GUIDE D'ADMINISTRATION

Point d'accès Cisco WAP571 bibande sans fil AC/N Premium avec PoE

Point d'accès extérieur bibande sans fil AC/N Premium Cisco WAP571/E

Sommaire

1

Prise en main

Cette section offre une introduction à l'utilitaire de configuration Web des périphériques WAP (Wireless Access Point) et inclut les rubriques suivantes :

- **Démarrage de l'utilitaire de configuration Web**
- **Utilisation de l'assistant d'installation de point d'accès**
- **Prise en main**
- **Navigation dans les fenêtres**

Démarrage de l'utilitaire de configuration Web

Cette section décrit la configuration système requise ainsi que la manière de se déplacer dans l'utilitaire de configuration Web.

Navigateurs pris en charge

- Internet Explorer 7.0 ou version ultérieure
- Chrome 5.0 ou version ultérieure
- Firefox 3.0 ou version ultérieure
- Safari 3.0 ou version ultérieure

Restrictions s'appliquant aux navigateurs

- Si vous utilisez Internet Explorer 6, vous ne pouvez pas utiliser directement une adresse IPv6 pour accéder au point d'accès. Vous pouvez néanmoins utiliser le serveur DNS (Domain Name System, système de noms de domaine) pour créer un nom de domaine contenant l'adresse IPv6, puis utiliser ce nom de domaine dans la barre d'adresse à la place de l'adresse IPv6.

- Si vous utilisez Internet Explorer 8, vous pouvez configurer les paramètres de sécurité à partir d'Internet Explorer. Sélectionnez **Outils > Options Internet**, puis sélectionnez l'onglet **Sécurité**. Sélectionnez **Intranet local**, puis **Sites**. Sélectionnez **Avancé**, puis **Ajouter**. Ajoutez l'adresse Intranet du point d'accès (http://*<adresse-ip>*) dans la zone Intranet locale. 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 locale.
- 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 au point d'accès depuis votre navigateur.

Déconnexion

Par défaut, l'utilitaire de configuration Web se déconnecte au bout de 10 minutes d'inactivité. Consultez la section **Service HTTP/HTTPS** pour obtenir des instructions sur la modification du délai d'expiration par défaut.

Pour vous déconnecter, cliquez sur **Déconnexion** en haut à droite de l'utilitaire de configuration Web.

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

La première fois que vous vous connectez au point d'accès (ou après avoir rétabli les 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 :

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

REMARQUE Si vous cliquez sur **Annuler** pour ignorer l'assistant, la page **Modifier le mot de passe** apparaît. Vous pouvez alors modifier le mot de passe de connexion par défaut. Pour l'ensemble des autres paramètres, les configurations d'usine par défaut s'appliquent.

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

ÉTAPE 1 Cliquez sur **Suivant** dans la page d'accueil de l'assistant. La fenêtre Configurer le périphérique – Mettre à niveau le microprogramme apparaît.

ÉTAPE 2 Cliquez sur le bouton Parcourir et recherchez le fichier image du microprogramme sur votre réseau.

REMARQUE 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 **Mettre à niveau** pour appliquer la nouvelle image du microprogramme. Sinon, cliquez sur **Ignorer pour afficher la fenêtre Configurer le périphérique – Restaurer la configuration**.

REMARQUE 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, le point d'accès redémarre et reprend son fonctionnement normal.

ÉTAPE 4 Cliquez sur le bouton **Parcourir** et recherchez le fichier de configuration sur votre réseau.

REMARQUE Le fichier de configuration doit être au format XML et contenir toutes les informations relatives aux paramètres du périphérique WAP.

ÉTAPE 5 Cliquez sur **Mettre à niveau** pour appliquer le fichier de configuration sélectionné. Sinon, cliquez sur **Ignorer pour afficher la fenêtre Configurer le périphérique - Adresse IP**.

REMARQUE : La restauration du fichier de configuration peut prendre plusieurs minutes. N'actualisez pas la page et n'ouvrez pas d'autre page pendant la restauration du fichier de configuration, car cela mettrait fin à l'opération de restauration. Une fois le processus terminé, le point d'accès redémarre et reprend son fonctionnement normal.

ÉTAPE 6 Cliquez sur **Adresse IP dynamique (DHCP)** si vous voulez que le périphérique WAP reçoive une adresse IP d'un serveur DHCP. Sinon, sélectionnez **Adresse IP statique** pour configurer manuellement l'adresse IP. Pour obtenir une description de ces champs, reportez-vous à **Paramètres IPv4**.

ÉTAPE 7 Cliquez sur **Suivant**. La fenêtre Configuration de point unique - Définissez une grappe apparaît. Pour obtenir une description de la configuration de point unique, reportez-vous à **Présentation de la configuration de point unique**.

ÉTAPE 8 Pour créer une nouvelle configuration de point unique de périphériques WAP, sélectionnez **Créer une grappe** et spécifiez un **Nom de la nouvelle grappe**. Si vous configurez vos périphériques avec le même nom de cluster et que vous activez le mode de configuration de point unique sur d'autres périphériques WAP, ils rejoignent automatiquement le groupe.

Si votre réseau possède déjà un cluster, vous pouvez lui ajouter ce périphérique en cliquant sur **Se connecter à une grappe existante**, puis en saisissant le nom du cluster existant dans le champ **Nom de la grappe existante**.

Si vous ne voulez pas que ce périphérique participe à la configuration de point unique pour le moment, cliquez sur **Ne pas activer la configuration de point unique**.

(Facultatif) Vous pouvez entrer du texte dans le champ Emplacement du point d'accès pour noter l'emplacement physique du périphérique WAP.

ÉTAPE 9 Cliquez sur **Suivant**. La fenêtre Configurer l'appareil - Définissez la date et l'heure du système apparaît.

ÉTAPE 10 Sélectionnez votre fuseau horaire, puis réglez l'heure système manuellement ou configurez le périphérique WAP de telle sorte qu'il obtienne l'heure à partir d'un serveur NTP. Pour obtenir une description de ces options, reportez-vous à **Paramètres d'heure**.

REMARQUE : La flèche à côté d'Heure système vous permet de configurer l'heure de l'ordinateur actuel si vous voulez utiliser l'heure et la date de votre ordinateur.

ÉTAPE 11 Cliquez sur **Suivant**. La fenêtre Activer la sécurité – Définissez le mot de passe apparaît.

ÉTAPE 12 Saisissez un **Nouveau mot de passe** et saisissez-le à nouveau dans le champ **Confirmer le mot de passe**. Vous pouvez modifier le nom d'utilisateur dans le champ **Nom d'utilisateur**. Pour obtenir plus d'informations sur les mots de passe, reportez-vous à **Comptes d'utilisateur**.

REMARQUE : Vous pouvez décocher la case Complexité du mot de passe si vous souhaitez désactiver les règles de sécurité de mot de passe. Nous vous recommandons toutefois fortement de conserver les règles de sécurité de mot de passe activées.

ÉTAPE 13 Cliquez sur **Suivant**. La fenêtre Activer la sécurité - Attribuez un nom à votre réseau sans fil apparaît pour l'interface Radio 1.

REMARQUE : Pour cette fenêtre et les deux fenêtres suivantes (Sécurité sans fil et ID VLAN), vous configurez ces paramètres pour l'interface Radio 1 en premier lieu. Puis, les fenêtres apparaissent à nouveau afin de vous permettre de configurer ces paramètres pour l'interface Radio 2.

ÉTAPE 14 Saisissez un **Nom de réseau**. Ce nom fait office de SSID pour le réseau sans fil par défaut.

ÉTAPE 15 Cliquez sur **Suivant**. La fenêtre Activer la sécurité - Sécurisez votre réseau sans fil apparaît.

ÉTAPE 16 Choisissez un type de cryptage de sécurité et entrez une clé de sécurité. Pour obtenir une description de ces options, reportez-vous à **Sécurité du système**.

ÉTAPE 17 Cliquez sur **Suivant**. L'assistant affiche la fenêtre Activer la sécurité - Attribuez l'ID de VLAN à votre réseau sans fil.

ÉTAPE 18 Entrez un 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) au trafic sans fil, afin de le séparer du trafic de gestion sur le VLAN 1.

ÉTAPE 19 Cliquez sur **Suivant**.

ÉTAPE 20 Dans le cas du périphérique WAP571/E, les pages Nom du réseau, Sécurité sans fil et ID de VLAN s'affichent en vue de permettre la configuration de Radio 2. Une fois la configuration de Radio 2 terminée, cliquez sur **Suivant**.

L'assistant affiche la fenêtre Activer le portail captif - Créez votre réseau invité.

ÉTAPE 21 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 29**.

Si vous cliquez sur **Oui**, l'assistant affiche la fenêtre Activer le portail captif - Attribuez au nom à votre réseau invité.

ÉTAPE 22 Spécifiez le **Nom du réseau invité** pour Radio 1. Dans le cas du périphérique WAP571/E, précisez si le réseau invité utilise **Radio 1** ou **Radio 2**.

ÉTAPE 23 Cliquez sur **Suivant**. L'assistant affiche la fenêtre Activer le portail captif - Sécurisez votre réseau invité.

ÉTAPE 24 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 **Sécurité du système**.

ÉTAPE 25 Cliquez sur **Suivant**. L'assistant affiche la fenêtre Activer le portail captif - Attribuez l'ID de VLAN.

ÉTAPE 26 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 27 Cliquez sur **Suivant**. L'assistant affiche la fenêtre Activer le portail captif - Activez l'URL de redirection.

ÉTAPE 28 Sélectionnez **Activer l'URL de redirection** et spécifiez un nom de domaine complet 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 29 Cliquez sur **Suivant**. L'assistant affiche la fenêtre Récapitulatif - Confirmez vos paramètres.

ÉTAPE 30 Vérifiez les paramètres que vous configurez. Cliquez sur **Retour** pour reconfigurer un ou plusieurs paramètres. Si vous cliquez sur **Annuler**, tous les paramètres sont rétablis aux valeurs précédentes ou par défaut.

ÉTAPE 31 S'ils sont corrects, cliquez sur **Soumettre**. Vos paramètres de configuration WAP sont enregistrés et une fenêtre de confirmation apparaît.

ÉTAPE 32 Cliquez sur **Terminer**. La fenêtre de connexion au point d'accès à l'aide du mot de passe modifié apparaît.

Prise en main

Afin de simplifier la configuration du périphérique grâce à une navigation rapide, la page Getting Started offre des liens permettant d'effectuer des tâches courantes. La page Prise en main est la fenêtre par défaut qui apparaît à chaque fois que vous vous connectez à l'utilitaire de configuration Web du point d'accès.

Catégorie	Nom du lien (sur la page)	Page correspondante
Configuration initiale	Exécuter l'assistant d'installation	Utilisation de l'assistant d'installation de point d'accès
	Configurer les paramètres de radio	Radio
	Configurer les paramètres de réseau sans fil	Réseaux
	Configurer les paramètres LAN	LAN
	Configurer un point unique	Présentation de la configuration de point unique
Statut du périphérique	Récapitulatif du système	Récapitulatif du système
	Statut du réseau sans fil	Interfaces réseau

Catégorie	Nom du lien (sur la page)	Page correspondante
Accès rapide	Modifier le mot de passe du compte	Comptes d'utilisateur
	Mettre à niveau le micrologiciel du périphérique	Gestion du micrologiciel
	Sauvegarder/Restaurer la configuration	Télécharger/ sauvegarder le fichier de configuration

Navigation dans les fenêtres

Servez-vous de la navigation pour parcourir l'utilitaire Web.

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. L'en-tête comporte les boutons suivants :

Volet de navigation / Menu principal

Nom du bouton	Description
(Utilisateur)	Nom du compte (Administrateur ou Invité) de l'utilisateur connecté au point d'accès. Le nom d'utilisateur par défaut est **cisco**.
Déconnexion	Sélectionnez cette option pour vous déconnecter de l'utilitaire de configuration Web du point d'accès.
Langue	Passez le pointeur de la souris sur le bouton et sélectionnez votre langue.
À propos de	Cliquez sur ce bouton pour afficher le type du point d'accès ainsi que son numéro de version.
Aide	Cliquez sur ce bouton pour afficher l'aide 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.

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 des périphériques 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 décrit les boutons couramment utilisés qui s'affichent sur différentes pages du système.

Nom du bouton	Description
Ajouter	Ajoute une nouvelle entrée à la table ou à la base de données.
Annuler	Annule les modifications apportées à la page.
Effacer tout	Efface toutes les entrées dans la table du journal.
À propos de	Cliquez sur ce bouton pour afficher le type du point d'accès ainsi que son numéro de version.
Supprimer	Supprime une entrée dans une table. Sélectionnez tout d'abord une entrée.
Modifier	Édite ou modifie une entrée existante. Sélectionnez tout d'abord une entrée.
Actualiser	Affiche à nouveau 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.

2

Statut et statistiques

Cette section explique comment afficher le statut et les statistiques, et elle contient les rubriques suivantes :

- **Récapitulatif du système**
- **Interfaces réseau**
- **Statistiques sur le trafic**
- **Statistiques de transfert de multidiffusion sans fil**
- **Transmission/Réception de pont de groupe de travail**
- **Clients associés**
- **Associations de client TSPEC**
- **Statut et statistiques TSPEC**
- **Statistiques de point d'accès TSPEC**
- **Statistiques sur la radio**
- **Statut des alertes par e-mail**
- **Journal**

Récapitulatif du système

La page Récapitulatif du système affiche des informations de base, telles que la description du modèle du matériel, la version du logiciel et le temps qui s'est écoulé depuis le dernier redémarrage.

Pour afficher les informations se rapportant au système, cliquez sur **Statut et statistiques** > **Récapitulatif du système**. Ou bien, sélectionnez **Récapitulatif du système** sous **État de l'appareil** à la page Mise en route.

La page Récapitulatif du système affiche les informations suivantes :

- **PID VID** : modèle et version du matériel WAP.
- **Numéro de série** : numéro de série du périphérique Cisco WAP.
- **Adresse MAC de base** : adresse MAC WAP.
- **Version du micrologiciel (image active)** : numéro de version du microprogramme 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 microprogramme de l'image de sauvegarde.
- **Somme de contrôle MD5 du micrologiciel (non active)** : somme de contrôle de l'image de sauvegarde.
- **Nom d'hôte** : nom affecté au périphérique.
- **Temps utilisation système** : temps qui s'est écoulé depuis le dernier redémarrage.
- **Heure système** : heure système actuelle.
- **Source d'alimentation** : le système bénéficie d'une alimentation PoE (Power over Ethernet) via un appareil PSE (Power Source Equipment) PoE.

Le tableau des services TCP/UDP affiche des informations de base sur les protocoles et les services fonctionnant sur le périphérique WAP.

- **Service** : nom du service, si ce dernier est disponible.
- **Protocole** : protocole de transport sous-jacent utilisé par le service (TCP ou UDP).

- **Adresse IP locale** : adresse IP, le cas échéant, d'un périphérique distant connecté à ce service sur le périphérique WAP. La valeur **Tout** indique que toutes les adresses IP sur le périphérique peuvent utiliser ce service.
- **Port local** : numéro de port du service.
- **Adresse IP distante** : adresse IP d'un hôte distant, le cas échéant, qui utilise ce service. La valeur **Tout** indique que le service est disponible pour l'ensemble des hôtes distants qui accèdent au système.
- **Port distant** : numéro de port de tout périphérique 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 Établie apparaissent dans la table. Les états TCP suivants sont disponibles :
  - **Écoute** : le service est à l'écoute des demandes de connexion.
  - **Actif** : une connexion est établie et les paquets sont transmis et reçus.
  - **Établie** : une session de connexion est établie entre le périphérique WAP et un serveur ou un client, selon le rôle de chaque périphérique par rapport à ce protocole.
  - **Attente** : la séquence de fermeture a été initiée et le périphérique WAP attend l'expiration d'un délai défini par le système (généralement 60 secondes) avant de fermer la connexion.

Vous pouvez cliquer sur **Actualiser** pour actualiser l'écran et afficher les informations les plus récentes.

Interfaces réseau

La page Interfaces réseau affiche les informations de configuration et d'état concernant les interfaces filaires et sans fil. Pour afficher des informations sur les interfaces réseau, sélectionnez Statut et statistiques > Interfaces réseau.

Les informations suivantes sont indiquées :

- **Statut du réseau local** : affiche des informations concernant l'interface LAN, notamment :
  - **Adresse MAC** : adresse MAC du périphérique WAP.
  - **Adresse IP** : adresse IP du périphérique WAP.

- **Masque de sous-réseau** : masque de sous-réseau du périphérique WAP.
- **Passerelle par défaut** : passerelle par défaut du périphérique WAP.
- **Serveur de noms de domaine-1** : adresse IP du serveur de noms de domaine 1 utilisé par le périphérique WAP.
- **Serveur de noms de domaine-2** : adresse IP du serveur de noms de domaine 2 utilisé par le périphérique WAP.
- **Adresse IPv6** : adresse IPv6 du périphérique WAP.
- **Adresse globale IPv6 configurée automatiquement** : adresse IPv6 globale configurée automatiquement.
- **Adresse IPv6 de liaison locale** : adresse IPv6 de liaison locale du périphérique WAP.
- **Passerelle IPv6 par défaut** : passerelle IPv6 par défaut du périphérique WAP.
- **IPv6-DNS-1** : adresse IPv6 du serveur DNS IPv6 1 utilisé par le périphérique WAP.
- **IPv6-DNS-2** : adresse IPv6 du serveur DNS IPv6 2 utilisé par le périphérique WAP.

Ces paramètres s'appliquent à l'interface interne. Pour modifier l'un de ces paramètres, cliquez sur le lien Modifier. Vous êtes redirigé sur la page **Paramètres IPv4**.

- **Statut des ports** : affiche le statut des interfaces LAN.
- **Interfaces** : numéro de l'interface Ethernet.
  - **Statut de la liaison** : état de l'interface Ethernet.
  - **Débit du port** : débit de l'interface Ethernet.
  - **Mode duplex** : mode duplex de l'interface Ethernet.
  - **Statut Green Ethernet** : l'état de l'interface Ethernet.

Pour modifier l'un de ces paramètres, cliquez sur le lien Modifier. Vous êtes redirigé sur la page **Paramètres des ports**.

- **État de VLAN** : affiche des informations concernant les VLAN existants, notamment :
  - **ID de VLAN** : identifiant du VLAN.
  - **Description** : description du VLAN.
  - **Eth** : l'interface est un membre balisé ou non balisé du VLAN.

Pour modifier l'un de ces paramètres, cliquez sur le lien Modifier. Vous êtes redirigé sur la page **Configuration du VLAN**.

- **Statut de la radio** : affiche des informations concernant les interfaces radio sans fil, notamment :
  - **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** : le 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.

Pour modifier l'un de ces paramètres, cliquez sur le lien Modifier. Vous êtes redirigé sur la page **Radio**.

- **Statut de l'interface** : affiche les informations d'état de chaque point d'accès virtuel (VAP, Virtual Access Point) et de chaque interface de système de distribution sans fil (WDS, Wireless Distribution System), notamment :
- **Interface** : interface sans fil du périphérique WAP.
- **Nom (SSID)** : nom de l'interface sans fil.
- **Statut** : état administratif (opérationnel ou non opérationnel) du point d'accès virtuel.
- **Adresse MAC** : adresse MAC de l'interface radio.
- **ID de VLAN** : ID de VLAN de l'interface radio.

- **Profil** : nom de tout profil de planificateur associé.
- **État** : état actuel (actif ou inactif). L'état indique si le point d'accès virtuel échange des données avec un client.

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

Statistiques sur le trafic

La page Statistiques sur le trafic permet d'afficher des informations de base sur le périphérique WAP. Elle offre également un affichage en temps réel des statistiques de transmission et de réception de l'interface Ethernet, des points d'accès virtuels et de toute interface WDS. Toutes les statistiques de transmission et de réception reflètent les totaux obtenus depuis le dernier démarrage du périphérique WAP. Si vous avez redémarré le périphérique WAP, ces données chiffrées indiquent les totaux de transmission et de réception depuis le redémarrage.

Pour afficher la page Statistiques sur le trafic, sélectionnez **Statut et statistiques** > **Statistiques sur le trafic**.

La page Statistiques sur le trafic affiche des données récapitulatives et des statistiques sur le trafic dans chaque direction.

- **Interface réseau** : nom de l'interface Ethernet et de chaque interface de point d'accès virtuel et WDS.

  WLAN0 et WLAN1 précèdent le nom de l'interface de point d'accès virtuel afin d'indiquer l'interface radio (WLAN0 représente la radio 1 et WLAN1 représente la radio 2).
- **Nombre total de paquets** : nombre total de paquets envoyés (dans la table Transmis) ou reçus (dans la table Reçus) par ce périphérique WAP.
- **Nombre total d'octets** : nombre total d'octets envoyés (dans la table Transmis) ou reçus (dans la table Reçus) par ce périphérique WAP.
- **Nombre total de paquets abandonnés** : nombre total de paquets abandonnés envoyés (dans la table Transmis) ou reçus (dans la table Reçus) par ce périphérique WAP.

- **Nombre total d'octets abandonnés** : nombre total d'octets abandonnés envoyés (dans la table Transmis) ou reçus (dans la table Reçus) par ce périphérique WAP.
- **Erreurs** : nombre total d'erreurs relatives à l'envoi et à la réception de données sur ce périphérique WAP.

Vous pouvez cliquer sur **Actualiser** pour actualiser l'écran et afficher les informations les plus récentes.

Statistiques de transfert de multidiffusion sans fil

La page **Statistiques de transfert de multidiffusion sans fil** fournit des informations basiques sur le point d'accès actuel et affiche des statistiques en temps réel de transmission et de réception concernant l'interface Trafic multidestination sans fil du point d'accès et concernant les points d'accès virtuels sur les deux interfaces radio. Toutes les statistiques de transmission et de réception affichées reflètent les totaux obtenus depuis le dernier démarrage du point d'accès. Si vous avez redémarré le point d'accès, ces données chiffrées indiquent les totaux de transmission et de réception depuis le redémarrage.

Pour afficher la page Statistiques de transfert de multidiffusion sans fil, sélectionnez **Statut et statistiques > Statistiques de transfert de multidiffusion sans fil** dans le volet de navigation.

Statistiques de transmission et de réception

- **Interface réseau** : nom de l'interface Ethernet et de chaque interface de point d'accès virtuel et WDS.

  WLAN0 et WLAN1 précèdent le nom de l'interface de point d'accès virtuel afin d'indiquer l'interface radio (WLAN0 représente la radio 1 et WLAN1 représente la radio 2).
- **Données de multidiffusion-Trames** : affiche les trames de données multidestination reçues.
- **Données de multidiffusion-Transférées** : affiche les trames de données multidestination réacheminées.
- **Données de multidiffusion-Inondées** : affiche les trames de données multidestination inondées.
- **Données de multidiffusion-Envoyées** : affiche les trames de données multidestination envoyées.

- **Données de multidiffusion-Abandonnées** : affiche les trames de données multidestination abandonnées.
- **Cache MFDB-Correspondances** : affiche les correspondances du cache MFDB.
- **Cache MFDB-Échecs** : affiche les échecs du cache MFDB.

Statistiques IGMP

- **Interface réseau** : nom de l'interface Ethernet et de chaque interface de point d'accès virtuel et WDS.

  WLAN0 et WLAN1 précèdent le nom de l'interface de point d'accès virtuel afin d'indiquer l'interface radio (WLAN0 représente la radio 1 et WLAN1 représente la radio 2).
- **Trames IGMP** : affiche les trames IGMP reçues.
- **Trames IGMP-Transférées** : affiche les requêtes d'appartenance IGMP reçues.
- **Trames IGMP-Envoyées** : affiche les rapports d'appartenance IGMP consultés.
- **Cache MFDB-Correspondances** : affiche les correspondances du cache MFDB.
- **Cache MFDB-Échecs** : affiche les échecs du cache MFDB.

Groupe de multidiffusion

- **Interface réseau** : nom de l'interface Ethernet et de chaque interface de point d'accès virtuel et WDS.

  WLAN0 et WLAN1 précèdent le nom de l'interface de point d'accès virtuel afin d'indiquer l'interface radio (WLAN0 représente la radio 1 et WLAN1 représente la radio 2).
- **Groupe de multidiffusion** : affiche l'adresse IP du groupe de multidestination.
- **Stations** : affiche l'adresse MAC de la station du groupe de multidestination.
- **Paquets** : affiche les paquets reçus des stations du groupe de multidestination.

Vous pouvez cliquer sur Actualiser pour actualiser l'écran et afficher les informations les plus récentes.

Transmission/Réception de pont de groupe de travail

La page Transmission/Réception de pont de groupe de travail affiche le nombre de paquets et d'octets du trafic entre postes sur un pont de groupe de travail. Pour obtenir des informations sur la configuration des ponts de groupe de travail, reportez-vous à la section **Pont de groupe de travail**.

Pour afficher la page Transmission/Réception de pont de groupe de travail, sélectionnez **Statut et statistiques** > **Pont de groupe de travail** dans le volet de navigation.

Chaque interface réseau configurée en tant qu'interface de pont de groupe de travail affiche les champs suivants :

- **Interface réseau** : nom de l'interface Ethernet ou de point d'accès virtuel. WLAN0 représente la radio 1 et WLAN1 représente la radio 2.
- **Statut et statistiques** : indique si l'interface est déconnectée ou si son état administratif est démarré ou arrêté.
- **ID de VLAN** : ID de réseau local virtuel (VLAN). Vous pouvez utiliser des VLAN pour créer plusieurs réseaux internes et invités sur le même périphérique WAP. L'ID de VLAN est défini dans l'onglet VAP.
- **Nom (SSID)** : nom du réseau sans fil. Également appelée SSID, cette clé alphanumérique identifie de manière unique un réseau local sans fil. Le SSID est défini dans l'onglet VAP.

Des informations supplémentaires s'affichent pour les directions de transmission et de réception pour chaque interface de pont de groupe de travail :

- **Nombre total de paquets** : nombre total de paquets pontés entre les clients filaires dans le pont de groupe de travail et le réseau sans fil.
- **Nombre total d'octets** : nombre total d'octets pontés entre les clients filaires dans le pont de groupe de travail et le réseau sans fil.

Vous pouvez cliquer sur **Actualiser** pour actualiser l'écran et afficher les informations les plus récentes.

Clients associés

Vous pouvez utiliser la page Clients associés pour afficher les postes client associés à un point d'accès particulier.

Pour afficher la page Clients associés, sélectionnez **Statut et statistiques** > **Clients associés**.

Les postes associés sont affichés avec des informations relatives au trafic des paquets transmis et reçus pour chaque poste.

- **Nombre total de clients associés** : le nombre total de clients actuellement associés au point d'accès.
- **Interface réseau** : point d'accès virtuel auquel le client est associé. WLAN0 et WLAN1 précèdent le nom de l'interface de point d'accès virtuel afin d'indiquer l'interface radio (WLAN0 représente la radio 1 et WLAN1 représente la radio 2).
- **Station** : adresse MAC du client sans fil associé.
- **Statut** : l'état authentifié et associé affiche l'état d'authentification et d'association IEEE 802.11 sous-jacent, qui est présent quel que soit le type de sécurité utilisé par le client pour se connecter au périphérique WAP. Cet état n'affiche pas l'état d'authentification ou d'association IEEE 802.1X.

  Quelques points importants sont à garder à l'esprit en ce qui concerne ce champ :

  - Si le mode de sécurité du périphérique WAP est Aucun ou WEP statique, l'état d'authentification et d'association des clients apparaît comme prévu, ce qui signifie que si un client s'affiche comme étant authentifié sur le périphérique WAP, il est capable de transmettre et de recevoir des données. (C'est la raison pour laquelle le mode WEP statique utilise uniquement l'authentification IEEE 802.11.)
  - Si le périphérique WAP utilise la sécurité IEEE 802.1X ou WPA, il se peut qu'une association de client apparaisse comme étant authentifiée (par le biais de la sécurité IEEE 802.11), bien qu'elle ne soit pas réellement authentifiée par la deuxième couche de sécurité.

- **De la station/À la station** : dans le cas de l'option De la station, les compteurs indiquent les paquets ou octets transmis par le client sans fil. Dans le cas de l'option À la station, les compteurs indiquent le nombre de paquets et d'octets transmis à partir du périphérique WAP vers le client sans fil.
  - **Paquets** : nombre de paquets reçus (transmis) à partir du client sans fil.
  - **Octets** : nombre d'octets reçus (transmis) à partir du client sans fil.
  - **Paquets abandonnés** : nombre de paquets abandonnés après leur réception (transmission).
  - **Octets abandonnés** : nombre d'octets abandonnés après leur réception (transmission).
  - **Paquets excédant le flux de trafic (De la station)** : nombre de paquets envoyés à partir d'un poste client vers le périphérique WAP au-delà de sa bande passante de liaison montante active de flux de trafic (TS, Traffic Stream) ou pour une catégorie d'accès nécessitant un contrôle d'admission auquel le poste client n'a pas été admis.
  - **Paquets excédant le flux de trafic (À la station)** : nombre de paquets envoyés à partir du périphérique WAP vers un poste client au-delà de sa bande passante de liaison descendante active de flux de trafic ou pour une catégorie d'accès nécessitant un contrôle d'admission auquel le poste client n'a pas été admis.
- **Temps de disponibilité** : temps pendant lequel le client a été associé au périphérique WAP.

Vous pouvez cliquer sur **Actualiser** pour actualiser l'écran et afficher les informations les plus récentes.

Associations de client TSPEC

La page Associations de client TSPEC fournit des informations en temps réel sur les données de client TSPEC transmises et reçues par ce point d'accès. Les tableaux de la page Associations de client TSPEC affichent les paquets voix et vidéo transmis et reçus depuis le démarrage de l'association, ainsi que des informations d'état.

Un TSPEC est une spécification de trafic envoyée à partir d'un client sans fil compatible QoS vers un périphérique WAP et nécessitant un certain niveau d'accès réseau pour le flux de trafic qu'il représente. Un flux de trafic est un ensemble de paquets de données identifiés par le client sans fil comme appartenant à une priorité d'utilisateur spécifique. Exemple de flux de trafic voix : combiné téléphonique CERTIFIÉ Wi-Fi marquant ses paquets de données générés par codec en tant que trafic de priorité voix. Exemple de flux de trafic vidéo : application de lecteur vidéo sur un ordinateur portable sans fil donnant la priorité à un flux de vidéoconférence à partir d'un serveur d'entreprise.

Pour afficher les statistiques des associations de client TSPEC, sélectionnez **Statut et statistiques > Associations de client TSPEC** dans le volet de navigation.

La page Associations de client TSPEC affiche les informations suivantes :

État et statistiques :

- **Interface réseau** : interface radio utilisée par le client. WLAN0 représente la radio 1 et WLAN1 représente la radio 2.
- **SSID** : identificateur d'ensemble de services associé à ce client de flux de trafic.
- **Station** : adresse MAC du poste client.
- **Identificateur de session de trafic** : identificateur de session de trafic TSPEC (plage de valeurs de 0 à 7).
- **Catégorie d'accès** : catégorie d'accès au flux de trafic (voix ou vidéo).
- **Direction** : direction du trafic pour ce flux de trafic. Les options possibles pour la direction sont les suivantes :
  - liaison ascendante : du client vers le périphérique (liaison montante).
  - liaison descendante : du périphérique vers le client (liaison descendante).
  - bidirectionnel : dans les deux sens.

- **Priorité d'utilisateur** : priorité d'utilisateur (UP, User Priority) de ce flux de trafic. La priorité d'utilisateur est envoyée avec chaque paquet dans la partie correspondante de l'en-tête IP. Les valeurs typiques sont les suivantes :
  - 6 ou 7 pour la voix
  - 4 ou 5 pour la vidéo

  La valeur peut varier en fonction des autres sessions de trafic de priorité.
- **Temps support** : temps pendant lequel le flux de trafic occupe le support de transmission.
- **Événements d'utilisation excédentaire** : nombre de fois que le client a dépassé le temps moyen établi pour son TSPEC. Les violations mineures et peu fréquentes sont ignorées.
- **Adresse MAC VAP** : adresse MAC de point d'accès virtuel.

Statistiques :

- **Interface réseau** : interface radio utilisée par le client.
- **Station** : adresse MAC du poste client.
- **Identificateur de session de trafic** : identificateur de session de trafic TSPEC (plage de valeurs de 0 à 7).
- **Catégorie d'accès** : catégorie d'accès au flux de trafic (voix ou vidéo).
- **Direction** : direction du trafic pour ce flux de trafic. Les options possibles pour la direction sont les suivantes :
  - liaison ascendante : du client vers le périphérique (liaison montante).
  - liaison descendante : du périphérique vers le client (liaison descendante).
  - bidirectionnel : dans les deux sens.
- **De la station** : affiche le nombre de paquets et d'octets reçus à partir du client sans fil.
  - **Paquets** : nombre de paquets excédentaires par rapport à un TSPEC admis.
  - **Octets** : nombre d'octets pour lesquels aucun TSPEC n'a été établi et avec une admission requise par le périphérique WAP.

- **À la station** : nombre de paquets et d'octets transmis à partir du périphérique WAP vers le client sans fil.
  - **Paquets** : nombre de paquets excédentaires par rapport à un TSPEC admis.
  - **Octets** : nombre d'octets pour lesquels aucun TSPEC n'a été établi et avec une admission requise par le périphérique WAP.

Vous pouvez cliquer sur **Actualiser** pour actualiser l'écran et afficher les informations les plus récentes.

Statut et statistiques TSPEC

La page Statut et statistiques TSPEC fournit les informations suivantes :

- Informations récapitulatives à propos des sessions TSPEC par radio
- Informations récapitulatives à propos des sessions TSPEC par point d'accès virtuel
- Statistiques en temps réel de transmission et de réception pour l'interface radio et la ou les interfaces réseau

Toutes les statistiques de transmission et de réception reflètent les totaux obtenus depuis le dernier démarrage du périphérique WAP. Si vous avez redémarré le périphérique WAP, ces données chiffrées indiquent les totaux de transmission et de réception depuis le redémarrage.

Pour afficher l'état et les statistiques TSPEC, sélectionnez **Statut et statistiques > Statut et statistiques TSPEC** dans le volet de navigation.

La page Statut et statistiques TSPEC fournit les informations d'état suivantes relatives aux interfaces WLAN (Radio) et de point d'accès virtuel :

- **Interface réseau** : nom de l'interface radio ou de point d'accès virtuel. WLAN0 représente la radio 1 et WLAN1 représente la radio 2.
- **Catégorie d'accès** : catégorie d'accès actuelle associée à ce flux de trafic (voix ou vidéo).
- **Statut** : indique si la session TSPEC est activée (démarrée) ou désactivée (arrêtée) pour la catégorie d'accès correspondante.

REMARQUE : L'état est un état de configuration, qui ne représente pas nécessairement l'activité de la session en cours.

- **Flux de trafic actif** : nombre de flux de trafic TSPEC actuellement actifs pour cette radio et cette catégorie d'accès.
- **Clients du flux de trafic** : nombre de clients de flux de trafic associés à cette radio et à cette catégorie d'accès.
- **Temps support alloué** : temps alloué à cette catégorie d'accès pour transporter des données sur le support de transmission. Cette valeur doit être inférieure ou égale à celle de la bande passante maximale autorisée sur le support pour ce flux de trafic.
- **Temps support non alloué** : temps de bande passante non utilisée pour cette catégorie d'accès.

Ces statistiques apparaissent séparément pour les chemins de transmission et de réception sur l'interface radio sans fil :

- **Catégorie d'accès** : catégorie d'accès associée à ce flux de trafic (voix ou vidéo).
- **Nombre total de paquets** : nombre total de paquets de flux de trafic envoyés (dans la table Transmis) ou reçus (dans la table Reçus) par cette radio pour la catégorie d'accès spécifiée.
- **Nombre total d'octets** : nombre total d'octets reçus dans la catégorie d'accès spécifiée.

