Configuration des ports avec des RLAN dans un réseau CBW

Objectif

L'objectif de cet article est de créer un réseau RLAN (Remote Local Area Network) et d'attribuer des ports et des groupes de points d'accès sur un point d'accès principal (AP) Cisco Business Wireless (CBW).

Périphériques pertinents | Version du logiciel

- 145AC (fiche technique) | 10.4.1.0 (Télécharger la dernière version)
- 240AC (fiche technique) | 10.4.1.0 (Télécharger la dernière version)

Introduction

Les points d'accès CBW sont basés sur 802.11 a/b/g/n/ac (phase 2), avec antennes internes. Ces points d'accès prennent en charge la dernière norme 802.11ac de phase 2 pour des réseaux plus performants, plus accessibles et plus denses.

Les points d'accès 145AC et 240AC référencés dans cet article peuvent être utilisés dans un réseau traditionnel ou maillé. Cet article utilise l'équipement pour un réseau sans fil traditionnel.

Si vous souhaitez en savoir plus sur les bases des réseaux maillés, consultez Cisco Business : Bienvenue dans la section Wireless Mesh Networking.

Si vous préférez effectuer la configuration des ports dans un réseau maillé, lisez Configurer les ports Ethernet du point d'accès sans fil professionnel Cisco en mode maillé.

Dans un réseau sans fil traditionnel, un RLAN est utilisé pour authentifier les clients filaires à l'aide du point d'accès principal. Une fois que le client filaire a réussi à joindre le point d'accès principal, les ports LAN commutent le trafic entre les modes de commutation central ou local. Le trafic provenant du client filaire est traité comme trafic client sans fil.

Le RLAN envoie la demande d'authentification pour authentifier le client filaire. L'authentification du client filaire dans un RLAN est similaire au client sans fil authentifié central.

Si vous n'avez besoin que d'un seul VLAN, vous n'avez pas besoin de configurer un RLAN. Un RLAN est fourni sur le point d'accès par défaut, le VLAN natif 1. Il dispose d'une sécurité ouverte et tous les ports sont affectés à ce RLAN par défaut.

Si vous ne connaissez pas les termes utilisés, consultez Cisco Business : Glossaire des nouveaux termes.

Les RLAN ne fonctionnent pas dans un réseau maillé. Le maillage n'est pas activé par défaut, donc, à moins que vous n'ayez précédemment exécuté le point d'accès en mode maillage, vous êtes paramétré pour passer.

Configuration Steps

Cette section vous propose des conseils pour les débutants.

Connexion

Connectez-vous à l'interface utilisateur Web du point d'accès principal. Pour ce faire, ouvrez un navigateur Web et saisissez https://ciscobusiness.cisco. Vous pouvez recevoir un avertissement avant de continuer. Entrez vos informations d'identification.Vous pouvez également accéder au point d'accès principal en entrant https://[adresse IP] (du point d'accès principal) dans un navigateur Web.

Conseils

Si vous avez des questions sur un champ de l'interface utilisateur, recherchez une info-bulle qui ressemble à ceci : 

Trouver l'icône Développer le menu principal pose problème ?

Accédez au menu situé à gauche de l'écran. Si le bouton de menu ne s'affiche pas, cliquez sur cette icône pour ouvrir le menu de la barre latérale. 

Application Cisco Business

Ces périphériques disposent d'applications complémentaires qui partagent certaines fonctions de gestion avec l'interface utilisateur Web. Toutes les fonctionnalités de l'interface utilisateur Web ne seront pas disponibles dans l'application.

Télécharger l'application iOS Télécharger l'application Android

Forum aux questions

Si vous avez encore des questions sans réponse, vous pouvez consulter notre foire aux questions . Forum aux questions

Étape 1

Mettez le point d'accès sous tension s'il n'est pas déjà sous tension. Vérifiez l'état des voyants. Lorsque le voyant DEL clignote en vert, passez à l'étape suivante.

Le démarrage du point d'accès prend entre 8 et 10 minutes. Le voyant clignote en vert sur plusieurs motifs, alternant rapidement en vert, rouge et orange avant de revenir au vert. Il peut y avoir de petites variations dans l'intensité et la teinte des DEL.

