# Configuration réseau totale : RV345P et Cisco Business Wireless à l'aide de l'interface utilisateur Web

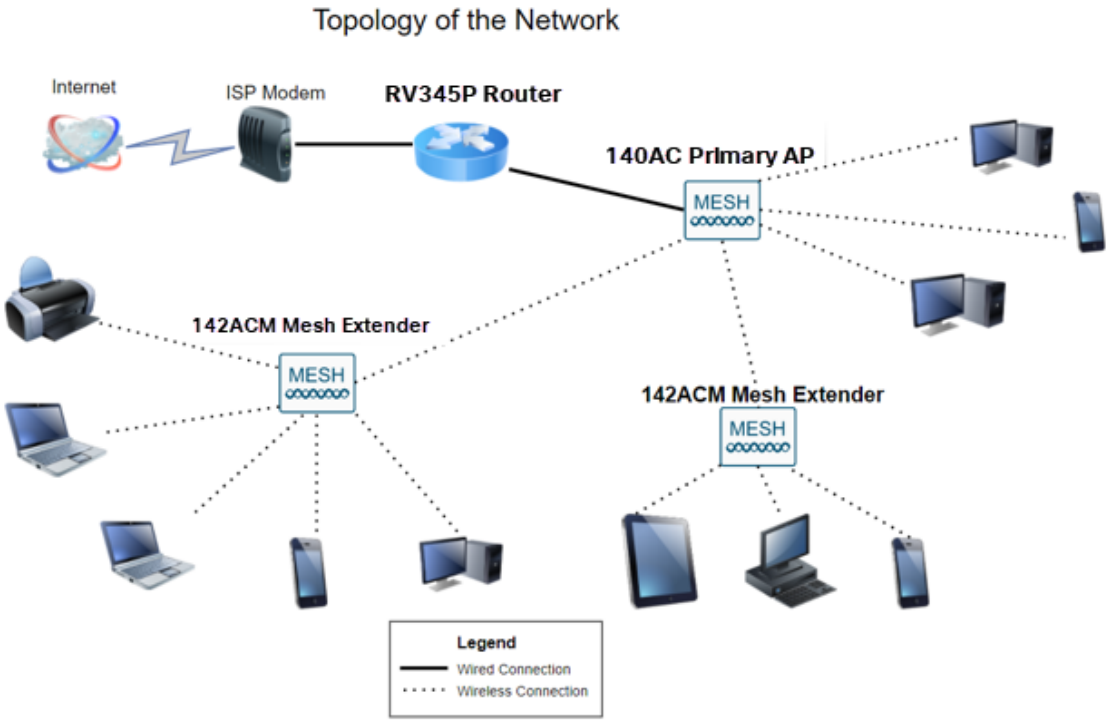
## Objectif

Ce guide explique comment configurer un réseau maillé sans fil à l'aide d'un routeur RV345P, 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.

## Table des matières

# Topologie




## Introduction

Toutes vos recherches se sont combinées et vous avez acheté votre équipement Cisco, c'est excitant ! Dans ce scénario, nous utilisons un routeur RV345P. 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.

Ce routeur avancé offre également la possibilité d'ajouter des fonctionnalités supplémentaires.

1. Le contrôle des applications vous permet de contrôler le trafic. Cette fonctionnalité peut être configurée pour autoriser le trafic mais pour le consigner, bloquer le trafic et le

consigner, ou simplement pour bloquer le trafic.

2. Le filtrage Web est utilisé pour empêcher le trafic Web vers des sites Web non sécurisés ou inappropriés. Il n'y a pas de journalisation avec cette fonctionnalité.
3. AnyConnect est un réseau privé virtuel (VPN) SSL (Secure Sockets Layer) disponible auprès de Cisco. Les VPN permettent aux utilisateurs et aux sites distants de se connecter au bureau ou aux data centers de votre entreprise en créant un tunnel sécurisé via Internet.

Pour utiliser ces fonctionnalités, vous devez acheter une licence. Les routeurs et les licences sont enregistrés en ligne, ce qui sera traité dans ce guide.

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

### Périphériques pertinents | Version du logiciel

- RV345P |1.0.03.21
- CBW140AC |10.4.1.0
- CBW142ACM | 10.4.1.0 (au moins un extendeur de maillage est nécessaire pour le réseau maillé)

## Conditions préalables

### Préparation du routeur

1. Vérifiez que vous disposez d'une connexion Internet en cours pour l'installation.
2. Contactez votre fournisseur d'accès à Internet (FAI) pour connaître les instructions spéciales qu'il peut suivre lors de l'utilisation de votre routeur RV345P. 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).

### Obtenir un compte Cisco.com

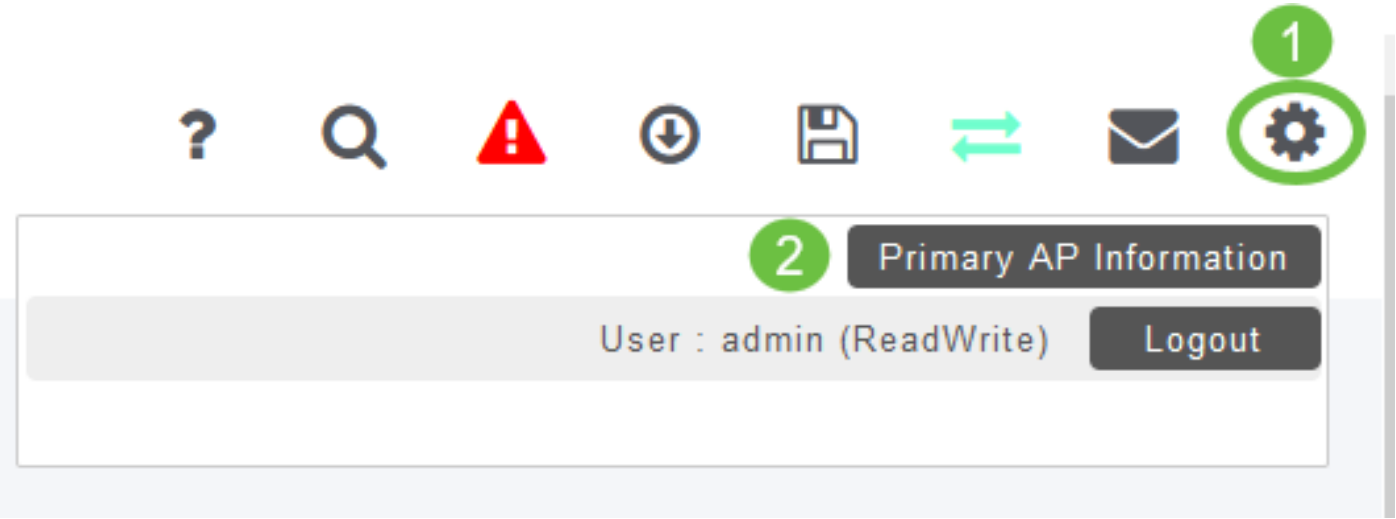
Maintenant que vous possédez un équipement Cisco, vous devez obtenir un compte Cisco.com, parfois appelé Cisco Connection Online Identification (CCO ID). Il n'y a pas

de frais pour un compte.

Si vous avez déjà un compte, vous pouvez passer à la section suivante de cet article.

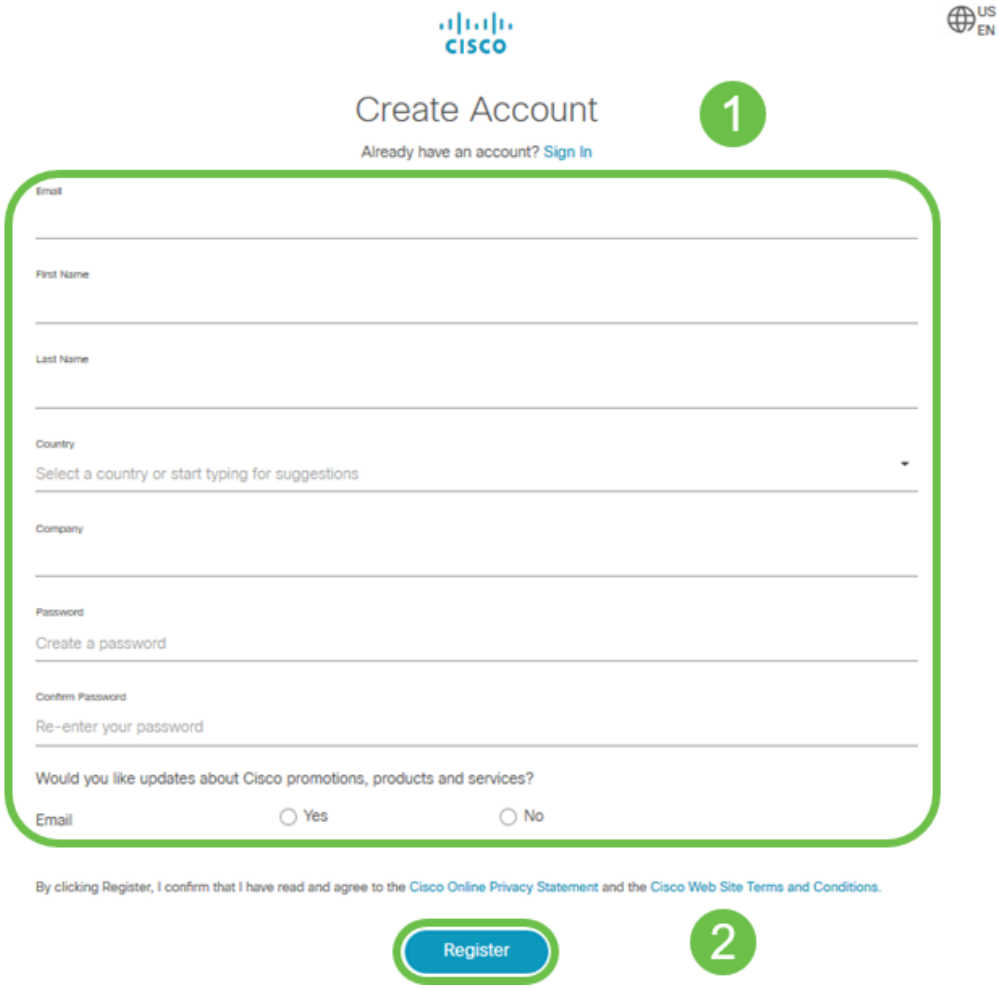
### Étape 1

Accédez à Cisco.com. Cliquez sur l'**icône de la personne**, puis **créez un compte**.




### Étape 2

Entrez les détails requis pour créer le compte et cliquez sur **Register**. Suivez les instructions pour terminer le processus d'inscription.




Si vous rencontrez des problèmes, cliquez sur pour accéder à la page d'aide sur l'enregistrement des comptes Cisco.com.

# Configuration du routeur RV345P

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 RV345P est livré avec des paramètres par défaut optimisés pour de nombreuses petites entreprises. Toutefois, vos demandes réseau ou votre fournisseur d'accès à Internet (FAI) peuvent nécessiter que vous modifiez 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.

Êtes-vous prêts ? Allons-y !

## RV345P prêt à l'emploi

### Étape 1

Connectez le câble Ethernet d'un des ports Ethernet (LAN) du RV345P 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 RV345P pour effectuer la configuration initiale.

### Étape 2

Veillez à utiliser l'adaptateur secteur fourni avec le RV345P. L'utilisation d'un autre adaptateur secteur peut endommager le RV345P ou provoquer l'échec des dongles USB. L'interrupteur d'alimentation est activé par défaut.

Connectez l'adaptateur électrique au port 12 VCC du RV345P, 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 RV345P.

### Étape 5

Branchez l'autre extrémité de l'adaptateur RV345P sur une prise électrique. Le RV345P est alors 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 RV345P a terminé le démarrage.

## Configuration du routeur

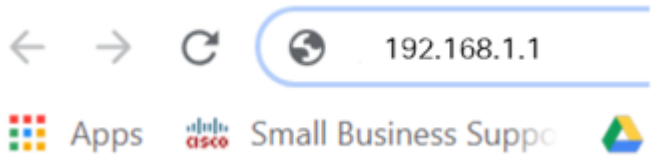
Le travail de préparation est terminé, il est maintenant temps d'accéder à certaines configurations ! Pour lancer l'interface utilisateur Web, procédez comme suit.

### 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.

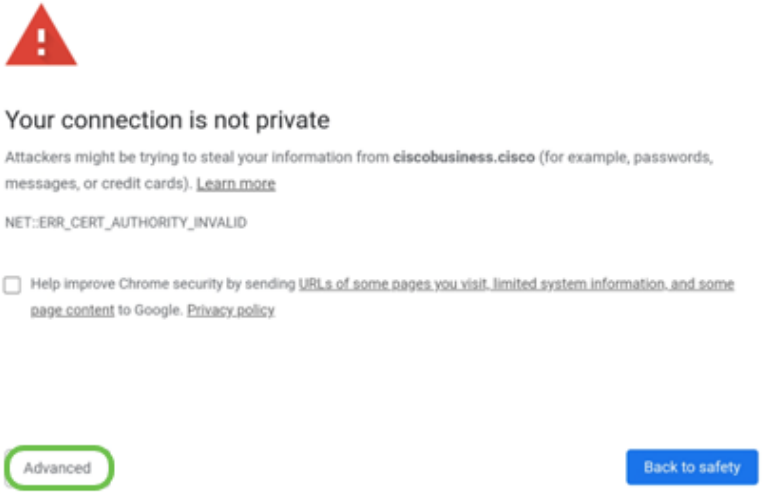
### Étape 2

Ouvrez un navigateur Web tel que Safari, Internet Explorer ou Firefox. Dans la barre d'adresses, saisissez l'adresse IP par défaut du routeur RV345P, 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.

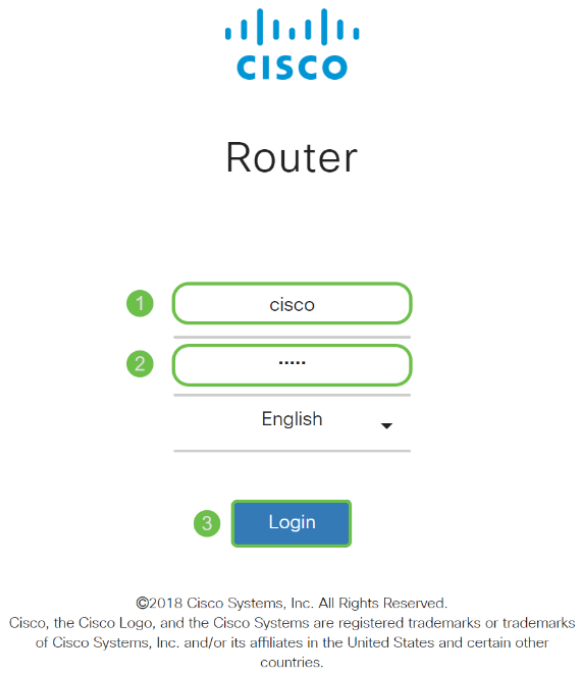



## Étape 4

Lorsque la page de connexion apparaît, saisissez le nom d'utilisateur par défaut *cisco* et le mot de passe par défaut *cisco*.

Cliquez sur **Connexion**.

Pour plus d'informations, cliquez sur Comment accéder à la page de configuration Web des routeurs VPN de la gamme Cisco RV340.




**Étape 5**

Cliquez sur **Connexion**. La page *Mise en route* s'affiche. Si le volet de navigation n'est pas ouvert, vous pouvez l'ouvrir en cliquant sur l'**icône de menu**.

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 cet article Dépannage.

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 RV345P). Pour vous connecter, vous devrez peut-être modifier les paramètres réseau du RV345P. Si vous utilisez Windows 10, consultez les

instructions de Windows 10 pour modifier les paramètres réseau.

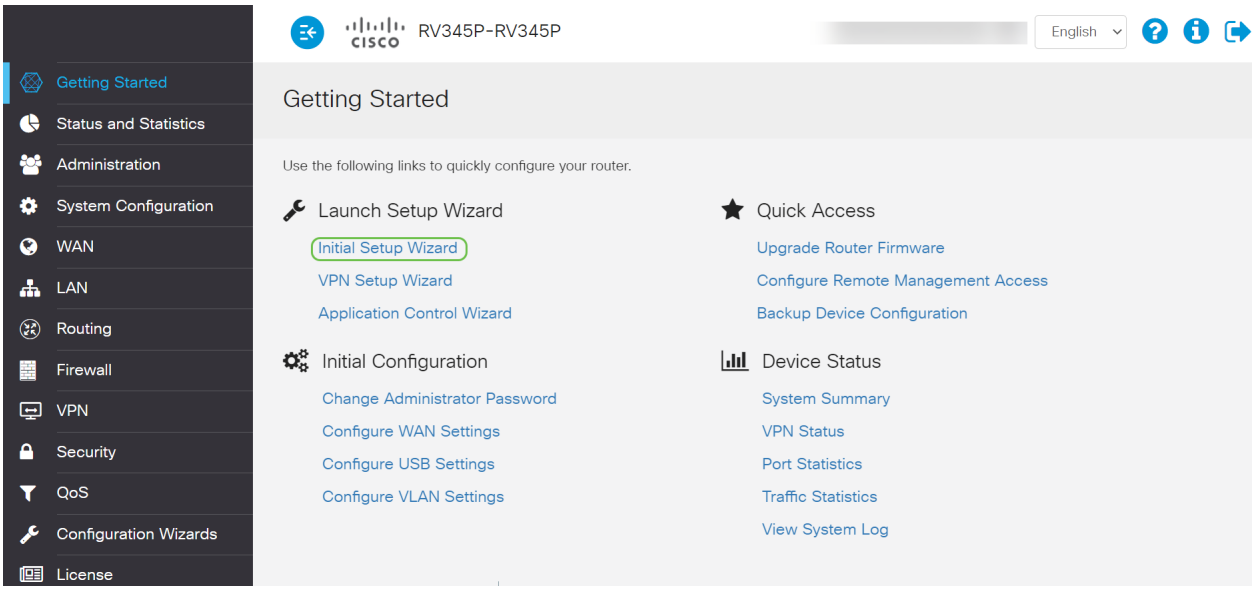
3. Si vous disposez d'un équipement occupant l'adresse IP 192.168.1.1, vous devez résoudre ce conflit pour que le réseau fonctionne. Pour en savoir plus à la fin de cette section, ou cliquez ici pour vous y rendre directement.
4. Réinitialisez le modem et le RV345P en éteignant les deux périphériques. Ensuite, mettez le modem sous tension et laissez-le inactif pendant environ 2 minutes. Mettez ensuite le RV345P 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 passer par les étapes *de l'Assistant de configuration initiale* répertoriées dans cette section. Vous pouvez modifier ces paramètres à tout moment.

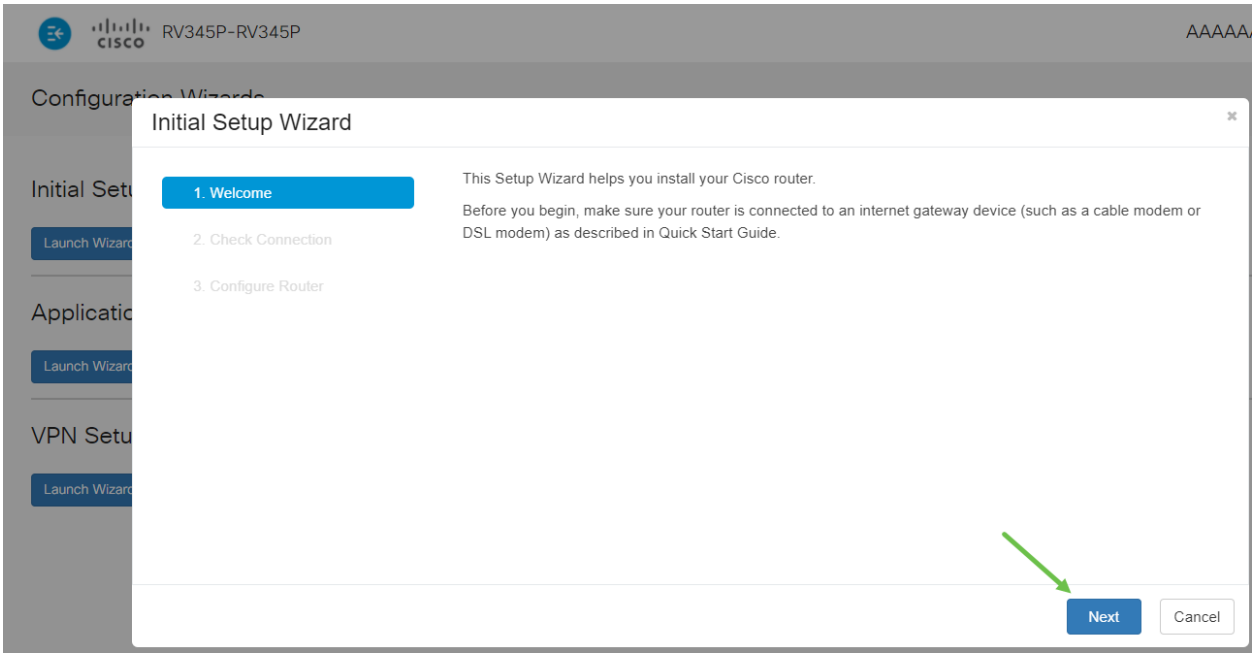
### Étape 1

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



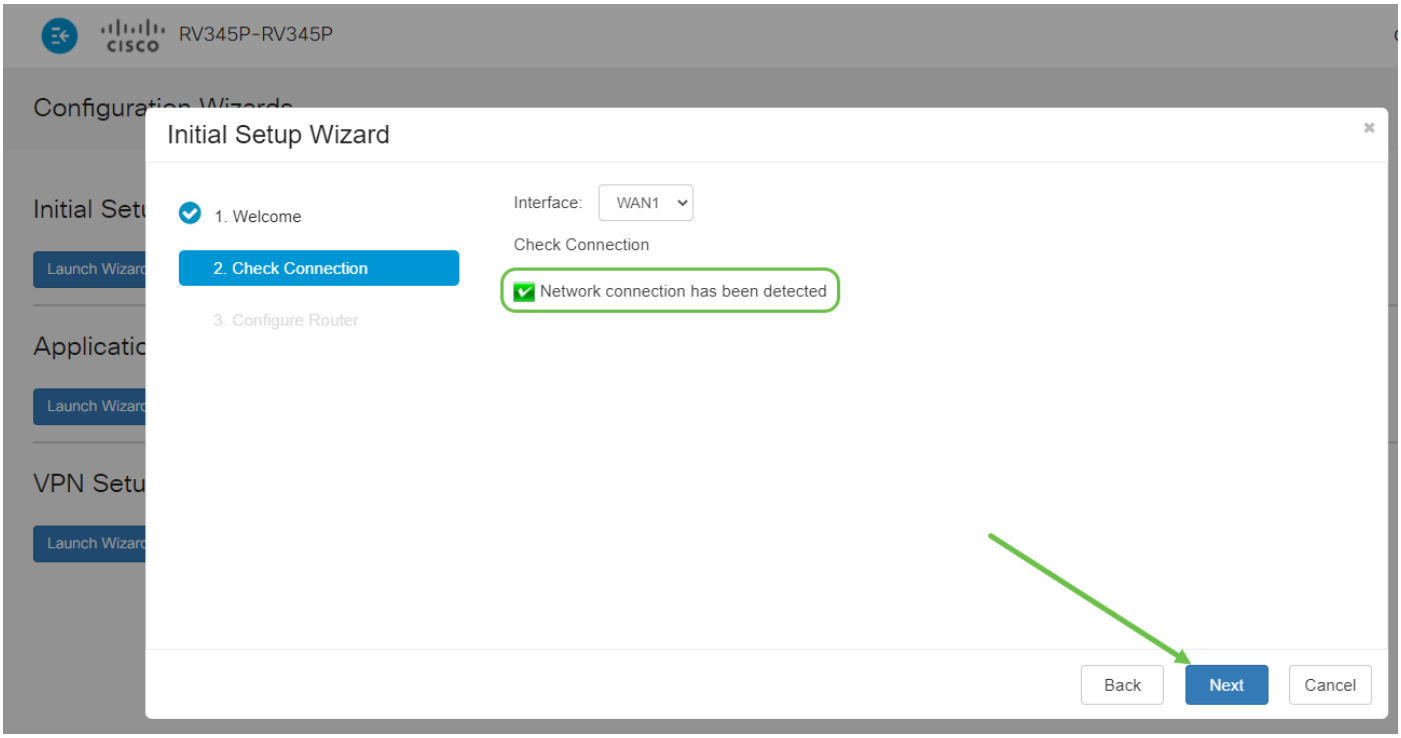

### Étape 2

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



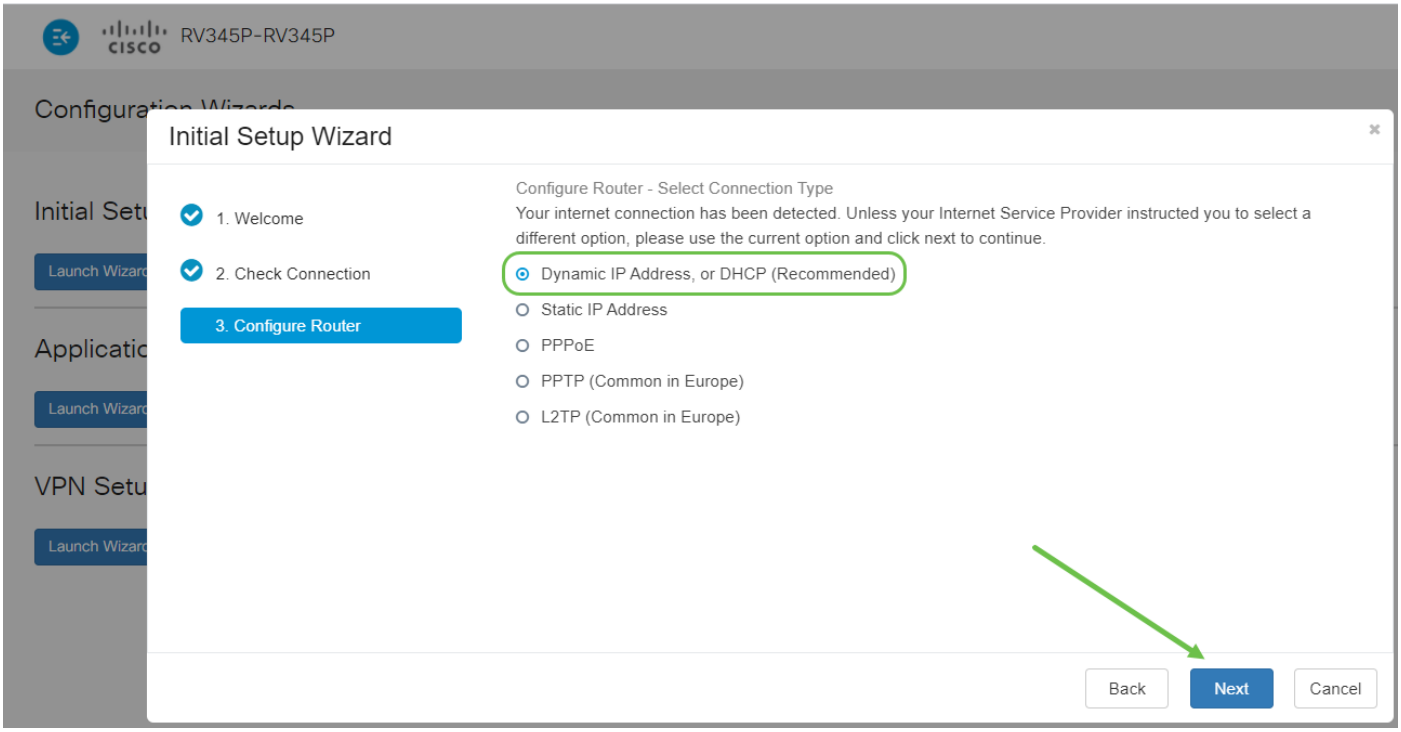

## Étape 3

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



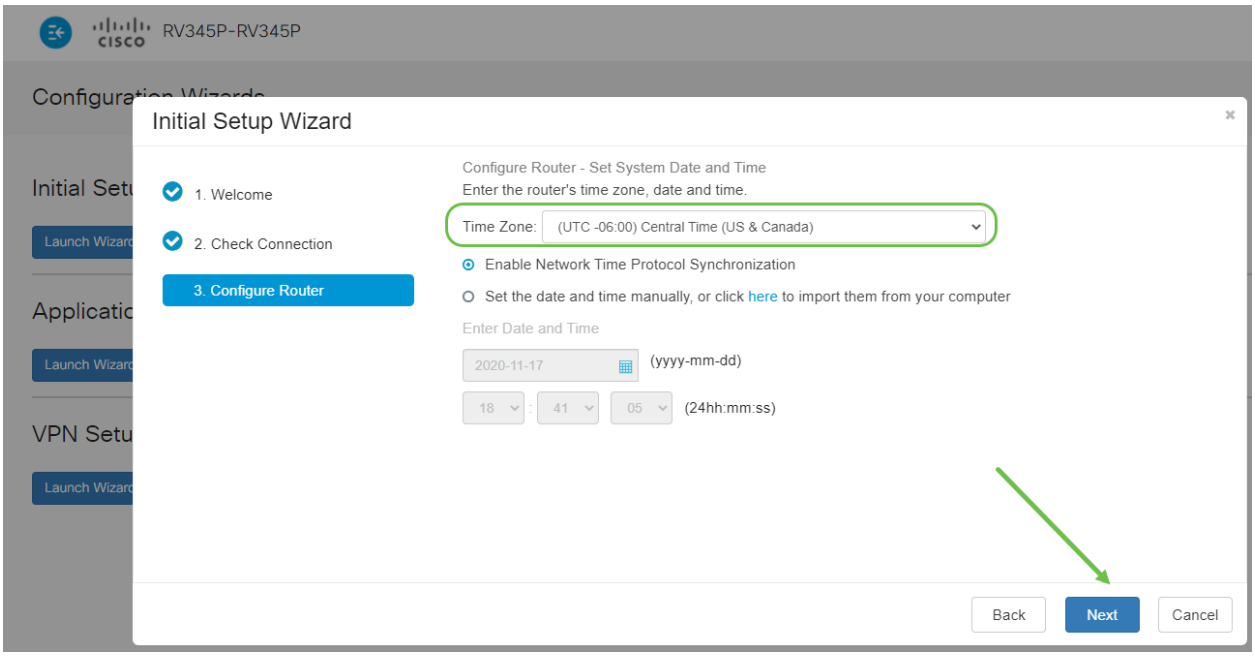

## Étape 4

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).



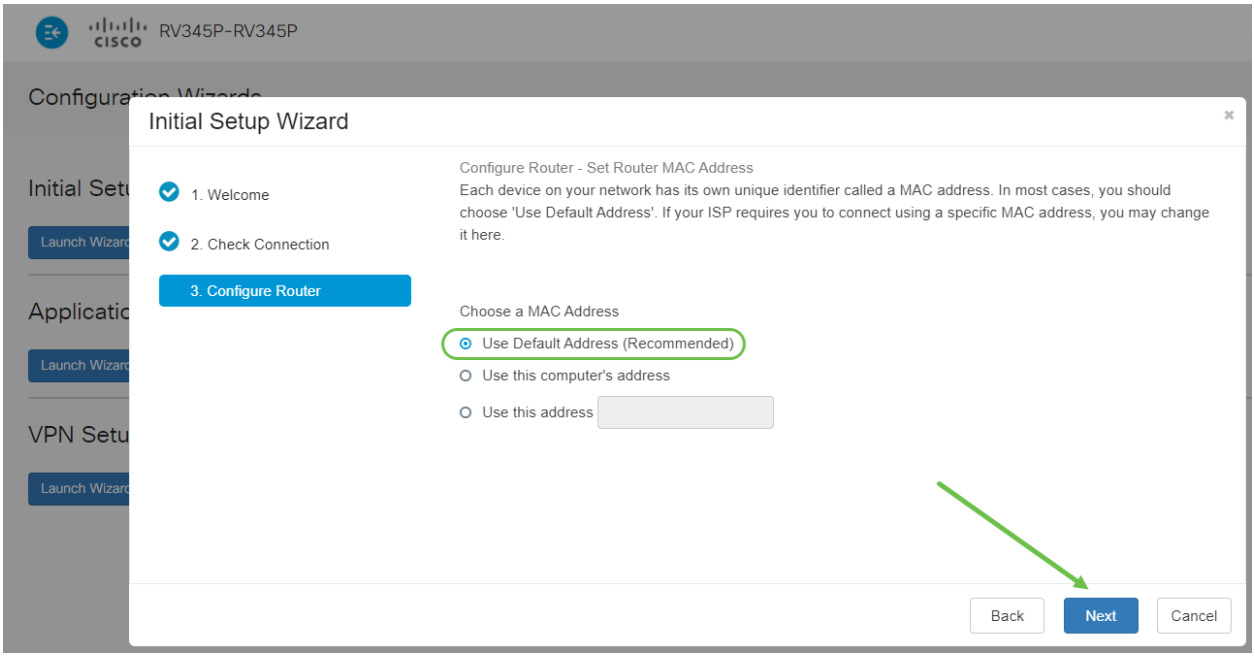

## Étape 5

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**.



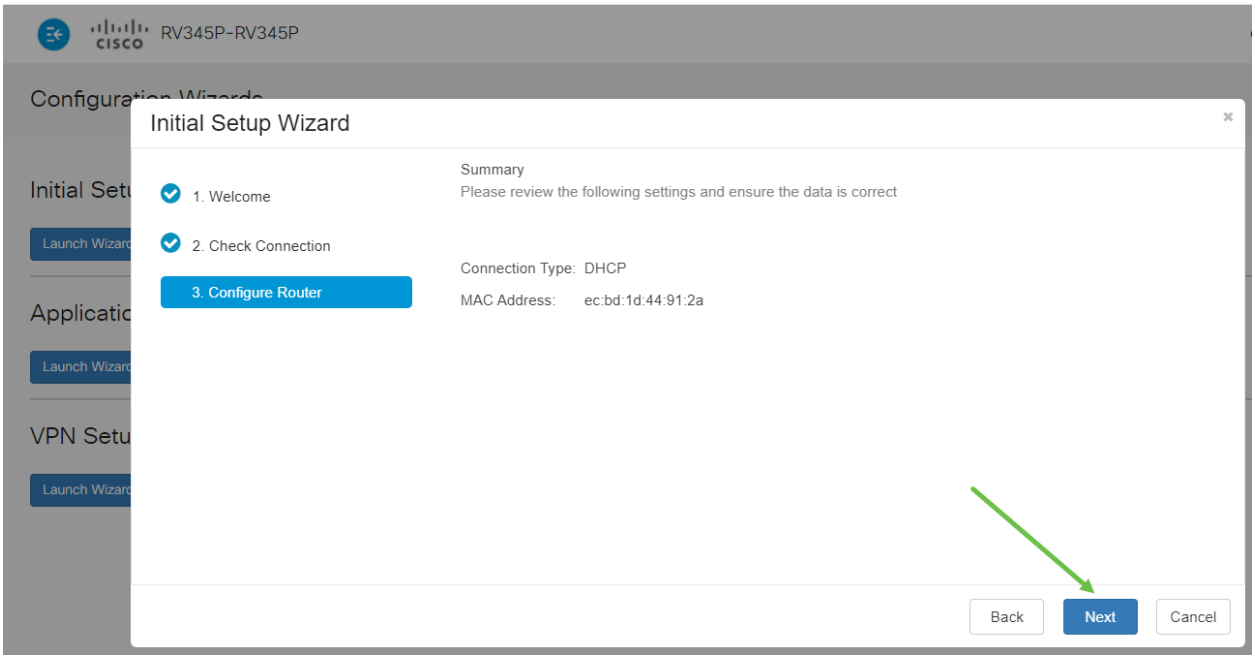

## Étape 6

Vous sélectionnerez les adresses MAC à attribuer aux périphériques. La plupart du temps, vous utiliserez l'adresse par défaut. Cliquez sur Next (Suivant).



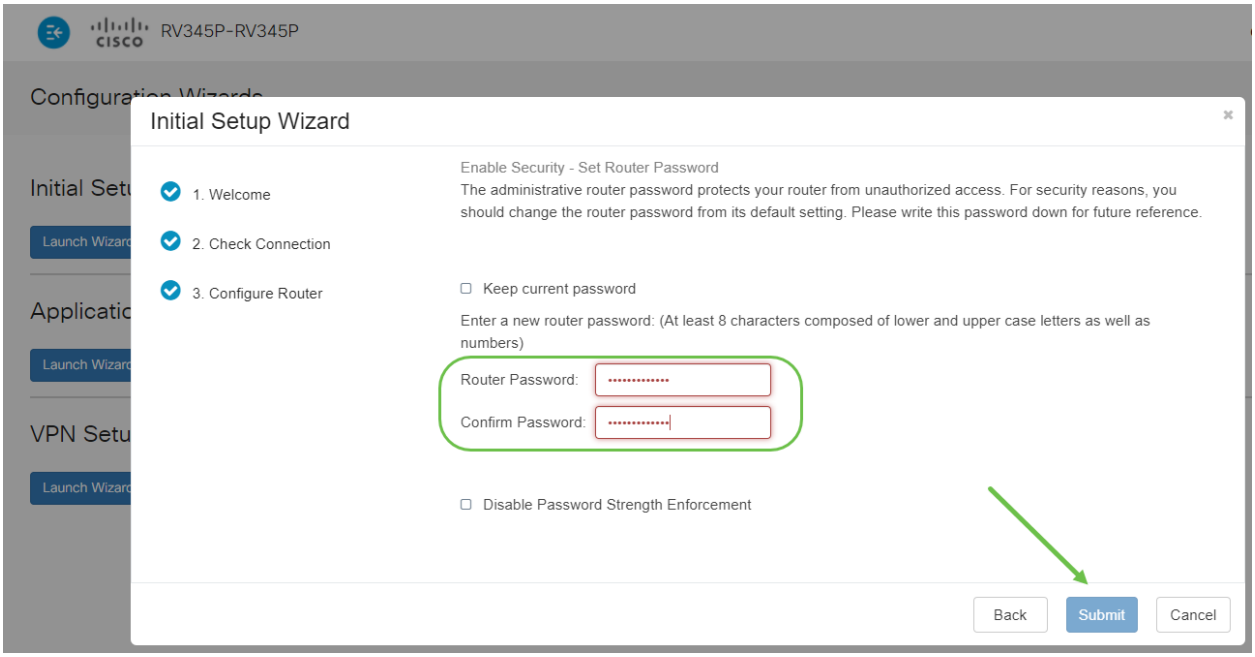

## Étape 7

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**.

Pour plus d'informations sur ces paramètres, vous pouvez lire Configurer les paramètres WAN DHCP sur le routeur RV34x.

La technologie PoE (Power over Ethernet) de votre routeur RV345P est activée par défaut, mais vous pouvez apporter des modifications. Si vous devez personnaliser les paramètres, consultez Configuration des paramètres PoE (Power over Ethernet) sur le routeur RV345P.

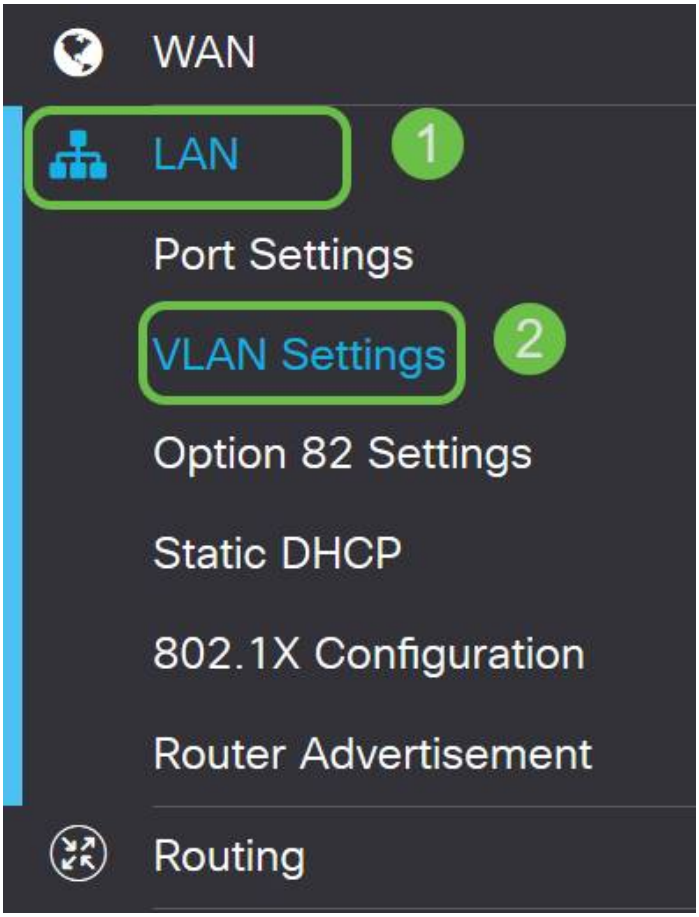
## Modifier une adresse IP si nécessaire (facultatif)

Après avoir terminé l'*Assistant de configuration initiale*, vous pouvez définir une adresse IP statique sur le routeur en modifiant les paramètres VLAN.

Ce processus n'est nécessaire que si l'adresse IP de votre routeur doit être affectée à une adresse spécifique dans votre réseau existant. Si vous n'avez pas besoin de modifier une adresse IP, vous pouvez passer à la section suivante de cet article.

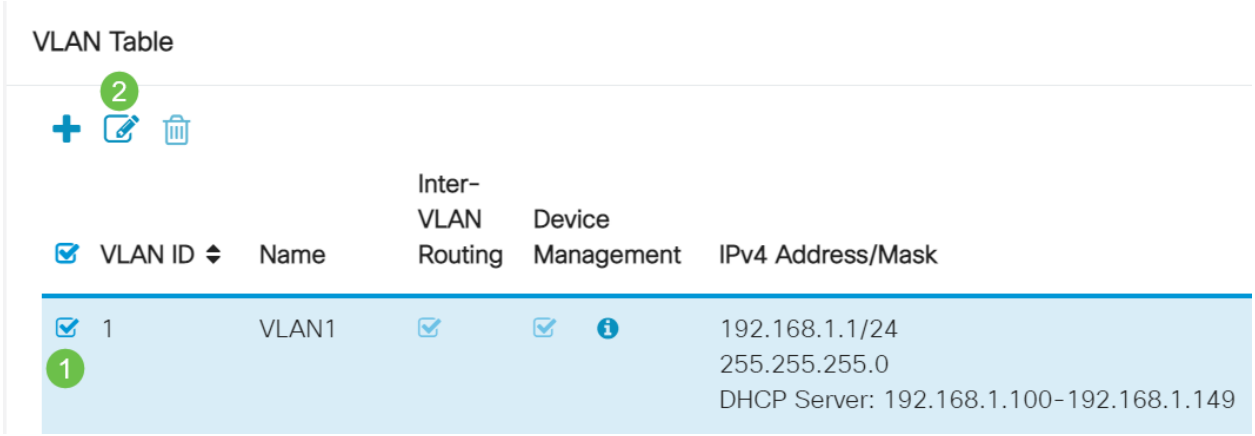
### Étape 1

Dans le menu de gauche, cliquez sur **LAN > VLAN Settings**.



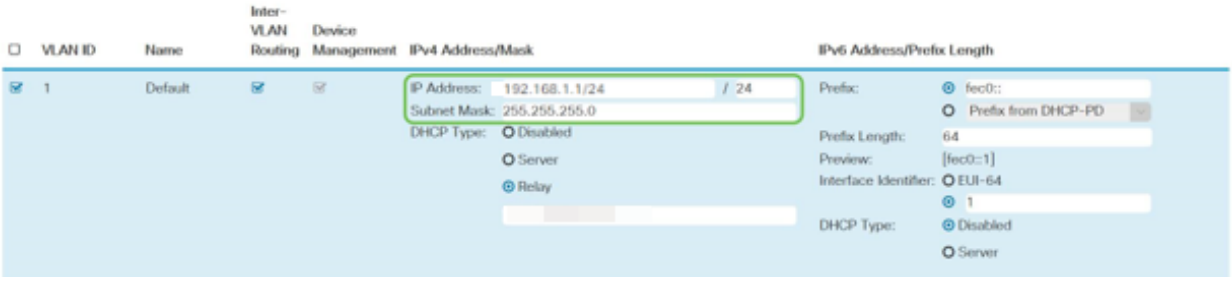

## Étape 2

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



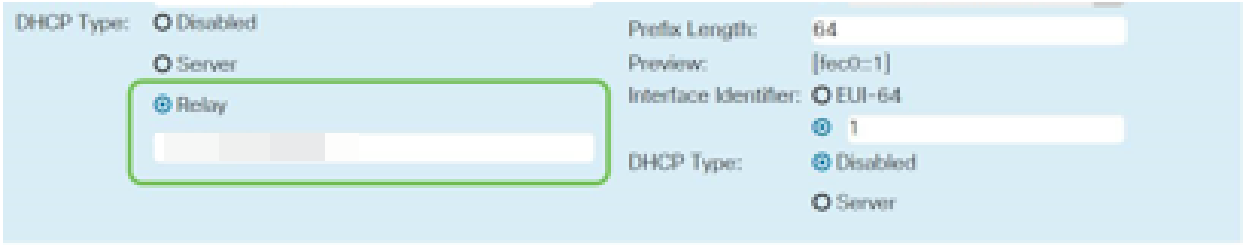

## Étape 3

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.

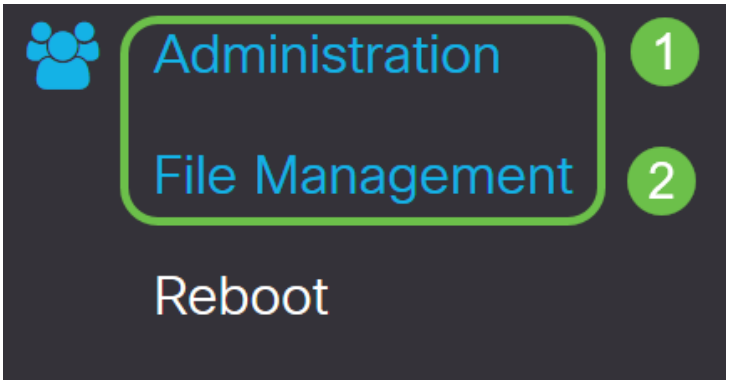



## Mettre à niveau le micrologiciel si nécessaire

C'est une étape importante, ne la sautez pas !

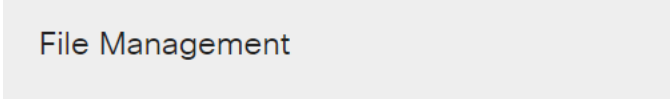
### Étape 1

Choisissez **Administration > File Management**.



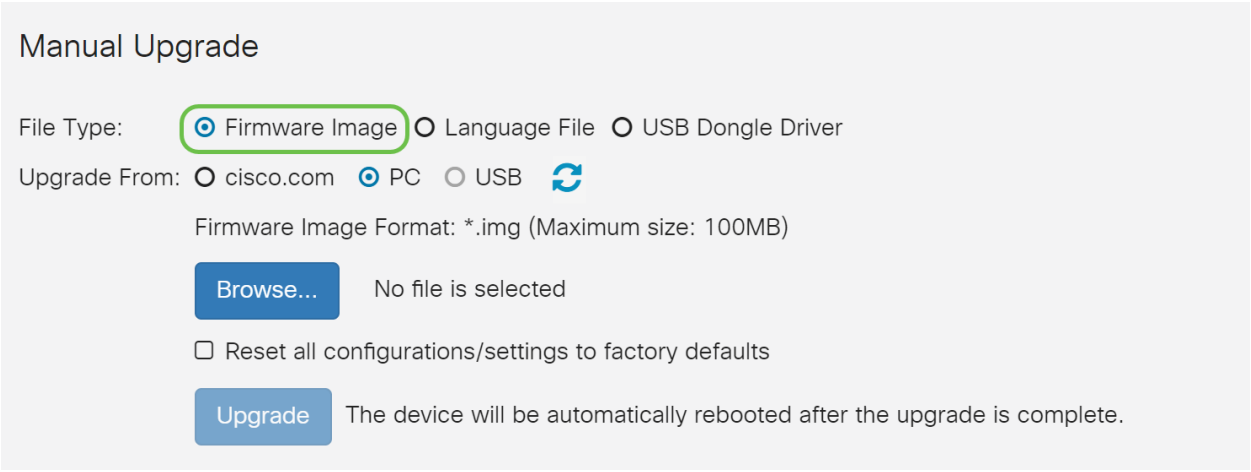

Dans la zone *Informations système*, les sous-zones suivantes décrivent les éléments suivants :

- 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

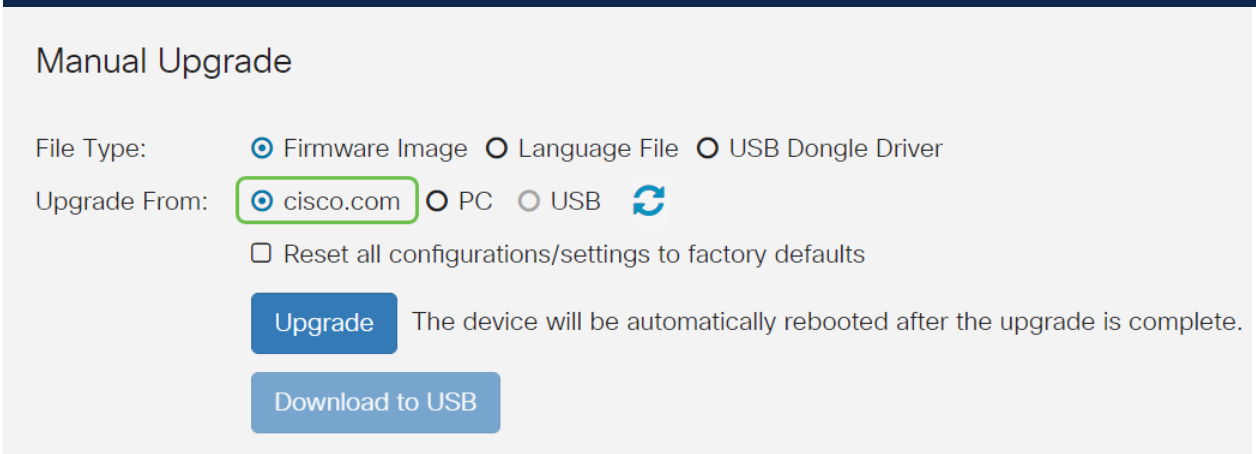
Sous la section *Mise à niveau manuelle*, cliquez sur la case d'option **Image du micrologiciel** pour *Type de fichier*.




## Étape 3

Sur la page *Manual Upgrade*, cliquez sur la 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.

Si votre périphérique n'est pas connecté à Internet ou souffre de déconnexions Internet, vous ne pourrez pas effectuer de mise à niveau depuis cisco.com. Si cela vous concerne, vous pouvez trouver d'autres options ici.

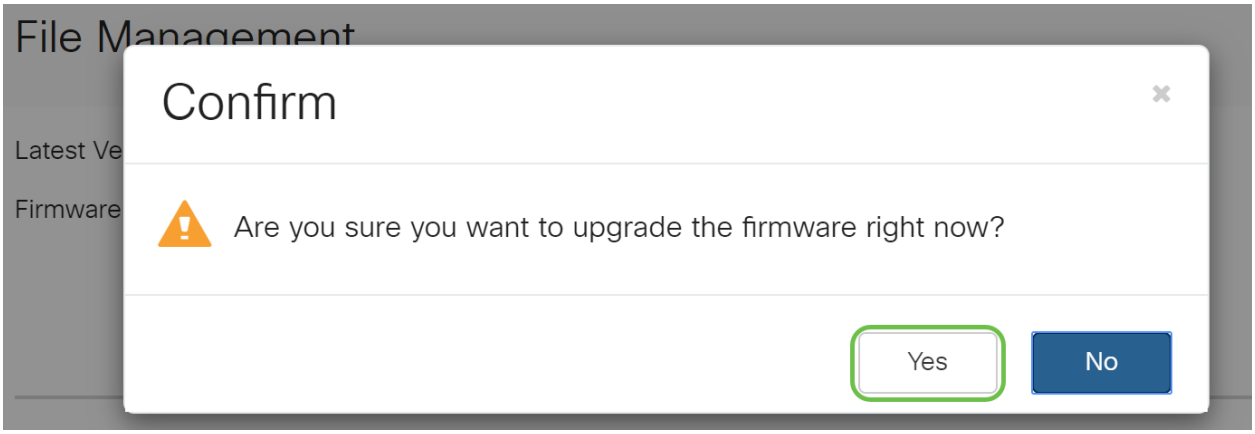



## Étape 4

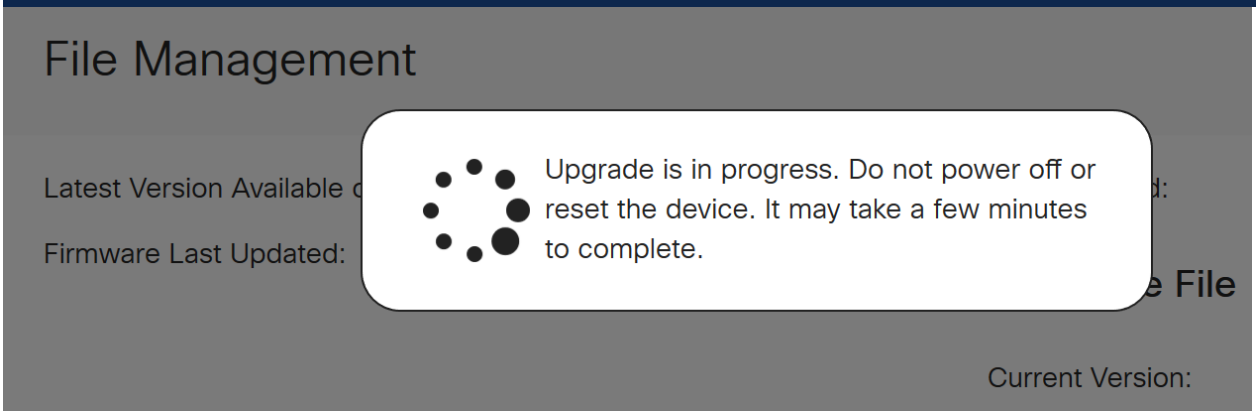
Cliquez sur **Mettre à niveau**.


**Étape 5**

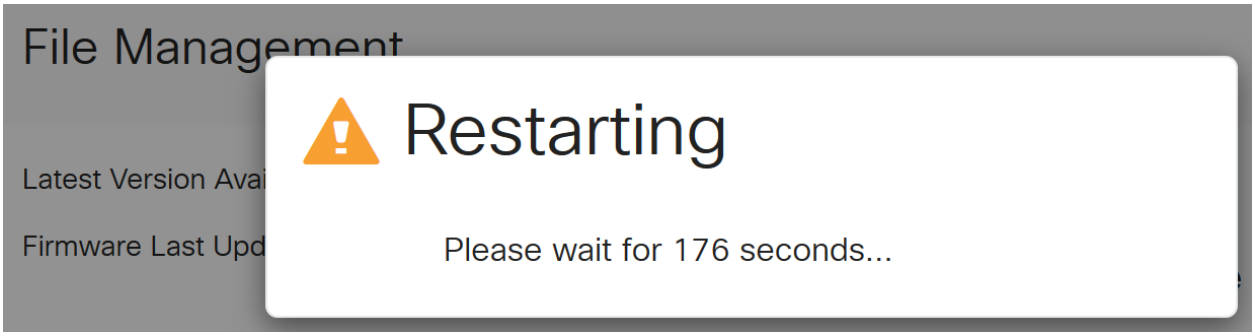
Cliquez sur **Oui** dans la fenêtre de confirmation pour continuer.




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.

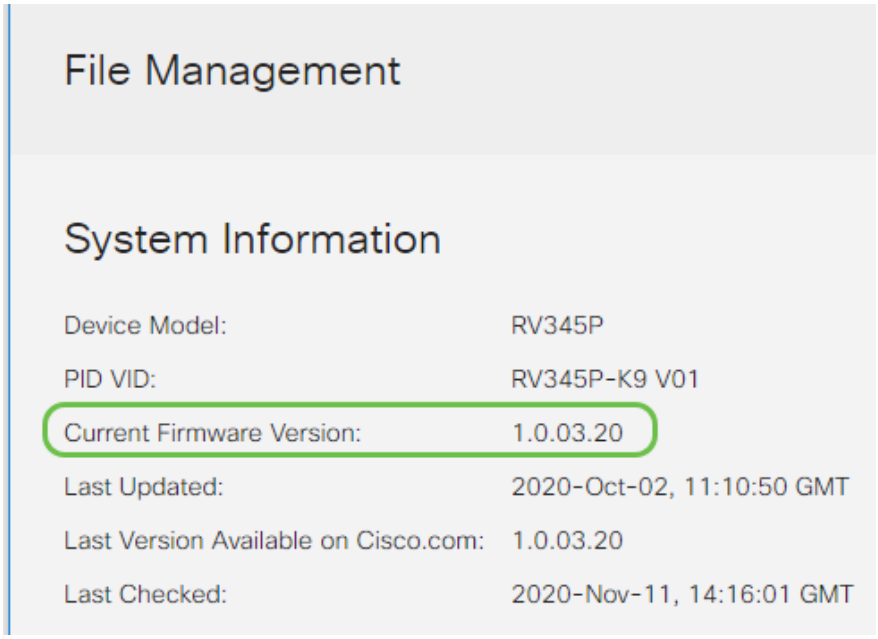



Une fois la mise à niveau terminée, une fenêtre de notification s'affiche pour vous informer que le routeur va *redémarrer* avec un compte à rebours du temps estimé pour la fin du processus. Ensuite, vous serez déconnecté.




