Configuration des ports avec des réseaux locaux virtuels dans un réseau CBW

Objectif

L'objectif de cet article est de créer un réseau local distant (RLAN) 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 logicielle

- 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 des antennes internes. Ces points d'accès prennent en charge la dernière norme 802.11ac 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 d'un réseau sans fil traditionnel.

Si vous souhaitez apprendre les bases de la mise en réseau maillé, consultez Cisco Business : Bienvenue dans le réseau maillé sans fil.

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 du trafic client sans fil.

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

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

Si vous n'êtes pas familier avec les termes utilisés, consultez Cisco Business : Glossaire de nouveaux termes.

Les réseaux locaux virtuels ne fonctionnent pas dans un réseau maillé. Le maillage n'est pas activé par défaut, donc à moins que vous ayez précédemment eu l'AP en cours d'exécution en mode maillage, vous êtes défini pour aller.

Configuration Steps

Aide aux débutants

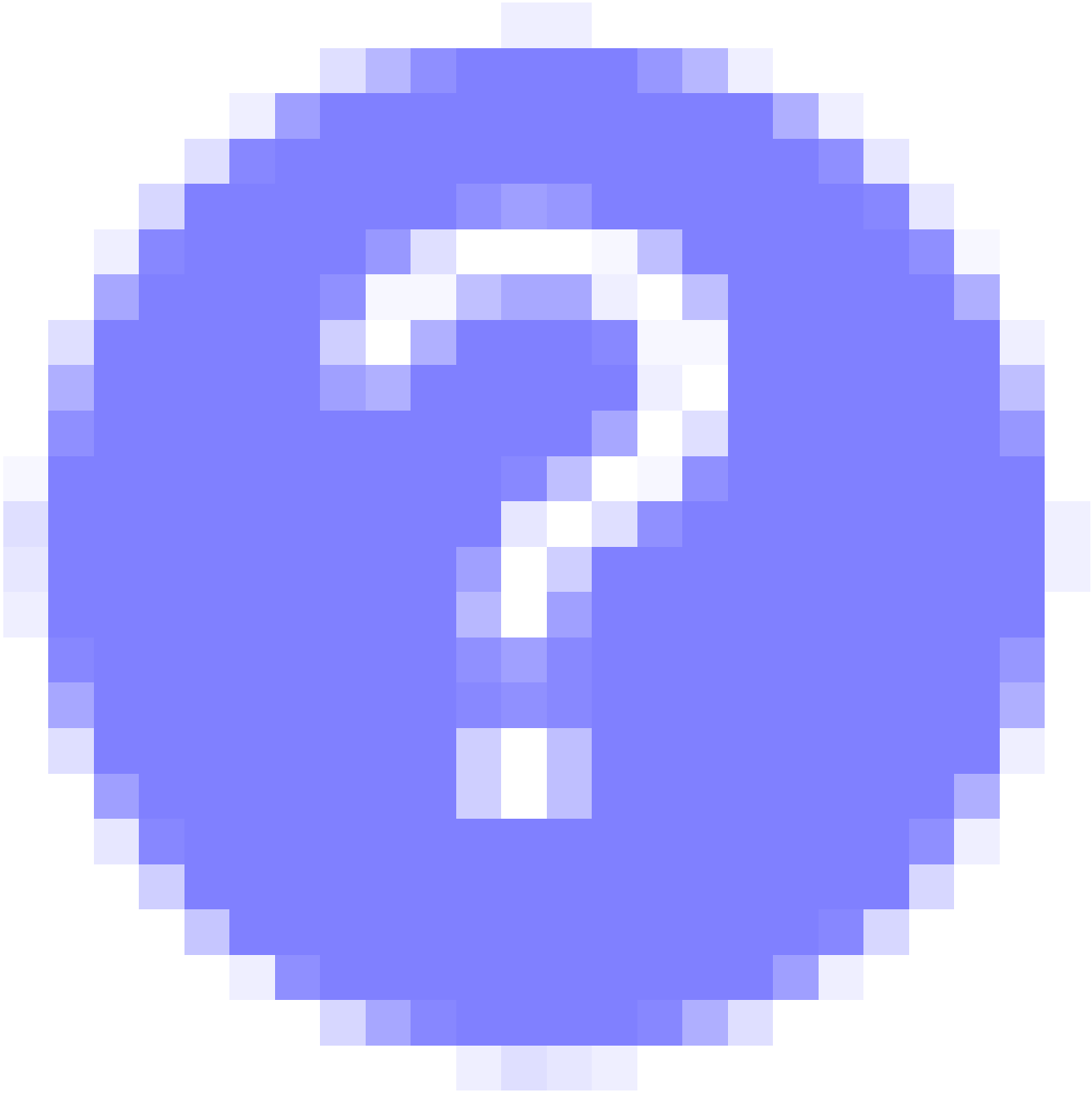
Cette section à bascule présente des conseils pour les débutants.

Connexion en cours

Connectez-vous à l'interface utilisateur Web du point d'accès principal. Pour ce faire, ouvrez un navigateur Web et entrez 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 sur les outils

Si vous avez des questions sur un champ de l'interface utilisateur, recherchez une info-bulle semblable à celle-ci :



Vous ne trouvez pas l'icône Développer le menu principal ?

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



Application professionnelle Cisco

Ces périphériques sont accompagnés d'applications 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 Forum 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 environ 8 à 10 minutes. Le voyant clignote en vert selon plusieurs modèles, alternant rapidement entre le vert, le rouge et l'ambre avant de redevenir vert. Il peut y avoir de petites variations dans l'intensité et la teinte de la couleur des LED.

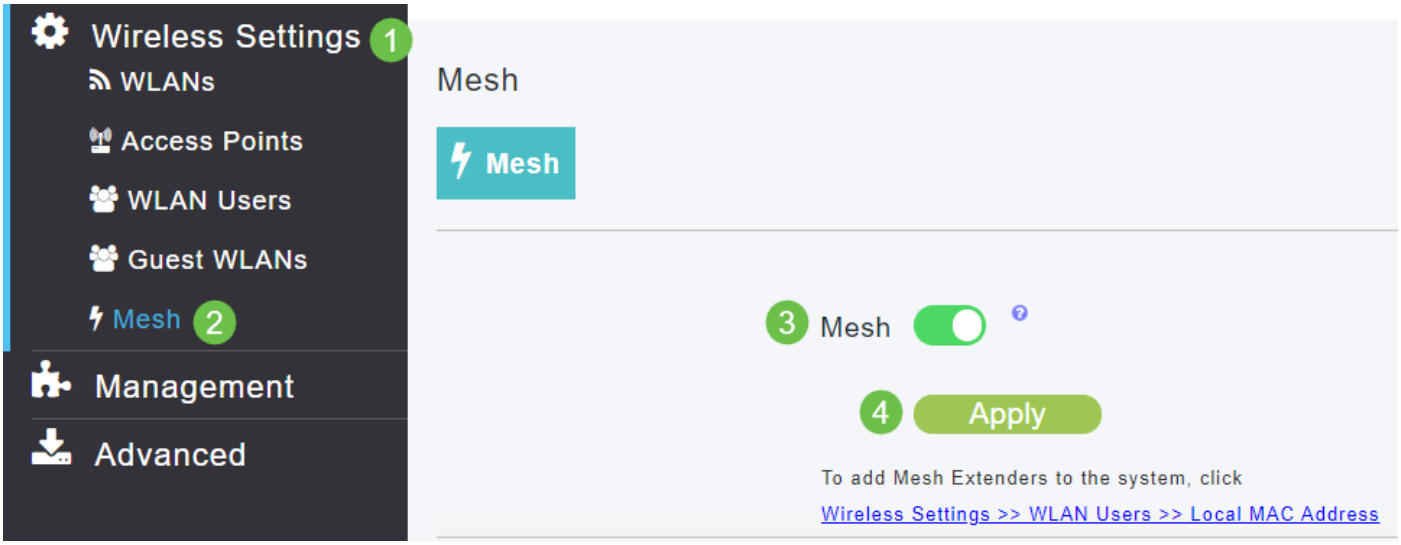
Étape 2

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.

