Configuration réseau totale : RV345P et Cisco Business Wireless à l'aide de l'interface 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 réseau maillé CBW142ACM.

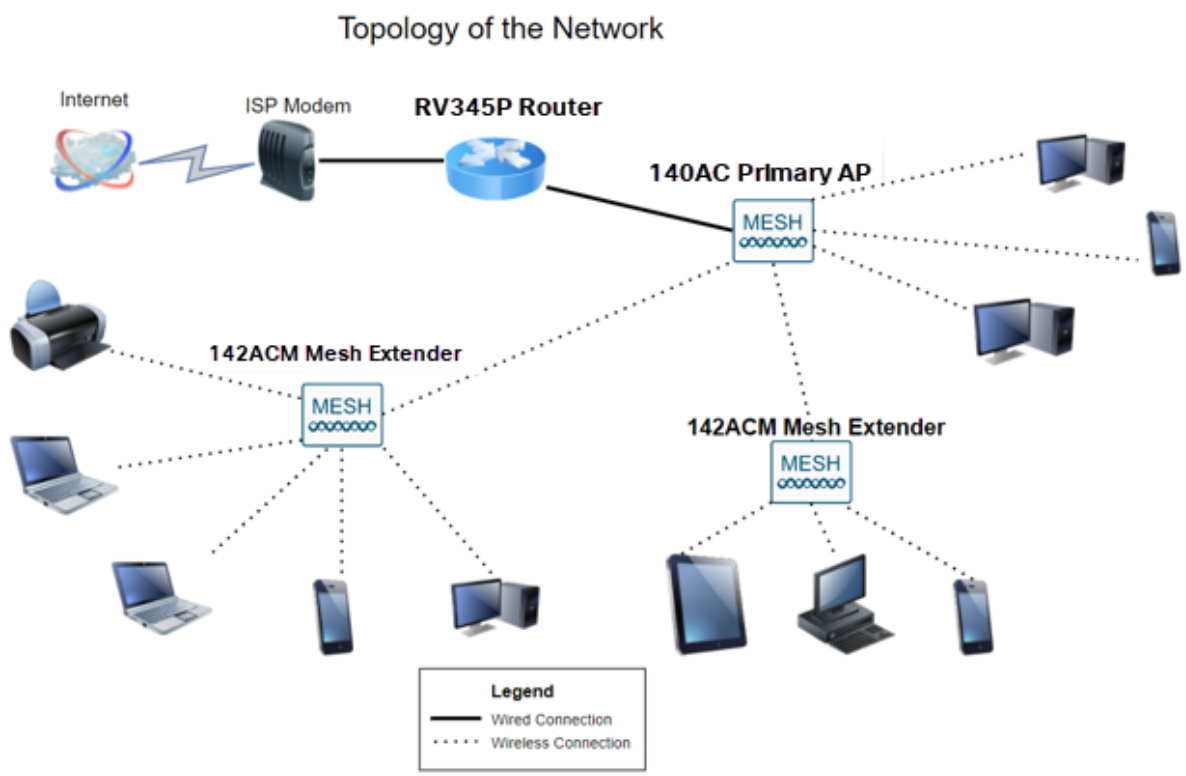
Cet article utilise l'interface utilisateur Web pour configurer le réseau sans fil maillé. Si vous préférez utiliser l'application mobile, qui est recommandée pour une configuration sans fil facile, cliquez pour passer à l'article qui utilise l'application mobile.

Table des matières

- Conditions préalables
  - Préparation du routeur
  - Obtenir un compte Cisco.com
- Configuration du routeur RV345P
  - RV345P prêt à l'emploi
  - Configuration du routeur
  - Dépannage de la connexion Internet
  - Configuration initiale
  - Modifiez une adresse IP si nécessaire (facultatif)
  - Mise à niveau du micrologiciel si nécessaire
  - Configuration des mises à jour automatiques sur le routeur de la gamme RV345P
- Options de sécurité
  - Licence de sécurité RV (en option)
  - Filtrage Web sur le routeur RV345P
  - Licence de filiale Umbrella RV (en option)
  - Autres options de sécurité
- Options VPN
  - Relais VPN
  - VPN AnyConnect
  - Shrew Soft VPN
  - Autres options VPN

- Configurations supplémentaires sur le routeur RV345P
    - Configuration des VLAN (facultatif)
    - Attribution de VLAN aux ports (facultatif)
    - Ajouter une adresse IP statique (facultatif)
    - Gestion des certificats (facultatif)
    - Configuration d'un réseau mobile à l'aide d'une clé et d'un routeur de la gamme RV345P (facultatif)
- Configuration du CBW140AC
    - CBW140AC prêt à l'emploi
    - Configuration du point d'accès sans fil principal 140AC sur l'interface utilisateur Web
- Conseils de dépannage sans fil
- Configuration des extendeurs de réseau maillé CBW142ACM à l'aide de l'interface utilisateur Web
- Vérifier et mettre à jour le logiciel via l'interface utilisateur Web
- Créer des WLAN sur l'interface utilisateur Web
- Configurations sans fil en option
    - Créer un WLAN invité à l'aide de l'interface utilisateur Web (facultatif)
    - Profilage d'application à l'aide de l'interface utilisateur Web (facultatif)
    - Profilage client à l'aide de l'interface utilisateur Web (facultatif)

Topologie



Introduction

Toutes vos recherches ont été regroupées et vous avez acheté votre équipement Cisco, c'est passionnant ! Dans ce scénario, nous utilisons un routeur RV345P. Ce routeur fournit une alimentation PoE (Power over Ethernet) qui vous permet de brancher le CBW140AC dans le routeur au lieu d'un commutateur. Les extendeurs de réseau maillé 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, le bloquer 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 de votre entreprise ou à vos data centers en créant un tunnel sécurisé via Internet.

Si vous souhaitez 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 n'êtes pas familier avec certains des termes utilisés dans ce document ou si vous voulez plus de détails sur la mise en réseau maillé, consultez les articles suivants :

- Cisco Business : Glossaire de nouveaux termes
- Bienvenue dans le réseau maillé sans fil professionnel Cisco
- Foire aux questions (FAQ) sur un réseau sans fil professionnel Cisco

Périphériques pertinents | Version logicielle

- 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 pour la configuration.
2. Contactez votre fournisseur d'accès Internet (FAI) pour connaître les instructions spéciales dont il dispose lors de l'utilisation de votre routeur RV345P. Certains FAI proposent des passerelles avec des routeurs intégrés. Si vous disposez d'une passerelle avec un routeur intégré, vous devrez peut-être désactiver le routeur et transmettre l'adresse IP du réseau étendu (WAN) (l'adresse de protocole Internet unique que le fournisseur Internet attribue à votre compte) et tout le trafic réseau à votre nouveau routeur.
3. Choisissez l'emplacement du routeur. Vous aurez besoin d'un espace ouvert si possible. Cela peut s'avérer difficile, car vous devez connecter le routeur à la passerelle large bande (modem) depuis votre fournisseur d'accès Internet (FAI).

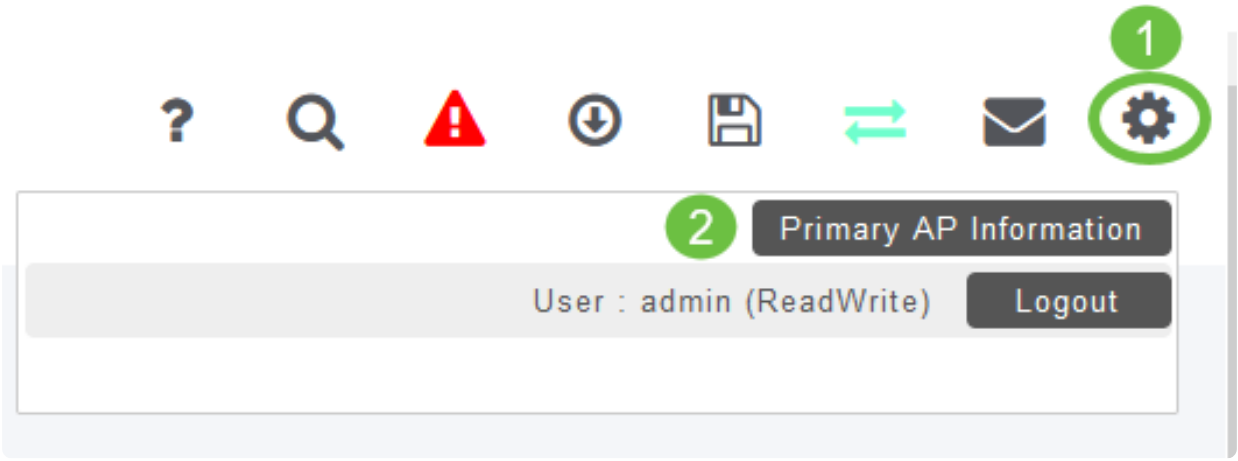
Obtenir un compte Cisco.com

Maintenant que vous possédez des équipements Cisco, vous devez obtenir un compte Cisco.com, parfois appelé ID CCO (Cisco Connection Online Identification). 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.

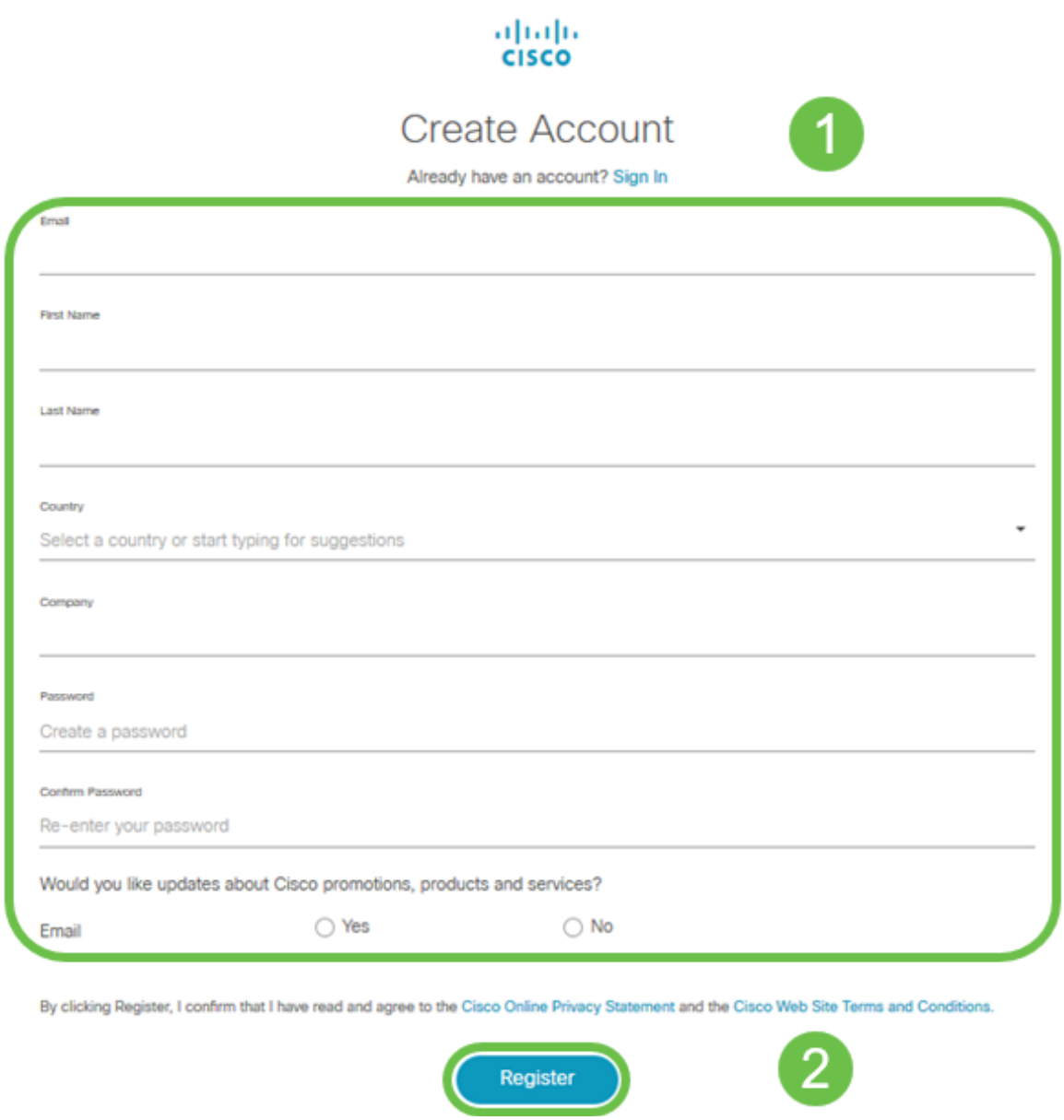
Étape 1

Accédez à Cisco.com. Cliquez sur l'icône Personne, puis sur Créer 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 Cisco.com page d'aide sur l'enregistrement de compte.

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 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 exigences réseau ou votre fournisseur d'accès Internet (FAI) peuvent vous demander de modifier 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.

Es-tu prêt ? Passons à l'étape suivante !

RV345P prêt à l'emploi

Étape 1

Connectez le câble Ethernet de l'un des ports LAN (Ethernet) 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 modèle RV345P. L'utilisation d'un adaptateur secteur différent peut endommager le RV345P ou provoquer la défaillance des clés USB. L'interrupteur d'alimentation est allumé par défaut.

Connectez l'adaptateur électrique au port 12 VCC du RV345P, mais ne le branchez pas encore sur le secteur.

Étape 3

Assurez-vous que le modem est éteint.

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 mis sous tension. Rebranchez le modem afin qu'il puisse également se mettre sous tension. Le voyant d'alimentation situé sur le panneau avant reste vert lorsque l'adaptateur électrique est correctement connecté et que le démarrage du RV345P est terminé.

Configuration du routeur

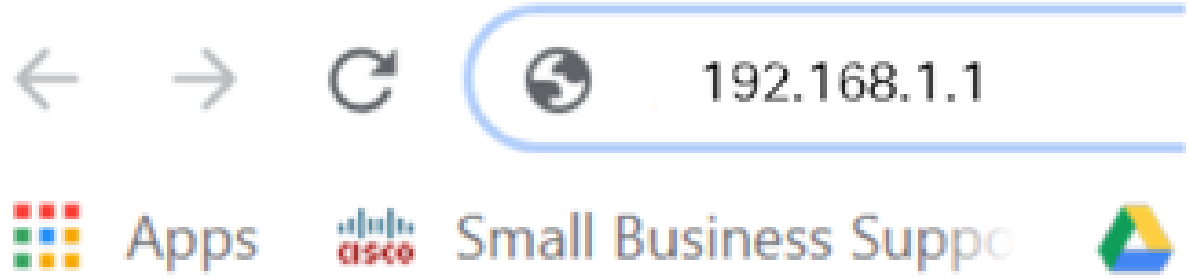
Le travail de préparation est terminé, il est temps d'accéder à certaines configurations ! Pour lancer l'interface utilisateur Web, procédez comme suit.

Étape 1

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

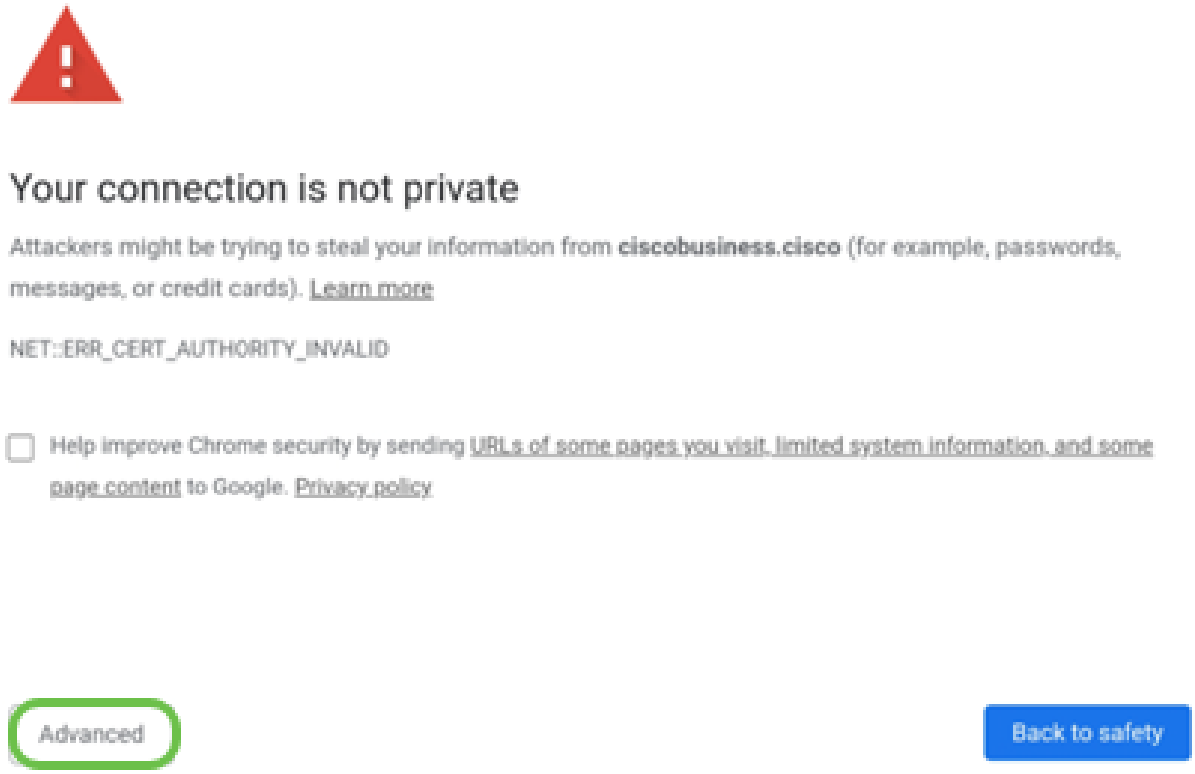
Étape 2

Ouvrez un navigateur Web tel que Safari, Internet Explorer ou Firefox. Dans la barre d'adresse, 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.

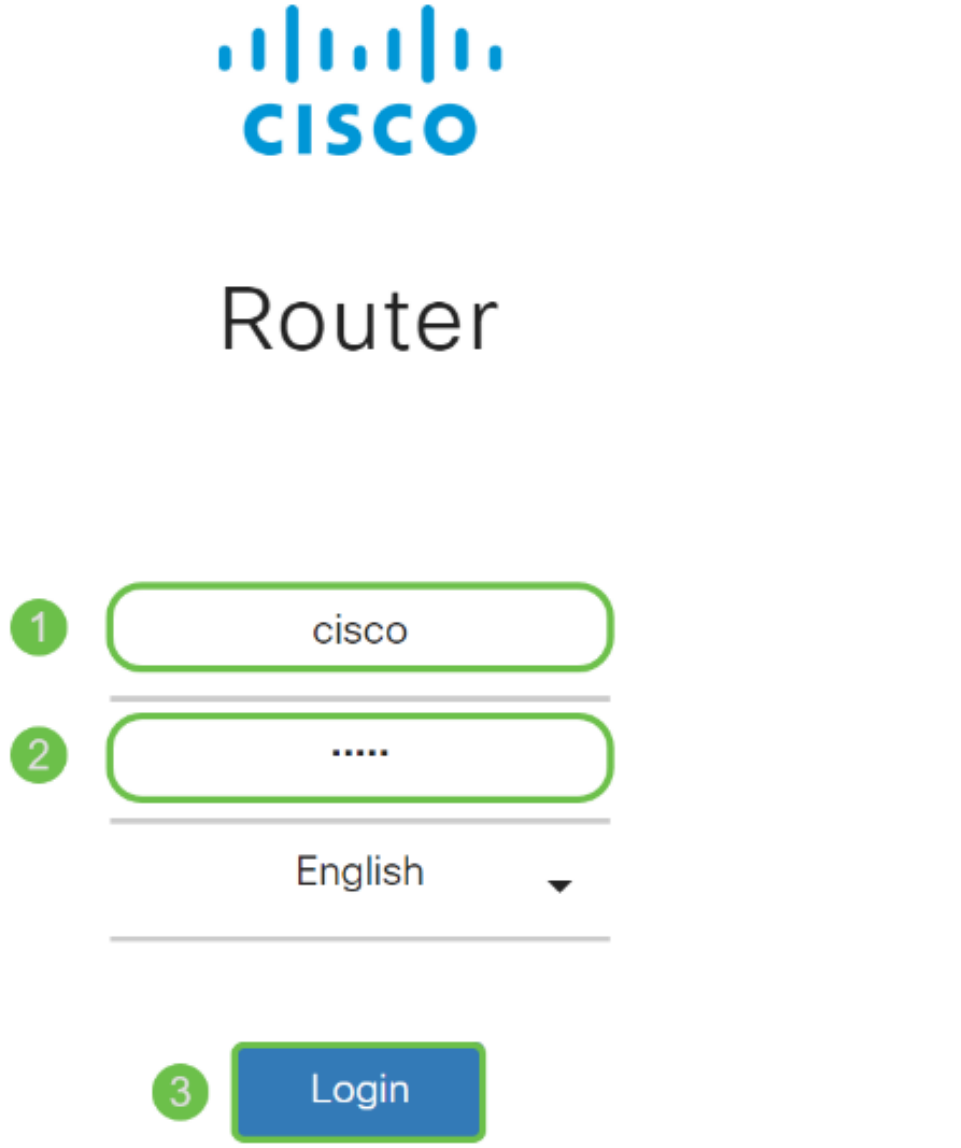


Étape 4

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

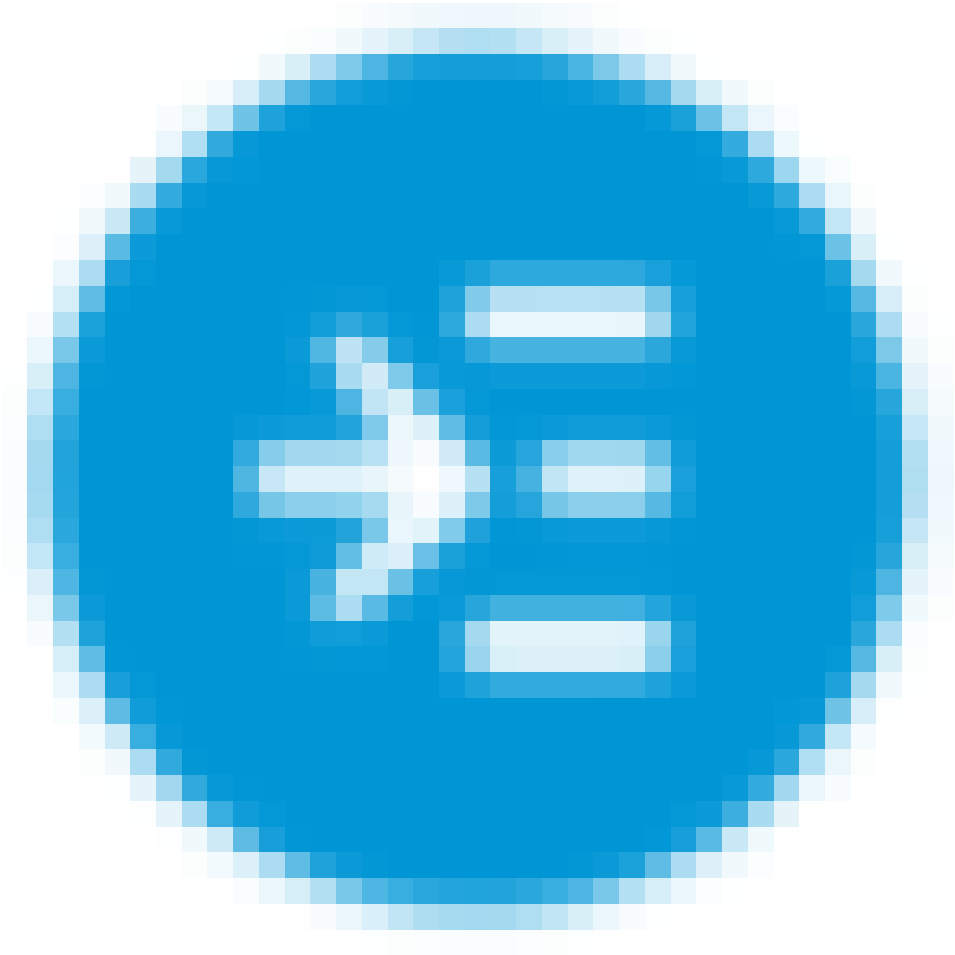
Cliquez sur Connexion.

Pour obtenir des informations détaillées, cliquez sur How to access the web-based setup page of Cisco RV340 series VPN routers.



Étape 5

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



Maintenant que vous avez confirmé la connexion et que vous êtes connecté au routeur, passez à la section Configuration initiale de cet article.

Dépannage de la connexion Internet

Mince, si vous lisez ceci, vous avez probablement des difficultés à vous connecter à Internet ou à l'interface utilisateur Web. L'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 (l'adresse IP par défaut du routeur). Si la demande expire, vous ne pouvez pas

communiquer avec le routeur.

Si la connectivité n'est pas établie, consultez cet article Dépannage.

Autres choses à essayer :

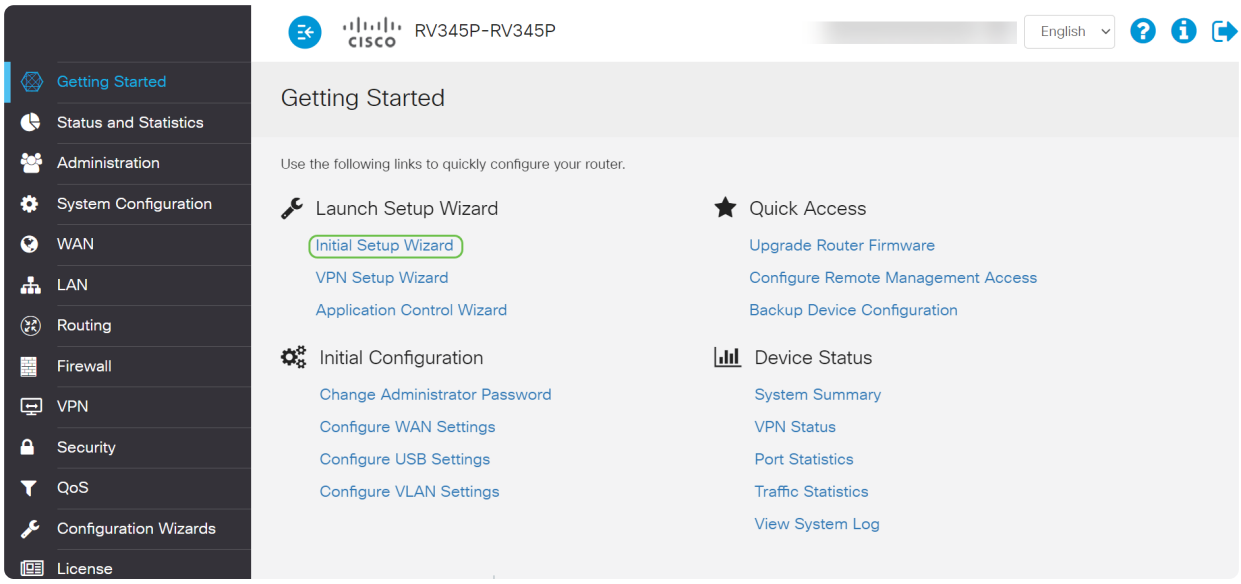
1. Vérifiez que votre navigateur Web n'est pas défini sur Travailler hors connexion.
2. Vérifiez les paramètres de connexion au réseau local de votre adaptateur Ethernet. Le PC doit obtenir une adresse IP via DHCP. Le PC peut également avoir une adresse IP statique dans la plage 192.168.1.x avec la passerelle 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 déjà d'un équipement qui occupe l'adresse IP 192.168.1.1, vous devrez résoudre ce conflit pour que le réseau fonctionne. Plus d'informations à ce sujet à la fin de cette section, ou cliquez ici pour être pris là directement.
4. Réinitialisez le modem et le RV345P en mettant les deux périphériques hors tension. 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 disposez d'un modem DSL, demandez à votre FAI de le mettre en mode pont.

Configuration initiale

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

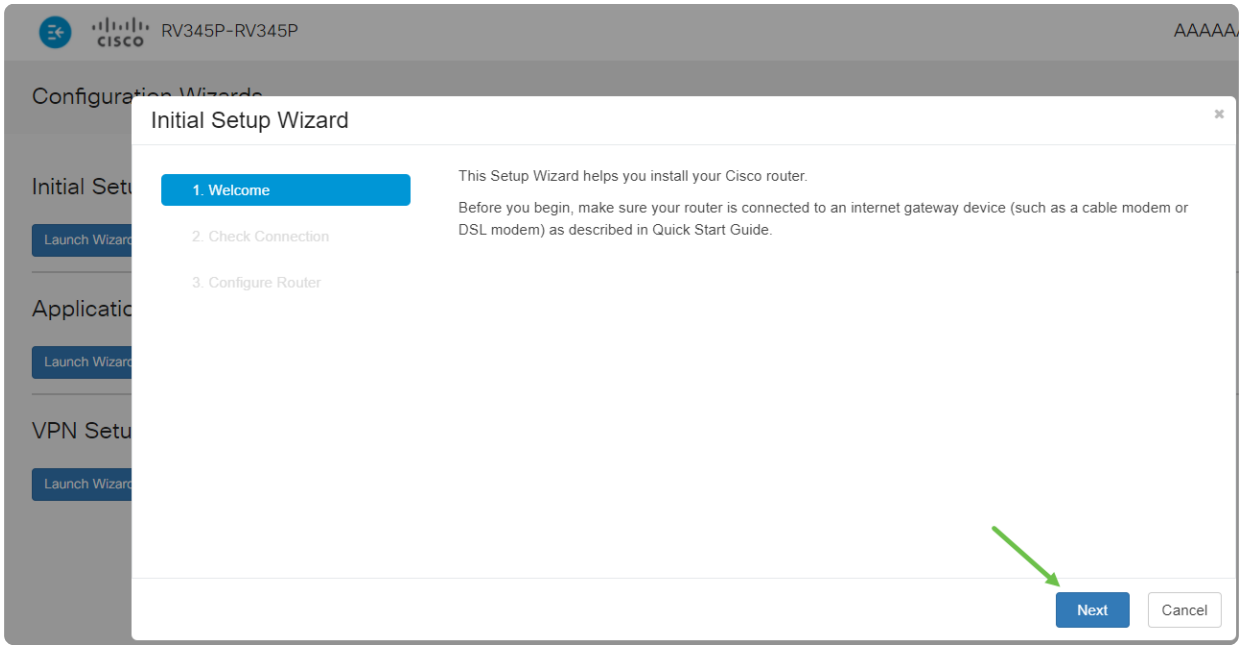
Étape 1

Cliquez sur Initial Setup Wizard dans la page Getting Started.



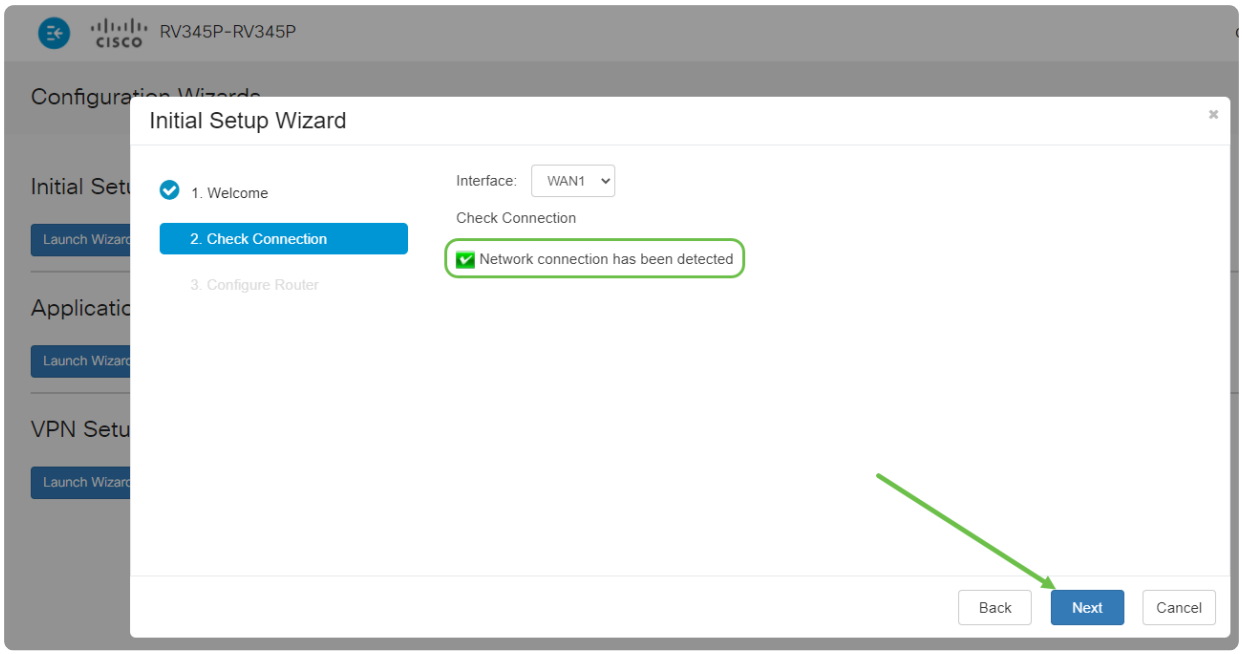
Étape 2

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



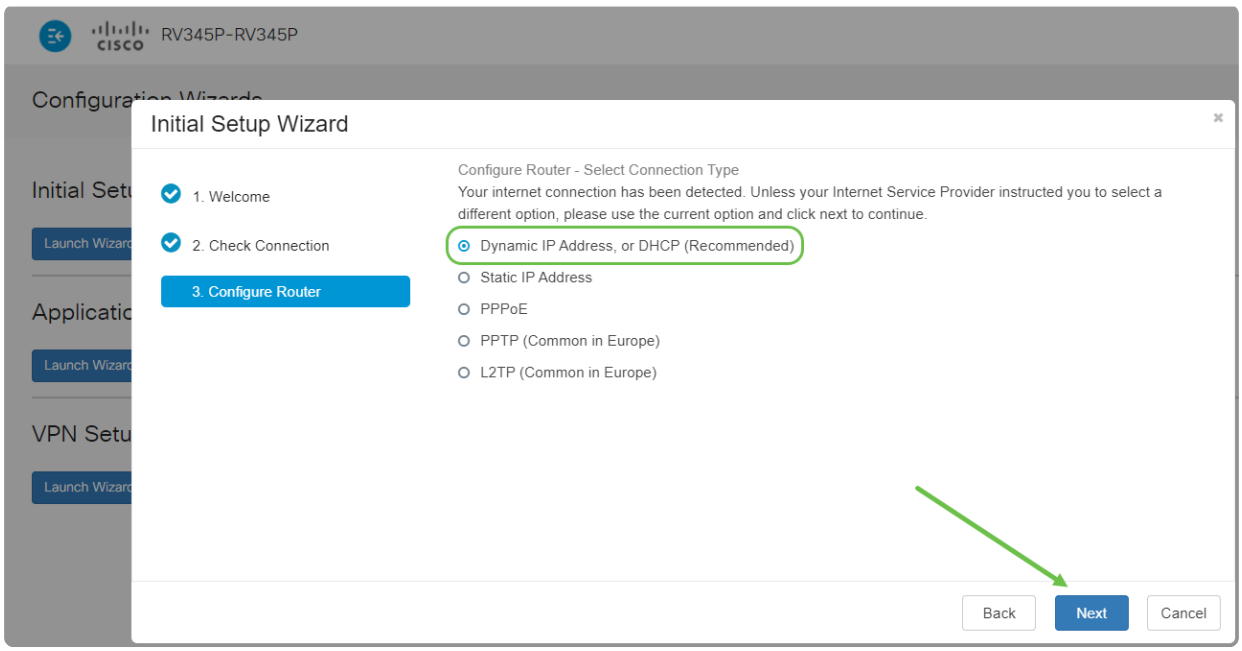
Étape 3

Cette étape couvre les étapes de base permettant de s'assurer que votre routeur est connecté. Comme vous l'avez déjà confirmé, cliquez sur Next.



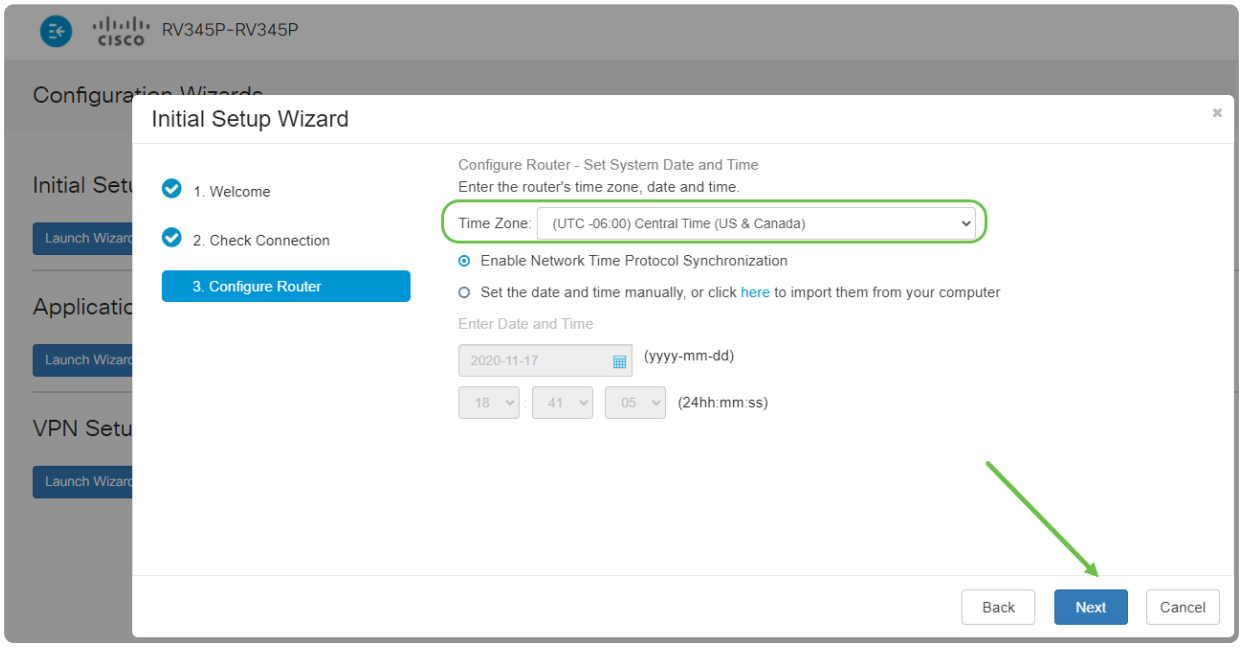
Étape 4

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).



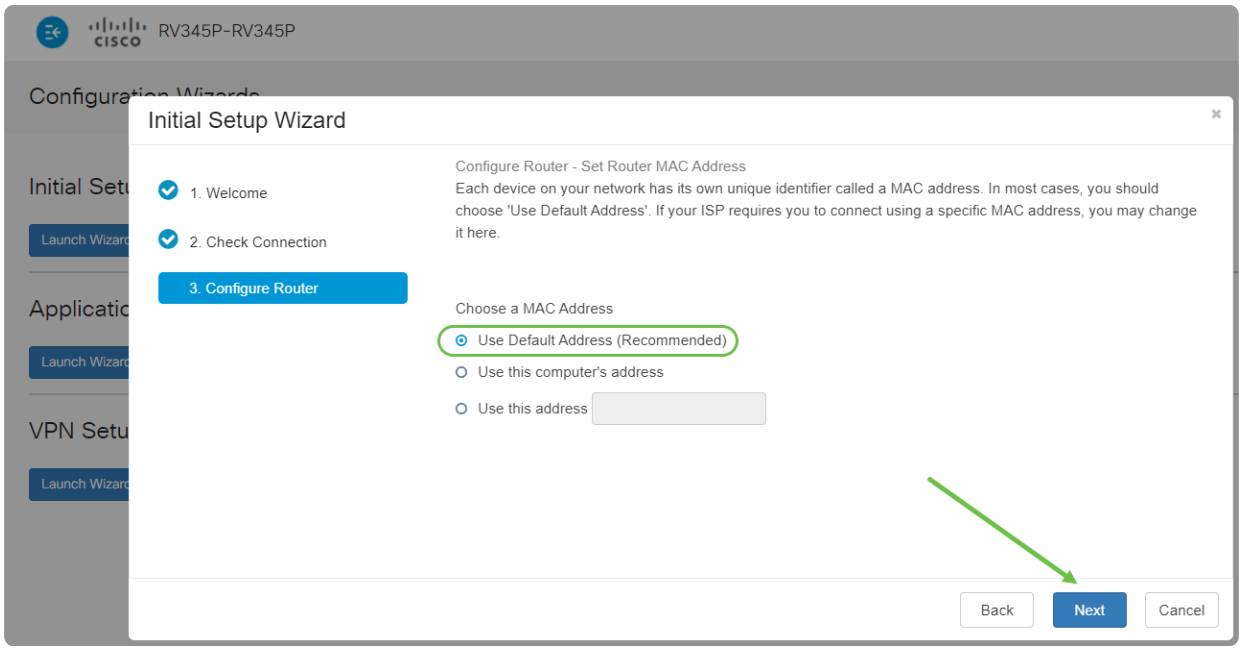
Étape 5

Vous serez invité à définir les paramètres d'heure de votre routeur. Ceci est important car il permet la précision lors de l'examen des journaux ou du dépannage des événements. Sélectionnez votre fuseau horaire, puis cliquez sur Suivant.



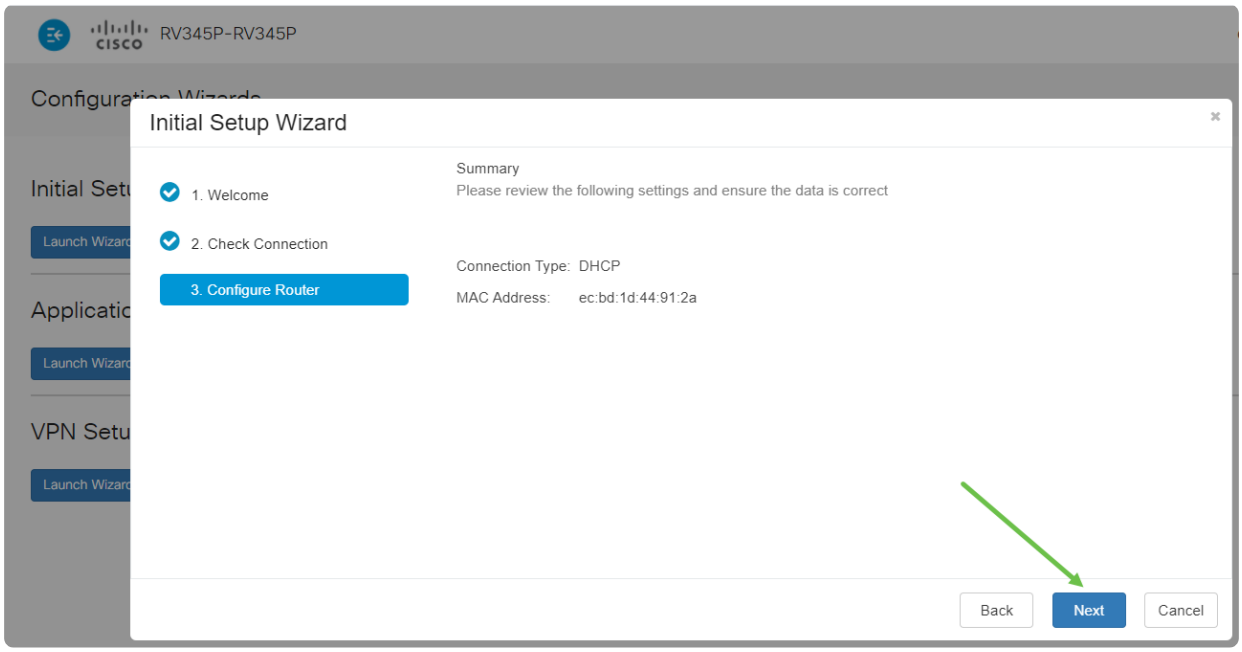
Étape 6

Vous allez sélectionner les adresses MAC à attribuer aux périphériques. Le plus souvent, vous utiliserez l'adresse par défaut. Cliquez sur Next (Suivant).