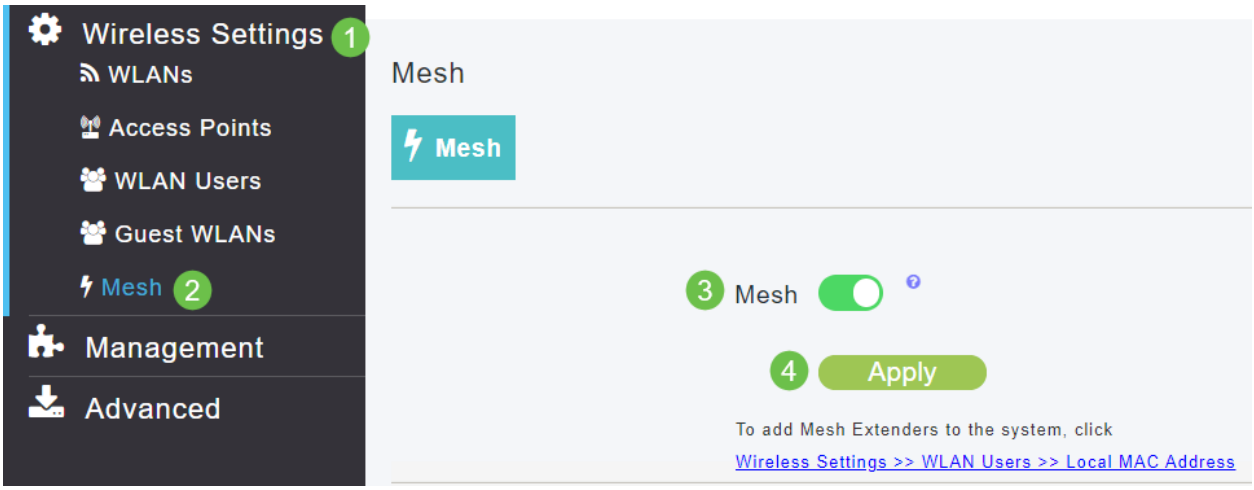
Étape 2

Connectez-vous à l'interface utilisateur Web du point d'accès principal. Ouvrez un navigateur Web et entrez https://ciscobusiness.cisco Vous pouvez recevoir un avertissement avant de continuer. Entrez dans vos informations d'identification.

Vous pouvez également y accéder en entrant l'adresse IP du point d'accès principal dans un navigateur Web.

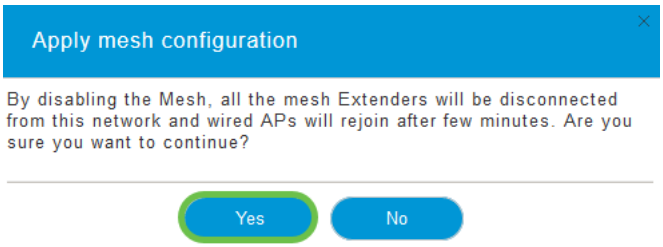
Étape 3

L'AP ne peut pas être en mode maillé pour qu'un RLAN fonctionne. Pour désactiver le mode maillage, accédez à **Wireless Settings > Mesh**. Sélectionnez cette option pour désactiver le maillage. Si votre point d'accès est nouveau ou si vous savez que le mode maillé n'est pas activé, vous pouvez passer à l'étape 7.



Étape 4

Vérifiez que vous souhaitez désactiver le mode maillage en cliquant sur **Oui**.

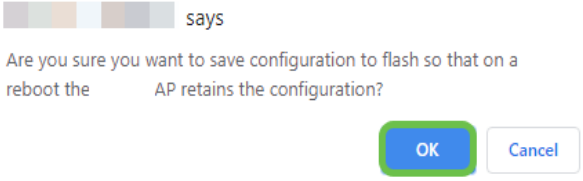


Étape 5

Veillez à enregistrer vos configurations en cliquant sur l'**icône Enregistrer** dans le panneau supérieur droit de l'écran de l'interface utilisateur Web.

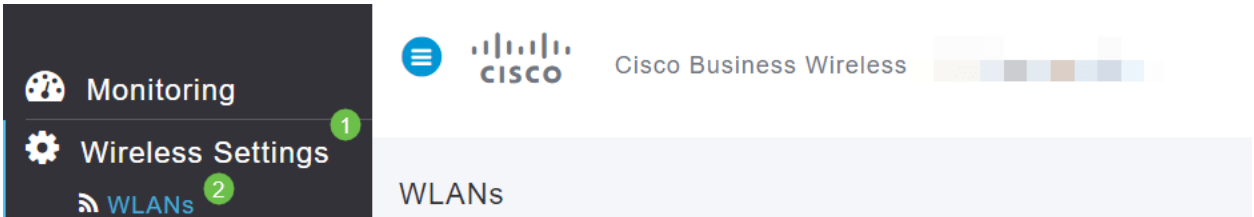
Étape 6

Confirmez l'enregistrement en cliquant sur **OK**. Le point d'accès redémarre. Cela prendra de 8 à 10 minutes.



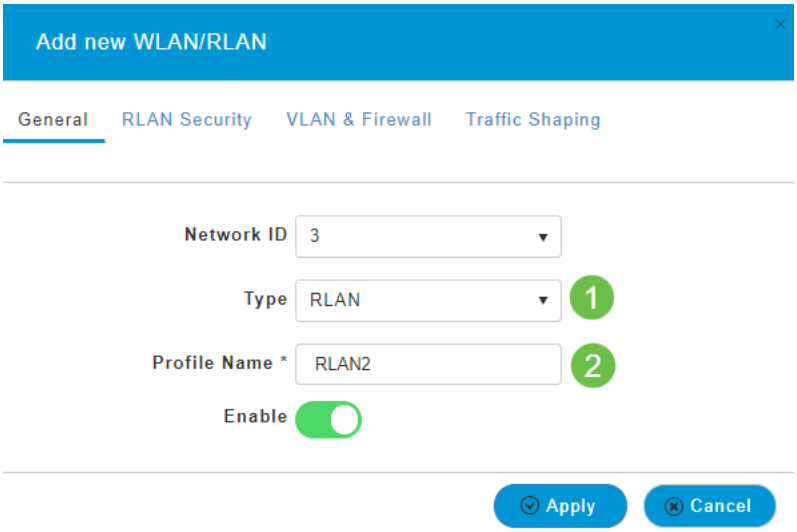
Étape 7

Vous pouvez créer un RLAN en accédant à **Wireless Settings > WLAN**. Sélectionnez ensuite **Ajouter un nouveau WLAN/RLAN**.