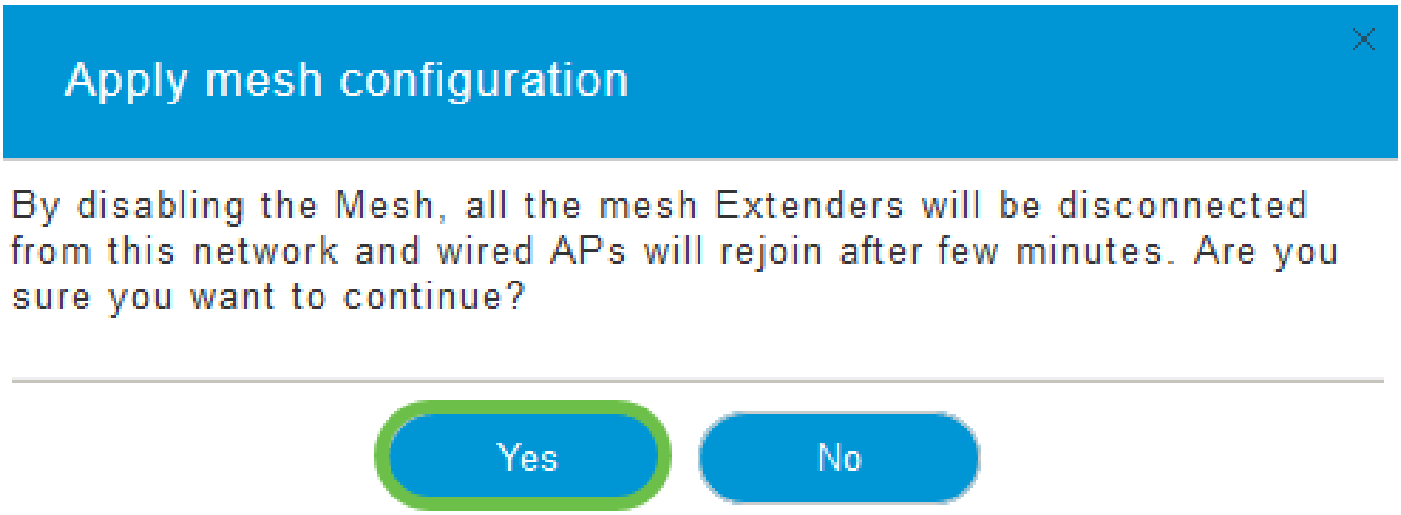
Étape 3

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



Étape 4

Confirmez que vous voulez désactiver le mode maillage en cliquant sur Oui.



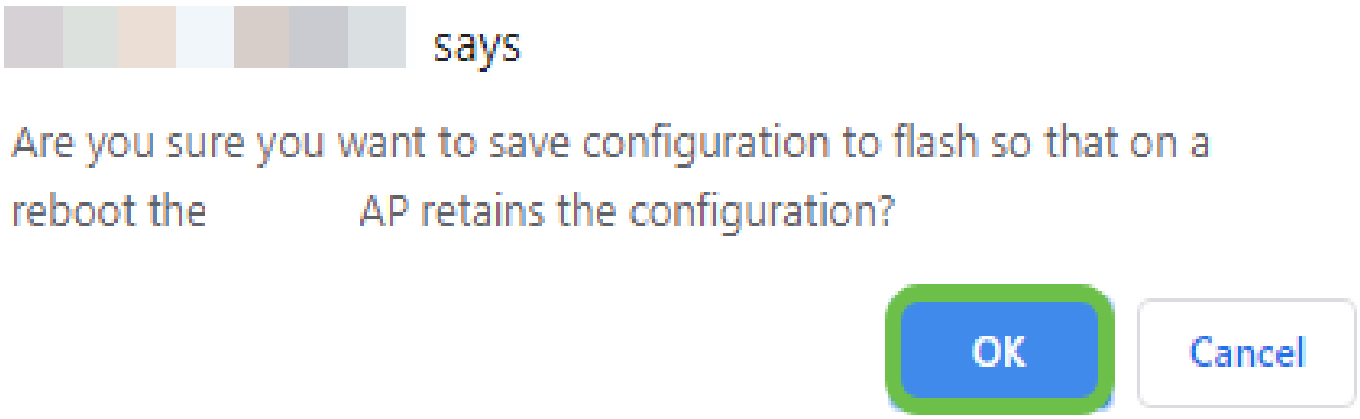
Étape 5

Assurez-vous d'enregistrer vos configurations en cliquant sur l'icône Save dans le panneau supérieur droit de l'écran Web UI.



Étape 6

Confirmez l'enregistrement en cliquant sur OK. Le point d'accès redémarre. Cela prendra entre 8 et 10 minutes.



Étape 7

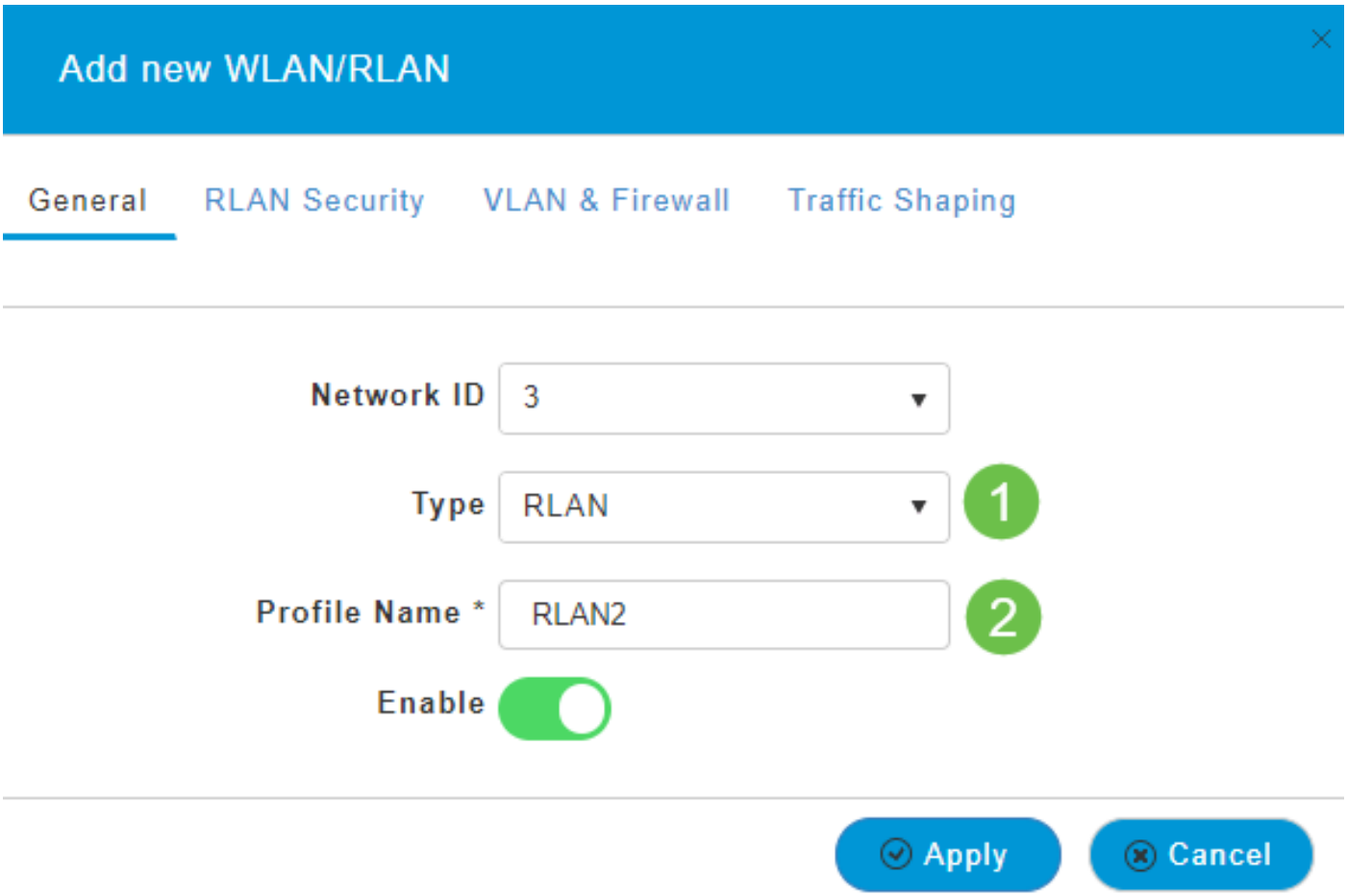
Vous pouvez créer un RLAN en sélectionnant Wireless Settings > WLANs. Sélectionnez ensuite

Add new WLAN/RLAN.



Étape 8

Sélectionnez RLAN. Créez un nom pour le profil.