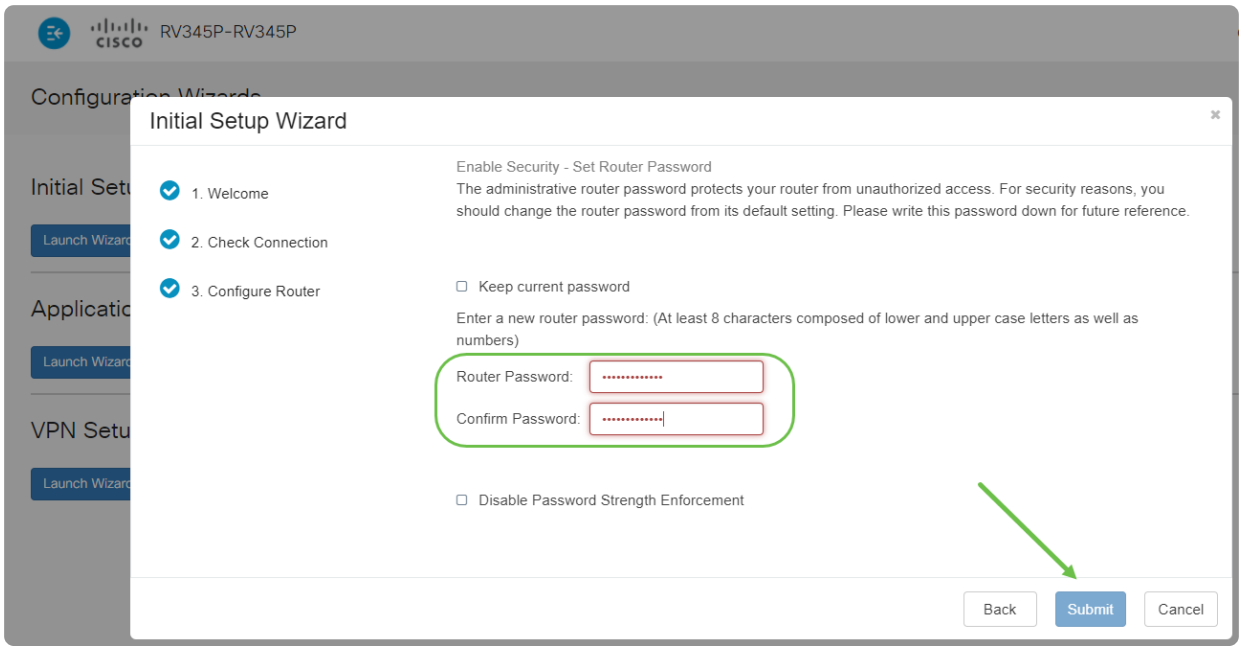
Étape 7

La page suivante récapitule les options sélectionnées. Vérifiez et cliquez sur Next 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. La norme pour les mots de passe est de contenir au moins 8 caractères (majuscules et minuscules) et d'inclure 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.



> ⓘ Note: 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, qui serait aussi facile que 1-2-3 pour les acteurs malveillants de craquer.

Étape 9

Cliquez sur l'icône Enregistrer.



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

Par défaut, la technologie Power over Ethernet (PoE) est activée sur votre RV345P, mais vous pouvez y apporter des modifications. Si vous devez personnaliser les paramètres, consultez Configurer les paramètres PoE (Power over Ethernet) sur le

routeur RV345P.

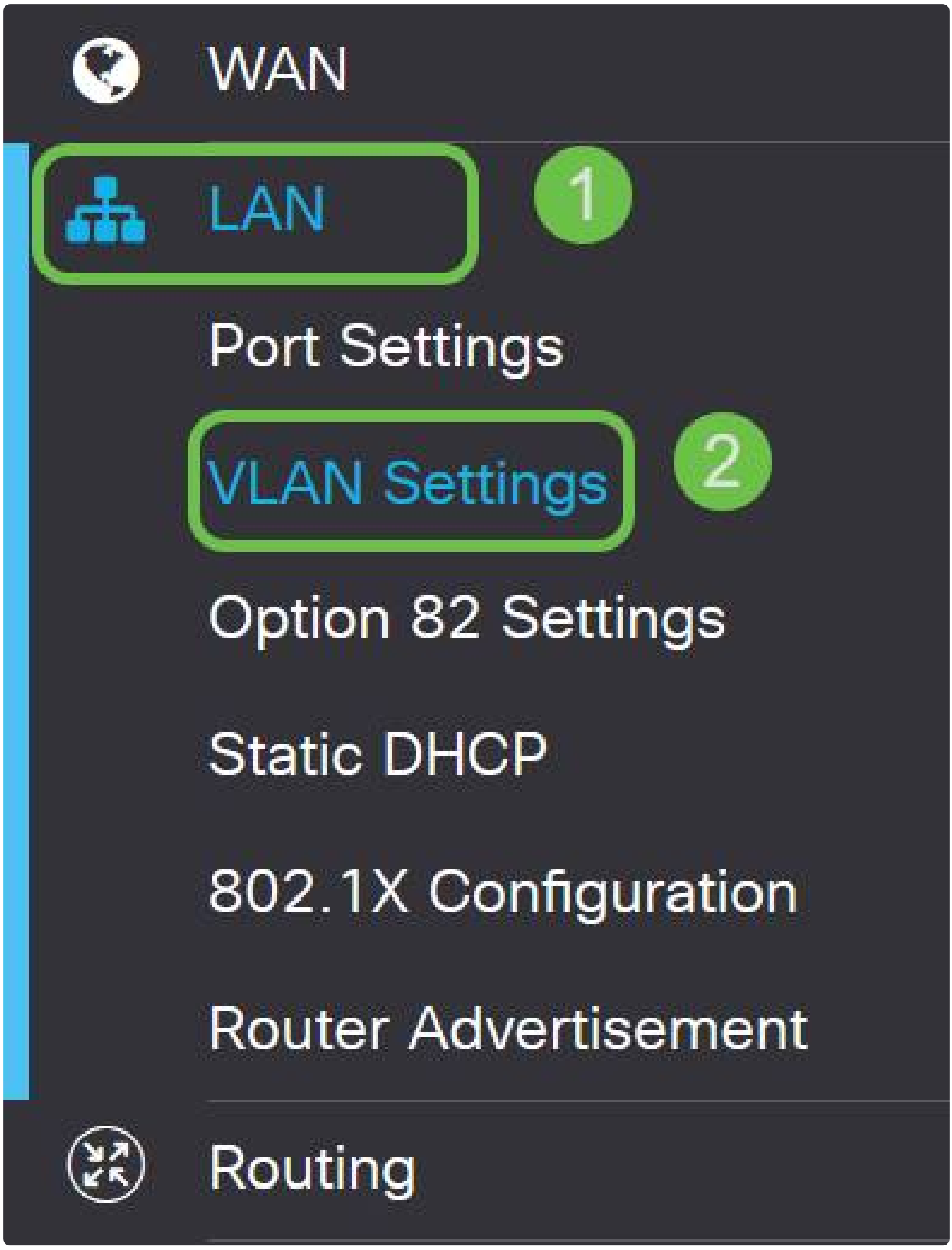
Modifiez une adresse IP si nécessaire (facultatif)

Une fois l'Assistant de configuration initiale terminé, 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.

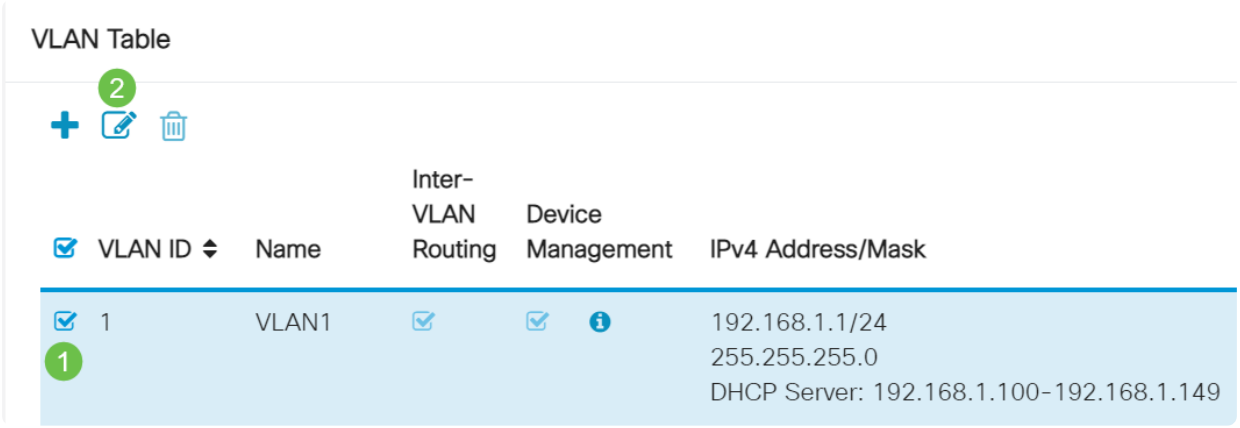
Étape 1

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



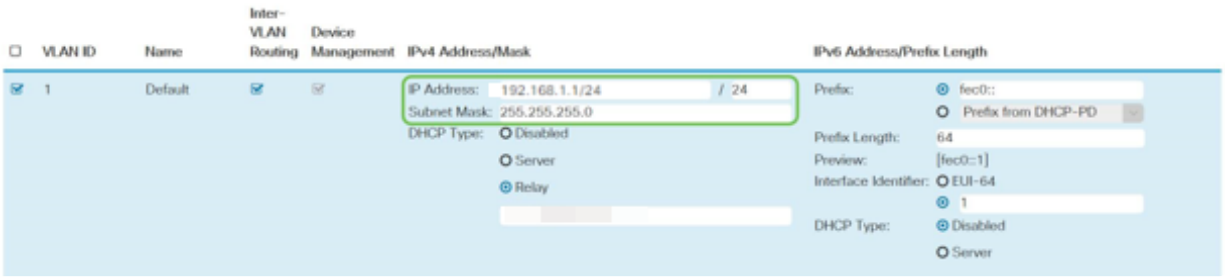
Étape 2

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



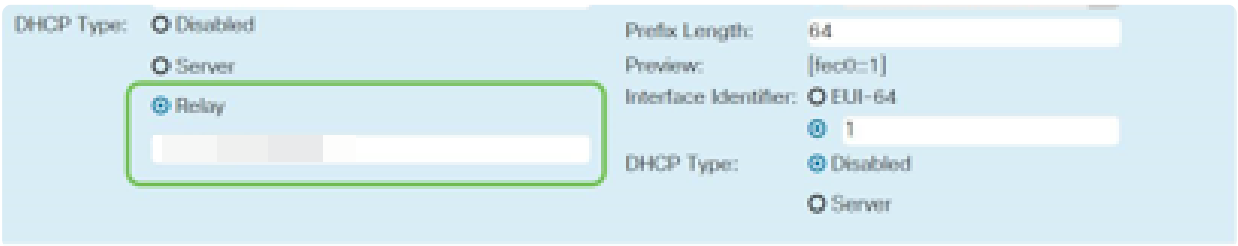
Étape 3

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 les adresses IP, vous pouvez utiliser la fonctionnalité de relais DHCP pour diriger les requêtes DHCP vers une adresse IP spécifique. L'adresse IP est probablement le routeur connecté au WAN/à Internet.

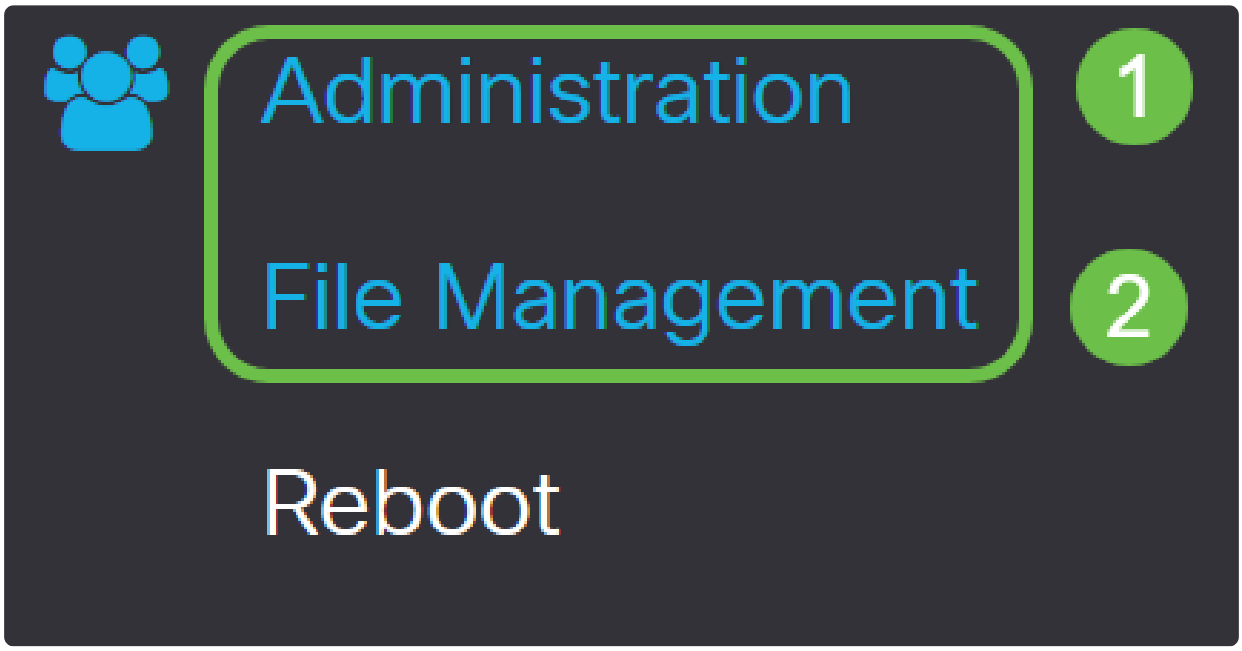


Mise à niveau du micrologiciel si nécessaire

Il s'agit d'une étape importante, ne la sautez pas !

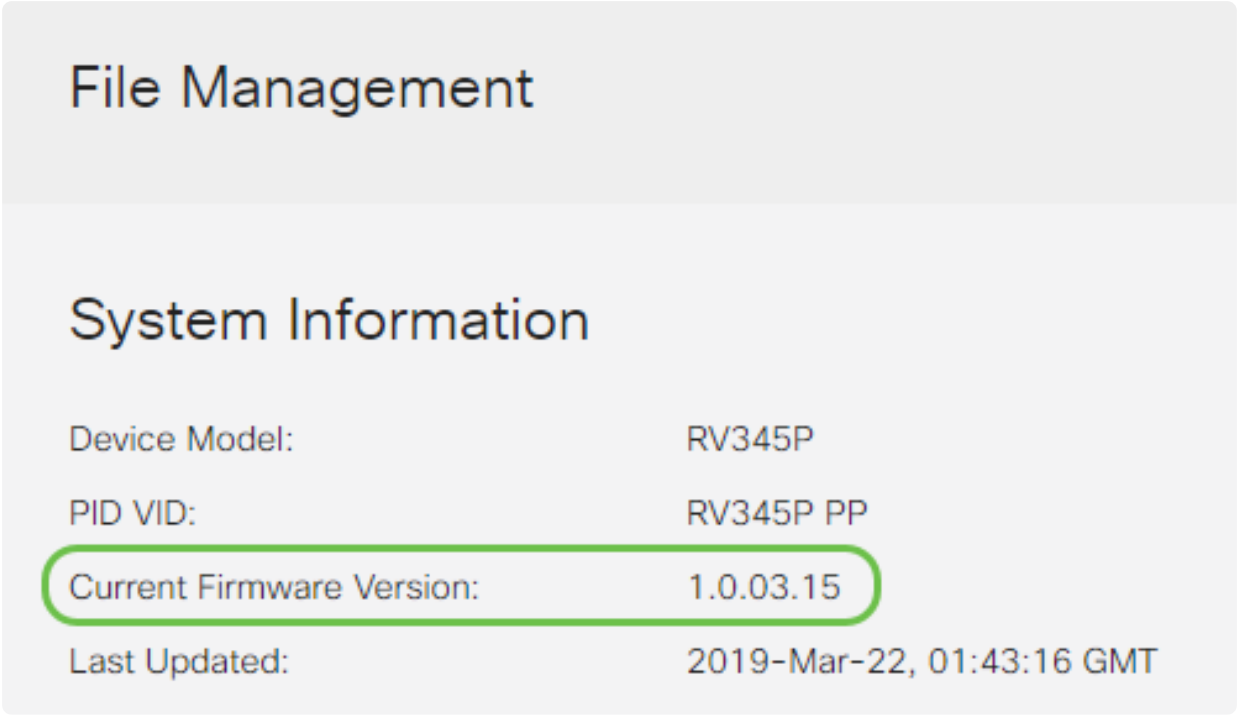
Étape 1

Choisissez Administration > File Management.



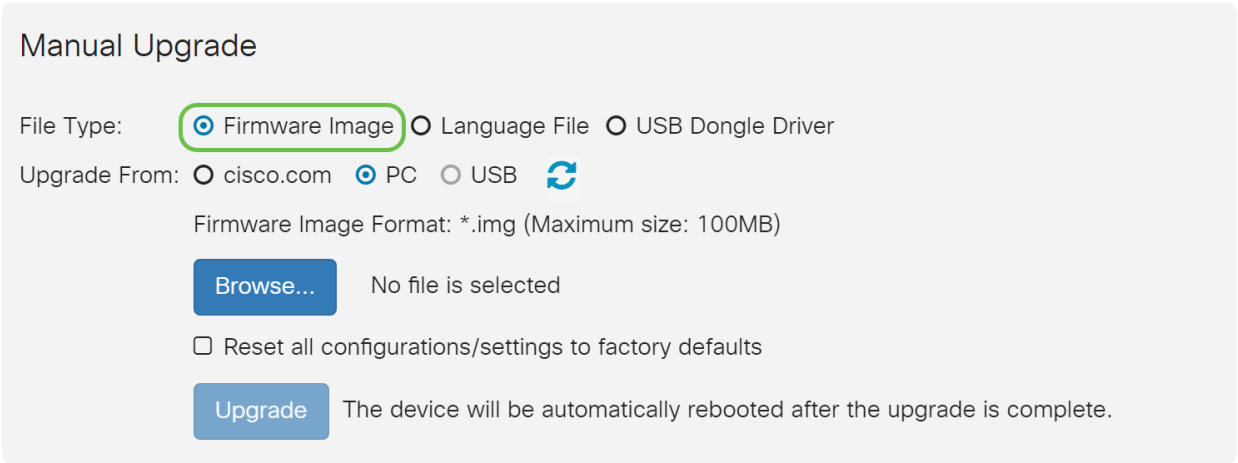
Dans la zone Informations système, les sous-zones suivantes décrivent les éléments suivants :

- Device Model : affiche le modèle de votre périphérique.
- PID VID - ID de produit et ID de fournisseur du routeur.
- Current Firmware Version (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.
- Firmware last update : date et heure de la dernière mise à jour du micrologiciel effectuée sur le routeur.



Étape 2

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

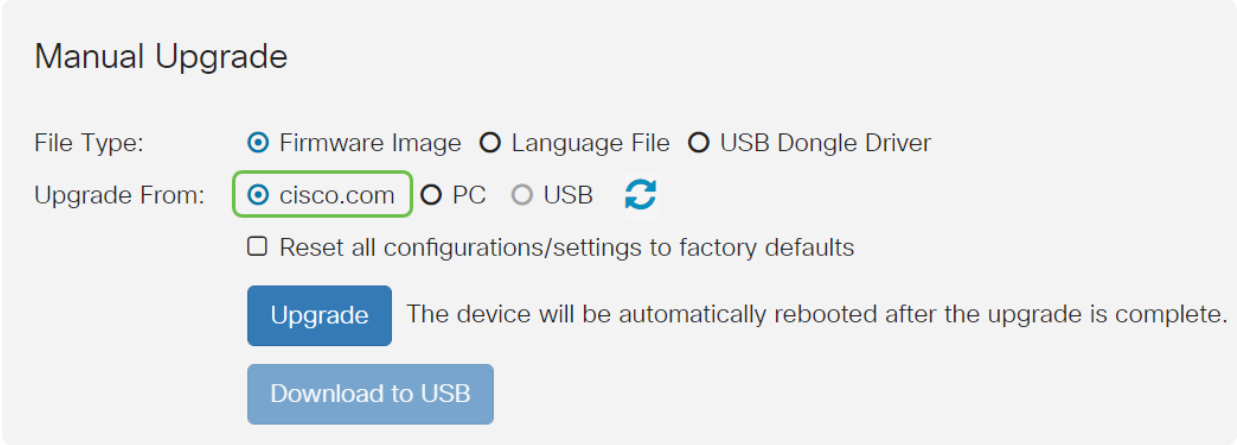


Étape 3

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

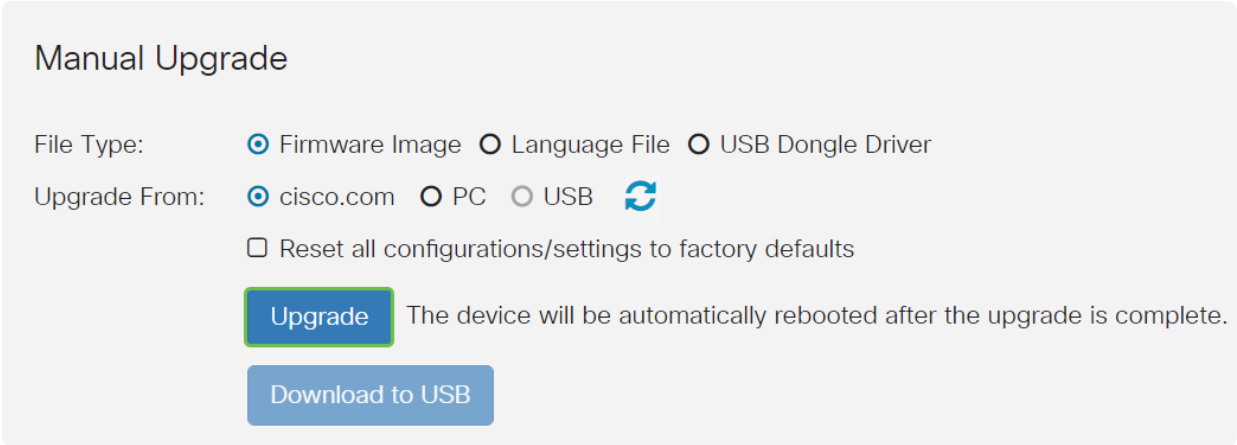
partir de la page Web Téléchargements de logiciels Cisco.

> ⓘ Note: Si votre appareil n'est pas connecté à Internet ou s'il souffre de déconnexions Internet, vous ne pourrez pas effectuer la mise à niveau à partir de cisco.com. Si cela vous concerne, d'autres options peuvent être trouvées ici.



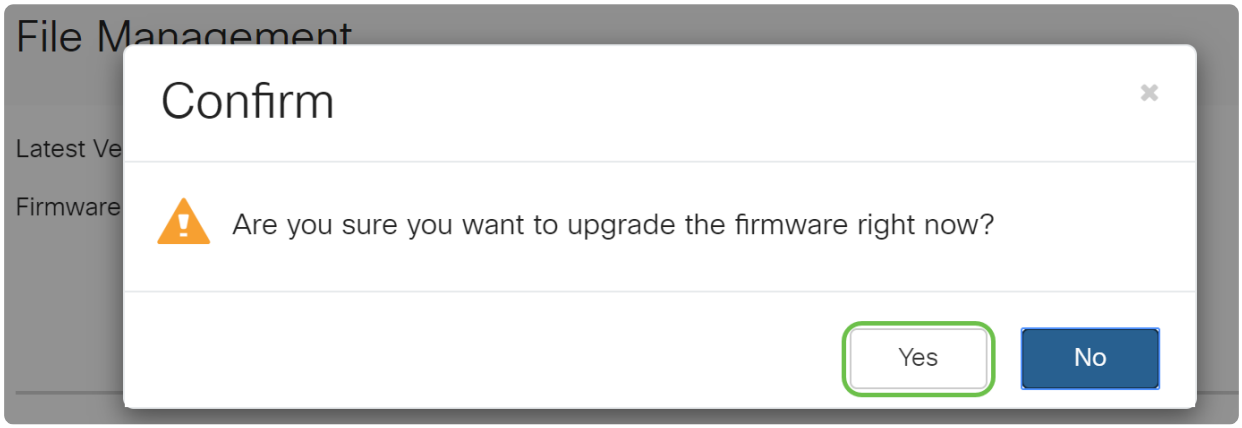
Étape 4

Cliquez sur Upgrade.

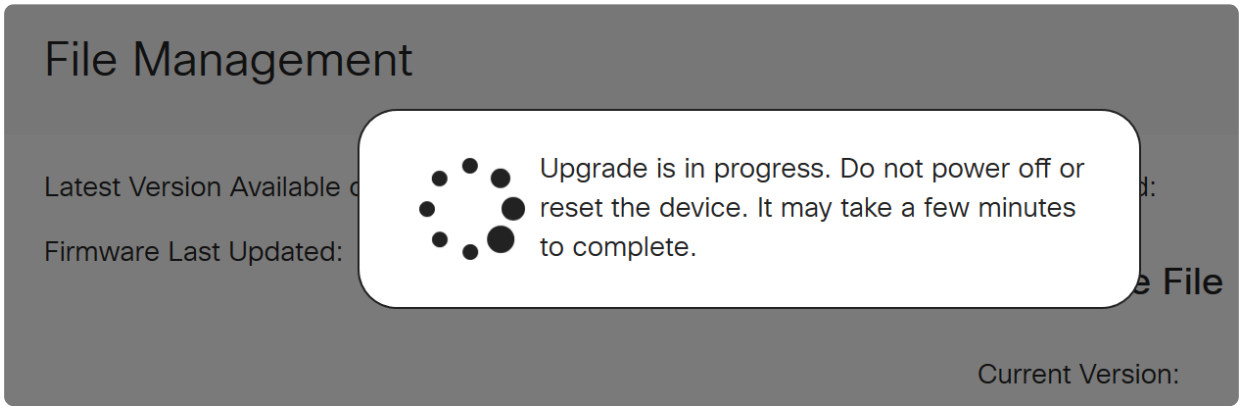


Étape 5

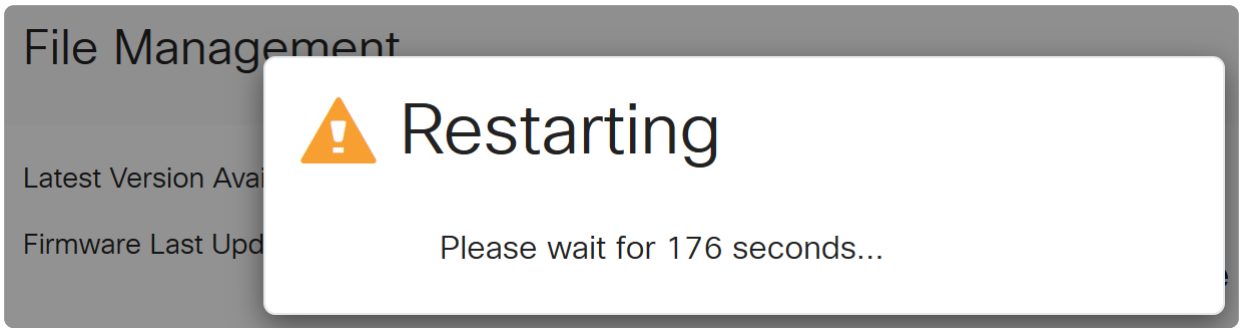
Cliquez sur Yes dans la fenêtre de confirmation pour continuer.



ⓘ Note: Le processus de mise à jour doit s'exécuter sans interruption. Le message suivant s'affiche à l'écran pendant la mise à niveau.

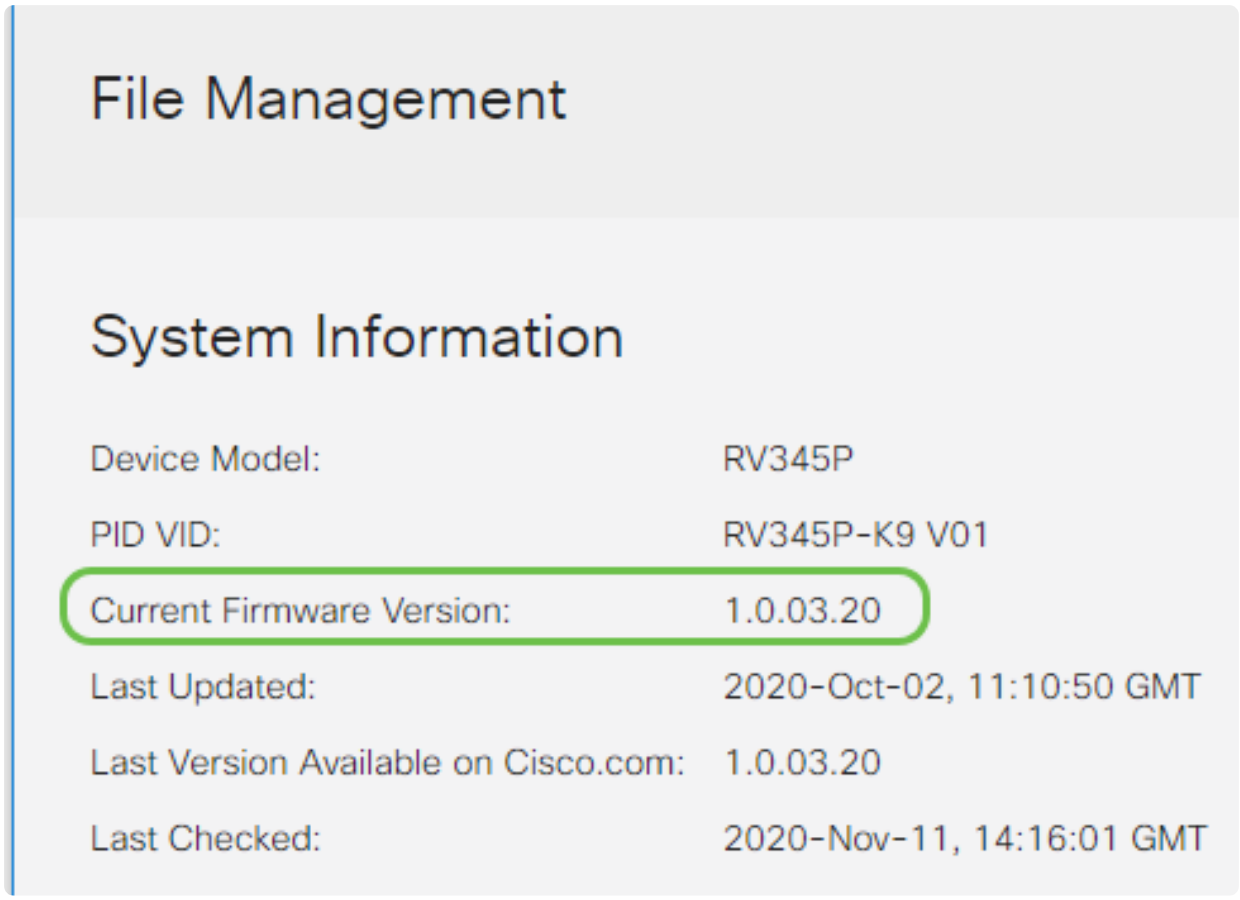


Une fois la mise à niveau terminée, une fenêtre de notification s'affiche pour vous informer que le routeur va redémarrer avec un compte à rebours du temps estimé pour la fin du processus. Ensuite, vous serez déconnecté(e).



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 Current Firmware Version doit maintenant afficher la version mise à niveau du micrologiciel.



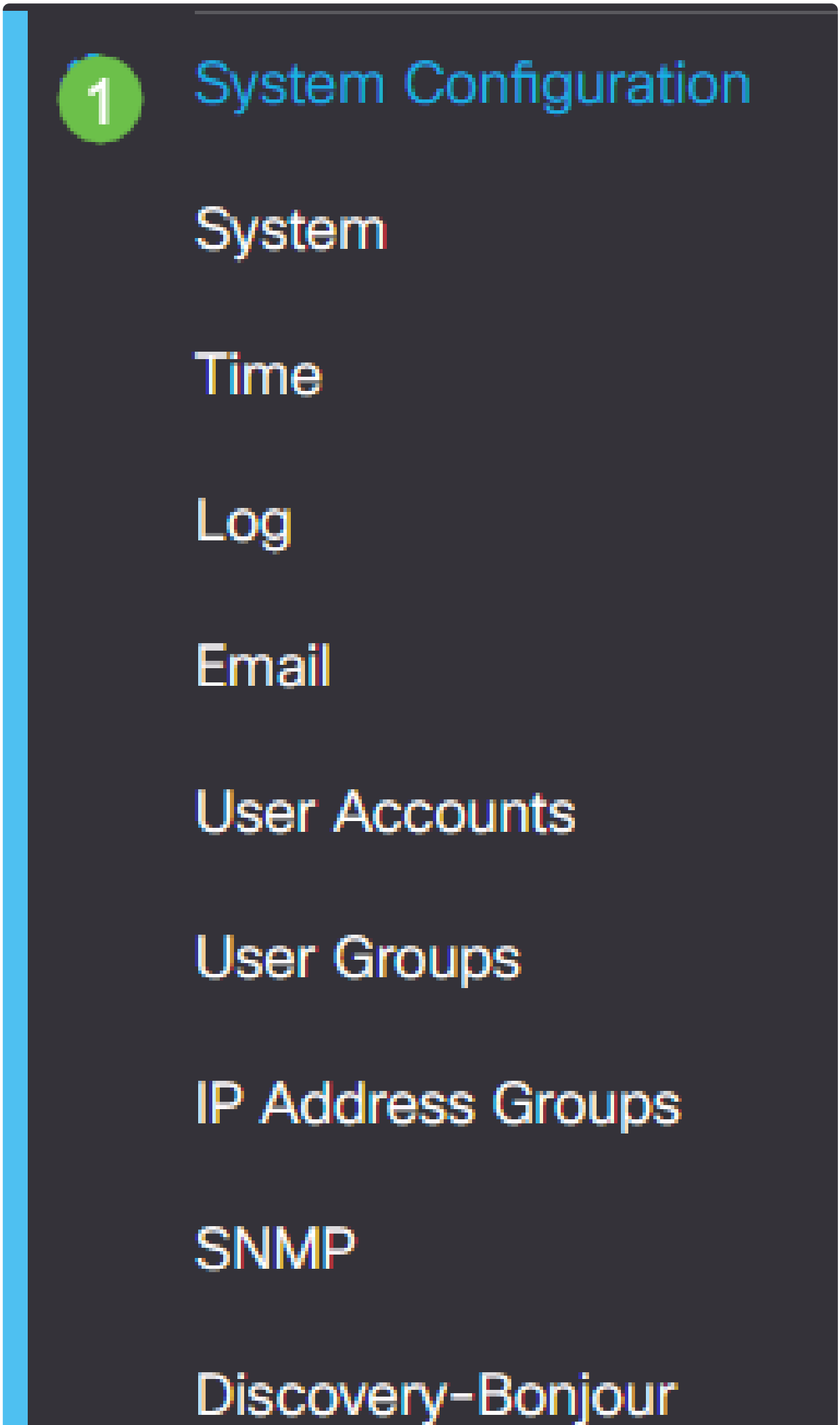
Configuration des mises à jour automatiques sur le routeur de la gamme RV345P

Puisque les mises à jour sont si importantes et que vous êtes très occupé, il est

logique de configurer les mises à jour automatiques dès maintenant !

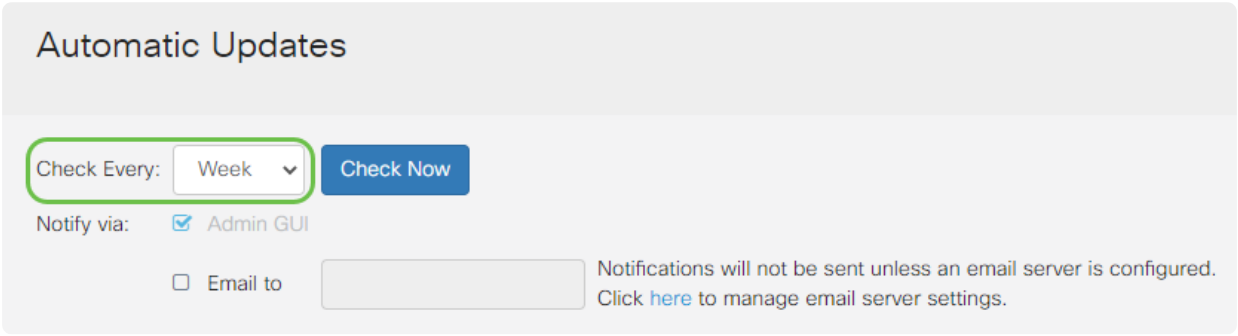
Étape 1

Connectez-vous à l'utilitaire Web et choisissez System Configuration > Automatic Updates.


1
System Configuration
System
Time
Log
Email
User Accounts
User Groups
IP Address Groups
SNMP
Discovery-Bonjour

Étape 2

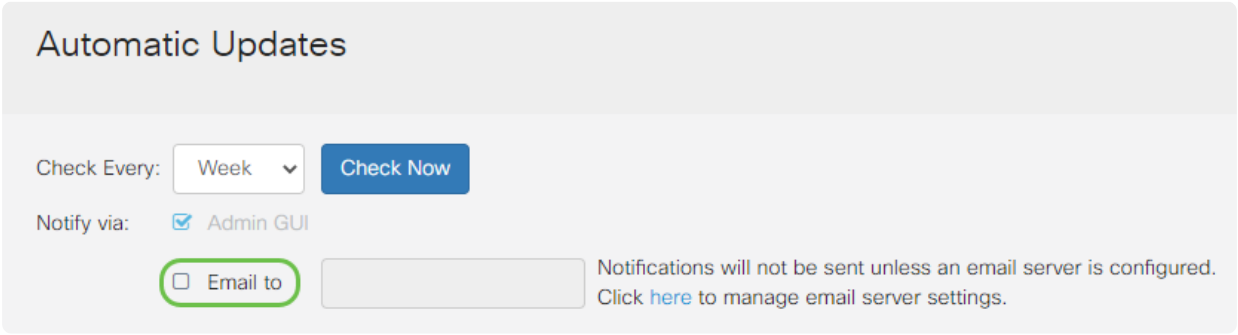
Dans la liste déroulante Check Every, choisissez la fréquence à laquelle le routeur doit rechercher les mises à jour.



Étape 3

Dans la zone Notify via, cochez la case Email to pour recevoir les mises à jour par e-mail. La case à cocher Admin GUI est activée par défaut et ne peut pas être désactivée. Une notification apparaît dans la configuration Web dès qu'une mise à jour est disponible.

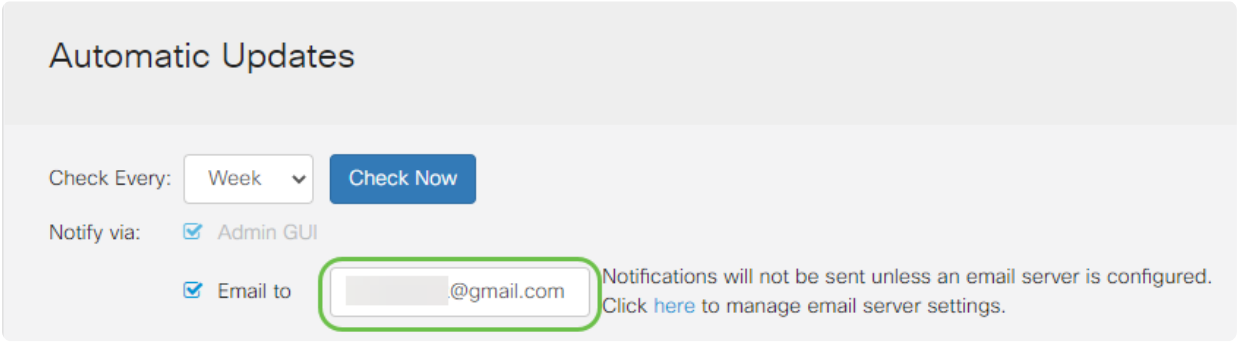
Si vous souhaitez configurer les paramètres du serveur de messagerie, cliquez ici pour en savoir plus.



Étape 4

Saisissez une adresse e-mail dans le champ Adresse e-mail.

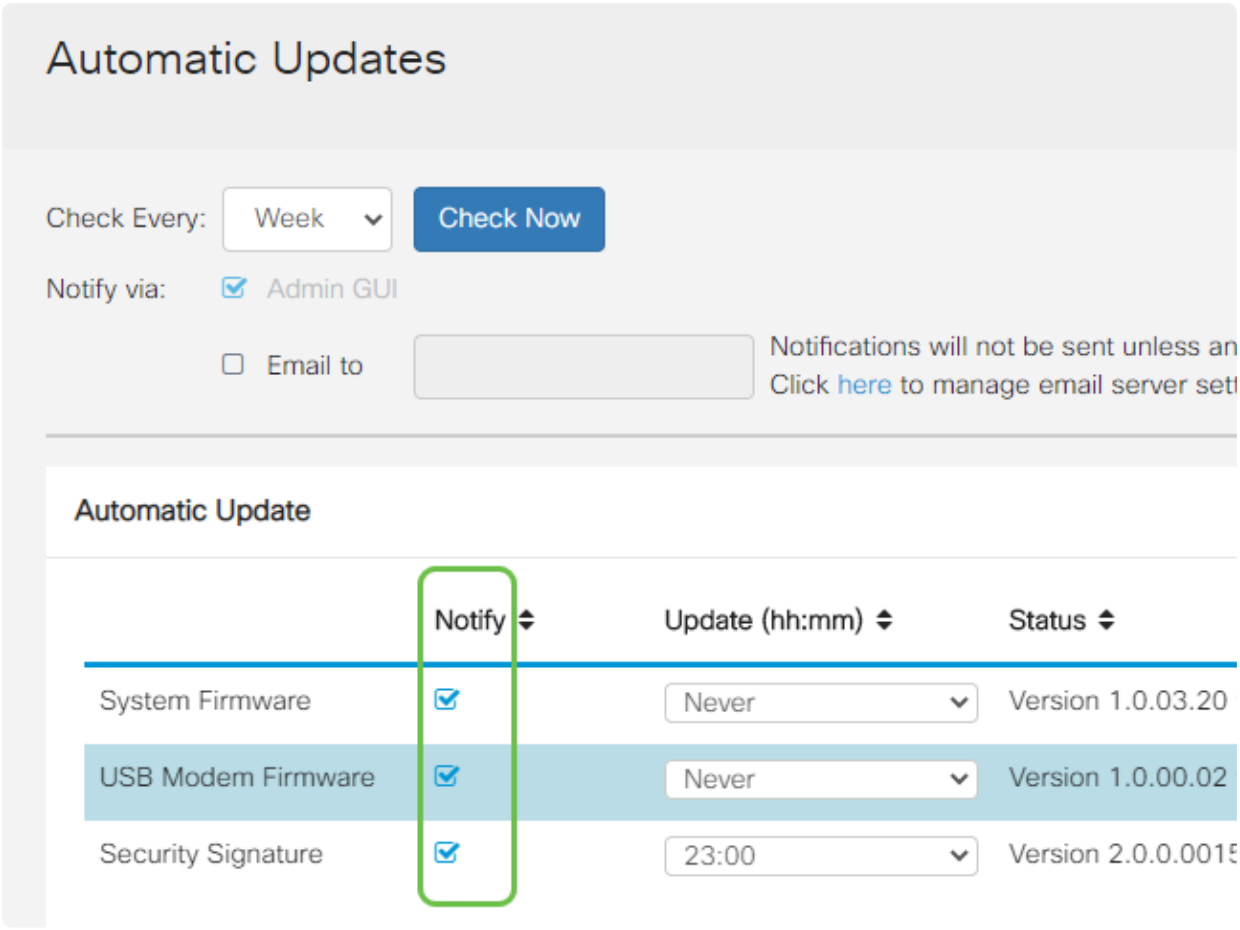
ⓘ Note: Il est vivement recommandé d'utiliser un compte de messagerie distinct au lieu d'utiliser votre messagerie personnelle pour préserver la confidentialité.