Étape 8

Sélectionnez **RLAN**. Créez un nom pour le profil.

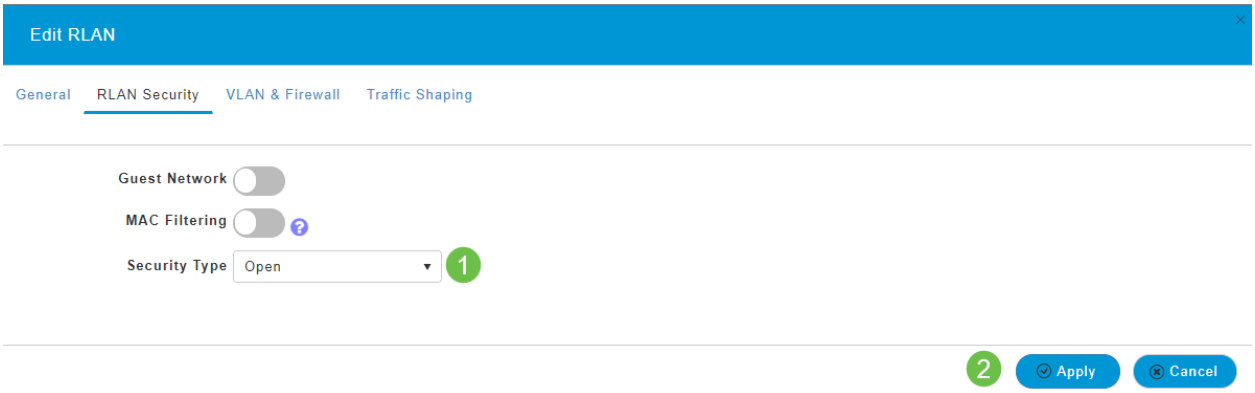


Étape 9 (Utilisation de la sécurité ouverte)

Sous l'onglet *Sécurité RLAN*. Sous *Type de sécurité*, vous pouvez sélectionner *Ouvrir* ou *802.1X*.

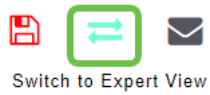
Dans cet exemple, le *type de sécurité* a été laissé comme valeur par défaut.

Cliquez sur Apply. Ceci active automatiquement ce RLAN de sécurité ouvert. Passez à l'étape 11.



Étape 10a (Utilisation de la sécurité 802.1X)

Pour configurer Radius externe, un serveur Radius doit être configuré dans *les comptes Admin* sous *RADIUS* dans *Expert View*. Cliquez sur l'**icône de flèche** dans le menu supérieur droit de l'interface utilisateur Web pour passer à *Expert View*. Pour plus d'informations sur la configuration d'un serveur RADIUS, consultez Radius