Ces statistiques apparaissent séparément pour les chemins de transmission et de réception sur les interfaces réseau (points d'accès virtuels) :

- **Nombre total de paquets voix** : nombre total de paquets voix de flux de trafic envoyés (dans la table Transmis) ou reçus (dans la table Reçus) par ce périphérique WAP pour ce point d'accès virtuel.
- **Nombre total d'octets voix** : nombre total d'octets voix de flux de trafic envoyés (dans la table Transmis) ou reçus (dans la table Reçus) par ce périphérique WAP pour ce point d'accès virtuel.
- **Nombre total de paquets vidéo** : nombre total de paquets vidéo de flux de trafic envoyés (dans la table Transmis) ou reçus (dans la table Reçus) par ce périphérique WAP pour ce point d'accès virtuel.
- **Nombre total d'octets vidéo** : nombre total d'octets vidéo de flux de trafic envoyés (dans la table Transmis) ou reçus (dans la table Reçus) par ce périphérique WAP pour ce point d'accès virtuel.

Vous pouvez cliquer sur **Actualiser** pour actualiser l'écran et afficher les informations les plus récentes.

Statistiques de point d'accès TSPEC

La page Statistiques de point d'accès TSPEC fournit des informations sur les flux de trafic voix et vidéo acceptés et rejetés par le périphérique WAP. Pour afficher la page Statistiques de point d'accès TSPEC, sélectionnez **Statut et statistiques > Statistiques de point d'accès TSPEC** dans le volet de navigation.

- **Statistiques TSPEC pour ACM voix** : nombre total de flux de trafic voix acceptés et nombre total de flux de trafic voix rejetés.
- **Statistiques TSPEC pour ACM vidéo** : nombre total de flux de trafic vidéo acceptés et nombre total de flux de trafic vidéo rejetés.

Vous pouvez cliquer sur **Actualiser** pour actualiser l'écran et afficher les informations les plus récentes.

Statistiques sur la radio

Utilisez la page Statistiques sur la radio pour afficher des statistiques au niveau des paquets et des octets pour chaque interface radio sans fil. Pour afficher la page Statistiques sur la radio, sélectionnez **Statut et statistiques > Statistiques sur la radio** dans le volet de navigation.

Dans le cas du périphérique WAP571/E, sélectionnez la radio dont vous souhaitez afficher les statistiques.

- **Paquets reçus** : nombre total de paquets reçus par le périphérique WAP.
- **Paquets transmis** : nombre total de paquets transmis par le périphérique WAP.
- **Octets reçus** : nombre total d'octets reçus par le périphérique WAP.
- **Octest transmis** : nombre total d'octets transmis par le périphérique WAP.
- **Paquets reçus abandonnés** : nombre de paquets reçus par le périphérique WAP et abandonnés.
- **Paquets transmis abandonnés** : nombre de paquets transmis par le périphérique WAP et abandonnés.
- **Octets reçus abandonnés** : nombre d'octets reçus par le périphérique WAP et abandonnés.

- **Octets transmis abandonnés** : nombre d'octets transmis par le périphérique WAP et abandonnés.
- **Fragments reçus** : nombre de trames fragmentées reçues par le périphérique WAP.
- **Fragments transmis** : nombre de trames fragmentées envoyées par le périphérique WAP.
- **Trames de multidiffusion reçues** : nombre de trames MSDU reçues avec le bit de multidiffusion défini dans l'adresse MAC de destination.
- **Trames de multidiffusion transmises** : nombre de trames MSDU transmises avec succès et pour lesquelles le bit de multidiffusion était défini dans l'adresse MAC de destination.
- **Nombre de trames dupliquées** : nombre de fois qu'une trame a été reçue et que le champ Sequence Control indique qu'il s'agit d'un doublon.
- **Nombre de transmissions ayant échoué** : nombre de fois qu'une trame MSDU n'a pas été transmise avec succès, car le nombre de tentatives de transmission dépassait la limite de tentatives trames courtes ou la limite de tentatives trames longues.
- **Nombre d'erreurs FCS** : nombre d'erreurs FCS détectées dans une trame MPDU reçue.
- **Nombre de nouvelles tentatives de transmission** : nombre de fois qu'une trame MSDU a été transmise avec succès après une ou plusieurs tentatives.
- **Nombre d'échecs ACK** : nombre de trames ACK non reçues au moment où elles étaient attendues.
- **Nombre de trames RTS non reçues** : nombre de trames CTS non reçues en réponse à une trame RTS.
- **Trames indéchiffrables via WEP** : nombre de trames abandonnées, car ne pouvant pas être décryptées par la radio. Les trames peuvent être abandonnées parce qu'elles n'ont pas été décryptées ou parce qu'elles ont été décryptées avec une option de confidentialité non prise en charge par le périphérique WAP.
- **Nombre de trames RTS reçues** : nombre de trames CTS reçues en réponse à une trame RTS.

- **Nombre de nouvelles tentatives multiples** : nombre de fois qu'une trame MSDU a été transmise avec succès après plus d'une tentative.
- **Nombre de trames transmises** : nombre de trames MSDU transmises avec succès.

Vous pouvez cliquer sur **Actualiser** pour actualiser l'écran et afficher les informations les plus récentes.

Statut des alertes par e-mail

La page Statut des alertes par e-mail fournit des informations sur les alertes par e-mail envoyées sur la base des messages syslog générés par le périphérique WAP. Pour afficher la page Statut des alertes par e-mail, sélectionnez **Statut et statistiques > Statut des alertes par e-mail** dans le volet de navigation.

- **Statut des alertes par e-mail** : état configuré des alertes par e-mail. L'état est soit Activée soit Désactivée. La valeur par défaut est Désactivée.
- **Nombre d'e-mails envoyés** : nombre total de messages électroniques envoyés. La valeur est un entier de 32 bits, non affecté d'un signe. La valeur par défaut est 0.
- **Nombre d'e-mails non envoyés** : nombre total de messages électroniques ayant échoué. La valeur est un entier de 32 bits, non affecté d'un signe. La valeur par défaut est 0.
- **Heure d'envoi du dernier e-mail** : jour, date et heure d'envoi du dernier message électronique.

Vous pouvez cliquer sur **Actualiser** pour afficher les informations les plus récentes.

Journal

La page Journal répertorie les événements système qui ont généré une entrée de journal, comme les tentatives de connexion et les modifications de configuration. 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 512 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 la page Journal, sélectionnez **Statut et statistiques > Journal** dans le volet de navigation.

- **Horodatage** : heure système de l'occurrence de l'événement.
- **Gravité** : indique si l'événement est dû à une erreur (err) ou est fourni à titre indicatif (info).
- **Service** : composant logiciel associé à l'événement.
- **Description** : description de l'événement.

Vous pouvez cliquer sur **Actualiser** pour actualiser l'écran et afficher les informations les plus récentes.

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

3

Administration

Cette section explique comment configurer les paramètres système globaux et effectuer des diagnostics.

Elle contient les sections suivantes :

- **Paramètres système**
- **Comptes d'utilisateur**
- **Paramètres d'heure**
- **Paramètres des journaux**
- **Alerte par e-mail**
- **Affichage DEL**
- **Service HTTP/HTTPS**
- **Contrôle d'accès de gestion**
- **Gestion du micrologiciel**
- **Télécharger/sauvegarder le fichier de configuration**
- **Propriétés des fichiers de configuration**
- **Copier/enregistrer la configuration**
- **Redémarrer**
- **Détection - Bonjour**
- **Capture des paquets**
- **Informations relatives au support**
- **Paramètres de STP**

Paramètres système

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

Configuration des paramètres système

Pour définir les paramètres système :

ÉTAPE 1 Cliquez sur **Administration** > **Paramètres système**.

ÉTAPE 2 Configurez les paramètres suivants :

- **Nom d'hôte** : nom attribué de façon administrative au périphérique WAP. Par convention, il s'agit du nom de domaine complet du nœud. Le nom d'hôte par défaut est **wap** concaténé avec les 6 derniers chiffres hexadécimaux de l'adresse MAC du périphérique WAP. Les noms d'hôte ne peuvent comporter que des lettres, des chiffres et des tirets. Les noms d'hôte ne peuvent pas être précédés ni suivis 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** : personne à contacter pour le périphérique WAP. Le contact système peut comporter de 0 à 255 caractères et peut inclure des espaces et des caractères spéciaux.
- **Emplacement du système** : description de l'emplacement physique du périphérique 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.

Comptes d'utilisateur

Par défaut, un utilisateur de gestion est configuré sur le périphérique WAP :

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

Vous pouvez utiliser 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

Pour ajouter un nouvel utilisateur :

ÉTAPE 1 Sélectionnez **Administration** > **Comptes d'utilisateur** dans le volet de navigation.

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.

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

ÉTAPE 2 Cliquez sur **Ajouter**. Une nouvelle ligne de zones de texte s'affiche.

ÉTAPE 3 Cochez la case correspondant au nouvel utilisateur, puis sélectionnez **Modifier**.

ÉTAPE 4 Dans **Nom d'utilisateur**, saisissez un nom d'utilisateur constitué de 1 à 32 caractères alphanumériques. Les noms d'utilisateur ne peuvent comporter que les chiffres 0 à 9 et les lettres a à z (en majuscules ou minuscules).

ÉTAPE 5 Saisissez un **nouveau mot de passe** constitué de 1 à 64 caractères, puis saisissez le même mot de passe dans la zone de texte **Confirmer le nouveau mot de passe**.

Une fois que vous avez saisi un mot de passe, le nombre et la couleur des barres verticales changent pour indiquer la sécurité 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 une sécurité élevée.

ÉTAPE 6 Cliquez sur **Enregistrer**. Les modifications sont enregistrées dans la configuration de démarrage.

REMARQUE : Pour supprimer un utilisateur, cochez la case en regard de son nom, puis sélectionnez **Supprimer**. Pour enregistrer définitivement votre suppression, sélectionnez **Enregistrer** lorsque vous avez terminé.

Modification d'un mot de passe utilisateur

Pour modifier un mot de passe utilisateur :

ÉTAPE 1 Sélectionnez **Administration** > **Comptes d'utilisateur** dans le volet de navigation.

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 un **nouveau mot de passe** constitué de 1 à 64 caractères, puis saisissez le même mot de passe dans la zone de texte **Confirmer le nouveau mot de passe**.

Une fois que vous avez saisi un mot de passe, le nombre et la couleur des barres verticales changent pour indiquer la sécurité 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 une sécurité élevée.

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.

Paramètres d'heure

Une horloge système fournit un service d'horodatage synchronisé sur le réseau pour les événements logiciels, tels que les journaux de messages. Vous pouvez configurer l'horloge système manuellement ou configurer le périphérique 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 pour configurer le système afin qu'il récupère ses paramètres d'heure d'un serveur NTP préconfiguré. Par défaut, le point d'accès est configuré de manière à obtenir l'heure depuis une liste prédéfinie de serveurs NTP.

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

Pour utiliser NTP afin que le périphérique WAP acquière automatiquement ses paramètres d'heure :

Acquisition automatique des paramètres d'heure via NTP

Acquisition automatique des paramètres d'heure via NTP :

ÉTAPE 1 Pour le champ Source d'horloge système, sélectionnez **NTP (Network Time Protocol)**.

ÉTAPE 2 Définissez les paramètres suivants :

- **Nom/Adresse IPv4/IPv6 du serveur NTP** : 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 se composer d'une ou plusieurs étiquettes, elles-mêmes constituées d'un maximum de 63 caractères alphanumériques. Si un nom d'hôte inclut plusieurs étiquettes, elles sont séparées par un point (.). La série entière d'étiquettes et de points peut comporter jusqu'à 253 caractères.

- **Fuseau horaire** : sélectionnez le fuseau horaire où vous vous trouvez.

ÉTAPE 3 Sélectionnez **Prendre en compte l'heure d'été** si l'heure d'été s'applique à votre fuseau horaire. Si vous sélectionnez cette option, configurez les champs suivants :

- **Début de l'heure d'été** : sélectionnez l'heure, le jour, la semaine et le mois du passage à l'heure d'été.
- **Fin de l'heure d'été** : 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 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 Pour le champ Source d'horloge système, sélectionnez **Manuellement**.

ÉTAPE 2 Définissez les paramètres suivants :

- **Date du système** : sélectionnez le jour, le mois et l'année actuels dans les listes déroulantes.
- **Heure système** : sélectionnez l'heure et les minutes actuelles au format 24 heures, tel que 22:00:00.

REMARQUE : La flèche à côté d'Heure système vous permet de configurer l'heure de l'ordinateur actuel si vous voulez utiliser l'heure et la date de votre ordinateur.

- **Fuseau horaire** : sélectionnez le fuseau horaire où vous vous trouvez.

ÉTAPE 3 Sélectionnez **Prendre en compte l'heure d'été** si l'heure d'été s'applique à votre fuseau horaire. Si vous sélectionnez cette option, configurez les champs suivants :

- **Début de l'heure d'été** : sélectionnez l'heure, le jour, la semaine et le mois du passage à l'heure d'été.
- **Fin de l'heure d'été** : 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 4 Cliquez sur **Enregistrer**. Les modifications sont enregistrées dans la configuration de démarrage.

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.

Configuration du journal persistant

Si le système redémarre de manière inattendue, les messages de journal peuvent être utiles pour 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 de la journalisation persistante

Pour configurer la journalisation persistante :

ÉTAPE 1 Sélectionnez **Administration** > **Paramètres des journaux** dans le volet de navigation.

ÉTAPE 2 Configurez les paramètres suivants :

- **Persistance** : cliquez sur **Activer** pour enregistrer les journaux système dans la mémoire non volatile, afin de permettre la conservation des journaux au redémarrage du périphérique WAP. Vous pouvez enregistrer jusqu'à 128 messages de journal dans la mémoire non volatile. Lorsque la limite de 128 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** : gravité minimale qu'un événement doit avoir pour être écrit dans le journal de la mémoire non volatile. Par exemple, si vous spécifiez 2 (critique), alors les événements de niveau critique, alerte et urgence sont journalisés dans la mémoire non volatile. Les messages d'erreur ayant un niveau de gravité 3 à 7 sont écrits dans la mémoire volatile.

- **Profondeur** : nombre maximal de messages (jusqu'à 512) 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. Veuillez noter que le nombre maximal de messages de journal pouvant être stockés dans la mémoire non volatile (le journal persistant) est 128, celui-ci n'étant pas configurable.

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

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, tels que des conditions d'erreur.

Vous pouvez ensuite configurer l'appareil WAP pour vous connecter au 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 du périphérique WAP offre les fonctions suivantes :

- Permet l'agrégation des messages syslog depuis plusieurs points d'accès
- Stocke un historique des messages plus long que celui conservé sur un seul périphérique WAP
- Déclenche des opérations de gestion scriptées et des alertes

Spécification d'un hôte en tant que serveur de journalisation distant

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

ÉTAPE 1 Sélectionnez **Administration** > **Paramètres des journaux** dans le volet de navigation.

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

- **Serveur de journalisation distant**: 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 ce serveur de journalisation distant, puis définissez le niveau de gravité des journaux et le port UDP.
- **Gravité des journaux**: définissez le niveau de gravité d'un événement pour que celui-ci soit envoyé au serveur de journalisation distant.
- **Port UDP** : numéro de port logique pour le processus syslog sur l'hôte distant. La plage est comprise entre 1 et 65 535. Le port par défaut est 514.

  Il est recommandé d'utiliser le port par défaut. Si vous choisissez de reconfigurer 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.

Si vous avez activé un hôte Journal distant et que vous cliquez sur **Enregistrer**, vous activez alors la journalisation distante. Le périphérique 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 vos configurations.

Si vous avez désactivé un hôte Journal distant et que vous cliquez sur **Enregistrer**, vous désactivez alors la journalisation distante.

REMARQUE : Une fois les nouveaux paramètres enregistrés, les processus correspondants peuvent être arrêtés et redémarrés. Toutefois, dans ce cas, il se peut que le périphérique WAP perde sa connectivité. Nous vous recommandons de modifier les paramètres du périphérique WAP lorsqu'une perte de connectivité peut affecter vos clients sans fil.

Alerte par e-mail

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

Cette fonction 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.

CONSEIL N'utilisez pas votre adresse e-mail personnelle, car les identifiants de connexion à votre messagerie personnelle seraient dévoilés inutilement. 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 votre messagerie afin de vous assurer qu'ils sont conformes à la politique de confidentialité de votre entreprise.

Configuration du point d'accès pour l'envoi d'alertes par e-mail

Pour configurer le point d'accès afin qu'il envoie des alertes par e-mail :

ÉTAPE 1 Sélectionnez **Administration** > **Alerte par e-mail** dans le volet de navigation.

ÉTAPE 2 Dans la zone Global Configuration, définissez les paramètres suivants :

- **Mode d'administration** : choisissez d'activer la fonction d'alerte par e-mail globalement.
- **Adresse e-mail de l'expéditeur** : entrez l'adresse à afficher en tant qu'expéditeur de l'e-mail. L'adresse est une chaîne de 255 caractères uniquement 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** : les messages de journal de ce niveau de gravité ou d'un niveau plus élevé sont regroupés et envoyés à l'adresse e-mail de configuration, à la fréquence définie dans Durée du journal. Sélectionnez l'une des valeurs suivantes : Aucun, Urgence, Alerte, Critique, Erreur, Avertissement, Notification, Info et Débogage. Si vous sélectionnez Aucun, aucun message de gravité planifié n'est envoyé. La gravité par défaut est Avertissement.
- **Urgent Message Severity** : les messages de journal de ce niveau de gravité ou d'un niveau plus élevé sont immédiatement envoyés à l'adresse e-mail configurée. Sélectionnez l'une des valeurs suivantes : Aucun, Urgence, Alerte, Critique, Erreur, Avertissement, Notification, Info et Débogage. Si vous sélectionnez Aucun, aucun message de gravité urgente n'est envoyé. La valeur par défaut est Alerte.

ÉTAPE 3 Dans la zone Configuration du serveur de messagerie, définissez les paramètres suivants :

- **Nom/adresse IPv4/IPv6 du serveur** : saisissez l'adresse IP ou le nom d'hôte du serveur SMTP sortant. (Vous pouvez demander à votre fournisseur de messagerie de vous indiquer le nom d'hôte.) L'adresse du serveur doit être une adresse IPv4 ou un nom d'hôte valide. 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 se composer d'une ou plusieurs étiquettes, elles-mêmes constituées d'un maximum de 63 caractères alphanumériques. Si un nom d'hôte inclut plusieurs étiquettes, elles sont séparées par un point (.). La série entière d'étiquettes et de points peut comporter jusqu'à 253 caractères.

- **Chiffrement de données** : saisissez le mode de sécurité de l'alerte par e-mail sortante. L'alerte peut être envoyée via le protocole TLS sécurisé ou le protocole Open par défaut. 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. Le numéro de port doit être compris entre 0 et 65535. Le port par défaut est 465. Le port dépend généralement du mode utilisé par le fournisseur de messagerie.

- **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 Configurez 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 **Message de test** pour envoyer un e-mail de test afin de valider le compte de messagerie configuré.

ÉTAPE 6 Cliquez sur **Enregistrer**. Les modifications sont enregistrées dans la configuration de démarrage.

Exemples d'alertes par e-mail

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

```
Gmail
Nom/adresse IPv4/IPv6 du serveur = smtp.gmail.com
Chiffrement de données = TLSv1
Port = 465
Nom d'utilisateur = votre adresse e-mail complète qui vous permet de vous
connecter à votre compte de messagerie associé au serveur ci-dessus
Mot de passe = xxxxxxxx est un mot de passe valide de votre compte de
messagerie valide.
Adresse e-mail du destinataire 1 = mon_email@gmail.com

Windows Live Hotmail
Windows Live Hotmail recommande les paramètres suivants :
Chiffrement de données = TLSv1
Serveur SMTP = smtp.live.com
Port SMTP = 587
Nom d'utilisateur : votre adresse e-mail complète, telle que
monNom@hotmail.com ou monNom@monDomaine.com
Mot de passe : votre mot de passe de compte Windows Live

Yahoo! Mail
Pour pouvoir profiter de ce type de service, Yahoo impose l'utilisation d'un
compte payant. Yahoo recommande les paramètres suivants :
Chiffrement de données = TLSv1
Serveur SMTP = plus.smtp.mail.yahoo.com
Port SMTP = 465 ou 587
Nom d'utilisateur : votre adresse e-mail sans le nom du domaine, telle que
monNom (sans @yahoo.com)
Mot de passe : votre mot de passe de compte Yahoo
```

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

```
De : AP-192.168.2.10@mailserver.com
Envoyé Wednesday, September 09, 2009 11:16 AM
À : administrator@mailserver.com
Objet : log message from AP

TIME           PriorityProcess Id          Message
Sep 8 03:48:25 info    login[1457]         root login on ttyp0
Sep 8 03:48:26 info    mini_http-ssl[1175] Max concurrent connections of 20
reached
```

Affichage DEL

Le périphérique WAP possède 1 voyant. La page Affichage des voyants vous permet d'activer ou de désactiver le voyant et de l'associer avec un profil de planificateur configuré.

L'affichage des voyants est **activé** par défaut. Lorsque l'affichage des voyants est **désactivé**, le voyant est éteint. Lorsque la valeur de l'affichage des voyants est définie sur **Associer un planificateur**, une liste déroulante s'affiche pour vous permettre de sélectionner un profil de planificateur. Lorsqu'il est activé, il indique l'état et l'activité correspondants du périphérique WAP.

Modification de l'affichage des voyants

Pour modifier l'affichage LED :

ÉTAPE 1 Sélectionnez **Administration > Affichage DEL** dans le volet de navigation.

ÉTAPE 2 Sélectionnez **Activer/Désactiver/Associer un planificateur** dans la liste déroulante.

ÉTAPE 3 Sélectionnez le nom du profil dans la liste déroulante pour associer un planificateur. Par défaut, aucun profil n'est associé aux voyants. La sélection indiquera les noms des profils de planificateurs comme sur la page **Technologie sans fil > Planificateur**.

Lorsque le voyant est associé à un profil de planificateur, cette colonne affiche l'état selon la présence ou l'absence d'une règle de profil active à cet instant de la journée.

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

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 la page Service HTTP/HTTPS pour gérer les certificats SSL requis.

Configuration des services HTTP et HTTPS

Pour configurer les services HTTP et HTTPS :

ÉTAPE 1 Sélectionnez **Administration** > **Service HTTP/HTTPS** dans le volet de navigation.

ÉTAPE 2 Configurez les paramètres globaux suivants :

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

  Lorsqu'un utilisateur se connecte à l'utilitaire de configuration de périphérique 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** : durée maximale en minutes pendant laquelle un utilisateur inactif peut rester connecté à l'utilitaire de configuration de périphérique WAP. Lorsque le délai d'expiration est atteint, l'utilisateur est automatiquement déconnecté. La plage valide va de 1 à 60 minutes. La valeur par défaut est 10 minutes.

ÉTAPE 3 Configurez les services HTTP et HTTPS :

- **Serveur HTTP** : active 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** : numéro de port logique à utiliser pour les connexions HTTP, de 1 025 à 65 535. Le numéro de port par défaut pour les connexions HTTP est le numéro de port bien connu IANA 80.
- **Serveur HTTPS** : active l'accès par HTTP sécurisé. L'accès HTTPS est activé par défaut. Si vous le désactivez, toutes les connexions actives qui utilisent ce protocole sont déconnectées.

- **Port HTTPS** : numéro de port logique à utiliser pour les connexions HTTP, de 1 025 à 65 535. Le numéro de port par défaut pour les connexions HTTP est le numéro de port bien connu IANA 443.
- **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.

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

Gestion des certificats SSL

Pour utiliser les services HTTPS, le périphérique WAP doit avoir un certificat SSL valide. Le périphérique WAP peut générer un certificat ou vous pouvez le télécharger depuis votre réseau ou un serveur TFTP.

Pour générer le certificat avec le périphérique WAP, cliquez sur **Générer le certificat SSL**. L'opération est effectuée une fois que le point d'accès a obtenu une adresse IP, afin de garantir que le nom commun du certificat correspond à l'adresse IP du point d'accès. 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, vous pouvez voir s'il existe déjà un certificat sur le périphérique WAP et obtenir les informations suivantes sur celui-ci :

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

S'il existe un certificat SSL (avec une extension .pem) sur le périphérique WAP, vous pouvez le télécharger vers votre ordinateur en tant que sauvegarde. Dans la zone Télécharger le certificat SSL (sur l'ordinateur à partir de l'appareil), sélectionnez la méthode de téléchargement **HTTP** ou **TFTP** dans **Méthode de téléchargement**, puis cliquez sur **Télécharger**.

- Si vous sélectionnez HTTP, vous devez confirmer le téléchargement, puis accéder à l'emplacement d'enregistrement du fichier sur votre réseau.
- Si vous sélectionnez TFTP, d'autres champs apparaissent pour vous permettre de saisir le nom de fichier à attribuer au fichier téléchargé. Vous devez ensuite saisir l'adresse du serveur TFTP où le fichier sera téléchargé.

Vous pouvez également télécharger un fichier de certificat (portant une extension .pem) depuis votre ordinateur vers le périphérique WAP. Dans la zone Télécharger le certificat SSL (sur l'appareil à partir de l'ordinateur), sélectionnez la méthode de téléchargement **HTTP** ou **TFTP** dans **Méthode de chargement**.

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

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

Contrôle d'accès de gestion

Vous pouvez créer une liste de contrôle d'accès (ACL) contenant jusqu'à cinq hôtes IPv4 et cinq hôtes IPv6 autorisés à accéder à l'utilitaire de configuration de périphérique WAP. 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 du périphérique WAP.

Si la liste de contrôle d'accès de gestion est activée, l'accès via le Web et SNMP est limité aux hôtes IP spécifiés.

AVERTISSEMENT 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 fortement recommandé d'attribuer une adresse IP statique à l'ordinateur d'administration, afin que cette adresse reste toujours la même.

Création d'une liste d'accès

Pour créer une liste d'accès :

ÉTAPE 1 Sélectionnez **Administration** > **Contrôle d'accès de gestion** dans le volet de navigation.

ÉTAPE 2 Sélectionnez **Activer** pour **Mode de l'ACL de gestion**.

ÉTAPE 3 Saisissez un maximum de cinq adresses IPv4 et cinq adresses IPv6 auxquelles vous donnez accès.

ÉTAPE 4 Vérifiez que les adresses IP sont correctes.

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

Gestion du micrologiciel

Le périphérique WAP gère deux images de micrologiciel. 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 du point d'accès sont disponibles, vous pouvez le mettre à niveau sur vos périphériques afin de bénéficier des nouvelles fonctionnalités et améliorations. Le point d'accès utilise un client TFTP ou HTTP pour les mises à niveau du microprogramme.

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

REMARQUE : Lorsque vous mettez à niveau le microprogramme, le point d'accès conserve les informations de configuration existantes.

Pour permuter l'image du microprogramme exécuté sur le point d'accès :

ÉTAPE 1 Sélectionnez **Administration** > **Gestion du micrologiciel** dans le volet de navigation.

ÉTAPE 2 Cliquez sur **Permuter l'image active**.

La boîte de dialogue qui s'affiche confirme la permutation de l'image du micrologiciel et le redémarrage qui suit.

ÉTAPE 3 Cliquez sur **OK** pour effectuer l'opération.

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

Mise à niveau TFTP

Pour mettre à niveau le microprogramme sur un point d'accès via TFTP :

ÉTAPE 1 Sélectionnez **Administration** > **Gestion du micrologiciel** dans le volet de navigation.

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

ÉTAPE 2 Sélectionnez **Méthode de transfert TFTP**.

ÉTAPE 3 Saisissez un nom (de 1 à 128 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 micrologiciel 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 éléments suivants : espaces, <, >, |, \, : , (,), &, ; , #, ? , *, ainsi que deux points successifs ou plus.

ÉTAPE 4 Renseignez **Adresse IPv4 du serveur TFTP**, puis cliquez sur **Mettre à niveau**.

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

ÉTAPE 5 Pour vous assurer que la mise à niveau du microprogramme s'est correctement effectuée, connectez-vous à l'interface utilisateur, affichez la page Mise à niveau du micrologiciel, puis vérifiez la version active du microprogramme.

Mise à niveau HTTP

Pour effectuer une mise à niveau via HTTP :

ÉTAPE 1 Sélectionnez **Méthode de transfert HTTP**.

ÉTAPE 2 Si vous connaissez le nom du nouveau fichier et le chemin d'accès à celui-ci, saisissez-les dans le champ **Nom du fichier source**. Sinon, cliquez sur le bouton **Parcourir** et recherchez le fichier image du microprogramme sur votre réseau.

Le fichier de mise à niveau du micrologiciel 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 **Mettre à niveau** pour appliquer la nouvelle image du micrologiciel.

Le téléchargement du nouveau logiciel peut prendre quelques minutes. N'actualisez pas la page et n'ouvrez pas d'autre page pendant le téléchargement du nouveau logiciel, sous peine d'interrompre celui-ci. Une fois le processus terminé, le point d'accès 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'interface utilisateur, affichez la page Mise à niveau du micrologiciel, puis vérifiez la version active du microprogramme.

Télécharger/sauvegarder le fichier de configuration

Les fichiers de configuration du point d'accès sont au format XML et contiennent toutes les informations relatives aux paramètres du périphérique 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 le point d'accès afin de modifier la configuration.

Le point d'accès prend en charge les fichiers de configuration suivants :

- **Configuration de démarrage** : fichier de configuration enregistré dans la mémoire flash.
- **Configuration de sauvegarde** : fichier de configuration supplémentaire enregistré sur le périphérique WAP à des fins de 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 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.

REMARQUE : En plus du téléchargement et du transfert de ces fichiers vers un autre système, vous pouvez les copier vers différents types de fichier sur le périphérique WAP. Reportez-vous à la section **Copier/enregistrer la configuration**.

Sauvegarde d'un fichier de configuration

Pour sauvegarder (télécharger) le fichier de configuration vers un hôte réseau ou le serveur TFTP :

ÉTAPE 1 Sélectionnez **Administration** > **Télécharger/sauvegarder le fichier de configuration** dans le volet de navigation.

ÉTAPE 2 Sélectionnez la méthode de transfert **Via TFTP** ou **Via HTTP/HTTPS** dans **Méthode de transfert**.

ÉTAPE 3 Sélectionnez l'action d'enregistrement **Sauvegarder (Point d'accès vers ordinateur)** dans **Mode d'enregistrement**.

ÉTAPE 4 Pour une sauvegarde TFTP uniquement, renseignez **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 renseignez **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 uniquement, renseignez **Adresse IPv4 du serveur TFTP**.

ÉTAPE 6 Sélectionnez le fichier de configuration que vous souhaitez sauvegarder :

- **Configuration de démarrage** : type de fichier de configuration utilisé lors du dernier démarrage du périphérique WAP. Ce fichier n'inclut pas les modifications de configuration appliquées mais non encore enregistrées sur le périphérique WAP.
- **Configuration de sauvegarde** : type de fichier de configuration de sauvegarde enregistré sur le périphérique 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. Le fichier de 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 **Enregistrer** pour commencer la sauvegarde. Pour les sauvegardes HTTP, une fenêtre s'affiche afin de vous permettre d'accéder à l'emplacement souhaité pour l'enregistrement du fichier.

Vous pouvez télécharger un fichier vers le point d'accès pour mettre à jour la configuration ou restaurer le point d'accès à une configuration précédemment sauvegardée.

Téléchargement d'un fichier de configuration

Pour télécharger un fichier de configuration vers le périphérique WAP :

ÉTAPE 1 Sélectionnez **Administration** > **Télécharger/sauvegarder le fichier de configuration** dans le volet de navigation.

ÉTAPE 2 Sélectionnez la méthode de transfert **Via TFTP** ou **Via HTTP/HTTPS** dans **Méthode de transfert**.

ÉTAPE 3 Sélectionnez l'action d'enregistrement **Télécharger Ordinateur vers point d'accès** dans **Mode d'enregistrement**.

ÉTAPE 4 Pour un téléchargement TFTP uniquement, renseignez **Nom du fichier source** avec une extension .xml. Incluez le chemin d'accès à l'emplacement du fichier sur le serveur, puis renseignez **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 le fichier de configuration sur le point d'accès que vous souhaitez remplacer par le fichier téléchargé : la **configuration de démarrage** ou la **configuration de sauvegarde**.

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 du point d'accès.

ÉTAPE 6 Cliquez sur **Enregistrer** pour commencer la mise à niveau ou la sauvegarde. Pour les téléchargements HTTP, une fenêtre s'affiche afin de vous permettre de sélectionner le fichier à télécharger. Une fois le téléchargement terminé, une fenêtre vous confirme le succès de l'opération.

AVERTISSEMENT Veillez à ce que le point d'accès 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.

Propriétés des fichiers de configuration

La page Propriétés des fichiers de configuration vous permet d'effacer le fichier de configuration de démarrage ou de sauvegarde. Si vous effacez le fichier de configuration de démarrage, le fichier de configuration de sauvegarde s'activera lors du prochain redémarrage du point d'accès.

Lorsque le point d'accès est activé, il tente d'appliquer la configuration de démarrage. En cas de problème quelconque lié à la configuration de démarrage, le point d'accès tente d'appliquer la configuration miroir. Si la configuration miroir ne peut pas être appliquée, pour une raison quelconque, le point d'accès tente alors d'appliquer la configuration de sauvegarde.

Suppression du fichier de configuration de démarrage ou de configuration de sauvegarde

Pour supprimer le fichier de configuration de démarrage ou de configuration de sauvegarde :

ÉTAPE 1 Sélectionnez **Administration** > **Propriétés des fichiers de configuration** dans le volet de navigation.

ÉTAPE 2 Sélectionnez le type de fichier **Configuration de démarrage** ou **Configuration de sauvegarde**.

ÉTAPE 3 Cliquez sur **Effacer les fichiers**.

Copier/enregistrer la configuration

La page Copier/Enregistrer la configuration vous permet de copier des fichiers dans le système de fichiers du point d'accès. 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 du périphérique WAP.

Copie d'un fichier vers un autre type de fichier

Pour copier un fichier vers un autre type de fichier :

ÉTAPE 1 Sélectionnez **Administration** > **Copier/enregistrer la configuration** dans le volet de navigation.

ÉTAPE 2 Sélectionnez le **nom du fichier source** :

- **Configuration de démarrage** : type de fichier de configuration utilisé lors du dernier démarrage du périphérique WAP. Ce fichier n'inclut pas les modifications de configuration appliquées mais non encore enregistrées sur le périphérique WAP.
- **Configuration de sauvegarde** : type de fichier de configuration de sauvegarde enregistré sur le périphérique 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. Le fichier de 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 Pour **Nom du fichier de destination**, sélectionnez le type de fichier à remplacer par le fichier que vous copiez.

ÉTAPE 4 Cliquez sur **Enregistrer** pour commencer la copie.

Une fois l'opération terminée, une fenêtre affiche le message Opération de copie réussie.

Redémarrer

Redémarrage du point d'accès

Vous pouvez utiliser la page Redémarrage pour redémarrer le point d'accès.

ÉTAPE 1 Pour redémarrer le WAP, sélectionnez **Administration** > **Redémarrer** dans le volet de navigation.

ÉTAPE 2 Sélectionnez l'une des options suivantes :

- **Redémarrer** : redémarre le WAP en utilisant la configuration de démarrage.
- **Redémarrer avec les paramètres d'usine par défaut** : redémarre le WAP en utilisant le fichier de configuration par défaut d'origine. Tous les paramètres personnalisés sont perdus.

Une fenêtre s'affiche pour vous permettre de confirmer ou d'annuler le redémarrage. Il est possible que la session de gestion en cours soit arrêtée.

ÉTAPE 3 Cliquez sur **OK** pour redémarrer.

Détection - Bonjour

Bonjour permet au point d'accès 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 les petites entreprises.

Le point d'accès notifie les types de services suivants :

- **Description d'appareils spécifiques à Cisco** (csco-sb) : ce service permet aux clients de détecter les périphériques WAP Cisco et d'autres produits déployés sur des réseaux d'entreprise.