Étape 5

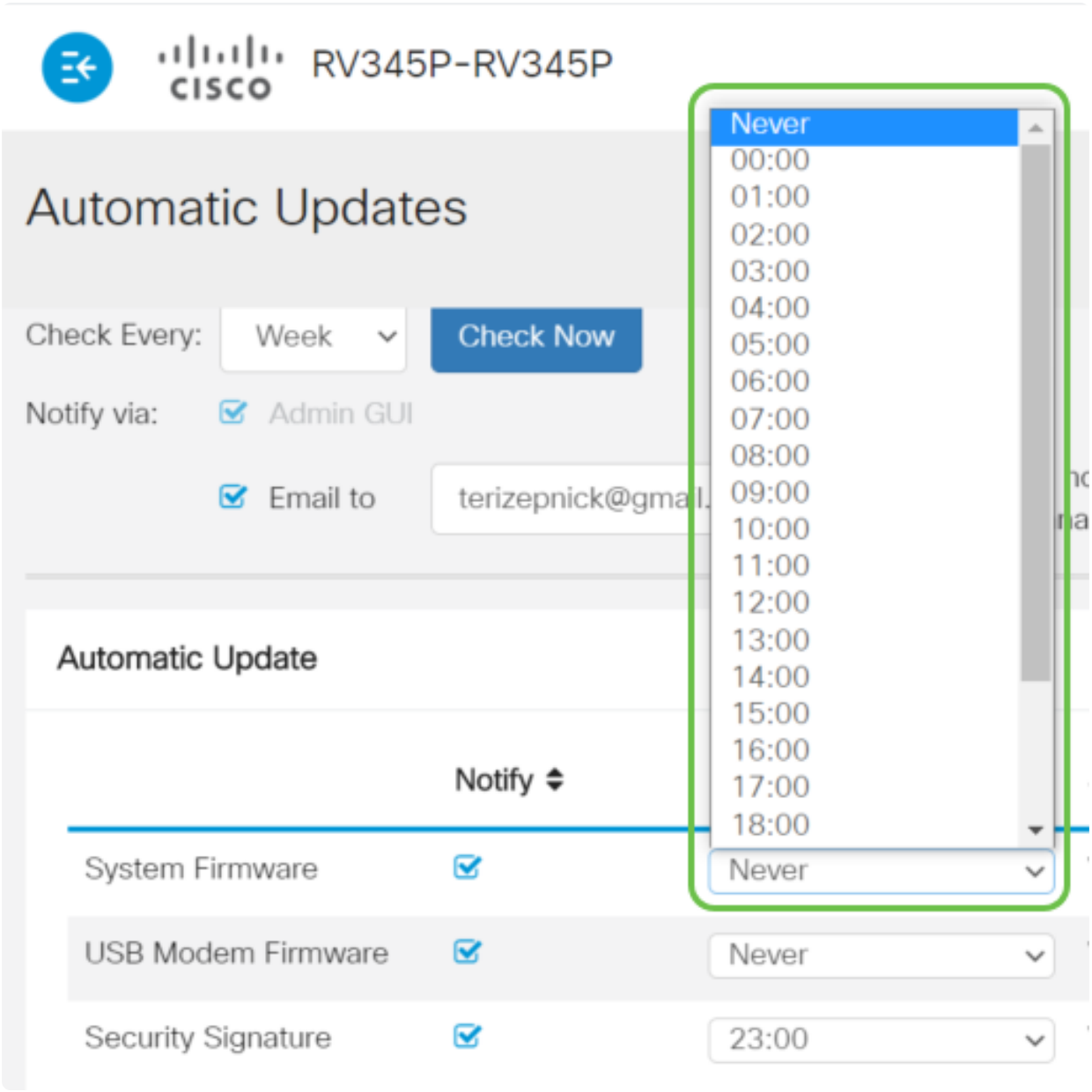
Dans la zone Mise à jour automatique, cochez les cases Notifier du type de mises à jour dont vous souhaitez être averti. Les options sont les suivantes :

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



Étape 6

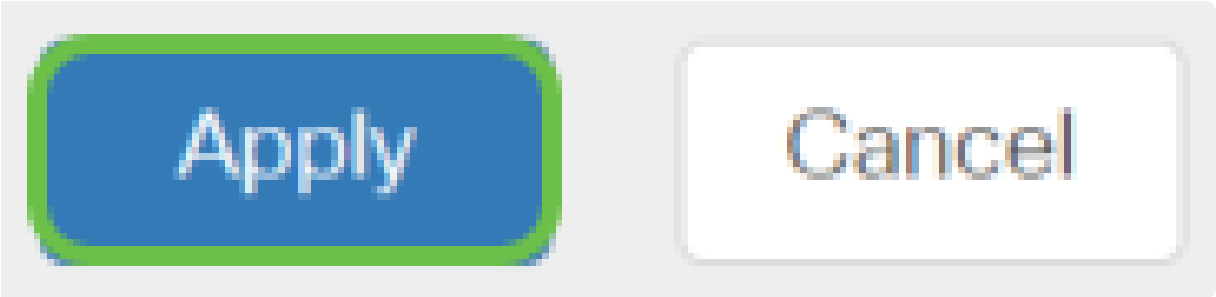
Dans la liste déroulante Mise à jour automatique, sélectionnez l'heure de la journée à laquelle vous souhaitez que la mise à jour automatique soit effectuée. Certaines options peuvent varier selon le type de mise à jour que vous avez choisi. La signature de sécurité est la seule option permettant une mise à jour immédiate. Il est recommandé de définir une heure de fermeture de votre bureau afin que le service ne soit pas interrompu à un moment inopportun.



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 la configuration de manière permanente, accédez à la page Copier/Enregistrer la configuration ou cliquez sur l'icône d'enregistrement située dans la partie supérieure de la page.



Impressionnant, vos paramètres de base sur votre routeur sont terminés ! Vous avez

maintenant des options de configuration à explorer.

Options de sécurité

Bien sûr, vous voulez que votre réseau soit sécurisé. Il existe quelques options simples, comme avoir 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 (en option)

Les fonctionnalités de cette licence de sécurité RV protègent votre réseau contre les attaques provenant d'Internet :

- Système de prévention des intrusions (IPS) Inspecte les paquets réseau, consigne et/ou bloque un large éventail d'attaques réseau. Il offre une disponibilité accrue du réseau, une correction plus rapide et une protection complète contre les menaces.
- Antivirus : Protection contre les virus en recherchant dans les applications divers protocoles tels que HTTP, FTP, les pièces jointes SMTP, POP3 et IMAP via le routeur.
- Sécurité Web : Efficacité et sécurité de l'entreprise lors de la connexion à Internet, politiques d'accès à Internet pour les périphériques finaux et les applications Internet afin de garantir les performances et la sécurité. Il est basé sur le cloud et contient plus de 80 catégories avec plus de 450 millions de domaines classés.
- Identification de la demande : Identifiez et attribuez des stratégies aux applications Internet. 500 applications uniques sont automatiquement identifiées.
- Identification du client : Identifier et classer les clients de manière dynamique. Possibilité d'attribuer des stratégies en fonction de la catégorie du périphérique final et du système d'exploitation.

La licence de sécurité RV assure le filtrage Web. Le filtrage Web est une fonctionnalité 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.

ⓘ Note: Les fonctionnalités de sécurité sous licence peuvent être testées

gratuitement pendant 90 jours. Si vous souhaitez continuer à utiliser les fonctions de sécurité avancées sur 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 passer à la section Umbrella (Parapluie).

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

Présentation des comptes Smart

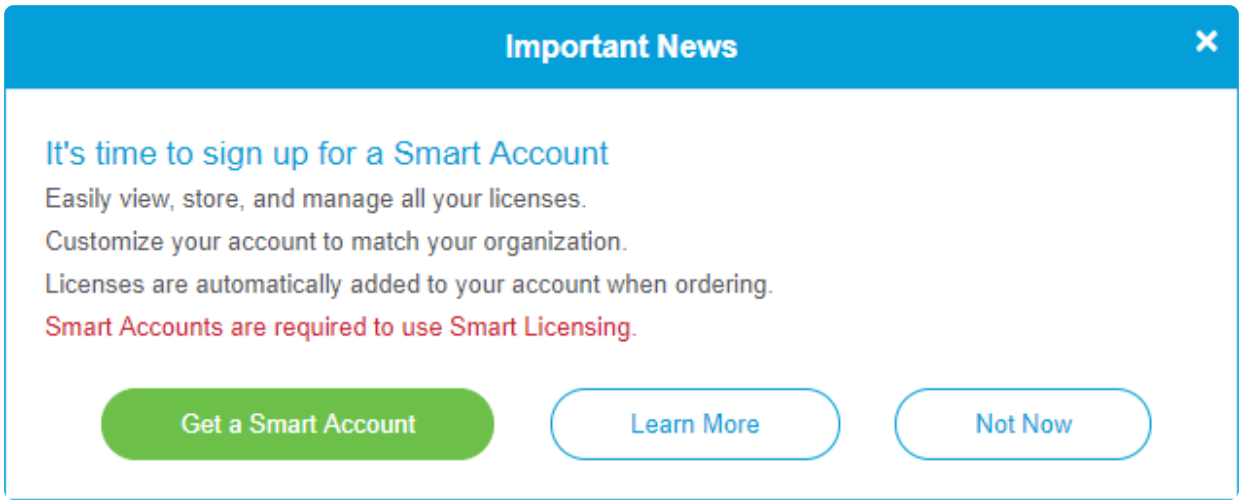
Pour acheter la licence de sécurité RV, vous avez besoin d'un compte Smart.

En autorisant l'activation de ce compte Smart, vous acceptez d'être autorisé à créer des comptes et à gérer les droits relatifs aux produits et services, les accords de licence et l'accès des utilisateurs aux comptes pour le compte de votre organisation. Les partenaires Cisco ne peuvent pas autoriser la création de comptes pour le compte des clients.

La création d'un nouveau compte Smart est un événement unique et la gestion est assurée à partir de ce moment 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), un message vous invite à créer un compte Smart.



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

Pour plus d'informations sur les étapes inhérentes à la demande de votre compte Smart, cliquez ici.

Veillez à prendre note du nom de votre compte ainsi que d'autres informations d'inscription.

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

ⓘ Note: Il est très important que vous disposiez d'un compte Cisco.com (ID CCO) et d'un compte Cisco Smart avant d'acheter la licence de sécurité RV.

Acheter une licence de sécurité RV

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

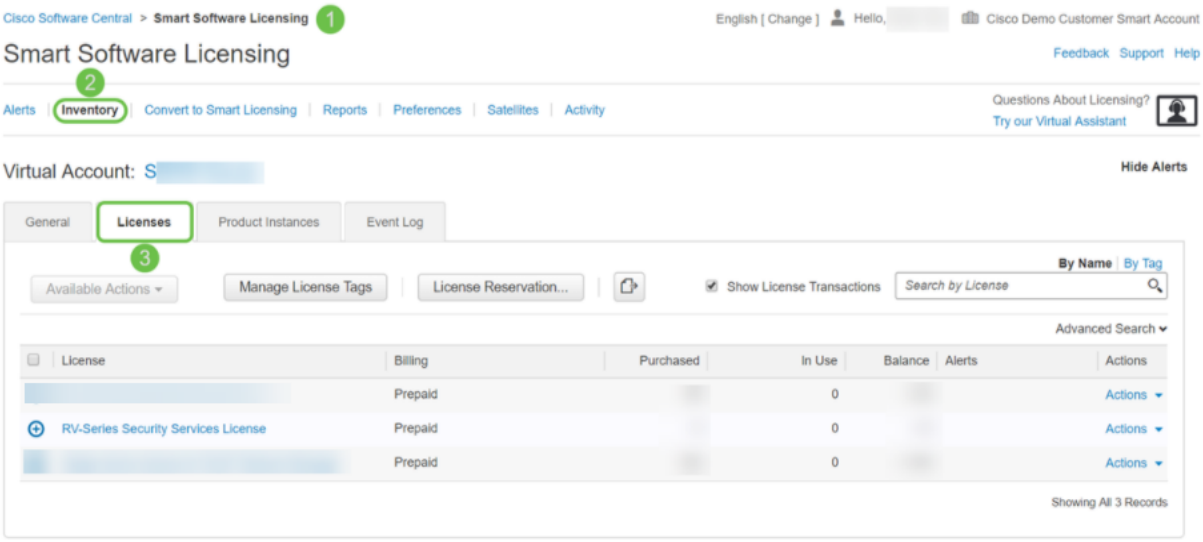
Le tableau ci-dessous indique la référence de la licence.

Type	ID de produit	Description
Licence de sécurité RV	LS-RV34X-SEC-1YR=	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 attribuée à votre compte Cisco Smart après que vous aurez commandé la licence. La durée d'affichage de la licence sur votre compte dépend du moment où le partenaire accepte la commande et où le revendeur lie les licences à votre compte, ce qui est généralement 24 à 48 heures.

Confirmer que la licence se trouve dans le compte Smart

Accédez à la page de votre compte de licence Smart, puis cliquez sur Page de licence logicielle Smart > Inventaire > Licences.



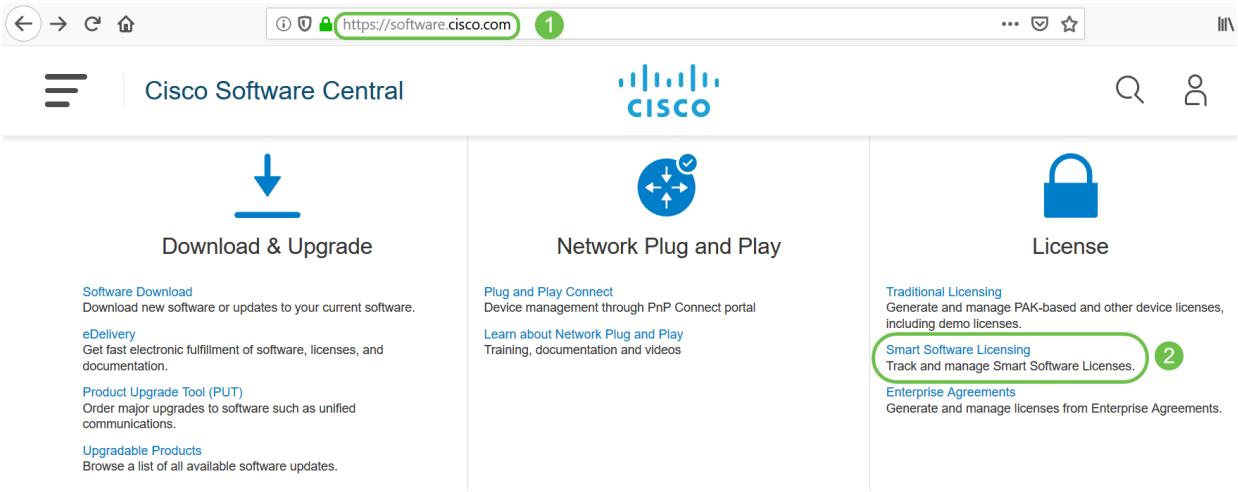
ⓘ Note: Si vous ne voyez pas votre licence dans votre compte Smart,

contactez votre partenaire Cisco.

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

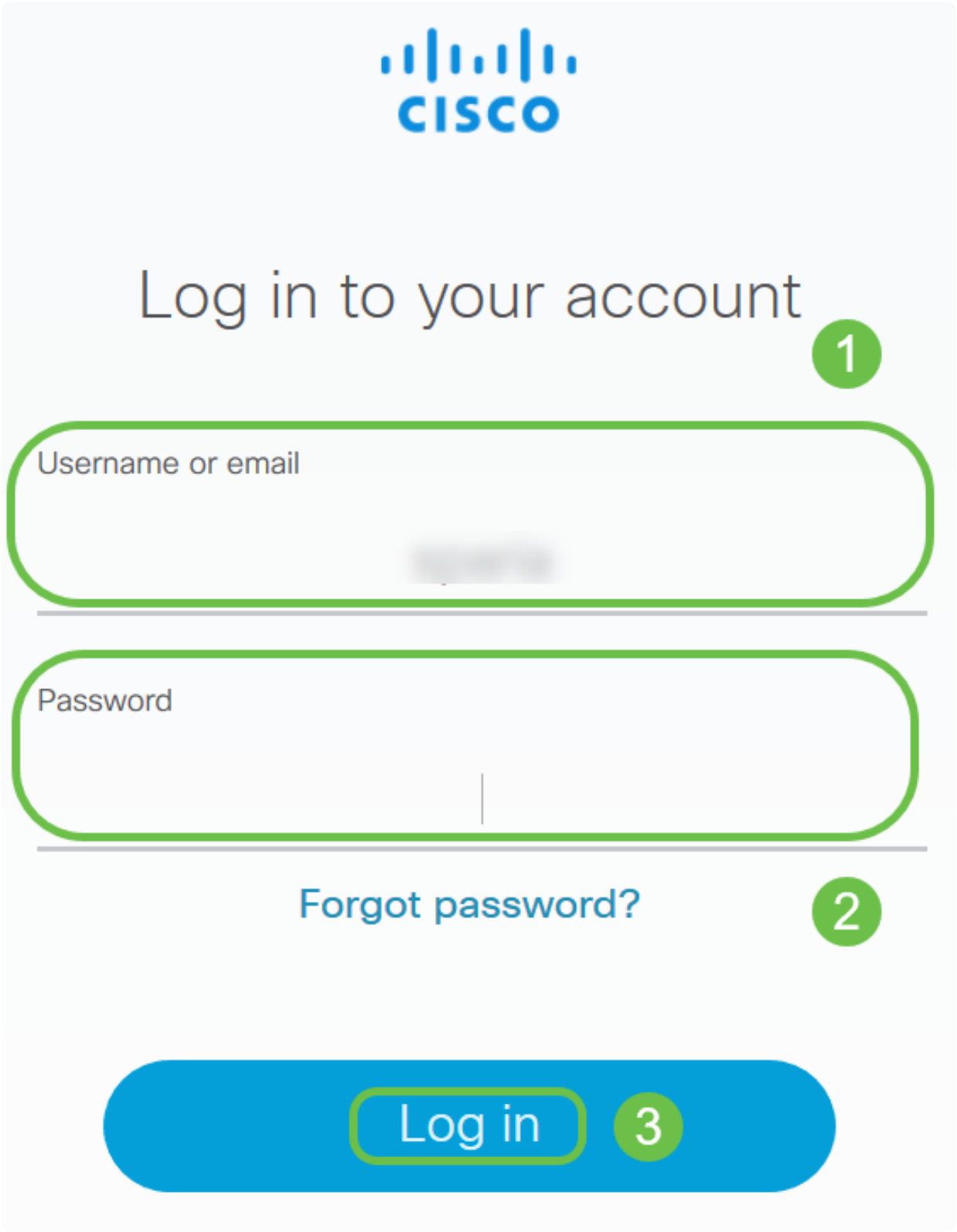
Étape 1

Accédez à Cisco Software et accédez à Smart Software Licensing.



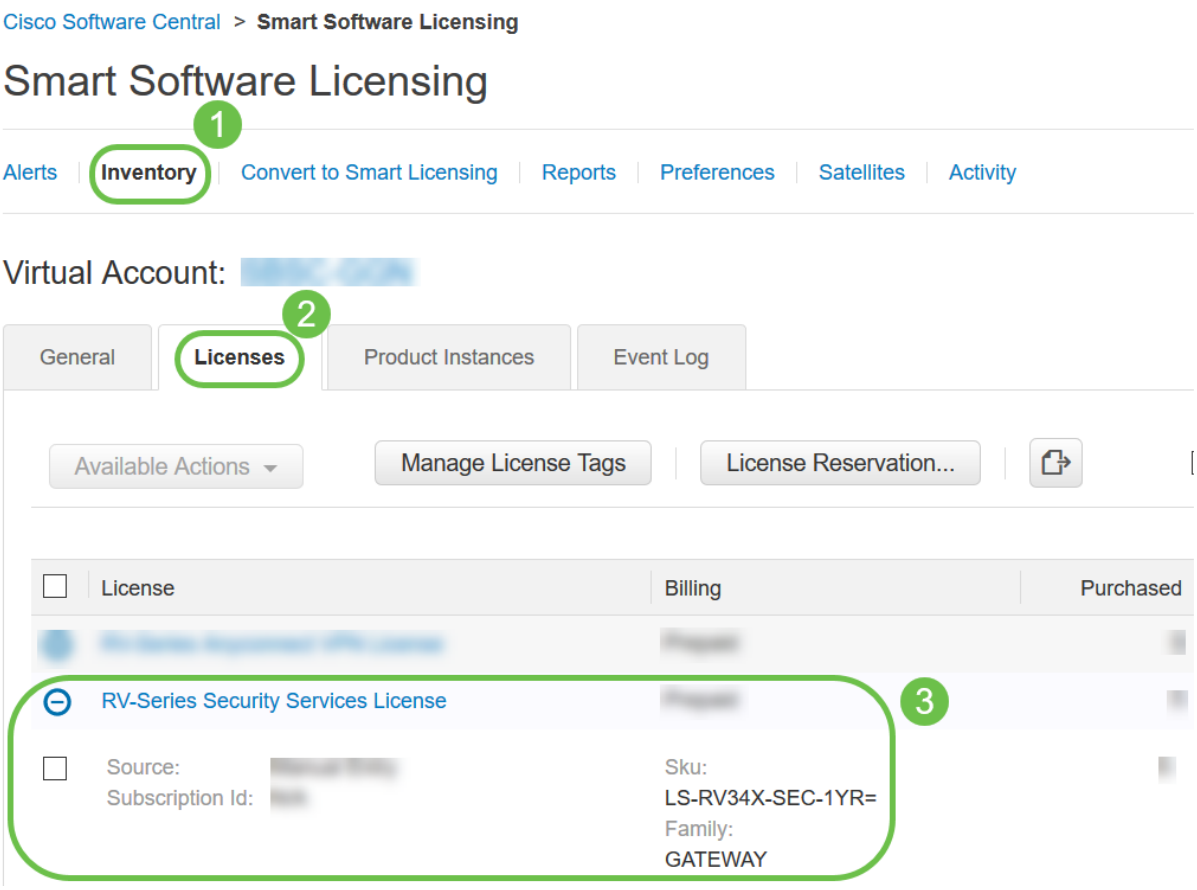
Étape 2

Saisissez votre nom d'utilisateur ou votre adresse e-mail et votre mot de passe pour vous connecter à votre compte Smart. Cliquez sur Log in.



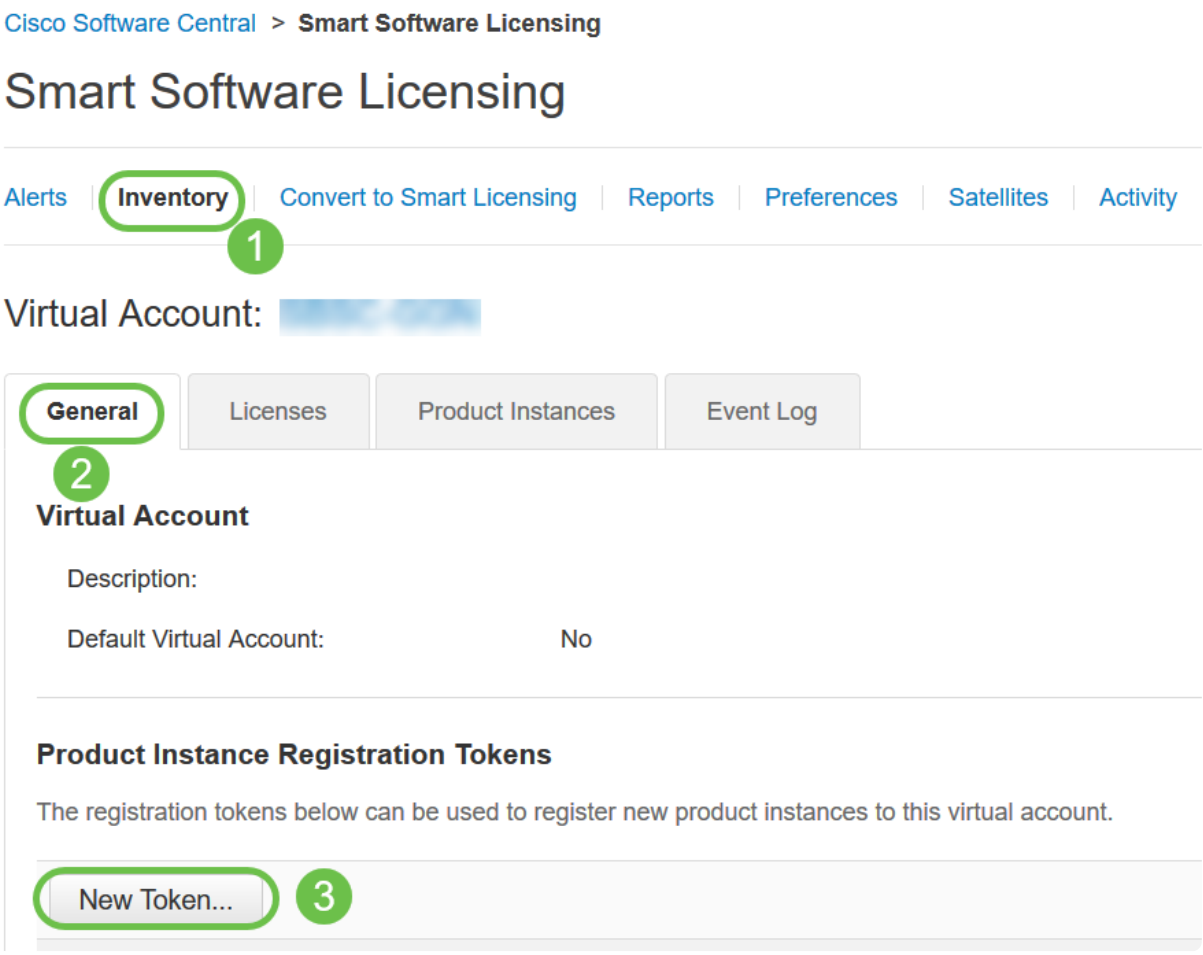
Étape 3

Accédez à Inventory > Licenses et vérifiez que la licence de services de sécurité de la gamme RV est répertoriée sur votre compte Smart. Si la licence ne s'affiche pas, contactez votre partenaire Cisco.



Étape 4

Accédez à Inventory > General. Sous Product Instance Registration Tokens, cliquez sur New Token.



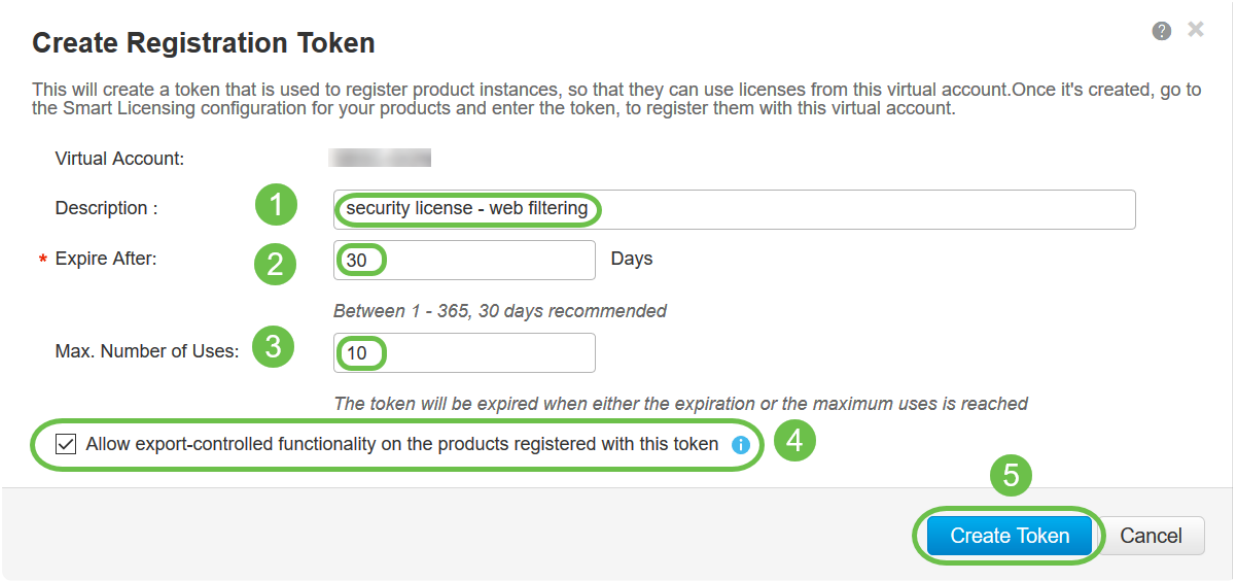
Étape 5

Une fenêtre Create Registration Token s'affiche. La zone Virtual Account affiche le compte virtuel sous lequel le jeton d'inscription sera créé. Sur la page Create Registration Token, renseignez les champs suivants :

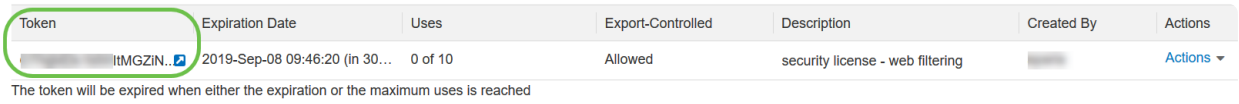
- Dans le champ Description, saisissez une description unique pour le jeton. Dans cet exemple, licence de sécurité - filtrage Web est entré.
- Dans le champ Expire après, saisissez une valeur comprise entre 1 et 365 jours. Cisco recommande la valeur 30 jours pour ce champ ; toutefois, vous pouvez modifier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

vous êtes conforme à la fonctionnalité d'exportation contrôlée. Certaines fonctions d'exportation contrôlée sont restreintes par le département du Commerce des États-Unis. Ces fonctionnalités sont restreintes pour les produits enregistrés utilisant ce jeton lorsque vous décochez la case. Toute infraction est passible de sanctions et de frais administratifs.

- Cliquez sur Create Token pour générer le jeton.

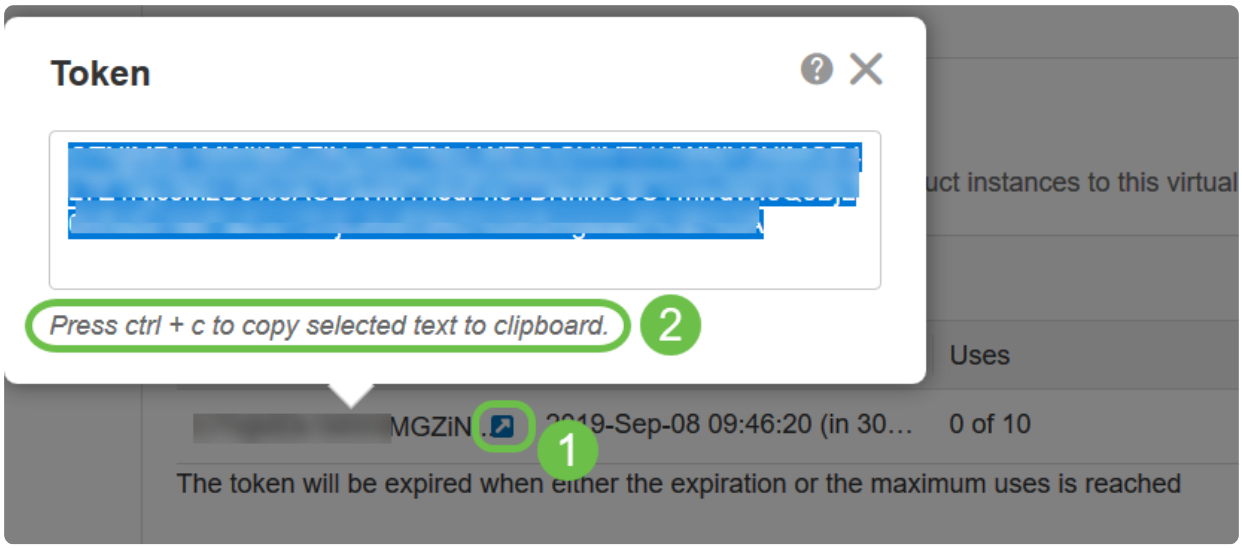


Vous venez de générer un jeton d'enregistrement d'instance de produit.



Étape 6

Cliquez sur l'icône en forme de flèche dans la colonne Token, pour copier le jeton dans le Presse-papiers, appuyez sur ctrl + c sur votre clavier.



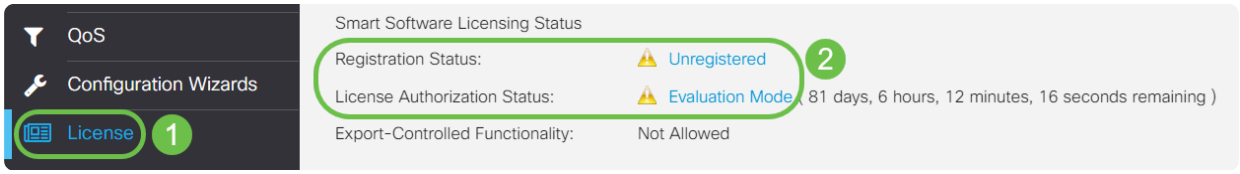
Étape 7 (facultative)

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



Étape 8

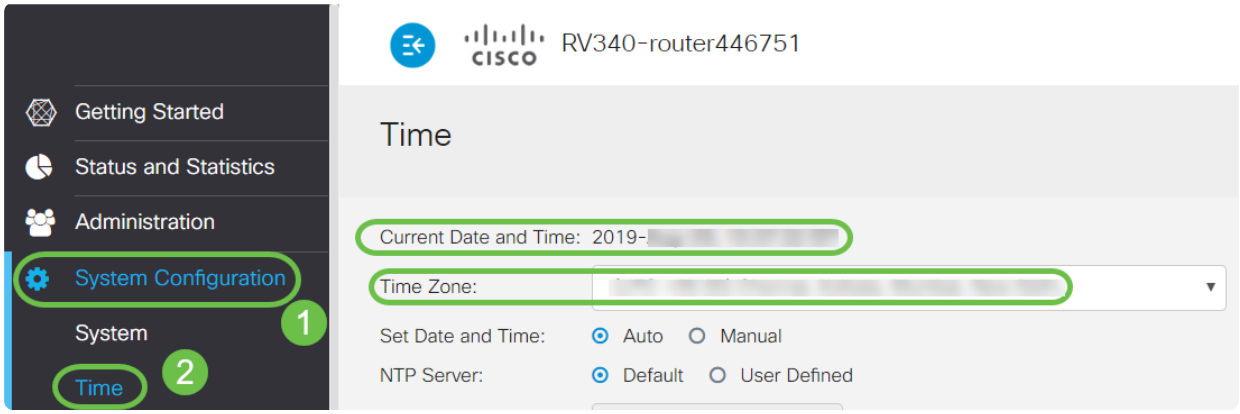
Accédez à License et vérifiez que l'état d'enregistrement est Unregistered et que l'état d'autorisation de licence est affiché en mode d'évaluation.



Étape 9

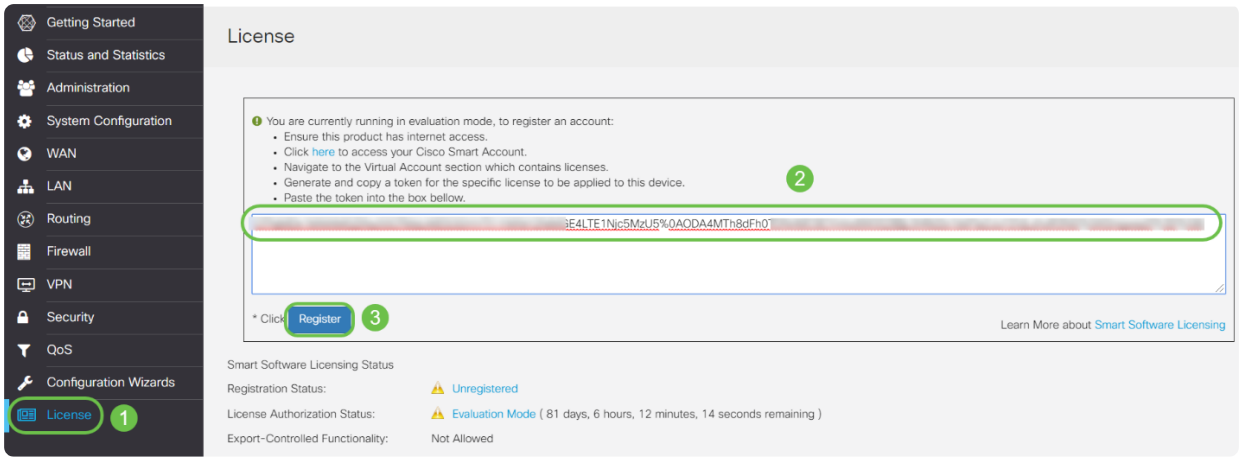
Accédez à Configuration système > Heure et vérifiez que la date et l'heure actuelles et

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.

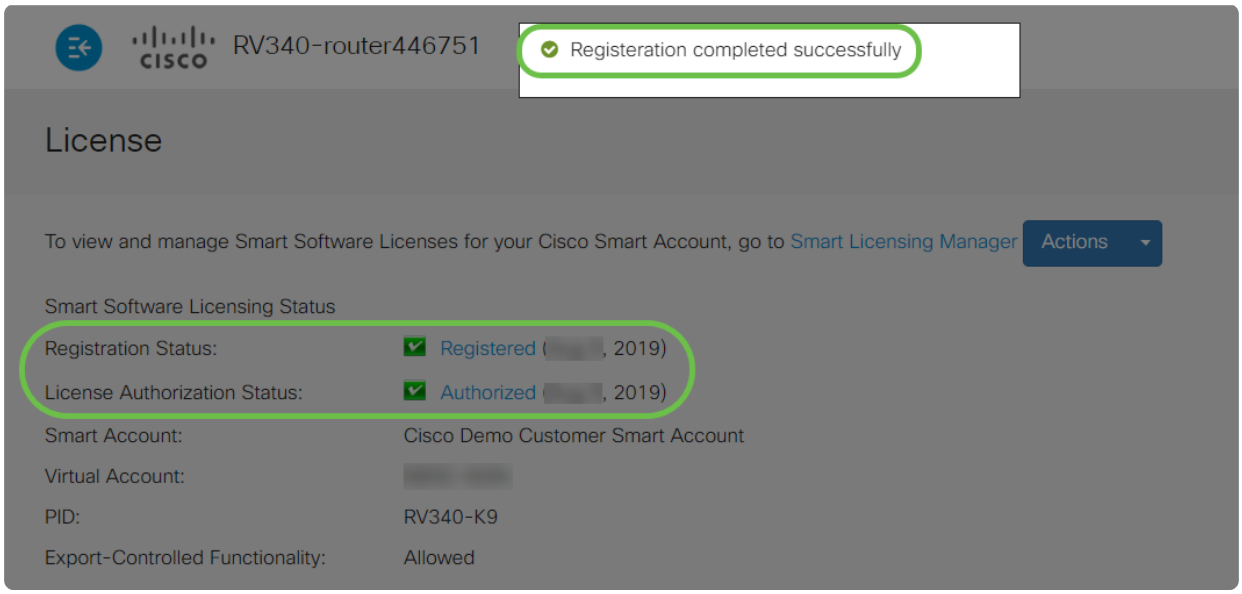


L'enregistrement peut prendre quelques minutes. Ne quittez pas la page lorsque le routeur tente de contacter le serveur de licences.

Étape 11

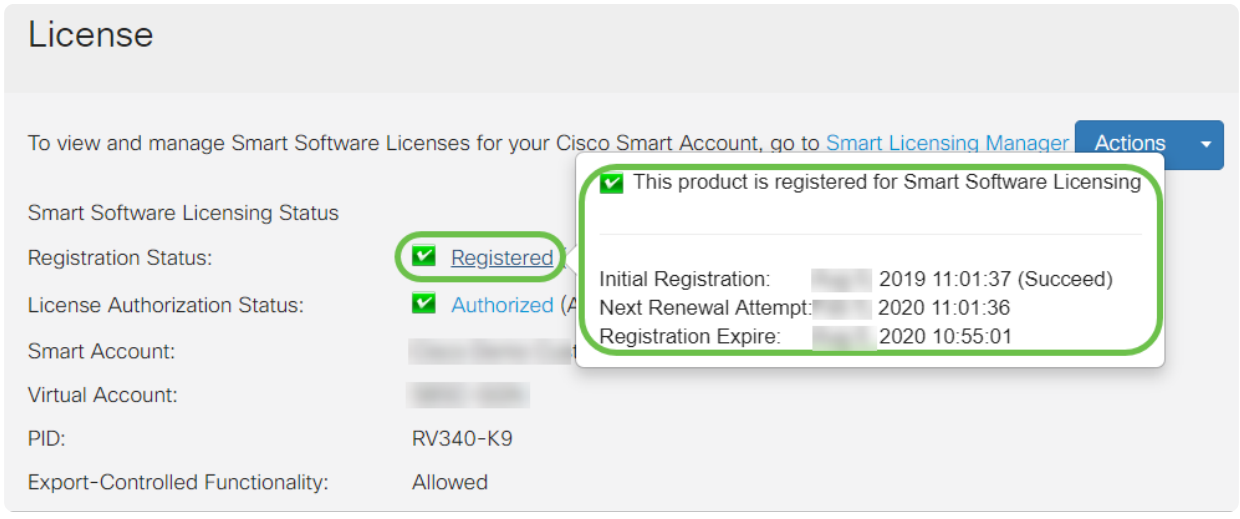
Vous devez maintenant avoir enregistré et autorisé votre routeur de la gamme RV345P avec une licence Smart. Une notification s'affiche à l'écran Enregistrement terminé avec succès. En outre, vous pourrez voir que l'état d'enregistrement est affiché comme

enregistré et que l'état d'autorisation de la licence est affiché comme autorisé.



Étape 12 (facultative)

Pour afficher plus de détails sur l'état d'enregistrement de la licence, placez le pointeur de la souris sur l'état Registered. Un message de dialogue contenant les informations suivantes s'affiche :



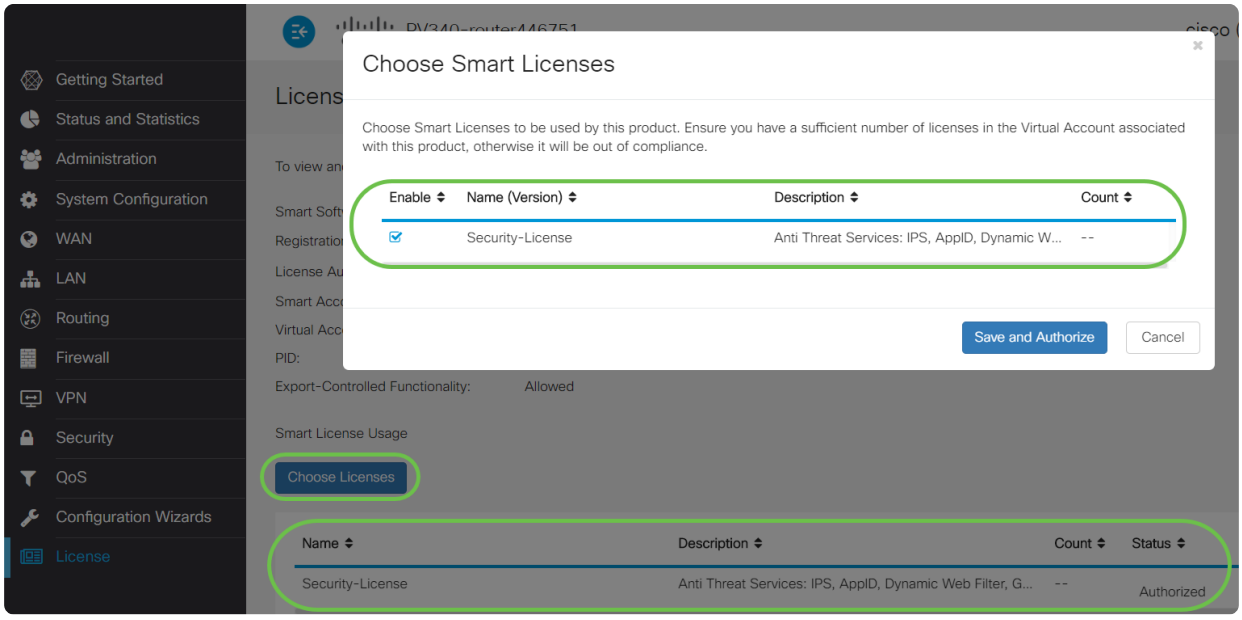
- Enregistrement initial : cette zone indique la date et l'heure d'enregistrement de la licence.
- Next Renewal Attempt : cette zone indique la date et l'heure auxquelles le routeur tentera de renouveler la licence.

