrer**.

Remarque Pour être mis en œuvre, un profil de planificateur doit être associé à une interface radio ou une interface VAP.

Pour supprimer une règle, sélectionnez le profil dans la colonne Nom de profil, puis cliquez sur **Supprimer**.

QoS

Les paramètres de qualité de service (QoS) permettent de configurer les files d'attente de transmission pour optimiser le débit et améliorer les performances lors de la gestion du trafic sans fil différencié. Ce trafic peut être VoIP, d'autres types de données audio et vidéo, la lecture multimédia et les données IP classiques.

Pour configurer la qualité de service (QoS) sur l'appareil WAP, définissez les paramètres sur les files d'attente de transmission pour les différents types de trafic sans fil et spécifiez les temps d'attente minimum et maximum pour la transmission.

Les paramètres EDCA (Enhanced Distributed Channel Access) du WAP affectent le trafic transmis de l'appareil WAP vers le poste client. Les paramètres EDCA du poste affectent le trafic transmis du poste client vers l'appareil WAP.

En utilisation normale, les valeurs EDCA par défaut de l'appareil WAP et du poste ne doivent pas être modifiées. La modification de ces valeurs affecte la qualité de service (QoS) fournie.

Pour configurer l'appareil WAP et les paramètres EDCA :

Étape 1 Sélectionnez **Réseau sans fil > QoS**.

Étape 2 Sélectionnez l'interface radio **Radio 1** ou **Radio 2**.

Étape 3 Sélectionnez l'une des options suivantes dans la liste déroulante EDCA :

- **Valeurs WFA par défaut** : renseigne les paramètres EDCA de l'appareil WAP et du poste avec les valeurs Wi-Fi Alliance par défaut, qui sont optimales pour un trafic mixte général.
- **Optimisé pour le trafic vocal** : renseigne les paramètres EDCA de l'appareil WAP et du poste avec les valeurs les mieux adaptées au trafic vocal.
- **Personnalisé** : vous permet de choisir des paramètres EDCA personnalisés.

Ces quatre files d'attente sont définies pour les différents types de données transmises du WAP vers le poste. Si vous choisissez un modèle personnalisé, les paramètres qui définissent les files d'attente sont configurables ; sinon, ils ont des valeurs prédéfinies adaptées à votre sélection. Les quatre files d'attente sont les suivantes :

- **Données 0 (Voix)** : file d'attente de haute priorité, délai minimal. Les données devant être transmises rapidement, comme le VoIP et la lecture multimédia en continu, sont automatiquement envoyées vers cette file d'attente.
- **Données 1 (Vidéo)** : file d'attente de haute priorité, délai minimal. Les données vidéo devant être transmises rapidement sont automatiquement envoyées vers cette file d'attente.
- **Données 2 (Au mieux)** : file d'attente de moyenne priorité, débit et délai moyens. La plupart des données IP classiques sont envoyées vers cette file d'attente.
- **Données 3 (Arrière-plan)** : file d'attente de basse priorité, haut débit. Les données en bloc nécessitant un débit maximal et dont la rapidité n'est pas essentielle sont envoyées vers cette file d'attente (les données FTP, par exemple).

Étape 4 Cochez la case **Activer** pour activer les extensions Wi-Fi Multimedia (WMM).

Wi-Fi MultiMedia (WMM) : ce champ est activé par défaut. Lorsque WMM est activé, la définition des priorités de qualité de service (QoS) et la coordination de l'accès au support sans fil sont activées. Lorsque WMM est activé, les paramètres de qualité de service (QoS) sur l'appareil WAP contrôlent le trafic descendant transmis de l'appareil WAP vers le poste client (paramètres EDCA de point d'accès), ainsi que le trafic montant transmis du poste vers le point d'accès (paramètres EDCA du poste).

La désactivation de WMM désactive le contrôle de qualité de service (QoS) des paramètres EDCA de poste sur le trafic montant transmis du poste vers l'appareil WAP. Lorsque WMM est désactivé, vous pouvez toujours définir certains paramètres sur le trafic descendant transmis de l'appareil WAP vers le poste client (paramètres EDCA de point d'accès).

Étape 5 Définissez les paramètres EDCA et EDCA de poste suivants :

- **Espace intertrames d'arbitrage (AIFS)** : temps d'attente pour les trames de données. Le temps d'attente se mesure en emplacements. Les valeurs valides pour AIFS sont comprises entre 1 et 255.
- **Fenêtre de contention minimale** : entrée dans l'algorithme qui détermine le temps d'attente d'interruption aléatoire initial (fenêtre) pour une nouvelle tentative en cas d'échec de transmission.

Cette valeur est la limite supérieure (en millisecondes) d'une plage à partir de laquelle le temps d'attente d'interruption aléatoire initial est déterminé. Le premier nombre aléatoire généré est un nombre compris entre 0 et le nombre spécifié ici. Si le premier temps d'attente d'interruption aléatoire expire avant l'envoi de la trame de données, un compteur de tentatives est incrémenté et la valeur d'interruption aléatoire (fenêtre) est doublée. Le doublage continue jusqu'à ce que la taille de la valeur d'interruption aléatoire atteigne le nombre défini dans le champ Maximum Contention Window.

Les valeurs valides sont les suivantes : 1, 3, 7, 15, 31, 63, 127, 255, 511 ou 1 023. Cette valeur doit être inférieure à celle définie pour Fenêtre de contention minimale.

- **Fenêtre de contention maximale** : limite supérieure (en millisecondes) pour le doublage de la valeur d'interruption aléatoire. Ce doublage continue jusqu'à ce que la trame de données soit envoyée ou que la taille Maximum Contention Window soit atteinte.

Une fois la taille Maximum Contention Window atteinte, les nouvelles tentatives se poursuivent jusqu'à ce que le nombre maximal autorisé de tentatives soit atteint.

Les valeurs valides sont les suivantes : 1, 3, 7, 15, 31, 63, 127, 255, 511 ou 1 023. Cette valeur doit être supérieure à celle définie pour Fenêtre de contention minimale.

- **Rafale maximale** : paramètre EDCA WAP qui s'applique uniquement au trafic entre le WAP et le poste client.
Cette valeur spécifie (en millisecondes) la longueur de rafale maximale autorisée pour les rafales de paquets sur le réseau sans fil. Une rafale de paquets est un groupe de plusieurs trames transmises sans informations d'en-tête. La baisse de la charge de traitement génère un débit plus élevé et de meilleures performances. Les valeurs valides sont comprises entre 0,0 et 999.
- **Limite TXOP** (station uniquement) : la limite TXOP est un paramètre EDCA de station. Il s'applique uniquement au trafic transmis du poste client vers l'appareil WAP. L'opportunité de transmission (Transmission Opportunity, TXOP) est l'intervalle, en millisecondes, pendant lequel un poste client WME est autorisé à initier des transmissions sur le support sans fil (Wireless Medium, WM) vers l'appareil WAP. La valeur maximale du paramètre Limite TXOP est 65535.

Étape 6 Définissez les paramètres supplémentaires suivants :

- **Aucune validation** : cochez la case **Activer** pour spécifier que l'appareil WAP ne doit pas accepter les trames ayant la valeur de classe de service QoSNoAck.
- **Économie d'énergie automatique non programmée (APSD)** : cochez la case **Activer** pour activer APSD. L'option APSD est recommandée si les téléphones VoIP accèdent au réseau via l'appareil WAP.

Étape 7 Cliquez sur **Enregistrer**.



CHAPITRE 4

Pont sans fil

Ce chapitre explique comment configurer les paramètres du pont sans fil. Il contient les rubriques suivantes :

- [Pont sans fil, à la page 61](#)
- [Configuration du pont WDS, à la page 62](#)
- [WEP sur les liaisons WDS, à la page 63](#)
- [WPA/PSK sur les liaisons WDS, à la page 63](#)
- [Pont de groupe de travail, à la page 63](#)

Pont sans fil

Le système de distribution sans fil (Wireless Distribution System, WDS) vous permet de connecter plusieurs appareils WAP. Le WDS permet d'établir une communication sans fil entre les appareils WAP. Cette fonctionnalité est essentielle au bon fonctionnement des clients en itinérance et à la gestion de plusieurs réseaux sans fil. Vous pouvez configurer l'appareil WAP en mode de pontage point à point ou point à multipoint en fonction du nombre de liaisons à connecter.

En mode point à point, l'appareil WAP accepte les associations de clients et communique avec les clients sans fil. L'appareil WAP transfère l'ensemble du trafic destiné à l'autre réseau via le tunnel établi entre les points d'accès. Le pont n'est pas ajouté au nombre de sauts. Il fonctionne comme simple appareil réseau OSI de couche 2.

En mode de pontage point à point, un appareil WAP fonctionne en tant que liaison commune entre plusieurs points d'accès. Dans ce mode, l'appareil WAP central accepte les associations de clients et communique avec les clients. Tous les autres points d'accès s'associent uniquement à l'appareil WAP central qui transfère les paquets au pont sans fil approprié à des fins de routage.

L'appareil WAP peut également fonctionner en tant que répéteur. Dans ce mode, l'appareil WAP sert de connexion entre deux appareils WAP qui sont trop éloignés pour être à portée cellulaire. Lorsqu'il fonctionne en tant que répéteur, l'appareil WAP n'a aucune connexion filaire au réseau local (LAN) et répète les signaux par l'intermédiaire de la connexion sans fil. Aucune configuration spéciale n'est requise pour permettre à l'appareil WAP de fonctionner en tant que répéteur et il n'existe pas de paramètres de mode répéteur. Les clients sans fil peuvent toujours se connecter à un appareil WAP qui fonctionne en tant que répéteur.

Avant de configurer WDS sur l'appareil WAP, notez les informations ci-après :

- Tous les appareils WAP Cisco participant à une liaison WDS doivent avoir les paramètres identiques suivants :
 - Radio

- IEEE 802.11 Mode
- Bande passante de canal
- Channel (l'option Auto n'est pas recommandée)

Si vous effectuez un pontage dans la bande 802.11n 2,4 GHz, définissez l'option Bande passante de canal sur 20 MHz au lieu du paramètre 20/40 MHz par défaut. Dans la bande 2,4 GHz 20/40 MHz, la bande passante de fonctionnement peut passer de 40 MHz à 20 MHz si des appareils WAP 20 MHz sont détectés dans la zone. Une bande passante de canal incohérente peut entraîner la déconnexion de la liaison.

- Lorsque vous utilisez WDS, veillez à le configurer sur les deux appareils WAP intégrés à la liaison WDS.
- Vous ne pouvez avoir qu'une seule liaison WDS entre n'importe quelle paire d'appareils WAP. Ainsi, une adresse MAC distante ne peut apparaître qu'une seule fois sur la page WDS pour un appareil WAP donné.

Configuration du pont WDS

Pour configurer un pont WDS :

Étape 1 Sélectionnez **Pont sans fil**.

Étape 2 Sélectionnez **WDS** comme mode de pont sans fil.

Étape 3 Cochez la case **Activer** pour activer un port WDS dans les paramètres WDS.

Étape 4 Définissez les paramètres restants :

- **Radio** : spécifie l'ID de la radio (Radio 1 (2,4 GHz) ou Radio 2 (5 GHz)).
- **Adresse MAC locale** : spécifie l'adresse physique ou MAC de l'appareil WAP actuel ou local à partir duquel les données sont transmises.
- **Adresse MAC distante** : spécifie l'adresse MAC de l'appareil WAP de destination. L'adresse MAC se trouve sur la page **Moniteur > Tableau de bord > Réseau sans fil**.
- **Cryptage** : sélectionnez le type de cryptage à utiliser sur le lien WDS (**Aucun, WEP statique ou WPA personnel**).

Si vous ne souhaitez pas sécuriser la liaison WDS, vous pouvez choisir de ne définir aucun type de cryptage. De même, si vous souhaitez sécuriser la liaison, vous pouvez choisir WPA personnel. En mode WPA personnel, l'appareil WAP utilise le cryptage WPA2-PSK avec CCMP (AES) sur la liaison WDS. Consultez la section [WPA/PSK sur les liaisons WDS, à la page 63](#) pour de plus amples informations sur les options de cryptage.

Étape 5 Répétez ces étapes pour un maximum de quatre interfaces WDS.

Étape 6 Cliquez sur **Enregistrer**.

Étape 7 Répétez cette procédure sur les appareils connectés au pont.

Remarque Vous pouvez vérifier si la liaison de pont est active en accédant à la page **Moniteur > Tableau de bord > Réseau sans fil**. Dans la table État de l'interface, l'état WDS(x) doit être **Actif**.

WEP sur les liaisons WDS

Ces champs supplémentaires apparaissent lorsque vous sélectionnez le type de cryptage WEP :

- **Longueur de clé** : si le WEP est activé, spécifiez si la clé WEP doit avoir une longueur de 64 bits ou 128 bits.
- **Type de clé** : si le WEP est activé, sélectionnez le type de clé WEP **ASCII** ou **Hex**.
- **Clé WEP** : si vous avez sélectionné **ASCII**, saisissez toute combinaison de 0 à 9, a à z, et A à Z. Si vous avez sélectionné **Hex**, saisissez des chiffres hexadécimaux (toute combinaison de 0 à 9, a à f, ou A à F). Il s'agit des clés de cryptage RC4 partagées avec les stations par l'intermédiaire de l'appareil WAP.

Notez que le nombre de caractères requis est indiqué à droite du champ et change en fonction de vos sélections dans les champs Type de clé et Longueur de clé.

WPA/PSK sur les liaisons WDS

Ces champs supplémentaires apparaissent lorsque vous sélectionnez le type de cryptage WPA/PSK.

- **ID WDS** : saisissez un nom approprié pour la nouvelle liaison WDS que vous avez créée. Il est important de saisir le même ID WDS à l'autre extrémité de la liaison WDS. Si cet ID WDS n'est pas identique pour les deux appareils WAP sur la liaison WDS, ceux-ci ne pourront pas communiquer et échanger des données.

Le WDS ID peut être n'importe quelle combinaison alphanumérique.

- **Clé** : saisissez une clé partagée unique pour le pont WDS. Cette clé partagée unique doit aussi être saisie pour l'appareil WAP situé à l'autre extrémité de la liaison WDS. Si cette clé n'est pas identique pour les deux WAP, ceux-ci ne pourront pas communiquer et échanger des données.

La clé WPA-PSK est une chaîne de 8 caractères minimum et de 63 caractères maximum. Les caractères acceptés sont les lettres alphabétiques majuscules et minuscules, les chiffres numériques et les symboles spéciaux comme @ et #.

Pont de groupe de travail

La fonction Pont de groupe de travail permet à l'appareil WAP d'étendre l'accessibilité d'un réseau distant. En mode Pont de groupe de travail, l'appareil WAP fonctionne comme une station sans fil (STA) sur le réseau local (LAN) sans fil. Il peut acheminer le trafic entre un réseau filaire distant ou des clients sans fil associés et le réseau local (LAN) sans fil qui est connecté via le mode Pont de groupe de travail.

La fonction Pont de groupe de travail permet la prise en charge simultanée du mode STA et du mode AP. L'appareil WAP peut fonctionner dans un seul BSS (Basic Service Set) en tant qu'appareil STA tout en fonctionnant sur un autre BSS en tant qu'appareil WAP. Lorsque le mode Pont de groupe de travail est activé, l'appareil WAP prend en charge un seul BSS pour les clients sans fil qui s'associent à celui-ci et un autre BSS auquel l'appareil WAP s'associe en tant que client sans fil.

Nous vous recommandons d'utiliser le mode Pont de groupe de travail uniquement lorsque la fonction Pont WDS ne peut pas fonctionner avec un appareil WAP homologué. WDS est une meilleure solution et doit être préférée.

à la solution Pont de groupe de travail. Utilisez WDS si vous effectuez un pontage des appareils Cisco WAP150 et WAP361. Si ce n'est pas le cas, optez pour Pont de groupe de travail. Lorsque la fonction Pont de groupe de travail est activée, les configurations VAP ne sont pas appliquées ; seule la configuration Pont de groupe de travail est appliquée.

**Remarque**

La fonction WDS ne fonctionne pas lorsque le mode Pont de groupe de travail est activé sur l'appareil WAP.

En mode Pont de groupe de travail, le BSS géré par l'appareil WAP fonctionnant en mode d'appareil WAP est appelé l'interface de point d'accès et les STA associés sont appelés les STA descendants. Le BSS géré par l'autre appareil WAP (c'est-à-dire celui auquel le appareil WAP s'associe en tant que STA) est appelé l'interface cliente d'infrastructure et l'autre appareil WAP est appelé le point d'accès montant.

Les appareils connectés à l'interface filaire de l'appareil WAP, ainsi que les stations descendantes associées à l'interface de point d'accès de l'appareil, peuvent accéder au réseau connecté par l'interface cliente d'infrastructure. Pour autoriser le pontage des paquets, la configuration VLAN de l'interface de point d'accès et de l'interface filaire doivent correspondre à celle de l'interface cliente d'infrastructure.

Le mode Pont de groupe de travail peut être utilisé comme extension de portée afin de permettre au BSS de fournir un accès aux réseaux distants ou difficiles d'accès. Une radio unique peut être configurée pour transférer les paquets des STA associés vers un autre appareil WAP du même ESS, sans utiliser de WDS.

Avant de configurer **Pont de groupe de travail** sur l'appareil WAP, notez les informations ci-après :

- Tous les appareils WAP intégrés à Pont de groupe de travail doivent avoir les paramètres identiques suivants :
 - Radio
 - IEEE 802.11 Mode
 - Bande passante de canal
 - Channel (l'option Auto n'est pas recommandée)

Reportez-vous à la section [Radio](#), à la page 41 (paramètres de base) pour obtenir des informations sur la définition de ces paramètres.

- Le mode Pont de groupe de travail prend actuellement en charge le trafic IPv4 uniquement.
- Le mode Pont de groupe de travail n'est pas pris en charge via une configuration de point unique.