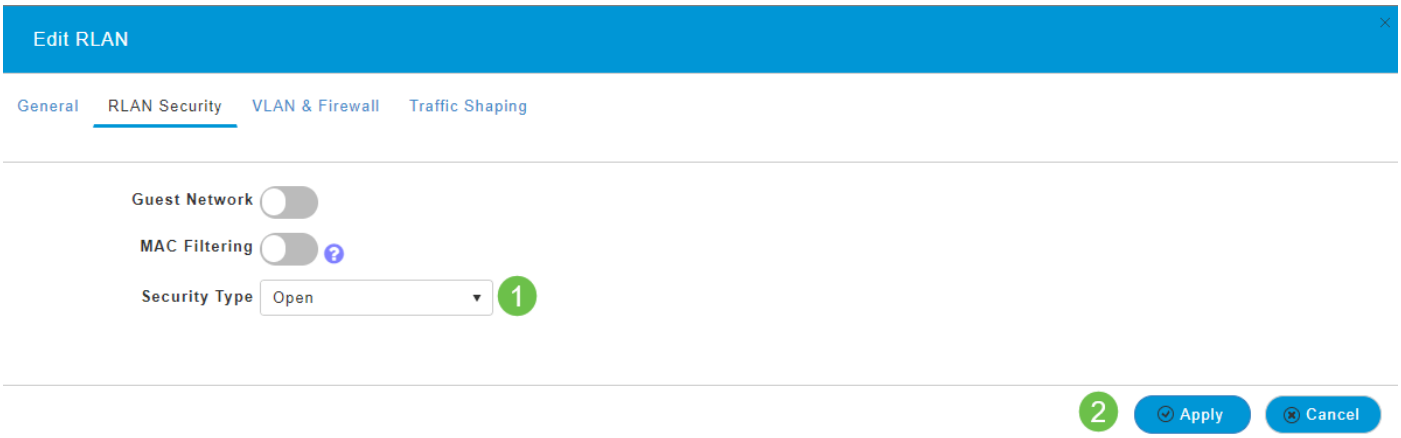


Étape 9 (Utilisation de la sécurité ouverte)

Sous l'onglet RLAN Security. Sous Security Type, vous pouvez sélectionner Open ou 802.1X.

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

Cliquez sur Apply. Cette opération active automatiquement ce RLAN de sécurité ouverte. Passez à l'étape 11.



Étape 10a (utilisation de la sécurité 802.1X)

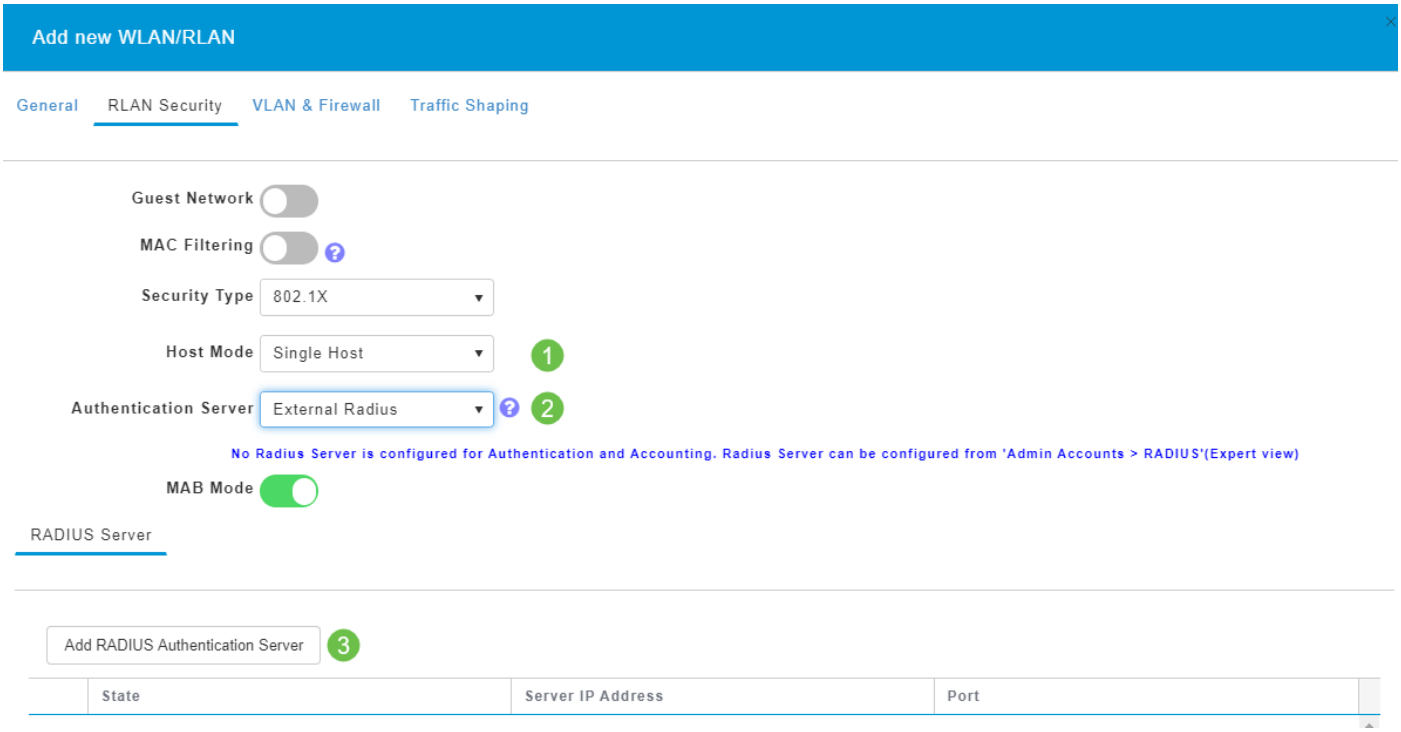
Pour configurer Radius externe, vous devez avoir un serveur Radius configuré dans Admin Accounts sous RADIUS dans Expert View. Cliquez sur l'icône en forme de flèche dans le menu supérieur droit de l'interface utilisateur Web pour passer à Expert View. Pour plus d'informations sur la configuration d'un serveur RADIUS, consultez Radius



Étape 10b (utilisation de la sécurité 802.1X)

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

- Mode hôte - Hôte unique ou multi-hôte
- Serveur d'authentification - Radius externe ou AP
- Mode MAB : activé ou désactivé. Pour ajouter des adresses MAC, suivez les instructions de l'étape suivante.

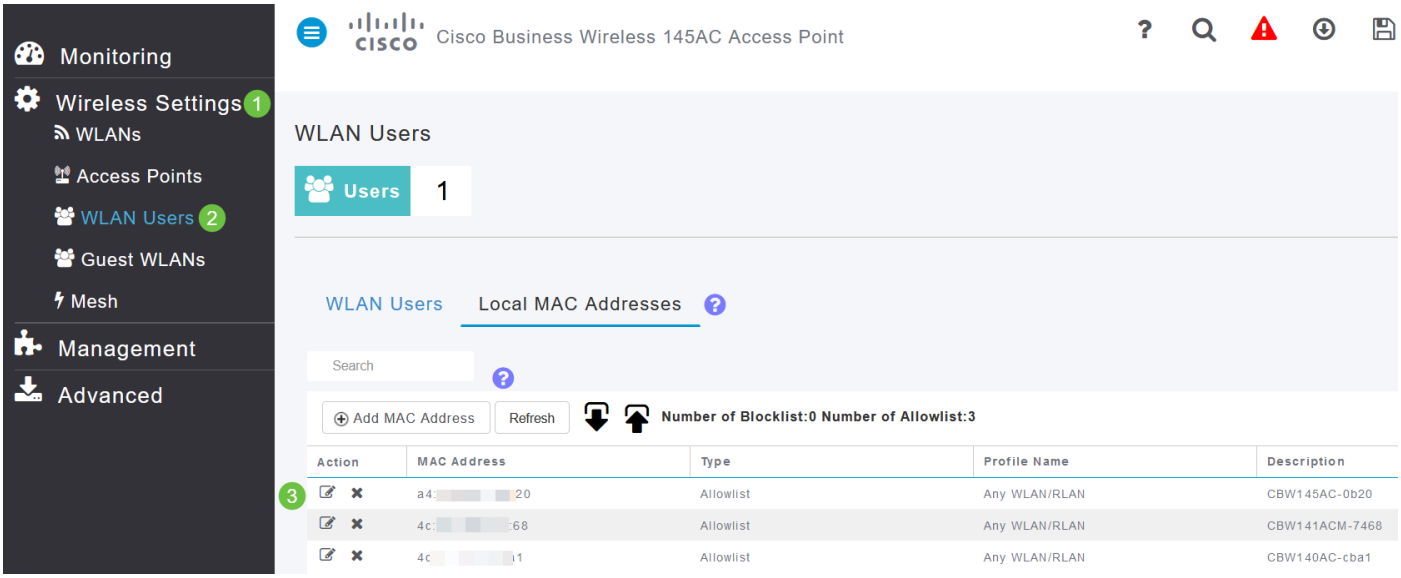


Étape 11 (facultative)

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 pour être automatiquement refusées. Cela peut s'avérer utile dans le cas où un téléphone IP est branché sur un port PoE d'un commutateur.