- Registration Expire : cette zone indique la date et l'heure d'expiration de l'enregistrement.

Étape 13

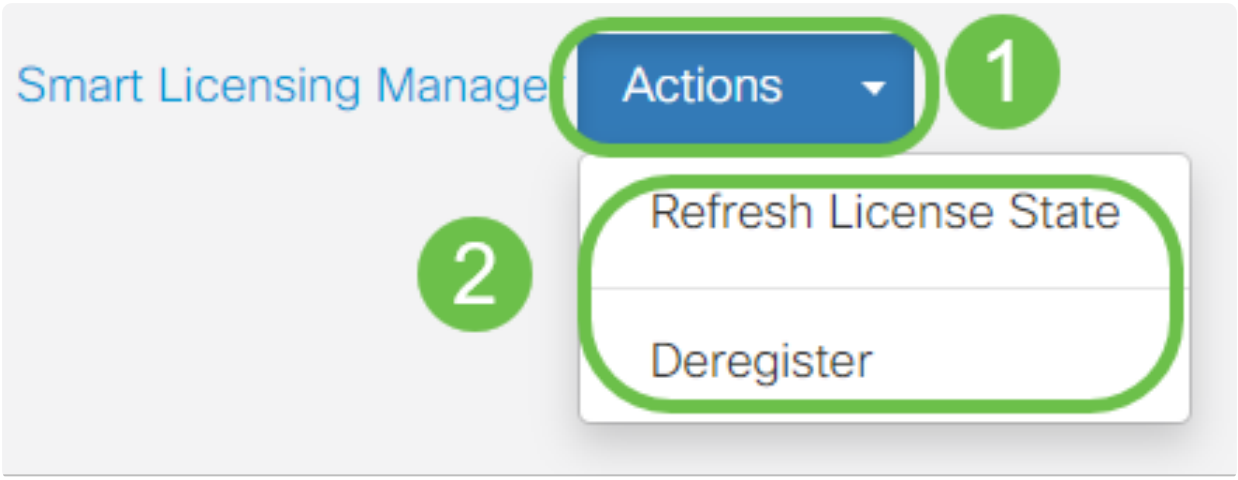
Sur la page License, vérifiez que l'état Security-License indique Authorized. Vous pouvez également cliquer sur le bouton Choisir une licence pour vérifier que Security-License est activé.

> ⓘ Note: Si vous rencontrez des problèmes au cours de cette étape, vous devrez peut-être redémarrer votre routeur.



Étape 14 (facultative)

Pour actualiser l'état de licence ou annuler l'enregistrement de la licence à partir du routeur, cliquez sur le menu déroulant Actions de Smart Licensing Manager, puis sélectionnez une action.



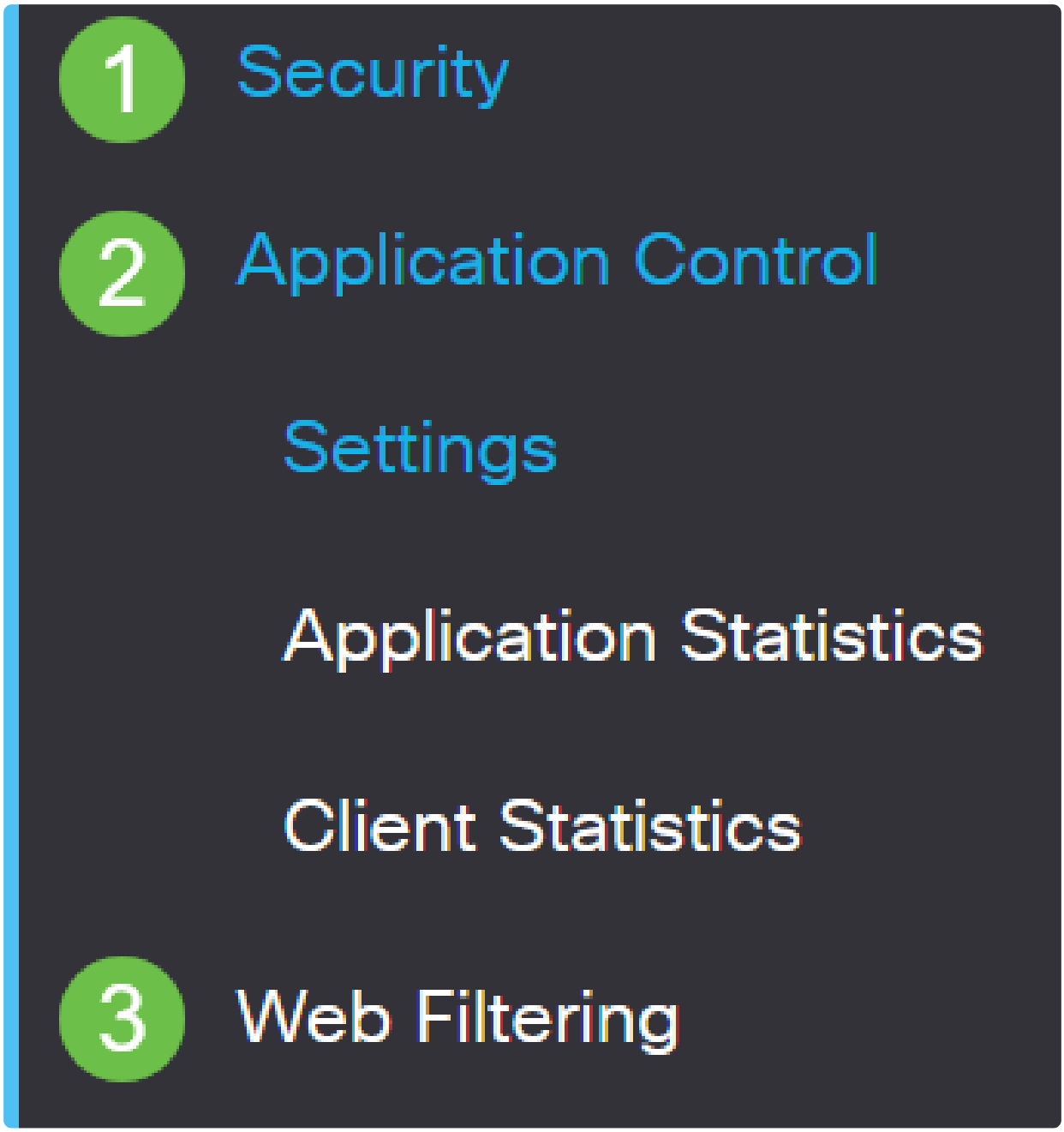
Maintenant que vous disposez de votre licence sur le routeur, vous devez effectuer les étapes de la section suivante.

Filtrage Web sur le routeur RV345P

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

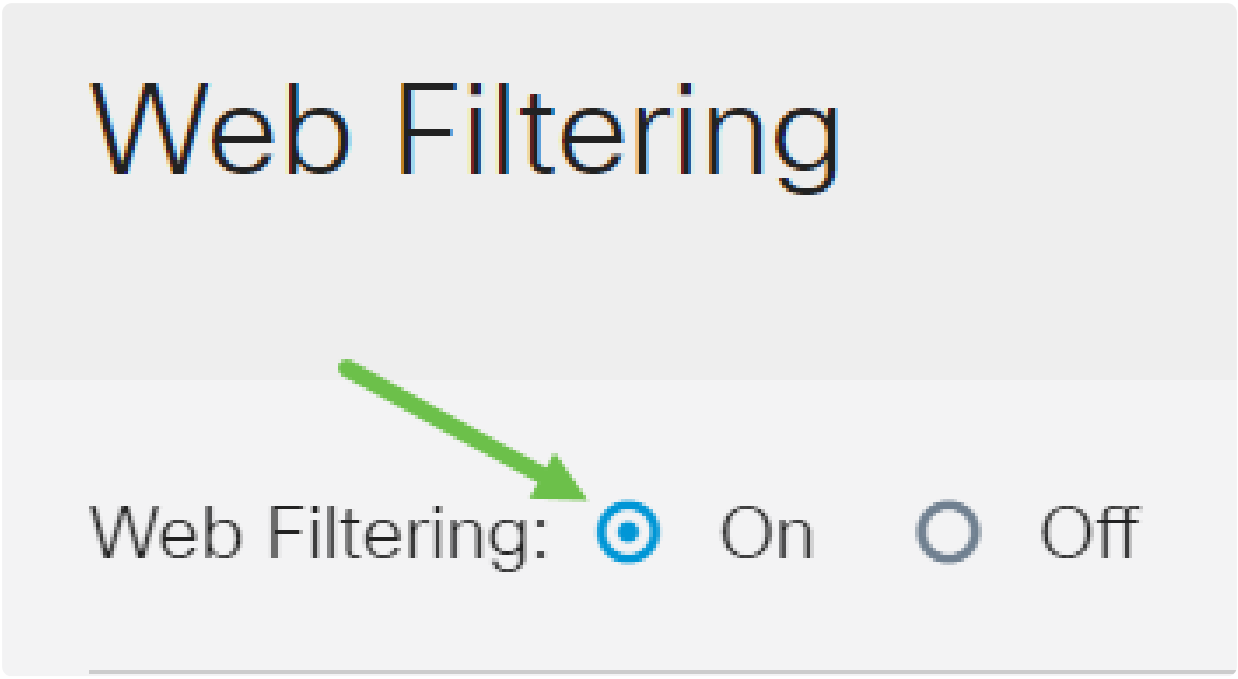
Étape 1

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



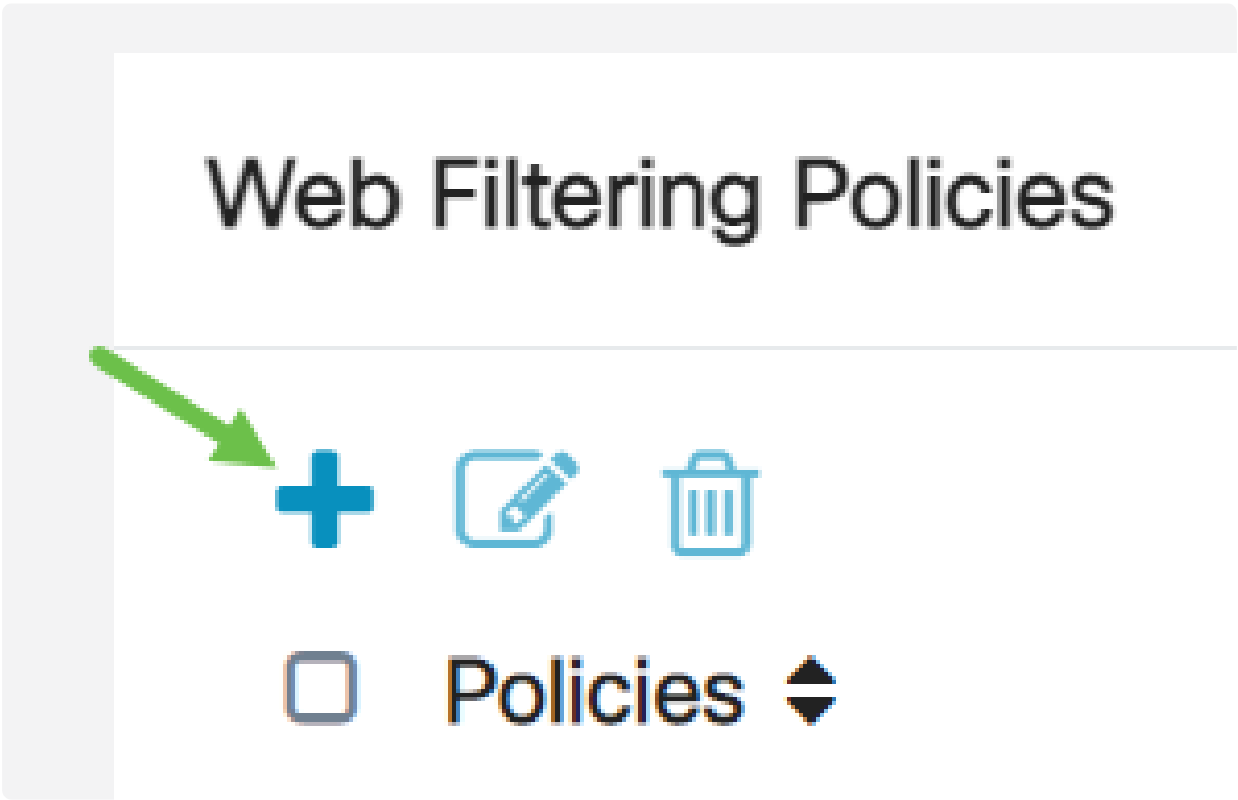
Étape 2

Sélectionnez la case d'option On.



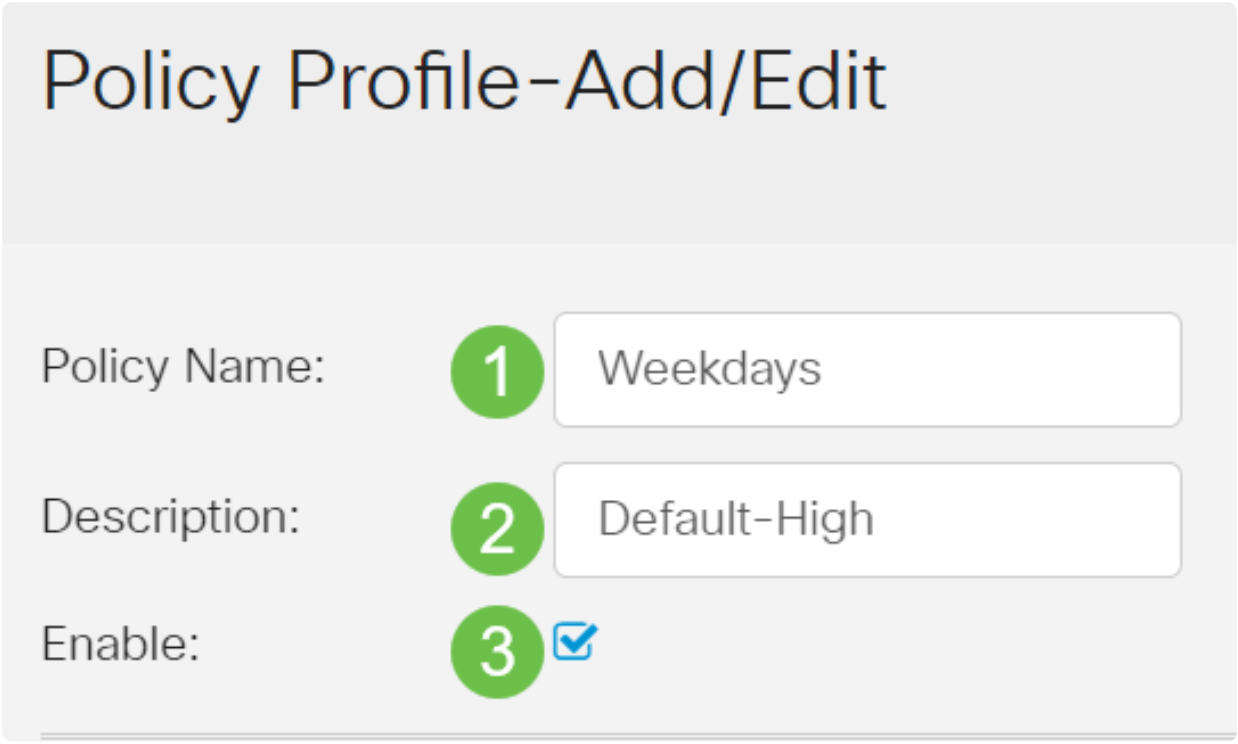
Étape 3

Cliquez sur l'icône Ajouter.



Étape 4

Saisissez un nom de stratégie, une description et la case à cocher Enable.



ⓘ Note: Si le filtrage de contenu est activé sur votre routeur, une notification s'affiche 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 Réputation Web pour activer le filtrage basé sur un index de réputation Web.

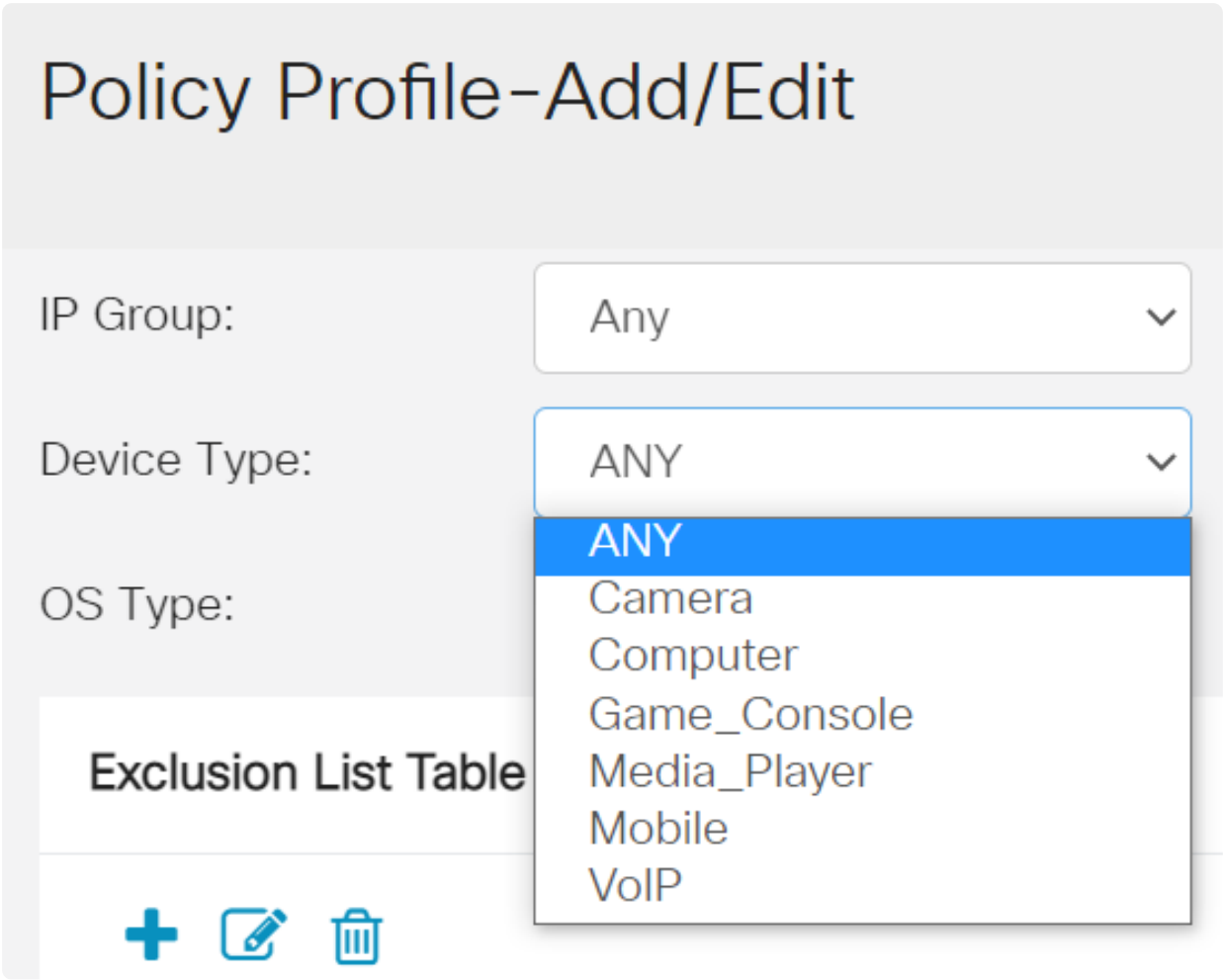


ⓘ Note: Le contenu sera filtré en fonction de la notoriété d'un site Web ou d'une URL basée sur un index de réputation Web. Si le score est inférieur à 40, le site Web sera bloqué. Pour en savoir plus sur la technologie de réputation Web, cliquez ici pour plus de détails.

Étape 6

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

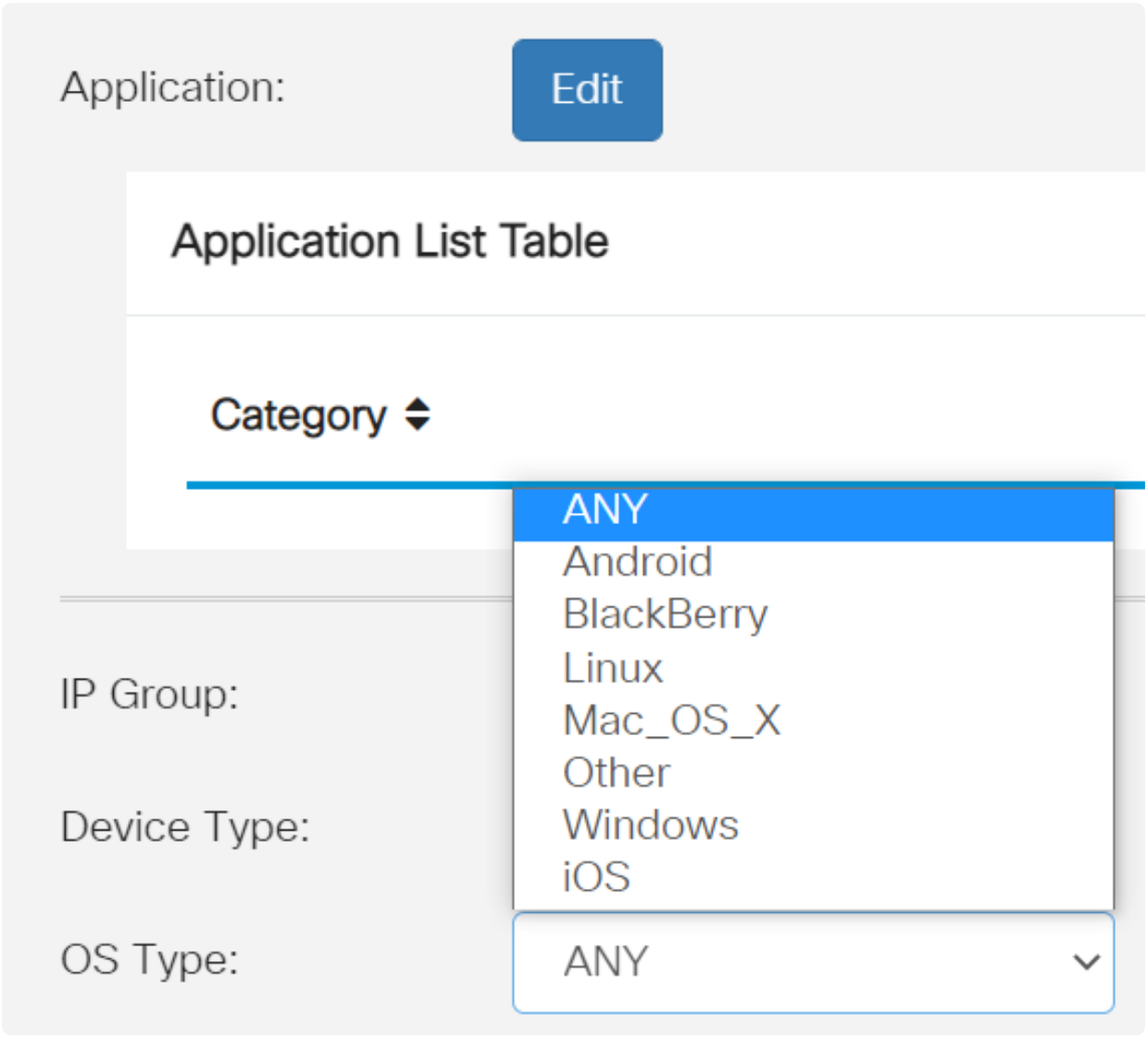
- ANY : sélectionnez cette option pour appliquer la stratégie à n'importe quel périphérique.
- Caméra : sélectionnez cette option pour appliquer la stratégie aux caméras (telles que les caméras de sécurité IP).
- Ordinateur : sélectionnez cette option pour appliquer la stratégie aux ordinateurs.
- Game_Console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



Étape 7

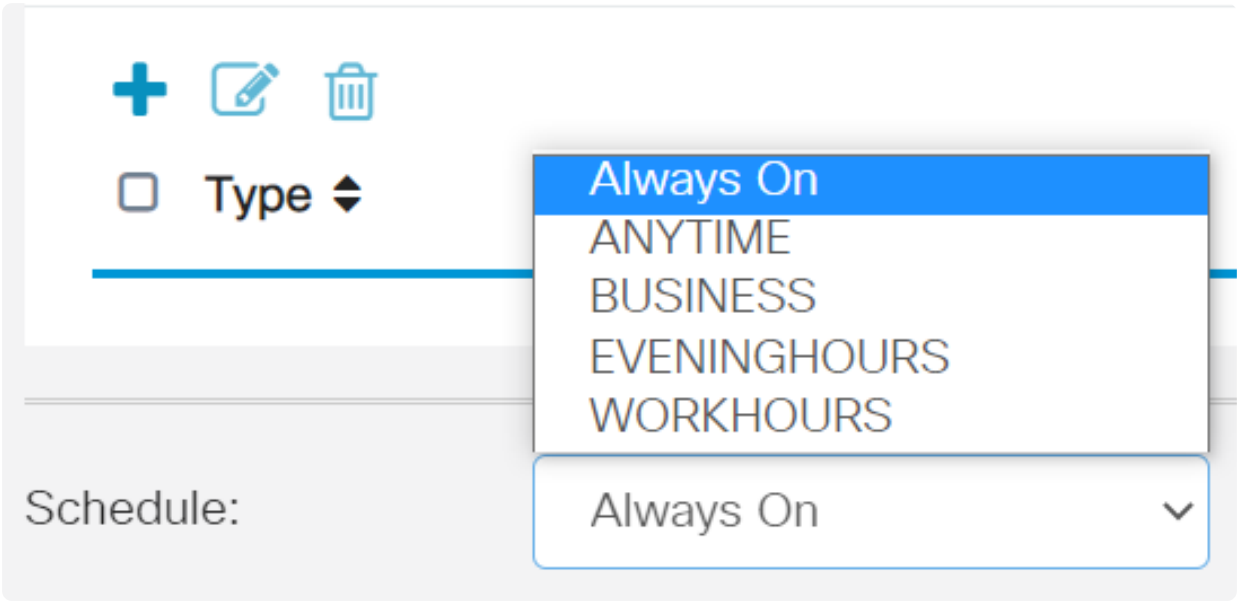
Dans la liste déroulante OS Type, sélectionnez le système d'exploitation auquel la stratégie doit s'appliquer. Une seule option peut être choisie à la fois. Les options sont les suivantes :

- ANY : applique la stratégie à tout type de système d'exploitation. Il s'agit de la configuration par défaut.
- Android : applique la stratégie au système d'exploitation Android uniquement.
- BlackBerry : applique la stratégie au système d'exploitation Blackberry 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 n'est pas répertorié.
- Windows : applique la stratégie au système d'exploitation Windows.
- iOS : applique la stratégie à iOS OS uniquement.



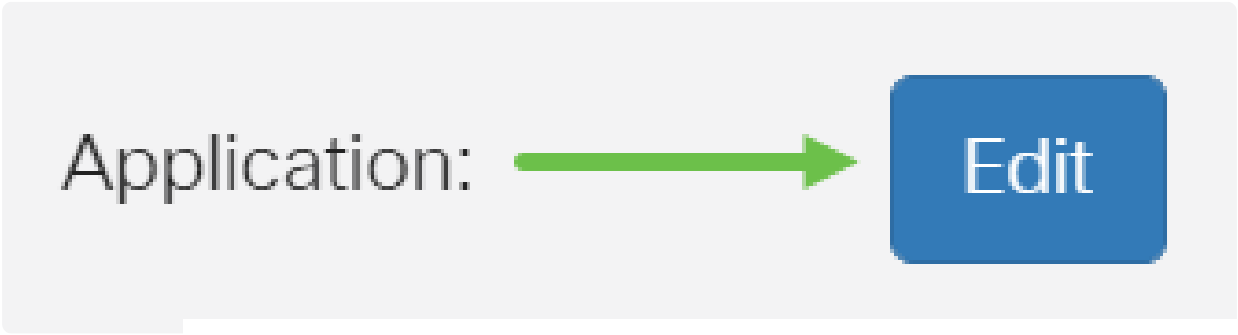
Étape 8

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



Étape 9

Cliquez sur l'icône de modification.



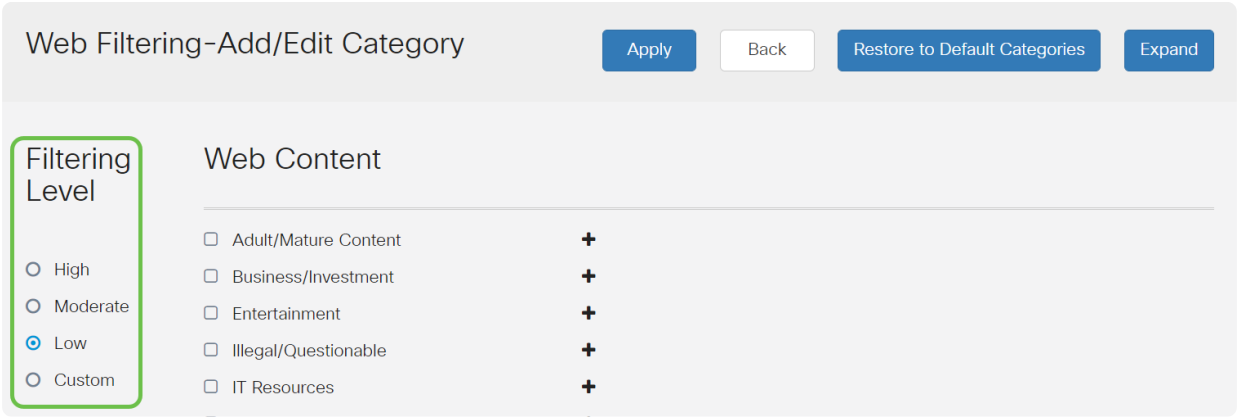
Étape 10

Dans la colonne Filtering Level (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 Elevée, Modérée, Faible et Personnalisée. Cliquez sur l'un des niveaux de filtrage ci-dessous pour connaître les sous-catégories prédéfinies spécifiques filtrées pour chacune de leurs catégories de contenu Web activées. Les filtres prédéfinis ne peuvent plus être modifiés et sont grisés.

- Low : option par défaut. La sécurité est activée avec cette option.
- Modéré : le contenu pour adultes/adulte, illégal/discutable et la sécurité sont activés

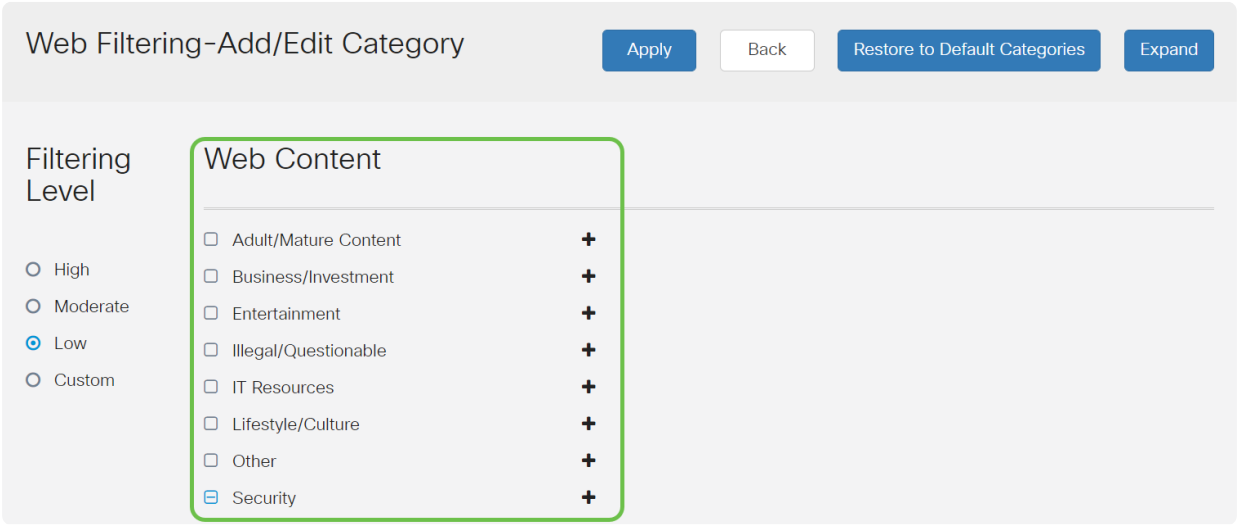
avec cette option.

- Élevé : les contenus pour adultes/adultes, les activités/investissements, les contenus illégaux/discutables, 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

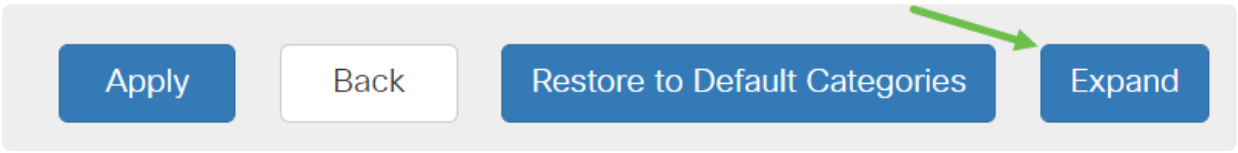
Saisissez le contenu Web que vous souhaitez filtrer. Cliquez sur l'icône plus si vous voulez plus de détails sur une section.



Étape 12 (facultative)

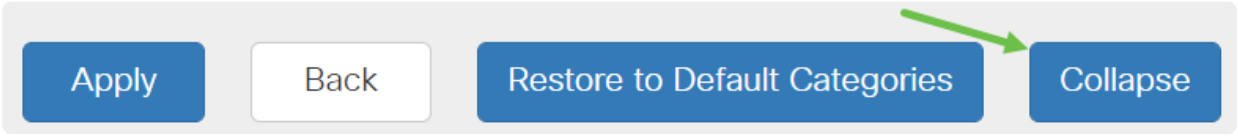
Pour afficher toutes les sous-catégories et descriptions de contenu Web, cliquez sur le

bouton Développer.



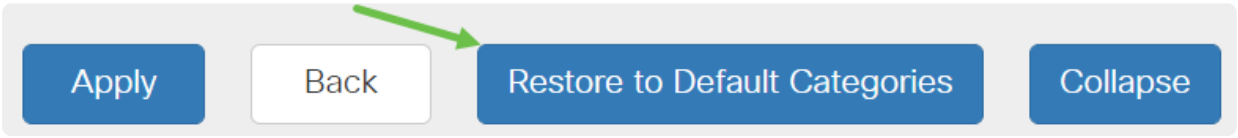
Étape 13 (facultative)

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



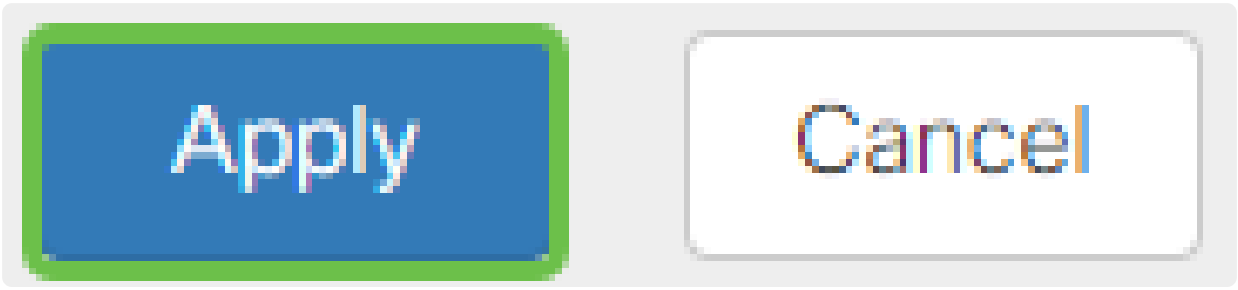
Étape 14 (facultative)

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



Étape 15

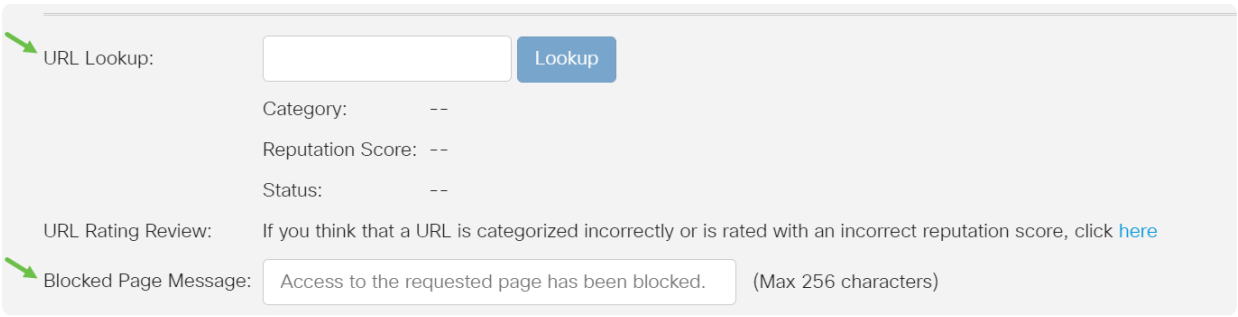
Cliquez sur Apply pour enregistrer la configuration et revenir à la page Filter pour poursuivre la configuration.



ⓘ Note: Dans le tableau Liste d'applications, les sous-catégories correspondantes basées sur le niveau de filtrage choisi rempliront le tableau.

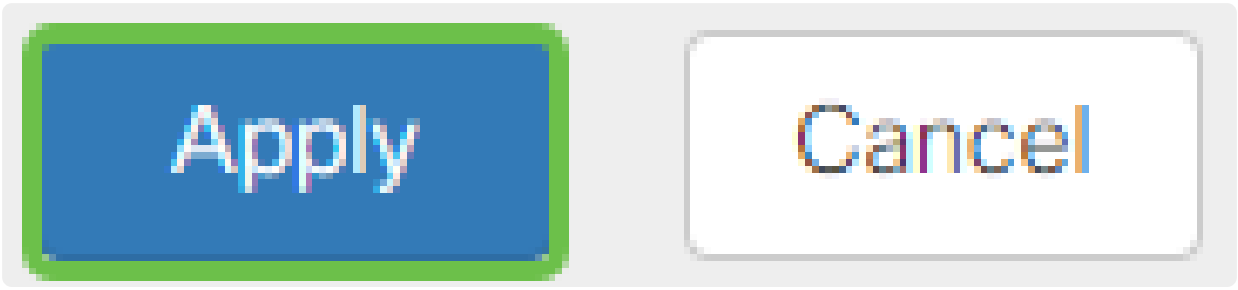
Étape 16 (facultative)

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



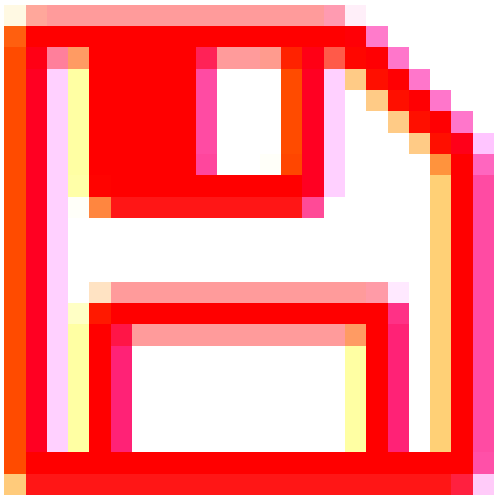
Étape 17 (facultative)

Cliquez sur Apply.



Étape 18

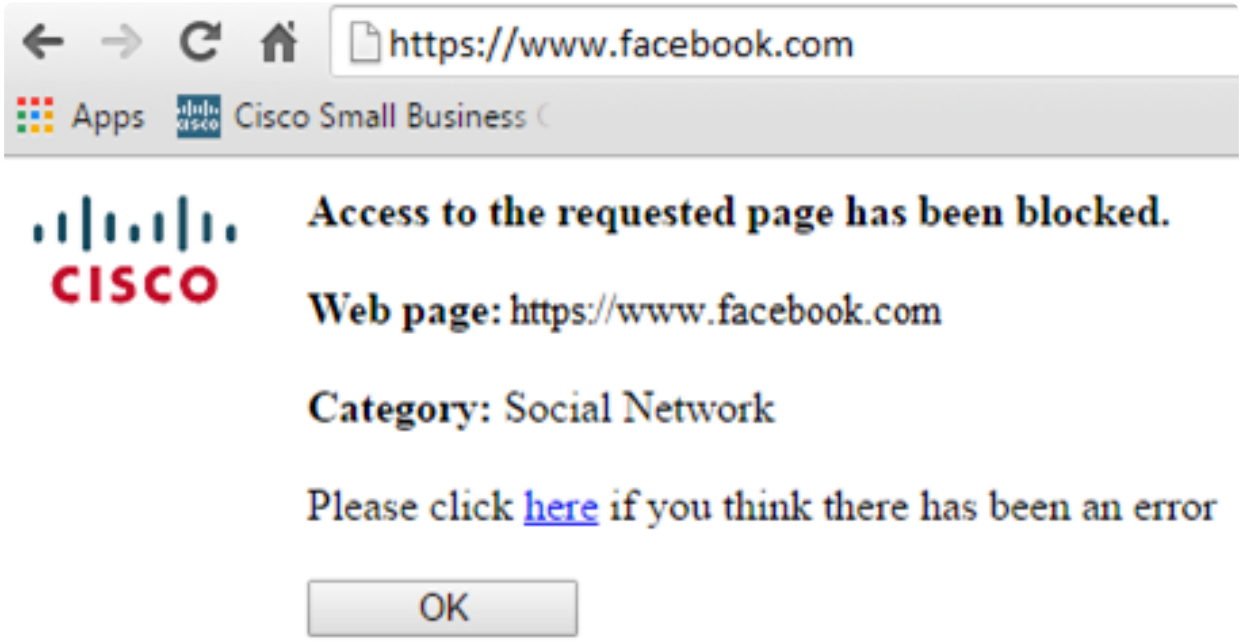
Pour enregistrer la configuration de façon permanente, accédez à la page Copy/Save Configuration ou cliquez sur l'icône save dans la partie supérieure de la page.



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 de suffisamment de sécurité, cliquez sur 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 prendrons contact avec le revendeur.

Idéalement, vous n'auriez pas à faire l'un ou l'autre, mais si vous arrivez à ce carrefour, nous serons heureux de vous aider ! Pour que le processus soit aussi rapide que possible, vous aurez besoin des références dans le tableau ci-dessus ainsi que de celles décrites ci-dessous.

Informations requises	Localisation des informations
Facture de licence	Vous devriez recevoir ce message par e-mail après avoir acheté les licences.
Numéro de commande client Cisco	Il se peut que vous deviez retourner chez le revendeur pour obtenir ce service.
Capture d'écran de la page de licence de votre compte Smart	La capture d'écran capture le contenu de votre écran pour le partager avec notre équipe. Si vous n'êtes pas familier avec les captures d'écran, vous pouvez utiliser les méthodes ci-dessous.

Captures d'écran

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

Étant donné les différences dans la procédure requise pour capturer une capture d'écran, voir ci-dessous pour les liens spécifiques à votre système d'exploitation.

