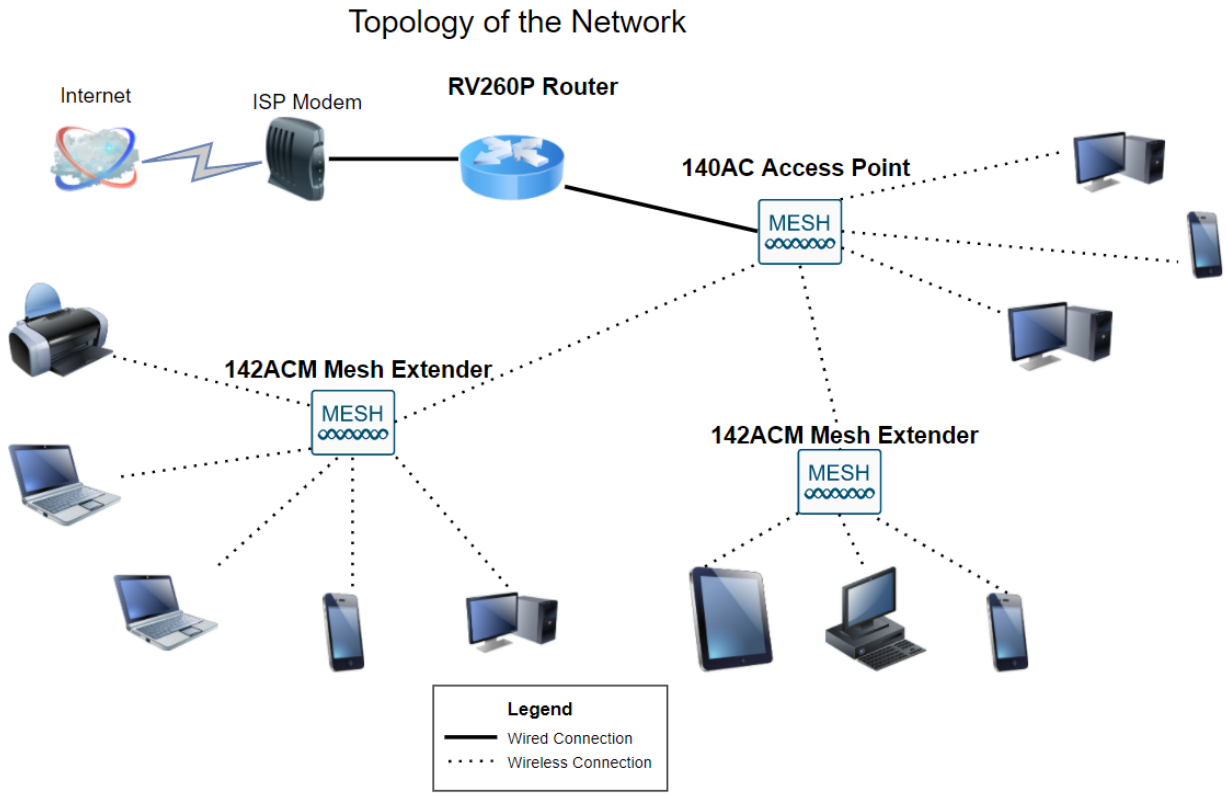
Configuration réseau totale : RV260P avec Cisco Business Wireless et interface utilisateur Web

Objectif:

Ce guide explique comment configurer un réseau maillé sans fil à l'aide d'un routeur RV260P, d'un point d'accès CBW140AC et de deux extenseurs de maillage CBW142ACM.

Cet article utilise l'interface utilisateur Web pour configurer le réseau sans fil maillé. Si vous préférez utiliser l'application mobile, recommandée pour une configuration sans fil aisée, cliquez pour accéder directement à l'article qui utilise l'application mobile. Si vous voulez utiliser l'interface utilisateur Web, continuez à lire !

Topologie:



Introduction

Vous êtes prêt à configurer votre nouveau réseau. C'est une journée passionnante ! Dans ce scénario, nous utilisons un routeur RV260P. Ce routeur fournit une alimentation PoE (Power over Ethernet) qui vous permet de brancher le CBW140AC sur le routeur au lieu d'un commutateur. Les extendeurs de maillage CBW140AC et CBW142ACM seront utilisés pour créer un réseau maillé sans fil.

Si vous ne connaissez pas certains des termes utilisés dans ce document ou si vous souhaitez en savoir plus sur la mise en réseau maillée, consultez les articles suivants :

- Cisco Business : Glossaire des nouveaux termes
- Bienvenue dans Cisco Business Wireless Mesh Networking
- Foire aux questions (FAQ) pour un réseau sans fil professionnel Cisco

Êtes-vous prêts ? Allons-y !

Périphériques pertinents | Version du logiciel

- RV260P |1.0.0.17
- CBW140AC |10.3.1.0
- CBW142ACM | 10.3.1.0 (au moins un extendeur de maillage est nécessaire pour le réseau maillé)

Table des matières

Avant de commencer

1. Vérifiez que vous disposez d'une connexion Internet en cours pour l'installation.
2. Contactez votre FAI pour connaître les instructions spéciales qu'il a à suivre lors de l'utilisation de votre routeur RV260. Certains FAI offrent des passerelles avec des routeurs intégrés. Si vous disposez d'une passerelle avec un routeur intégré, vous devrez peut-être désactiver le routeur et passer l'adresse IP WAN (Wide Area Network) (l'adresse de protocole Internet unique que le fournisseur d'accès Internet attribue à votre compte) et tout le trafic réseau via votre nouveau routeur.

3. Déterminez où placer le routeur. Vous aurez besoin d'un espace ouvert si possible. Cela peut ne pas être facile car vous devez connecter le routeur à la passerelle haut débit (modem) à partir de votre fournisseur d'accès à Internet (FAI).

Configuration du routeur RV260P

Un routeur est essentiel dans un réseau, car il achemine les paquets. Elle permet à un ordinateur de communiquer avec d'autres ordinateurs qui ne se trouvent pas sur le même réseau ou sous-réseau. Un routeur accède à une table de routage pour déterminer où les paquets doivent être envoyés. La table de routage répertorie les adresses de destination. Les configurations statiques et dynamiques peuvent toutes deux être répertoriées dans la table de routage afin d'acheminer les paquets vers leur destination spécifique.

Votre RV260P est livré avec des paramètres par défaut optimisés pour de nombreuses petites entreprises. Cependant, vos demandes réseau ou votre fournisseur d'accès à Internet (FAI) peuvent nécessiter que vous modifiiez certains de ces paramètres. Après avoir contacté votre FAI pour connaître les conditions requises, vous pouvez apporter des modifications à l'aide de l'interface utilisateur Web.

RV260P prêt à l'emploi

Étape 1

Connectez le câble Ethernet d'un des ports Ethernet (LAN) du RV260P au port Ethernet de l'ordinateur. Vous aurez besoin d'un adaptateur si votre ordinateur ne dispose pas d'un port Ethernet. Le terminal doit se trouver dans le même sous-réseau câblé que le RV260P pour effectuer la configuration initiale.

Étape 2

Veillez à utiliser l'adaptateur secteur fourni avec le RV260P. L'utilisation d'un autre adaptateur secteur peut endommager le RV260P ou provoquer l'échec des dongles USB. L'interrupteur d'alimentation est activé par défaut.

Connectez l'adaptateur électrique au port 12 VCC du RV260P, mais ne le branchez pas encore à l'alimentation.

Étape 3

Assurez-vous que le modem est désactivé.

Étape 4

Utilisez un câble Ethernet pour connecter votre modem câble ou DSL au port WAN du routeur RV260P.

Étape 5

Branchez l'autre extrémité de l'adaptateur RV260P sur une prise électrique. Le routeur RV260 est ainsi mis sous tension. Rebranchez le modem pour qu'il puisse également être mis sous tension. Le voyant d'alimentation situé sur la façade est vert fixe lorsque l'adaptateur secteur est correctement connecté et que le routeur RV260P a terminé le démarrage.

Configuration du routeur

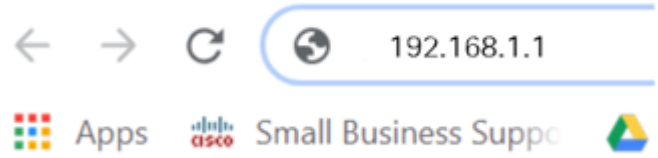
Le travail de préparation est terminé, maintenant il est temps de faire quelques configurations ! Pour lancer l'interface utilisateur Web, procédez comme suit :

Étape 1

Si votre ordinateur est configuré pour devenir un client DHCP (Dynamic Host Configuration Protocol), une adresse IP de la plage 192.168.1.x est attribuée au PC. Le protocole DHCP automatise le processus d'attribution d'adresses IP, de masques de sous-réseau, de passerelles par défaut et d'autres paramètres aux ordinateurs. Les ordinateurs doivent être configurés pour participer au processus DHCP pour obtenir une adresse. Pour ce faire, sélectionnez cette option pour obtenir automatiquement une adresse IP dans les propriétés de TCP/IP sur l'ordinateur.

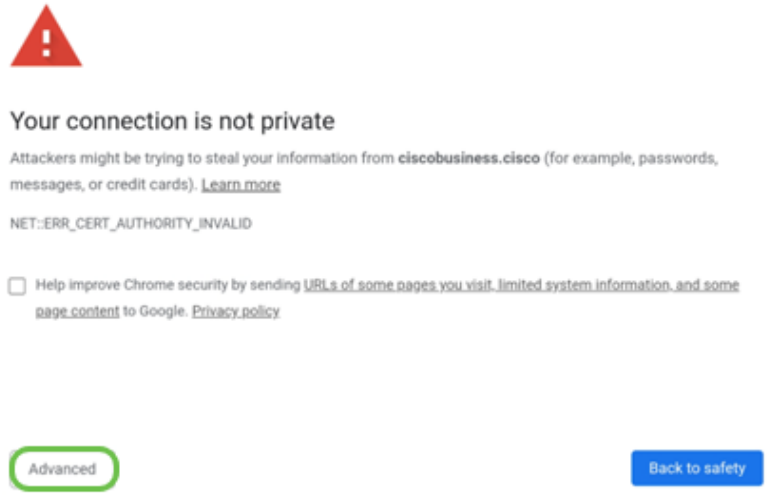
Étape 2

Ouvrez un navigateur Web tel que Safari, Internet Explorer ou Firefox. Dans la barre d'adresses, saisissez l'adresse IP par défaut du routeur RV260P qui est 192.168.1.1.



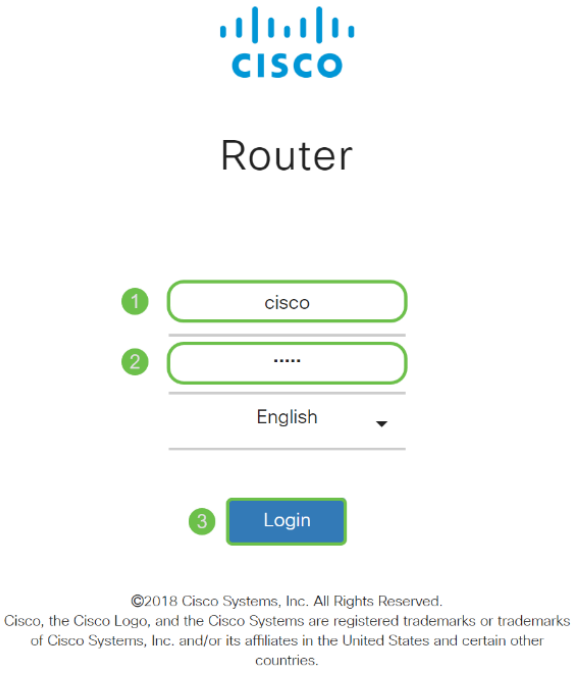
Étape 3

Le navigateur peut émettre un avertissement indiquant que le site Web n'est pas approuvé. Accédez au site Web. Si vous n'êtes pas connecté, accédez à Dépannage de la connexion Internet.



Étape 4

Lorsque la page de connexion apparaît, saisissez le nom d'utilisateur par défaut cisco et le mot de passe par défaut *cisco*. Le nom d'utilisateur et le mot de passe sont tous deux sensibles à la casse.



Étape 5

Cliquez sur **Connexion**. La page *Mise en route* s'affiche. Maintenant que vous avez confirmé la connexion et que vous vous êtes connecté au routeur, accédez à la section Configuration initiale de cet article.

Dépannage de la connexion Internet

Si vous lisez ceci, vous avez probablement des difficultés à vous connecter à Internet ou à l'interface utilisateur Web. Une de ces solutions devrait aider.

Sur votre système d'exploitation Windows connecté, vous pouvez tester votre connexion réseau en ouvrant l'invite de commandes. Entrez ping 192.168.1.1 (adresse IP par défaut du routeur). Si la requête expire, vous ne pouvez pas communiquer avec

le routeur.

Si la connectivité ne se produit pas, vous pouvez consulter Dépannage sur les routeurs RV160 et RV260.

Autres choses à essayer :

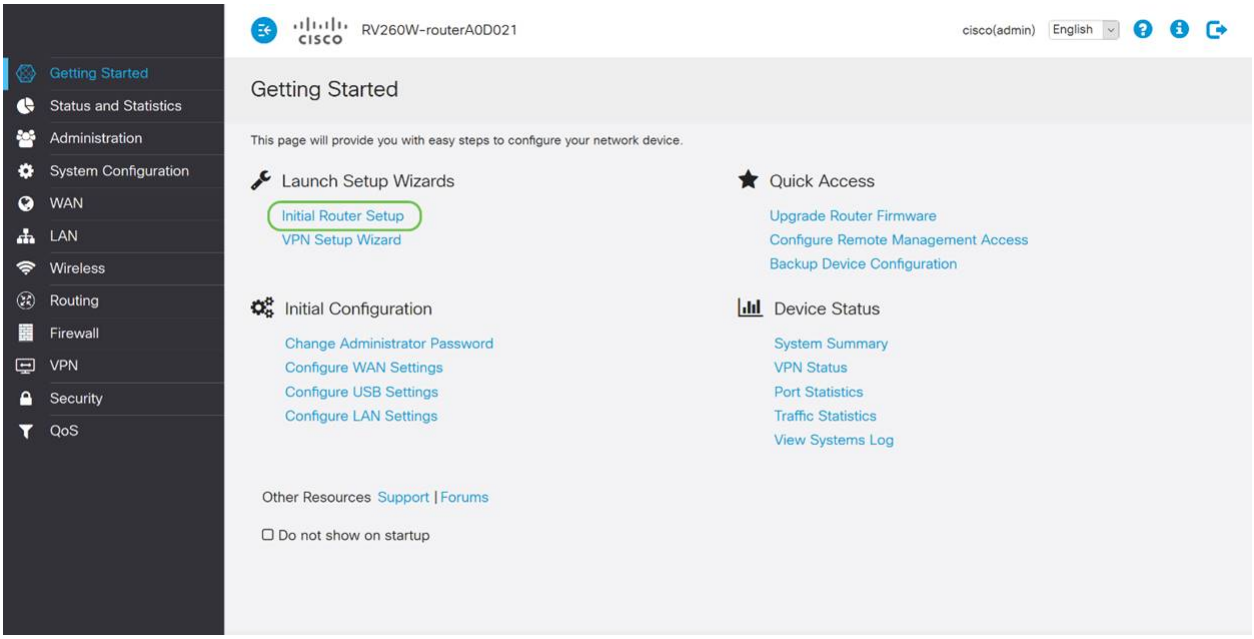
1. Vérifiez que votre navigateur Web n'est pas défini sur Travail hors connexion.
2. Vérifiez les paramètres de connexion au réseau local de votre adaptateur Ethernet. Le PC doit obtenir une adresse IP via DHCP. Le PC peut également avoir une adresse IP statique dans la plage 192.168.1.x avec la passerelle par défaut définie sur 192.168.1.1 (l'adresse IP par défaut du RV260P). Pour vous connecter, vous devrez peut-être modifier les paramètres réseau du routeur RV260P. Si vous utilisez Windows 10, consultez les instructions de Windows 10 pour modifier les paramètres réseau.
3. Si vous disposez d'un équipement occupant l'adresse IP 192.168.1.1, vous devez résoudre ce conflit pour que le réseau fonctionne. Pour en savoir plus à la fin de cette section, ou cliquez ici pour vous y rendre directement.
4. Réinitialisez le modem et le RV260P en éteignant les deux périphériques. Ensuite, mettez le modem sous tension et laissez-le inactif pendant environ 2 minutes. Mettez ensuite le routeur RV260P sous tension. Vous devez maintenant recevoir une adresse IP WAN.
5. Si vous avez un modem DSL, demandez à votre FAI de mettre le modem DSL en mode pont.

Configuration initiale

Nous vous recommandons de suivre les étapes de l'Assistant de configuration initiale répertoriées dans cette section. Vous pouvez modifier ces paramètres à tout moment.

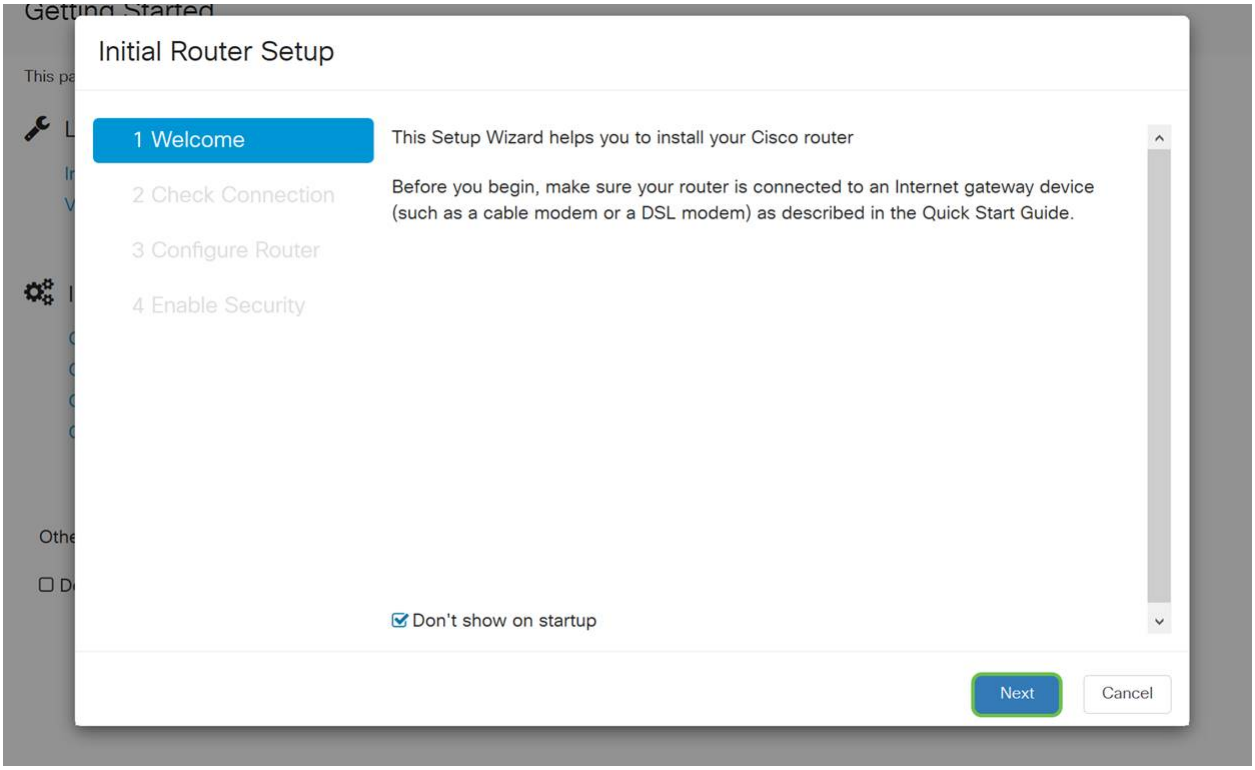
Étape 1

Cliquez sur **Initial Setup Wizard** à partir de la page *Getting Started*.



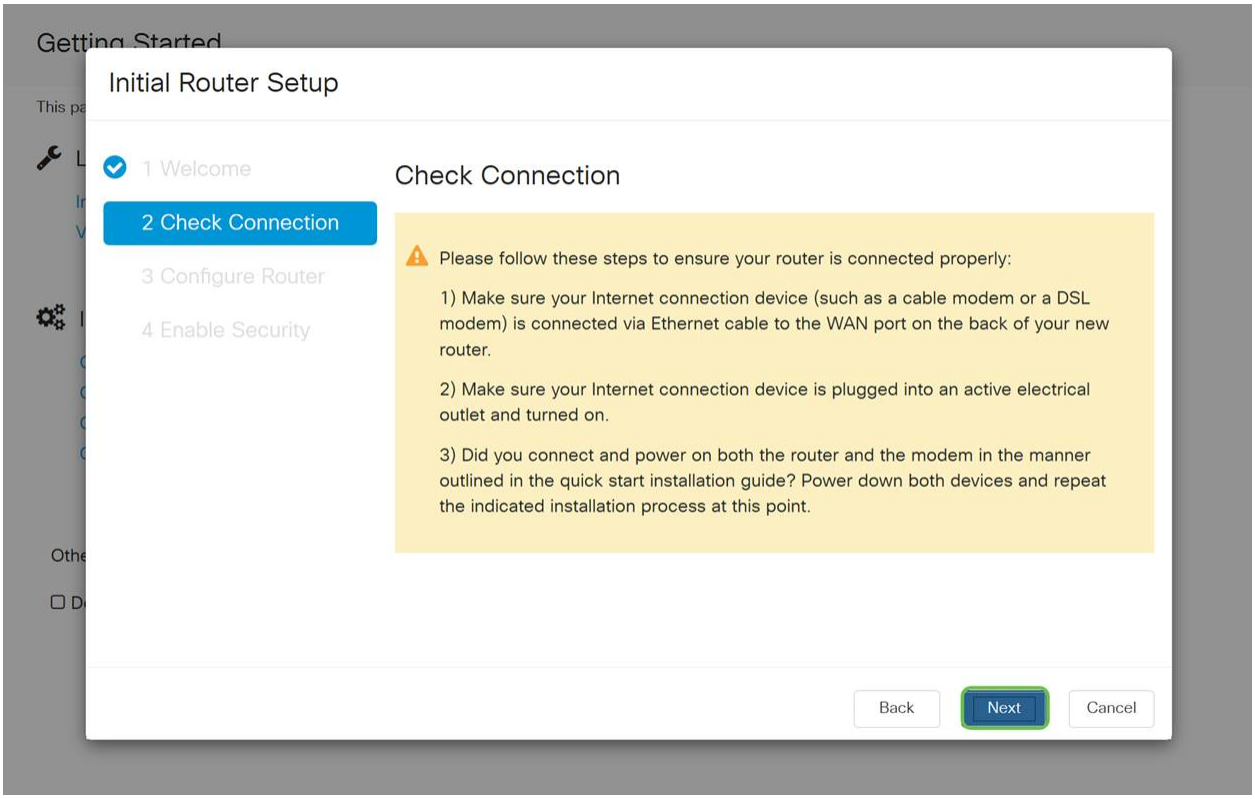
Étape 2

Cette étape confirme que les câbles sont connectés. Comme vous l'avez déjà confirmé, cliquez sur **Suivant**.



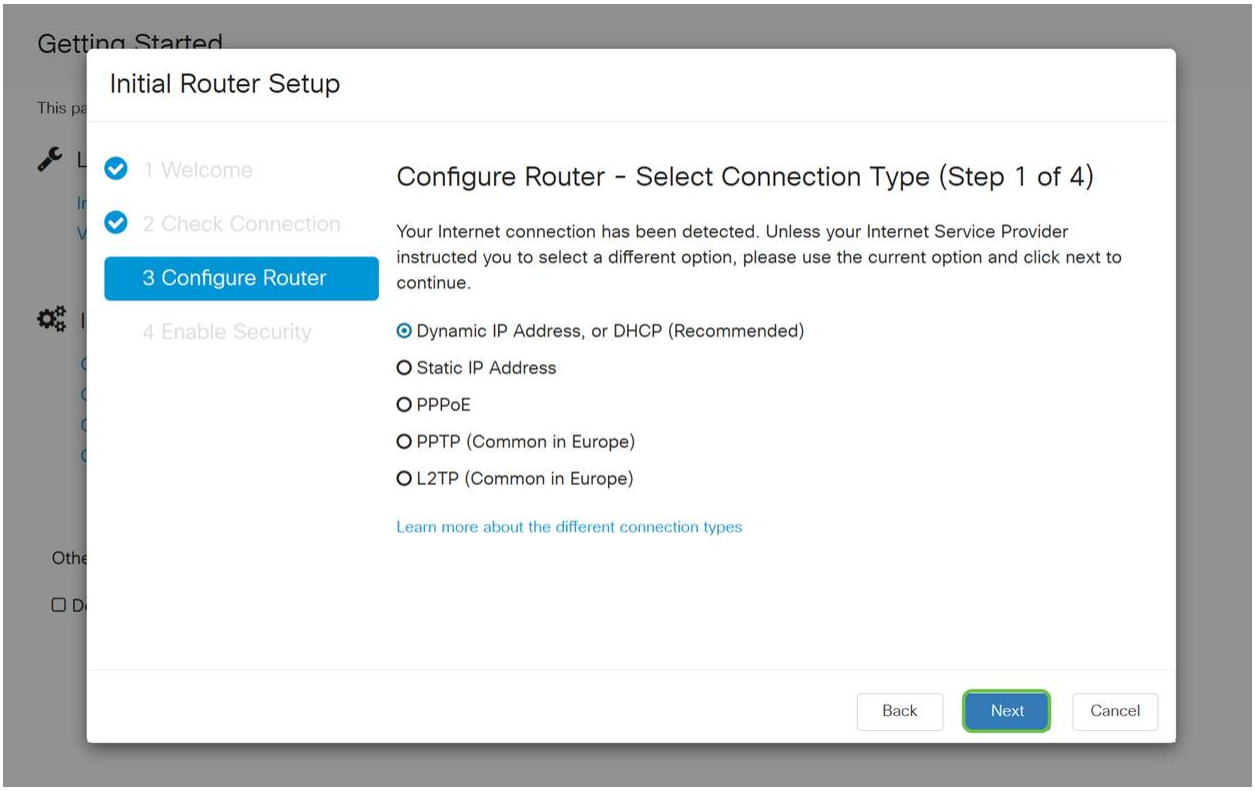
Étape 3

Cette étape décrit les étapes de base pour vous assurer que votre routeur est connecté. Comme vous l'avez déjà confirmé, cliquez sur **Suivant**.



Étape 4

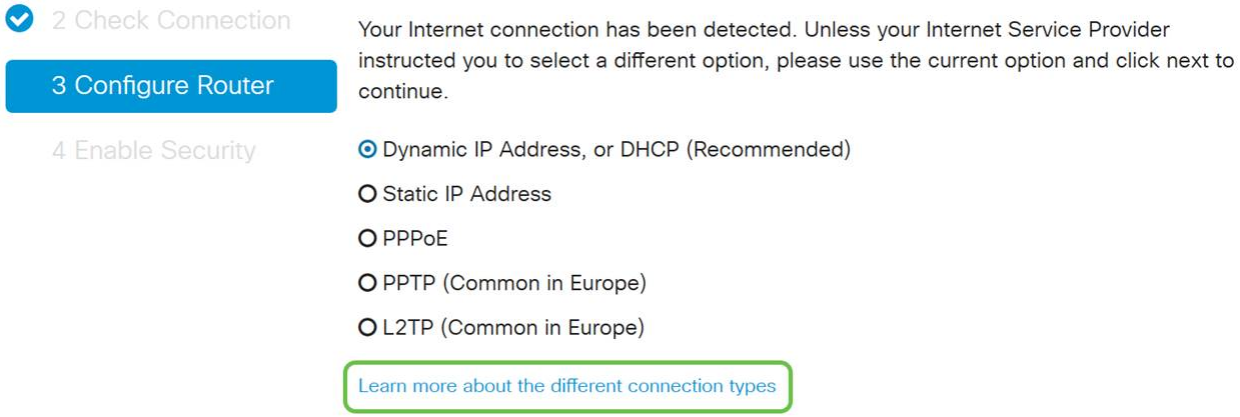
L'écran suivant affiche vos options d'attribution d'adresses IP à votre routeur. Vous devez sélectionner DHCP dans ce scénario. Cliquez sur Next (Suivant).



Bien que vous deviez utiliser DHCP pour cette configuration initiale, vous pouvez sélectionner pour *en savoir plus sur les différents types de connexion* en bas de l'écran la référence future. Pour en savoir plus, consultez les articles suivants :

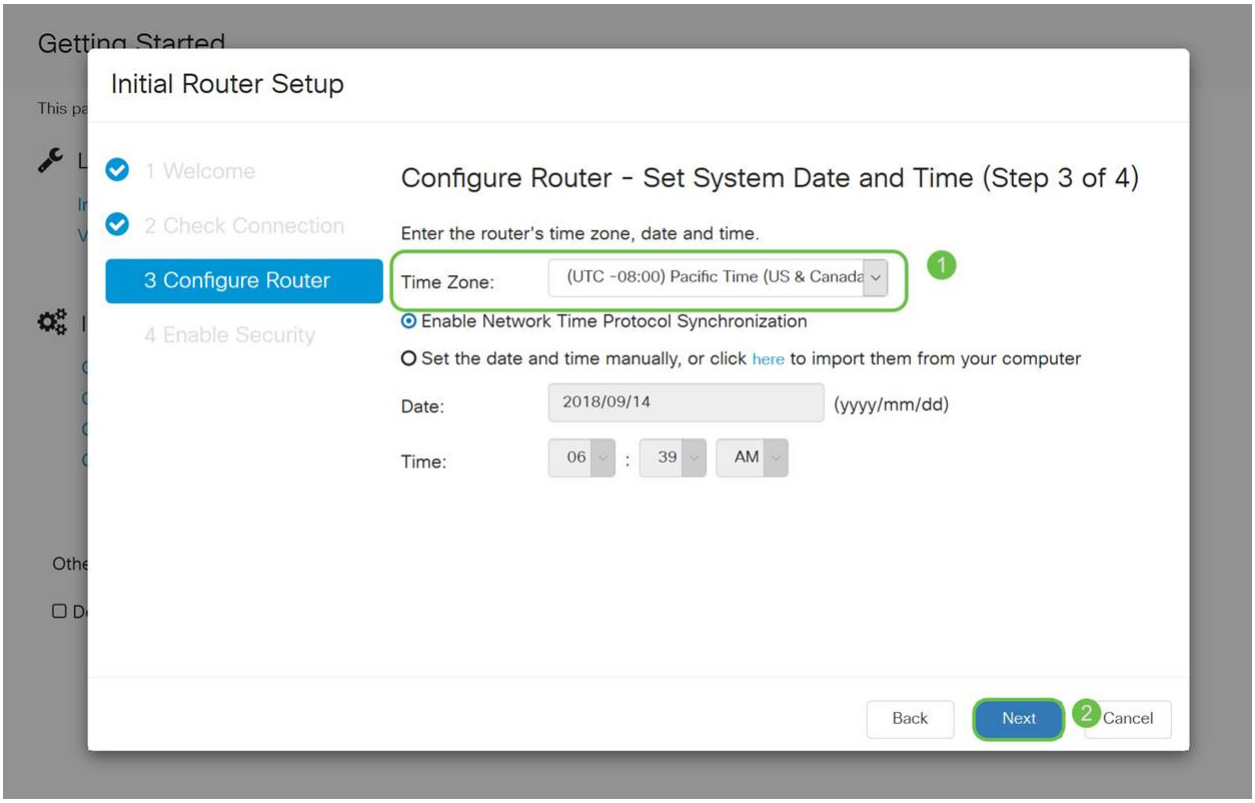
- Configuration WAN sur les périphériques RV160x et RV260x

- [Configuration du routage statique sur les routeurs RV160 et RV260]



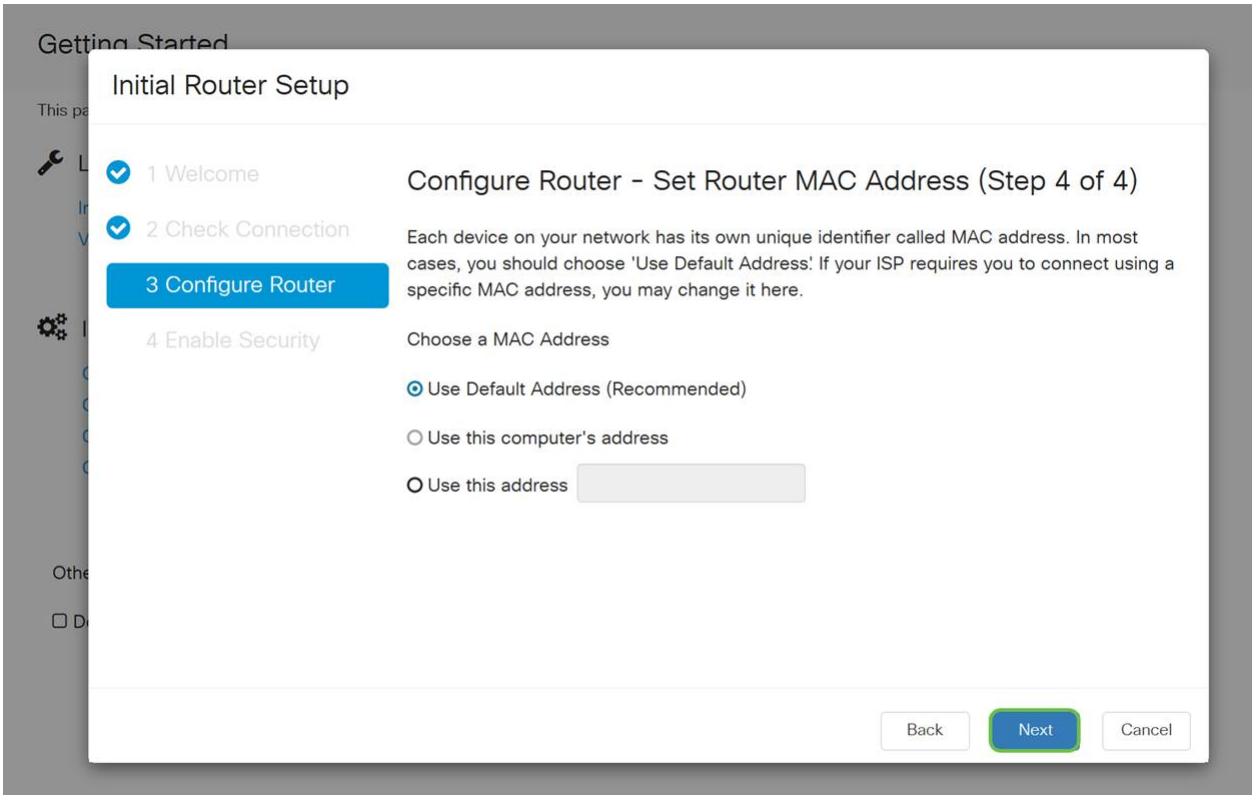
Étape 5

Ici, vous serez invité à définir les paramètres d'heure de votre routeur. Cela est important car il permet de vérifier avec précision les journaux ou les événements de dépannage. Sélectionnez votre **fuseau horaire**, puis cliquez sur **Suivant**.