- **Interfaces utilisateur de gestion** : ce service identifie les interfaces de gestion disponibles sur le périphérique WAP (HTTP, HTTPS et SNMP).

Lorsqu'un périphérique 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 le périphérique WAP. L'utilitaire de configuration web apparaît sous forme d'onglet dans le navigateur.

Bonjour fonctionne sur les réseaux IPv4 et IPv6.

Bonjour est activé par défaut.

Modification de l'état administratif

Pour modifier l'état administratif :

ÉTAPE 1 Sélectionnez **Administration** > **Détection - Bonjour** dans le volet de navigation.

ÉTAPE 2 Cochez **Activer** pour activer Bonjour ou décochez **Activer** pour désactiver Bonjour.

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

Capture des paquets

La fonction de capture de paquets sans fil permet de capturer et stocker les paquets reçus et transmis par le périphérique 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 le périphérique WAP. Le périphérique WAP peut transférer le fichier vers un serveur TFTP ou le télécharger par HTTP(S) vers un ordinateur. Le fichier est mis au format pcap et peut être examiné à l'aide d'outils comme Wireshark et OmniPeek.
- **Méthode de capture distante** : les paquets capturés sont redirigés en temps réel vers un ordinateur externe qui exécute l'outil Wireshark.**Capture**

à distance : les paquets capturés sont redirigés en temps réel vers un ordinateur externe qui exécute l'outil Wireshark.

- **Capture CloudShark** : les paquets capturés sont téléchargés en temps réel vers l'appliance CloudShark. L'appliance CloudShark organise la capture afin que tous les paquets puissent être nommés, identifiés et recherchés.

REMARQUE CloudShark est un outil d'analyse réseau Web accessible depuis n'importe quel navigateur Web sans utilitaire, plug-in ni téléchargement requis.

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.

Sélectionnez **Administration > Capture de paquets** pour afficher la page Capture de paquets. Depuis la page Capture de paquets, vous pouvez :

- Définir les paramètres de capture de paquets.
- Démarrer une capture de paquets locale ou distante.
- Afficher l'état de la capture de paquets en cours.
- Télécharger un fichier de capture de paquets.

La zone Configuration de la capture de paquets vous permet de définir les paramètres d'une capture de paquets et de lancer cette dernière.

Configuration de la capture de paquets

Pour définir les paramètres de capture de paquets :

ÉTAPE 1 Définissez les paramètres suivants :

- **Capturer les balises** : active ou désactive la capture des balises 802.11 détectées ou transmises par radio.
- **Capture de proximité** : active ou désactive le mode de proximité lorsque la capture est active.

  En mode de proximité, la radio reçoit tout le trafic sur le canal, y compris le trafic qui n'est pas destiné à ce périphérique WAP. Lorsque la radio fonctionne en mode de proximité, elle continue à servir les clients associés. Les paquets qui ne sont pas destinés au périphérique WAP ne sont pas transférés.

Lorsque la capture est terminée, la radio repasse en mode de non-proximité.

- **Filtre client radio** : active ou désactive le filtre de client WLAN de façon à capturer uniquement les trames transmises à un client WLAN ayant une adresse MAC spécifiée ou reçues de celui-ci.
- **Adresse MAC du filtre client** : spécifie l'adresse MAC pour le filtrage de client WLAN.

REMARQUE Le filtre MAC est uniquement actif lorsqu'une capture est réalisée sur une interface 802.11.

- **Méthode de capture des paquets** : sélectionnez l'une des options suivantes :
  - **Fichier local** : les paquets capturés sont stockés dans un fichier sur le périphérique WAP.
  - **À distance** : les paquets capturés sont redirigés en temps réel vers un ordinateur externe qui exécute l'outil Wireshark.
  - **CloudShark** : les paquets capturés sont téléchargés en temps réel vers l'appliance CloudShark.

ÉTAPE 2 En fonction de la méthode sélectionnée, suivez les étapes de la section Capture de paquets locale/CloudShark ou Capture de paquets distante pour continuer.

- Les modifications apportées aux paramètres de configuration de la capture de paquets prendront effet une fois la capture de paquets redémarrée. La modification des paramètres alors que la capture de paquets est en cours d'exécution n'a aucune incidence sur la session de capture de paquets active. Pour commencer à utiliser les nouvelles valeurs des paramètres, vous devez arrêter puis redémarrer une session de capture de paquets existante.

REMARQUE : Les modifications apportées aux paramètres de configuration de la capture de paquets prendront effet une fois la capture de paquets redémarrée. La modification des paramètres alors que la capture de paquets est en cours d'exécution n'a aucune incidence sur la session de capture de paquets active. Pour commencer à utiliser les nouvelles valeurs des paramètres, vous devez arrêter puis redémarrer une session de capture de paquets existante.

Capture de paquets locale

Pour démarrer une capture de paquets locale :

ÉTAPE 1 Assurez-vous que l'option **Fichier local** est sélectionnée pour **Méthode de capture de paquets**.

ÉTAPE 2 Définissez les paramètres suivants :

- **Interface de capture** : saisissez un type d'interface de capture pour la capture de paquets :
  - **radio1** : trafic 802.11 sur l'interface radio Radio 1.
  - **radio2** : trafic 802.11 sur Radio 2.
  - **eth0** : trafic 802.3 sur le port Ethernet.
  - **wlan0** : trafic VAP0 sur Radio 1.
  - **wlan1** : trafic VAP0 sur Radio 2.
  - **wlan0vap1** à **wlan0vap7** : trafic sur le point d'accès virtuel spécifié sur Radio 1.
  - **wlan1vap1** à **wlan1vap 7** : trafic sur le point d'accès virtuel spécifié sur Radio 2.
  - **wlan0wds0** à **wlan0wds3** : trafic sur l'interface WDS spécifiée.
  - **brtrunk** : interface bridge Linux dans le périphérique WAP.
- **Durée de capture** : saisissez la durée en secondes de la capture. La plage est comprise entre 10 et 3600. La valeur par défaut est 60. Définissez la valeur sur 0 seconde pour la méthode de capture de paquets illimitée via CloudShark.
- **Taille maximale des fichiers de capture** : saisissez la taille maximale autorisée pour le fichier de capture en Ko. La plage est comprise entre 64 et 4096. La valeur par défaut est 1024. Cette option n'est pas activée pour la méthode de capture de paquets via CloudShark.

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

ÉTAPE 4 Cliquez sur **Démarrer la capture**.

En mode Capture de fichiers de paquets, le périphérique 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 qu'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.

La zone Statut de la capture de paquets de la page indique l'état d'une capture de paquets si celle-ci est active sur le périphérique WAP.

- **Statut de capture actuel** : indique si la capture de paquets est en cours d'exécution ou arrêtée.
- **Durée de capture de paquets** : durée de capture écoulée.
- **Taille du fichier de capture de paquets** : taille actuelle du fichier de capture. Cette valeur est généralement supérieure à la taille du fichier de capture dans CloudShark si vous utilisez un compte CloudShark avec une taille de capture limitée.
- **Statut du chargement du fichier de capture CloudShark** : affiche un lien hypertexte si la capture de paquets CloudShark est chargée avec succès. Vous pouvez cliquer sur le lien hypertexte **Afficher la capture dans CloudShark** pour afficher les paquets capturés dans l'appliance CloudShark dans une nouvelle fenêtre de navigateur.

REMARQUE Un message d'erreur s'affiche lorsque le chargement échoue.

- Cliquez sur **Actualiser** pour afficher les dernières données issues du périphérique WAP.

REMARQUE : Pour arrêter la capture d'un fichier de paquets, cliquez sur **Arrêter la capture**.

Capture de paquets distante

La fonction Capture de paquets distante vous permet de spécifier un port distant comme 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 le périphérique 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 http://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 le périphérique WAP.

Lorsque le mode de capture distante est utilisé, le périphérique WAP ne stocke pas les données capturées localement dans son système de fichiers.

Si un pare-feu est installé entre l'ordinateur Wireshark et le périphérique 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 le périphérique WAP.

Lancement d'une capture distante sur un périphérique WAP

Pour initier une capture distante sur un périphérique WAP :

ÉTAPE 1 Sélectionnez **Administration** > **Capture de paquets**.

ÉTAPE 2 Activez **Capture de proximité**.

ÉTAPE 3 Pour **Méthode de capture de paquets**, sélectionnez **Distant**.

ÉTAPE 4 Pour **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 au périphérique WAP. La plage de ports est comprise entre 1025 et 65530.

ÉTAPE 5 Si vous souhaitez enregistrer les paramètres en vue d'une utilisation ultérieure, cliquez sur **Enregistrer**.

ÉTAPE 6 Cliquez sur **Démarrer la capture**.

Démarrage de l'outil d'analyse du réseau

Pour lancer l'outil d'analyse réseau Wireshark pour Microsoft Windows :

ÉTAPE 1 Sur le même ordinateur, lancez l'outil Wireshark.

ÉTAPE 2 Dans le menu, sélectionnez **Capture** > **Options**. Une fenêtre contextuelle s'affiche.

ÉTAPE 3 Pour **Interface**, sélectionnez **Distant**. Une fenêtre contextuelle s'affiche.

ÉTAPE 4 Pour **Hôte**, saisissez l'adresse IP du périphérique WAP.

ÉTAPE 5 Pour **Port**, saisissez le numéro de port du 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, une liste déroulante vous permet de sélectionner les interfaces. L'interface peut être l'une des suivantes :

Interface bridge Linux dans le périphérique WAP
--rpcap://[192.168.1.220]:2002/brtrunk
Interface LAN filaire
-- rpcap://[192.168.1.220]:2002/eth0
Trafic VAP0 sur radio 1
-- rpcap://[192.168.1.220]:2002/wlan0
Trafic 802.11
-- rpcap://[192.168.1.220]:2002/radio1
Sur WAP371/E, trafic VAP1 ~ VAP7 pour radio 1
-- rpcap://[192.168.1.220]:2002/wlan0vap1 ~ wlan0vap7
Sur WAP371/E, trafic VAP1 ~ VAP7 pour radio 2
-- rpcap://[192.168.1.220]:2002/wlan1vap1 ~ wlan1vap7

Vous pouvez effectuer le suivi simultané de quatre interfaces maximum sur le périphérique WAP. Toutefois, vous devez démarrer une session Wireshark distincte pour chaque interface. Pour initier des sessions de capture distante supplémentaires, répétez les étapes de configuration Wireshark ; aucune configuration n'est requise sur le périphérique 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, le périphérique 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 58000, alors le filtre de capture suivant est automatiquement installé sur le périphérique WAP :

not portrange 58000-58004

Pour éviter les problèmes de performances et de sécurité, le mode de capture de paquets n'est pas enregistré dans la NVRAM du périphérique WAP ; si le périphérique WAP est réinitialisé, le mode de capture est désactivé et vous devez le réactiver pour rétablir 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 au périphérique WAP et d'effectuer un suivi des données utilisateur. En outre, les performances du périphérique 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 du périphérique 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 le périphérique WAP de réacheminer les paquets de balise 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.

Vous pouvez télécharger un fichier de capture par TFTP vers un serveur TFTP configuré, ou par HTTP(S) vers un ordinateur. Le fichier de capture étant stocké dans le système de fichiers RAM, il disparaît si le périphérique WAP est réinitialisé.

Téléchargement d'un fichier de capture de paquets via TFTP

Pour télécharger un fichier de capture de paquets via TFTP :

ÉTAPE 1 Sélectionnez **Utiliser TFTP pour télécharger le fichier de capture**.

ÉTAPE 2 Dans **Nom de fichier du serveur TFTP**, 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 le périphérique WAP.

ÉTAPE 3 Renseignez **Adresse IPv4 du serveur TFTP** dans le champ prévu à cet effet.

ÉTAPE 4 Cliquez sur **Télécharger**.

Téléchargement d'un fichier de capture de paquets via HTTP

Pour télécharger un fichier de capture de paquets via HTTP :

ÉTAPE 1 Décochez **Utiliser TFTP pour télécharger le fichier de capture**.

ÉTAPE 2 Cliquez sur **Télécharger**. Une fenêtre de confirmation s'affiche.

ÉTAPE 3 Cliquez sur **OK**. Une boîte de dialogue apparaît. Celle-ci vous permet de choisir l'emplacement d'enregistrement du fichier sur le réseau.

Informations relatives au support

La page Support Information vous permet de télécharger un fichier texte qui contient des informations de configuration détaillées sur le point d'accès. Le fichier inclut les informations de version matérielle et logicielle, les adresses MAC et IP, l'état d'administration et opérationnel des fonctions, les paramètres définis par l'utilisateur, les statistiques de trafic, etc. Vous pouvez fournir ce fichier texte aux membres de l'assistance technique pour les aider à résoudre les différents problèmes.

Pour afficher la page des informations d'assistance, sélectionnez **Administration > Informations relatives au support**.

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.

Paramètres de STP

Utilisez la page Paramètres de STP pour définir les paramètres STP sur l'appareil Cisco WAP571/E.

Configuration des paramètres STP sur l'appareil Cisco WAP571

Pour configurer les paramètres STP sur l'appareil Cisco WAP571 :

ÉTAPE 1 Sélectionnez **Administration > Paramètres de STP**.

ÉTAPE 2 Configurez le paramètre :

Statut STP : active ou désactive STP sur l'ensemble de l'appareil Cisco WAP571/E. STP est activé par défaut.

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

4

LAN

Cette section explique comment configurer les paramètres pour le port, le VLAN et l'adressage IPv4 et IPv6 du périphérique WAP.

Elle contient les rubriques suivantes :

- **Paramètres des ports**
- **Configuration du VLAN**
- **Paramètres IPv4**
- **Paramètres IPv6**
- **Tunnel IPv6**
- **LLDP**

Paramètres des ports

Utilisez la page Paramètres des ports pour afficher et configurer les paramètres du port qui connecte physiquement le périphérique WAP à un réseau local.

Pour configurer les paramètres de port :

ÉTAPE 1 Sélectionnez **LAN** > **Paramètres des ports**.

La Table des paramètres de port répertorie les configurations et les états suivants pour les 2 interfaces (Eth0 et Eth1) :

- **Statut de la liaison** : affiche l'état actuel de la liaison du port.
- **Débit du port** : en mode vérification, affiche la vitesse actuelle du port. En mode d'édition, si la négociation automatique est désactivée, sélectionnez une vitesse de port, comme 100 Mbit/s ou 10 Mbit/s. La vitesse 1000 Mbit/s n'est prise en charge que si la négociation automatique est activée.

- Mode duplex : en mode de vérification, affiche le mode duplex actuel du port. En mode d'édition, si la négociation automatique est désactivée, sélectionnez Semi-duplex ou Duplex intégral.

Négociation automatique : lorsque cette option est activée, le port négocie avec son partenaire de liaison afin de définir la vitesse de liaison la plus rapide et le mode duplex disponible. Si cette option est désactivée, vous pouvez configurer manuellement la vitesse du port et le mode duplex.

Green Ethernet : le mode Green Ethernet prend en charge le mode basse puissance automatique et le mode EEE (Energy Efficient Ethernet, IEEE 802.3az). Le mode Green Ethernet fonctionne uniquement lorsque la négociation automatique de port est activée. Le mode basse puissance automatique permet de diminuer la consommation des puces en cas d'absence de signal émanant d'un partenaire de liaison. Le périphérique WAP passe automatiquement en mode basse puissance en cas de perte d'énergie sur la ligne et il reprend un fonctionnement normal lorsqu'il détecte de l'énergie. Le mode EEE accepte des périodes silencieuses en cas de faible utilisation de la liaison, ce qui permet aux deux extrémités d'une liaison de désactiver des parties de chaque circuit de la couche physique afin d'économiser de l'énergie.

- **Statut Green Ethernet** : affiche l'état EEE actuel.

ÉTAPE 2 Sélectionnez les interfaces à modifier, puis cliquez sur le bouton Modifier pour passer en mode d'édition. Entrez ensuite vos paramètres.

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

REMARQUE : Les deux interfaces Eth0 et Eth1 de l'appareil WAP571/E peuvent être utilisés en mode d'agrégation de liaisons. Le partenaire de liaison doit également prendre en charge l'agrégation de liaisons. Eth1 suivra toujours les configurations Eth0.

Configuration du VLAN

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

Pour configurer les paramètres d'un VLAN :

ÉTAPE 1 Sélectionnez **LAN** > **Configuration du VLAN.**

ÉTAPE 2 Dans la Table des paramètres du VLAN, chaque enregistrement VLAN comporte les champs suivants :

- **ID de VLAN** : identifiant du VLAN. Chaque ID de VLAN est compris entre 1 et 4 094 et doit être différent des autres ID de VLAN.
- **Description** : description du réseau VLAN associé. Elle ne doit pas comporter plus de 64 caractères (A-Z, a-z, 0-9, _).

ÉTAPE 3 **VLAN de gestion** : sélectionnez le VLAN de gestion utilisé pour accéder au périphérique WAP via l'interface utilisateur graphique (GUI) Web. Il ne doit exister qu'un seul et unique VLAN de gestion. Si aucune interface (filaire ou sans fil) n'appartient au VLAN de gestion, l'utilisateur ne dispose d'aucune interface pour accéder à l'utilitaire de configuration.

- **Eth0 - Eth1** : chaque port ne doit avoir qu'un seul VLAN non balisé. Les options sont les suivantes :
  - **Non balisé** : le port est un membre du VLAN. Un paquet du VLAN émis à partir du port sera non balisé. Un paquet non balisé reçu par le port sera classifié comme appartenant au VLAN (balisé).
  - **Balisé** : le port est un membre du VLAN. Un paquet du VLAN émis à partir du port sera balisé avec l'en-tête du VLAN.
  - **Exclu** : le port n'appartient pas au VLAN.

REMARQUE : Il est impossible de supprimer l'ID de VLAN 1. Si un port (filaire ou sans fil) associé au VLAN a été supprimé, le périphérique WAP définira automatiquement son ID VLAN à 1.

REMARQUE : Une fois les nouveaux paramètres enregistrés, les processus correspondants peuvent être arrêtés et redémarrés. Toutefois, dans ce cas, il se peut que le périphérique WAP perde sa connectivité. Nous vous recommandons de modifier les paramètres du périphérique WAP lorsqu'une perte de connectivité peut affecter vos clients sans fil.

Paramètres IPv4

Utilisez la page Paramètres IPv4 pour configurer l'affectation d'adresses IPv4 statiques ou dynamiques.

Pour configurer les paramètres d'adresses IPv4 :

ÉTAPE 1 Sélectionnez **LAN > Paramètres IPv4**.

ÉTAPE 2 Configurez les paramètres IPv4 suivants :

- **Type de connexion** : par défaut, le client DHCP sur le périphérique 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** : le périphérique WAP acquiert son adresse IP d'un serveur DHCP sur le réseau local.
  - **Adresse IP statique** : configurez manuellement l'adresse IPv4. La forme de l'adresse IPv4 doit être similaire à celle-ci : xxx.xxx.xxx.xxx (192.0.2.10).
- Adresse IP statique, Masque de sous-réseau et Passerelle par défaut : si vous avez choisi d'affecter une adresse IP statique, saisissez les informations IP dans ces champs.
- **Serveurs de noms de domaine** : sélectionnez l'une des options suivantes :
  - **Dynamique** : le périphérique WAP acquiert les adresses de serveur DNS d'un serveur DHCP sur le réseau local.
  - **Manuel** : configurez manuellement une ou plusieurs adresses de serveur DNS. Entrez jusqu'à deux adresses IP dans les champs fournis.

ÉTAPE 3 Définissez les paramètres de configuration automatique DCHP IPv4 suivants :

- **Options de configuration automatique DHCP** : par défaut, les « Options de configuration automatique DHCP » sont activées. 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 sur l'appareil WAP 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/l'administrateur 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, celle-ci est utilisée en cas d'échec de récupération du 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, celui-ci est récupéré auprès du serveur TFTP lors de la configuration automatique du point d'accès, dans le cas où le nom du fichier de démarrage n'est pas reçu du serveur DHCP. 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 permet à l'utilisateur d'utiliser les services activés après 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.

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

REMARQUE : Une fois les nouveaux paramètres enregistrés, les processus correspondants peuvent être arrêtés et redémarrés. Toutefois, dans ce cas, il se peut que le périphérique WAP perde sa connectivité. Nous vous recommandons de modifier les paramètres du périphérique WAP lorsqu'une perte de connectivité peut affecter vos clients sans fil.

Paramètres IPv6

Utilisez la page Paramètres IPv6 pour configurer le périphérique WAP afin qu'il utilise une adresse IPv6.

Pour configurer les paramètres d'adresse IPv6 :

ÉTAPE 1 Sélectionnez **LAN** > **Paramètres IPv6**.

ÉTAPE 2 Définissez les paramètres suivants :

- **Type de connexion IPv6** : choisissez la façon dont le périphérique WAP obtient une adresse IPv6 :
  - **DHCPv6** : l'adresse IPv6 est affectée par un serveur DHCPv6.
  - **IPv6 statique** : configurez manuellement les adresses IPv6. La forme de l'adresse IPv6 doit être similaire à celle-ci : xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx (2001:DB8::CAD5:7D91).

REMARQUE : Lorsqu'une adresse IPv6 statique est configurée, DHCPv6 est à l'arrêt. Lorsque DHCPv6 est configuré, une adresse IPv6 statique peut être opérationnelle si la configuration existe.

- **Mode d'administration IPv6** : active ou désactive l'accès de gestion IPv6.
- **Mode d'administration de la configuration automatique des adresses IPv6** : active ou désactive la configuration automatique des adresses IPv6 sur le périphérique WAP.

  Lorsque cette option est activée, le périphérique WAP apprend ses adresses et sa passerelle IPv6 en traitant les messages de notification de routeur reçus sur le port LAN. Le périphérique WAP peut posséder plusieurs adresses IPv6 configurées automatiquement.
- **Adresse IPv6 statique** : adresse IPv6 statique. Le périphérique WAP peut posséder une adresse IPv6 statique, même si des adresses ont déjà été configurées automatiquement.
- **Longueur du préfixe de l'adresse IPv6 statique** : 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 :
  - **Opérationnelle** : l'adresse IP a été vérifiée comme étant unique sur le réseau local et elle est utilisable sur l'interface.
  - **Tentative** : le périphérique WAP initie automatiquement un processus de détection des adresses en double (DAD, Duplicate Address Detection) lors de l'affectation d'une adresse IP statique. Une adresse IPv6 reste à l'état provisoire pendant que le système vérifie qu'elle est unique sur le réseau. Lorsqu'elle se trouve dans cet état, l'adresse IPv6 ne peut pas être utilisée pour transmettre ou recevoir le trafic normal.
  - **Vide (aucune valeur)** : aucune adresse IP n'est affectée ou l'adresse affectée n'est pas opérationnelle.
- **Adresses globales IPv6 configurées automatiquement** : si une ou plusieurs adresses IPv6 ont été affectées automatiquement au périphérique WAP, ces adresses sont répertoriées ici.
- **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 de noms DNS sont appris dynamiquement par le biais de DHCPv6.
  - **Manuel** : spécifiez manuellement jusqu'à deux serveurs de noms DNS IPv6 dans les champs prévus à cet effet.

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

REMARQUE : Une fois les nouveaux paramètres enregistrés, les processus correspondants peuvent être arrêtés et redémarrés. Toutefois, dans ce cas, il se peut que le périphérique WAP perde sa connectivité. Nous vous recommandons de modifier les paramètres du périphérique WAP lorsqu'une perte de connectivité peut affecter vos clients sans fil.

Tunnel IPv6

Le périphérique WAP571/E prend en charge le protocole ISATAP (Intra-Site Automatic Tunnel Addressing Protocol). Le protocole ISATAP permet au périphérique WAP de transmettre des paquets IPv6 encapsulés dans des paquets IPv4 sur le réseau local. Grâce à ce protocole, le périphérique WAP peut communiquer avec des hôtes compatibles IPv6 distants, même si le réseau local qui les connecte ne prend pas en charge IPv6.

Le périphérique 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 le périphérique WAP (par défaut, il s'agit d'isatap). S'il est configuré en tant que nom d'hôte, le périphérique WAP communique avec un serveur DNS pour résoudre le nom en une ou plusieurs adresses de routeur ISATAP. Le périphérique WAP envoie ensuite des messages de sollicitation au(x) routeur(s). Lorsqu'un routeur prenant en charge le protocole ISATAP répond par le biais d'un message d'annonce, le périphérique 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 le périphérique WAP connecté par l'intermédiaire du routeur ISATAP, les paquets IPv6 sont encapsulés dans des paquets IPv4 par le routeur ISATAP.

Pour configurer un tunnel IPv6 à l'aide du protocole ISATAP :

ÉTAPE 1 Sélectionnez **LAN** > **Tunnel IPv6** dans le volet de navigation.

ÉTAPE 2 Configurez les paramètres suivants :

- **Statut ISATAP** : active ou désactive le mode d'administration du protocole ISATAP sur le périphérique WAP.
- **Hôte compatible ISATAP** : adresse IP ou nom DNS du routeur ISATAP. La valeur par défaut est isatap.
- **Intervalle des requêtes ISATAP** : spécifie à quelle fréquence le point d'accès doit envoyer des requêtes au serveur DNS pour tenter de résoudre le nom d'hôte ISATAP en une adresse IP. Le périphérique WAP n'envoie des requêtes DNS que lorsque l'adresse IP du routeur ISATAP est inconnue. La plage valide va de 120 à 3600 secondes. La valeur par défaut est 120 secondes.
- **Intervalle de sollicitation ISATAP** : spécifie à quelle fréquence le périphérique WAP doit envoyer des messages de sollicitation de routeur au routeur ISATAP dont il obtient des informations par le biais de messages de consultation DNS. Le périphérique 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.

ÉTAPE 3 Cliquez sur **Enregistrer**. Les paramètres sont enregistrés dans la configuration initiale.

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 avec le réseau IPv4.

LLDP

Le protocole LLDP (Link Layer Discovery Protocol) est défini par la norme IEEE 802.1AB et permet au UAP de fournir des informations le concernant, comme 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 configurations incorrectes 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 périphériques peuvent se transmettre en vue d'améliorer la gestion du réseau.

Pour configurer les paramètres LLDP :

ÉTAPE 1 Sélectionnez **LAN > LLDP** dans le volet de navigation.

ÉTAPE 2 Configurez les paramètres suivants :

- **Mode LLDP** : le mode d'administration du protocole LLDP sur le point d'accès. Lorsque le protocole LLDP est activé, le point d'accès transmet les unités de données du protocole LLDP aux périphériques voisins.
- **Intervalle de transmission** : le 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** : niveau de priorité transmis par le point d'accès dans l'élément d'information d'alimentation étendue. Le niveau de priorité PoE permet à un appareil PSE (Power Sourcing Equipment), par exemple un commutateur, de déterminer à quels périphériques alimentés il doit donner la priorité en matière d'affectation de puissance lorsque le PSE n'est pas capable d'alimenter l'ensemble des périphériques connectés. La priorité PoE peut prendre l'une des valeurs suivantes :
  - Critique
  - Élevé
  - Faible
  - Inconnu

ÉTAPE 3 Cliquez sur **Enregistrer**. Les paramètres sont enregistrés dans le système.

5

Technologie sans fil

Cette section décrit comment configurer les propriétés de fonctionnement de la radio sans fil.

Elle contient les rubriques suivantes :

- **Radio**
- **Détection de point d'accès non autorisé**
- **Réseaux**
- **Transfert de multidiffusion sans fil**
- **Planificateur**
- **Association au planificateur**
- **Filtrage MAC**
- **Pont**
- **QoS**

Radio

Les paramètres radio contrôlent directement le comportement de la radio dans le périphérique WAP et son interaction avec le support physique, à savoir le type de signal émis par le périphérique WAP et la façon dont il procède.

Configuration des paramètres de radio

Pour définir les paramètres radio :

ÉTAPE 1 Sélectionnez **Technologie sans fil** > **Radio** dans le volet de navigation.

ÉTAPE 2 Dans la zone Paramètres globaux, configurez l'option **Intervalle de violation TSPEC**, qui correspond à la durée en secondes pendant laquelle le

périphérique 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. Entrez une durée comprise entre 0 et 900 secondes. La valeur par défaut est 300 secondes.

ÉTAPE 3 Sélectionnez l'interface **Radio** à configurer (Radio 1 ou Radio 2).

ÉTAPE 4 Dans la zone Paramètres de base, configurez les paramètres suivants :

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** : active ou désactive l'interface radio. Par défaut, la radio est activée.

REMARQUE : Si vous activez la radio 5 GHz avec une bande passante de 80 MHz et si la radio transporte un trafic très intense, le périphérique WAP aura besoin de plus d'énergie que ce que fournit la norme PoE IEEE 802.3af (12,95 W). Lors de l'utilisation du canal 80 MHz, il est vivement recommandé d'alimenter le périphérique WAP à l'aide d'un appareil PSE (Power Source Equipment) 802.3at. Si l'énergie requise par le périphérique WAP est supérieure à la valeur maximale fournie par l'appareil PSE, il se peut que le périphérique WAP redémarre.

- **Adresse MAC** : adresse Media Access Control (MAC) de l'interface. L'adresse MAC est attribuée par le fabricant et ne peut pas être modifiée.
- **Mode** : norme IEEE 802.11 et fréquence utilisées par la radio. La valeur par défaut de Mode est 802.11a/n/ac pour Radio 1 et 802.11b/g/n pour Radio 2. Pour chaque radio, sélectionnez l'un des modes disponibles.

  Radio 1 prend en charge les modes radio suivants :

  - 802.11a **:** seuls les clients 802.11a peuvent se connecter au périphérique WAP.
  - 802.11a/n/ac : les clients 802.11a, 802.11n et 802.11ac fonctionnant dans la fréquence 5-GHz peuvent se connecter au périphérique WAP.
  - 802.11n/ac : les clients 802.11n et 802.11ac fonctionnant dans la fréquence 5-GHz peuvent se connecter au périphérique WAP.

  Radio 2 prend en charge les modes radio suivants :

  - 802.11b/g : les clients 802.11b et 802.11g peuvent se connecter au périphérique WAP.
  - 802.11b/g/n (par défaut) : les clients 802.11b, 802.11g et 802.11n fonctionnant dans la fréquence 2,4 GHz peuvent se connecter au périphérique WAP.

- 802.11n 2,4 GHz : seuls les clients 802.11n fonctionnant dans la fréquence 2,4 GHz peuvent se connecter au périphérique WAP.

- **Bande passante de canal** (modes 802.11n et 802.11ac uniquement) : la spécification 802.11n autorise un canal de 40 MHz en plus du canal de 20 MHz hérité qui est disponible avec les autres modes. Le canal de 40 MHz offre des débits de données plus élevés, mais laisse moins de canaux à la disposition des autres périphériques de 2,4 GHz et 5 GHz.

  La spécification 802.11ac autorise la présence d'un canal d'une largeur de 80 MHz en plus des canaux de 20 et 40 MHz.

  Définissez le champ à 20 MHz afin de restreindre l'utilisation de la bande passante du canal à un canal 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 du canal de 80 MHz.

- **Canal principal** (modes 802.11n avec une bande passante de 20/40 MHz seulement) : on peut considérer qu'un canal de 40 MHz se compose de deux canaux de 20 MHz contigus dans le domaine de fréquence. Ces deux canaux de 20 MHz sont souvent appelés canal principal et 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 ainsi que 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.
  - **Plus faible** : 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 **Automatique** pour le paramètre de canal, le périphérique 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).

- **Mode d'analyse de spectre**: état du mode d'analyse de spectre. Le mode d'analyse de spectre peut être défini sur Désactiver, Analyseur de spectre dédié ou Analyseur de spectre hybride. La valeur par défaut est Désactiver..

ÉTAPE 5 Dans la zone Paramètres avancés, définissez les paramètres suivants :

- **Air Time Fairness**: ce paramètre permet d'activer ou de désactiver la fonction ATF. Cette fonction résout le problème lié aux transferts de données lents qui ralentissent les transferts rapides.
- **Prise en charge DFS** : ce champ est disponible uniquement si le mode radio sélectionné fonctionne dans la fréquence de 5 GHz.

  En ce qui concerne les radios situées dans la bande de 5 GHz, lorsque la prise en charge DFS est active et que le domaine de réglementation nécessite une détection radar sur le canal, les fonctionnalités DFS (Dynamic Frequency Selection) et TPC (Transmit Power Control) de 802.11h sont activées.

  DFS est une fonctionnalité qui demande aux périphériques sans fil de partager leur spectre et d'éviter le fonctionnement associé des canaux avec les systèmes radar dans la bande de 5 GHz. Les exigences de la fonctionnalité DFS varient en fonction du domaine de réglementation, qui est déterminé par le paramètre de code de pays du point d'accès.

  Lorsque vous utilisez le mode sans fil 802.11h, il y a plusieurs éléments clés que vous devez connaître à propos de la norme IEEE 802.11h :

  - Le mode 802.11h ne fonctionne que pour la bande de 5 GHz. Il n'est pas requis pour la bande de 2,4 GHz.
  - Si vous opérez dans un domaine 802.11h, le point d'accès tente d'utiliser le canal que vous attribuez. Si le canal a été bloqué par une détection de radar précédente ou si le point d'accès détecte un radar sur le canal, alors le point d'accès sélectionne automatiquement un autre canal.
  - Si 802.11h est activée, le point d'accès ne sera pas opérationnel dans la bande 5 GHz pendant au moins 60 secondes en raison de la recherche de radar.
  - La configuration des liaisons WDS peut s'avérer difficile lorsque la norme 802.11h est opérationnelle. Ceci est dû au fait que les canaux de fonctionnement des deux points d'accès sur la liaison WDS peuvent changer constamment en fonction de l'utilisation du canal et des interférences radar. WDS fonctionnera uniquement si les deux points d'accès se trouvent sur le même canal. Pour plus d'informations sur WDS, reportez-vous à la section **Pont**.

- **Intervalle de garde 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 pour cent du débit de données.

  Le client avec lequel le périphérique WAP communique doit aussi prendre en charge l'intervalle de sûreté court.

  Sélectionnez l'une des options suivantes :

  - **Oui** : le périphérique WAP transmet les données avec un intervalle de sûreté de 400 nanosecondes lorsqu'il communique avec des clients qui prennent aussi en charge l'intervalle de sûreté court. Oui est la sélection par défaut.
  - **Non** : le périphérique 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 (Automatique). Lorsque la protection est activée, celle-ci est appelée si des périphériques hérités se trouvent à portée du périphérique WAP.

  Vous pouvez désactiver la protection (Désactivée) ; cependant, les clients hérités ou les périphériques 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 périphériques WAP contre les transmissions 802.11g.

REMARQUE : Ce paramètre n'empêche pas le client de s'associer au périphérique WAP.

- **Intervalle de balise** : intervalle entre la transmission des trames de balise. Le périphérique WAP les transmet 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).

  Entrez un entier compris entre 20 et 2 000 millisecondes. La valeur par défaut est 100 millisecondes.

- **Période DTIM** : période DTIM (Delivery Traffic Information Map). Entrez 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 basse puissance qui ont des données mises en mémoire tampon sur le périphérique WAP en attente de sélection.

  La période DTIM que vous spécifiez indique la fréquence à laquelle les clients servis par ce périphérique WAP doivent rechercher les données mises en mémoire tampon qui se trouvent encore sur le périphérique WAP en attente de sélection.

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

- **Seuil de fragmentation** : seuil de la taille de trame en octets. L'entier valide doit être pair et se trouver dans la plage comprise entre 256 et 2 346. La valeur par défaut est 2 346.

  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 que vous avez défini, la fonction de 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 une valeur la plus élevée (2 346 octets, qui est la valeur par défaut) désactive effectivement la fragmentation.

  La fragmentation implique une charge de traitement supérieure, en raison du travail supplémentaire nécessaire à la division et au réassemblage des trames, mais aussi parce qu'elle augmente le trafic des messages sur le réseau. Toutefois, la fragmentation améliore la performance et la fiabilité du réseau si elle est correctement configurée.