Pour configurer le mode Pont de groupe de travail :

-
- Étape 1** Sélectionnez **Pont sans fil**.
 - Étape 2** Cliquez sur **Groupe de travail**.
 - Étape 3** Sélectionnez le port WGB auquel seront appliqués les paramètres de configuration.
 - Étape 4** Cliquez sur **modifier** pour configurer les paramètres suivants pour l'interface cliente d'infrastructure (liaison ascendante/liaison descendante) :

Tableau 1 : Interface cliente d'infrastructure (liaison ascendante/liaison descendante)

Port WGB	Liaison ascendante	Liaison descendante
Activé	Cochez cette case pour activer l'interface cliente d'infrastructure.	Cochez cette case pour activer l'interface cliente d'infrastructure.
Radio	Spécifie l'ID de la radio (Radio 1 (2,4 GHz) ou Radio 2 (5 GHz)).	Spécifie l'ID de la radio (Radio 1 (2,4 GHz) ou Radio 2 (5 GHz)).
SSID	Spécifie le SSID actuel du BSS. Remarque Une flèche est présente en regard du SSID pour l'analyse SSID. Cette fonction est désactivée par défaut et n'est activée que si la détection de point d'accès est activée dans la détection de point d'accès non autorisé (qui est également désactivée par défaut).	Le SSID de l'interface de point d'accès ne doit pas être identique au SSID client d'infrastructure.
Cryptage	Type de sécurité à utiliser pour l'authentification en tant que station cliente sur l'appareil WAP montant. Vous avez le choix entre les possibilités suivantes : <ul style="list-style-type: none"> • Aucun(e) • WEP statique • WPA personnel • WPA entreprise 	Type de sécurité à utiliser pour l'authentification. Les options disponibles sont les suivantes : <ul style="list-style-type: none"> • Aucun(e) • WPA personnel • WEP statique
Statut de la connexion	Indique si le WAP est connecté à l'appareil WAP montant.	Sans objet (s.o.)
ID de VLAN	Spécifie le VLAN associé au BSS.	Configurez l'interface de point d'accès avec le même ID de VLAN que celui annoncé sur l'interface cliente d'infrastructure.
Remarque L'interface cliente d'infrastructure sera associée à l'appareil WAP montant avec les informations d'identification configurées. L'appareil WAP peut obtenir son adresse IP d'un serveur DHCP sur la liaison montante. Vous pouvez également attribuer une adresse IP statique.		
Diffusion SSID	Indique si la diffusion SSID est disponible, activée ou désactivée.	Indiquez si vous souhaitez que le SSID descendant soit diffusé. La diffusion SSID est activée par défaut.

Port WGB	Liaison ascendante	Liaison descendante
Filtre de client	Sans objet (s.o.)	<p>Sélectionnez l'une des options suivantes :</p> <ul style="list-style-type: none"> • Désactivé : le groupe de clients dans le BSS de points d'accès pouvant accéder au réseau montant n'est pas restreint aux clients spécifiés dans une liste d'adresses MAC. • Local : le groupe de clients dans le BSS de points d'accès pouvant accéder au réseau montant est restreint aux clients spécifiés dans une liste d'adresses MAC localement définie. • RADIUS : le groupe de clients dans le BSS de points d'accès pouvant accéder au réseau montant est restreint aux clients spécifiés dans une liste d'adresses MAC sur un serveur RADIUS.
<p>Remarque Si vous sélectionnez Local ou RADIUS, reportez-vous à la section Filtre de client pour obtenir des instructions sur la création du filtre de client.</p>		

Étape 5

Cliquez sur **Enregistrer**. Les clients descendants associés sont désormais connectés au réseau montant.



CHAPITRE 5

Itinérance rapide

Ce chapitre explique comment configurer les paramètres d'itinérance rapide. Il contient les rubriques suivantes :

- [Itinérance rapide, à la page 67](#)
- [Configuration de l'itinérance rapide , à la page 67](#)
- [Configuration des profils de la liste de supports de clé distants, à la page 68](#)

Itinérance rapide

L'itinérance rapide, également appelée IEEE 802.11r ou Fast Basic Service Set Transition (FT), permet d'activer rapidement l'itinérance sur un appareil client dans des environnements qui implémentent la sécurité WPA2 entreprise, en évitant à l'appareil client de se réauthentifier auprès du serveur RADIUS chaque fois qu'il est en itinérance d'un point d'accès à un autre.

L'itinérance FT est un amendement du standard IEEE 802.11 qui permet d'établir une connectivité continue sur les appareils sans fil en itinérance grâce à des transferts rapides, sécurisés et sans interruption d'un point d'accès à un autre point d'accès géré. Pour assurer la qualité des communications vocales et la sécurité du réseau, une station portable doit être capable de maintenir un appel vocal sécurisé de faible latence lors de l'itinérance entre les points d'accès qui gèrent un autre type de trafic.

Cet appareil prend en charge le mode FBT (Fast Basic Service Set Transition) tel qu'il est défini dans le standard 802.11r pour le transfert rapide avec la sécurité WPA2 entreprise. Pour le mode Voix sur WI-FI Entreprise, seul un sous-réseau des fonctionnalités définies dans 802.11r est pris en charge. La transition BSS rapide réduit la latence lors de l'itinérance.

L'option FBT est activée par VAP par radio.



Remarque

Avant de configurer FBT sur un VAP, vérifiez que la sécurité WPA2 est configurée, que la pré-authentification est désactivée et que MFP est désactivé sur le VAP.

Configuration de l'itinérance rapide

Les étapes suivantes donnent une description générale de la manière de configurer l'itinérance rapide :

Étape 1 Sélectionnez **Itinérance rapide > Table d'itinérance**.

Étape 2 Cliquez sur pour ajouter une nouvelle ligne à la table d'itinérance.

Étape 3 Configurez les paramètres suivants :

- **Activer** : cette option est sélectionnée par défaut.
- **BSSID** : sélectionnez le VAP (**VAP 0 2,4 GHz** ou **VAP 0 5 GHz**) pour l'activer.
- **Domaine de mobilité** : spécifie l'identificateur du domaine de mobilité (MDID) du VAP FBT. Le MDID permet d'indiquer un groupe de points d'accès au sein d'un ESS, entre lesquels un STA peut utiliser les services de transition BSS rapides. Les transitions BSS rapides sont autorisées uniquement entre les points d'accès qui possèdent le même MDID et qui se trouvent au sein du même ESS. Elles ne sont pas autorisées entre les points d'accès qui possèdent des MDID différents ou qui se trouvent sur des ESS différents.
- **Mode FT** : le protocole de transition rapide permet une authentification complète de la station mobile uniquement avec le premier point d'accès dans le domaine (le groupe de points d'accès qui prend en charge le protocole FT et qui est connecté via le système de distribution), et utilise une procédure d'association plus courte avec les points d'accès suivants dans le même domaine. Sélectionnez l'une des méthodes de transition rapide suivantes :
 - **Sans fil** : avec cette méthode, la station mobile communique via une liaison 802.11 directe au nouveau point d'accès.
 - **Via le système de distribution** : avec cette méthode, la station mobile communique avec le nouveau point d'accès via l'ancien point d'accès.
- **Support de clé R0** : spécifie l'identificateur NAS à envoyer dans le message de demande d'accès Radius. L'identificateur NAS sert d'ID de support de clé R0.
- **Support de clé R1** : spécifie l'ID de support de clé R1 qui nomme le support de PMK-R1 dans l'authentificateur.
- **Liste de supports de clé distants** : sélectionnez une liste de supports de clé distants dans le menu déroulant que vous avez créé.

Étape 4 Cliquez sur **Enregistrer**.

Remarque Pour supprimer ou modifier un paramètre d'itinérance, sélectionnez-le, puis cliquez sur **Supprimer** ou sur **Modifier**

Après avoir configuré les paramètres FBT, cliquez sur **Enregistrer** pour les enregistrer. La modification de certains paramètres peut entraîner l'arrêt du point d'accès et le redémarrage des processus système. Le cas échéant, la connectivité sera temporairement désactivée sur les clients sans fil. Nous vous recommandons de modifier les paramètres du point d'accès lorsque le trafic WLAN est faible.

Configuration des profils de la liste de supports de clé distants

Pour configurer les profils de la liste de supports de clé distants R0 :

Étape 1 Sélectionnez **Itinérance rapide > Profil de la liste de supports de clé distants**.

- Étape 2** Cliquez sur pour ajouter un nouveau profil ou sur **Modifier** pour modifier un profil. La page **Profils de la liste de supports de clé distants** s'affiche.
- Étape 3** Donnez un nom au profil de la liste de supports de clé distants.
- Étape 4** Configurez les paramètres suivants. 10 entrées de supports de clé R0 maximum peuvent être configurées par VAP.
- **Adresse MAC** : saisissez l'adresse MAC du VAP de destination qui correspond au support de clé R0. Le message RRB PULL est envoyé à l'adresse MAC de ce point d'accès pour récupérer la clé PMKR1. Cette adresse MAC doit être unique sur tous les VAP.
 - **ID NAS** : ID NAS configuré sur le VAP compatible FBT de destination.
 - **Clé RRB** : clé utilisée pour crypter les messages de protocole RRM.
- Étape 5** Répétez les étapes 1 à 4, puis configurez le support de clé R1 dans la Liste des données du support de clé R1 distant. 10 entrées de supports de clé R1 maximum peuvent être configurées par VAP. Les données du support de clé sont configurées par VAP.
- **Adresse MAC** : saisissez l'adresse MAC du VAP de destination qui correspond au support de clé R1. Le PMKR1 est envoyé dans le message RRB PUSH à l'adresse MAC de ce point d'accès. Cette adresse MAC doit être unique sur tous les VAP.
 - **Support de clé R1** : ID de support de clé R1 qui nomme le support de PMK-R1 dans l'authentificateur.
 - **Clé RRB** : clé utilisée pour crypter les messages de protocole RRM.
- Remarque** Après avoir configuré les paramètres de la liste de supports de clé distants, vous pouvez cliquer sur **Restaurer** pour restaurer les anciens paramètres ou sur **Enregistrer** pour enregistrer les paramètres. Cliquez sur **Annuler** pour revenir à la page **Itinérance rapide**.
- Cliquez sur **Enregistrer** après la copie ou la suppression d'un profil.
- Avertissement** Si vous cliquez sur **Exporter** en regard du ou des profils sélectionnés, seuls ces profils sont exportés. Si vous cliquez sur **Exporter** sans sélectionner de profil, tous les profils sont exportés.
-



CHAPITRE 6

Contrôle d'accès

Ce chapitre explique comment configurer l'ACL et la fonction Qualité de service (QoS) sur l'appareil WAP. Il contient les rubriques suivantes :

- [ACL, à la page 71](#)
- [QoS des clients, à la page 79](#)
- [Accès invité, à la page 87](#)

ACL

Les ACL ou listes de contrôle d'accès sont un ensemble de conditions d'autorisation et de refus, appelées règles, qui assurent la sécurité en bloquant les utilisateurs non autorisés et en permettant aux utilisateurs autorisés d'accéder à des ressources spécifiques. Les ACL peuvent bloquer toutes les tentatives non fondées d'accès aux ressources réseau.

l'appareil WAP prend en charge jusqu'à 50 ACL IPv4, IPv6 et MAC, et jusqu'à 10 règles dans chaque ACL. Chaque ACL prend en charge plusieurs interfaces.

ACL IPv4 et IPv6

Chaque ACL est un ensemble de règles appliquées au trafic envoyé ou reçu par l'appareil WAP. Chaque règle spécifie si le contenu d'un champ donné doit être utilisé pour autoriser ou refuser l'accès au réseau. Les règles peuvent être basées sur divers critères et elles peuvent s'appliquer à un ou plusieurs champs au sein d'un paquet, comme l'adresse IP source ou de destination, le port source ou de destination, ou le protocole transporté dans le paquet. Les ACL IP classent le trafic selon les couches 3 et 4.



Remarque

Chaque règle créée se termine par une instruction de refus implicite. Afin d'éviter un refus complet, il est fortement recommandé d'ajouter une règle d'autorisation dans l'ACL en vue d'autoriser le trafic.

ACL MAC

Les ACL MAC sont des ACL de couche 2. Vous pouvez configurer les règles de manière à inspecter les champs d'une trame, comme l'adresse MAC source ou de destination, l'ID de VLAN ou la classe de service. Lorsqu'une trame entre dans le port de l'appareil WAP ou le quitte, l'appareil WAP inspecte la trame et vérifie

son contenu par rapport aux règles ACL. Si l'une des règles correspond à ce contenu, une action d'autorisation ou de refus est entreprise sur la trame.

Procédure de configuration des ACL

Utilisez la ou les règles ACL pour configurer les ACL, puis appliquez ces règles à une interface spécifique.

Pour configurer les ACL, procédez de la façon suivante :

-
- Étape 1** Sélectionnez **Contrôle d'accès > ACL**.
 - Étape 2** Dans la table des listes ACL, cliquez sur pour ajouter une nouvelle ligne et créer une ACL.
 - Étape 3** Spécifiez le nom de l'ACL.
 - Étape 4** Sélectionnez le type d'ACL dans la liste déroulante (**IPv4**, **IPv6** ou **MAC**).
 - Étape 5** Cliquez sur , sélectionnez les interfaces associées pour appliquer l'ACL, puis cliquez sur **OK**. Si vous souhaitez modifier les interfaces associées, vous pouvez cliquer sur pour supprimer les interfaces sélectionnées, puis sur pour sélectionner les nouvelles interfaces associées.
 - Étape 6** Cliquez sur **Plus** pour afficher les paramètres de l'ACL.
 - Étape 7** Configurez ensuite les règles de l'ACL. Pour les ACL IPv4, voir [Configurer les ACL IPv4, à la page 72](#). Pour les ACL IPv6, voir [Configurer les ACL IPv6, à la page 75](#). Pour les ACL MAC, voir [Configurer les ACL MAC, à la page 77](#).
 - Étape 8** Cliquez sur **Enregistrer** pour enregistrer toutes les modifications.
-

Configurer les ACL IPv4

Pour configurer une ACL IPv4 :

-
- Étape 1** Sélectionnez **Contrôle d'accès > ACL**.
 - Étape 2** Cliquez sur pour ajouter une nouvelle ACL.
 - Étape 3** Dans le champ Nom de l'ACL, saisissez le nom de l'ACL. Le nom ne doit pas comporter plus de 31 caractères alphanumériques et caractères spéciaux, sans espace.
 - Étape 4** Sélectionnez le type d'ACL **IPv4** dans la liste Type d'ACL. Les ACL IPv4 contrôlent l'accès aux ressources réseau sur la base des critères des couches 3 et 4.
 - Étape 5** Cliquez sur et sélectionnez les interfaces associées pour appliquer l'ACL. Cliquez sur **OK**. Si vous souhaitez modifier les interfaces associées, vous pouvez cliquer sur pour supprimer l'interface sélectionnée, puis sur pour sélectionner les nouvelles interfaces associées.
 - Étape 6** Cliquez sur **Plus** pour afficher les paramètres de configuration. Cliquez sur pour ajouter une règle et configurer les paramètres suivants :

Remarque Si aucune règle n'est ajoutée, le DUT refuse l'ensemble du trafic par défaut.

- **Priorité des règles** : si une ACL possède plusieurs règles, celles-ci sont appliquées au paquet ou à la trame en fonction de leur priorité. Plus la valeur est faible, plus la priorité est élevée. La priorité de la nouvelle règle est la plus faible de toutes les règles explicites. Notez qu'il existe toujours une règle implicite qui refuse tout le trafic avec la plus faible priorité.

- **Action** : indiquez si vous souhaitez **Refuser** ou **Autoriser** l'action. L'action par défaut est **Refuser**.

Si vous sélectionnez **Autoriser**, la règle autorise tout le trafic qui satisfait aux critères de la règle en matière d'entrée de l'appareil WAP. Le trafic qui ne satisfait pas aux critères est abandonné.

Si vous sélectionnez **Refuser**, la règle bloque tout le trafic qui satisfait aux critères de la règle en matière d'entrée de l'appareil WAP. Le trafic qui ne satisfait pas aux critères est transféré, sauf si cette règle est la règle finale. Étant donné la présence d'une règle implicite de refus de tout trafic à la fin de chaque ACL, le trafic qui n'est pas explicitement autorisé est abandonné.

- **Service (Protocole)** : utilise une condition de correspondance de protocole de couche 3 ou 4 sur la base de la valeur du champ Protocole IP. Vous pouvez sélectionner l'une des options suivantes :
 - **Tout le trafic** : autorise tout le trafic qui satisfait aux critères de la règle.
 - **Sélectionner dans la liste** : sélectionnez l'un des protocoles suivants : **IP, ICMP, IGMP, TCP** ou **UDP**.
 - **Personnalisé** : saisissez un ID de protocole standard affecté par l'IANA compris entre 0 et 255. Choisissez cette méthode pour identifier un protocole qui ne figure pas dans le champ Sélectionner dans la liste.
- **Adresse IPv4 source** : nécessite que l'adresse IP source d'un paquet corresponde à l'adresse définie dans les champs appropriés.
 - **Toute** : autorise toute adresse IP.
 - **Adresse individuelle** : saisissez l'adresse IP pour appliquer ces critères.
 - **Adresse/Masque** : saisissez le masque générique de l'adresse IP source. Le masque générique détermine quels bits sont utilisés et quels bits sont ignorés. Un masque de caractères génériques 255.255.255.255 indique qu'aucun bit n'est important. Un masque générique égal à 0.0.0.0 indique en revanche que tous les bits sont importants. Ce champ est requis lors de la sélection de l'option **Adresse IP source**.

Un masque générique est en fait l'inverse d'un masque de sous-réseau. Par exemple, pour que les critères correspondent à une adresse hôte unique, utilisez un masque générique égal à 0.0.0.0. Pour faire correspondre les critères à un sous-réseau 24 bits (par exemple, 192.168.10.0/24), utilisez un masque générique égal à 0.0.0.255.
- **Port source** : inclut un port source dans la condition de correspondance de la règle. Le port source est identifié dans l'en-tête de datagramme.
 - **Tout le trafic** : autorise tout le trafic qui satisfait aux critères de la règle.
 - **Sélectionner dans la liste** : sélectionnez le mot-clé associé au port source à mettre en correspondance : ftp, ftpdata, http, smtp, snmp, telnet, tftp, www. Chacun de ces mots clés est traduit en son numéro de port équivalent.
 - **Personnalisé** : saisissez le numéro de port IANA à mettre en correspondance avec le port source identifié dans l'en-tête de datagramme. La plage de ports va de 0 à 65535 et inclut trois types de ports différents :
 - 0 à 1023 : ports connus
 - 1024 à 49151 : ports enregistrés
 - 49152 à 65535 : ports dynamiques et/ou privés
- **Adresse IPv4 de destination** : nécessite que l'adresse IP de destination d'un paquet corresponde à l'adresse définie dans les champs appropriés.