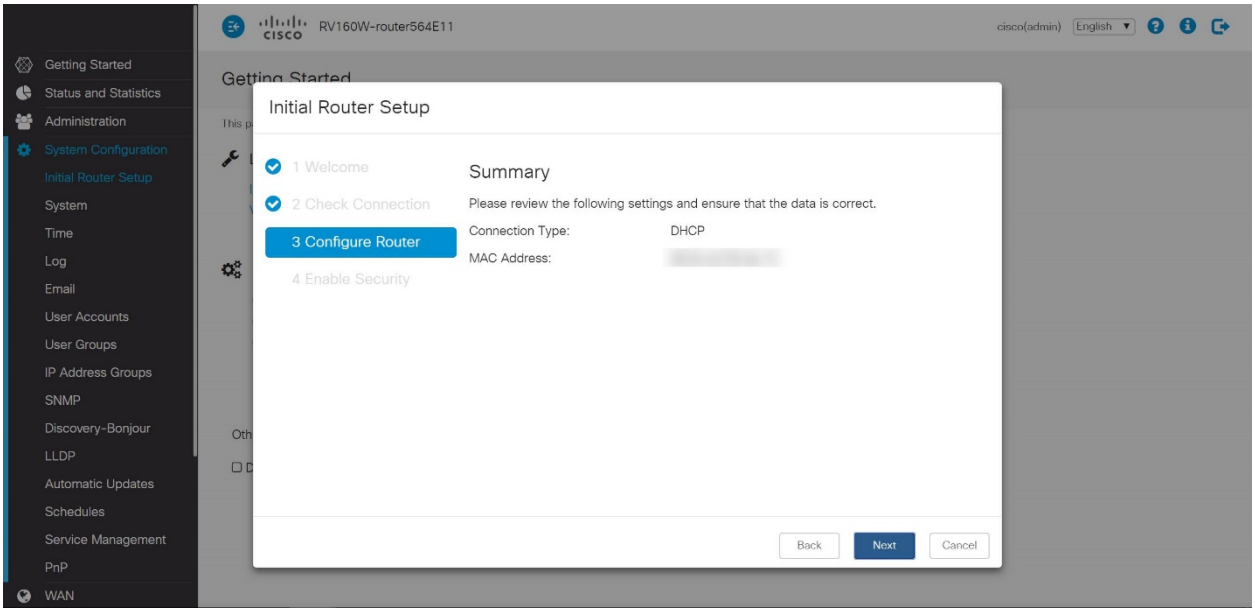
Étape 6

Dans cet écran, vous allez sélectionner les adresses MAC à attribuer aux périphériques. La plupart du temps, vous utiliserez l'adresse par défaut. Cliquez sur Next (Suivant).



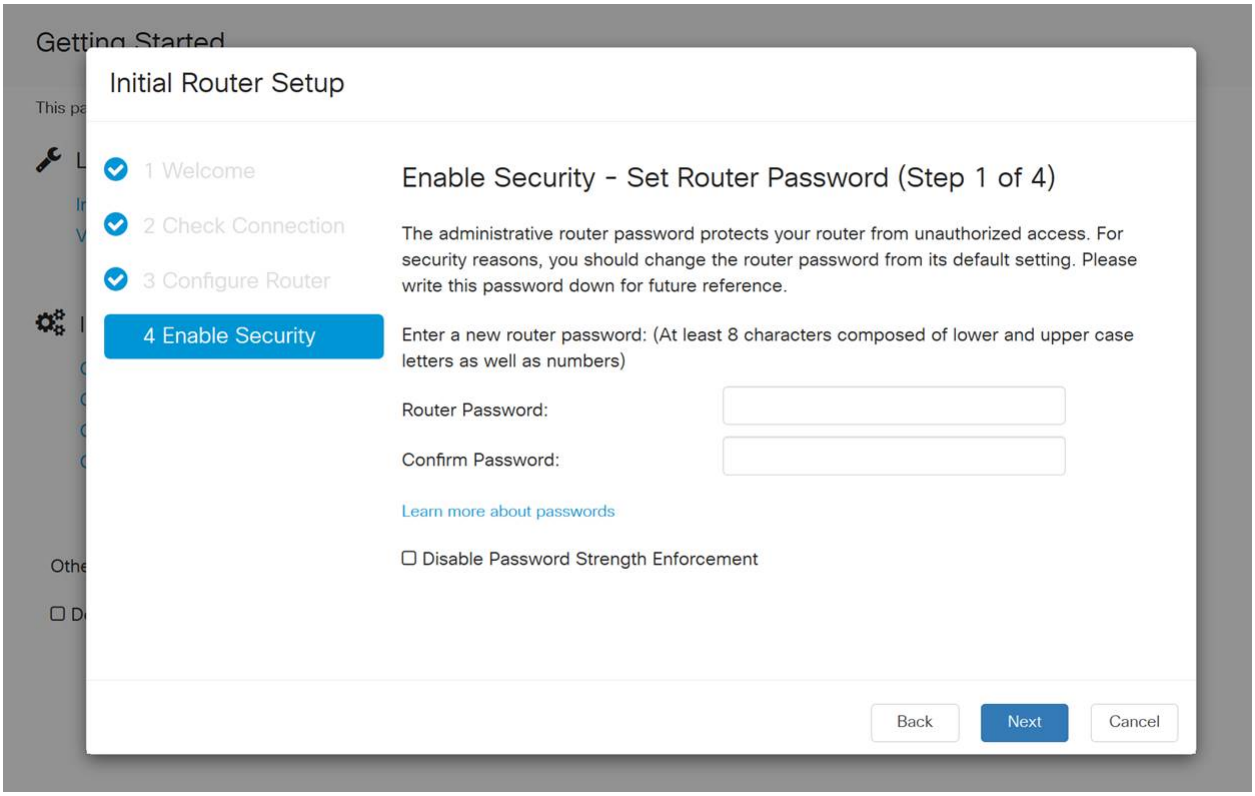
Étape 7

La page suivante récapitule les options sélectionnées. Vérifiez et cliquez sur **Suivant** si vous êtes satisfait.



Étape 8

Pour l'étape suivante, vous allez sélectionner un mot de passe à utiliser lors de la connexion au routeur. Les mots de passe doivent contenir au moins 8 caractères (majuscules et minuscules) et des chiffres. **Entrez un mot de passe** conforme aux exigences de résistance. Cliquez sur Next (Suivant). Prenez note de votre mot de passe pour les connexions futures.



Il *n*'est *pas* recommandé de sélectionner Désactiver l'*application de la force du mot de passe*. Cette option vous permet de sélectionner un mot de passe aussi simple que 123, ce qui serait aussi facile que 1-2-3 pour les acteurs malveillants de craquer.

Étape 9

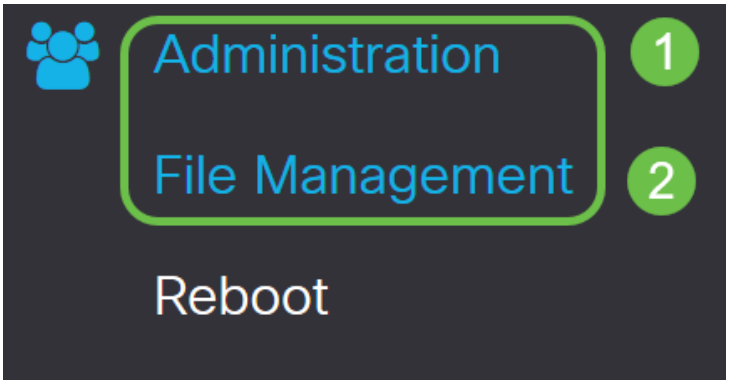
Cliquez sur l'**icône Enregistrer**.

Mettre à niveau le micrologiciel si nécessaire

Il s'agit d'une section importante, ne l'échappe pas !

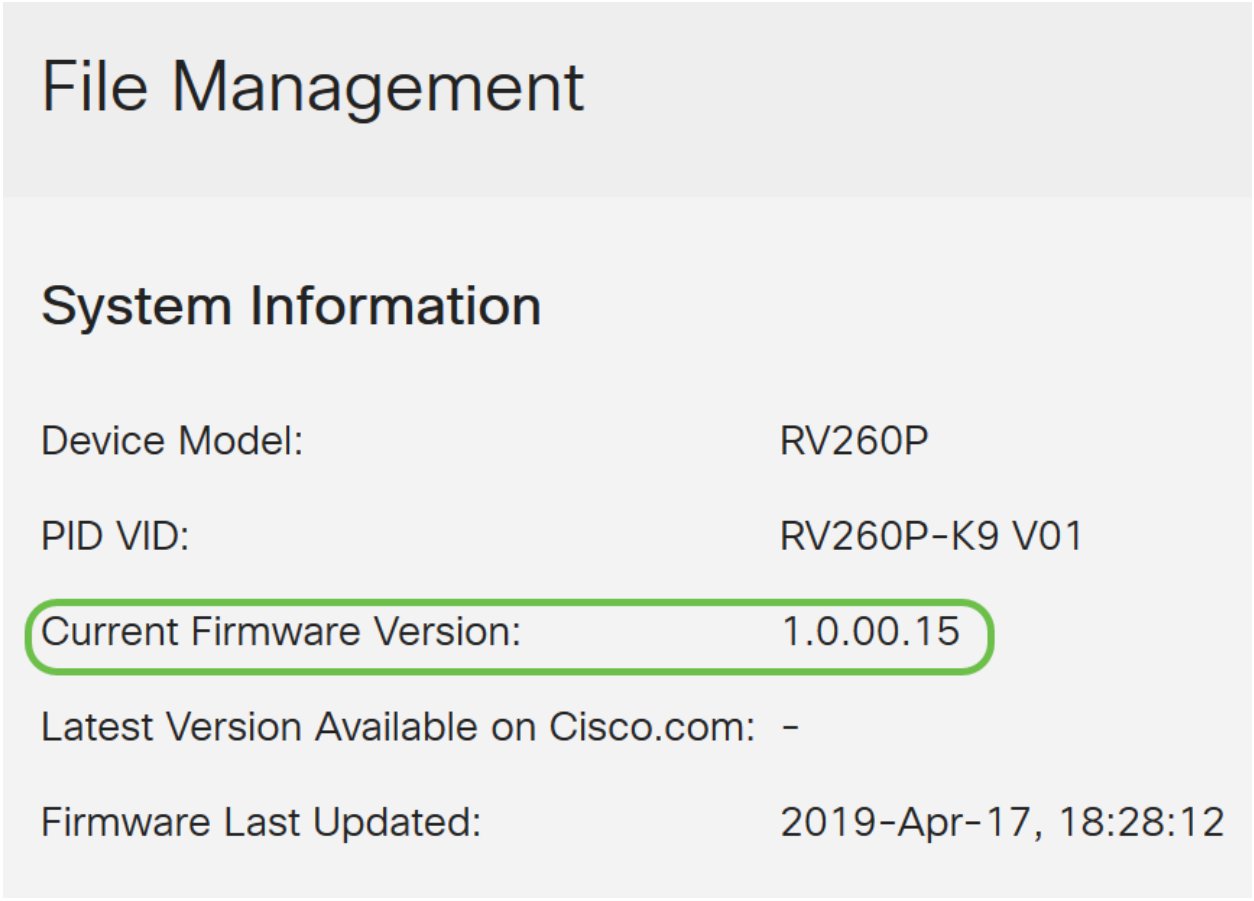
Étape 1

Choisissez **Administration > File Management**.



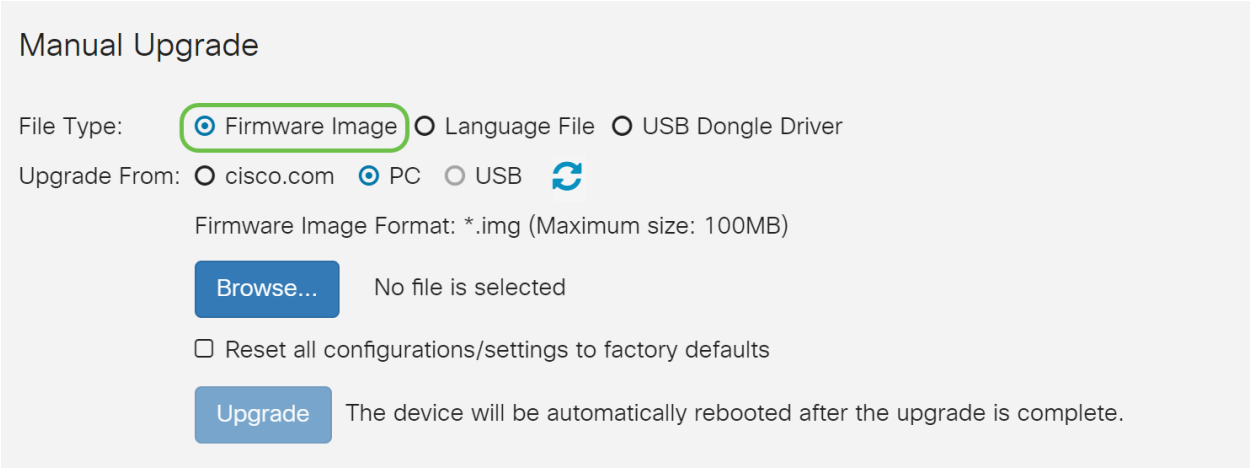
Dans la zone *Informations système*, les sous-zones suivantes décrivent les éléments suivants :

- Device Model (Modèle de périphérique) : affiche le modèle de votre périphérique.
- PID VID - ID de produit et ID de fournisseur du routeur.
- Version actuelle du micrologiciel : micrologiciel en cours d'exécution sur le périphérique.
- Dernière version disponible sur Cisco.com - Dernière version du logiciel disponible sur le site Web de Cisco.
- Dernière mise à jour du micrologiciel : date et heure de la dernière mise à jour du micrologiciel effectuée sur le routeur.



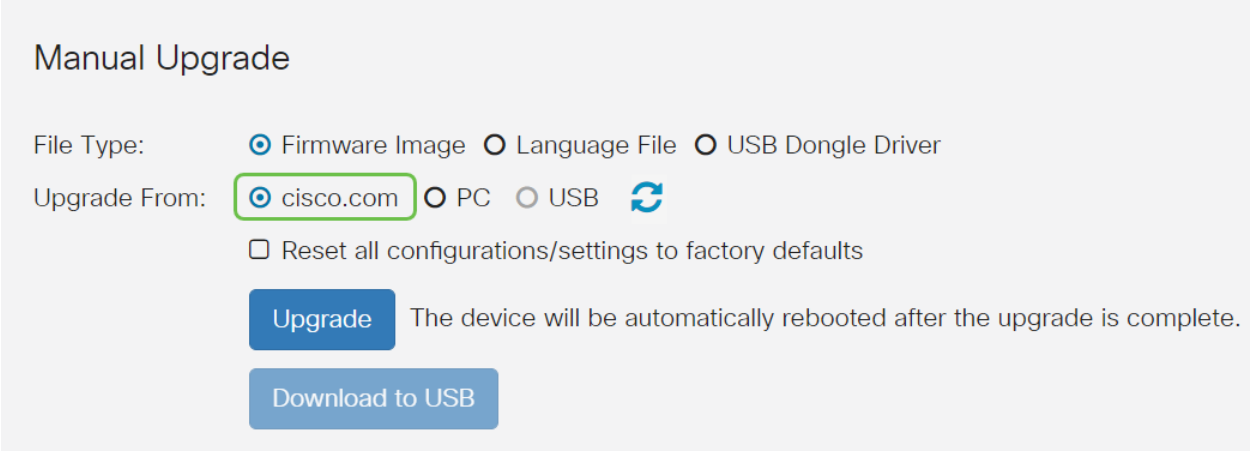
Étape 2

Sous la section *Mise à niveau manuelle*, cliquez sur la case d'option **Image du micrologiciel** pour *Type de fichier*.



Étape 3

Sur la page *Manual Upgrade*, cliquez sur une case d'option pour sélectionner cisco.com. Il y a quelques autres options pour cela, mais c'est la façon la plus facile de faire une mise à niveau. Ce processus installe le dernier fichier de mise à niveau directement à partir de la page Web Téléchargements de logiciels Cisco.

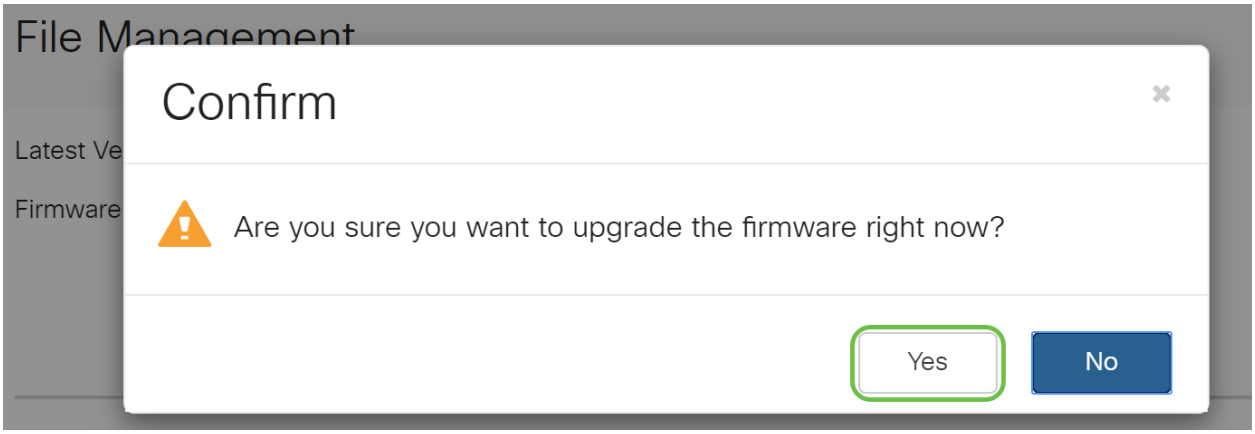


Étape 4

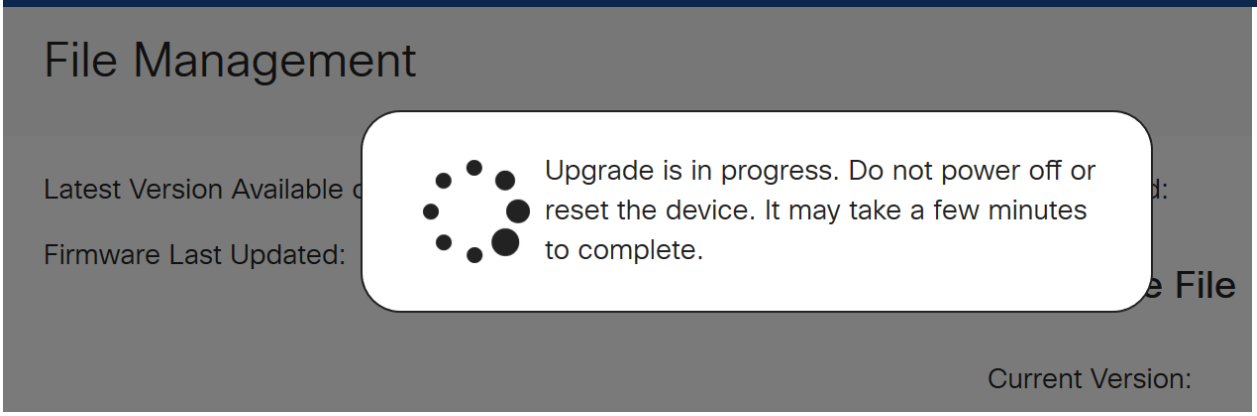
Cliquez sur **Mise à niveau**.

Étape 5

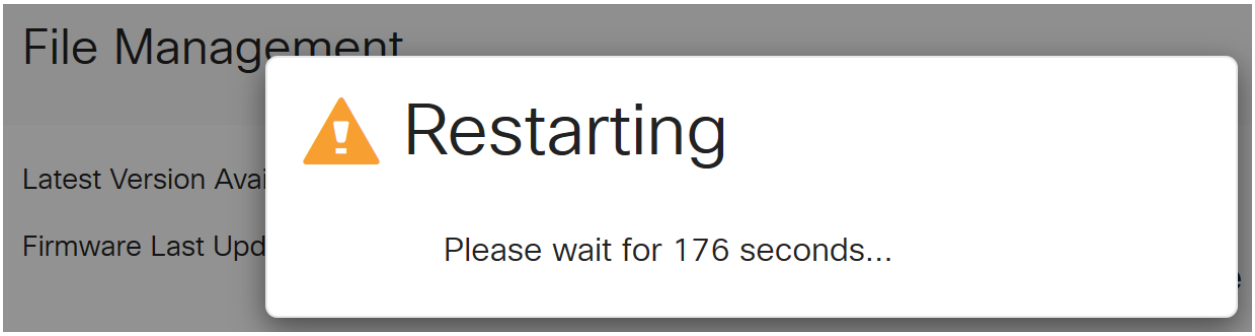
Cliquez sur **Oui** dans la fenêtre de confirmation pour continuer.



Le processus de mise à jour doit s'exécuter sans interruption. Le message suivant s'affiche alors que la mise à niveau est en cours.

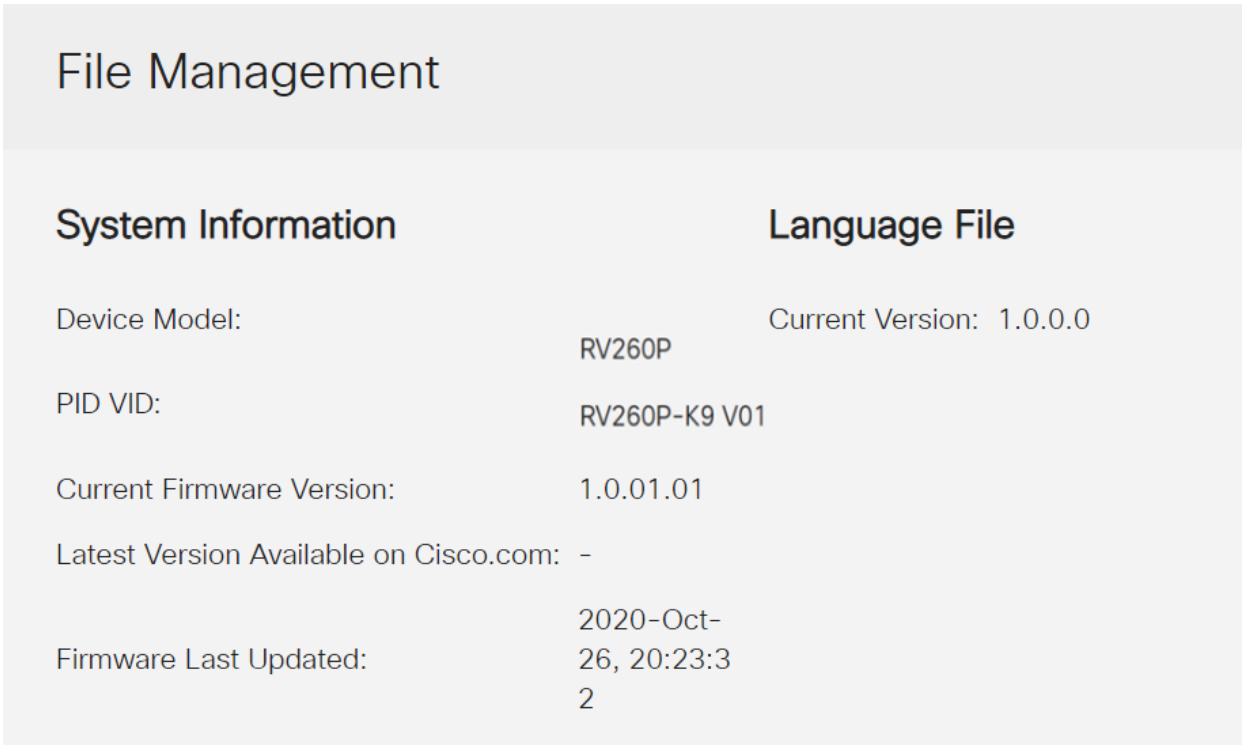


Une fois la mise à niveau terminée, une fenêtre de notification s'affiche pour vous informer que le routeur va *redémarrer* avec un compte à rebours du temps estimé pour la fin du processus. Ensuite, vous serez déconnecté.



Étape 6

Reconnectez-vous à l'utilitaire Web pour vérifier que le micrologiciel du routeur a été mis à niveau, faites défiler jusqu'à *Informations système*. La zone *Version actuelle du micrologiciel* doit maintenant afficher la version mise à niveau du micrologiciel.



Félicitations, vos paramètres de base sur votre routeur sont terminés ! Certaines options de configuration vont de l'avant.

Je vous encourage à continuer de parcourir l'article pour en savoir plus sur ces options et si elles s'appliquent à vous. Si vous préférez, vous pouvez cliquer sur l'un des liens hypertexte pour accéder à une section.

- Configuration des VLAN (facultatif)
- Modifier l'adresse IP (facultatif)
- Ajouter des adresses IP statiques (facultatif)
- Je suis prêt à configurer la partie sans fil maillé de mon réseau !

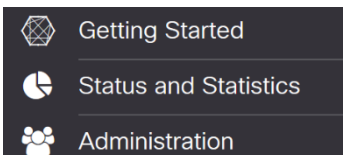
Configuration des VLAN (facultatif)

Un réseau local virtuel (VLAN) vous permet de segmenter logiquement un réseau local (LAN) en différents domaines de diffusion. Dans les scénarios où des données sensibles peuvent être diffusées sur un réseau, des VLAN peuvent être créés pour améliorer la sécurité en désignant une diffusion à un VLAN spécifique. Les VLAN peuvent également être utilisés pour améliorer les performances en réduisant la nécessité d'envoyer des diffusions et des multidiffusions vers des destinations inutiles. Vous pouvez créer un VLAN, mais cela n'a aucun effet tant que le VLAN n'est pas connecté à au moins un port, manuellement ou dynamiquement. Les ports doivent toujours appartenir à un ou plusieurs VLAN.

Si vous ne voulez pas créer de VLAN, vous pouvez passer à la section suivante.

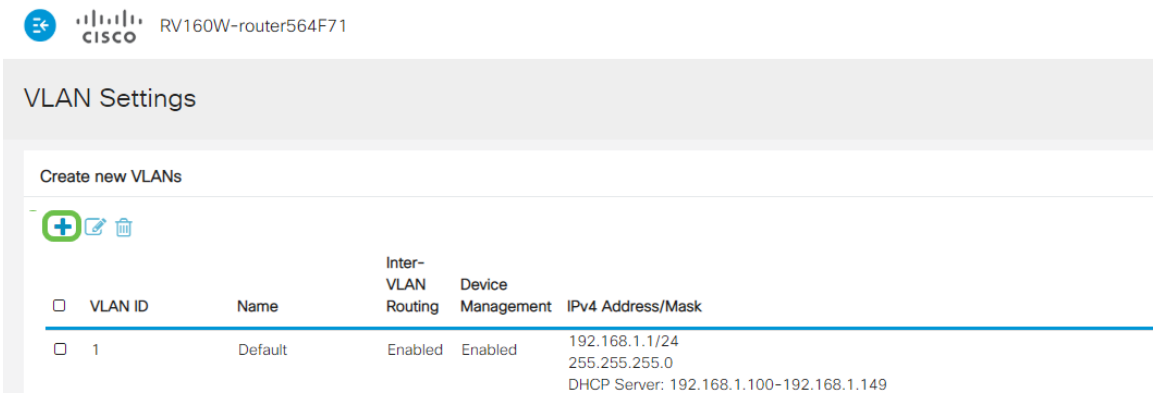
Étape 1

Accédez à **LAN > VLAN Settings**.



Étape 2

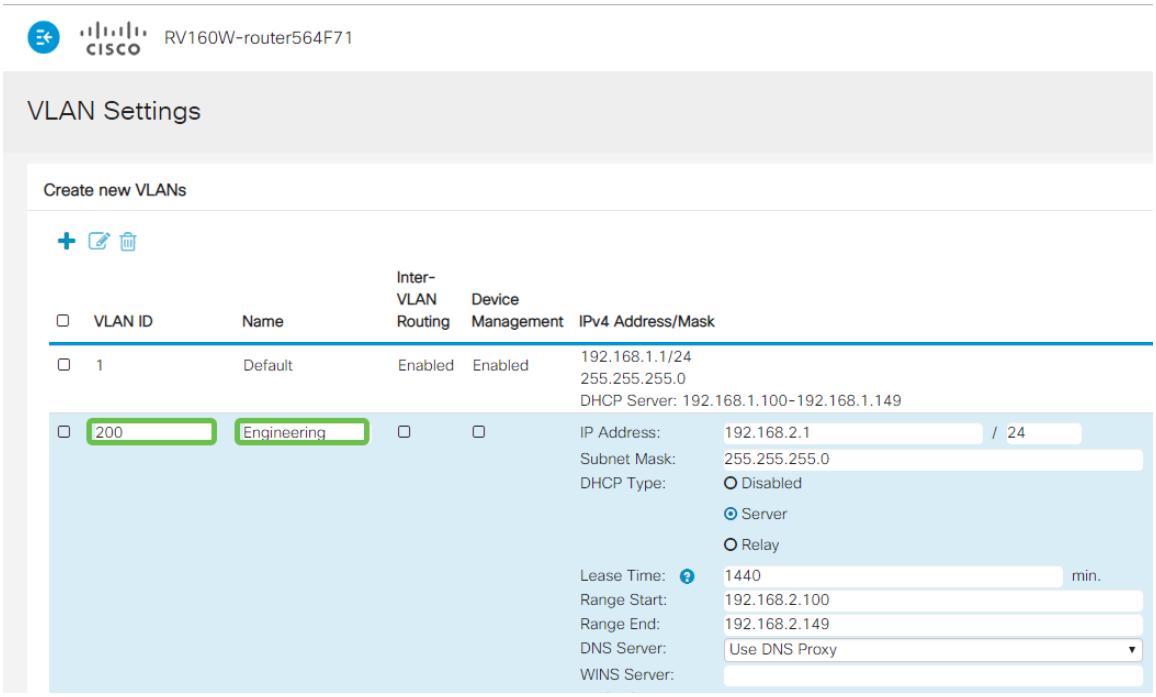
Cliquez sur **Add** pour créer un nouveau VLAN.