**Étape 6**

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

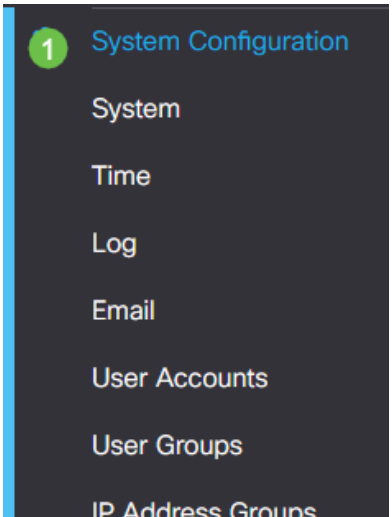



## Configuration des mises à jour automatiques sur le routeur de la gamme RV345P

Puisque les mises à jour sont si importantes et que vous êtes occupé, il est logique de configurer les mises à jour automatiques à partir d'ici !

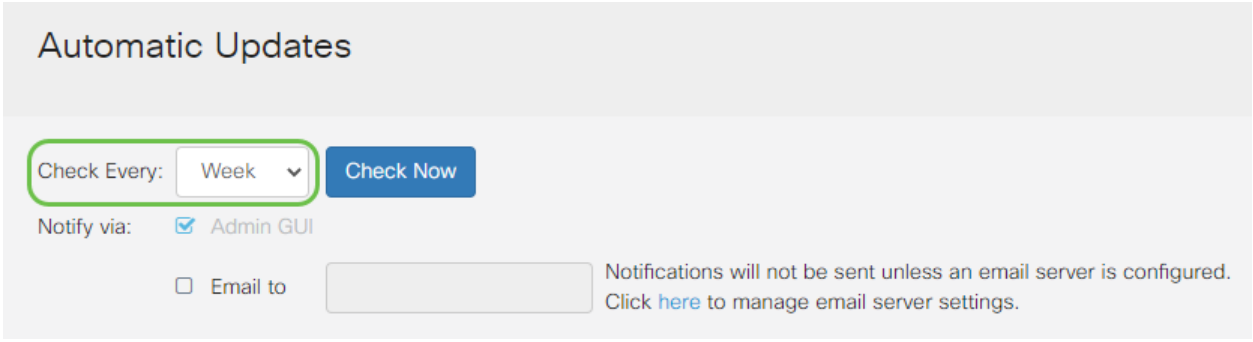
**Étape 1**

Connectez-vous à l'utilitaire Web et choisissez **Configuration système > Mises à jour automatiques**.



**Étape 2**

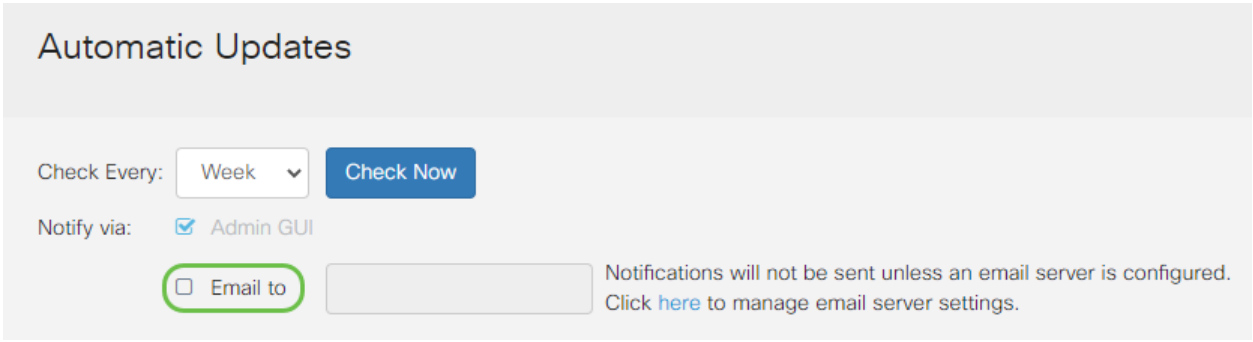
Dans la liste déroulante *Vérifier chaque*, choisissez la fréquence à laquelle le routeur doit rechercher les mises à jour.




**Étape 3**

Dans la zone *Notifier via*, cochez la case **Envoyer par e-mail** pour recevoir les mises à jour par e-mail. La case à cocher *Interface utilisateur graphique Admin* est activée par défaut et ne peut pas être désactivée. Une notification apparaît dans la configuration Web une fois qu'une mise à jour est disponible.

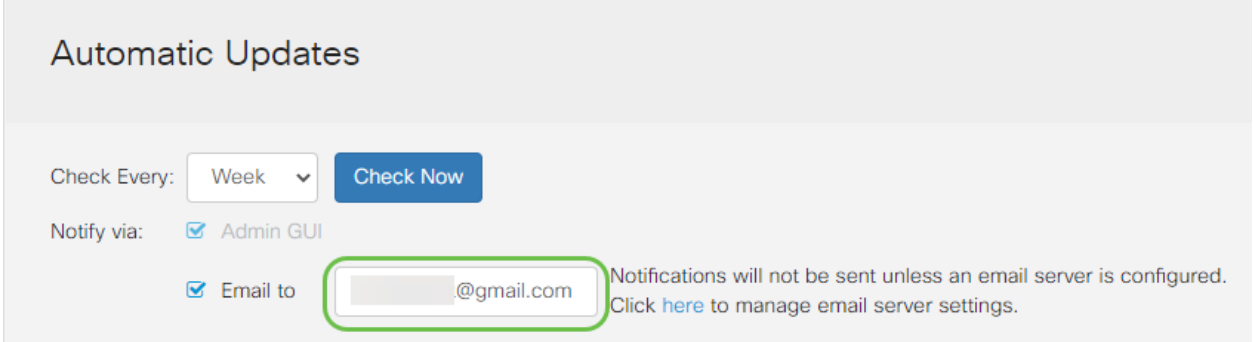
Si vous souhaitez configurer les paramètres du serveur de messagerie, cliquez ici pour savoir comment procéder.




**Étape 4**

Entrez une adresse e-mail dans le champ *E-mail à* adresse.

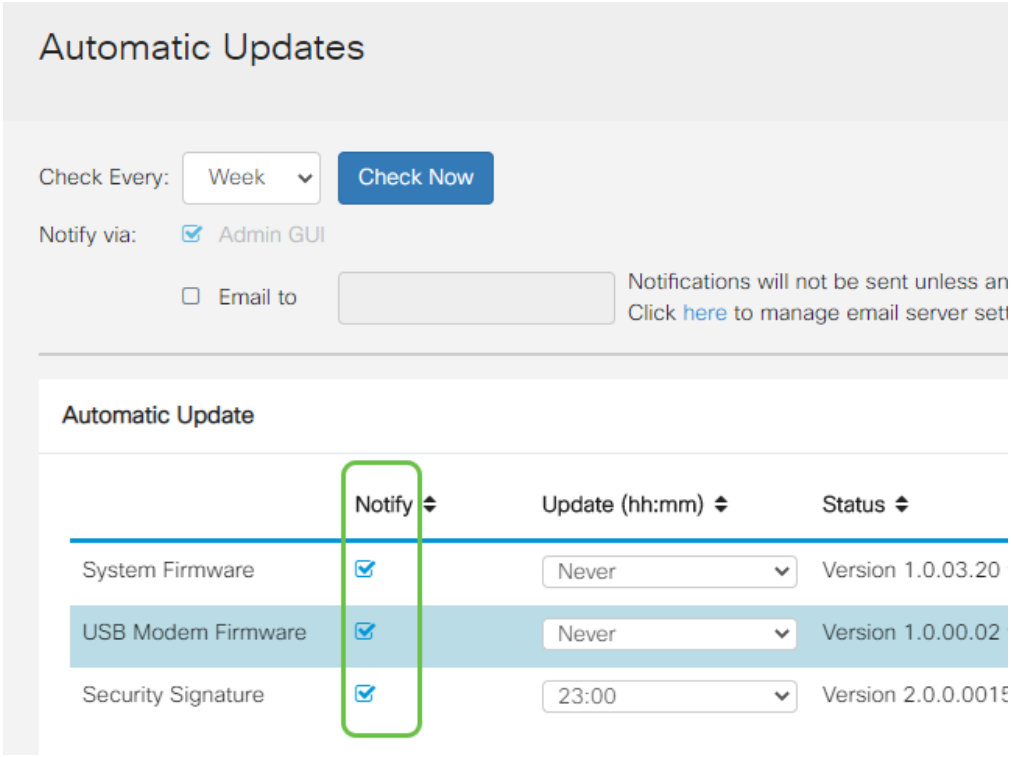
Il est fortement recommandé d'utiliser un compte de messagerie distinct au lieu d'utiliser votre courriel personnel pour préserver la confidentialité.




**Étape 5**

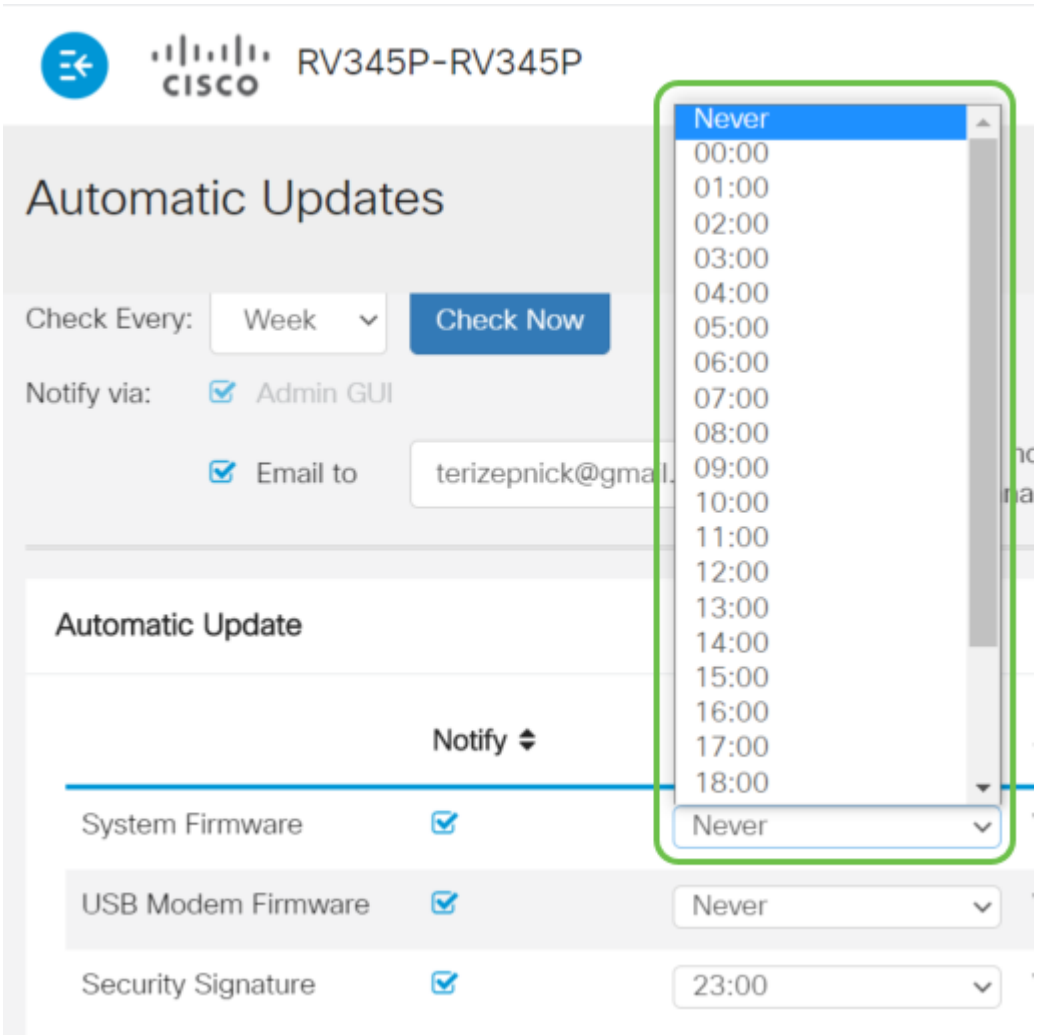
Sous la zone *Mise à jour automatique*, cochez les cases **Notifier** du type de mises à jour dont vous voulez être informé. Les options sont les suivantes :

- Microprogramme système : programme de contrôle principal du périphérique.
- Microprogramme du modem USB : programme ou pilote de contrôle du port USB.
- Signature de sécurité : contient des signatures pour le contrôle des applications afin d'identifier les applications, les types de périphériques, les systèmes d'exploitation, etc.




## Étape 6

Dans la liste déroulante *Mise à jour automatique*, sélectionnez l'heure de la journée à laquelle vous souhaitez effectuer la mise à jour automatique. Certaines options peuvent varier en fonction du type de mise à jour que vous avez choisi. La signature de sécurité est la seule option permettant d'avoir une mise à jour immédiate. Il est recommandé de définir une heure à laquelle votre bureau est fermé afin que le service ne soit pas interrompu à un moment qui vous dérange.




L'état affiche la version en cours d'exécution du micrologiciel ou de la signature de sécurité.

**Étape 7**

Cliquez sur Apply.


**Étape 8**

Pour enregistrer définitivement la configuration, accédez à la page Copier/Enregistrer la configuration ou cliquez sur l'**icône Enregistrer** dans la partie supérieure de la page.

Fantastique, vos paramètres de base sur votre routeur sont complets ! Vous avez maintenant quelques options de configuration à explorer.

## Options de sécurité

Bien sûr, vous voulez que votre réseau soit sûr. Il existe certaines options simples, telles que l'utilisation d'un mot de passe complexe, mais si vous voulez prendre des mesures pour un réseau encore plus sécurisé, consultez cette section sur la sécurité.

## Licence de sécurité RV (facultatif)

Cette licence de sécurité RV protège votre réseau des attaques provenant d'Internet :

- Système de prévention des intrusions (IPS) : Inspecte les paquets réseau, les journaux et/ou bloque une large gamme d'attaques réseau. Il offre une disponibilité accrue du réseau, une résolution plus rapide des problèmes et une protection complète contre les menaces.
- Antivirus : Protection contre les virus en analysant les applications pour divers protocoles tels que HTTP, FTP, pièces jointes de messagerie SMTP, pièces jointes de messagerie POP3 et pièces jointes de messagerie IMAP passant par le routeur.
- Sécurité Web : Permet l'efficacité et la sécurité de l'entreprise tout en se connectant à Internet, autorise les politiques d'accès à Internet pour les périphériques finaux et les applications Internet afin d'assurer performances et sécurité. Il est basé sur le cloud et contient plus de 80 catégories avec plus de 450 millions de domaines classés.
- Identification de l'application : Identifier et affecter des stratégies aux applications Internet. 500 applications uniques sont automatiquement identifiées.
- Identification du client : Identifier et catégoriser les clients de manière dynamique. Possibilité d'attribuer des stratégies en fonction de la catégorie de périphériques finaux et du système d'exploitation.

La licence de sécurité RV fournit le filtrage Web. Le filtrage Web est une fonction qui vous permet de gérer l'accès à des sites Web inappropriés. Il peut filtrer les demandes d'accès Web d'un client pour déterminer s'il doit autoriser ou refuser ce site Web.

Les fonctionnalités de sécurité sous licence peuvent être testées gratuitement pendant 90 jours. Si vous souhaitez continuer à utiliser les fonctions de sécurité avancées de votre routeur après la période d'évaluation, vous devez acquérir et activer une licence.

Cisco Umbrella est une autre option de sécurité. Cliquez ici si vous souhaitez accéder à la section Umbrella à la place.

Si vous ne voulez pas de licence de sécurité, cliquez sur pour accéder à la section VPN de ce document.

### Présentation des comptes Smart

Pour acheter la licence de sécurité RV, vous avez besoin d'un compte Smart.

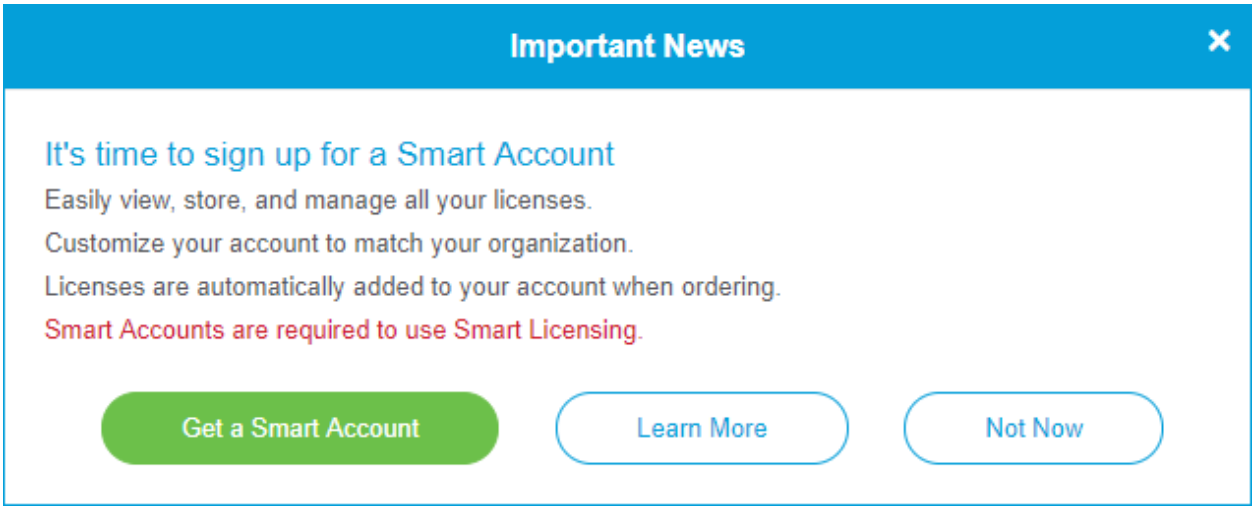
En autorisant l'activation de ce compte Smart, vous acceptez d'être autorisé à créer des comptes et à gérer les droits de produit et de service, les contrats de licence et l'accès utilisateur aux comptes pour le compte de votre organisation. Les partenaires

Cisco ne peuvent autoriser la création de comptes pour le compte de clients.

La création d'un nouveau compte Smart est un événement unique et la gestion à partir de ce moment-là est assurée par l'outil.

### Créer un compte Smart

Lorsque vous accédez à votre compte Cisco général à l'aide de votre compte Cisco.com ou de l'ID CCO (celui que vous avez créé au début de ce document), vous pouvez être accueilli par un message vous invitant à créer un compte Smart.




Si vous n'avez pas vu cette fenêtre contextuelle, vous pouvez cliquer pour accéder à la page de création de compte Smart. Vous devrez peut-être vous connecter avec vos informations d'identification de compte Cisco.com.

Pour plus de détails sur les étapes de demande de votre compte Smart, cliquez ici.

N'oubliez pas de prendre note du nom de votre compte ainsi que des autres détails d'inscription.

**Astuce rapide :** si vous devez entrer un domaine et que vous n'en avez pas, vous pouvez saisir votre adresse e-mail sous la forme de *name@domain.com*. Les domaines courants sont gmail, yahoo, etc. selon votre entreprise ou votre fournisseur.

Il est très important de disposer d'un compte Cisco.com (ID CCO) et d'un compte Cisco Smart avant d'acheter la licence de sécurité RV.

### Achat d'une licence de sécurité RV

Vous devez acheter une licence auprès de votre distributeur Cisco ou de votre partenaire Cisco. Pour trouver un partenaire Cisco, cliquez ici.

Le tableau ci-dessous affiche le numéro de référence de la licence.

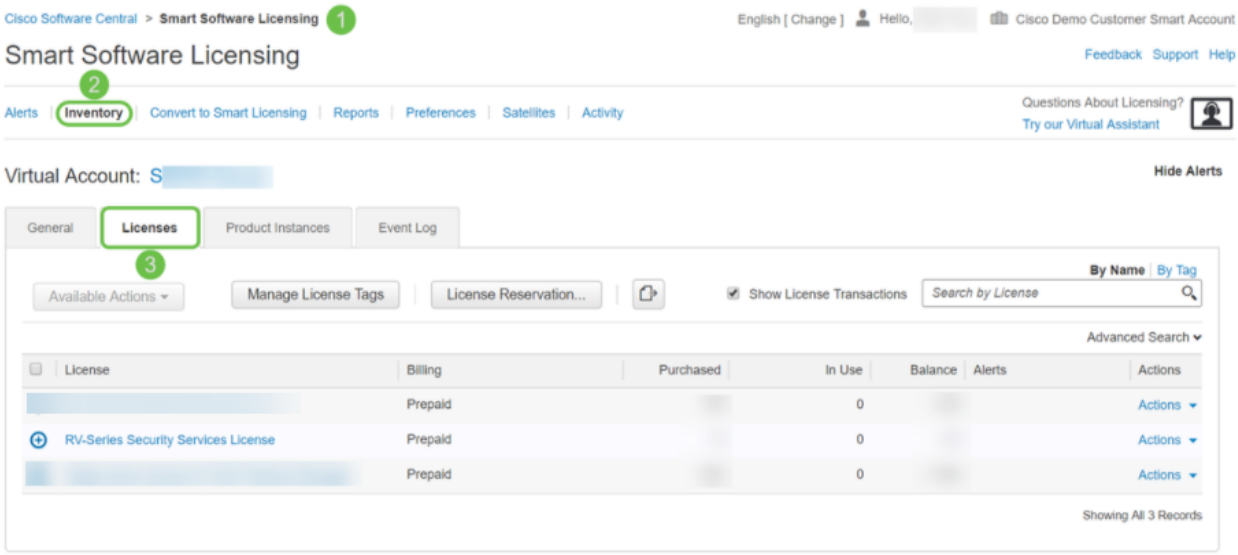
| Type | ID de produit | Description |
|---|---|---|

| | | |
|---|---|---|
| Licence de sécurité RV | LS-RV34X-SEC-1 an= | Sécurité RV : 1 an : Dynamic Web Filter, Application Visibility, Client Identification and Statistics, Gateway Antivirus et Intrusion Prevention System IPS. |

La clé de licence n'est pas entrée directement dans votre routeur, mais elle sera affectée à votre compte Cisco Smart après avoir commandé la licence. Le temps nécessaire pour que la licence s'affiche sur votre compte dépend du moment où le partenaire accepte la commande et du moment où le revendeur lie les licences à votre compte, qui est généralement de 24 à 48 heures.

### Confirmer que la licence est dans le compte Smart

Accédez à la page de votre compte Smart License, puis cliquez sur **Smart Software License page > Inventory > Licenses**.

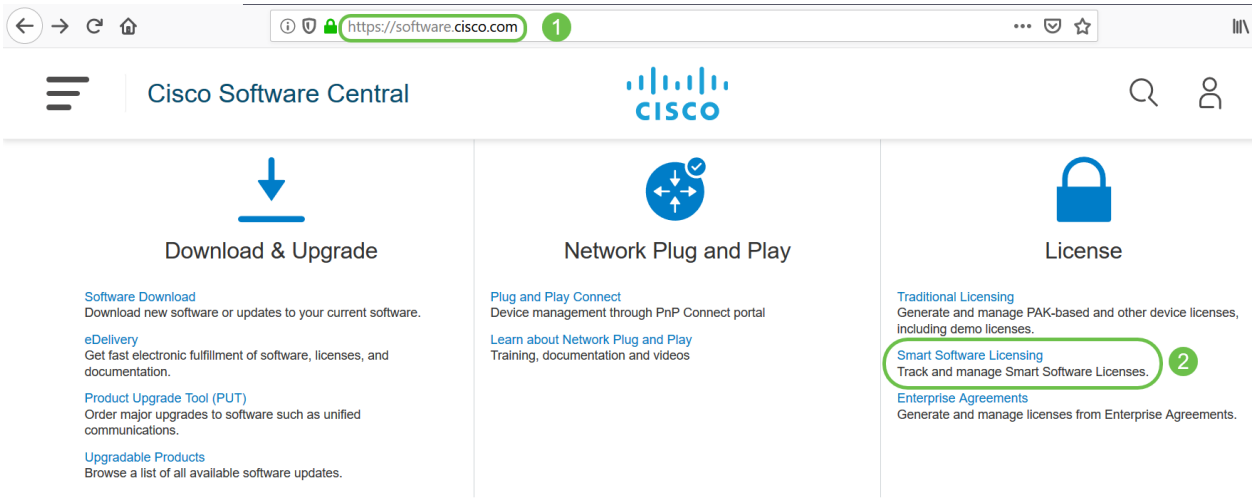



Si votre licence n'apparaît pas dans votre compte Smart, contactez votre partenaire Cisco.

### Configuration de la licence de sécurité RV sur le routeur de la gamme RV345P

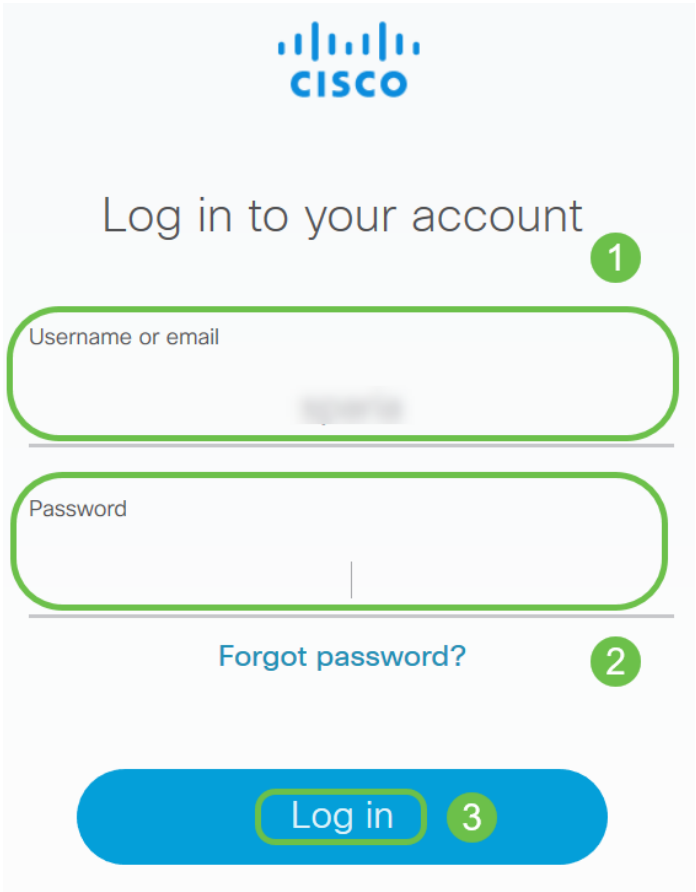
#### Étape 1

Accédez au logiciel Cisco et accédez à **Licence logicielle Smart**.



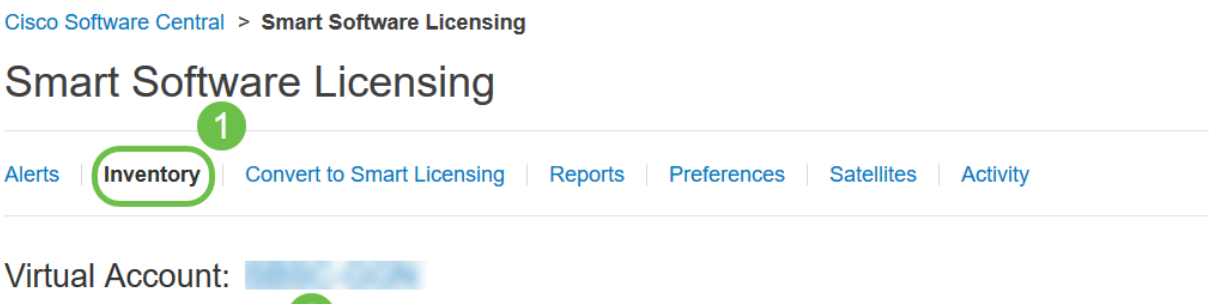

## Étape 2

Entrez votre *nom d'utilisateur ou votre adresse e-mail* et votre *mot de passe* pour vous connecter à votre compte Smart. Cliquez sur **Connexion**.



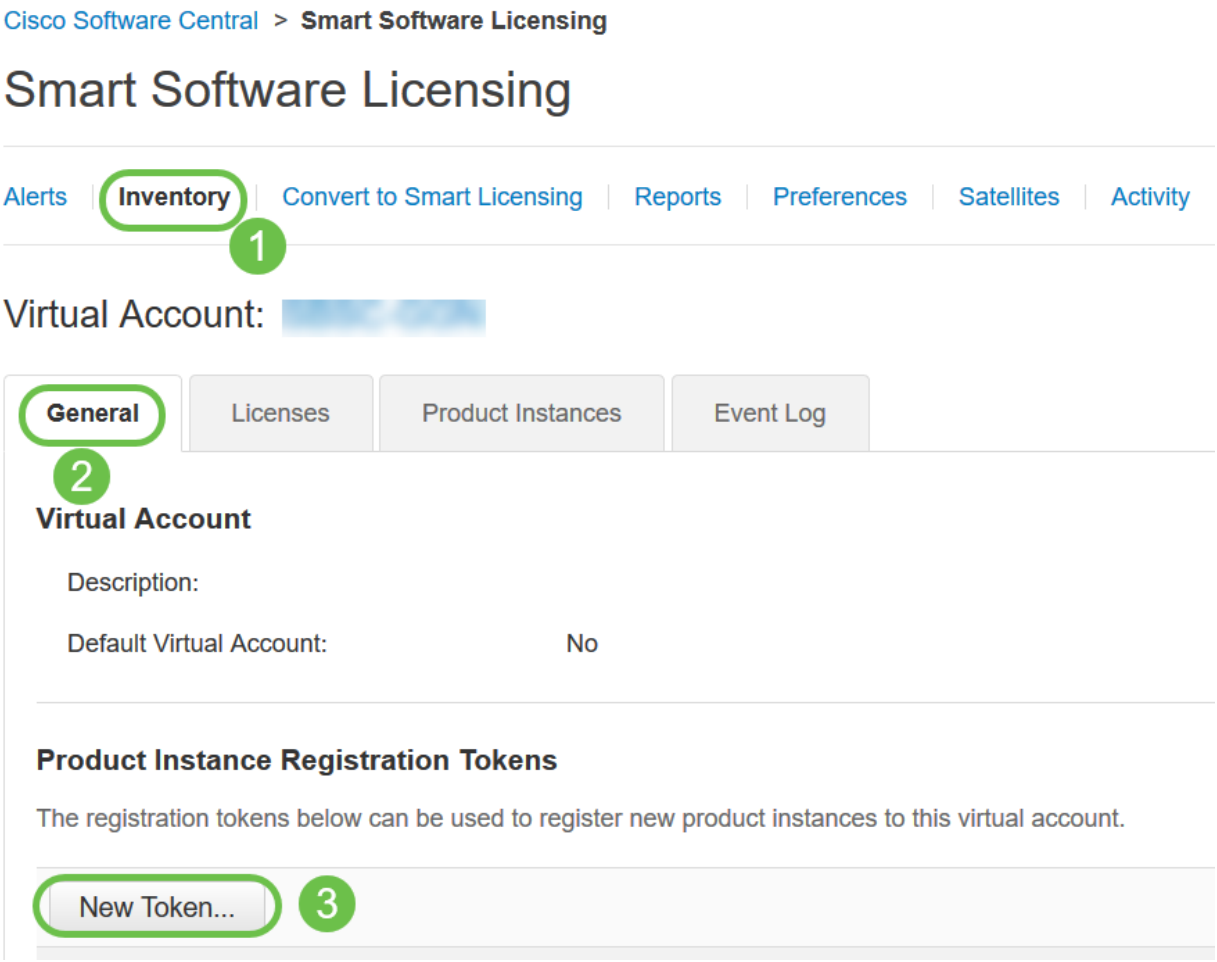

## Étape 3

Accédez à **Inventory > Licenses** et vérifiez que la *licence de services de sécurité série RV* figure sur votre compte Smart. Si la licence ne figure pas dans la liste, contactez votre partenaire Cisco.



## Étape 4

Accédez à **Stock > Général**. Sous *Product Instance Registration Tokens*, cliquez sur **New Token**.



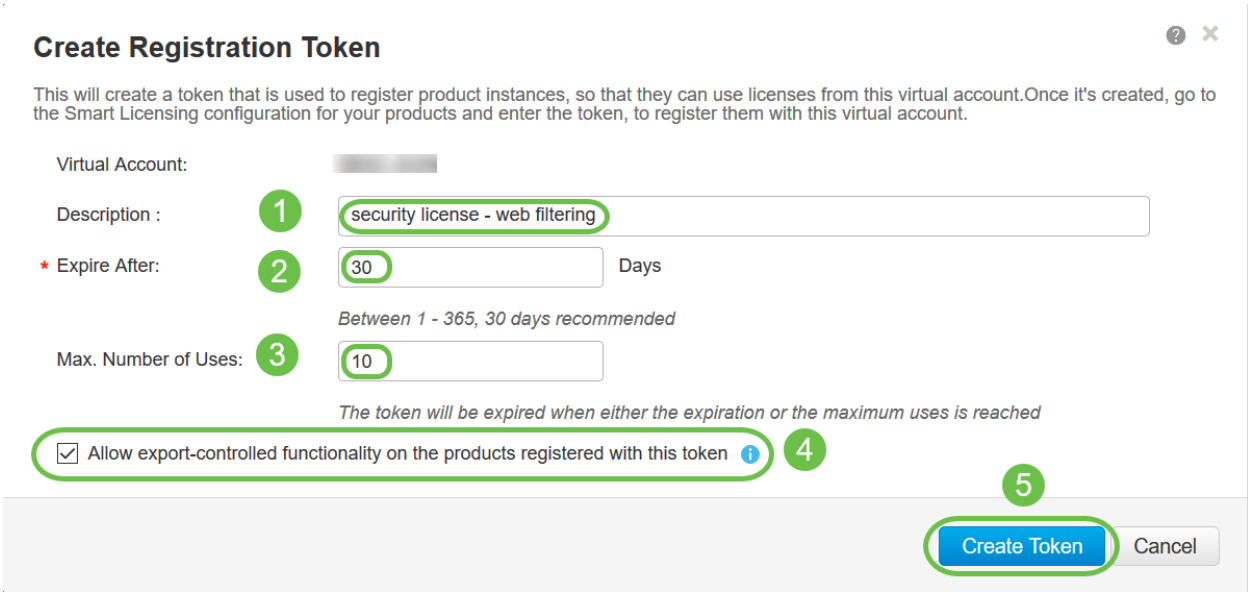

## Étape 5

Une fenêtre Create Registration Token s'affiche. La zone *Compte virtuel* affiche le compte virtuel sous lequel le jeton d'inscription sera créé. Sur la page *Créer un jeton d'enregistrement*, procédez comme suit :

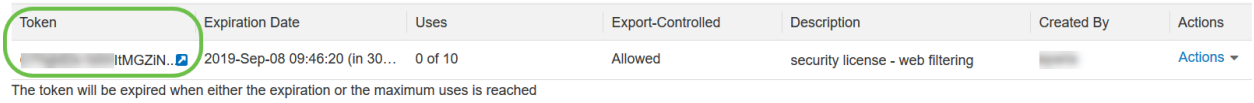
- Dans le champ Description, saisissez une description unique pour le jeton. Dans cet exemple, la licence de sécurité - filtrage Web est entrée.
- Dans le champ Expire après, saisissez une valeur comprise entre 1 et 365 jours. Cisco recommande une valeur de 30 jours pour ce champ ; toutefois, vous pouvez modifier la valeur en fonction de vos besoins.
- Dans Max. Champ Nombre d'utilisations : saisissez une valeur pour définir le nombre de fois que vous souhaitez utiliser ce jeton. Le jeton expirera lorsque le nombre de jours ou le nombre maximal d'utilisations est atteint.
- Cochez la case Autoriser les fonctionnalités contrôlées par exportation sur les produits enregistrés avec ce jeton pour activer la fonctionnalité contrôlée par exportation pour les jetons d'une instance de produit dans votre compte virtuel. Décochez la case si vous ne voulez pas autoriser l'utilisation de la fonctionnalité contrôlée par l'exportation avec ce jeton. Utilisez cette option uniquement si vous êtes conforme à la fonctionnalité

exportée. Certaines caractéristiques contrôlées par les exportations sont limitées par le Département du commerce des États-Unis. Ces fonctionnalités sont limitées aux produits enregistrés à l'aide de ce jeton lorsque vous décochez la case. Toute violation est passible de sanctions et de poursuites administratives.

- Cliquez sur **Créer un jeton** pour générer le jeton.

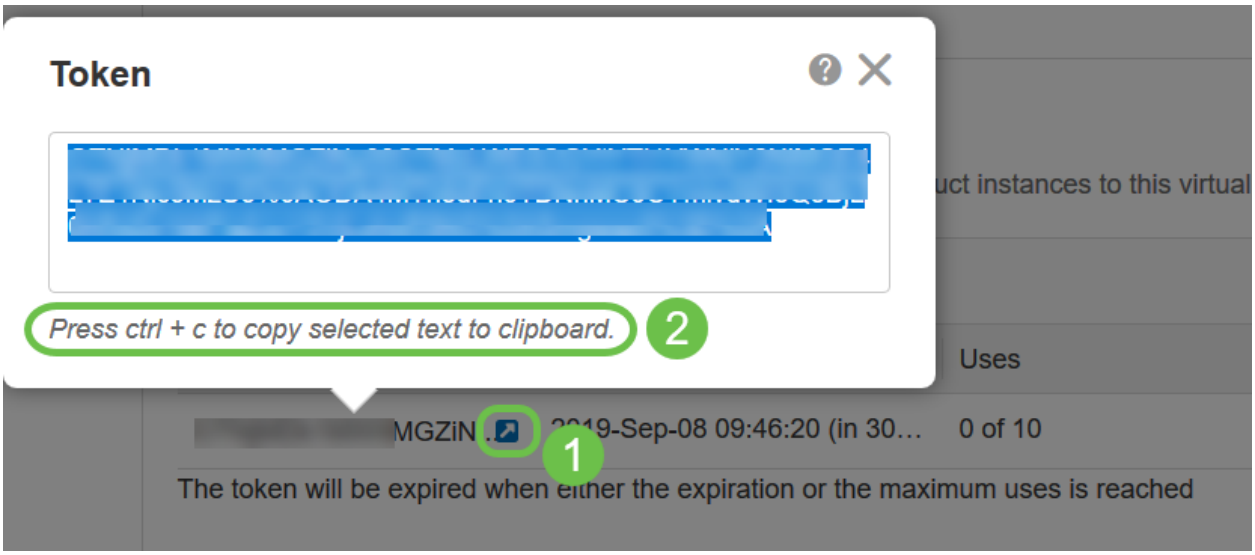



Vous avez maintenant généré un jeton d'enregistrement d'instance de produit.




## Étape 6

Cliquez sur l'**icône de flèche** dans la colonne *Jeton*, pour copier le jeton dans le presse-papiers, appuyez **sur ctrl + c** sur votre clavier.

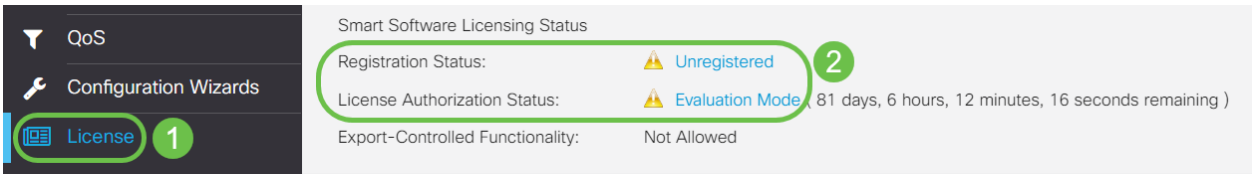



## Étape 7 (facultative)

Cliquez sur le menu déroulant **Actions**, choisissez **Copier** pour copier le jeton dans le presse-papiers ou **Télécharger...** pour télécharger une copie de fichier texte du jeton à partir duquel vous pouvez copier.

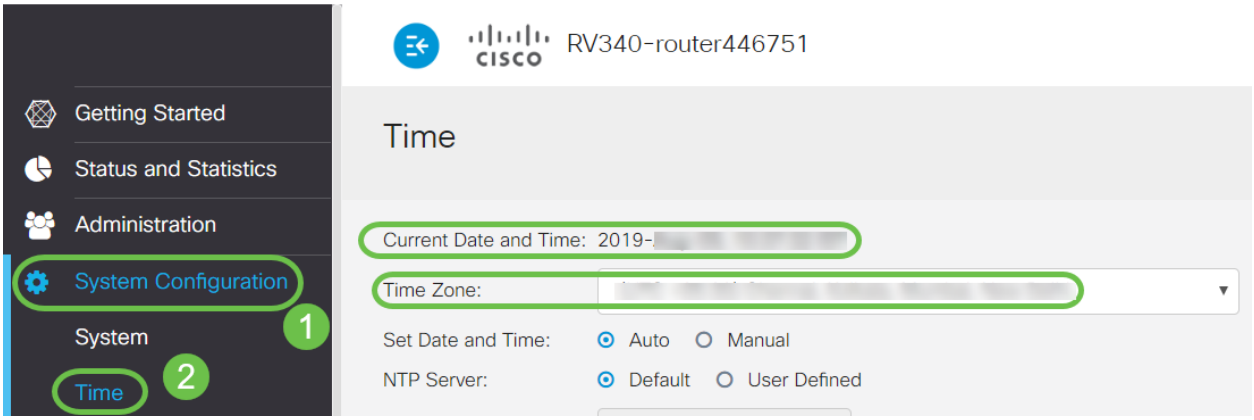

## Étape 8

Accédez à License et vérifiez que le *statut d'enregistrement* s'affiche comme *Unregistered* et que le *statut d'autorisation de licence* s'affiche comme *mode d'évaluation*.



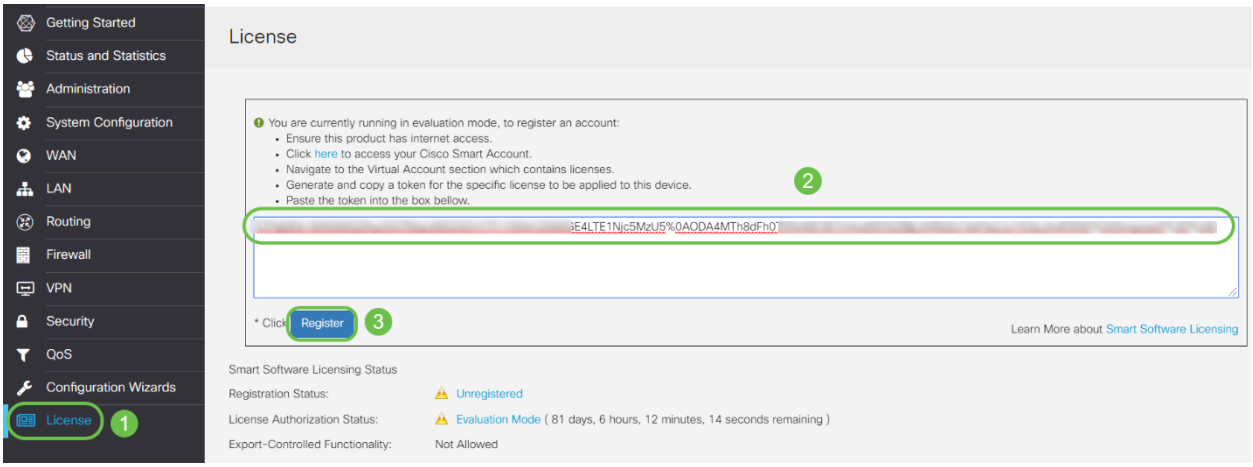

## Étape 9

Accédez à **Configuration système > Heure** et vérifiez que la *date et l'heure actuelles* et le *fuseau horaire* reflètent correctement selon votre fuseau horaire.




## Étape 10

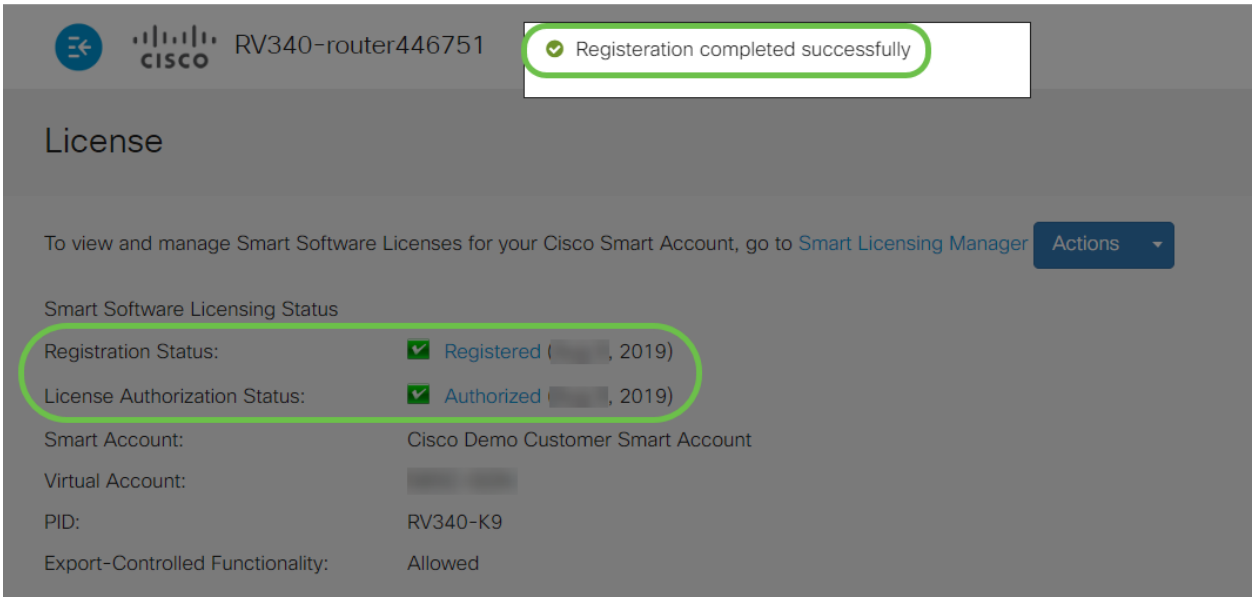
Accédez à **Licence**. Collez le jeton copié à l'étape 6 dans la zone de texte sous l'onglet *Licence* en sélectionnant **ctrl + v** sur votre clavier. Cliquez sur **Register**.




L'inscription peut prendre quelques minutes. Ne quittez pas la page lorsque le routeur tente de contacter le serveur de licences.

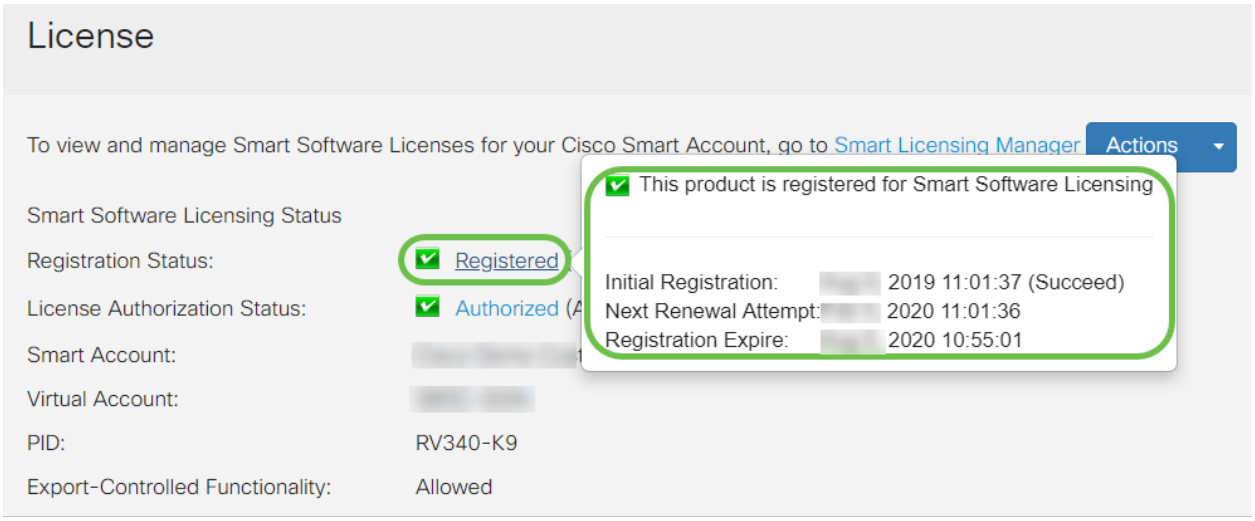
## Étape 11

Vous devez maintenant avoir enregistré et autorisé votre routeur de la gamme RV345P avec une licence Smart. Vous recevrez une notification à l'écran *Enregistrement terminé*. De plus, vous verrez que le *statut* d'*enregistrement* s'affiche comme *enregistré* et *statut d'autorisation de licence* s'affiche comme *autorisé*.




## Étape 12 (facultative)

Pour afficher plus de détails sur le *statut d'enregistrement* de la licence, placez votre pointeur sur le statut *enregistré*. Un message de dialogue s'affiche avec les informations suivantes :

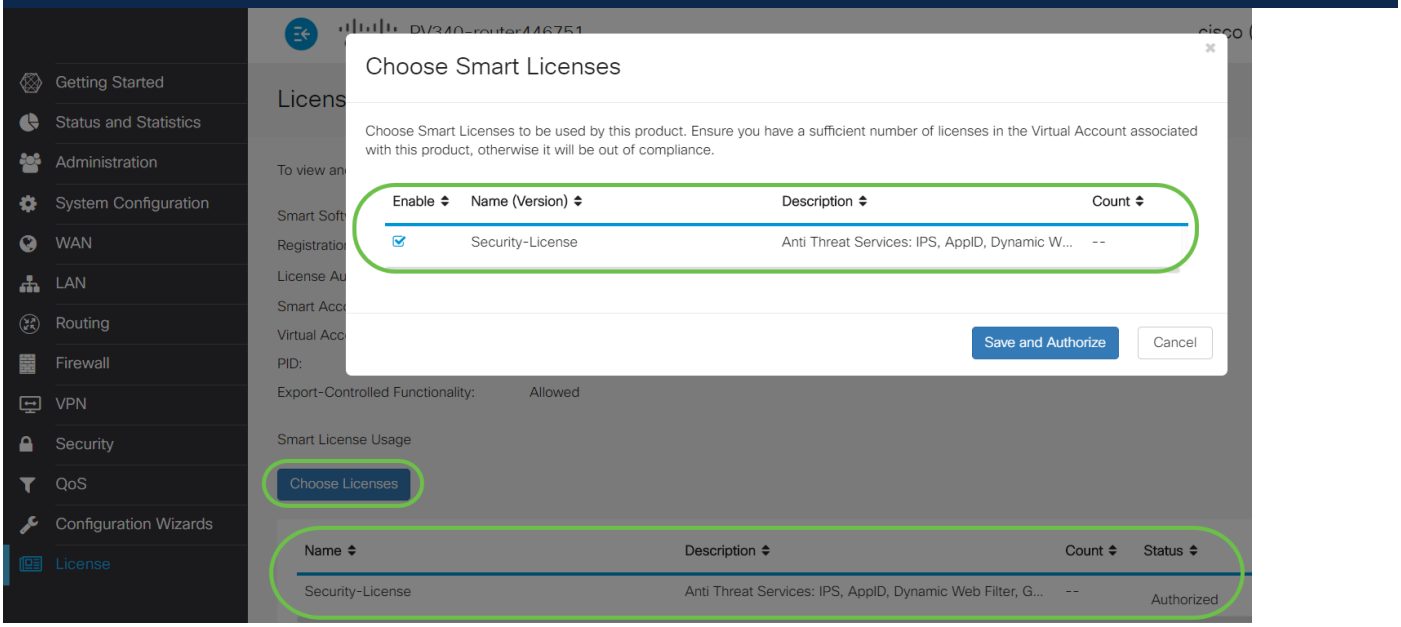



- Enregistrement initial — Cette zone indique la date et l'heure d'enregistrement de la licence.
- Prochaine tentative de renouvellement : cette zone indique la date et l'heure auxquelles le routeur tentera de renouveler la licence.
- Registration Expire : cette zone indique la date et l'heure d'expiration de l'enregistrement.

## Étape 13

Sur la page *Licence*, vérifiez que le statut *Security-License* affiche *Authorized*. Vous pouvez également cliquer sur le bouton **Choisir une licence** pour vérifier que *Security-License* est activée.

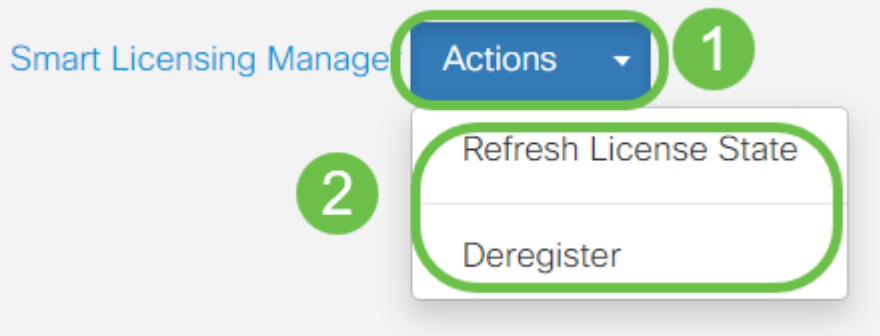
Si vous rencontrez des problèmes à cette étape, vous devrez peut-être redémarrer votre routeur.




## Étape 14 (facultative)

Pour *actualiser l'état de la licence* ou *annuler* l'enregistrement de la licence à partir du routeur, cliquez sur le menu déroulant *Smart Licensing Manager* **Actions** et

sélectionnez un élément d'action.



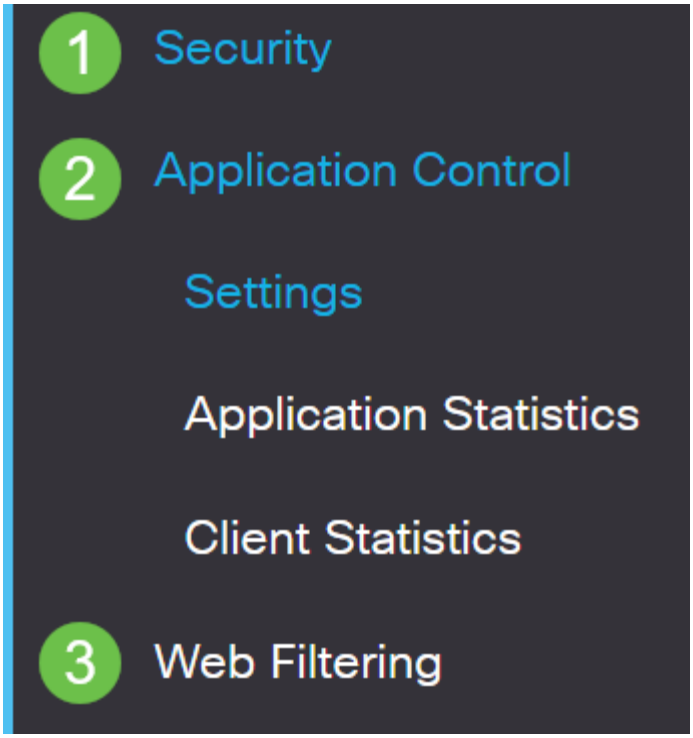

Maintenant que vous disposez de votre licence sur le routeur, vous devez effectuer les étapes de la section suivante.

## Filtrage Web sur le routeur RV345P

Vous disposez de 90 jours après l'activation pour utiliser le filtrage Web gratuitement. Après l'essai gratuit, si vous voulez continuer à utiliser cette fonctionnalité, vous devez acheter une licence. Cliquez pour revenir à cette section.

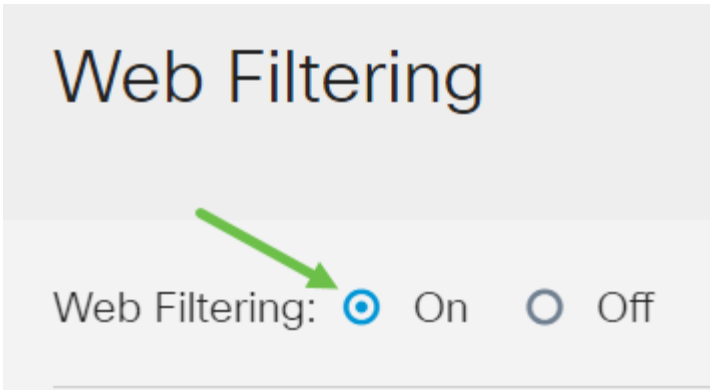
### Étape 1

Connectez-vous à l'utilitaire Web et choisissez **Security > Application Control > Web Filtering**.