- **Toute** : saisissez toute adresse IP.
- **Adresse individuelle** : saisissez une adresse IP pour appliquer ces critères.
- **Adresse/Masque** : saisissez le masque générique de l'adresse IP de destination. Le masque générique détermine quels bits sont utilisés et quels bits sont ignorés. Un masque de caractères génériques 255.255.255 indique qu'aucun bit n'est important. Un masque générique égal à 0.0.0.0 indique en revanche que tous les bits sont importants. Ce champ est requis lors de la sélection de l'adresse IP source.

Un masque générique est en fait l'inverse d'un masque de sous-réseau. Par exemple, pour que les critères correspondent à une adresse hôte unique, utilisez un masque générique égal à 0.0.0.0. Pour faire correspondre les critères à un sous-réseau 24 bits (par exemple, 192.168.10.0/24), utilisez un masque générique égal à 0.0.0.255.
- **Port de destination** : inclut un port de destination dans la condition de correspondance de la règle. Le port de destination est identifié dans l'en-tête de datagramme.
 - **Tout** : tout port qui satisfait les critères de la règle.
 - **Sélectionner dans la liste** : sélectionnez le mot-clé associé au port de destination à mettre en correspondance : ftp, ftpdata, http, smtp, snmp, telnet, tftp, www. Chacun de ces mots clés est traduit en son numéro de port équivalent.
 - **Personnalisé** : saisissez le numéro de port IANA à mettre en correspondance avec le port de destination identifié dans l'en-tête de datagramme. La plage de ports va de 0 à 65535 et inclut trois types de ports différents :
 - 0 à 1023 : ports connus
 - 1024 à 49151 : ports enregistrés
 - 49152 à 65535 : ports dynamiques et/ou privés
- **Type de service** : met en correspondance les paquets en fonction du type de service spécifique.
 - **Tout** : tout type de service.
 - **Sélectionner dans la liste** : met en correspondance les paquets en fonction de leurs valeurs Transfert DSCP (AF), Classe de service (CS) ou Acheminement attendu (EF).
 - **DSCP** : met en correspondance les paquets sur la base d'une valeur DSCP personnalisée. Si vous sélectionnez cette option, saisissez une valeur comprise entre 0 et 63.
 - **Priorité** : met en correspondance les paquets sur la base de leur valeur de priorité IP. Si vous sélectionnez cette option, entrez une valeur IP Precedence comprise entre 0 et 7.
 - **Type de service/Masque** : saisissez une valeur Masque du type de service IP pour identifier les positions de bits dans la valeur Bits du type de service IP, utilisées pour la comparaison avec le champ Type de service IP dans un paquet.

La valeur Masque du type de service IP est un nombre hexadécimal à deux chiffres, compris entre 00 et FF, représentant un masque inversé (à savoir un masque générique). Les bits égaux à zéro dans le champ Masque du type de service IP indiquent les positions de bits dans la valeur Bits du type de service IP qui sont utilisées pour la comparaison avec le champ Type de service IP d'un paquet. Par exemple, pour vérifier une valeur Type de service IP possédant les bits 7 et 5 définis et le bit 1 vide, dans laquelle le bit 7 est le plus significatif, utilisez une valeur Bits du type de service IP égale à 0 et une valeur Masque du type de service IP égale à 00.

Étape 7 Cliquez sur **OK**. Les modifications sont enregistrées dans la configuration de démarrage.

Remarque Pour supprimer ou modifier une ACL, sélectionnez-la, puis cliquez sur **Supprimer** ou sur **Modifier**.

Pour supprimer ou modifier une règle, sélectionnez-la dans la zone Configuration de la règle, puis cliquez sur **Supprimer** ou sur **Modifier**.

Étape 8 Cliquez sur **Enregistrer**.

Configurer les ACL IPv6

Pour configurer une ACL IPv6 :

Étape 1 Sélectionnez **Contrôle d'accès > ACL**.

Étape 2 Cliquez sur pour ajouter une nouvelle ACL.

Étape 3 Dans le champ Nom de l'ACL, saisissez le nom de l'ACL.

Étape 4 Sélectionnez le type d'ACL **IPv6** dans la liste Type d'ACL. Les ACL IPv4 contrôlent l'accès aux ressources réseau sur la base des critères des couches 3 et 4.

Étape 5 Cliquez sur et sélectionnez les interfaces associées pour appliquer l'ACL. Cliquez ensuite sur **OK**. Si vous souhaitez modifier les interfaces associées, vous pouvez cliquer sur pour supprimer l'interface sélectionnée, puis sur pour sélectionner les nouvelles interfaces associées.

Étape 6 Cliquez sur **Plus** pour afficher les paramètres de configuration. Cliquez sur pour ajouter une règle et configurer les paramètres suivants :

Remarque Si aucune règle n'est ajoutée, le DUT refuse l'ensemble du trafic par défaut.

- **Priorité des règles** : si une ACL possède plusieurs règles, celles-ci sont appliquées au paquet ou à la trame en fonction de leur priorité. Plus la valeur est faible, plus la priorité est élevée. La priorité de la nouvelle règle est la plus faible de toutes les règles explicites. Vous pouvez cliquer sur le bouton Suivant ou Précédent pour modifier sa priorité. Notez qu'il existe toujours une règle implicite qui refuse tout le trafic avec la plus faible priorité.

- **Action** : indiquez si vous souhaitez **Refuser** ou **Autoriser** l'action. L'action par défaut est **Refuser**.

Si vous sélectionnez **Autoriser**, la règle autorise tout le trafic qui satisfait aux critères de la règle en matière d'entrée de l'appareil WAP. Le trafic qui ne satisfait pas aux critères est abandonné.

Si vous sélectionnez **Refuser**, la règle bloque tout le trafic qui satisfait aux critères de la règle en matière d'entrée de l'appareil WAP. Le trafic qui ne satisfait pas aux critères est transféré, sauf si cette règle est la règle finale.

Étant donné la présence d'une règle implicite de refus de tout trafic à la fin de chaque ACL, le trafic qui n'est pas explicitement autorisé est abandonné.

- **Service (Protocole)** : utilise une condition de correspondance de protocole de couche 3 ou 4 sur la base de la valeur du champ Protocole IP. Vous pouvez sélectionner l'une des options suivantes :

- **Tout le trafic** : autorise tout le trafic qui satisfait aux critères de la règle.

- **Sélectionner dans la liste** : sélectionnez l'un des protocoles suivants : **IPv6, ICMPv6, TCP** ou **UDP**.

- **Personnalisé** : saisissez un ID de protocole standard affecté par l'IANA compris entre 0 et 255. Choisissez cette méthode pour identifier un protocole qui ne figure pas dans le champ Sélectionner dans la liste.

- **Adresse IPv6 source** : nécessite que l'adresse IP source d'un paquet corresponde à l'adresse définie dans les champs appropriés.
 - **Toute** : autorise toute adresse IP.
 - **Adresse individuelle** : saisissez l'adresse IP pour appliquer ces critères.
 - **Adresse/Masque** : saisissez le masque générique de l'adresse IP source. Le masque générique détermine quels bits sont utilisés et quels bits sont ignorés. Un masque de caractères génériques 255.255.255.255 indique qu'aucun bit n'est important. Un masque générique égal à 0.0.0.0 indique en revanche que tous les bits sont importants. Ce champ est requis lors de la sélection de l'option **Adresse IP source**.

Un masque générique est en fait l'inverse d'un masque de sous-réseau. Par exemple, pour que les critères correspondent à une adresse hôte unique, utilisez un masque générique égal à 0.0.0.0. Pour faire correspondre les critères à un sous-réseau 24 bits (par exemple, 192.168.10.0/24), utilisez un masque générique égal à 0.0.0.255.
- **Port source** : inclut un port source dans la condition de correspondance de la règle. Le port source est identifié dans l'en-tête de datagramme.
 - **Tout** : autorise tout port source.
 - **Sélectionner dans la liste** : sélectionnez le mot-clé associé au port source à mettre en correspondance : ftp, ftpdata, http, smtp, snmp, telnet, tftp, www. Chacun de ces mots clés est traduit en son numéro de port équivalent.
 - **Personnalisé** : saisissez le numéro de port IANA à mettre en correspondance avec le port source identifié dans l'en-tête de datagramme. La plage de ports va de 0 à 65535 et inclut trois types de ports différents :
 - 0 à 1023 : ports connus
 - 1024 à 49151 : ports enregistrés
 - 49152 à 65535 : ports dynamiques et/ou privés
- **Adresse IPv6 de destination** : nécessite que l'adresse IP de destination d'un paquet corresponde à l'adresse définie dans les champs appropriés.
 - **Toute** : saisissez toute adresse IP.
 - **Adresse individuelle** : saisissez une adresse IP pour appliquer ces critères.
 - **Adresse/Masque** : saisissez le masque générique de l'adresse IP de destination. Le masque générique détermine quels bits sont utilisés et quels bits sont ignorés. Un masque de caractères génériques 255.255.255.255 indique qu'aucun bit n'est important. Un masque générique égal à 0.0.0.0 indique en revanche que tous les bits sont importants. Ce champ est requis lors de la sélection de l'adresse IP source.

Un masque générique est en fait l'inverse d'un masque de sous-réseau. Par exemple, pour que les critères correspondent à une adresse hôte unique, utilisez un masque générique égal à 0.0.0.0. Pour faire correspondre les critères à un sous-réseau 24 bits (par exemple, 192.168.10.0/24), utilisez un masque générique égal à 0.0.0.255.
- **Port de destination** : inclut un port de destination dans la condition de correspondance de la règle. Le port de destination est identifié dans l'en-tête de datagramme.
 - **Tout** : tout port qui satisfait les critères de la règle.

- **Sélectionner dans la liste** : sélectionnez le mot-clé associé au port de destination à mettre en correspondance : ftp, ftpdata, http, smtp, snmp, telnet, tftp, www. Chacun de ces mots clés est traduit en son numéro de port équivalent.
- **Personnalisé** : saisissez le numéro de port IANA à mettre en correspondance avec le port de destination identifié dans l'en-tête de datagramme. La plage de ports va de 0 à 65535 et inclut trois types de ports différents :
 - 0 à 1023 : ports connus
 - 1024 à 49151 : ports enregistrés
 - 49152 à 65535 : ports dynamiques et/ou privés
- **Étiquette du flux** : spécifie un nombre de 20 bits unique pour un paquet IPv6.
 - **Tout** : tout nombre de 20 bits.
 - **DSCP** : met le nombre en correspondance sur la base d'une valeur DSCP personnalisée.
- **DSCP** : met en correspondance les paquets sur la base de leur valeur DSCP IP.
 - **Toute** : autorise toute valeur DSCP.
 - **Sélectionner dans la liste** : sélectionnez une valeur DSCP dans la liste déroulante.
 - **Personnalisé** : saisissez une valeur DSCP personnalisée, comprise entre 0 et 63.

Étape 7 Cliquez sur **OK**. Les modifications sont enregistrées dans la configuration de démarrage.

Remarque Pour supprimer ou modifier une ACL, sélectionnez-la, puis cliquez sur **Supprimer** ou sur **Modifier**.

Pour supprimer ou modifier une règle, sélectionnez-la dans la zone Configuration de la règle, puis cliquez sur **Supprimer** ou sur **Modifier**.

Étape 8 Cliquez sur **Enregistrer**.

Configurer les ACL MAC

Pour configurer une ACL MAC :

Étape 1 Sélectionnez **Contrôle d'accès > ACL**.

Étape 2 Cliquez sur pour ajouter une ACL MAC.

Étape 3 Dans le champ Nom de l'ACL, saisissez le nom qui identifie l'ACL.

Étape 4 Sélectionnez le type d'ACL **MAC** dans la liste. Les ACL MAC contrôlent l'accès aux ressources réseau sur la base des critères de la couche 2.

Étape 5 Cliquez sur et sélectionnez les interfaces associées pour appliquer l'ACL, puis cliquez sur **OK**. Si vous souhaitez modifier les interfaces associées, vous pouvez cliquer sur pour supprimer l'interface sélectionnée, puis sur pour sélectionner les nouvelles interfaces associées.

Étape 6 Cliquez ensuite sur **Plus** pour afficher les paramètres de configuration. Cliquez sur pour ajouter une règle et configurer les paramètres suivants :

- **Priorité des règles** : si une ACL possède plusieurs règles, celles-ci sont appliquées au paquet ou à la trame en fonction de leur priorité. Plus la valeur est faible, plus la priorité est élevée. La priorité de la nouvelle règle sera la plus faible de toutes les règles explicites et vous pouvez cliquer sur le bouton Suivant ou Précédent pour modifier sa priorité. Notez qu'il existe toujours une règle implicite qui refuse tout le trafic avec la plus faible priorité.

- **Action** : indiquez si vous souhaitez **Refuser** ou **Autoriser** l'action. L'action par défaut est **Refuser**.

Si vous sélectionnez **Autoriser**, la règle autorise tout le trafic qui satisfait aux critères de la règle en matière d'entrée de l'appareil WAP. Le trafic qui ne satisfait pas aux critères est abandonné.

Si vous sélectionnez **Refuser**, la règle bloque tout le trafic qui satisfait aux critères de la règle en matière d'entrée de l'appareil WAP. Le trafic qui ne satisfait pas aux critères est transféré, sauf si cette règle est la règle finale. Étant donné la présence d'une règle implicite de refus de tout trafic à la fin de chaque ACL, le trafic qui n'est pas explicitement autorisé est abandonné.

- **Service (Type ETH)** : sélectionnez cette option pour comparer les critères de correspondance avec la valeur figurant dans l'en-tête d'une trame Ethernet. Sélectionnez un type ETH dans la liste déroulante.

- **Tout** : autorise tout protocole.

- **Sélectionner dans la liste** : sélectionnez l'un des types de protocoles suivants : **ARP, IPv4, IPv6, IPX, NetBIOS, PPPoE**.

- **Personnalisé** : saisissez un identificateur de protocole personnalisé avec lequel les paquets sont mis en correspondance. La valeur est un nombre hexadécimal à 4 chiffres dans la plage 0600 à FFFF.

- **Adresse MAC source** : nécessite que l'adresse MAC source d'un paquet corresponde à l'adresse définie dans les champs appropriés.

- **Toute** : autorise toute adresse MAC source.

- **Adresse individuelle** : saisissez l'adresse MAC source à comparer à une trame Ethernet.

- **Adresse/Masque** : saisissez le masque d'adresse MAC source indiquant quels bits de l'adresse MAC source il faut comparer à une trame Ethernet.

Pour chaque position de bit dans le masque MAC, une valeur 0 indique que le bit d'adresse correspondant est significatif et une valeur 1 indique que le bit d'adresse est ignoré. Par exemple, pour ne vérifier que les quatre premiers octets d'une adresse MAC, utilisez un masque MAC de 00:00:00:00:ff:ff. Un masque MAC de 00:00:00:00:00:00 vérifie tous les bits d'adresse et est utilisé pour mettre en correspondance une seule adresse MAC.

- **Adresse MAC de destination** : nécessite que l'adresse MAC de destination d'un paquet corresponde à l'adresse définie dans les champs appropriés.

- **Toute** : autorise toute adresse MAC de destination.

- **Adresse individuelle** : saisissez l'adresse MAC de destination à comparer à une trame Ethernet.

- **Adresse/Masque** : saisissez le masque d'adresse MAC de destination afin de spécifier quels bits de l'adresse MAC de destination il faut comparer à une trame Ethernet.

- **ID de VLAN** : ID de VLAN à comparer à une trame Ethernet.

- **Tout** : autorise tout ID de VLAN.

- **Personnalisé** : saisissez l'ID de VLAN spécifique à comparer à une trame Ethernet. Ce champ se trouve dans la première et seule balise VLAN 802.1Q. La plage de ports est comprise entre 1 et 4094.

- **Classe de service** : spécifie la valeur de priorité d'utilisateur 802.1p de la classe de service.
 - **Toute** : autorise toute classe de service.
 - **Personnalisé** : saisissez une priorité d'utilisateur 802.1p à comparer à une trame Ethernet. La plage valide est comprise entre 0 et 7.

Étape 7 Cliquez sur **OK**. Les modifications sont enregistrées dans la configuration de démarrage.

Remarque Pour supprimer ou modifier une ACL, sélectionnez-la, puis cliquez sur **Supprimer** ou sur **Modifier**. Pour supprimer ou modifier une règle, sélectionnez-la dans la zone **Configuration de la règle**, puis cliquez sur **Supprimer** ou sur **Modifier**.

Étape 8 Cliquez sur **Enregistrer**.

QoS des clients

La qualité de service (QoS) des clients permet de contrôler les clients sans fil connectés au réseau et de gérer la bande passante utilisée. La QoS des clients peut gérer le trafic, notamment le trafic HTTP ou le trafic provenant d'un sous-réseau spécifique à l'aide de listes de contrôle d'accès (ACL). Une ACL est un ensemble de conditions d'autorisation et de refus, appelées règles, qui assurent la sécurité, bloquent les utilisateurs non autorisés et permettent aux utilisateurs autorisés d'accéder à des ressources spécifiques. Les ACL peuvent bloquer toutes les tentatives non fondées d'accès aux ressources réseau.

Classes de trafic

La fonction QoS prend en charge les services différenciés (DiffServ, Differentiated Services), qui permettent de classer le trafic en flux. Un certain traitement QoS est également donné conformément aux comportements par saut définis.

Les réseaux IP standard sont conçus pour offrir un service de livraison des données de type « au mieux ». Le service « au mieux » implique que le réseau livre les données dans des délais corrects, mais sans garantie totale de livraison. En cas d'encombrement du réseau, il se peut que des paquets soient retardés, envoyés de manière sporadique, voire abandonnés. En ce qui concerne les applications Internet typiques, comme le courrier électronique et le transfert de fichiers, une légère dégradation du service est acceptable et dans de nombreux cas indétectable. Toutefois, dans le cas des applications présentant des exigences strictes en matière de délais d'exécution, comme la voix ou le multimédia, toute dégradation du service a des effets indésirables.

Une configuration DiffServ débute par la définition de mappages de classe, ce qui permet de classifier le trafic en fonction du protocole IP et d'autres critères. Chaque mappage de classe peut ensuite être associé à un mappage de stratégie, qui définit le mode de traitement de la classe de trafic. Les classes dont le trafic doit être transmis rapidement peuvent être attribuées à des mappages de politique.