Étape 3

Entrez l'*ID de VLAN* que vous voulez créer et un *nom* pour celui-ci. La plage *ID de VLAN* est comprise entre 1 et 4 093.

Nous avons entré **200** comme *ID de VLAN* et **Engineering** comme *Nom* pour le VLAN.



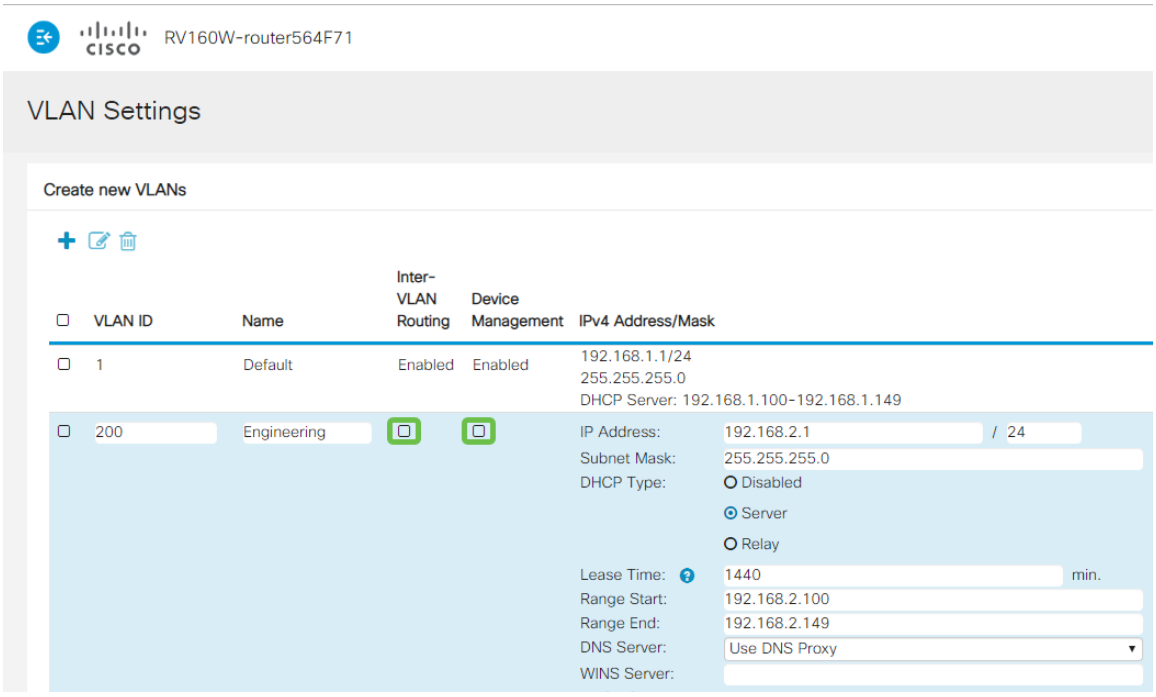
Étape 4

Décochez la case *Enabled* pour le *routage inter-VLAN* et *la gestion des périphériques* si vous le souhaitez.

Le routage inter-VLAN est utilisé pour acheminer les paquets d'un VLAN à un autre VLAN. En règle générale, cela n'est pas recommandé pour les réseaux invités car vous voudrez isoler les utilisateurs invités, ce qui rend les VLAN moins sécurisés. Il peut être nécessaire que les VLAN se routent entre eux. Si c'est le cas, consultez Routage inter-VLAN sur un routeur RV34x avec restrictions de liste de contrôle d'accès ciblée pour configurer le trafic spécifique que vous autorisez entre les VLAN.

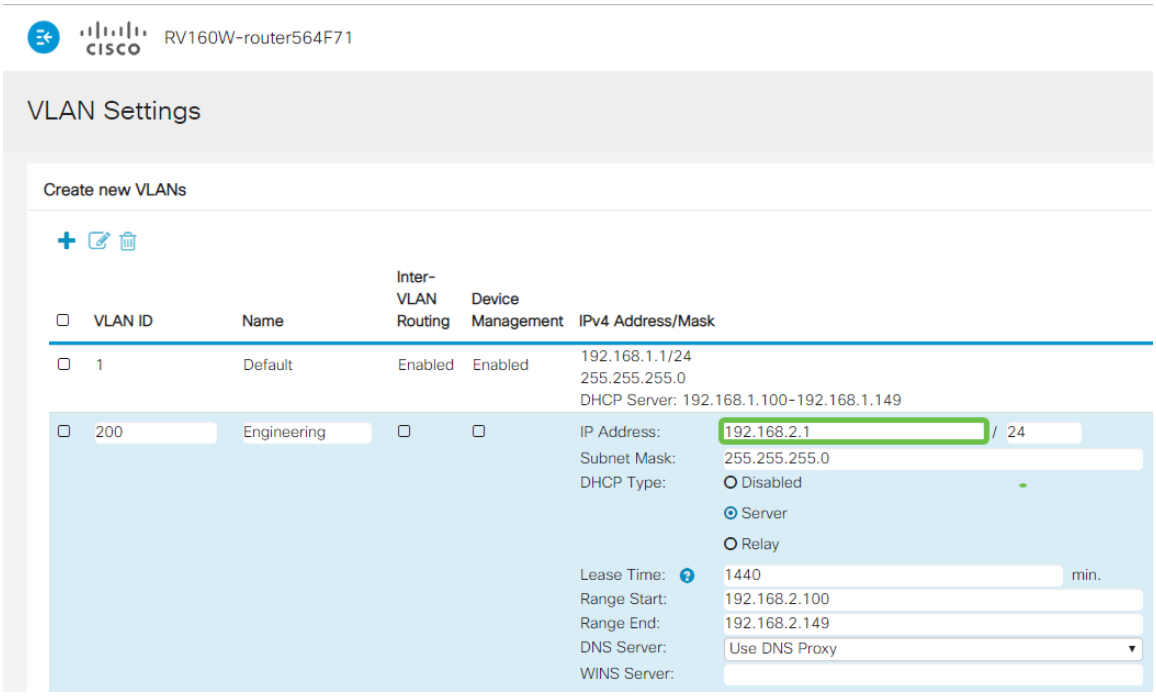
Device Management est le logiciel qui vous permet d'utiliser votre navigateur pour vous connecter à l'interface utilisateur Web du RV260P, à partir du VLAN, et de gérer le RV260P. Ceci doit également être désactivé sur les réseaux invités.

Dans cet exemple, nous n'avons pas activé ni le *routage inter-VLAN* ni *la gestion des périphériques* pour sécuriser davantage le VLAN.



Étape 5

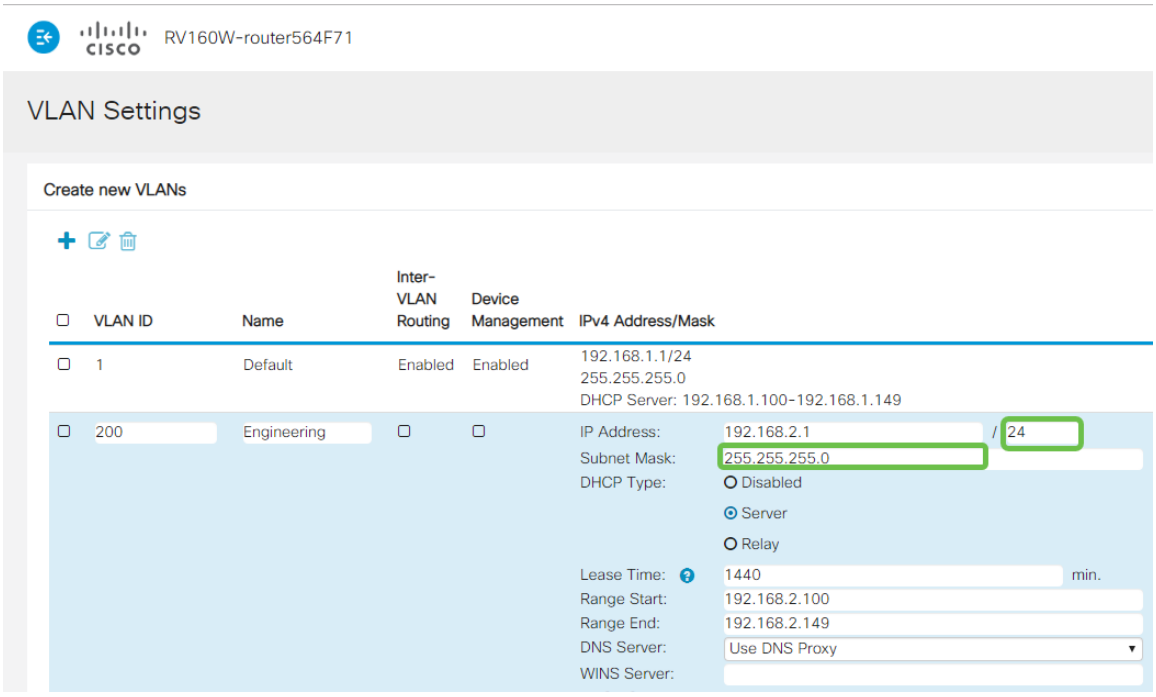
L'adresse IPv4 privée est automatiquement renseignée dans le champ *Adresse IP*. Vous pouvez ajuster ceci si vous le souhaitez. Dans cet exemple, le sous-réseau a 192.168.2.100-192.168.2.149 adresses IP disponibles pour DHCP. 192.168.2.1-192.168.2.99 et 192.168.2.150-192.168.2.254 sont disponibles pour les adresses IP statiques.



Étape 6

Le masque de sous-réseau sous *Masque de sous-réseau* sera renseigné automatiquement. Si vous apportez des modifications, le champ sera automatiquement ajusté.

Pour cette démonstration, nous quitterons le *masque de sous-réseau* en **255.255.255.0** ou **/24**.



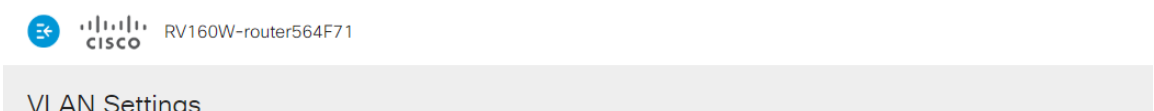
Étape 7

Sélectionnez un *type DHCP (Dynamic Host Configuration Protocol)*. Les options suivantes sont disponibles :

Disabled : désactive le serveur DHCP IPv4 sur VLAN. Ceci est recommandé dans un environnement de test. Dans ce scénario, toutes les adresses IP doivent être configurées manuellement et toutes les communications doivent être internes.

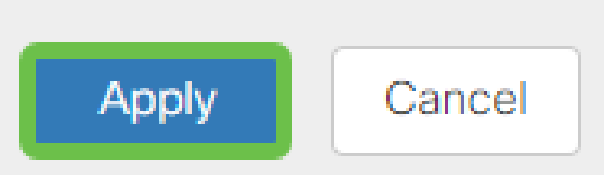
Serveur : option la plus souvent utilisée.

- Lease Time (Durée du bail) : saisissez une valeur de temps comprise entre 5 et 43 200 minutes. La valeur par défaut est 1 440 minutes (soit 24 heures).
- Range Start and Range End (Début et fin de la plage) : saisissez le début et la fin de la plage des adresses IP qui peuvent être attribuées dynamiquement.
- DNS Server (Serveur DNS) : sélectionnez cette option pour utiliser le serveur DNS en tant que proxy ou dans la liste déroulante ISP.
- WINS Server : saisissez le nom du serveur WINS.
- Options DHCP :
    - Option 66 : saisissez l'adresse IP du serveur TFTP.
    - Option 150 : saisissez l'adresse IP d'une liste de serveurs TFTP.
    - Option 67 - Entrez le nom du fichier de configuration.
- Relay : saisissez l'adresse IPv4 du serveur DHCP distant pour configurer l'agent de relais DHCP. Il s'agit d'une configuration plus avancée.



Étape 8

Cliquez sur **Apply** pour créer le nouveau VLAN.



Affecter des VLAN aux ports

16 VLAN peuvent être configurés sur le routeur RV260, avec un VLAN pour le réseau étendu (WAN). Les VLAN qui ne sont pas sur un port doivent être *exclus*. Cela garde le trafic sur ce port exclusivement pour les VLAN/VLAN que l'utilisateur a spécifiquement attribués. Il s'agit d'une bonne pratique.

Les ports peuvent être définis comme un port d'accès ou un port agrégé :

- Port d'accès : un VLAN est attribué. Les trames non étiquetées sont transmises.
- Port trunk : peut transporter plusieurs VLAN. 802.1q. L'agrégation permet à un VLAN natif d'être déétiqueté. Les VLAN que vous ne voulez pas sur le trunk doivent être exclus.

Un VLAN a attribué son propre port :

- Considéré comme un port d'accès.
- Le VLAN affecté à ce port doit être étiqueté Non étiqueté.
- Tous les autres VLAN doivent être étiquetés Excluded pour ce port.

Deux VLAN ou plus qui partagent un port :

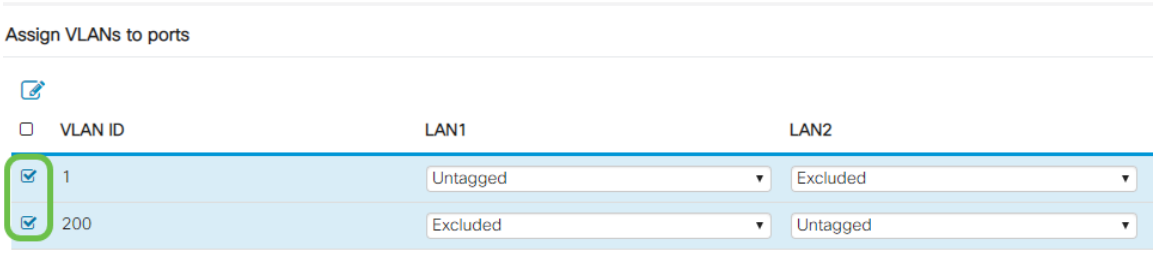
- Considéré comme un port agrégé.
- Un des VLAN peut être étiqueté Untagged.
- Les autres VLAN qui font partie du port agrégé doivent être étiquetés Tagged.
- Les VLAN qui ne font pas partie du port agrégé doivent être étiquetés Excluded pour ce port.

Remarque : Dans cet exemple, il n'y a pas de jonctions.

Étape 9

Sélectionnez les *ID de VLAN* à modifier. Cliquez sur Edit.

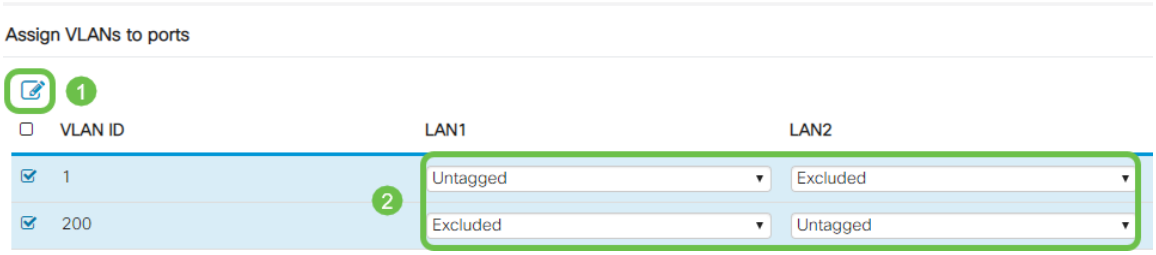
Dans cet exemple, nous avons sélectionné *VLAN 1* et *VLAN 200*.



Étape 10

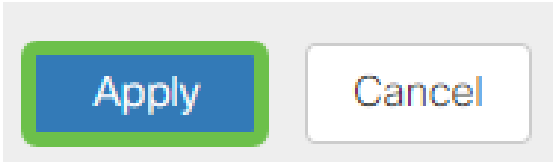
Cliquez sur **Edit** pour affecter un VLAN à un port LAN et spécifiez chaque paramètre comme *Tagged*, *Untagged* ou *Excluded*.

Dans cet exemple, sur le LAN1, nous avons attribué le VLAN 1 comme **Non étiqueté** et le VLAN 200 comme **Excluded**. Pour le LAN2, nous avons attribué le VLAN 1 comme **Excluded** et le VLAN 200 comme **Untagged**.



Étape 11

Cliquez sur **Apply** pour enregistrer la configuration.



Vous devez maintenant avoir créé un nouveau VLAN et configuré les VLAN sur les ports du RV260. Répétez le processus de création des autres VLAN. Par exemple, VLAN300 sera créé pour Marketing avec un sous-réseau de 192.168.3.x et VLAN400 sera créé pour Accounting avec un sous-réseau de 192.168.4.x.

C'est l'essentiel des VLAN. Cliquez sur le lien hypertexte pour en savoir plus sur les meilleures pratiques VLAN et les conseils de sécurité pour les routeurs professionnels Cisco.

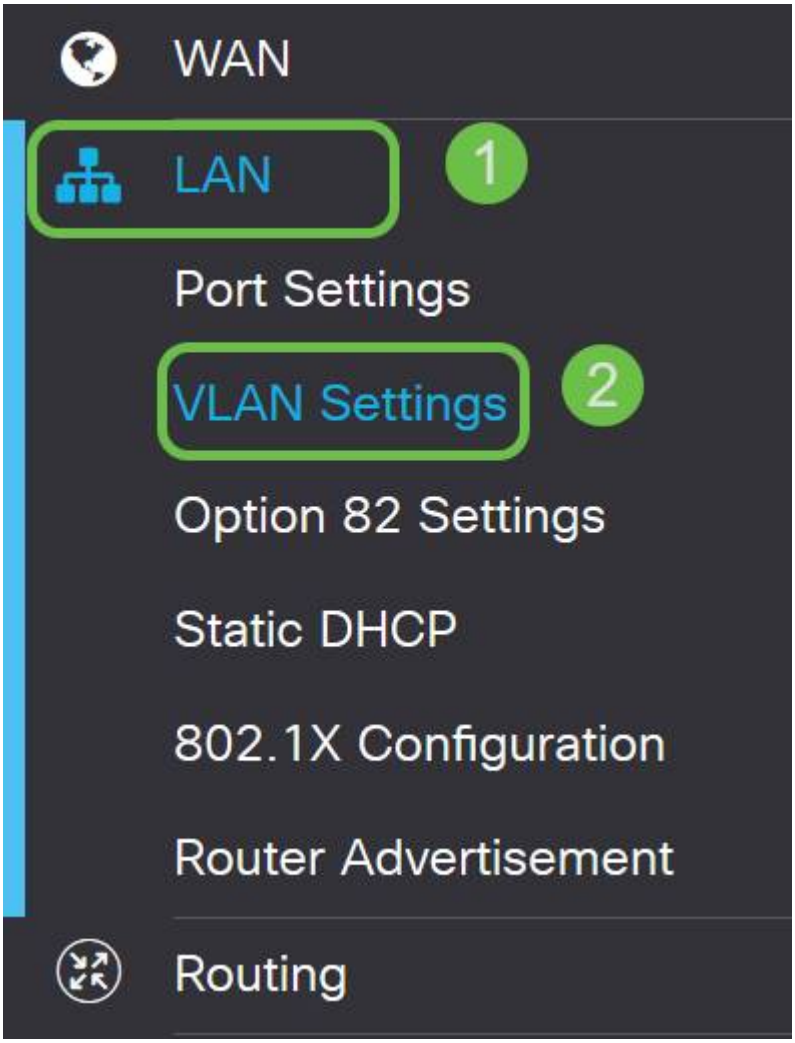
Modifier une adresse IP (facultatif)

Après avoir terminé l'*Assistant de configuration initiale*, vous pouvez définir une adresse IP statique sur le routeur en modifiant les paramètres VLAN. Ignorez la réexécution de l'assistant de configuration initiale. Pour effectuer cette modification, procédez comme suit.

Si vous n'avez pas besoin de modifier une adresse IP, vous pouvez passer à la section suivante de cet article.

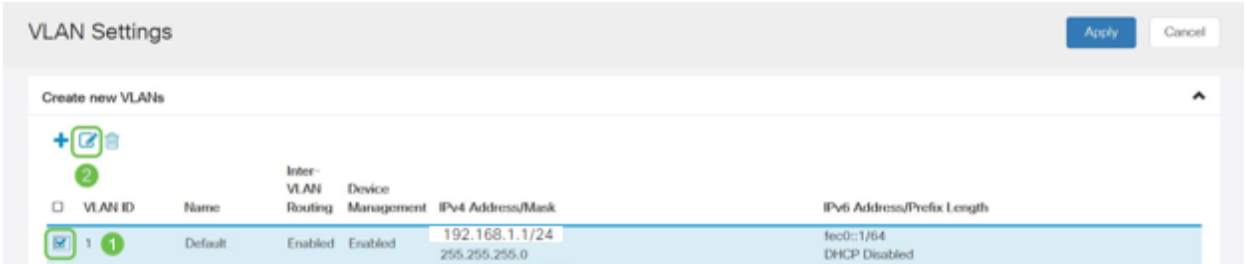
Étape 1

Dans la barre de menus de gauche, cliquez sur **LAN > VLAN Settings**.



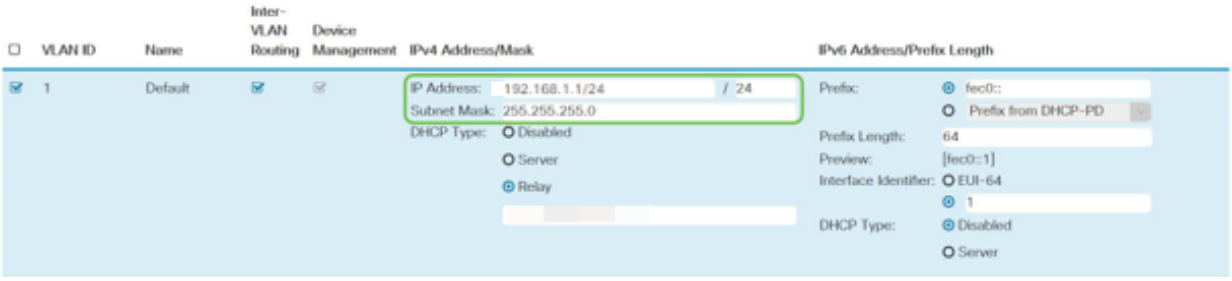
Étape 2

Sélectionnez ensuite le **VLAN** qui contient votre périphérique de routage, puis cliquez sur l'**icône de modification**.



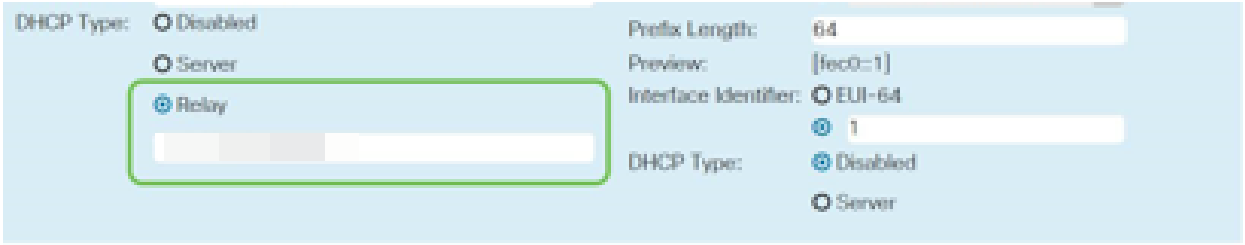
Étape 3

Entrez l'**adresse IP statique** souhaitée et cliquez sur **Apply** dans le coin supérieur droit.



Étape 4 (facultative)

Si votre routeur n'est pas le serveur/périphérique DHCP qui attribue des adresses IP, vous pouvez utiliser la fonction de relais DHCP pour diriger les requêtes DHCP vers une adresse IP spécifique. L'adresse IP est probablement le routeur connecté au WAN/Internet.



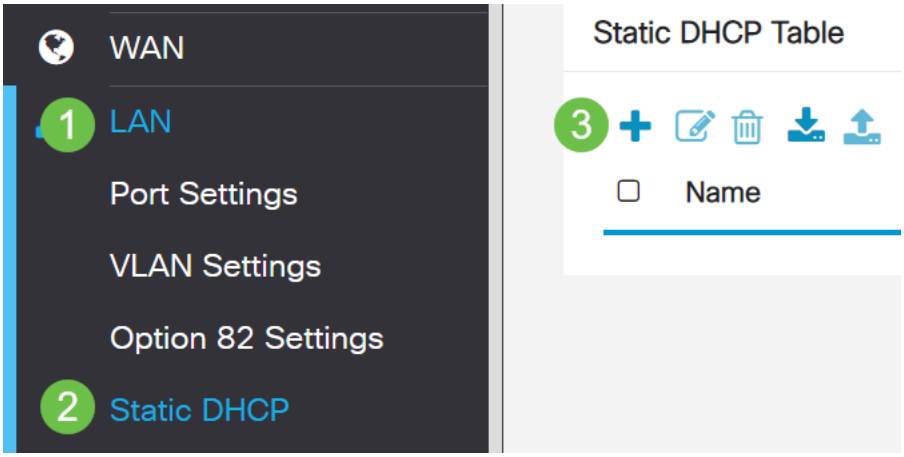
Ajouter une adresse IP statique

Si vous souhaitez qu'un périphérique donné soit accessible à d'autres VLAN, vous pouvez lui attribuer une adresse IP locale statique et créer une règle d'accès pour le rendre accessible. Cela ne fonctionne que si le routage inter-VLAN est activé. Il existe d'autres situations où une adresse IP statique peut être utile. Pour plus d'informations sur la définition des adresses IP statiques, consultez les Méthodes Recommandées pour la définition des adresses IP statiques sur le matériel Cisco Business.

Si vous n'avez pas besoin d'ajouter une adresse IP statique, vous pouvez passer à la section suivante de cet article pour configurer les points d'accès.

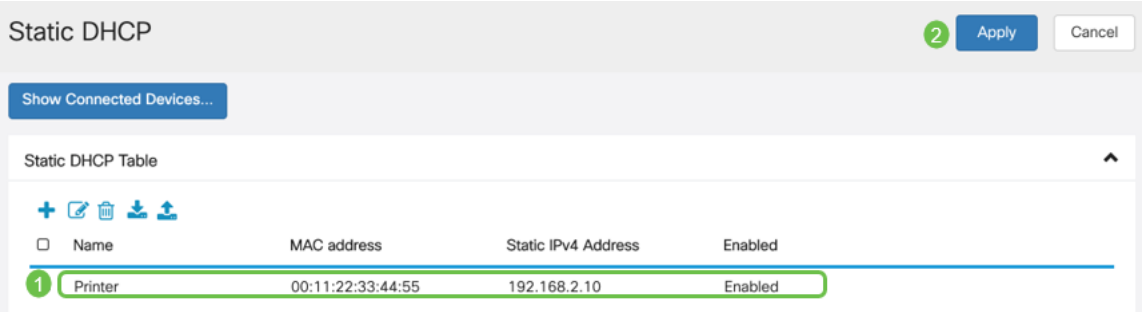
Étape 1

Accédez à **LAN > Static DHCP.** Cliquez sur l'**icône plus**.



Étape 2

Ajoutez les informations **DHCP statiques** pour le périphérique. Dans cet exemple, le périphérique est une imprimante.



Félicitations, vous avez terminé la configuration de votre routeur RV260P. Nous allons maintenant configurer vos périphériques Cisco Business Wireless.

Configuration du CBW140AC

CBW140AC prêt à l'emploi

Commencez par brancher un câble Ethernet du port PoE de votre CBW140AC sur un port PoE du RV260P. Les 4 premiers ports du RV260P peuvent fournir la technologie PoE, de sorte que chacun d'eux peut être utilisé.

Vérifiez l'état des voyants. Le démarrage du point d'accès prend environ 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 d'une unité à l'autre. Lorsque le voyant DEL clignote en vert, passez à l'étape suivante.

Le port de liaison ascendante PoE Ethernet sur le point d'accès principal ne peut être utilisé que pour fournir une liaison ascendante au réseau local, et NON pour se connecter à d'autres périphériques d'extension principaux ou maillés.

Si votre point d'accès n'est pas nouveau, assurez-vous qu'il est réinitialisé aux paramètres d'usine par défaut pour que le SSID *CiscoBusiness-Setup* s'affiche dans vos options Wi-Fi. Pour obtenir de l'aide, consultez Comment redémarrer et rétablir les paramètres d'usine par défaut sur les routeurs RV260.

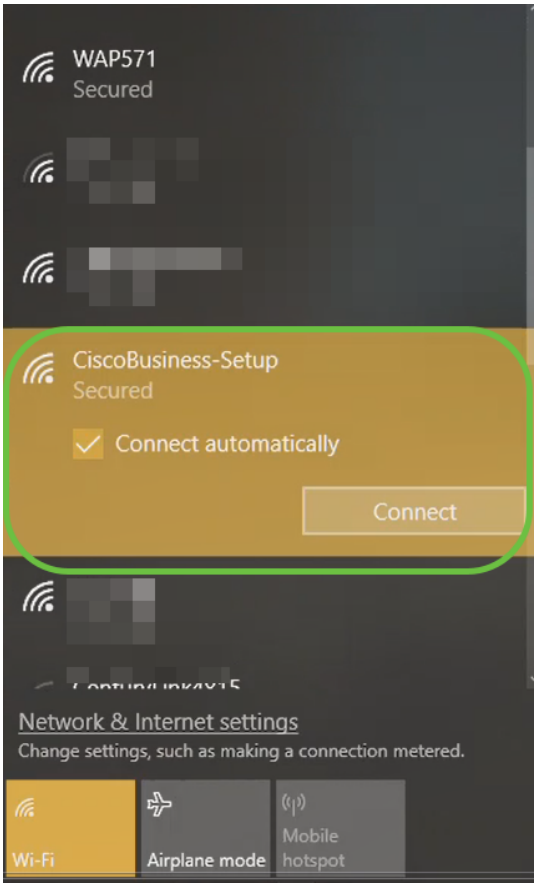
Configuration du point d'accès sans fil principal 140AC sur l'interface utilisateur Web

Vous pouvez configurer le point d'accès à l'aide de l'application mobile ou de l'interface utilisateur Web. Cet article utilise l'interface utilisateur Web pour la configuration, ce qui donne plus d'options pour la configuration mais est un peu plus compliqué. Si vous souhaitez utiliser l'application mobile pour les sections suivantes, cliquez sur pour accéder aux instructions de l'application mobile.

Si vous rencontrez des problèmes de connexion, reportez-vous à la section Conseils de dépannage sans fil de cet article.

Étape 1

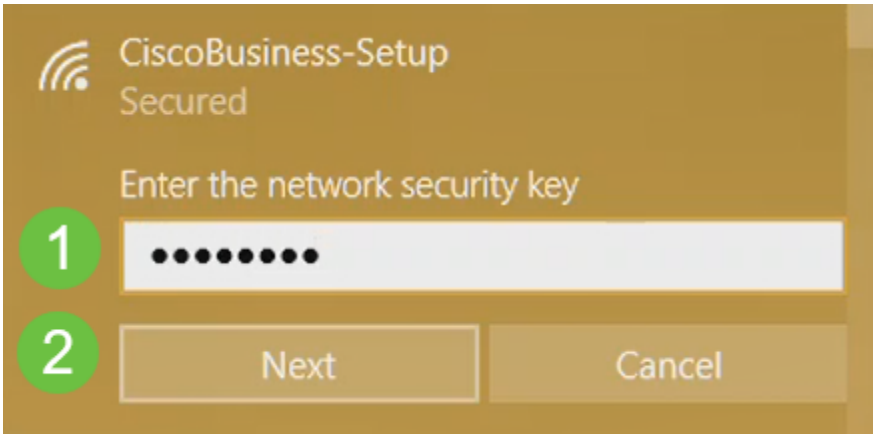
Sur votre ordinateur, cliquez sur l'**icône Wi-Fi** et choisissez *Cisco* Wireless Network *Business-Setup*. Cliquez sur Connect.