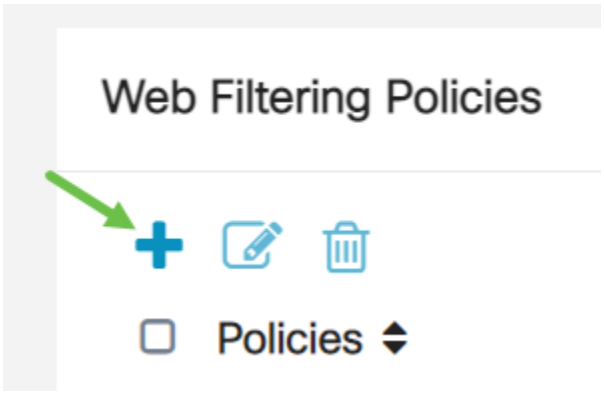

### Étape 2

Sélectionnez la case d'option **On**.



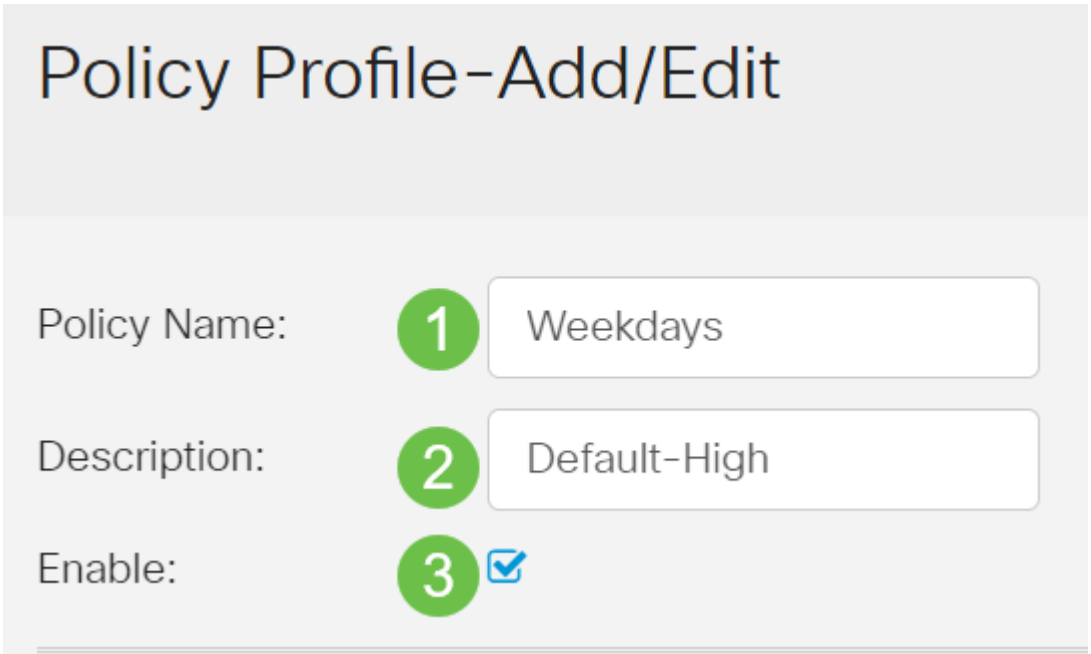

**Étape 3**

Cliquez sur l'**icône Ajouter**.




**Étape 4**

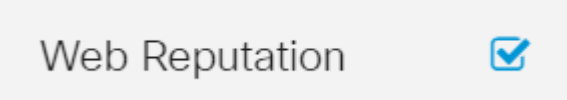
Entrez un *nom de stratégie*, une *description* et la case à cocher *Activer*.




Si le filtrage de contenu est activé sur votre routeur, une notification apparaît pour vous informer que le filtrage de contenu a été désactivé et que les deux fonctionnalités ne peuvent pas être activées simultanément. Cliquez sur **Apply** pour poursuivre la configuration.

### Étape 5

Cochez la case Web Reputation pour activer le filtrage basé sur un index de réputation Web.

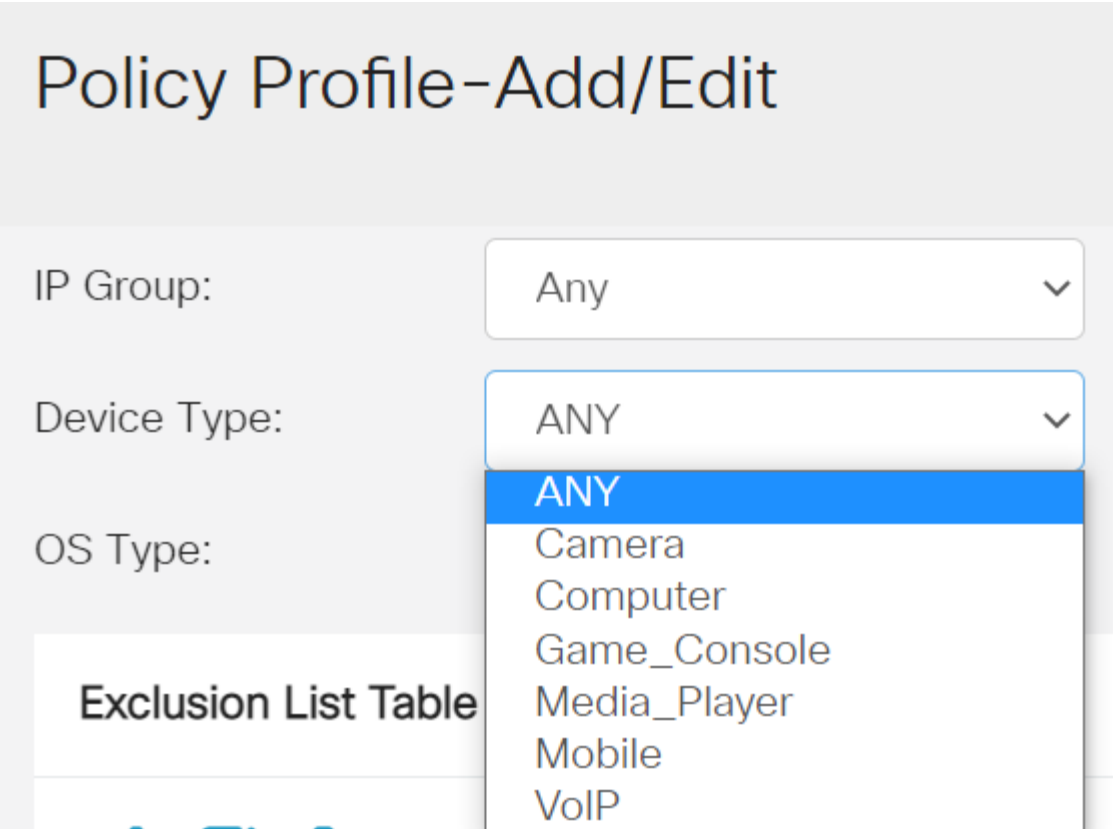



Le contenu sera filtré en fonction de la notoriété d'un site Web ou d'une URL basée sur un index de réputation Web. Si le score est inférieur à 40, le site sera bloqué. Pour en savoir plus sur la technologie de réputation Web, cliquez ici pour plus de détails.

### Étape 6

Dans la liste déroulante *Type de périphérique*, sélectionnez la source/destination des paquets à filtrer. Une seule option peut être choisie à la fois. Les options sont les suivantes :

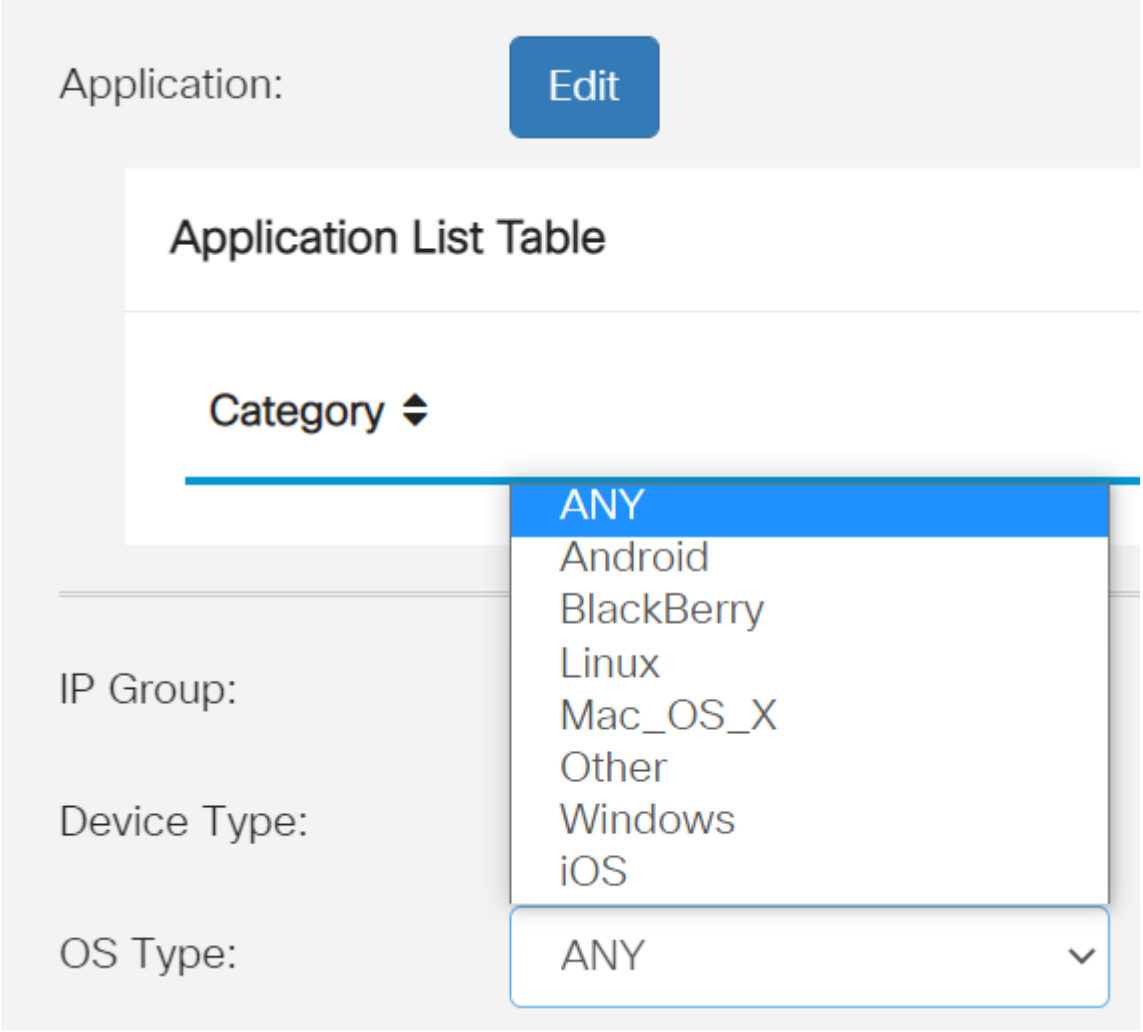
- ANY : sélectionnez cette option pour appliquer la stratégie à n'importe quel périphérique.
- Camera : sélectionnez cette option pour appliquer la stratégie aux caméras (telles que les caméras de sécurité IP).
- Ordinateur : sélectionnez cette option pour appliquer la stratégie aux ordinateurs.
- Game_Console : sélectionnez cette option pour appliquer la stratégie aux consoles de jeux.
- Media_Player : sélectionnez cette option pour appliquer la stratégie aux lecteurs multimédia.
- Mobile : sélectionnez cette option pour appliquer la stratégie aux périphériques mobiles.
- VoIP : sélectionnez cette option pour appliquer la stratégie aux périphériques Voice over Internet Protocol.



**Étape 7**

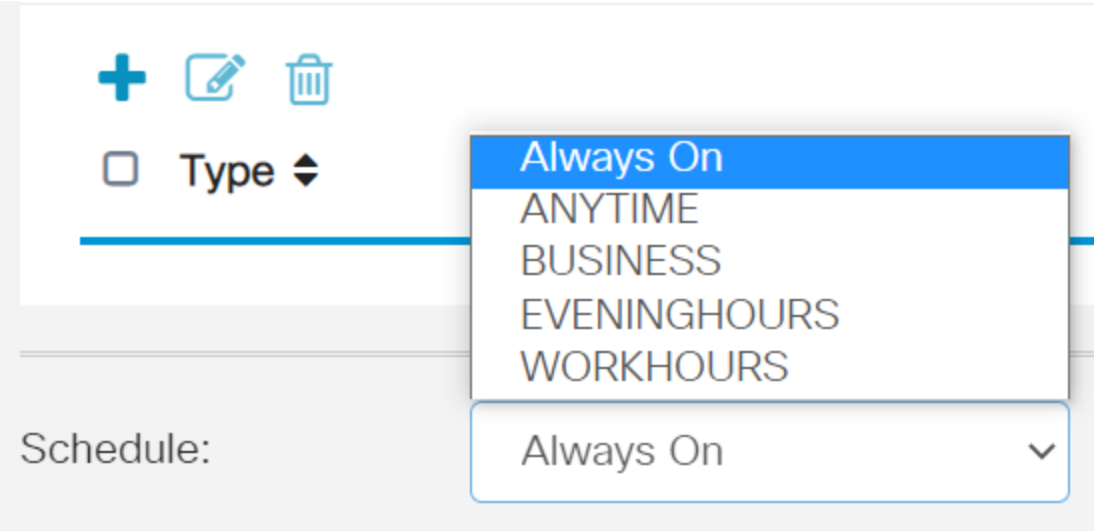
Dans la liste déroulante *Type de système d'exploitation*, sélectionnez un système d'exploitation auquel la stratégie doit s'appliquer. Une seule option peut être choisie à la fois. Les options sont les suivantes :

- ANY : applique la stratégie à n'importe quel type de système d'exploitation. Il s'agit de la configuration par défaut.
- Android : applique la stratégie à Android OS uniquement.
- BlackBerry — Applique la stratégie à Blackberry OS uniquement.
- Linux : applique la stratégie au système d'exploitation Linux uniquement.
- Mac_OS_X — Applique la stratégie à Mac OS uniquement.
- Autre : applique la stratégie à un système d'exploitation qui ne figure pas dans la liste.
- Windows : applique la stratégie au système d'exploitation Windows.
- iOS : applique la stratégie à iOS uniquement.



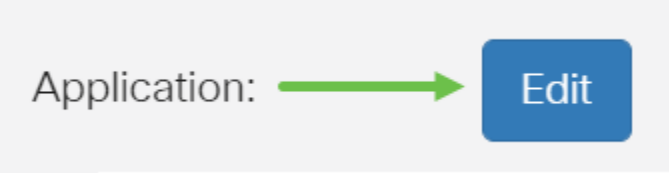

**Étape 8**

Faites défiler jusqu'à la section *Programmer* et sélectionnez l'option qui correspond le mieux à vos besoins.




**Étape 9**

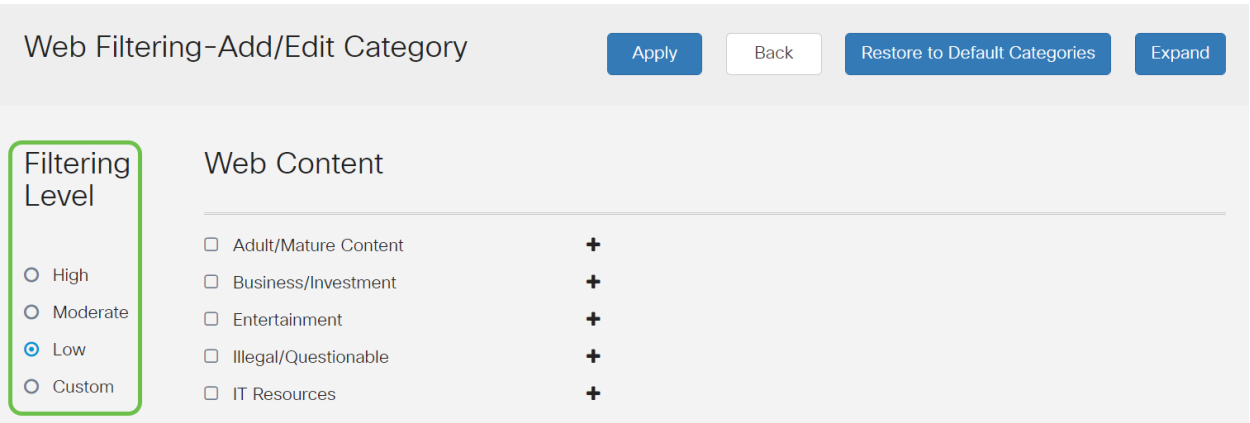
Cliquez sur l'**icône de modification**.




**Étape 10**

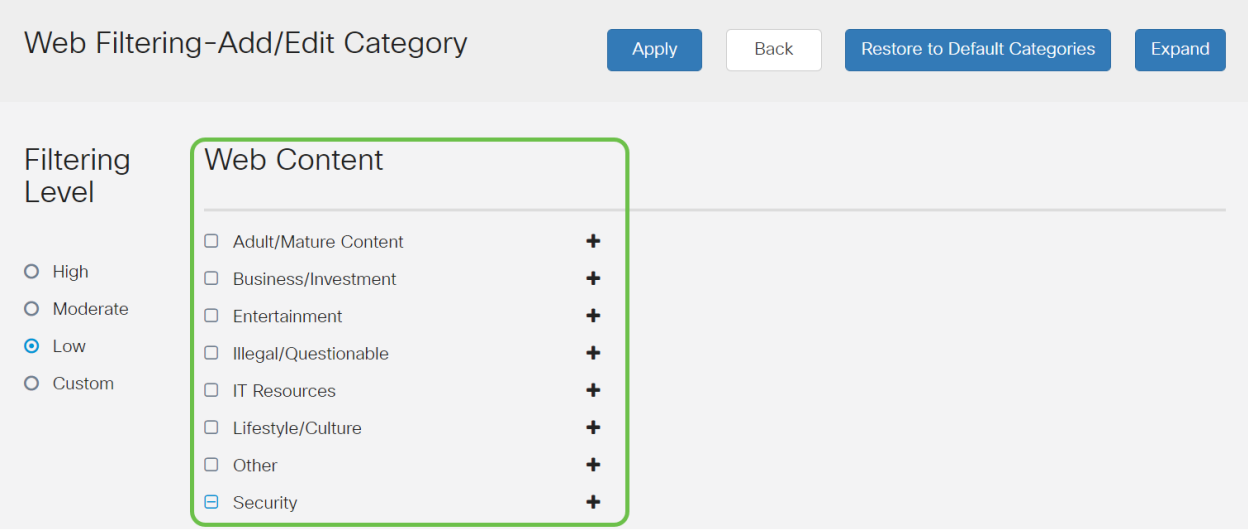
Dans la colonne Niveau de filtrage, cliquez sur une case d'option pour définir rapidement l'étendue de filtrage la mieux adaptée aux stratégies réseau. Les options disponibles sont High (Élevée), Modéré (Modérée), Low (Faible) et Custom (Personnalisé). Cliquez sur l'un des niveaux de filtrage ci-dessous pour connaître les sous-catégories prédéfinies spécifiques filtrées dans chacune de leurs catégories de contenu Web activées. Les filtres prédéfinis ne peuvent plus être modifiés et sont grisés.

- Faible : option par défaut. La sécurité est activée avec cette option.
- Modéré - Le contenu adulte/mature, Illégal/douteux et Sécurité sont activés avec cette option.
- Élevé : les contenus adultes/matures, les investissements, les ressources informatiques et la sécurité sont activés avec cette option.
- Personnalisé : aucune valeur par défaut n'est définie pour autoriser les filtres définis par l'utilisateur.



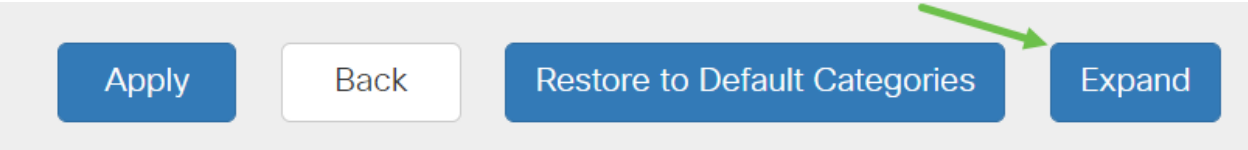
## Étape 11

Saisissez le contenu Web à filtrer. Cliquez sur l'**icône plus** si vous voulez plus de détails sur une section.



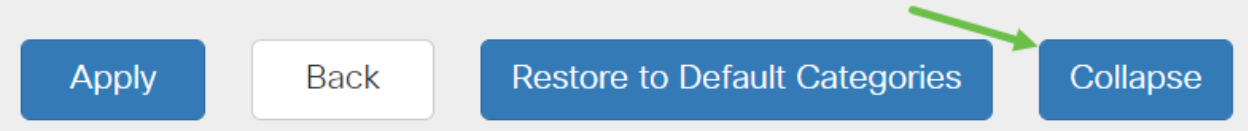

## Étape 12 (facultative)

Pour afficher toutes les sous-catégories et descriptions de contenu Web, cliquez sur le bouton **Développer**.



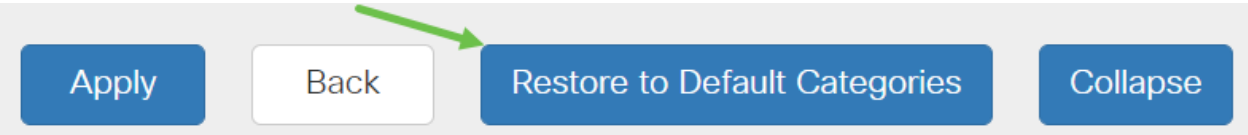

## Étape 13 (facultative)

Cliquez sur **Réduire** pour réduire les sous-catégories et les descriptions.




## Étape 14 (facultative)

Pour revenir aux catégories par défaut, cliquez sur **Restaurer les catégories par défaut**.



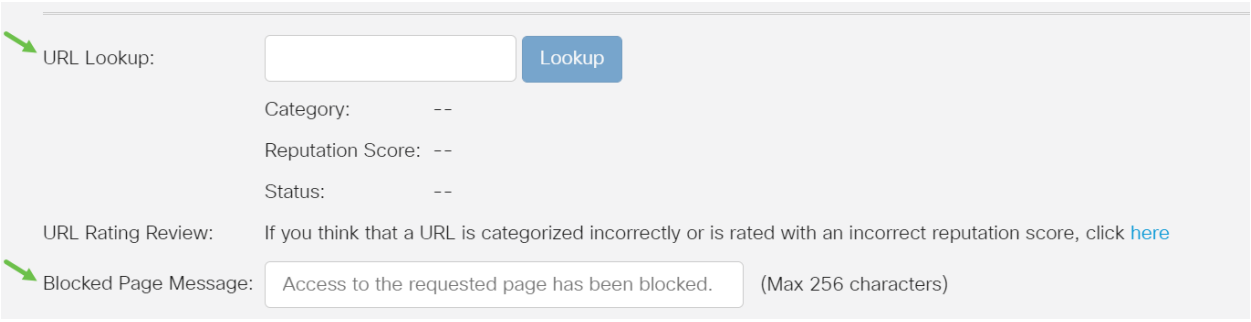

## Étape 15

Cliquez sur **Apply** pour enregistrer la configuration et revenir à la page Filter pour poursuivre la configuration.


Dans la table Liste des applications, les sous-catégories correspondantes basées sur le niveau de filtrage choisi renseigneront le tableau.

### Étape 16 (facultative)

D'autres options incluent la recherche d'URL et le message qui indique quand une page demandée a été bloquée.




### Étape 17 (facultative)

Cliquez sur Apply.

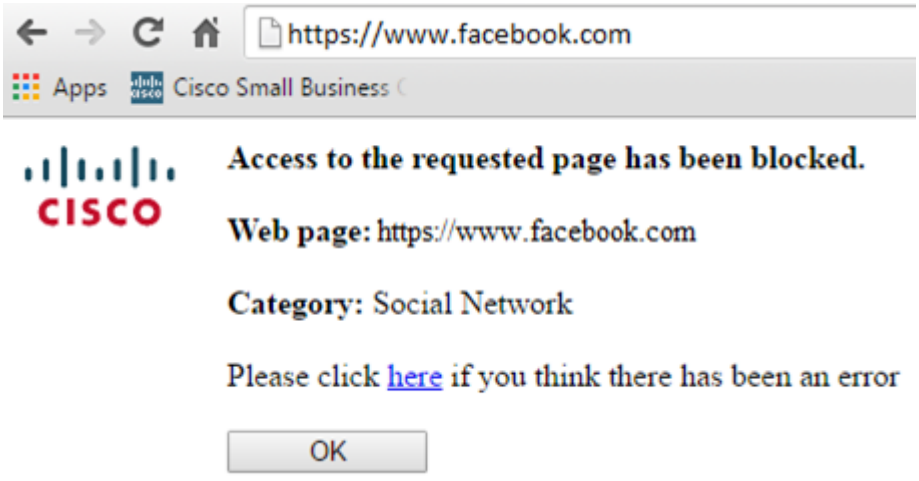

### Étape 18

Pour enregistrer définitivement la configuration, accédez à la page *Copier/Enregistrer la configuration* ou cliquez sur l'**icône Enregistrer** dans la partie supérieure de la page.

### Étape 19 (facultative)

Pour vérifier qu'un site Web ou une URL a été filtré ou bloqué, lancez un navigateur Web ou ouvrez un nouvel onglet dans votre navigateur. Entrez le nom de domaine que vous avez bloqué ou filtré pour être bloqué ou refusé.

Dans cet exemple, nous avons utilisé www.facebook.com.




Vous devez maintenant avoir correctement configuré le filtrage Web sur votre routeur RV345P. Puisque vous utilisez la licence de sécurité RV pour le filtrage Web, vous n'avez probablement pas besoin d'Umbrella. Si vous voulez aussi Umbrella, cliquez ici

. Si vous disposez d'une sécurité suffisante, cliquez pour passer à la section suivante.

### Dépannage

Si vous avez acheté une licence mais qu'elle n'apparaît pas dans votre compte virtuel, vous avez deux options :

1. Effectuez un suivi auprès du revendeur pour lui demander d'effectuer le transfert.
2. Contactez-nous et nous contacterons le revendeur.

Idéalement, vous n'auriez pas à faire non plus, mais si vous arrivez à ce carrefour, nous sommes heureux de vous aider ! Pour que le processus soit le plus rapide possible, vous aurez besoin des informations d'identification figurant dans le tableau ci-dessus ainsi que de celles qui sont présentées ci-dessous.

| Informations requises | Localisation des informations |
|---|---|
| Facture de licence | Vous devez envoyer ce message par courriel après avoir complété l'achat des licences. |
| Numéro de commande Cisco | Vous devrez peut-être revenir au revendeur pour obtenir ce résultat. |
| Capture d'écran de la page de licence de votre compte Smart | La prise d'une capture d'écran capture le contenu de votre écran à partager avec notre équipe. Si vous ne connaissez pas les captures d'écran, vous pouvez utiliser les méthodes ci-dessous. |

### Captures d'écran

Une fois que vous disposez d'un jeton ou que vous effectuez un dépannage, il est recommandé de prendre une capture d'écran pour capturer le contenu de votre écran.

Étant donné les différences de procédure requises pour capturer une capture d'écran, reportez-vous à la section ci-dessous pour connaître les liens spécifiques à votre système d'exploitation.

- Fenêtres
- MAC
- iPhone/iPad
- Android

## Licence de filiale RV Umbrella (facultatif)

Umbrella est une plate-forme de sécurité cloud simple mais très efficace de Cisco.

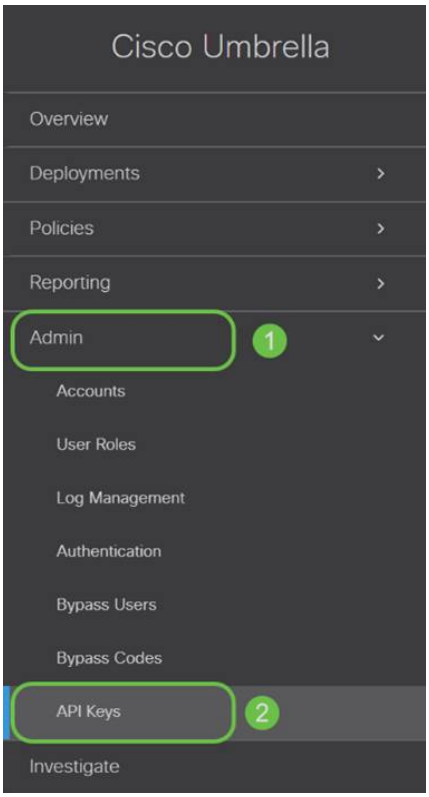
Umbrella fonctionne dans le cloud et fournit de nombreux services liés à la sécurité. De la menace émergente à l'enquête post-événement. Umbrella détecte et empêche les attaques sur tous les ports et protocoles.

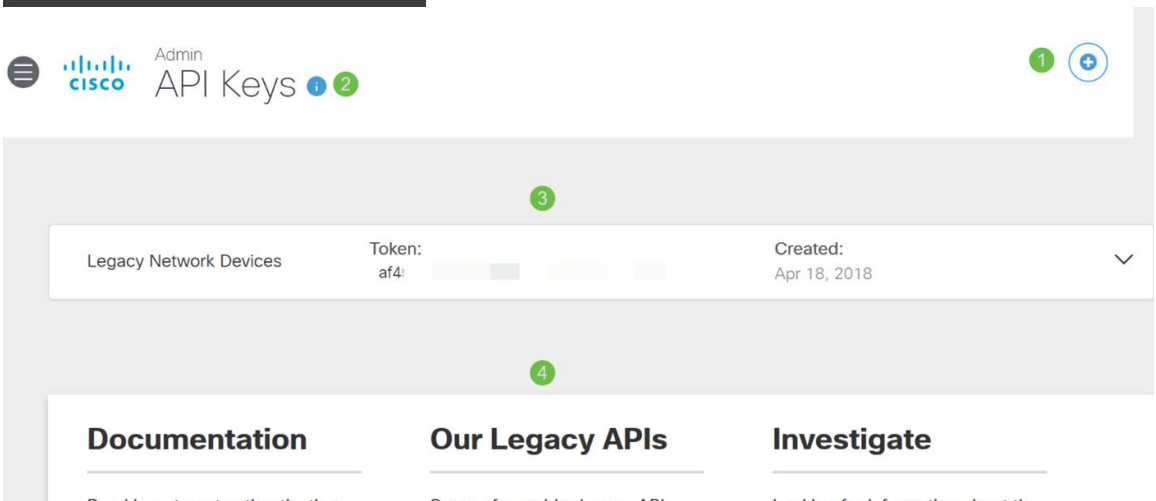
Umbrella utilise DNS comme principal vecteur de défense. Lorsque les utilisateurs entrent une URL dans leur barre de navigation et cliquent sur *Entrée*, Umbrella participe au transfert. Cette URL est transmise au résolveur DNS d'Umbrella et si un avertissement de sécurité est associé au domaine, la demande est bloquée. Cette télémétrie transfère les données et est analysée en microsecondes, ajoutant presque aucune latence. Les données de télémétrie utilisent des journaux et des instruments de suivi de milliards de requêtes DNS dans le monde entier. Lorsque ces données sont omniprésentes, les corréler à travers le monde permet une réponse rapide aux attaques dès leur début. Consultez la politique de confidentialité de Cisco ici pour plus d'informations : politique complète, version récapitulative. Considérez les données de télémétrie comme des données provenant d'outils et de journaux.

Visitez Cisco Umbrella pour en savoir plus et créer un compte. Si vous rencontrez des problèmes, consultez ici pour obtenir de la documentation, et ici pour les options de support Umbrella.

## Étape 1

Après vous être connecté à votre compte Umbrella, dans l'écran *Tableau de bord*, cliquez sur **Admin > Clés API**.



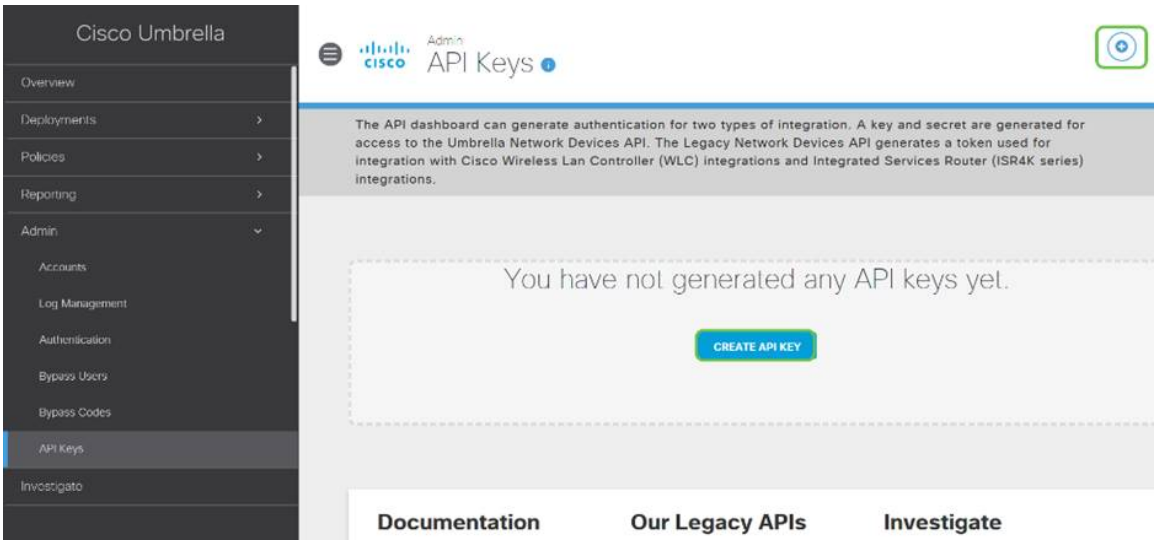



### Anatomie de l'écran API Keys (avec une clé API préexistante)

1. Add API Key : initie la création d'une nouvelle clé à utiliser avec l'API Umbrella.
2. Informations supplémentaires : glissez vers le bas ou vers le haut avec un explorateur pour cet écran.
3. Puits de jeton : contient toutes les clés et tous les jetons créés par ce compte. (Remplit une fois qu'une clé a été créée)
4. Documents de soutien - Liens vers la documentation du site Umbrella relative aux sujets de chaque section.

## Étape 2

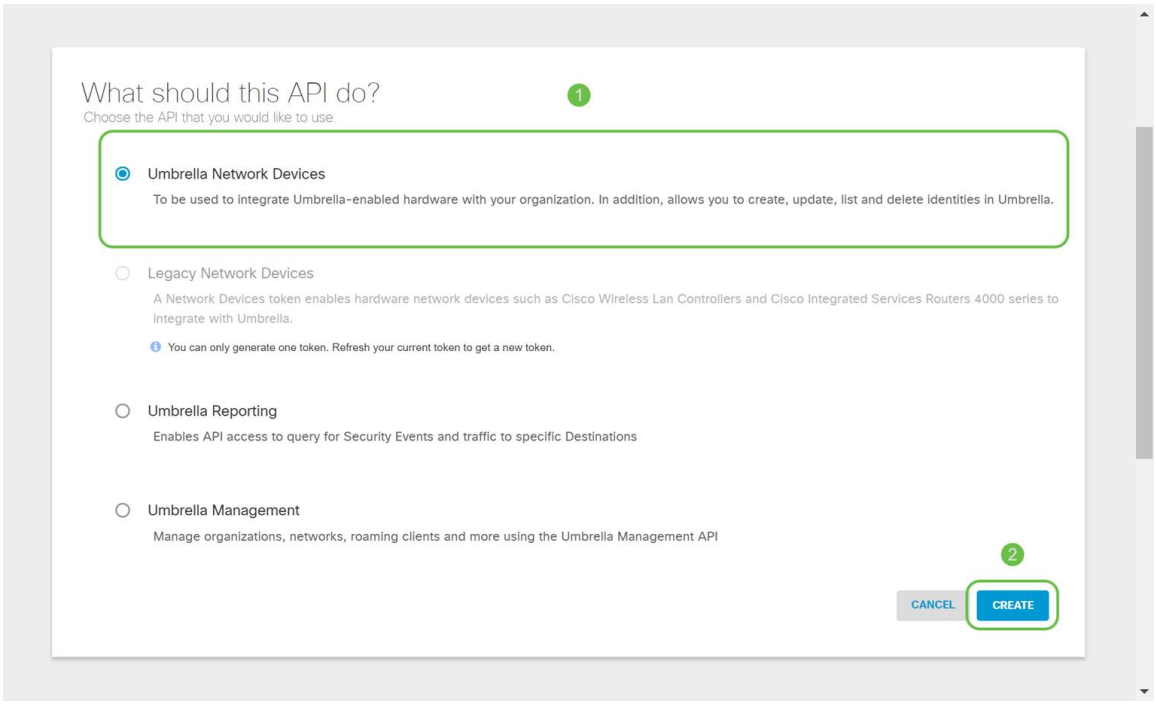
Cliquez sur le bouton **Ajouter une clé API** dans l'angle supérieur droit ou cliquez sur le bouton **Créer une clé API**. Tous deux fonctionnent de la même manière.




La capture d'écran ci-dessus serait similaire à celle que vous verriez ouvrir ce menu pour la première fois.

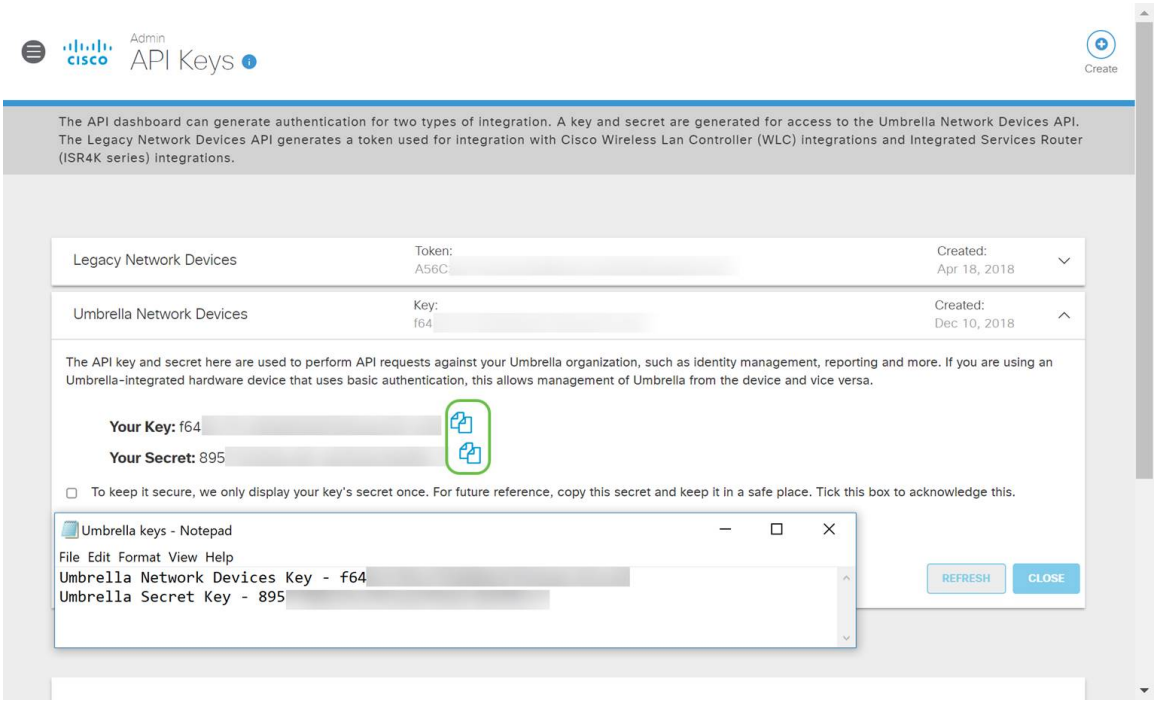
## Étape 3

Sélectionnez **Périphériques réseau** Umbrella, puis cliquez sur le bouton **Créer**.



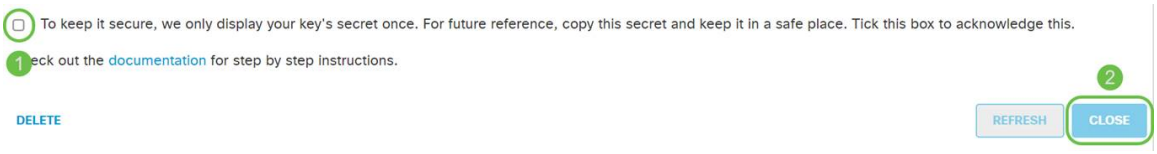

## Étape 4

Ouvrez un éditeur de texte tel que Bloc-notes, puis cliquez sur l'**icône de copie** à droite de votre API et *Clé secrète* API, une notification contextuelle confirmera que la clé est copiée dans votre presse-papiers. Un par un, collez votre clé secrète et API dans le document, en les étiquetant pour référence future. Dans ce cas, son étiquette est " Umbrella network devices key ". Ensuite, enregistrez le fichier texte dans un emplacement sécurisé auquel vous pourrez accéder plus tard.




## Étape 5

Après avoir copié la clé et la clé secrète dans un emplacement sûr, dans l'*écran API Umbrella*, cochez la **case** pour confirmer l'accusé de réception de l'affichage temporaire de la clé secrète, puis cliquez sur le bouton **Fermer**.




Si vous perdez ou supprimez accidentellement la clé secrète, il n'y a aucune fonction ou numéro de support à appeler pour récupérer cette clé. En cas de perte, vous devrez supprimer la clé et réautoriser la nouvelle clé API avec chaque périphérique que vous souhaitez protéger avec Umbrella.

## Configuration de Umbrella sur votre RV345P

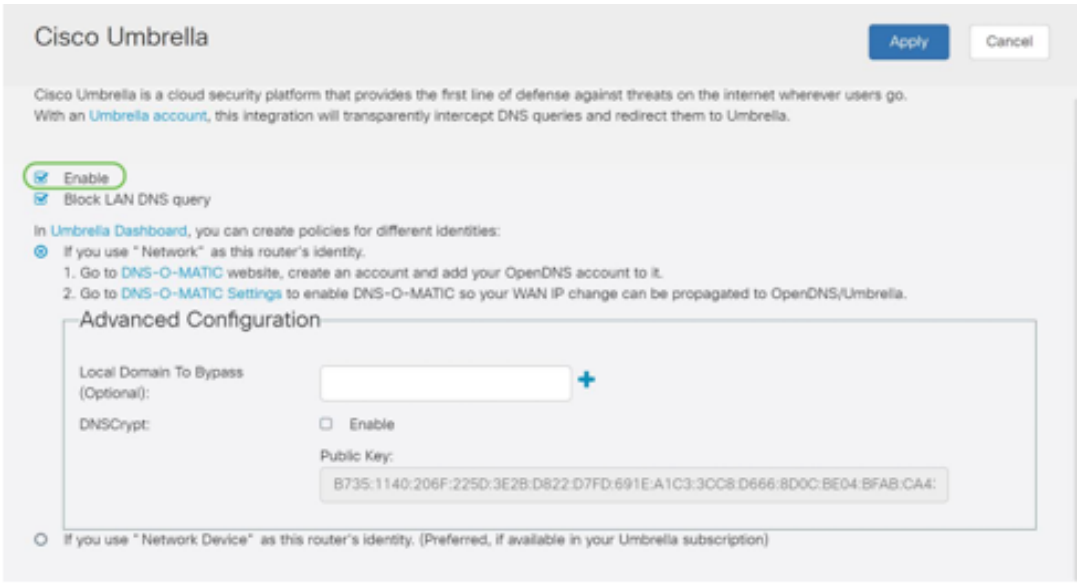
Maintenant que nous avons créé des clés API dans Umbrella, vous pouvez les prendre et les installer sur votre RV345P.

### Étape 1

Après vous être connecté à votre routeur RV345P, cliquez sur **Security > Umbrella** dans le menu latéral.


### Étape 2

L'écran de l'API Umbrella comporte une série d'options, commencez à activer Umbrella en cochant la case **Activer**.

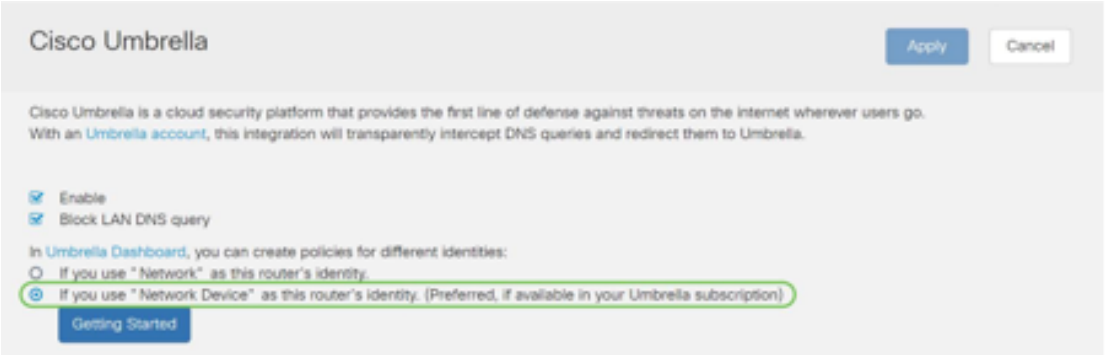



## Étape 3 (facultative)

Par défaut, la case *Bloquer les requêtes DNS du réseau local* est sélectionnée. Cette fonctionnalité permet de créer automatiquement des listes de contrôle d'accès sur votre routeur, ce qui empêche le trafic DNS de se rendre sur Internet. Cette fonctionnalité force toutes les demandes de traduction de domaine à être dirigées via le RV345P et est une bonne idée pour la plupart des utilisateurs.

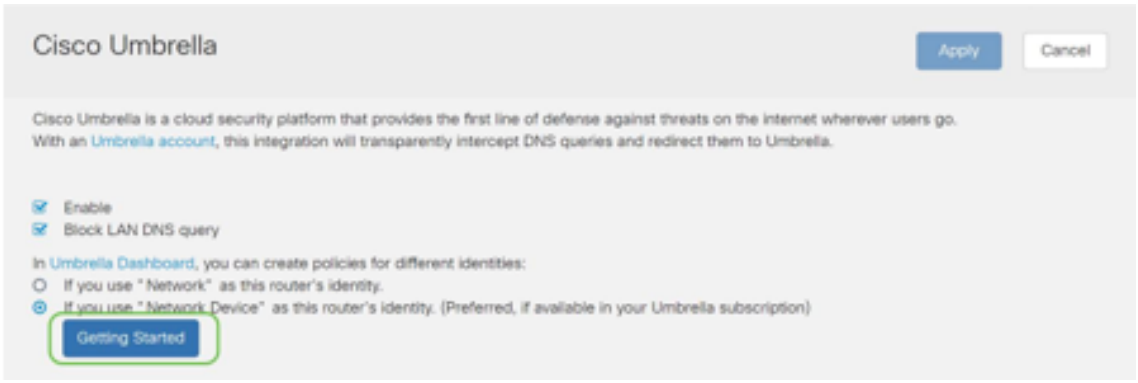
## Étape 4

L'étape suivante se déroule de deux manières différentes. Tous deux dépendent de la configuration de votre réseau. Si vous utilisez un service tel que DynDNS ou NoIP, vous quittez le schéma de dénomination par défaut de " Network ". Vous devez vous connecter à ces comptes pour vous assurer que Umbrella assure des interfaces avec ces services, car il assure une protection. Pour nos besoins, nous comptons sur " Network Device ", nous cliquons donc sur la case d'option inférieure.




## Étape 5

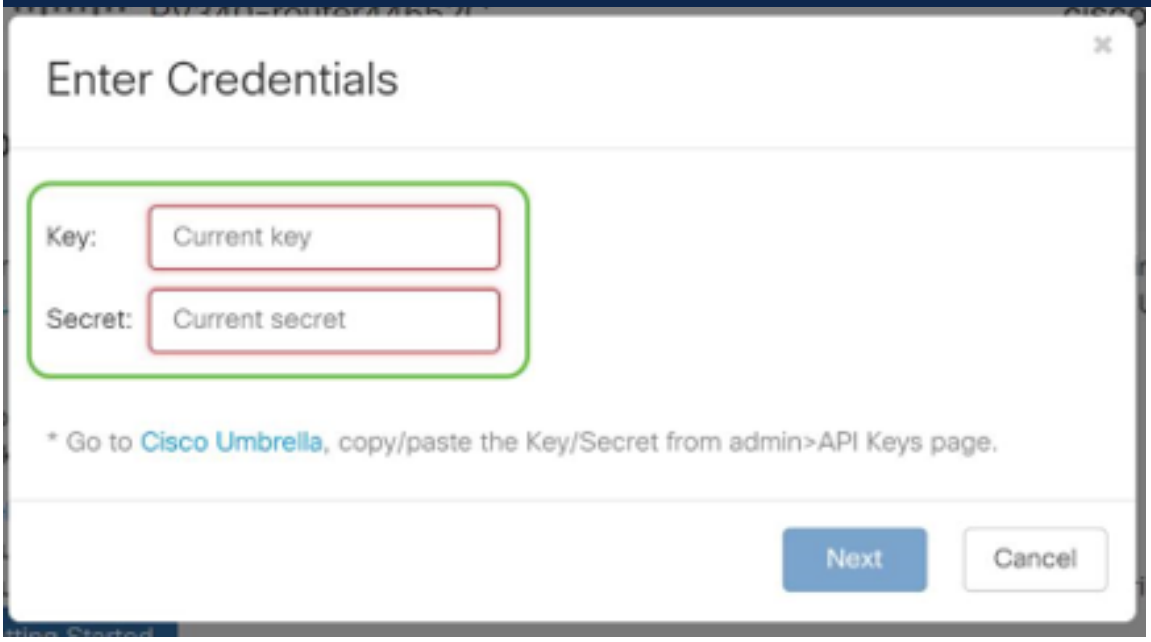
Cliquez sur **Mise en route**.




**Étape 6**

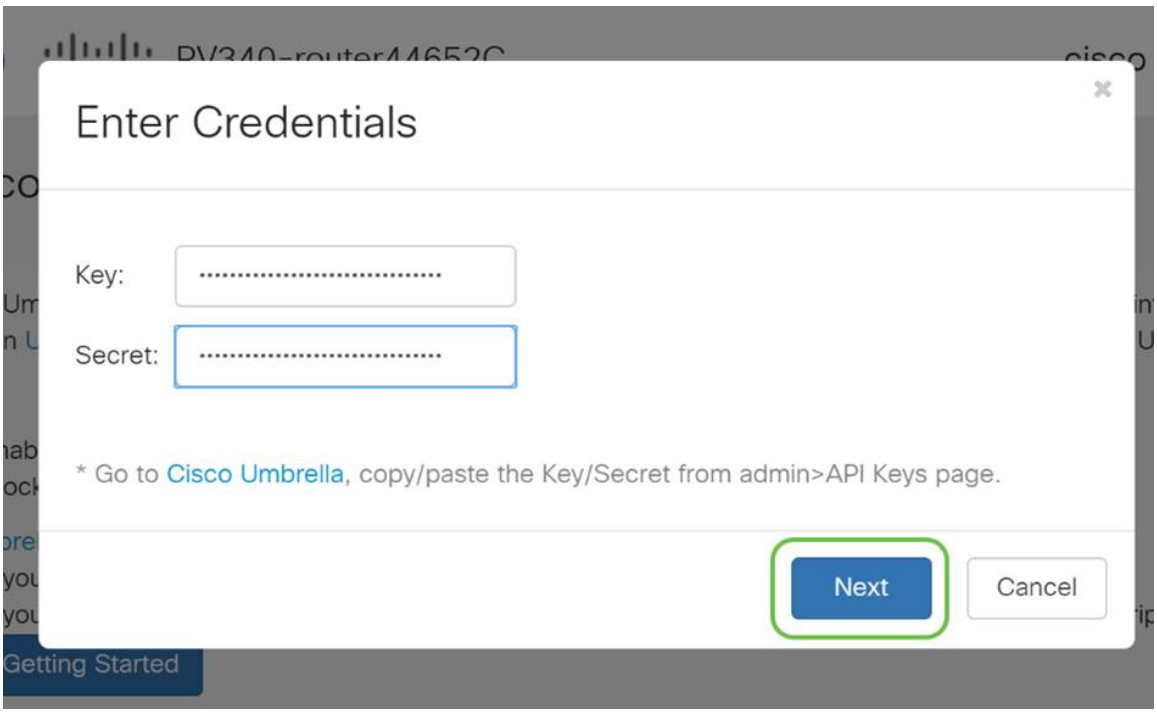
Entrez la **clé API** et la **clé secrète** dans les zones de texte.

Appelez-le deux fois pour que vous sachiez que c'est important ! Si vous perdez ou supprimez accidentellement la clé secrète, il n'y a aucune fonction ou numéro de support à appeler pour récupérer cette clé. Gardez-le secret et en sécurité. En cas de perte, vous devrez supprimer la clé et réautoriser la nouvelle clé API avec chaque périphérique que vous souhaitez protéger avec Umbrella.



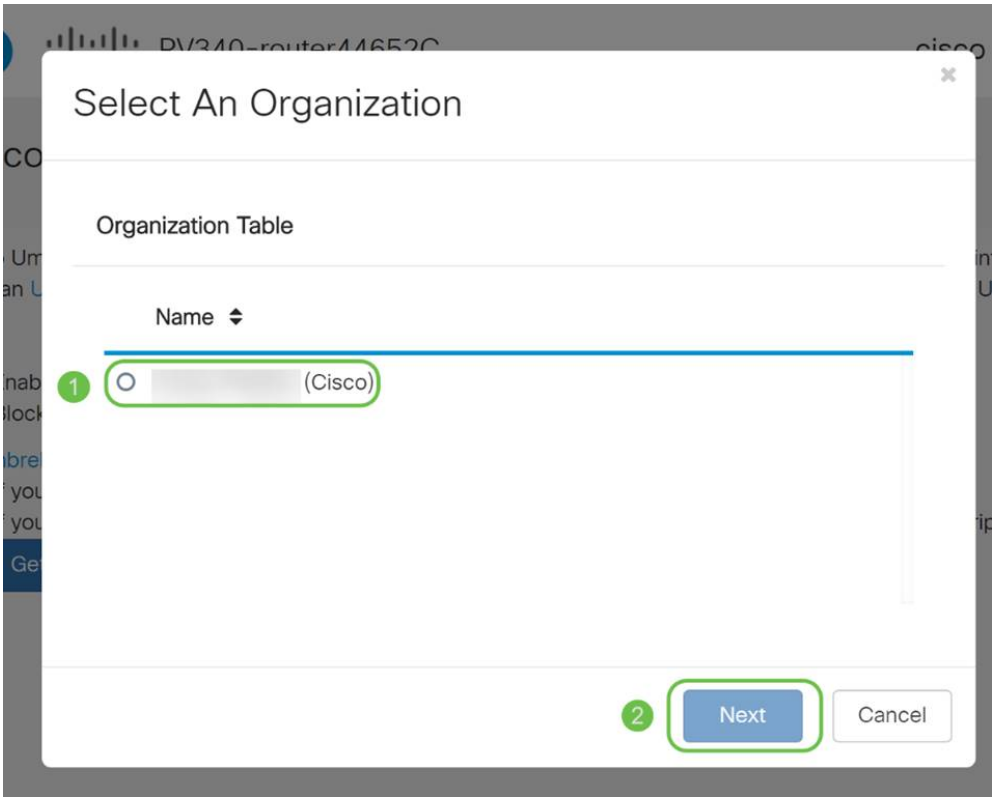

**Étape 7**

Après avoir saisi votre API et votre clé secrète, cliquez sur le bouton **Suivant**.