Configuration des classes de trafic IPv4

Pour ajouter et configurer un mappage de classe IPv4 :

Étape 1 Sélectionnez **QoS des clients > Classes de trafic**.

Étape 2 Cliquez sur pour ajouter une classe de trafic.

Remarque Le nombre maximal de mappages de classes est de 50.

Étape 3 Dans la zone de texte **Nom de classe de trafic**, saisissez le nom du nouveau mappage de classe. Le nom peut comporter de 1 à 31 caractères alphanumériques et caractères spéciaux. Les espaces ne sont pas autorisés.

Étape 4 Dans la liste **Type de classe**, sélectionnez **IPv4**. Les classes de trafic IPv4 s'appliquent uniquement au trafic IPv4 sur l'appareil WAP.

Étape 5 Configurez les options suivantes :

- **Adresse source** : nécessite que l'adresse IPv4 source d'un paquet corresponde à l'adresse IPv4 définie dans les champs appropriés.
 - **Toute** : toute adresse IPv4 à utiliser comme adresse source.
 - **Adresse individuelle** : saisissez une adresse IPv4 individuelle pour appliquer ces critères.
 - **Adresse/Masque** : saisissez le masque générique de l'adresse IPv4 source. Le masque de DiffServ est un masque de bits de type réseau au format décimal IP séparé par des points, indiquant quelle(s) partie(s) de l'adresse IP de destination il faut utiliser pour effectuer la correspondance avec le contenu des paquets.
 Un masque DiffServ égal à 255.255.255.255 indique que tous les bits sont importants, tandis qu'un masque égal à 0.0.0.0 indique qu'aucun bit n'est important. Le contraire est vrai avec un masque générique d'ACL. Par exemple, pour que les critères correspondent à une adresse hôte unique, utilisez un masque égal à 255.255.255.255. Pour faire correspondre les critères à un sous-réseau 24 bits (par exemple, 192.168.10.0/24), utilisez un masque égal à 255.255.255.0.
- **Adresse de destination** : nécessite que l'adresse IPv4 de destination d'un paquet corresponde à l'adresse IPv4 définie dans les champs appropriés.
 - **Toute** : toute adresse IPv4 à utiliser comme adresse de destination.
 - **Adresse individuelle** : saisissez l'adresse IPv4 pour appliquer ces critères.
 - **Adresse/Masque** : saisissez le masque de l'adresse IP de destination.

Étape 6 Cliquez sur **Plus** et configurez les paramètres suivants :

- **Protocole** : utilise une condition de correspondance de protocole de couche 3 ou 4 sur la base de la valeur du champ Protocole IP dans les paquets IPv4 ou du champ En-tête suivant dans les paquets IPv6. Sélectionnez le protocole à mettre en correspondance par mot-clé ou entrez un ID de protocole :
 - **Tout le trafic** : autorise tout le trafic via n'importe quel protocole.
 - **Sélectionner dans la liste** : met en correspondance le protocole sélectionné : IP, ICMP, IGMP, TCP, UDP.
 - **Personnalisé** : met en correspondance un protocole qui ne figure pas dans la liste. Saisissez l'ID de protocole. L'ID de protocole est une valeur standard affectée par l'IANA. La valeur est un nombre compris entre 0 et 255.

Remarque Si vous définissez **Protocole** sur Tout le trafic, les champs **Adresse source** et **Adresse de destination** ne sont pas facultatifs.

- **Port source** : inclut un port source dans la condition de correspondance de la règle. Le port source est identifié dans l'en-tête de datagramme.
 - **Tout** : tous les ports sont autorisés comme port source.

- **Sélectionner dans la liste** : met en correspondance un mot-clé associé avec le port source : ftp, ftpdata, http, smtp, snmp, telnet, tftp, www. Chacun de ces mots clés est traduit en son numéro de port équivalent.
- **Personnalisé** : met en correspondance le numéro de port source figurant dans l'en-tête de datagramme avec un numéro de port IANA que vous spécifiez. La plage de ports va de 0 à 65535 et inclut trois types de ports différents :
 - 0 à 1023 : ports connus
 - 1024 à 49151 : ports enregistrés
 - 49152 à 65535 : ports dynamiques et/ou privés
- **Port de destination** : inclut un port de destination dans la condition de correspondance de la règle. Le port de destination est identifié dans l'en-tête de datagramme.
 - **Tout** : tous les ports sont autorisés comme port de destination.
 - **Sélectionner dans la liste** : met en correspondance un mot-clé associé avec le port source : ftp, ftpdata, http, smtp, snmp, telnet, tftp, www. Chacun de ces mots clés est traduit en son numéro de port équivalent.
 - **Personnalisé** : met en correspondance le numéro de port source figurant dans l'en-tête de datagramme avec un numéro de port IANA que vous spécifiez. La plage de ports va de 0 à 65535 et inclut trois types de ports différents :
 - 0 à 1023 : ports connus
 - 1024 à 49151 : ports enregistrés
 - 49152 à 65535 : ports dynamiques et/ou privés
- **Type de service** : spécifie le type de service à utiliser lors de la mise en correspondance des paquets avec les critères de classe.
 - **Tout** : autorise tout type de service en guise de critère de correspondance.
 - **Sélectionner la valeur IP DSCP dans la liste** : sélectionnez la valeur DSCP à utiliser comme critère de mise en correspondance.
 - **Valeur correspondante IP DSCP** : saisissez une valeur DSCP personnalisée, comprise entre 0 et 63.
 - **Priorité IP** : met en correspondance la valeur de priorité IP avec la valeur de priorité IP définie dans ce champ. La plage des priorités IP est comprise entre 0 et 7.
 - **Bits du type de service IP** : utilise les bits du type de service du paquet dans l'en-tête IP en guise de critères de correspondance. La plage des valeurs de bits du type de service IP valeur est comprise entre 00 et FF. Les trois bits d'ordre haut représentent la valeur IP Precedence. Les six bits d'ordre haut représentent la valeur DSCP IP.
 - **Masque du type de service IP** : saisissez une valeur Masque du type de service IP pour identifier les positions de bits dans la valeur Bits du type de service IP, utilisées pour la comparaison avec le champ Type de service IP dans un paquet.

La valeur Masque du type de service IP est un nombre hexadécimal à deux chiffres, compris entre 00 et FF. Les bits non égaux à zéro dans le champ Masque du type de service IP indiquent les positions de bits dans la valeur Bits du type de service IP qui sont utilisées pour la comparaison avec le champ Type de service IP d'un paquet.

Étape 7 Cliquez sur **OK**. Les modifications sont enregistrées dans la configuration de démarrage.

Remarque Pour supprimer ou modifier un mappage de classe, sélectionnez le nom du mappage de classe dans la liste et cliquez sur **Supprimer**. Le mappage de classe ne peut pas être supprimé s'il est déjà lié à une stratégie.

Étape 8 Cliquez sur **Enregistrer**.

Configuration des classes de trafic IPv6

Pour ajouter et configurer un mappage de classe IPv6 :

Étape 1 Sélectionnez **QoS des clients > Classes de trafic**.

Étape 2 Cliquez sur pour ajouter une classe de trafic.

Remarque Le nombre maximal de mappages de classes est de 50.

Étape 3 Dans le champ **Nom de classe de trafic**, saisissez le nom du nouveau mappage de classe. Le nom peut comporter de 1 à 31 caractères alphanumériques et caractères spéciaux. Les espaces ne sont pas autorisés.

Étape 4 Sélectionnez le type de classes de trafic **IPv6** dans la liste. Les classes de trafic IPv6 s'appliquent uniquement au trafic IPv6 sur l'appareil WAP.

Étape 5 Configurez les options suivantes :

- **Adresse source** : nécessite que l'adresse IPv6 source d'un paquet corresponde à l'adresse IPv6 définie dans les champs appropriés.
 - **Toute** : toute adresse IPv6 à utiliser comme adresse source.
 - **Adresse individuelle** : saisissez l'adresse IPv6 pour appliquer ces critères.
 - **Adresse/Masque** : saisissez la longueur de préfixe de l'adresse IPv6 source.
- **Adresse de destination** : nécessite que l'adresse IPv4 de destination d'un paquet corresponde à l'adresse IPv4 définie dans les champs appropriés.
 - **Toute** : toute adresse IPv6 à utiliser comme adresse de destination.
 - **Adresse individuelle** : saisissez l'adresse IPv6 pour appliquer ces critères.
 - **Adresse/Masque** : saisissez l'adresse IPv6 de destination et la longueur du préfixe de l'adresse IPv6 de destination.

Étape 6 Cliquez sur **Plus** et configurez les paramètres suivants :

- **Protocole** : utilise une condition de correspondance de protocole de couche 3 ou 4 sur la base de la valeur du champ Protocole IP dans les paquets IPv4 ou du champ En-tête suivant dans les paquets IPv6. Sélectionnez le protocole à mettre en correspondance par mot-clé ou entrez un ID de protocole :
 - **Tout le trafic** : autorise tout le trafic via n'importe quel protocole.
 - **Sélectionner dans la liste** : met en correspondance le protocole sélectionné : IP, ICMP, IGMP, TCP, UDP.

- **Personnalisé** : met en correspondance un protocole qui ne figure pas dans la liste. Saisissez l'ID de protocole. L'ID de protocole est une valeur standard affectée par l'IANA. La valeur est un nombre compris entre 0 et 255.
- **Port source** : inclut un port source dans la condition de correspondance de la règle. Le port source est identifié dans l'en-tête de datagramme.
Remarque Si vous définissez **Protocole** sur Tout le trafic, les champs **Adresse source** et **Adresse de destination** ne sont pas facultatifs.
 - **Tout** : tous les ports sont autorisés comme port source.
 - **Sélectionner dans la liste** : met en correspondance un mot-clé associé avec le port source : ftp, ftpdata, http, smtp, snmp, telnet, tftp, www. Chacun de ces mots clés est traduit en son numéro de port équivalent.
 - **Personnalisé** : met en correspondance le numéro de port source figurant dans l'en-tête de datagramme avec un numéro de port IANA que vous spécifiez. La plage de ports va de 0 à 65535 et inclut trois types de ports différents :
 - 0 à 1023 : ports connus
 - 1024 à 49151 : ports enregistrés
 - 49152 à 65535 : ports dynamiques et/ou privés
- **Port de destination** : inclut un port de destination dans la condition de correspondance de la règle. Le port de destination est identifié dans l'en-tête de datagramme.
 - **Tout** : tous les ports sont autorisés comme port de destination.
 - **Sélectionner dans la liste** : met en correspondance un mot-clé associé avec le port source : ftp, ftpdata, http, smtp, snmp, telnet, tftp, www. Chacun de ces mots clés est traduit en son numéro de port équivalent.
 - **Personnalisé** : met en correspondance le numéro de port source figurant dans l'en-tête de datagramme avec un numéro de port IANA que vous spécifiez. La plage de ports va de 0 à 65535 et inclut trois types de ports différents :
 - 0 à 1023 : ports connus
 - 1024 à 49151 : ports enregistrés
 - 49152 à 65535 : ports dynamiques et/ou privés
- **Étiquette du flux IPv6** : l'étiquette du flux est utilisée par un nœud pour étiqueter les paquets dans un flux.
 - **Tout** : tout nombre de 20 bits unique pour un paquet IPv6.
 - **Défini par l'utilisateur** : saisissez un nombre de 20 bits unique pour un paquet IPv6. Ce nombre est utilisé par les stations finales pour indiquer la gestion de la QoS dans les routeurs (plage de 0 à FFFFF).
- **Type de service** : spécifie le type de service à utiliser lors de la mise en correspondance des paquets avec les critères de classe.
 - **Tout** : autorise tout type de service en guise de critère de correspondance.
 - **Sélectionner la valeur IP DSCP dans la liste** : sélectionnez la valeur DSCP à utiliser comme critère de mise en correspondance.

- **Valeur correspondante IP DSCP** : saisissez une valeur DSCP personnalisée, comprise entre 0 et 63.

Étape 7 Cliquez sur **OK**. Les modifications sont enregistrées dans la configuration de démarrage.

Remarque Pour supprimer ou modifier un mappage de classe, sélectionnez le nom du mappage de classe dans la liste et cliquez sur **Supprimer**. Le mappage de classe ne peut pas être supprimé s'il est déjà lié à une stratégie.

Étape 8 Cliquez sur **Enregistrer**.

Configuration des classes de trafic MAC

Pour ajouter et configurer un mappage de classe MAC :

Étape 1 Sélectionnez **QoS des clients > Classes de trafic**.

Étape 2 Cliquez sur pour ajouter une classe de trafic.

Remarque Le nombre maximal de mappages de classes est de 50.

Étape 3 Dans le champ Nom de classe de trafic, saisissez le nom du nouveau mappage de classe. Le nom peut comporter de 1 à 31 caractères alphanumériques et caractères spéciaux. Les espaces ne sont pas autorisés.

Étape 4 Sélectionnez le type de mappage de classe **MAC** dans la liste. Le mappage de classe MAC s'applique aux critères de couche 2.

Étape 5 **Adresse source** : inclut une adresse source MAC dans la condition de correspondance de la règle.

- **Toute** : toute adresse MAC à utiliser en guise d'adresse source.
- **Adresse individuelle** : saisissez l'adresse MAC source à comparer à une trame Ethernet.
- **Adresse/Masque** : saisissez le masque d'adresse MAC source indiquant quels bits de l'adresse MAC de destination il faut comparer à une trame Ethernet.

Pour chaque position de bit dans le masque MAC, une valeur 1 indique que le bit d'adresse correspondant est significatif et une valeur 0 indique que le bit d'adresse est ignoré. Par exemple, pour ne vérifier que les quatre premiers octets d'une adresse MAC, utilisez un masque MAC de ff:ff:ff:00:00. Un masque MAC de ff:ff:ff:ff:ff vérifie tous les bits d'adresse et est utilisé pour mettre en correspondance une seule adresse MAC.

Étape 6 **Adresse de destination** : inclut une adresse MAC de destination dans la condition de correspondance de la règle.

- **Toute** : toute adresse MAC à utiliser en guise d'adresse de destination.
- **Adresse individuelle** : saisissez l'adresse MAC de destination à comparer à une trame Ethernet.
- **Adresse/Masque** : saisissez le masque d'adresse MAC de destination indiquant quels bits de l'adresse MAC de destination il faut comparer à une trame Ethernet.

Étape 7 Cliquez sur **Plus** et configurez les paramètres suivants :

- **Protocole** : compare les critères de correspondance avec la valeur figurant dans l'en-tête d'une trame Ethernet. Sélectionnez le mot-clé EtherType ou saisissez une valeur EtherType pour spécifier les critères de correspondance :
 - **Tout le trafic** : autorise tout le trafic via n'importe quel protocole.

- **Sélectionner dans la liste** : met en correspondance la valeur Ethertype figurant dans l'en-tête de datagramme avec les types de protocoles sélectionnés : Apple Talk, ARP, IPv4, IPv6, IPX, NETBIOS, PPPoE.
- **Personnalisé** : met en correspondance la valeur Ethertype figurant dans l'en-tête de datagramme avec un identificateur de protocole personnalisé que vous spécifiez. La valeur est un nombre hexadécimal à 4 chiffres dans la plage 0600 à FFFF.

Remarque Si vous définissez **Protocole** sur Tout le trafic, les champs **Adresse source** et **Adresse de destination** ne sont pas facultatifs.

- **Classe de service** : spécifie la valeur de priorité d'utilisateur 802.1p de la classe de service.
 - **Toute** : autorise toute classe de service.
 - **Défini par l'utilisateur** : saisissez une priorité d'utilisateur 802.1p à comparer à une trame Ethernet. La plage valide est comprise entre 0 et 7.
- **ID de VLAN** : ID de VLAN à comparer à une trame Ethernet.
 - **Tout** : autorise tout ID de VLAN.
 - **Défini par l'utilisateur** : saisissez l'ID de VLAN spécifique à comparer à une trame Ethernet. Ce champ se trouve dans la première et seule balise VLAN 802.1Q. La plage de ports est comprise entre 1 et 4094.

Étape 8 Cliquez sur **OK**. Les modifications sont enregistrées dans la configuration de démarrage.

Remarque Pour supprimer ou modifier un mappage de classe, sélectionnez-le dans la liste et cliquez sur **Supprimer**. Le mappage de classe ne peut pas être supprimé s'il est déjà lié à une stratégie.

Étape 9 Cliquez sur **Enregistrer**.

Stratégie de QoS

Les paquets sont classés et traités sur la base des critères définis. Les critères de classification sont définis par l'intermédiaire d'une classe sur la page Mappage de classe. Le traitement est défini par les attributs d'une stratégie à la page Policy Map. Les attributs de stratégie peuvent être définis sur la base d'une instance par classe et ils déterminent le mode de traitement du trafic correspondant aux critères de classe.

L'appareil WAP peut comporter jusqu'à 50 politiques et jusqu'à 10 catégories dans chaque politique.

Pour ajouter et configurer un mappage de stratégie :

Étape 1 Sélectionnez **QoS de client > Politique de QoS**.

Étape 2 Cliquez sur pour ajouter une politique de QoS. Dans le champ Nom de la politique de QoS, saisissez le nom de la politique de QoS. Le nom peut comporter de 1 à 31 caractères alphanumériques et caractères spéciaux. Les espaces ne sont pas autorisés.

Étape 3 Vous pouvez sélectionner une classe de trafic associée créée précédemment.