Si votre point d'accès n'est pas nouveau, assurez-vous qu'il est réinitialisé aux paramètres d'usine par défaut pour que le SSID *CiscoBusiness-Setup* s'affiche dans vos options Wi-Fi.

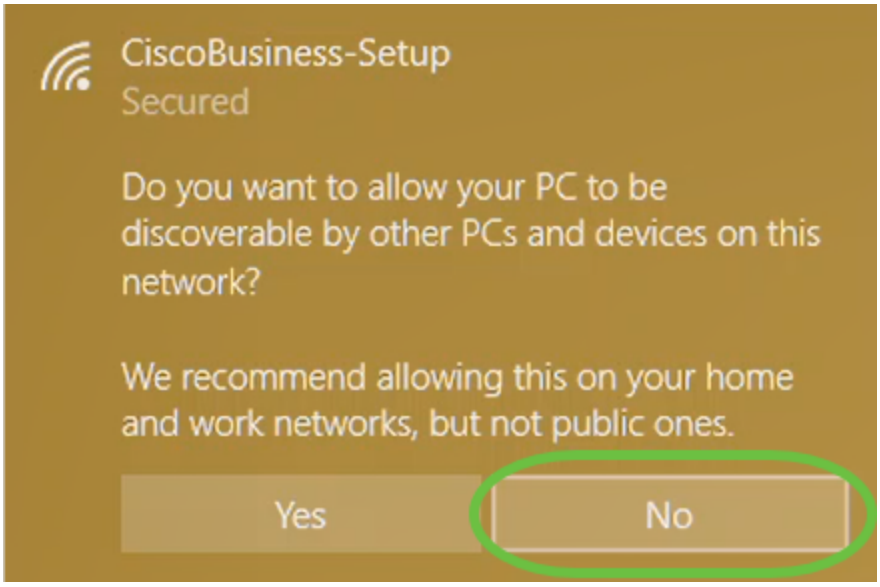
Étape 2

Saisissez la phrase de passe **cisco123** et cliquez sur **Next (Suivant)**.



Étape 3

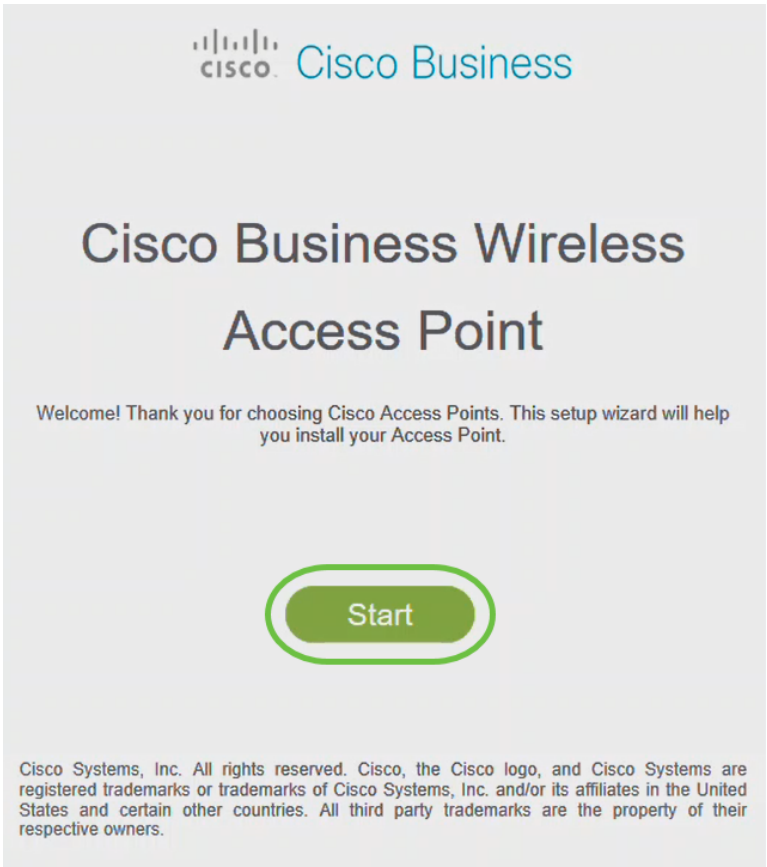
Vous obtiendrez l'écran suivant. Puisque vous ne pouvez configurer qu'un seul périphérique à la fois, cliquez sur **Non**.



Un seul périphérique peut être connecté au SSID *CiscoBusiness-Setup*. Si un second périphérique tente de se connecter, il ne pourra pas le faire. Si vous ne parvenez pas à vous connecter au SSID et que vous avez validé le mot de passe, un autre périphérique peut avoir établi la connexion. Redémarrez l'AP et réessayez.

Étape 4

Une fois connecté, le navigateur Web doit rediriger automatiquement vers l'assistant de configuration du point d'accès CBW. Sinon, ouvrez un navigateur Web, tel qu'Internet Explorer, Firefox, Chrome ou Safari. Dans la barre d'adresse, tapez **http://ciscobusiness.cisco** et appuyez sur **Entrée**. Cliquez sur **Démarrer** sur la page Web.



Si la page Web ne s'affiche pas, attendez quelques minutes de plus ou rechargez la page.

Après cette configuration initiale, vous utiliserez https://ciscobusiness.cisco pour vous connecter. Si votre navigateur Web est automatiquement renseigné avec *http://*, vous devez taper manuellement dans le *dossier https://* pour accéder à l'accès.

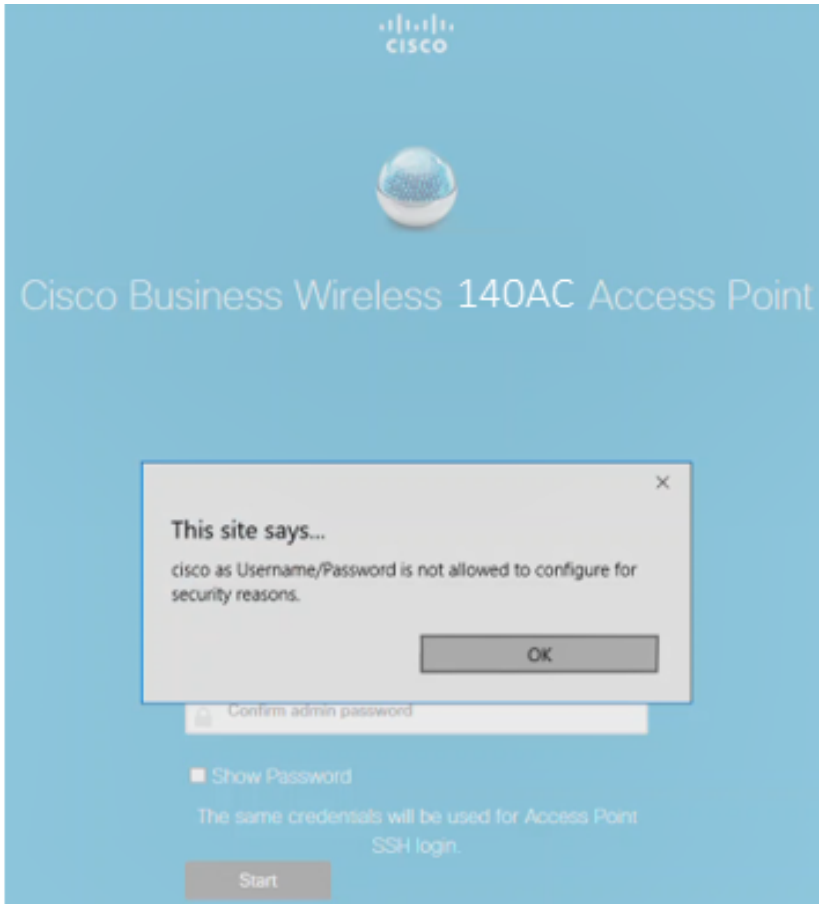
Étape 5

Créez un *compte d'administrateur* en saisissant les informations suivantes :

- Nom d'utilisateur Admin (24 caractères maximum)
- Mot de passe administrateur
- Confirmer le mot de passe admin

Vous pouvez choisir d'afficher le mot de passe en cochant la case *Afficher le mot de passe*. Cliquez sur **Démarrer**.

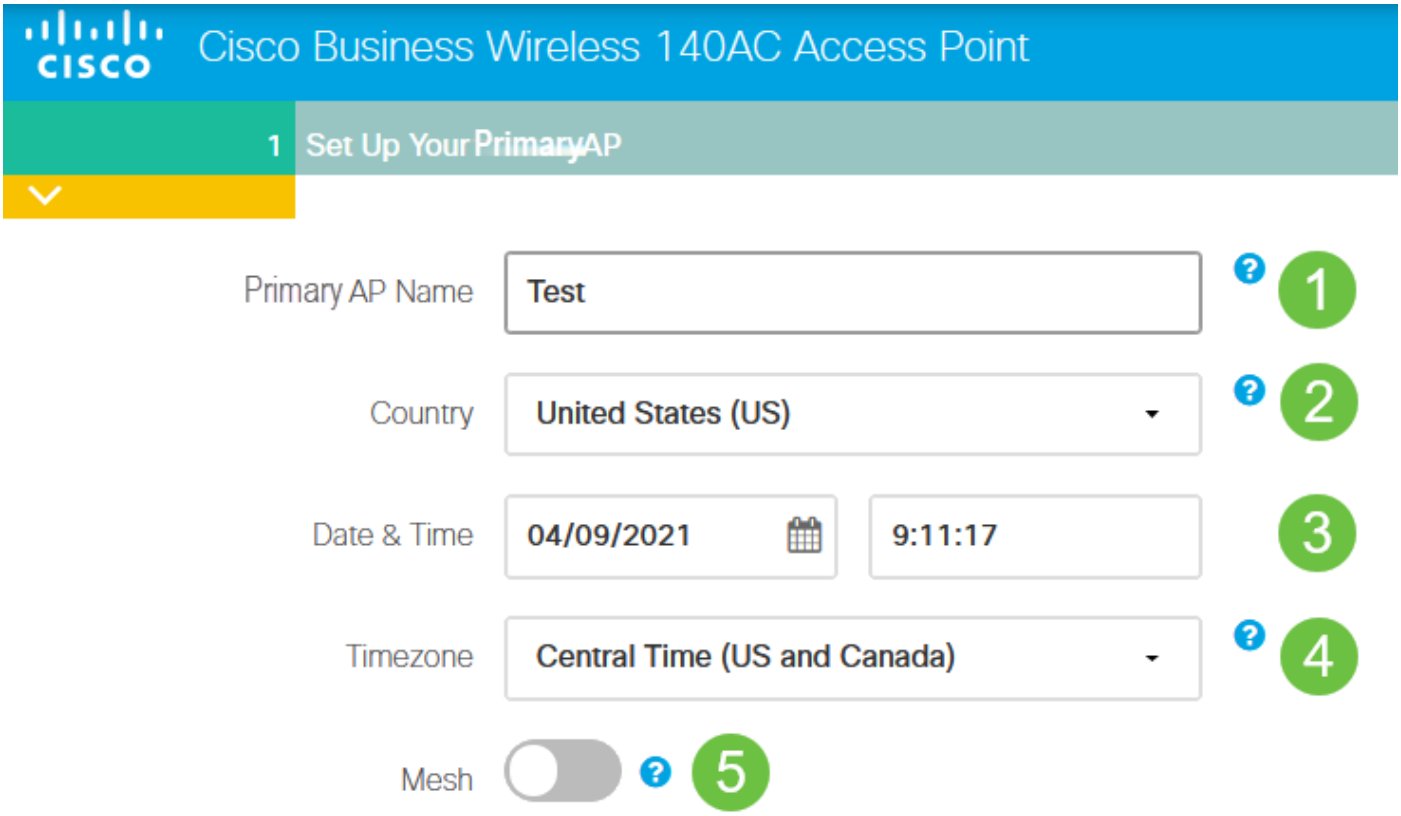
N'utilisez pas *cisco*, ni ses variantes dans les champs username ou password. Si vous le faites, vous obtiendrez un message d'erreur comme indiqué ci-dessous.



Étape 6

Configurez votre point d'accès principal en saisissant les éléments suivants :

- Nom du point d'accès principal
- Pays
- Date et heure
- Fuseau horaire
- Maillage



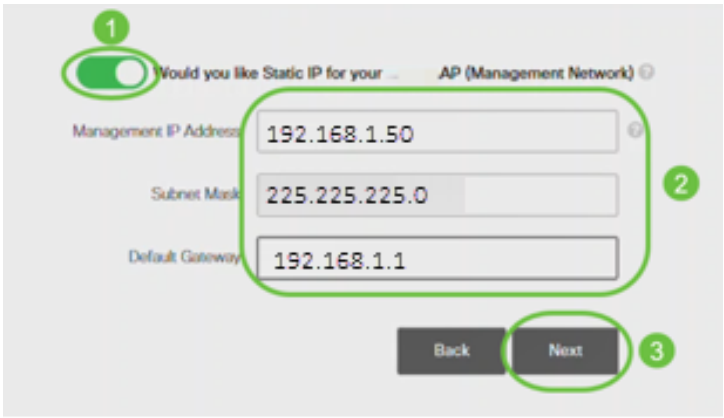
Le maillage ne doit être activé que si vous prévoyez de créer un réseau maillé. Par défaut, il est désactivé.

Étape 7

(Facultatif) Vous pouvez activer *l'IP statique pour votre* CBW140AC à des fins de gestion. Si ce n'est pas le cas, l'interface obtient une adresse IP de votre serveur DHCP. Pour configurer l'adresse IP statique, saisissez ce qui suit :

- Adresse IP de gestion
- Subnet Mask (Masque de sous-réseau)
- Passerelle par défaut

Cliquez sur Next (Suivant).



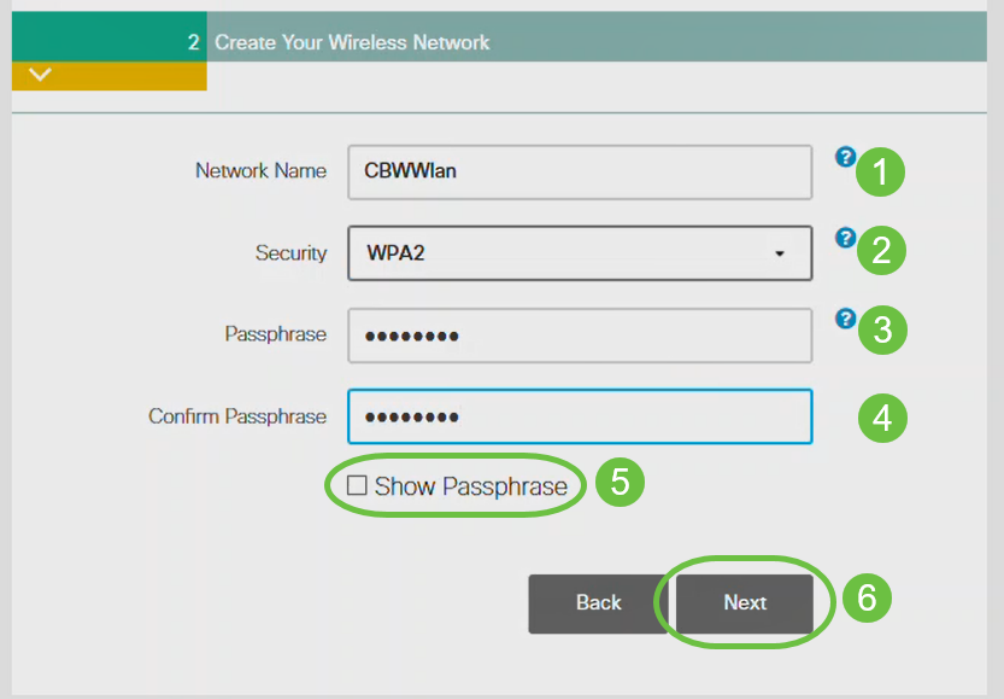
Par défaut, cette option est désactivée.

Étape 8

Créez vos réseaux sans fil en saisissant les informations suivantes :

- Nom du réseau
- Choisir la sécurité
- Phrase de passe
- Confirmer la phrase de passe
- (Facultatif) Cochez cette case pour afficher la phrase de passe.

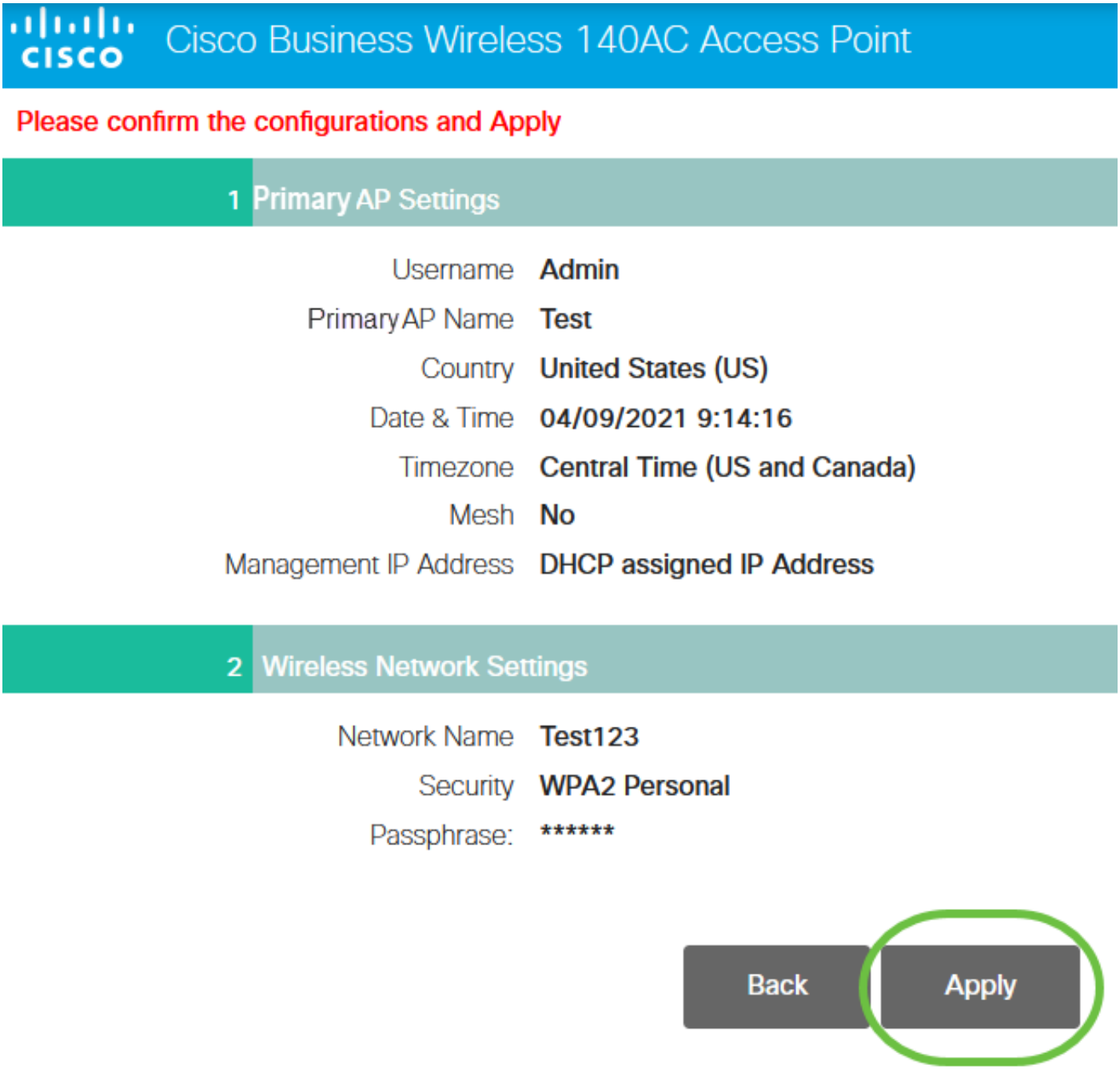
Cliquez sur Next (Suivant).



WPA2 (Wi-Fi Protected Access) version 2 (WPA2) est la norme actuelle de sécurité Wi-Fi.

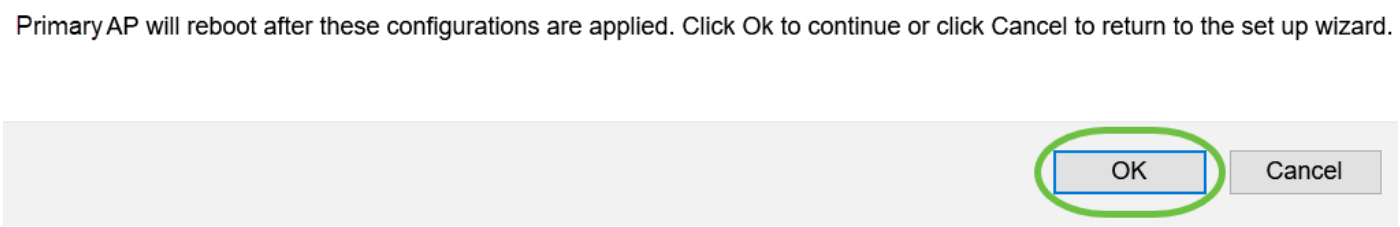
Étape 9

Confirmez les paramètres et cliquez sur **Apply**.

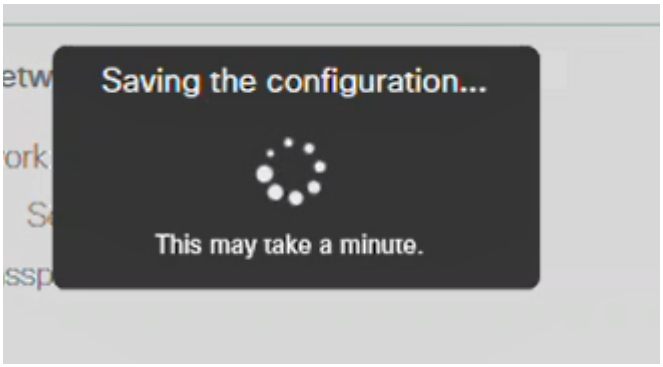


Étape 10

Cliquez sur **OK** pour appliquer les paramètres.



L'écran suivant s'affiche pendant l'enregistrement des configurations et le redémarrage du système. Cela peut prendre 10 minutes.

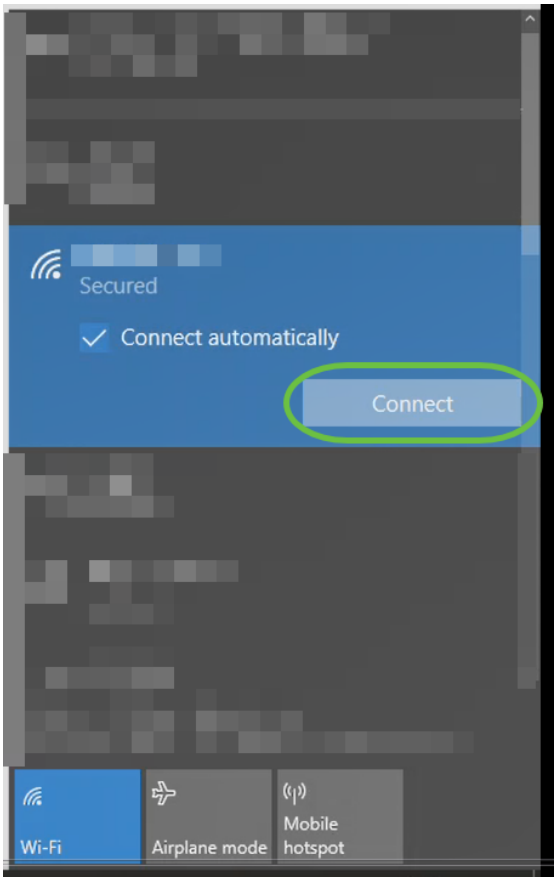


Au cours du redémarrage, la DEL du point d'accès passe par plusieurs modèles de couleurs. Lorsque le voyant clignote en vert, passez à l'étape suivante. Si le voyant ne dépasse pas le modèle clignotant rouge, il indique qu'il n'y a pas de serveur DHCP dans votre réseau. Assurez-vous que le point d'accès est connecté à un commutateur ou à un routeur avec un serveur DHCP.

Étape 11

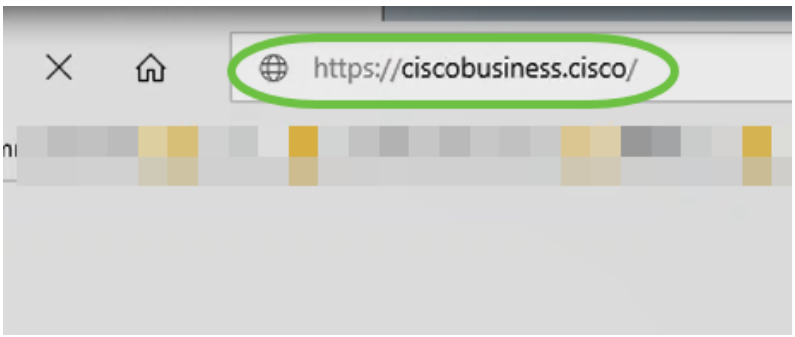
Accédez aux options sans fil de votre ordinateur et sélectionnez le réseau que vous avez configuré. Cliquez sur Connect.

Le SSID *CiscoBusiness-Setup* disparaîtra après le redémarrage.



Étape 12

Ouvrez un navigateur Web et tapez *https://[adresse IP du point d'accès CBW]*. Vous pouvez également taper *https://ciscobusiness.cisco* dans la barre d'adresse et appuyer sur Entrée.



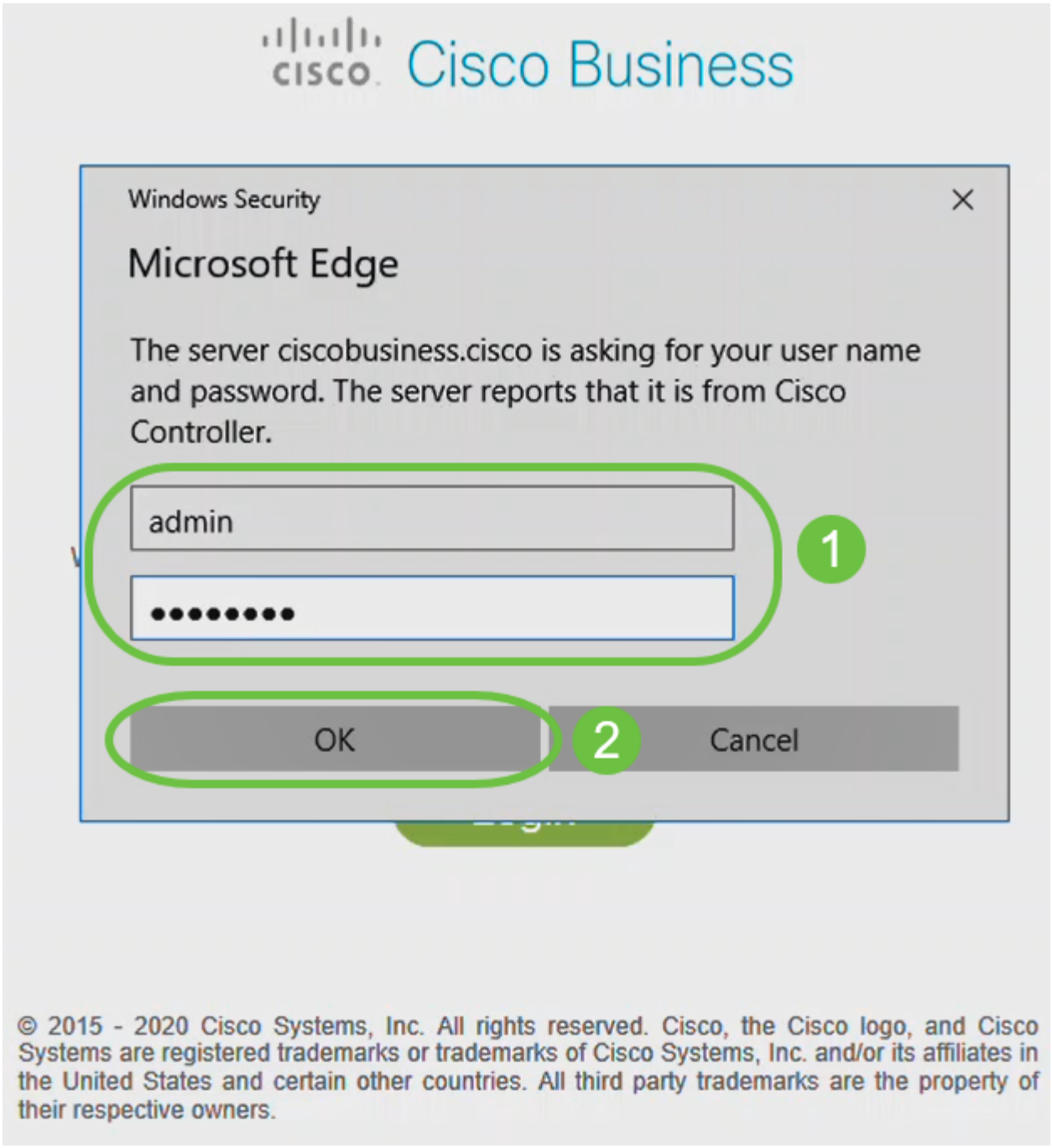
Assurez-vous que vous tapez *https* et non *http* à cette étape.

Étape 13

Cliquez sur **Connexion**.

Étape 14

Connectez-vous à l'aide des informations d'identification configurées. Click OK.



Étape 15

Vous pourrez accéder à la page Web UI de l'AP.

Conseils de dépannage sans fil

Si vous rencontrez des problèmes, consultez les conseils suivants :

- Assurez-vous que le SSID (Service Set Identifier) correct est sélectionné. Nom que vous avez créé pour le réseau sans fil.
- Déconnectez tout VPN pour l'application mobile ou sur un ordinateur portable. Vous pouvez même être connecté à un VPN que votre fournisseur de services mobiles utilise et que vous ne connaissez peut-être même pas. Par exemple, un téléphone Android (Pixel 3) avec Google Fi comme fournisseur de services, il existe un VPN intégré qui se connecte automatiquement sans notification. Cette opération doit être désactivée pour trouver le point d'accès principal.
- Connectez-vous au point d'accès principal avec https://<adresse IP du point d'accès principal>.
- Une fois la configuration initiale effectuée, assurez-vous que https:// is est utilisé, que vous vous connectiez à *ciscobusiness.cisco* ou en saisissant l'adresse IP dans votre navigateur Web. En fonction de vos paramètres, votre ordinateur peut être automatiquement renseigné avec http:// since qui est ce que vous avez utilisé la première fois que vous vous êtes connecté.
- Pour aider à résoudre les problèmes liés à l'accès à l'interface Web ou aux problèmes de navigateur pendant l'utilisation du point d'accès, dans le navigateur Web (Firefox dans ce cas), cliquez sur le menu Ouvrir, allez à Aide > Informations de dépannage et cliquez sur Actualiser Firefox.

Configurer les extendeurs de maillage CBW142ACM à l'aide de l'interface utilisateur Web

Vous êtes dans la partie principale de la configuration de ce réseau. Il vous suffit d'ajouter vos extendeurs de maillage !