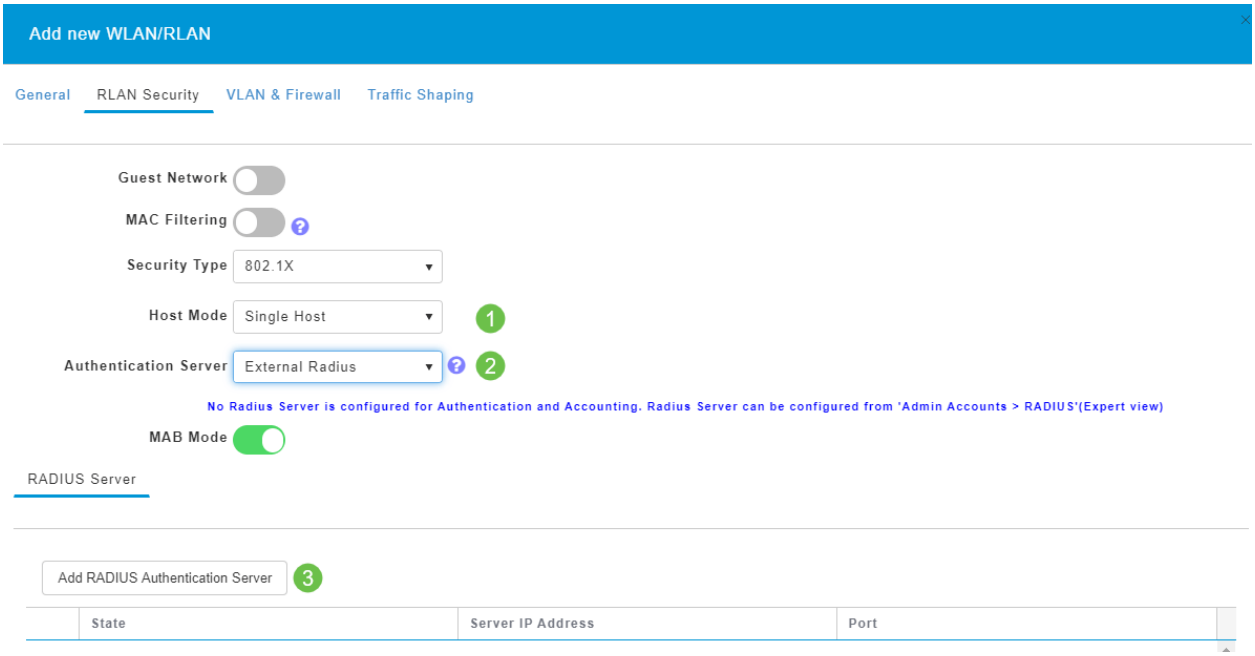


Étape 10b (Utilisation de la sécurité 802.1X)

Si vous choisissez 802.1X pour le type de sécurité, d'autres options doivent être sélectionnées. Vous devez sélectionner les éléments suivants :

- *Mode hôte - Hôte unique* ou *multihôte*
- *Serveur d'authentification - Radius externe* ou *AP*

- *Mode MAB - Activé* ou *Désactivé.* Pour ajouter des adresses MAC, suivez les instructions de l'étape suivante.

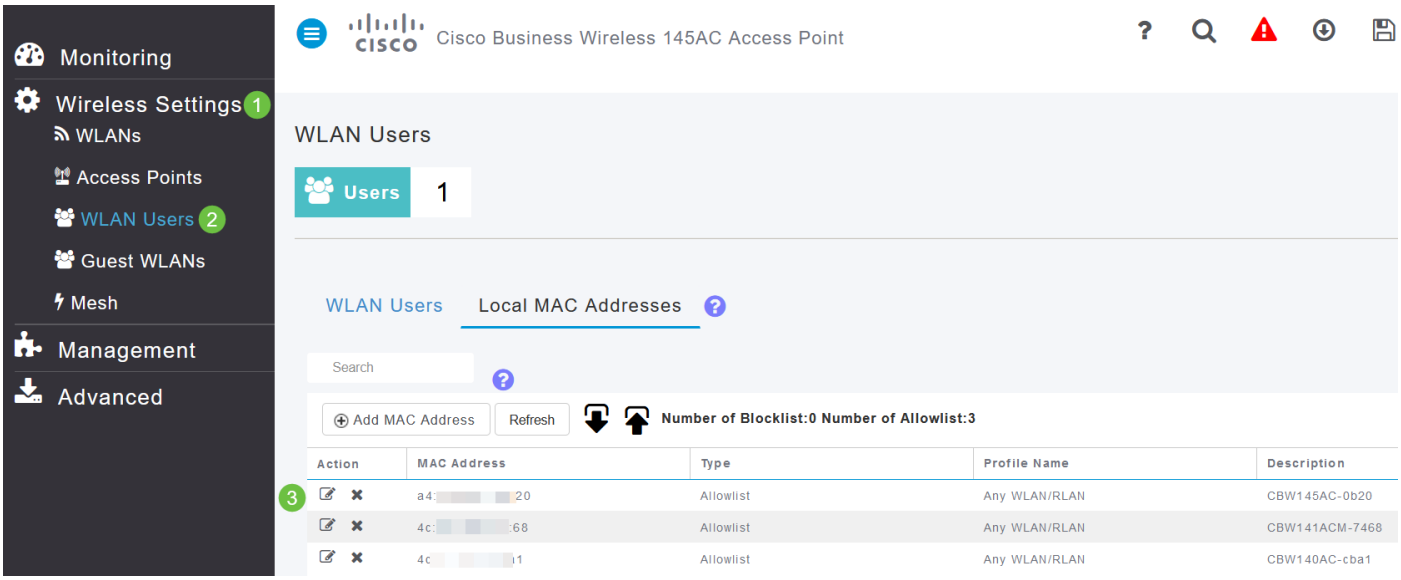


Étape 11 (facultative)

Le mode MAB (MAC Authentication Bypass) signifie que si vous avez une adresse MAC répertoriée sous Utilisateurs WLAN, le périphérique n'a pas besoin de s'authentifier. Les adresses MAC répertoriées peuvent contourner l'authentification pour obtenir un accès automatique au réseau ou un refus automatique. Cela serait utile dans le cas où un téléphone IP est branché sur un port PoE d'un commutateur.

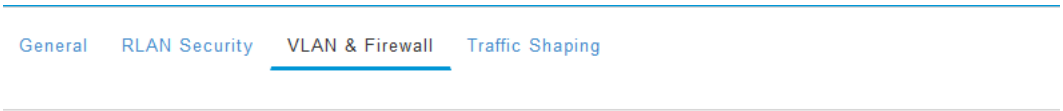
Vous pouvez étiqueter chaque adresse MAC de deux manières :

1. *Autorisé* - Le périphérique reçoit un accès automatique.
2. *Blocklist* : l'accès au périphérique sera automatiquement refusé.