Étape 4 Dans la zone Définition de la politique de QoS, configurez les paramètres de mappage de politique suivants :

- **Débit engagé** : débit engagé, en Kbit/s, auquel le trafic doit se conformer. Cette valeur est comprise entre 1 et 1.000.000 Kbit/s.
- **Rafale engagée** : taille de rafale engagée, en octets, à laquelle le trafic doit se conformer. La plage est comprise entre 1 et 1600 000 octets.
- **Action** : sélectionnez l'une des options suivantes :
 - **Envoyer** : spécifie que tous les paquets du flux de trafic associé doivent être transférés si les critères de classe de trafic sont satisfaits.
 - **Abandonner** : spécifie que tous les paquets du flux de trafic associé doivent être abandonnés si les critères de classe de trafic sont satisfaits.
- **Remarquer le trafic** : marque tous les paquets du flux de trafic associé avec la valeur de la classe de service spécifiée dans le champ de priorité de l'en-tête 802.1p. Si le paquet ne contient pas encore cet en-tête, celui-ci est inséré. La valeur CoS est un entier compris entre 0 et 7.
 - **Remarquer CoS** : le trafic réseau peut être partitionné en plusieurs niveaux de priorité ou classes de service. La plage de valeurs de CoS est comprise entre 0 et 7, 0 représentant la priorité la plus basse et 7 la priorité la plus élevée.
 - **Remarquer DSCP** : spécifie un comportement par saut (PHB) particulier appliqué à un paquet, en fonction de la QoS fournie. Sélectionnez une valeur dans la liste déroulante.
 - **Remarquer la priorité IP** : marque tous les paquets du flux de trafic associé avec la valeur Priorité IP spécifiée. La valeur Priorité IP est un entier compris entre 0 et 7.

Étape 5 Cliquez sur **ajouter un attr. de politique**. Vous pouvez ajouter un autre mappage de classe, mais le nombre de mappages de classe pour cette politique spécifique est limité à 10.

Étape 6 Cliquez sur **Enregistrer**.

Remarque Pour supprimer ou modifier une politique de QoS, sélectionnez-la dans la liste et cliquez sur **Supprimer** ou sur **Modifier**.

Association de la QoS

La page Association de la QoS assure un contrôle supplémentaire sur certains aspects de la QoS des interfaces sans fil et Ethernet.

En plus de contrôler les catégories générales de trafic, la QoS vous permet également de configurer le conditionnement par client des divers micro-flux par le biais du nom de la politique de QoS. Le nom de la politique de QoS est un outil utile pour l'établissement d'une définition générale des micro-flux et de caractéristiques de traitement pouvant être appliquées à chaque client sans fil, entrant et sortant, lors de son authentification sur le réseau.

Pour configurer les paramètres d'association de la QoS :

Étape 1 Sélectionnez **QoS de client > Association de la QoS**.

Étape 2 Dans la **Table d'association QoS**, cliquez sur pour ajouter une association de la QoS.

Étape 3 Dans la liste déroulante **Nom de la politique de QoS**, sélectionnez un nom.

Étape 4 Configurez les options suivantes :

- **Interface d'association** : sélectionnez l'interface dans la liste déroulante (**2,4 GHz-ciscosb, 5 GHz-ciscosb ou LAN0**).
- **Limite de débit (du point d'accès vers le client)** : vitesse de transmission maximale autorisée depuis l'appareil WAP vers le client en bits par seconde (bit/s). La valeur doit être comprise entre 0 et 866Mbps.
- **Limite de débit (du client vers le point d'accès)** : vitesse de transmission maximale autorisée depuis le client vers l'appareil WAP en bits par seconde (bit/s). La valeur doit être comprise entre 0 et 866Mbps.

Étape 5 Cliquez sur **Enregistrer**.

Remarque Vous pouvez associer une interface à une politique de QoS ou une liste de contrôle d'accès (ACL), mais pas aux deux.

Accès invité

Vous pouvez configurer l'instance de portail captif (CP) par défaut sur l'appareil WAP. L'instance de portail captif est un ensemble de paramètres d'instance défini. L'instance peut être associée à un ou plusieurs points d'accès virtuels.

Lorsque vous utilisez un client sans fil pour le connecter au VAP et accédez à une URL, le portail web détourne l'URL vers la page Paramètres régionaux du portail web que vous configurez sur la page Contrôle d'accès/Accès invité.

La page Paramètres régionaux du portail web définit le style d'affichage de la page de l'interface utilisateur graphique (GUI) détournée, et la page Groupe Invité définit le nom d'utilisateur et le mot de passe de l'utilisateur.

Pour configurer l'instance d'accès invité :

Étape 1 Modifiez la **Table des paramètres régionaux du portail web** pour créer l'affichage de la page de l'interface utilisateur graphique (GUI) détournée. Cliquez sur l'onglet **Aperçu** pour visualiser l'affichage.

Étape 2 Modifiez la **Table des groupes Invité**, cliquez sur le lien de valeur sur **Nombre total d'utilisateurs Invité** pour ajouter un utilisateur, puis cliquez sur **Enregistrer**.

Étape 3 Configurez la **Table des instances d'accès invité**, puis sélectionnez le **Groupe Invité** et les **Paramètres régionaux du portail web** que vous avez configurés en suivant les étapes ci-dessus.

Étape 4 Accédez à **Réseau sans fil > Réseaux** pour associer l'accès invité du VAP et configurer l'instance d'accès invité.

Table des instances d'accès invité

Étape 1 Sélectionnez **Accès invité > Table des instances d'accès invité**.

- Étape 2** Spécifiez un nom pour l'instance de portail captif dans le champ **Nom de l'instance d'accès invité**. Ce nom peut comporter jusqu'à 32 caractères alphanumériques.
- Étape 3** La zone Paramètres de l'instance de portail captif réapparaît avec des options supplémentaires. Définissez les paramètres suivants :
- **Protocole** : spécifiez HTTP ou HTTPS en guise de protocole utilisé par l'instance de portail captif durant le processus de vérification.
 - **HTTP** : n'utilise pas le cryptage durant la vérification.
 - **HTTPS** : utilise le protocole SSL (Secure Sockets Layer), qui nécessite un certificat pour le cryptage. Le certificat est présenté à l'utilisateur lors de la connexion.
 - **Méthode d'authentification** : sélectionnez la méthode d'authentification utilisée par le portail captif pour la vérification des clients. Les options disponibles sont les suivantes :
 - **Base de données locale** : l'appareil WAP utilise une base de données locale pour authentifier les utilisateurs. Définissez les options suivantes si vous utilisez le paramètre Base de données locale.
 - **Nom du groupe Invité** : saisissez le nom à attribuer au groupe Invité.
 - **Délai d'expiration de session inactive** : saisissez le délai d'expiration de session inactive, en minutes.
 - **Bande passante amont maximale** : saisissez le débit maximal de chargement, en mégabits par seconde, auquel un client peut transmettre le trafic lorsqu'il utilise le portail captif. Ce paramètre limite la bande passante utilisée pour envoyer des données sur le réseau. La plage valide va de 0 à 300 Mbits/s. La valeur par défaut est 0.
 - **Bande passante en aval maximale** : saisissez le débit maximal de téléchargement, en mégabits par seconde, auquel un client peut recevoir le trafic lorsqu'il utilise le portail captif. Ce paramètre limite la bande passante utilisée pour recevoir des données du réseau. La plage valide va de 0 à 300 Mbits/s. La valeur par défaut est 0.
 - **Nombre total d'utilisateurs Invité** : nombre total d'utilisateurs Invité.
 - **Authentification Radius** : l'appareil WAP utilise une base de données située sur un serveur RADIUS distant pour authentifier les utilisateurs. Définissez les options suivantes si vous utilisez le paramètre Authentification Radius.
 - **Réseau IP Radius** : sélectionnez le réseau IP Radius dans la liste déroulante (**IPv4 ou IPv6**).
 - **RADIUS global** : cochez la case **Activer** pour activer RADIUS global. Si vous souhaitez que la fonction Portail captif utilise un ensemble de serveurs RADIUS différents, décochez cette case et configurez les serveurs dans les champs de cette page.
 - **Gestion de comptes RADIUS** : cochez la case **Activer** pour activer le suivi et la mesure des ressources consommées par un utilisateur donné, comme le temps système ou les quantités de données transmises et reçues.

Si vous activez la gestion des comptes RADIUS, cette fonctionnalité est active à la fois pour le serveur RADIUS principal, pour l'ensemble des serveurs de secours et pour tous les serveurs configurés.
 - **Adresse IP du serveur-1 ou Adresse IPv6 du serveur-1** : saisissez l'adresse IPv4 ou IPv6 du serveur RADIUS principal pour ce VAP. La forme de l'adresse IPv4 doit être similaire à celle-ci : xxx.xxx.xxx.xxx (192.0.2.10). Le format de l'adresse IPv6 doit être similaire à celui-ci : xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx (2001:DB8:CAD5:7D91).

Lorsque le premier client sans fil tente de s'authentifier auprès d'un VAP, l'appareil WAP envoie une demande d'authentification au serveur principal. Si le serveur principal répond à la demande d'authentification, l'appareil WAP continue à utiliser ce serveur RADIUS en guise de serveur principal et les demandes d'authentification sont envoyées à l'adresse spécifiée.

Adresse IP du serveur-2 ou Adresse IPv6 du serveur-2 : saisissez jusqu'à trois adresses de serveur RADIUS IPv4 ou IPv6 de secours. Si l'authentification auprès du serveur principal échoue, une tentative est effectuée sur chaque serveur de secours configuré.

- **Clé-1** : saisissez la clé secrète partagée que l'appareil WAP utilise pour s'authentifier auprès du serveur RADIUS principal. Vous pouvez utiliser jusqu'à 63 caractères alphanumériques standard et caractères spéciaux. La clé est sensible à la casse et doit correspondre à la clé configurée sur le serveur RADIUS. Le texte que vous saisissez s'affiche sous forme d'astérisques.

Clé-2 : saisissez la clé RADIUS associée aux serveurs RADIUS de secours configurés. Le serveur spécifié dans le champ Adresse IP du serveur-1 utilise la Clé-1 ; le serveur spécifié dans le champ Adresse IP du serveur-2 utilise la Clé-2 et ainsi de suite.

- **Aucune authentification** : les utilisateurs n'ont pas besoin d'être authentifiés par une base de données.
- **Informations d'identification tierces** : l'appareil WAP utilise les informations d'identification d'un réseau social pour authentifier les utilisateurs. Définissez les options suivantes si vous utilisez le paramètre Authentification avec des informations d'identification tierces.
 - **Informations d'identification acceptées** : sélectionnez Facebook ou Google, ou les deux, pour utiliser les informations d'identification de ces plates-formes.
 - **Walled Garden** : la configuration par défaut pertinente est définie automatiquement lorsque les **Informations d'identification acceptées** sont sélectionnées.

Remarque Cisco intègre les exigences en matière de protection, de confidentialité et de sécurité des données dans ses produits et ses méthodologies de développement, depuis la conception jusqu'au lancement. Pour plus d'informations, visitez <https://www.cisco.com/c/en/us/about/trust-center/gdpr.html>.

- **Service Active Directory** : l'appareil WAP utilise une base de données située sur un serveur ADS distant pour authentifier les utilisateurs. Si vous utilisez le paramètre Authentification ADS, définissez les options suivantes.
 - **Serveurs Active Directory** : cliquez sur l'icône pour ajouter un nouveau serveur ADS. Vous pouvez ajouter jusqu'à 3 serveurs. Utilisez la **flèche** pour déplacer et classer les serveurs par ordre de priorité. Sélectionnez la **corbeille** pour supprimer la configuration. Utilisez le bouton **Test** pour vérifier la validité du serveur ADS.
- **Groupe Invité** : si la méthode d'authentification est définie sur Base de données locale ou sur Authentification Radius, sélectionnez un groupe Invité créé précédemment. Tous les utilisateurs appartenant à ce groupe sont autorisés à accéder au réseau par l'intermédiaire de ce portail.
- **URL de redirection** : pour activer cette option, saisissez l'URL (y compris http://). La plage valide va de 0 à 256 caractères.
- **Délai d'expiration de la session** : saisissez le temps de validité restant, en secondes, de la session de portail captif. Lorsque ce temps atteint la valeur zéro, l'authentification du client est annulée. La plage valide va de 0 à 1440 minutes. La valeur par défaut est 0.

- **Paramètres régionaux du portail Web** : dans la liste déroulante, sélectionnez les paramètres régionaux du portail web créés précédemment.

Étape 4 Cliquez sur **Enregistrer**. Les modifications que vous avez effectuées sont enregistrées dans la configuration initiale.

Table des groupes Invité

Sur l'appareil, chaque utilisateur local est attribué à un groupe d'utilisateurs et ce groupe est attribué à une instance de portail captif. Le groupe facilite la gestion de l'affectation des utilisateurs aux instances de portail captif.

Le groupe d'utilisateurs nommé Default est intégré et ne peut pas être supprimé.

Pour configurer un utilisateur local :

Étape 1 Sélectionnez **Accès Invité > Table des groupes Invité**.

Étape 2 Dans la zone Paramètres des groupes Invité, définissez les paramètres suivants :

- **Nom du groupe Invité** : spécifiez le nom du nouveau groupe Invité. Le nom par défaut du groupe Invité est **Par défaut**

Étape 3 Définissez les paramètres suivants :

- **Délai d'expiration de session inactive** : saisissez la période pendant laquelle un utilisateur reste dans la liste des clients authentifiés de portail captif après la dissociation du client de l'appareil WAP. Si la période spécifiée dans ce champ expire avant que le client ne tente de se réauthentifier, l'entrée du client est supprimée de la liste des clients authentifiés. La plage valide va de 0 à 1440 minutes. La valeur par défaut est 60. La valeur de délai d'expiration configurée dans ce champ a préséance sur celle spécifiée pour l'instance de portail captif, à moins que la valeur utilisateur soit définie sur 0. Dans ce cas, la valeur de délai d'expiration définie pour l'instance de portail captif est utilisée.
- **Bande passante amont maximale** : saisissez le débit maximal de chargement, en mégabits par seconde, auquel un client peut transmettre le trafic lorsqu'il utilise le portail captif. Ce paramètre limite la bande passante utilisée pour envoyer des données sur le réseau. La plage valide va de 0 à 866 Mbits/s. La valeur par défaut est 0.
- **Bande passante en aval maximale** : saisissez le débit maximal de téléchargement, en mégabits par seconde, auquel un client peut recevoir le trafic lorsqu'il utilise le portail captif. Ce paramètre limite la bande passante utilisée pour recevoir des données du réseau. La plage valide va de 0 à 866 Mbits/s. La valeur par défaut est 0.
- **Nombre total d'utilisateurs Invité** : indique le nombre total d'utilisateurs Invité. Cliquez sur le lien de valeur du champ **Nombre total d'utilisateurs Invité** pour afficher la page **Compte utilisateur Invité**.

Étape 4 Cliquez sur **Enregistrer**.

Compte utilisateur Invité

Pour configurer un compte utilisateur Invité :

-
- Étape 1** Sélectionnez **Accès Invité > Table des groupes Invité**.
- Étape 2** Cliquez sur le lien de valeur du champ **Nombre total d'utilisateurs Invité** pour afficher le **Tableau des comptes utilisateur Invité** sur la page **Compte utilisateur Invité**.
- Étape 3** Cliquez sur pour ajouter un utilisateur.
- Étape 4** **Nom du groupe Invité** : saisissez le nom du nouveau groupe Invité. Ce nom peut comporter jusqu'à 32 caractères alphanumériques.
- Étape 5** **Mot de passe de l'utilisateur Invité** : saisissez le mot de passe. Le mot de passe peut comporter de 8 à 64 caractères alphanumériques et caractères spéciaux.
- Étape 6** Cliquez sur **Enregistrer**.

Remarque Vous pouvez cliquer sur le bouton **Retour** pour afficher la page **Accès Invité**.

Pour supprimer ou modifier un utilisateur Invité, sélectionnez-le, puis cliquez sur **Supprimer** ou sur **Modifier**

Personnalisation du portail web

Après avoir associé votre instance de portail captif à un point d'accès virtuel, créez des paramètres régionaux et mappez-les à l'instance de portail captif. Lorsque l'utilisateur accède à un point d'accès virtuel associé à une instance de portail captif, la page d'authentification s'affiche.

Utilisez la page Personnalisation du portail web pour créer des pages uniques pour les différents paramètres régionaux sur votre réseau et personnaliser le texte et les images sur les pages.

- Étape 1** Sélectionnez **Accès invité > Table Paramètres régionaux du portail Web**.
- Étape 2** Dans cette table, cliquez sur **ajouter** pour accéder à la page **Personnalisation du portail captif**. Pour modifier les paramètres régionaux, cochez la ligne et cliquez sur **Modifier** ou sur **Supprimer** pour les supprimer.
- Vous pouvez créer jusqu'à trois pages d'authentification différentes avec différents paramètres régionaux sur votre réseau.
- Étape 3** Dans la zone **Paramètres régionaux web du portail captif**, définissez les options suivantes :
- **Nom des paramètres régionaux du portail web** : saisissez le nom des paramètres régionaux web à affecter à la page. Ce nom peut être constitué de 1 à 32 caractères alphanumériques.
- Étape 4** La zone Paramètres régionaux web du portail captif contient des options supplémentaires pour modifier les paramètres régionaux. Il est impossible de modifier le nom de l'instance d'accès invité. Les champs modifiables sont préremplis avec les valeurs par défaut. Configurez les paramètres suivants :
- **Nom de l'instance d'accès invité** : affiche le nom de l'instance d'accès invité.
 - **Image d'arrière-plan** : cliquez sur **Parcourir** pour sélectionner l'image. Vous pouvez cliquer sur **Charger** pour charger les images pour les instances de portail captif.
 - **Logo** : cliquez sur **Parcourir** pour sélectionner le logo. Vous pouvez cliquer sur **Charger** pour charger les logos.
 - **Couleur de premier plan** : saisissez le code HTML de la couleur de premier plan au format hexadécimal à 6 chiffres. La plage valide est comprise entre 1 et 32 caractères. La valeur par défaut est #FFFFFF.