  L'envoi de trames plus petites (par l'intermédiaire d'un seuil de fragmentation plus bas) peut aider à résoudre les problèmes d'interférences, par exemple avec les fours à micro-ondes.

  Les trames agrégées 802.11n ou 802.11ac (AMPDU) ne peuvent pas être fragmentées. La fragmentation n'est possible que pour les modes radio hérités 802.11a et 802.11b/g.

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 RTS (Request to Send). La plage de nombres entiers valides est comprise 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 aider à contrôler le flux de trafic dans le périphérique WAP, notamment lorsqu'il comporte un grand nombre de clients. Si vous spécifiez une faible valeur de seuil, 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.

  Le seuil RTS est utilisé uniquement pour les trames de données 802.11 héritées (c'est-à-dire pas pour 802.11n ou 802.11ac). Dans le cas des modes 802.11n et 802.11ac, les transmissions AMPDU sont protégées par un échange RTS/CTS, indépendamment de la longueur des trames.

- **Utilisation de la bande passante** : **indique le volume de bande passante radio pouvant être consommé avant que le périphérique WAP ne cesse d'autoriser de nouvelles associations de clients. La plage de nombres entiers valide est comprise entre 0 et 100 pour cent. Si elle est définie à 0, toutes les nouvelles associations sont autorisées quel que soit le taux d'utilisation. La valeur par défaut est 0.**

- **Nombre maximal de clients associés** : nombre maximal de stations autorisées à accéder à chaque radio de ce périphérique WAP à tout moment. Vous pouvez entrer un entier compris entre 0 et 200. La valeur par défaut est 200 stations. Le périphérique bibande WAP571/E peut prendre en charge un maximum de 400 clients.

- **Puissance de transmission** : valeur de pourcentage du niveau de puissance de transmission pour ce périphérique WAP.

La valeur par défaut de 100 pour cent peut être plus économique qu'un pourcentage inférieur, car elle donne au périphérique WAP une plage de diffusion maximale et réduit le nombre de points d'accès requis.

Pour accroître la capacité du réseau, rapprochez les périphériques 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 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 des rafales 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.**
- **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 **Automatique** est sélectionné, le périphérique 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 débits pris en charge par le périphérique WAP sont indiqués dans Ensembles de débits pris en charge. Vous pouvez sélectionner plusieurs débits (cochez une case pour sélectionner un débit ou décochez-la pour le désélectionner). Le périphérique 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 du périphérique WAP.

Ensembles de débits de base indique les débits annoncés au réseau par le périphérique 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 périphérique 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, l'option Limites de débit de diffusion/multidiffusion est désactivée. Tant que vous n'activez pas l'option Limites de débit de diffusion/multidiffusion, 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.

- **Mode TSPEC** : régule le mode TSPEC global sur le périphérique WAP. Par défaut, le mode TSPEC est désactivé. Les options sont les suivantes :

  - **Activé** : le périphérique WAP traite les demandes TSPEC en fonction des paramètres TSPEC définis sur la page Radio. Utilisez ce paramètre si le périphérique WAP gère le trafic provenant de périphériques QoS, tels qu'un téléphone certifié Wi-Fi.

  - **Désactivé** : le périphérique WAP ignore les demandes TSPEC des stations clientes. Utilisez ce paramètre si vous ne souhaitez pas utiliser TSPEC pour donner la priorité aux périphériques QoS en cas de trafic urgent.

- **Mode ACM voix TSPEC** : régule le contrôle d'admission obligatoire (ACM) pour la catégorie d'accès vocal. Par défaut, le mode ACM voix TSPEC est désactivé. Les options sont les suivantes :

  - **Activé** : une station doit envoyer une demande TSPEC de bande passante au périphérique WAP avant d'envoyer ou de recevoir un flux de trafic vocal. Le périphérique 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 vocale sans nécessiter de TSPEC autorisée ; le périphérique WAP ignore les demandes TSPEC vocales des stations clientes.

- **Limite ACM voix TSPEC** : limite supérieure du volume de trafic que le périphérique 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 pour cent du trafic total.
- **Mode ACM vidéo TSPEC** : régule le contrôle d'admission obligatoire pour la catégorie d'accès vidéo. Par défaut, le mode ACM vidéo TSPEC est désactivé. Les options sont les suivantes :
  - **Activé** : une station doit envoyer une demande TSPEC de bande passante au périphérique WAP avant d'envoyer ou de recevoir un flux de trafic vidéo. Le périphérique 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 ; le périphérique WAP ignore les demandes TSPEC vidéo des stations clientes.
- **Limite ACM vidéo TSPEC** : limite supérieure du volume de trafic que le périphérique 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 pour cent du trafic total.
- **Délai d'inactivité du point d'accès TSPEC** : durée nécessaire à un périphérique 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 périphérique 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** : active ou désactive l'interaction du trafic hérité dans les files d'attente fonctionnant comme ACM. Par défaut, ce mode est désactivé.
- **TurboQAM** : cette fonctionnalité a pour but d'activer/de désactiver les extensions spécifiques à Broadcom dans VHT pour les liaisons Broadcom-vers-Broadcom. La fonction VHT prend en charge les débits VHT 256QAM non spécifiés par le projet de norme 802.11ac. Les débits sont les suivants :

mode LDPC VHT global, MCS 9 Nss 1 20 MHz, MCS 9 Nss 2 20 MHz, MCS 6 Nss 3 80 MHz. La fonction VHT est prise en charge pour la couche physique 802.11ac.

ÉTAPE 6 Cliquez sur **Enregistrer**. Les modifications sont enregistrées dans la configuration de démarrage.

AVERTISSEMENT Une fois les nouveaux paramètres enregistrés, les processus correspondants peuvent être arrêtés et redémarrés. Toutefois, dans ce cas, il se peut que le périphérique WAP perde sa connectivité. Nous vous recommandons de modifier les paramètres du périphérique WAP lorsqu'une perte de connectivité peut affecter vos clients sans fil.

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. Les points d'accès non autorisés constituent une menace en matière de sécurité car toute personne ayant accès aux locaux peut, par ignorance ou par malveillance, installer un point d'accès sans fil bon marché pouvant potentiellement permettre à des personnes non autorisées d'accéder au réseau.

Le point d'accès effectue une analyse RF sur tous les canaux de chaque radio 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 Détection de point d'accès non autorisé. 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 Liste des points d'accès non autorisés détectés et la Liste des points d'accès approuvés fournissent les informations vous permettant de prendre les mesures adéquates. Le point d'accès n'a aucun contrôle sur les points d'accès non autorisés qui sont indiqués dans les listes et ne peut pas appliquer de stratégies de sécurité aux points d'accès détectés via l'analyse RF.

Pour obtenir des informations supplémentaires sur les points d'accès non autorisés, sélectionnez Technologie sans fil > Détection de point d'accès non autorisé dans le volet de navigation principal.

Pour obtenir des informations supplémentaires sur les points d'accès non autorisés, sélectionnez **Technologie sans fil > Détection de point d'accès non autorisé**.

Lorsque la détection de point d'accès 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

La détection de point d'accès non autorisé peut être activée et désactivée. Pour que la radio puisse collecter des informations sur les points d'accès non autorisés, cliquez sur **Activer** en regard de **Détection du point d'accès** pour Radio 1 ou Radio 2, puis cliquez sur **Enregistrer**.

La détection des points d'accès non autorisés ne possède aucune méthode d'actualisation et le SSID est conservé dans la base de données une fois détecté.

Les informations relatives aux points d'accès non autorisés détectés et approuvés s'affichent. Vous pouvez cliquer sur **Actualiser** pour actualiser l'écran et afficher les informations les plus à jour :

- **Action** : si le point d'accès se trouve dans la Liste des points d'accès non autorisés détectés, vous pouvez cliquer sur **Approuvé** pour le déplacer vers la Liste des points d'accès approuvés.

  Si le point d'accès se trouve dans la Liste des points d'accès approuvés, vous pouvez cliquer sur **Non approuvé** pour le déplacer vers la Liste des points d'accès non autorisés détectés.

REMARQUE : La Liste des points d'accès non autorisés détectés et la Liste des points d'accès approuvés fournissent des informations. Le point d'accès n'a aucun contrôle sur les points d'accès figurant dans la liste et ne peut pas appliquer de stratégies de sécurité aux points d'accès détectés via l'analyse RF.

- **Adresse MAC** : adresse MAC du point d'accès non autorisé.
- **Radio** : indique si le point d'accès non autorisé a été détecté sur la Radio 1 (wlan0) ou la Radio 2 (wlan1).
- **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).

REMARQUE : Vous pouvez définir l'intervalle de balise sur la page **Radio**.

- **Type** : type de périphérique :
  - Point d'accès indique que le périphérique non autorisé est un point d'accès qui prend en charge la structure de réseau sans fil IEEE 802.11 en mode Infrastructure.
  - Ad hoc indique une station non autorisée fonctionnant en mode Ad hoc. Les stations définies en mode Ad hoc communiquent directement entre elles, sans utiliser de point d'accès classique. Le mode Ad hoc est une structure de réseau sans fil IEEE 802.11, également appelée mode peer-to-peer, ou un ensemble de services de base indépendants (IBSS).
- **SSID** : SSID (Service Set Identifier) du périphérique WAP.

  Le SSID est une chaîne alphanumérique de 32 caractères maximum qui identifie de manière unique un réseau local sans fil. On l'appelle également Nom du réseau.
- **Confidentialité** : indique si un processus de sécurité est appliqué au périphérique non autorisé :
  - L'option Désactivé indique que le mode de Sécurité sur le périphérique non autorisé est défini sur Aucun (aucune sécurité).
  - L'option Activé indique que le périphérique non autorisé intègre un processus de sécurité.

REMARQUE : Vous pouvez utiliser la page **Réseaux** pour configurer la sécurité sur le point d'accès.

- **WPA** : spécifie si la sécurité WPA est activée ou désactivée pour le point d'accès non autorisé.
- **Bande** : mode IEEE 802.11 utilisé sur le point d'accès non autorisé. (Par exemple, IEEE 802.11a, IEEE 802.11b, 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, 802.11n ou 802.11ac (ou une combinaison des modes).
- **Canal** : canal sur lequel le point d'accès non autorisé diffuse actuellement.

Le canal définit la partie du spectre radio utilisée par la radio pour la transmission et la réception.

REMARQUE : La page **Radio** vous permet de définir le canal.

REMARQUE : Lorsque le point d'accès fonctionne dans le canal DFS, l'analyse est interdite. Par conséquent, aucun point d'accès non autorisé ne sera détecté.

- **Débit** : débit, en mégabits par seconde, auquel le point d'accès non autorisé transmet actuellement.

  Le débit actuel est toujours l'un des débits spécifiés dans Débits pris en charge.

  La vitesse signalée est la vitesse du dernier paquet transmis au client à partir du point d'accès. Cette valeur peut varier dans la gamme des vitesses annoncées sur la base de la qualité du signal entre le point d'accès et le client, et de la vitesse à laquelle les trames de diffusion ou de multidiffusion sont envoyées. Lorsque le point d'accès envoie une trame de diffusion à une station en utilisant les vitesses par défaut, le champ indique 1 Mbit/s pour les radios 2,4 GHz et 6 Mbit/s pour les radios 5 GHz. Les clients non actifs sont les plus susceptibles de signaler des vitesses par défaut faibles.

- **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** : ensembles 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**.

Création et enregistrement d'une Liste des points d'accès approuvés

Pour créer une Liste des points d'accès approuvés et l'enregistrer dans un fichier :

ÉTAPE 1 Dans la Liste des points d'accès non autorisés détectés, cliquez sur **Confiance** pour les points d'accès que vous connaissez. Les points d'accès approuvés sont déplacés vers la Liste des points d'accès approuvés.

ÉTAPE 2 Dans la zone Télécharger/sauvegarder la liste des points d'accès approuvés, sélectionnez **Sauvegarder (Point d'accès vers ordinateur)**.

ÉTAPE 3 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 approuvés

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, procédez comme suit :

ÉTAPE 1 Dans la zone Télécharger/sauvegarder la liste des points d'accès approuvés, sélectionnez **Télécharger (Ordinateur vers point d'accès)**.

ÉTAPE 2 Cliquez sur **Parcourir** et choisissez le fichier à importer.

Le fichier que vous importez 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 3 Indiquez si vous souhaitez remplacer la Liste des points d'accès approuvés existante ou ajouter les entrées du fichier importé à la Liste des points d'accès approuvés.

a. Sélectionnez **Remplacer** pour importer la liste et remplacer le contenu de la Liste des points d'accès connus.

b. Sélectionnez **Fusionner** pour importer la liste et ajouter les points d'accès du fichier importé aux points d'accès qui sont déjà présents dans la Liste des points d'accès connus.

ÉTAPE 4 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.

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 périphérique WAP physique. Le point d'accès prend en charge jusqu'à 16 points d'accès virtuels. 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 imprimables plus l'espace (ASCII 0x20) sont autorisés.

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 de 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 inclus. Le périphérique WAP571/E prend en charge 33 VLAN actifs (32 pour le réseau local sans fil, plus un VLAN de gestion).

Par défaut, le VID attribué à l'utilitaire de configuration pour le périphérique 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 le périphérique 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 **Technologie sans fil** > **Réseaux** dans le volet de navigation.

ÉTAPE 2 Sélectionnez l'interface **Radio** sur laquelle vous voulez configurer les VAP (**Radio 1** ou **Radio 2**).

ÉTAPE 3 Activez la case à cocher **Activé** correspondant au VAP que vous voulez configurer.

—Ou—

Si VAP0 est le seul VAP configuré sur le système et que vous souhaitez ajouter un VAP, cliquez sur **Ajouter**. Sélectionnez ensuite le VAP, puis cliquez sur **Modifier**.

ÉTAPE 4 Configurez les paramètres suivants :

- **ID de VLAN** : VID du VLAN à associer au VAP.

AVERTISSEMENT 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 est incorrectement configuré.
Si un client sans fil se connecte au périphérique WAP par l'intermédiaire de ce VAP, le périphérique WAP balise tout le trafic à partir du client sans fil avec l'ID de VLAN

que vous saisissez dans ce champ, 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.

REMARQUE : 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 le périphérique. Vérifiez la configuration des ID de VLAN non balisés et de gestion sur la page du réseau local (LAN). Pour obtenir plus d'informations, reportez-vous à la section **Configuration du VLAN**.

- **Nom SSID** : nom du réseau sans fil. Le SSID est une chaîne alphanumérique constituée de 32 caractères maximum. Choisissez un SSID unique pour chaque VAP.

REMARQUE : Si vous êtes connecté en tant que client sans fil au périphérique WAP que vous administrez, la réinitialisation du SSID entraînera une perte de connexion au périphérique 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 le périphérique WAP à diffuser le SSID dans ses trames de balise. Le paramètre Diffusion 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.

- **Sécurité** : type d'authentification requis pour l'accès au VAP :
  - Aucune
  - WEP statique
  - WEP dynamique
  - WPA personnel

- WPA entreprise

Si vous sélectionnez un autre mode de sécurité que Aucune, des champs supplémentaires s'affichent. Nous vous conseillons d'utiliser WPA personnel ou WPA entreprise comme type d'authentification, car ils offrent une sécurité plus élevée. Utilisez WEP statique ou WEP dynamique uniquement pour les périphériques ou ordinateurs sans fil hérités qui ne prennent pas en charge WPA personnel/entreprise. Si vous devez définir la sécurité sur WEP statique ou WEP dynamique, configurez Radio sur le mode 802.11a ou 802.11b/g (voir **Radio**). Le mode 802.11n restreint l'utilisation de WEP statique ou WEP dynamique en tant que mode de sécurité.

- **Filtrage MAC** : indique si les stations qui peuvent accéder à ce VAP sont limitées à une liste globale configurée d'adresses MAC (voir **Filtrage MAC**). Vous pouvez sélectionner l'un de ces types de filtrage MAC :
  - **Désactivé** : vous n'utilisez pas le filtrage MAC.
  - **Local** : vous utilisez la liste d'authentification MAC que vous configurez sur la page **Filtrage MAC**.
  - **RADIUS** : vous utilisez la liste d'authentification MAC sur un serveur RADIUS externe.
- **Isolation des canaux** : active et désactive l'isolation des stations.
- Lorsque ce paramètre est désactivé, les clients sans fil peuvent communiquer entre eux normalement en envoyant le trafic via le périphérique WAP.
  - Lorsque ce paramètre est activé, le périphérique WAP bloque les communications entre les clients sans fil situés sur le même VAP. Le périphérique WAP autorise toujours le trafic de données entre ses clients sans fil et les périphériques 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.

REMARQUE : L'isolation des canaux peut être appliquée aux clients connectés au même VAP d'un point d'accès donné, mais pas à l'ensemble des clients connectés au même VAP de différents points d'accès. Ainsi, les clients connectés au même VAP d'un point d'accès donné ne peuvent pas s'envoyer de requêtes ping, contrairement aux clients connectés au même VAP de différents points d'accès.

- **Guidage de bandes** : active le guidage de bande lorsque les deux radios sont actives. La bande passante d'ordre n de la radio n'est pas prise en considération pour le guidage de bande. Même si la radio 5 GHz utilise la bande passante de 20 MHz, le point d'accès tente de guider les clients vers cette radio après configuration du guidage de bande.

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

AVERTISSEMENT Une fois les nouveaux paramètres enregistrés, les processus correspondants peuvent être arrêtés et redémarrés. Toutefois, dans ce cas, il se peut que le périphérique WAP perde sa connectivité. Nous vous recommandons de modifier les paramètres du périphérique WAP lorsqu'une perte de connectivité peut affecter vos clients sans fil.

REMARQUE : Pour supprimer un VAP, sélectionnez-le, puis cliquez sur **Supprimer**. Pour enregistrer définitivement votre suppression, cliquez sur **Enregistrer** lorsque vous avez terminé.

Configuration des paramètres de sécurité

Ces sections décrivent les paramètres de sécurité que vous définissez, en fonction de votre sélection dans la liste Sécurité de la page Réseaux.

Aucun

Si vous sélectionnez **Aucun** comme mode de sécurité, aucun paramètre de sécurité supplémentaire ne peut être défini sur le point d'accès. Ce mode signifie que toutes les données transférées de et vers le point d'accès 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 chiffrement 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 chiffrement des données.

WEP statique n'est pas le mode offrant le plus de sécurité, mais il fournit davantage de protection que le mode Aucun, 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 chiffrement est un chiffrement de flux appelé RC4.)

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

- **Index de clé de transfert** : liste des index de clé. Les index de clé 1 à 4 sont disponibles. La valeur par défaut est 1.

  Index de clé de transfert indique la clé WEP utilisée par le périphérique WAP pour chiffrer les données qu'il transmet.

- **Longueur de clé** : longueur de la clé. Sélectionnez-en un :
  - 64 bits
  - 128 bits
- **Type de clé** : type de clé. Sélectionnez-en un :
  - ASCII
  - Hex
- **Clés WEP** : vous pouvez spécifier un maximum de 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 alphabétiques majuscules et minuscules, les chiffres numériques et les symboles spéciaux comme @ et #.
  - Hex : 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 RC4 WEP partagées avec les stations par l'intermédiaire du périphérique WAP.

  Chaque station cliente doit être configurée pour utiliser l'une de ces mêmes clés WEP, dans le même logement que celui spécifié sur le périphérique WAP.

- **Caractères requis** : le nombre de caractères que vous saisissez dans les champs Clé WEP est déterminé par la longueur de clé et le type de clé que vous sélectionnez. Par exemple, si vous utilisez des clés ASCII 128 bits, vous devez saisir 26 caractères dans le champ Clé WEP. Le nombre de

caractères requis est automatiquement mis à jour en fonction de votre sélection de la longueur de clé et du type de clé.

- **Authentification 802.1X** : l'algorithme d'authentification définit la méthode utilisée pour déterminer si une station cliente est autorisée à s'associer à un périphérique 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 :

  - L'authentification **Système ouvert** permet à n'importe quelle station cliente de s'associer au périphérique WAP, peu importe si cette station cliente dispose de la clé WEP correcte. Cet algorithme est aussi utilisé en mode plaintext (texte en clair), IEEE 802.1X et WPA. Lorsque l'algorithme d'authentification est défini sur Système ouvert, tout client peut s'associer au périphérique WAP.

REMARQUE : Le fait qu'une station cliente soit autorisée à s'associer ne signifie pas qu'elle pourra systématiquement échanger des données avec un périphérique WAP. Une station doit disposer de la clé WEP correcte pour pouvoir accéder au périphérique WAP et déchiffrer ses données, mais aussi pour transmettre des données lisibles à celui-ci.

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

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

Règles du mode WEP statique

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

- Toutes les stations clientes doivent avoir la sécurité du LAN sans fil (WLAN) définie sur WEP, et tous les clients doivent disposer de l'une des clés WEP spécifiées sur le périphérique WAP pour pouvoir décoder les transmissions de données du point d'accès vers la station.

- Le périphérique WAP doit avoir 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 le périphérique WAP définit la clé abc123 comme clé WEP 3, alors 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 déchiffrer 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 chiffrer 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.

WEP dynamique

WEP dynamique se réfère à la combinaison de la technologie 802.1x et du protocole EAP (Extensible Authentication Protocol). Avec la sécurité WEP dynamique, les clés WEP sont changées dynamiquement.

Les messages EAP sont envoyés via un réseau sans fil IEEE 802.11 par l'intermédiaire d'un protocole appelé EAP Encapsulation Over LANs (EAPOL). IEEE 802.1X fournit des clés générées dynamiquement qui sont régulièrement actualisées. Un chiffrement de flux RC4 est utilisé pour déchiffrer le corps de trame et le contrôle de redondance cyclique (CRC) de chaque trame 802.11.

Ce mode nécessite l'utilisation d'un serveur RADIUS externe pour l'authentification des utilisateurs. Le périphérique WAP requiert un serveur RADIUS prenant en charge EAP, tel que le serveur d'authentification Internet Microsoft. Pour fonctionner avec les clients Microsoft Windows, le serveur d'authentification doit prendre en charge Protected EAP (PEAP) et MSCHAP V2.

Vous pouvez recourir à un large choix de méthodes d'authentification prises en charge par le mode IEEE 802.1X, notamment les certificats, Kerberos et l'authentification par clé publique. Vous devez configurer les stations clientes afin qu'elles utilisent la même méthode d'authentification que le périphérique WAP.

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

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

  Pour utiliser les paramètres de serveur RADIUS globaux, veillez à cocher la case.

  Pour utiliser un serveur RADIUS distinct pour le VAP, décochez la case et saisissez l'adresse IP du serveur RADIUS, puis renseignez les champs ci-dessous :

- **Type d'adresse IP du serveur** : version IP utilisée par le serveur RADIUS.

  Vous pouvez basculer entre les différents types d'adresse afin de définir les paramètres d'adresse RADIUS globaux IPv4 et IPv6, mais le périphérique 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.

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

  La forme de l'adresse IPv4 doit être similaire à celle-ci : xxx.xxx.xxx.xxx (192.0.2.10). La forme de l'adresse IPv6 doit être similaire à celle-ci : xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx (2001:DB8::CAD5:7D91).

- **Adresse IP du serveur 2** à **4** ou **Adresse IPv6 du serveur-2** à **4** : jusqu'à trois adresses de serveur RADIUS IPv4 ou IPv6 de sauvegarde.

  Si l'authentification auprès du serveur principal échoue, une tentative est effectuée sur chaque serveur de secours configuré.

- **Clé** : clé secrète partagée que le périphérique WAP utilise pour s'authentifier sur le 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** à **Clé 4** : clé RADIUS associée aux serveurs RADIUS de sauvegarde configurés. Le serveur spécifié dans le champ Adresse IP (IPv6) du serveur 2 utilise Clé 2 ; le serveur spécifié dans le champ Adresse IP (IPv6) du serveur 3 utilise Clé 3, etc.
- **Activer la gestion de comptes RADIUS** : active 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.
- **Serveur actif** : permet de sélectionner administrativement le serveur RADIUS actif, ce qui évite au périphérique 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 300. La plage valide est comprise entre 0 et 86400 secondes. La valeur 0 indique que la clé de diffusion n'est pas actualisée.
- **Taux d'actualisation de la clé de session** : intervalle auquel le périphérique 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.

WPA personnel

WPA personnel est une norme IEEE 802.11i Wi-Fi Alliance qui inclut le chiffrement AES-CCMP et TKIP. La version Personnel de WPA 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 personnel est également appelé WPA-PSK.

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

Les paramètres ci-après permettent de configurer WPA Personal :

- **Versions WPA** : types de stations clientes à prendre en charge :
  - **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 que le fait de sélectionner uniquement WPA-TKIP pour le point d'accès n'est pas autorisé, conformément aux dernières exigences de la WiFi Alliance.
  - **WPA2-AES** : toutes les stations clientes du réseau prennent en charge la version WPA2 ainsi que le protocole de chiffrement et de sécurité AES-CCMP. Cette version de WPA fournit une sécurité optimale avec la norme IEEE 802.11i. Conformément aux dernières exigences de la WiFi 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, cochez les deux cases. 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 avoir l'une des clés ci-dessous pour pouvoir s'associer au périphérique WAP :
  - Une clé TKIP valide
  - Une clé AES-CCMP valide
- **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 #.
- **Mesure de la fiabilité de la clé** : le périphérique 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 **Complexité WPA-PSK**.
- **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 300 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.

WPA entreprise

WPA entreprise avec RADIUS est une implémentation de la norme IEEE 802.11i Wi-Fi Alliance, qui inclut le chiffrement 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 pour les clients sans fil qui prennent en charge le WPA d'origine.

Les paramètres ci-après permettent de configurer WPA entreprise :

- **Versions WPA** : types de stations clientes à prendre en charge :
  - **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 que le fait de sélectionner uniquement WPA-TKIP pour le point d'accès n'est pas autorisé, conformément aux dernières exigences de la WiFi Alliance.
  - **WPA2-AES** : toutes les stations clientes du réseau prennent en charge la version WPA2 ainsi que le protocole de chiffrement et de sécurité AES-CCMP. Cette version de WPA fournit une sécurité optimale avec la norme IEEE 802.11i. Conformément aux dernières exigences de la WiFi Alliance, le point d'accès doit prendre en charge ce mode en permanence.
- **MFP** : assure la sécurité des trames de gestion 802.11 non protégées et non cryptées. Ce champ ne s'affiche que lorsque les champs CCMP et de sécurité WPA2 sont activés. Vous pouvez configurer les valeurs des trois cases à cocher suivantes. La valeur par défaut est Compatible.
  - Non requis
  - Compatible
  - Obligatoire
- **Activer la pré-authentification** : si pour WPA Versions, vous sélectionnez uniquement WPA2, ou à la fois WPA et WPA2, vous pouvez activer la pré-authentification pour les clients WPA2.

Cliquez sur Activer la pré-authentification si vous souhaitez que les clients sans fil WPA2 puissent envoyer des paquets de pré-authentification. Les informations de pré-authentification sont relayées du périphérique WAP que le client utilise actuellement vers le périphérique 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 Versions WPA, 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

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

  Pour utiliser les paramètres de serveur RADIUS globaux, veillez à cocher la case.

  Pour utiliser un serveur RADIUS distinct pour le VAP, décochez la case et saisissez l'adresse IP du serveur RADIUS, puis renseignez les champs ci-dessous :

- **Type d'adresse IP du serveur** : version IP utilisée par le serveur RADIUS.

  Vous pouvez basculer entre les différents types d'adresse afin de définir les paramètres d'adresse RADIUS globaux IPv4 et IPv6, mais le périphérique 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.

  Si **IPv4** est sélectionné en tant que **Type d'adresse IP du serveur**, saisissez l'adresse IP du serveur RADIUS que tous les VAP utilisent par défaut (par exemple, 192.168.10.23). Si **IPv6** est sélectionné, saisissez l'adresse IPv6 du serveur RADIUS global principal (par exemple, 2001:DB8:1234::abcd).

- **Adresse IP du serveur 2** à **4** ou **Adresse IPv6 du serveur 2** à **4** : 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 le périphérique WAP et sur votre serveur RADIUS. Le texte que vous entrez s'affiche sous forme d'astérisques pour empêcher d'autres personnes de voir la clé RADIUS pendant que vous la saisissez.

- **Clé 2** à **Clé 4** : clé RADIUS associée aux serveurs RADIUS de sauvegarde configurés. Le serveur spécifié dans le champ **Adresse IP (IPv6) du serveur 2** utilise **Clé 2** ; le serveur spécifié dans le champ **Adresse IP (IPv6) du serveur 3** utilise **Clé 3**, etc.

- **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 au périphérique 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 300 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 le périphérique 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.

Transfert de multidiffusion sans fil

L'acheminement multidestination sans fil permet de réacheminer efficacement le trafic multidestination sur un support sans fil et de résoudre les problèmes de transmission multidestination sur le réseau local sans fil grâce à la destination unique répétée de trames multidestination.

Cette fonction se sert de trames IGMP pour suivre la participation des membres d'un groupe et transmet des paquets multidestination uniquement aux membres intéressés après la conversion d'adresses MAC de destination unique.

Grâce à cette fonction, le transfert des données gagne en fiabilité, car les trames sont envoyées vers une destination unique. De plus, la transmission est plus robuste parce que les débits peuvent être contrôlés dynamiquement sur chaque station en fonction des erreurs de liaison et du bruit.

Une station peut être membre d'un groupe de multidestination. La diffusion entre les stations sera également prise en charge. Le serveur de diffusion multidestination peut être connecté à n'importe quel port LAN.

Configuration des paramètres d'acheminement multidestination sans fil

Pour configurer les paramètres d'acheminement multidestination sans fil :

ÉTAPE 1 Sélectionnez **Technologie sans fil > Transfert de multidiffusion sans fil** dans le volet de navigation.

ÉTAPE 2 Configurez le paramètre suivant :

- **Transfert de multidiffusion sans fil** : active ou désactive globalement l'acheminement multidestination sans fil sur l'appareil Cisco WAP571/E.

REMARQUE : Une fois les nouveaux paramètres enregistrés, les processus correspondants peuvent être arrêtés et redémarrés. Toutefois, dans ce cas, il se peut que le périphérique WAP perde sa connectivité. Nous vous recommandons de modifier les paramètres du périphérique WAP lorsqu'une perte de connectivité peut affecter vos clients sans fil.

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, ce qui automatise l'activation ou la désactivation des VAP et de la radio.

L'une des manières d'utiliser cette fonction est de planifier la radio pour qu'elle ne fonctionne que pendant les heures de bureau, afin de bénéficier de la sécurité adéquate et de diminuer la consommation électrique. Vous pouvez aussi utiliser le planificateur pour autoriser les clients sans fil à accéder aux VAP uniquement à certaines heures de la journée.

Le point d'accès prend en charge jusqu'à 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.

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

Ajout de profils de planificateur

Pour afficher l'état du planificateur et ajouter un profil de planificateur :

ÉTAPE 1 Sélectionnez **Technologie sans fil** > **Planificateur** dans le volet de navigation.

ÉTAPE 2 Assurez-vous que **Mode d'administration** est activé. Il est désactivé par défaut.

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

- **Statut** : état opérationnel du planificateur. L'état est soit Activé soit Désactivé. La valeur par défaut est Désactivé.
- **Motif** : raison de l'état opérationnel du planificateur. Les valeurs possibles sont les suivantes :
  - **Est activé** : le planificateur est activé sur le plan administratif.
  - **Le mode d'administration est désactivé** : l'état opérationnel est inactif, car la configuration globale est désactivée.
  - **L'heure du système est obsolète** : l'heure système n'est plus synchronisée.

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 des règles de planificateur

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 (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.

Configuration d'une règle pour un profil

Pour configurer une règle pour un profil :

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

ÉTAPE 2 Cliquez sur **Ajouter une règle**.

La nouvelle règle s'affiche dans la table des règles.

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

ÉTAPE 4 Dans le menu **Jour de la semaine**, sélectionnez le planning récurrent 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 la radio ou le VAP est opérationnellement activé(e). L'heure est au format 24 heures HH:MM. La plage est <00-23>:<00-59>. La valeur par défaut est 00:00.
- Heure de fin : heure à laquelle la radio ou le VAP est opérationnellement désactivé(e). L'heure est au format 24 heures HH:MM. La plage est <00-23>:<00-59>. La valeur par défaut est 00:00.

ÉTAPE 6 Cliquez sur **Enregistrer**. Les modifications sont enregistrées dans la configuration de démarrage.

REMARQUE : Pour être mis en œuvre, un profil de planificateur doit être associé à une interface radio ou une interface VAP. Reportez-vous à la page **Association au planificateur**.

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

Portée des règles de planificateur

La portée des règles de planificateur est décrite ci-dessous.

- Une règle qui affecte uniquement un jour spécifique n'affecte pas les autres jours.
- Une règle qui utilise des groupes tels que « Tous les jours », « Jour de semaine » ou « Weekend » affecte plusieurs jours.
- Une règle définie pour « Weekend » n'affecte que le samedi et le dimanche, et pas les autres jours de la semaine. Le comportement par défaut du planificateur consiste à activer la radio lorsqu'aucune règle explicite ne contrôle l'activation de la radio pour ce jour précis.
- La fonction du planificateur est conçue de telle manière que chaque règle définit une limite indiquant à quel moment une radio ou un VAP est activé.
- L'entrée « Jour de la semaine » crée la portée des règles. La règle influe UNIQUEMENT la portée définie. « Weekend » signifie uniquement le samedi et le dimanche. « Tous les jours » signifie chaque jour de la semaine, etc. Lors de la définition des règles, l'entrée « Jour de la semaine » de l'interface graphique utilisateur définit la portée de la règle : Weekend, Tous les jours, Jour de la semaine, Dimanche, Lundi, etc.
- Cela permet des règles détaillées. Aucune règle « tout refuser » implicite n'est créée lorsque la portée d'une règle n'inclut pas tous les jours de la semaine. Créez une règle « refuser » ou « désactiver » en définissant la portée appropriée avec une activation pendant uniquement 1 minute. Pour désactiver la radio ou le VAP en permanence SAUF à des heures explicitement autorisées, vous devez créer une règle « Tous les jours » active uniquement pendant 1 minute de minuit à 00:01, ce qui signifie que la radio est active uniquement pendant 1 minute chaque jour. Il est ensuite possible d'ajouter des exceptions correspondant à chaque période pendant laquelle vous voulez que la radio soit active.

Exemple classique :

- Activer la radio de 09:00 à 17:00 du lundi au vendredi

- Aucune radio activée durant le weekend

Créez un profil utilisant deux règles :

Jours de la semaine : Heure de début : 09:00:00 Heure de fin : 17:00

Weekends : Heure de début : 00:00 Heure de fin : 00:01

Association au planificateur

Pour être mis en œuvre, les profils de planificateur doivent être associés à l'interface WLAN ou à une interface VAP. Par défaut, aucun profil de planificateur n'est créé et aucun profil n'est associé à une radio ou un VAP.

Un seul profil de planificateur peut être associé à l'interface WLAN ou à chaque VAP. Un seul profil peut être associé à plusieurs VAP. En cas de suppression du profil de planificateur associé à un VAP ou à l'interface WLAN, l'association est supprimée.

Association d'un profil de planificateur à l'interface WLAN ou à un VAP :

Pour associer un profil de planificateur à l'interface WLAN ou un VAP :

ÉTAPE 1 Sélectionnez **Technologie sans fil** > **Association au planificateur** dans le volet de navigation. Sélectionnez l'interface **Radio** à laquelle vous voulez associer un profil de planificateur (**Radio 1** ou **Radio 2**).

ÉTAPE 2 Pour l'interface WLAN ou un VAP, sélectionnez le profil dans la liste **Nom du profil**.

La colonne **Statut opérationnel de l'interface** indique si l'interface est actuellement activée ou désactivée.