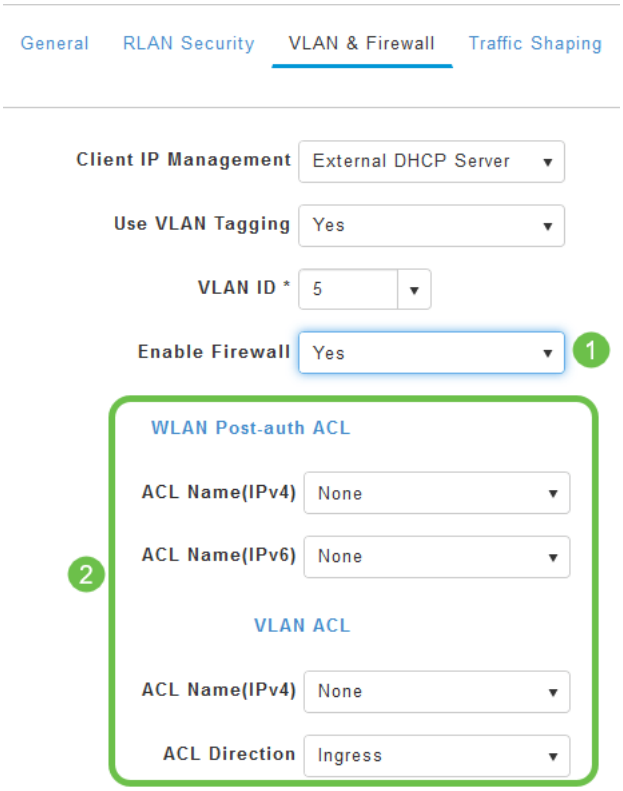
Étape 12

Sous l'onglet *VLAN & Firewall*, vous pouvez sélectionner Utiliser l'*étiquetage VLAN* et sélectionner un numéro *d'ID VLAN*.



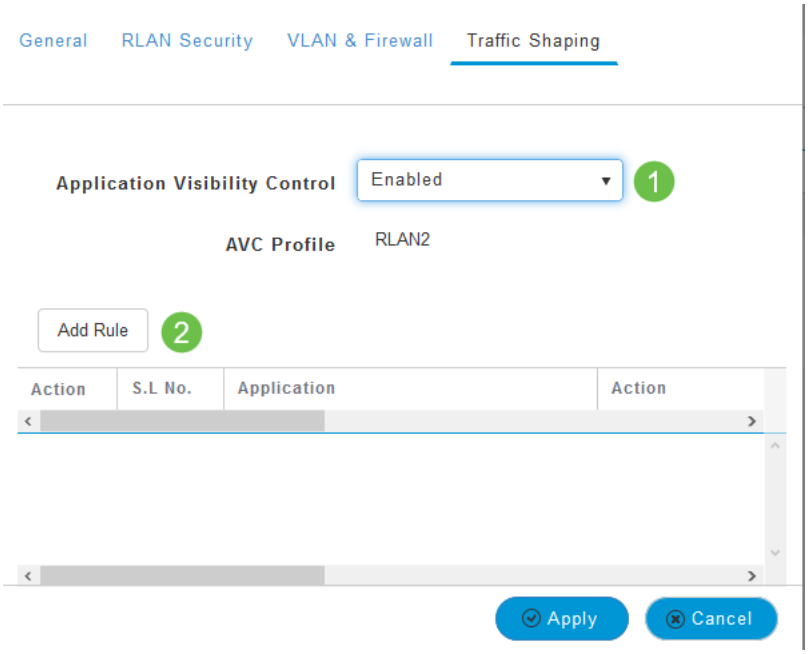
Étape 13 (facultative)

Vous pouvez sélectionner **Activer le pare-feu** si vous souhaitez configurer des *listes de contrôle d'accès (ACL)* qui vous permettent d'autoriser ou de rejeter l'accès pour des adresses IP ou des VLAN spécifiques. Cette option est utilisée si une personne se connecte au périphérique du port réseau pour se connecter au réseau.



Étape 14 (facultative)