Étape 1

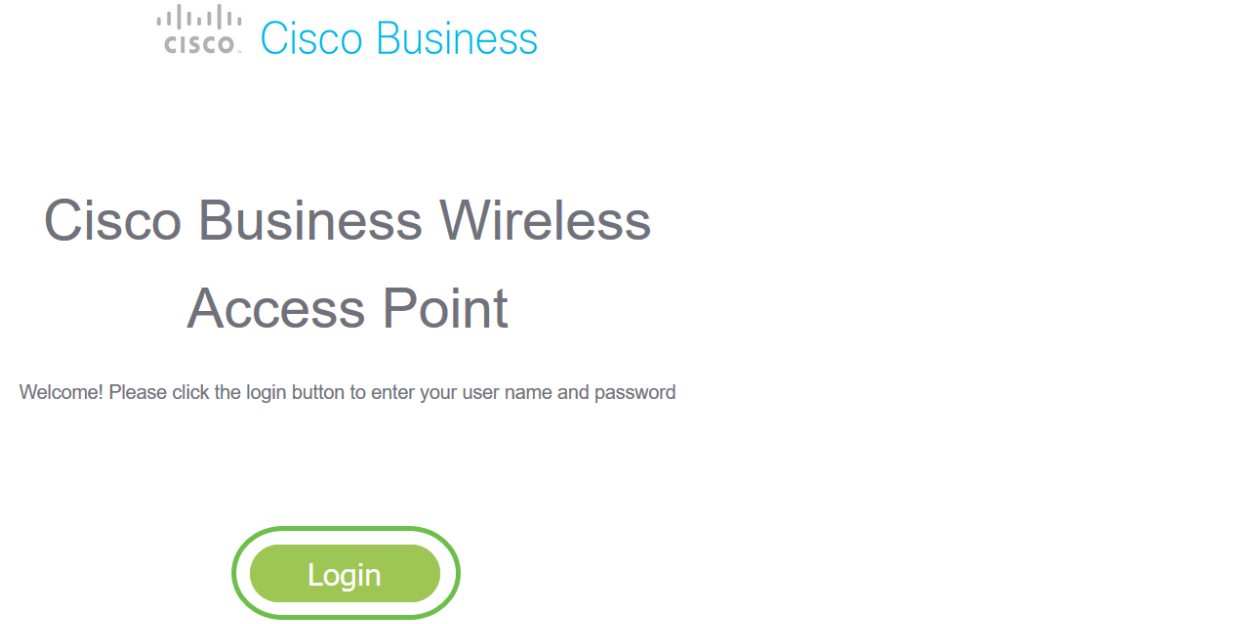
Branchez les deux extenseurs de maillage sur le mur aux emplacements sélectionnés. Notez l'adresse MAC de chaque extendeur de maillage.

Étape 2

Attendez environ 10 minutes que les extendeurs de maillage démarrent.

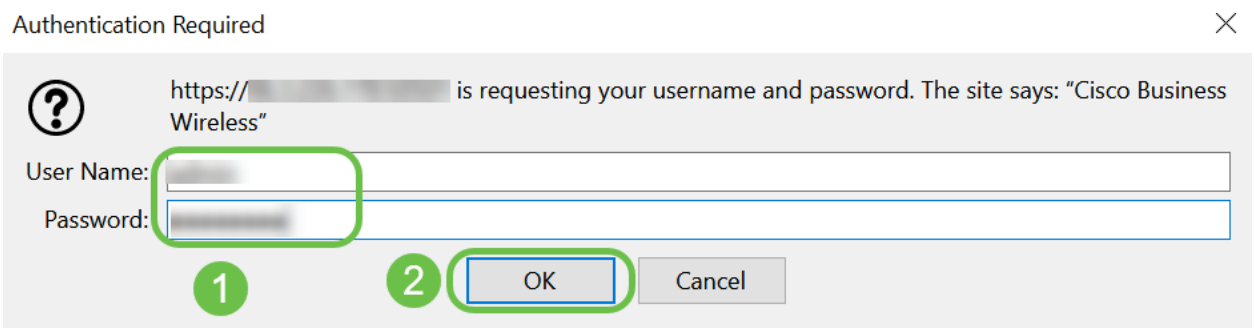
Étape 3

Saisissez l'adresse IP des points d'accès principaux (AP) dans le navigateur Web. Cliquez sur **Login** pour accéder au point d'accès principal.



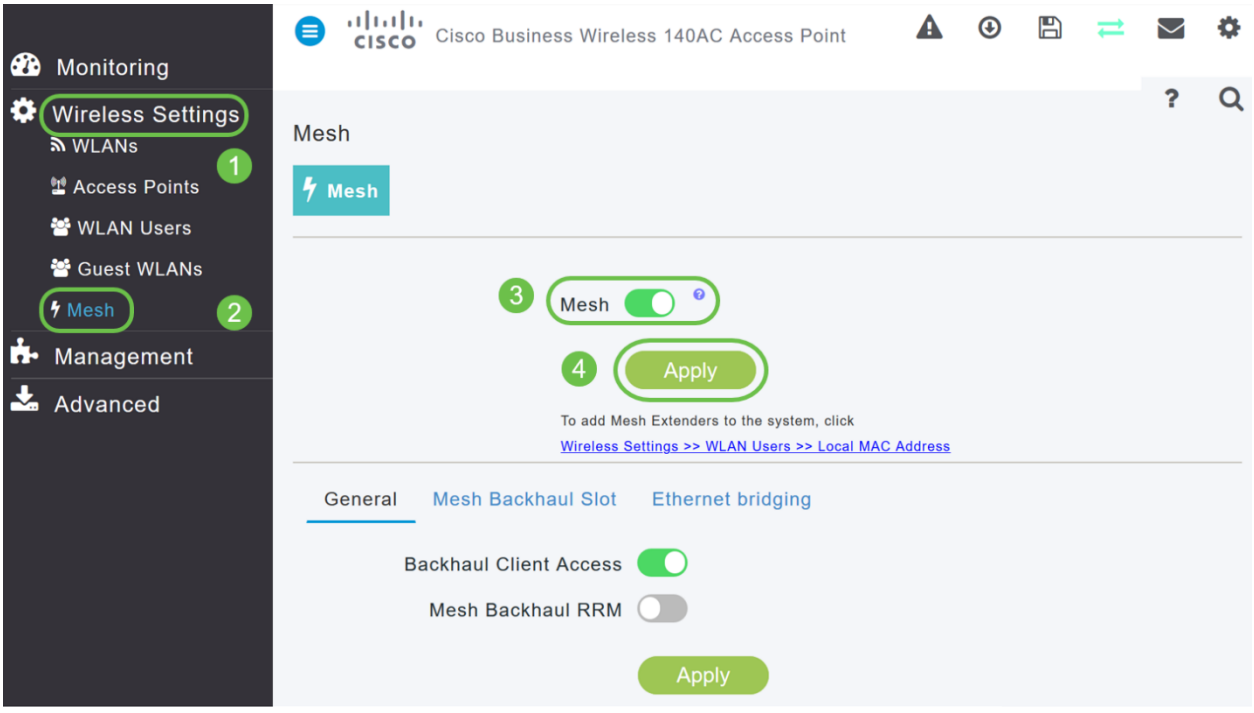
Étape 4

Entrez vos informations d'identification *User Name* et *Password* pour accéder au point d'accès principal. Click OK.



Étape 5

Accédez à **Wireless Settings > Mesh**. Assurez-vous que le *maillage* est activé. Cliquez sur Apply.

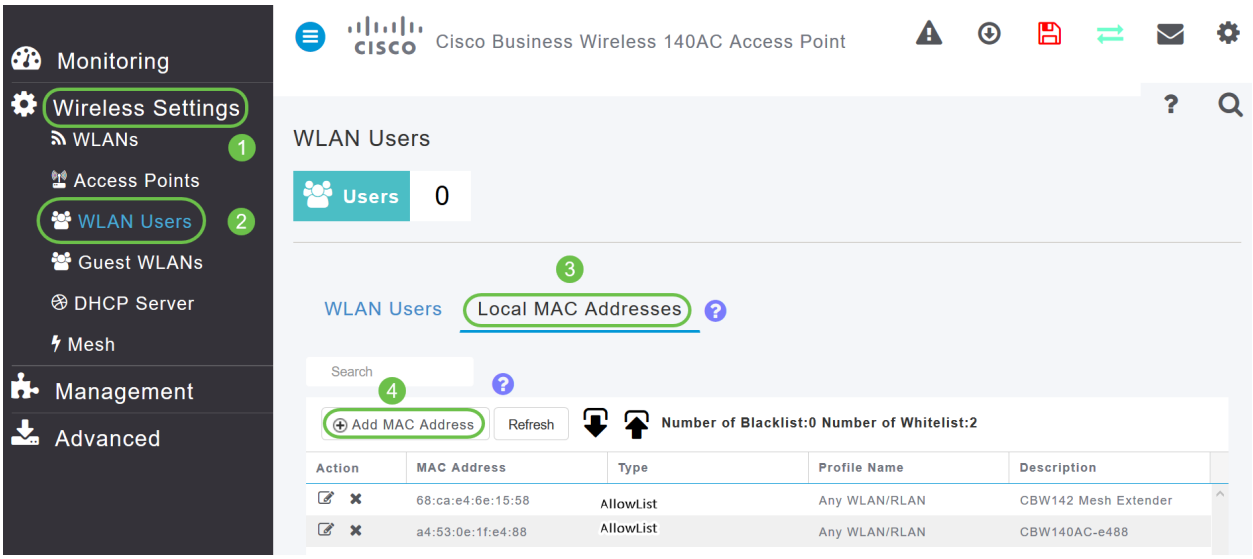


Étape 6

Si Mesh n'était pas déjà activé, le WAP peut avoir besoin d'effectuer un redémarrage. Une fenêtre contextuelle apparaît pour redémarrer. Confirmer. Cela prendra environ 10 minutes. Lors d'un redémarrage, 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 d'une unité à l'autre.

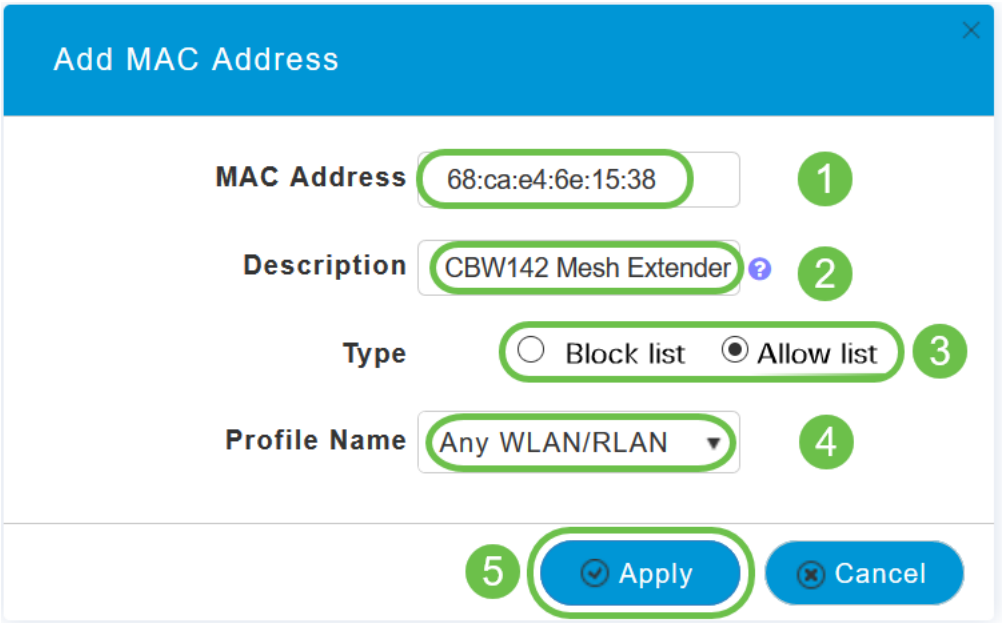
Étape 7

Accédez à **Wireless Settings > WLAN Users > Local MAC Addresses**. Cliquez sur **Ajouter une adresse MAC**.



Étape 8

Saisissez l'adresse MAC et la description de l'extendeur de maillage. Sélectionnez la liste *Type* comme Autorisé. Sélectionnez le *nom du profil* dans le menu déroulant. Cliquez sur Apply.



Étape 9

Veillez à enregistrer toutes vos configurations en appuyant sur l'**icône d'enregistrement** dans le volet supérieur droit de l'écran.

Répétez cette opération pour chaque extendeur de maillage.

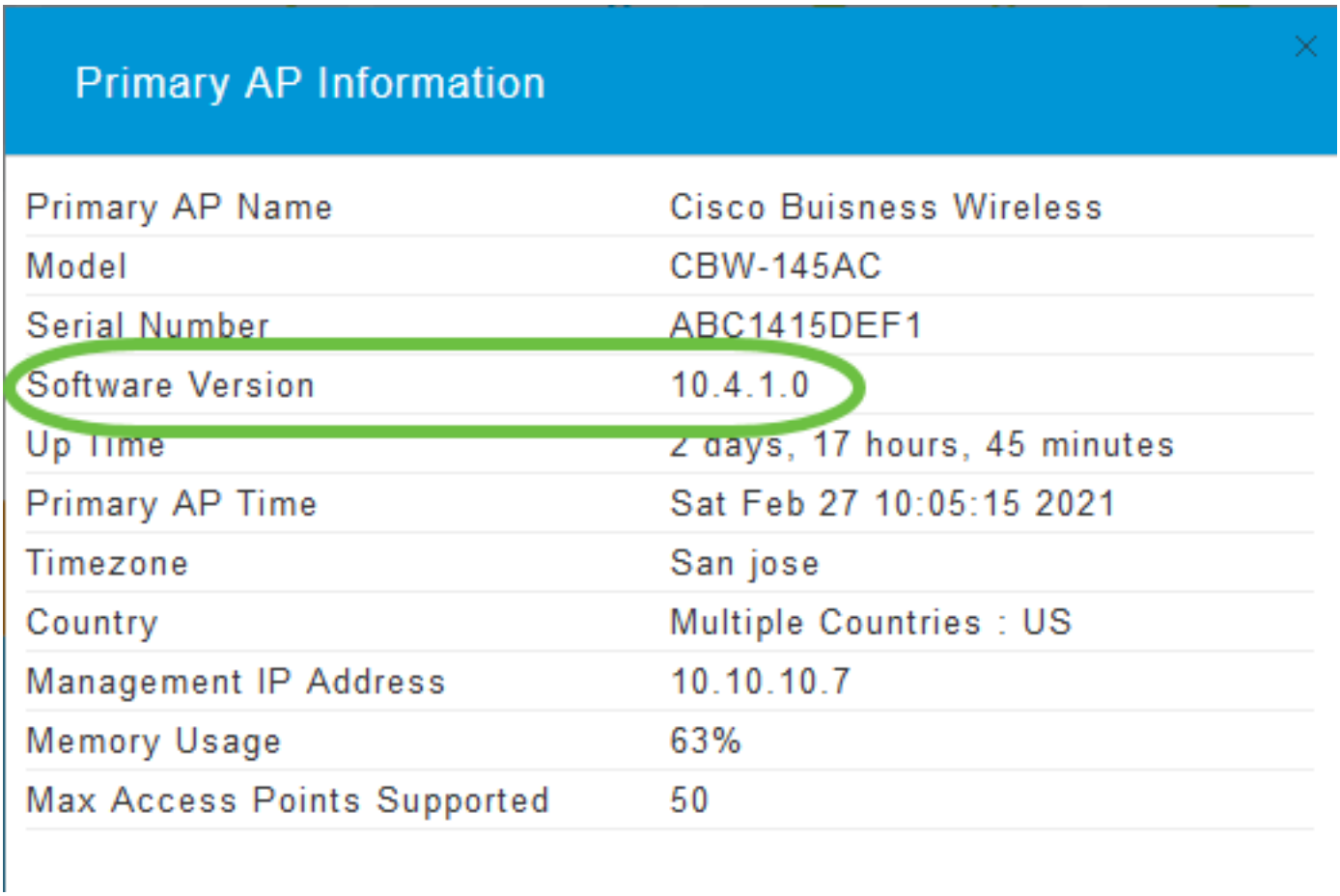
Vérification et mise à jour du logiciel à l'aide de l'interface utilisateur Web

Ne passez pas à côté de cette étape importante ! Il existe quelques façons de mettre à jour le logiciel, mais les étapes ci-dessous sont recommandées comme étant les plus faciles à exécuter lorsque vous utilisez l'interface utilisateur Web.

Pour afficher et mettre à jour la version logicielle actuelle de votre point d'accès principal, procédez comme suit.

Étape 1

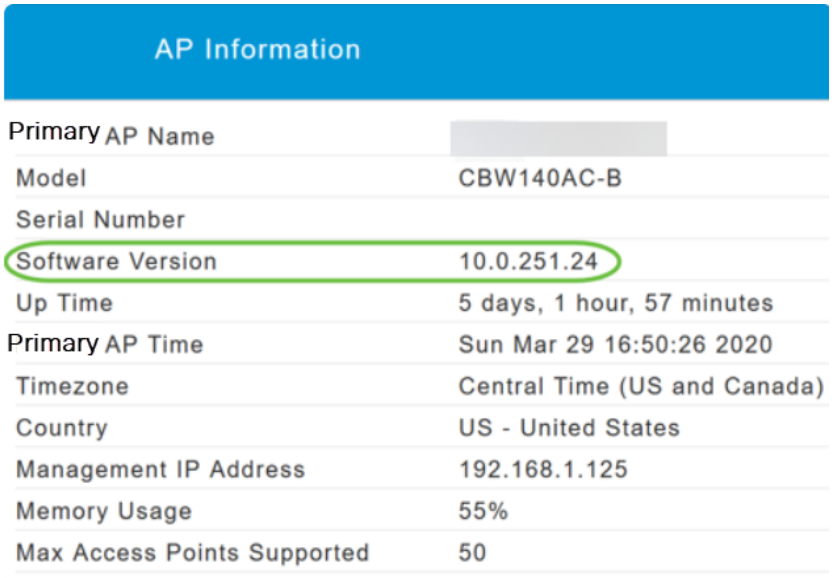
Cliquez sur l'**icône d'engrenage** dans le coin supérieur droit de l'interface Web, puis cliquez sur **Informations principales du point d'accès**.



Étape 2

Comparez la version en cours d'exécution à la dernière version du logiciel. Fermez la

fenêtre une fois que vous savez si vous devez mettre à jour le logiciel.

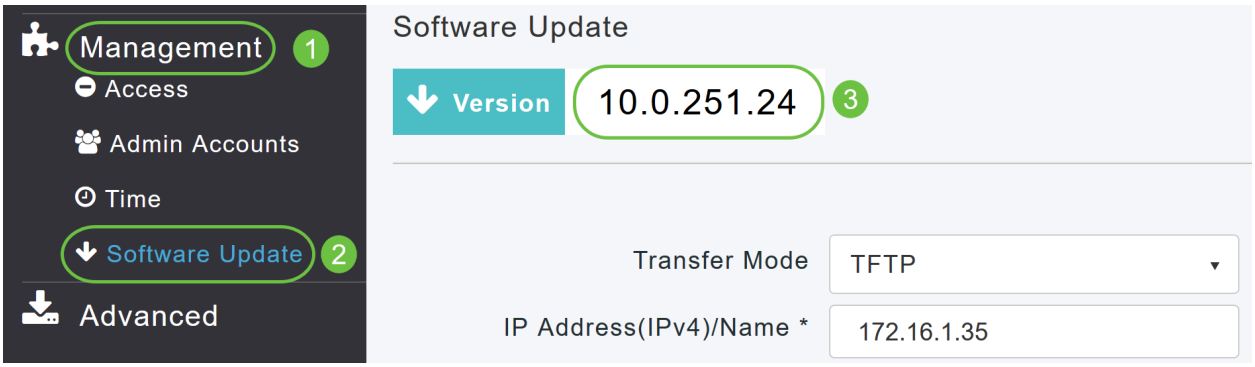


Si vous exécutez la dernière version du logiciel, vous pouvez accéder à la section Créer des WLAN.

Étape 3

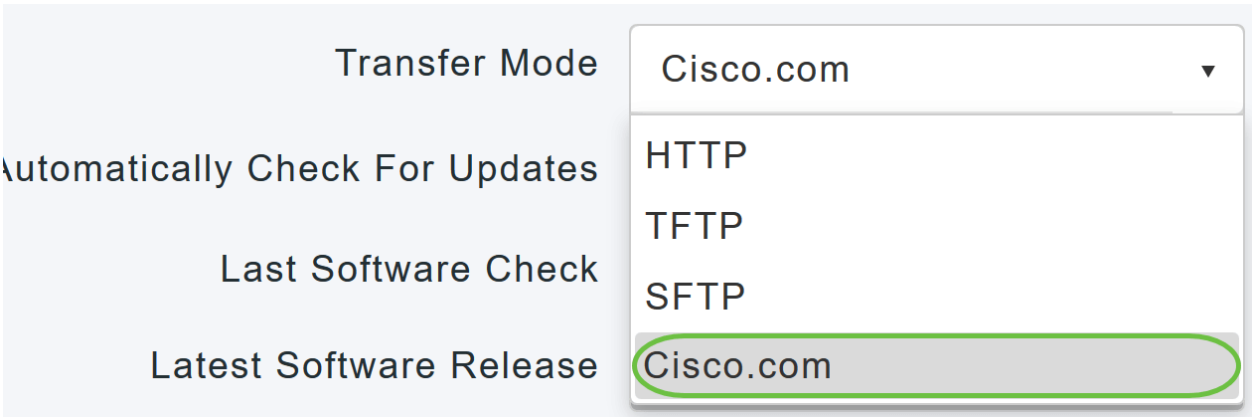
Choisissez **Management > Software Update** dans le menu.

La fenêtre *Mise à jour logicielle* s'affiche avec le numéro de version du logiciel en cours figurant en haut.



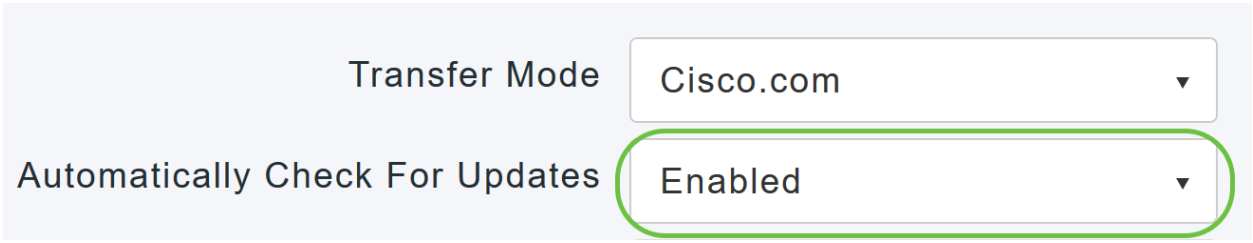
Vous pouvez mettre à jour le logiciel de point d'accès CBW et les configurations actuelles sur le point d'accès principal ne seront pas supprimées.

Dans la liste déroulante *Mode de transfert*, sélectionnez **Cisco.com**.



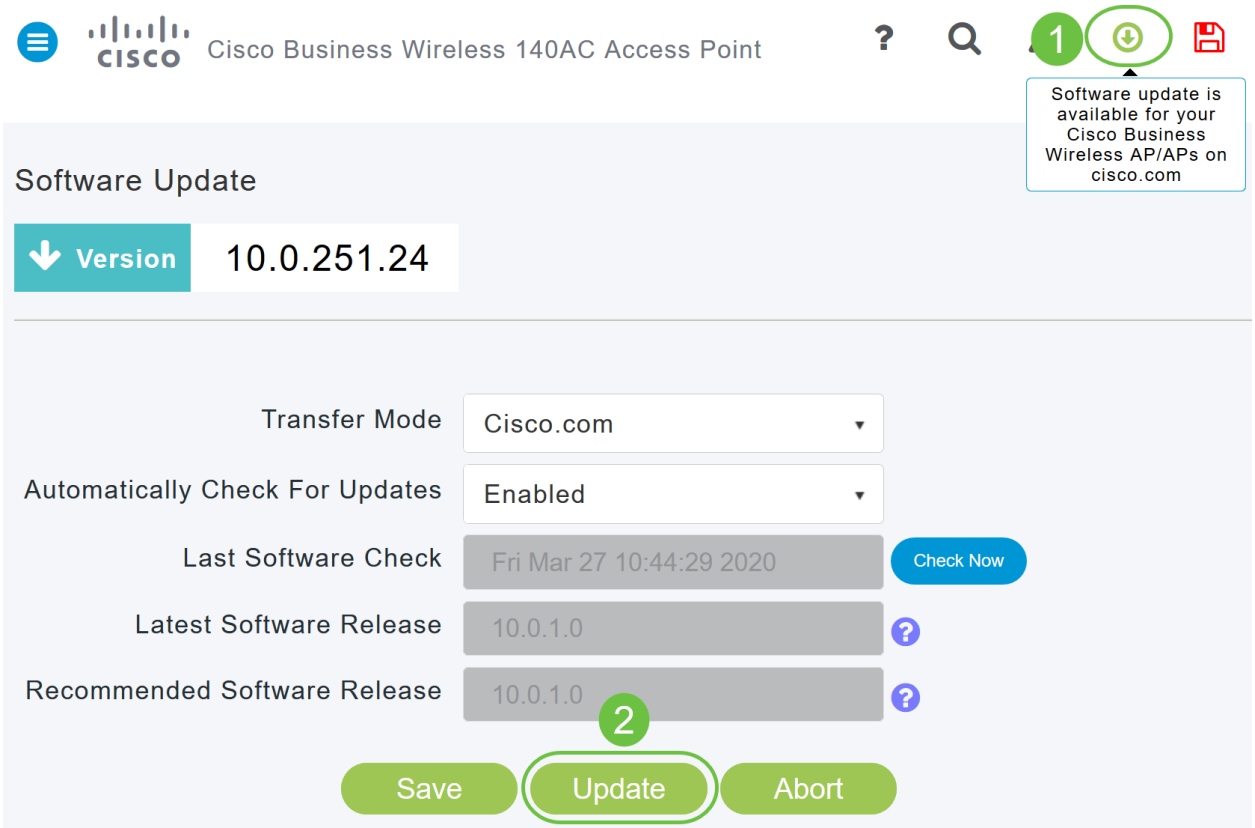
Étape 4

Pour configurer le point d'accès principal pour qu'il vérifie automatiquement les mises à jour logicielles, sélectionnez **Activé** dans la liste déroulante *Vérifier automatiquement les mises à jour*. Ceci est activé par défaut.



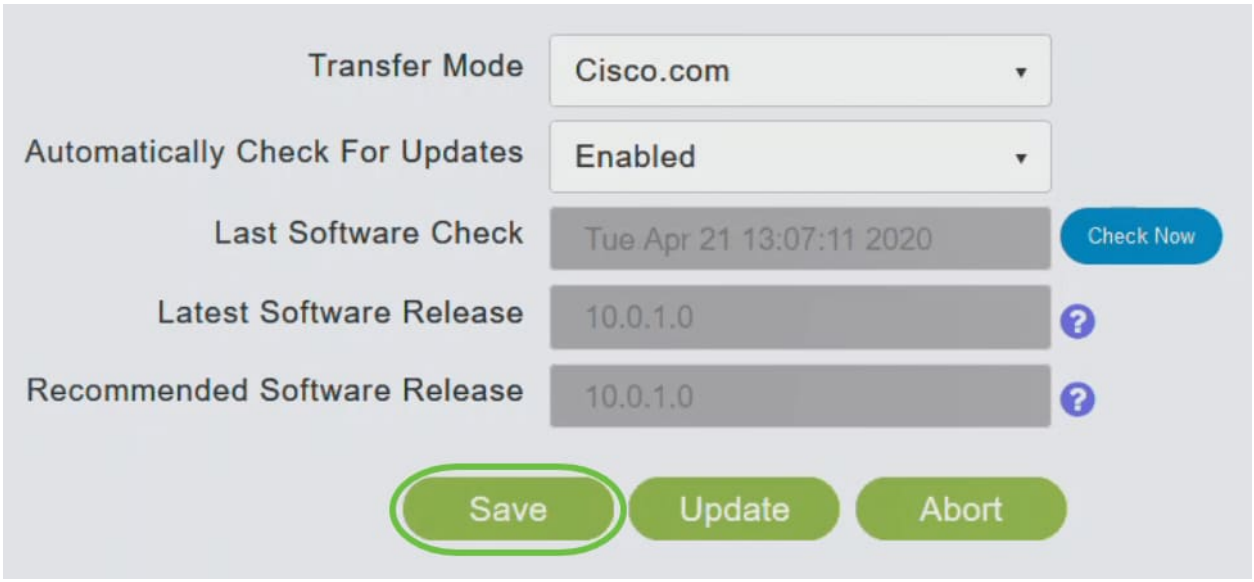
Lorsqu'une vérification logicielle est effectuée et qu'une mise à jour logicielle plus récente ou recommandée est disponible sur Cisco.com, alors :

- L'**icône d'alerte de mise à jour logicielle** située dans le coin supérieur droit de l'interface utilisateur Web est verte (ou grise). Cliquez sur l'icône pour accéder à la page Mise à jour logicielle.
- Le bouton Mettre à jour en bas de la page *Mise à jour logicielle* est activé.

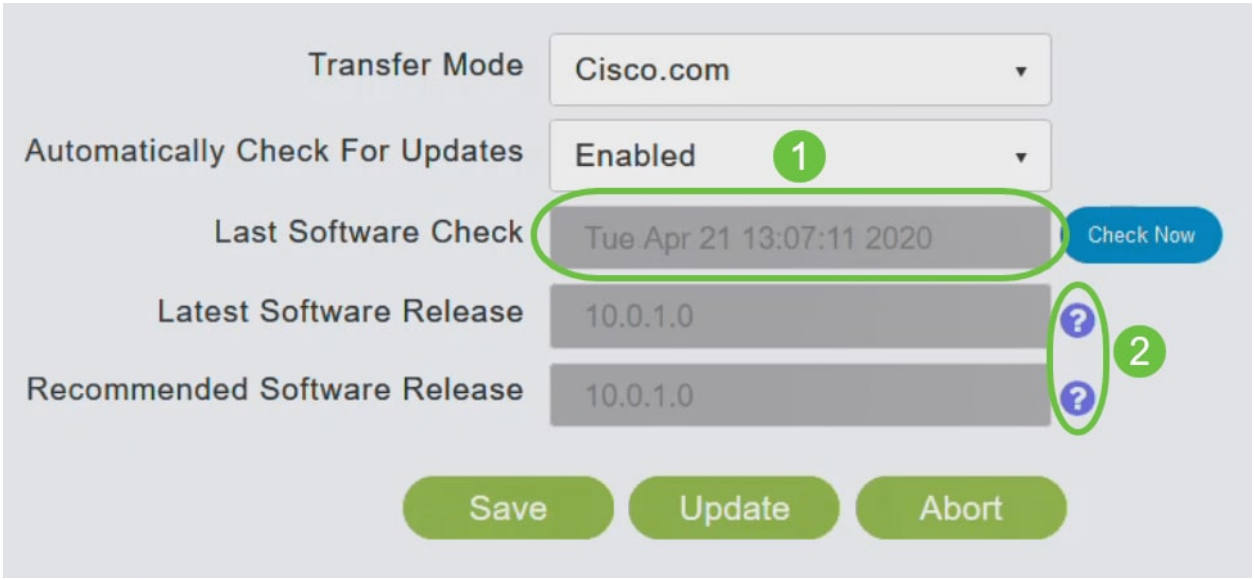


Étape 5

Click Save. Ceci enregistre les entrées ou les modifications que vous avez apportées en *mode Transfert* et *Vérifier automatiquement les mises à jour*.

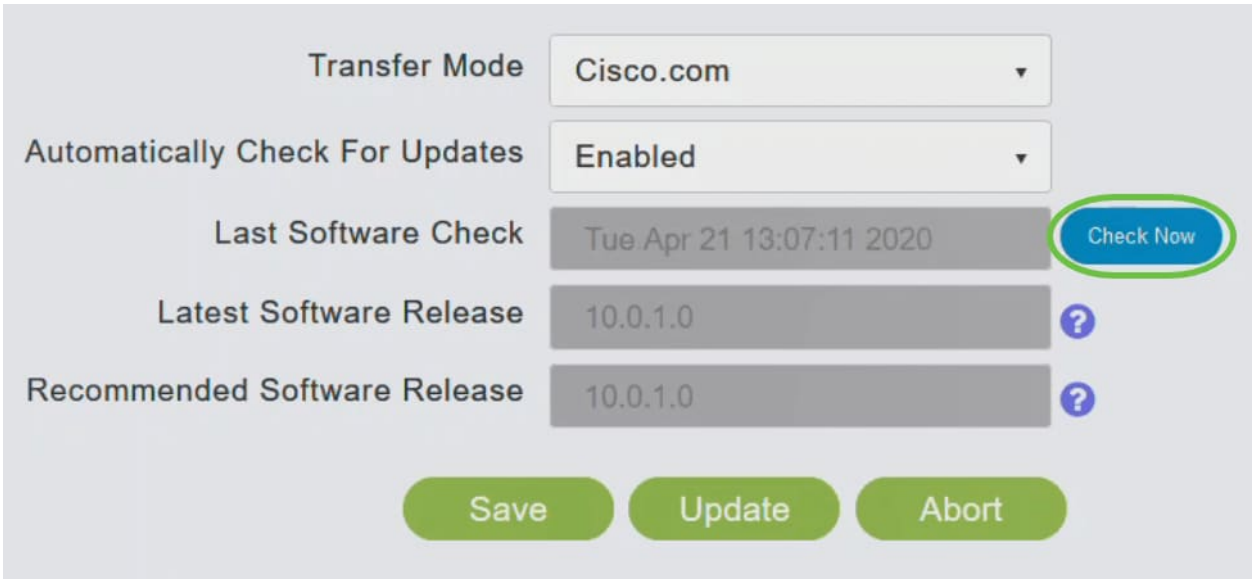


Le champ *Dernier contrôle logiciel* affiche l'horodatage du dernier contrôle logiciel automatique ou manuel. Vous pouvez afficher les notes des versions affichées en cliquant sur l'**icône de point d'interrogation** à côté.