- Fenêtres
- MAC
- iPhone/iPad
- Android

Licence de filiale Umbrella RV (en option)

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

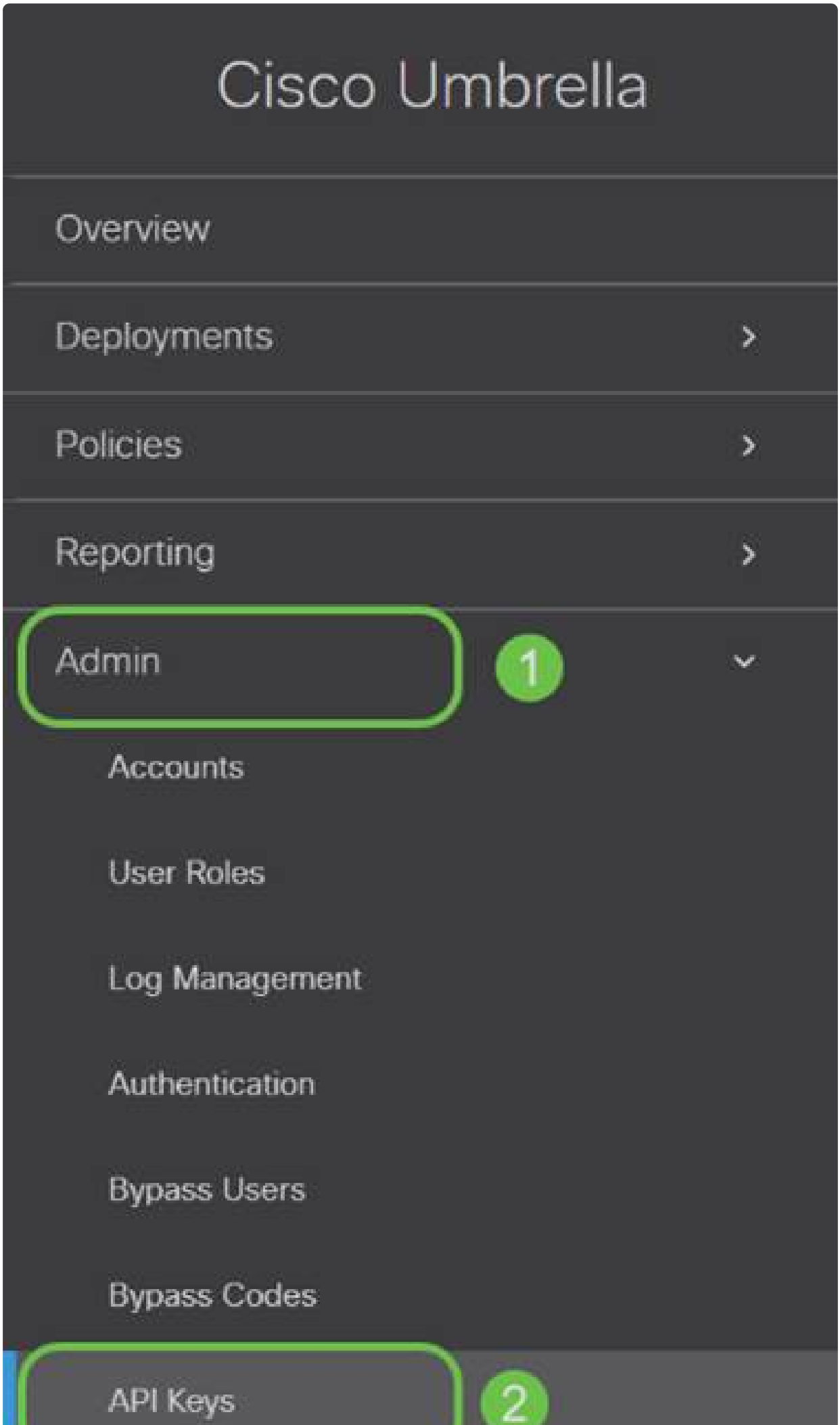
Umbrella opère dans le cloud et fournit de nombreux services liés à la sécurité. De la menace émergente à l'enquête post-événement. Umbrella détecte et empêche les attaques sur tous les ports et protocoles.

Umbrella utilise le DNS comme principal vecteur de défense. Lorsque les utilisateurs entrent une URL dans leur barre de navigateur 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 requête est bloquée. Ces données télémétriques sont transférées et analysées en microsecondes, ce qui n'ajoute pratiquement aucune latence. Les données de télémétrie utilisent des journaux et des instruments pour suivre des milliards de requêtes DNS dans le monde entier. Lorsque ces données sont omniprésentes, les corréler dans le monde entier permet de réagir rapidement aux attaques dès leur apparition. 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 la documentation, et ici les options d'assistance Umbrella.

Étape 1

Après vous être connecté à votre compte Umbrella, dans l'écran Dashboard cliquez sur Admin > API Keys.


Cisco Umbrella
Overview
Deployments
Policies
Reporting
Admin
1
Accounts
User Roles
Log Management
Authentication
Bypass Users
Bypass Codes
API Keys
2

Écran Anatomie des clés API (avec une clé API préexistante)

1 Add API Key (Ajouter une clé API) : lance la création d'une nouvelle clé à utiliser avec l'API Umbrella.

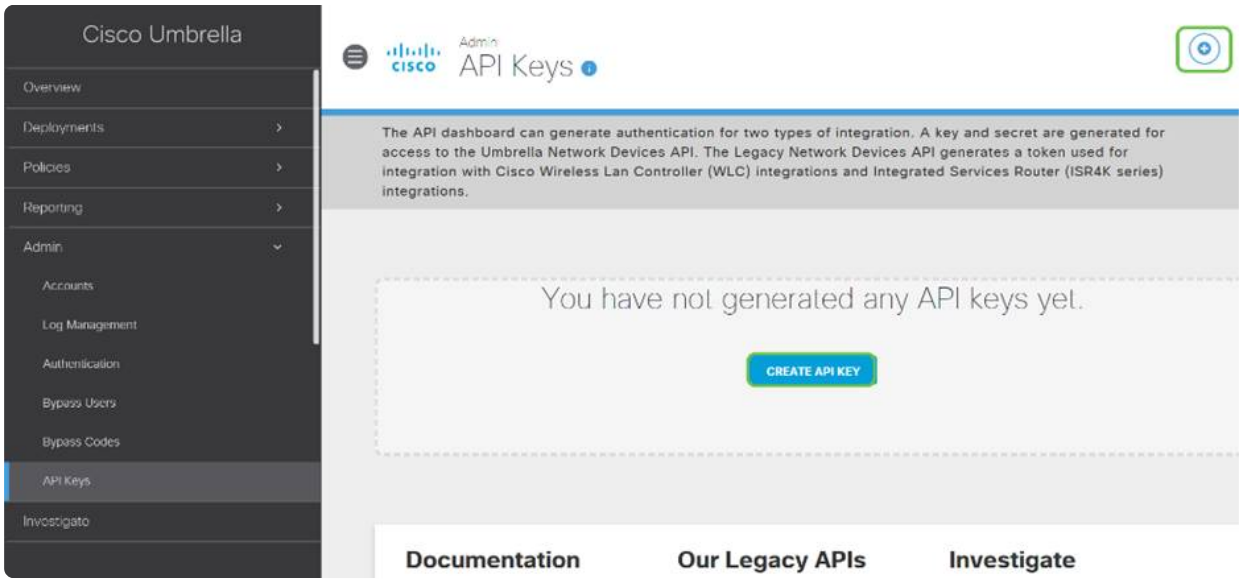
2 Informations supplémentaires : glisse vers le bas/haut avec un explicateur pour cet écran.

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 d'assistance - Liens vers la documentation du site Umbrella concernant les sujets de chaque section.

Étape 2

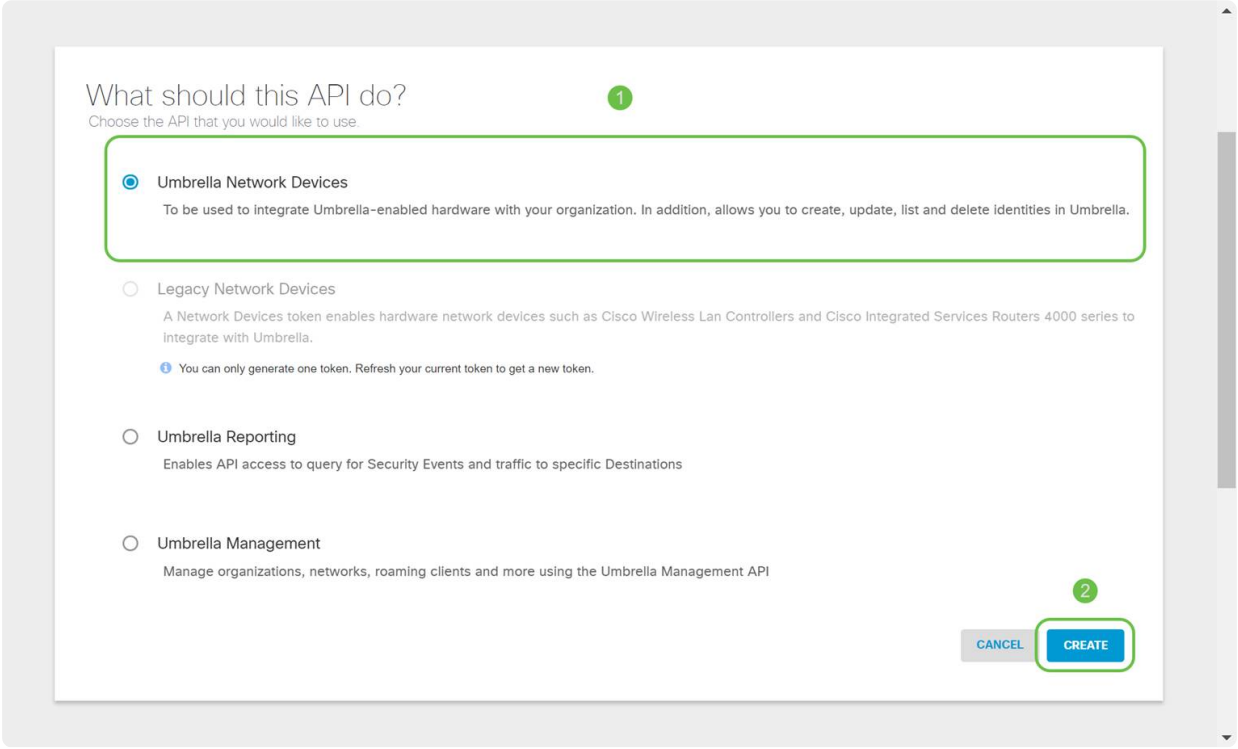
Cliquez sur le bouton Add API Key dans le coin supérieur droit ou cliquez sur le bouton Create API Key. Ils fonctionnent tous les deux de la même manière.



ⓘ Note: La capture d'écran ci-dessus serait similaire à ce que vous verriez en ouvrant ce menu pour la première fois.

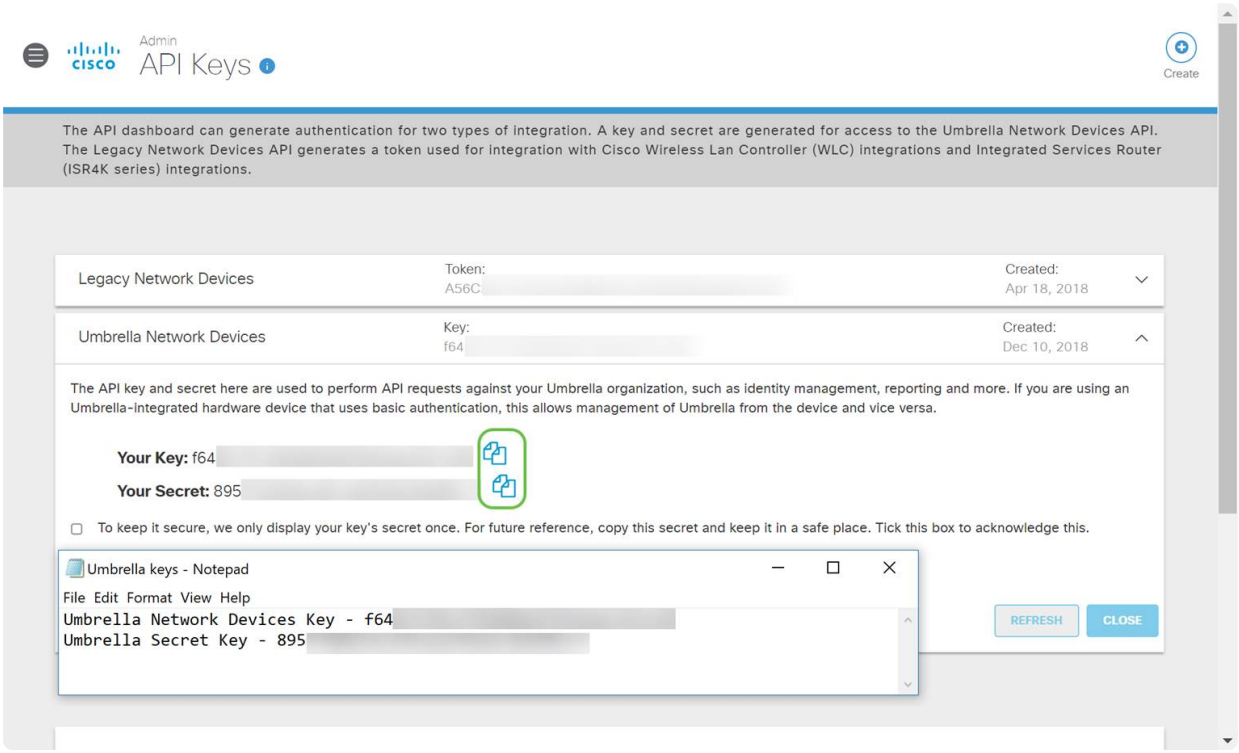
Étape 3

Sélectionnez Périphériques réseau parapluie, puis cliquez sur le bouton Créer.



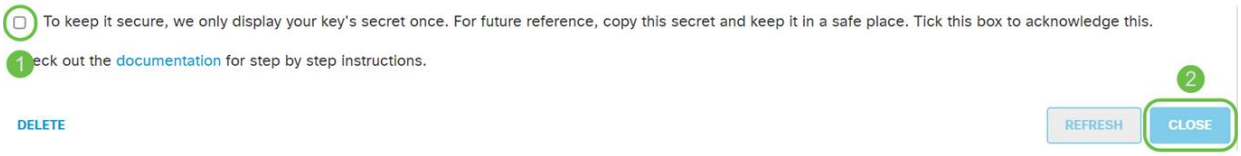
Étape 4

Ouvrez un éditeur de texte tel que le bloc-notes, puis cliquez sur l'icône Copier à droite de votre API et de votre clé secrète API, une notification contextuelle confirmera que la clé est copiée dans votre Presse-papiers. Une par une, collez votre clé secrète et votre clé API dans le document, en les étiquetant pour référence ultérieure. Dans ce cas, son étiquette est « clé de périphériques réseau Umbrella ». Enregistrez ensuite le fichier texte dans un emplacement sécurisé auquel vous pourrez accéder facilement ultérieurement.



Étape 5

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



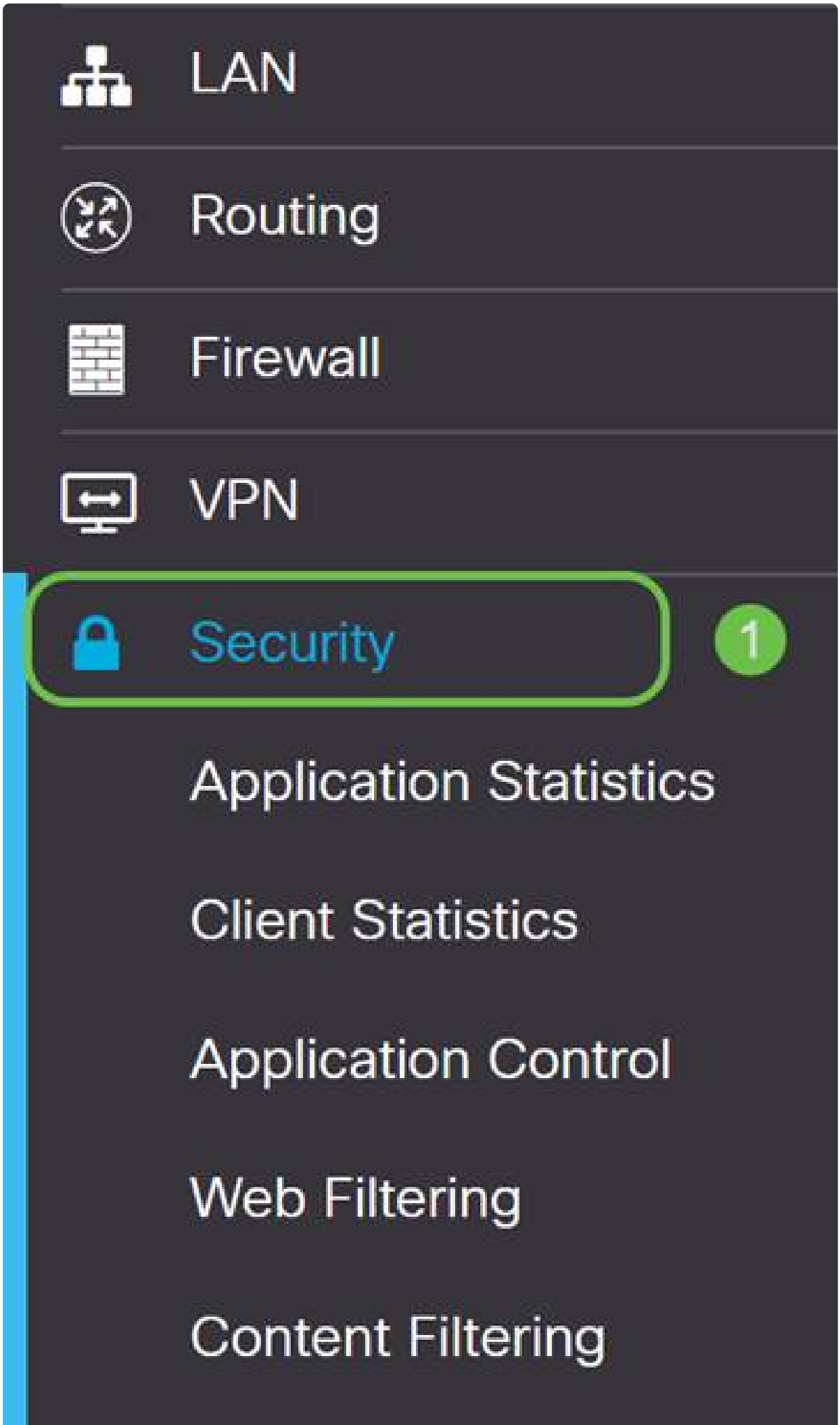
ⓘ Note: Si vous perdez ou supprimez accidentellement la clé secrète, il n'y a pas de fonction ou de numéro de support à appeler pour récupérer cette clé. En cas de perte, vous devrez supprimer la clé et réautoriser la nouvelle clé API avec chaque périphérique que vous souhaitez protéger avec Umbrella.

Configuration d'Umbrella sur votre RV345P

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

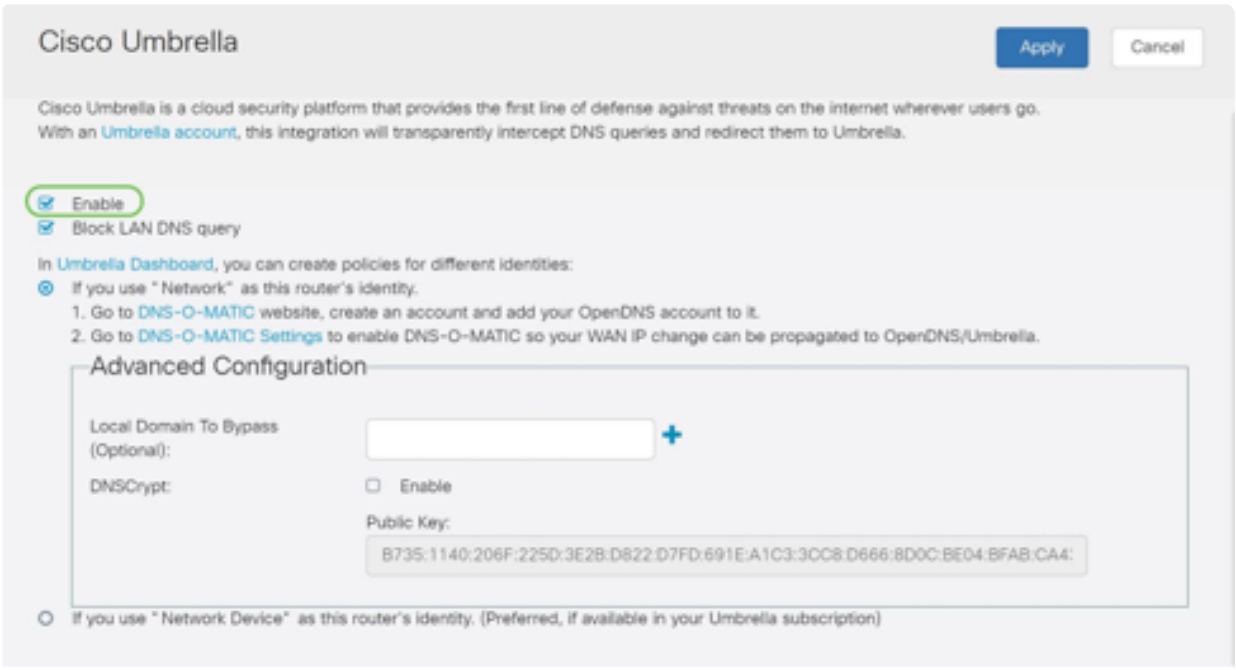
Étape 1

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


LAN
Routing
Firewall
VPN
Security
1
Application Statistics
Client Statistics
Application Control
Web Filtering
Content Filtering

Étape 2

L'écran de l'API Umbrella propose une gamme d'options. Commencez par activer Umbrella en cochant la case Enable.

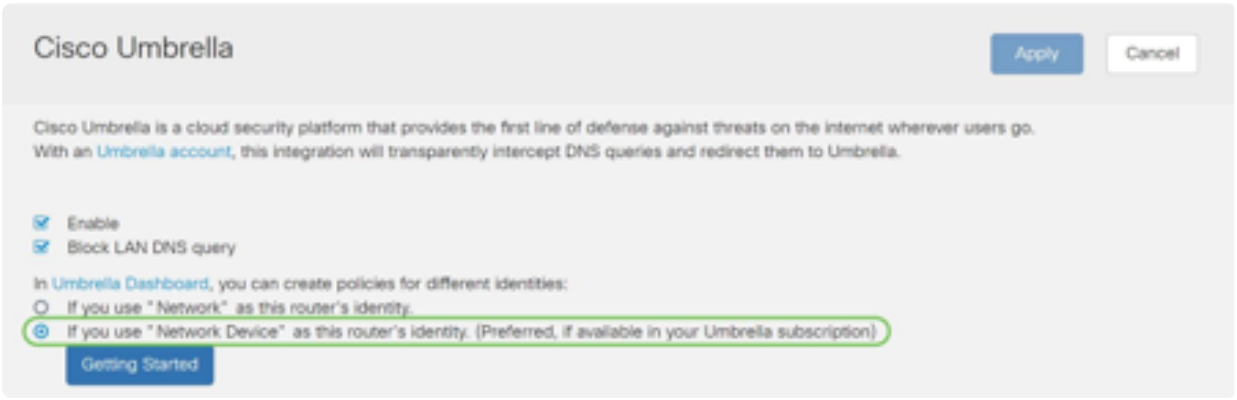


Étape 3 (facultative)

Activé par défaut, la case Block LAN DNS Queries est cochée. Cette fonctionnalité intelligente crée automatiquement des listes de contrôle d'accès sur votre routeur, ce qui empêche le trafic DNS d'accéder à Internet. Cette fonctionnalité force toutes les requêtes de traduction de domaine à être dirigées par le RV345P et est une bonne idée pour la plupart des utilisateurs.

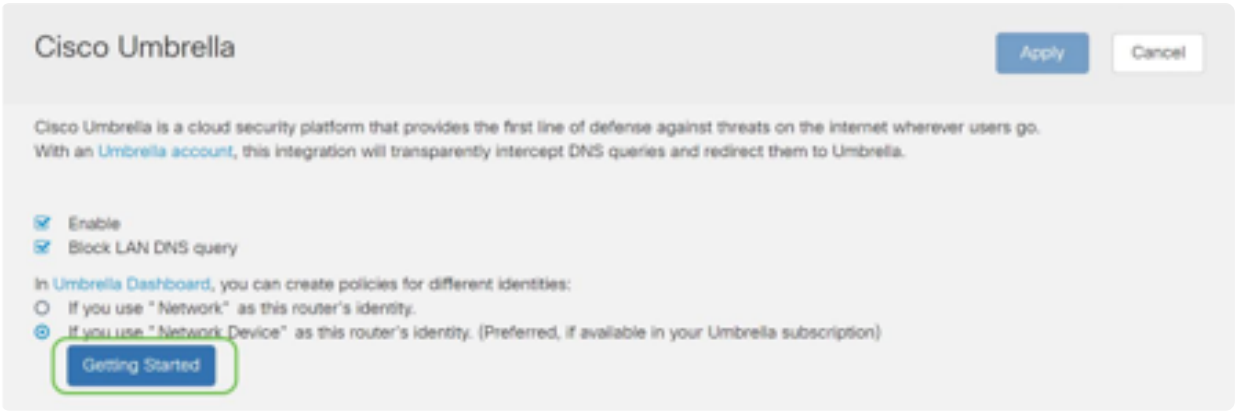
Étape 4

L'étape suivante se déroule de deux manières différentes. Ils dépendent tous les deux de la configuration de votre réseau. Si vous utilisez un service tel que DynDNS ou NoIP, vous conservez le schéma d'attribution de noms par défaut « Réseau ». Vous devrez vous connecter à ces comptes pour assurer l'interface d'Umbrella avec ces services, car ils offrent une protection. Pour nos besoins, nous utilisons l'option « Network Device » (Périphérique réseau). Nous sélectionnons donc la case d'option inférieure.



Étape 5

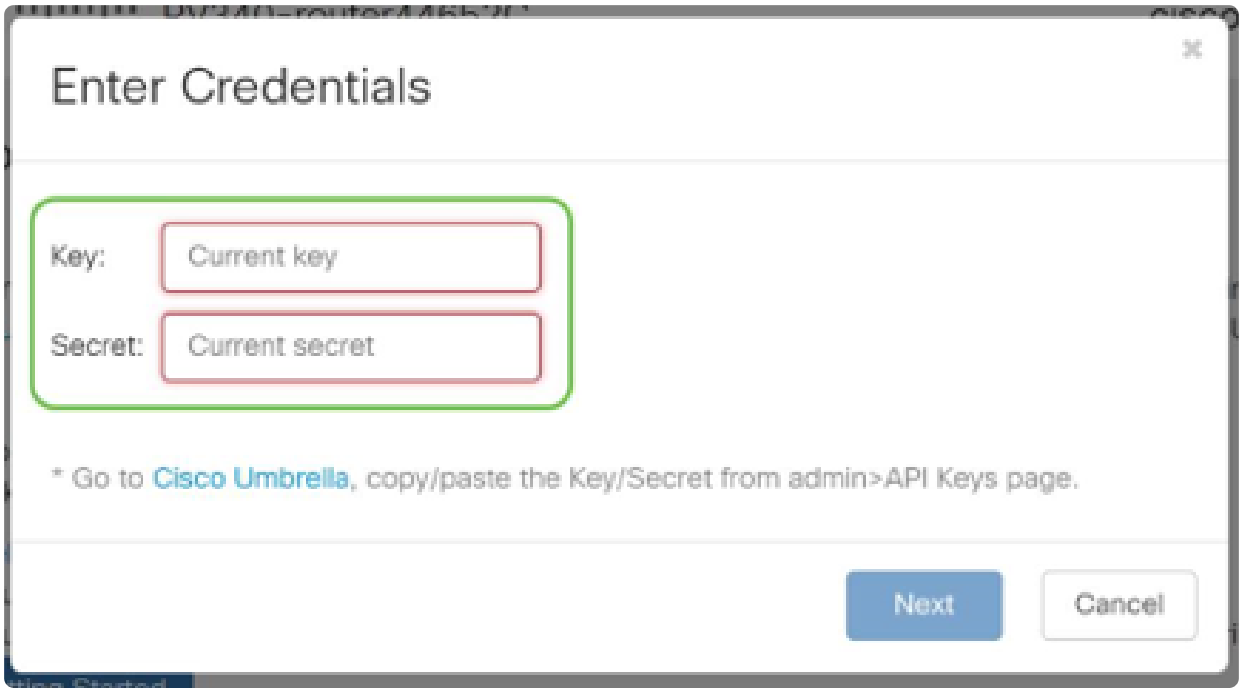
Cliquez sur Getting Started.



Étape 6

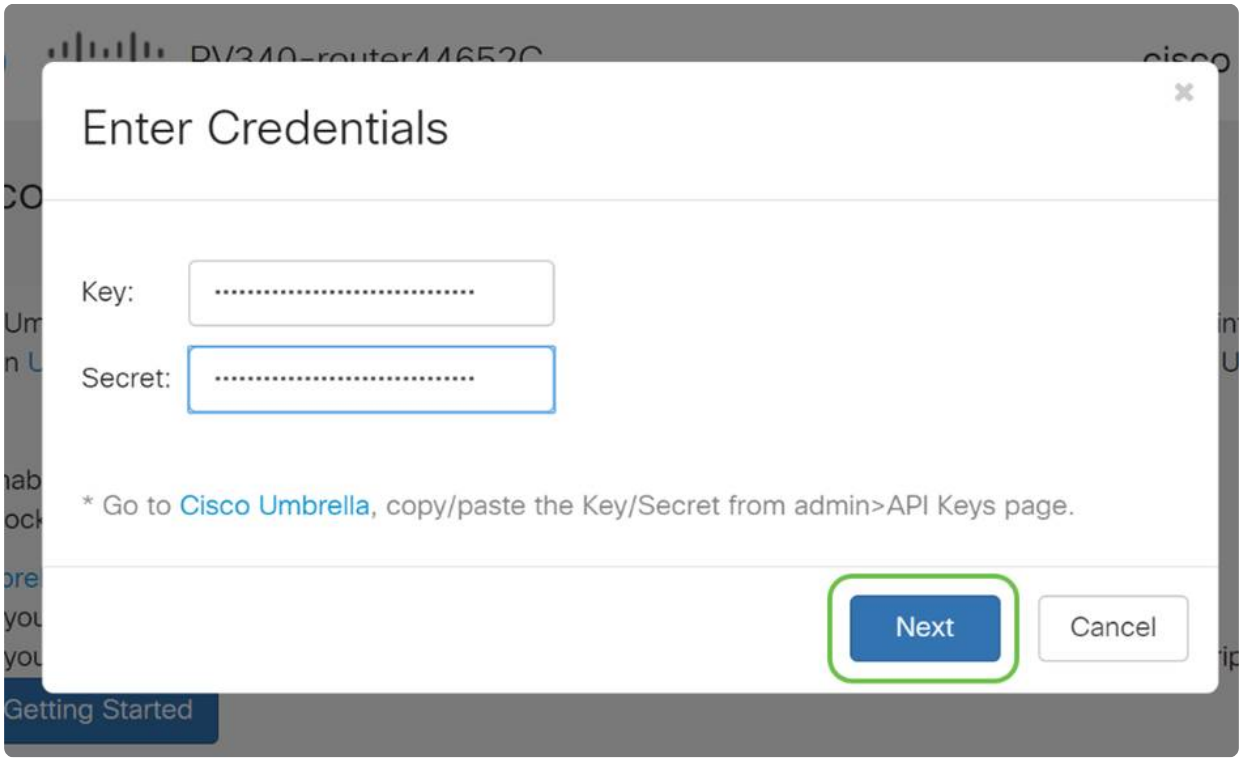
Entrez la clé API et la clé secrète dans les zones de texte.

> ⓘ Note: 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 pas de fonction ou de numéro de support à appeler pour récupérer cette clé. Gardez-la secrète et sécurisée. En cas de perte, vous devrez supprimer la clé et réautoriser la nouvelle clé API avec chaque périphérique que vous souhaitez protéger avec Umbrella.



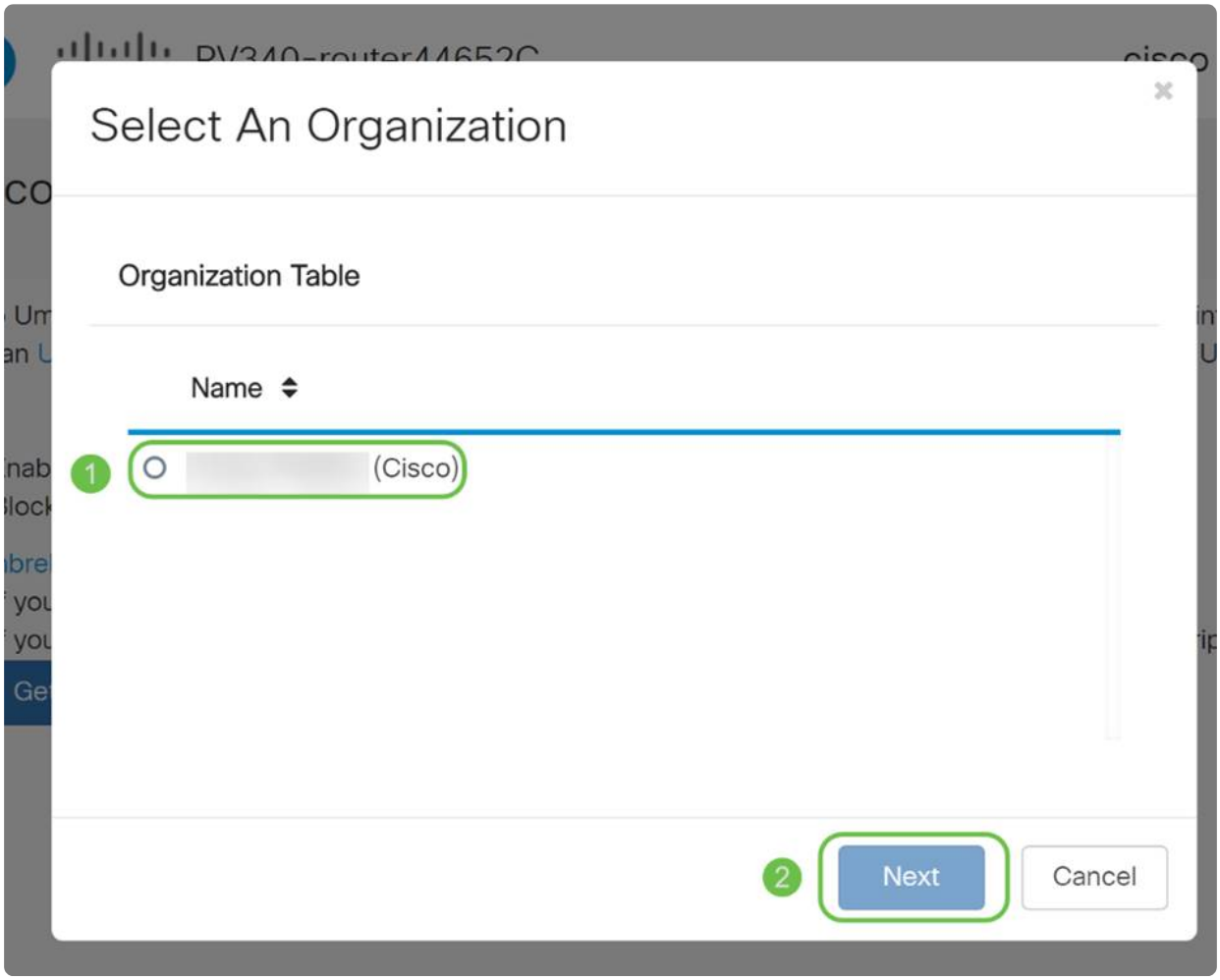
Étape 7

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



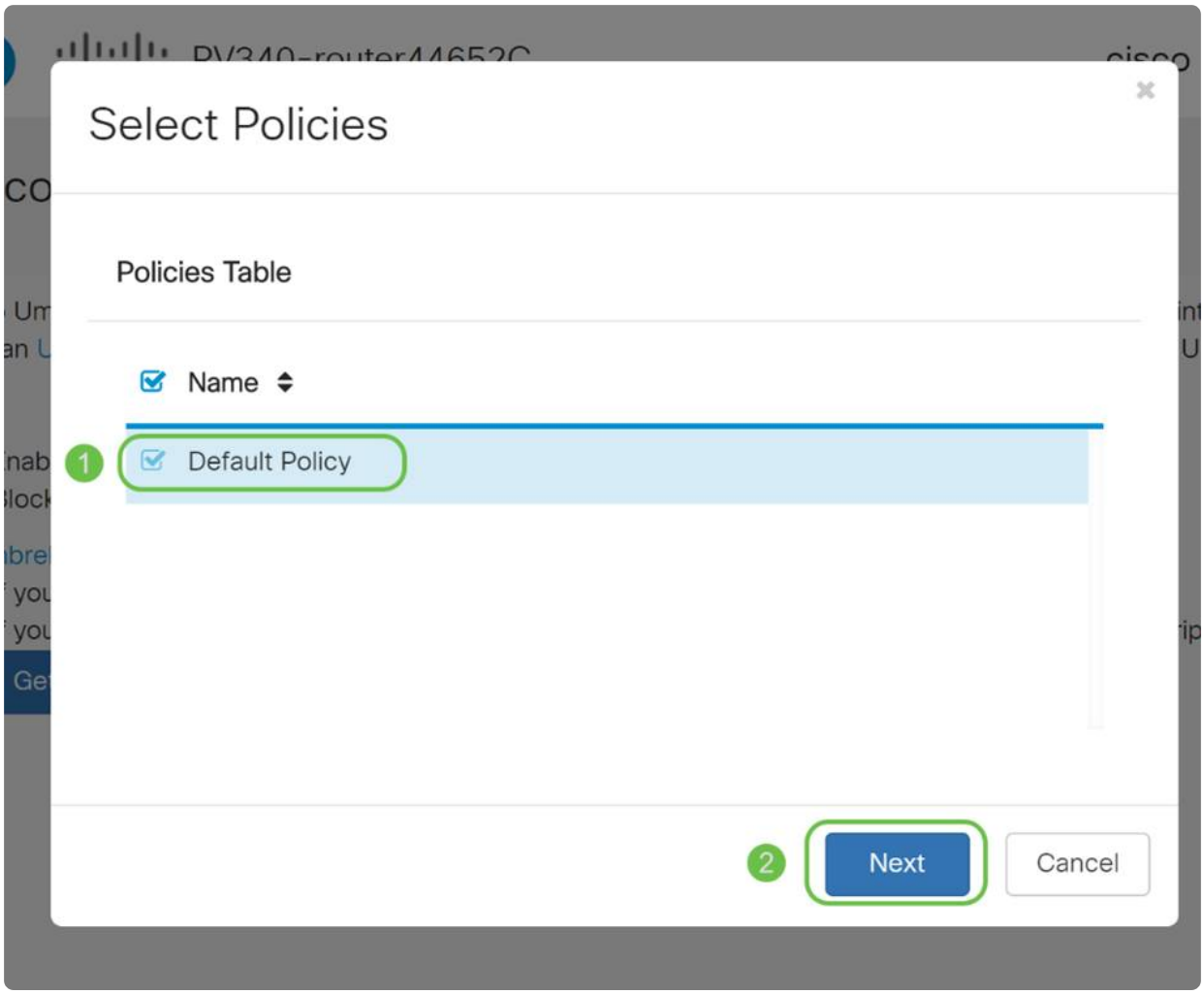
Étape 8

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



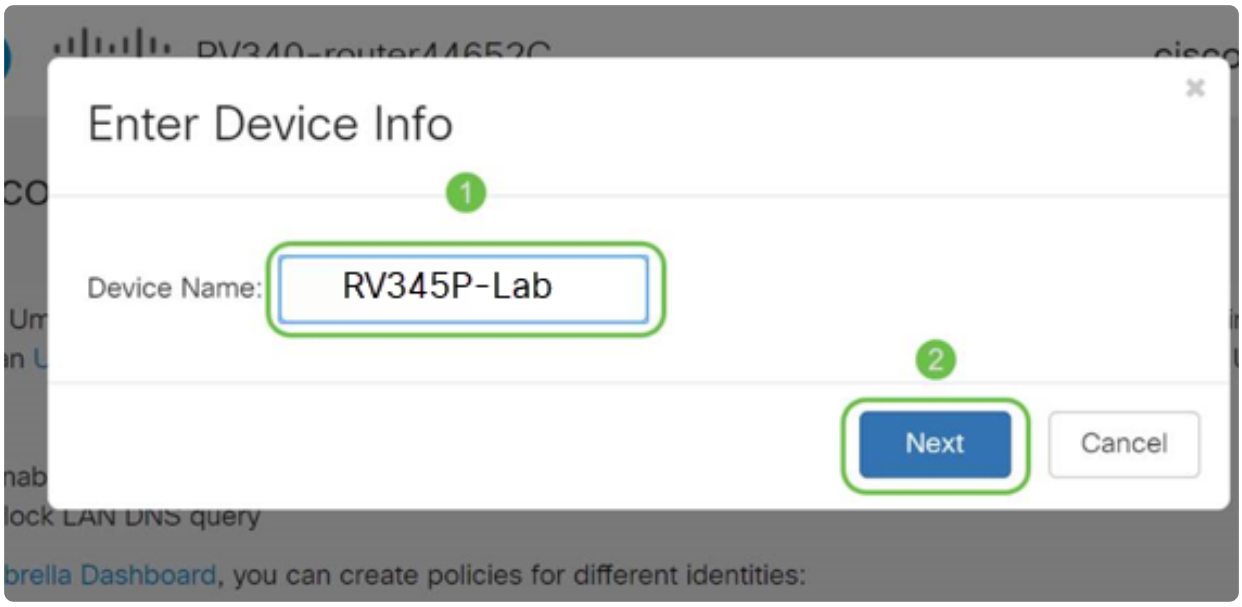
Étape 9

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



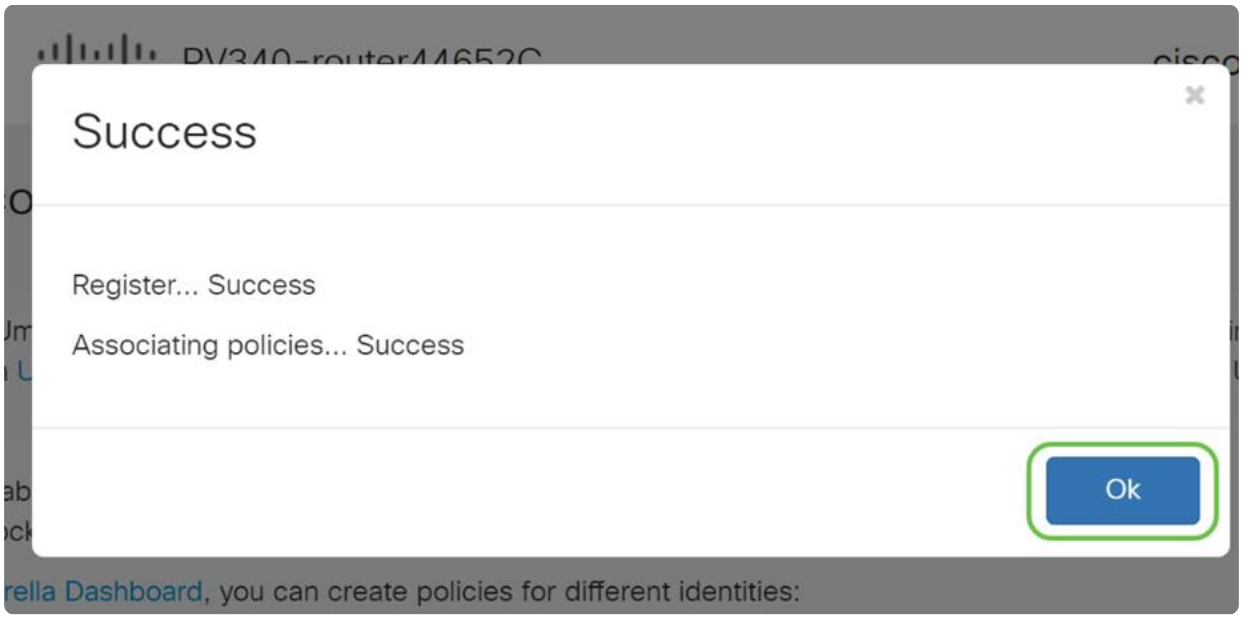
Étape 10

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



Étape 11

L'écran suivant permet de valider les paramètres sélectionnés et de fournir une mise à jour lorsque l'association est réussie. Click OK.