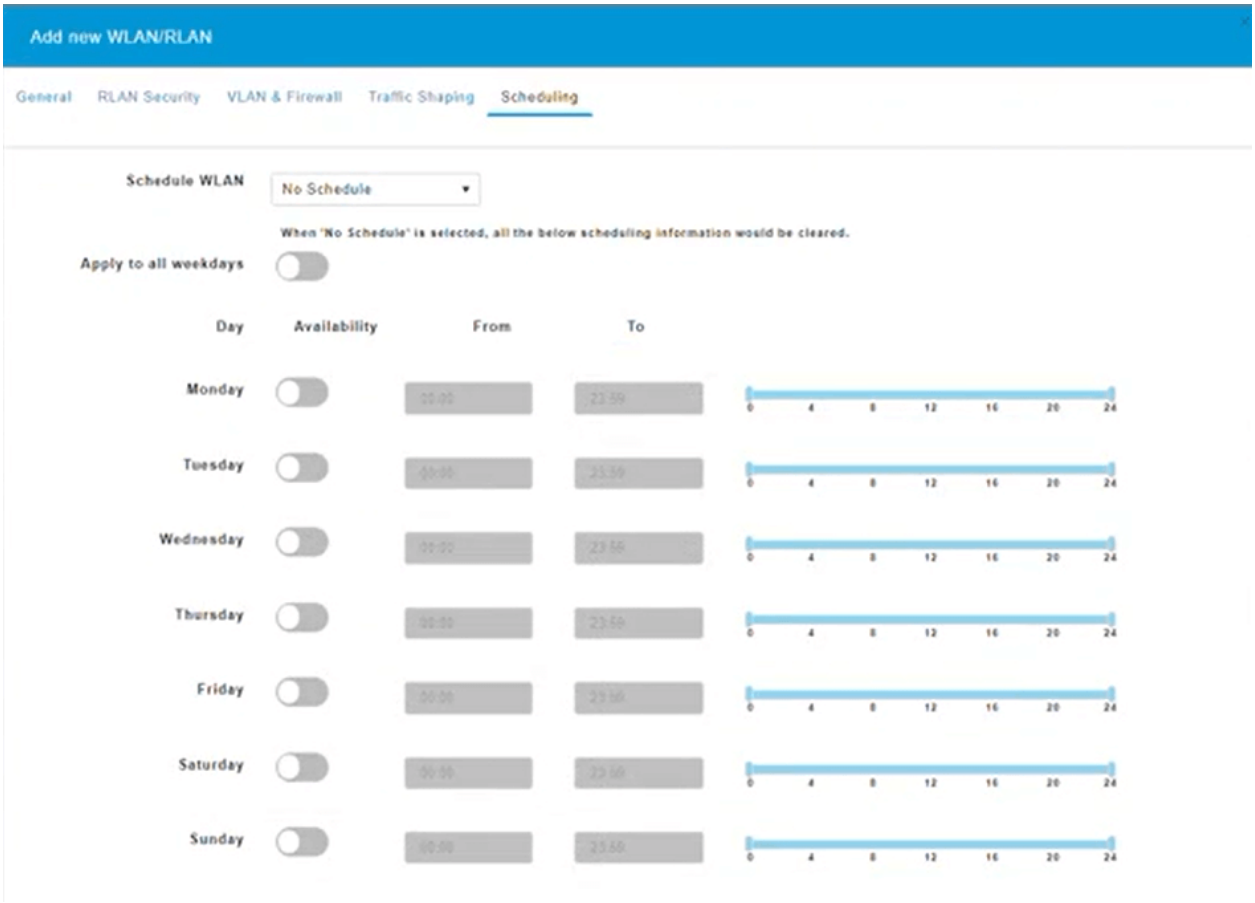
Sous l'onglet *Formatage du trafic*, vous pouvez configurer le formatage du trafic en activant **le contrôle de visibilité des applications**. Cela définit la hiérarchisation du trafic.



Étape 15 (facultative)

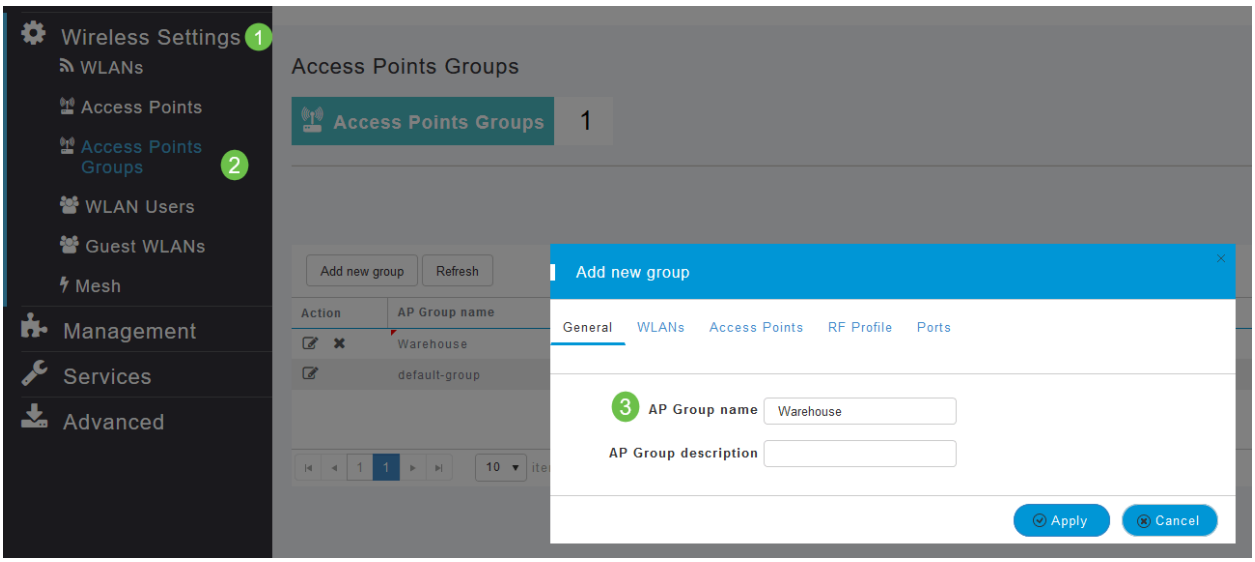
Sous l'onglet *Planification*, vous pouvez sélectionner une planification. Cela définit les heures

auxquelles le port pourra être connecté au réseau.