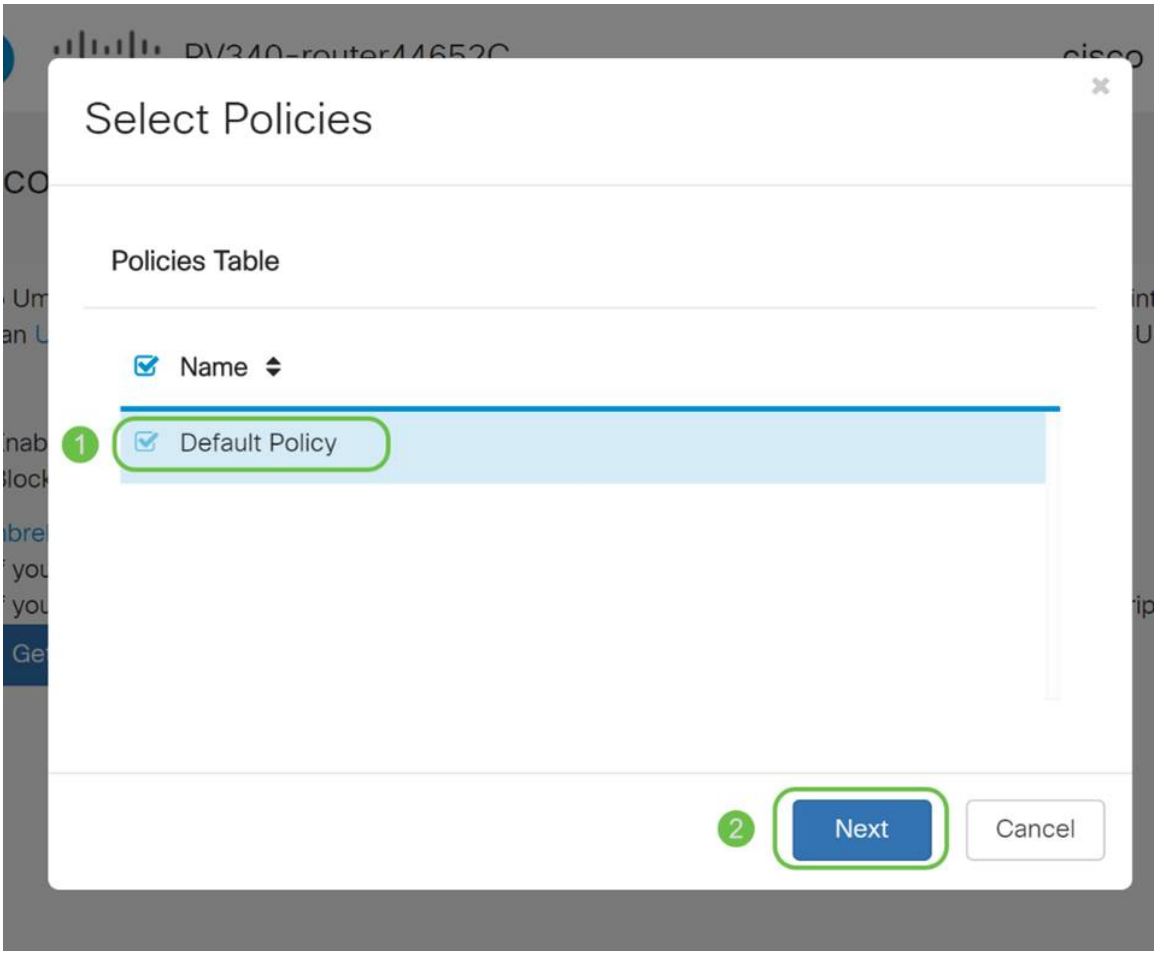

**Étape 8**

Dans l'écran suivant, sélectionnez l'**organisation** que vous souhaitez associer au routeur. Cliquez sur Next (Suivant).



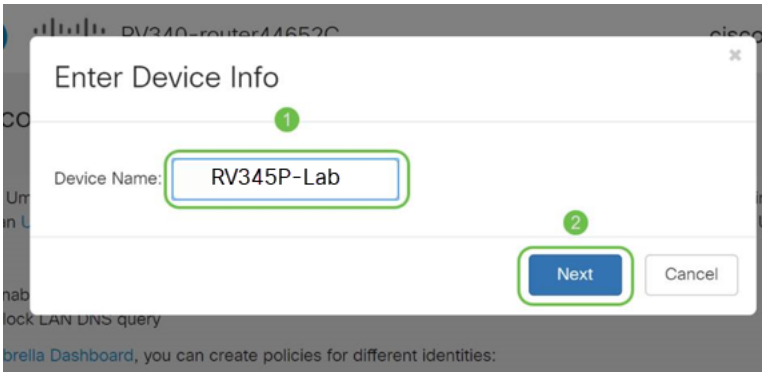

**Étape 9**

Sélectionnez la stratégie à appliquer au trafic acheminé par le RV345P. Pour la plupart des utilisateurs, la stratégie par défaut fournit une couverture suffisante.



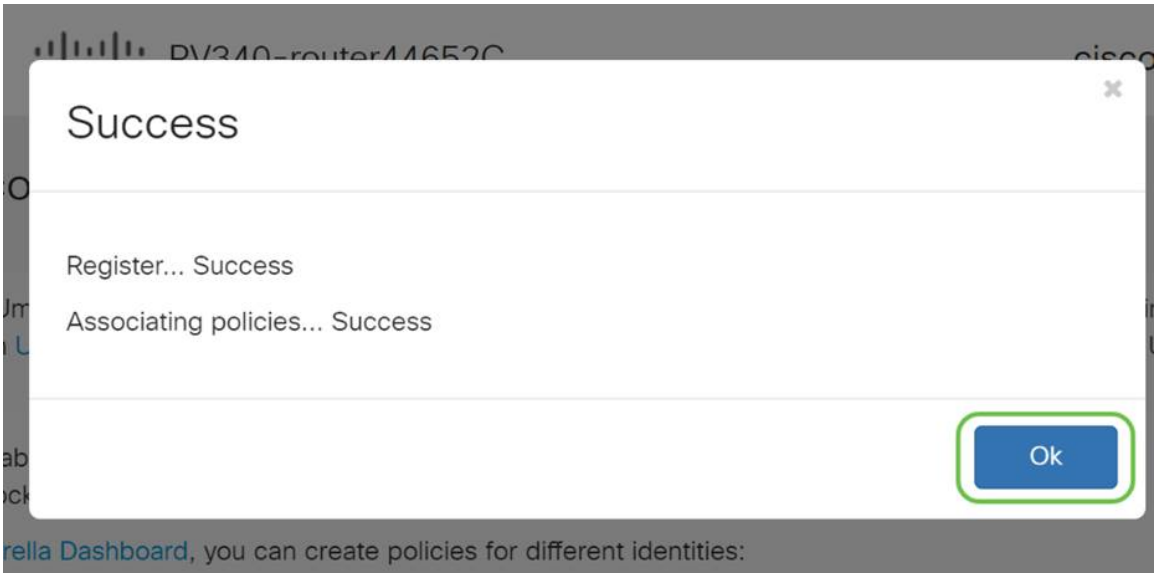

Étape 10

Attribuez un nom au périphérique afin qu'il puisse être désigné dans la création de rapports Umbrella. Dans notre configuration, nous l'avons nommé *RV345P-Lab*.




Étape 11

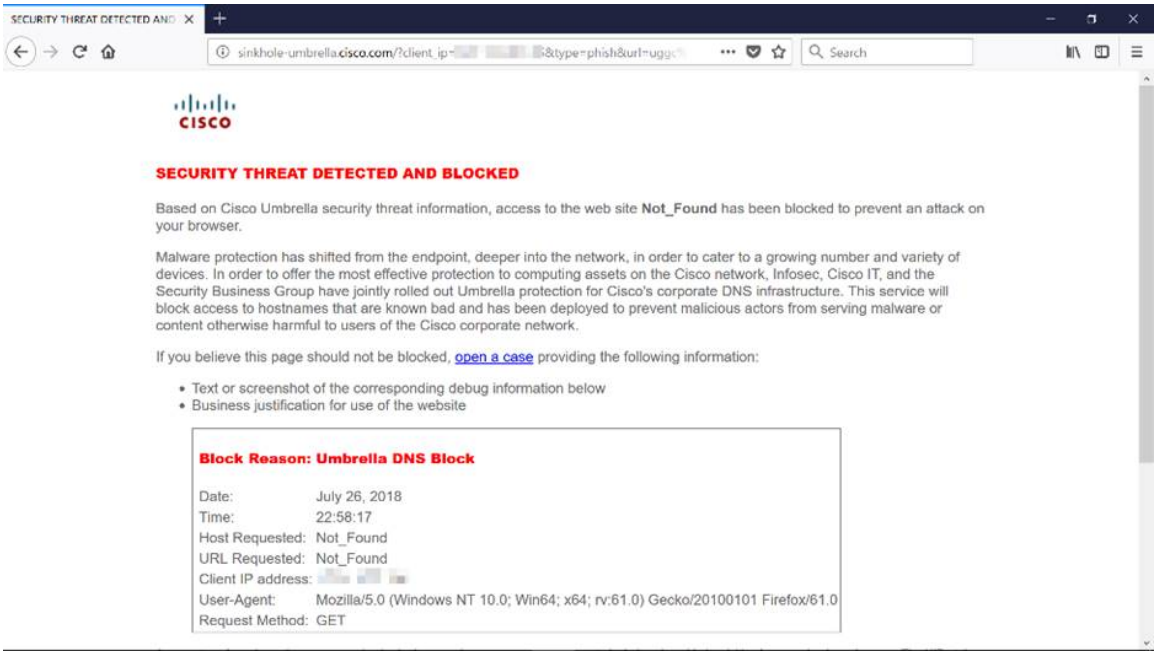
L'écran suivant valide les paramètres sélectionnés et fournit une mise à jour une fois l'association réussie. Click OK.




**Confirmation**

Félicitations, vous êtes désormais protégé par Cisco Umbrella. Ou vous ? En vérifiant deux fois l'exemple en direct, Cisco a créé un site Web dédié à la détermination de ce problème aussi rapidement que la page se charge. Cliquez ici ou tapez https://InternetBadGuys.com dans la barre de navigation.

Si Umbrella est configuré correctement, vous serez accueilli par un écran similaire à celui-ci.




## Autres options de sécurité

Craignez-vous que quelqu'un tente d'accéder au réseau sans autorisation en débranchant un câble Ethernet d'un périphérique réseau et en le connectant ? Dans ce cas, il est important d'enregistrer une liste d'hôtes autorisés à se connecter directement au routeur avec leurs adresses IP et MAC respectives. Les instructions se trouvent dans l'article Configurer la protection de source IP sur le routeur de la gamme RV34x.

# Options VPN

Une connexion de réseau privé virtuel (VPN) permet aux utilisateurs d'accéder, d'envoyer et de recevoir des données depuis et vers un réseau privé en passant par un réseau public ou partagé tel qu'Internet, tout en assurant une connexion sécurisée à une infrastructure réseau sous-jacente afin de protéger le réseau privé et ses ressources.

Un tunnel VPN établit un réseau privé qui peut envoyer des données en toute sécurité à l'aide du chiffrement et de l'authentification. Les bureaux d'entreprise utilisent principalement une connexion VPN car il est à la fois utile et nécessaire de permettre à leurs employés d'accéder à leur réseau privé même s'ils se trouvent en dehors du bureau.

Le VPN permet à un hôte distant d'agir comme s'il se trouvait sur le même réseau local. Le routeur prend en charge jusqu'à 50 tunnels. Une connexion VPN peut être configurée entre le routeur et un point d'extrémité une fois que le routeur a été configuré pour la connexion Internet. Le client VPN dépend entièrement des paramètres du routeur VPN pour établir une connexion.

Si vous ne savez pas quel VPN répond le mieux à vos besoins, consultez la présentation et les meilleures pratiques de Cisco Business VPN.

AnyConnect VPN est le seul produit pris en charge par Cisco VPN figurant dans ce guide de configuration. Les produits tiers non Cisco, notamment TheGreenBow et Shrew Soft, ne sont pas pris en charge par Cisco. Ils sont inclus strictement à des fins d'orientation. Si vous avez besoin d'assistance sur ces éléments au-delà de l'article, vous devez contacter ce tiers pour obtenir de l'assistance.

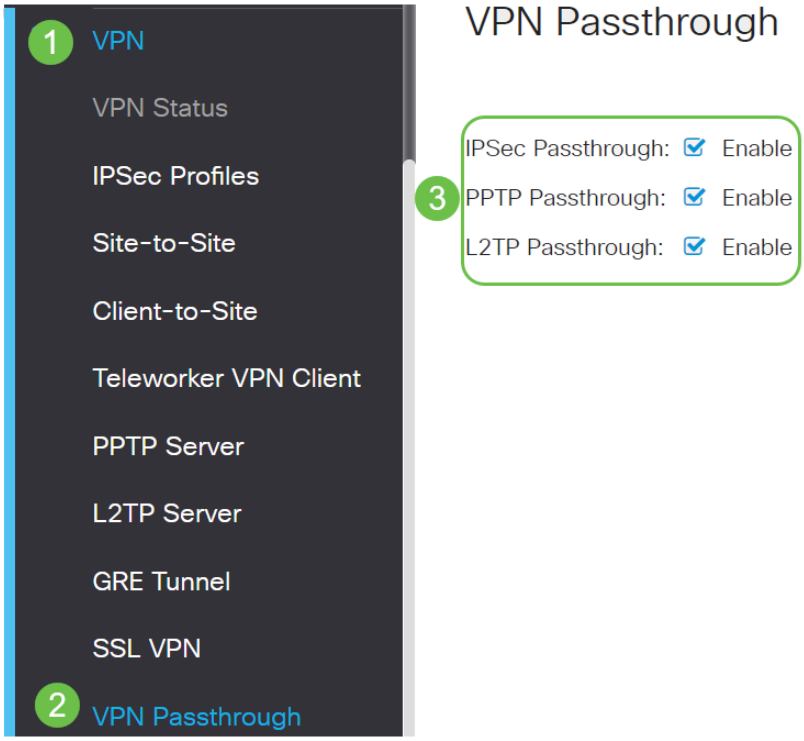
Si vous ne prévoyez pas de configurer un VPN, vous pouvez cliquer pour passer à la section suivante.

## Relais VPN

En général, chaque routeur prend en charge la traduction d'adresses de réseau (NAT) afin de conserver les adresses IP lorsque vous souhaitez prendre en charge plusieurs clients avec la même connexion Internet. Cependant, le protocole PPTP (Point-to-Point Tunneling Protocol) et le VPN IPsec (Internet Protocol Security) ne prennent pas en charge NAT. C'est là que le Passthrough VPN entre en jeu. Un Passthrough VPN est une fonctionnalité qui permet au trafic VPN généré par des clients VPN connectés à ce routeur de passer par ce routeur et de se connecter à un point d'extrémité VPN. Le Passthrough VPN permet aux VPN PPTP et IPsec de passer uniquement à Internet, qui est initié à partir d'un client VPN, puis d'atteindre la passerelle VPN distante. Cette fonctionnalité est couramment utilisée sur les routeurs domestiques qui prennent en charge la fonction NAT.

Par défaut, IPsec, PPTP et L2TP Passthrough sont activés. Pour afficher ou ajuster

ces paramètres, sélectionnez **VPN > VPN Passthrough**. Affichez ou réglez selon vos besoins.




## VPN AnyConnect

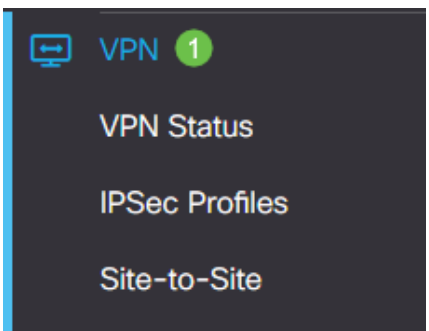
L'utilisation de Cisco AnyConnect présente plusieurs avantages :

1. Connectivité sécurisée et permanente
2. Sécurité permanente et application des politiques
3. Déployable à partir de l'appareil de sécurité adaptatif (ASA) ou des systèmes de déploiement de logiciels d'entreprise
4. Personnalisable et traduisible
5. Facilement configuré
6. Prend en charge IPsec (Internet Protocol Security) et SSL (Secure Sockets Layer)
7. Prise en charge du protocole Internet Key Exchange version 2.0 (IKEv2.0)

### Configuration du VPN SSL AnyConnect sur le RV345P

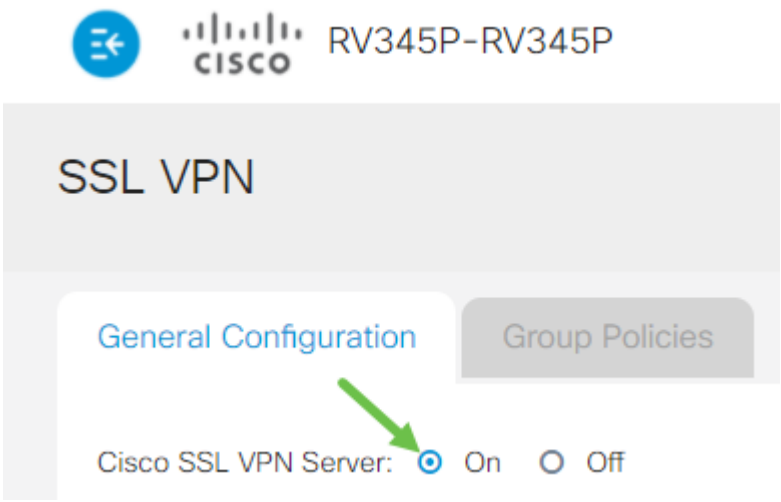
### Étape 1

Accédez à l'utilitaire Web du routeur et choisissez **VPN > SSL VPN**.



### Étape 2

Activez la case d'option **On** pour activer Cisco SSL VPN Server.




## Paramètres de passerelle obligatoires

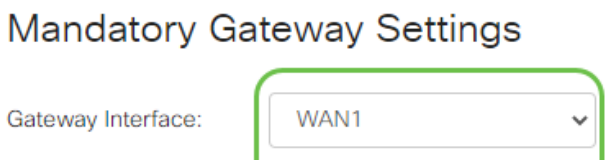
### Étape 1

Les paramètres de configuration suivants sont obligatoires :

1. Sélectionnez Gateway Interface dans la liste déroulante. Il s'agit du port qui sera utilisé pour transmettre le trafic via les tunnels VPN SSL. Les options sont les suivantes : WAN1, WAN2, USB1, USB2
2. Saisissez le numéro de port utilisé pour la passerelle VPN SSL dans le champ Gateway Port (Port de passerelle) compris entre 1 et 65535.
3. Sélectionnez le fichier de certificat dans la liste déroulante. Ce certificat authentifie les utilisateurs qui tentent d'accéder à la ressource réseau via les tunnels VPN SSL. La liste déroulante contient un certificat par défaut et les certificats importés.
4. Entrez l'adresse IP du pool d'adresses client dans le champ *Client Address Pool*. Ce pool sera la plage d'adresses IP qui sera allouée aux clients VPN distants.

   Assurez-vous que la plage d’adresses IP ne chevauche aucune des adresses IP du réseau local.

6. Sélectionnez le masque de réseau du client dans la liste déroulante.
7. Entrez le nom de domaine du client dans le champ *Domaine du client*. Il s'agit du nom de domaine qui doit être envoyé aux clients VPN SSL.
8. Entrez le texte qui apparaîtra comme bannière de connexion dans le champ *Bannière de connexion*. Il s'agit de la bannière qui s'affiche chaque fois qu'un client se connecte.



### Étape 2

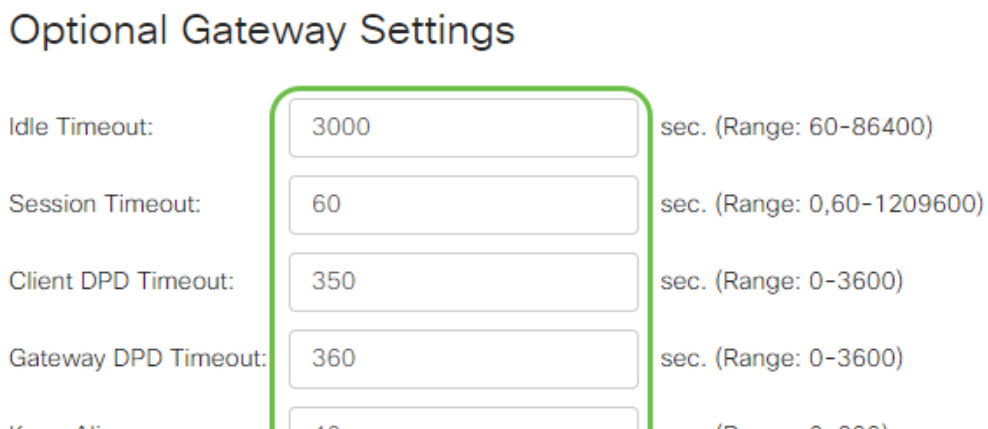
Cliquez sur Apply.


## Paramètres de passerelle facultatifs

### Étape 1

Les paramètres de configuration suivants sont facultatifs :

1. Saisissez une valeur en secondes pour le délai d'inactivité compris entre 60 et 86400. Il s'agit de la durée pendant laquelle la session VPN SSL peut rester inactive.
2. Entrez une valeur en secondes dans le champ *Temporisation de session*. Il s'agit du temps nécessaire pour que la session TCP (Transmission Control Protocol) ou UDP (User Datagram Protocol) expire après le temps d'inactivité spécifié. Elle est située entre 60 et 1209600.
3. Entrez une valeur en secondes dans le champ *ClientDPD Timeout* compris entre 0 et 3600. Cette valeur spécifie l'envoi périodique de messages HELLO/ACK pour vérifier l'état du tunnel VPN. Cette fonctionnalité doit être activée aux deux extrémités du tunnel VPN.
4. Entrez une valeur en secondes dans le champ *GatewayDPD Timeout* compris entre 0 et 3600. Cette valeur spécifie l'envoi périodique de messages HELLO/ACK pour vérifier l'état du tunnel VPN. Cette fonctionnalité doit être activée aux deux extrémités du tunnel VPN.
5. Entrez une valeur en secondes dans le champ *Keep Alive* comprise entre 0 et 600. Cette fonctionnalité garantit que votre routeur est toujours connecté à Internet. Il tentera de rétablir la connexion VPN si elle est abandonnée.
6. Entrez une valeur en secondes pour la durée du tunnel à connecter dans le champ *Durée du bail*. Elle est située entre 600 et 1209600.
7. Entrez la taille du paquet en octets qui peut être envoyé sur le réseau. Elle est située entre 576 et 1406.
8. Saisissez le délai d'intervalle de relais dans le champ *Rekey Interval*. La fonction Rekey permet aux clés SSL de renégocier une fois la session établie. Elle est située entre 0 et 43200.



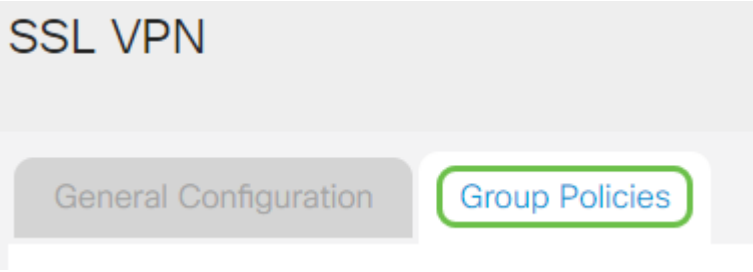
### Étape 2

Cliquez sur Apply.


## Configurer les stratégies de groupe

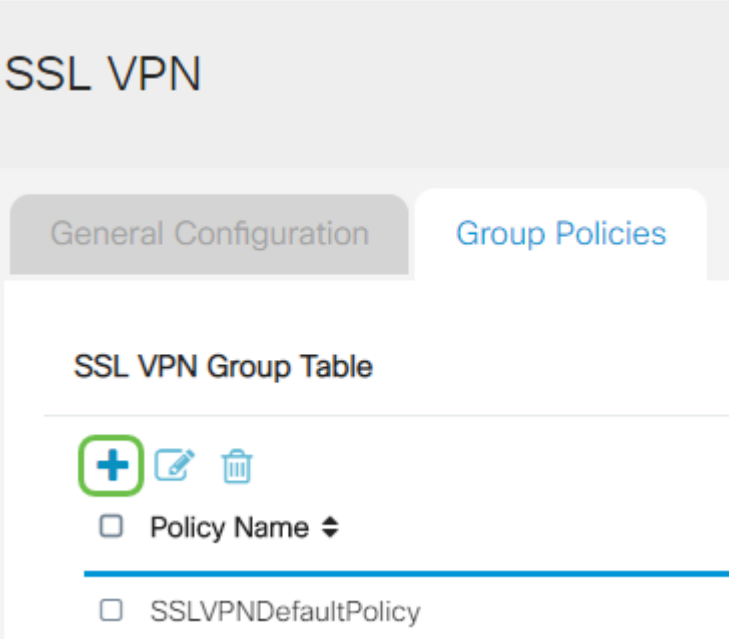
### Étape 1

Cliquez sur l'onglet **Stratégies de groupe**.




### Étape 2

Cliquez sur l'**icône Ajouter** sous la table de groupe VPN SSL pour ajouter une stratégie de groupe.

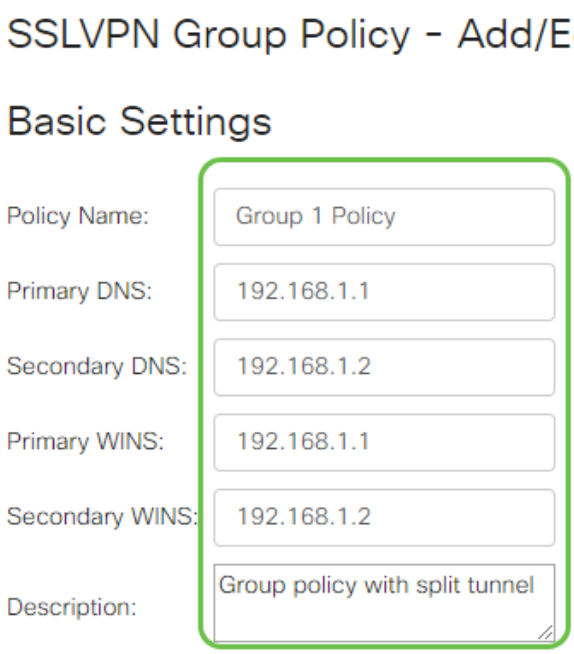



Le tableau Groupe VPN SSL affiche la liste des stratégies de groupe sur le périphérique. Vous pouvez également modifier la première stratégie de groupe de la liste, nommée SSLVPNDefaultPolicy. Il s'agit de la stratégie par défaut fournie par le périphérique.

### Étape 3

1. Entrez le nom de stratégie préféré dans le champ *Nom de la stratégie*.

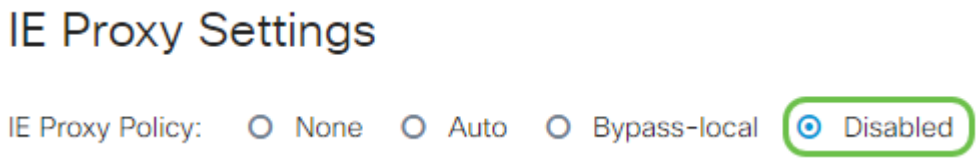
2. Saisissez l'adresse IP du DNS principal dans le champ fourni. Par défaut, cette adresse IP est déjà fournie.
3. *(Facultatif) Saisissez l'adresse IP du DNS secondaire dans le champ fourni. Cela servira de sauvegarde en cas d'échec du DNS principal.*
4. (Facultatif) Saisissez l'adresse IP du WINS principal dans le champ fourni.
5. (Facultatif) Saisissez l'adresse IP du WINS secondaire dans le champ fourni.
6. (Facultatif) Entrez une description de la stratégie dans le champ *Description*.




**Étape 4 (facultative)**

Cliquez sur une case d'option pour sélectionner la stratégie de proxy IE pour activer les paramètres de proxy Microsoft Internet Explorer (MSIE) pour établir un tunnel VPN. Les options sont les suivantes :

- Aucun : permet au navigateur d'utiliser aucun paramètre de proxy.
- Auto : permet au navigateur de détecter automatiquement les paramètres du proxy.
- Bypass-local : permet au navigateur de contourner les paramètres de proxy configurés sur l'utilisateur distant.
- Désactivé : désactive les paramètres du proxy MSIE.




**Étape 5 (facultative)**

Dans la zone Split Tunneling Settings, cochez la case **Enable Split Tunneling** pour permettre au trafic destiné à Internet d'être envoyé sans cryptage directement à Internet. La transmission tunnel complète envoie tout le trafic vers le périphérique final où il est ensuite acheminé vers les ressources de destination, éliminant ainsi le réseau

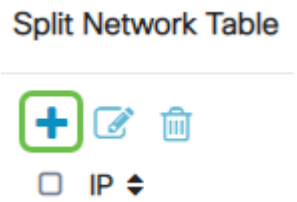
d'entreprise du chemin d'accès Web.


**Étape 6 (facultative)**

Cliquez sur une case d'option pour choisir d'inclure ou d'exclure le trafic lors de l'application de la tunnellisation fractionnée.

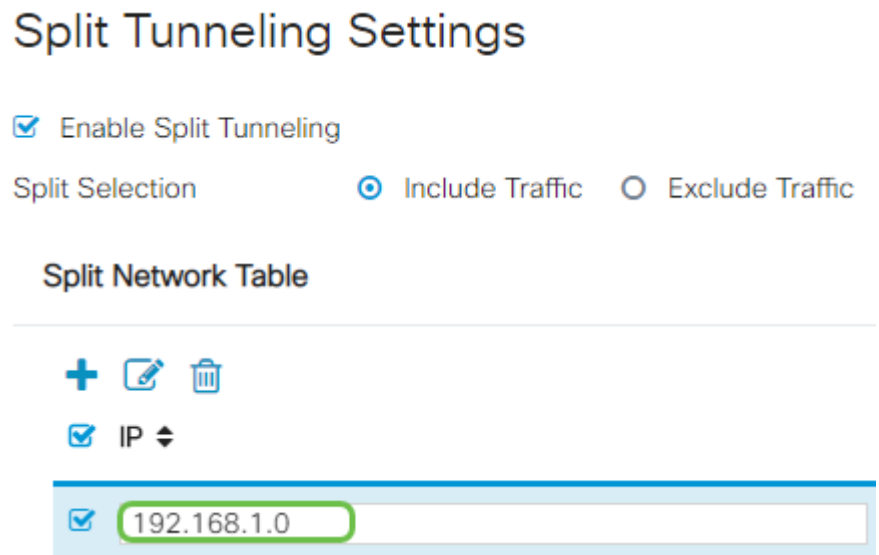

**Étape 7**

Dans la table Réseau divisé, cliquez sur l'**icône Ajouter** pour ajouter une exception Réseau divisé.



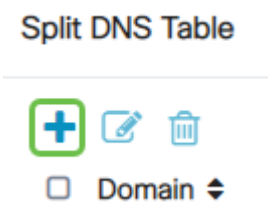

**Étape 8**

Saisissez l'adresse IP du réseau dans le champ prévu à cet effet.



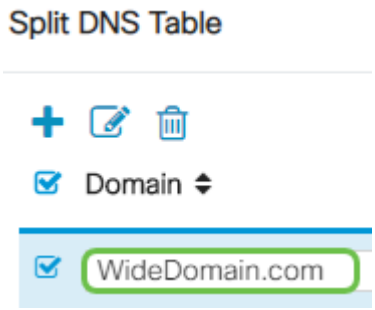

**Étape 9**

Dans la table DNS fractionnée, cliquez sur l'**icône add** pour ajouter une exception DNS fractionnée.




### Étape 10

Entrez le nom de domaine dans le champ fourni, puis cliquez sur **Apply**.




Le routeur est fourni avec 2 licences de serveur AnyConnect par défaut. Cela signifie qu'une fois que vous avez des licences client AnyConnect, vous pouvez établir 2 tunnels VPN simultanément avec n'importe quel autre routeur de la gamme RV340.

En bref, le routeur RV345P n'a pas besoin de licence, mais tous les clients en auront besoin. Les licences client AnyConnect permettent aux clients mobiles et de bureau d'accéder au réseau VPN à distance.

Cette section explique comment obtenir des licences pour vos clients.

### Client de mobilité AnyConnect

Un client VPN est un logiciel installé et exécuté sur un ordinateur qui souhaite se connecter au réseau distant. Ce logiciel client doit être configuré avec la même configuration que celle du serveur VPN, telle que l'adresse IP et les informations d'authentification. Ces informations d'authentification incluent le nom d'utilisateur et la clé pré-partagée qui seront utilisés pour chiffrer les données. Selon l'emplacement physique des réseaux à connecter, un client VPN peut également être un périphérique matériel. Cela se produit généralement si la connexion VPN est utilisée pour connecter deux réseaux situés à des emplacements distincts.

Le client Cisco AnyConnect Secure Mobility est une application logicielle permettant de se connecter à un VPN qui fonctionne sur différents systèmes d'exploitation et configurations matérielles. Cette application logicielle permet aux ressources distantes d'un autre réseau d'être accessibles comme si l'utilisateur était directement connecté à son réseau, mais de manière sécurisée.

Une fois le routeur enregistré et configuré avec AnyConnect, le client peut installer des licences sur le routeur à partir du pool de licences disponibles que vous achetez, qui est détaillé dans la section suivante.

## Licence d'achat

Vous devez acheter une licence auprès de votre distributeur Cisco ou de votre partenaire Cisco. Lors de la commande d'une licence, vous devez fournir votre ID de compte Cisco Smart ou votre ID de domaine sous la forme *name@domain.com*.

Si vous n'avez pas de distributeur ou de partenaire Cisco, vous pouvez en trouver un ici.

Au moment de la rédaction du présent rapport, les références produit suivantes peuvent être utilisées pour acheter des licences supplémentaires dans des offres groupées de 25. Notez qu'il existe d'autres options pour les licences client AnyConnect, comme indiqué dans le guide de commande Cisco AnyConnect. Cependant, l'ID de produit indiqué serait la condition minimale requise pour la fonctionnalité complète.

Notez que la référence produit de licence client AnyConnect indiquée en premier, fournit des licences pour une durée d'un an et nécessite un achat minimum de 25 licences. D'autres références de produits applicables aux routeurs de la gamme RV340 sont également disponibles avec différents niveaux d'abonnement, comme suit :

- **LS-AC-PLS-1Y-S1** — Licence client Cisco AnyConnect Plus d'un an
- **LS-AC-PLS-3Y-S1** — Licence client Cisco AnyConnect Plus de 3 ans
- **LS-AC-PLS-5Y-S1** — Licence client Cisco AnyConnect Plus de 5 ans
- **LS-AC-PLS-P-25-S** — 25 licences client perpétuelles Cisco AnyConnect Plus
- **LS-AC-PLS-P-50-S** — 50 licences perpétuelles Cisco AnyConnect Plus

## Informations sur le client

Lorsque votre client configure l'un des liens suivants, vous devez lui envoyer ces liens :

- Fenêtres: AnyConnect sur un ordinateur Windows
- Mac : Installez AnyConnect sur Mac.
- Bureau Ubuntu : Installation et utilisation d'AnyConnect sur Ubuntu Desktop
- Si vous rencontrez des problèmes, accédez à Collecte d'informations pour le dépannage de base sur les erreurs du client Cisco AnyConnect Secure Mobility.

## Vérification de la connectivité VPN AnyConnect

### Étape 1

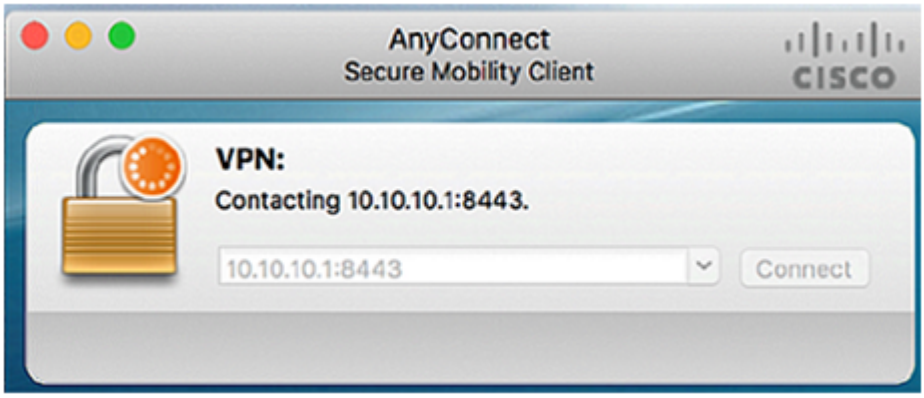
Cliquez sur l'**icône AnyConnect Secure Mobility Client**.

### Étape 2

Dans la fenêtre AnyConnect Secure Mobility Client, saisissez l'adresse IP de la

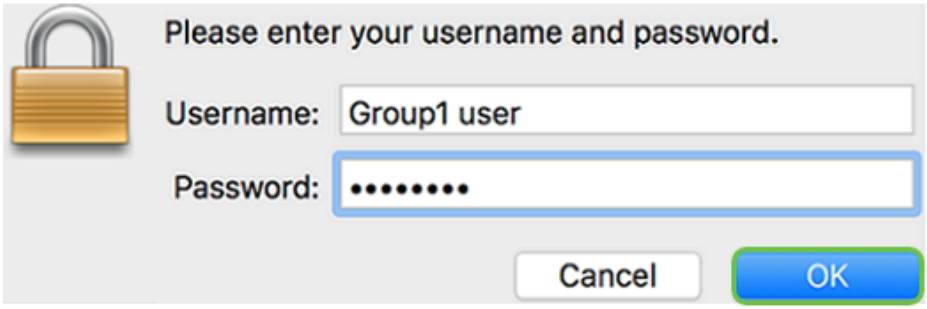
passerelle et le numéro de port de la passerelle séparés par deux-points (:), puis cliquez sur **Connect**.


Le logiciel indique maintenant qu'il contacte le réseau distant.



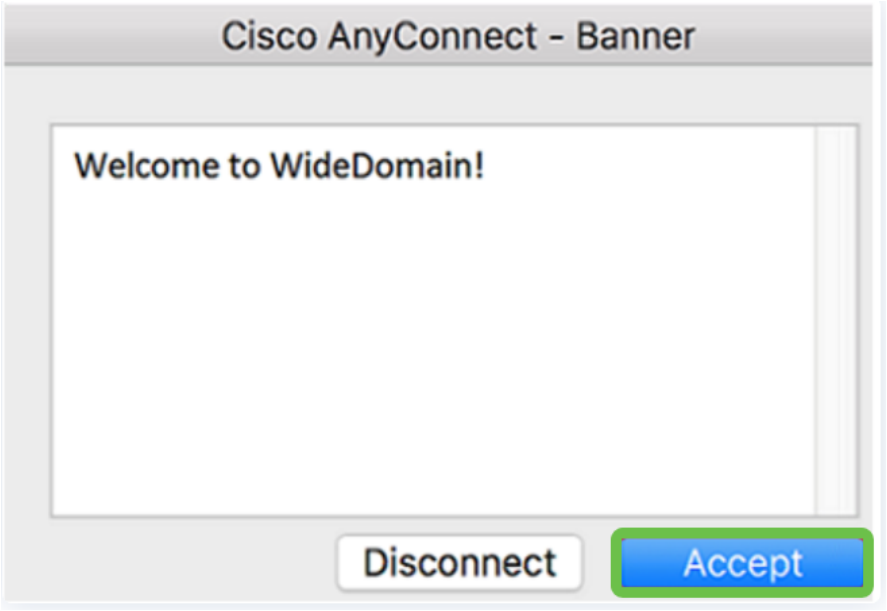

**Étape 3**

Entrez votre nom d'utilisateur et votre mot de passe dans les champs respectifs, puis cliquez sur **OK**.

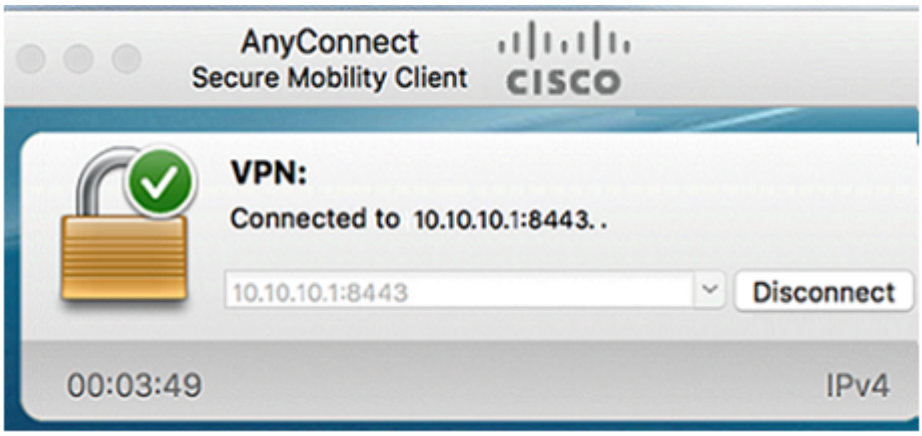



**Étape 4**

Dès que la connexion est établie, la bannière de connexion apparaît. Cliquez sur **Accepter**.




La fenêtre AnyConnect doit maintenant indiquer la connexion VPN réussie au réseau.




Si vous utilisez maintenant AnyConnect VPN, vous pouvez passer outre d'autres options VPN et passer à la section suivante.

## VPN logiciel Shrew

Un VPN IPsec vous permet d'obtenir des ressources distantes en toute sécurité en établissant un tunnel chiffré sur Internet. Les routeurs de la gamme RV34X fonctionnent comme des serveurs VPN IPsec et prennent en charge le client VPN logiciel Shrew. Cette section explique comment configurer votre routeur et le client logiciel Shrew pour sécuriser une connexion à un VPN.

Cisco ne prend pas en charge Shrew Soft. Cet exemple est fourni à des fins de démonstration uniquement. Si vous avez des problèmes avec Shrew Soft, veuillez les contacter pour obtenir de l'aide.

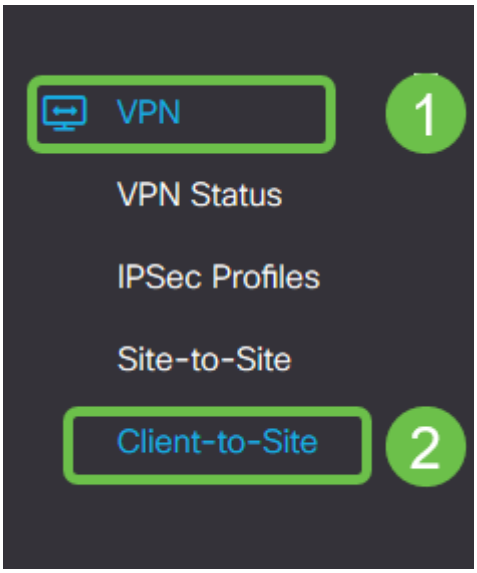
Vous pouvez télécharger la dernière version du logiciel client VPN Shrew Soft ici : https://www.shrew.net/download/vpn

### Configuration du logiciel Shrew sur le routeur de la gamme RV345P

Nous commencerons par configurer le **VPN client à site** sur le RV345P.

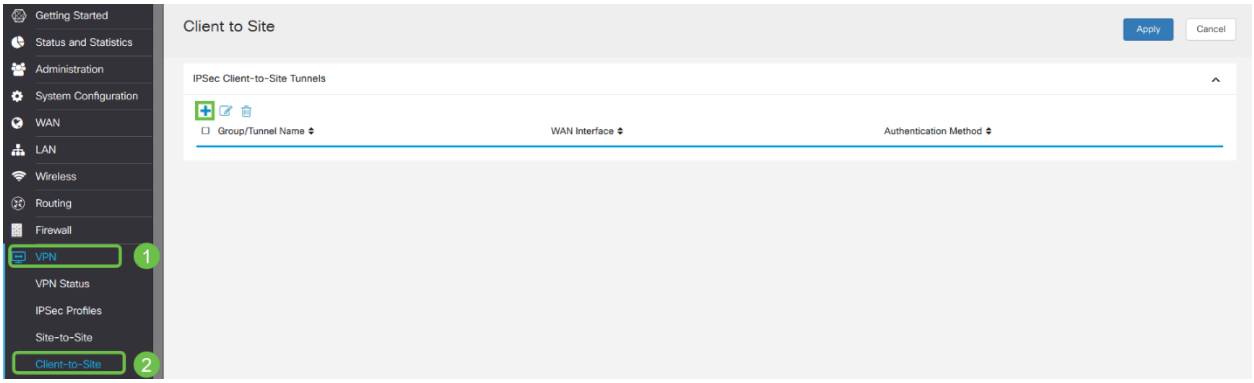
## Étape 1

Accédez à **VPN > Client-to-Site.**



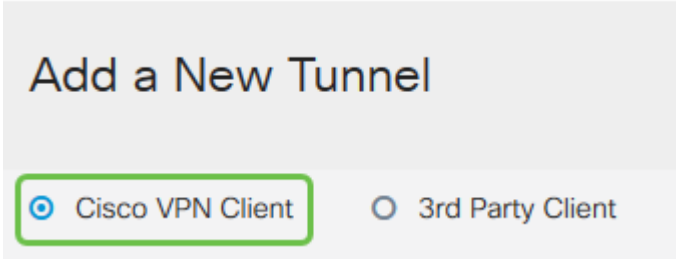

## Étape 2

Ajoutez un profil VPN **client à site**.




## Étape 3

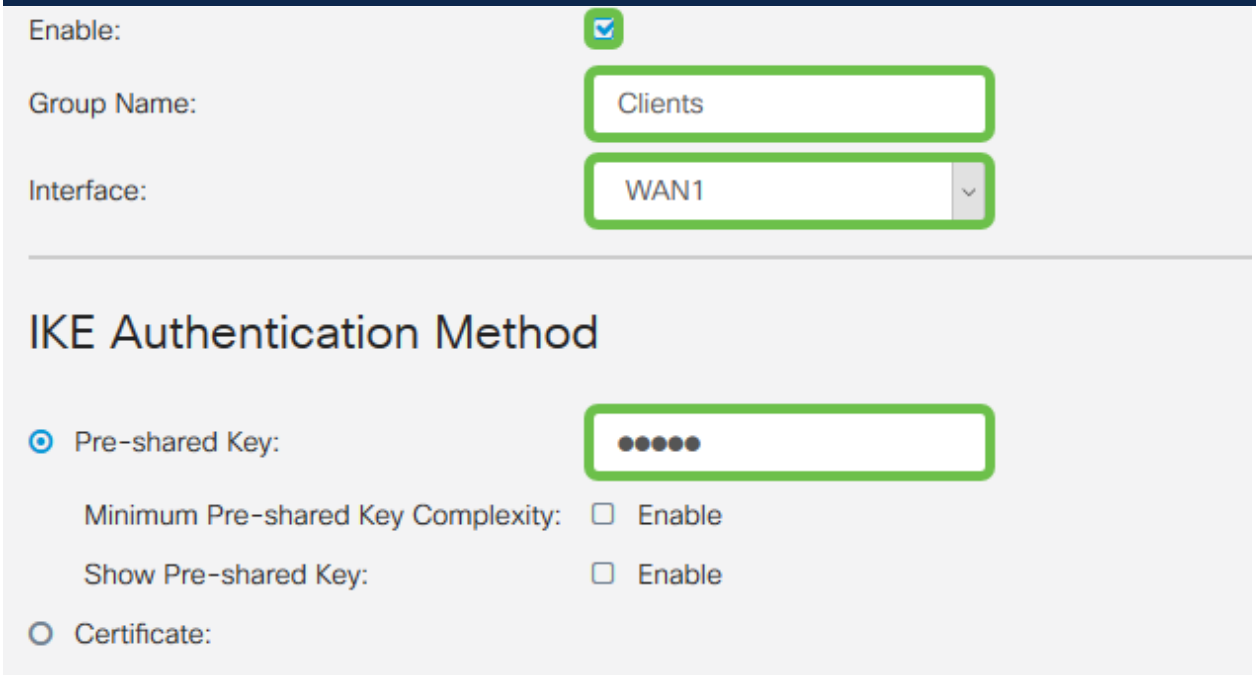
Sélectionnez l'option **Client VPN Cisco**.




## Étape 4

Cochez la case **Enable** pour activer le profil de client VPN. Nous allons également configurer le *nom de groupe*, sélectionner l'**interface WAN** et saisir une **clé prépartagée** .

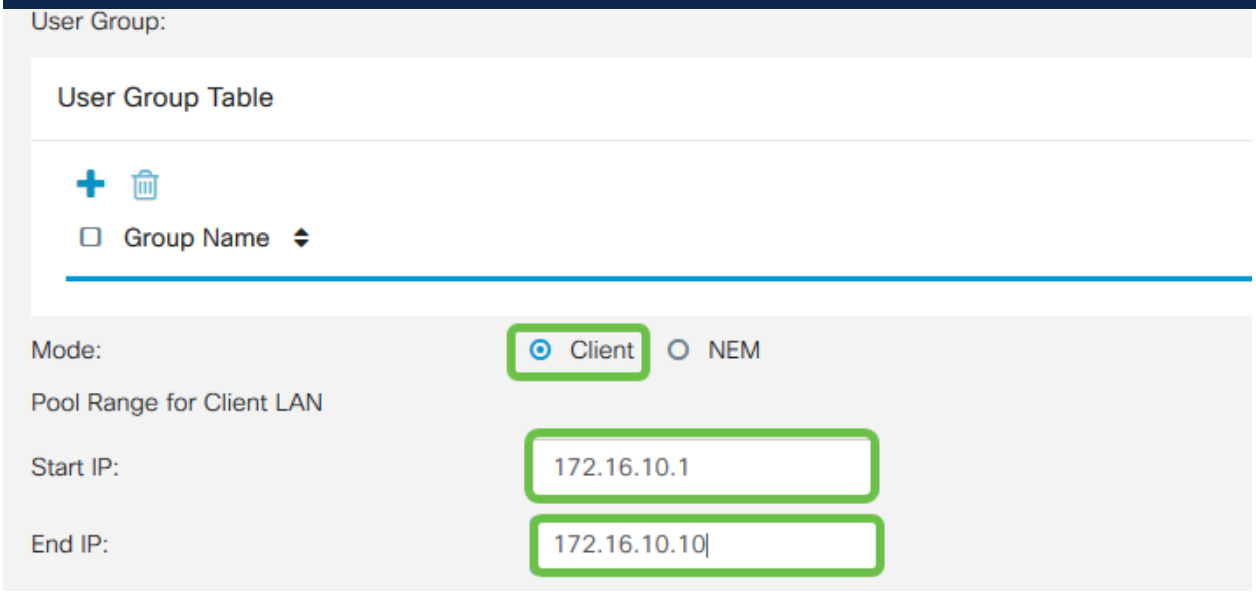
Notez le *nom de groupe* et la *clé prépartagée*, car ils seront utilisés ultérieurement lors de la configuration du client.




**Étape 5**

Laissez la **table Groupe d'utilisateurs** vide pour le moment. Il s'agit du *groupe d'utilisateurs* sur le routeur, mais nous ne l'avons pas encore configuré. Assurez-vous que le **mode** est défini sur **Client**. Entrez la **plage de pools pour le réseau local du client** . Nous utiliserons 172.16.10.1 à 172.16.10.10.

La plage de pools doit utiliser un sous-réseau unique qui n'est pas utilisé ailleurs sur le réseau.

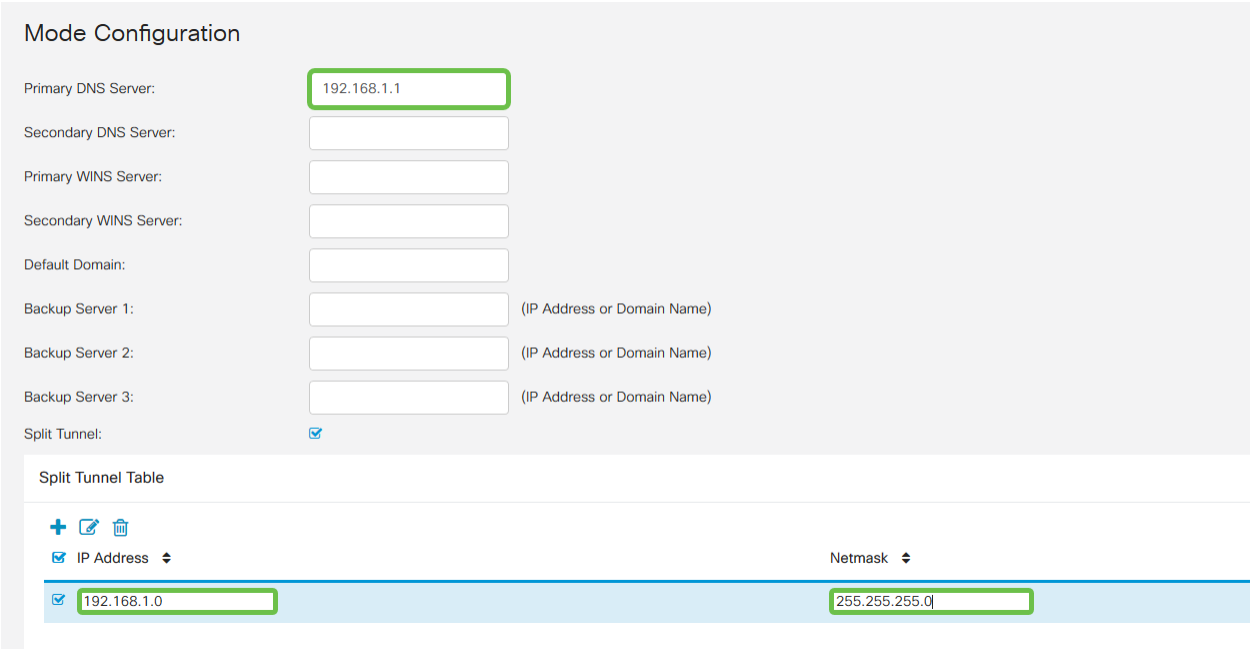



**Étape 6**

Voici où nous configurons les paramètres **de configuration du mode**. Voici les

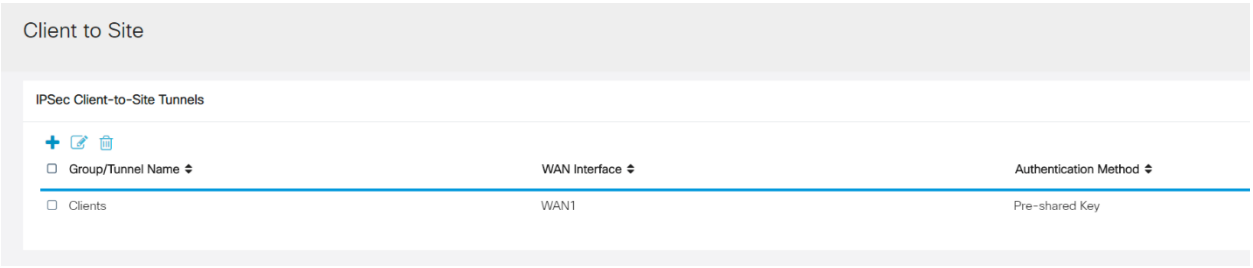
paramètres que nous allons utiliser :

- **Serveur DNS principal** : Si vous avez un serveur DNS interne ou souhaitez utiliser un serveur DNS externe, vous pouvez le saisir ici. Sinon, la valeur par défaut est l'adresse IP du réseau local RV345P. Nous utiliserons la valeur par défaut dans notre exemple.
- **Tunnel fractionné :** cochez cette case pour activer la tunnellisation fractionnée. Ceci est utilisé pour spécifier le trafic qui passera par le tunnel VPN. Nous allons utiliser le tunnel partagé dans notre exemple.
- **Table de tunnels fractionnés :** saisissez les réseaux auxquels le client VPN doit avoir accès via le VPN. Cet exemple utilise le réseau local RV345P.



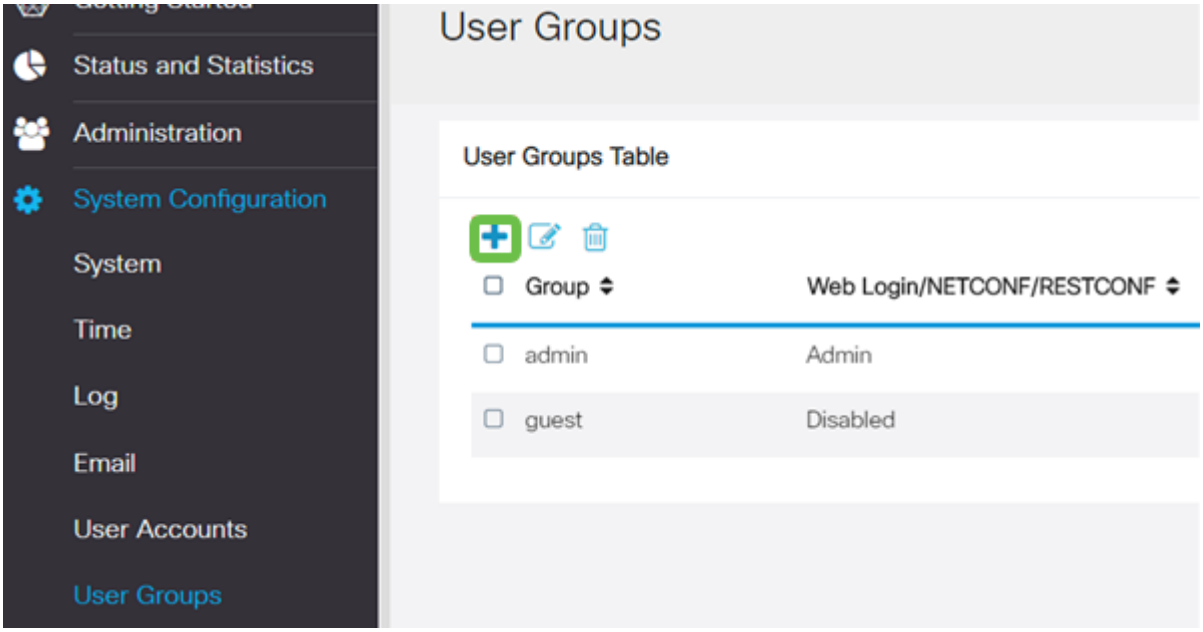

## Étape 7

Après avoir cliqué sur **Enregistrer**, nous pouvons voir le profil dans la liste **Groupes client-site IPsec**.