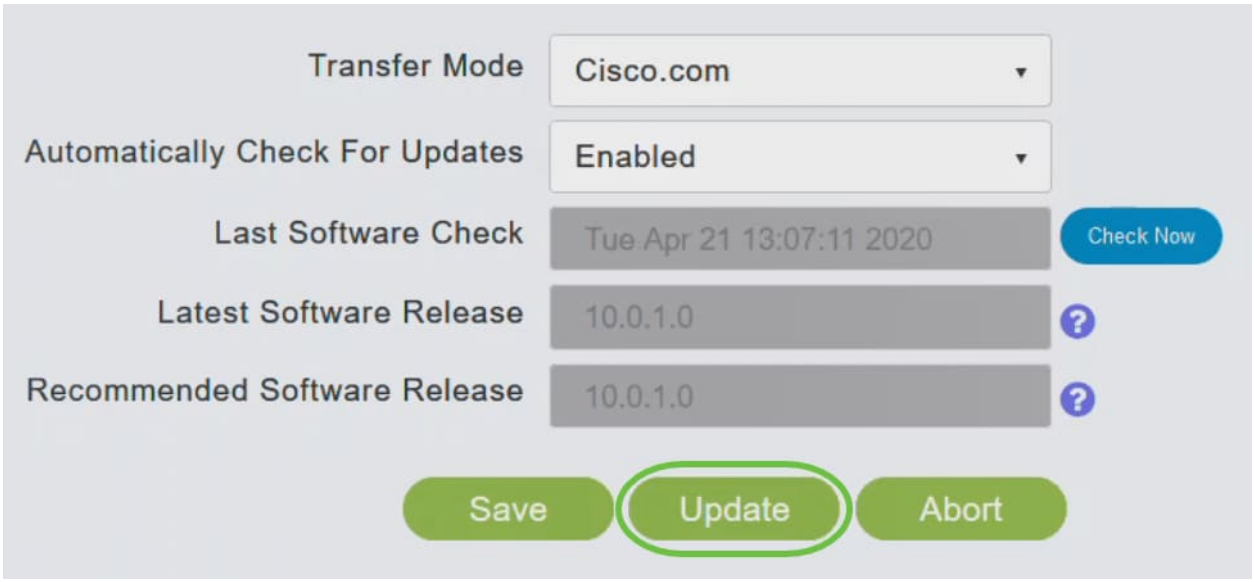
Étape 6

Vous pouvez exécuter manuellement une vérification logicielle à tout moment en cliquant sur *Vérifier maintenant*.



Étape 7

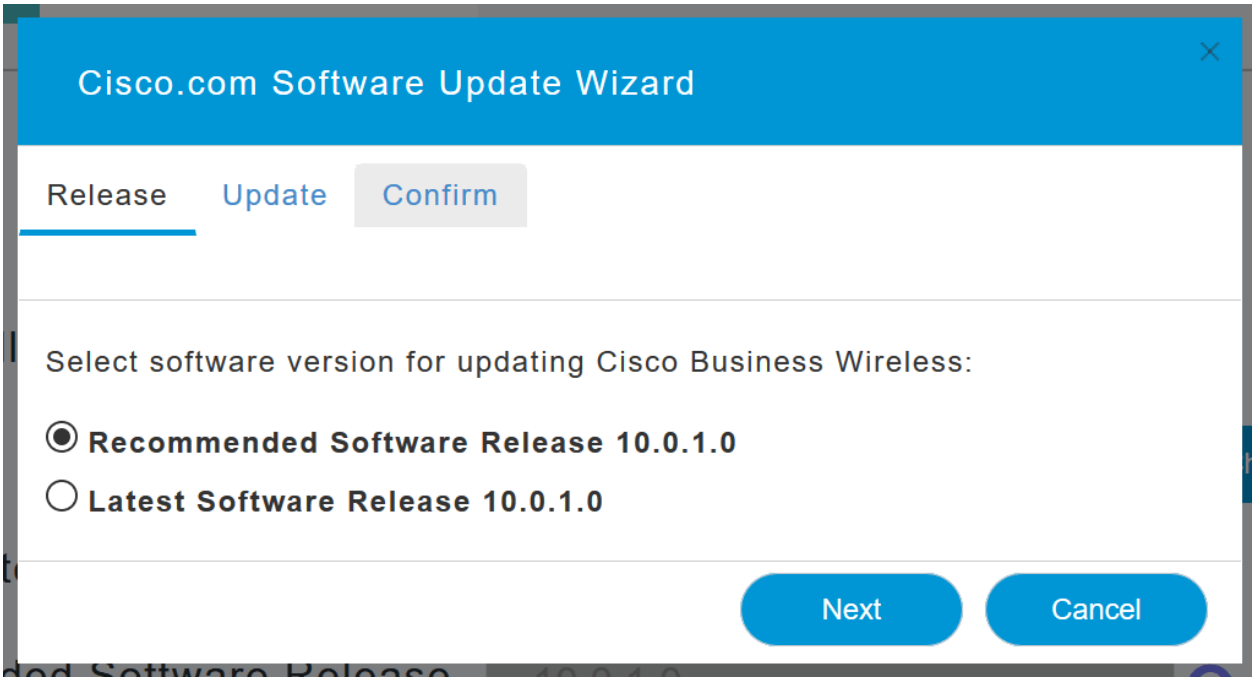
Pour continuer la mise à jour logicielle, cliquez sur **Mettre à jour**.



L'*Assistant Mise à jour logicielle* apparaît. L'Assistant vous guide dans l'ordre des trois onglets suivants :

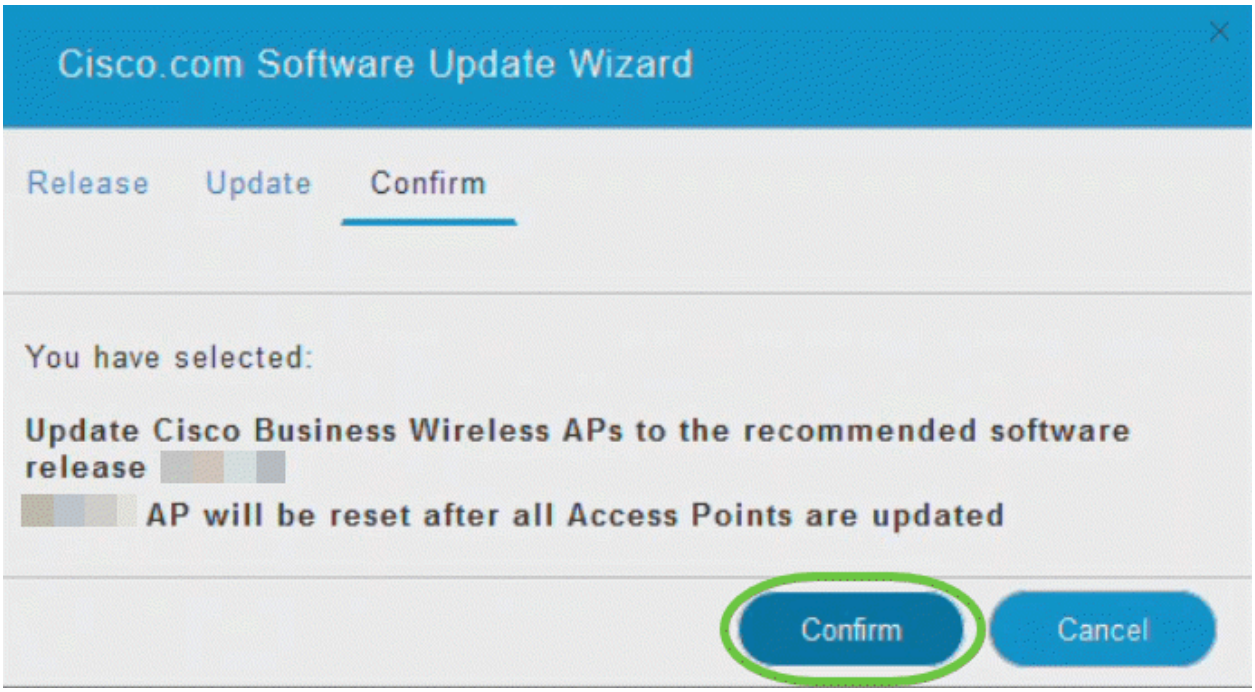
- Onglet Version : indiquez si vous souhaitez effectuer une mise à jour vers la version logicielle recommandée ou vers la dernière version logicielle.
- Onglet Update : indiquez quand les points d'accès doivent être réinitialisés. Vous pouvez choisir de le faire faire immédiatement ou de le planifier ultérieurement. Pour configurer le point d'accès principal pour qu'il redémarre automatiquement une fois le prétéléchargement de l'image terminé, cochez la case Redémarrage automatique.
- Onglet Confirmer - Confirmer vos sélections.

Suivez les instructions de l'assistant. Vous pouvez revenir à n'importe quel onglet à tout moment avant de cliquer sur *Confirmer*.



Étape 8

Cliquez sur **Confirmer**.

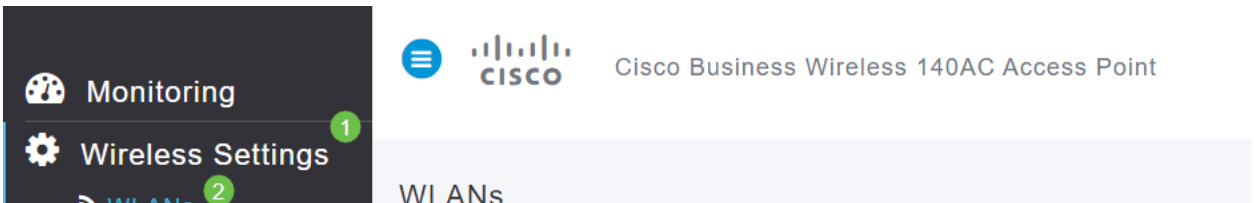


Créer des WLAN sur l'interface utilisateur Web

Cette section vous permet de créer des réseaux locaux sans fil (WLAN).

Étape 1

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



Étape 2

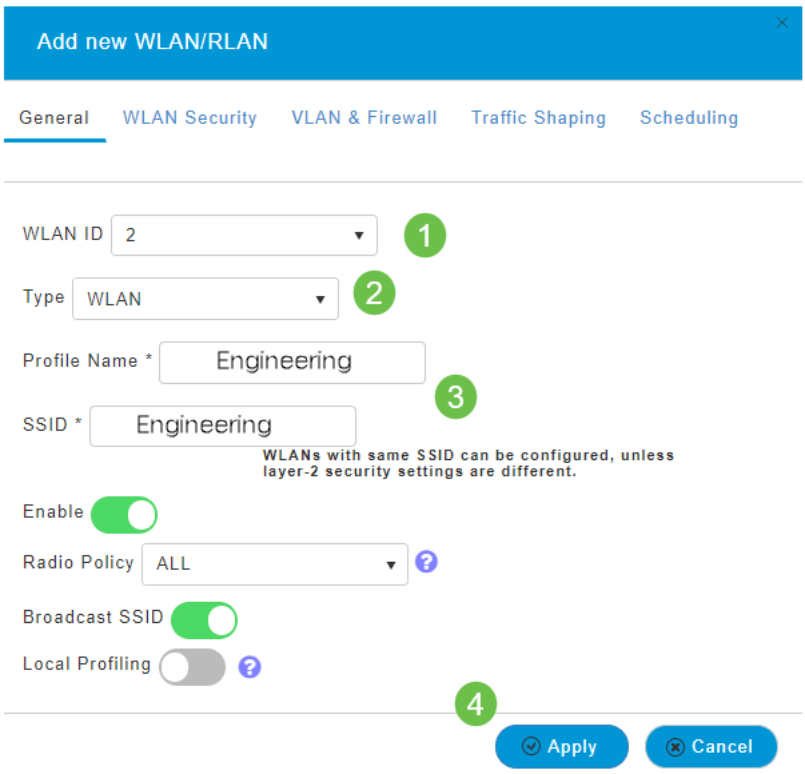
Sous l'onglet *Général*, saisissez les informations suivantes :

- WLAN ID : sélectionnez un numéro pour le WLAN.
- Type - Sélectionnez **WLAN**
- Profile Name (Nom du profil) : lorsque vous saisissez un nom, le SSID est automatiquement renseigné avec le même nom. Le nom doit être unique et ne doit pas dépasser 31 caractères.

Les champs suivants ont été laissés par défaut dans cet exemple, mais les explications sont répertoriées au cas où vous voudriez les configurer différemment.

- SSID : le nom du profil agit également en tant que SSID. Vous pouvez changer ceci si vous voulez. Le nom doit être unique et ne doit pas dépasser 31 caractères.
- Enable (Activer) : cette option doit être laissée activée pour que le WLAN fonctionne.
- Stratégie radio - En règle générale, vous devez laisser cette option comme **Tous** afin que les clients 2,4 GHz et 5 GHz puissent accéder au réseau.
- SSID de diffusion : généralement, vous souhaitez que le SSID soit découvert afin de laisser cette option activée.
- Profilage local : vous ne souhaitez activer cette option que pour afficher le système d'exploitation qui s'exécute sur le client ou le nom d'utilisateur.

Cliquez sur Apply.



Étape 3

Vous accédez à l'onglet *Sécurité WLAN*.

Dans cet exemple, les options suivantes ont été laissées par défaut :

- Le réseau invité, Captive Network Assistant et le filtrage MAC ont été désactivés. Les détails de la configuration d'un réseau invité sont détaillés dans la section suivante.
- WPA2 Personal (WPA2 personnel) - Wi-Fi Protected Access 2 avec clé prépartagée (PSK) - Format de phrase de passe ASCII. Cette option correspond à Wi-Fi Protected Access 2 avec clé prépartagée (PSK).

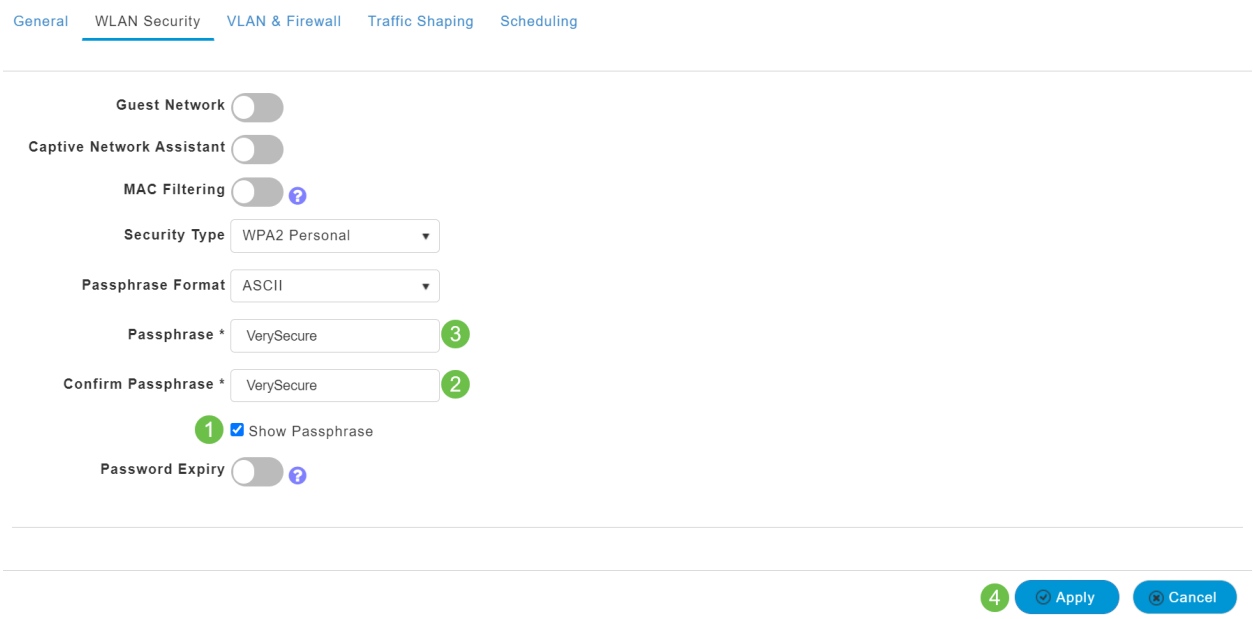
WPA2 Personal (WPA2 personnel) est une méthode utilisée pour sécuriser votre réseau à l'aide d'une authentification PSK. Le PSK est configuré séparément sur le point d'accès principal, sous la stratégie de sécurité WLAN, et sur le client. WPA2 Personal ne dépend pas d'un serveur d'authentification sur votre réseau.

- Format de phrase de passe - **ASCII est laissé par défaut.**

Les champs suivants ont été entrés dans ce scénario :

- Show Passphrase (Afficher la phrase de passe) : cochez la case pour afficher la phrase de passe que vous saisissez.
- Passphrase (Phrase de passe) : saisissez un nom pour la phrase de passe (mot de passe).
- Confirmer la phrase de passe : saisissez à nouveau le mot de passe pour le confirmer.

Cliquez sur Apply. Ceci active automatiquement le nouveau WLAN.

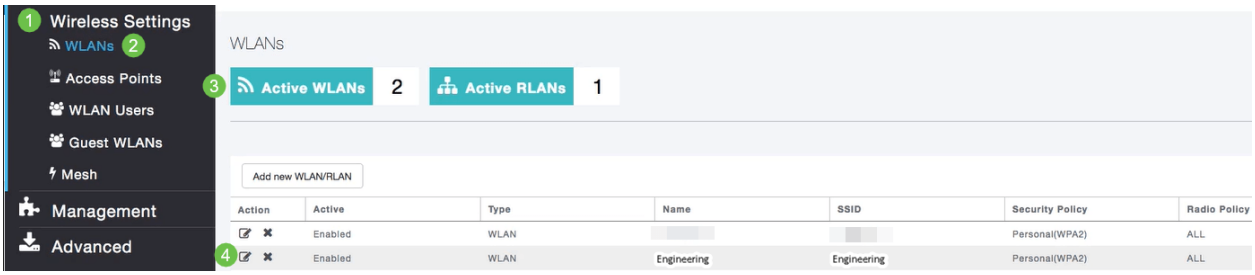


Étape 4

Veillez à enregistrer vos configurations en cliquant sur l'**icône d'enregistrement** dans le panneau supérieur droit de l'écran Web UI.

Étape 5

Pour afficher le WLAN que vous avez créé, sélectionnez **Wireless Settings > WLAN**. Le nombre de WLAN actifs est porté à 2 et le nouveau WLAN s'affiche.



Répétez ces étapes pour les autres WLAN que vous voulez créer.

Configurations sans fil optionnelles

Toutes les configurations de base sont maintenant définies et sont prêtes à être lancées. Vous disposez de certaines options. N'hésitez donc pas à passer à l'une des sections suivantes :

- Créer un WLAN invité à l'aide de l'interface utilisateur Web (facultatif)
- Profilage des applications (facultatif)
- Profilage client (facultatif)
- Je suis prêt à conclure et à utiliser mon réseau !

Créer un WLAN invité à l'aide de l'interface utilisateur Web (facultatif)

Un WLAN invité donne un accès invité à votre réseau Cisco Business Wireless.

Étape 1

Connectez-vous à l'interface utilisateur Web du point d'accès principal. Ouvrez un navigateur Web et entrez www.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.

Étape 2

Vous pouvez créer un réseau local sans fil (WLAN) en accédant à **Wireless Settings > WLAN**. Sélectionnez ensuite **Ajouter un nouveau WLAN/RLAN**.

Étape 3

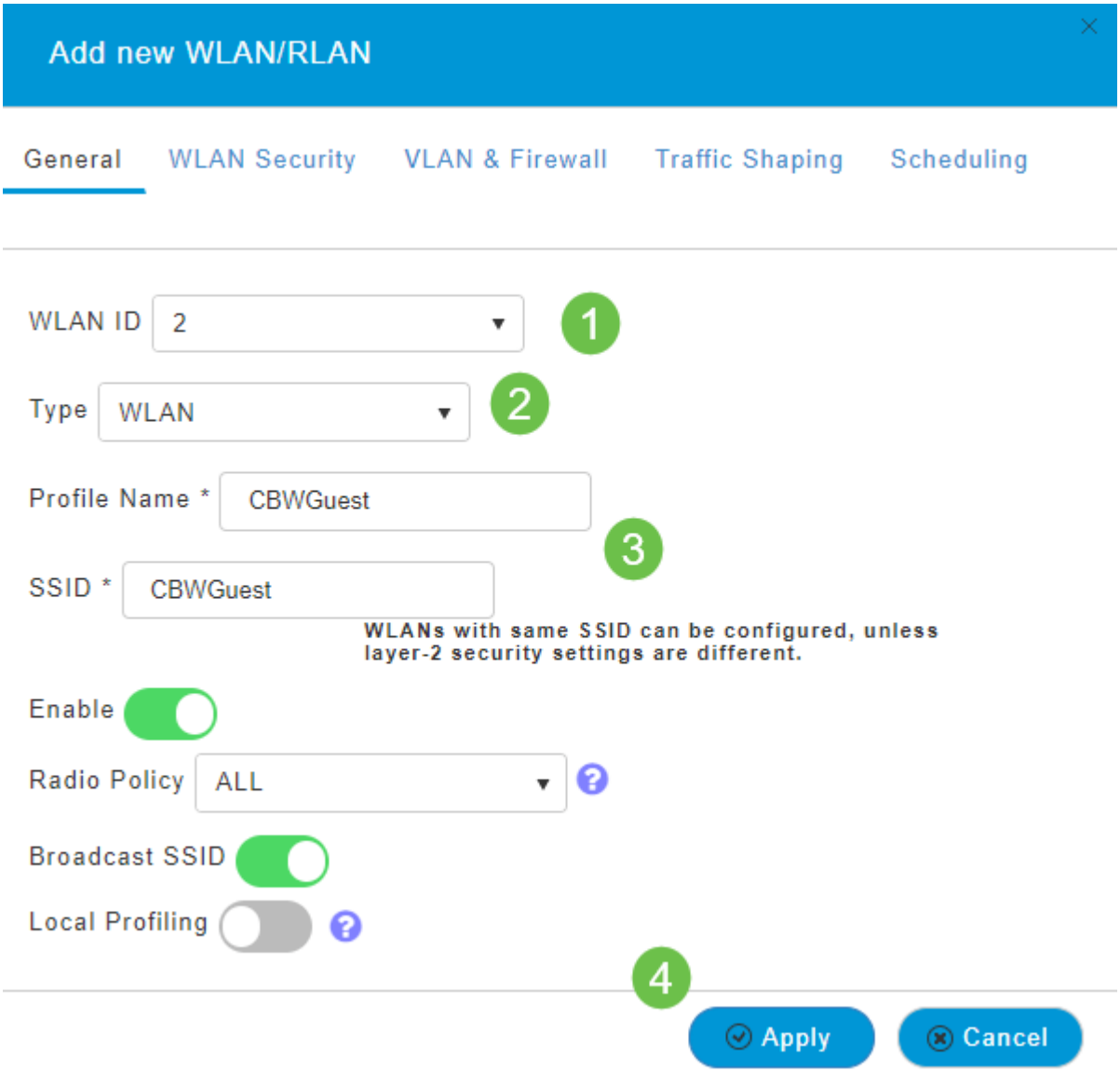
Sous l'onglet *Général*, saisissez les informations suivantes :

WLAN ID - Sélectionnez un numéro pour le WLAN.
Type - Sélectionnez **WLAN**
Nom du profil - Lorsque vous entrez un nom, le SSID est automatiquement renseigné avec le même nom. Le nom doit être unique et ne doit pas dépasser 31 caractères.

Les champs suivants ont été laissés par défaut dans cet exemple, mais les explications sont répertoriées au cas où vous voudriez les configurer différemment.

SSID - Le nom du profil agit également en tant que SSID. Vous pouvez changer ceci si vous voulez. Le nom doit être unique et ne doit pas dépasser 31 caractères.
Enable : cette option doit être laissée activée pour que le WLAN fonctionne.
Stratégie radio - En règle générale, vous devez laisser cette option comme **All** pour que les clients 2,4 GHz et 5 GHz puissent accéder au réseau.
SSID de diffusion - En règle générale, vous souhaitez que le SSID soit découvert afin de laisser cette option activée.
Profilage local - Vous ne souhaitez activer cette option que pour afficher le système d'exploitation qui s'exécute sur le client ou pour afficher le nom d'utilisateur.

Cliquez sur Apply.

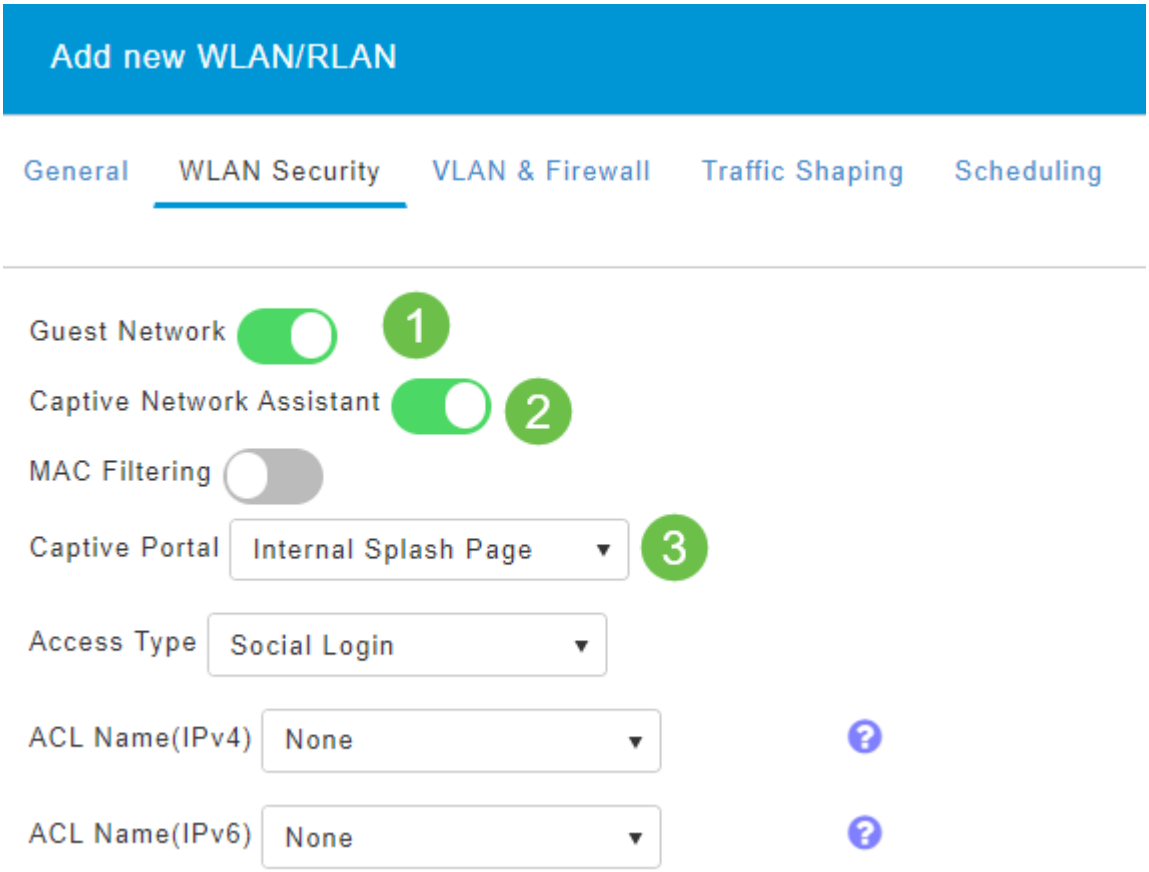


Étape 4

Vous accédez à l'onglet *Sécurité WLAN*. Dans cet exemple, les options suivantes ont été sélectionnées.

- Réseau invité - Activer
- Captive Network Assistant : si vous utilisez Mac ou IOS, vous voudrez probablement l'activer. Cette fonctionnalité détecte la présence d'un portail captif en envoyant une demande Web lors de la connexion à un réseau sans fil. Cette demande est dirigée vers une URL (Uniform Resource Locator) pour les modèles iPhone et si une réponse est reçue, alors l'accès Internet est supposé disponible et aucune autre interaction n'est requise. Si aucune réponse n'est reçue, l'accès à Internet est censée être bloqué par le portail captif et l'Assistant Réseau captif (CNA) d'Apple lance automatiquement le pseudo-navigateur pour demander la connexion au portail dans une fenêtre contrôlée. La CNA peut être interrompue lors de la redirection vers un portail captif ISE (Identity Services Engine). Le point d'accès principal empêche ce pseudo-navigateur de s'afficher.
- Captive Portal : ce champ n'est visible que lorsque l'option Guest Network est activée. Permet de spécifier le type de portail Web qui peut être utilisé à des fins d'authentification. Sélectionnez Internal Splash Page (Page de démarrage interne) pour utiliser l'authentification Cisco basée sur le portail Web par défaut. Sélectionnez Page de

démarrage externe si vous disposez d'une authentification de portail captive, à l'aide d'un serveur Web en dehors de votre réseau. Spécifiez également l'URL du serveur dans le champ URL du site.



Dans cet exemple, le WLAN invité avec un type d'accès de connexion sociale activé sera créé. Une fois que l'utilisateur se connecte à ce WLAN invité, il sera redirigé vers la page de connexion par défaut de Cisco, où il trouvera les boutons de connexion de Google et de Facebook. L'utilisateur peut se connecter à l'aide de son compte Google ou Facebook pour accéder à Internet.

Étape 5

Dans ce même onglet, sélectionnez un *type d'accès* dans le menu déroulant. Dans cet exemple, *Connexion sociale* a été sélectionnée. Cette option permet aux invités d'utiliser leurs identifiants Google ou Facebook pour s'authentifier et accéder au réseau.

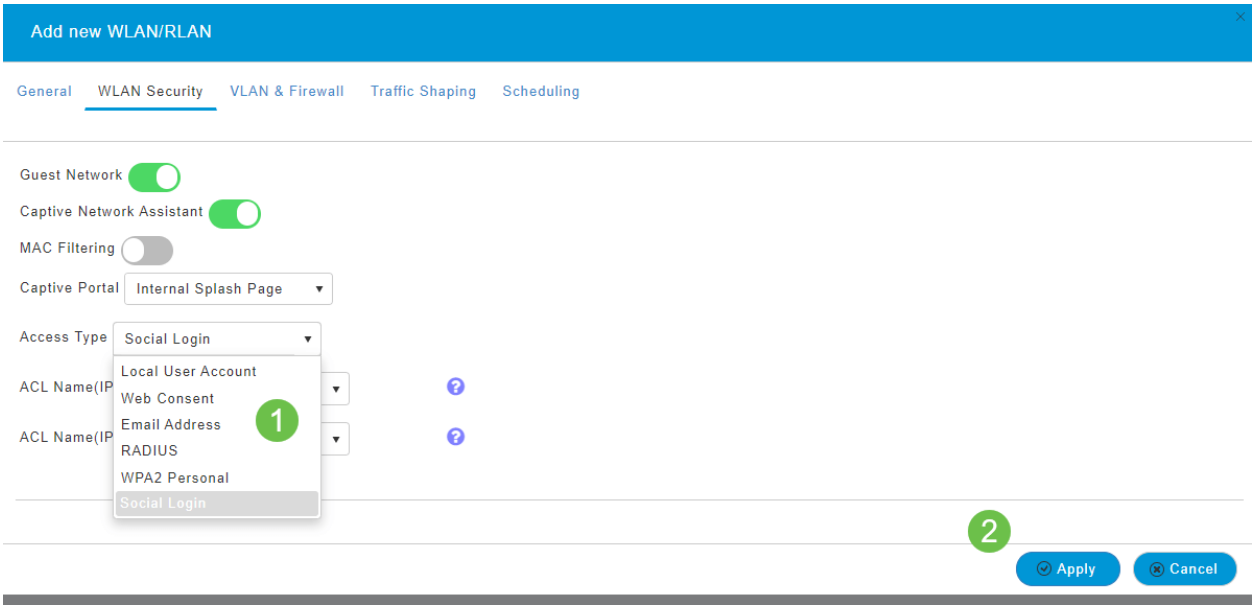
D'autres options pour *le type d'accès* sont les suivantes :

Compte d'utilisateur local - Option par défaut. Choisissez cette option pour authentifier les invités à l'aide du nom d'utilisateur et du mot de passe que vous pouvez spécifier pour les utilisateurs invités de ce WLAN, sous **Wireless Settings > WLAN Users**. Voici un exemple de la page de démarrage interne par défaut.