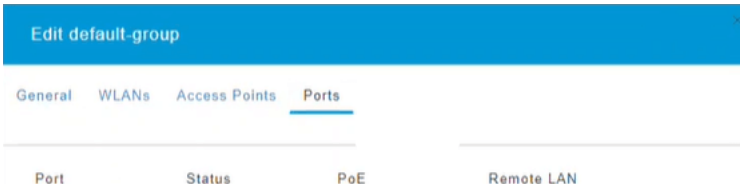
Étape 16 (facultative)

Maintenant que le RLAN est créé, vous pouvez accéder à **Wireless Settings > Access Point Groups**. Vous pouvez ajouter ou modifier des groupes. Pour afficher cet écran, vous devez être dans *Expert View*, que vous avez sélectionné à l'étape 10a.



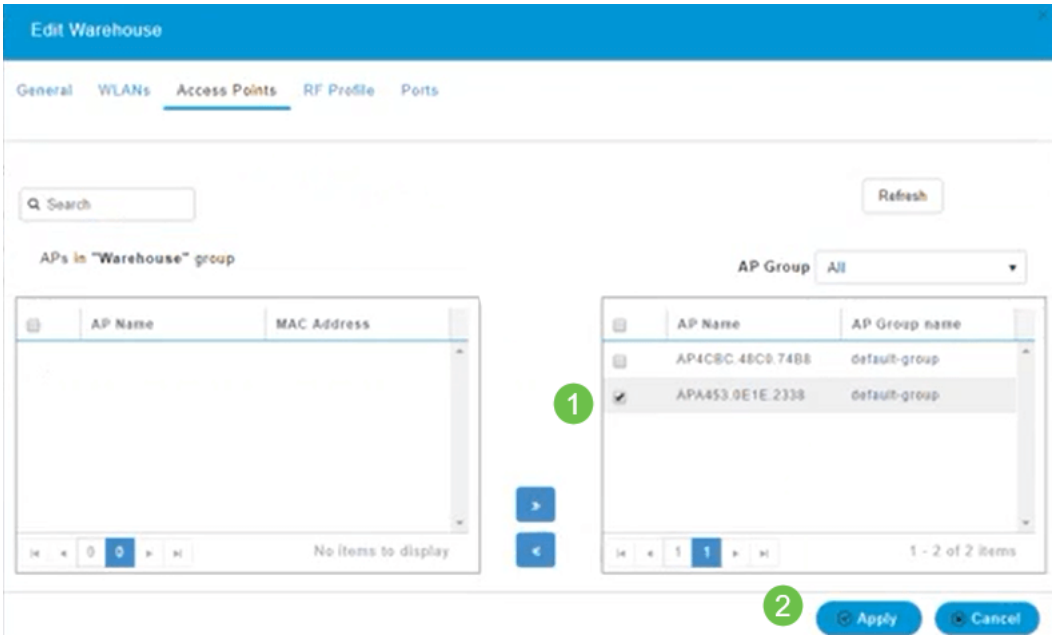
Étape 17

Sous l'onglet *Ports*, vous pouvez affecter les ports du point d'accès à des LAN distants spécifiques.



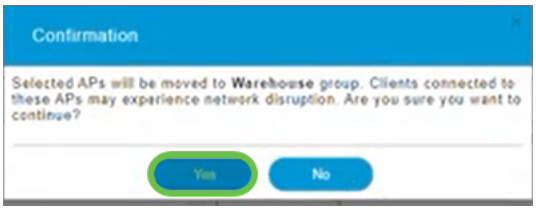
Étape 18

Sous l'onglet *Points d'accès*, vous devez affecter un point d'accès particulier à ce groupe de points d'accès. Cliquez sur Apply.



Étape 19

Sélectionnez **Oui** pour confirmer.

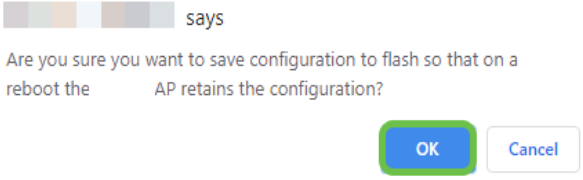


Étape 20

Veillez à enregistrer vos configurations en cliquant sur l'**icône Enregistrer** dans le panneau supérieur droit de l'écran de l'interface utilisateur Web.

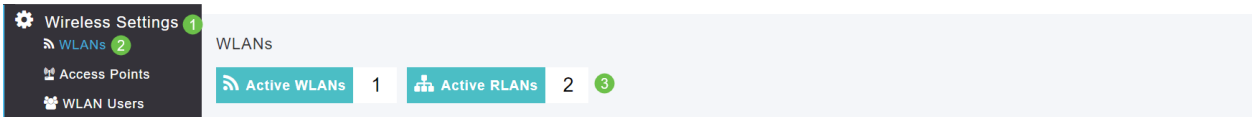
Étape 21

Confirmez l'enregistrement en cliquant sur **OK**. Le point d'accès redémarre. Cela prendra de 8 à 10 minutes.



Afficher le RLAN

Pour afficher le RLAN que vous avez créé, sélectionnez **Wireless Settings > WLAN**. Le nombre de RLAN actifs est élevé à 2 et le nouveau RLAN est répertorié.