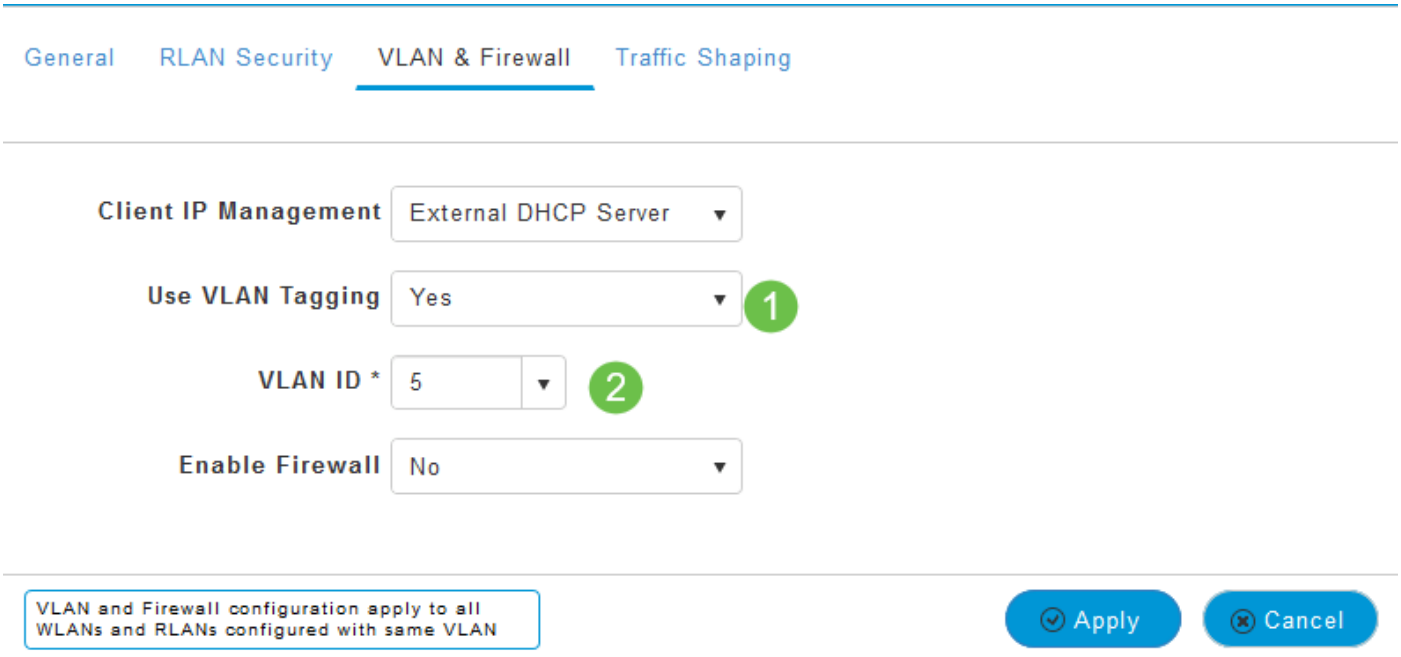
Vous pouvez attribuer une étiquette à chaque adresse MAC de deux manières :

1. Autorisé - Le périphérique reçoit un accès automatique.
2. Bloqué - L'accès au périphérique sera automatiquement refusé.



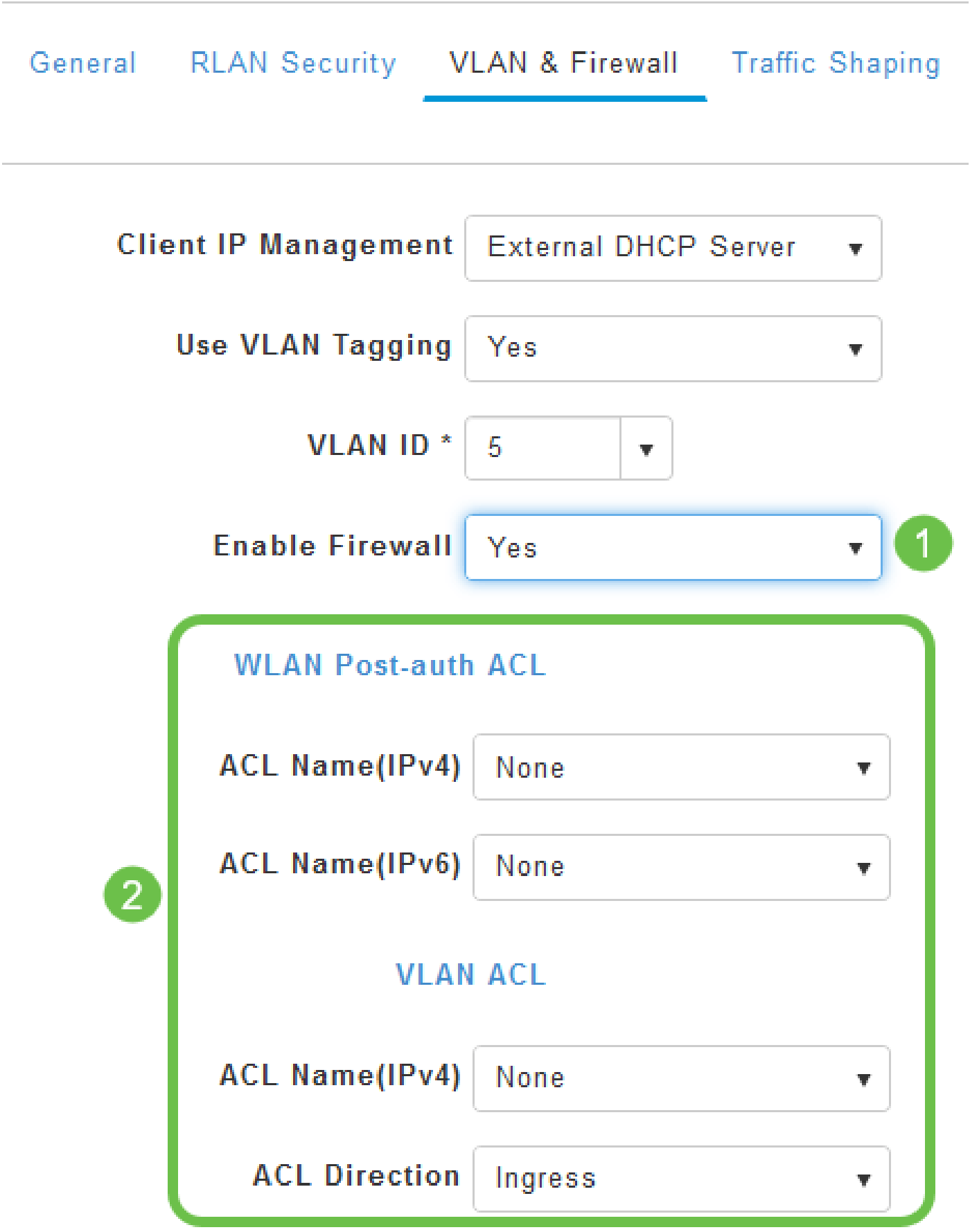
Étape 12

Sous l'onglet VLAN & Firewall, vous pouvez sélectionner Use VLAN Tagging et sélectionner un numéro d'ID de VLAN.



Étape 13 (facultative)