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

Filtrage MAC

Le filtrage Media Access Control (MAC) peut être utilisé pour interdire ou autoriser uniquement l'authentification des stations clientes répertoriées sur le point d'accès. L'authentification MAC doit être activée ou désactivée pour chaque VAP sur la page **Réseaux**. Selon la configuration du VAP, le périphérique WAP peut se référer à une liste de filtrage MAC stockée sur un serveur RADIUS externe ou stockée localement sur le périphérique WAP.

Configuration d'une liste de filtrage MAC stockée localement sur le périphérique WAP

Le périphérique WAP ne prend en charge qu'une seule liste de filtrage MAC locale. Ainsi, la même liste s'applique à tous les VAP autorisés à utiliser la liste locale. 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.

Configuration du filtrage MAC

Pour configurer le filtrage MAC :

ÉTAPE 1 Sélectionnez **Technologie sans fil** > **Filtrage MAC** dans le volet de navigation.

ÉTAPE 2 Sélectionnez la façon dont le périphérique WAP utilise la liste de filtrage :

- **Autoriser uniquement les stations répertoriées** : toute station qui n'apparaît pas dans la Liste des stations se voit interdire l'accès au réseau via le périphérique WAP.
- **Bloquer toutes les stations répertoriées** : seules les stations qui figurent dans la liste se voient interdire l'accès au réseau via le périphérique WAP. L'accès est autorisé pour toutes les autres stations.

REMARQUE : Le paramètre de filtre s'applique également à la liste de filtrage MAC stockée sur le serveur RADIUS, s'il en existe une.

ÉTAPE 3 Dans le champ **Adresse MAC**, saisissez l'adresse MAC à autoriser ou bloquer, puis cliquez sur **Ajouter**.

L'adresse MAC s'affiche dans la **Liste des stations**.

ÉTAPE 4 Continuez à saisir des adresses MAC jusqu'à ce que la liste soit terminée, puis cliquez sur **Enregistrer**. Les modifications sont enregistrées dans la configuration de démarrage.

REMARQUE : Pour supprimer une adresse MAC de la Liste des stations, sélectionnez-la, puis cliquez sur **Retirer**.

REMARQUE : Une fois les nouveaux paramètres enregistrés, les processus correspondants peuvent être arrêtés et redémarrés. Toutefois, dans ce cas, il se peut que le périphérique WAP perde sa connectivité. Nous vous recommandons de modifier les paramètres du périphérique WAP lorsqu'une perte de connectivité peut affecter vos clients sans fil.

Configuration de l'authentification MAC sur le serveur RADIUS

Si un ou plusieurs VAP sont configurés pour utiliser un filtre MAC stocké sur un serveur d'authentification RADIUS, 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
Nom-d'utilisateur (1)	Adresse MAC de la station cliente.	Adresse MAC Ethernet valide.
Mot de passe utilisateur (2)	Mot de passe global fixe utilisé pour rechercher une entrée MAC de client.	NOPASSWORD

Pont

Cette section décrit les deux types de ponts. Elle contient les rubriques suivantes :

Pont WDS

Le Système de distribution sans fil (WDS) vous permet de connecter plusieurs périphériques WAP571/E. Avec WDS, les points d'accès peuvent communiquer entre eux sans câbles. Cette fonctionnalité est essentielle à la satisfaction des clients en itinérance et à la gestion de plusieurs réseaux sans fil. Elle simplifie également l'infrastructure réseau en réduisant la quantité de câbles nécessaire. Vous pouvez configurer le périphérique WAP en mode point à point ou point à multipoint en fonction du nombre de liaisons à connecter.

En mode point à point, le périphérique WAP accepte les associations de clients et communique avec les clients sans fil et autres répéteurs. Le périphérique WAP transfère tout le 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 périphérique réseau OSI Layer 2.

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

Le point d'accès peut également fonctionner en tant que répéteur. Dans ce mode, le point d'accès sert de connexion entre deux périphériques WAP qui sont trop éloignés pour être à portée cellulaire. Lorsqu'il fonctionne en tant que répéteur, le point d'accès 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 au point d'accès 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 périphérique WAP qui fonctionne en tant que répéteur.

Avant de configurer WDS sur le périphérique WAP, veuillez noter les informations ci-après :

- Dans le cas d'un mode de pontage pur ne permettant pas les associations de clients, nous recommandons d'utiliser une clé WPA complexe pour VAP0 ou de désactiver la diffusion SSID.
- Tous les périphériques WAP Cisco participant à une liaison WDS doivent avoir les paramètres identiques suivants :
  - Radio
  - IEEE 802.11 Mode
  - Bande passante de canal
  - Canal (l'option Automatique n'est pas recommandée)

REMARQUE : Si vous effectuez un pontage dans la bande 802.11n 2,4 GHz, définissez 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 périphériques WAP 20 MHz sont détectés dans la zone. Une bande passante de canal incohérente peut entraîner la déconnexion de la liaison.

Reportez-vous à la section **Radio** (paramètres de base) pour obtenir des informations sur la définition de ces paramètres.

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

Pour configurer un pont WDS :

ÉTAPE 1 Sélectionnez **Technologie sans fil** > **Pont** dans le volet de navigation.

ÉTAPE 2 Sélectionnez le pont WDS dans le menu déroulant.

ÉTAPE 3 Cochez **Activer** en regard de l'**interface WDS** à configurer.

ÉTAPE 4 Définissez les paramètres restants :

- **Adresse MAC distante** : spécifie l'adresse MAC du périphérique WAP de destination, à savoir le périphérique WAP situé à l'autre extrémité de la liaison WDS et auquel les données sont envoyées ou transmises et à partir duquel les données sont reçues.

CONSEIL L'adresse MAC est indiquée sur la page Statut et statistiques > Interface réseau.

- **Chiffrement** : type de chiffrement à utiliser sur la liaison WDS ; il ne doit pas obligatoirement correspondre au VAP pour lequel vous effectuez un pontage. Les paramètres de chiffrement WDS sont propres au pont WDS. Les options disponibles sont Aucun, WEP et WPA personnel. WPA2-PSK est une option relative au chiffrement des liaisons WDS et à la sécurité des VAP. L'administrateur doit sélectionner ces options pour qu'elles soient mises en œuvre.

  Si vous ne souhaitez pas sécuriser la liaison WDS, vous pouvez choisir de ne définir aucun type de chiffrement. De même, si vous souhaitez sécuriser la liaison, vous pouvez choisir entre WEP statique et WPA personnel. En mode WPA personnel, le périphérique WAP utilise le chiffrement WPA2-PSK avec CCMP (AES) sur la liaison WDS. Pour plus d'informations sur les options de chiffrement, reportez-vous à la section **WEP sur les liaisons WDS** ou **WPA/PSK sur les liaisons WDS** après cette procédure.

REMARQUE : Le mode WEP statique est applicable uniquement lorsque la radio fonctionne en mode hérité : 802.11a pour une radio 5 GHz et 802.11b/g pour une radio 2,4 GHz.

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

ÉTAPE 6 Répliquez cette procédure sur le ou les autres périphériques connectés au pont.

CONSEIL Vous pouvez vérifier si la liaison de pont est active en vous rendant sur la page Statut et statistiques > Interface réseau. Dans le tableau Statut de l'interface, l'état Actif doit être spécifié pour WLAN0:WDS(x).

REMARQUE : Un point d'accès WDS partenaire situé dans le réseau distant retient son adresse IP de gestion acquise à partir d'un serveur DHCP connecté au point d'accès WDS situé dans le réseau principal, même si la liaison WDS est rompue. L'adresse IP est libérée lorsque l'interface WDS est désactivée sur le plan administratif.

AVERTISSEMENT Une fois les nouveaux paramètres enregistrés, les processus correspondants peuvent être arrêtés et redémarrés. Toutefois, dans ce cas, il se peut que le périphérique WAP perde sa connectivité. Nous vous recommandons de modifier les paramètres du périphérique WAP lorsqu'une perte de connectivité peut affecter vos clients sans fil.

WEP sur les liaisons WDS

Ces champs supplémentaires apparaissent lorsque vous sélectionnez le type de chiffrement 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, spécifiez 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 chiffrement RC4 partagées avec les stations par l'intermédiaire du périphérique WAP.

  Veuillez noter 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 chiffrement WPA/PSK.

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

  L'ID WDS 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 le périphérique 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 du point d'accès permet au périphérique WAP d'étendre l'accessibilité d'un réseau distant. En mode Pont de groupe de travail, le point d'accès fonctionne comme une station sans fil (STA) sur le réseau local (LAN) sans fil. Il peut acheminer le trafic entre un réseau filaire distant et le réseau local (LAN) sans fil qui est connecté via le mode Pont de groupe de travail.

Cette fonction assure la prise en charge du mode STA. Le périphérique WAP peut fonctionner dans un seul BSS (Basic Service Set) en tant que périphérique STA. Lorsque le mode Pont de groupe de travail est activé, le point d'accès ne prend en charge qu'un seul BSS auquel il est associé en tant que client sans fil.

Il est recommandé d'utiliser le mode Pont de groupe de travail uniquement lorsque la fonction Pont WDS ne peut pas fonctionner avec un point d'accès homologue. 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 périphériques Cisco WAP571/E. 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 le point d'accès.

En mode Pont de groupe de travail, le BSS géré par l'autre périphérique WAP (c'est-à-dire celui auquel le périphérique WAP s'associe en tant que STA) est appelé l'interface cliente d'infrastructure, et l'autre périphérique WAP est appelé le point d'accès en amont.

Les périphériques connectés à l'interface filaire du périphérique WAP peuvent accéder au réseau connecté par l'interface cliente d'infrastructure.

Avant de configurer Pont de groupe de travail sur le périphérique WAP, veuillez noter les informations ci-après :

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

  Reportez-vous à la section **Radio** (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 **Technologie sans fil > Pont** dans le volet de navigation.

ÉTAPE 2 Sélectionnez le mode Pont de groupe de travail dans le menu déroulant.

ÉTAPE 3 Sélectionnez **Activer** pour **Mode du pont de groupe de travail**.

ÉTAPE 4 Sélectionnez l'interface radio sur laquelle vous souhaitez définir le mode Pont de groupe de travail (**Radio 1** ou **Radio 2**).

ÉTAPE 5 Configurez les paramètres suivants pour l'interface cliente d'infrastructure (montante) :

- **SSID** : SSID du BSS.

REMARQUE : Une flèche est présente à côté du SSID pour l'analyse SSID (SSID Scanning) ; cette fonction est désactivée par défaut et est uniquement activée si la détection de point d'accès est activée dans la détection de point d'accès non autorisé (qui est également désactivée par défaut).

- **Sécurité** : type de sécurité à utiliser pour l'authentification en tant que station cliente sur le périphérique WAP montant. Les choix possibles sont :
  - **Aucune**
  - **WEP statique**
  - **WPA personnel**
  - **WPA entreprise**
- **ID de VLAN** : VLAN associé au BSS.

REMARQUE : L'interface cliente d'infrastructure sera associée au périphérique WAP montant avec les informations d'identification configurées. Le périphérique WAP peut obtenir son adresse IP d'un serveur DHCP sur la liaison montante. Vous pouvez également attribuer une adresse IP statique. Le champ Statut de la connexion indique si le WAP est connecté au périphérique WAP montant. Vous pouvez cliquer sur le bouton Actualiser pour afficher l'état le plus récent de la connexion.

Le point d'accès WGB (celui qui joue le rôle de client pour le point d'accès en amont) conserve l'adresse IP de gestion acquise auprès d'un serveur DHCP en amont, même s'il est dissocié du point d'accès en amont.

REMARQUE : Le mode WEP statique est applicable uniquement lorsque la radio fonctionne en mode hérité : 802.11a pour une radio 5 GHz et 802.11b/g pour une radio 2,4 GHz.

QoS

Les paramètres de qualité de service (QoS) vous permettent de configurer des files d'attente de transmission pour bénéficier d'un meilleur débit et de meilleures performances si vous administrez un trafic sans fil différencié, comme la voix sur IP (VoIP), d'autres types de lecture audio, vidéo et multimédia en continu, ainsi que des données IP classiques.

Pour configurer la qualité de service (QoS) sur le point d'accès, 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 (via les fenêtres de contention) pour la transmission.

Les paramètres EDCA (Enhanced Distributed Channel Access) du WAP affectent le trafic transmis du périphérique WAP vers la station cliente.

Les paramètres EDCA de la station affectent le trafic transmis de la station cliente vers le périphérique WAP.

En utilisation normale, les valeurs EDCA par défaut du périphérique WAP et de la station ne requièrent aucune modification. La modification de ces valeurs affecte la qualité de service (QoS) fournie.

Configuration des paramètres EDCA du périphérique WAP et de la station

Pour définir les paramètres EDCA du périphérique WAP et de la station :

ÉTAPE 1 Sélectionnez **Technologie sans fil** > **QoS** dans le volet de navigation. Sélectionnez l'interface radio sur laquelle vous souhaitez définir les paramètres de qualité de service (QoS) (**Radio 1** ou **Radio 2**).

ÉTAPE 2 Sélectionnez une option dans la liste **Modèle EDCA** :

- **Paramètres WFA par défaut** : renseigne les paramètres EDCA du périphérique WAP et de la station avec les valeurs WiFi Alliance par défaut, qui sont optimales pour un trafic mixte général.
- **Optimisé pour la voix** : renseigne les paramètres EDCA du périphérique WAP et de la station avec les valeurs les plus adaptées au trafic vocal.
- **Personnalisés** : 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 la station. Si vous choisissez un modèle personnalisé, les paramètres qui définissent les files d'attente sont configurables ; sinon, ils ont des valeurs prédéfinies appropriées à votre sélection. Les quatre files d'attente sont :

- **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 (en fonction des ressources)** : file d'attente de priorité moyenne, 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 priorité la plus faible, débit élevé. 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 3 Définissez les paramètres EDCA de station suivants :

REMARQUE : Ces paramètres ne peuvent être définis que si vous avez sélectionné Personnalisés à l'étape précédente.

- **Espace intertrame d'arbitrage** : 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 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 Fenêtre de contention maximale.

  Les valeurs valides sont 1, 3, 7, 15, 31, 63, 127, 255, 511 ou 1023. La valeur spécifiée doit être inférieure à celle du champ Fenêtre de contention maximale.
- **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 Fenêtre de contention maximale soit atteinte.

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

Les valeurs valides sont 1, 3, 7, 15, 31, 63, 127, 255, 511 ou 1023. La valeur spécifiée doit être supérieure à celle du champ Fenêtre de contention minimale.

- **Rafale maximale** (WAP uniquement) : paramètre EDCA WAP qui s'applique uniquement au trafic ente le WAP et la station cliente.

  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.

- **WMM (Wi-Fi Multimedia)** : sélectionnez **Activer** pour activer les extensions WMM (Wi-Fi Multimedia). 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 le point d'accès contrôlent le trafic descendant depuis le périphérique WAP vers la station cliente (paramètres EDCA du point d'accès) ainsi que le trafic montant depuis la station vers le point d'accès (paramètres EDCA de la station).

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

- **Limite TXOP** (station uniquement) : la limite TXOP est un paramètre EDCA de station. Il s'applique uniquement au trafic transmis de la station cliente vers le périphérique WAP. L'opportunité de transmission (Transmission Opportunity, TXOP) est l'intervalle en millisecondes pendant lequel une station cliente WME est autorisée à initier des transmissions sur le support sans fil (WM) vers le périphérique WAP. La valeur maximale du paramètre Limite TXOP est 65 535.

ÉTAPE 4 Définissez les paramètres supplémentaires suivants :

- **Aucune validation** : sélectionnez **Activer** pour spécifier que le périphérique WAP ne doit pas accepter les trames ayant la valeur de classe de service QosNoAck.

- **Économie d'énergie automatique non programmée** : sélectionnez **Activer** pour activer APSD, qui est une méthode de gestion de l'alimentation. APSD est recommandée si les téléphones VoIP accèdent au réseau via le périphérique WAP.

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

AVERTISSEMENT Une fois les nouveaux paramètres enregistrés, les processus correspondants peuvent être arrêtés et redémarrés. Toutefois, dans ce cas, il se peut que le périphérique WAP perde sa connectivité. Nous vous recommandons de modifier les paramètres du périphérique WAP lorsqu'une perte de connectivité peut affecter vos clients sans fil.

6

Analyseur de spectre

Cette section décrit la fonction d'analyseur de spectre du point d'accès.

Analyseur de spectre

Cette fonction assure une surveillance complète de l'environnement de radiofréquence (RF) pour une gestion en temps réel du réseau sans fil. Grâce à elle, l'administrateur du réseau sans fil peut consulter des informations en temps réel et l'historique des données relatives à l'environnement RF.

L'analyseur de spectre analyse l'ensemble des canaux IEEE 802.11 dans les bandes de fréquences 2,4 et 5 GHz à la recherche d'interférences non-Wi-Fi. Il classe ensuite les interférences et les consigne dans des journaux d'événements locaux à la périphérie du réseau.

REMARQUE : L'analyseur de spectre enregistre les interférences suivantes : téléphone sans fil analogique, caméra sans fil, four à micro-ondes, détecteur de mouvement à bande S, brouilleur à bande étroite et à large bande, et brouilleur inconnu.

La page Analyseur de spectre indique l'état de cette fonction et propose un lien permettant d'afficher les données du spectre.

Configuration de l'analyseur de spectre

Pour configurer l'analyseur de spectre :

ÉTAPE 1 Sélectionnez **Analyseur de spectre** dans le panneau de navigation.

ÉTAPE 2 L'état du mode d'analyse de spectre. Cet état est défini sur Analyseur de spectre dédié, Analyseur de spectre hybride ou Désactiver. La valeur par défaut est Désactiver. L'analyseur de spectre prend en charge une seule radio en même temps.

REMARQUE En mode dédié, la radio est utilisée pour l'analyse de spectre pendant plus de 10% du temps et les connexions client peuvent fonctionner, sans toutefois aucune garantie. En mode hybride, les connexions client sont garanties, mais cela risque de ralentir le débit.

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

ÉTAPE 4 Appuyez sur le bouton **Afficher les données de spectre** pour lancer le visualiseur de spectre lorsque le mode d'analyse est défini sur Analyseur de spectre dédié ou sur Analyseur de spectre hybride.

REMARQUE : Vous ne pouvez y accéder que via une adresse IPv4.

7

Sécurité du système

Cette section explique comment configurer les paramètres de sécurité sur le point d'accès.

Elle contient les sections suivantes :

- **Serveur RADIUS**
- **Demandeur 802.1X**
- **Complexité des mots de passe**
- **Complexité WPA-PSK**

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 le point d'accès, vous pouvez définir les méthodes de sécurité qui contrôlent l'accès des clients sans fil (voir la page **Radio**). Les méthodes de sécurité WEP dynamique et WPA Entreprise utilisent 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.

Vous pouvez utiliser 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. Toutefois, vous devez 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 les autres font office de serveurs de sauvegarde.

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. Reportez-vous à la page **Réseaux**.

Pour configurer des serveurs RADIUS globaux :

ÉTAPE 1 Sélectionnez **Sécurité du système** > **Serveur Radius** dans le volet de navigation.

ÉTAPE 2 Configurez les paramètres suivants :

- **Type d'adresse IP du serveur** : version IP utilisée par le serveur RADIUS.

  Vous pouvez basculer entre les types d'adresses pour configurer les paramètres d'adresse RADIUS globale IPv4 et IPv6, mais notez que le périphérique WAP ne contacte que le ou les serveurs RADIUS correspondant au type d'adresse sélectionné dans ce champ.

- **Adresse IP du serveur 1** ou **Adresse IPv6 du serveur 1** : adresses du serveur RADIUS global principal.

  Lorsque le premier client sans fil tente de s'authentifier à l'aide du périphérique WAP, le périphérique envoie une demande d'authentification au serveur principal. Si le serveur principal répond à la demande d'authentification, le périphérique 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** à **4)** ou **Adresse IPv6 du serveur (2** à **4)** : jusqu'à trois adresses de serveur RADIUS IPv4 ou IPv6 de sauvegarde.

  Si l'authentification auprès du serveur principal échoue, une tentative est effectuée sur chaque serveur de secours configuré.

- **Clé 1** : clé secrète partagée utilisée par le périphérique WAP pour s'authentifier au 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 entrez apparaît sous la forme d'astérisques.

- **Clé (2** à **4)** : clé RADIUS associée aux serveurs RADIUS de sauvegarde configurés. Le serveur spécifié dans le champ **Adresse IP (IPv6) du serveur 2** utilise **Clé 2** ; le serveur spécifié dans le champ **Adresse IP (IPv6) du serveur 3** utilise **Clé 3**, etc.

- **Activer la gestion de comptes RADIUS** : active 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 au point d'accès d'atteindre un réseau filaire sécurisé. Vous pouvez activer le point d'accès 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 cryptés à l'aide de l'algorithme MD5 afin d'autoriser le point d'accès 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 le périphérique WAP, de telle sorte qu'il puisse les transmettre à l'authentificateur.

La page Demandeur 802.1X est divisée en trois zones : Configuration du demandeur, Statut du fichier de certificats et Chargement du fichier de certificats.

La zone Configuration du demandeur permet de configurer l'état opérationnel et les paramètres de base de 802.1X.

Pour configurer le demandeur 802.1X :

ÉTAPE 1 Sélectionnez **Sécurité du système** > **Demandeur 802.1X** dans le volet de navigation.

ÉTAPE 2 Cliquez sur **Actualiser** pour mettre à jour l'état du fichier de certificat.

ÉTAPE 3 Configurez les paramètres suivants :

- **Mode d'administration** : active la fonctionnalité de demandeur 802.1X.

- **Méthode EAP** : algorithme à utiliser pour le cryptage des noms d'utilisateur et des mots de passe utilisés lors de l'authentification.
  - **MD5** : fonction de hachage définie dans la norme RFC 3748 et offrant une sécurité de base.
  - **PEAP** : protocole (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, telle que définie dans la norme RFC 5216, à savoir une norme ouverte offrant un haut niveau de sécurité.
- **Nom d'utilisateur** : le périphérique WAP utilise ce nom d'utilisateur lorsqu'il répond à des demandes émanant d'un authentificateur 802.1X. Le nom d'utilisateur peut comporter de 1 à 64 caractères. Les caractères imprimables ASCII sont autorisés, ce qui inclut les lettres majuscules et minuscules, les chiffres et tous les caractères spéciaux à l'exception des guillemets.
- **Mot de passe** : le périphérique WAP utilise ce mot de passe MD5 lorsqu'il répond à des demandes émanant d'un authentificateur 802.1X. La longueur du mot de passe peut être de 1 à 64 caractères. Les caractères imprimables ASCII sont autorisés, ce qui inclut les lettres majuscules et minuscules, les chiffres et tous les caractères spéciaux à l'exception des guillemets.

REMARQUE : En mode EAP-TLS, le périphérique WAP utilise cette identité lorsqu'il répond à des demandes émanant d'un authentificateur 802.1X. Le périphérique WAP prend en charge les fichiers de certificats au format PEM. Le fichier de certificat doit englober une clé privée et des certificats racines. Le périphérique WAP s'attend à ce que ce fichier de certificat soit protégé par un mot de passe. Le périphérique WAP utilise le mot de passe de la clé privée pour déverrouiller ce fichier de certificat.

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

REMARQUE : Une fois les nouveaux paramètres enregistrés, les processus correspondants peuvent être arrêtés et redémarrés. Toutefois, dans ce cas, il se peut que le périphérique WAP perde sa connectivité. Nous vous recommandons de modifier les paramètres du périphérique WAP lorsqu'une perte de connectivité peut affecter vos clients sans fil.

La zone Statut du fichier de certificats indique s'il existe un certificat actuel :

- **Fichier de certificat présent** : indique si le fichier de certificat SSL HTTP est présent. Ce champ contient la valeur Oui si ce fichier est présent. La valeur par défaut est Non.
- **Date d'expiration du certificat** : indique la date d'expiration du fichier de certificat SSL HTTP. La plage est une date valide.

La zone Chargement du fichier de certificats permet de charger un fichier de certificat sur le point d'accès :

ÉTAPE 1 Sélectionnez **HTTP** ou **TFTP** en guise de **Méthode de transfert**).

ÉTAPE 2 Si vous avez sélectionné HTTP, cliquer sur **Parcourir** pour sélectionner le fichier.

REMARQUE : Pour configurer les paramètres des serveurs HTTP et HTTPS, reportez-vous à **Service HTTP/HTTPS**.

Si vous avez sélectionné TFTP, complétez les champs **Nom de fichier** et **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 3 Cliquer sur **Charger**.

Une fenêtre de confirmation apparaît, suivie d'une barre de progression indiquant l'état du téléchargement.

Complexité des mots de passe

Vous pouvez configurer les exigences de complexité des mots de passe utilisés pour accéder à l'utilitaire de configuration du périphérique WAP. Des mots de passe complexes augmentent la sécurité.

Pour configurer les exigences de complexité des mots de passe :

ÉTAPE 1 Sélectionnez **Sécurité du système** > **Complexité des mots de passe** dans le volet de navigation.

ÉTAPE 2 Pour le paramètre **Complexité des mots de passe**, sélectionnez **Activer**.

ÉTAPE 3 Configurez les paramètres suivants :

- **Nombre minimal de classes de caractères dans le mot de passe** : nombre minimal de classes 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 d'entrer un autre mot de passe lorsque leur mot de passe actuel arrive à expiration. Si vous ne sélectionnez pas cette option, les utilisateurs peuvent entrer 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 80 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.

Complexité WPA-PSK

Lorsque vous configurez des points d'accès virtuels (VAP) sur le périphérique 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 pour tous les points d'accès virtuels (VAP), vous pouvez également utiliser la page Complexité WPA-PSK pour configurer les exigences de complexité de la clé utilisée dans le processus d'authentification. Des clés plus complexes offrent une sécurité accrue.

Pour configurer la complexité WPA-PSK :

ÉTAPE 1 Sélectionnez **Sécurité du système** > **Complexité WPA-PSK** dans le volet de navigation.

ÉTAPE 2 Cliquez sur **Activer** pour le paramètre **Complexité WPA-PSK** afin de permettre au périphérique WAP de contrôler les clés WPA-PSK en fonction des critères que vous configurez. Si vous désactivez cette case à cocher, aucun de ces paramètres ne sera utilisé. La complexité WPA-PSK est désactivée par défaut.

ÉTAPE 3 Configurez 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** : sélectionnez l'une des options suivantes :
  - **Activer** : les utilisateurs doivent configurer une autre clé lorsque leur clé actuelle arrive à expiration.
  - **Désactiver** : les utilisateurs peuvent continuer à utiliser leur ancienne clé ou leur clé précédente lorsque leur clé actuelle arrive à expiration.
- **Longueur WPA-PSK maximale** : la longueur maximale de la clé est comprise entre 32 et 63 caractères. La valeur par défaut est 63.
- **Minimum WPA-PSK Length** : la longueur minimale de la clé est comprise entre 8 et 16 caractères. La valeur par défaut est 8. Activez cette case à cocher pour rendre le champ modifiable et activer cette condition.

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

8

QoS des clients

Cette section offre un aperçu de la qualité de service (QoS) de client et explique les fonctionnalités QoS disponibles depuis le menu QoS des clients. Elle contient les sections suivantes :

- **Paramètres globaux**
- **Mappage de classe**
- **Mappage de stratégie**
- **Association de la QoS des clients**
- **Statut de la QoS des clients**

Paramètres globaux

Utilisez la page Paramètres globaux de la QoS des clients pour activer ou désactiver la fonctionnalité de qualité de service sur le périphérique WAP.

Si vous désactivez le mode **QoS client**, les limitations de débit et les configurations DiffServ seront désactivées de manière globale.

Si vous activez ce mode, vous pouvez également activer ou désactiver le mode QoS de client sur des points d'accès virtuels spécifiques ou Ethernet. Reportez-vous au paramètre **Mode QoS des clients** à la page **Association de la QoS des clients**.

Mappage de classe

La fonctionnalité QoS inclut la prise en charge de services différenciés (DiffServ) permettant la classification du trafic en flux et offrant un traitement QoS correspondant à des 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 contenant du trafic devant être transmis rapidement peuvent être affectées à des mappages de stratégie accordant la priorité par rapport aux autres types de trafic.

Utilisez la page Mappage de classe pour définir des classes de trafic. Utilisez la page **Mappage de stratégie** pour définir des stratégies et leur associer des mappages de classe.

Configuration des mappages de classe IPv4

Pour ajouter et configurer un mappage de classe IPv4 :

ÉTAPE 1 Sélectionnez **QoS des clients > Mappage de classe**.

ÉTAPE 2 Dans le champ Nom du mappage de classe, 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 3 Choisissez IPv4 comme type de mappage de classe dans la liste Type de mappage de classe. Le mappage de classe IPv4 s'applique uniquement au trafic IPv4 sur le périphérique WAP.

ÉTAPE 4 Dans la zone Configuration des critères de correspondance, configurez ces paramètres pour faire correspondre les paquets à une classe :

- **Nom du mappage de classe** : choisissez le mappage de classe IPv4 dans la liste.
- **Correspondre à tous les paquets** : la condition de correspondance est vraie pour l'ensemble des paramètres dans un paquet de couche 3. Si vous activez cette option, tous les paquets de couche 3 répondront à la condition.
- **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. Choisissez le protocole à mettre en correspondance par mot clé ou entrez un ID de protocole :
  - **Sélectionner dans la liste** : met en correspondance le protocole sélectionné : IP, ICMP, IGMP, TCP, UDP.
  - **Valeur correspondante** : met en correspondance un protocole dont le nom ne figure pas dans la liste. Entrez 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.
- **IP source** : nécessite que l'adresse IPv4 source d'un paquet corresponde à l'adresse IPv4 définie dans les champs appropriés.
  - **Adresse IP source** : entrez l'adresse IPv4 pour appliquer ce critère.
  - **Masque IP source** : entrez le masque 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 la ou les parties de l'adresse IP de destination à 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.

- **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.
  - **Sélectionner dans la liste** : met en correspondance un mot clé associé au port source : ftp, ftpdata, http, smtp, snmp, telnet, tftp ou www. Chacun de ces mots clés est traduit en son numéro de port équivalent.

- **Port correspondant** : 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 1 023 : ports connus

  1 024 à 49 151 : ports enregistrés

  49 152 à 65 535 : ports dynamiques et/ou privés

- **Masque** : masque du port. Le masque détermine quels bits sont utilisés et quels bits sont ignorés. Seul le chiffre hexadécimal (0-0xFFFF) est autorisé. 1 signifie que le bit est significatif et 0 indique qu'il peut être ignoré.

- **IP de destination** : nécessite que l'adresse IPv4 destination d'un paquet corresponde à l'adresse IPv4 définie dans les champs appropriés.
  - **Adresse IP de destination** : entrez l'adresse IPv4 pour appliquer ce critère.
  - **Masque IP de destination** : entrez le masque d'adresse IP de destination.
- **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.
  - **Sélectionner dans la liste** : met en correspondance le port de destination figurant dans l'en-tête de datagramme avec le mot clé sélectionné : ftp, ftpdata, http, smtp, snmp, telnet, tftp ou www. Chacun de ces mots clés est traduit en son numéro de port équivalent.
  - **Port correspondant** : met en correspondance le port de destination 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 1 023 : ports connus

    1 024 à 49 151 : ports enregistrés

    49 152 à 65 535 : ports dynamiques et/ou privés

- **Masque** : masque du port. Le masque détermine quels bits sont utilisés et quels bits sont ignorés. Seul le chiffre hexadécimal (0-0xFFFF) est autorisé. 1 signifie que le bit est significatif et 0 indique qu'il peut être ignoré.

▪ **Type de service** : spécifie le type de service à utiliser lors de la mise en correspondance des paquets avec les critères de classe.

- **Sélectionner la valeur IP DSCP dans la liste** : choisissez une valeur DSCP à utiliser en guise de critère de correspondance.
- **Valeur correspondante IP DSCP** : entrez une valeur DSCP personnalisée, comprise entre 0 et 63.
- **Priorité IP** : met en correspondance la valeur Priorité IP du paquet avec la valeur Priorité IP définie dans ce champ. La plage des valeurs Priorité IP va de 0 à 7.
- **Bits du type de service IP** : utilise les bits du type de service (ToS) du paquet dans l'en-tête IP en guise de critères de correspondance. Cette valeur est comprise entre 00 et FF. Les trois bits d'ordre haut représentent la valeur Priorité IP. Les six bits d'ordre haut représentent la valeur IP DSCP.
- **Masque du type de service IP** : entrez 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 5 Cliquez sur **Enregistrer**. Les modifications sont enregistrées dans la configuration de démarrage.

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

Configuration des mappages de classe IPv6

Pour ajouter et configurer un mappage de classe IPv6 :

ÉTAPE 1 Sélectionnez **QoS des clients > Mappage de classe**.

ÉTAPE 2 Dans le champ Nom du mappage de classe, 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 3 Choisissez IPv6 comme type de mappage de classe dans la liste Type de mappage de classe. Le mappage de classe IPv6 s'applique uniquement au trafic IPv6 sur le périphérique WAP.

ÉTAPE 4 Dans la zone Configuration des critères de correspondance, configurez ces paramètres pour faire correspondre les paquets à une classe :

- **Nom du mappage de classe** : choisissez le mappage de classe IPv6 dans la liste.
- **Correspondre à tous les paquets** : la condition de correspondance est vraie pour l'ensemble des paramètres dans un paquet de couche 3. Si vous activez cette option, tous les paquets de couche 3 répondront à la condition.
- **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. Choisissez le protocole à mettre en correspondance par mot clé ou entrez un ID de protocole :
  - **Sélectionner dans la liste** : met en correspondance le protocole sélectionné : IPv6, ICMPv6, TCP ou UDP.
  - **Valeur correspondante** : met en correspondance un protocole dont le nom ne figure pas dans la liste. Entrez 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.
- **IPv6 source** : nécessite que l'adresse IPv6 source d'un paquet corresponde à l'adresse IPv6 définie dans les champs appropriés.
  - **Adresse IPv6 source** : entrez l'adresse IPv6 pour appliquer ce critère.

- **Longueur du préfixe IPv6 source** : entrez la longueur de préfixe de l'adresse IPv6 source.

- **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.
  - **Sélectionner dans la liste** : met en correspondance un mot clé associé au port source : ftp, ftpdata, http, smtp, snmp, telnet, tftp ou www. Chacun de ces mots clés est traduit en son numéro de port équivalent.
  - **Port correspondant** : 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 1 023 : ports connus

    1 024 à 49 151 : ports enregistrés

    49 152 à 65 535 : ports dynamiques et/ou privés
  - **Masque** : masque du port. Le masque détermine quels bits sont utilisés et quels bits sont ignorés. Seul un chiffre hexadécimal (0 à 0xFFFF) est autorisé. 1 signifie que le bit est significatif et 0 indique qu'il peut être ignoré.

- **IPv6 de destination** : nécessite que l'adresse IPv6 destination d'un paquet corresponde à l'adresse IPv6 définie dans les champs appropriés.
  - **Adresse IPv6 de destination** : entrez l'adresse IPv6 pour appliquer ce critère.
  - **Longueur du préfixe IPv6 de destination** : entrez la longueur de préfixe de l'adresse IPv6 de destination.

- **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.
  - **Sélectionner dans la liste** : met en correspondance le port de destination figurant dans l'en-tête de datagramme avec le mot clé sélectionné : ftp, ftpdata, http, smtp, snmp, telnet, tftp ou www. Chacun de ces mots clés est traduit en son numéro de port équivalent.
  - **Port correspondant** : met en correspondance le port de destination 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 1 023 : ports connus

1 024 à 49 151 : ports enregistrés

49 152 à 65 535 : ports dynamiques et/ou privés

- **Masque** : masque du port. Le masque détermine quels bits sont utilisés et quels bits sont ignorés. Seul un chiffre hexadécimal (0 à 0xFFFF) est autorisé. 1 signifie que le bit est significatif et 0 indique qu'il peut être ignoré.