- **Couleur d'arrière-plan** : saisissez le code HTML de la couleur d'arrière-plan au format hexadécimal à 6 chiffres. La plage valide est comprise entre 1 et 32 caractères. La valeur par défaut est #FFFFFF.
- **Couleur de séparation** : saisissez le code HTML de la couleur de l'épaisse ligne horizontale séparant l'en-tête de la page du corps de la page, au format hexadécimal à 6 chiffres. La plage valide est comprise entre 1 et 32 caractères. La valeur par défaut est #FFFFFF.
- **Image du compte** : cliquez sur **Parcourir** pour sélectionner l'image. Vous pouvez cliquer sur **Charger** pour charger les images du compte.
- **Polices** : sélectionnez une police dans la liste déroulante. Cette police sera utilisée pour afficher le texte.
- **Invite - Compte** : saisissez un nom d'utilisateur. La plage valide est comprise entre 1 et 32 caractères.
- **Invite - Nom d'utilisateur** : étiquette de la zone de texte du nom d'utilisateur. La plage valide est comprise entre 1 et 32 caractères.
- **Invite - Mot de passe** : étiquette de la zone de texte du mot de passe d'utilisateur. La plage valide est comprise entre 1 et 64 caractères.
- **Invite - Bouton** : étiquette du bouton sur lequel les utilisateurs cliquent afin de soumettre leur nom d'utilisateur et leur mot de passe pour authentification. La plage valide va de 2 à 32 caractères. La valeur par défaut est Connect.
- **Invite - En-tête de navigateur** : texte qui s'affiche dans la barre de titre du navigateur. La plage valide est comprise entre 1 et 128 caractères. La valeur par défaut est Captive Portal.
- **Invite - Titre de portail** : texte qui apparaît dans l'en-tête de page, à droite du logo. La plage valide est comprise entre 1 et 128 caractères. La valeur par défaut est Welcome to the Wireless Network.
- **Invite - Conseils pour la gestion de compte** : texte qui s'affiche dans le corps de la page en dessous des zones de texte du nom d'utilisateur et du mot de passe. La plage valide est comprise entre 1 et 256 caractères. La valeur par défaut est To start using this service, enter your credentials and click the connect button.
- **Acceptation de la politique d'utilisation** : texte qui apparaît dans la zone de texte Acceptation de la politique d'utilisation. La plage valide est comprise entre 1 et 4 096 caractères. La valeur par défaut est Acceptance Use Policy.
- **Invite - Acceptation de la politique d'utilisation** : texte demandant aux utilisateurs de cocher la case relative à la lecture et à l'acceptation de la politique d'utilisation. La plage valide est comprise entre 1 et 128 caractères.
- **Avertissement - Absence d'acceptation** : texte qui s'affiche dans une fenêtre contextuelle lorsqu'un utilisateur soumet ses informations d'identification de connexion sans avoir coché la case J'accepte la politique d'utilisation. La plage valide est comprise entre 1 et 128 caractères.
- **Invite - Opération en cours** : texte qui s'affiche durant l'authentification. La plage valide est comprise entre 1 et 128 caractères.
- **Invite - Informations d'identification non valides** : texte qui s'affiche lors de l'échec de l'authentification d'un utilisateur. La plage valide est comprise entre 1 et 128 caractères.
- **Invite - Connexion réussie** : texte qui s'affiche lorsque le client s'est authentifié sur le point d'accès virtuel. La plage valide est comprise entre 1 et 128 caractères.
- **Invite - Bienvenue** : texte qui s'affiche lorsque le client s'est connecté au réseau. La plage valide est comprise entre 1 et 256 caractères.
- **Restaurer** : supprime les paramètres régionaux en cours.

- Étape 5** Cliquez sur **Enregistrer**. Les modifications que vous avez effectuées sont enregistrées dans la configuration initiale.
- Étape 6** Cliquez sur **Aperçu** pour afficher la page mise à jour.
- Vous pouvez cliquer sur **Aperçu** pour afficher le texte et les images qui ont déjà été enregistrés dans la configuration initiale. Si vous apportez des modifications, cliquez sur **Enregistrer** avant de cliquer sur **Aperçu** pour voir vos modifications.
-



CHAPITRE 7

Umbrella

Ce chapitre explique comment configurer le service **Cisco Umbrella**. Il contient les rubriques suivantes :

- [Cisco Umbrella, à la page 95](#)

Cisco Umbrella

Cisco Umbrella est une plate-forme de sécurité cloud qui constitue la première ligne de défense contre les menaces sur Internet. Elle agit comme une passerelle entre Internet et vos systèmes et données pour bloquer les malwares, les botnets et les tentatives de phishing visant un port, un protocole ou une application.

En utilisant un compte Umbrella, cette intégration interceptera les requêtes DNS et les redirigera vers Umbrella de façon transparente. Cet appareil s'affichera sur le tableau de bord Umbrella en tant qu'appareil d'application des politiques et d'affichage des rapports.

-
- Étape 1** Cochez la case pour activer la fonction Umbrella.
- Étape 2** Saisissez le secret et la clé d'API récupérés sur le site Web **Umbrella** dans le champ approprié.
- Remarque** Connectez-vous sur votre compte Cisco Umbrella et accédez au tableau de bord : Accédez à **Admin** > **Clés d'API de plate-forme** pour ajouter un nom et créer les informations sur le secret et la clé.
- Étape 3** Dans le champ **Domaines locaux à contourner (facultatif)**, saisissez le nom de domaines dignes de confiance et les paquets issus de ces domaines atteindront leur destination sans passer par Umbrella.
- Remarque** Cette étape est requise pour tous les domaines intranet et pour tous les domaines DNS divisés.
- Étape 4** Pour ajouter une balise à l'appareil, saisissez un nom de balise dans le champ **Balise de l'appareil (facultatif)**.
- Étape 5** Cochez la case pour activer le cryptage DNS.
- Remarque** Le protocole DNSCrypt sert à sécuriser les communications entre un client DNS et un programme de résolution DNS. Il permet d'éviter plusieurs types d'attaques DNS et de snooping. Il est activé par défaut.
- Étape 6** Cliquez sur **Enregistrer** pour appliquer ces configurations. Le statut de l'enregistrement est indiqué dans le champ **Statut de l'enregistrement**.
-



CHAPITRE 8

Moniteur

Ce chapitre explique comment afficher le statut et les statistiques de l'appareil WAP. Il contient les rubriques suivantes :

- [Tableau de bord, à la page 97](#)
- [Clients, à la page 101](#)
- [Invités, à la page 102](#)

Tableau de bord

Le tableau de bord affiche l'état du débit et vous explique comment configurer ou contrôler facilement votre appareil réseau. Cette page est mise à jour toutes les 30 secondes.

Clients connectés

Nombre total de clients actuellement associés à l'appareil WAP Cliquez sur cette case pour accéder à la page Clients.

Internet/Réseau local/Réseau sans fil

Les icônes en forme de cercle situées en haut à droite de la page indiquent l'état de la connexion Internet, du réseau local et de la connexion sans fil.

Internet

- **Cercle rouge** : pas de connexion Internet.
- **Cercle vert** : la connexion Internet est bonne.

Réseau local

- **Cercle rouge** : pas de connexion câblée.
- **Cercle vert** : connexion câblée.

Cliquez sur le lien **Réseau local** pour ouvrir la page **Statut du réseau local**.

Technologie sans fil

- **Cercle rouge** : toutes les radios sont désactivées.
- **Cercle vert** : au moins une radio fonctionne. Une ou deux radios sont activées.

Cliquez sur le lien **Réseau sans fil** pour ouvrir la page **Statut du réseau sans fil**.

Débit de radio 2,4 GHz

Ce graphique en courbes indique le débit de la radio 2,4 GHz et se met à jour toutes les 30 secondes.

- **Transférer** : débit des 30 dernières secondes transmises.
- **Télécharger** : débit des 30 dernières secondes reçues.

Cliquez sur **Transférer** ou **Télécharger** pour ne pas afficher les données.

Débit de radio 5 GHz

Ce graphique en courbes indique le débit de la radio 5 GHz et se met à jour toutes les 30 secondes.

- **Transférer** : débit des 30 dernières secondes transmises.
- **Télécharger** : débit des 30 dernières secondes reçues.

Cliquez sur **Transférer** ou **Télécharger** pour ne pas afficher les données.

Principaux clients

Selon l'ordre du trafic, ce graphique à barres indique les cinq principaux appareils clients de trafic.

- **Transférer** : débit des 30 dernières secondes transmises.
- **Télécharger** : débit des 30 dernières secondes reçues.

Cliquez sur **Transférer** ou **Télécharger** pour ne pas afficher les données.

Utilisation SSID

Selon l'ordre du trafic, ce graphique à barres indique les cinq principaux SSID de trafic.

- **Trafic** : nombre total d'octets transmis et reçus.

Utilisation du réseau

Ce graphique en courbes indique le débit Ethernet.

- **Transférer** : débit des 30 dernières secondes transmises.
- **Télécharger** : débit des 30 dernières secondes reçues.

Cliquez sur **Transférer** ou **Télécharger** pour ne pas afficher les données.

Accès rapide

Afin de simplifier la configuration de l'appareil grâce à une navigation rapide, la page **Mise en route** contient des liens permettant d'effectuer des tâches courantes. Pour plus d'informations, reportez-vous à la section [Configuration du démarrage rapide, à la page 7](#).

Statut du réseau local

Cliquez sur le cercle Réseau local pour afficher les paramètres de configuration et d'état suivants sur l'interface LAN.

- **Adresse MAC** : adresse MAC de l'appareil WAP.

- **Adresse IP** : adresse IP de l'appareil WAP.
- **Masque de sous-réseau** : masque de sous-réseau de l'appareil WAP.
- **Passerelle par défaut** : passerelle par défaut de l'appareil WAP.
- **Serveur de noms de domaine-1** : adresse IP du serveur de noms de domaine 1 utilisé par l'appareil WAP.
- **Serveur de noms de domaine-2** : adresse IP du serveur de noms de domaine 2 utilisé par l'appareil WAP.
- **Mode Green Ethernet** : mode Green Ethernet de l'interface Ethernet.
- **Adresse IPv6** : adresse IPv6 de l'appareil WAP.
- **Adresses globales IPv6 configurées automatiquement** : adresses globales IPv6 configurées automatiquement.
- **Adresse IPv6 de liaison locale** : adresse IPv6 de liaison locale de l'appareil WAP.
- **Passerelle IPv6 par défaut** : passerelle IPv6 par défaut de l'appareil WAP.
- **IPv6-DNS-1** : adresse IPv6 du serveur IPv6 DNS 1 utilisé par l'appareil WAP.
- **IPv6-DNS-2** : adresse IPv6 du serveur IPv6 DNS 2 utilisé par l'appareil WAP.
- **ID de VLAN** : identifiant du réseau VLAN.

**Remarque**

Ces paramètres s'appliquent à l'interface interne. Cliquez sur **Modifier** si vous souhaitez modifier l'un de ces paramètres. Vous serez redirigé vers la page **Réseau local**.

Cliquez sur **Actualiser** pour actualiser l'écran et afficher les informations les plus récentes.

Cliquez sur **Retour** pour revenir à la page **Tableau de bord**.

Statut du réseau sans fil

Cliquez sur le cercle **Réseau sans fil** pour afficher les interfaces radio sans fil, à savoir :

- **Radio sans fil** : le mode Radio sans fil est activé ou désactivé pour l'interface radio.
- **Adresse MAC** : adresse MAC associée à l'interface radio.
- **Mode** : mode 802.11 (a/b/g/n/ac) utilisé par l'interface radio.
- **Canal** : canal utilisé par l'interface radio.
- **Bande passante opérationnelle** : bande passante opérationnelle utilisée par l'interface radio.
- Cliquez sur **Modifier** si vous souhaitez modifier l'un de ces paramètres. Vous serez redirigé vers la page **Radio**.

Cliquez sur **Actualiser** pour actualiser l'écran et afficher les informations les plus récentes.

Cliquez sur **Retour** pour revenir à la page **Tableau de bord**.

Statut de l'interface

Le tableau Statut de l'interface répertorie les informations suivantes relatives à l'état de chaque point d'accès virtuel et de chaque interface de système de distribution sans fil (WDS, Wireless Distribution System) :

- **Interface réseau** : interface sans fil de l'appareil WAP.
- **Nom (SSID)** : nom de l'interface sans fil.
- **Statut** : statut administratif (actif ou inactif) du VAP.
- **Adresse MAC** : adresse MAC de l'interface radio.
- **ID VLAN** : ID de VLAN de l'interface radio.
- **Profil** : nom du profil du planificateur associé.
- **État** : état actuel (actif ou inactif). L'état indique si le point d'accès virtuel échange des données avec un client.

Statistiques de trafic

La page Statistiques de trafic offre un affichage en temps réel des statistiques de transmission et de réception de l'interface Ethernet, des points d'accès virtuels (VAP) et de toutes les interfaces WDS. Toutes les statistiques de transmission et de réception reflètent les totaux obtenus depuis le dernier démarrage de l'appareil WAP. Si vous avez redémarré l'appareil WAP, ces données chiffrées indiquent les totaux de transmission et de réception depuis le redémarrage.

Pour afficher les statistiques de trafic, sélectionnez **Moniteur > Tableau de bord > Accès rapide > Statistiques de trafic**.

Les informations suivantes s'affichent :

- **Interface** : nom de l'interface Ethernet, de chaque interface de point d'accès virtuel et de chaque interface WDS. Le nom de chaque interface VAP est suivi par son SSID entre parenthèses.
- **Nombre total de paquets** : nombre total de paquets envoyés (dans la table de transmission) ou reçus (dans la table de réception) par cet appareil WAP.
- **Nombre total d'octets** : nombre total d'octets envoyés (dans la table de transmission) ou reçus (dans la table de réception) par cet appareil WAP.
- **Nombre total de paquets abandonnés** : nombre total de paquets abandonnés envoyés (dans la table de transmission) ou reçus (dans la table de réception) par cet appareil WAP.
- **Nombre total d'octets abandonnés** : nombre total d'octets abandonnés envoyés (dans la table de transmission) ou reçus (dans la table de réception) par cet appareil WAP.
- **Erreurs** : nombre total d'erreurs relatives à l'envoi et à la réception de données sur l'appareil WAP.



Remarque

Vous pouvez cliquer sur **Actualiser** pour afficher les informations mises à jour.

Clients

Clients

La page Clients contient les stations clientes associées à l'appareil.

Nombre total de clients associés : nombre total des clients sur l'appareil WAP.

Récapitulatif des clients

Affiche le récapitulatif des clients par type de client 802.11 actuellement sur l'appareil.

Bande passante moyenne

Indique la bande passante moyenne du client, en Mbit/s.

- **Transférer** : débit des 30 dernières secondes transmises.
- **Télécharger** : débit des 30 dernières secondes reçues.



Remarque Cliquez sur **Transférer** ou **Télécharger** pour ne pas afficher les données.

Clients présentant le rapport signal/bruit le plus faible

Liste des 5 appareils présentant le rapport signal/bruit le plus faible.

Clients présentant le débit le plus bas

Liste des 5 appareils présentant le débit le plus bas.

Clients associés

- **Détails des clients** : Le nom d'hôte et l'adresse MAC du client sans fil associé.
- **Adresse IP** : l'adresse IP du client sans fil associé.
- **Réseau (SSID)** : SSID (Service Set Identifier) de l'appareil WAP. Le SSID est une chaîne alphanumérique de 32 caractères maximum qui identifie de manière unique un réseau local sans fil. Il porte également le nom de Network Name (nom réseau).
- **Mode** : mode IEEE 802.11 actuellement utilisé sur le client, notamment IEEE 802.11a, IEEE 802.11b ou IEEE 802.11g.
- **Débit de données** : vitesse de transmission des données actuelle.
- **Canal** : canal auquel le client est actuellement connecté. Le canal définit la partie du spectre radio utilisée par la radio pour la transmission et la réception. La page Radio vous permet de définir le canal.
- **Trafic (ascendant/descendant)** : nombre total d'octets envoyés (trafic ascendant) ou reçus (trafic descendant) par l'appareil client.
- **Rapport signal/bruit (dB)** : puissance du rapport signal/bruit, en décibels (dB).

- **Calculateur de débit** : débit/débit de données des 30 dernières secondes.


Remarque

Vous pouvez classer les clients par Détails des clients, Réseau (SSID), etc.

Vous pouvez filtrer les clients par Détails des clients, Réseau (SSID), etc.

Invités

La page Invités contient deux tableaux. Le tableau Clients authentifiés fournit des informations sur les clients qui ont été authentifiés sur n'importe quelle instance du portail captif. Le tableau Clients dont l'authentification a échoué fournit des informations sur les clients qui ont tenté de s'authentifier sur un portail captif et qui ont échoué.

Pour afficher la liste des clients authentifiés ou la liste des clients dont l'authentification a échoué, sélectionnez **Moniteur > Invités**.

Les informations suivantes s'affichent :

- **MAC** : adresse MAC du client.
- **Adresse IP** : adresse IP du client.
- **Nom d'utilisateur** : nom d'utilisateur de portail captif du client.
- **Protocole** : protocole employé par l'utilisateur pour établir la connexion (HTTP ou HTTPS).
- **Vérification** : méthode utilisée pour l'authentification de l'utilisateur sur le portail captif. Les valeurs possibles sont les suivantes :
 - **Invité** : l'utilisateur n'a pas besoin d'être authentifié par une base de données.
 - **Local** : l'appareil WAP utilise une base de données locale pour authentifier les utilisateurs.
 - **RADIUS** : l'appareil WAP utilise une base de données située sur un serveur RADIUS distant pour authentifier les utilisateurs.
- **ID de point d'accès virtuel/radio** : point d'accès virtuel et radio auxquels l'utilisateur est associé.
- **Délai d'expiration** : temps de validité restant, en secondes, de la session de portail captif. Lorsque ce temps atteint la valeur zéro, l'authentification du client est annulée.
- **Délai d'expiration en cas d'absence** : temps de validité restant, en secondes, de l'entrée du client. Le compte à rebours commence lorsque le client se dissocie du portail captif. Lorsque ce temps atteint la valeur zéro, l'authentification du client est annulée.
- **Amont/Aval (Mo)** : nombre d'octets transmis et reçus par l'appareil WAP depuis la station utilisateur.
- **Heure de l'échec** : heure à laquelle l'échec de l'authentification s'est produit. Un horodatage est inclus, indiquant l'heure de l'échec.

Vous pouvez cliquer sur Exporter pour charger le message des clients authentifiés/dont l'authentification a échoué actuels.

**Remarque**

Avant de cliquer sur le bouton Exporter, sélectionnez le client authentifié ou le client dont l'authentification a échoué pour procéder au chargement, puis cliquez sur **Exporter**.



CHAPITRE 9

Administration

Ce chapitre explique comment configurer les paramètres d'administration et effectuer des diagnostics. Il contient les rubriques suivantes :

- [Microprogramme, à la page 105](#)
- [Fichiers de configuration, à la page 107](#)
- [Redémarrage, à la page 109](#)

Microprogramme

L'appareil WAP gère deux images de microprogramme. Une image est active et l'autre est inactive. Si l'image active ne parvient pas à se charger au démarrage, l'image inactive est chargée et devient l'image active. Vous pouvez également permuter l'image active et l'image inactive.