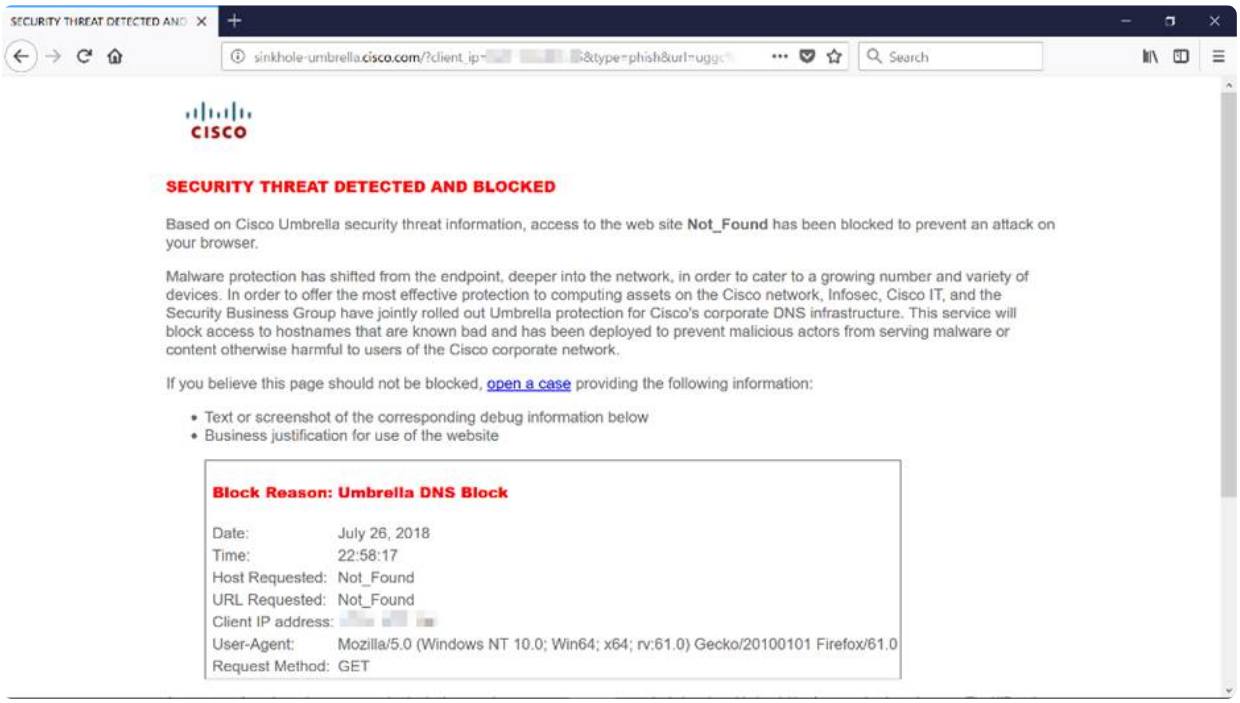


Confirmation

Félicitations, vous êtes désormais protégé par Cisco Umbrella. Ou tu l'es ? Assurez-vous qu'en vérifiant à nouveau avec un exemple en direct, Cisco a créé un site Web

dédié à la détermination de ce problème dès que la page se charge. Cliquez ici ou tapez https://InternetBadGuys.com dans la barre du navigateur.

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



Autres options de sécurité

Craignez-vous qu'une personne tente un accès non autorisé au réseau en débranchant un câble Ethernet d'un périphérique réseau et en s'y connectant ? Dans ce cas, il est important d'enregistrer une liste des hôtes autorisés à se connecter directement au routeur avec leurs adresses IP et MAC respectives. Pour obtenir des instructions, reportez-vous à l'article Configure IP Source Guard on the RV34x Series Router.

Options VPN

Une connexion de réseau privé virtuel (VPN) permet aux utilisateurs d'accéder à un réseau privé, d'envoyer et de recevoir des données vers et depuis 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 sont à l'extérieur 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 établie 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 pouvoir établir une connexion.

Si vous n'êtes pas sûr de savoir quel VPN correspond le mieux à vos besoins, consultez la présentation et les meilleures pratiques de Cisco Business VPN.

> ⓘ Note: AnyConnect VPN est le seul produit pris en charge par Cisco VPN répertorié 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 uniquement à titre indicatif. Si vous avez besoin d'aide sur ces éléments au-delà de l'article, vous devez contacter ce tiers pour obtenir de l'aide.

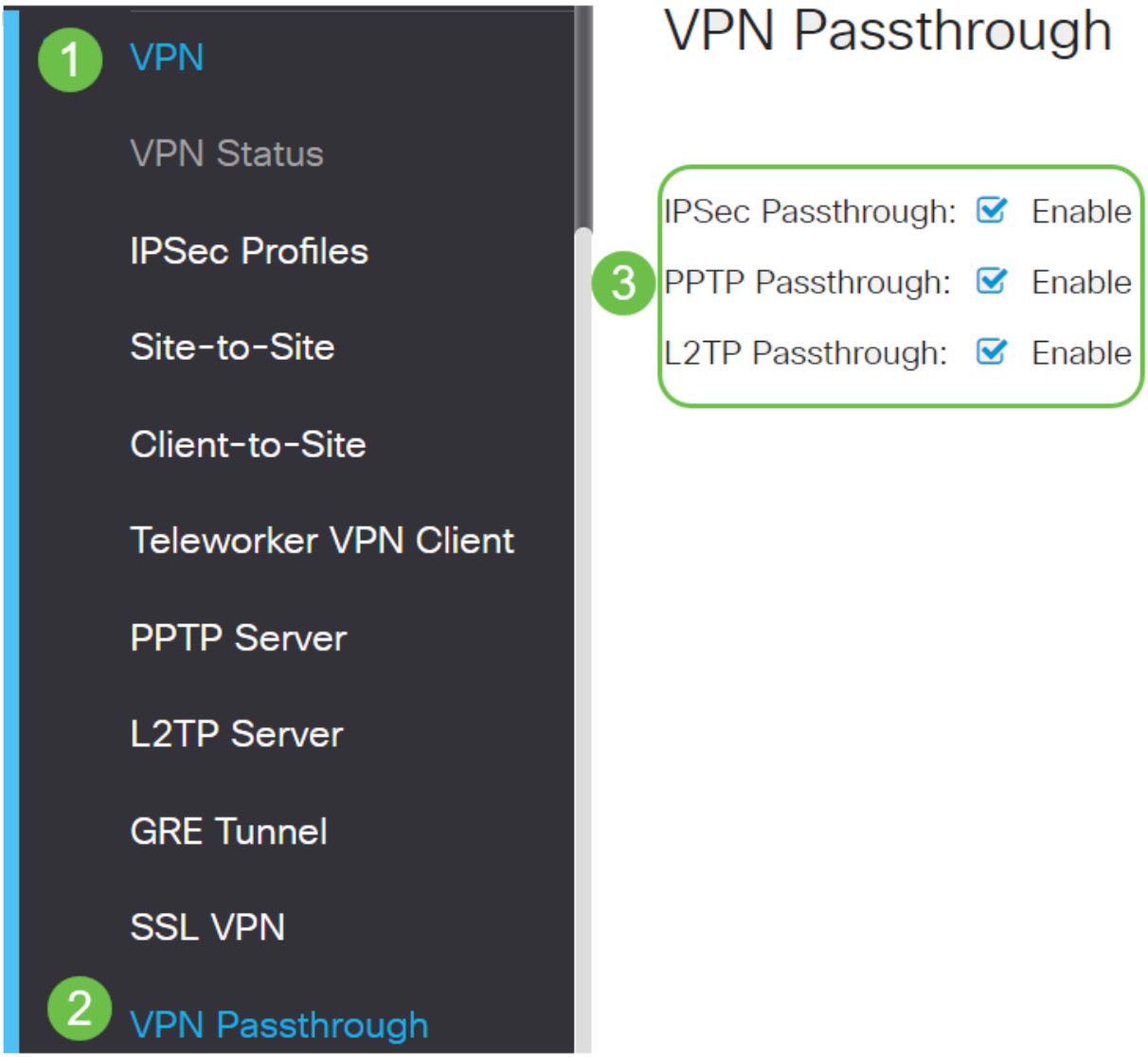
Si vous ne prévoyez pas de configurer un VPN, vous pouvez cliquer pour passer à la section suivante.

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, les protocoles PPTP (Point-to-Point Tunneling Protocol) et IPsec (Internet Protocol Security) VPN ne prennent pas en charge la fonction NAT. C'est là que le Passthrough VPN intervient. Un VPN Passthrough est une fonctionnalité qui permet au trafic VPN généré à partir des clients VPN connectés à ce routeur de passer par ce routeur et de se connecter à un point

d'extrémité VPN. Le VPN Passthrough permet au VPN PPTP et IPsec de passer uniquement sur Internet, à partir d'un client VPN, puis d'atteindre la passerelle VPN distante. Cette fonctionnalité est généralement présente sur les routeurs domestiques qui prennent en charge la fonction NAT.

Par défaut, les protocoles IPsec, PPTP et L2TP Passthrough sont activés. Si vous souhaitez afficher ou ajuster ces paramètres, sélectionnez VPN > VPN Passthrough. Afficher ou ajuster selon les besoins.



VPN AnyConnect

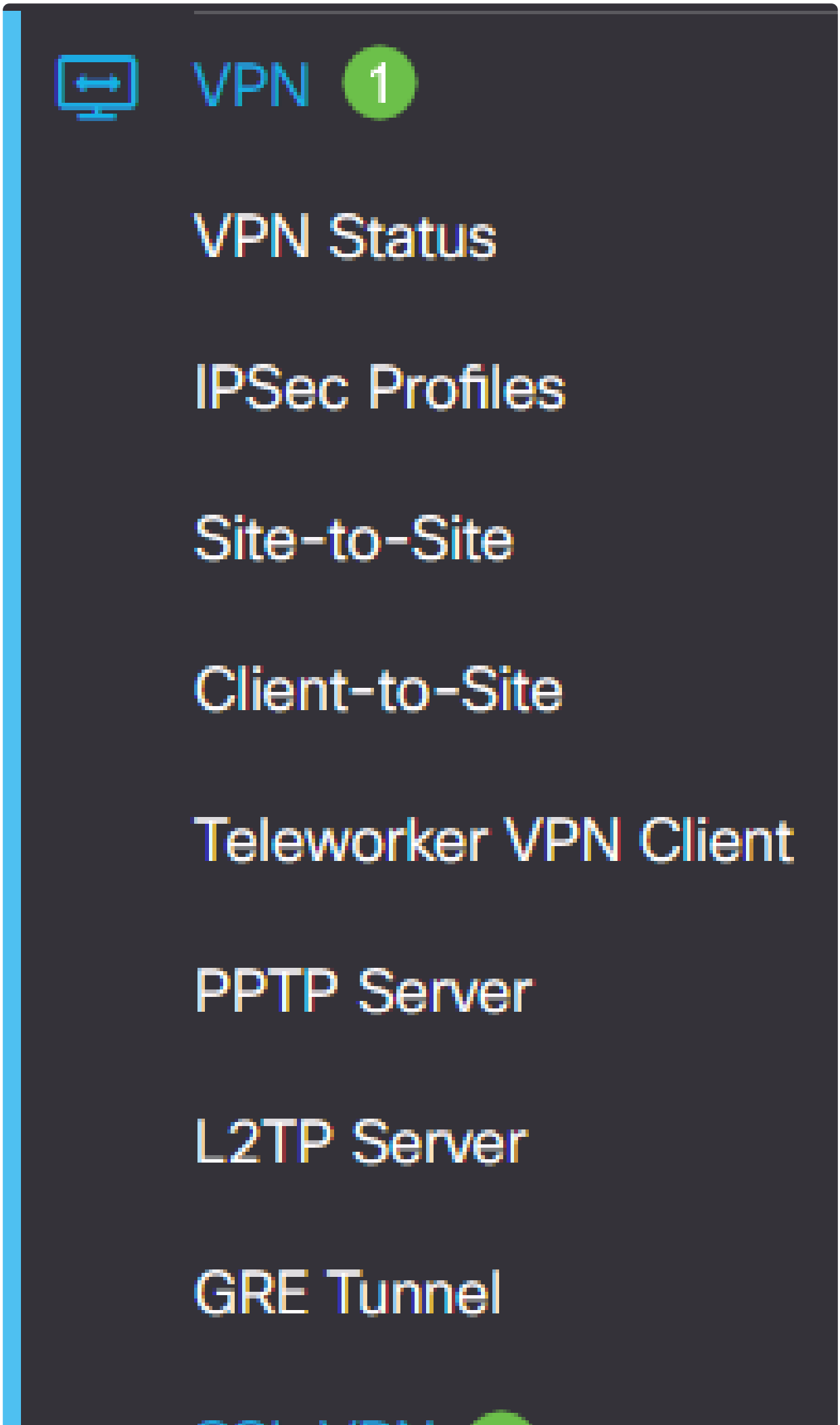
L'utilisation de Cisco AnyConnect présente plusieurs avantages :

1. Connectivité sécurisée et permanente
2. Sécurité permanente et application des stratégies
3. Déploiement à partir de l'appliance de sécurité adaptative (ASA) ou des systèmes de déploiement de logiciels d'entreprise
4. Personnalisable et traduisible
5. Configuration facile
6. Prise en charge d'IPsec (Internet Protocol Security) et de SSL (Secure Sockets Layer)
7. Prise en charge du protocole IKEv2.0 (Internet Key Exchange version 2.0)

Configurer un VPN SSL AnyConnect sur le RV345P

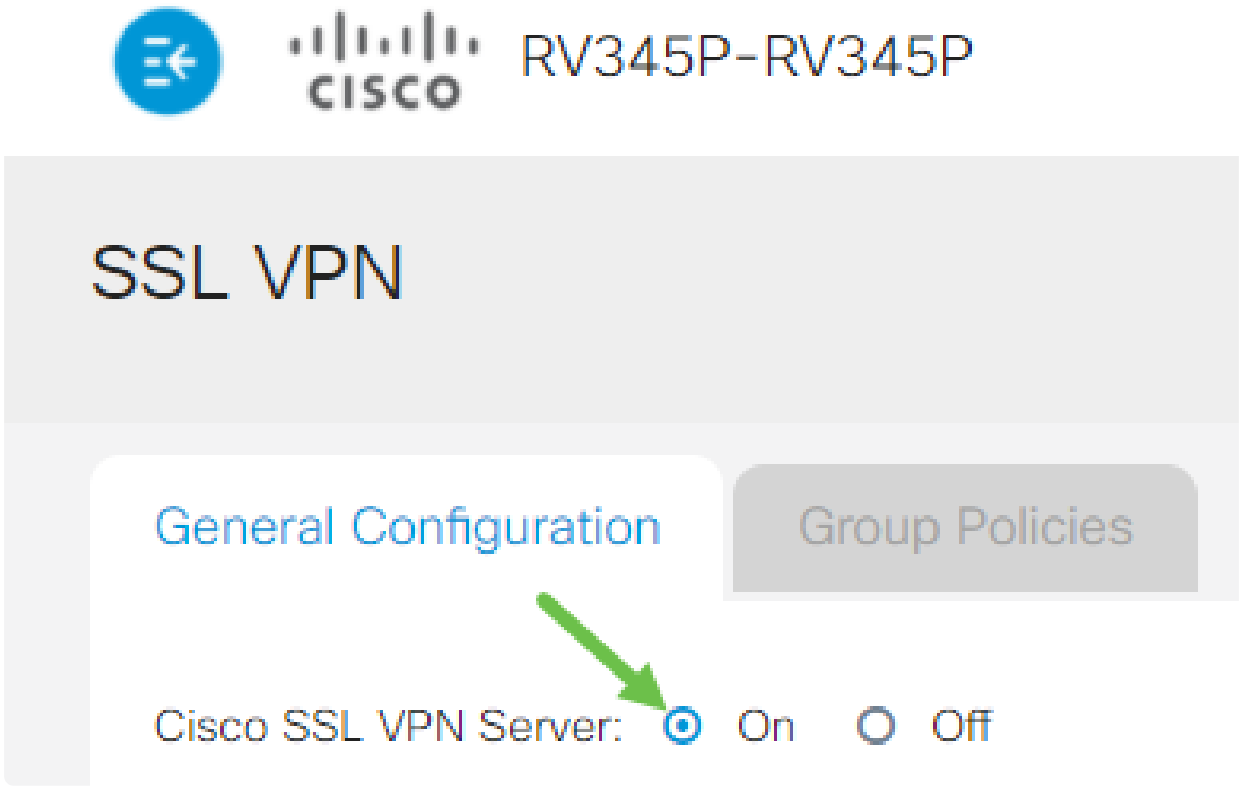
Étape 1

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


VPN
1
VPN Status
IPSec Profiles
Site-to-Site
Client-to-Site
Teleworker VPN Client
PPTP Server
L2TP Server
GRE Tunnel

Étape 2

Cliquez sur la case d'option On pour activer le serveur VPN SSL Cisco.



Paramètres de passerelle obligatoires

Étape 1

Les paramètres de configuration suivants sont obligatoires :

1 Sélectionnez l'interface de passerelle dans la liste déroulante. Il s'agit du port qui sera utilisé pour acheminer 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 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.

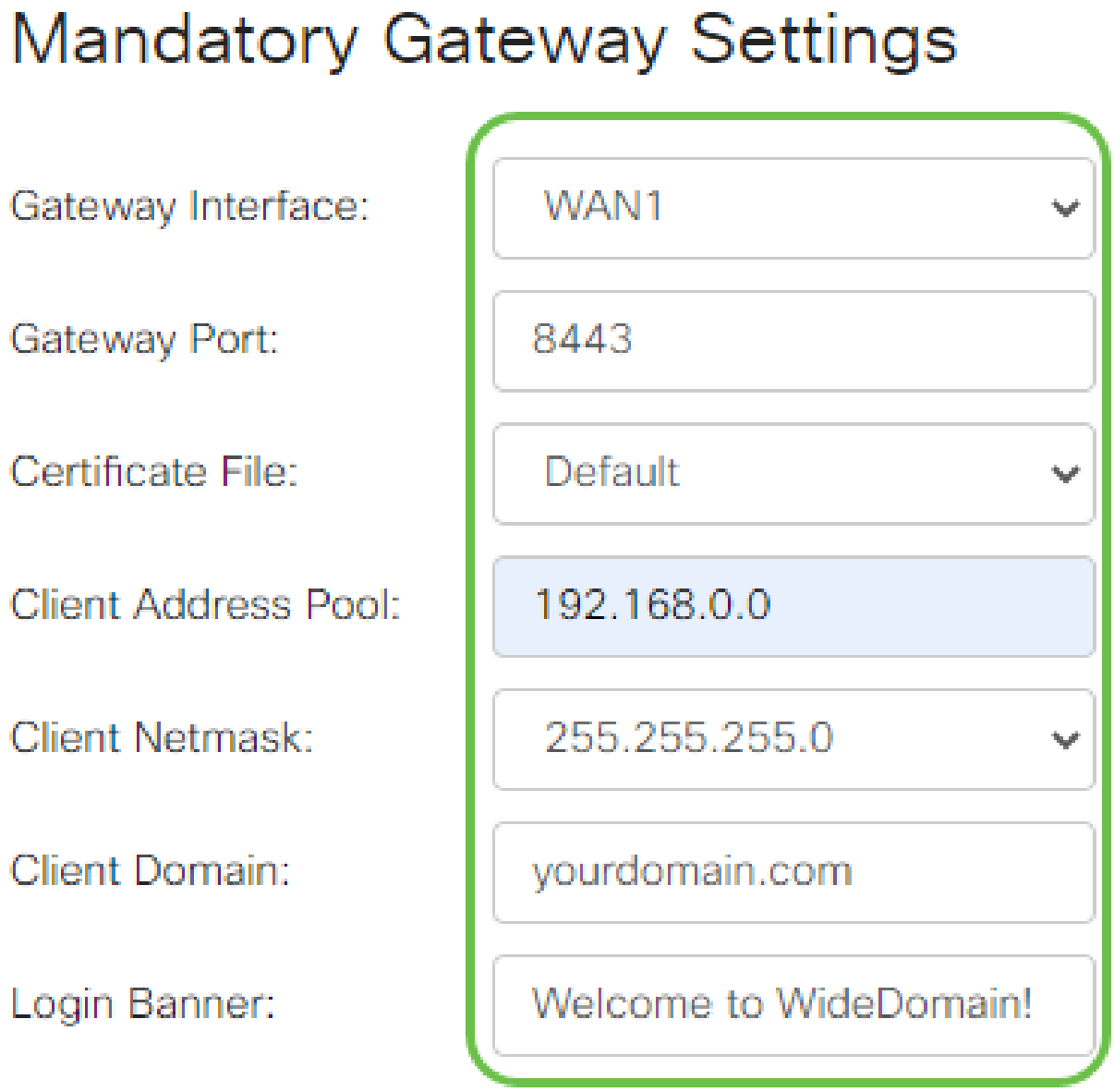
4 Saisissez l'adresse IP du pool d'adresses client dans le champ Client Address Pool. Ce pool correspond à la plage d'adresses IP qui sera allouée aux clients VPN distants.

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

5 Sélectionnez le masque de réseau du client dans la liste déroulante.

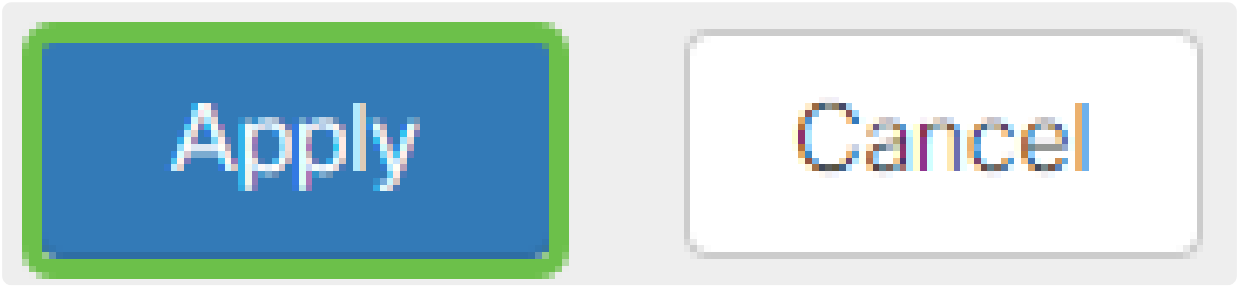
6 Entrez le nom de domaine du client dans le champ Client Domain. Il s'agit du nom de domaine qui doit être envoyé aux clients VPN SSL.

7 Saisissez le texte qui apparaîtra sous la forme d'une 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.



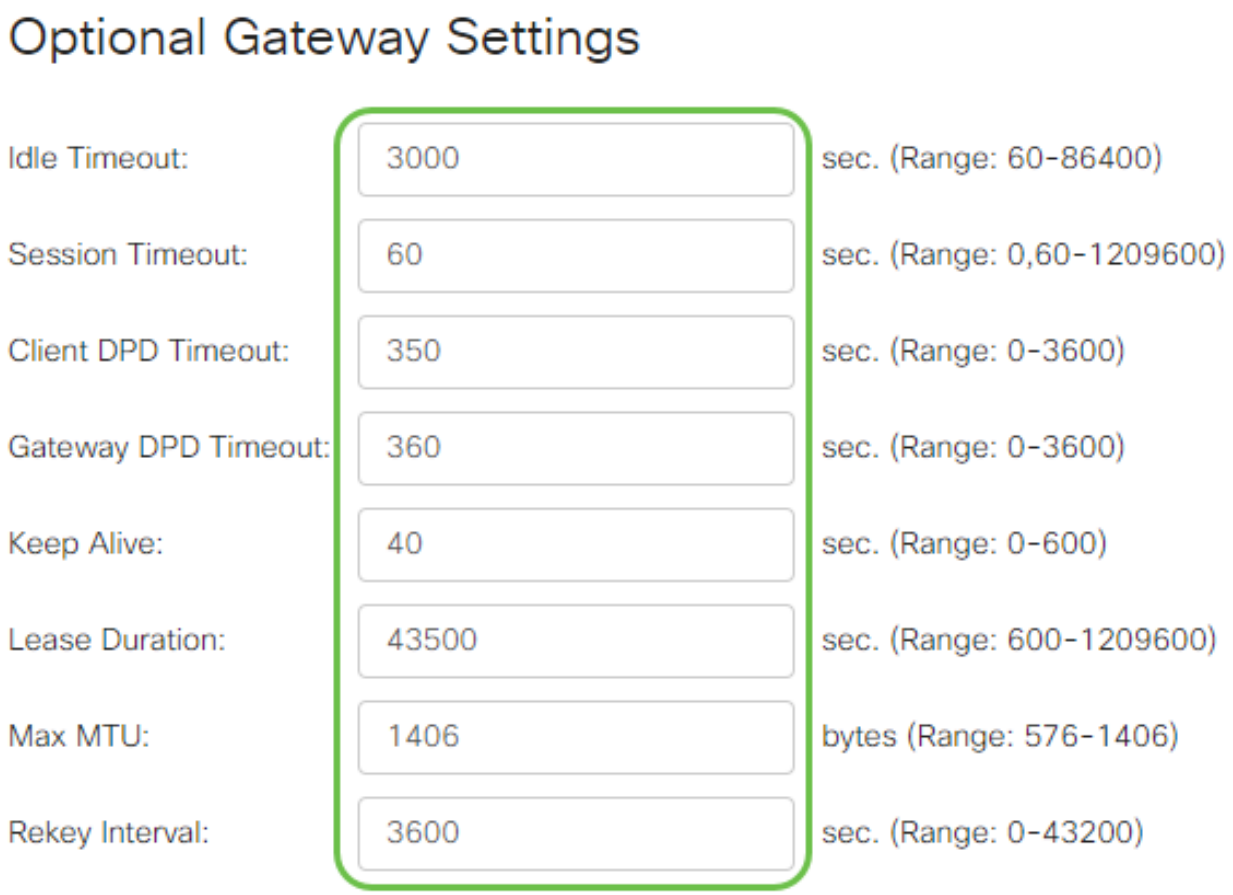
Paramètres de passerelle facultatifs

Étape 1

Les paramètres de configuration suivants sont facultatifs :

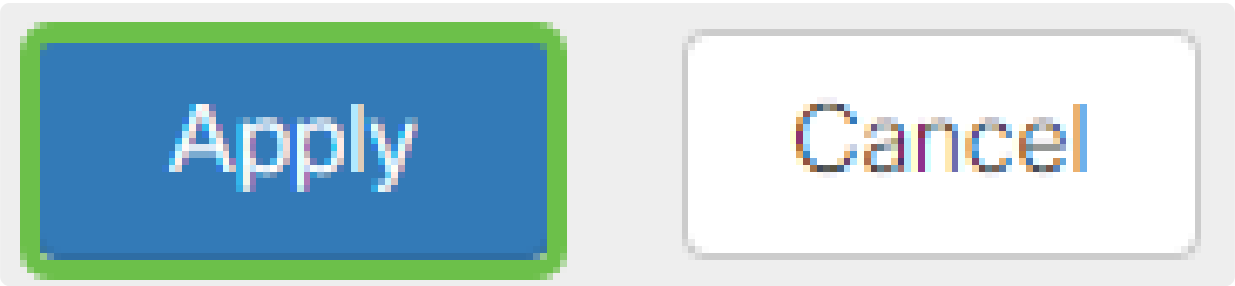
1. Entrez une valeur en secondes pour le délai d'inactivité compris entre 60 et 86400. Il s'agira de la durée pendant laquelle la session VPN SSL peut rester inactive.
2. Entrez une valeur en secondes dans le champ Session Timeout. Il s'agit du temps nécessaire à la session TCP (Transmission Control Protocol) ou UDP (User Datagram Protocol) pour expirer après le temps d'inactivité spécifié. Elle est située entre 60 et 1209600.
3. Entrez une valeur en secondes dans le champ ClientDPD Timeout comprise 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 comprise 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 Lease Duration. Elle est située entre 600 et 1209600.
7. Saisissez la taille de paquet en octets qui peut être envoyée sur le réseau. Elle est située entre 576 et 1406.

8 Saisissez la durée de l'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

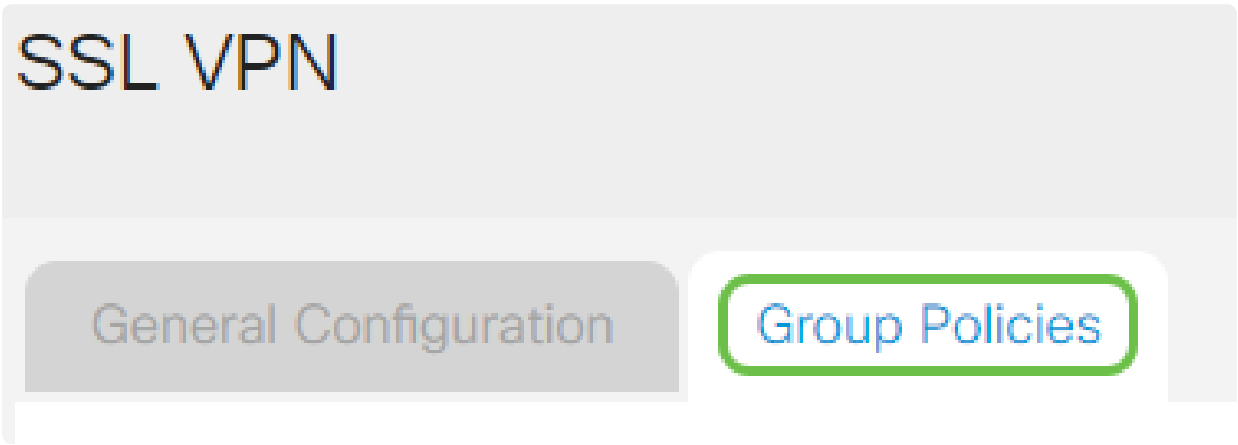
Cliquez sur Apply.



Configurer les stratégies de groupe

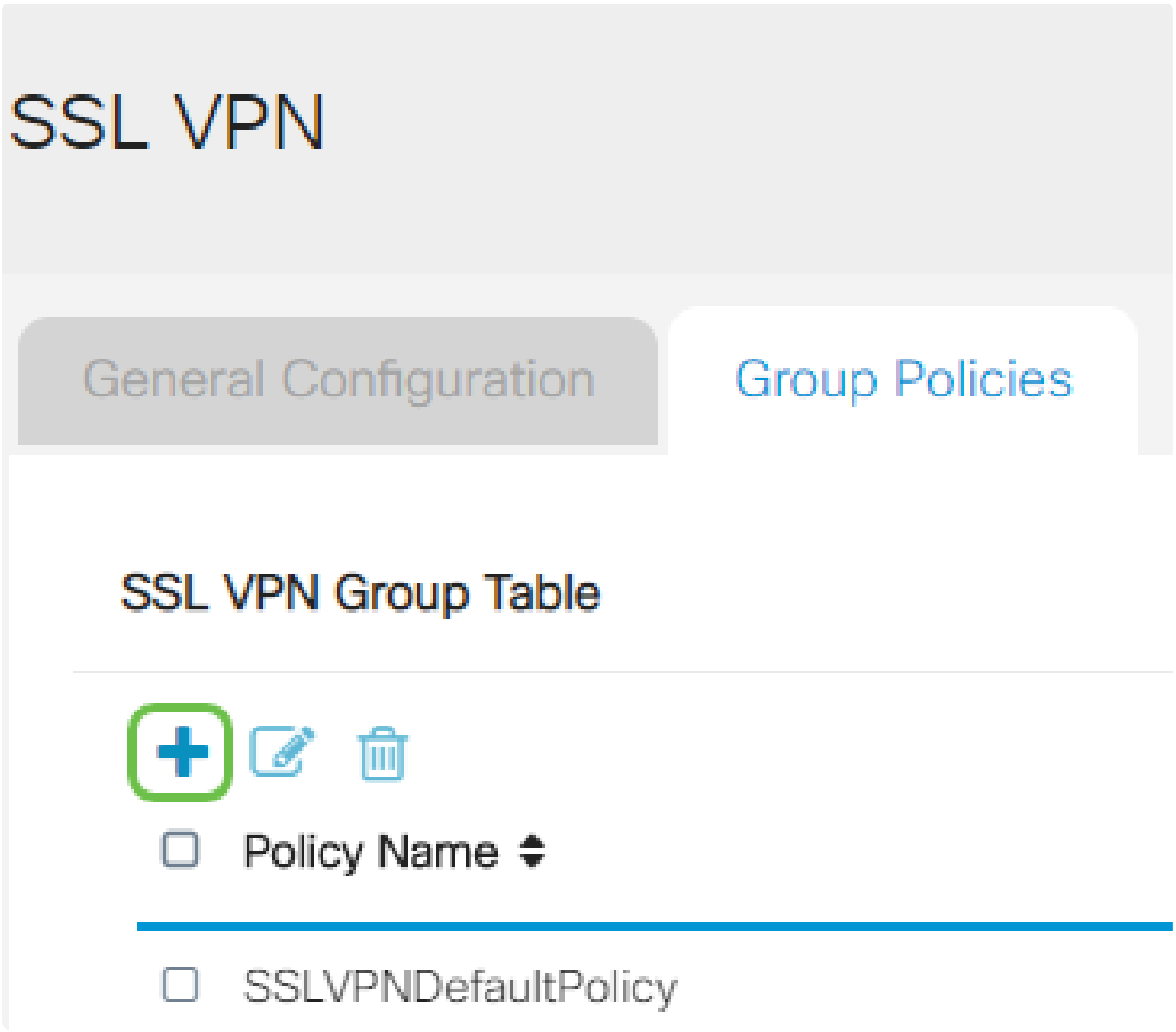
Étape 1

Cliquez sur l'onglet Stratégies de groupe.



Étape 2

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



ⓘ Note: La table 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 Saisissez votre nom de stratégie préféré dans le champ Nom de la stratégie.

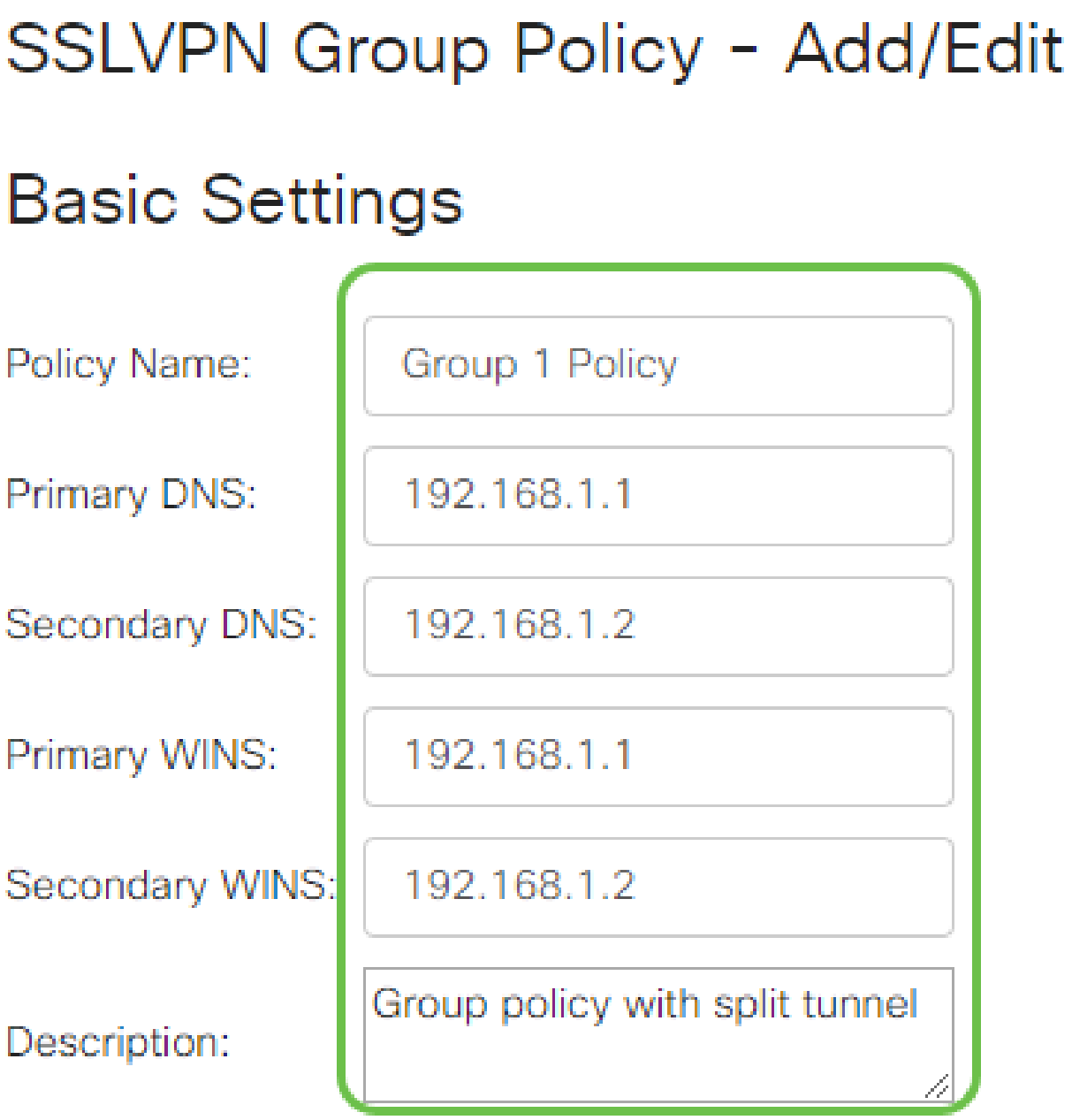
2 Saisissez l'adresse IP du DNS principal dans le champ prévu à cet effet. Par défaut, cette adresse IP est déjà fournie.

3 (Facultatif) Saisissez l'adresse IP du DNS secondaire dans le champ prévu à cet effet. Cela servira de sauvegarde en cas d'échec du DNS principal.

4 (Facultatif) Entrez l'adresse IP du WINS principal dans le champ prévu à cet effet.

5 (Facultatif) Entrez l'adresse IP du WINS secondaire dans le champ prévu à cet effet.

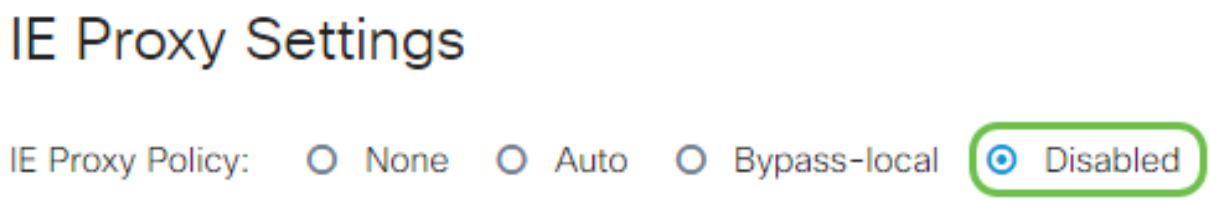
6 (Facultatif) Saisissez une description de la stratégie dans le champ Description.



Étape 4 (facultative)

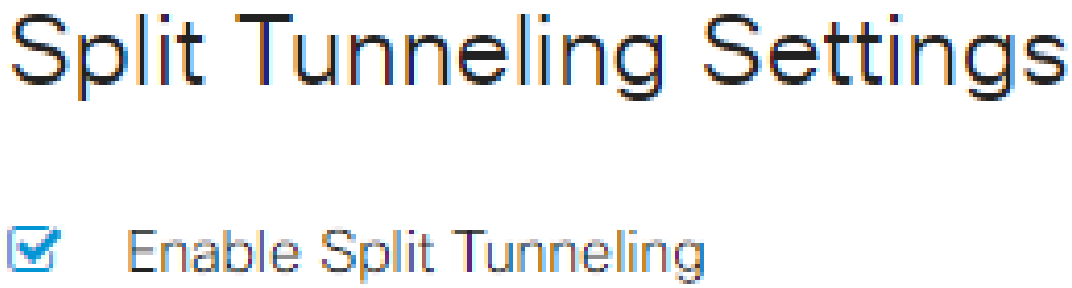
Cliquez sur une case d'option pour sélectionner la stratégie de proxy IE afin d'activer les paramètres de proxy Microsoft Internet Explorer (MSIE) pour établir un tunnel VPN. Les options sont les suivantes :

- 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.
- Disabled : 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 Internet destiné d'être envoyé directement à Internet sans être chiffré. La transmission tunnel complète envoie tout le trafic au 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 transmission tunnel partagée.



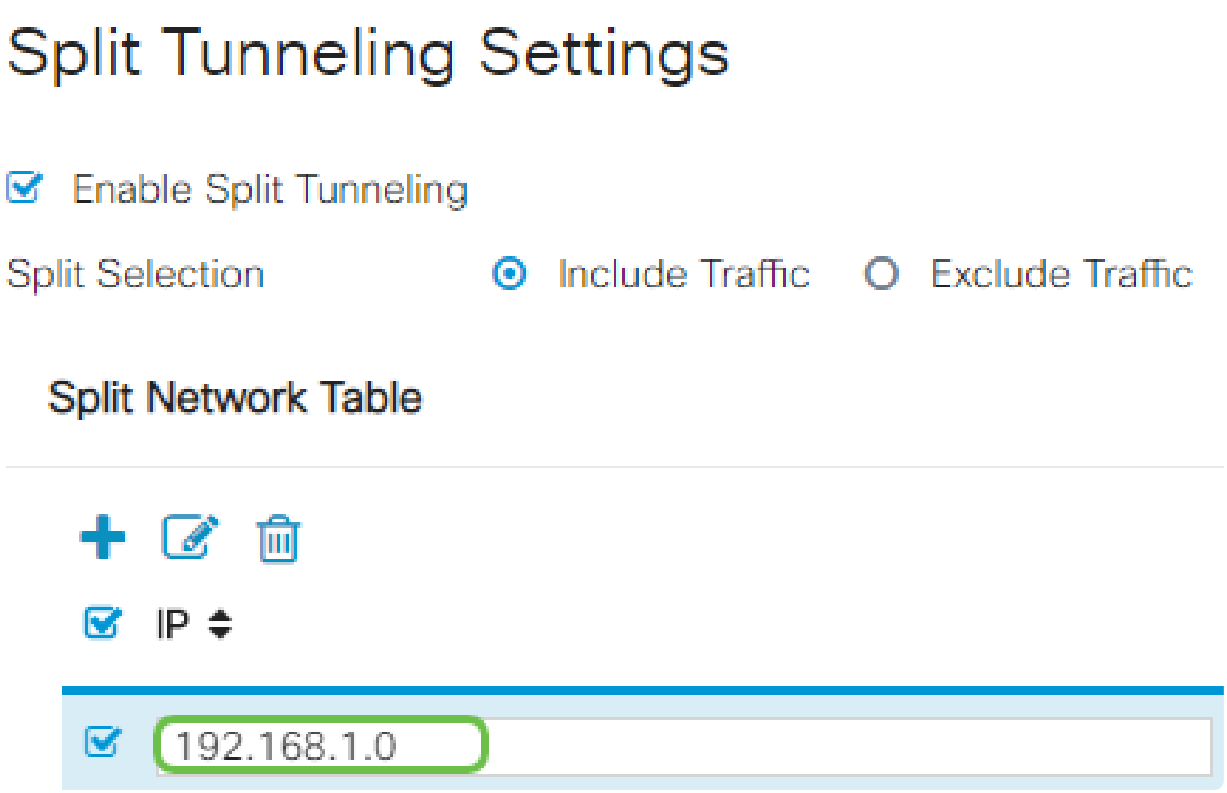
Étape 7

Dans le tableau Réseau partagé, cliquez sur l'icône Ajouter pour ajouter une exception Réseau partagé.