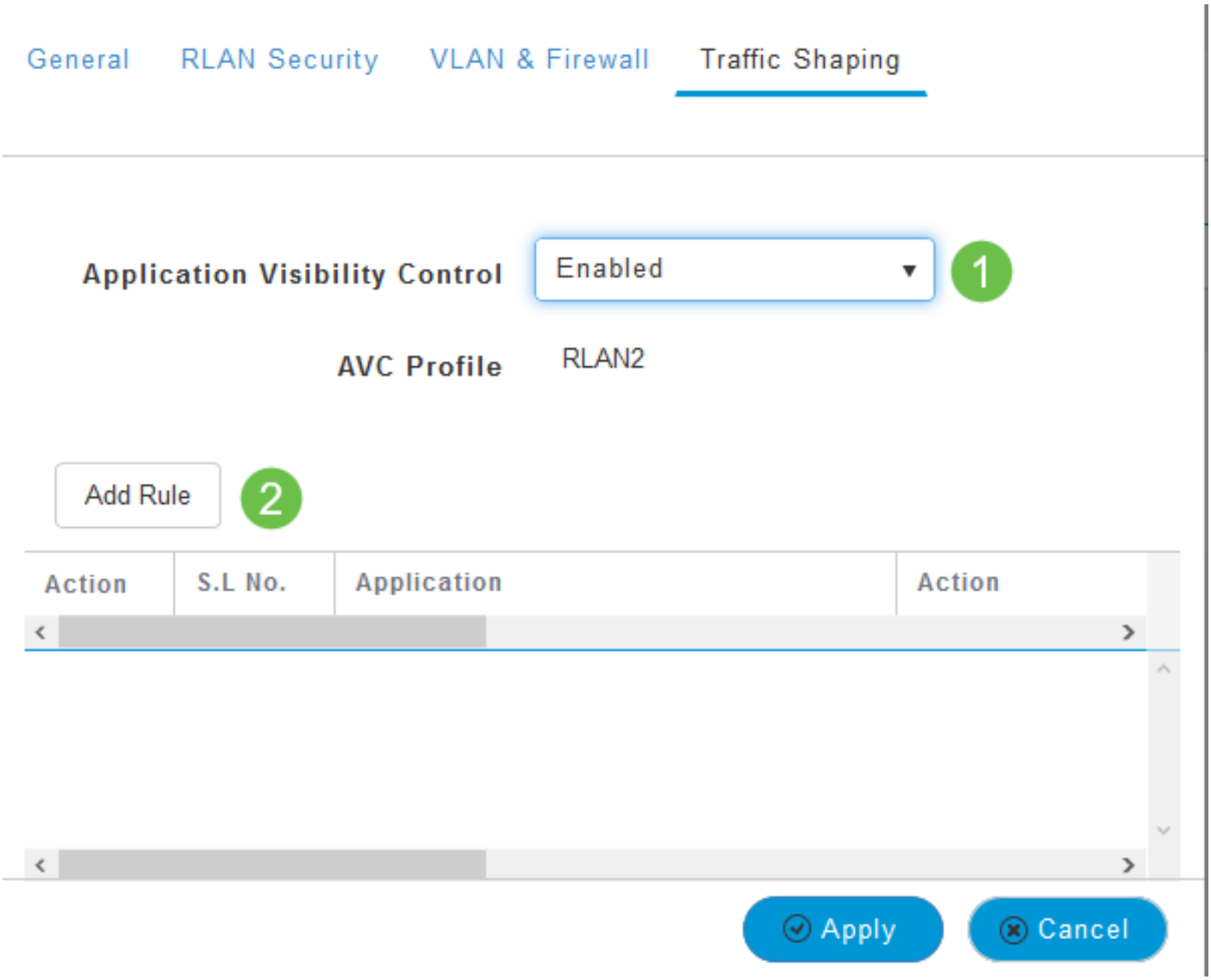
Vous pouvez sélectionner Enable Firewall si vous voulez configurer des listes de contrôle d'accès (ACL) qui vous permettent d'autoriser ou de rejeter l'accès pour des adresses IP ou VLAN spécifiques. Elle est utilisée si une personne se connecte au périphérique du port réseau pour se connecter au réseau.



Étape 14 (facultative)

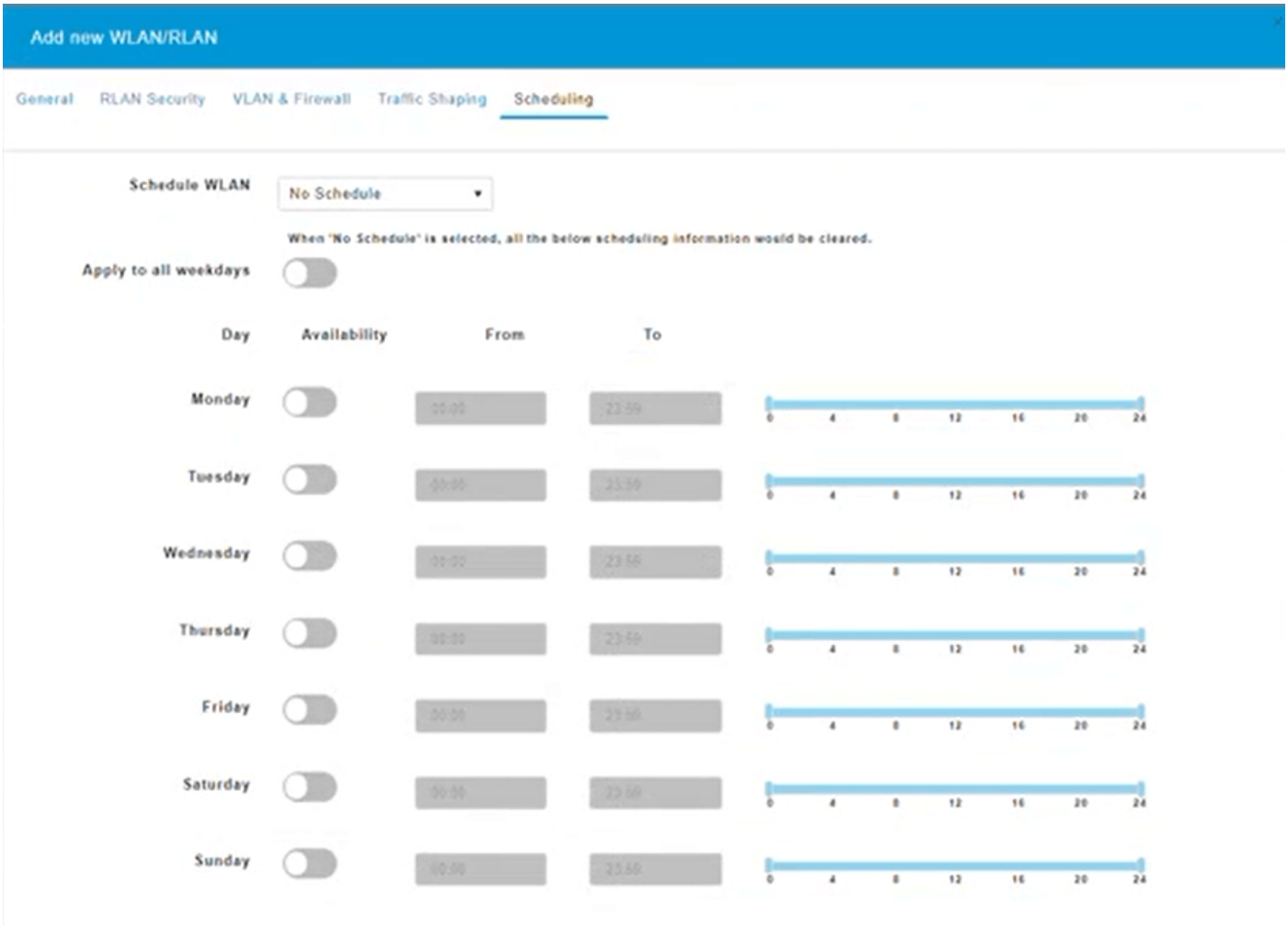
Sous l'onglet Traffic Shaping, vous pouvez configurer le formatage du trafic en activant le contrôle

de la visibilité des applications. Cela définit la hiérarchisation du trafic.



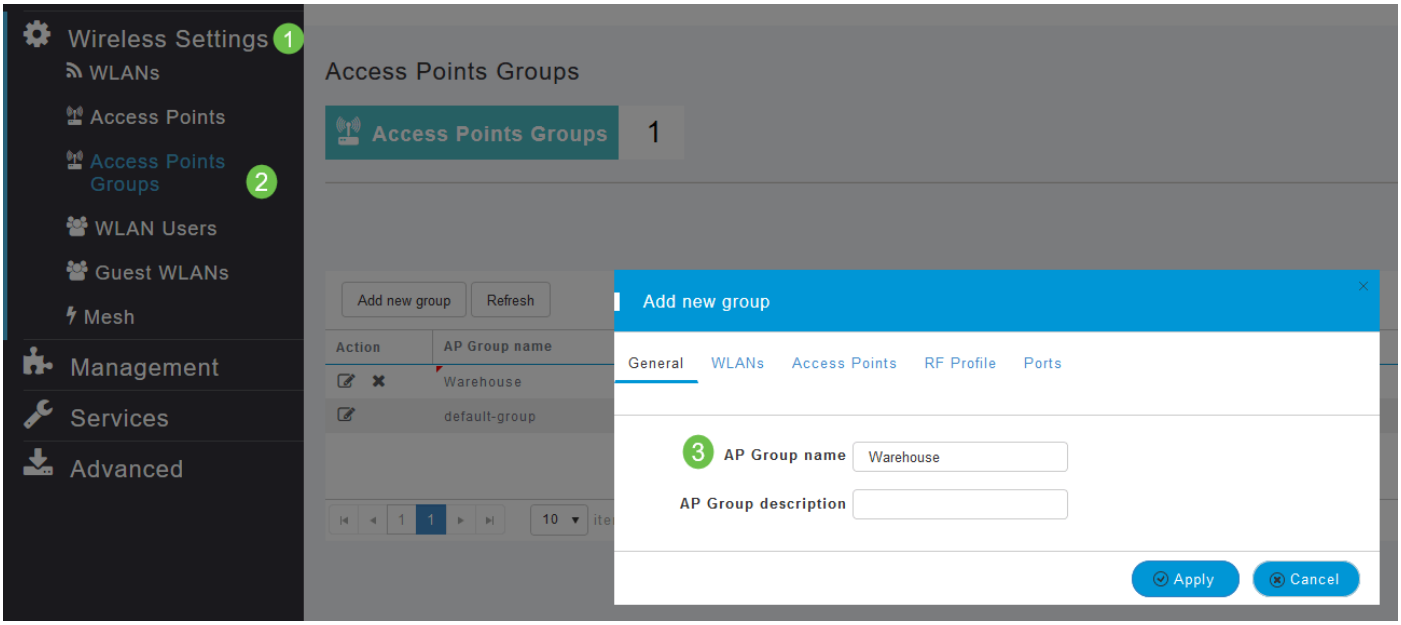
Étape 15 (facultative)

Sous l'onglet Planification, vous pouvez sélectionner une planification. Cette option définit les heures auxquelles le port peut être connecté au réseau.