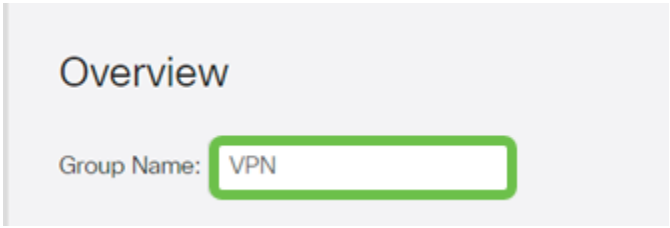

## Étape 8

Configurez un **groupe d'utilisateurs** à utiliser pour authentifier les utilisateurs du client VPN. Sous **Configuration système > Groupes d'utilisateurs**, cliquez sur l'**icône plus** pour ajouter un groupe d'utilisateurs.



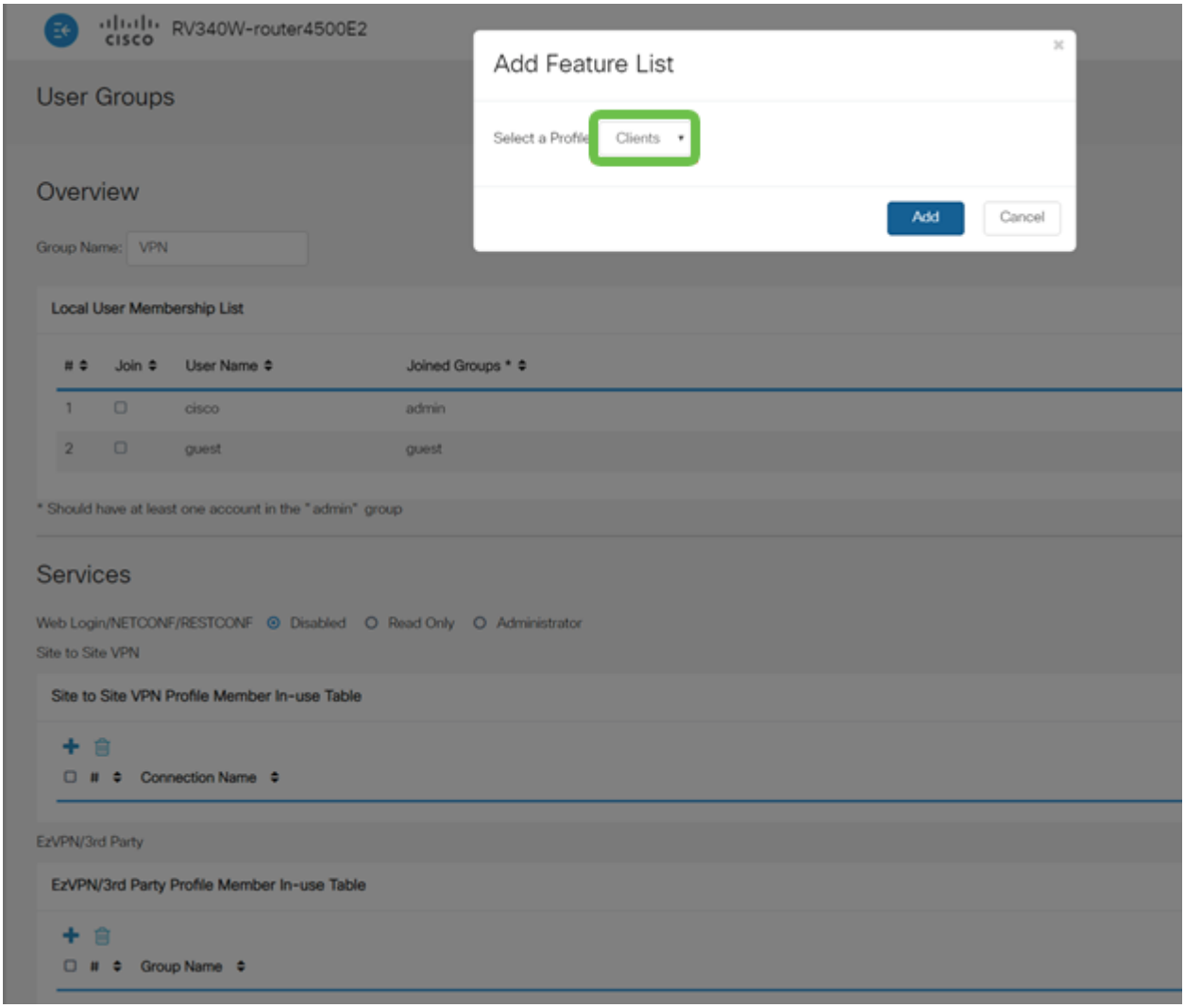

**Étape 9**

Entrez un **nom de groupe**.



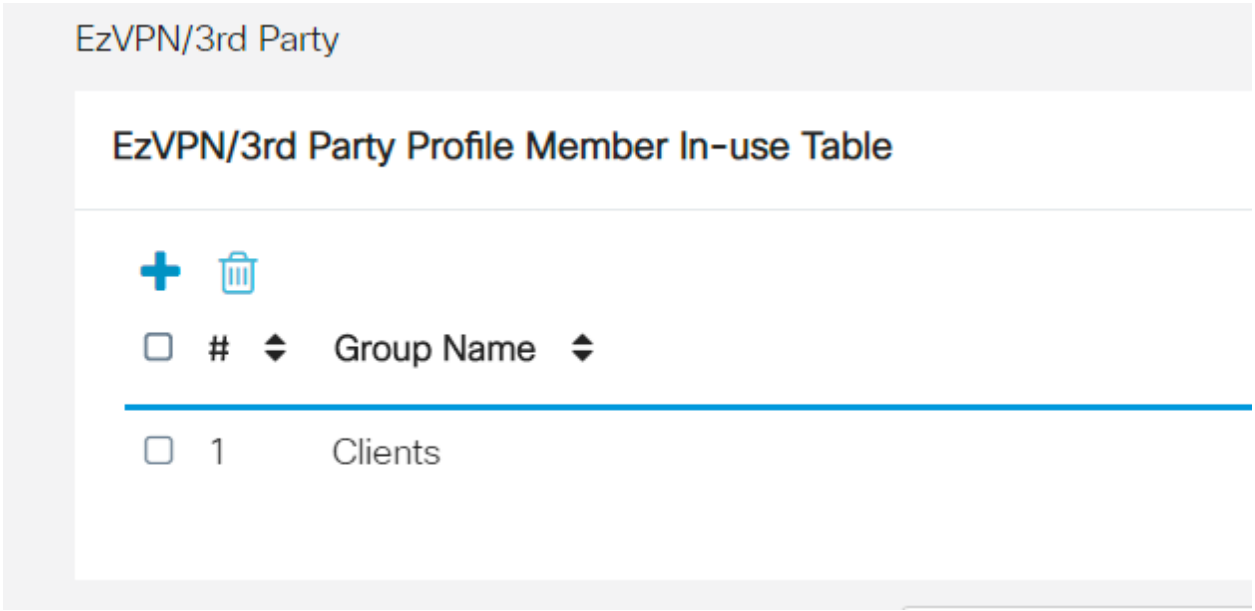

**Étape 10**

Sous **Services > EzVPN/tiers**, cliquez sur **Ajouter** pour lier ce groupe d'utilisateurs au profil **client-site** configuré précédemment.




**Étape 11**

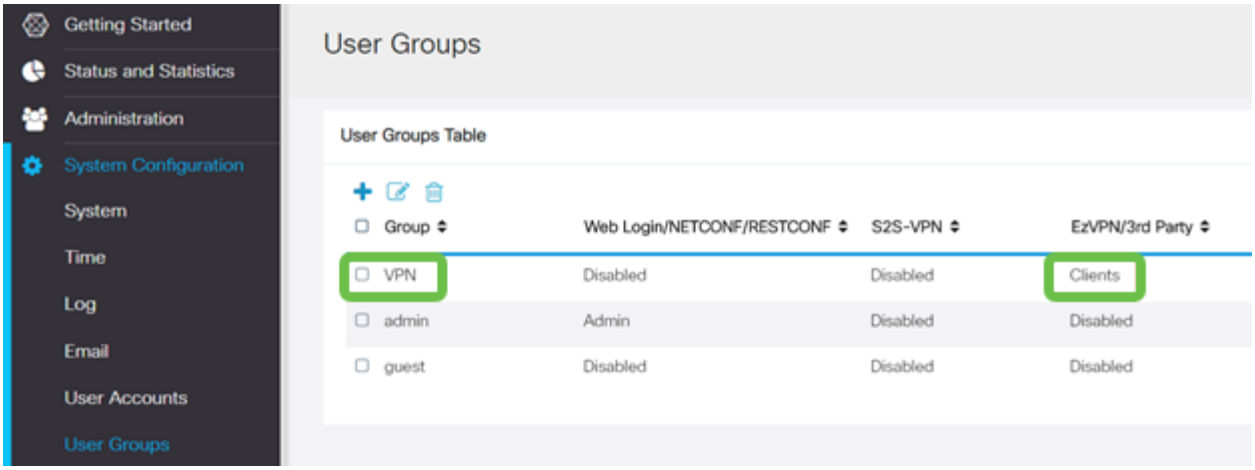
Vous devriez maintenant voir le nom du groupe **client-site** dans la liste pour **EzVPN/tiers.**




**Étape 12**

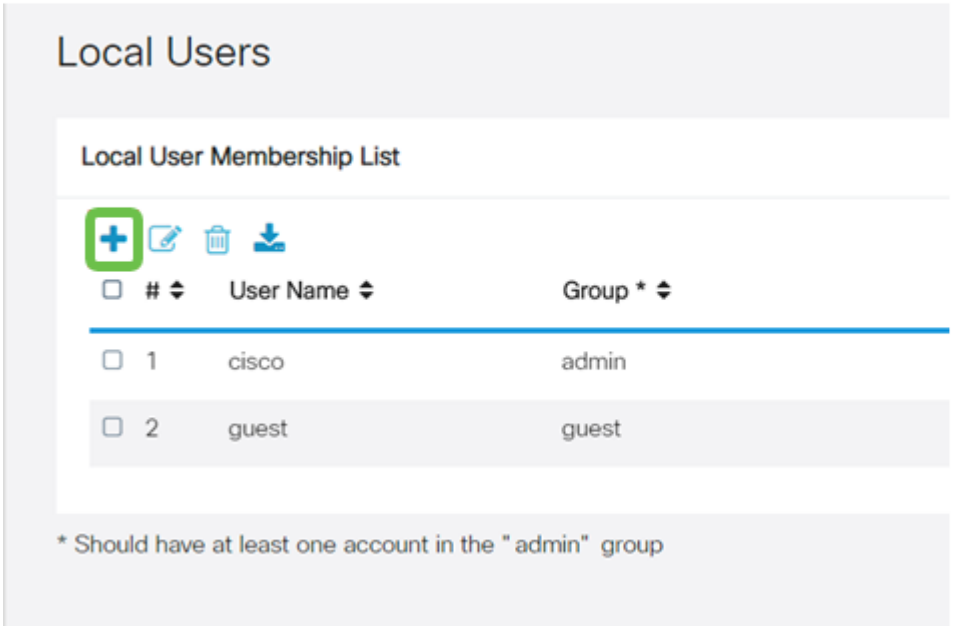
Après avoir **appliqué** la configuration du groupe d'utilisateurs, vous la verrez dans la liste **Groupes d'utilisateurs** et vous verrez que le nouveau groupe d'utilisateurs sera

utilisé avec le profil client-site que vous avez créé précédemment.



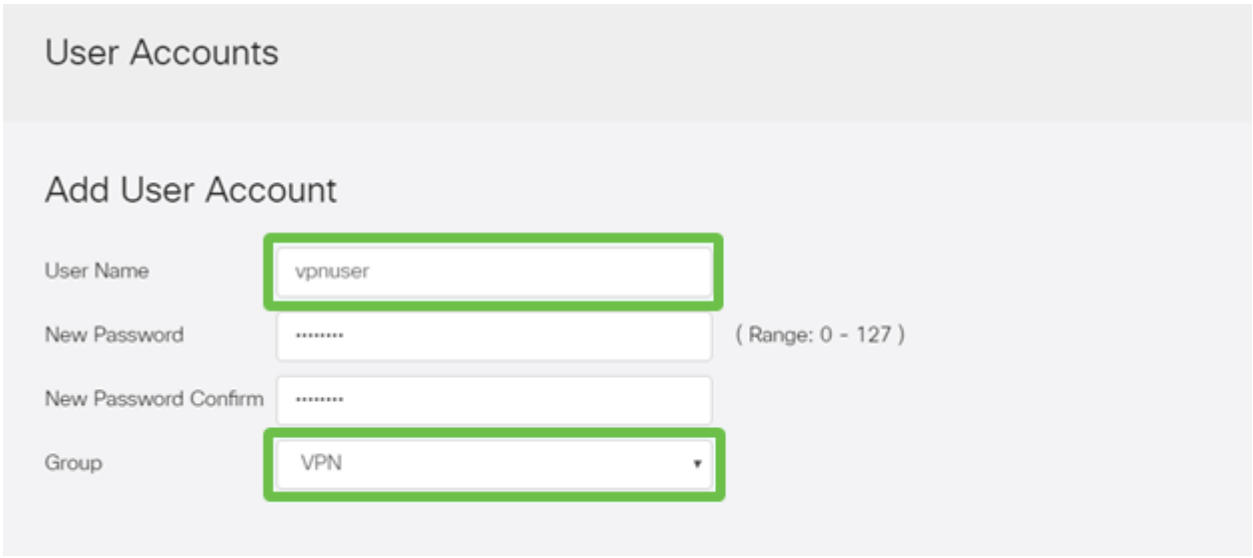

**Étape 13**

Configurez un nouvel utilisateur dans **Configuration système > Comptes d'utilisateurs**. Cliquez sur l'**icône plus** pour créer un nouvel utilisateur.



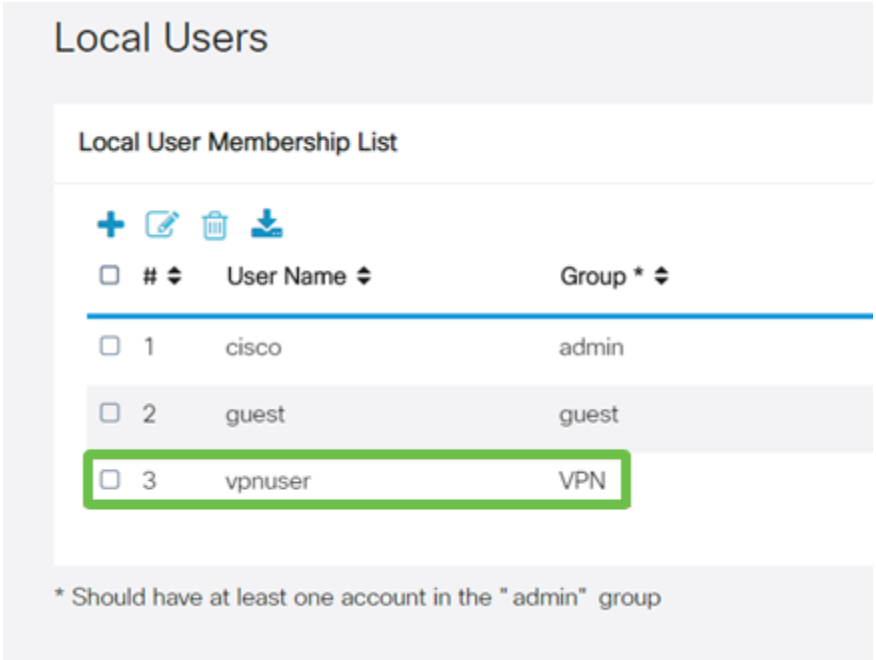

**Étape 14**

Entrez le nouveau **nom d'utilisateur** ainsi que le **nouveau mot de passe**. Vérifiez que le **groupe** est défini sur le nouveau **groupe d'utilisateurs** que vous venez de configurer. Cliquez sur **Apply** lorsque vous avez terminé.




### Étape 15

Le nouvel **utilisateur** apparaîtra dans la liste des **utilisateurs locaux**.




La configuration du routeur de la gamme RV345P est terminée. Ensuite, vous allez configurer le client VPN logiciel Shrew.

## Configurer le client VPN logiciel Shrew

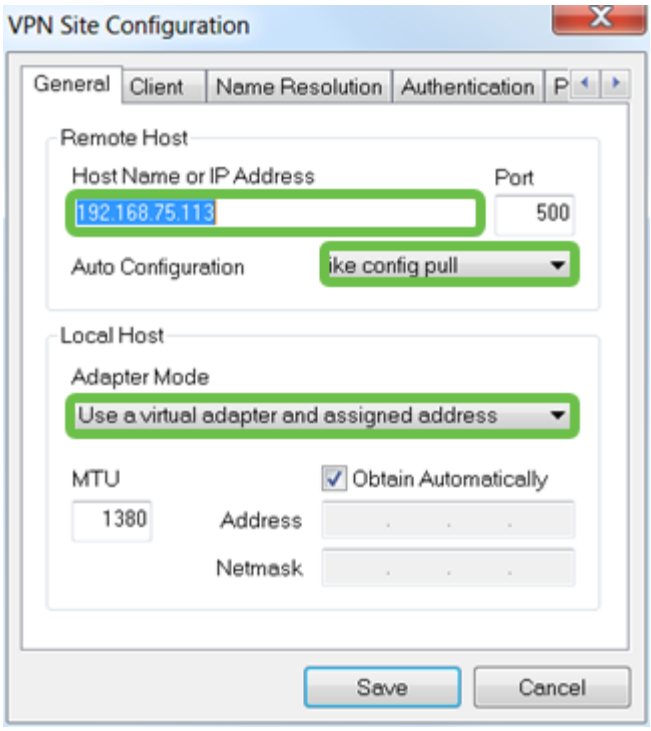
Procédez comme suit.

### Étape 1

Ouvrez Shrew Soft *VPN Access Manager* et cliquez sur **Add** pour ajouter un profil. Dans la fenêtre *Configuration du site VPN* qui s'affiche, configurez l'onglet **Général** :

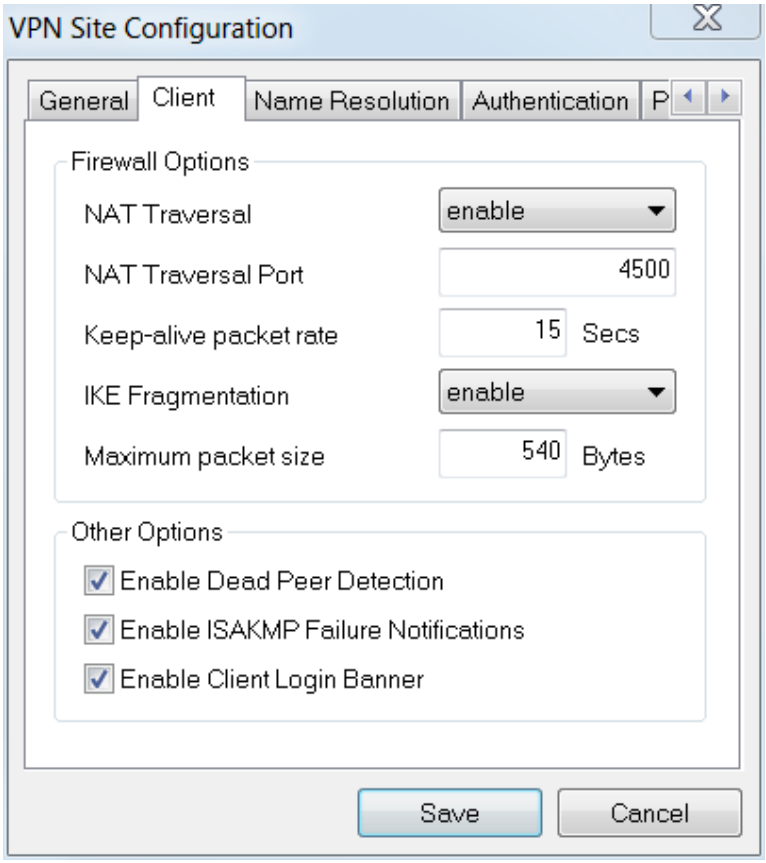
- **Nom d'hôte ou adresse IP** : Utiliser l'adresse IP WAN (ou le nom d'hôte du routeur RV345P)
- **Configuration automatique** : Sélectionner **comme configuration pull**

- **Mode adaptateur** : Sélectionnez **Utiliser une carte virtuelle et l'adresse attribuée**



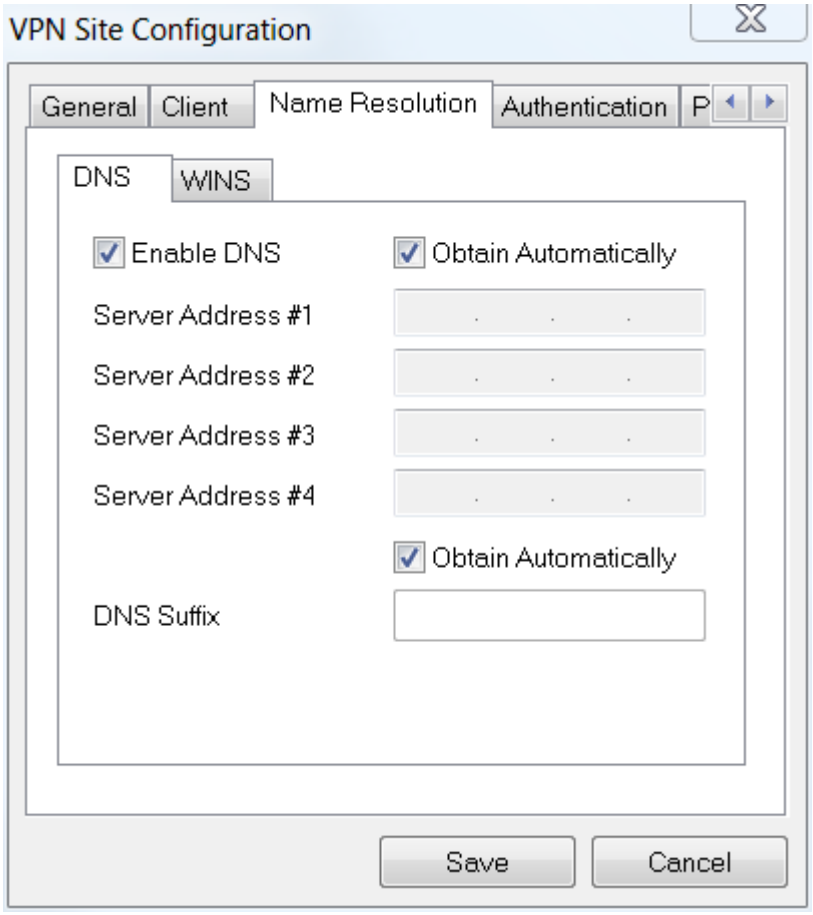

## Étape 2

Configurez l'onglet **Client**. Dans cet exemple, nous avons conservé les paramètres par défaut.



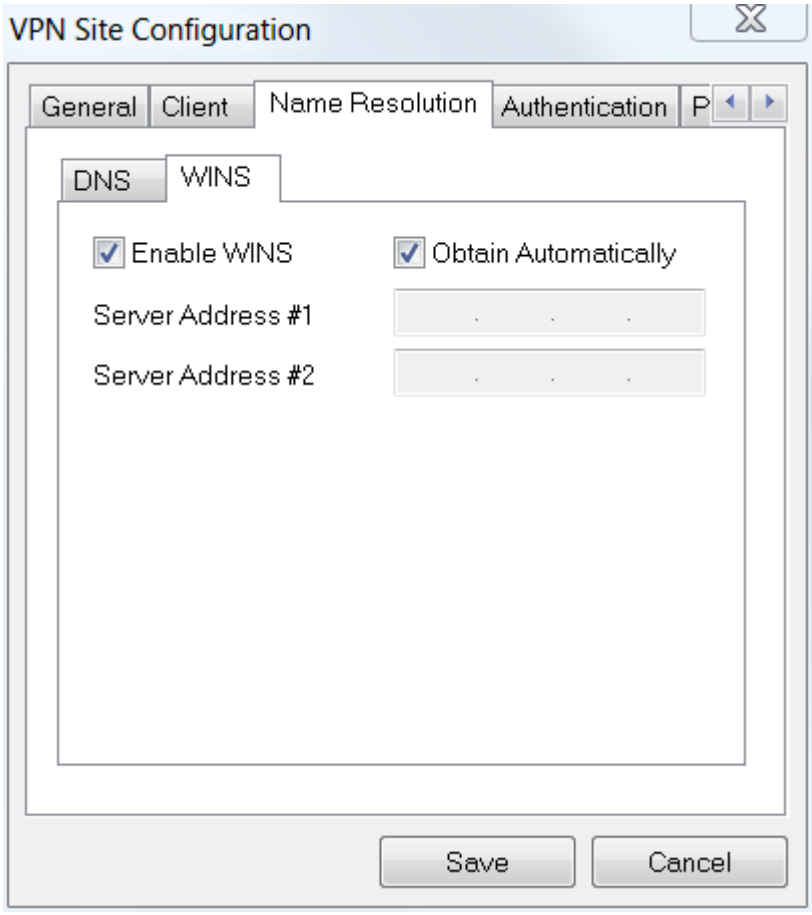

## Étape 3

Sous **Résolution de noms > DNS**, cochez la case **Activer DNS** et laissez les cases **Obtain Automatically** cochées.




**Étape 4**

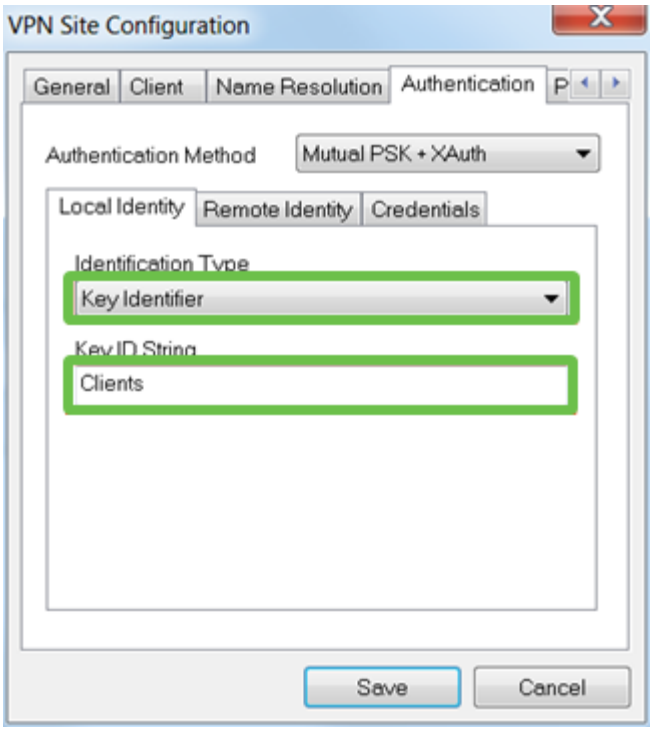
Sous l'onglet **Résolution de noms > WINS**, cochez la case **Activer WINS** et laissez la case **Obtenir automatiquement** cochée.




**Étape 5**

Cliquez sur **Authentication > Local Identity**.

- **Type d'identification** : Sélectionner **l'identificateur de clé**
- **Chaîne d'ID de clé** : Entrez le **nom de groupe** configuré sur le RV345P

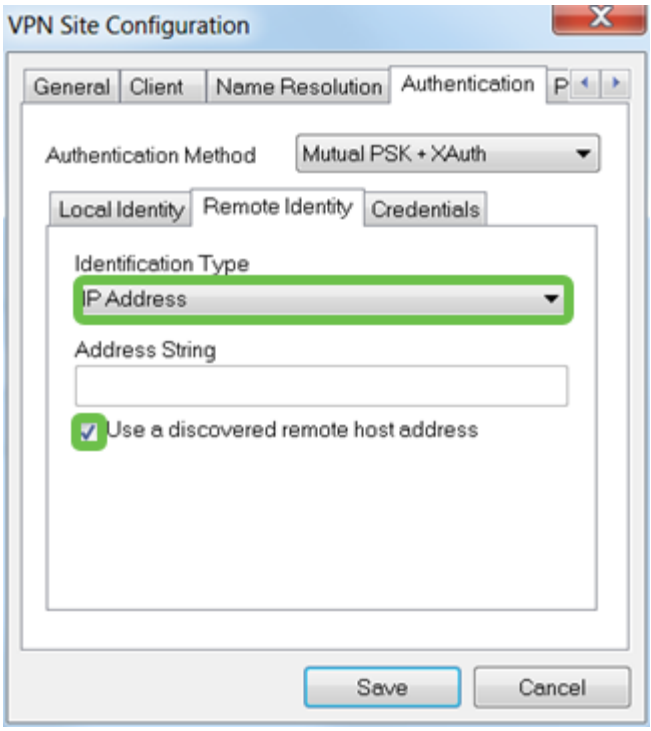



**Étape 6**

Sous **Authentication > Remote Identity**. Dans cet exemple, nous avons conservé les

paramètres par défaut.

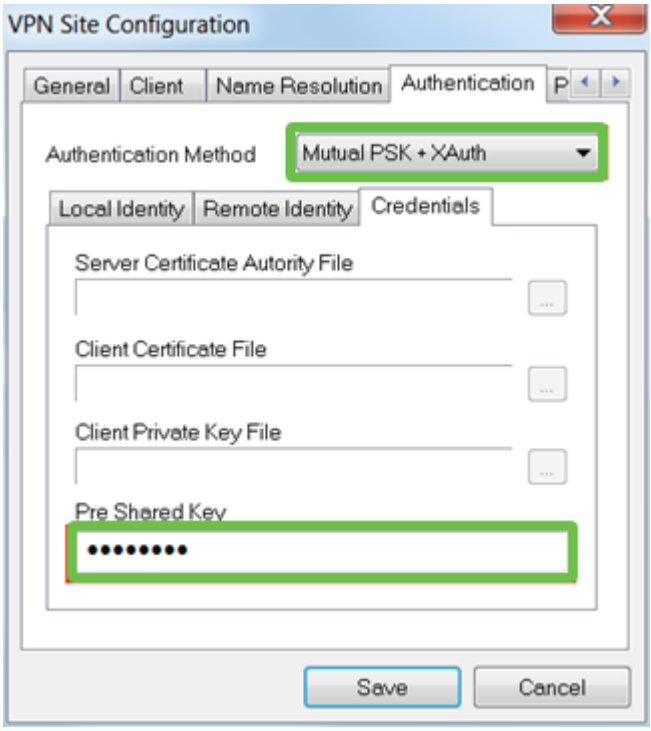
- **Type d'identification** : Adresse IP
- **Chaîne d'adresses** : <vierge>
- **Utilisez une** zone **d'adresse d'hôte distant découverte** : Coché




**Étape 7**

Sous **Authentification > Informations d'identification**, configurez les éléments suivants :

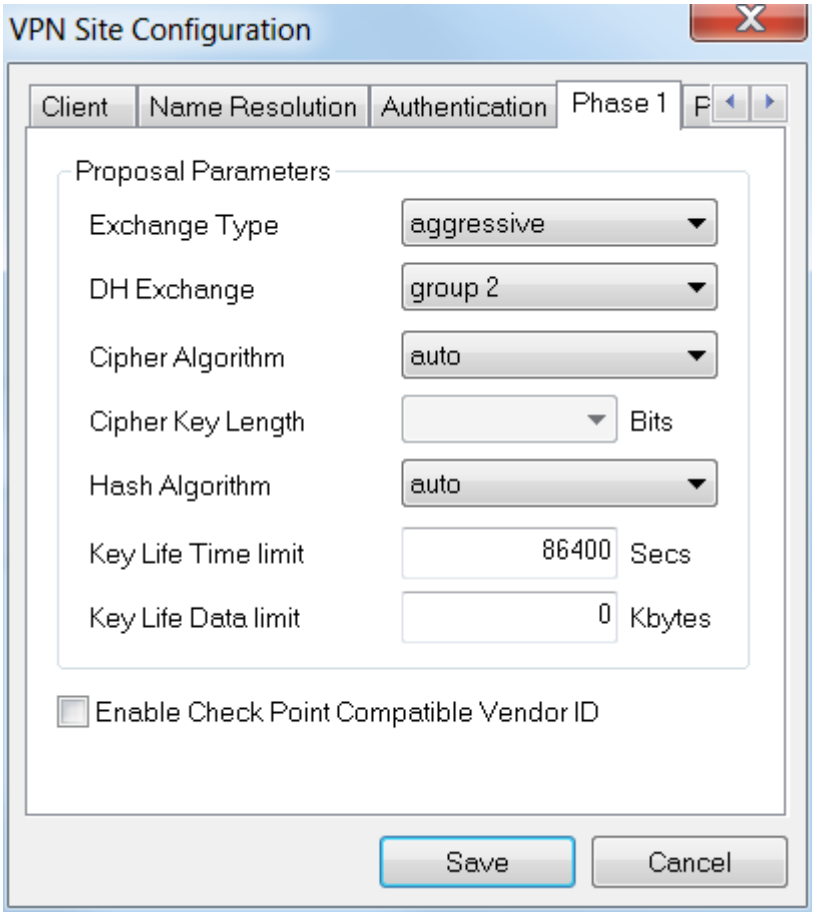
- **Méthode d'authentification** : Sélectionner **PSK mutuel + XAuth**
- **Clé pré-partagée** : Entrez la **clé prépartagée** configurée dans le profil client RV345P




**Étape 8**

Pour l'onglet **Phase 1**. Dans cet exemple, les paramètres par défaut ont été conservés :

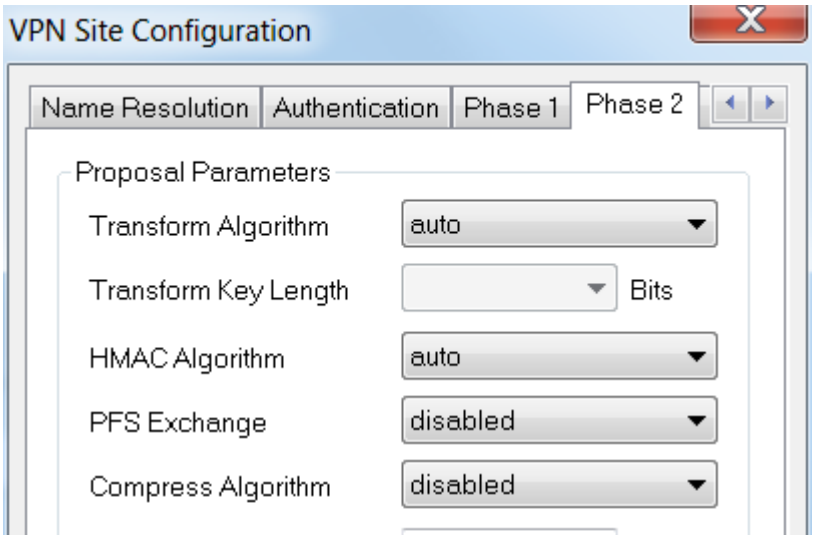
- **Type d'échange :** agressif
- **Échange DH :** groupe 2
- **Algorithme de chiffrement :** Auto
- **Algorithme de hachage :** Auto




**Étape 9**

Dans cet exemple, les valeurs par défaut de l'onglet **Phase 2** ont été conservées.

- **Algorithme de transformation :** Auto
- **Algorithme HMAC :** Auto
- **Échange PFS :** Désactivé
- **Algorithme de compression :** Désactivé

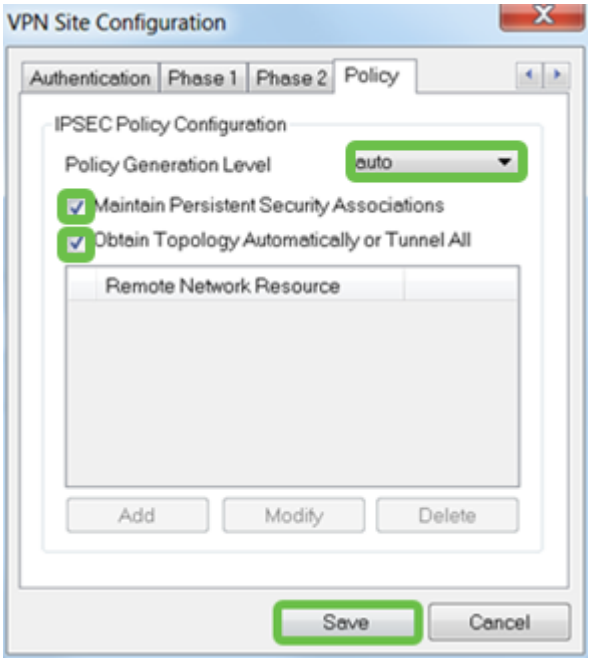


## Étape 10

Pour l'exemple d'onglet **Stratégie**, nous avons utilisé les paramètres suivants :

- **Niveau de génération de stratégie :** Auto
- **Tenir À Jour Les Associations De Sécurité Persistantes :** Coché
- **Obtenir la topologie automatiquement ou tout tunnel :** coché

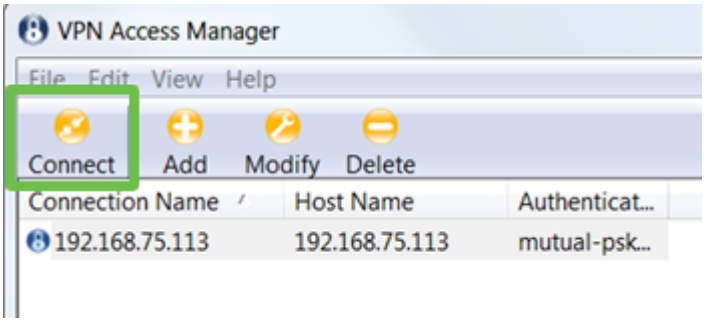
Puisque nous avons configuré la **transmission tunnel partagée** sur le RV345P, nous n'avons pas besoin de la configurer ici.




Une fois terminé, cliquez sur Save (enregistrer).

## Étape 11

Vous êtes maintenant prêt à tester la connexion. Dans *VPN Access Manager*, mettez en surbrillance le profil de connexion et cliquez sur le bouton **Connect**.

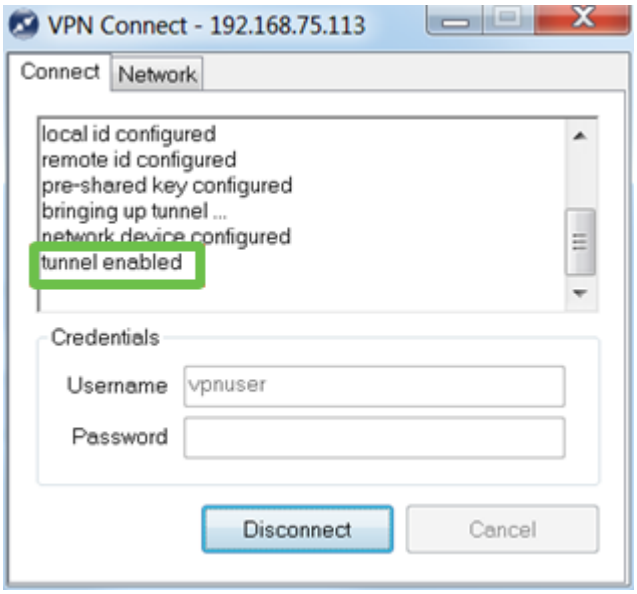



## Étape 12

Dans la fenêtre **VPN Connect** qui apparaît, entrez le **nom d'utilisateur** et le **mot de passe** à l'aide des informations d'identification du **compte d'utilisateur** que vous avez créé sur le RV345P (étapes 13 et 14). Lorsque vous avez terminé, cliquez sur **Connect** .


**Étape 13**

Vérifiez que le tunnel est connecté. Le **tunnel** doit être **activé**.




Shrew Soft a été utilisé comme exemple dans cette configuration. Comme Shrew Soft n'est pas un produit Cisco, veuillez contacter ce tiers si vous avez besoin d'assistance technique.

## Autres options VPN

Il existe d'autres options pour utiliser un VPN. Pour plus d'informations, cliquez sur les liens suivants :

- Utiliser le client VPN TheGreenBow pour se connecter avec un routeur de la gamme RV34x
- Configuration d'un client VPN de télétravailleur sur le routeur de la gamme RV34x
- Configurer un serveur PPTP (Point-to-Point Tunneling Protocol) sur le routeur de la gamme Rv34x
- Configurer un profil de sécurité IPsec (Internet Protocol Security) sur un routeur de la

gamme RV34x
- Configuration des paramètres WAN L2TP sur le routeur RV34x
- Configuration du VPN site à site sur le RV34x

# Configurations supplémentaires sur le routeur RV345P

## Configuration des VLAN (facultatif)

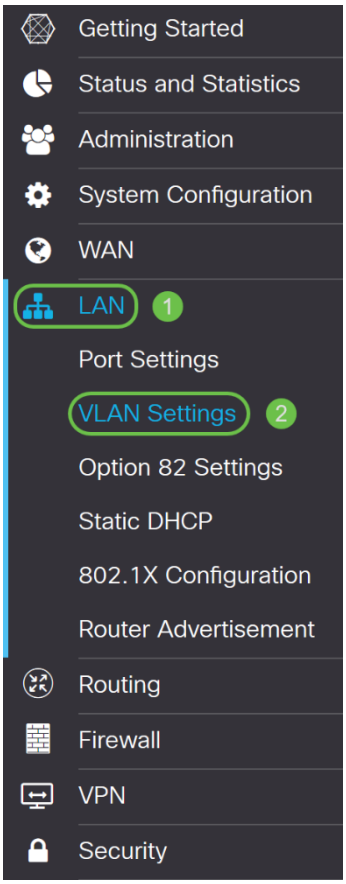
Un réseau local virtuel (VLAN) vous permet de segmenter logiquement un réseau local (LAN) en différents domaines de diffusion. Dans les scénarios où des données sensibles peuvent être diffusées sur un réseau, des VLAN peuvent être créés pour améliorer la sécurité en désignant une diffusion à un VLAN 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.

Vous pouvez consulter les Méthodes Recommandées et les conseils de sécurité pour obtenir des conseils supplémentaires.

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

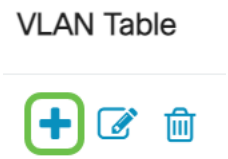
### Étape 1

Accédez à **LAN > VLAN Settings**.



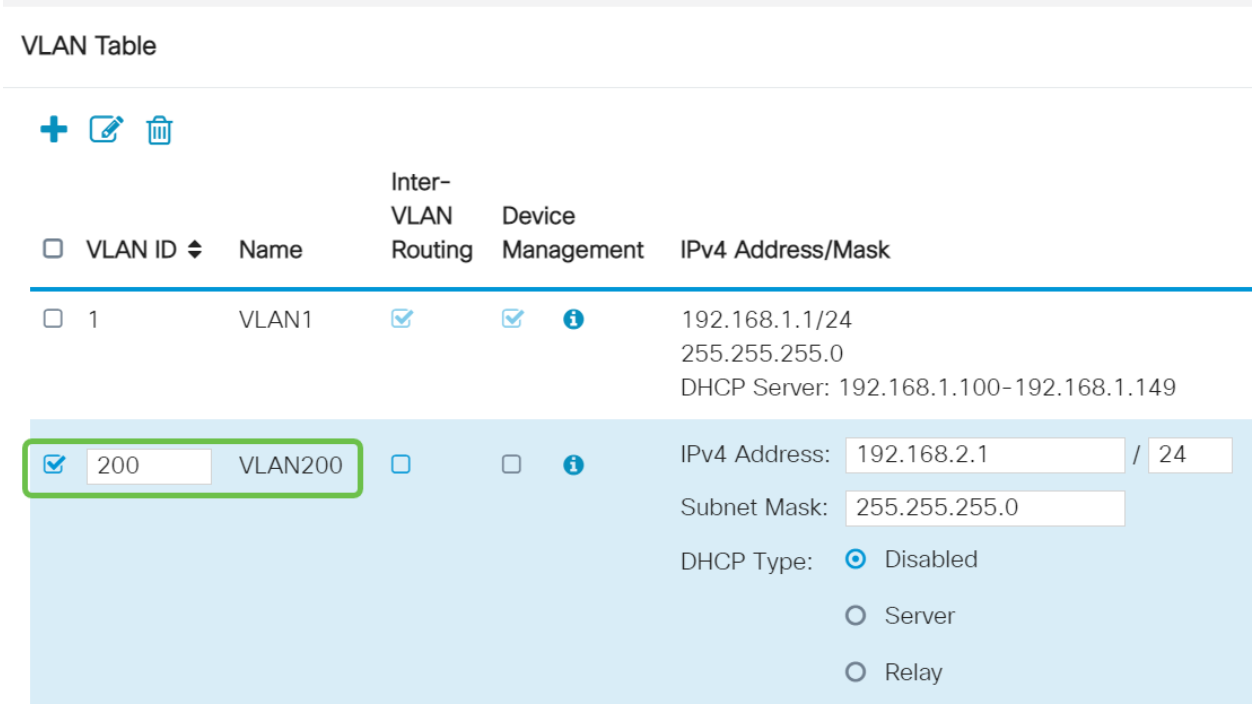
## Étape 2

Cliquez sur l'**icône Ajouter** 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.



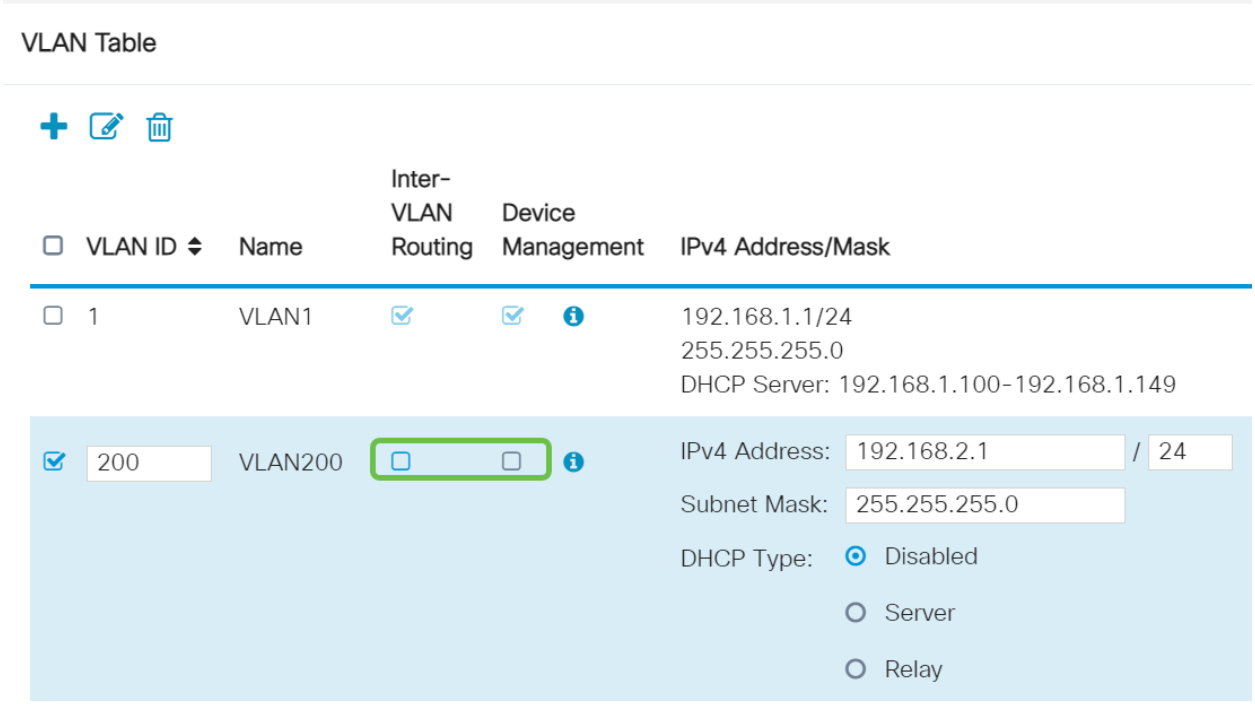

## Étape 4

**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.

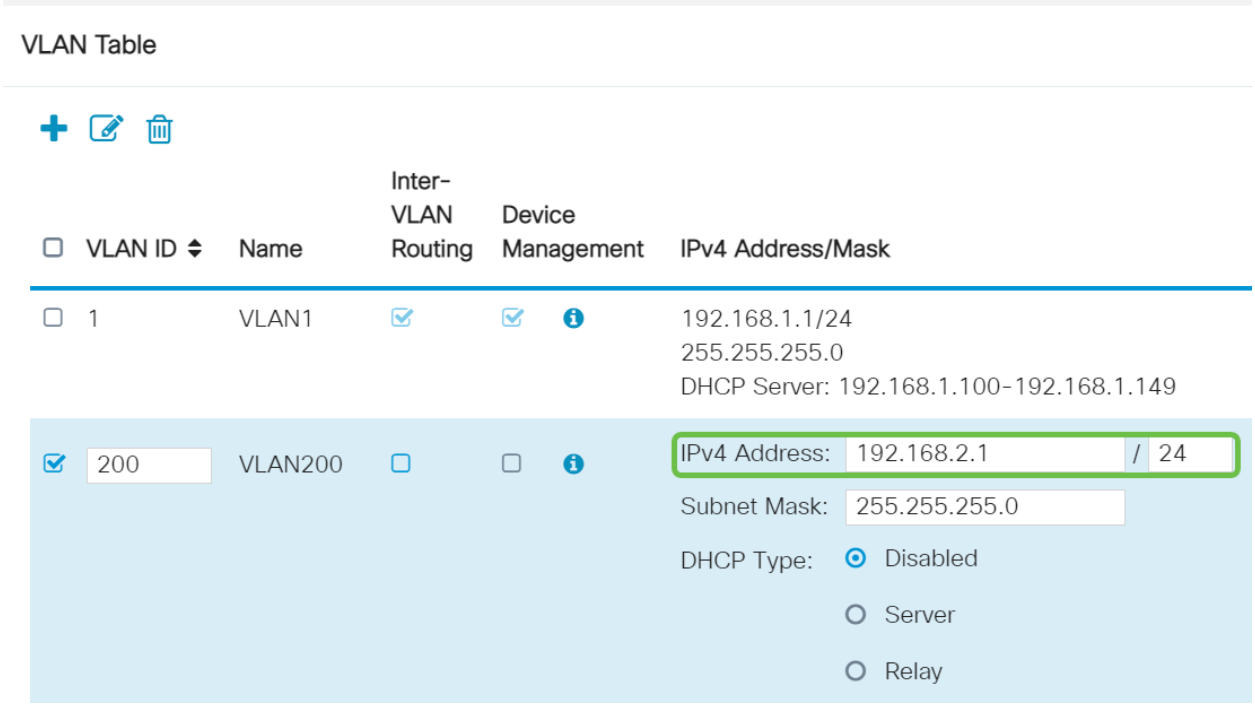
Device Management est le logiciel qui vous permet d'utiliser votre navigateur pour vous connecter à l'interface utilisateur Web du RV345P, à partir du VLAN, et de gérer le RV345P. Ceci doit également être désactivé sur les réseaux invités.

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.

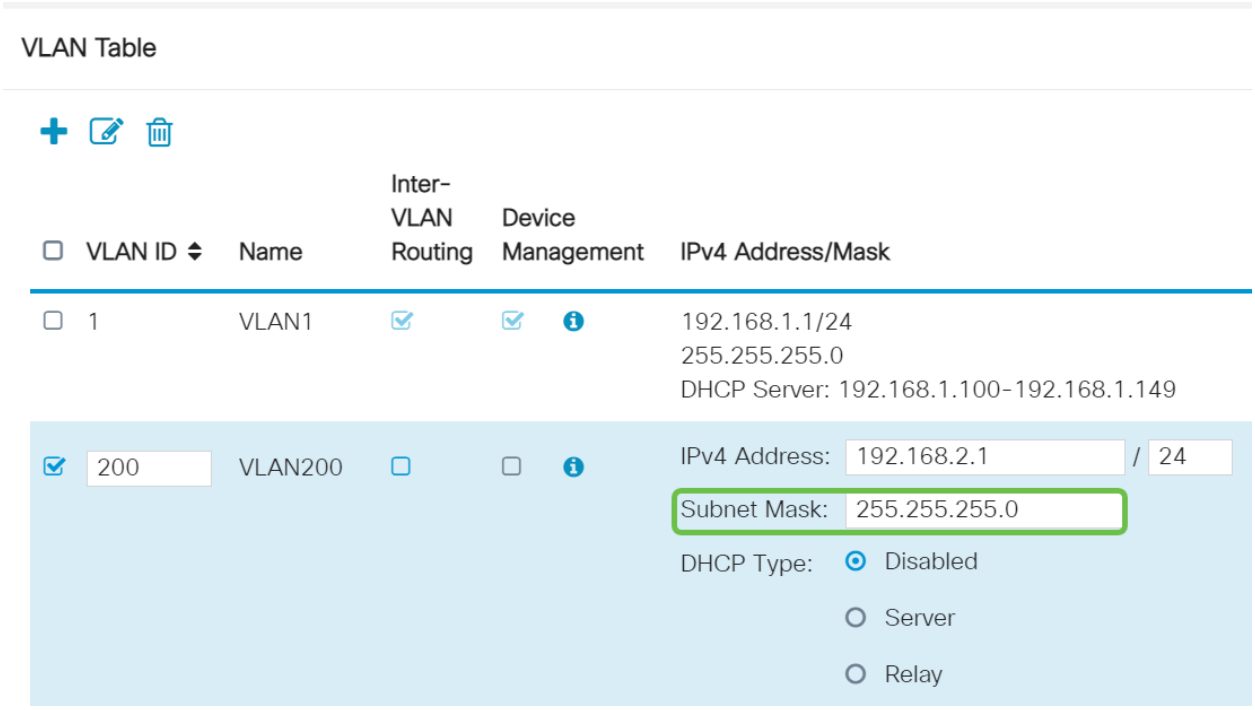



## Étape 6

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**.



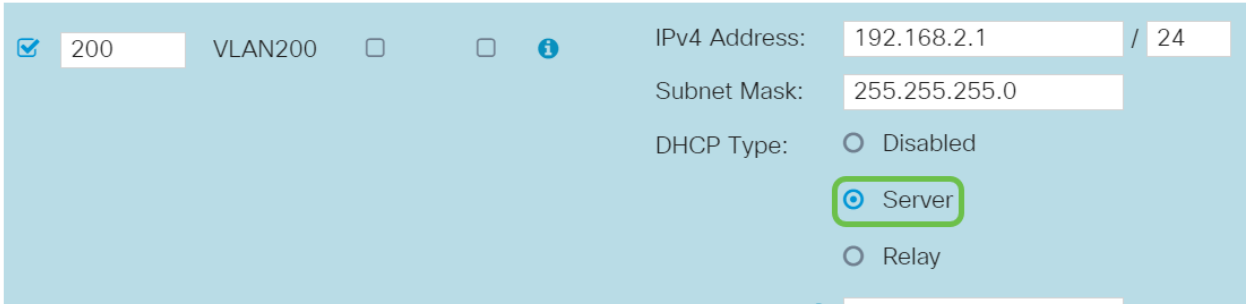

## Étape 7

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.

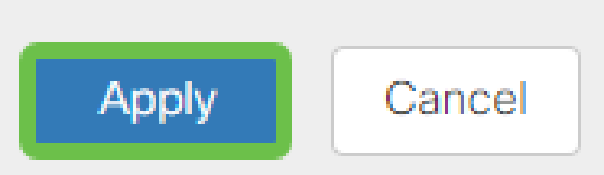
*Serveur* : option la plus souvent utilisée.

- 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 (facultatif)

16 VLAN peuvent être configurés sur le routeur RV345P, 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 non étiqueté. Les VLAN que vous ne voulez pas sur l'agrégation doivent être exclus.

Un VLAN a attribué son propre port :

- Considéré comme un port d'accès.
- Le VLAN attribué 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 :

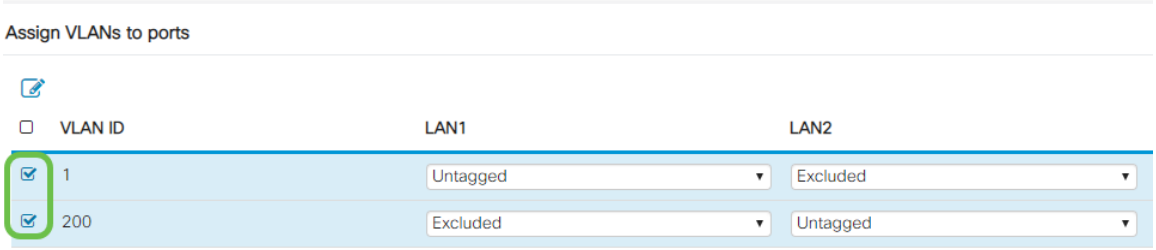
- Considéré comme un port agrégé.
- Un des VLAN peut être étiqueté Untagged.
- Les autres VLAN qui font partie du port agrégé doivent être étiquetés Tagged.
- Les VLAN qui ne font pas partie du port agrégé doivent être étiquetés Excluded pour ce port.