- **Étiquette du flux IPv6** : entrez un nombre de 20 bits unique pour un paquet IPv6. Ce nombre est utilisé par les postes finaux pour indiquer la gestion de la QoS dans les routeurs (plage de 0 à 1048575).
- **IP DSCP** : utilise la valeur DSCP comme critère de correspondance.
  - **Sélectionner dans la liste** : choisissez le type DSCP dans la liste.
  - **Valeur correspondante** : entrez une valeur DSCP personnalisée, comprise entre 0 et 63.

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

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

Configuration des mappages de classe MAC

Pour configurer un mappage de classe MAC :

ÉTAPE 1 Sélectionnez **QoS des clients** > **Mappage de classe**.

ÉTAPE 2 Dans le champ Nom du mappage de classe, 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 3 Choisissez MAC comme type de mappage de classe dans la liste Type de mappage de classe. Le mappage de classe MAC s'applique aux critères de couche 2.

ÉTAPE 4 Dans la zone Configuration des critères de correspondance, configurez ces paramètres pour faire correspondre les paquets à une classe :

- **Nom du mappage de classe** : choisissez le mappage de classe MAC dans la liste.
- **Correspondre à tous les paquets** : si vous activez cette option, tous les paquets de couche 2 répondront à la condition.
- **Type Ethernet** : compare les critères de correspondance avec la valeur figurant dans l'en-tête d'une trame Ethernet. Choisissez un mot clé Type Ethernet ou entrez une valeur Type Ethernet pour spécifier les critères de correspondance :
  - **Sélectionner dans la liste** : met en correspondance la valeur Type Ethernet figurant dans l'en-tête de datagramme avec les types de protocole sélectionnés : appletalk, arp, ipv4, ipv6, ipx, netbios ou pppoe.
  - **Valeur correspondante** : met en correspondance la valeur Type Ethernet 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.
- **Classe de service** : spécifie la valeur de priorité utilisateur 802.1p de classe de service à mettre en correspondance pour les paquets. La valeur doit être comprise entre 0 et 7.
- **MAC source** : inclut une adresse MAC source dans la condition de correspondance de la règle.
  - **Adresse MAC source** : entrez l'adresse MAC source à comparer à une trame Ethernet.
  - **Masque MAC source** : entrez 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 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** : inclut une adresse MAC de destination dans la condition de correspondance de la règle.
  - **Adresse MAC de destination** : entrez l'adresse MAC de destination à comparer à une trame Ethernet.
  - **Masque MAC de destination** : entrez 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 spécifié à mettre en correspondance pour les paquets. L'ID de VLAN doit être compris entre 0 et 4095.

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

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

Mappage de stratégie

Les paquets sont classifiés et traités sur la base des critères définis. Les critères de classification sont définis par l'intermédiaire d'une classe à la page **Mappage de classe**. Le traitement est défini par les attributs d'une stratégie à la page Mappage de stratégie. 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.

Le périphérique WAP peut prendre en charge un maximum de 50 mappages de stratégie. Un mappage de stratégie peut contenir jusqu'à 10 mappages de classe.

Ajout et configuration d'un mappage de stratégie

Pour ajouter et configurer un mappage de stratégie :

ÉTAPE 1 Sélectionnez **QoS des clients** > **Mappage de stratégie**.

ÉTAPE 2 Dans le champ Nom du mappage de stratégie, saisissez le nom du mappage de stratégie. Le nom peut comporter de 1 à 31 caractères alphanumériques et caractères spéciaux. Les espaces ne sont pas autorisés.

ÉTAPE 3 Cliquez sur **Ajouter un mappage de stratégie**.

ÉTAPE 4 Dans la zone Définition de la classe de stratégies, configurez ces paramètres pour le mappage de stratégie :

- **Nom du mappage de stratégie** : choisissez le mappage de stratégie à configurer.
- **Nom du mappage de classe** : choisissez le mappage de classe à appliquer à cette stratégie.
- **Police Simple** : établit le style de réglementation du trafic de la classe. La forme simple du style de réglementation utilise un seul débit de données et une seule taille de rafale, d'où deux résultats possibles : conforme et non conforme.

  Si vous activez cette fonctionnalité, configurez l'un des champs suivants :

  - **Débit engagé** : débit garanti, 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. Cette valeur est comprise entre 1 et 204 800 000 octets.
- **Envoyer** : spécifie que tous les paquets du flux de trafic associé doivent être transférés si les critères de mappage de classe sont satisfaits.
- **Abandonner** : spécifie que tous les paquets du flux de trafic associé doivent être abandonnés si les critères de mappage de classe sont satisfaits.
- **Marquer la classe de service** : 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.
- **Marquer la valeur IP DSCP** : marque tous les paquets du flux de trafic associé avec la valeur IP DSCP que vous sélectionnez dans la liste.

- **Sélectionner dans la liste** : liste des types DSCP.

- **Marquer 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.
- **Dissocier le mappage de classe** : supprime la classe sélectionnée dans la liste Nom du mappage de classe de la stratégie sélectionnée dans la liste Nom du mappage de stratégie.
- **Classes membres** : répertorie toutes les classes DiffServ actuellement définies en tant que membres de la stratégie sélectionnée. Ce champ est vide si aucune classe n'est associée à la stratégie.

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

REMARQUE : Pour supprimer un mappage de stratégie, sélectionnez-le dans la liste Nom du mappage de stratégie et cliquez sur Supprimer.

REMARQUE : Vous ne pouvez supprimer un mappage de stratégie que s'il n'est associé à aucun point d'accès virtuel.

REMARQUE : Les paramètres de marquage de stratégie tels que Marquer la classe de service, Marquer la valeur IP DSCP et Marquer la priorité IP ne sont pas pris en charge pour le mappage de classe IPv6.

Association de la QoS des clients

La page Association de la QoS offre un contrôle supplémentaire de certains aspects de la qualité de service des interfaces sans fil et Ethernet. En outre, elle permet de contrôler la quantité de bande passante qu'un client individuel est autorisé à envoyer et à recevoir.

En plus de contrôler les catégories générales de trafic, la QoS vous permet de configurer le conditionnement par client de divers micro-flux par le biais de services différenciés (DiffServ, Differentiated Services). Les stratégies DiffServ sont 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.

Configuration des paramètres d'association de la QoS

Pour configurer les paramètres d'association de la QoS :

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

ÉTAPE 2 Dans le champ Interface, choisissez l'interface radio ou Ethernet sur laquelle vous voulez configurer les paramètres QoS.

ÉTAPE 3 Sélectionnez **Activée** pour **l'interface sélectionnée**.

ÉTAPE 4 Configurez les paramètres suivants pour l'interface sélectionnée :

- **Limite de bande passante en aval** : saisissez la vitesse de transmission maximale autorisée depuis le périphérique WAP vers le client en bits par seconde (bit/s). La plage valide va de 0 à 1300 Mbit/s.
- **Limite de bande passante en amont** : vitesse de transmission maximale autorisée depuis le client vers le périphérique WAP en bits par seconde (bit/s). La plage valide va de 0 à 1300 Mbit/s.
- **Stratégie DiffServ** : choisissez une stratégie DiffServ appliquée au trafic envoyé au périphérique WAP pour l'interface sélectionnée.

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

Statut de la QoS des clients

La page Statut de la QoS des clients indique les détails des mappages de stratégie et de classe, notamment le mappage de classe présent dans un mappage de stratégie et les interfaces liées à ce mappage de stratégie.

Les tables IPv4 QoS, IPv6 QoS et MAC QoS indiquent les informations des mappages de classe définis dans la page Mappage de classe, notamment :

- **Classe membre** : nom du mappage de classe.
- **Rechercher tout** : indique si ce mappage correspond à tous les paquets.

Champ de la règle : affiche la définition détaillée de ce mappage de classe. Pour plus d'informations, reportez-vous à la section **Mappage de classe**.

La table Mappage de stratégie indique les informations des mappages de stratégie définies dans la page Mappage de stratégie, notamment :

- **Nom du mappage de stratégie** : nom du mappage de stratégie.
- **Liaison de l'interface** affiche l'interface associée à ce mappage de stratégie.
- **Nom du mappage de classe** : répertorie les mappages de classe contenus par cette stratégie.

Stratégie : affiche les détails de stratégie de ce mappage de classe. Pour plus d'informations, reportez-vous à la section **Mappage de stratégie**.

Vous pouvez cliquer sur **Actualiser** pour actualiser l'écran et afficher les informations les plus récentes.

9

ACL

Cette section explique comment configurer la fonction ACL sur le périphérique WAP. Elle contient les sections suivantes :

- **Règle ACL**
- **Association d'ACL**
- **Statut ACL**

Règle ACL

Une ACL ou liste de contrôle d'accès est un ensemble de conditions d'autorisation et de refus, appelées règles, qui offrent une protection 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.

Le périphérique WAP peut prendre en charge jusqu'à 50 règles ACL IPv4, IPv6 et MAC.

ACL IPv4 et IPv6

Les ACL IP classent le trafic selon les couches 3 et 4.

Chaque ACL est un ensemble de règles qui s'appliquent au trafic reçu par le périphérique 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.

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 du périphérique WAP, le périphérique WAP l'inspecte 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 page Règle ACL pour configurer les ACL et leurs règles, puis appliquer ces dernières à une interface particulière.

Configuration des ACL

Pour configurer des ACL :

ÉTAPE 1 Sélectionnez **ACL > Règle ACL**.

ÉTAPE 2 Spécifiez le nom de l'ACL.

ÉTAPE 3 Sélectionnez le type d'ACL à ajouter.

ÉTAPE 4 Ajoutez l'ACL.

ÉTAPE 5 Ajoutez de nouvelles règles à l'ACL.

ÉTAPE 6 Configurez les critères de correspondance des règles.

ÉTAPE 7 Utilisez la page Association d'ACL pour appliquer l'ACL à une ou plusieurs interfaces.

Configuration des ACL IPv4

Pour configurer une ACL IPv4 :

ÉTAPE 1 Sélectionnez **ACL > Règle ACL**.

ÉTAPE 2 Dans le champ Nom de l'ACL, saisissez le nom identifiant l'ACL. Le nom peut comporter de 1 à 31 caractères alphanumériques et caractères spéciaux. Les espaces ne sont pas autorisés.

ÉTAPE 3 Dans la liste Type d'ACL, choisissez IPv4. Les ACL IPv4 et IPv6 contrôlent l'accès aux ressources réseau sur la base des critères des couches 3 et 4.

ÉTAPE 4 Cliquez sur Ajouter une ACL.

ÉTAPE 5 Dans la zone Configuration de la règle ACL, définissez les paramètres de règle ACL suivants :

- **Nom de l'ACL - Type d'ACL** : sélectionnez l'ACL à configurer avec la nouvelle règle.
- **Règle** : sélectionnez Nouvelle règle pour configurer une nouvelle règle pour l'ACL sélectionnée. Lorsqu'une ACL possède plusieurs règles, celles-ci sont appliquées au paquet ou à la trame dans l'ordre selon lequel vous les avez ajoutées à l'ACL. La règle finale est une instruction implicite de refus de tout trafic.
- **Action** : indiquez si la règle ACL autorise ou refuse une action.
- Lorsque vous sélectionnez Autoriser, la règle permet à tout le trafic répondant à ses critères d'entrer dans le périphérique WAP. Le trafic qui ne satisfait pas aux critères est abandonné.
- Lorsque vous sélectionnez Refuser, la règle empêche tout le trafic qui ne répond pas à ses critères d'entrer dans le périphérique 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.
- **Correspondre à tous les paquets** : si cette option est activée, la règle, qui possède une action d'autorisation ou de refus, met en correspondance la trame ou le paquet, quel que soit son contenu. Si vous sélectionnez cette fonction, vous ne pouvez configurer aucun critère de correspondance supplémentaire. Cette option est sélectionnée par défaut pour chaque nouvelle règle. Vous devez désactiver l'option pour configurer d'autres champs de correspondance.
- **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. Vous pouvez choisir l'une de ces options ou sélectionner Tout :
  - **Sélectionner dans la liste** : sélectionnez l'un des protocoles suivants : IP, ICMP, IGMP, TCP ou UDP.
  - **Valeur correspondante** : entrez un ID de protocole standard affecté par l'IANA, compris entre 0 et 255. Choisissez cette méthode pour identifier un protocole dont le nom ne figure pas dans le champ Sélectionner dans la liste.

- **IP source** : nécessite que l'adresse IP source d'un paquet corresponde à l'adresse définie dans les champs appropriés.
  - **Adresse IP source** : saisissez l'adresse IP pour appliquer ces critères.
  - **Masque générique** : saisissez le masque générique de l'adresse IP source. Le masque générique détermine quels bits sont utilisés et quels bits sont ignorés. Un masque générique égal à 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 vérification 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 source** : inclut un port source dans la condition de correspondance de la règle. Le port source est identifié dans l'en-tête de datagramme.
  - **Sélectionner dans la liste** : sélectionnez le mot clé associé au port source à mettre en correspondance : ftp, ftpdata, http, smtp, snmp, telnet, tftp ou www. Chacun de ces mots clés est traduit en son numéro de port équivalent.
  - **Port correspondant** : 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 1 023 : ports connus

    1 024 à 49 151 : ports enregistrés

    49 152 à 65 535 : ports dynamiques et/ou privés
  - **Masque** : entrez le masque du port. Le masque détermine quels bits sont utilisés et quels bits sont ignorés. Seul le chiffre hexadécimal (0-0xFFFF) est autorisé. 0 signifie que le bit est significatif et 1 indique qu'il peut être ignoré.

- **IP de destination** : nécessite que l'adresse IP de destination d'un paquet corresponde à l'adresse définie dans les champs appropriés.
  - **Adresse IP de destination** : saisissez une adresse IP pour appliquer ces critères.

    Masque générique : saisissez le masque générique de l'adresse IP destination. Le masque générique détermine quels bits sont utilisés et quels bits sont ignorés. Un masque générique égal à 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.
  - **Sélectionner dans la liste** : sélectionnez le mot clé associé au port destination à mettre en correspondance : ftp, ftpdata, http, smtp, snmp, telnet, tftp ou www. Chacun de ces mots clés est traduit en son numéro de port équivalent.
  - **Port correspondant** : saisissez le numéro de port IANA à mettre en correspondance avec le port 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 1 023 : ports connus

    1 024 à 49 151 : ports enregistrés

    49 152 à 65 535 : ports dynamiques et/ou privés
  - **Masque** : entrez le masque du port. Le masque détermine quels bits sont utilisés et quels bits sont ignorés. Seul le chiffre hexadécimal (0-0xFFFF) est autorisé. 0 signifie que le bit est pris en compte, 1 signifie que ce bit doit être ignoré.

- **Type de service** : met en correspondance les paquets selon un type de service spécifique.
  - **Sélectionner la valeur IP DSCP dans la liste** : met en correspondance les paquets selon les valeurs transfert DSCP (AF), classe de service (CS) ou acheminement attendu (EF).
  - **Valeur correspondante IP DSCP** : met en correspondance les paquets selon une valeur DSCP personnalisée. Si vous sélectionnez cette option, saisissez une valeur comprise entre 0 et 63 dans ce champ.
  - **Priorité IP** : met en correspondance les paquets selon leur valeur Priorité IP. Si vous sélectionnez cette option, entrez une valeur Priorité IP comprise entre 0 et 7.
  - **Bits du type de service IP** : spécifie une valeur relative à l'utilisation des bits du type de service du paquet dans l'en-tête IP en guise de critères de correspondance.

    Le champ Type de service IP dans un paquet est défini comme l'ensemble des huit bits de l'octet du type de service dans l'en-tête IP. La valeur Bits du type de service IP est un nombre hexadécimal à deux chiffres, compris entre 00 et ff. Les trois bits d'ordre haut représentent la valeur Priorité IP. Les six bits d'ordre haut représentent la valeur DSCP (Differentiated Services Code Point) IP.
  - **Masque du type de service IP** : entrez 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 6 Cliquez sur **Enregistrer**. Les modifications sont enregistrées dans la configuration de démarrage.

REMARQUE : Pour supprimer une ACL, assurez-vous qu'elle est sélectionnée dans la liste Nom de l'ACL - Type d'ACL, sélectionnez Supprimer l'ACL et cliquez sur Enregistrer.

Configuration des ACL IPv6

Pour configurer une ACL IPv6 :

ÉTAPE 1 Sélectionnez **ACL > Règle ACL**.

ÉTAPE 2 Dans le champ Nom de l'ACL, saisissez le nom identifiant l'ACL.

ÉTAPE 3 Dans la liste Type d'ACL, choisissez IPv6. Les ACL IPv6 contrôlent l'accès aux ressources réseau sur la base des critères des couches 3 et 4.

ÉTAPE 4 Cliquez sur Ajouter une ACL.

ÉTAPE 5 Dans la zone Configuration de la règle ACL, définissez les paramètres de règle ACL suivants :

- **Nom de l'ACL - Type d'ACL** : sélectionnez l'ACL à configurer avec la nouvelle règle.
- **Règle** : sélectionnez Nouvelle règle pour configurer une nouvelle règle pour l'ACL sélectionnée. Lorsqu'une ACL possède plusieurs règles, celles-ci sont appliquées au paquet ou à la trame dans l'ordre selon lequel vous les avez ajoutées à l'ACL. La règle finale est une instruction implicite de refus de tout trafic.
- **Action** : indiquez si la règle ACL autorise ou refuse une action.
- Lorsque vous sélectionnez Autoriser, la règle permet à tout le trafic répondant à ses critères d'entrer dans le périphérique WAP. Le trafic qui ne satisfait pas aux critères est abandonné.
- Lorsque vous sélectionnez Refuser, la règle empêche tout le trafic qui ne répond pas à ses critères d'entrer dans le périphérique 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.
- **Correspondre à tous les paquets** : si cette option est activée, la règle, qui possède une action d'autorisation ou de refus, met en correspondance la trame ou le paquet, quel que soit son contenu. Si vous sélectionnez cette fonction, vous ne pouvez configurer aucun critère de correspondance supplémentaire. Cette option est sélectionnée par défaut pour chaque nouvelle règle. Vous devez désactiver l'option pour configurer d'autres champs de correspondance.
- **Protocole** : sélectionnez le protocole à mettre en correspondance par mot clé ou ID de protocole.

- **IPv6 source** : nécessite que l'adresse IPv6 source d'un paquet corresponde à l'adresse IPv6 définie dans les champs appropriés.
  - **Adresse IPv6 source** : entrez l'adresse IPv6 pour appliquer ce critère.
  - **Longueur du préfixe IPv6 source** : entrez la longueur de préfixe de l'adresse IPv6 source.
- **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.
  - **Sélectionner dans la liste** : si vous sélectionnez cette option, choisissez le nom du port dans la liste.
  - **Port correspondant** : 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 1 023 : ports connus

    1 024 à 49 151 : ports enregistrés

    49 152 à 65 535 : ports dynamiques et/ou privés
  - **Masque** : entrez le masque du port. Le masque détermine quels bits sont utilisés et quels bits sont ignorés. Seul le chiffre hexadécimal (0-0xFFFF) est autorisé. 0 signifie que le bit est significatif et 1 indique qu'il peut être ignoré.
- **IPv6 de destination** : nécessite que l'adresse IPv6 destination d'un paquet corresponde à l'adresse IPv6 définie dans les champs appropriés.
  - **Adresse IPv6 de destination** : saisissez une adresse IPv6 pour appliquer ces critères.
  - **Longueur du préfixe IPv6 de destination** : entrez la longueur de préfixe de l'adresse IPv6 de destination.
- **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.
  - **Sélectionner dans la liste** : si vous sélectionnez cette option, choisissez le nom du port dans la liste.

- **Port correspondant** : 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 1 023 : ports connus

  1 024 à 49 151 : ports enregistrés

  49 152 à 65 535 : ports dynamiques et/ou privés

- **Masque** : entrez le masque du port. Le masque détermine quels bits sont utilisés et quels bits sont ignorés. Seul le chiffre hexadécimal (0-0xFFFF) est autorisé. 0 signifie que le bit est pris en compte, 1 signifie que ce bit doit être ignoré.

▪ **Étiquette du flux IPv6** : indique un nombre de 20 bits qui est propre à un paquet IPv6. Ce nombre est utilisé par les postes finaux pour indiquer la gestion de la QoS dans les routeurs (plage de 0 à 1048575).

▪ **IPv6 DSCP** : met en correspondance les paquets selon leur valeur IP DSCP. Si vous sélectionnez cette option, choisissez l'une des options suivantes en tant que critères de correspondance :

- **Sélectionner dans la liste** : sélectionnez l'une des valeurs suivantes : Transfert DSCP (AF), classe de service (CS) ou acheminement attendu (EF).

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

ÉTAPE 6 Cliquez sur **Enregistrer**. Les modifications sont enregistrées dans la configuration de démarrage.

REMARQUE : Pour supprimer une ACL, assurez-vous qu'elle est sélectionnée dans la liste Nom de l'ACL-Type d'ACL, sélectionnez Supprimer l'ACL et cliquez sur Enregistrer.

Configuration des ACL MAC

Pour configurer une ACL MAC :

ÉTAPE 1 Sélectionnez **ACL > Règle ACL**.

ÉTAPE 2 Dans le champ Nom de l'ACL, saisissez le nom identifiant l'ACL.

ÉTAPE 3 Dans la liste Type d'ACL, choisissez MAC. Les ACL MAC contrôlent l'accès aux ressources réseau sur la base des critères de la couche 2.

ÉTAPE 4 Cliquez sur Ajouter une ACL.

ÉTAPE 5 Dans la zone Configuration de la règle ACL, définissez les paramètres de règle ACL suivants :

- **Nom de l'ACL - Type d'ACL** : sélectionnez l'ACL à configurer avec la nouvelle règle.
- **Règle** : sélectionnez Nouvelle règle pour configurer une nouvelle règle pour l'ACL sélectionnée. Lorsqu'une ACL possède plusieurs règles, celles-ci sont appliquées au paquet ou à la trame dans l'ordre selon lequel vous les avez ajoutées à l'ACL. La règle finale est une instruction implicite de refus de tout trafic.
- **Action** : indiquez si la règle ACL autorise ou refuse une action.
- Lorsque vous sélectionnez Autoriser, la règle permet à tout le trafic répondant à ses critères d'entrer dans le périphérique WAP. Le trafic qui ne satisfait pas aux critères est abandonné.
- Lorsque vous sélectionnez Refuser, la règle empêche tout le trafic qui ne répond pas à ses critères d'entrer dans le périphérique 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.
- **Correspondre à tous les paquets** : si cette option est activée, la règle, qui possède une action d'autorisation ou de refus, met en correspondance la trame ou le paquet, quel que soit son contenu. Si vous sélectionnez cette fonction, vous ne pouvez configurer aucun critère de correspondance supplémentaire. Cette option est sélectionnée par défaut pour chaque nouvelle règle. Vous devez désactiver l'option pour configurer d'autres champs de correspondance.
- **Type Ethernet** : sélectionnez cette option pour comparer les critères de correspondance avec la valeur de trame Ethernet figurant dans l'en-tête. Vous pouvez sélectionner un mot clé Type Ethernet ou entrer une valeur Type Ethernet pour spécifier les critères de correspondance.
  - **Sélectionner dans la liste** : sélectionnez l'un des types de protocole suivants : appletalk, arp, ipv4, ipv6, ipx, netbios ou pppoe.
  - **Valeur correspondante** : entrez 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.

- **Classe de service** : entrez une priorité d'utilisateur 802.1p à comparer à une trame Ethernet. La plage valide va de 0 à 7. Ce champ se trouve dans la première et seule balise VLAN 802.1Q.
- **MAC source** : nécessite que l'adresse MAC source d'un paquet corresponde à l'adresse définie dans les champs appropriés.
  - **Adresse MAC source** : entrez l'adresse MAC source à comparer à une trame Ethernet.
  - **Masque MAC source** : entrez 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 égale à 0 indique que le bit d'adresse correspondant est significatif et une valeur égale à 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.
- **MAC de destination** : nécessite que l'adresse MAC destination d'un paquet corresponde à l'adresse définie dans les champs appropriés.
  - **Adresse MAC de destination** : entrez l'adresse MAC de destination à comparer à une trame Ethernet.
  - **Masque MAC de destination** : entrez 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** : entrez l'ID de VLAN spécifique à comparer à une trame Ethernet.

  Ce champ se trouve dans la première et seule balise VLAN 802.1Q.

ÉTAPE 6 Cliquez sur **Enregistrer**. Les modifications sont enregistrées dans la configuration de démarrage.

REMARQUE : Pour supprimer une ACL, assurez-vous qu'elle est sélectionnée dans la liste Nom de l'ACL-Type d'ACL, sélectionnez Supprimer l'ACL et cliquez sur Enregistrer.

Association d'ACL

La page ACL Association fournit la liste d'ACL liée aux interfaces sans fil et Ethernet. Vous pouvez configurer des listes de contrôle d'accès (ACL) et les affecter à une ou plusieurs interfaces afin de contrôler des catégories générales de trafic, comme le trafic HTTP ou le trafic issu d'un sous-réseau spécifique.

Pour associer une ACL à une interface :

ÉTAPE 1 Sélectionnez **ACL > Association d'ACL**.

ÉTAPE 2 Dans le champ Interface, cliquez sur l'interface radio ou Ethernet dans laquelle vous souhaitez configurer les paramètres ACL.

ÉTAPE 3 Configurez les paramètres suivants pour l'interface sélectionnée :

- **Type d'ACL** : sélectionnez le type d'ACL appliqué au trafic entrant dans le périphérique WAP, parmi les valeurs ci-dessous :
  - **IPv4** : examine les paquets IPv4 qui correspondent aux règles ACL.
  - **IPv4** : examine les paquets IPv6 qui correspondent aux règles ACL.
  - **MAC** : examine les trames de couche 2 qui correspondent aux règles ACL.
  - **Aucun** : n'examine pas le trafic entrant dans le périphérique WAP.
- **Nom de l'ACL** : sélectionnez le nom de l'ACL appliquée au trafic entrant dans le périphérique WAP.

  Lors de la réception d'un paquet ou d'une trame par le périphérique WAP, une correspondance avec les règles ACL est vérifiée. Le paquet ou la trame est traité s'il est autorisé, ou abandonné s'il est refusé.

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

Statut ACL

La page Statut ACL affiche des informations détaillées pour les différents types de règles ACL.

Pour afficher l'état ACL, sélectionnez ACL > Statut ACL.

Les informations suivantes sont indiquées :

- **Nom de l'ACL** : nom de l'ACL.
- **Liaison de l'interface** : interface à laquelle l'ACL a été associée.
- **Numéro de la règle** : numéro de la règle que l'ACL contient.
- **Action** : action à prendre par l'ACL.
- **Rechercher tout** : indique si la règle ACL correspond on non à tous les paquets.

Champ de la règle : affiche les paramètres détaillés de l'ACL. Pour plus d'informations, reportez-vous à la section **Règle ACL**.

Vous pouvez cliquer sur **Actualiser** pour actualiser l'écran et afficher les informations les plus récentes.

10

SNMP

Cette section explique comment configurer le protocole SNMP (Protocole de gestion de réseau simple) en vue d'effectuer des tâches de configuration et de collecte de statistiques.

Elle contient les sections suivantes :

- **Général**
- **Vues**
- **Groupes**
- **Utilisateurs**
- **Cibles**

Général

Utilisez la page Général pour activer SNMP et configurer les paramètres de base de ce protocole.

Pour configurer les paramètres SNMP généraux :

ÉTAPE 1 Sélectionnez **SNMP** > **Général** dans le volet de navigation.

ÉTAPE 2 Sélectionnez **Activé** pour le paramètre **SNMP**. SNMP est désactivé par défaut.

ÉTAPE 3 Spécifiez un **Port UDP** pour le trafic SNMP.

Par défaut, un agent SNMP n'écoute que les demandes qui émanent du port 161. Toutefois, vous pouvez configurer le protocole de telle sorte que l'agent écoute les demandes issues d'un autre port. La valeur doit être comprise entre 1025 et 65535.

ÉTAPE 4 Configurez les paramètres SNMPv2 :

- **Communauté en lecture seule** : 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'ordinateurs 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** : 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 acceptés.

- **Poste de gestion** : détermine quelles stations peuvent accéder au périphérique WAP par le biais du protocole SNMP. Sélectionnez l'une des options suivantes :

  - **Tout** : l'ensemble des stations pouvant accéder au périphérique WAP par le biais du protocole SNMP n'est pas limité.
  - **Défini par l'utilisateur** : l'ensemble des demandes SNMP autorisées est limité aux demandes spécifiées.

- **Nom/adresse IPv4 du système de gestion de réseau** : adresse IP IPv4, nom d'hôte DNS ou sous-réseau du système de gestion de réseau (NMS), ou ensemble d'ordinateurs pouvant exécuter des demandes d'obtention et de configuration vers les périphériques gérés.

  Un nom d'hôte DNS peut se composer d'une ou plusieurs étiquettes, elles-mêmes constituées d'un maximum de 63 caractères alphanumériques. Si un nom d'hôte inclut plusieurs étiquettes, elles sont séparées par un point (.). La série entière d'étiquettes et de points peut comporter 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, entrez une ou plusieurs plages d'adresses de sous-réseau sous la forme *adresse/longueur_masque* où *adresse* est une adresse IP et *longueur_masque* est le nombre de bits du masque. Les deux

formats *adresse/masque* et *adresse/longueur_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.

La plage d'adresses est utilisée pour spécifier le sous-réseau du système de gestion de réseau (NMS) désigné. Seuls les ordinateurs dont les adresses IP sont incluses dans cette plage sont autorisés à exécuter, obtenir et définir des demandes sur le périphérique géré. Dans l'exemple ci-dessus, les ordinateurs dont les adresses sont comprises entre 192.168.1.1 et 192.168.1.254 peuvent exécuter des commandes SNMP sur le périphérique. (L'adresse identifiée par le suffixe .0 dans une plage de sous-réseau est toujours réservée à l'adresse de sous-réseau, tandis que l'adresse identifiée par .255 dans la plage est toujours réservée à l'adresse de diffusion.)

Autre exemple : si vous entrez la plage 10.10.1.128/25, les ordinateurs dont les adresses IP sont comprises entre 10.10.1.129 et 10.10.1.254 peuvent exécuter des demandes SNMP sur les périphériques gérés. Dans cet exemple, 10.10.1.128 est l'adresse réseau et 10.10.1.255 est l'adresse de diffusion. Un total de 126 adresses seront dans ce cas désignées.

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

  Un nom d'hôte peut se composer d'une ou plusieurs étiquettes, elles-mêmes constituées d'un maximum de 63 caractères alphanumériques. Si un nom d'hôte inclut plusieurs étiquettes, elles sont séparées par un point (.). La série entière d'étiquettes et de points peut comporter jusqu'à 253 caractères.

ÉTAPE 5 Configurez les paramètres de déroutement SNMPv2 suivants :

- **Communauté de filtre** : chaîne de communauté globale associée aux déroutements SNMP. Les déroutements envoyés à partir du périphérique 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** : liste de trois adresses IP ou noms d'hôtes au maximum pouvant recevoir des déroutements SNMP. Activez la case à cocher 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 déroutementssnmp.foo.com. Les déroutements SNMP étant envoyés de manière aléatoire à partir de l'agent SNMP, il est logique de spécifier à quel emplacement exact les déroutements doivent être envoyés. Le nombre maximal de noms d'hôte DNS est égal à trois. Vérifiez que vous avez activé la case à cocher **Activé** et sélectionnez le **Type d'adresse IP hôte** approprié.

Consultez également la remarque relative aux noms d'hôte dans l'étape précédente.

ÉTAPE 6 Cliquez sur **Enregistrer**. Les modifications sont enregistrées dans la configuration de démarrage.

REMARQUE : Une fois les nouveaux paramètres enregistrés, les processus correspondants peuvent être arrêtés et redémarrés. Toutefois, dans ce cas, il se peut que le périphérique WAP perde sa connectivité. Nous vous recommandons de modifier les paramètres du périphérique WAP lorsqu'une perte de connectivité peut affecter vos clients sans fil.

Vues

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.

Le point d'accès prend en charge un maximum de 16 vues.

Les remarques suivantes résument quelques consignes importantes relatives à la configuration des vues SNMPv3. Veuillez lire l'ensemble de ces remarques avant de continuer.

REMARQUE : Une vue MIB appelée « tout » 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 « vue complète » et « aucune vue » sont créées sur le périphérique WAP. Ces vues ne peuvent pas être supprimées ou modifiées.

Pour ajouter et configurer une vue SNMP :

ÉTAPE 1 Sélectionnez **SNMP** > **Vues** dans le volet de navigation.

ÉTAPE 2 Cliquez sur **Ajouter** pour créer une nouvelle ligne dans le tableau des vues SNMPv3.

ÉTAPE 3 Activez la case à cocher dans la nouvelle ligne et cliquez sur **Modifier**.

- **Nom de la vue** : 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 .3.6.1.2.1.1.
- **Masque** : 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 4 Cliquez sur **Enregistrer**. La vue est ajoutée à la liste des vues SNMPv3 et vos modifications sont enregistrées dans la configuration initiale.

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

Groupes

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, le point d'accès possède deux groupes :

- **RO** : groupe en lecture seule utilisant l'authentification et le cryptage des données. Les utilisateurs figurant dans ce groupe utilisent une clé ou un mot de passe MD5 pour l'authentification et une clé ou un mot de passe DES pour le cryptage. Les clés ou mots de passe MD5 et DES doivent être définis. Par défaut, les utilisateurs de ce groupe ont un accès en lecture à la vue MIB par défaut « tout ».
- **RW** : groupe en lecture-écriture utilisant l'authentification et le cryptage des données. Les utilisateurs figurant dans ce groupe utilisent une clé ou un mot de passe MD5 pour l'authentification et une clé ou un mot de passe DES pour le cryptage. Les clés ou mots de passe MD5 et DES doivent être définis. Par défaut, les utilisateurs de ce groupe ont un accès en lecture et en écriture à la vue MIB par défaut « tout ».

REMARQUE : Les groupes par défaut RO et RW ne peuvent pas être supprimés.

REMARQUE : Le point d'accès prend en charge un maximum de huit groupes.

Pour ajouter et configurer un groupe SNMP :

ÉTAPE 1 Sélectionnez >**Groupes SNMP** dans le volet de navigation.

ÉTAPE 2 Cliquez sur **Ajouter** pour créer une nouvelle ligne dans le tableau des groupes SNMPv3.

ÉTAPE 3 Activez la case à cocher du nouveau groupe et cliquez sur **Modifier**.

ÉTAPE 4 Configurez les paramètres suivants :

- **Nom du groupe** : 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** : définit le niveau de sécurité du groupe, qui peut être l'une des valeurs ci-dessous :

- **Aucune Authentification-Aucune confidentialité** : pas d'authentification et pas de cryptage des données (aucune sécurité).
- **Authentification-Aucune confidentialité** : présence d'authentification, mais pas de cryptage des données. Avec ce niveau de sécurité, les utilisateurs envoient des messages SNMP utilisant une clé ou un mot de passe MD5 pour l'authentification, mais n'utilisant pas de clé ou de mot de passe DES pour le cryptage.
- **Authentification-Confidentialité** : présence d'authentification et de cryptage des données. Avec ce niveau de sécurité, les utilisateurs envoient une clé ou un mot de passe MD5 pour l'authentification et une clé ou un mot de passe DES pour le cryptage.

  En ce qui concerne les groupes qui nécessitent l'authentification, le cryptage ou les deux, vous devez définir les clés ou les mots de passe MD5 et DES à la page Utilisateurs SNMP.

▪ **Vues en écriture** : accès en écriture aux MIB pour le groupe, qui peut être l'une des valeurs ci-dessous :

- **vue complète** : le groupe peut créer, modifier et supprimer des MIB.
- **aucune vue** : le groupe ne peut pas créer, ni modifier, ni supprimer des MIB.

▪ **Vues en lecture** : accès en lecture aux MIB pour le groupe :

- **vue complète** : le groupe est autorisé à afficher et à lire l'ensemble des MIB.
- **aucune vue** : le groupe ne peut ni afficher ni lire des MIB.