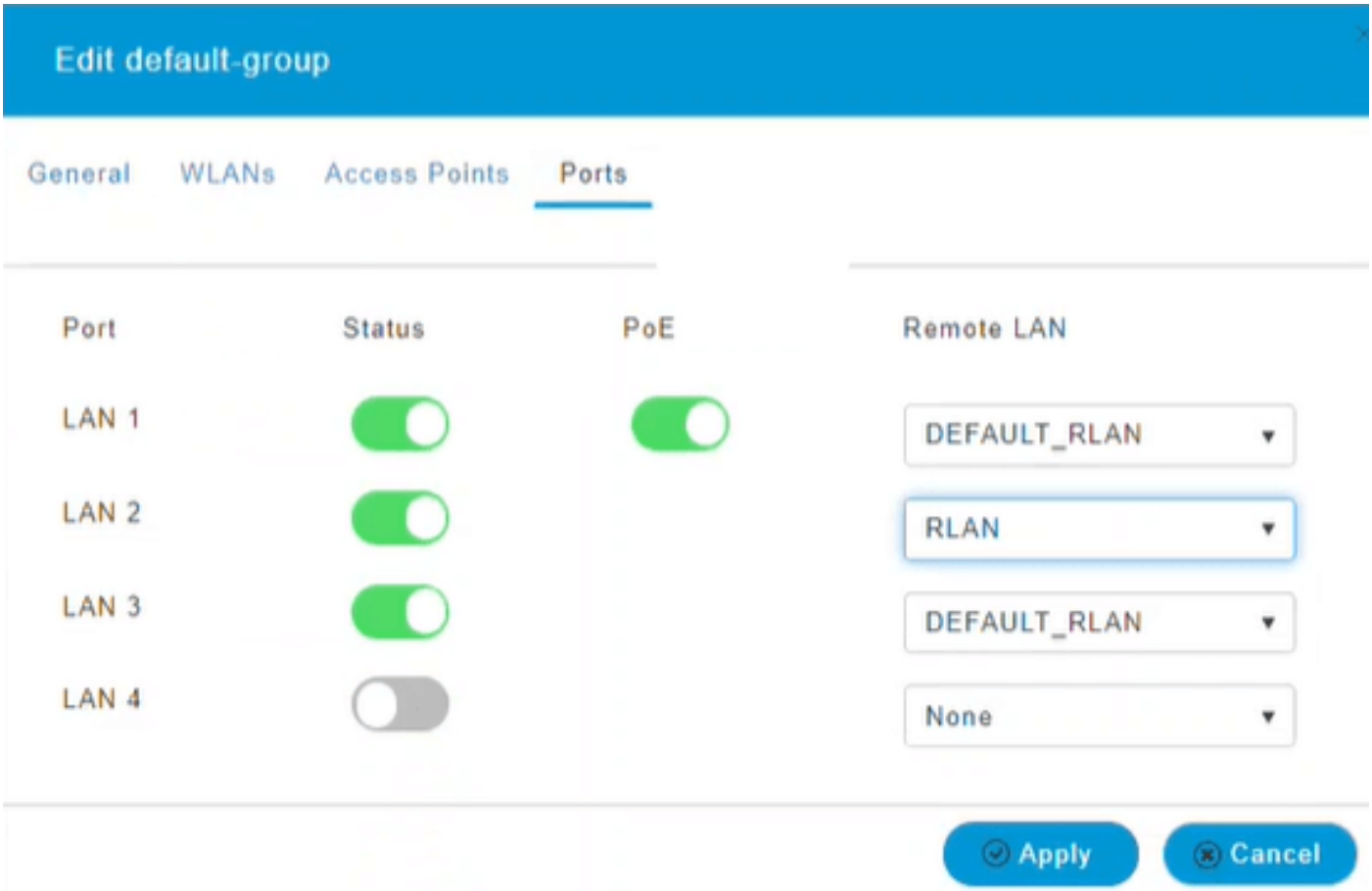
Étape 16 (facultative)

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



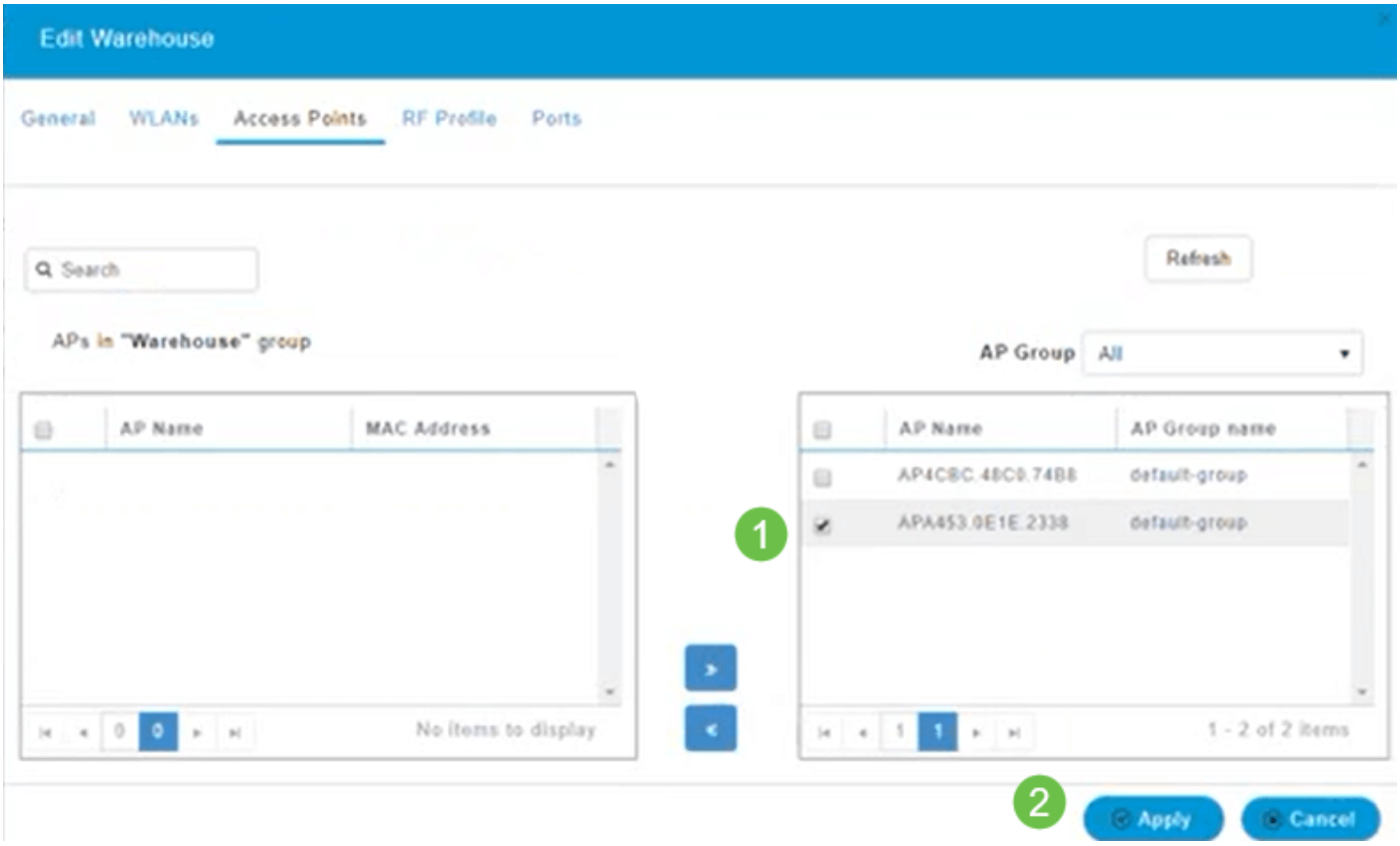
Étape 17

Sous l'onglet Ports, vous pouvez attribuer les ports sur le point d'accès à des LAN distants spécifiques.