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

### Étape 1

Sélectionnez les *ID de VLAN* à modifier.

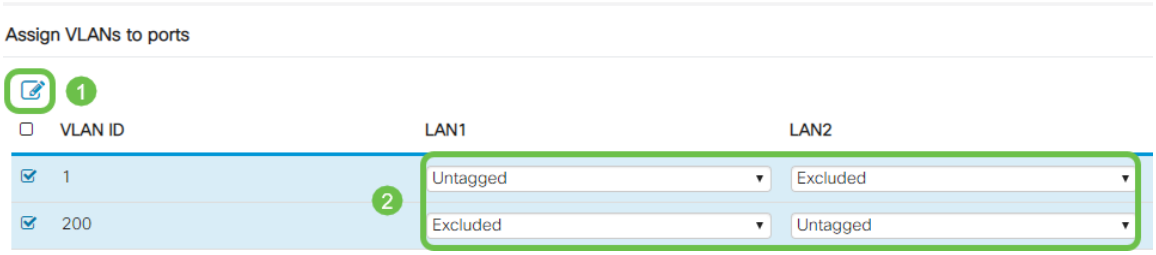
Dans cet exemple, nous avons sélectionné *VLAN 1* et *VLAN 200*.




### Étape 2

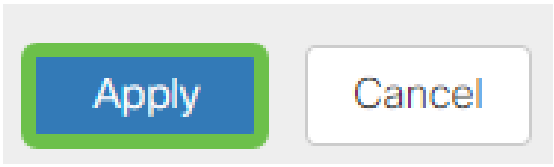
Cliquez sur **Edit** pour affecter un VLAN à un port LAN et spécifiez chaque paramètre comme *Tagged*, *Untagged* ou *Excluded*.

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 3

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




Vous devez maintenant avoir créé un nouveau VLAN et configuré les VLAN sur les ports du RV345P. 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.

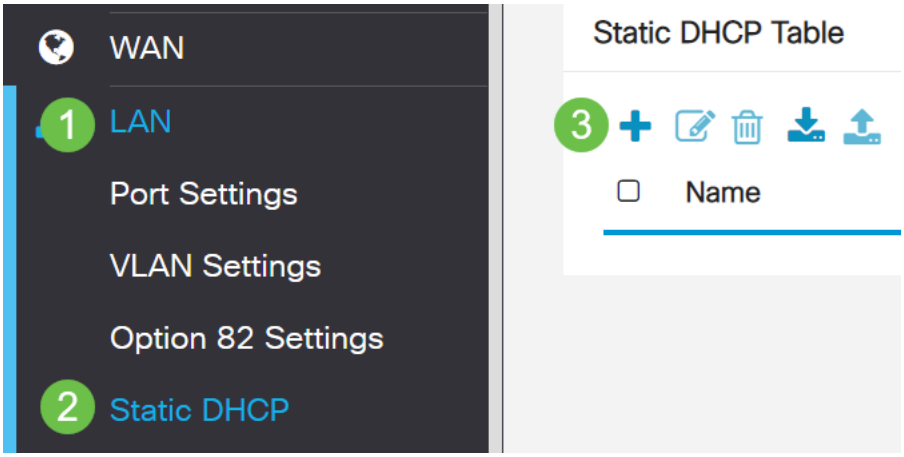
## Ajouter une adresse IP statique (facultatif)

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.

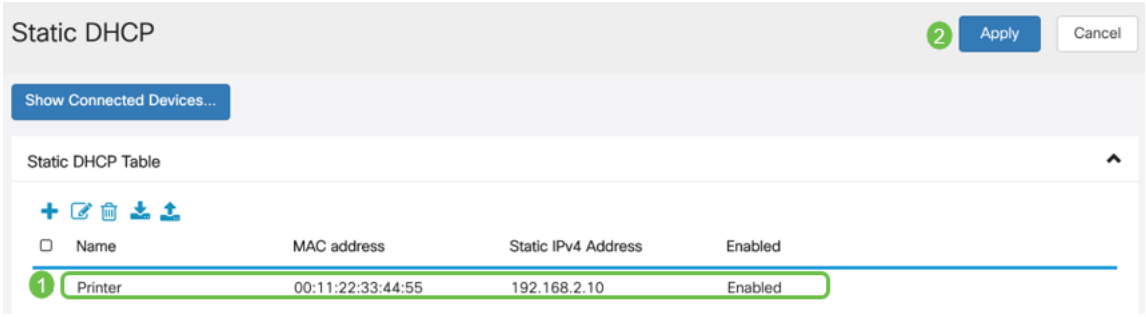
### Étape 1

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.




## Gestion des certificats (facultatif)

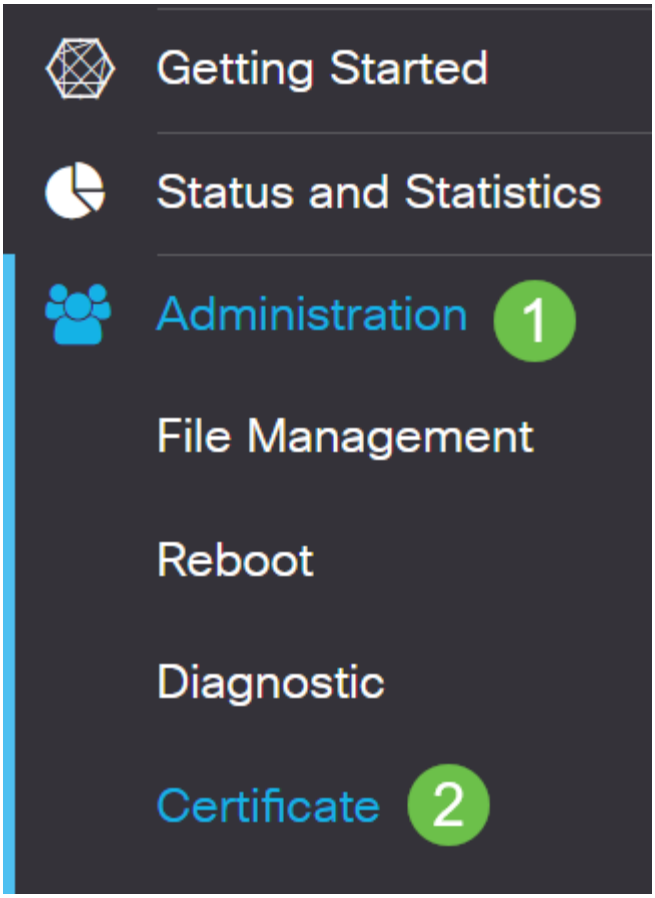
Un certificat numérique certifie la propriété d'une clé publique par l'objet nommé du certificat. Cela permet aux parties de confiance de dépendre des signatures ou des assertions faites par la clé privée qui correspond à la clé publique qui est certifiée. Un routeur peut générer un certificat auto-signé, un certificat créé par un administrateur réseau. Il peut également envoyer des demandes aux autorités de certification (AC) pour demander un certificat d'identité numérique. Il est important d'avoir des certificats légitimes provenant de demandes tierces.

Une autorité de certification (CA) est utilisée pour l'authentification. Les certificats peuvent être achetés sur n'importe quel site tiers. C'est un moyen officiel de prouver que votre site est sécurisé. Essentiellement, l'AC est une source fiable qui vérifie que vous êtes une entreprise légitime et qu'elle peut être approuvée. Selon vos besoins, un certificat à un coût minime. Vous êtes extrait par l'autorité de certification, et une fois qu'ils vérifient vos informations, ils vous délivrent le certificat. Ce certificat peut être téléchargé sous forme de fichier sur votre ordinateur. Vous pouvez ensuite accéder à votre routeur (ou à votre serveur VPN) et le télécharger ici.

### Générer CSR/Certificat

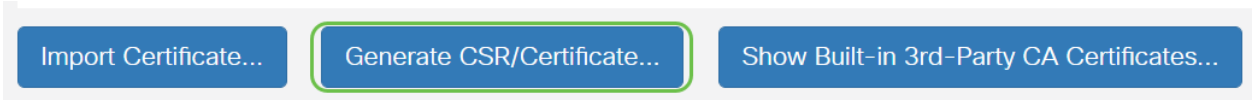
### Étape 1

Connectez-vous à l'utilitaire Web du routeur et sélectionnez **Administration > Certificate** .




**Étape 2**

Cliquez sur **Générer CSR/Certificate**. Vous accéderez à la page Generate CSR/Certificate.



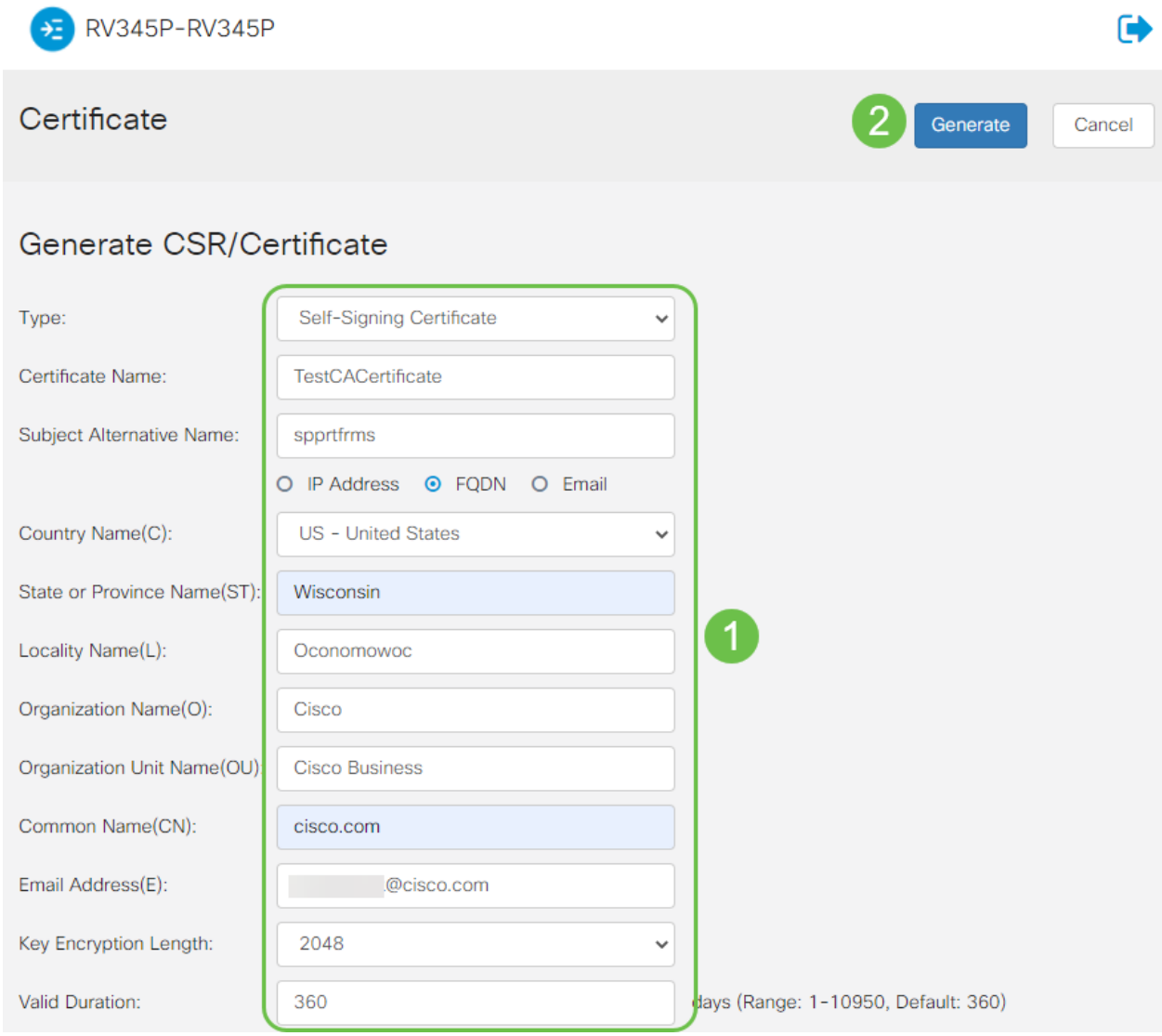

**Étape 3**

Remplissez les zones suivantes :

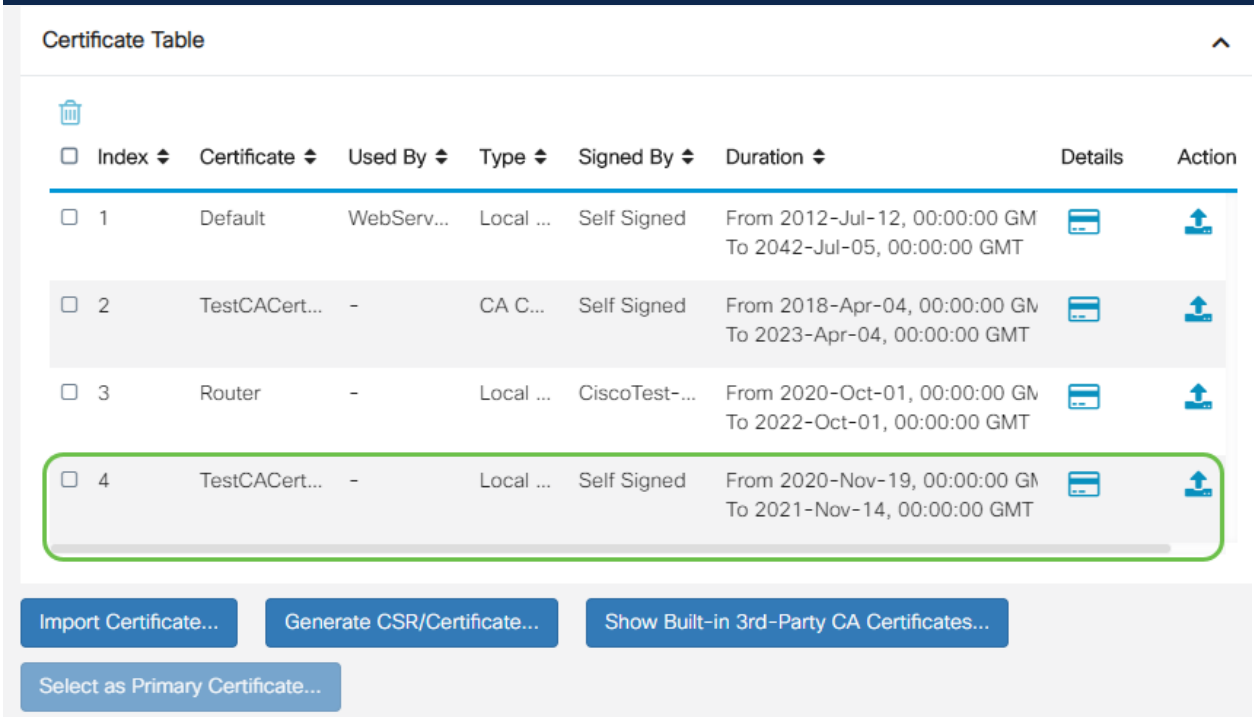
- Choisissez le type de certificat approprié
  - Certificat auto-signant : certificat SSL (Secure Socket Layer) signé par son créateur. Ce certificat est moins fiable, car il ne peut pas être annulé si la clé privée est compromise d'une manière ou d'une autre par un pirate.
  - Demande de signature certifiée — Il s'agit d'une infrastructure à clé publique (ICP) qui est envoyée à l'autorité de certification pour demander un certificat d'identité numérique. Il est plus sécurisé que autosigné car la clé privée est gardée secrète.
- Entrez un nom pour votre certificat dans le champ Nom du certificat pour identifier la demande. Ce champ ne peut pas être vide ni contenir d'espaces et de caractères spéciaux.
- (Facultatif) Sous la zone Nom alternatif de l'objet, cliquez sur une case d'option. Les options sont les suivantes :
  - IP Address : saisissez une adresse IP (Internet Protocol).
  - FQDN : saisissez un nom de domaine complet (FQDN)

    - E-mail : saisissez une adresse e-mail

- Dans le champ Subject Alternative Name, saisissez le nom de domaine complet (FQDN).
- Choisissez un nom de pays dans lequel votre organisation est légalement enregistrée dans la liste déroulante Nom du pays.
- Entrez un nom ou une abréviation de l'état, de la province, de la région ou du territoire où se trouve votre organisation dans le champ State or Province Name(ST).
- Saisissez le nom de la localité ou de la ville dans laquelle votre organisation est enregistrée ou se trouve dans le champ Nom de la localité.
- Entrez un nom sous lequel votre entreprise est légalement enregistrée. Si vous vous inscrivez en tant que petite entreprise ou propriétaire unique, saisissez le nom du demandeur de certificat dans le champ Nom de l'organisation. Les caractères spéciaux ne peuvent pas être utilisés.
- Entrez un nom dans le champ Nom de l'unité d'organisation pour différencier les divisions d'une organisation.
- Entrez un nom dans le champ Common Name. Ce nom doit être le nom de domaine complet du site Web pour lequel vous utilisez le certificat.
- Saisissez l'adresse e-mail de la personne qui souhaite générer le certificat.
- Dans la liste déroulante Key Encryption Length, sélectionnez une longueur de clé. Les options sont 512, 1024 et 2048. Plus la longueur de la clé est grande, plus le certificat est sécurisé.
- Dans le champ Durée valide, saisissez le nombre de jours pendant lesquels le certificat sera valide. Il est défini par défaut à 360.
- Cliquez sur **Generate**.




Le certificat généré doit maintenant apparaître dans la table de certificats.

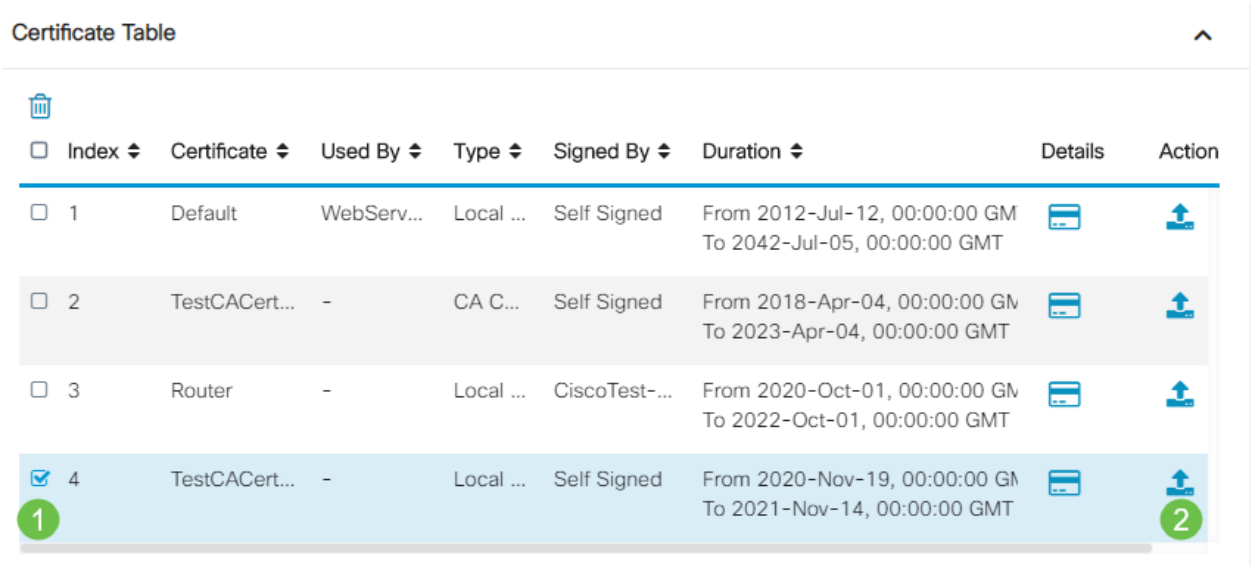


Vous devez maintenant avoir créé un certificat sur le routeur RV345P.

## Exporter un certificat

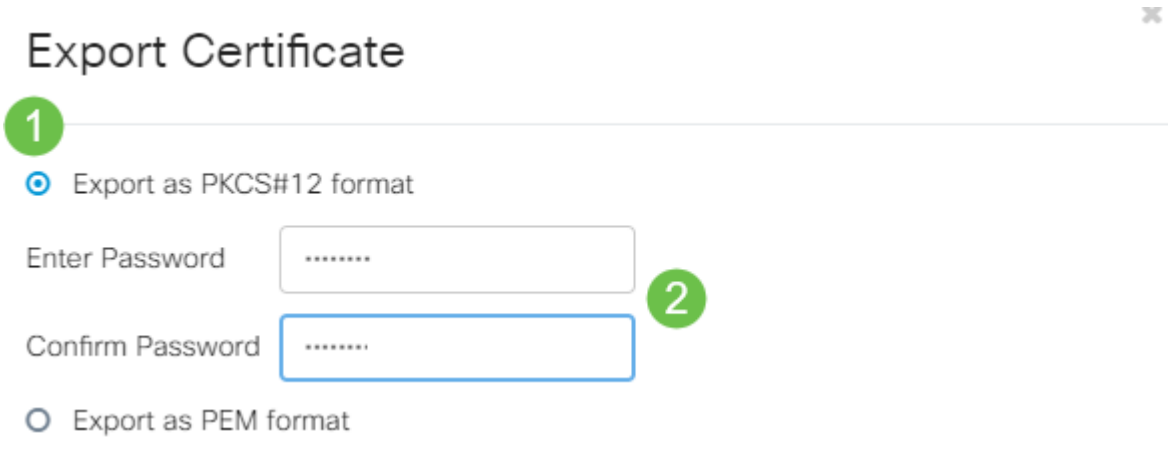
### Étape 1

Dans la table des certificats, cochez la case du certificat à exporter et cliquez sur l'**icône d'exportation**.



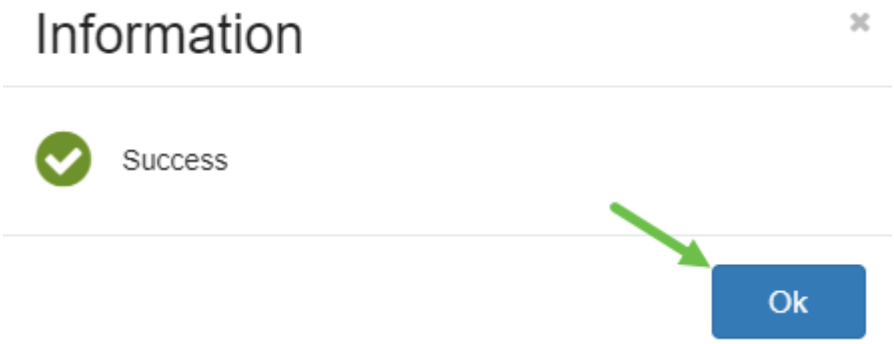

### Étape 2

- Cliquez sur un format pour exporter le certificat. Les options sont les suivantes :
  - PKCS #12 — Public Key Cryptography Standards (PKCS) #12 est un certificat exporté qui vient dans une extension .p12. Un mot de passe est nécessaire pour chiffrer le fichier afin de le protéger lors de son exportation, de son importation et de sa suppression.
  - PEM - La fonction PEM (Privacy Enhanced Mail) est souvent utilisée pour les serveurs Web afin qu'ils puissent être facilement traduits en données lisibles à l'aide d'un éditeur de texte simple tel que le bloc-notes.
- Si vous avez choisi PEM, cliquez simplement sur **Exporter**.
- Entrez un mot de passe pour sécuriser le fichier à exporter dans le champ Enter Password.
- Saisissez à nouveau le mot de passe dans le champ Confirmer le mot de passe.
- Dans la zone Sélectionner la destination, PC a été choisi et est la seule option actuellement disponible.
- Cliquez sur **Exporter**.



### Étape 3

Un message indiquant le succès du téléchargement apparaît sous le bouton Télécharger. Un fichier commence à être téléchargé dans votre navigateur. Click OK.

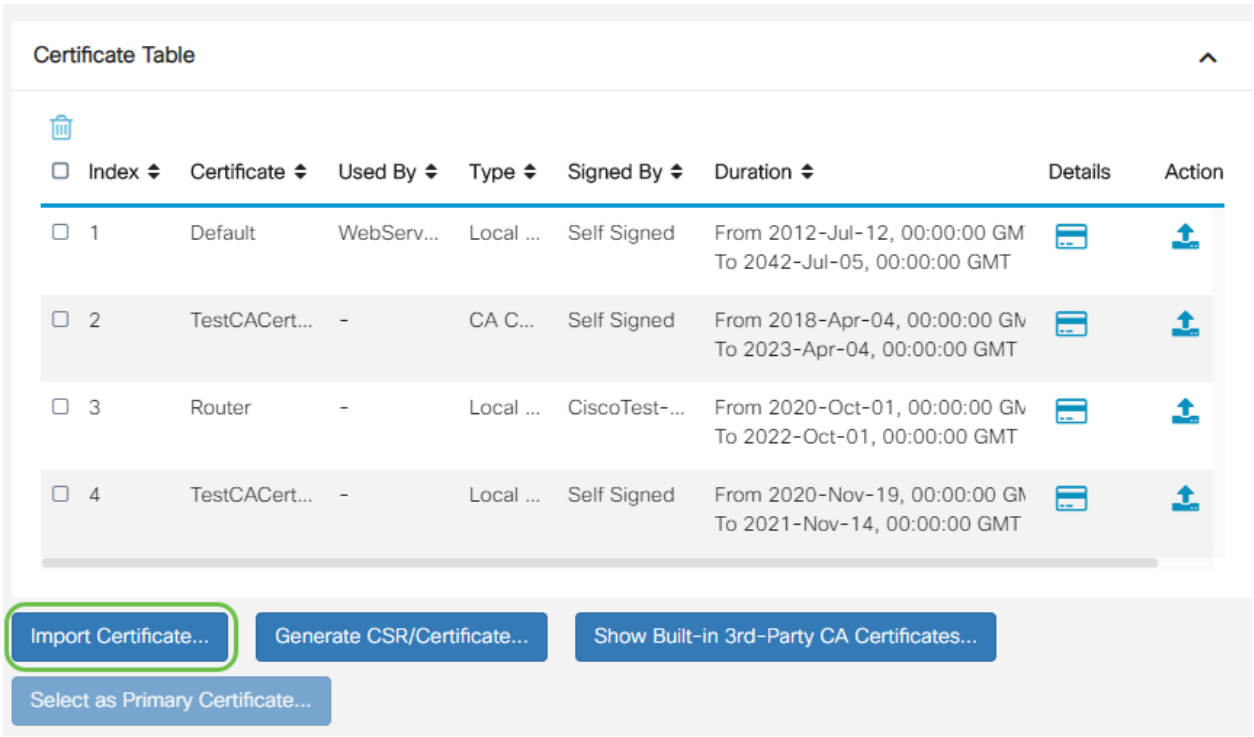



Vous devez maintenant avoir exporté un certificat sur le routeur de la gamme RV345P.

## Importer un certificat

### Étape 1

Cliquez sur **Importer un certificat...**.

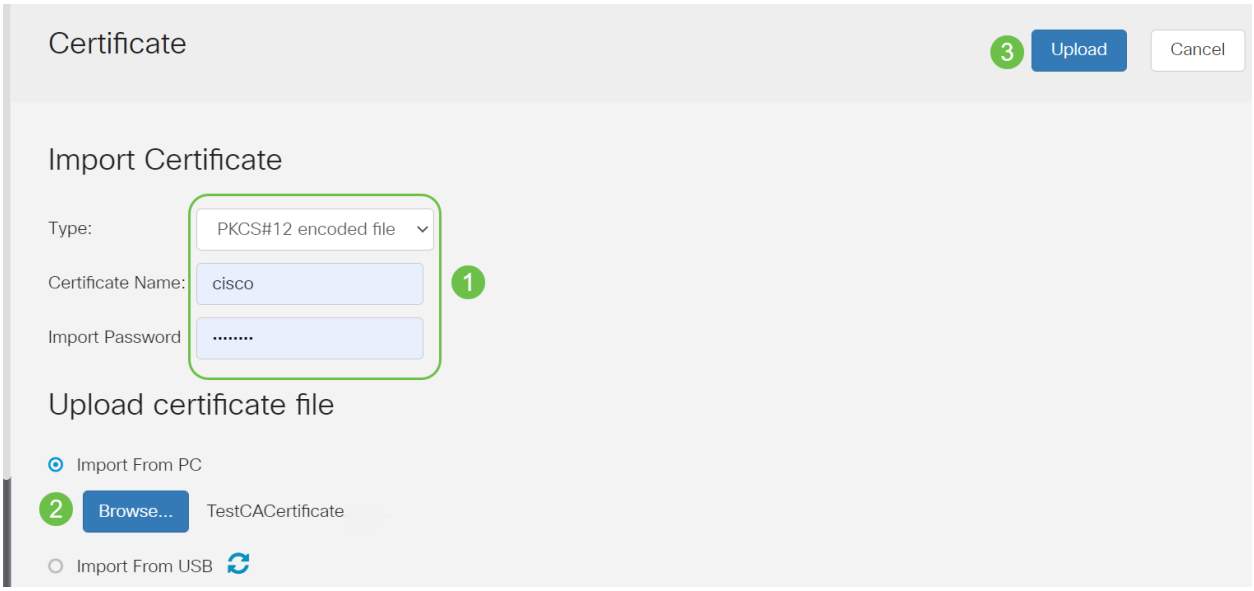



### Étape 2

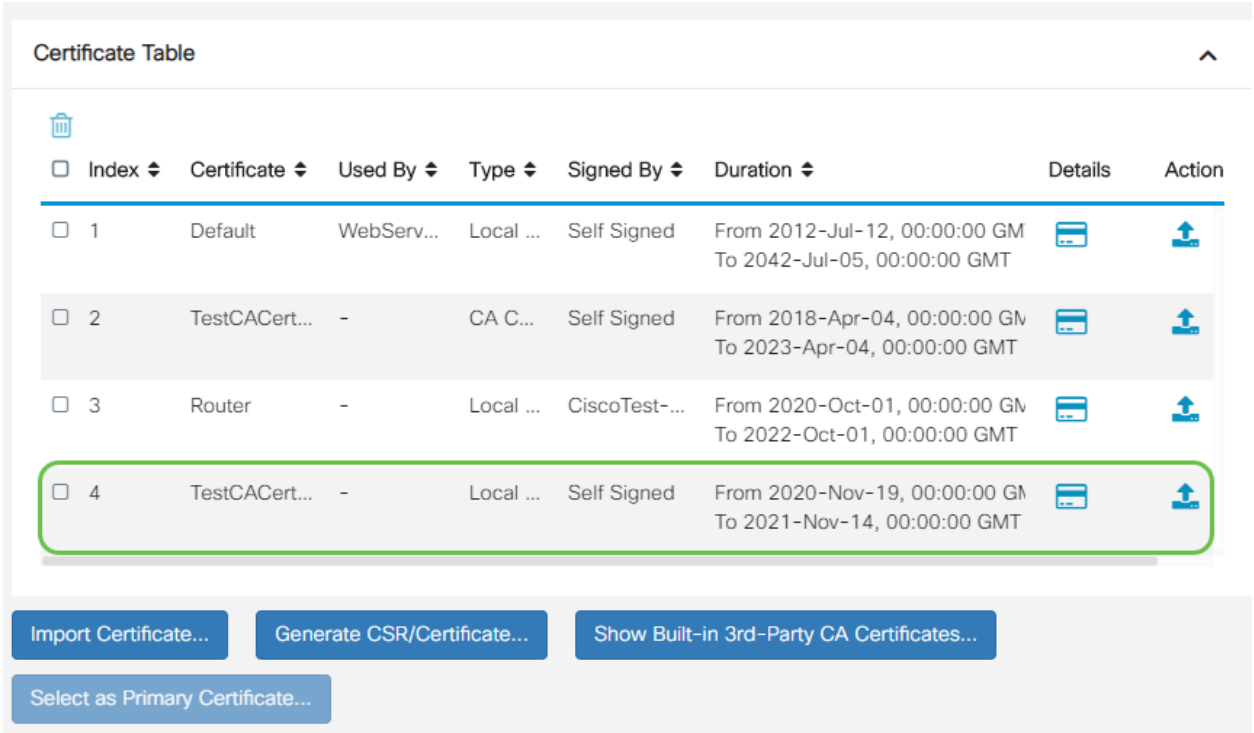
- Sélectionnez le type de certificat à importer dans la liste déroulante. Les options sont les suivantes :
  - Local Certificate : certificat généré sur le routeur.
  - Certificat CA — Certificat certifié par une autorité tierce de confiance qui a confirmé que les informations contenues dans le certificat sont exactes.
  - Fichier codé PKCS #12 — Les normes de cryptographie à clé publique (PKCS) #12 sont un format de stockage d'un certificat de serveur.

- Entrez un nom pour le certificat dans le champ Nom du certificat.
- Si PKCS #12 a été sélectionné, saisissez un mot de passe pour le fichier dans le champ Import Password (Importer le mot de passe). Sinon, passez à l'étape 3.
- Cliquez sur une source pour importer le certificat. Les options sont les suivantes :
    - Importer à partir du PC
    - Importer depuis USB

- Si le routeur ne détecte pas de lecteur USB, l'option Import from USB est grisée.
- Si vous avez choisi Import From USB et que votre port USB n'est pas reconnu par le routeur, cliquez sur Refresh.
- Cliquez sur le bouton Choisir un fichier et choisissez le fichier approprié.
- Cliquez sur Upload (charger).




Une fois que vous avez réussi, vous accédez automatiquement à la page principale du certificat. La table de certificats contient le certificat récemment importé.




Vous devez maintenant avoir importé un certificat sur votre routeur RV345P.

### Configuration d'un réseau mobile à l'aide d'un dongle et d'un routeur de la gamme RV345P (facultatif)

Peut-être souhaitez-vous configurer un réseau mobile de secours à l'aide d'un dongle et de votre routeur RV345P. Si c'est le cas, lisez Configurer un réseau mobile à l'aide d'un dongle et d'un routeur de la gamme RV34x.

Félicitations, vous avez terminé la configuration de votre routeur RV345P ! Vous allez 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 RV345P. Les 4 premiers ports du RV345P 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 réinitialiser les paramètres d'usine par défaut sur les routeurs RV345x.

### 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

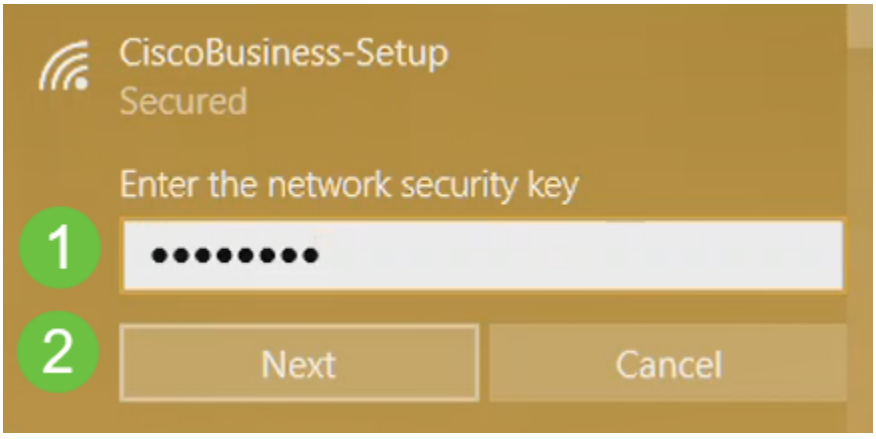
Sur votre ordinateur, cliquez sur l'**icône Wi-Fi** et choisissez *Cisco* Wireless Network

*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.

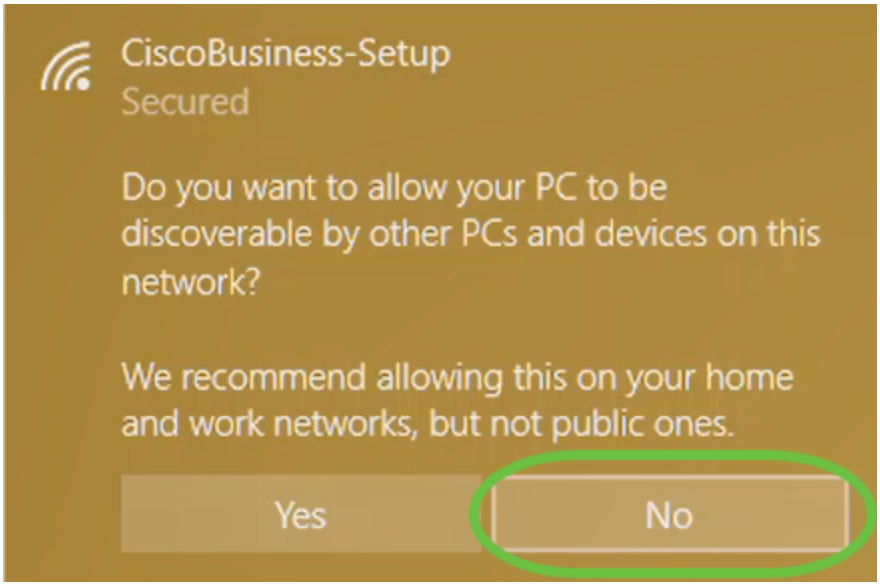
## Étape 2

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




## Étape 3

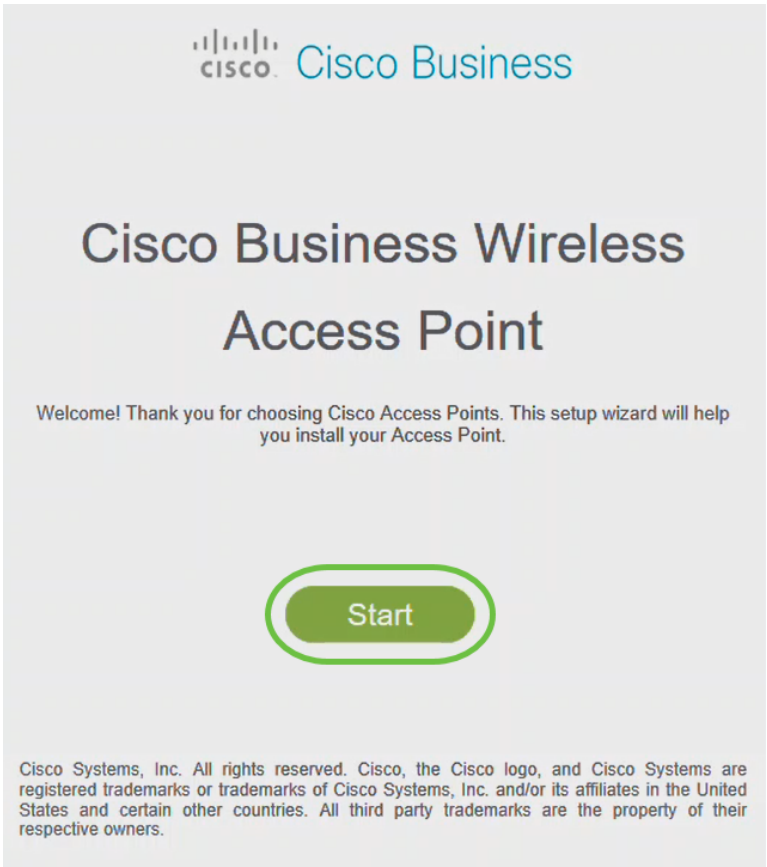
Vous obtiendrez l'écran suivant. Puisque vous ne pouvez configurer qu'un seul périphérique à la fois, cliquez sur **Non**.




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.

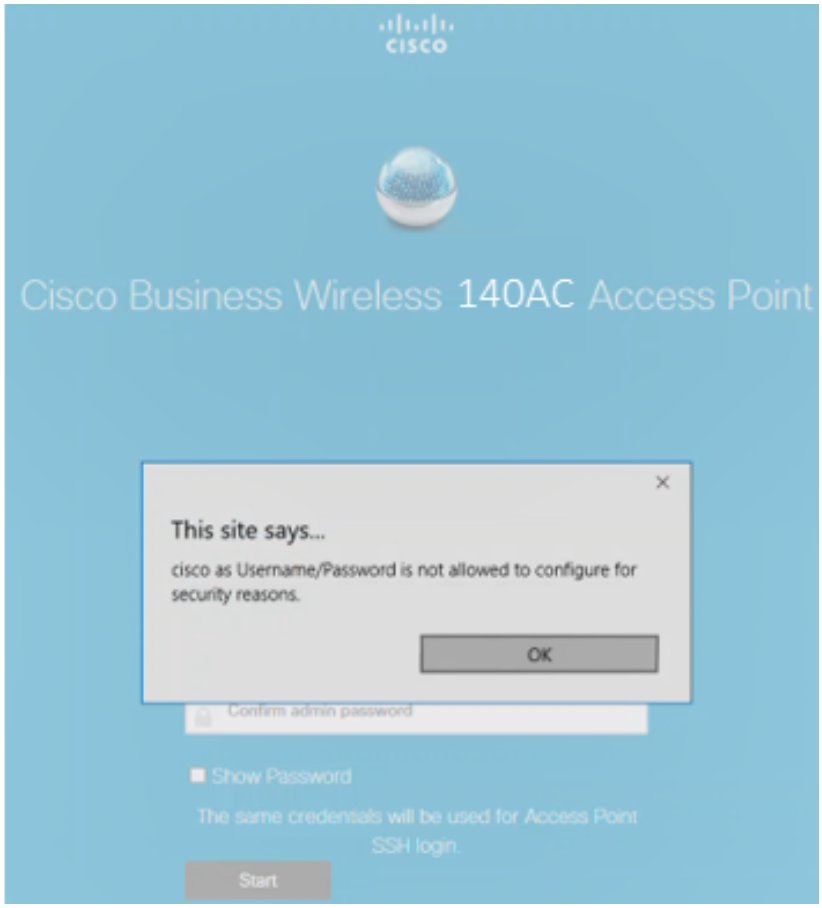
**Étape 5**

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**.

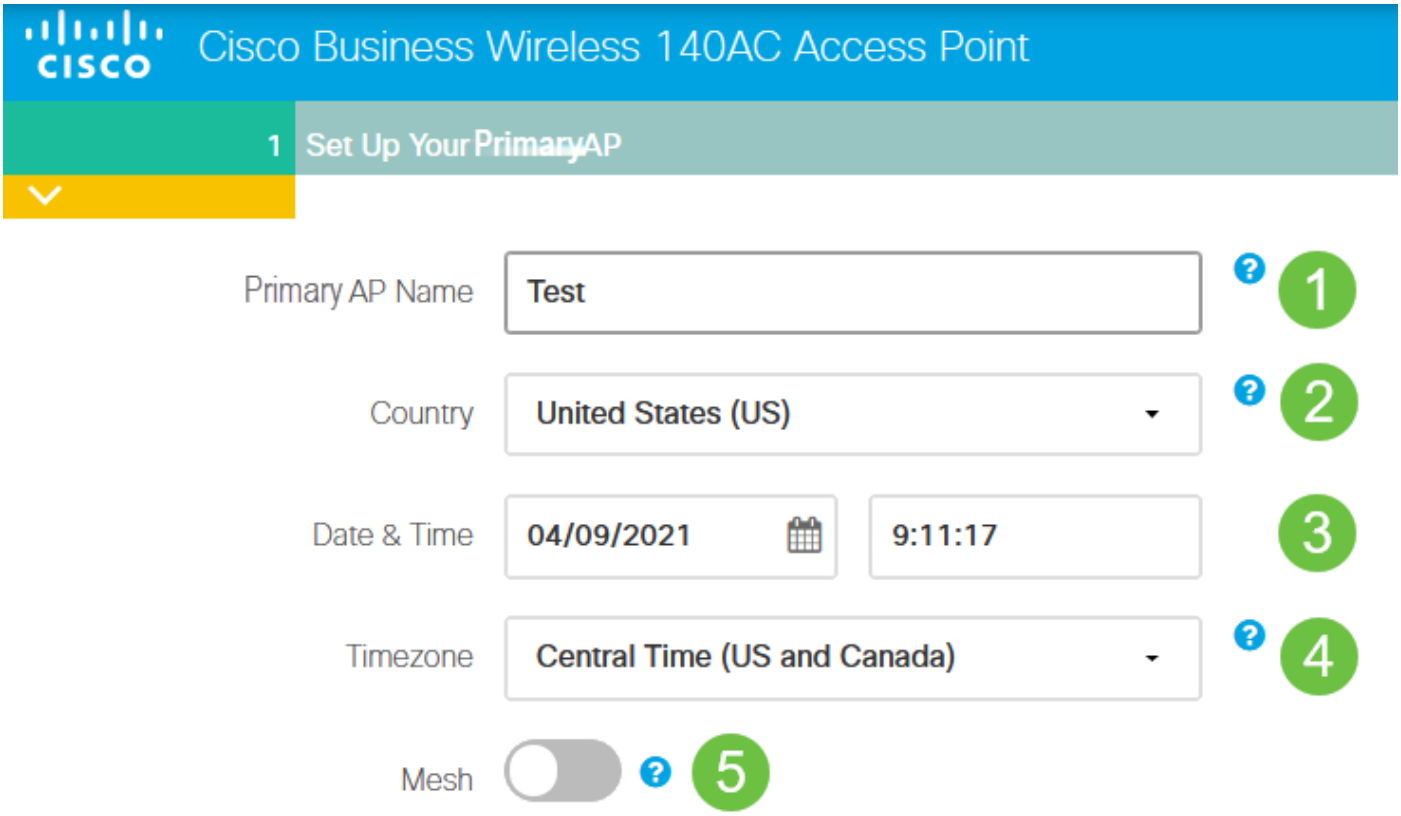

N'utilisez pas *cisco*, ni ses variantes dans les champs username ou password. Si vous le faites, vous obtiendrez un message d'erreur comme indiqué ci-dessous.




**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



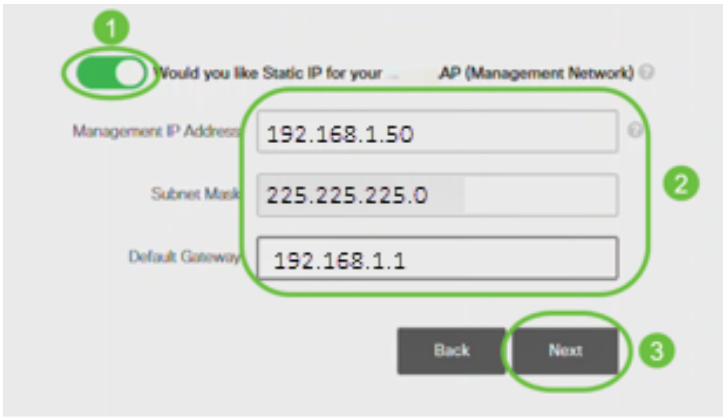

*Le maillage* ne doit être activé que si vous prévoyez de créer un réseau maillé. Par défaut, il est désactivé.

**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).



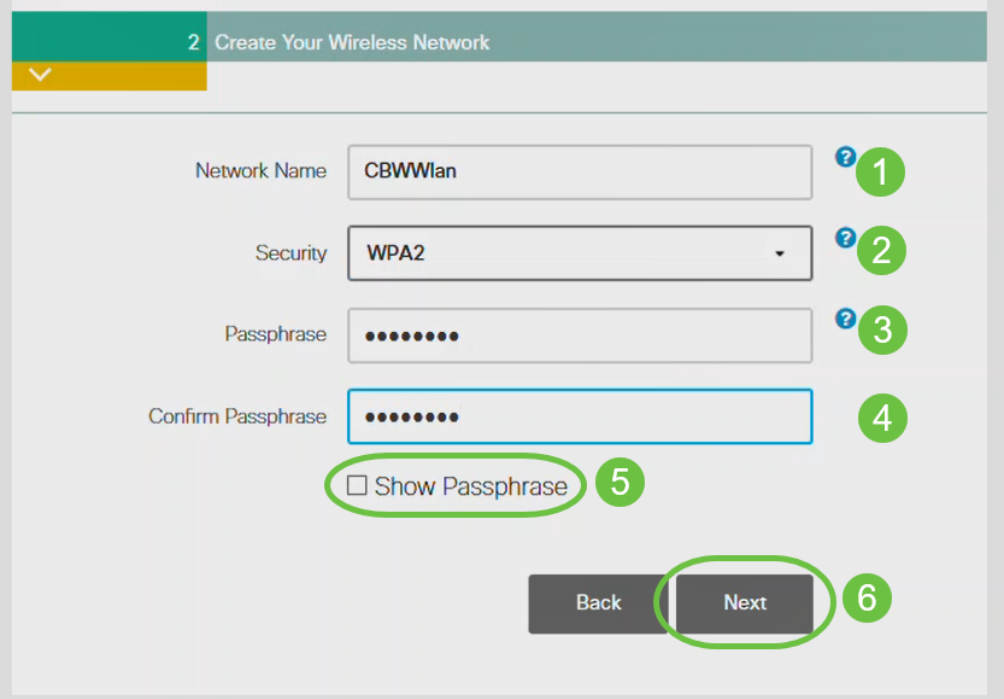

Par défaut, cette option est désactivée.

## 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.

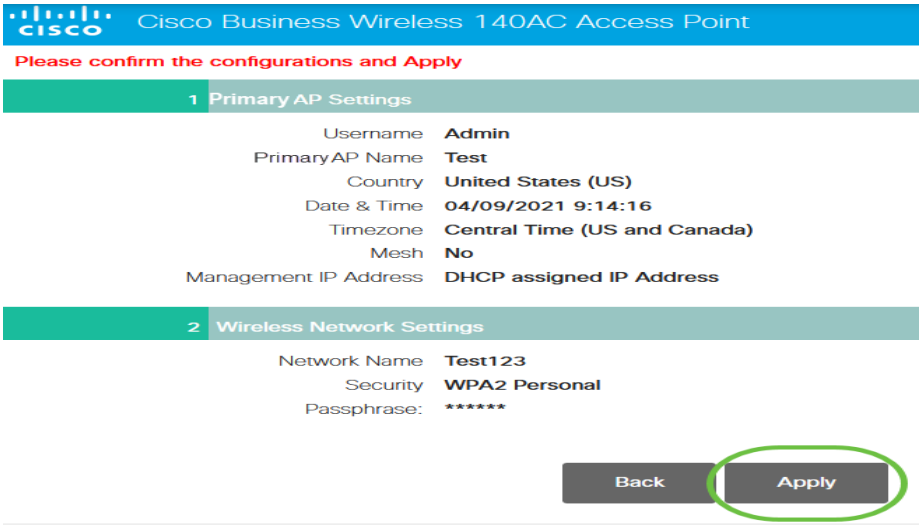
Cliquez sur Next (Suivant).




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

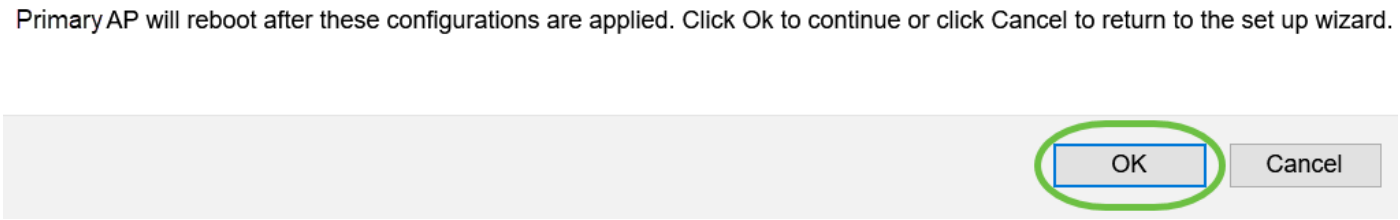
## Étape 9

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

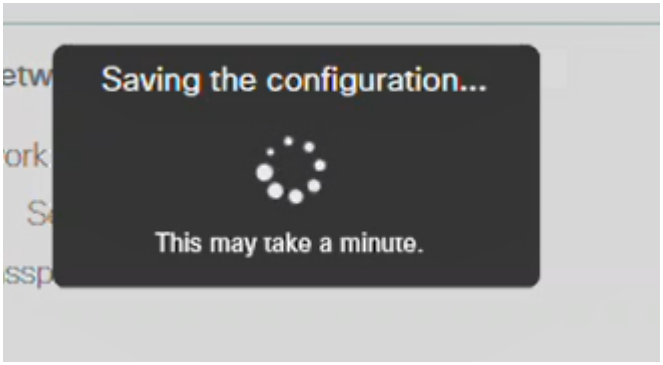



## Étape 10

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.

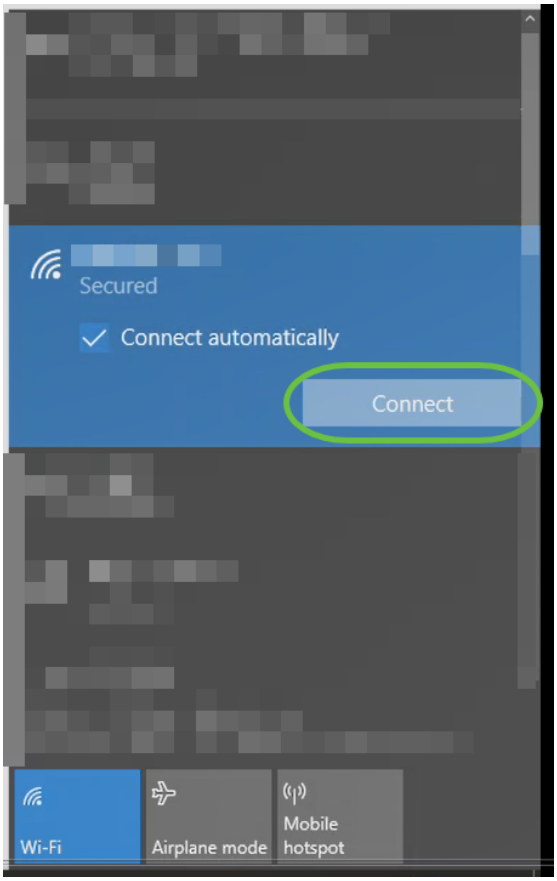



Au cours du redémarrage, la DEL du point d'accès passe par plusieurs modèles de couleurs. Lorsque le voyant clignote en vert, passez à l'étape suivante. Si le voyant ne dépasse pas le modèle clignotant rouge, il indique qu'il n'y a pas de serveur DHCP dans votre réseau. Assurez-vous que le point d'accès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

## Étape 11

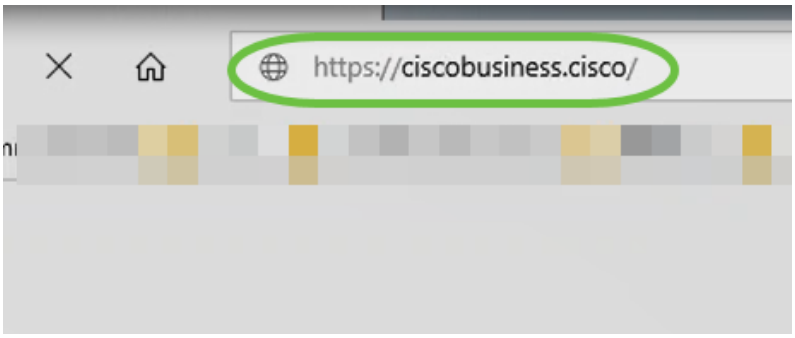
Accédez aux options sans fil de votre ordinateur et sélectionnez le réseau que vous avez configuré. Cliquez sur Connect.

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.