ÉTAPE 5 Cliquez sur **Enregistrer**. Le groupe est ajouté à la liste des groupes SNMPv3 et vos modifications sont enregistrées dans la configuration initiale.

REMARQUE : Pour supprimer un groupe, sélectionnez-le dans la liste et cliquez sur **Supprimer**.

Utilisateurs

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 MD5 est pris en charge. Pour le cryptage, seul le type DES est pris en charge. Il n'y a pas d'utilisateur SNMPv3 par défaut sur le point d'accès et vous pouvez ajouter jusqu'à huit utilisateurs.

Pour ajouter des utilisateurs SNMP :

ÉTAPE 1 Sélectionnez **SNMP** > **Utilisateurs** dans le volet de navigation.

ÉTAPE 2 Cliquez sur **Ajouter** pour créer une nouvelle ligne dans le tableau des utilisateurs SNMPv3.

ÉTAPE 3 Activez la case à cocher dans la nouvelle ligne et cliquez sur **Modifier**.

ÉTAPE 4 Configurez les paramètres suivants :

- **Nom d'utilisateur** : nom identifiant l'utilisateur SNMPv3. Les noms d'utilisateur peuvent comporter jusqu'à 32 caractères alphanumériques.
- **Groupe** : groupe sur lequel l'utilisateur est mappé. Les groupes par défaut sont RW et RO. Vous pouvez définir des groupes supplémentaires à la page Groupes SNMP.
- **Type d'authentification** : type d'authentification à utiliser dans le cas des demandes SNMPv3 émanant de l'utilisateur, pouvant être l'une des options suivantes :
  - **MD5** : requérir l'authentification MD5 dans le cas des demandes SNMP émanant de l'utilisateur.
  - **Aucun** : les demandes SNMPv3 émanant de cet utilisateur ne requièrent pas d'authentification.
- **Phrase secrète d'authentification** : (si vous spécifiez MD5 en tant que type d'authentification) 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 chiffrement** : type de confidentialité à utiliser dans le cas des demandes SNMP émanant de l'utilisateur, pouvant être l'une des options suivantes :
  - **DES** : utiliser le cryptage DES dans le cas des demandes SNMPv3 émanant de l'utilisateur.

- **Aucun** : les demandes SNMPv3 émanant de cet utilisateur ne requièrent pas de confidentialité.

- **Phrase secrète de cryptage** : (si vous spécifiez DES en tant que type de confidentialité) phrase secrète utilisée pour le cryptage des demandes SNMP. La longueur de la phrase secrète doit être comprise entre 8 et 32 caractères.

ÉTAPE 5 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**.

Cibles

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 des déroutements. Dans le cas des versions 1 et 2 du protocole SNMP, des déroutements 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**) doit être terminée avant celle des cibles SNMPv3.

REMARQUE : Le point d'accès prend en charge un maximum de huit cibles.

Pour ajouter des cibles SNMP :

ÉTAPE 1 Sélectionnez **Cibles** > **SNMP** dans le volet de navigation.

ÉTAPE 2 Cliquez sur **Ajouter**. Une nouvelle ligne est créée dans le tableau.

ÉTAPE 3 Activez la case à cocher dans la nouvelle ligne et cliquez sur **Modifier**.

ÉTAPE 4 Configurez les paramètres suivants :

- **Adresse IP** : entrez l'adresse IPv4 du gestionnaire SNMP distant qui doit recevoir la cible.

- **Port UDP** : entrez le port UDP à utiliser pour l'envoi des cibles SNMPv3.

- **Utilisateurs** : entrez le nom de l'utilisateur SNMP à associer à la cible. Pour configurer les utilisateurs SNMP, reportez-vous à la page **Utilisateurs**.

ÉTAPE 5 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**.

11

Portail captif

Cette section décrit la fonctionnalité de portail captif (CP, Captive Portal), qui permet de bloquer l'accès au réseau pour les clients sans fil tant que la vérification de l'utilisateur n'a pas été établie. Vous pouvez configurer la vérification de portail captif de manière à autoriser l'accès à la fois pour les utilisateurs invités et les utilisateurs authentifiés.

Les utilisateurs authentifiés doivent être validés à l'aide d'une base de données des groupes ou des utilisateurs CP autorisés avant de se voir autoriser l'accès. Cette base de données peut être stockée localement sur le périphérique WAP ou sur un serveur RADIUS.

Le portail captif se compose de deux instances de CP. Il est possible de configurer chaque instance de manière indépendante, avec des méthodes de vérification différentes pour chaque point d'accès virtuel ou SSID. Les périphériques Cisco WAP571/E fonctionnent simultanément avec certains points d'accès virtuels configurés pour l'authentification de portail captif et avec d'autres points d'accès virtuels configurés pour les méthodes normales d'authentification sans fil, comme WPA ou WPA Entreprise.

Cette section inclut les rubriques suivantes :

- **Configuration globale**
- **Groupes/Utilisateurs locaux**
- **Configuration d'instance**
- **Association d'instance**
- **Personnalisation du portail Web**
- **Clients authentifiés**

Configuration globale

Utilisez la page Global CP Configuration pour contrôler l'état administratif de la fonctionnalité de portail captif et configurer les paramètres globaux qui affectent toutes les instances de portail captif configurées sur le périphérique WAP.

Configuration des paramètres globaux du portail captif

Pour configurer les paramètres globaux du portail captif :

ÉTAPE 1 Sélectionnez **Portail captif > Configuration globale**.

ÉTAPE 2 Définissez les paramètres suivants :

- **Mode du portail captif** : active ou désactive le fonctionnement du portail captif sur le périphérique WAP.
- **Délai d'authentification** : pour pouvoir accéder au réseau par l'intermédiaire d'un portail, le client doit tout d'abord entrer des informations d'authentification sur une page Web d'authentification. Ce champ spécifie le temps en secondes pendant lequel le périphérique WAP maintient une session d'authentification ouverte avec le client sans fil associé. Si le client n'entre pas ses identifiants d'authentification durant le temps alloué, il se peut qu'il doive actualiser la page Web d'authentification. Le délai d'authentification par défaut est de 3600 secondes. La plage valide va de 60 à 3600 secondes.
- **Port HTTP supplémentaire** : le trafic HTTP utilise le port de gestion HTTP, qui est le port 80 par défaut. Vous pouvez configurer un port supplémentaire pour le trafic HTTP. Entrez un numéro de port compris entre 1025 et 65535, ou 80. Les ports HTTP et HTTPS ne peuvent pas être identiques.
- **Port HTTP supplémentaire** : le trafic HTTP sur SSL (HTTPS) utilise le port de gestion HTTPS, qui est le port 443 par défaut. Vous pouvez configurer un port supplémentaire pour le trafic HTTPS. Entrez un numéro de port compris entre 1025 et 65535, ou 443. Les ports HTTP et HTTPS ne peuvent pas être identiques.

ÉTAPE 3 La zone Compteurs de configuration du portail captif affiche des informations de portail captif en lecture seule :

- **Nombre d'instances** : nombre d'instances de portail captif actuellement configurées sur le périphérique WAP. Il est possible de configurer jusqu'à deux instances.

- **Nombre de groupes** : nombre de groupes de portail captif actuellement configurés sur le périphérique WAP. Il est possible de configurer jusqu'à deux groupes. Le groupe par défaut existe et ne peut pas être supprimé.
- **Nombre d'utilisateurs** : nombre d'utilisateurs de portail captif actuellement configurés sur le périphérique WAP. Il est possible de configurer jusqu'à 128 utilisateurs.

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

Groupes/Utilisateurs locaux

Utilisez la page Groupes/Utilisateurs locaux pour gérer les groupes et les utilisateurs locaux.

Chaque utilisateur local est affecté à un groupe d'utilisateurs. Chaque groupe est affecté 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 Par défaut est intégré et ne peut pas être supprimé. Vous pouvez créer jusqu'à deux groupes d'utilisateurs supplémentaires.

Pour ajouter des groupes d'utilisateurs locaux :

ÉTAPE 1 Sélectionnez **Portail captif > Groupes/Utilisateurs locaux**.

ÉTAPE 2 Dans la zone Paramètres des groupes locaux, définissez les paramètres suivants :

- **Groupes du portail captif** : sélectionnez Créer pour créer un nouveau groupe.
- **Nom du groupe** : saisissez le nom du nouveau groupe.

ÉTAPE 3 Cliquez sur **Ajouter un groupe**. Les modifications sont enregistrées dans la configuration de démarrage.

Pour supprimer des groupes d'utilisateurs locaux :

ÉTAPE 1 Sélectionnez **Portail captif > Groupes/Utilisateurs locaux**.

ÉTAPE 2 Dans la zone Paramètres des groupes locaux, sélectionnez le groupe à supprimer.

ÉTAPE 3 Cochez l'option Supprimer un groupe.

ÉTAPE 4 Cliquez sur **Supprimer un groupe**. Les modifications sont enregistrées dans la configuration de démarrage.

Vous pouvez configurer une instance de portail captif pour répondre à la fois aux besoins des utilisateurs invités et des utilisateurs autorisés. Les utilisateurs invités ne possèdent pas de noms d'utilisateur ni de mots de passe.

Les utilisateurs autorisés fournissent un nom d'utilisateur et un mot de passe valides qui doivent tout d'abord être validés à partir d'une base de données locale ou d'un serveur RADIUS. Les utilisateurs autorisés sont généralement affectés à une instance de portail captif associée à un autre point d'accès virtuel que les utilisateurs invités.

Vous pouvez configurer jusqu'à 128 utilisateurs autorisés dans la base de données locale.

Pour ajouter et configurer un utilisateur local :

ÉTAPE 1 Sélectionnez **Portail captif** > **Groupes/Utilisateurs locaux**.

ÉTAPE 2 Dans la zone Paramètres des utilisateurs locaux, définissez les paramètres suivants :

- **Utilisateurs de portail captif** : sélectionnez Créer pour créer un nouvel utilisateur.
- **Nom d'utilisateur** : saisissez le nom du nouvel utilisateur.

ÉTAPE 3 Cliquez sur Ajouter un utilisateur.

ÉTAPE 4 La zone Paramètres des utilisateurs locaux s'affiche à nouveau avec des options supplémentaires. Définissez les paramètres suivants :

- **Mot de passe utilisateur** : entrez le mot de passe, composé de 8 à 64 caractères alphanumériques et caractères spéciaux. Un utilisateur doit entrer son mot de passe pour se connecter au réseau par l'intermédiaire du portail captif.
- **Afficher le mot de passe en texte clair** : lorsque cette option est activée, le texte que vous tapez est visible. Si cette option est désactivée, le texte n'est pas masqué lors de sa saisie.
- **Délai d'expiration en cas d'absence** : saisissez la période pendant laquelle un utilisateur reste dans la liste des clients authentifiés de portail captif après la dissociation du client du périphérique 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 d'expiration configurée ici a priorité sur la valeur configurée pour l'instance de portail captif, sauf si la valeur utilisateur est définie à 0. Lorsque cette valeur est définie à 0, la valeur d'expiration configurée pour l'instance de portail captif est utilisée.

- **Nom du groupe** : sélectionnez le groupe d'utilisateurs affecté. Chaque instance de portail captif est configurée de manière à prendre en charge un groupe d'utilisateurs particulier.
- **Bande passante amont maximale** : saisissez la vitesse maximale de chargement, en mégabits par seconde, à laquelle un client peut transmettre du 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 1300 Mbit/s. La valeur par défaut est 0.
- **Bande passante aval maximale** : saisissez la vitesse maximale de téléchargement, en mégabits par seconde, à laquelle un client peut recevoir du 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 1300 Mbit/s. La valeur par défaut est 0.

ÉTAPE 5 Cliquez sur **Enregistrer l'utilisateur**. Les modifications sont enregistrées dans la configuration de démarrage.

Pour supprimer un utilisateur local :

ÉTAPE 1 Sélectionnez **Portail captif > Groupes/Utilisateurs locaux**.

ÉTAPE 2 Dans la zone Paramètres des utilisateurs locaux, sélectionnez l'utilisateur à supprimer.

ÉTAPE 3 Cochez l'option Supprimer un utilisateur.

ÉTAPE 4 Cliquez sur **Supprimer un utilisateur.** Les modifications sont enregistrées dans la configuration de démarrage.

Configuration d'instance

Vous pouvez créer jusqu'à deux instances de portail captif, chacune d'entre elles étant un ensemble défini de paramètres d'instance. Les instances peuvent être associées à un ou plusieurs points d'accès virtuels. Des instances différentes peuvent être configurées de manière à répondre différemment aux utilisateurs lorsque ceux-ci tentent d'accéder au point d'accès virtuel associé.

REMARQUE : Commencez par passer en revue les puces suivantes avant de créer une instance :

- Avez-vous besoin d'ajouter un nouveau point d'accès virtuel ? Si oui, accédez à la page **Réseaux, page 96** pour ajouter un point d'accès virtuel.

Devez-vous ajouter un nouveau groupe ou un nouvel utilisateur ? Si oui, accédez à la page **Groupes/Utilisateurs locaux** pour ajouter un groupe ou un utilisateur.

Création d'une instance de portail captif et configuration de ses paramètres

Pour créer une instance de portail captif et configurer ses paramètres :

ÉTAPE 1 Sélectionnez **Portail captif** > **Configuration d'instance**.

ÉTAPE 2 Sélectionnez **Créer** dans la liste **Instances de portail captif**.

ÉTAPE 3 Dans le champ Nom de l'instance, entrez le nom (1 à 32 caractères alphanumériques) choisi pour l'instance de portail captif.

ÉTAPE 4 Cliquez sur **Enregistrer**.

ÉTAPE 5 La zone Paramètres de l'instance de portail captif réapparaît avec des options supplémentaires. Définissez les paramètres suivants :

- **ID de l'instance** : affiche l'ID de l'instance. Ce champ ne peut pas être modifié.
- **Mode d'administration** : active et désactive l'instance de portail captif.
- **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.
- **Vérification** : méthode d'authentification utilisée par le portail captif pour la vérification des clients :

- **Invité** : les utilisateurs n'ont pas besoin d'être authentifiés par une base de données.
- **Local** : le périphérique WAP utilise une base de données locale pour authentifier les utilisateurs.
- **RADIUS** : le périphérique WAP utilise une base de données située sur un serveur RADIUS distant pour authentifier les utilisateurs.
- **Serveur Active Directory** : le périphérique WAP établit une liaison LDAP sécurisée via le protocole SSL\TLS à l'aide de la commande `starttls` pour authentifier les utilisateurs à partir de leur attribut sAMAccountName dans Active Directory.
- **Informations d'identification tierces** : le périphérique WAP authentifie les utilisateurs à l'aide de leur compte Facebook ou Google.

▪ **Méthode de connexion aux réseaux sociaux :** le périphérique WAP authentifie les utilisateurs à l'aide de leur compte Facebook ou Google via le protocole OAuth.

- **Facebook** : active ou désactive la méthode de connexion aux réseaux sociaux pour authentifier les clients à l'aide de leur compte Facebook.
- **Google** : active ou désactive la méthode de connexion aux réseaux sociaux pour authentifier les clients à l'aide de leur compte Google.

▪ **Hôte 1 du serveur Active Directory** : ajoutez un serveur et saisissez l'adresse IP du contrôleur de domaine.

▪ **Hôte 2 du serveur Active Directory** : ajoutez un serveur et saisissez l'adresse IP du contrôleur de domaine.

▪ **Hôte 3 du serveur Active Directory** : ajoutez un serveur et saisissez l'adresse IP du contrôleur de domaine.

REMARQUE

▪ Vous pouvez ajouter plusieurs serveurs. Le point d'accès interrogera ces serveurs dans un ordre séquentiel, de l'hôte 1 à l'hôte 3.

▪ **Plage de « Walled Garden » : spécifiez la liste de domaines** auxquels peuvent accéder les utilisateurs avant d'atteindre la page du portail Web. Les éléments de la liste doivent être séparés par une virgule, et les domaines peuvent inclure des astérisques (*) comme caractères de remplacement.

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
- Lorsque la connexion via Facebook ou Google est activée, la fonctionnalité Walled Garden est automatiquement activée et ajoute les domaines suivants à la liste d'options d'authentification. La liste de domaines peut être modifiée par Facebook ou Google, et peut ne pas être à jour. Vous avez la possibilité d'ajouter des domaines manuellement.
  - **Facebook**: *.facebook.com, *.facebook.net, *.fbcdn.net
  - **Google**: *.googleapis.com, apis.google.com, accounts.google.com, *.googleusercontent.com, , ssl.gstatic.com, fonts.gstatic.com
  - **Windows 10**: ww.msftconnecttest.com
- **Rediriger** : lorsque cette option est activée, le portail captif doit rediriger le client nouvellement authentifié vers l'URL configurée. Si cette option est désactivée, l'utilisateur voit la page d'accueil correspondant à ses paramètres régionaux après une vérification réussie.
- **URL de redirection** : si le mode Rediriger est activé, saisissez ici l'URL (y compris le préfixe http://) vers laquelle le client nouvellement authentifié sera redirigé. La plage valide va de 0 à 256 caractères.
- **Délai d'expiration** : saisissez la période pendant laquelle un utilisateur reste dans la liste des clients authentifiés de portail captif après la dissociation du client du périphérique 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 1 440 minutes. La valeur par défaut est de 60 minutes.

Un délai d'expiration est également configuré pour chaque utilisateur. Reportez-vous à la page **Groupes/Utilisateurs locaux**. Le délai d'expiration défini à la page Utilisateurs locaux a priorité sur la valeur configurée ici, sauf si la valeur est définie à 0 (valeur par défaut). Une valeur égale à 0 indique que la valeur d'expiration de l'instance est utilisée.

- **Délai d'expiration de la session** : saisissez la période de validité restant, en secondes, de la session de portail captif. Lorsque ce temps atteint la valeur zéro, le client est désauthentifié. La plage valide va de 0 à 1440 minutes. La valeur par défaut est 0.

- **Bande passante amont maximale** : saisissez la vitesse maximale de chargement, en mégabits par seconde, à laquelle un client peut transmettre du trafic lorsqu'il utilise le portail captif. Ce paramètre limite la bande passante à laquelle le client peut envoyer des données sur le réseau. La plage valide va de 0 à 1300 Mbit/s. La valeur par défaut est 0.
- **Bande passante aval maximale** : saisissez la vitesse maximale de téléchargement, en mégabits par seconde, à laquelle un client peut recevoir du trafic lorsqu'il utilise le portail captif. Ce paramètre limite la bande passante à laquelle le client peut recevoir des données du réseau. La plage valide va de 0 à 1300 Mbit/s. La valeur par défaut est 0.
- **Nom du groupe d'utilisateurs** : si le mode de vérification est Local ou RADIUS, ce paramètre affecte un groupe d'utilisateurs existant à l'instance de portail captif. Tous les utilisateurs appartenant à ce groupe sont autorisés à accéder au réseau par l'intermédiaire de ce portail.
- **Réseau IP RADIUS** : déterminez si le client WAP RADIUS utilise les adresses configurées de serveur RADIUS IPv4 ou IPv6.
- **RADIUS global** : si le mode de vérification est RADIUS, cochez l'option Activer de façon à utiliser la liste des serveurs RADIUS globaux par défaut pour authentifier les clients. (Reportez-vous à **Serveur RADIUS** pour plus d'informations sur la configuration des serveurs RADIUS globaux.) Si vous souhaitez que la fonctionnalité de portail captif utilise un ensemble différent de serveurs RADIUS, décochez la case et configurez les serveurs dans les champs correspondants de cette page.
- **Gestion de comptes RADIUS** : active le suivi et la mesure des ressources consommées par un utilisateur donné, comme le temps système ou les volumes de données transmis et reçus. 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 sauvegarde et pour les serveurs configurés globalement et localement.
- **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). La forme de l'adresse IPv6 doit être similaire à celle-ci : xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx (2001:DB8::CAD5:7D91).

Lorsque le premier client sans fil tente de s'authentifier à l'aide du VAP, le périphérique WAP envoie une demande d'authentification au serveur principal. Si le serveur principal répond à la demande d'authentification, le périphérique 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** à **4)** ou **Adresse IPv6 du serveur (2** à **4)** : saisissez jusqu'à trois adresses de serveur RADIUS IPv4 ou IPv6 de sauvegarde. Si l'authentification auprès du serveur principal échoue, une tentative est effectuée sur chaque serveur de secours configuré.
- **Clé 1** : entrez la clé secrète partagée utilisée par le périphérique WAP 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** à **Clé 4** : saisissez la clé RADIUS associée aux serveurs RADIUS de sauvegarde configurés. Le serveur spécifié dans le champ Adresse IP (IPv6) du serveur 1 utilise Clé 1 ; le serveur spécifié dans le champ Adresse IP (IPv6) du serveur 2 utilise Clé 2, etc.
- **Nombre de paramètres régionaux** : nombre de paramètres régionaux associés à l'instance. Vous pouvez créer et affecter jusqu'à trois paramètres régionaux différents à chaque instance de portail captif à partir de la page Personnalisation Web.
- **Supprimer l'instance** : cochez l'option pour supprimer l'instance en cours.

ÉTAPE 6 Cliquez sur **Enregistrer**. Les modifications que vous avez effectuées sont enregistrées dans la configuration de démarrage.

Association d'instance

Après avoir créé une instance, utilisez la page Association d'instance pour associer une instance de portail captif à un point d'accès virtuel. Les paramètres de l'instance de portail captif associée s'appliquent aux utilisateurs qui tentent de s'authentifier sur le point d'accès virtuel.

Association d'une instance à un point d'accès virtuel

Pour associer une instance à un point d'accès virtuel :

ÉTAPE 1 Sélectionnez **Portail captif** > **Association d'instance**.

ÉTAPE 2 Choisissez le mode radio à configurer:

ÉTAPE 3 Sélectionnez le nom d'instance pour chaque point d'accès virtuel auquel vous voulez associer une instance.

ÉTAPE 4 Cliquez sur **Enregistrer**. Les modifications que vous avez effectuées sont enregistrées dans la configuration de démarrage.

Personnalisation du portail Web

Une fois l'instance de portail captif associée à un point d'accès virtuel, vous devez créer des paramètres régionaux (une page Web d'authentification) et les mapper avec l'instance de portail captif. Lorsqu'un utilisateur accède à un point d'accès virtuel associé à une instance de portail captif, une page d'authentification s'affiche.

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

Configuration de la page d'authentification du portail captif

Création et personnalisation de la page d'authentification du portail captif

Pour créer et personnaliser une page d'authentification de portail captif :

ÉTAPE 1 Sélectionnez **Portail captif > Personnalisation du portail Web**.

ÉTAPE 2 Sélectionnez **Créer** dans la liste **Paramètres régionaux Web du portail captif**.

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 paramètres suivants :

- **Nom des paramètres régionaux Web** : saisissez un nom de paramètres régionaux Web à affecter à la page. Le nom peut être constitué de 1 à 32 caractères alphanumériques.

- **Instances de portail captif** : sélectionnez l'instance de portail captif à laquelle ces paramètres régionaux sont associés. Vous pouvez associer plusieurs paramètres régionaux à une instance. Lorsqu'un utilisateur tente d'accéder à un point d'accès virtuel spécifique associé à une instance de portail captif, les paramètres régionaux qui sont associés à cette instance apparaissent sous la forme de liens sur la page d'authentification. L'utilisateur peut alors sélectionner un lien pour passer à ces paramètres régionaux.

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

ÉTAPE 5 La zone Paramètres régionaux Web du portail captif s'affiche à nouveau avec des options supplémentaires permettant de modifier les paramètres régionaux. Les champs ID de paramètre régional et Nom de l'instance ne peuvent pas être modifiés. Les champs modifiables sont préremplis avec les valeurs par défaut.

ÉTAPE 6 Définissez les paramètres suivants :

- **Nom de l'image d'arrière-plan** : sélectionnez l'image à afficher en tant qu'arrière-plan de la page. Vous pouvez cliquer sur **Charger/supprimer l'image personnalisée** pour charger des images pour les instances de portail captif. Pour plus d'informations, reportez-vous à la section **Chargement et suppression d'images**.
- **Nom de l'image du logo** : sélectionnez le fichier image à afficher dans le coin supérieur gauche de la page. Cette image est utilisée à des fins commerciales (il s'agit par exemple du logo de l'entreprise). Si vous avez téléchargé un logo personnalisé vers le périphérique WAP, vous pouvez le sélectionner dans la liste.
- **Couleur de premier plan** : saisissez le code HTML de la couleur de premier plan au format hexadécimal à 6 chiffres. La plage valide va de 1 à 32 caractères. La valeur par défaut est #999999.
- **Couleur d'arrière-plan** : saisissez le code HTML de la couleur d'arrière-plan au format hexadécimal à 6 chiffres. La plage valide va de 1 à 32 caractères. La valeur par défaut est #BFBFBF.
- **Séparateur** : saisissez le code HTML de la couleur de l'épaisse ligne horizontale séparant l'en-tête de page du corps de page, au format hexadécimal à 6 chiffres. La plage valide va de 1 à 32 caractères. La valeur par défaut est #BFBFBF.
- **Étiquette des paramètres régionaux** : saisissez l'étiquette descriptive des paramètres régionaux, composée de 1 à 32 caractères. Les paramètres régionaux par défaut sont l'anglais.

- **Paramètres régionaux** : saisissez l'abréviation des paramètres régionaux, composée de 1 à 32 caractères. La valeur par défaut est en.
- **Image du compte** : sélectionnez le fichier image à afficher au-dessus du champ de connexion pour représenter une connexion authentifiée.
- **Étiquette du compte** : texte demandant à l'utilisateur d'entrer un nom d'utilisateur. La plage valide va de 1 à 32 caractères.
- **Étiquette utilisateur** : étiquette de la zone de texte du nom d'utilisateur. La plage valide va de 1 à 32 caractères.
- **Étiquette du mot de passe** : étiquette de la zone de texte du mot de passe d'utilisateur. La plage valide va de 1 à 64 caractères.
- **Étiquette de 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 Connexion.
- **Polices** : nom de la police à utiliser pour l'ensemble du texte de la page de portail captif. Vous pouvez entrer plusieurs noms de police, chaque nom devant être séparé des autres par une virgule. Si la première police n'est pas disponible sur le système client, la police suivante est utilisée, etc. Si un nom de police contient des espaces, mettez le nom complet entre guillemets. La plage valide va de 1 à 512 caractères. La valeur par défaut est MS UI Gothic, Arial, sans-serif.
- **Titre du navigateur** : texte à afficher dans la barre de titre du navigateur. La plage valide va de 1 à 128 caractères. La valeur par défaut est Portail captif.
- **Contenu du navigateur** : texte qui apparaît dans l'en-tête de page, à droite du logo. La plage valide va de 1 à 128 caractères. La valeur par défaut est Bienvenue dans le réseau sans fil.
- **Contenu** : texte d'instruction qui s'affiche dans le corps de page en dessous des zones de texte du nom d'utilisateur et du mot de passe. La plage valide va de 1 à 256 caractères. La valeur par défaut est Pour commencer à utiliser ce service; saisissez vos informations d'identification et cliquez sur le bouton de connexion.
- **Stratégie d'utilisation acceptable** : texte qui apparaît dans la zone de texte Stratégie d'utilisation acceptable. La plage valide va de 1 à 4096 caractères. La valeur par défaut est Stratégie d'utilisation acceptable.

- **Étiquette d'acceptation** : texte demandant aux utilisateurs d'activer la case à cocher relative à la lecture et à l'acceptation de la stratégie d'utilisation. La plage valide va de 1 à 128 caractères.
- **Texte sans acceptation** : texte qui s'affiche dans une fenêtre contextuelle lorsqu'un utilisateur soumet ses informations d'identification de connexion sans avoir activé la case à cocher Stratégie d'utilisation acceptable. La plage valide va de 1 à 128 caractères.
- **Texte lors de l'authentification** : texte qui s'affiche durant l'authentification. La plage valide va de 1 à 128 caractères.
- **Texte en cas d'échec** : texte qui s'affiche lors de l'échec de l'authentification d'un utilisateur. La plage valide va de 1 à 128 caractères.
- **Titre de bienvenue** : texte qui s'affiche lorsque le client s'est authentifié sur le point d'accès virtuel. La plage valide va de 1 à 128 caractères.
- **Contenu de bienvenue** : texte qui s'affiche lorsque le client s'est connecté au réseau. La plage valide va de 1 à 256 caractères.
- **Supprimer les paramètres régionaux** : supprime les paramètres régionaux actuels.

ÉTAPE 7 Cliquez sur **Enregistrer**. Les modifications que vous avez effectuées sont enregistrées dans la configuration de démarrage.

ÉTAPE 8 Cliquez sur **Aperçu** pour afficher la page mise à jour.

REMARQUE : Vous pouvez cliquer sur **Aperçu** pour afficher le texte et les images qui ont déjà été enregistrés dans la configuration de démarrage. Si vous apportez des modifications, cliquez sur **Enregistrer** avant de cliquer sur **Aperçu** pour voir vos modifications.

Chargement et suppression d'images

Lorsque les utilisateurs créent l'accès à un point d'accès virtuel associé à une instance de portail captif, une page d'authentification apparaît. Vous pouvez personnaliser la page d'authentification avec votre propre logo ou d'autres images.

Vous pouvez charger jusqu'à 18 images (à savoir six valeurs de paramètres régionaux, chaque valeur possédant trois images). Les images doivent être au format GIF ou JPG, et leur taille maximale est de 5 kilo-octets.

Les images sont redimensionnées conformément aux dimensions spécifiées. Pour obtenir des résultats optimaux, les images de votre logo et de votre compte doivent être de proportions similaires à celles des images par défaut, comme indiqué ci-dessous :

Type d'image	Utilisation	Largeur x hauteur par défaut
Arrière-plan	S'affiche en tant qu'arrière-plan de page.	10 x 800 pixels
Logo	S'affiche en haut à gauche de la page en vue de fournir des informations commerciales.	168 x 78 pixels
Compte	S'affiche au-dessus du champ de connexion pour représenter une connexion authentifiée.	295 x 55 pixels

Chargement de fichiers graphiques binaires sur le périphérique WAP

Pour charger des fichiers graphiques binaires sur le périphérique WAP :

ÉTAPE 1 Sur la page Personnalisation du portail Web, cliquez sur **Charger/supprimer l'image personnalisée** à côté des champs **Nom de l'image d'arrière-plan**, **Nom de l'image du logo** ou **Image du compte**.

La page Image personnalisée Web du portail apparaît.

ÉTAPE 2 Cliquez sur Parcourir pour sélectionner l'image.

ÉTAPE 3 Cliquer sur **Charger**.

ÉTAPE 4 Cliquez sur **Retour** pour revenir à la page Image personnalisée Web du portail.

ÉTAPE 5 Dans la zone **Paramètres régionaux Web du portail captif**, sélectionnez les paramètres régionaux Web à configurer pour le portail captif.

ÉTAPE 6 Pour les champs **Nom de l'image d'arrière-plan**, **Nom de l'image du logo** ou **Image du compte**, sélectionnez l'image nouvellement chargée.

ÉTAPE 7 Cliquez sur **Enregistrer**.

ÉTAPE 8 Pour supprimer une image, sur la page Image personnalisée Web du portail, sélectionnez-la dans la liste **Supprimer l'image personnalisée Web**, puis cliquez sur **Supprimer**. Vous ne pouvez pas supprimer les images par défaut.

Clients authentifiés

La page Authenticated Clients propose deux tables. La première, Authenticated Clients, fournit des informations sur les clients qui ont été authentifiés sur une instance quelconque du portail captif. L'autre, Failed Authenticated Clients, 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 qui n'ont pas réussi à s'authentifier, sélectionnez Portail captif > Clients authentifiés. Les informations suivantes sont indiquées :

- **Adresse 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** : le périphérique WAP utilise une base de données locale pour authentifier les utilisateurs.
  - **RADIUS** : le périphérique WAP utilise une base de données située sur un serveur RADIUS distant pour authentifier les utilisateurs.
  - **Facebook** : le périphérique WAP utilise des comptes Facebook pour authentifier les utilisateurs.
  - **Google** : le périphérique WAP utilise des comptes Google pour authentifier les utilisateurs.
  - **Serveur Active Directory** : le périphérique WAP utilise la base de données du serveur Active Directory pour authentifier les utilisateurs.
- **ID VAP** : point d'accès virtuel auquel l'utilisateur est associé.
- **ID de radio** : ID de la radio.
- **ID de portail captif** : ID de l'instance de portail captif à laquelle l'utilisateur est associé.

- **Délai d'expiration de la session** : temps de validité restant, en secondes, de la session de portail captif. Lorsque ce temps atteint la valeur zéro, le client est désauthentifié.
- **Délai d'expiration en cas d'absence** : temps de validité restant, en secondes, de l'entrée du client. La minuterie démarre lorsque le client se dissocie du portail captif. Lorsque la valeur zéro est atteinte, le client est désauthentifié.
- **Paquets reçus** : nombre de paquets IP reçus par le périphérique WAP depuis la station utilisateur.
- **Paquets émis** : nombre de paquets IP transmis depuis le périphérique WAP vers la station utilisateur.
- **Octets reçus** : nombre d'octets reçus par le périphérique WAP depuis la station utilisateur.
- **Octets transmis** : nombre d'octets transmis depuis le périphérique WAP vers 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 **Actualiser** pour afficher les dernières données en provenance du périphérique WAP.

12

Configuration par point unique

Cette section explique comment paramétrer une configuration de point unique sur plusieurs périphériques WAP.

Elle contient les rubriques suivantes :

- **Présentation de la configuration de point unique**
- **Points d'accès**
- **Sessions**
- **Gestion des canaux**
- **Voisinage sans fil**
- **Mise à niveau du microprogramme de la grappe**

Présentation de la configuration de point unique

La configuration de point unique est une méthode centralisée permettant d'administrer et de contrôler les services sans fil sur plusieurs périphériques. La configuration de point unique sert à créer un groupe ou un cluster unique de périphériques sans fil. Lorsque les périphériques WAP sont regroupés en un cluster, vous pouvez afficher, déployer, configurer et sécuriser le réseau sans fil en tant qu'entité unique. Après la création d'un cluster sans fil, la configuration de point unique facilite également la planification des canaux sur l'ensemble de vos services sans fil afin de réduire les interférences radio et d'optimiser la bande passante du réseau sans fil.

Lors de la première configuration d'un périphérique WAP, vous pouvez paramétrer la configuration de point unique à l'aide de l'assistant de configuration ou ajouter le périphérique à une configuration de point unique existante. Si vous ne souhaitez pas utiliser l'assistant de configuration, vous pouvez vous servir de l'utilitaire de configuration Web.

Gestion de la configuration de point unique sur les points d'accès

La configuration de point unique créé, dans le même sous-réseau, un cluster ou un groupe de périphériques WAP dynamique et sensible à la configuration. Une grappe prend en charge un groupe de 16 appareils WAP571/E configurés au maximum, mais aucun modèle non WAP571/E n'est admis.

La configuration de point unique permet la gestion de plusieurs clusters dans un même sous-réseau ou réseau. Toutefois, les clusters sont gérés en tant qu'entités indépendantes uniques. Le tableau indique les limites des services sans fil à configuration de point unique.

Type de groupe/ cluster	Nombre de périphériques WAP par configuration de point unique	Nombre de clients actifs par configuration de point unique	Nombre maximal de clients (actifs et inactifs)
WAP571/E	16	960 pour le système WAP571 /E bibande	2048 pour le système WAP571/ E bibande

Un cluster peut propager des informations de configuration, telles que les paramètres du point d'accès virtuel, de file d'attente QoS et de radio. Lorsque vous paramétrez une configuration de point unique sur un périphérique, les paramètres de celui-ci (qu'ils aient été définis manuellement ou par défaut) sont propagés aux autres périphériques lorsqu'ils rejoignent le cluster.

Configuration requise et conditions pour former une grappe

Pour former un cluster, suivez la procédure suivante :

ÉTAPE 1 Planifiez votre cluster à configuration de point unique. Vérifiez que les périphériques WAP que vous souhaitez regrouper dans le cluster sont compatibles entre eux. Par exemple, les appareils Cisco WAP571/E peuvent uniquement être regroupés dans une grappe contenant des appareils Cisco WAP571/E.