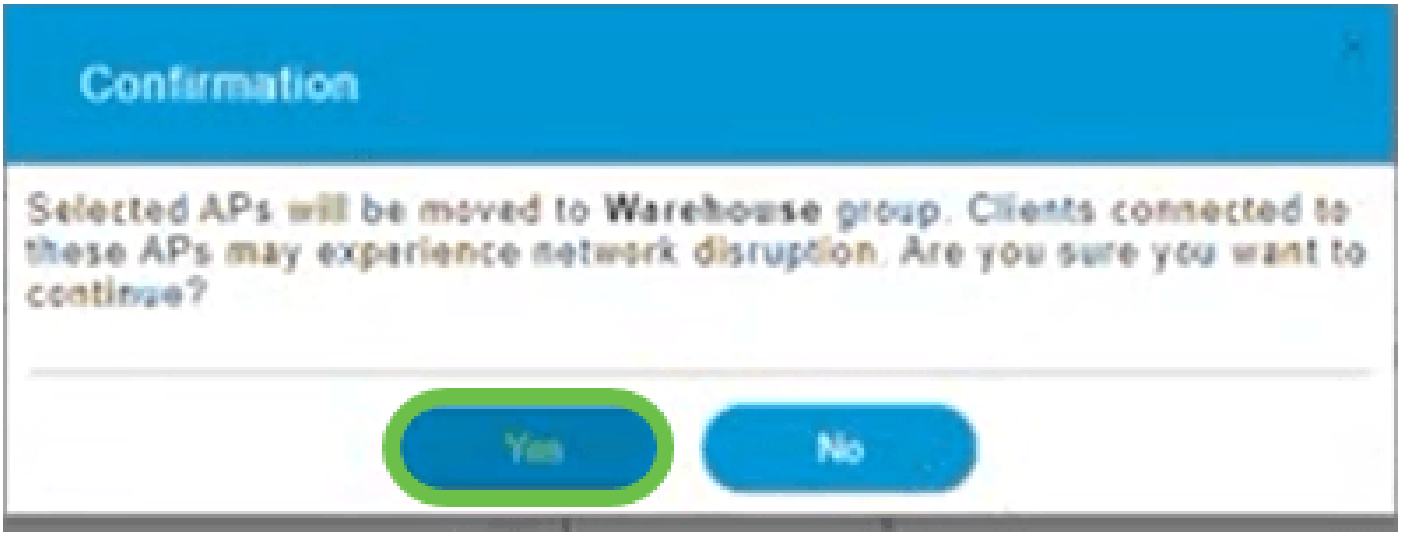
Étape 18

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



Étape 19

Sélectionnez Oui pour confirmer.



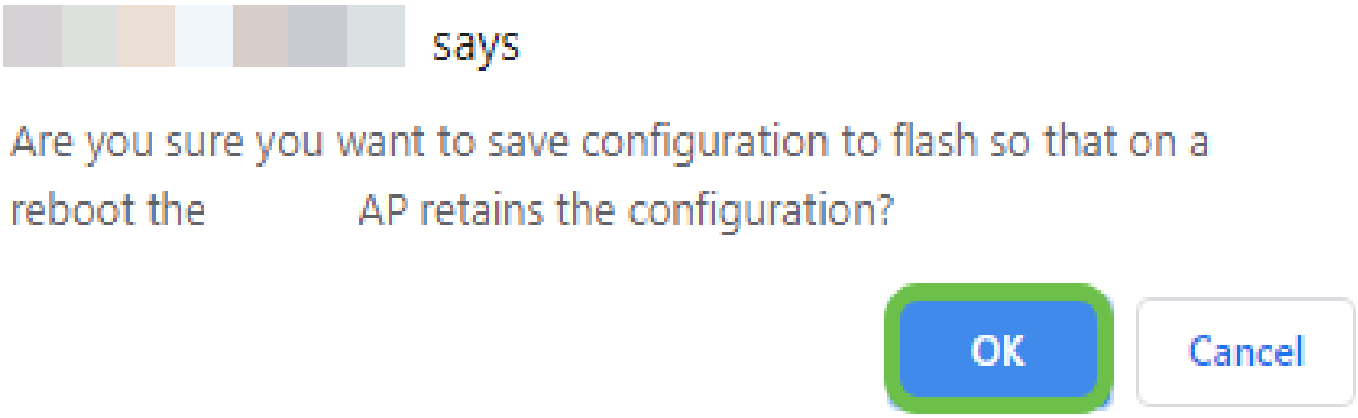
Étape 20

Assurez-vous d'enregistrer vos configurations en cliquant sur l'icône Save dans le panneau supérieur droit de l'écran Web UI.



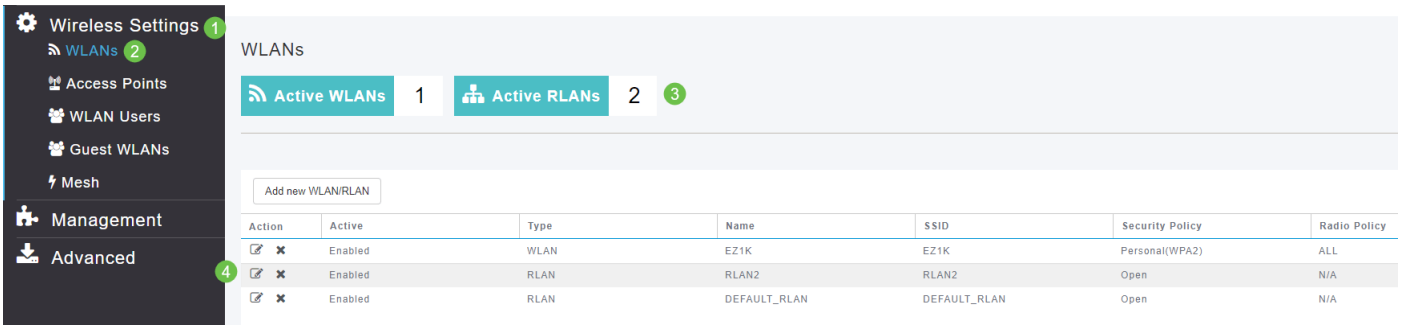
Étape 21

Confirmez l'enregistrement en cliquant sur OK. Le point d'accès redémarre. Cela prendra entre 8 et 10 minutes.



Afficher le RLAN

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

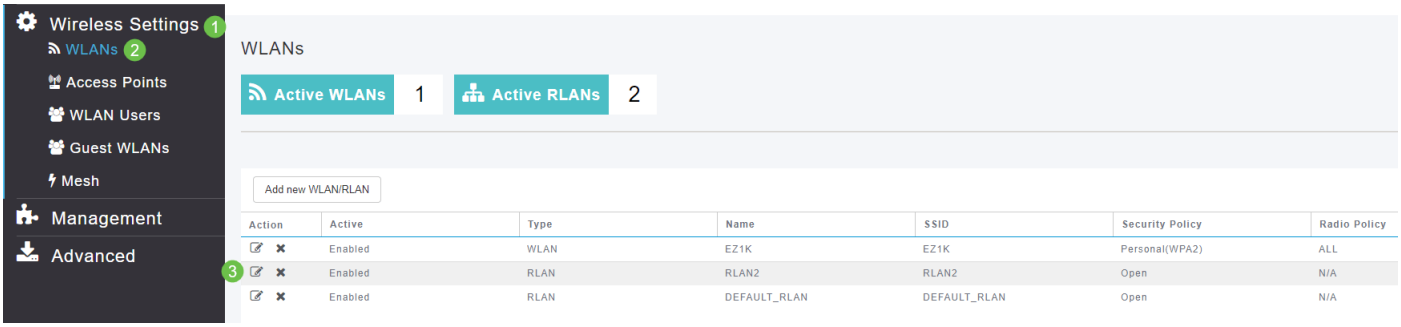


Modifier le RLAN

Lorsque vous avez cliqué sur Apply à la fin de la configuration de votre RLAN, le RLAN s'est automatiquement activé. Si vous devez désactiver le RLAN ou apporter d'autres modifications, suivez ces étapes simples ci-dessous.