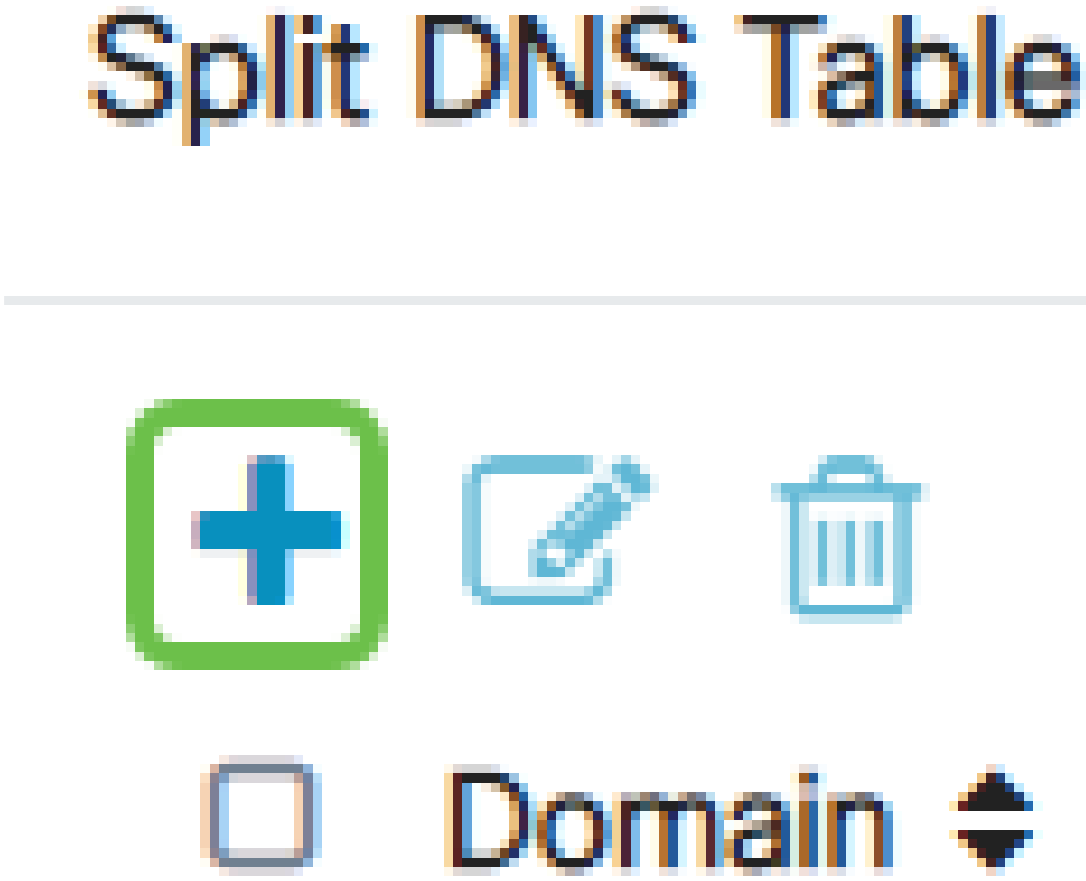
Étape 8

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



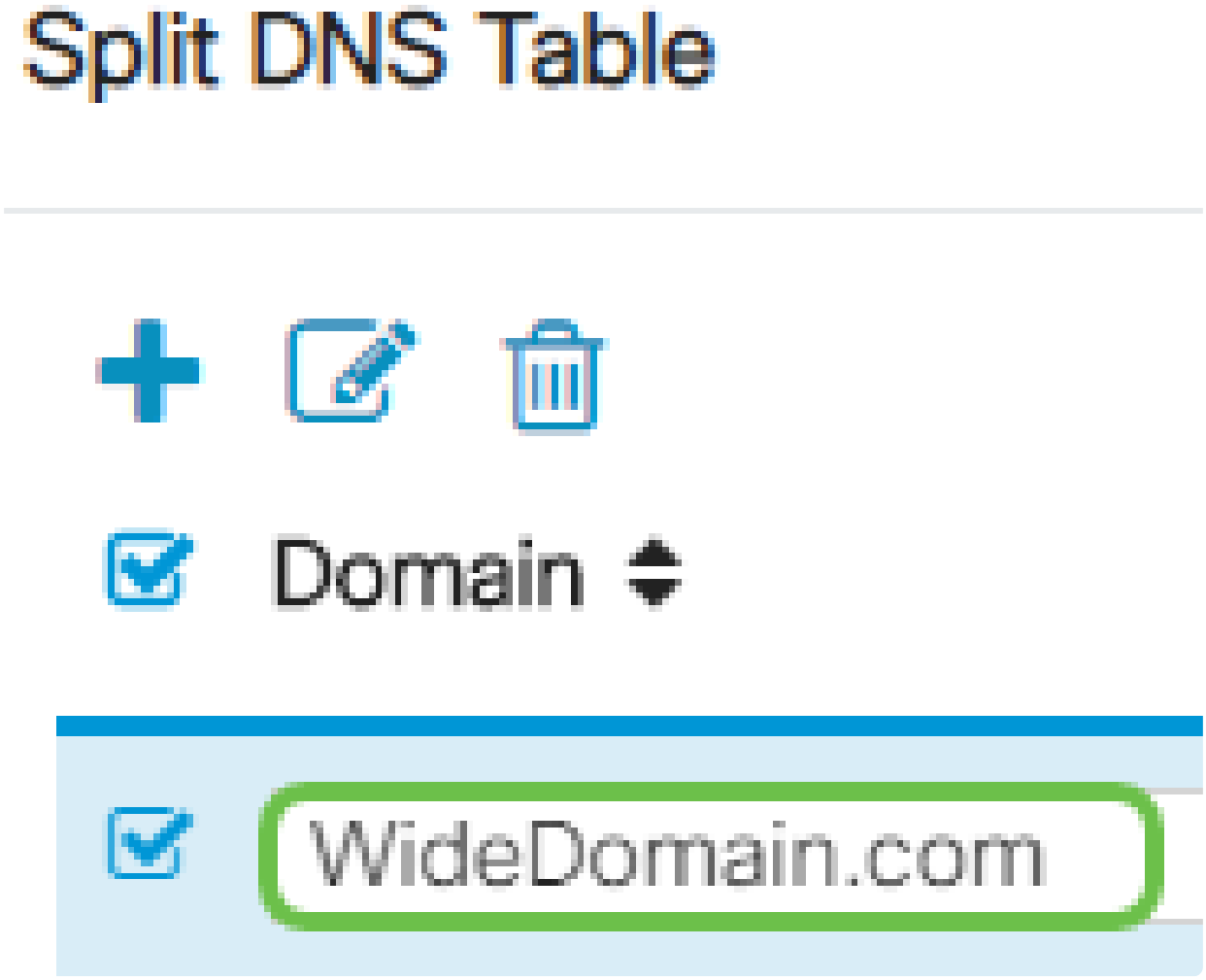
Étape 9

Dans le tableau Split DNS, cliquez sur l'icône Add pour ajouter une exception Split DNS.



Étape 10

Saisissez le nom de domaine dans le champ prévu à cet effet, puis cliquez sur Apply.



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

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

Cette section suivante 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, par exemple 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 fonctionnant sur divers 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 de votre pool de licences disponible que vous achetez, qui est détaillé dans la section suivante.

Achat de licence

Vous devez acheter une licence auprès de votre distributeur Cisco ou de votre partenaire Cisco. Lorsque vous commandez 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 de ce document, les références produit suivantes peuvent être utilisées pour acheter des licences supplémentaires par lots de 25. Notez qu'il existe d'autres options pour les licences client AnyConnect, comme indiqué dans le Guide de commande Cisco AnyConnect. Toutefois, l'ID de produit indiqué est la condition minimale requise pour bénéficier de toutes les fonctionnalités.

Veuillez noter que la référence produit de licence client AnyConnect indiquée en premier, fournit des licences pour une durée d'1 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 1 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 — Pack de 25 licences client perpétuelles Cisco AnyConnect Plus
- LS-AC-PLS-P-50-S — Pack de 50 licences client perpétuelles Cisco AnyConnect Plus

Informations client

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

- Fenêtres: AnyConnect sur un ordinateur Windows
- Mac : installez AnyConnect sur Mac.
- Bureau Ubuntu : Installer et utiliser AnyConnect sur un poste de travail Ubuntu
- Si vous rencontrez des problèmes, vous pouvez accéder à Collecter des 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.

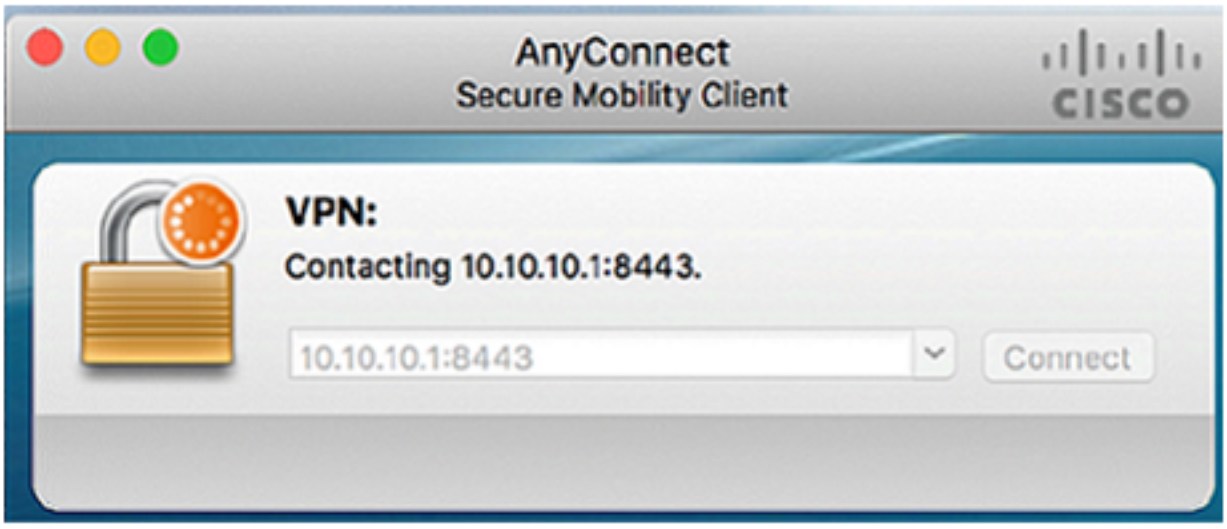


Étape 2

Dans la fenêtre AnyConnect Secure Mobility Client, entrez l'adresse IP de la passerelle et le numéro de port de la passerelle séparés par deux points (:), puis cliquez sur Connect.

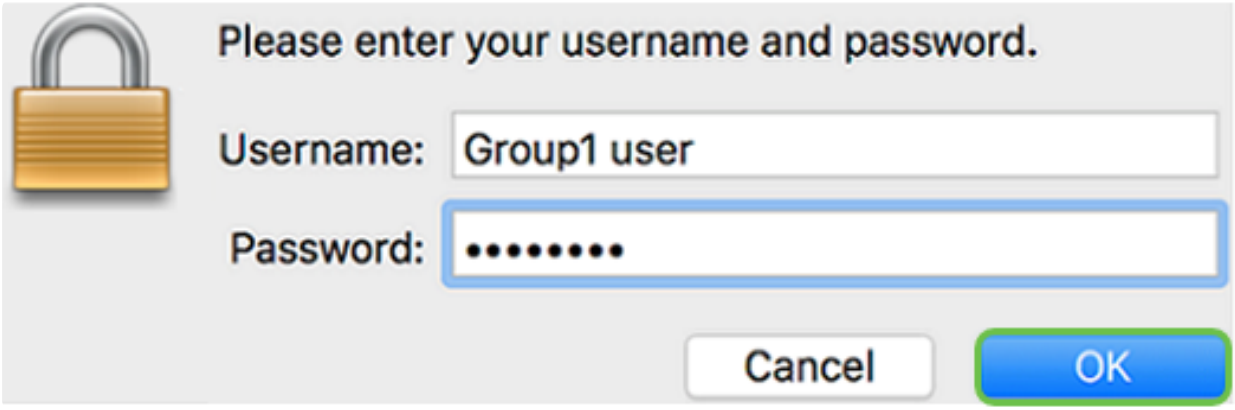


Le logiciel indique maintenant qu'il contacte le réseau distant.



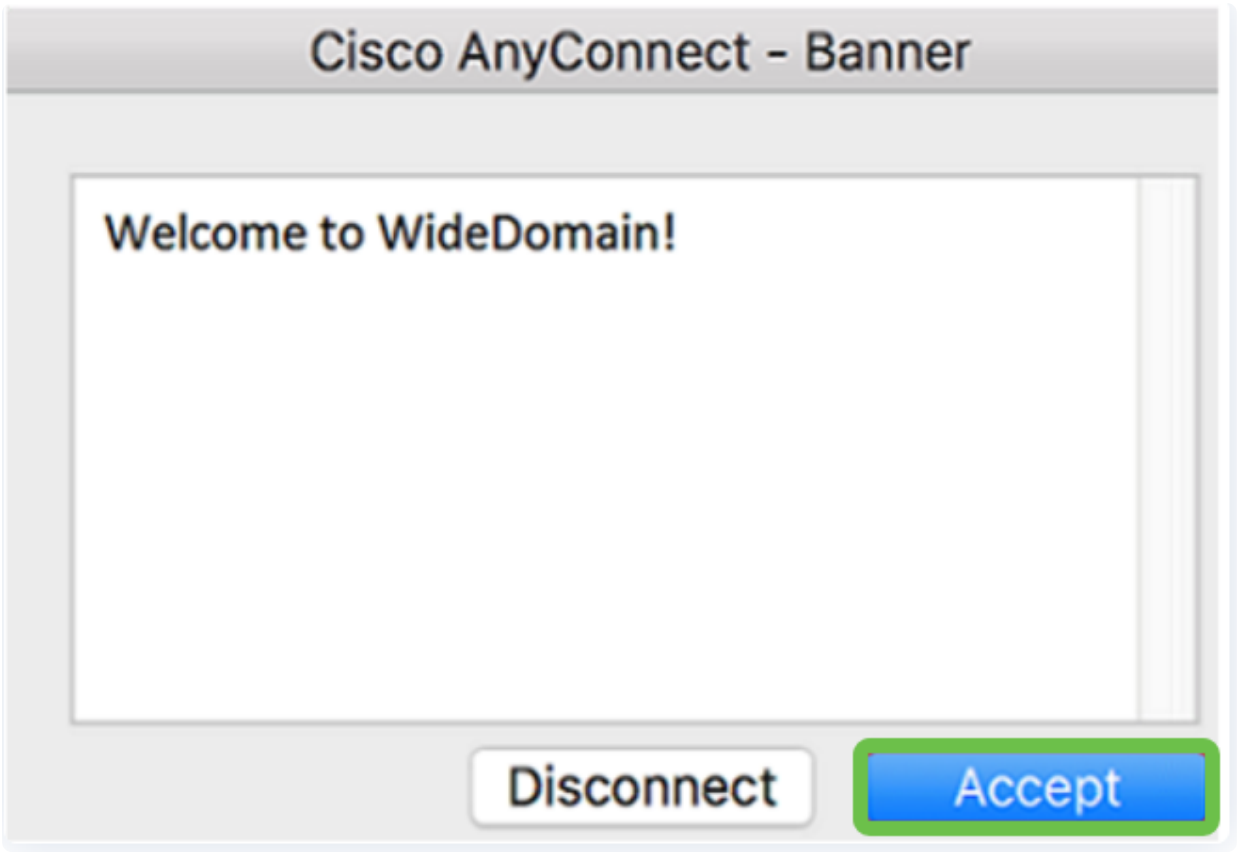
Étape 3

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

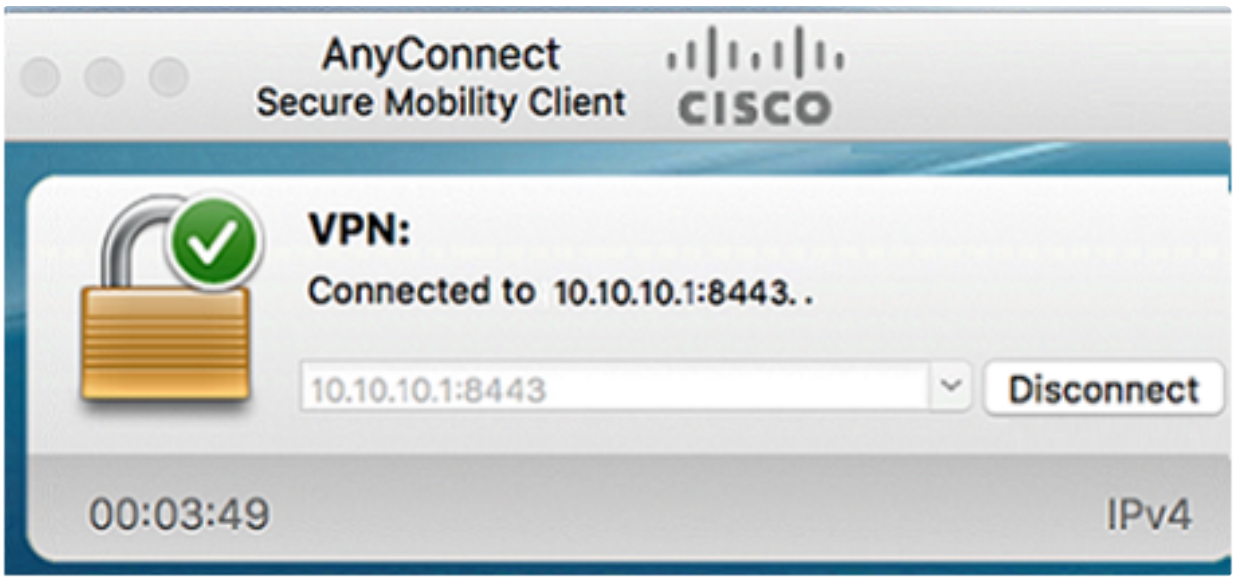


Étape 4

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



La fenêtre AnyConnect doit maintenant indiquer que la connexion VPN au réseau a réussi.



Si vous utilisez maintenant AnyConnect VPN, vous pouvez passer au-delà des autres options VPN et passer à la section suivante.

Shrew Soft VPN

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 vous explique comment configurer votre routeur et le client logiciel Shrew pour sécuriser une connexion à un VPN.

> ⓘ Note: Cisco ne prend pas en charge Shrew Soft. Cet exemple est fourni à des fins de démonstration uniquement. Si vous rencontrez des problèmes avec Shrew Soft, contactez-le pour obtenir de l'aide.

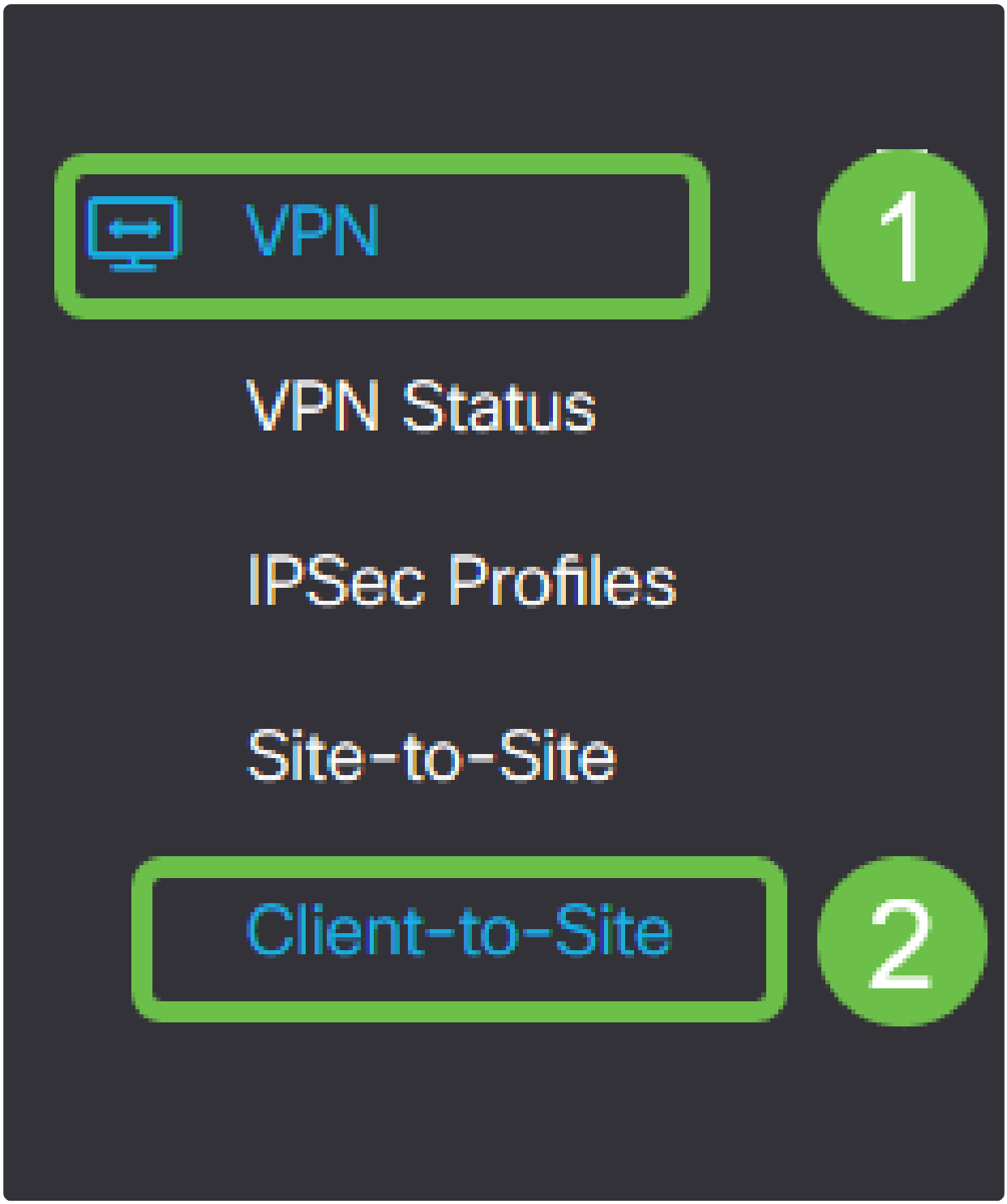
Vous pouvez télécharger la dernière version du logiciel client Shrew Soft VPN ici : https://www.shrew.net/download/vpn

Configuration de Shrew Soft sur le routeur de la gamme RV345P

Nous allons commencer par configurer le VPN client-à-site sur le RV345P.

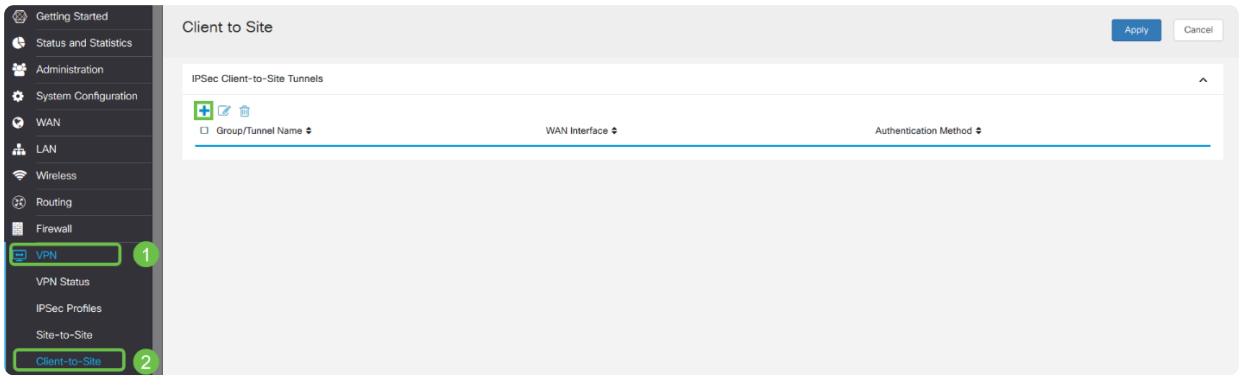
Étape 1

Accédez à VPN > Client-to-Site.



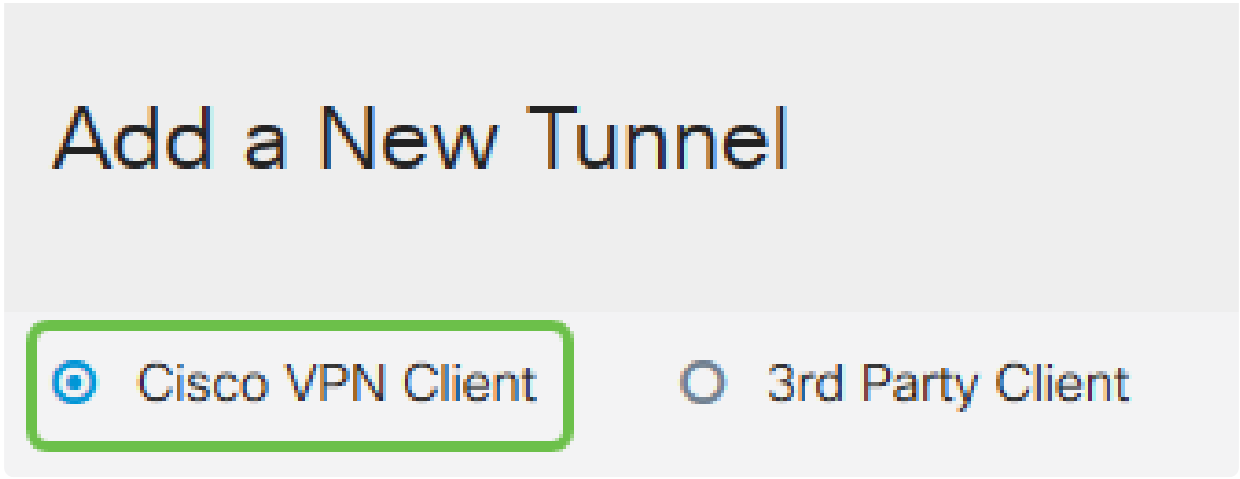
Étape 2

Ajoutez un profil VPN client-à-site.



Étape 3

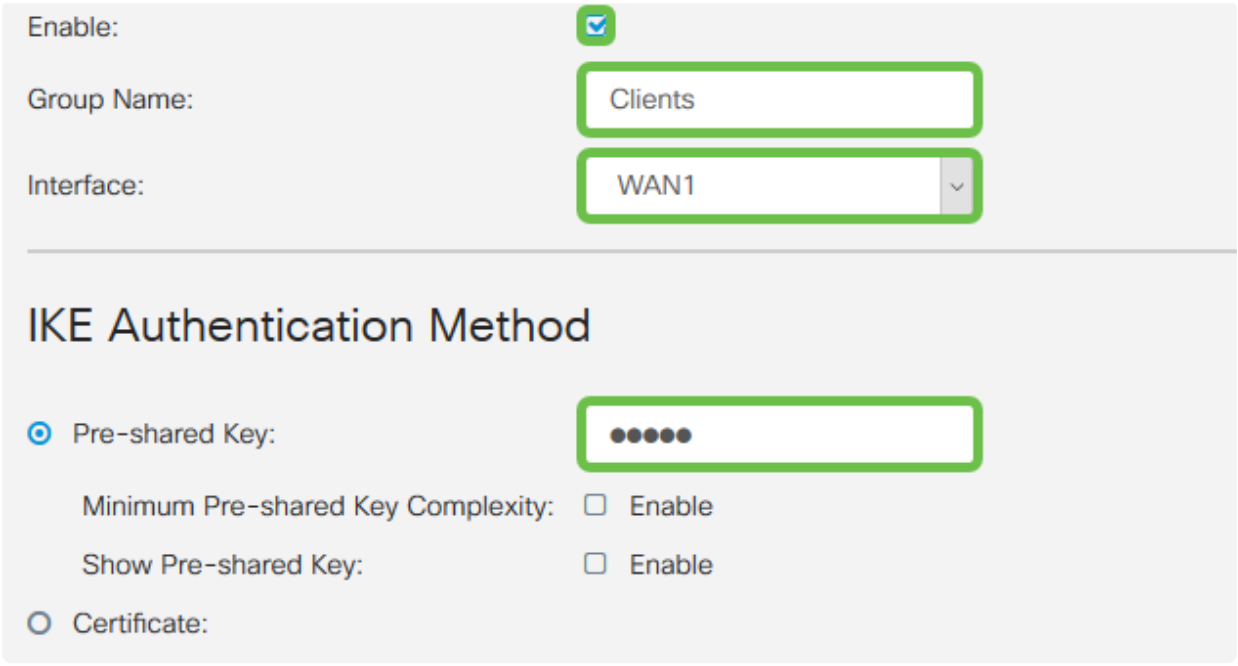
Sélectionnez l'option Client VPN Cisco.



Étape 4

Cochez la case Enable pour activer le profil de client VPN. Nous allons également configurer le nom du groupe, sélectionner l'interface WAN et entrer une clé pré-partagée.

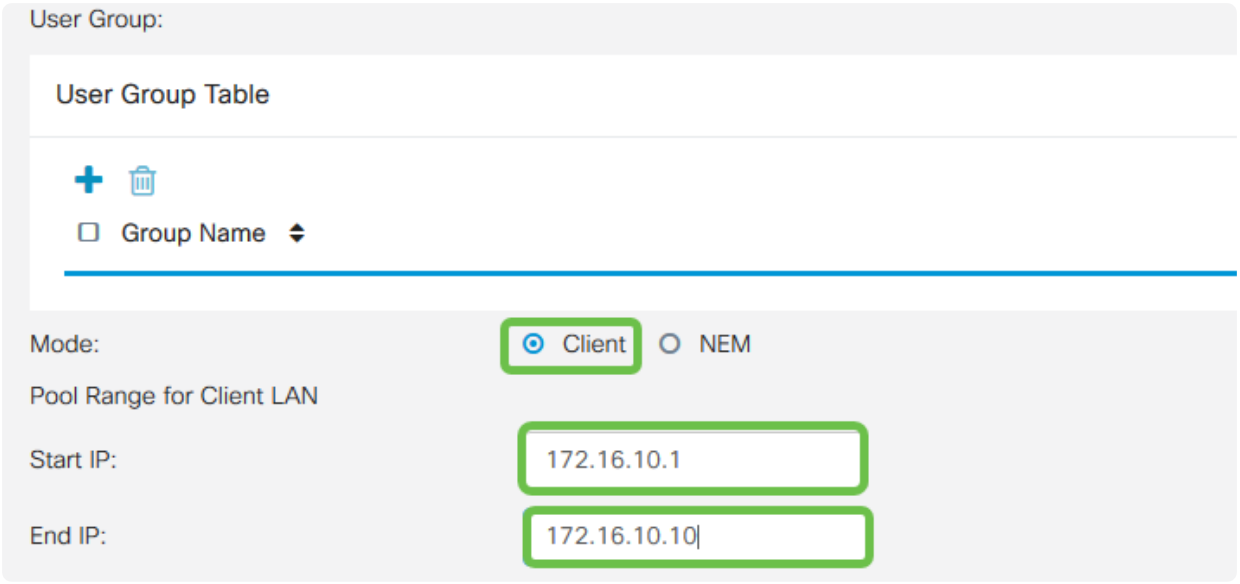
ⓘ Note: Notez le nom du groupe et la clé prépartagée car ils seront utilisés ultérieurement lors de la configuration du client.



Étape 5

Pour l'instant, laissez la table des groupes d'utilisateurs vide. Ceci est pour le groupe d'utilisateurs sur le routeur, mais nous ne l'avons pas encore configuré. Assurez-vous que le mode est défini sur Client. Saisissez la plage de pool pour le réseau local du client. Nous utiliserons les réseaux 172.16.10.1 à 172.16.10.10.

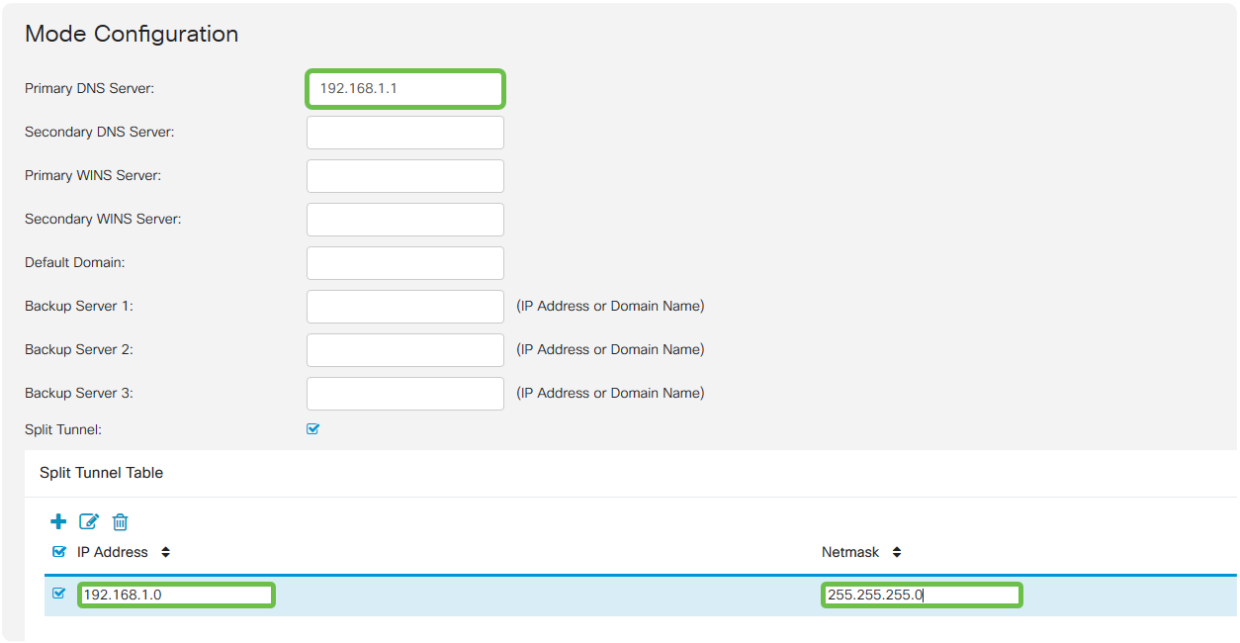
ⓘ Note: La plage du pool doit utiliser un sous-réseau unique qui n'est pas utilisé ailleurs sur le réseau.



Étape 6

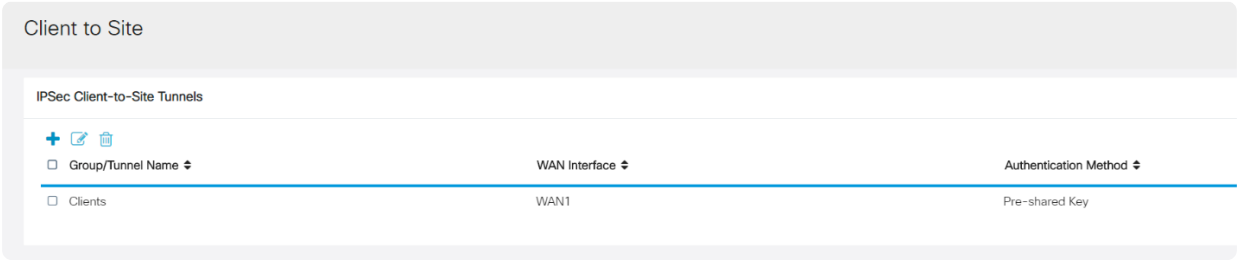
C'est ici que nous configurons les paramètres de configuration du mode. Voici les paramètres que nous allons utiliser :

- Serveur DNS principal : Si vous disposez d'un serveur DNS interne ou si vous souhaitez utiliser un serveur DNS externe, vous pouvez l'entrer ici. Sinon, l'adresse IP du réseau local RV345P est définie par défaut. Nous utiliserons la valeur par défaut dans notre exemple.
- Split Tunnel : cochez cette case pour activer la transmission tunnel partagée. Elle est utilisée pour spécifier le trafic qui passera sur le tunnel VPN. Nous allons utiliser le tunnel partagé dans notre exemple.
- Split Tunnel Table : saisissez les réseaux auxquels le client VPN doit avoir accès via le VPN. Cet exemple utilise le réseau local RV345P.



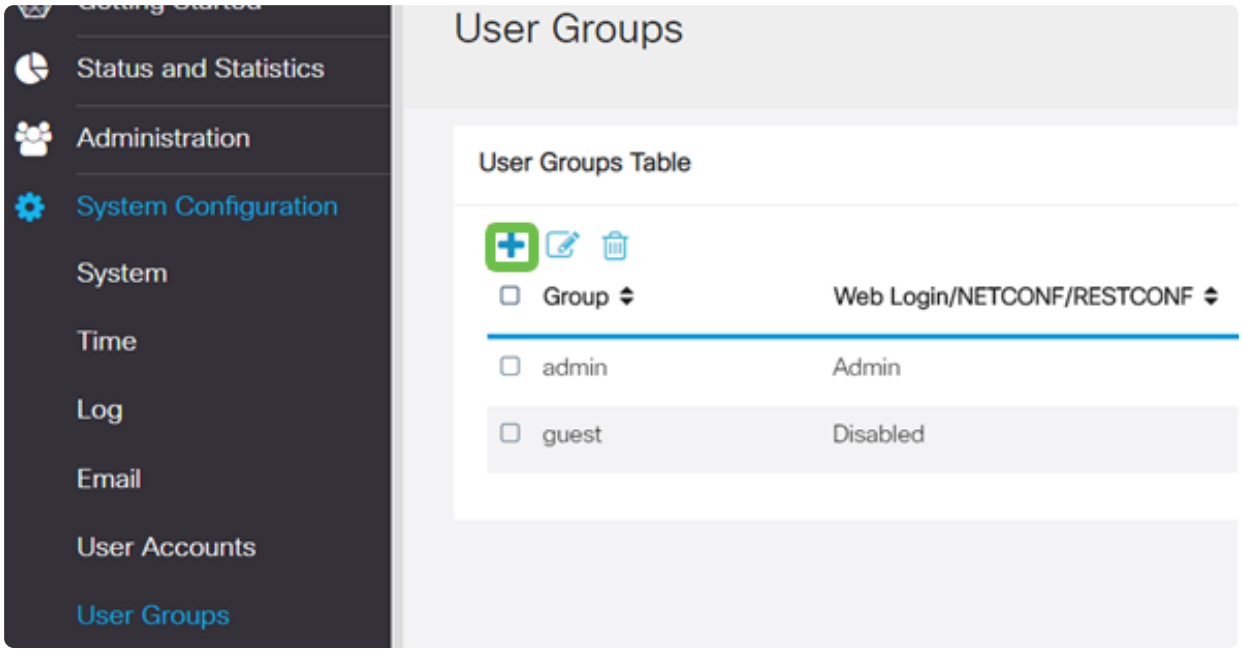
Étape 7

Après avoir cliqué sur Save, nous pouvons voir le profil dans la liste IPsec Client-to-Site Groups.



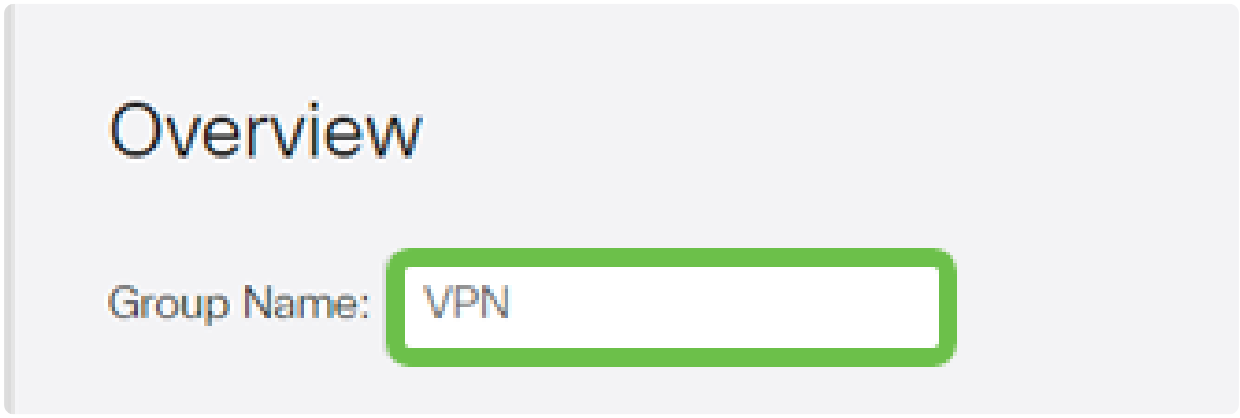
Étape 8

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



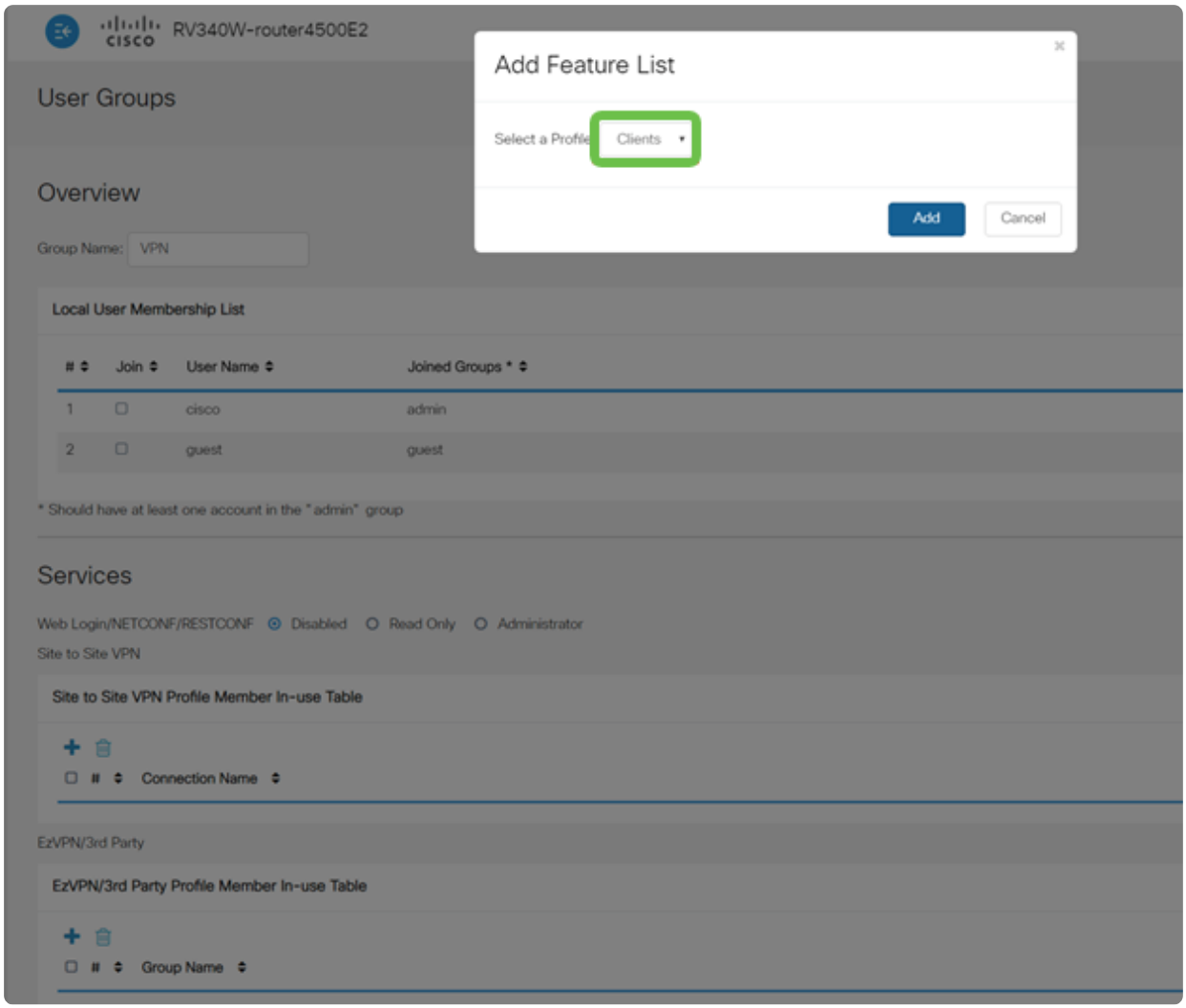
Étape 9

Saisissez un nom de groupe.