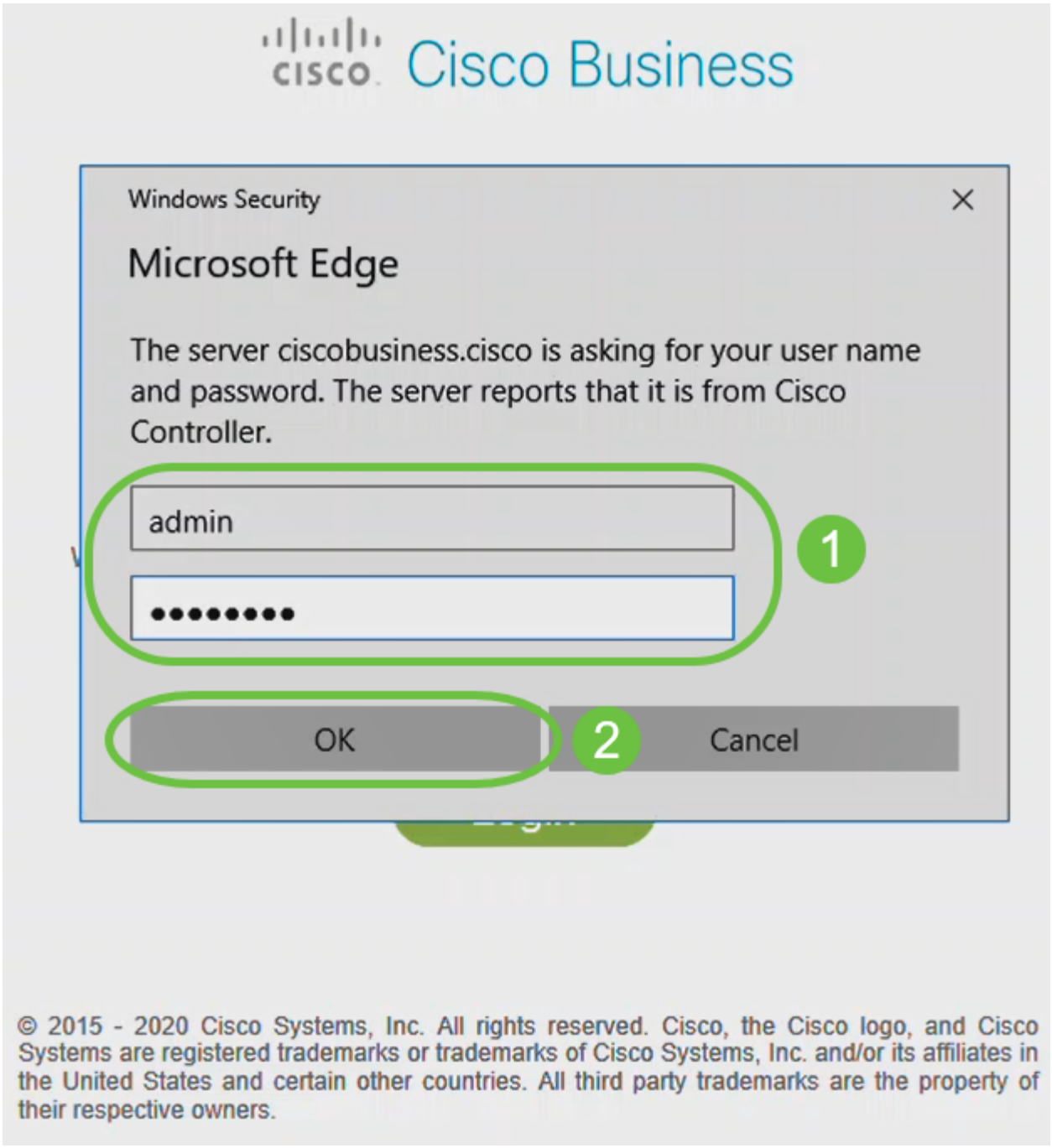

Assurez-vous que vous tapez *https* et non *http* à cette étape.

## 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

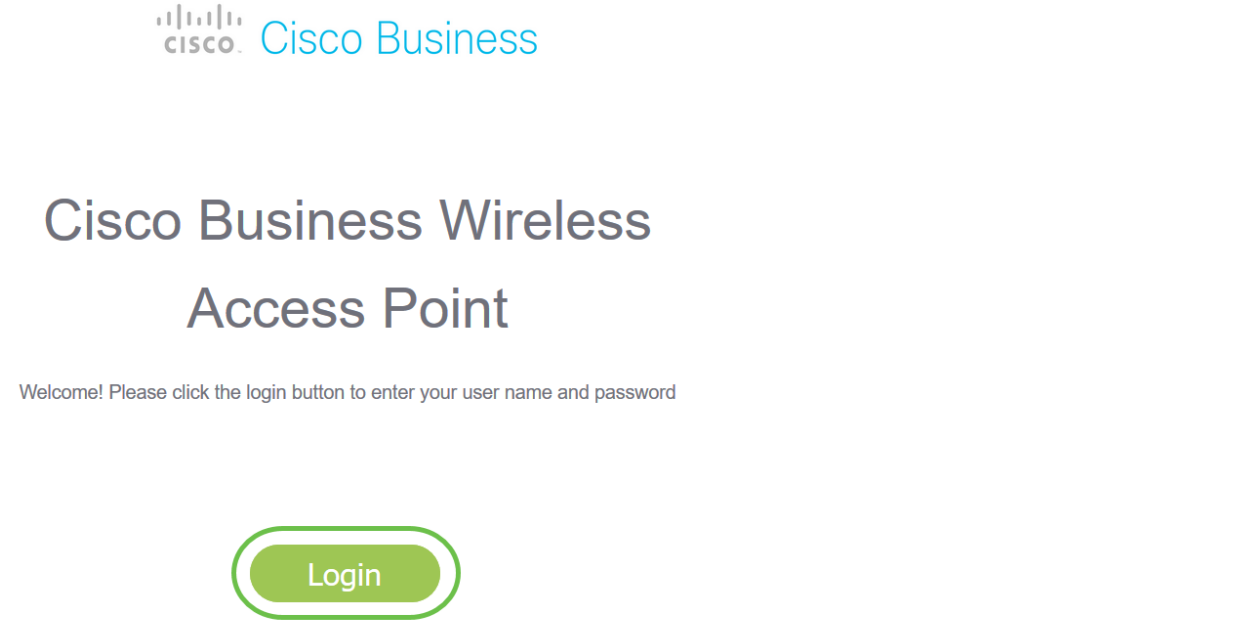
Branchez les deux extenseurs de maillage sur le mur aux emplacements sélectionnés. Notez l'adresse MAC de chaque extendeur de maillage.

### Étape 2

Attendez environ 10 minutes que les extendeurs de maillage démarrent.

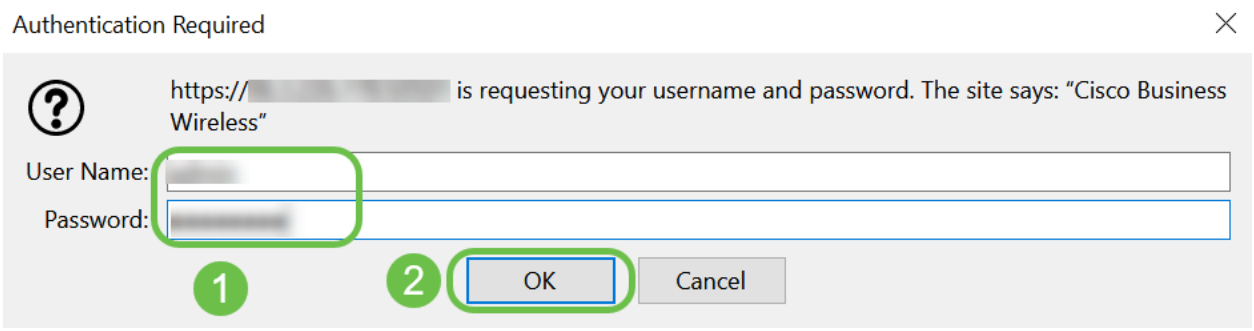
### Étape 3

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



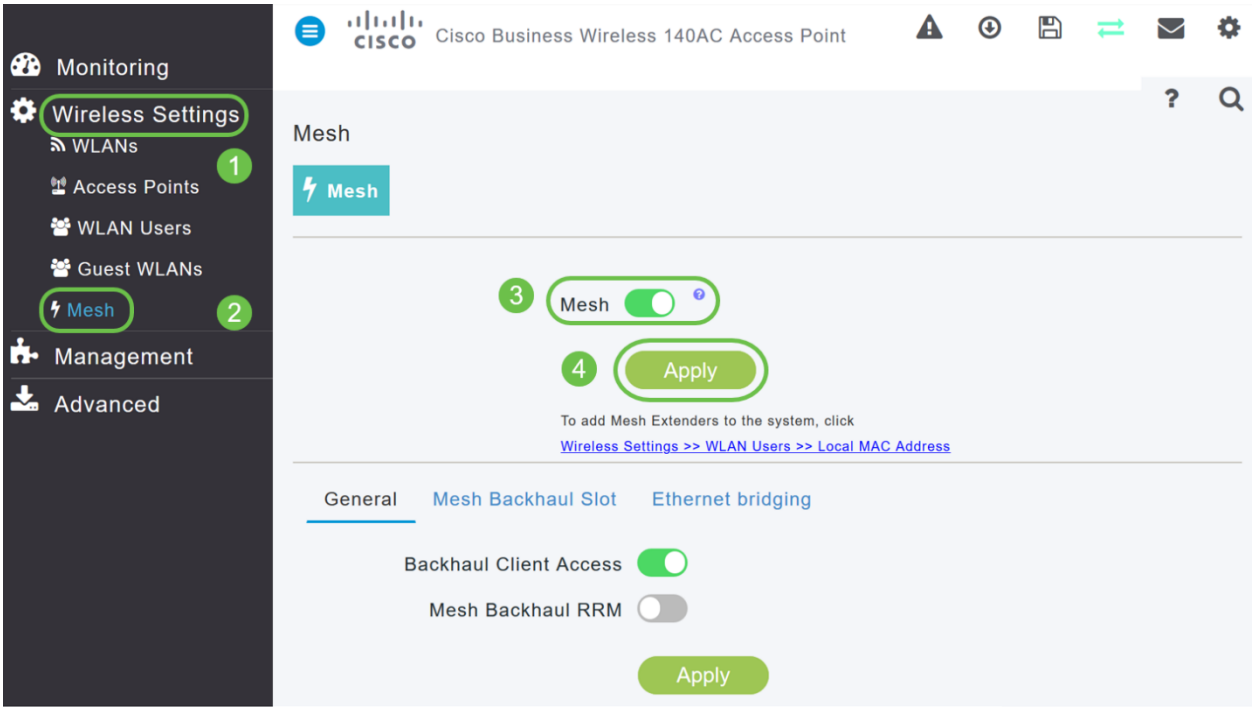

## Étape 4

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.

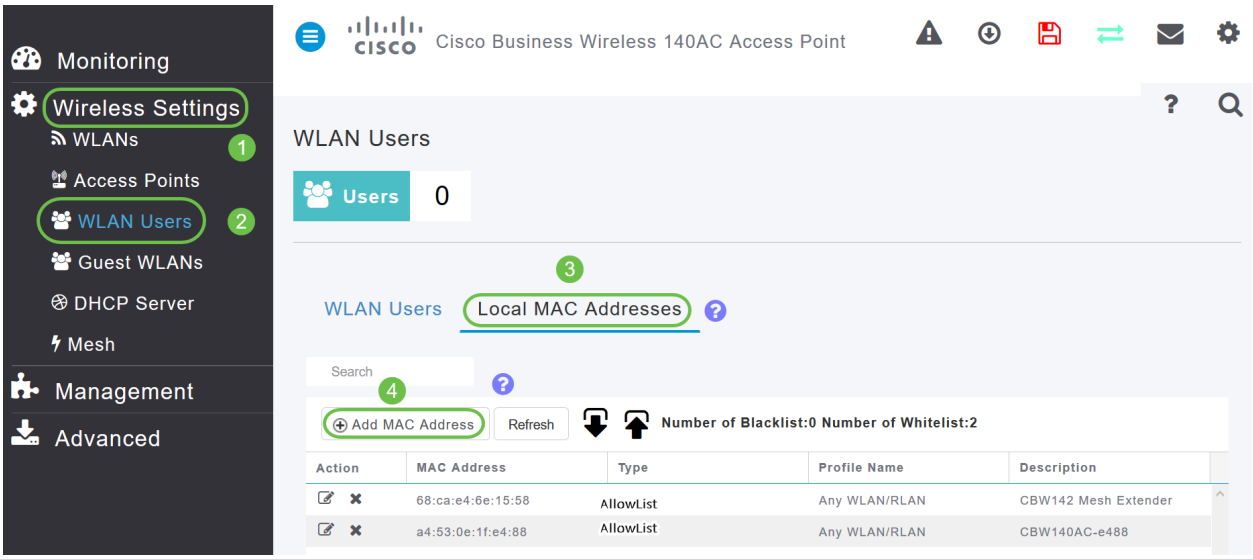


## Étape 6

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.

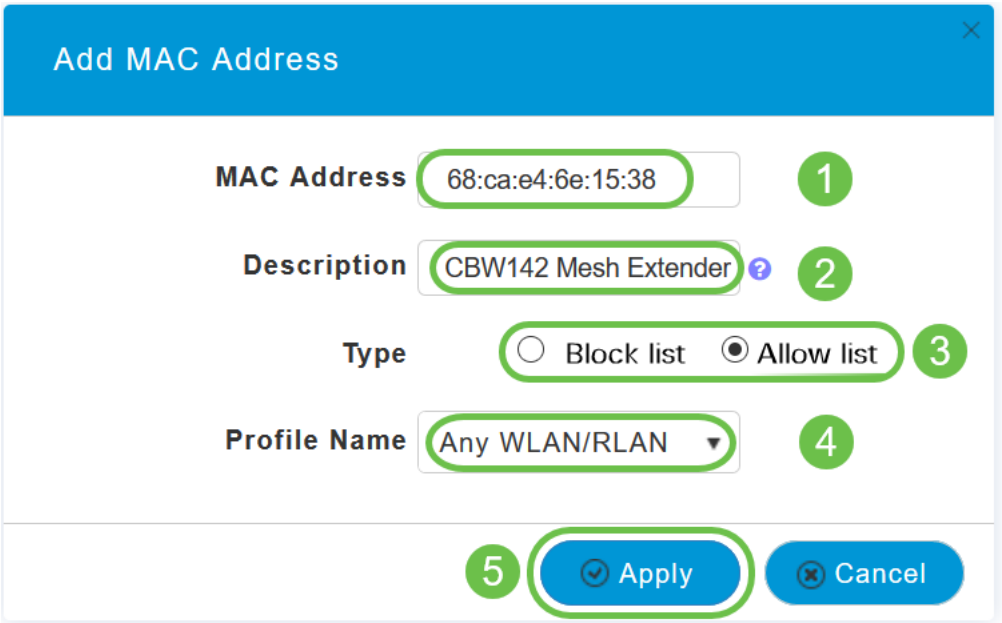
## Étape 7

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.

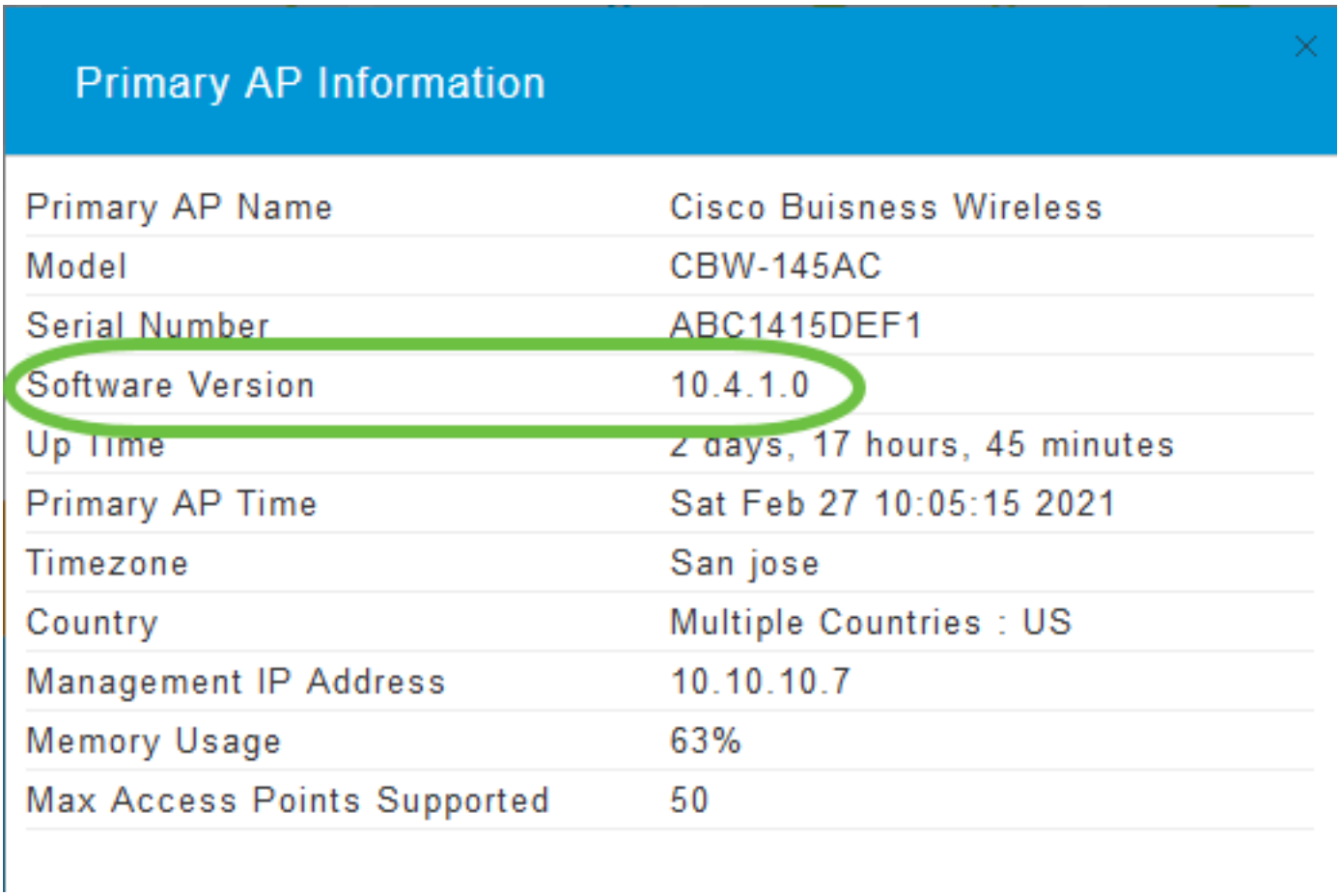
## Vérification et mise à jour du logiciel à l'aide de l'interface utilisateur Web

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

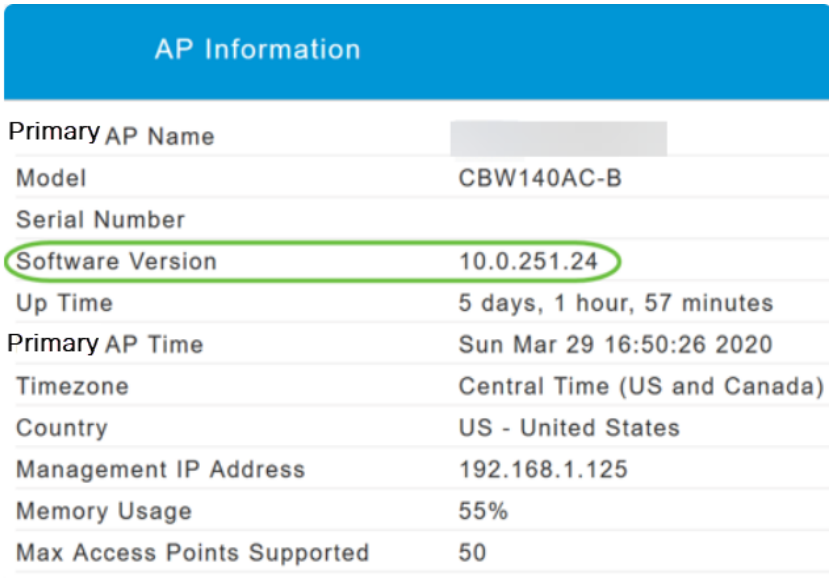
Cliquez sur l'**icône d'engrenage** dans le coin supérieur droit de l'interface Web, puis cliquez sur **Informations principales du point d'accès**.




### 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.

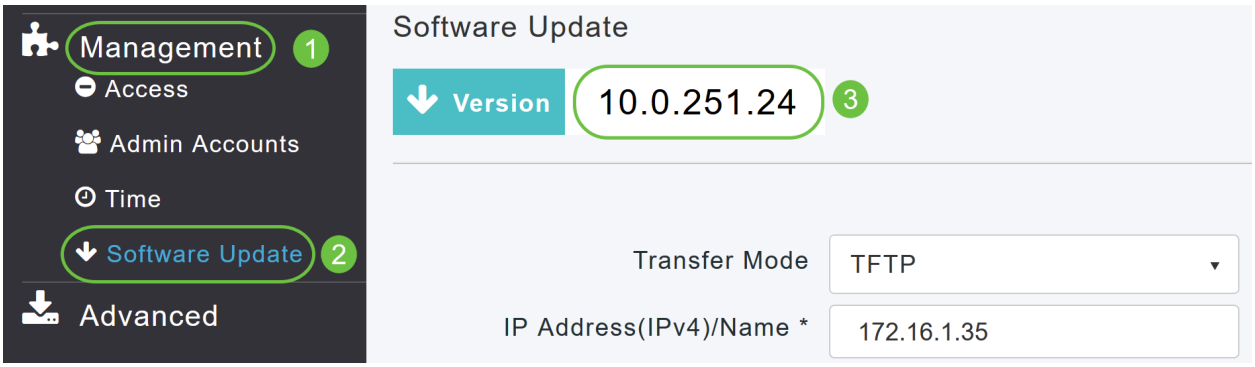



Si vous exécutez la dernière version du logiciel, vous pouvez accéder à la section Créer des WLAN.

## Étape 3

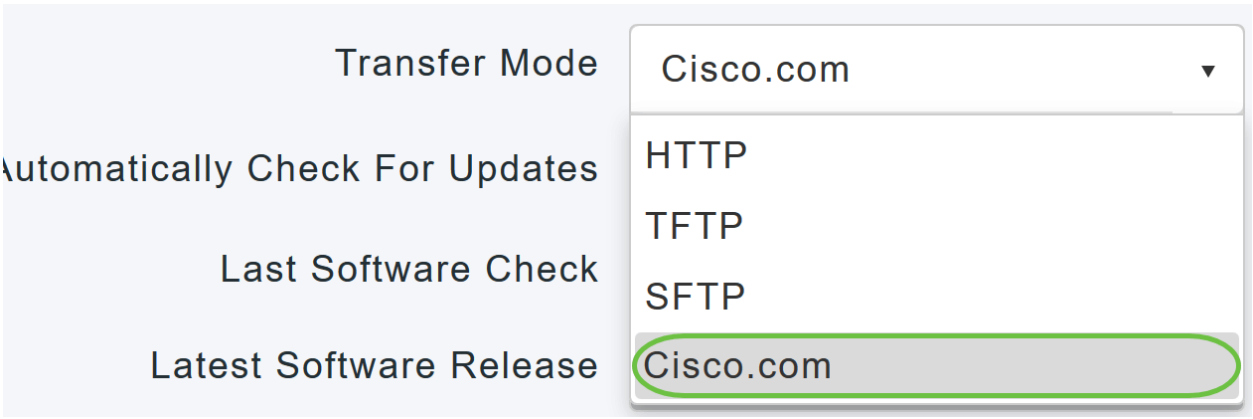
Choisissez **Management > Software Update** dans le menu.

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



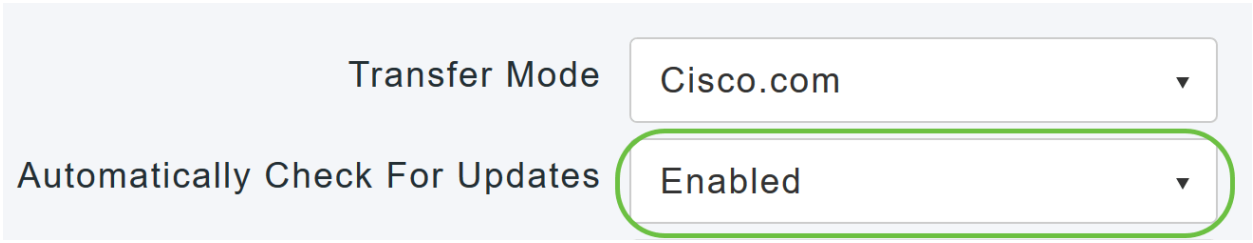

Vous pouvez mettre à jour le logiciel de point d'accès CBW et les configurations actuelles sur le point d'accès principal ne seront pas supprimées.

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



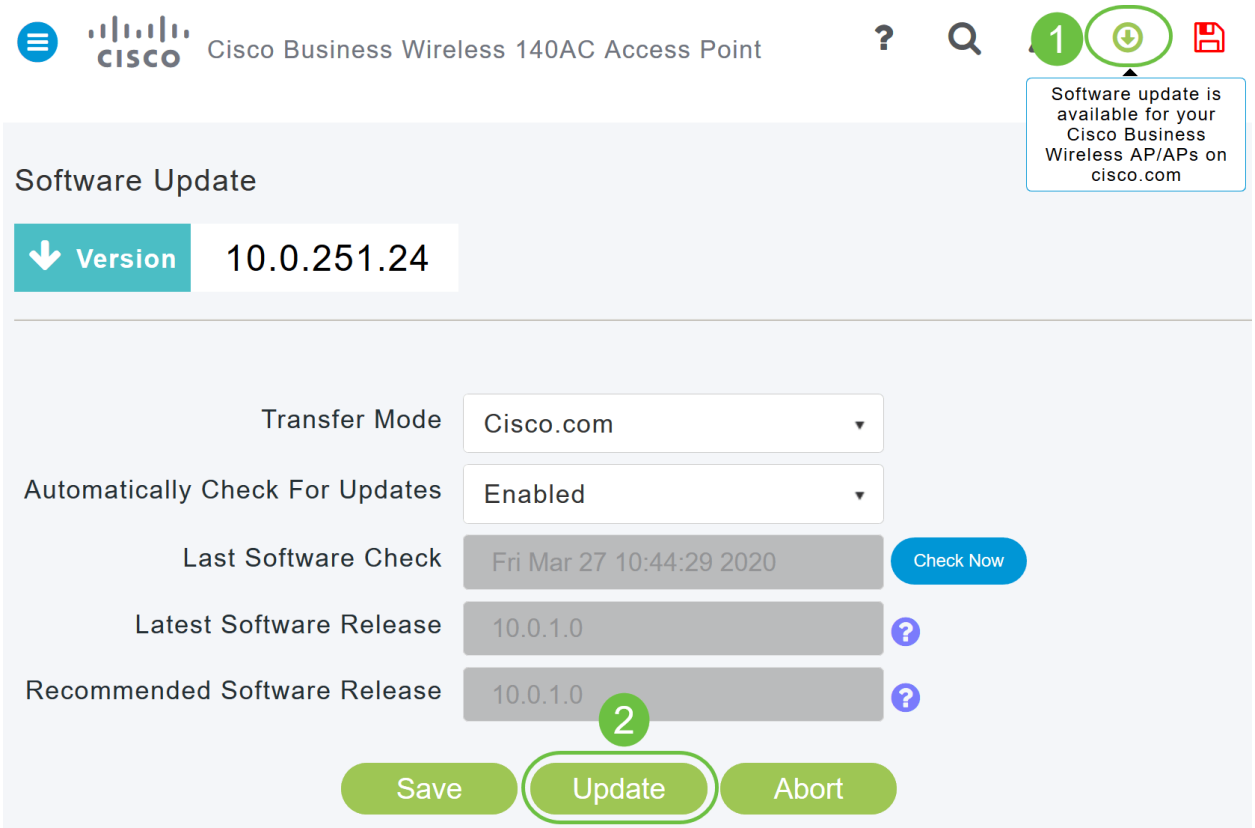

**Étape 4**

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.



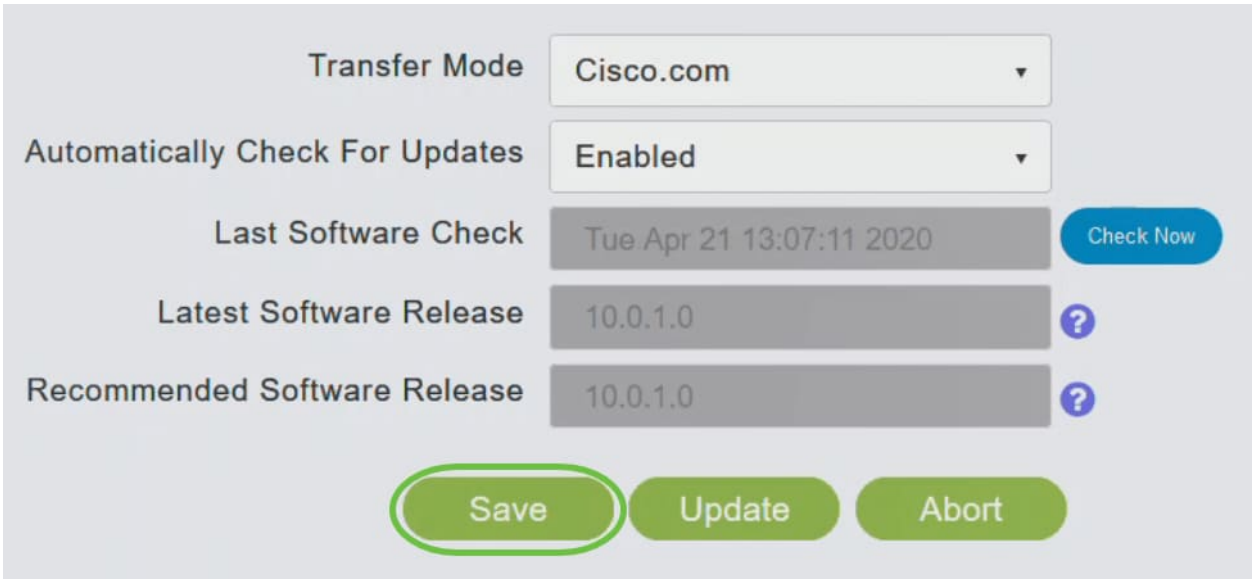

Lorsqu'une vérification logicielle est effectuée et qu'une mise à jour logicielle plus récente ou recommandée est disponible sur Cisco.com, alors :

- 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.

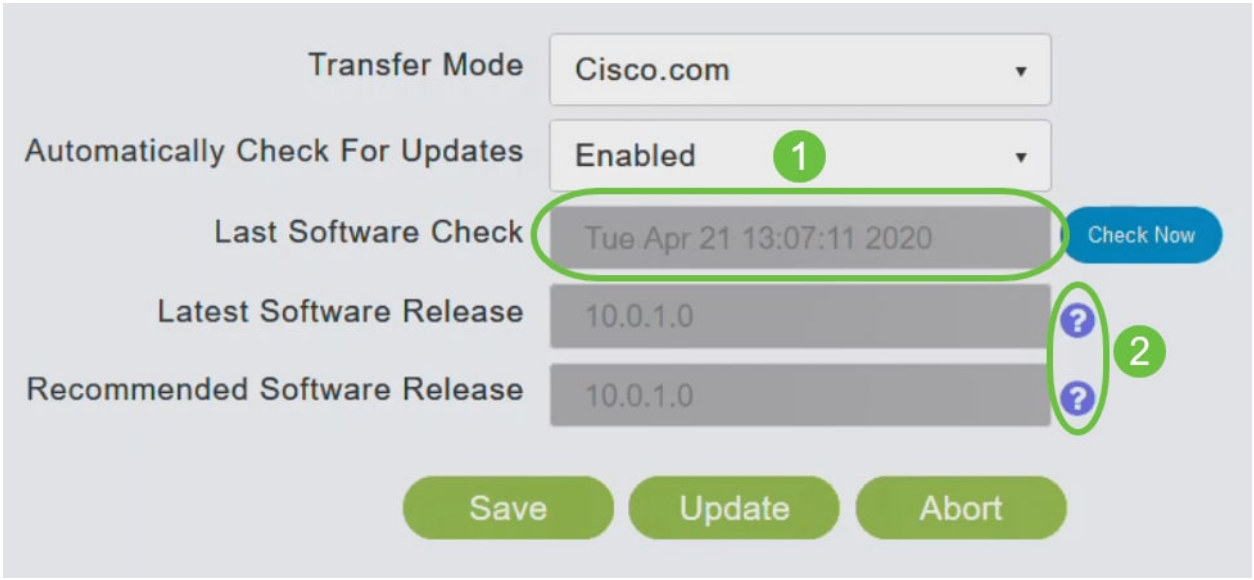


## Étape 5

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

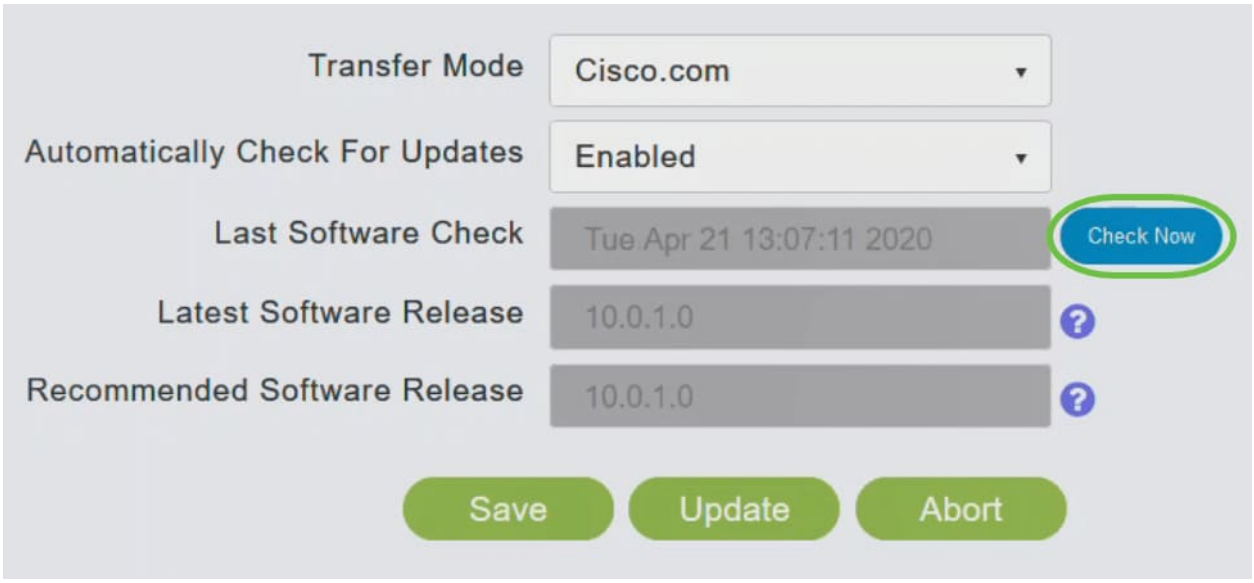



Le champ *Dernier contrôle logiciel* affiche l'horodatage du dernier contrôle logiciel automatique ou manuel. Vous pouvez afficher les notes des versions affichées en cliquant sur l'**icône de point d'interrogation** à côté.



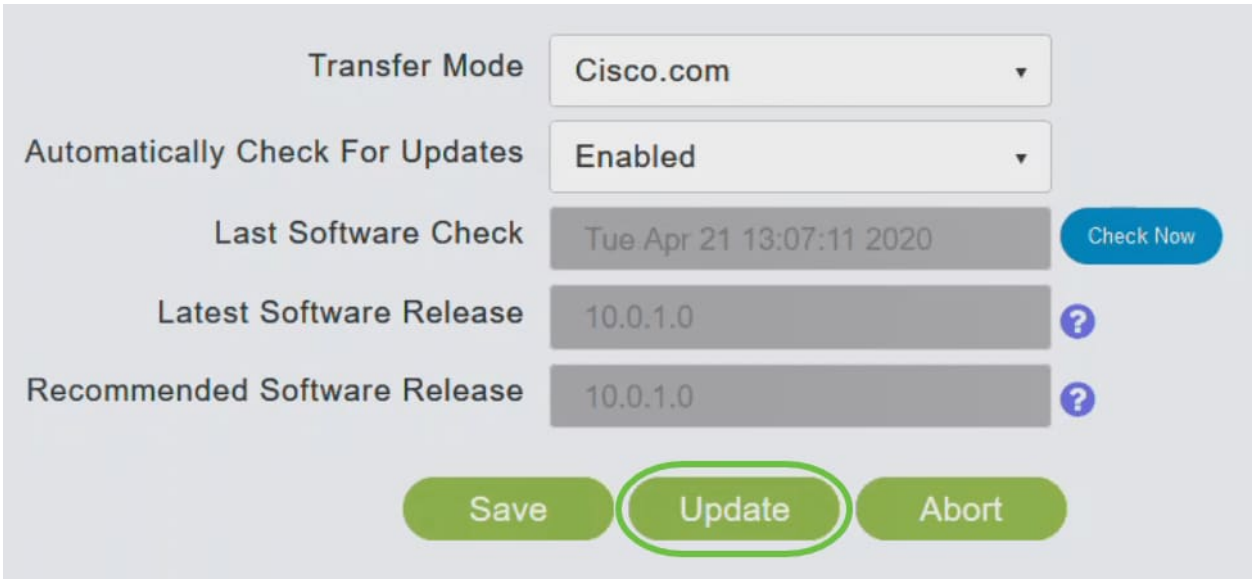

## Étape 6

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




**Étape 7**

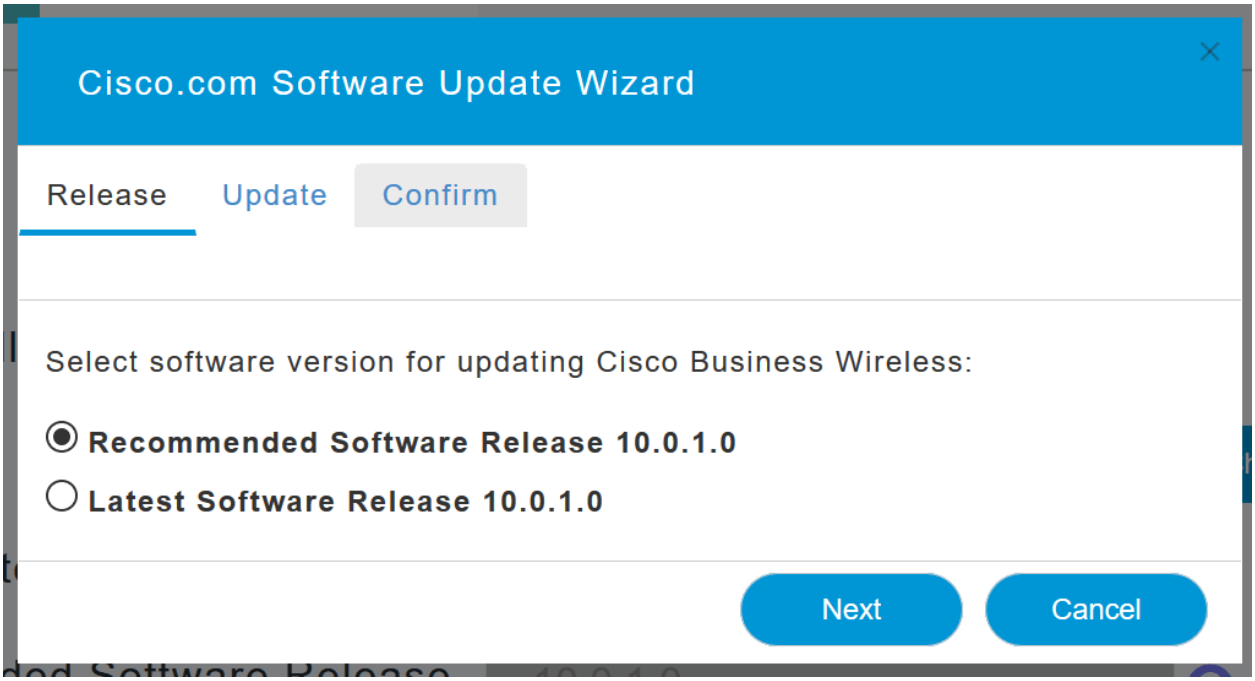
Pour continuer la mise à jour logicielle, cliquez sur **Mettre à jour**.




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

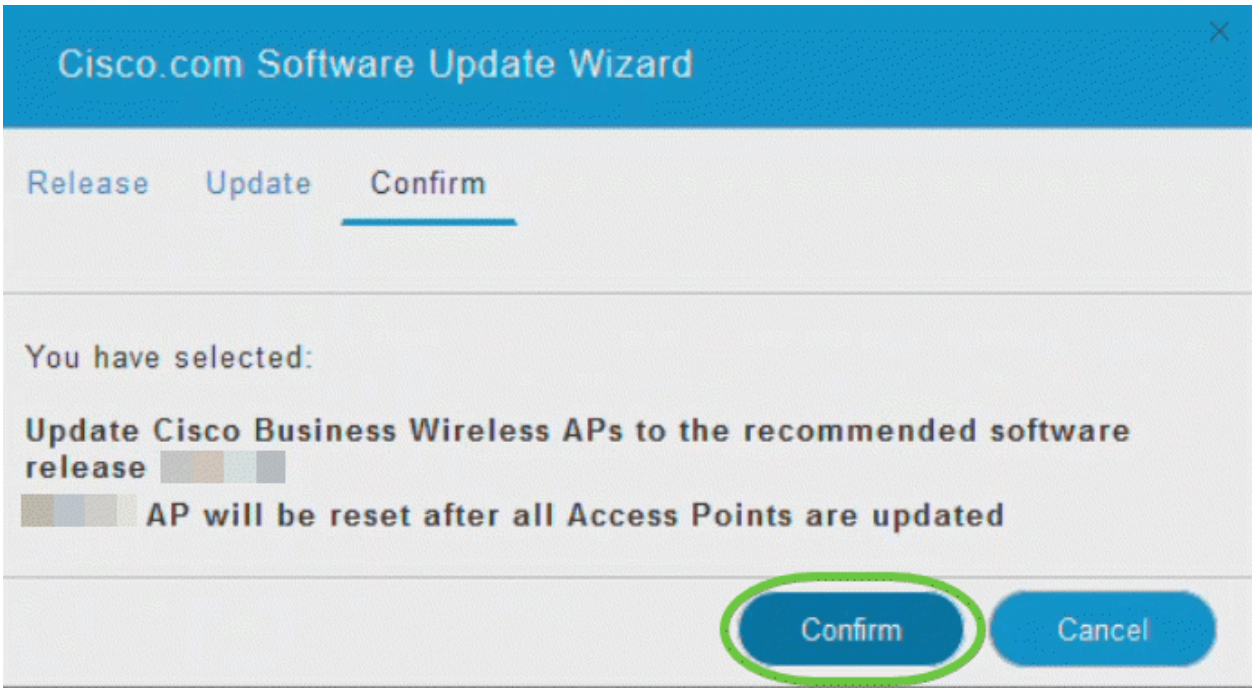
- Onglet Version : indiquez si vous souhaitez effectuer une mise à jour vers la version logicielle recommandée ou vers la dernière version logicielle.
- Onglet Update : indiquez quand les points d'accès doivent être réinitialisés. Vous pouvez choisir de le faire faire immédiatement ou de le planifier 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**.

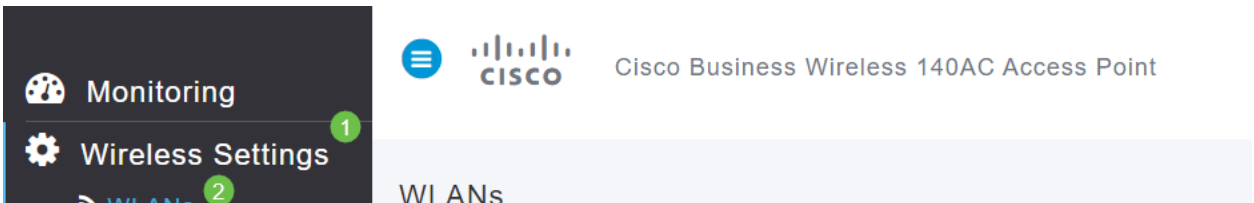



## Créer des WLAN sur l'interface utilisateur Web

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

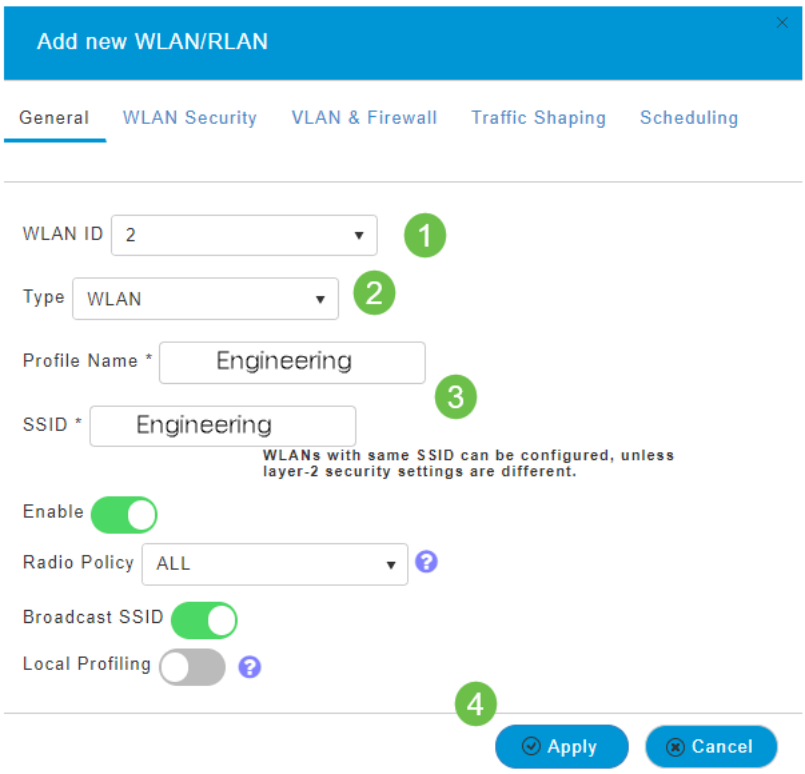
Sous l'onglet *Général*, saisissez les informations suivantes :

- 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).

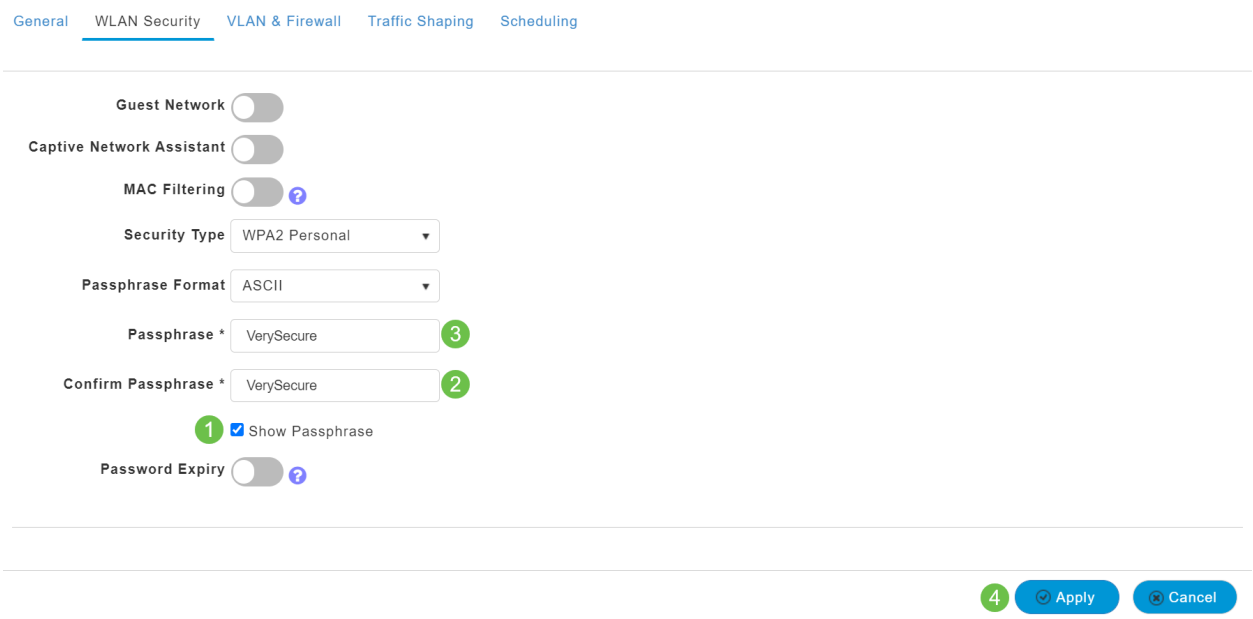
WPA2 Personal (WPA2 personnel) est une méthode utilisée pour sécuriser votre réseau à l'aide d'une authentification PSK. Le PSK est configuré séparément sur le point d'accès principal, sous la stratégie de sécurité WLAN, et sur le client. WPA2 Personal ne dépend pas d'un serveur d'authentification sur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

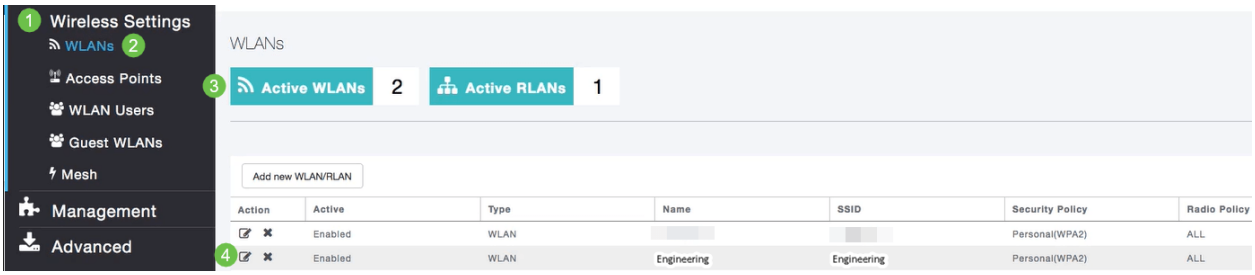



## Étape 4

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

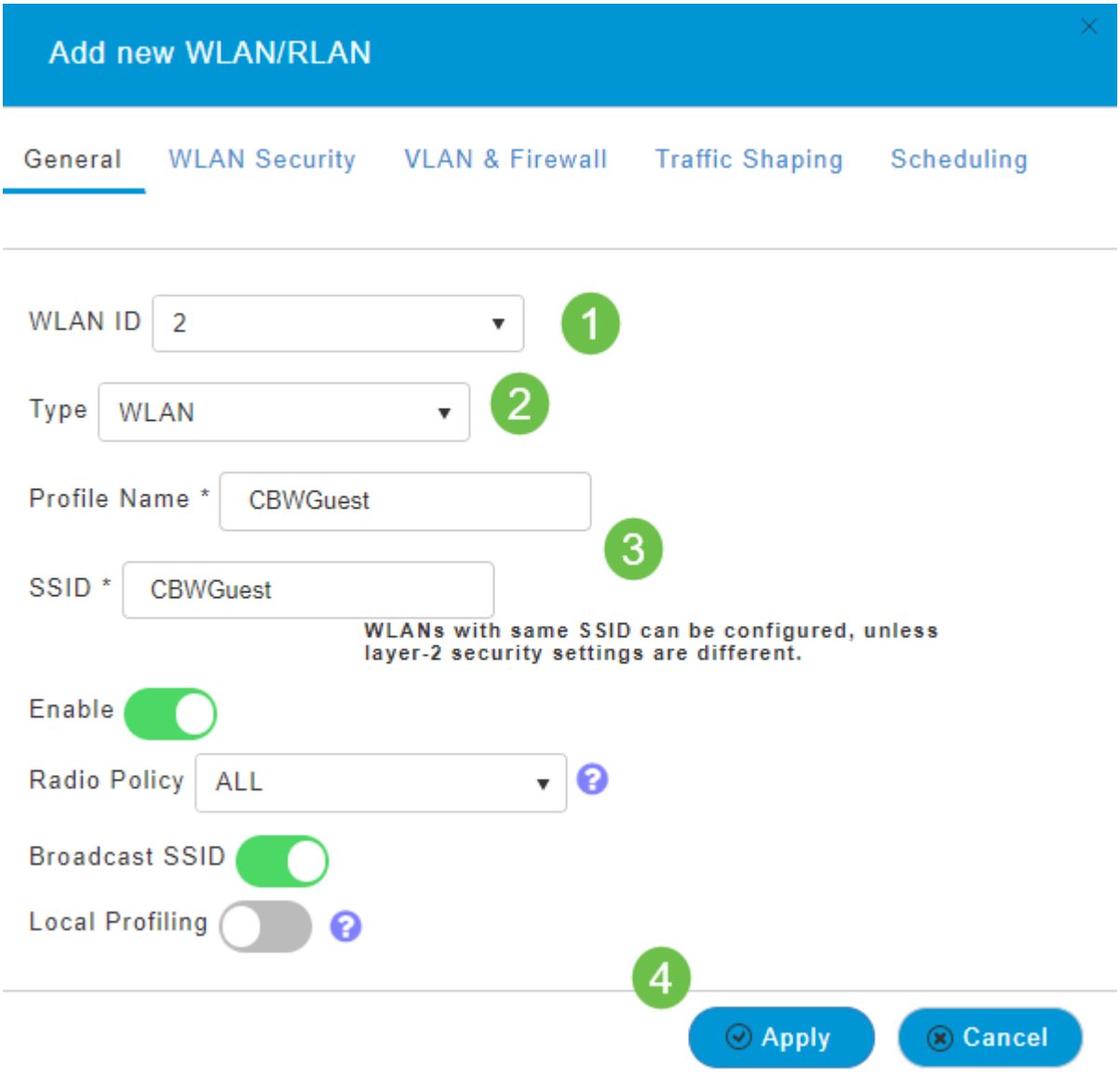
Sous l'onglet *Général*, saisissez les informations suivantes :

*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.

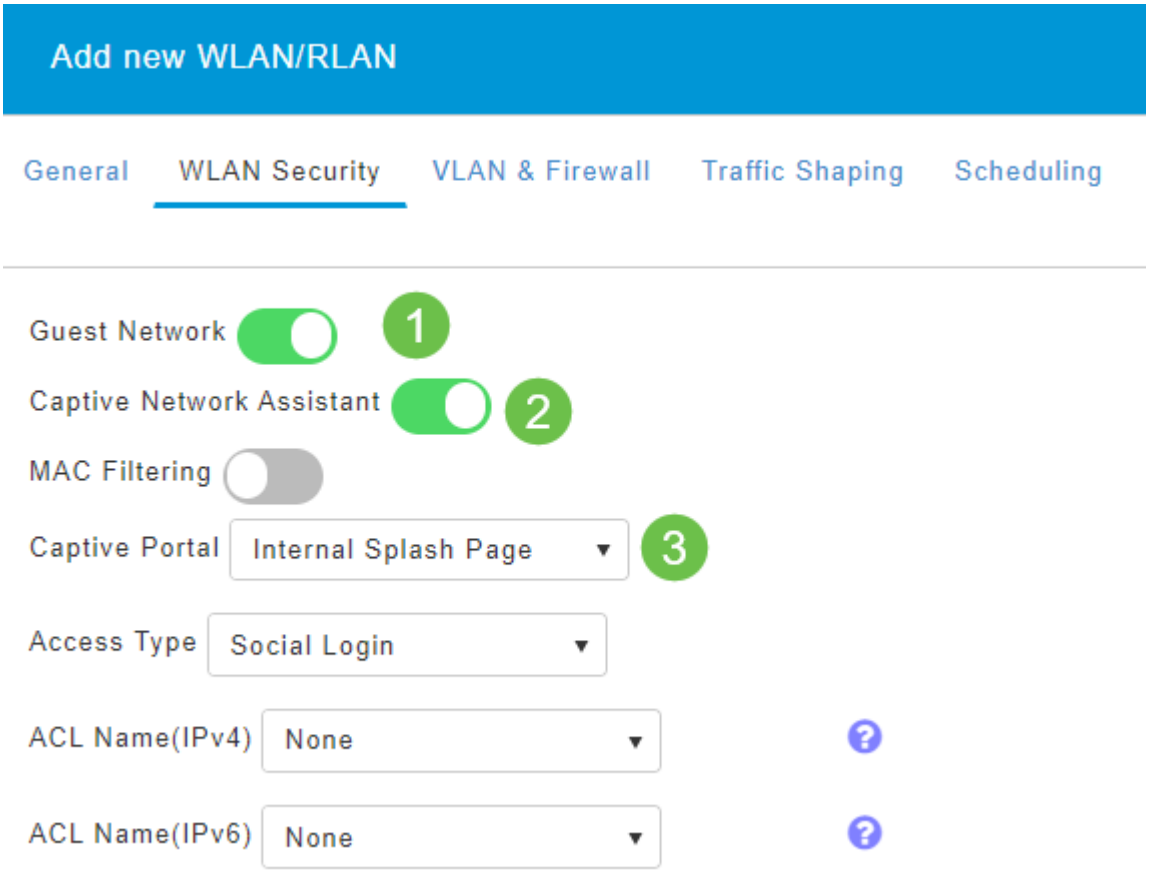



**Étape 4**

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.