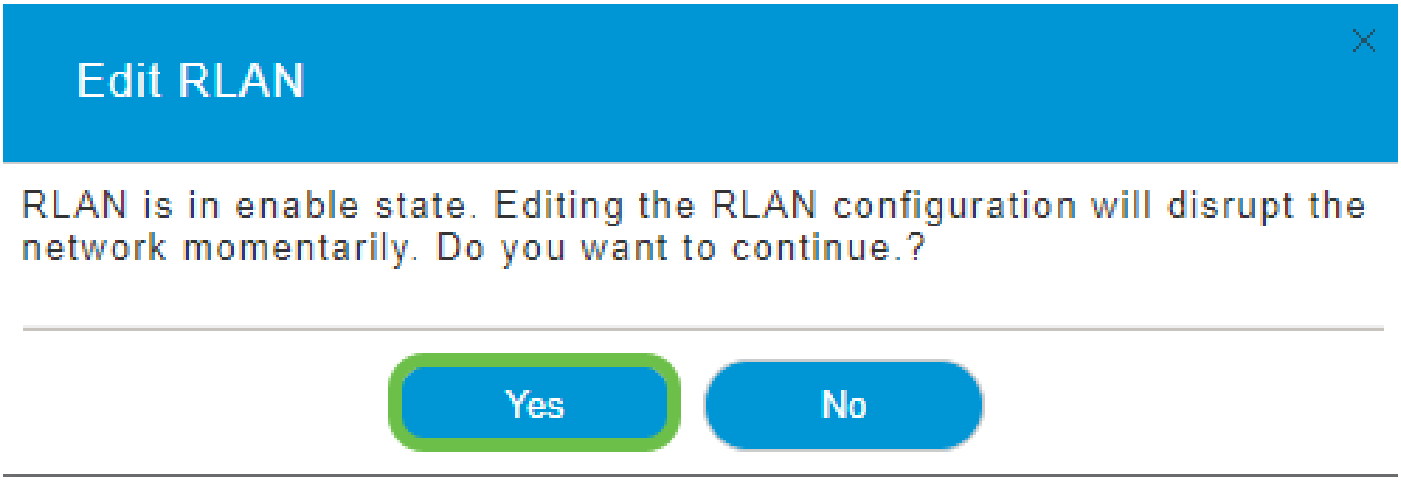
Étape 1

Sélectionnez Wireless Settings > WLANs. Cliquez sur l’icône edit (modifier).



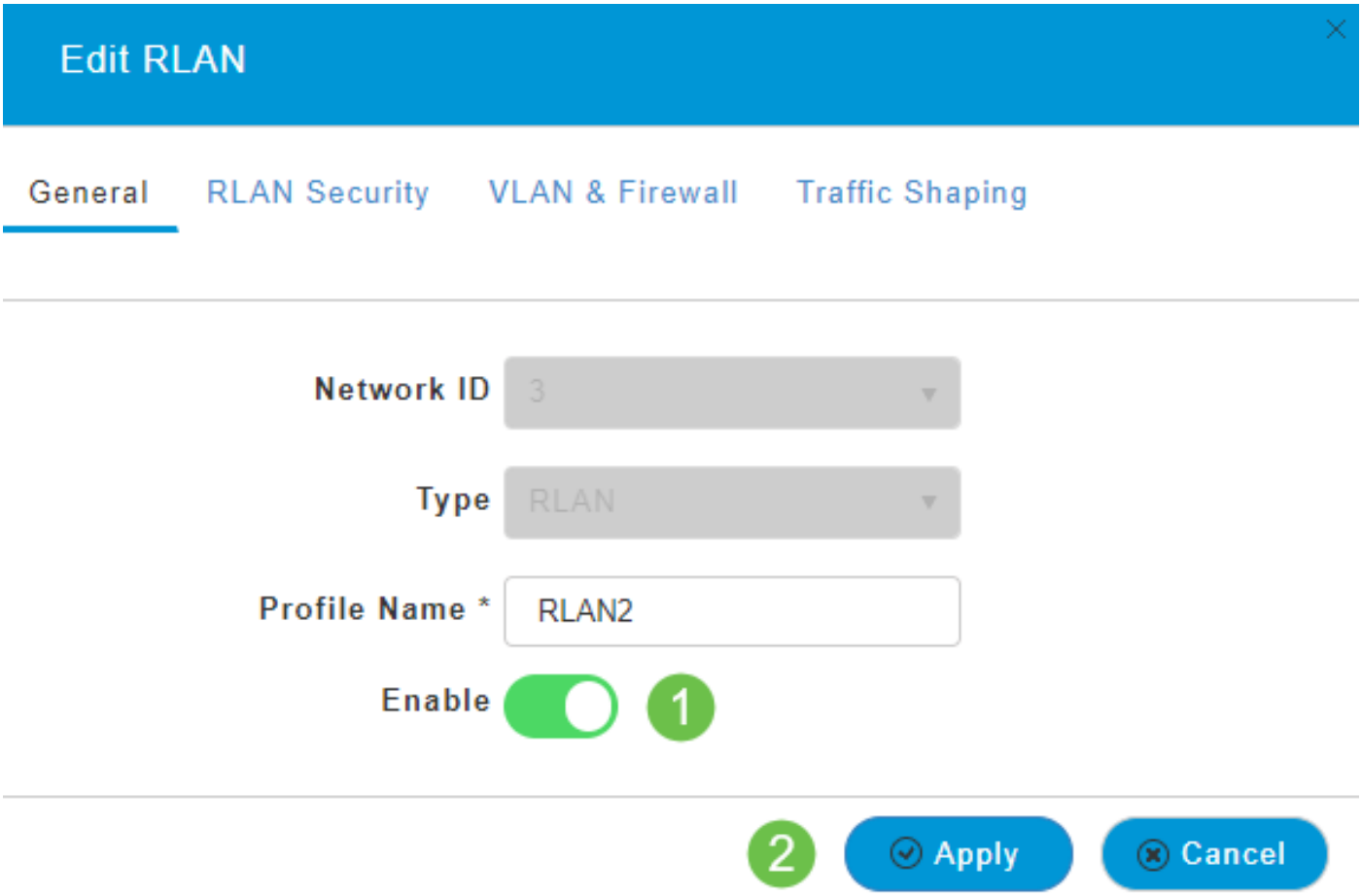
Étape 2

Vous recevrez une fenêtre contextuelle vous indiquant que la modification du RLAN perturbera momentanément le réseau. Confirmez que vous souhaitez continuer en cliquant sur Yes.



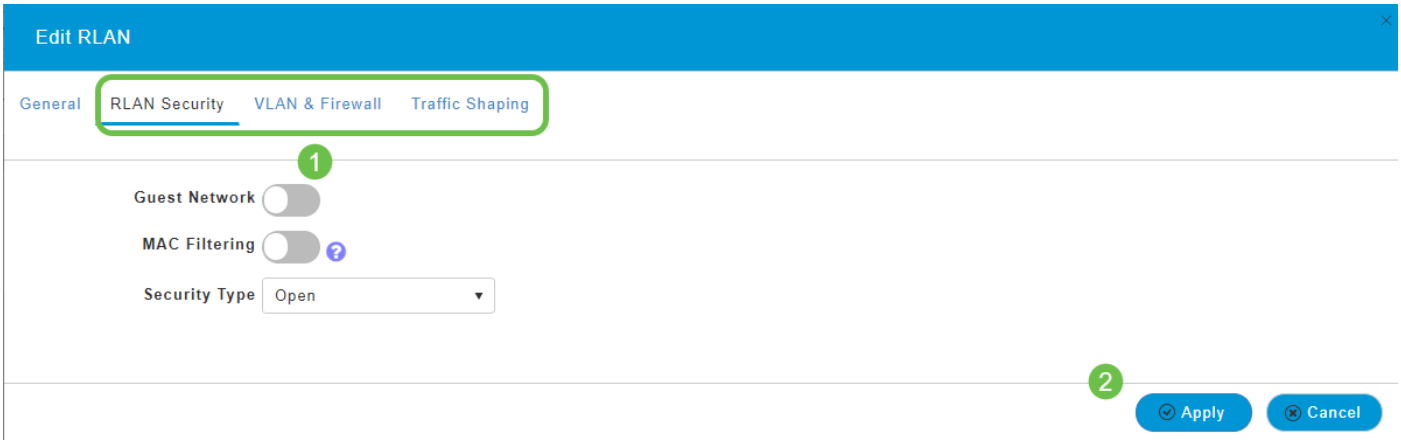
Étape 3 (activation/désactivation)

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



Étape 4 (Modification des autres paramètres)

Accédez aux onglets RLAN Security, VLAN & Firewall ou Traffic Shaping si vous devez modifier les paramètres. Cliquez sur Apply une fois que vous avez apporté des modifications.



Étape 5

Assurez-vous d'enregistrer vos configurations en cliquant sur l'icône Save dans le panneau supérieur droit de l'écran Web UI.

Conclusion

Vous venez de créer un RLAN sur votre réseau CBW. Profitez-en et n'hésitez pas à en ajouter si cela correspond à vos besoins.

Foire aux questions Mise à niveau du micrologiciel Radius RLAN Profilage d'application Client Profilage Outils principaux AP Utilisateurs WLAN parapluie Journalisation Formatage du trafic Interférants Gestion de la configuration Port Configuration Mesh Mode Bienvenue sur le réseau maillé CBW Réseau d' invité utilisant l'authentification de messagerie et la comptabilité RADIUS Dépannage utilisant un routeur Draytek avec CBW

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.