REMARQUE : Il est fortement recommandé d'utiliser la dernière version du microprogramme sur tous les périphériques WAP du cluster. Les mises à niveau du microprogramme **ne sont pas** propagées sur tous les périphériques WAP d'un cluster. Vous devez donc mettre à niveau individuellement chaque périphérique.

ÉTAPE 2 Configurez les périphériques WAP qui seront regroupés en cluster sur un même sous-réseau IP et vérifiez qu'ils sont interconnectés et accessibles sur l'ensemble du réseau local commuté.

ÉTAPE 3 Activez la configuration de point unique sur tous les périphériques WAP. Reportez-vous à la section **Points d'accès**.

ÉTAPE 4 Vérifiez que tous les périphériques WAP indiquent le même nom de configuration de point unique. Reportez-vous à la section **Points d'accès**.

Négociation de la configuration de point unique

Lorsque la configuration de point unique est activée et paramétrée sur un point d'accès, celui-ci commence à envoyer des annonces toutes les 10 secondes pour signaler sa présence. Si d'autres périphériques WAP correspondent aux critères du cluster, un arbitrage a lieu afin de déterminer quel périphérique WAP distribuera la configuration principale aux autres membres du cluster.

Les règles suivantes s'appliquent à la formation et à l'arbitrage du cluster à configuration de point unique :

- Pour les clusters à configuration de point unique existants, dès que l'administrateur met à jour la configuration de l'un des membres du cluster, la modification est propagée à tous les membres du cluster et le périphérique WAP configuré prend le contrôle du cluster.
- Lorsque deux clusters à configuration de point unique distincts sont regroupés en un seul cluster, le cluster modifié en dernier remporte l'arbitrage de la configuration. Il écrase et met alors à jour la configuration de tous les périphériques WAP du cluster.
- Si un périphérique WAP d'un cluster ne reçoit pas les annonces d'un autre périphérique WAP pendant plus de 60 secondes (par exemple si le périphérique n'est plus connecté aux autres périphériques du cluster), celui-ci est supprimé du cluster.
- Si un périphérique WAP en mode de configuration de point unique perd sa connexion, il n'est pas immédiatement exclu du cluster. S'il se reconnecte et rejoint le cluster sans être exclu et que des modifications ont été apportées à la configuration de ce périphérique lorsqu'il était déconnecté, les modifications sont propagées aux autres membres du cluster lorsque la connexion est rétablie.
- Si un périphérique WAP d'un cluster perd sa connexion, est exclu, puis rejoint à nouveau le cluster et que des modifications ont été apportées à la configuration du cluster lorsqu'il était déconnecté, les modifications sont propagées au périphérique lorsqu'il rejoint le cluster. Si des modifications de configuration sont effectuées à la fois sur le périphérique déconnecté et sur le cluster, le périphérique ayant subi le plus de modifications, puis, en deuxième lieu, celui ayant subi la modification la plus récente propagera sa configuration au cluster. (C'est-à-dire que WAP1 a subi davantage de

modifications, mais que WAP2 a subi la modification la plus récente, c'est WAP1 qui propagera sa configuration. S'ils ont tous les deux subi le même nombre de modifications, mais que WAP2 a subi la modification la plus récente, alors c'est WAP2 qui propagera sa configuration.)

Fonctionnement d'un périphérique exclu d'une configuration de point unique

Lorsqu'un périphérique WAP qui était auparavant un membre d'un cluster est déconnecté de celui-ci, les règles suivantes s'appliquent :

- La perte du contact avec le cluster empêche le périphérique WAP de recevoir les derniers paramètres de configuration opérationnels. La déconnexion provoque l'interruption du service sans fil correct sur l'ensemble du réseau de production.
- Le périphérique WAP continue de fonctionner selon les paramètres sans fil qu'il a reçus en dernier du cluster.
- Les clients sans fil associés au périphérique WAP non inclus dans le cluster continuent à s'associer au périphérique sans provoquer d'interruption de la connexion sans fil. En d'autres termes, la perte du contact avec le cluster n'interrompt pas forcément l'accès aux ressources réseau des clients sans fil associés au périphérique WAP déconnecté.
- Si la perte du contact avec le cluster est liée à une déconnexion physique ou logique de l'infrastructure LAN, elle peut avoir une incidence sur les services réseau voire sur les clients sans fil, selon la nature de la panne.

Le tableau suivant récapitule les configurations partagées et propagées à l'ensemble des périphériques WAP du cluster.

Paramètres de configuration propagés et non propagés aux points d'accès à configuration de point unique

Paramètres de configuration communs propagés en mode de configuration de point unique	
Portail captif	Complexité des mots de passe
QoS des clients	Comptes d'utilisateur
Alerte par e-mail	QoS
Service HTTP/HTTPS (sauf configuration du certificat SSL)	Paramètres radio y compris Paramètres TSpec (sauf quelques exceptions)

Paramètres de configuration communs propagés en mode de configuration de point unique	
Paramètres des journaux	Détection de point d'accès non autorisé
Filtrage MAC	Planificateur
Contrôle d'accès de gestion	SNMP général et SNMPv3
Réseaux	Complexité WPA-PSK
Paramètres d'heure	Acheminement multidestination sans fil
Affichage des voyants	
LLDP (sauf configuration de priorité POE)	
Umbrella	

Paramètres de configuration radio propagés en mode de configuration de point unique
Mode
Seuil de fragmentation
Seuil RTS
Ensembles de débits
Canal principal
Protection
Taux de multidiffusion fixe
Limites de débit de diffusion/multidiffusion
Bande passante de canal
Intervalle de garde court pris en charge

Paramètres de configuration radio non propagés en mode de configuration de point unique
Canal
Intervalle de balise
Période DTIM
Nombre maximal de stations
Puissance de transmission

Autres paramètres de configuration non propagés en mode de configuration de point unique	
Utilisation de la bande passante	Paramètres des ports
Bonjour	VLAN et IPv4
Adresse IPv6	Pont WDS
Tunnel IPv6	
Capture des paquets	Pont de groupe de travail

Points d'accès

La page Points d'accès vous permet d'activer et de désactiver la configuration de point unique sur un périphérique WAP, d'afficher les membres d'un cluster et de configurer l'emplacement et le nom du cluster sur un membre. Vous pouvez également cliquer sur l'adresse IP d'un membre pour configurer et afficher les données de ce périphérique.

Configuration du périphérique WAP pour la configuration de point unique

Pour configurer l'emplacement et le nom d'un membre d'un cluster à configuration de point unique, procédez comme suit :

ÉTAPE 1 Cliquez sur **Configuration de point unique > Points d'accès** dans le volet de navigation.

La configuration de point unique est désactivée par défaut sur le point d'accès. Lorsque celle-ci est désactivée, le bouton **Activer la configuration de point unique** s'affiche. Si la configuration de point unique est activée, le bouton **Désactiver la configuration de point unique** s'affiche. Vous ne pouvez modifier les options de configuration de point unique que si la configuration de point unique est désactivée.

Des icônes situées sur la droite de la page indiquent si elle est activée et, dans l'affirmative, elles spécifient également le nombre de périphériques WAP formant actuellement le cluster.

ÉTAPE 2 Après vous être assuré que la configuration de point unique est désactivée, configurez les paramètres suivants pour chaque membre du cluster à configuration de point unique.

- **Emplacement** : saisissez une description de l'emplacement physique du point d'accès, par exemple « Réception ». Ce champ est facultatif.
- **Nom de la grappe** : indiquez le nom du cluster auquel le périphérique WAP doit se joindre, par exemple « Cluster_Réception ».

  Le nom du cluster n'est pas envoyé aux autres périphériques WAP. Vous devez donc configurer le même nom sur chaque périphérique membre d'un même cluster. Le nom du cluster doit par ailleurs être unique pour chaque configuration de point unique que vous paramétrez sur le réseau. Le nom par défaut est « ciscosb-cluster ».
- **Version du protocole IP du regroupement** : indiquez la version du protocole IP que les périphériques WAP du cluster utilisent pour communiquer avec les autres membres du cluster. La version par défaut est IPv4.

  Si vous choisissez la version IPv6, la configuration de point unique peut utiliser l'adresse de liaison locale, l'adresse IPv6 globale autoconfigurée et l'adresse IPv6 globale configurée de manière statique. Dans ce cas, assurez-vous que tous les périphériques WAP du cluster utilisent soit uniquement des adresses de liaison locales soit uniquement des adresses globales.

  La configuration de point unique fonctionne uniquement sur des périphériques utilisant le même type d'adressage IP. Elle ne fonctionne pas dans les groupes de périphériques WAP dont certains utilisent des adresses IPv4 et d'autres des adresses IPv6.

ÉTAPE 3 Cliquez sur **Activer la configuration de point unique**.

Le périphérique WAP commence à rechercher dans le sous-réseau d'autres périphériques WAP configurés avec le même nom de cluster et la même version du protocole IP. Les membres éventuels du cluster envoient des annonces toutes les 10 secondes afin de signaler leur présence.

Pendant la recherche d'autres membres du cluster, l'état indique que la configuration est en cours d'application. Actualisez la page pour afficher la nouvelle configuration.

Si un ou plusieurs périphériques WAP sont déjà configurés avec les mêmes paramètres de cluster, le périphérique WAP rejoint le cluster et les informations sur chaque membre s'affichent dans un tableau.

ÉTAPE 4 Répétez cette procédure sur les autres périphériques WAP que vous souhaitez ajouter à la configuration de point unique.

Affichage des informations de la configuration de point unique

Lorsque le mode Configuration de point unique est activé, le point d'accès forme automatiquement une grappe avec les autres appareils WAP partageant la même configuration. Sur la page Points d'accès, les périphériques WAP détectés sont répertoriés dans un tableau et les informations suivantes sont affichées :

- **Emplacement** : description de l'emplacement physique du point d'accès.
- **Adresse MAC** : adresse MAC (Media Access Control) du point d'accès. Cette adresse correspond à l'adresse MAC du pont (br0) et à l'adresse du périphérique WAP connue des autres réseaux.
- **Adresse IP** : adresse IP du point d'accès.

Remarque : l'état de la configuration de point unique et le nombre de périphériques WAP sont indiqués par des graphiques sur la droite de la page.

Ajout d'un point d'accès à une configuration de point unique

Pour ajouter à un cluster à configuration de point unique un nouveau point d'accès actuellement en mode autonome, procédez comme suit :

ÉTAPE 1 Accédez à l'utilitaire de configuration Web sur le point d'accès autonome.

ÉTAPE 2 Cliquez sur **Configuration de point unique > Points d'accès** dans le volet de navigation.

ÉTAPE 3 Dans **Nom de la grappe**, indiquez le nom de cluster que vous avez configuré sur les membres du cluster.

ÉTAPE 4 Dans le champ **Emplacement**, saisissez une description de l'emplacement physique du point d'accès, par exemple « Réception » (facultatif).

ÉTAPE 5 Cliquez sur **Activer la configuration de point unique**.

Le point d'accès rejoint automatiquement la configuration de point unique.

Suppression d'un point d'accès d'une configuration de point unique

Pour supprimer un point d'accès d'une grappe à configuration de point unique :

ÉTAPE 1 Dans le tableau affichant les périphériques détectés, cliquez sur l'adresse IP du périphérique WAP que vous souhaitez supprimer du cluster.

L'utilitaire de configuration Web de ce périphérique s'affiche.

ÉTAPE 2 Cliquez sur **Configuration de point unique > Points d'accès** dans le volet de navigation.

ÉTAPE 3 Cliquez sur **Désactiver la configuration de point unique.**

Le champ d'état **Configuration de point unique** de ce point d'accès indique alors **Désactivé**.

Accès aux informations de configuration d'un appareil spécifique

Tous les périphériques WAP d'une grappe à configuration de point unique présentent la même configuration (à condition que les éléments configurables puissent être propagés). Peu importe le périphérique WAP auquel vous vous connectez pour l'administration, les modifications de la configuration de n'importe quel périphérique WAP du cluster sont propagées aux autres membres.

Cependant, il peut arriver que vous souhaitiez afficher ou gérer des informations d'un périphérique WAP spécifique. Par exemple, vous souhaiterez peut-être consulter des informations relatives à l'état d'un point d'accès, notamment les associations de clients ou les événements. Dans ce cas, vous pouvez cliquer sur l'adresse IP figurant dans le tableau de la page Points d'accès pour afficher l'utilitaire de configuration Web de ce point d'accès.

Accès à un périphérique à l'aide de son adresse IP dans une URL

Vous pouvez également vous connecter à l'utilitaire de configuration Web d'un périphérique WAP spécifique en saisissant l'adresse IP de ce point d'accès directement dans la barre d'adresse d'un navigateur Web. Pour cela, utilisez la forme d'URL suivante :

http://AdresseIPDuPointD'Accès (si vous utilisez le protocole HTTP)

https://AdresseIPDuPointD'Accès (si vous utilisez le protocole HTTPS)

Sessions

La page Sessions affiche des informations sur les clients WLAN associés aux périphériques WAP du cluster à configuration de point unique. Chaque client WLAN est identifié par son adresse MAC et l'emplacement du périphérique auquel il est actuellement connecté.

REMARQUE : La page Sessions affiche un maximum de 20 clients par radio des périphériques WAP du cluster. Pour afficher tous les clients WLAN associés à un périphérique WAP, consultez la page Statut > Clients associés directement sur ce périphérique.

Pour afficher une statistique spécifique d'une session de client WLAN, sélectionnez un élément de la liste Affichage et cliquez sur **OK**. Vous pouvez consulter des informations sur le temps d'inactivité, le débit et la puissance du signal.

Dans ce contexte, une session correspond à la période pendant laquelle un utilisateur d'un périphérique client (station) doté d'une adresse MAC unique maintient une connexion au réseau sans fil. La session commence lorsque le client WLAN se connecte au réseau. Elle se termine lorsque le client WLAN se déconnecte, intentionnellement ou non.

REMARQUE : Une session diffère d'une association, qui décrit la connexion de clients WLAN à un point d'accès spécifique. Une association de clients WLAN peut passer d'un point d'accès du cluster à un autre au cours d'une même session.

Pour afficher les sessions associées à la grappe, cliquez sur **Configuration de point unique > Sessions**.

Les données suivantes s'affichent pour chaque session de client WLAN avec une configuration de point unique.

- **Emplacement du point d'accès** : emplacement du point d'accès

  L'emplacement est celui spécifié sur la page Administration > Paramètres système.

- **Adresse MAC utilisateur** : adresse MAC du client sans fil.

  Une adresse MAC est une adresse matérielle unique qui identifie chaque nœud d'un réseau.

- **Inactif** : temps d'inactivité d'un client WLAN.

  Un client WLAN est considéré comme inactif lorsqu'il ne reçoit et ne transmet aucune donnée.

- **Débit** : débit de données négocié. Les débits réels peuvent varier en fonction de la surcharge.

La vitesse de transmission des données est mesurée en mégabits par seconde (Mbit/s). Cette valeur doit être comprise dans la plage de débit annoncée pour le mode utilisé sur le point d'accès. Par exemple entre 6 et 54 Mbit/s pour le mode 802.11a.

La vitesse signalée est la vitesse du dernier paquet transmis au client à partir du point d'accès. Cette valeur peut varier dans la gamme des vitesses annoncées sur la base de la qualité du signal entre le point d'accès et le client, et de la vitesse à laquelle les trames de diffusion ou de multidiffusion sont envoyées. Lorsque le point d'accès envoie une trame de diffusion à une station en utilisant les vitesses par défaut, le champ indique 1 Mbit/s pour les radios 2,4 GHz et 6 Mbit/s pour les radios 5 GHz. Les clients non actifs sont les plus susceptibles de signaler des vitesses par défaut faibles.

- **Signal** : puissance du signal de radiofréquence (RF) reçu du point d'accès par le client WLAN. Cette valeur est appelée RSSI (Received Signal Strength Indication) et se situe entre 0 et 100.
- **Total reçu** : nombre total de paquets reçus par le client WLAN au cours de la session actuelle.
- **Total transmis** : nombre total de paquets transmis au client WLAN au cours de cette session.
- **Taux d'erreurs** : pourcentage d'abandons de trames au cours de la transmission sur ce point d'accès.

Pour trier les informations affichées dans les tableaux selon un indicateur spécifique, cliquez sur l'étiquette de la colonne qui déterminera le tri. Par exemple, si vous souhaitez classer les lignes du tableau en fonction de la puissance du signal, cliquez sur l'étiquette de colonne Signal.

Gestion des canaux

La page Gestion des canaux affiche les attributions actuelles et prévues des canaux aux périphériques WAP d'un cluster à configuration de point unique.

Lorsque la gestion des canaux est activée, le point d'accès attribue automatiquement les canaux radio utilisés par les périphériques WAP dans une grappe à configuration de point unique. L'attribution automatique des canaux réduit les interférences mutuelles des périphériques du cluster (ou les interférences avec d'autres périphériques WAP extérieurs au cluster) et optimise la bande passante Wi-Fi afin d'assurer une communication efficace sur le réseau sans fil.

La fonction d'attribution automatique des canaux est désactivée par défaut. L'état de la fonction de gestion des canaux (activé ou désactivé) est propagé aux autres périphériques du cluster à configuration de point unique.

À un intervalle défini, le gestionnaire des canaux (c'est-à-dire le périphérique ayant fourni la configuration au cluster) mappe tous les périphériques WAP du cluster avec différents canaux et mesure les niveaux d'interférence des membres du cluster. Si des interférences importantes sont détectées entre les canaux, le gestionnaire de canaux réattribue automatiquement certains ou tous les périphériques à d'autres canaux à l'aide d'un algorithme d'efficacité (ou d'une stratégie de canaux automatisée). Si le gestionnaire de canaux détermine qu'un changement est nécessaire, les informations de réattribution sont envoyées à tous les membres du cluster. Un message Syslog indiquant également le périphérique d'émission et les nouvelles et anciennes attributions des canaux est généré.

Configuration et affichage des attributions des canaux pour les membres de la configuration de point unique

Pour configurer et afficher les attributions de canaux pour les membres de la configuration de point unique :

ÉTAPE 1 Cliquez sur **Configuration de point unique** > **Gestion des canaux** dans le volet de navigation.

La page Gestion des canaux affiche les attributions de canaux de tous les périphériques WAP du cluster et vous permet d'interrompre ou de démarrer la gestion automatique des canaux. Les paramètres avancés vous permettent de modifier le potentiel de réduction des interférences qui entraîne la réattribution des canaux, de modifier le calendrier des mises à jour automatiques et de reconfigurer l'ensemble de canaux utilisé pour l'attribution.

ÉTAPE 2 Pour lancer l'attribution automatique des canaux, cliquez sur **Démarrer**.

La gestion des canaux remplace le comportement par défaut du cluster qui consiste à synchroniser les canaux radio de tous les périphériques WAP membres du cluster. Lorsque la gestion des canaux est activée, le canal radio n'est pas synchronisé entre le cluster et les autres périphériques.

Lorsque l'attribution automatique des canaux est activée, le gestionnaire de canaux mappe régulièrement les canaux radio utilisés par les périphériques WAP d'un cluster à configuration de point unique et réattribue les canaux, le cas échéant, pour réduire les interférences entre les membres du cluster ou avec les périphériques extérieurs au cluster. La stratégie de canaux radio est définie automatiquement sur le mode statique et l'option **Automatique** n'est pas disponible pour le champ **Canal** de la page Technologie sans fil > Radio.

Reportez-vous à la section Affichage des attributions de canaux et configuration des verrouillages pour obtenir des informations sur les attributions de canaux actuelles et proposées.

ÉTAPE 3 Pour interrompre l'attribution automatique des canaux, cliquez sur **Arrêter**.

Aucun mappage de l'utilisation des canaux ni aucune réattribution de ceux-ci ne sont effectués. Seules les mises à jour manuelles affectent l'attribution des canaux.

Affichage des attributions de canaux et configuration des verrouillages

Lorsque la gestion des canaux est activée, la page affiche le tableau Attributions actuelles des canaux et le tableau Attributions proposées des canaux.

Tableau Attributions actuelles des canaux

Le tableau Attributions actuelles des canaux affiche la liste de tous les périphériques WAP du cluster à configuration de point unique par adresse IP.

Il indique les informations suivantes sur les attributions de canaux actuelles.

- **Emplacement** : emplacement physique du périphérique.
- **Adresse IP** : adresse IP du point d'accès.
- **Radio sans fil** : adresse MAC de la radio.
- **Bande** : bande de diffusion du point d'accès.
- **Canal** : canal radio sur lequel le point d'accès diffuse actuellement.
- **Verrouillé** : force le point d'accès à rester sur le canal actuel.

- **Statut** : état de la radio sans fil du périphérique. (Pour les périphériques WAP disposant de plusieurs radios sans fil, chaque radio est indiquée sur une ligne distincte du tableau.) L'état de la radio est soit Active (opérationnelle), soit Inactive (non opérationnelle).

Lorsqu'elles sont sélectionnées pour un point d'accès, les stratégies de gestion automatique des canaux ne réattribuent pas les périphériques WAP à un autre canal dans le cadre de la stratégie d'optimisation. Les périphériques WAP dont les canaux sont verrouillés sont considérés comme immuables dans la stratégie de gestion.

Cliquez sur **Enregistrer** pour mettre à jour le paramètre Verrouillé. Le canal des périphériques verrouillés est le même dans le tableau Attributions actuelles des canaux et le tableau Attributions proposées des canaux. Les périphériques verrouillés conservent leurs canaux actuels.

Tableau Attributions proposées des canaux

Le tableau Attributions proposées des canaux affiche les canaux proposés qui seront attribués à chaque périphérique WAP lors de la prochaine mise à jour. Les canaux verrouillés ne sont pas réattribués ; l'optimisation de la distribution des canaux entre les périphériques tient compte du fait que les périphériques verrouillés doivent rester sur leurs canaux actuels. Les périphériques WAP non verrouillés peuvent être attribués à des canaux différents de ceux qu'ils utilisaient auparavant, selon les résultats de la stratégie.

Pour chaque périphérique WAP de la configuration de point unique, le tableau Attributions proposées des canaux indique l'emplacement, l'adresse IP et la radio sans fil, de la même manière que le tableau Attributions actuelles des canaux. Il affiche également le Canal proposé, c'est-à-dire le canal radio auquel le périphérique WAP devrait être réattribué lors de l'application de la stratégie.

Configuration des paramètres avancés

La zone Paramètres avancés vous permet de personnaliser et de planifier la stratégie de canaux de la configuration de point unique.

Par défaut, les canaux sont réattribués automatiquement toutes les heures, à condition que les interférences puissent être réduites d'au moins 25 pour cent. Les canaux sont réattribués même si le réseau est occupé. Les paramètres par défaut sont conçus pour servir la plupart des scénarios qui vous obligeraient à mettre en œuvre la gestion des canaux.

Vous pouvez modifier les paramètres avancés pour configurer les options suivantes :

- **Modifier les canaux en cas de réduction des interférences d'au moins** : pourcentage minimal de réduction des interférences qu'une stratégie proposée doit atteindre pour être appliquée. La valeur par défaut est 75 pour cent. Choisissez le pourcentage souhaité entre 5 et 75 pour cent dans le menu déroulant. L'utilisation de ce paramètre vous permet de définir un seuil de gain d'efficacité relatif à la réattribution des canaux pour éviter une interruption trop fréquente du réseau alors que le gain d'efficacité est minime.

  Par exemple, si les interférences des canaux doivent être réduites de 75 pour cent et que les attributions de canaux proposées permettent de réduire les interférences de seulement 30 pour cent, alors la réattribution n'est pas effectuée. Cependant, si vous réglez le gain minimal sur 25 pour cent et cliquez sur **Enregistrer**, la stratégie de canaux proposée sera mise en œuvre et les canaux seront réattribués selon les besoins.

- **Rechercher un meilleur jeu de paramètres de canaux à intervalle de** : calendrier des mises à jour automatiques. Une plage d'intervalles allant de 30 minutes à 6 mois est proposée.

  La valeur par défaut est de 1 heure, ce qui signifie que l'utilisation des canaux est réévaluée et que le plan de canal résultant est appliqué toutes les heures.

Si vous modifiez ces paramètres, cliquez sur **Enregistrer**. Les modifications sont enregistrées dans la configuration active et la configuration initiale.

Voisinage sans fil

La page Voisinage sans fil affiche jusqu'à 20 périphériques par radio dans la plage de chaque radio sans fil au sein du cluster. (Par exemple, si un périphérique WAP possède deux radios sans fil, 40 périphériques s'affichent pour ce périphérique.) La page Voisinage sans fil effectue également une distinction entre les membres et les non membres du cluster.

La page Voisinage sans fil peut vous aider à effectuer les opérations suivantes :

- détecter et localiser les périphériques inattendus (ou non autorisés) dans un domaine sans fil, de telle sorte que vous puissiez entreprendre des actions visant à limiter les risques associés ;
- vérifier les attentes en matière de couverture. En évaluant quels périphériques WAP sont visibles et à quelle puissance de signal à partir des

autres périphériques, vous pouvez vérifier que le déploiement satisfait vos objectifs de planification ;

- détecter les défaillances. Les modifications inattendues dans le modèle de couverture apparaissent de manière évidente grâce au système de couleurs.

Pour afficher les périphériques voisins, sélectionnez **Configuration de point unique** > **Voisinage sans fil**. Pour afficher l'ensemble des périphériques détectés au cours d'une même configuration de point unique, accédez à l'interface Web d'un membre et sélectionnez **Technologie sans fil** > **Détection de point d'accès non autorisé** dans le volet de navigation.

Pour chaque point d'accès voisin, les informations suivantes sont affichées :

- **Afficher les points d'accès voisins** : sélectionnez l'une des cases d'option suivantes pour modifier la vue :
  - **Dans la grappe** : affiche uniquement les périphériques WAP voisins qui sont membres du cluster.
  - **Pas dans la grappe** : affiche uniquement les périphériques WAP voisins qui ne sont pas membres du cluster.
  - **Les deux** : affiche tous les périphériques WAP voisins (membres et non membres du cluster).

REMARQUE : Dans le cas d'un point d'accès détecté qui est également membre d'une grappe, seuls les SSID du point d'accès virtuel par défaut (VAP0) s'affichent avec l'option Dans la grappe. Les points d'accès virtuels non définis par défaut sur le point d'accès s'affichent avec l'option Pas dans la grappe.

- **Cluster** : la liste présente en haut du tableau affiche les adresses IP de l'ensemble des périphériques WAP qui appartiennent au même cluster. (Cette liste est identique à la liste des membres figurant à la page **Configuration de point unique** > **Points d'accès**.)

  S'il n'y a qu'un seul périphérique WAP dans le cluster, une seule colonne d'adresses IP s'affiche, indiquant que le périphérique WAP est groupé avec lui-même.

  Vous pouvez cliquer sur une adresse IP pour afficher plus de détails sur un périphérique WAP particulier.

- **Voisins** : les périphériques qui sont voisins d'un ou plusieurs périphériques en cluster sont répertoriés dans la colonne de gauche par SSID (nom de réseau).

Un périphérique détecté en tant que voisin peut également être lui-même membre du cluster. Les voisins qui sont aussi des membres de cluster sont toujours affichés en haut de la liste avec une barre épaisse et un indicateur d'emplacement.

Les barres de couleur situées à droite de chaque périphérique WAP dans la liste Voisins représentent la puissance du signal de chaque périphérique WAP voisin, tel que détecté par le membre de cluster dont l'adresse IP est affichée en haut de la colonne. Si vous passez le pointeur de la souris sur les barres, un nombre représentant la puissance en décibels (dB) apparaît.

Affichage des détails d'un membre de la configuration de point unique

Pour afficher les détails relatifs à un membre du cluster, cliquez sur l'adresse IP d'un membre en haut de la page.

Les détails suivants du périphérique apparaissent en dessous de la liste Voisins.

- **SSID** : identificateur d'ensemble de services du point d'accès voisin.
- **Adresse MAC** : adresse MAC du point d'accès voisin.
- **Canal** : canal sur lequel le point d'accès diffuse actuellement.
- **Débit** : débit, en mégabits par seconde, auquel ce point d'accès transmet actuellement. Le débit actuel est toujours l'un des débits spécifiés dans Débits pris en charge.
- **Signal** : puissance du signal radio détecté à partir du point d'accès, mesurée en décibels (dB).
- **Intervalle de balise** : intervalle de balise utilisé par le point d'accès.
- **Ancienneté de la balise** : date et heure de la dernière balise reçue de ce point d'accès.

Mise à niveau du microprogramme de la grappe

La grappe propose une fonctionnalité de mise à niveau centralisée du microprogramme qui réalise la mise à niveau de tous les points d'accès de la grappe à partir du point d'accès dominant (contrôleur de grappe). La mise à niveau du microprogramme de la grappe ne peut être effectuée que depuis le point d'accès dominant.

Sur la page de mise à niveau du microprogramme de la grappe, les périphériques WAP détectés sont répertoriés dans un tableau et les informations suivantes sont affichées :

- **Emplacement** : description de l'emplacement physique du point d'accès.
- **Adresse IP** : adresse IP du point d'accès.
- **Adresse MAC** : adresse MAC (Media Access Control) du point d'accès. Cette adresse correspond à l'adresse MAC du pont (br0) et à l'adresse du périphérique WAP connue des autres réseaux.
- **Version actuelle du microprogramme** : la version actuelle du microprogramme exécuté sur le point d'accès.
- **Statut du transfert du microprogramme** : indique si le téléchargement et la validation du microprogramme dans le membre de la grappe est Aucun/Démarré/Téléchargé/Réussite/Échec/Abandon_admin/Abandon_local/Dap_annulé.
- **Barre de progression du transfert du microprogramme** : affiche la barre de progression lors du téléchargement du microprogramme.

Sélection d'un membre de la grappe à mettre à niveau

Pour sélectionner un membre de la grappe à mettre à niveau :

ÉTAPE 1 Cliquez sur **Configuration de point unique > Mise à niveau du microprogramme de la grappe** dans le volet de navigation.

ÉTAPE 2 Cochez la case du point d'accès à mettre à niveau.

ÉTAPE 3 Cliquez sur **Enregistrer**.

Pour connaître le statut le plus récent de la mise à niveau du microprogramme de la grappe :

Cliquez sur **Actualiser**.

Mise à niveau du microprogramme d'un membre de la grappe via TFTP

Pour mettre à niveau le microprogramme d'un membre de la grappe via TFTP :

ÉTAPE 1 Sélectionnez **Méthode de transfert TFTP**.

ÉTAPE 2 Saisissez un nom (de 1 à 128 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 micrologiciel 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 éléments suivants : espaces, <, >, |, \, : , (,), &, ; , #, ? , *, ainsi que deux points successifs ou plus.

ÉTAPE 3 Saisissez l'**Adresse IPv4 du serveur TFTP**, puis cliquez sur **Démarrer la mise à niveau**.

Mise à niveau via HTTP

Pour effectuer une mise à niveau via HTTP :

ÉTAPE 1 Sélectionnez **Méthode de transfert HTTP**.

ÉTAPE 2 Si vous connaissez le nom du nouveau fichier et le chemin d'accès à celui-ci, saisissez-les dans le champ **Nouvelle image de microprogramme**. Sinon, cliquez sur le bouton **Parcourir** et recherchez le fichier image du microprogramme sur votre réseau.

Le fichier de mise à niveau du micrologiciel 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 **Démarrer la mise à niveau** pour appliquer la nouvelle image de microprogramme.

REMARQUE : L'option **Statut de la mise à niveau globale** présente l'état de la mise à niveau combinée (Non initialisée/En cours/Terminée/Échec/Abandon_admin/Aucune) de tous les membres de la grappe.

Pour arrêter la mise à niveau d'un membre de la grappe depuis le point d'accès dominant :

Cliquez sur **Arrêter la mise à niveau**.

13

Umbrella

Ce chapitre explique comment configurer la fonctionnalité Umbrella sur les périphériques WAP.

Il contient les rubriques suivantes :

- **Présentation de Cisco Umbrella**
- **Configuration d'Umbrella**

Présentation de Cisco Umbrella

Cisco Umbrella est un service de sécurité réseau basé dans le cloud qui fournit des renseignements précieux visant à protéger en temps réel les périphériques des programmes malveillants et autres menaces. Il utilise des méthodes avancées de Big Data et d'exploration des données pour détecter les attaques de manière proactive et assurer un filtrage par catégorie.

Les serveurs Cisco Umbrella résolvent la requête DNS et appliquent des règles de filtrage de sécurité préconfigurées en tenant compte des identités. Ils peuvent ainsi marquer le domaine comme malveillant, et donc bloquer l'accès à la page pour le client, ou comme sécurisé, et renvoyer une adresse IP résolue au client.

Configuration d'Umbrella

Pour configurer la fonctionnalité Umbrella, procédez comme suit :

ÉTAPE 1 Sélectionnez **Umbrella** dans le volet de navigation.

ÉTAPE 2 Configurez les paramètres suivants :

- **Activer** : active ou désactive la fonctionnalité Umbrella sur le périphérique WAP.

- **Clé API** : pour obtenir votre clé API, accédez à votre tableau de bord Umbrella : **Admin**. -> **Clés API**.
- **Clé API secrète** : la clé API secrète s'affiche une fois que vous avez créé votre clé API dans le tableau de bord Umbrella.

REMARQUE

- Toute modification apportée à la clé API, à la clé API secrète et à la balise de périphérique génère un processus de ré-enregistrement pour créer un périphérique réseau.
- **Balise de périphérique (facultatif)** : balise au format texte qui décrit le périphérique ou une propriété d'origine spécifique attribuée au périphérique. Cette balise doit être unique à votre entreprise.
- **Domaines locaux à ignorer (facultatif)** : le point d'accès transfère la requête DNS si celle-ci apparaît dans la liste. Les éléments de la liste doivent être séparés par une virgule, et les domaines peuvent inclure des astérisques (*) comme caractères de remplacement. Par exemple : *.cisco.com.*.
- **DNSCrypt :** indique si la fonctionnalité DNSCrypt est activée.
- **État de l'enregistrement** : les valeurs possibles sont **Opération effectuée**, **Enregistrement en cours** ou **Échec**.

A

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 **Statut et statistiques > Journal**.

Tableau des codes des motifs de désauthentification

Le tableau suivant décrit les 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
6	Trame de classe 2 reçue d'une station non authentifiée
7	Trame de classe 3 reçue d'une station non associée

Code de motif	Signification
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	Désassociation due à la gestion des transitions BSS
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 8
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

B

Pour en savoir plus

Cisco fournit une gamme étendue de ressources pour vous aider, ainsi que votre client, à profiter de tous les avantages du Cisco WAP571/E.

Assistance	
Communauté d'assistance Cisco	www.cisco.com/go/smallbizsupport
Numéros de téléphone du centre d'assistance Cisco Small Business (SBSC)	www.cisco.com/go/sbsc
Assistance et ressources pour entreprises	www.cisco.com/go/smallbizhelp
Informations sur le service d'assistance	www.cisco.com/go/sbs www.cisco.com/go/software (enregistrement/ ouverture de session requis).
Téléchargements de microprogrammes Cisco	www.cisco.com/go/smallbizfirmware Sélectionnez un lien pour télécharger le microprogramme d'un produit Cisco. Aucune connexion n'est requise. Les téléchargements de logiciels et de microprogrammes se rapportant à tous les autres produits Cisco sont disponibles dans la zone de téléchargement de Cisco.com, à l'adresse www.cisco.com/go/software (enregistrement/ ouverture de session requis).
Demandes Open Source Cisco	www.cisco.com/go/smallbiz_opensource_request

Cisco Partner Central (connexion partenaire requise)	www.cisco.com/web/partners/sell/smb
Documentation sur les produits	
Guide d'administration et de démarrage rapide du point d'accès Cisco WAP571/E bibande sans fil AC/N Premium avec PoE	http://www.cisco.com/go/500_wap_resources