Lorsque de nouvelles versions du microprogramme deviennent disponibles, vous pouvez le mettre à niveau sur vos appareils afin de bénéficier des nouvelles fonctionnalités et améliorations. L'appareil WAP utilise un client TFTP ou HTTP/HTTPS pour les mises à niveau du microprogramme.

Une fois que vous avez chargé le nouveau microprogramme et que le système redémarre, le microprogramme nouvellement ajouté devient l'image principale. Si la mise à niveau échoue, le microprogramme d'origine reste l'image principale.



Remarque

Lorsque vous mettez à niveau le microprogramme, l'appareil WAP conserve les paramètres de configuration.

Permutation de l'image du microprogramme

Pour permuter l'image du microprogramme exécuté sur l'appareil WAP :

Étape 1 Sélectionnez **Administration > Microprogramme**.

L'ID de produit (PID VID) ainsi que les versions du microprogramme active et inactive apparaissent.

Étape 2 Cliquez sur **Permuter l'image**.

La boîte de dialogue qui s'affiche confirme le basculement de l'image du microprogramme et le redémarrage qui suit.

Étape 3 Cliquez sur **OK** pour continuer.

Ce processus peut prendre plusieurs minutes pendant lesquelles l'appareil WAP est indisponible. Ne mettez pas l'appareil WAP hors tension pendant le basculement de l'image. Une fois le basculement de l'image terminé, l'appareil WAP redémarre. L'appareil WAP reprend son fonctionnement normal avec les paramètres de configuration qu'il utilisait avant la mise à niveau.

Mise à niveau HTTP/HTTPS

Pour effectuer une mise à niveau via HTTP/HTTPS :

Étape 1 Sélectionnez la méthode de transfert **HTTP/HTTPS**.

Étape 2 Cliquez sur **Parcourir**, puis recherchez le fichier image du microprogramme sur votre réseau.

Le fichier de mise à niveau du microprogramme fourni doit être un fichier tar. Pour la mise à niveau, n'essayez pas d'utiliser des fichiers bin ou des fichiers ayant un autre format ; ces types de fichiers ne fonctionnent pas.

Étape 3 Cliquez sur **Upgrade** pour appliquer la nouvelle image du microprogramme.

Le téléchargement du nouveau microprogramme peut prendre quelques minutes. N'actualisez pas la page et n'ouvrez pas d'autre page pendant le chargement du nouveau micrologiciel, sous peine d'interrompre celui-ci. Une fois le processus terminé, l'appareil WAP redémarre et reprend son fonctionnement normal.

Étape 4 Pour vous assurer que la mise à niveau du microprogramme s'est correctement déroulée, connectez-vous à l'utilitaire de configuration web, affichez la page Mise à niveau du microprogramme, puis vérifiez la version active du microprogramme.

Mise à niveau TFTP

Pour mettre à niveau le microprogramme sur l'appareil WAP via TFTP :

Étape 1 Sélectionnez la méthode de transfert **TFTP**.

Étape 2 Saisissez un nom (de 1 à 256 caractères) pour le fichier image dans le champ Nom du fichier source, en incluant le chemin d'accès au répertoire qui contient l'image à télécharger.

Par exemple, pour télécharger l'image ap_upgrade.tar située dans le répertoire /share/builds/ap, saisissez :
/share/builds/ap/ap_upgrade.tar

Le fichier de mise à niveau du microprogramme fourni doit être un fichier tar. Pour la mise à niveau, n'essayez pas d'utiliser des fichiers bin ou des fichiers ayant un autre format ; ces types de fichiers ne fonctionnent pas.

Le nom de fichier ne peut pas contenir les caractères suivants : espaces, <, >, |, \, :, (,), &, ;, #, ?, *, ainsi que deux points successifs ou plus.

Étape 3 Saisissez l'adresse IPv4 du serveur TFTP, puis cliquez sur **Mettre à niveau**.

Le téléchargement du nouveau microprogramme peut prendre quelques minutes. N'actualisez pas la page et n'ouvrez pas d'autre page pendant le chargement du nouveau micrologiciel, sous peine d'interrompre celui-ci. Une fois le processus terminé, l'appareil WAP redémarre et reprend son fonctionnement normal.

Étape 4 Pour vous assurer que la mise à niveau du microprogramme s'est correctement effectuée, connectez-vous à l'utilitaire de configuration, affichez la page Mise à niveau du microprogramme, puis vérifiez la version active du microprogramme.

Fichiers de configuration

Les fichiers de configuration de l'appareil WAP sont au format XML et contiennent toutes les informations relatives aux paramètres de l'appareil WAP. Vous pouvez sauvegarder (télécharger) les fichiers de configuration sur un hôte réseau ou un serveur TFTP, afin de modifier manuellement le contenu ou de créer des sauvegardes. Une fois que vous avez modifié un fichier de configuration sauvegardé, vous pouvez le télécharger vers l'appareil WAP afin de modifier la configuration. L'appareil WAP prend en charge les fichiers de configuration suivants :

- **Configuration de démarrage** : fichier de configuration enregistré dans la mémoire flash.
- **Configuration de secours** : fichier de configuration supplémentaire enregistré sur l'appareil WAP pour être utilisé comme sauvegarde.
- **Configuration miroir** : si la configuration de démarrage n'est pas modifiée pendant au moins 24 heures, elle est automatiquement enregistrée dans un fichier de configuration miroir. Le fichier de configuration miroir est un instantané de la configuration de démarrage antérieure. La configuration miroir est conservée malgré les restaurations des paramètres d'usine. Elle peut donc être utilisée pour récupérer une configuration système après une restauration des paramètres d'usine en copiant la configuration miroir vers la configuration de démarrage.



Remarque

En plus du téléchargement et du transfert de ces fichiers vers un autre système, vous pouvez les copier vers différents types de fichiers sur l'appareil WAP.

Sauvegarde des fichiers de configuration

Pour enregistrer (charger) le fichier de configuration vers un hôte réseau ou le serveur TFTP :

Étape 1 Sélectionnez **Administration > Fichiers de configuration > Télécharger/Enregistrer**.

Étape 2 Sélectionnez la méthode de transfert **Via TFTP** ou **Via HTTP/HTTPS**.

Étape 3 Sélectionnez **Enregistrer (Point d'accès vers ordinateur)** pour enregistrer les données de configuration sur l'ordinateur.

Étape 4 Pour une sauvegarde TFTP, saisissez le nom du fichier de destination avec une extension .xml. Incluez également le chemin d'accès à l'emplacement de stockage du fichier sur le serveur, puis saisissez l'adresse IPv4 du serveur TFTP.

Le nom de fichier ne peut pas contenir les caractères suivants : espaces, <, >, |, \, :, (,), &, ;, #, ?, *, ainsi que deux points successifs ou plus.

Étape 5 Pour une sauvegarde TFTP, saisissez l'adresse IPv4 du serveur TFTP.

- Étape 6** Sélectionnez le fichier de configuration à enregistrer :
- **Configuration de démarrage** : type de fichier de configuration utilisé lors du dernier démarrage de l'appareil WAP. Ce fichier n'inclut pas les modifications de configuration appliquées, mais non encore enregistrées sur l'appareil WAP.
 - **Configuration de sauvegarde** : type de fichier de configuration de sauvegarde enregistré sur l'appareil WAP.
 - **Configuration miroir** : si la configuration de démarrage n'est pas modifiée pendant au moins 24 heures, elle est automatiquement enregistrée dans un fichier de configuration miroir. La configuration miroir est un instantané d'une configuration de démarrage antérieure. La configuration miroir est conservée malgré les restaurations des paramètres d'usine. Elle peut donc être utilisée pour récupérer une configuration système après une restauration des paramètres d'usine en copiant la configuration miroir vers la configuration de démarrage.
- Étape 7** Cliquez sur **Save** pour commencer la sauvegarde. Pour les sauvegardes HTTP/HTTPS, une fenêtre s'affiche afin de vous permettre d'accéder à l'emplacement souhaité pour l'enregistrement du fichier.
-

Téléchargement des fichiers de configuration

Vous pouvez télécharger un fichier vers l'appareil WAP pour mettre à jour la configuration ou restaurer l'appareil WAP vers une configuration précédemment sauvegardée.

Pour télécharger un fichier de configuration vers l'appareil WAP :

-
- Étape 1** Sélectionnez **Administration > Fichiers de configuration > Télécharger/Enregistrer**.
- Étape 2** Sélectionnez la méthode de transfert **Via TFTP** ou **Via HTTP/HTTPS**.
- Étape 3** Sélectionnez **Télécharger (Ordinateur vers point d'accès)** pour sauvegarder les données de configuration sur l'ordinateur.
- Étape 4** Pour une sauvegarde TFTP, saisissez le nom du fichier de destination avec une extension. xml. Incluez également le chemin d'accès à l'emplacement de stockage du fichier sur le serveur, puis saisissez l'adresse IPv4 du serveur TFTP.
- Le nom de fichier ne peut pas contenir les caractères suivants : espaces, <, >, |, \, :, (,), &, ;, #, ?, *, ainsi que deux points successifs ou plus.
- Étape 5** Sélectionnez **Configuration de démarrage** ou **Configuration de sauvegarde** pour remplacer le fichier par le fichier téléchargé.
- Si le fichier téléchargé écrase le fichier de configuration de démarrage et que le fichier réussit un contrôle de validité, la configuration téléchargée prendra effet au prochain redémarrage de l'appareil WAP.
- Étape 6** Cliquez sur **Save** pour commencer la mise à niveau ou la sauvegarde. Pour les téléchargements HTTP/HTTPS, une fenêtre s'affiche afin de vous permettre de sélectionner le fichier à télécharger.
- Avertissement** Veillez à ce que l'appareil WAP soit en permanence alimenté lors du téléchargement du fichier de configuration. En cas de panne de courant lors du téléchargement du fichier de configuration, ce dernier est perdu et le processus doit être redémarré.
-

Copie des fichiers de configuration

Vous pouvez copier les fichiers dans le système de fichiers de l'appareil WAP. Vous pouvez par exemple copier le fichier de configuration de sauvegarde dans le type de fichier de configuration de démarrage, afin qu'il soit utilisé lors du prochain démarrage de l'appareil WAP.

Pour copier un fichier vers un autre type de fichier :

-
- Étape 1** Sélectionnez **Administration > Fichiers de configuration > Copier**.
- Étape 2** Dans le champ Copier depuis, sélectionnez l'un des types de fichiers sources suivants à copier :
- **Configuration de démarrage** : fichier de configuration utilisé pour le démarrage.
 - **Configuration de sauvegarde** : fichier de configuration de sauvegarde enregistré sur l'appareil WAP.
 - **Configuration miroir** : si la configuration de démarrage n'est pas modifiée pendant au moins 24 heures, elle est automatiquement enregistrée dans un fichier de configuration miroir. La configuration miroir est un instantané d'une configuration de démarrage antérieure. La configuration miroir est conservée malgré les restaurations des paramètres d'usine. Elle peut donc être utilisée pour récupérer une configuration système après une restauration des paramètres d'usine en copiant la configuration miroir vers la configuration de démarrage.
- Étape 3** Dans le champ Vers, sélectionnez le type de fichier à remplacer par le fichier que vous copiez.
- Étape 4** Cliquez sur **Save** pour commencer la copie.
-

Suppression des fichiers de configuration

Vous pouvez effacer le fichier de configuration de démarrage ou de configuration de sauvegarde. Si vous effacez le fichier de configuration de démarrage, le fichier de configuration de sauvegarde s'activera lors du prochain redémarrage de l'appareil WAP.

Pour supprimer le fichier de configuration de démarrage ou de configuration de sauvegarde :

-
- Étape 1** Sélectionnez **Administration > Fichiers de configuration > Effacer**.
- Étape 2** Sélectionnez **Configuration de démarrage** ou **Configuration de sauvegarde**.
- Étape 3** Cliquez sur **Clear Files**.
- Étape 4** Cliquez sur **OK**.
-

Redémarrage

Utilisez la page Redémarrage pour redémarrer l'appareil WAP ou rétablir ses paramètres d'usine par défaut. Pour redémarrer ou réinitialiser l'appareil WAP, procédez comme suit :

-
- Étape 1** Sélectionnez **Administration > Redémarrage**.

- Étape 2** Pour redémarrer l'appareil WAP à l'aide du fichier de configuration par défaut, cochez la case **Rétablir les paramètres d'usine par défaut**. Tous les paramètres personnalisés sont perdus.
- Étape 3** Cliquez sur **Reboot** (Redémarrer). Une fenêtre s'affiche vous invitant à confirmer ou annuler le redémarrage.
- Étape 4** Cliquez sur **OK** pour redémarrer.
-

Programmer le redémarrage

Pour programmer un redémarrage sur l'appareil WAP, procédez comme suit :

Étape 1 Cochez la case **Programmer le redémarrage** pour activer cette fonction.

Étape 2 Deux options sont disponibles pour programmer un redémarrage.

- **Date** : définissez la date et l'heure exactes du redémarrage de l'appareil.
- **Dans** : définissez l'heure du redémarrage après l'activation de la fonction.

Remarque Pour **Dans**, le programmeur de redémarrage est toujours effectif après le redémarrage de l'appareil.

Étape 3 Cliquez sur **Enregistrer**.



CHAPITRE 10

Résolution des problèmes

Ce chapitre explique comment configurer la capture de paquets sur plusieurs appareils WAP à des fins de dépannage. Elle contient les rubriques suivantes :

- [Capture de paquets, à la page 111](#)
- [Informations relatives au support, à la page 117](#)

Capture de paquets

La fonction de capture de paquets sans fil permet de capturer et de stocker les paquets reçus et transmis par l'appareil WAP. Les paquets capturés peuvent ensuite être analysés par un analyseur de protocole réseau pour des opérations de dépannage ou d'optimisation des performances.

Les deux méthodes de capture de paquets sont les suivantes :

- **Méthode de capture locale** : les paquets capturés sont stockés dans un fichier sur l'appareil WAP. L'appareil WAP peut transférer le fichier vers un serveur TFTP. Le fichier est mis au format pcap et peut être examiné à l'aide de l'outil Wireshark. Vous pouvez sélectionner **Enregistrer le fichier sur cet appareil** pour sélectionner la méthode de capture locale.
- **Méthode de capture distante** : les paquets capturés sont redirigés en temps réel vers un ordinateur externe qui exécute l'outil Wireshark. Vous pouvez sélectionner **Envoyer en flux vers un hôte distant** pour sélectionner la méthode de capture distante.

Les paquets capturés peuvent être redirigés en temps réel vers CloudShark, un décodeur de paquets et un analyseur, similaire à WireShark pour l'analyse des paquets. Pour utiliser la méthode de capture distante, choisissez l'option **Envoyer vers CloudShark**.

l'appareil WAP peut capturer les types de paquets suivants :

- Les paquets 802.11 reçus et transmis sur les interfaces radio. Les paquets capturés sur les interfaces radio incluent l'en-tête 802.11.
- Les paquets 802.3 reçus et transmis sur l'interface Ethernet.
- Les paquets 802.3 reçus et transmis sur les interfaces logiques internes, telles que les interfaces VAP et WDS.

Utilisez la page Capture de paquets pour configurer les paramètres de capture de paquets, démarrer une capture locale ou distante, afficher l'état de capture actuel et télécharger un fichier de capture de paquets.

Capture de paquets locale

Pour initier une capture de paquets locale :

-
- Étape 1** Sélectionnez **Résolution des problèmes > Capture de paquets**.
- Étape 2** Assurez-vous que la méthode de capture de paquets est définie sur **Enregistrer le fichier sur cet appareil**.
- Étape 3** Définissez les paramètres suivants :
- **Interface** : saisissez un type d'interface de capture pour la capture de paquets :
 - **Ethernet** : trafic 802.3 sur le port Ethernet.
 - **Radio 1/Radio 2** : trafic 802.11 sur l'interface radio.
 - **Durée** : saisissez la durée de la capture, en secondes. La plage valide est de 10 à 3600. La valeur par défaut est 60.
 - **Taille de fichier maximale** : saisissez la taille maximale autorisée pour le fichier de capture, en kilooctets (Ko). La plage valide est de 64 à 4096. La valeur par défaut est 1024.
- Étape 4** Les deux modes de capture de paquets sont les suivants :
- **Tout le trafic sans fil** : tous les paquets sans fil sont capturés.
 - **Trafic vers/depuis ce point d'accès** : les paquets envoyés ou reçus par le point d'accès sont capturés.
- Étape 5** Cliquez sur **Activer les filtres**. Trois cases à cocher sont disponibles (**Ignorer les balises, Filtrer sur Client, Filtrer sur SSID**).
- **Ignorer les balises** : active ou désactive la capture des balises 802.11 détectées ou transmises par radio.
 - **Filtrer sur Client** : spécifie l'adresse MAC pour le filtre de client WLAN. Notez que le filtre de client est uniquement actif lorsqu'une capture est réalisée sur une interface 802.11.
 - **Filtrer sur SSID** : sélectionnez un nom de SSID pour la capture de paquets.
- Étape 6** Cliquez sur **Enregistrer les paramètres**. Les modifications sont enregistrées dans la configuration de démarrage.
- Étape 7** Cliquez sur **Démarrer la capture**, puis sur **Actualiser** pour mettre à jour le champ **État de la capture de paquets**, qui contient les données suivantes :
- a) **Statut de capture actuel**
 - b) **Durée de capture de paquets**
 - c) **Taille du fichier de capture de paquets**
- En mode Capture de fichiers de paquets, l'appareil WAP stocke les paquets capturés dans le système de fichiers RAM. Une fois l'activation terminée, la capture de paquets s'effectue jusqu'à ce que l'un des événements suivants se produise :
- La durée de capture atteint la durée configurée.
 - Le fichier de capture atteint sa taille maximale.
 - L'administrateur arrête la capture.
-

Capture de paquets distante

La fonction Capture de paquets distante vous permet de spécifier un port distant comme port de destination des captures de paquets. Cette fonction opère conjointement avec l'outil d'analyse réseau Wireshark pour Windows. Un serveur de capture de paquets est exécuté sur l'appareil WAP et envoie les paquets capturés via une connexion TCP vers l'outil Wireshark. Wireshark est un outil open source disponible gratuitement ; vous pouvez le télécharger à l'adresse <https://www.wireshark.org/>.