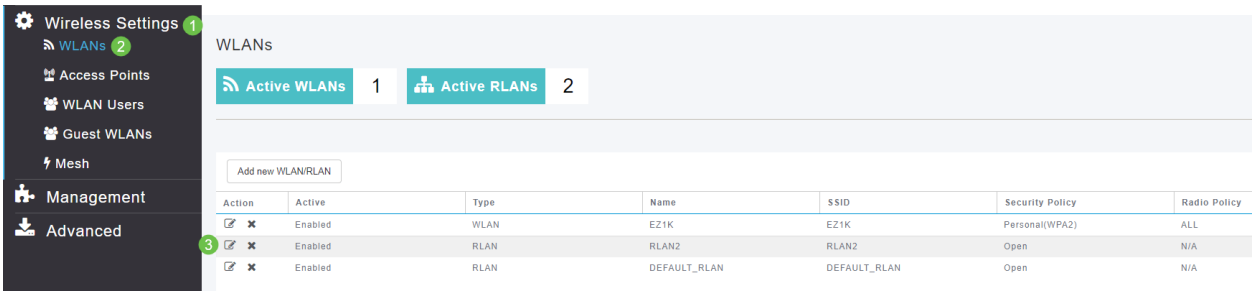


Modifier le RLAN

Lorsque vous cliquez sur **Apply** à la fin de la configuration de votre RLAN, ce dernier est automatiquement activé. Si vous avez besoin de désactiver le RLAN ou d'effectuer d'autres modifications, procédez comme suit.

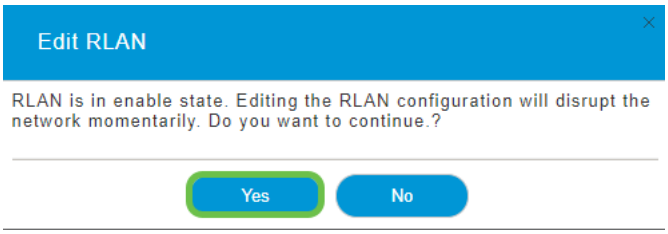
Étape 1

Sélectionnez **Wireless Settings > WLAN**. Cliquez sur l'**icône de modification**.



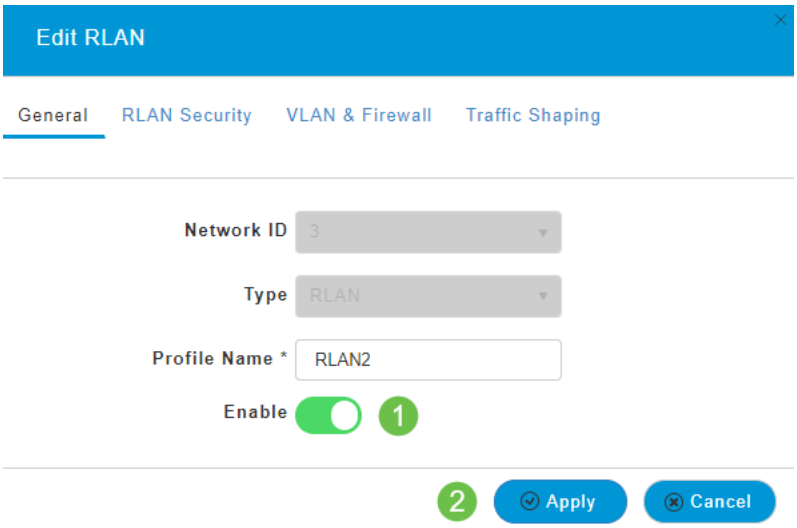
Étape 2

Une fenêtre contextuelle s'affiche pour vous informer que la modification du RLAN perturbera momentanément le réseau. Confirmez que vous voulez continuer en cliquant sur **Oui**.



Étape 3 (Activer/Désactiver)

Dans la fenêtre **Edit WLAN/RLAN**, sous **General**, sélectionnez ***Enabled*** ou ***Disabled*** pour activer/désactiver le RLAN. Cliquez sur Apply.



Étape 4 (Modification d'autres paramètres)

Accédez aux onglets *RLAN Security*, *VLAN & Firewall* ou *Traffic Shaping* si vous devez modifier les paramètres. Cliquez sur **Appliquer** une fois les modifications apportées.

Étape 5

Veillez à enregistrer vos configurations en cliquant sur l'**icône Enregistrer** dans le panneau supérieur droit de l'écran de l'interface utilisateur Web.

Conclusion

Vous avez maintenant créé un RLAN sur votre réseau CBW. Profitez-en et n'hésitez pas à en ajouter si cela répond à vos besoins.

Forum aux questions RADIUS Mise à niveau du micrologiciel RLAN Profilage des applications Profilage client Outils PA principaux Umbrella Utilisateurs WLAN Journalisation Modélisation du trafic Rogues Interféreurs Gestion de la configuration Mode de maillage de configuration de port Bienvenue dans CBW Mesh Networking Réseau invité à l'aide de l'authentification par e-mail et de la comptabilité RADIUS Dépannage Utilisation d'un routeur Draytek avec CBW