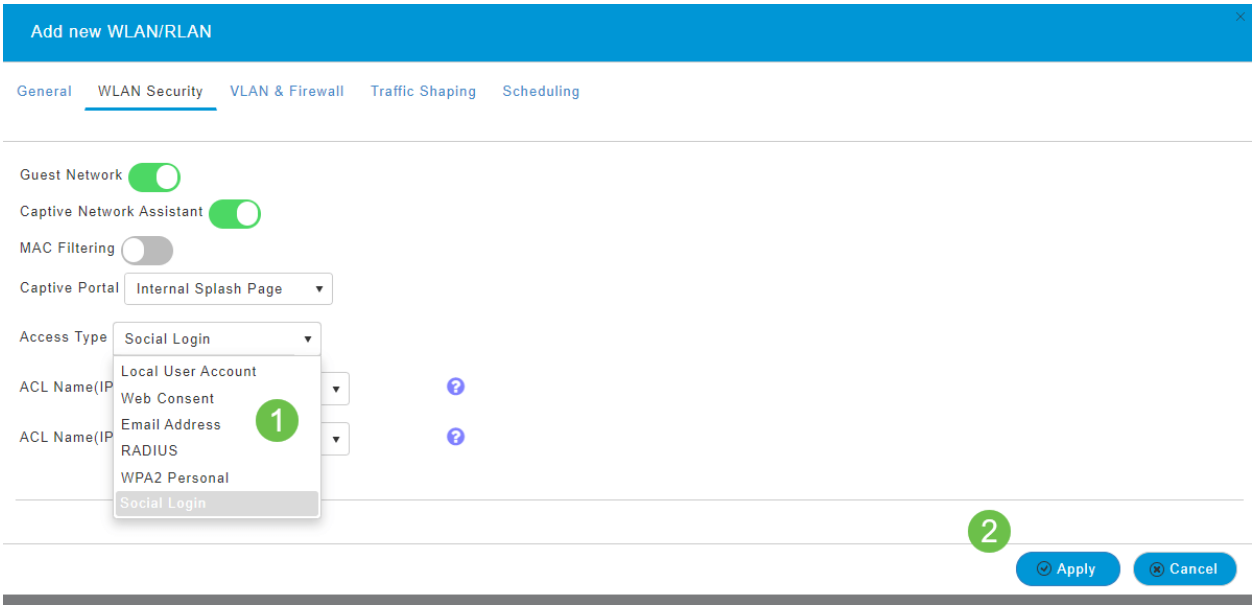
D'autres options pour *le type d'accès* sont les suivantes :

*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

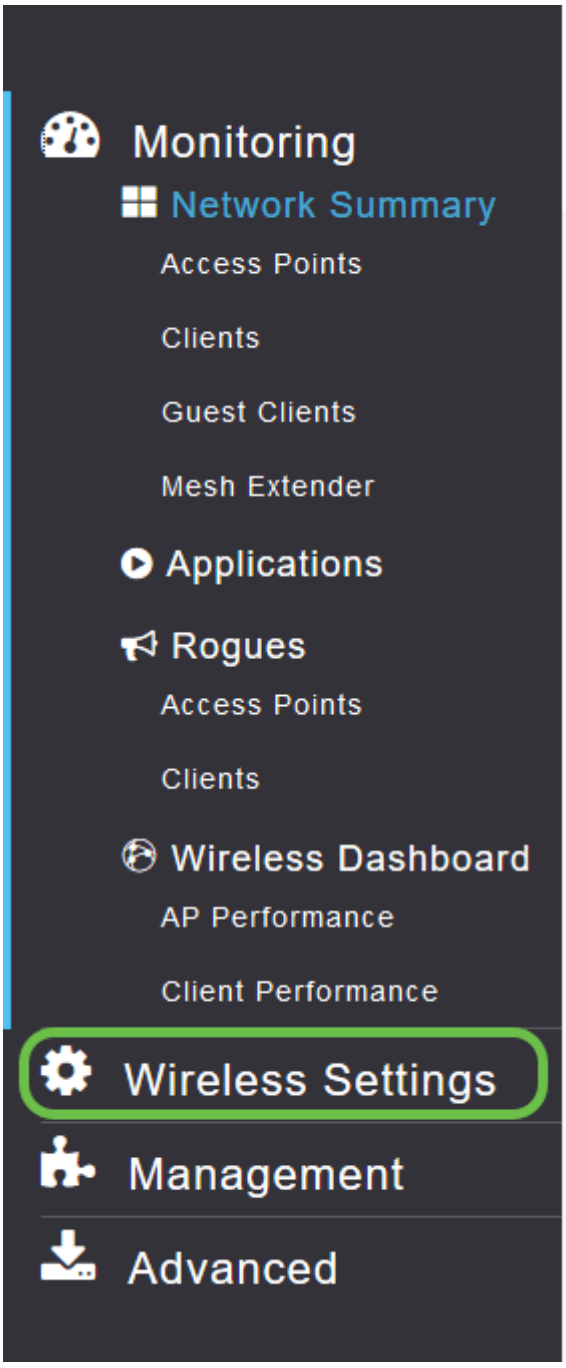
invité, les listes de contrôle d'accès et la qualité de service.

### Étape 1

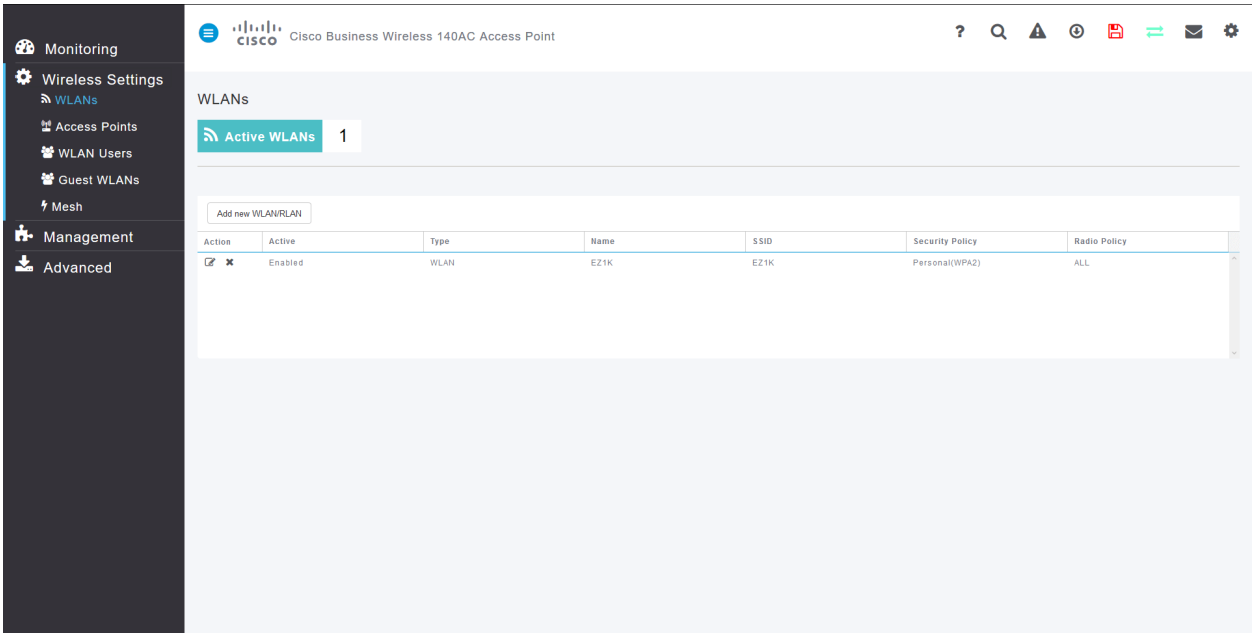
Naviguez jusqu'au menu situé à gauche de l'écran si vous ne voyez pas la barre de menu à gauche.

### Étape 2

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

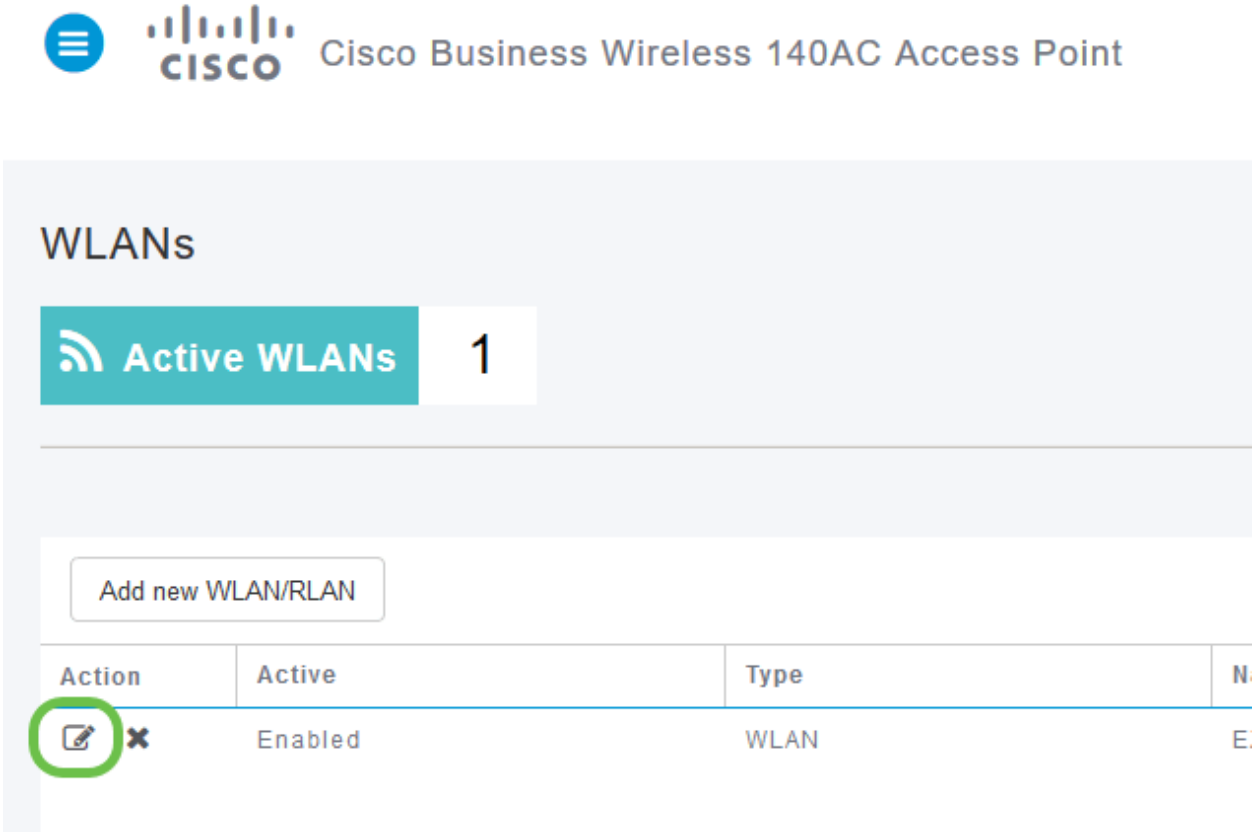



L'image ci-dessous est similaire à celle que vous verrez lorsque vous cliquez sur le lien Wireless Settings (Paramètres sans fil).

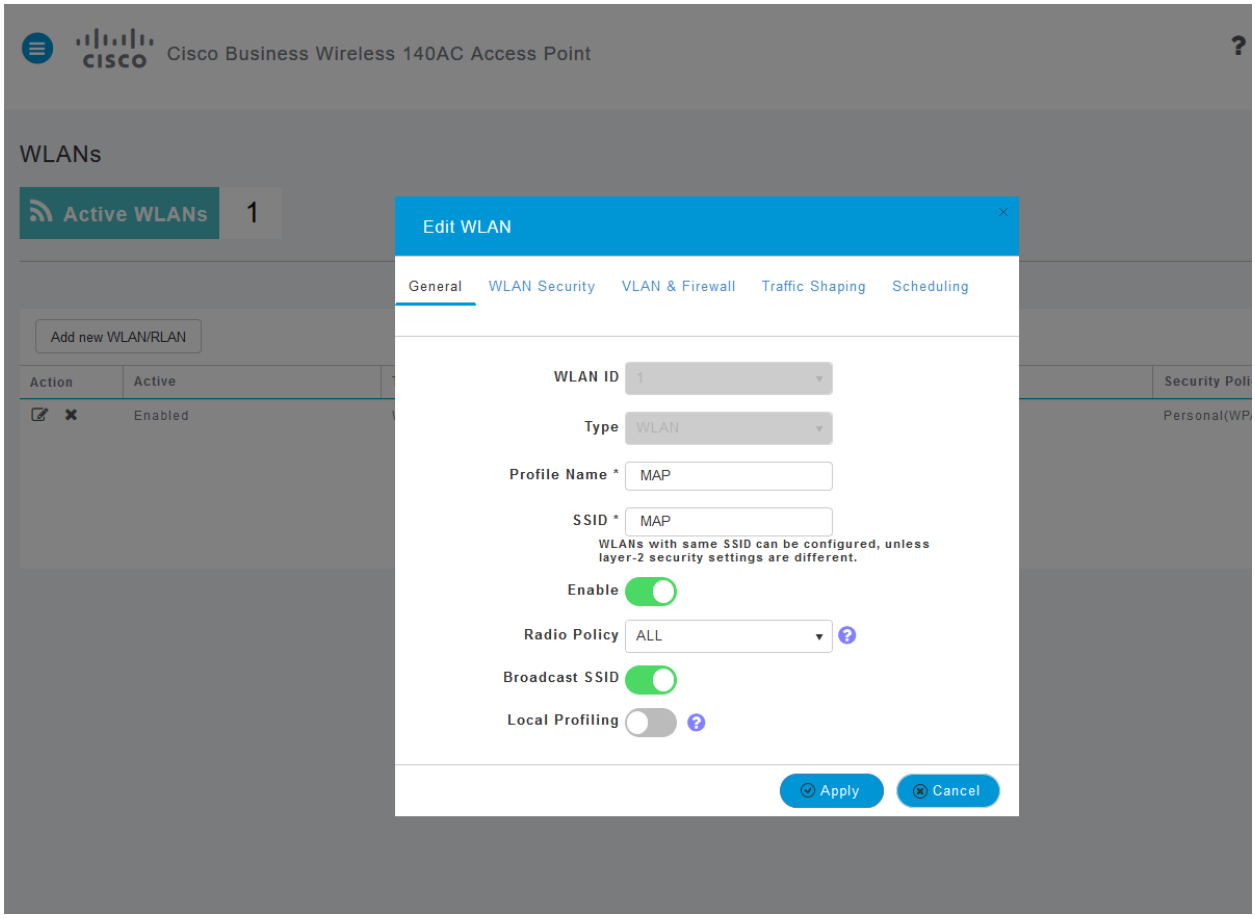



## Étape 3

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

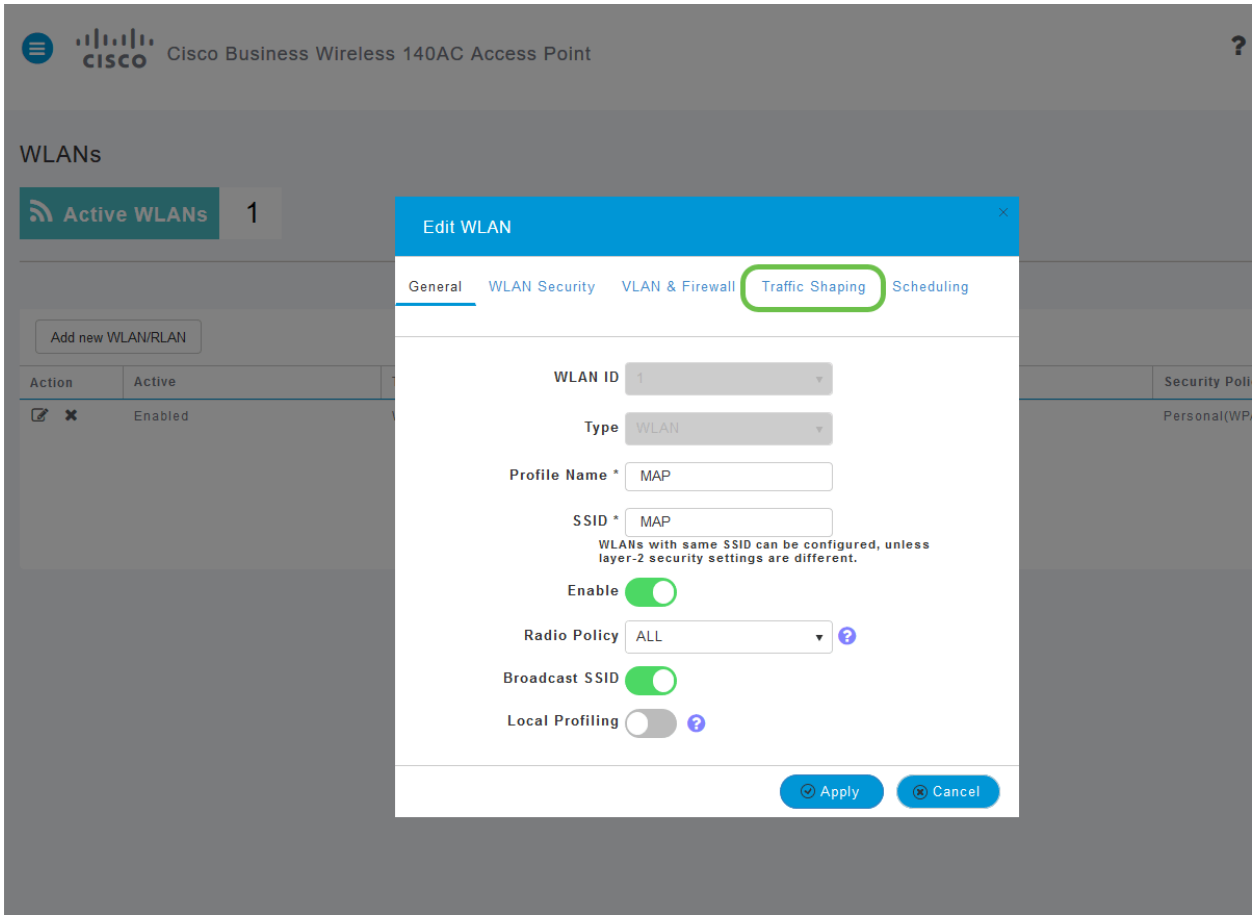



Depuis que vous avez récemment ajouté le WLAN, votre page *Edit WLAN* peut apparaître comme suit :

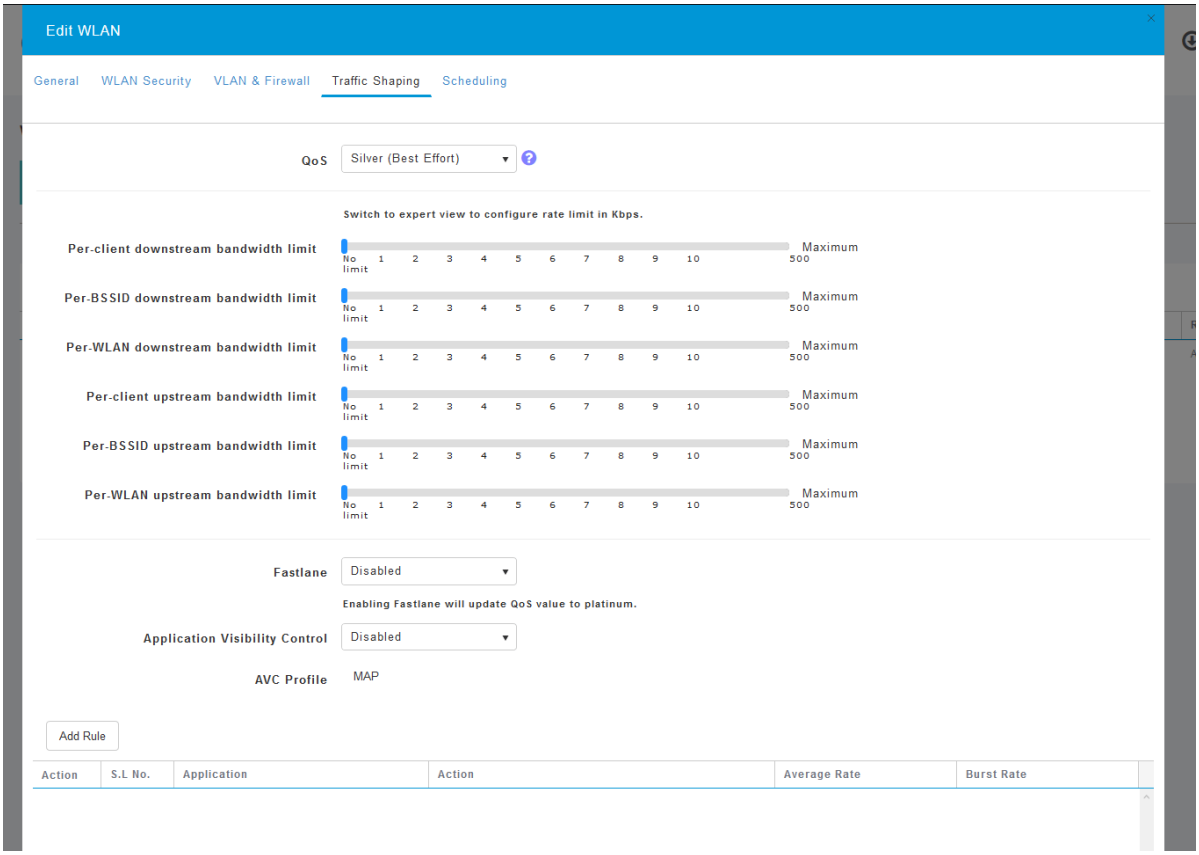



## Étape 4

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

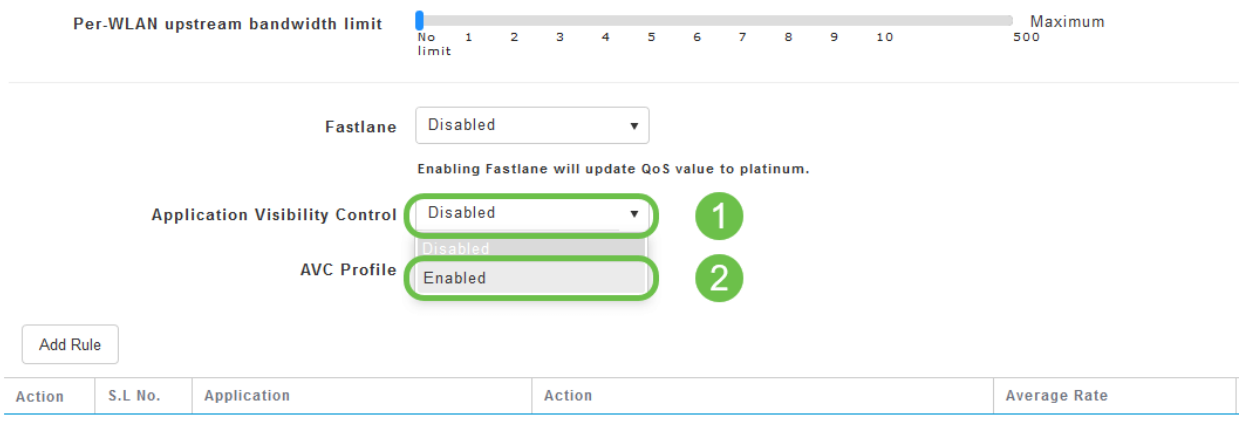



Votre écran peut apparaître comme suit :



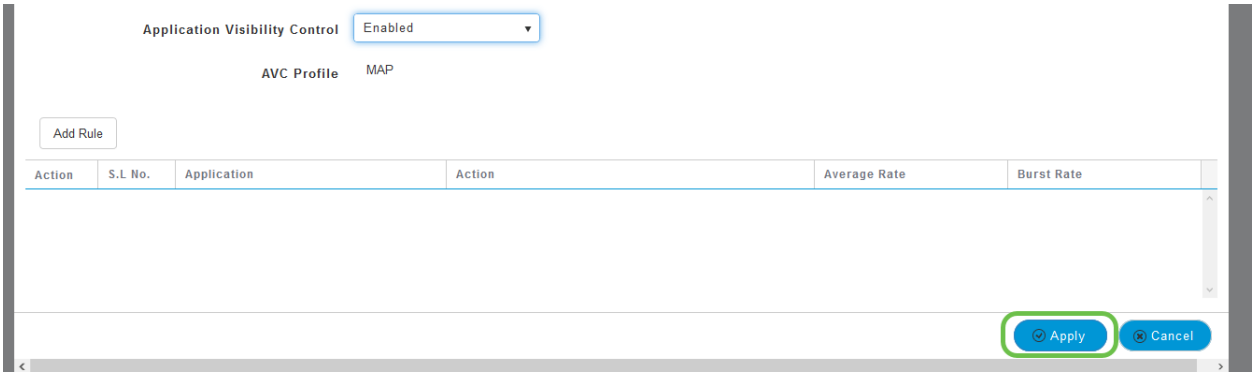

## Étape 5

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

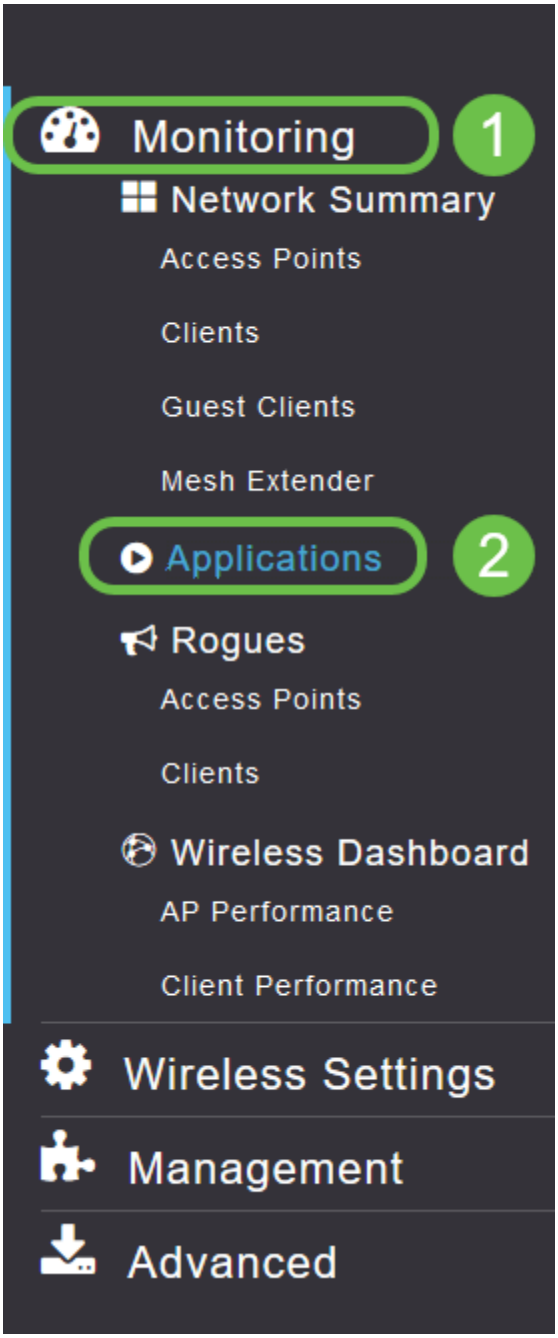
Cliquez sur le bouton **Appliquer**.



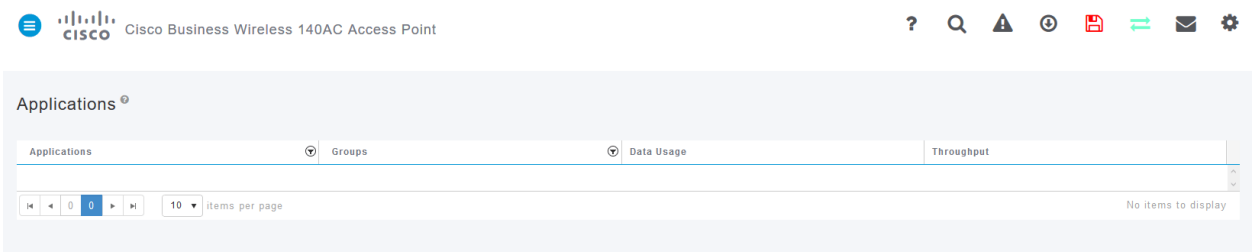

Ce paramètre doit être activé, sinon la fonction ne fonctionnera pas.

## 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 :

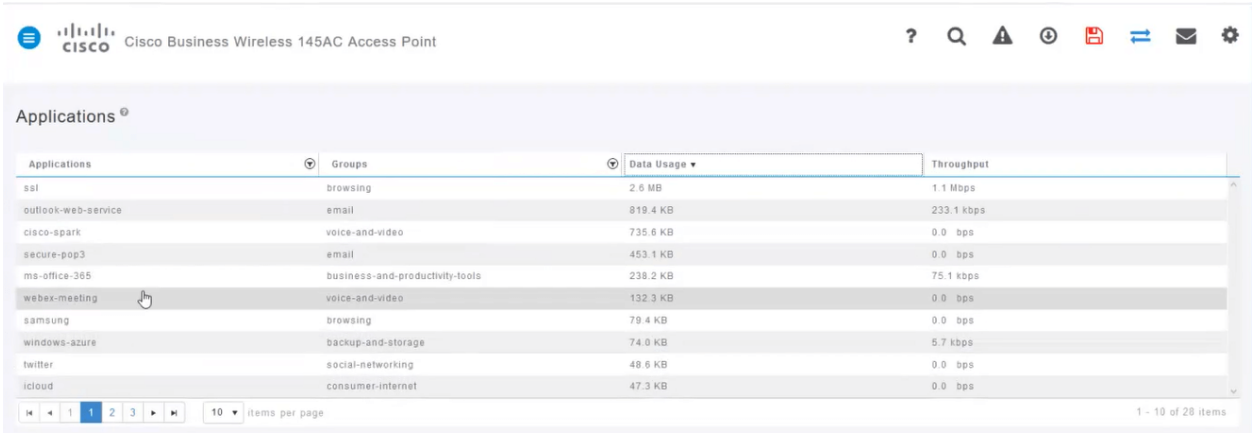
- Application : inclut de nombreux types différents
- Groupes : indique le type de groupe d'applications pour faciliter le tri
- Utilisation des données - Quantité de données utilisées par ce service dans son ensemble
- Débit : quantité de bande passante utilisée par l'application

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

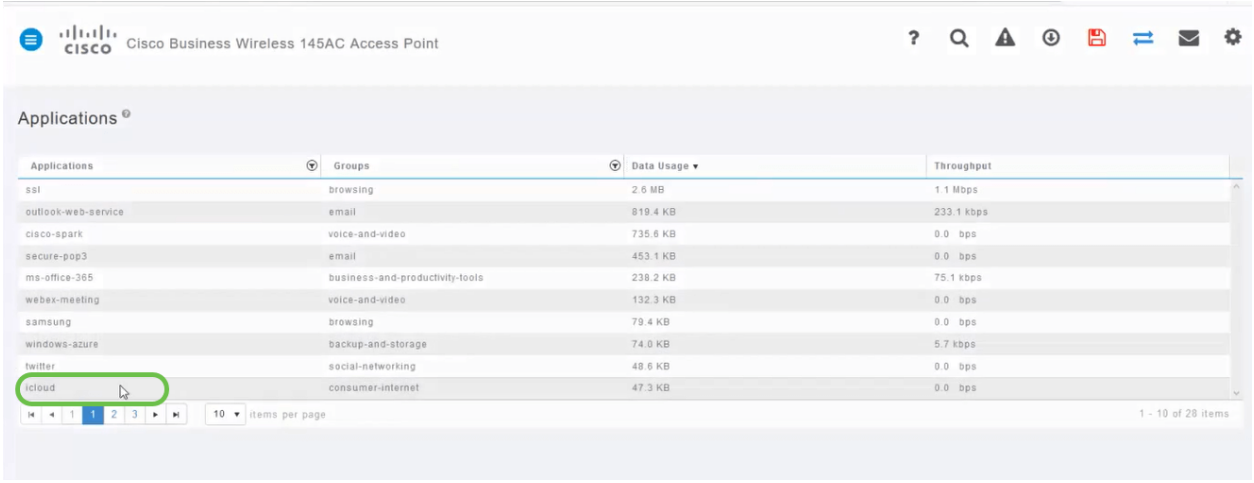
Voici un exemple de ce à quoi ressemblera la page lorsqu'elle sera remplie.




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

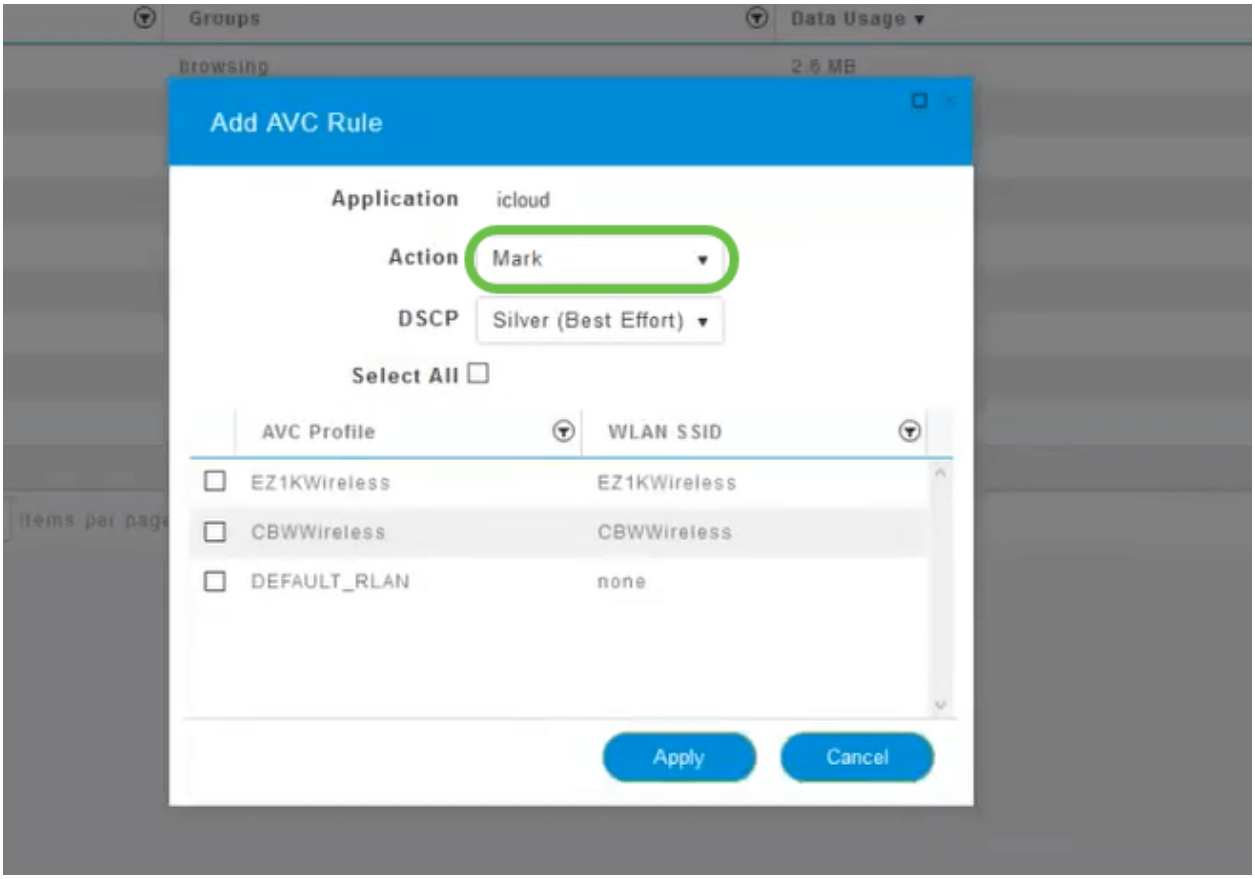
## Étape 8

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.



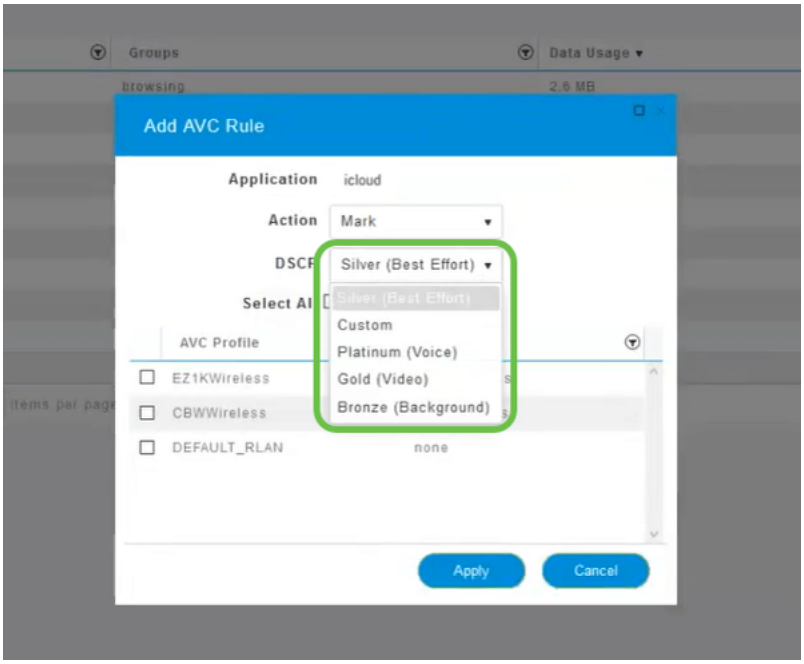

Pour cet exemple, nous laissons cette option à *Mark*.

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.



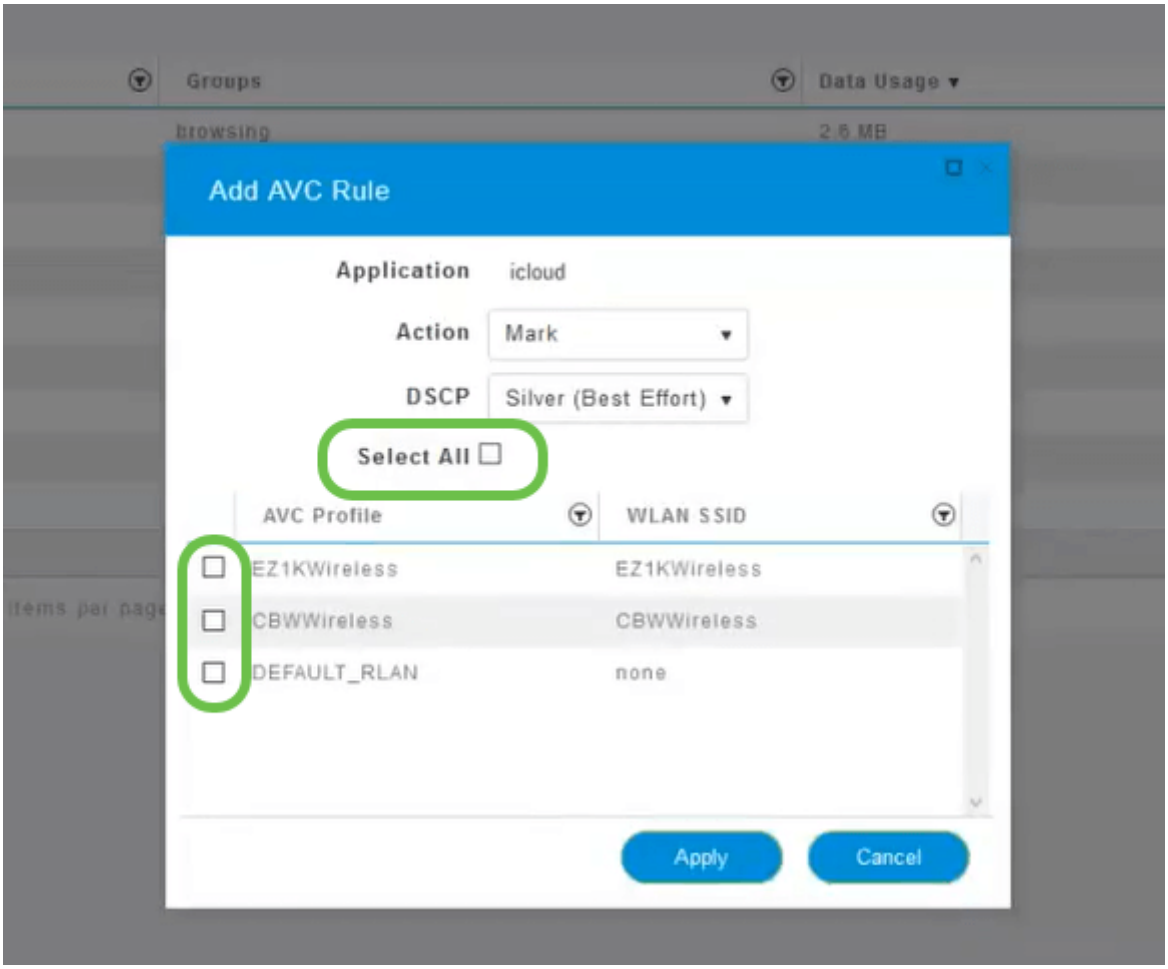

Vous trouverez ci-dessous les options DSCP du trafic à marquer. Ces options passent de moins de ressources à plus de ressources disponibles pour le type de trafic que vous modifiez.

- 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.

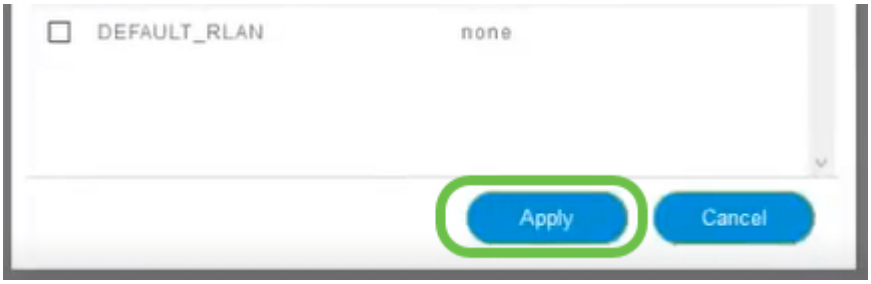
## Étape 11

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

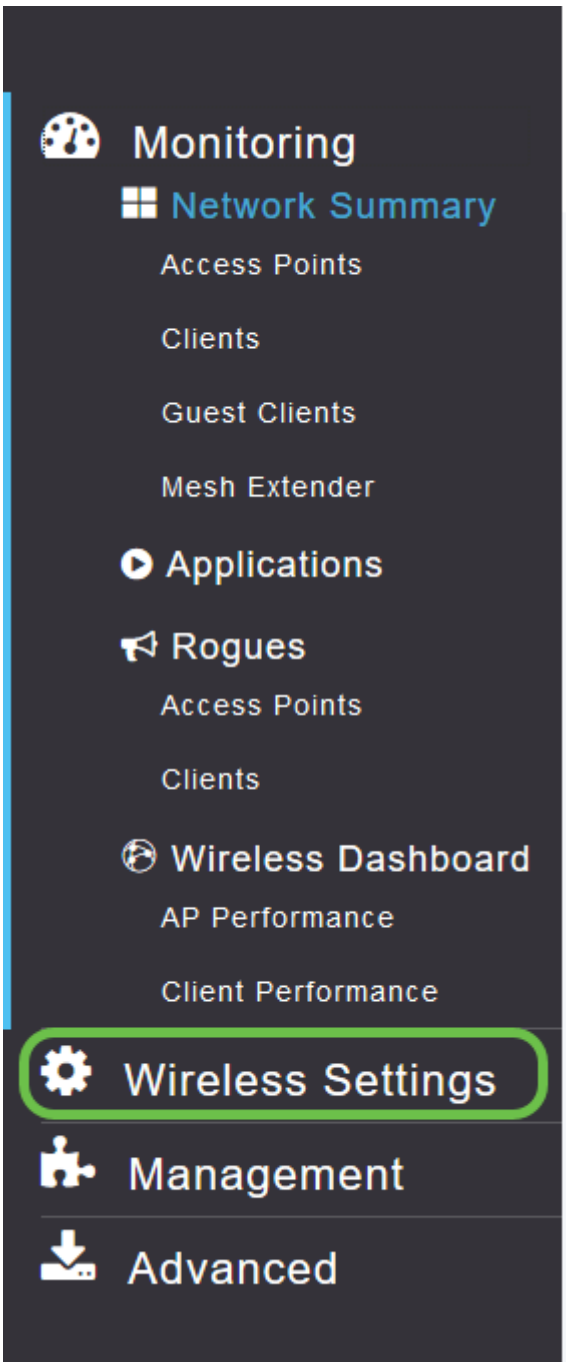
Les statistiques relatives à ces clients incluent la quantité de données utilisées et le débit.

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.

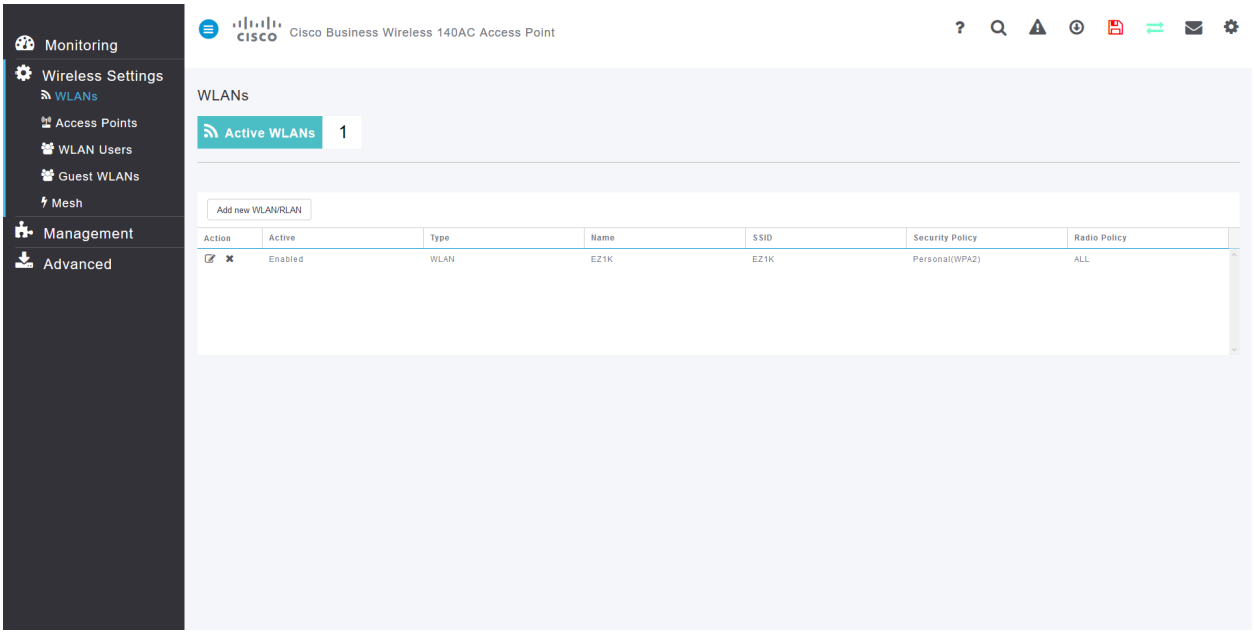
Une fois activé, les détails du client pour votre réseau se trouvent dans la section Surveillance de l'interface utilisateur Web.

## Étape 1

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

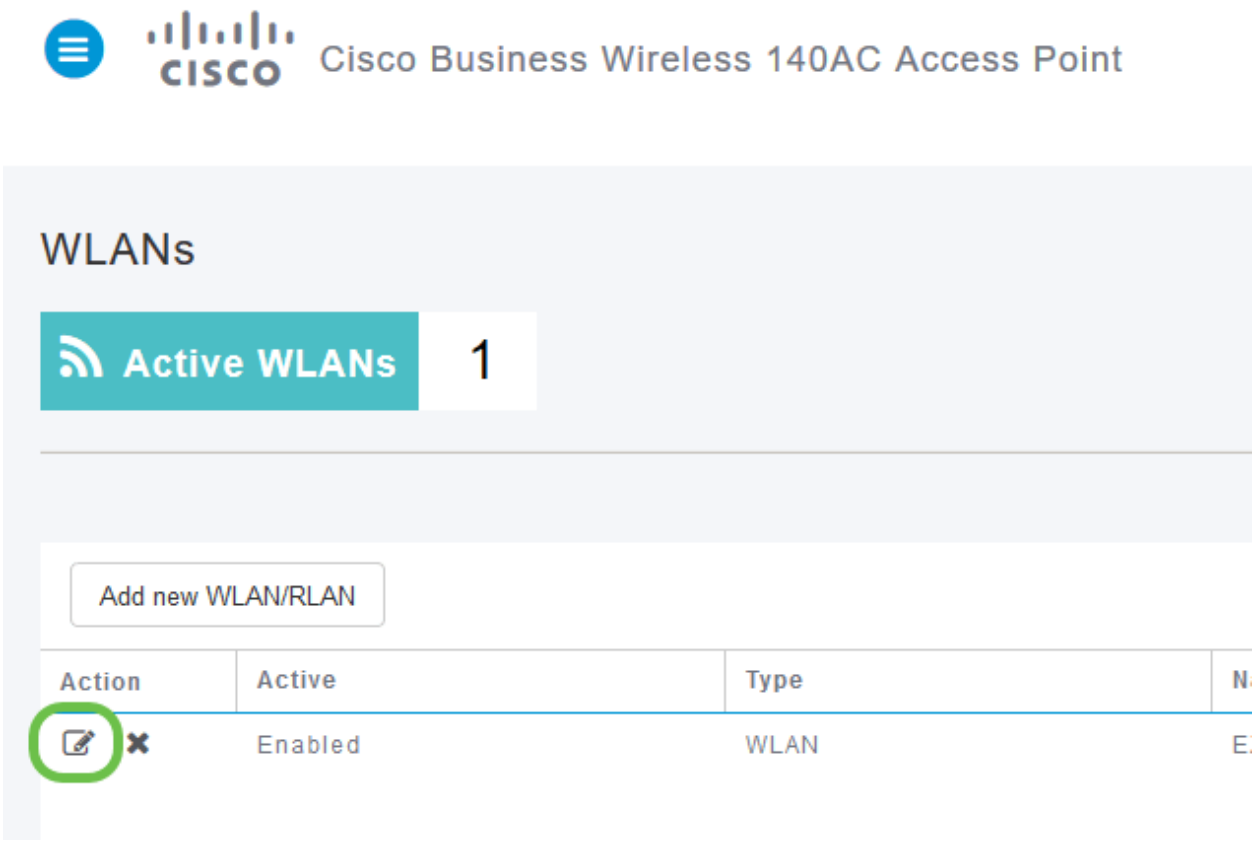



Les informations ci-dessous sont similaires à celles que vous verrez lorsque vous cliquez sur le lien Wireless Settings (Paramètres sans fil) :



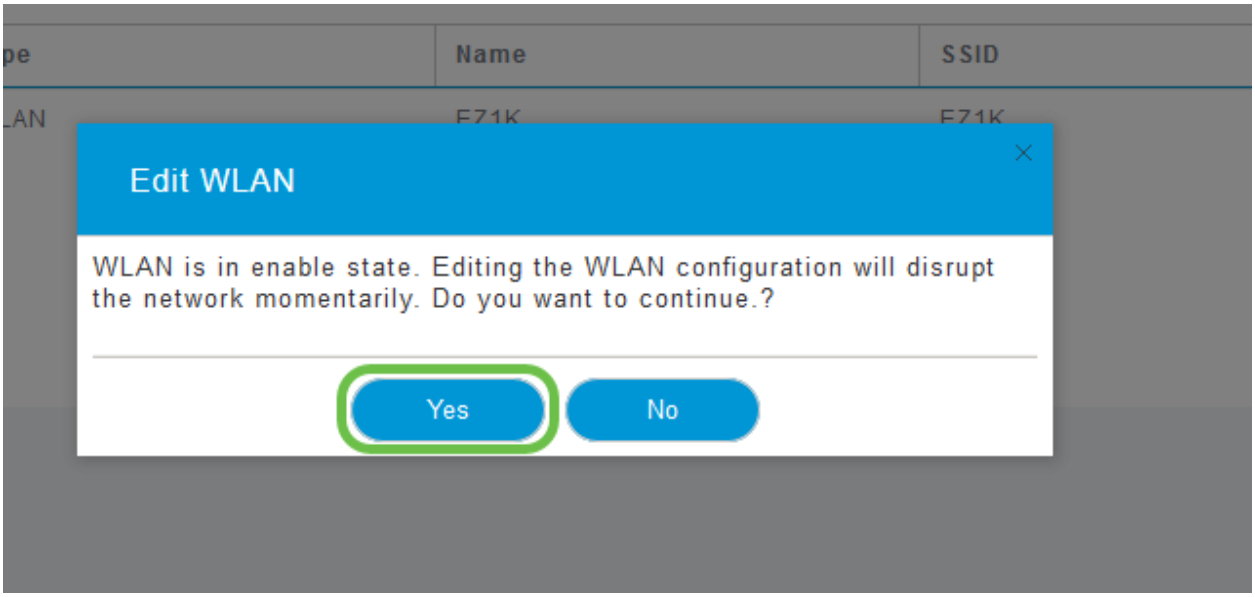

## Étape 2

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.

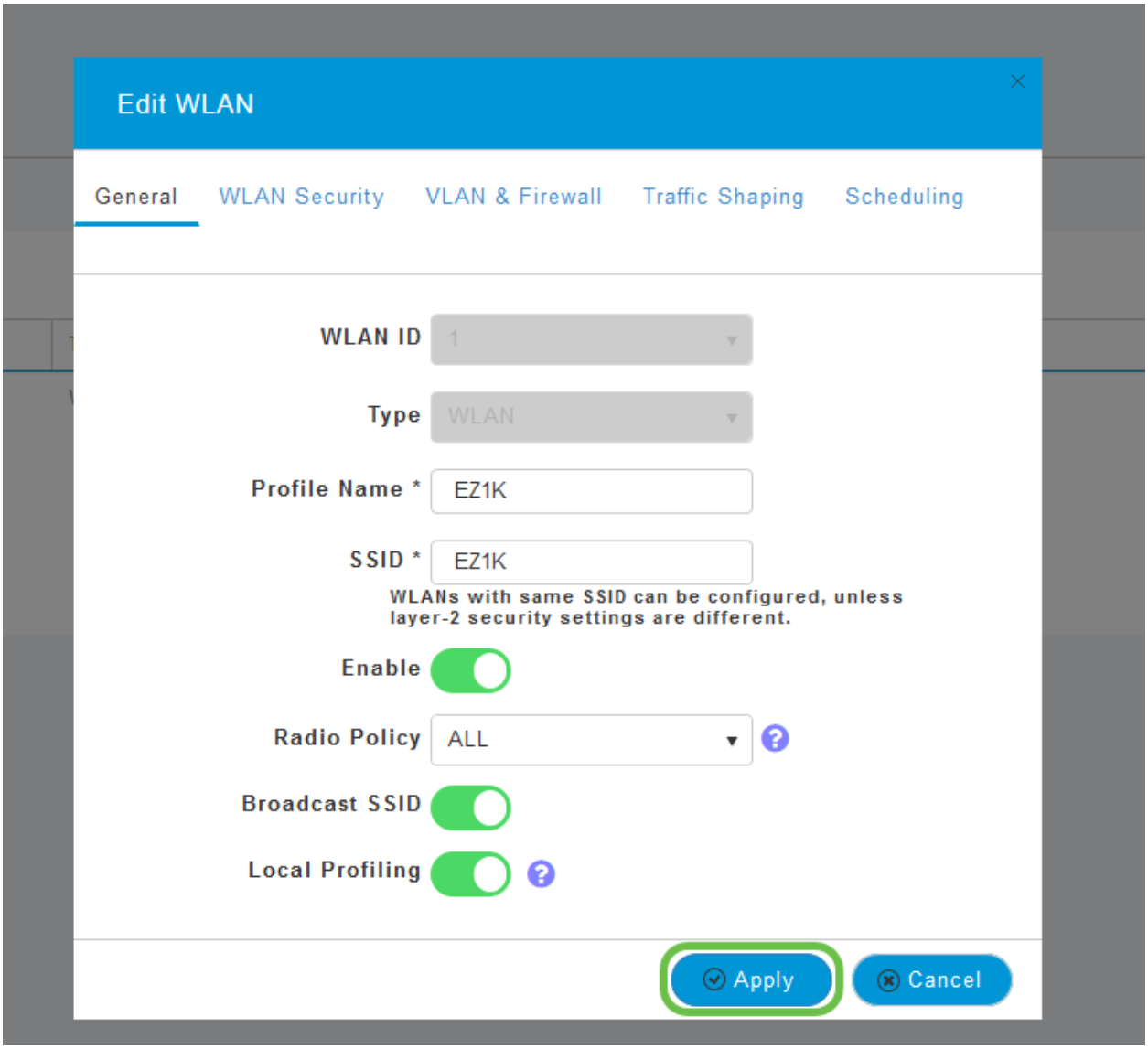



**Étape 4**

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

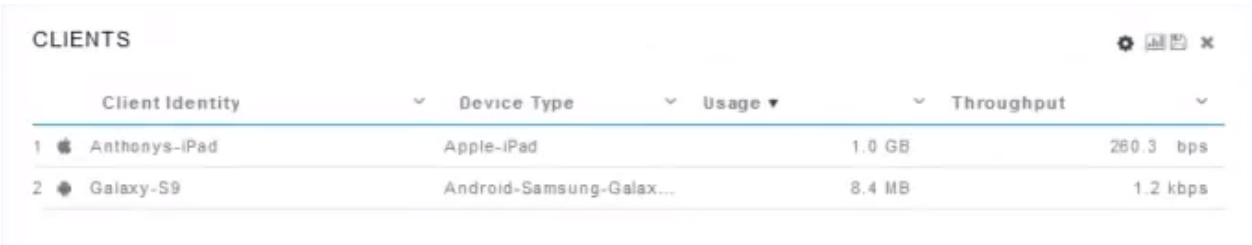

**Étape 5**

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 RV345P avec PoE
- Point d'accès Cisco Business 140AC
- Extendeur maillé Cisco Business 142ACM