Un ordinateur Microsoft Windows exécutant l'outil Wireshark vous permet d'afficher, de journaliser et d'analyser le trafic capturé. La fonction de capture de paquets distante est une fonction standard de l'outil Wireshark pour Windows. La version Linux ne fonctionne pas avec l'appareil WAP.

Lorsque le mode de capture distante est utilisé, l'appareil WAP ne stocke pas les données capturées localement dans son système de fichiers.

Si un pare-feu est installé entre l'ordinateur Wireshark et l'appareil WAP, le trafic de ces ports doit être autorisé à traverser le pare-feu. Le pare-feu doit aussi être configuré pour autoriser l'ordinateur Wireshark à initier une connexion TCP vers l'appareil WAP.

Envoyer vers un hôte distant

Pour démarrer une capture distante sur un appareil WAP qui utilise l'option Envoyer vers un hôte distant :

-
- Étape 1** Sélectionnez **Résolution des problèmes > Capture de paquets**.
- Étape 2** Sous **Méthode de capture de paquets**, cliquez sur le bouton radio **Envoyer en flux vers un hôte distant**.
- Étape 3** Dans le champ Port de capture distante, utilisez le port par défaut (2002) ou, si vous utilisez un autre port que celui par défaut, saisissez le numéro de port souhaité pour la connexion de Wireshark à l'appareil WAP. La plage de ports est comprise entre 1025 et 65530.
- Étape 4** Les deux modes de capture de paquets sont les suivants :
- **Tout le trafic sans fil** : tous les paquets sans fil sont capturés.
 - **Trafic vers/depuis ce point d'accès** : les paquets envoyés ou reçus par le point d'accès sont capturés.
- Étape 5** Cochez la case **Activer les filtres**. Sélectionnez ensuite l'une des options suivantes :
- **Ignorer les balises** : active ou désactive la capture des balises 802.11 détectées ou transmises par radio.
 - **Filtrer sur Client** : spécifie l'adresse MAC pour le filtre de client WLAN. Notez que le filtre de client est uniquement actif lorsqu'une capture est réalisée sur une interface 802.11.
 - **Filtrer sur SSID** : sélectionnez un nom de SSID pour la capture de paquets.
- Étape 6** Si vous souhaitez enregistrer les paramètres en vue d'une utilisation ultérieure, cliquez sur **Save**. Toutefois, la sélection de la méthode de capture de paquets distante n'est pas enregistrée.
- Étape 7** Cliquez sur **Démarrer la capture** pour lancer la capture. Pour arrêter la capture, cliquez sur **Arrêter la capture**.
-

Envoyer vers CloudShark

Pour démarrer une capture distante sur un appareil WAP qui utilise l'option **Envoyer vers CloudShark**, procédez comme suit ::

-
- Étape 1** Sélectionnez **Dépannage > Capture de paquets**.
- Étape 2** Pour définir la **Méthode de capture de paquets**, cochez la case **Envoyer vers CloudShark**.
- Étape 3** Configurez les paramètres suivants:
- Interface : spécifiez un type d'interface de capture pour la capture de paquets.
 - Ethernet : trafic 802.3 sur le port Ethernet.
 - Radio 1 (2,4 GHz)/Radio 2 (5 GHz) : trafic 802.11 sur l'interface radio.
 - Durée : spécifiez la durée (en secondes) de la capture. Aucune limite de durée avec CloudShark. La valeur par défaut est 60.
 - URL CloudShark : saisissez le nom d'hôte de CloudShark. L'URL par défaut est : <https://www.cloudshark.org>
 - Clé d'API CloudShark : saisissez le jeton d'API valide que vous avez enregistré depuis CloudShark.
- Étape 4** La communication avec CloudShark s'effectue selon le protocole HTTPS. Si vous souhaitez utiliser un certificat SSL autosigné, sélectionnez Oui, puis cliquez sur Charger un certificat pour charger le certificat que vous avez signé.
- Étape 5** Indiquez les protocoles que vous souhaitez capturer dans le champ Expression de filtre. Seuls les paquets filtrés sont ensuite transférés sur CloudShark.
- Étape 6** Les deux modes de capture de paquets sont les suivants :
- Tout le trafic sans fil** : tous les paquets sans fil sont capturés.
 - Trafic vers/depuis ce point d'accès** : les paquets envoyés depuis le point d'accès ou reçus par le point d'accès sont capturés.
- Étape 7** Cliquez sur **Activer les filtres**. Les trois options suivantes sont disponibles :
- Ignorer les balises** : active ou désactive la capture des balises 802.11 détectées ou transmises par radio.
 - Filtrer sur Client** : spécifie l'adresse MAC pour le filtre Client WLAN.
- Remarque** Le filtre Client n'est actif que lorsqu'une capture est réalisée sur une interface 802.11.
- Filtrer sur SSID** : sélectionnez un nom de SSID pour la capture de paquets.
- Étape 8** Cliquez sur **Enregistrer**. Les modifications sont enregistrées dans la configuration de démarrage.
- Étape 9** Cliquez sur **Démarrer la capture**. En mode Capture de paquets, les paquets capturés sont transmis au site CloudShark en temps réel. Une fois l'activation terminée, la capture de paquets se poursuit jusqu'à ce que l'un des événements suivants se produise :
- La durée de capture atteint la durée configurée.
 - Le fichier de capture atteint sa taille maximale.
 - L'administrateur arrête la capture.
-

Wireshark

Vous devez tout d'abord télécharger Wireshark et l'installer sur votre ordinateur. Vous pouvez télécharger cet outil depuis <https://www.wireshark.org/>.

Pour lancer l'outil d'analyse réseau Wireshark pour Microsoft Windows, procédez comme suit :

- Étape 1** Sur votre ordinateur, lancez l'outil Wireshark.
- Étape 2** Dans le menu, cliquez sur **Capture > Options**. Une fenêtre contextuelle s'affiche.

- Étape 3** Dans le champ Interface, sélectionnez **Distante**. Une fenêtre contextuelle s'affiche.
- Étape 4** Dans le champ Hôte, saisissez l'adresse IP de l'appareil WAP.
- Étape 5** Dans le champ Port, saisissez le numéro de port de l'appareil WAP. Par exemple, saisissez 2002 si vous avez utilisé le port par défaut ou saisissez le numéro de port si vous avez utilisé un autre port que le port par défaut.
- Étape 6** Cliquez sur **OK**.
- Étape 7** Sélectionnez l'interface à partir de laquelle vous devez capturer les paquets. Dans la fenêtre contextuelle Wireshark, en regard de l'adresse IP, un menu déroulant vous permet de sélectionner les interfaces. L'interface peut être l'une des suivantes :

```
Linux bridge interface in the wap device
--rpcap://[192.168.1.220]:2002/brtrunk

Wired LAN interface
-- rpcap://[192.168.1.220]:2002/eth0

VAP0 traffic on radio 1
-- rpcap://[192.168.1.220]:2002/wlan0

802.11 traffic
-- rpcap://[192.168.1.220]:2002/radio1

At WAP361, VAP1 ~ VAP7 traffic
-- rpcap://[192.168.1.220]:2002/wlan0vap1 ~ wlan0vap7

At WAP150, VAP1 ~ VAP3 traffic
-- rpcap://[192.168.1.220]:2002/wlan0vap1 ~ wlan0vap3
```

Vous pouvez effectuer le suivi simultané de quatre interfaces maximum sur l'appareil WAP. Toutefois, vous devez démarrer une session Wireshark distincte pour chaque interface. Pour lancer des sessions de capture distante supplémentaires, répétez les étapes de configuration de l'outil Wireshark. Aucune configuration n'est requise sur l'appareil WAP.

Remarque Le système utilise quatre numéros de port consécutifs, en commençant par le port configuré pour les sessions de capture de paquets distante. Vérifiez que vous disposez de quatre numéros de port consécutifs. Si vous n'utilisez pas le port par défaut, nous vous recommandons d'utiliser un numéro de port supérieur à 1024.

Lorsque vous capturez le trafic sur l'interface radio, vous pouvez désactiver la capture des balises, mais les autres trames de contrôle 802.11 sont toujours envoyées à Wireshark. Vous pouvez configurer un filtre d'affichage de façon à afficher uniquement :

- Les trames de données dans le suivi.
- Le trafic sur des BSSID (Basic Service Set ID) spécifiques.
- Le trafic entre deux clients.

Voici quelques exemples de filtres d'affichage utiles :

- Exclure les balises et les trames ACK/RTS/CTS :
!(wlan.fc.type_subtype == 8 || wlan.fc.type == 1)
- Les trames de données uniquement :
wlan.fc.type == 2

- Le trafic sur un BSSID spécifique :
wlan.bssid == 00:02:bc:00:17:d0
- Tout le trafic de et vers un client spécifique :
wlan.addr == 00:00:e8:4e:5f:8e

En mode de capture distante, le trafic est envoyé vers l'ordinateur qui exécute Wireshark via l'une des interfaces réseau. Selon l'emplacement de l'outil Wireshark, le trafic peut être envoyé sur une interface Ethernet ou l'une des radios. Pour éviter un flux de trafic causé par le suivi des paquets, l'appareil WAP installe automatiquement un filtre de capture afin d'éliminer tous les paquets destinés à l'application Wireshark. Par exemple, si le port IP Wireshark est configuré sur 58 000, alors le filtre de capture suivant est automatiquement installé sur l'appareil WAP :

```
not port range 58000-58004
```

Pour des raisons de performances et de sécurité, le mode de capture de paquets n'est pas enregistré dans la NVRAM sur l'appareil WAP. En cas de réinitialisation de l'appareil WAP, le mode de capture est désactivé ; il est donc nécessaire de le réactiver pour reprendre la capture du trafic. Les paramètres de capture de paquets (autres que le mode) sont enregistrés dans la NVRAM.

L'activation de la fonction de capture de paquets peut engendrer un problème de sécurité : Des clients non autorisés sont susceptibles de pouvoir se connecter à l'appareil WAP et d'effectuer un suivi des données utilisateur. En outre, les performances de l'appareil WAP sont dégradées pendant la capture de paquets et cet impact négatif continue à être détecté dans une moindre mesure même lorsqu'il n'y a pas de session Wireshark active. Pour réduire cet impact sur les performances de l'appareil WAP pendant la capture du trafic, installez des filtres de capture afin de contrôler le trafic envoyé vers l'outil Wireshark. Pendant la capture du trafic 802.11, les trames capturées sont pour une grande partie des balises (généralement envoyées toutes les 100 ms par tous les points d'accès). Même si Wireshark prend en charge un filtre d'affichage pour les trames de balise, il ne prend pas en charge un filtre de capture empêchant l'appareil WAP de réacheminer les paquets de balises capturés vers l'outil Wireshark. Pour réduire l'impact de la capture des balises 802.11 sur les performances, désactivez le mode de capture des balises.

Téléchargement du fichier de capture de paquets

Vous pouvez télécharger un fichier de capture par TFTP vers un serveur TFTP configuré ou par HTTP/HTTPS vers un ordinateur. Une capture s'arrête automatiquement lors du déclenchement de la commande de téléchargement du fichier de capture.

Étant donné que le fichier de capture est stocké dans le système de fichiers RAM, il disparaît si l'appareil WAP est réinitialisé.

Pour télécharger un fichier de capture de paquets via TFTP :

-
- Étape 1** Cliquez sur **Télécharger sur le serveur TFTP**.
 - Étape 2** Spécifiez l'adresse IPv4 du serveur TFTP dans le champ prévu à cet effet.
 - Étape 3** Saisissez le nom de fichier du serveur TFTP à télécharger s'il diffère du nom par défaut. Par défaut, les paquets capturés sont stockés dans le fichier de dossiers /tmp/apcapture.pcap sur l'appareil WAP.
 - Étape 4** Cliquez sur **Download**.
-

Utilisation de HTTP

Pour télécharger un fichier de capture de paquets via HTTP :

-
- Étape 1** Cliquez sur **Télécharger sur cet appareil**. Un message de confirmation s'affiche dans une fenêtre contextuelle.
- Étape 2** Cliquez sur **OK**. Une fenêtre contextuelle apparaît. Elle vous permet de choisir l'emplacement d'enregistrement du fichier sur le réseau.
-

Informations relatives au support

La page Informations relatives à l'assistance affiche le statut du processeur et de la mémoire RAM.

Pour enregistrer et afficher l'activité du processeur et de la mémoire RAM, procédez comme suit :

-
- Étape 1** Sélectionnez **Résolution des problèmes > Informations relatives au support**.
- Étape 2** Cliquez sur **Processeur** pour enregistrer et afficher l'activité du processeur. Pour arrêter l'enregistrement, cliquez de nouveau sur **Processeur**.
- Étape 3** Cliquez sur **Mémoire RAM** pour enregistrer et afficher l'activité de la mémoire RAM. Pour arrêter l'enregistrement, cliquez de nouveau sur **Mémoire RAM**.
- Le graphique indique le statut du processeur/de la mémoire RAM, comme suit :
- Une ligne bleue indique l'activité du processeur.
 - Une ligne rouge indique l'activité de la mémoire RAM.
 - Le premier graphique à courbes met à jour les données toutes les secondes. Il affiche l'activité du processeur/de la mémoire RAM en 60 secondes.
 - Le deuxième graphique à courbes met à jour les données toutes les 5 secondes. Il affiche l'activité du processeur/de la mémoire RAM en 5 minutes.
- Étape 4** Cliquez sur **Enregistrer**.
-

Télécharger les données du processeur/de la mémoire RAM

Utilisez la page Informations relatives à l'assistance pour télécharger l'activité du processeur/de la mémoire RAM correspondant à la période sélectionnée. Vous pouvez fournir ce fichier texte aux membres de l'assistance technique pour les aider à résoudre les différents problèmes. Pour télécharger les données du processeur/de la mémoire RAM, procédez comme suit :

-
- Étape 1** Sélectionnez **Résolution des problèmes > Informations relatives au support**.
- Étape 2** Dans la section Télécharger les données, cochez la case **Activer** pour activer le téléchargement.

- Étape 3** Sélectionnez la période pour le téléchargement des données : **Aujourd'hui, 7 derniers jours, 30 derniers jours, Tout, Personnalisé.**
- Étape 4** Renseignez les champs **À** et **De** au format aaaa-mm-jj, puis définissez l'heure au format hh:mm:ss.
- Étape 5** Cliquez sur **Télécharger** pour générer le fichier à partir des paramètres système actuels. Après un bref instant, une fenêtre s'affiche pour vous permettre d'enregistrer le fichier sur votre ordinateur.
-



ANNEXE **A**

Codes des motifs des messages de désauthentification

Cette annexe contient les sections suivantes:

- [Codes des motifs des messages de désauthentification, à la page 119](#)
- [Tableau des codes des motifs de désauthentification, à la page 119](#)

Codes des motifs des messages de désauthentification

Lorsqu'un client se désauthentifie du périphérique WAP, un message est envoyé au journal système. Ce message contient un code de motif pouvant être utile pour déterminer pourquoi le client a été désauthentifié. Vous pouvez afficher les messages du journal en cliquant sur **Configuration du système > Notification > Afficher le journal du système**.

Pour plus d'informations, voir, [Tableau des codes des motifs de désauthentification, à la page 119](#).

Tableau des codes des motifs de désauthentification

Le tableau suivant décrit les codes des motifs de désauthentification

Tableau 2 : Tableau des codes des motifs de désauthentification

Code de motif	Signification
0	Réservé
1	Motif non spécifié
2	L'authentification précédente n'est plus valide
3	Désauthentification due au fait que la station émettrice quitte ou a quitté l'ensemble de services de base indépendants (IBSS, Independent Basic Service Set) ou l'ESS
4	Désassociation due à l'inactivité
5	Désassociation due au fait que le périphérique WAP n'est pas capable de gérer l'ensemble des stations actuellement associées

Code de motif	Signification
6	Trame de classe 2 reçue d'une station non authentifiée
7	Trame de classe 3 reçue d'une station non associée
8	Désassociation due au fait que la station émettrice quitte ou a quitté l'ensemble de services de base (BSS, Basic Service Set)
9	La station qui demande l'association ou la réassociation n'est pas authentifiée avec la station répondante
10	Désassociation due au fait que les informations figurant dans l'élément de capacité d'alimentation ne sont pas acceptables
11	Désassociation due au fait que les informations figurant dans l'élément des canaux pris en charge ne sont pas acceptables
12	Réservé
13	Élément non valide, par exemple un élément défini dans cette norme et dont le contenu ne satisfait pas aux spécifications figurant dans la clause
14	Échec du code d'intégrité du message (MIC, Message Integrity Code)
15	Délai d'expiration de connexion en quatre étapes
16	Délai d'expiration de connexion de clé de groupe
17	Élément de connexion en quatre étapes différent de la trame Demande/Réponse de la sonde/Balise d'association ou de réassociation
18	Chiffrement de groupe non valide
19	Chiffrement par paire non valide
20	AKMP non valide
21	Version RSNE non prise en charge
22	Capacités RSNE non valides
23	Échec de l'authentification IEEE 802.1X
24	Suite de chiffrement rejetée en raison de la stratégie de sécurité



ANNEXE **B**

Pour en savoir plus

Cette annexe contient les sections suivantes:

- [Pour en savoir plus, à la page 121](#)

Pour en savoir plus

Assistance

Communauté d'assistance Cisco	http://www.cisco.com/go/smallbizsupport
Assistance et ressources Cisco	http://www.cisco.com/go/smallbizhelp
Coordonnées de l'assistance téléphonique	http://www.cisco.com/c/en/us/support/web/tsd-cisco-small-business-support-center-contacts.html
Téléchargement des microprogrammes Cisco	http://www.cisco.com/go/smallbizfirmware Sélectionnez un lien pour télécharger le microprogramme correspondant à votre produit Cisco. Aucune connexion n'est requise.
Demandes concernant les solutions Open Source Cisco	Si vous souhaitez recevoir une copie du code source auquel vous avez droit dans le cadre de la ou des licences gratuites ou Open Source (telles que la Licence publique générale/amointrie GNU), envoyez votre demande à l'adresse : external-opensource-requests@cisco.com . Dans votre demande, indiquez le nom et la version du produit Cisco, ainsi que le numéro de référence à 18 chiffres (par exemple : 7XEEX17D99-3X49X08 1) qui figure dans la documentation Open Source du produit.
Guide d'administration du Cisco WAP125	http://www.cisco.com/go/100_wap_resources
Adaptateurs secteur Cisco	http://www.cisco.com/go/wap_accessories