Vous pouvez personnaliser ceci en accédant à **Wireless Settings > Guest WLAN**. À partir de là, vous pouvez entrer un *titre* et un *message de page*. Cliquez sur Apply. Cliquez sur **Aperçu**.

Consentement Web - Permet aux invités d'accéder au WLAN après acceptation des conditions générales affichées. Les utilisateurs invités peuvent accéder au WLAN sans entrer de nom d'utilisateur ni de mot de passe.
Adresse e-mail : les utilisateurs invités doivent saisir leur adresse e-mail pour accéder au réseau.
RADIUS : utilisez cette option avec un serveur d'authentification externe.
WPA2 Personal - Wi-Fi Protected Access 2 avec clé prépartagée (PSK)

Cliquez sur Apply.



Étape 6

Veillez à enregistrer vos configurations en cliquant sur l'**icône d'enregistrement** dans le panneau supérieur droit de l'écran Web UI.

Vous avez maintenant créé un réseau invité disponible sur votre réseau CBW. Vos clients apprécieront la commodité.

Profilage d'applications à l'aide de l'interface utilisateur Web (facultatif)

Le profilage est un sous-ensemble de fonctionnalités qui permettent d'appliquer une politique d'organisation. Il vous permet de mettre en correspondance et de hiérarchiser les types de trafic. Comme les règles prennent des décisions sur la façon de classer ou de supprimer le trafic. Le système Cisco Business Mesh Wireless comporte un profilage des applications et des clients. L'accès à un réseau en tant qu'utilisateur commence par de nombreux échanges d'informations, parmi lesquels le type de trafic. La stratégie interrompt le flux de trafic pour diriger le chemin, tout comme un diagramme de flux. D'autres types de fonctionnalités de stratégie incluent l'accès

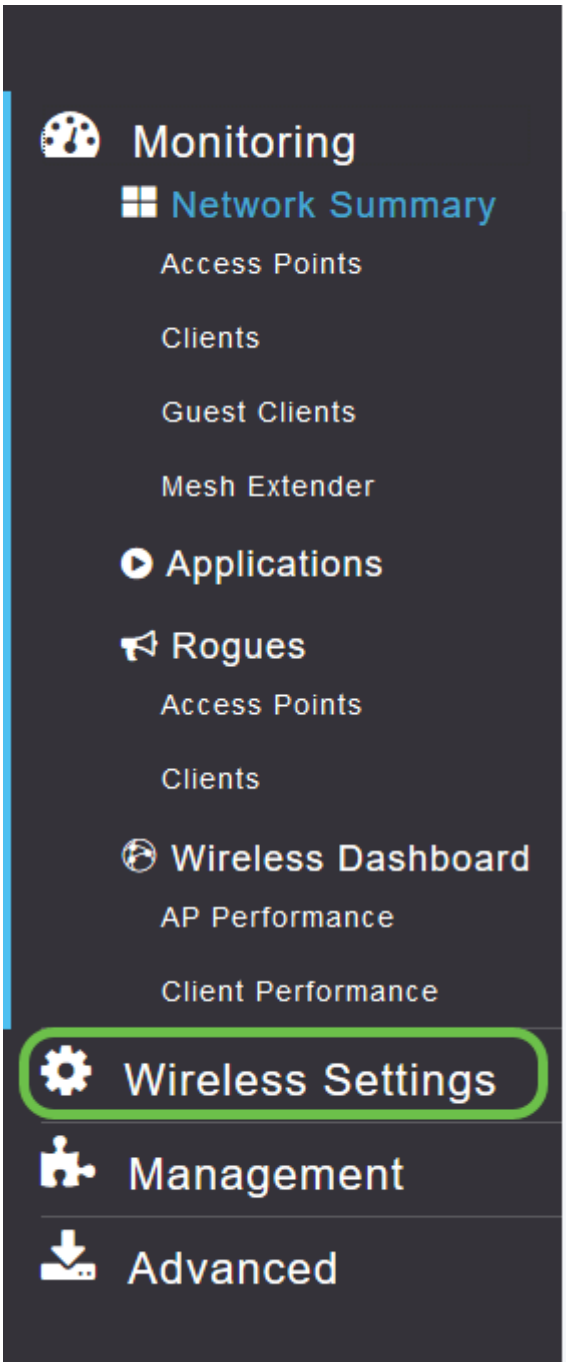
invité, les listes de contrôle d'accès et la qualité de service.

Étape 1

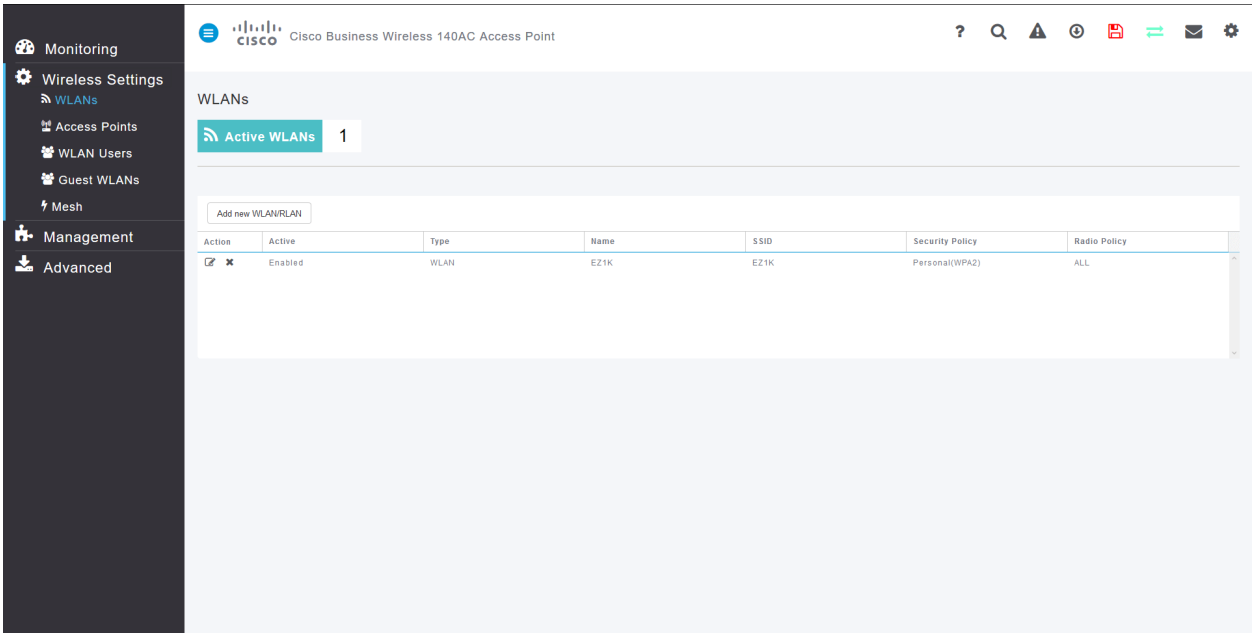
Naviguez jusqu'au menu situé à gauche de l'écran si vous ne voyez pas la barre de menu à gauche.

Étape 2

Le menu Surveillance se charge par défaut lors de la connexion au périphérique. Vous devez cliquer sur **Wireless Settings (Paramètres sans fil)**.

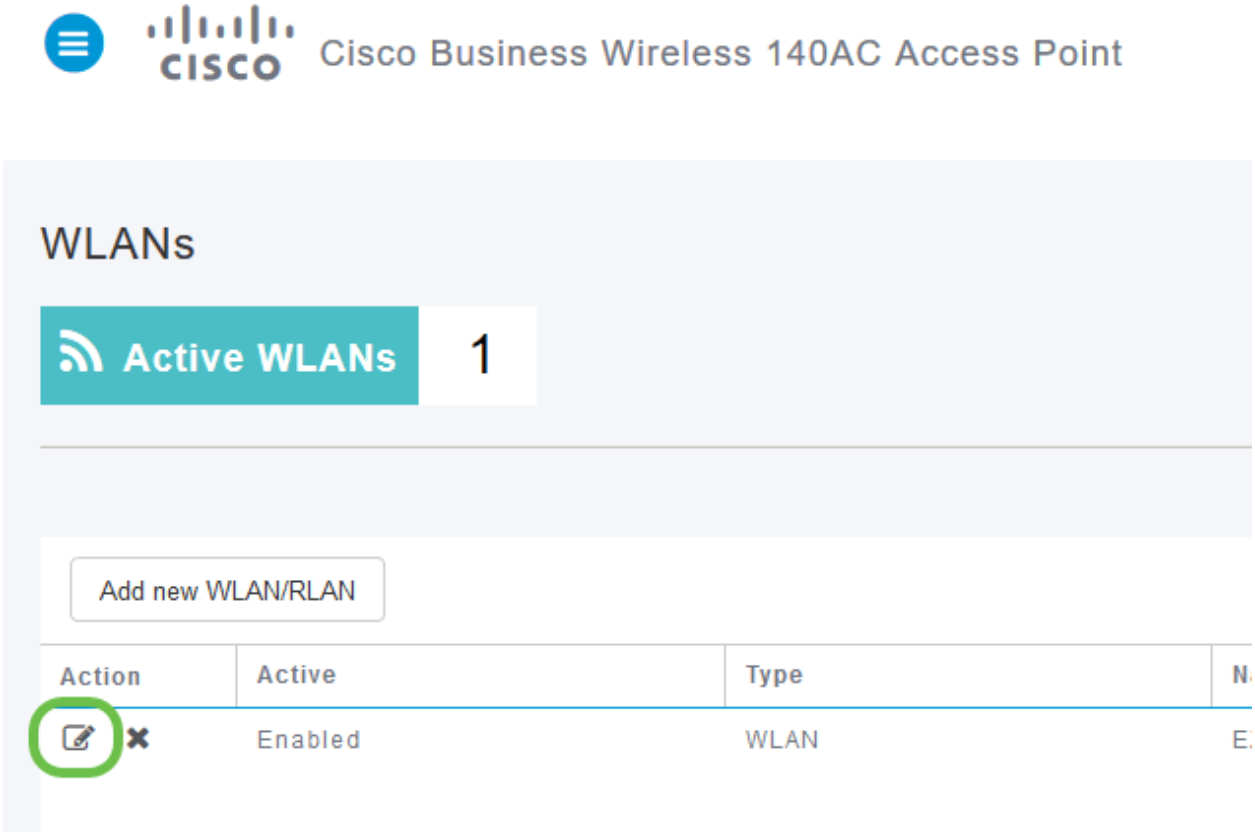


L'image ci-dessous est similaire à celle que vous verrez lorsque vous cliquez sur le lien Wireless Settings (Paramètres sans fil).

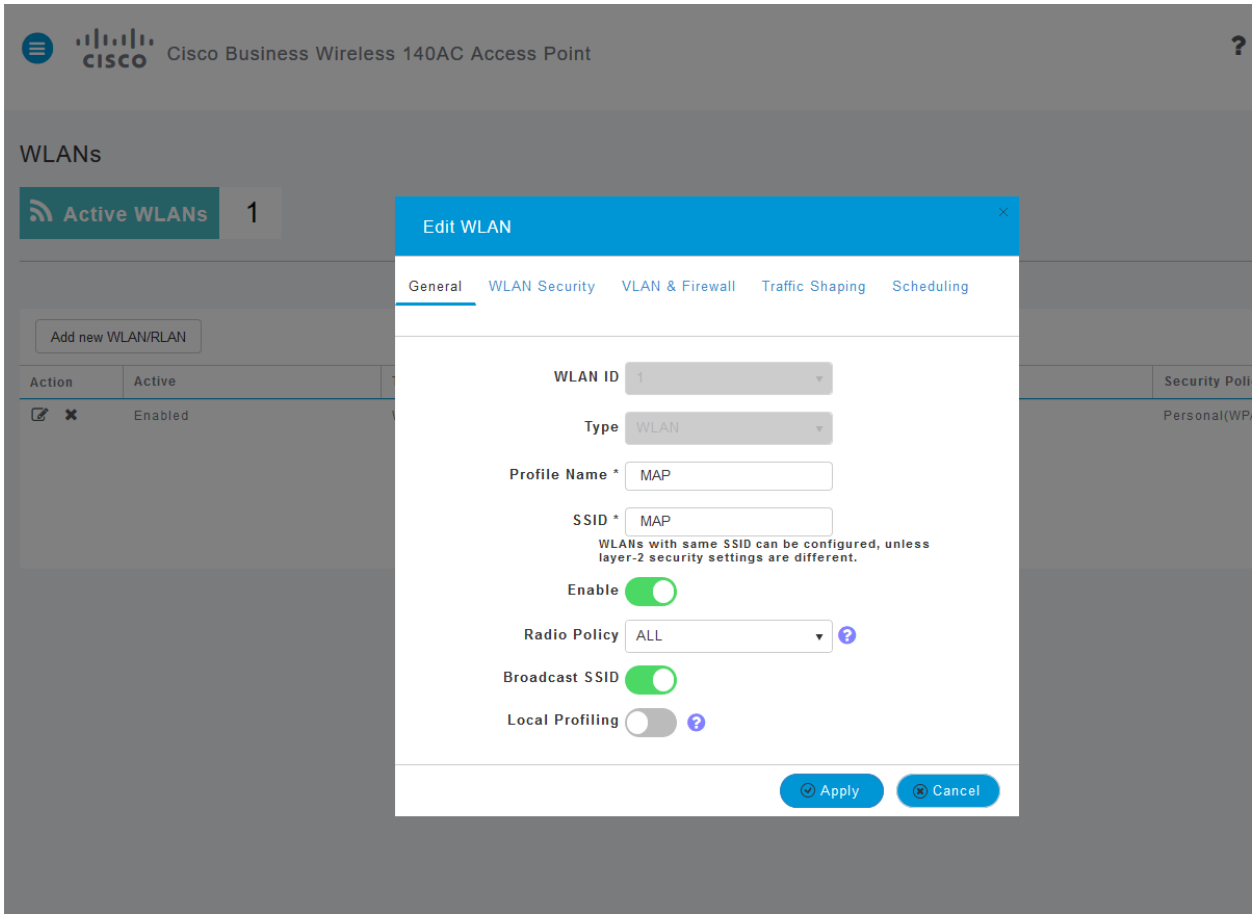


Étape 3

Cliquez sur l'**icône de modification** à gauche du réseau local sans fil sur lequel vous souhaitez activer l'application.

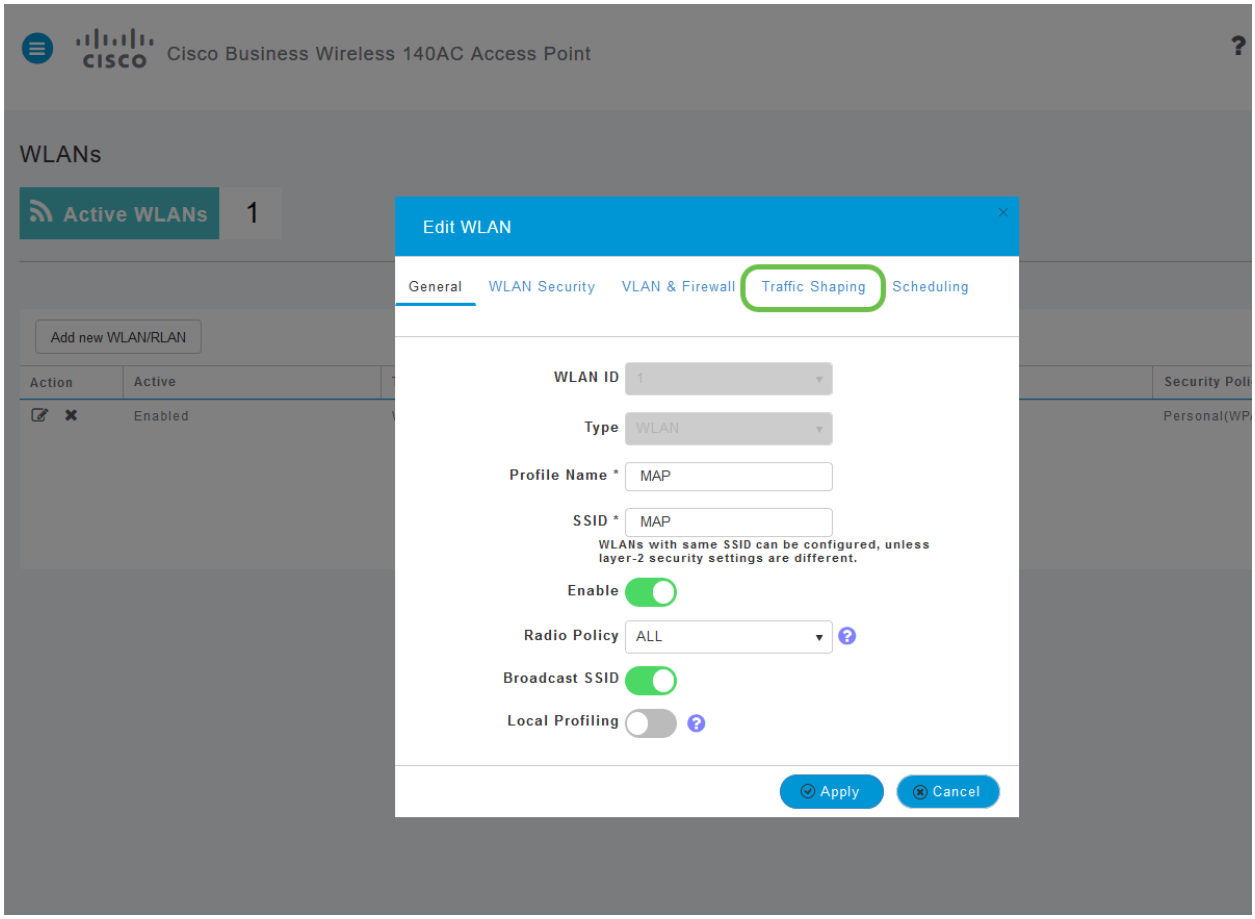


Depuis que vous avez récemment ajouté le WLAN, votre page *Edit WLAN* peut apparaître comme suit :

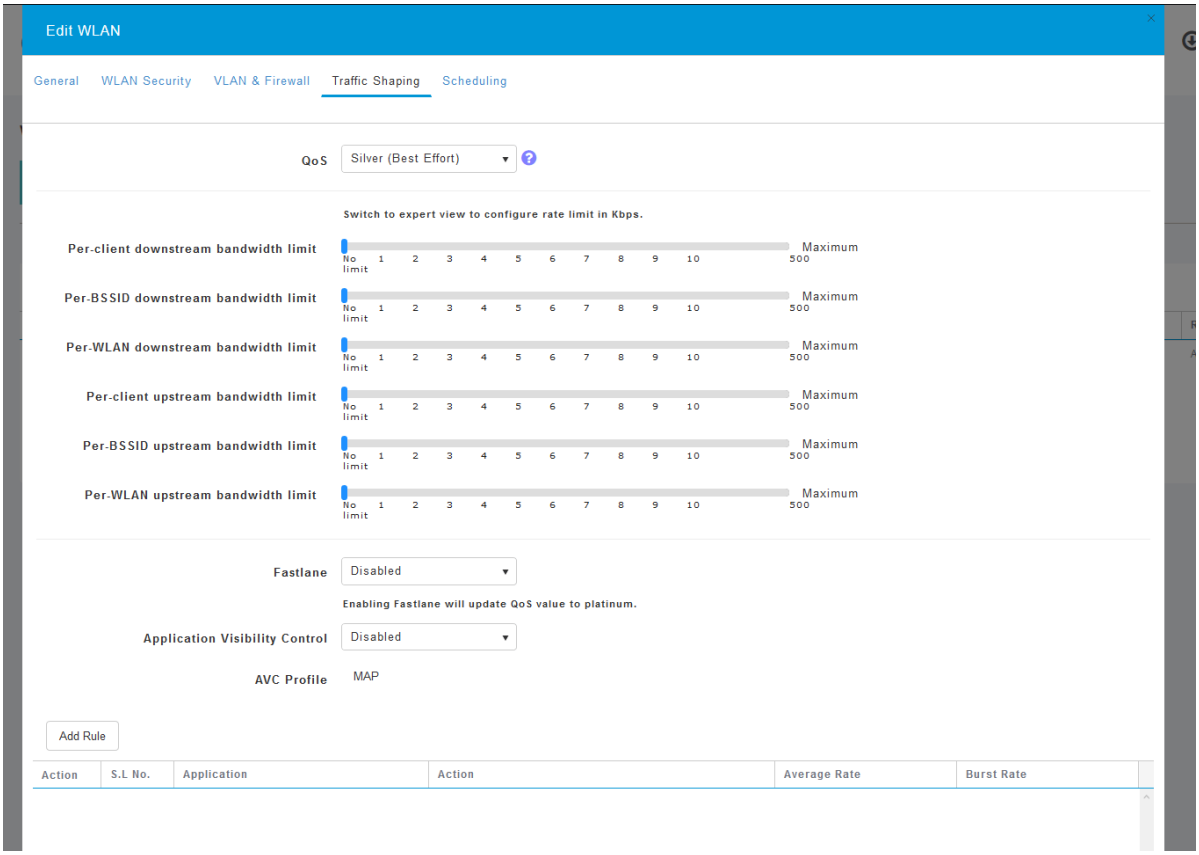


Étape 4

Accédez à l'onglet **Formatage du trafic** en cliquant dessus.

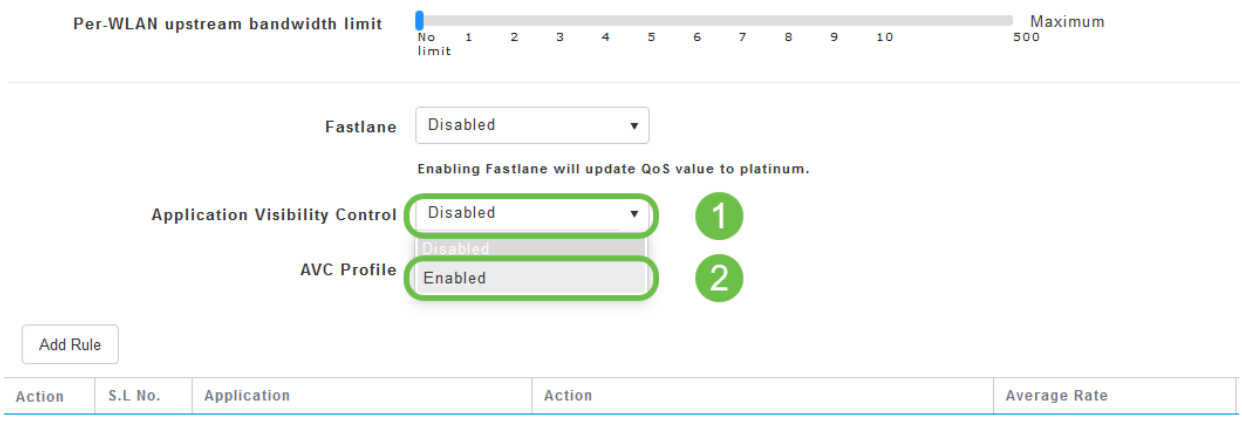


Votre écran peut apparaître comme suit :



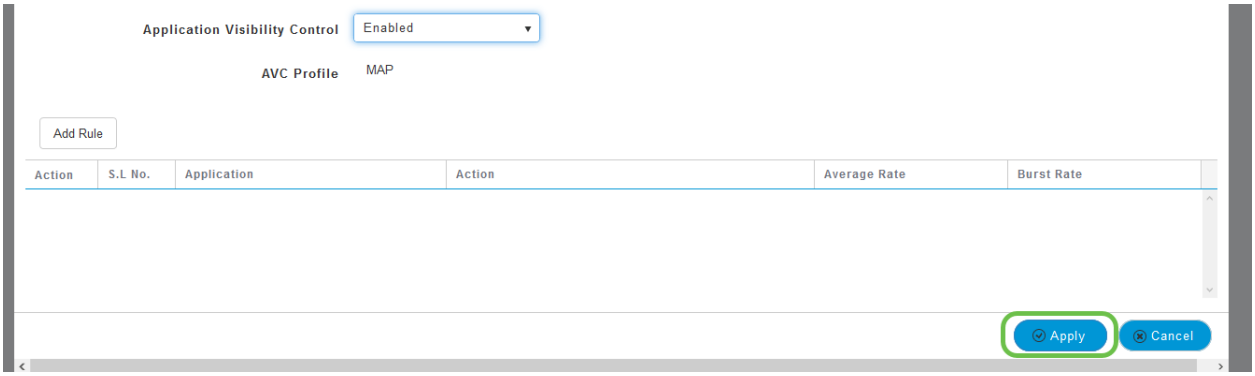
Étape 5

Vers le bas de la page, vous trouverez la fonction *Contrôle de visibilité des applications* . Ceci est désactivé par défaut. Cliquez sur la liste déroulante et sélectionnez **Activé**.



Étape 6

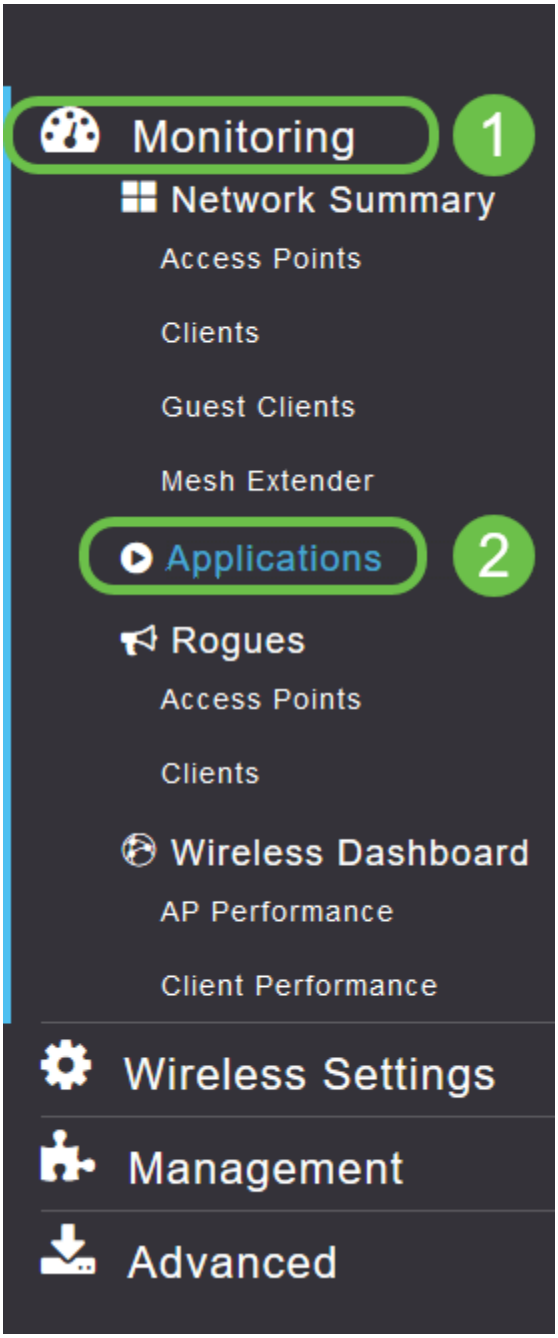
Cliquez sur le bouton **Appliquer**.



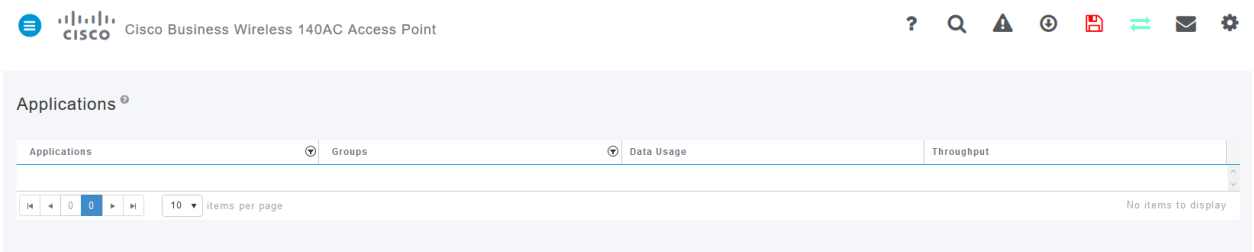
Ce paramètre doit être activé, sinon la fonction ne fonctionnera pas.

Étape 7

Cliquez sur le bouton Annuler pour fermer le sous-menu WLAN. Cliquez ensuite sur le menu **Surveillance** dans la barre de menus de gauche. Une fois que vous êtes en mesure de le faire, cliquez sur l'élément de menu **Applications**.



Si vous n'avez pas eu de trafic vers une source quelconque, votre page sera vierge comme indiqué ci-dessous.



Cette page affiche les informations suivantes :

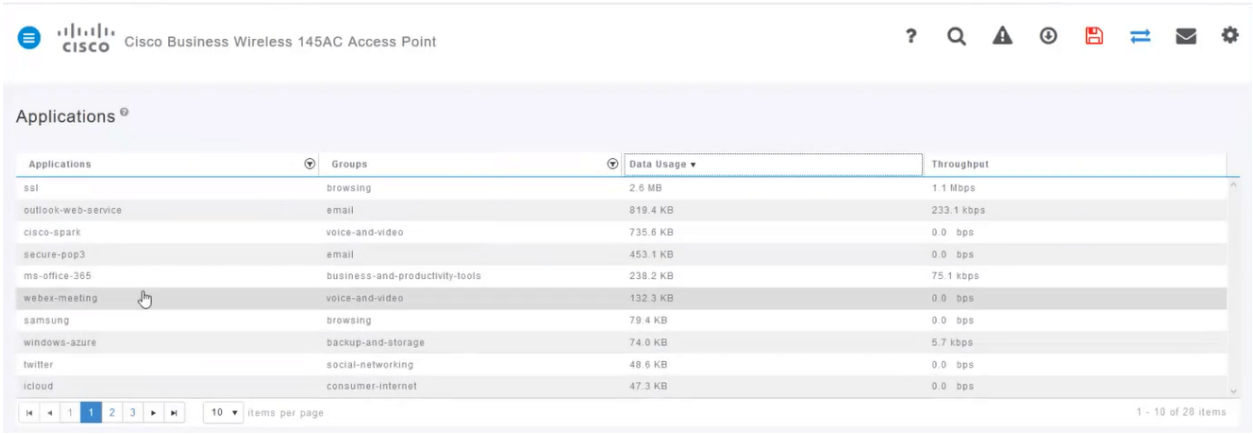
- Application : inclut de nombreux types différents
- Groupes : indique le type de groupe d'applications pour faciliter le tri
- Utilisation des données - Quantité de données utilisées par ce service dans son ensemble
- Débit : quantité de bande passante utilisée par l'application

Vous pouvez cliquer sur les onglets pour trier de la plus grande à la plus petite, ce qui permet d'identifier les plus grands consommateurs de ressources réseau.

Cette fonctionnalité est très puissante pour gérer vos ressources WLAN de manière granulaire. Voici quelques-uns des groupes et types d'applications les plus courants. Il est probable que votre liste contienne beaucoup d'autres éléments, notamment les groupes et les exemples suivants :

- Navigation
    - EX : Spécifique au client, SSL
- Courriel
    - EX : Outlook, Secure-pop3
- Voix et vidéo
    - EX : WebEx, Cisco Spark,
- Outils d'entreprise et de productivité
    - EX : Microsoft Office 365,
- Sauvegarde et stockage
    - EX : Windows-Azure,
- Internet grand public
    - iCloud, Google Drive
- Réseaux sociaux
    - EX : Twitter, Facebook
- Software Updates
    - EX : Google-Play, IOS
- Messagerie instantanée
    - EX : Raccrochements, messages

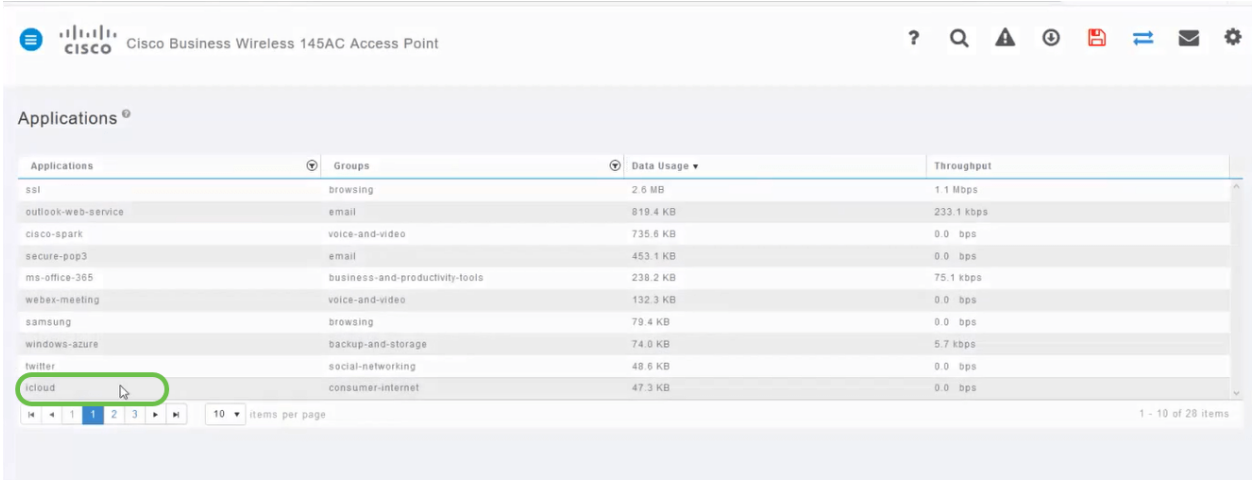
Voici un exemple de ce à quoi ressemblera la page lorsqu'elle sera remplie.



Chaque en-tête de table est cliquable pour le tri, ce qui est particulièrement utile pour les champs *Utilisation des données* et *Débit*.

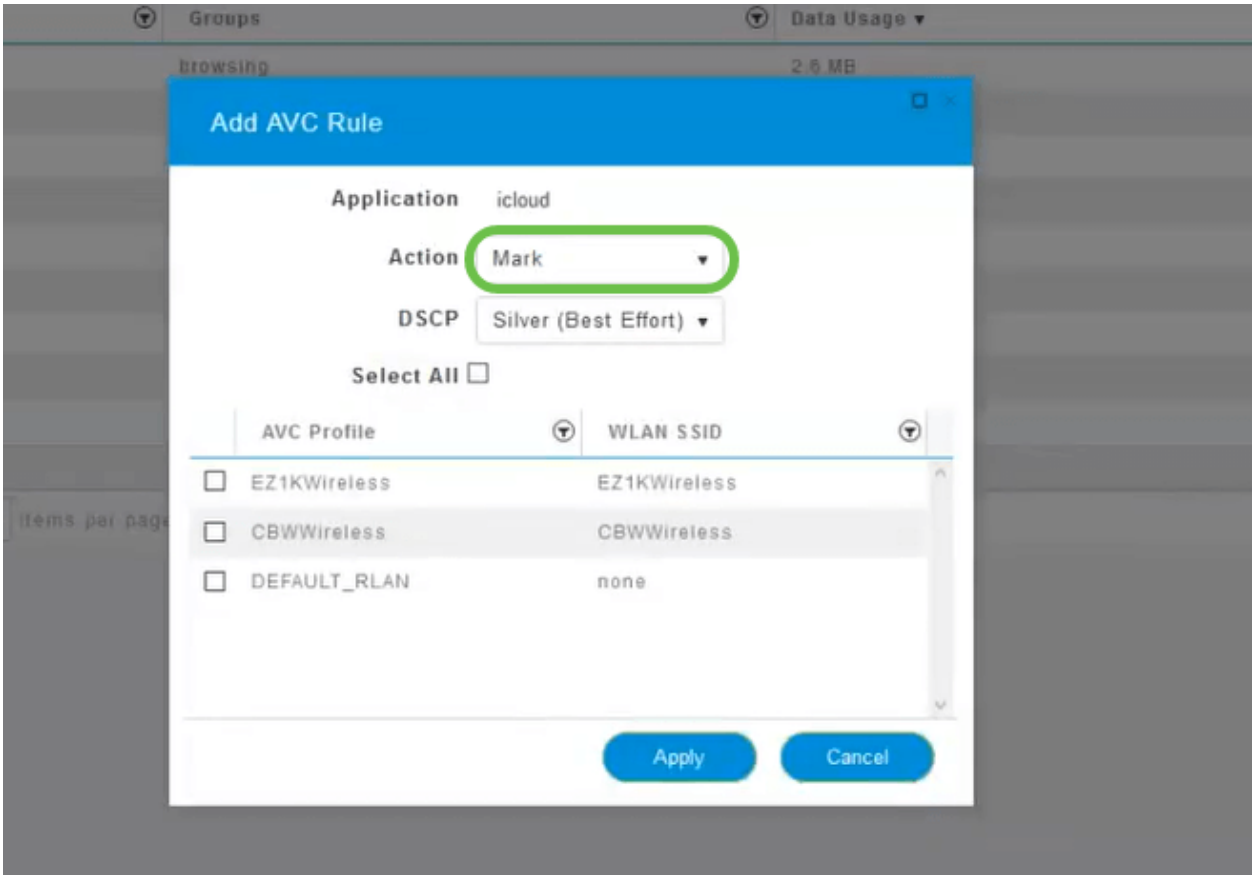
Étape 8

Cliquez sur la ligne correspondant au type de trafic que vous souhaitez gérer.



Étape 9

Cliquez sur la liste déroulante **Action** pour sélectionner la manière dont vous traiterez ce type de trafic.



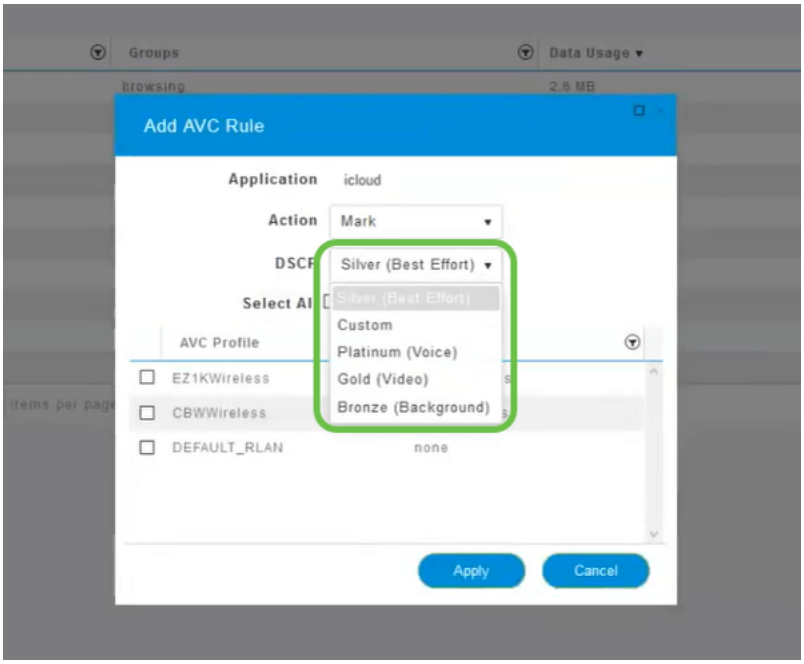
Pour cet exemple, nous laissons cette option à *Mark*.

Mesures à prendre en matière de trafic

- Marquer : place le type de trafic dans l'un des 3 niveaux DSCP (Differentiated Services Code Point), qui détermine le nombre de ressources disponibles pour le type d'application.
- Déposer - Ne faites rien d'autre que rejeter le trafic
- Limite de débit : permet de définir le taux moyen et le taux de rafale en Kbits/s.

Étape 10

Cliquez sur la liste déroulante du champ **DSCP** pour sélectionner l'une des options suivantes.



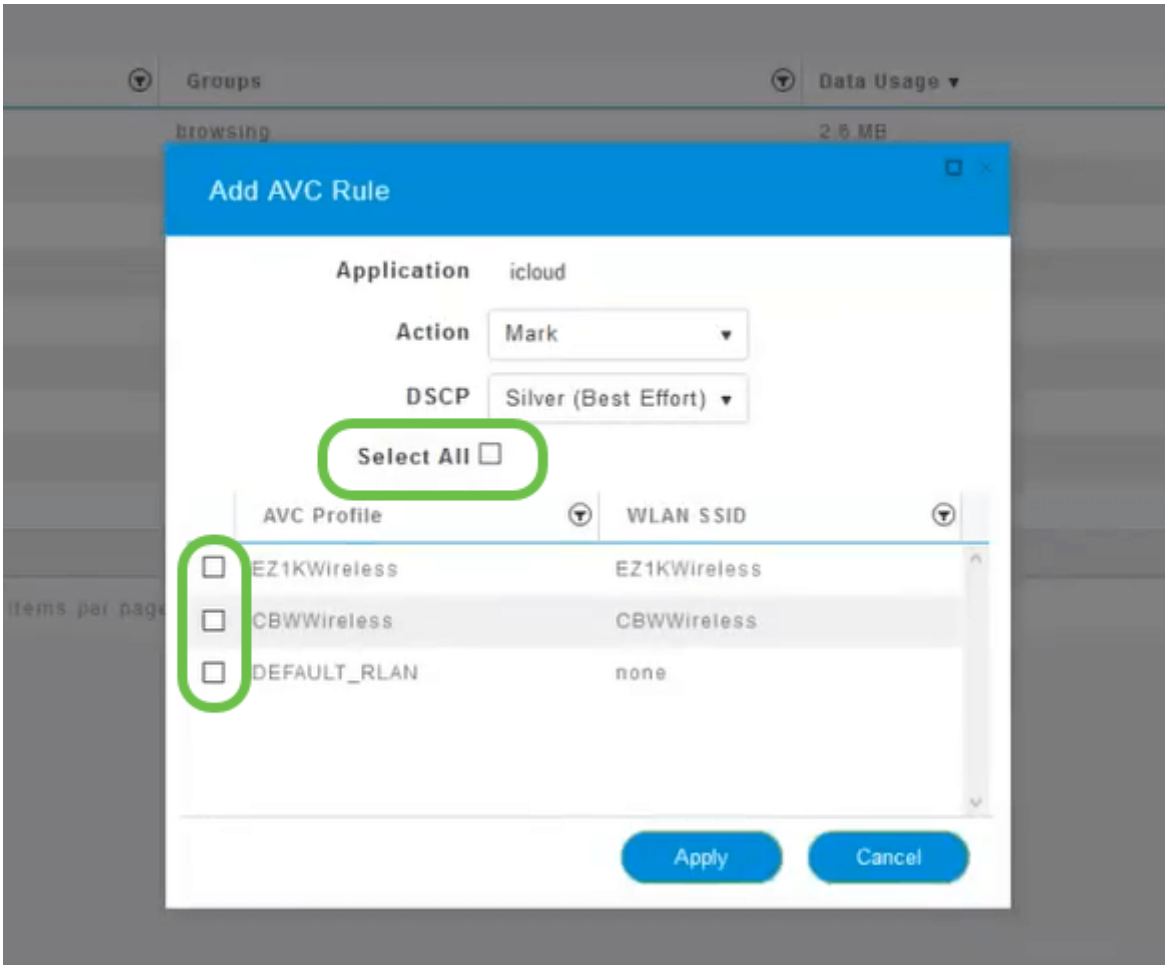
Vous trouverez ci-dessous les options DSCP du trafic à marquer. Ces options passent de moins de ressources à plus de ressources disponibles pour le type de trafic que vous modifiez.

- Bronze (arrière-plan) - Moins
- Argent (au mieux)
- Gold (vidéo)
- Platinum (voix) Plus
- Personnalisé - Ensemble d'utilisateurs

En tant que convention Web, le trafic a migré vers la navigation SSL, ce qui vous empêche de voir ce qui se trouve à l'intérieur des paquets lorsqu'ils se déplacent de votre réseau vers le WAN. Ainsi, une grande majorité du trafic Web utilisera SSL. La définition du trafic SSL pour une priorité inférieure peut affecter votre navigation.

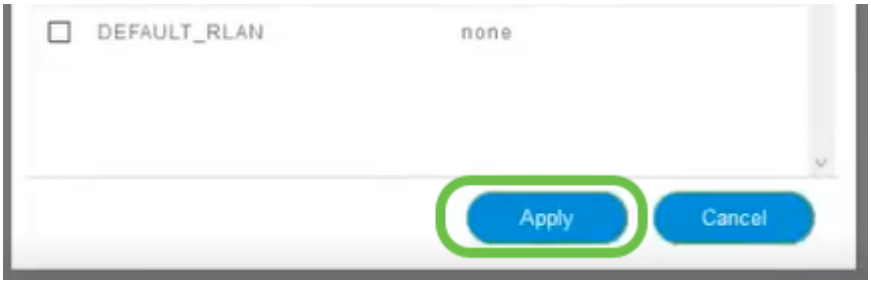
Étape 11

Sélectionnez maintenant le SSID individuel que vous souhaitez exécuter ou cliquez sur **Sélectionner tout**.



Étape 12

Cliquez maintenant sur **Appliquer** pour commencer cette stratégie.



Deux cas où cela pourrait s'appliquer :

- Les invités/utilisateurs diffusent une grande quantité de trafic, ce qui empêche le trafic critique de passer. Vous pouvez soit augmenter la priorité de la voix, soit diminuer la priorité du trafic Netflix pour améliorer les choses.
- Le téléchargement de mises à jour logicielles de grande taille pendant les heures de bureau peut être déclassé ou limité.

Tu l'as fait ! Le profilage des applications est un outil très puissant qui peut être activé en activant également le profilage des clients, comme indiqué dans la section suivante.

Profilage client à l'aide de l'interface utilisateur Web (facultatif)

Lors de la connexion à un réseau, les périphériques échangent des informations de

profilage client. Par défaut, le *profilage du client* est désactivé. Ces renseignements peuvent comprendre :

- Nom d'hôte - ou nom du périphérique
- Système d'exploitation : logiciel principal du périphérique
- Version du système d'exploitation : itération du logiciel applicable

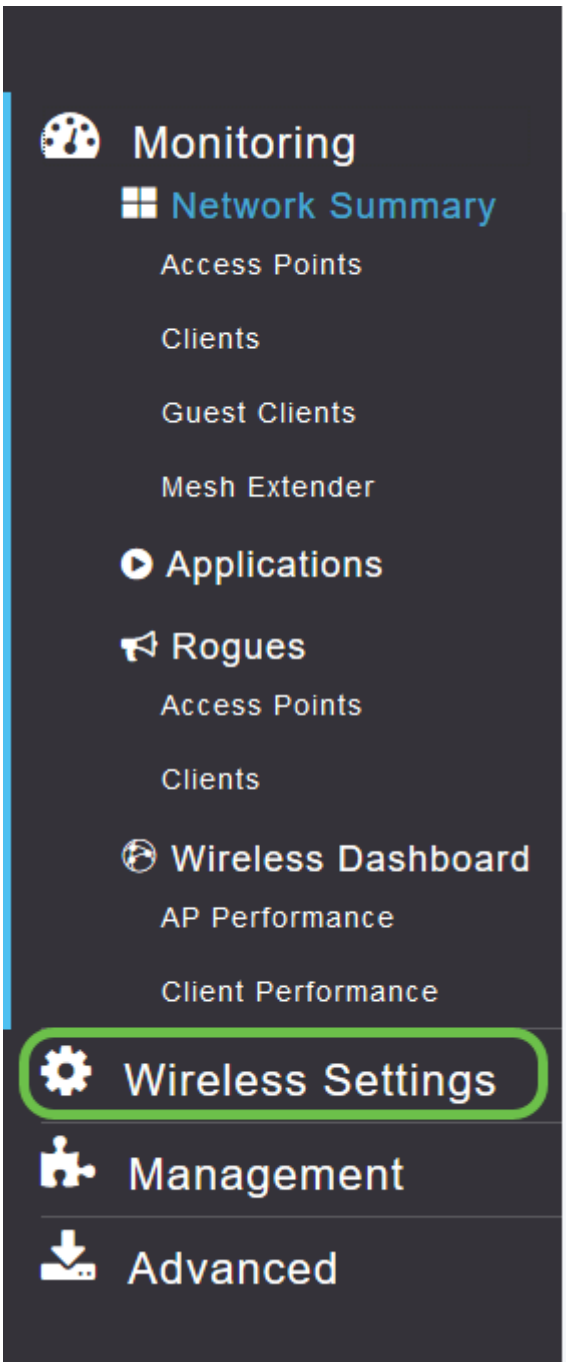
Les statistiques relatives à ces clients incluent la quantité de données utilisées et le débit.

Le suivi des profils clients permet un meilleur contrôle sur le réseau local sans fil. Ou vous pouvez l'utiliser en fonction d'une autre fonctionnalité. Par exemple, en utilisant des types de périphériques de limitation d'applications qui ne transportent pas de données critiques pour votre entreprise.

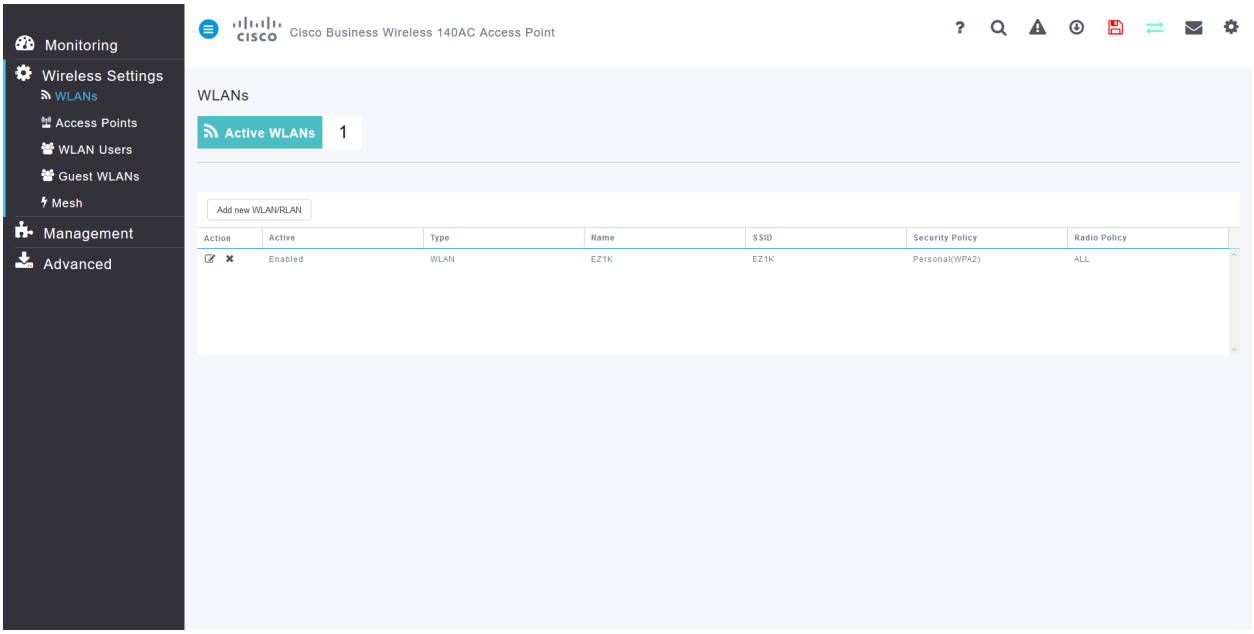
Une fois activé, les détails du client pour votre réseau se trouvent dans la section Surveillance de l'interface utilisateur Web.

Étape 1

Cliquez sur **Wireless Settings (Paramètres sans fil)**.

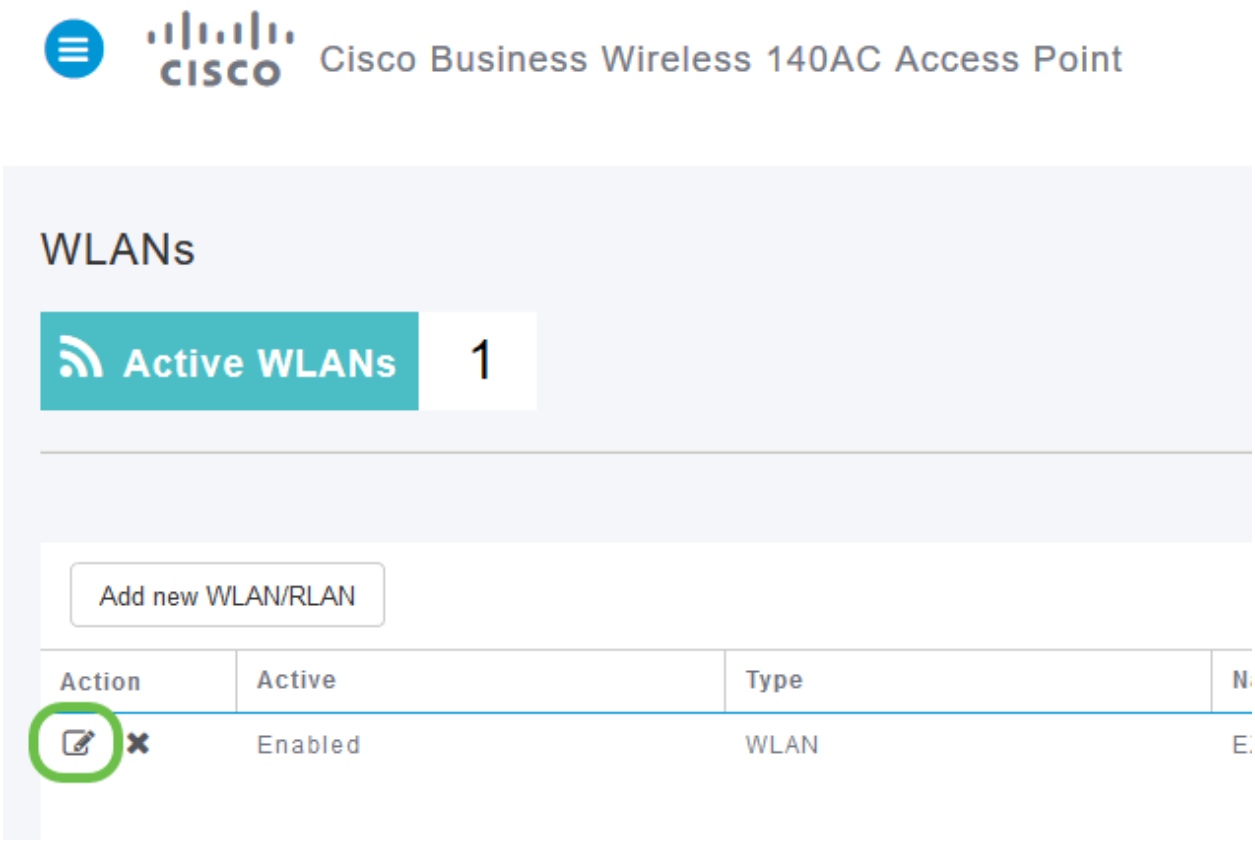


Les informations ci-dessous sont similaires à celles que vous verrez lorsque vous cliquez sur le lien Wireless Settings (Paramètres sans fil) :



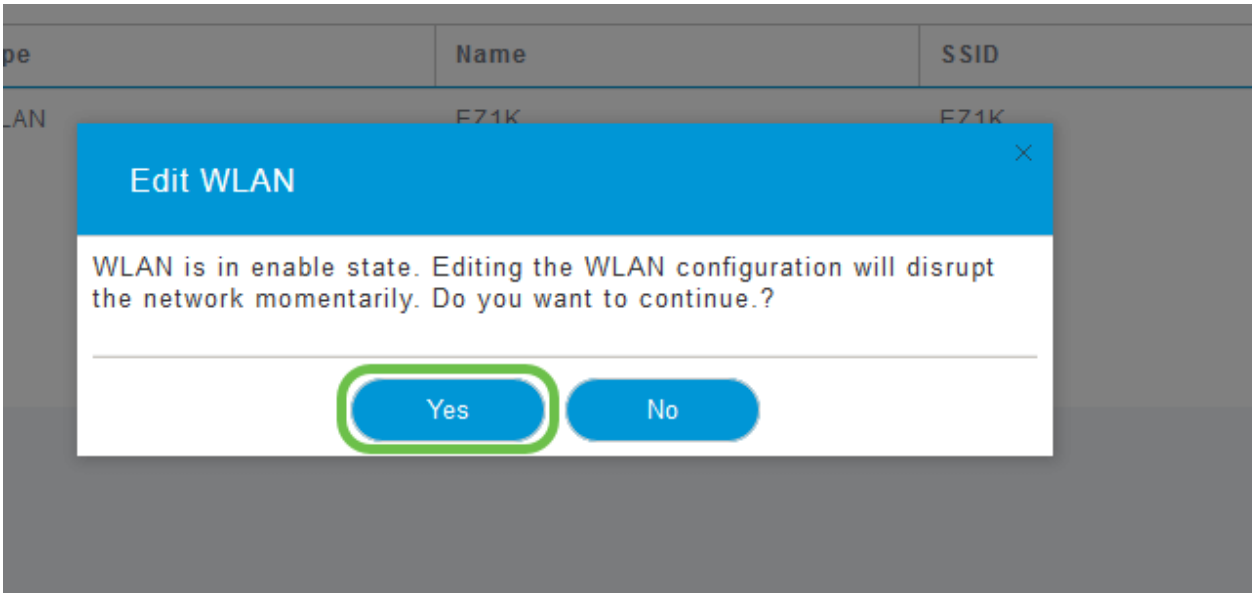
Étape 2

Choisissez le WLAN que vous voulez utiliser pour l'application et cliquez sur l'**icône de modification** à gauche de celle-ci.



Étape 3

Un menu contextuel peut s'afficher de la même manière que ci-dessous. Ce message important peut affecter temporairement le service sur votre réseau. Cliquez sur **Oui** pour avancer.

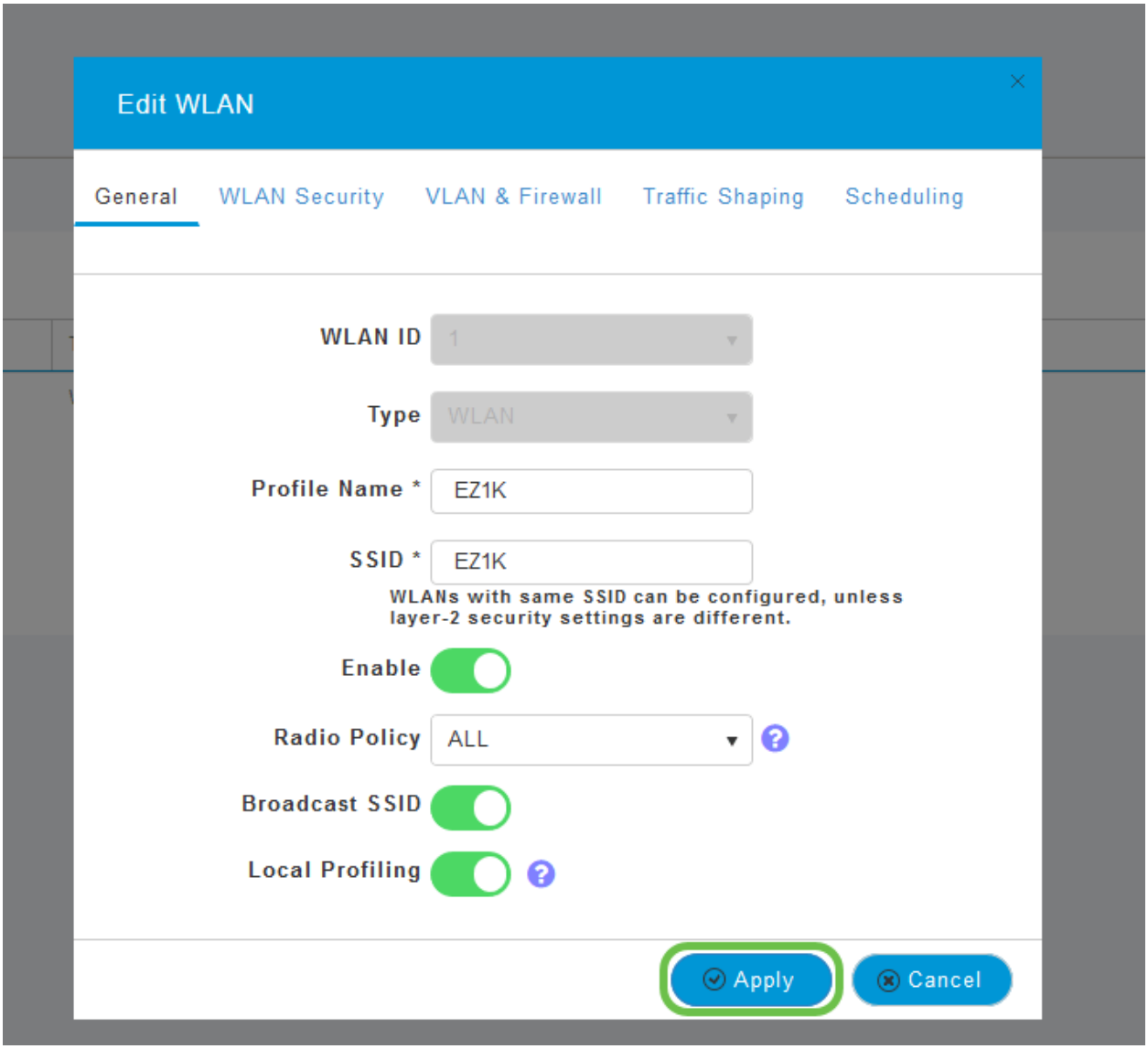


Étape 4

Basculer le profilage du client en cliquant sur le bouton bascule **Profilage local**.

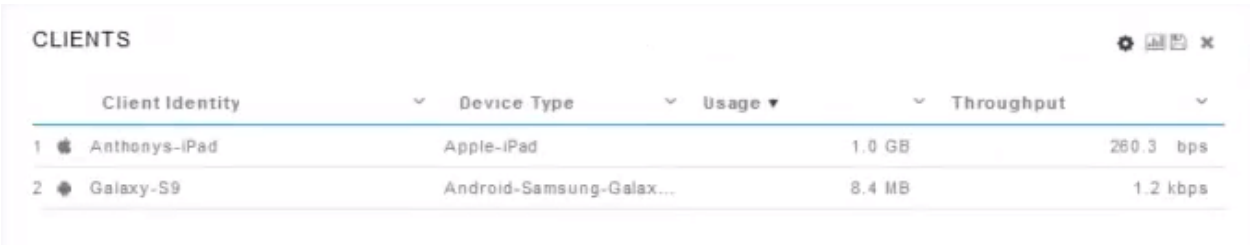
Étape 5

Cliquez sur Apply.



Étape 6

Cliquez sur l'élément de menu de la section **Surveillance** à gauche. Les données du client commencent à apparaître dans le tableau de bord de l'onglet *Surveillance*.



Conclusion

Vous avez maintenant terminé la configuration de votre réseau sécurisé. Quelle sensation, maintenant prenez une minute pour célébrer et ensuite vous mettez au travail!

Nous voulons le meilleur pour nos clients. Vous avez donc des commentaires ou des suggestions sur ce sujet, veuillez nous envoyer un e-mail à l'équipe de contenu Cisco.

Si vous souhaitez lire d'autres articles et documents, consultez les pages d'assistance

de votre matériel :

- Routeur VPN Cisco RV260P avec PoE
- Point d'accès Cisco Business 140AC
- Extendeur maillé Cisco Business 142ACM