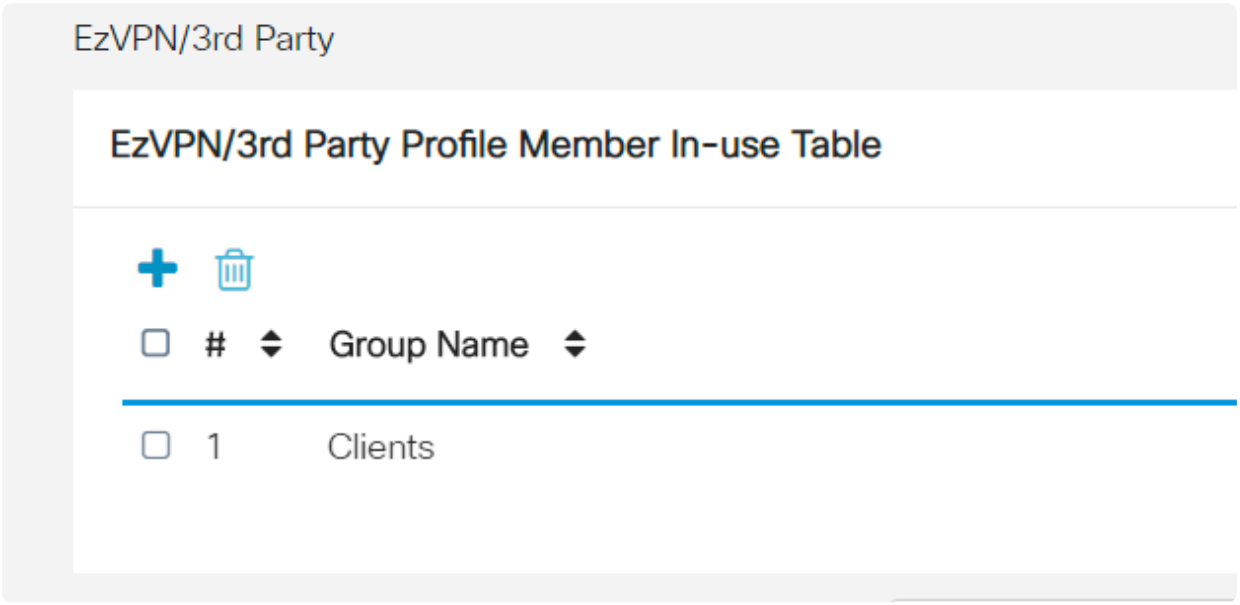
Étape 10

Sous Services > EzVPN/3rd Party, cliquez sur Add pour lier ce groupe d'utilisateurs au profil client-à-site configuré précédemment.



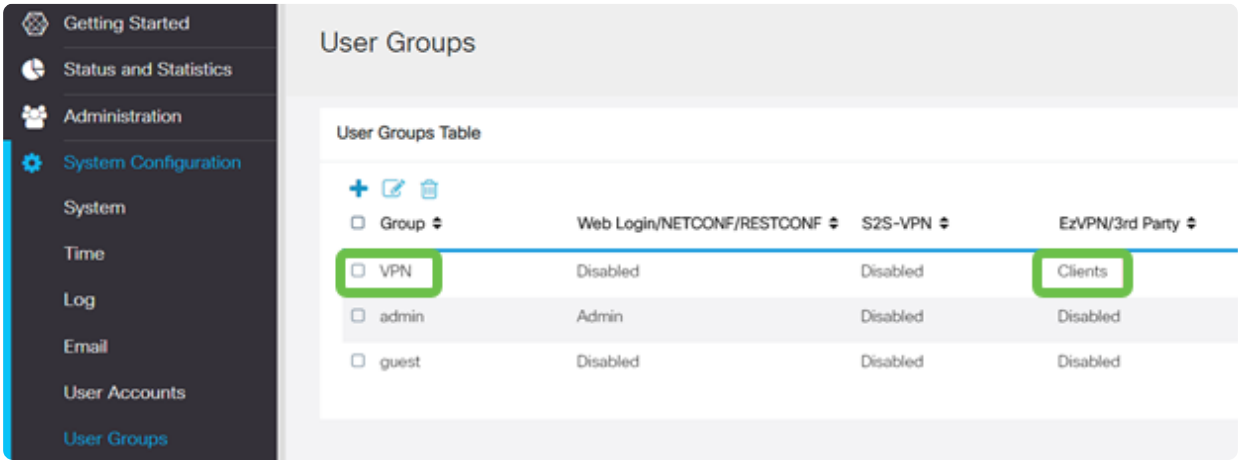
Étape 11

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



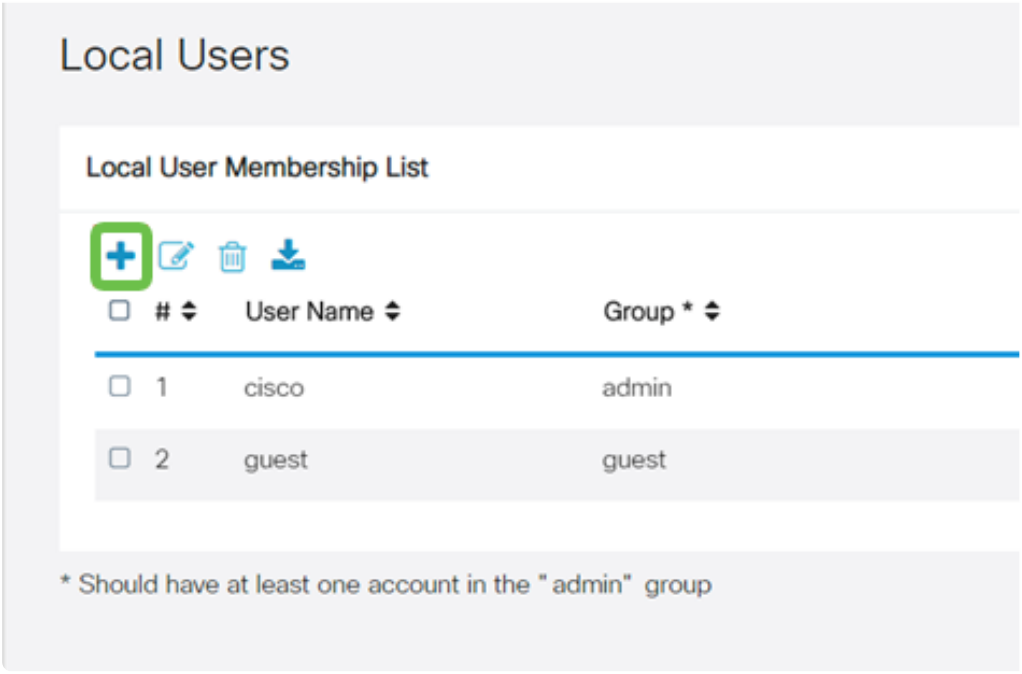
Étape 12

Une fois que vous avez appliqué la configuration de groupe d'utilisateurs, vous la verrez dans la liste Groupes d'utilisateurs et elle montrera le nouveau groupe d'utilisateurs sera utilisé avec le profil client-à-site que vous avez créé précédemment.



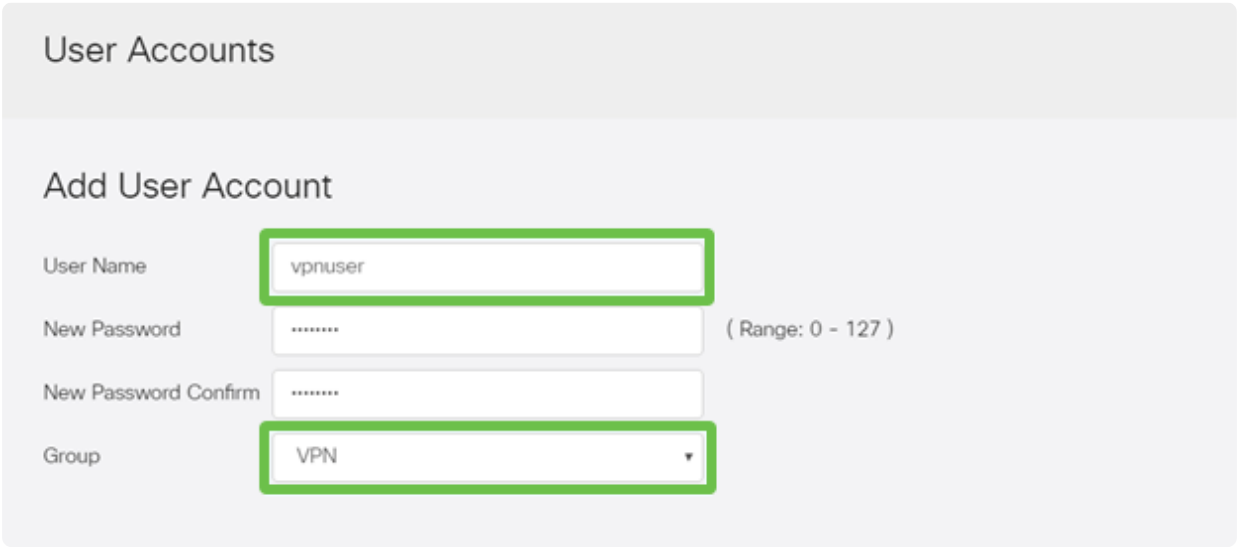
Étape 13

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



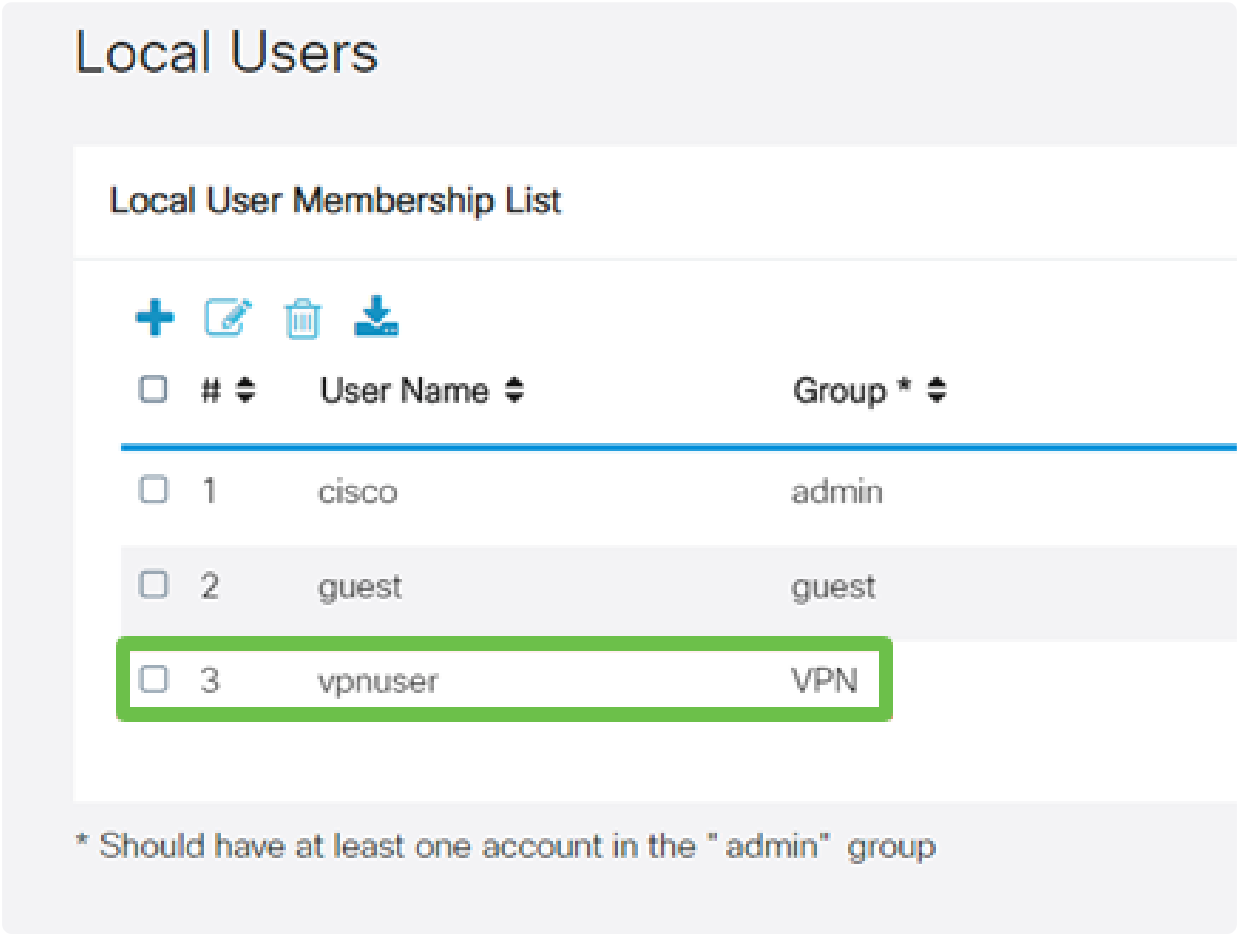
Étape 14

Saisissez le nouveau nom d'utilisateur avec 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 ainsi terminée. Ensuite, vous allez configurer le client VPN logiciel Shrew.

Configuration du client VPN logiciel Shrew

Procédez comme suit.

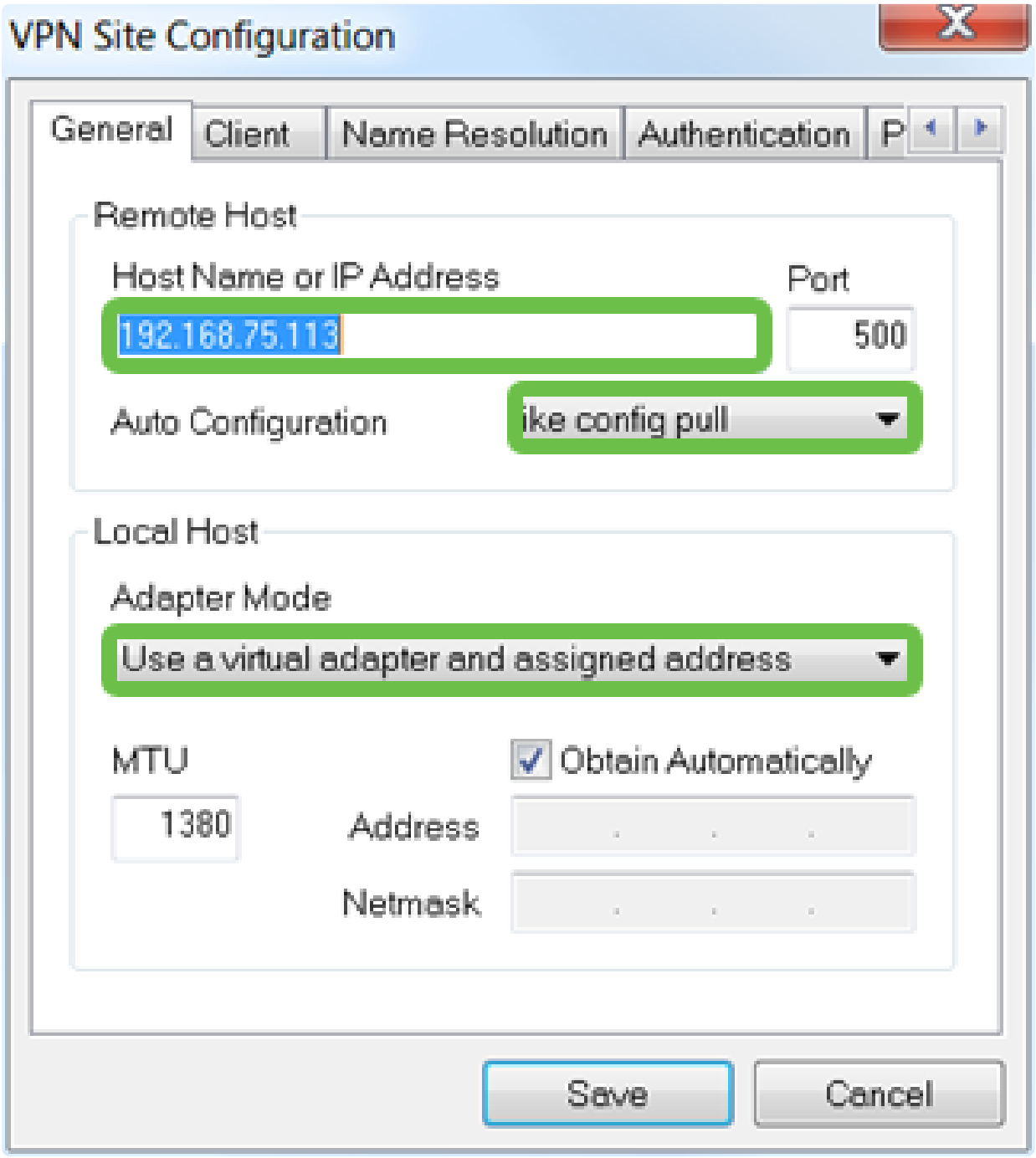
Étape 1

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

- Nom d'hôte ou adresse IP : Utilisez l'adresse IP WAN (ou le nom d'hôte du routeur

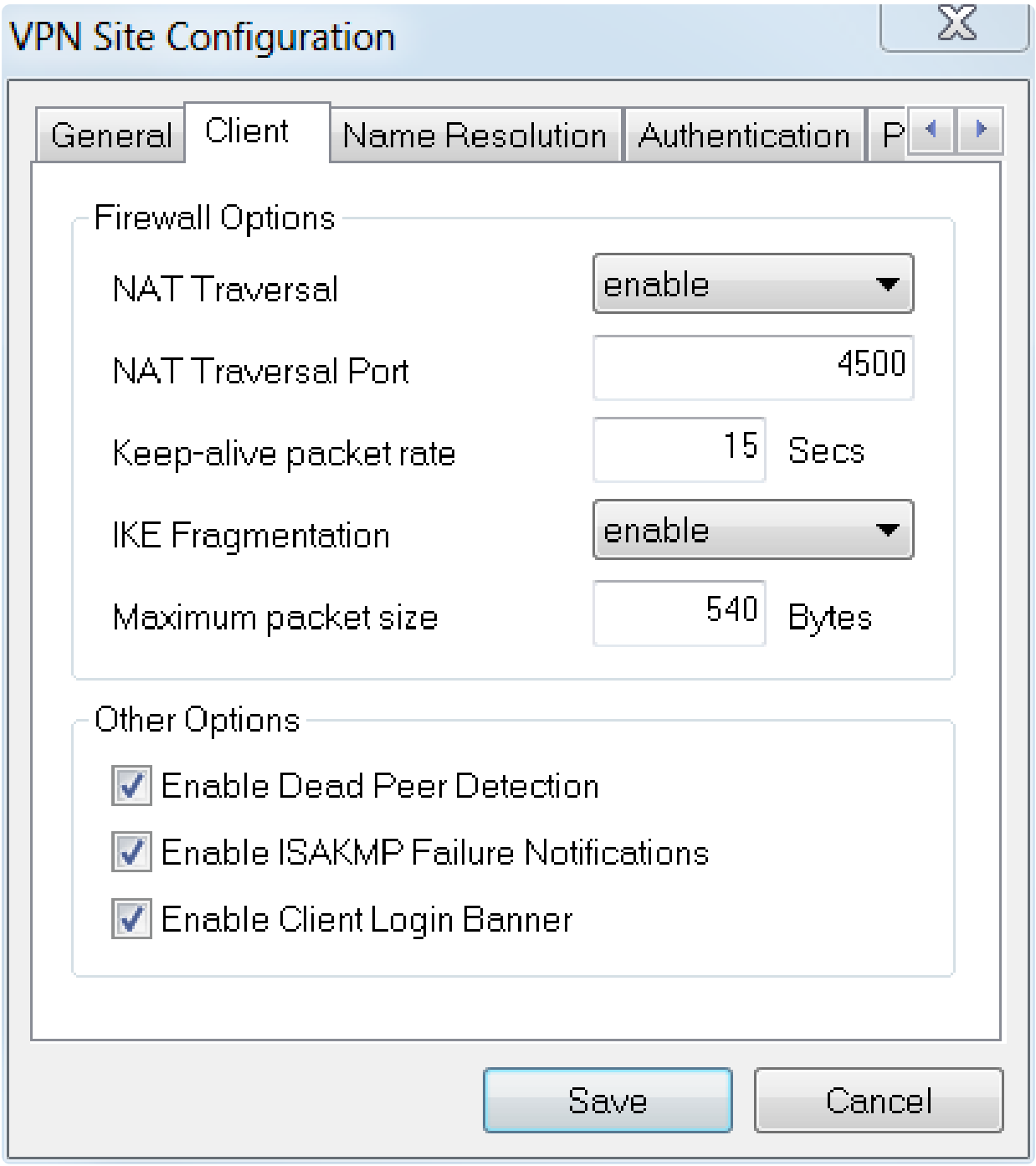
RV345P)

- Configuration automatique : Sélectionnez ike config pull
- Mode adaptateur : Sélectionnez Utiliser une carte virtuelle et l'adresse attribuée



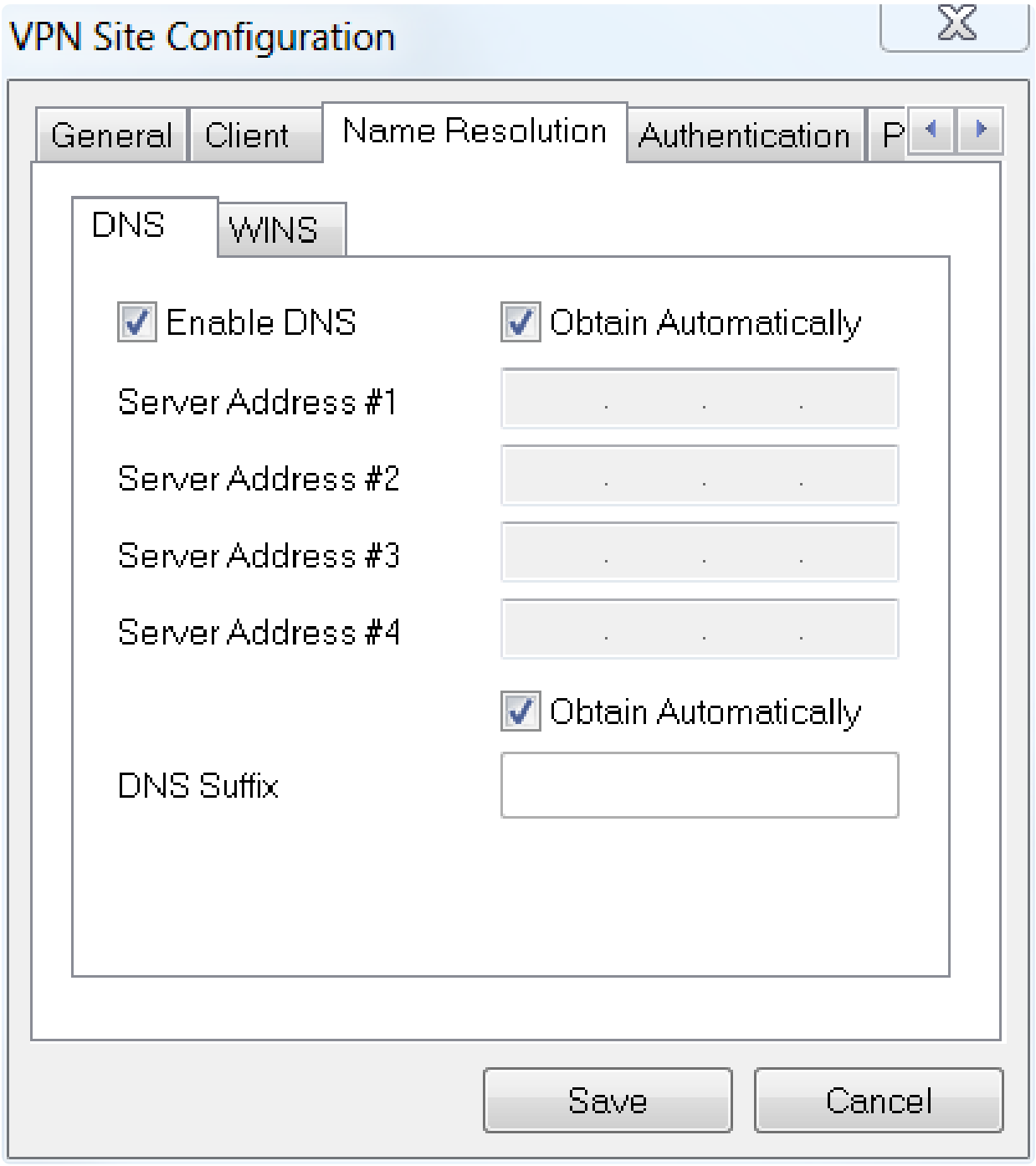
Étape 2

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



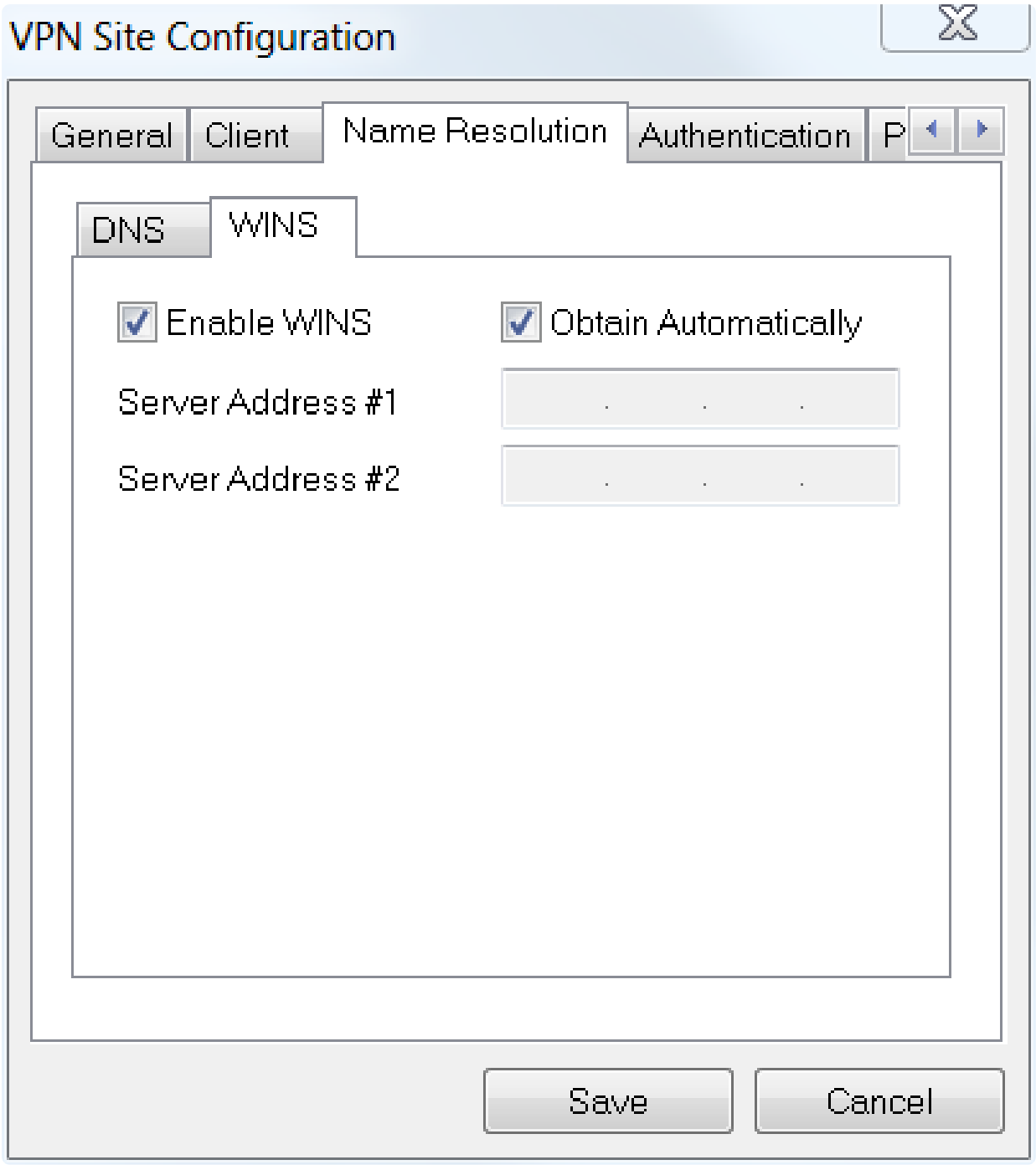
Étape 3

Sous Name Resolution > DNS, cochez la case Enable DNS et laissez les cases Obtain Automatically cochées.



Étape 4

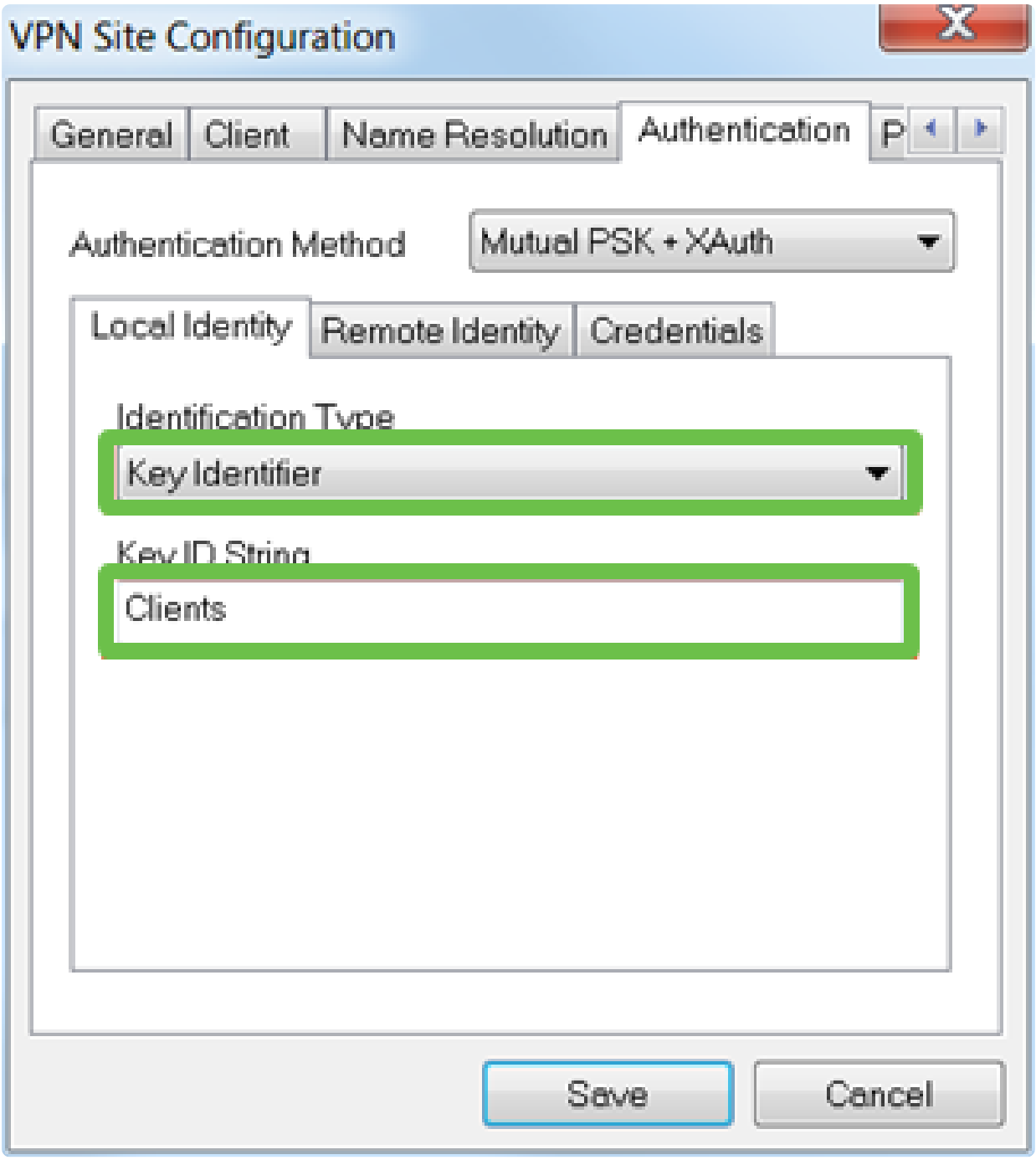
Sous l'onglet Résolution de noms > WINS, cochez la case Activer WINS et laissez la case Obtenir automatiquement cochée.



Étape 5

Cliquez sur Authentication > Local Identity.

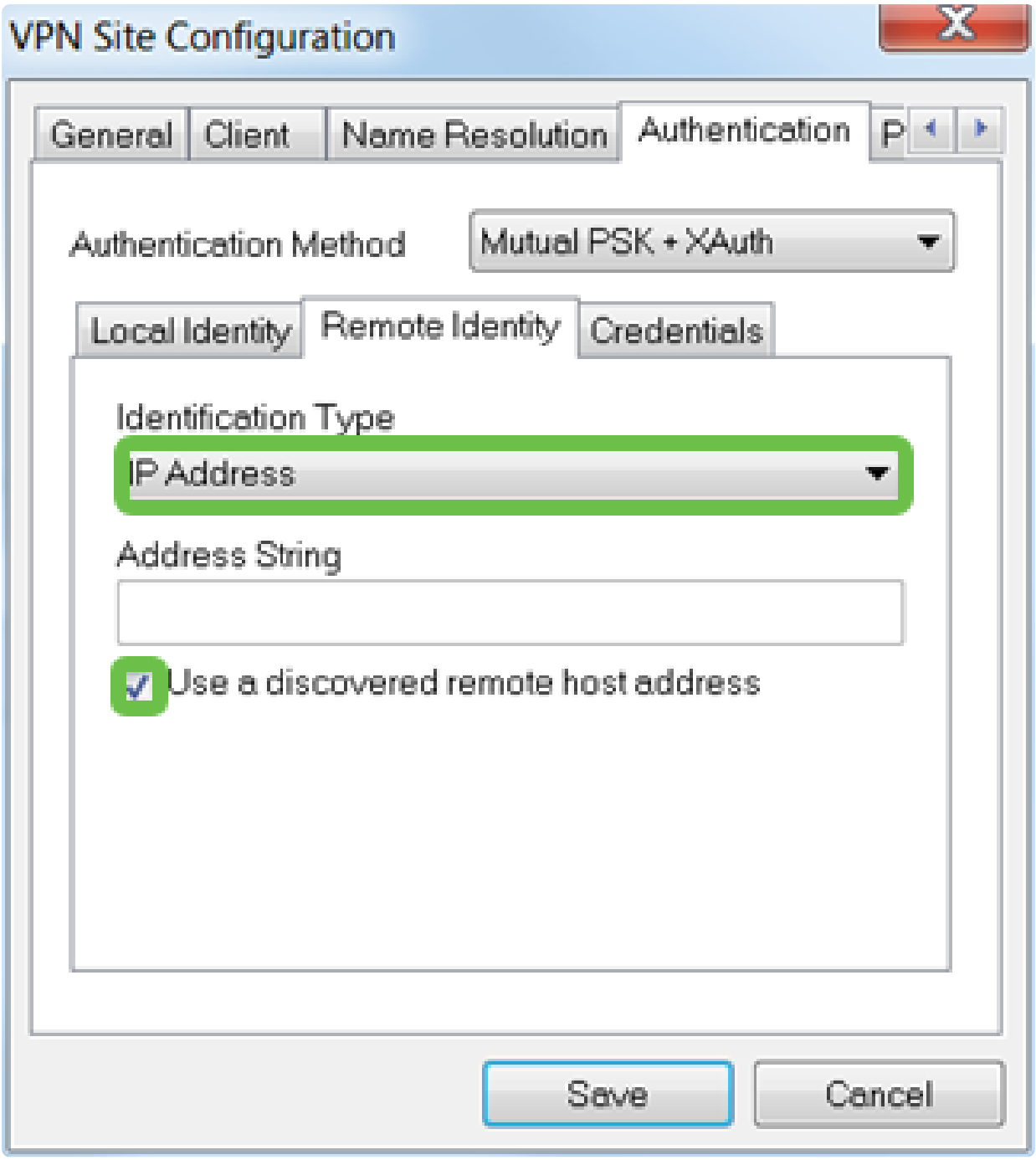
- Type d'identification : Sélectionner un identificateur de clé
- Chaîne d'ID de clé : Entrez le nom du groupe configuré sur le routeur RV345P



Étape 6

Sous Authentication > Remote Identity. Dans cet exemple, nous avons conservé les paramètres par défaut.

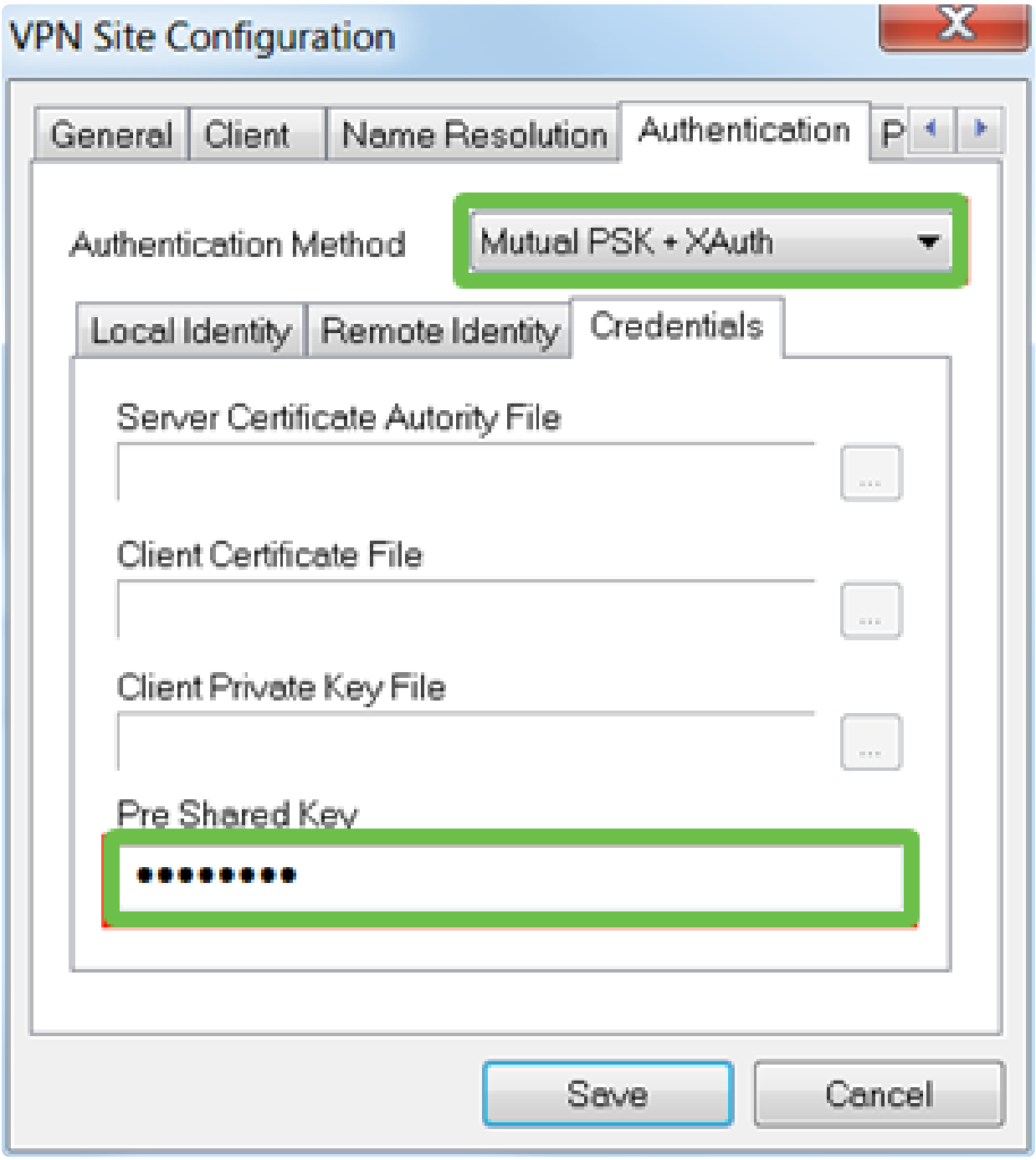
- Type d'identification : Adresse IP
- Chaîne d'adresse : <vide>
- Utilisez une zone d'adresse d'hôte distant découverte : Coché



Étape 7

Sous Authentication > Credentials, configurez les éléments suivants :

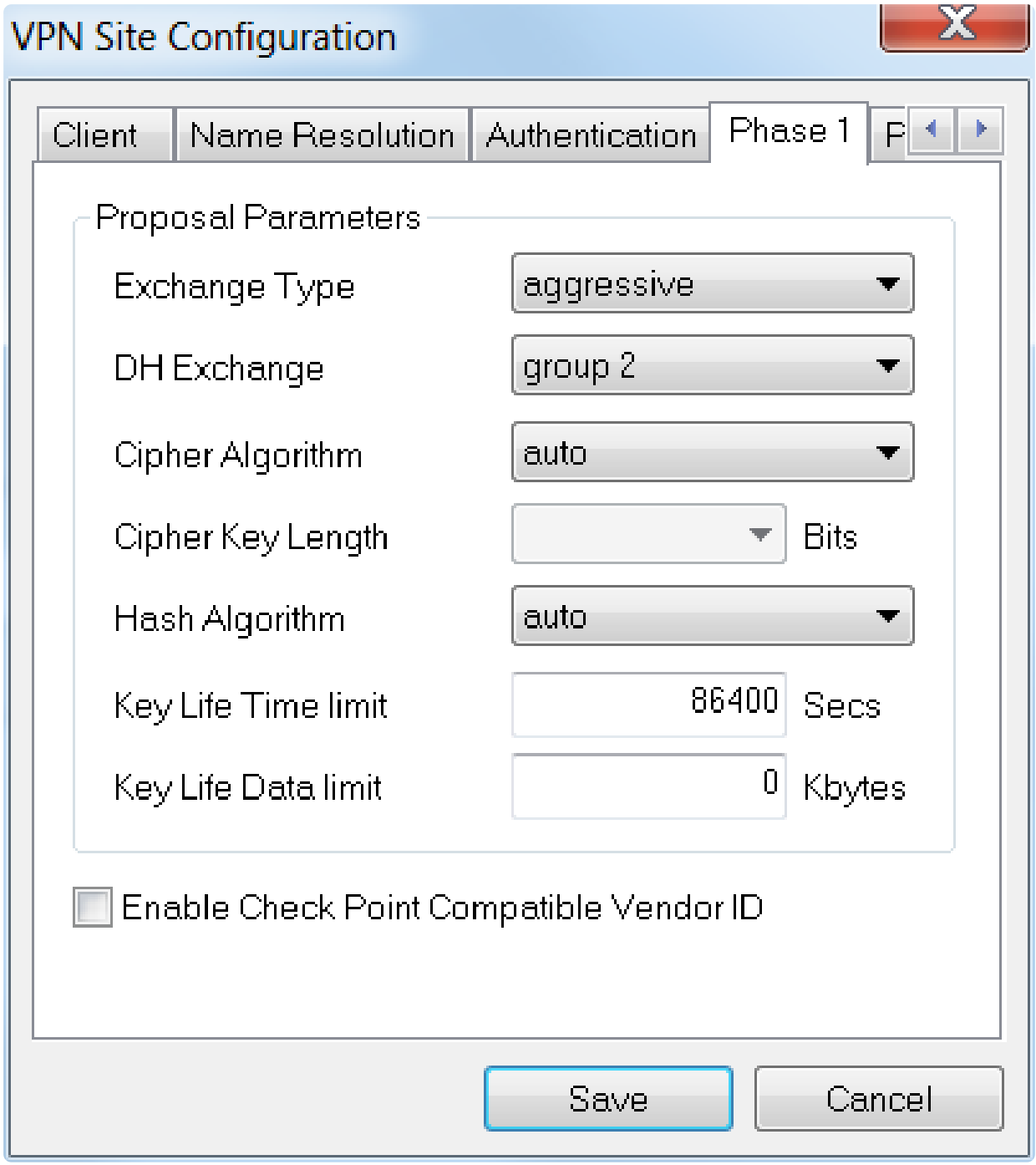
- Méthode d'authentification : Sélectionner PSK mutuel + XAuth
- Clé pré-partagée : Saisissez la clé prépartagée configurée dans le profil client RV345P



Étape 8

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

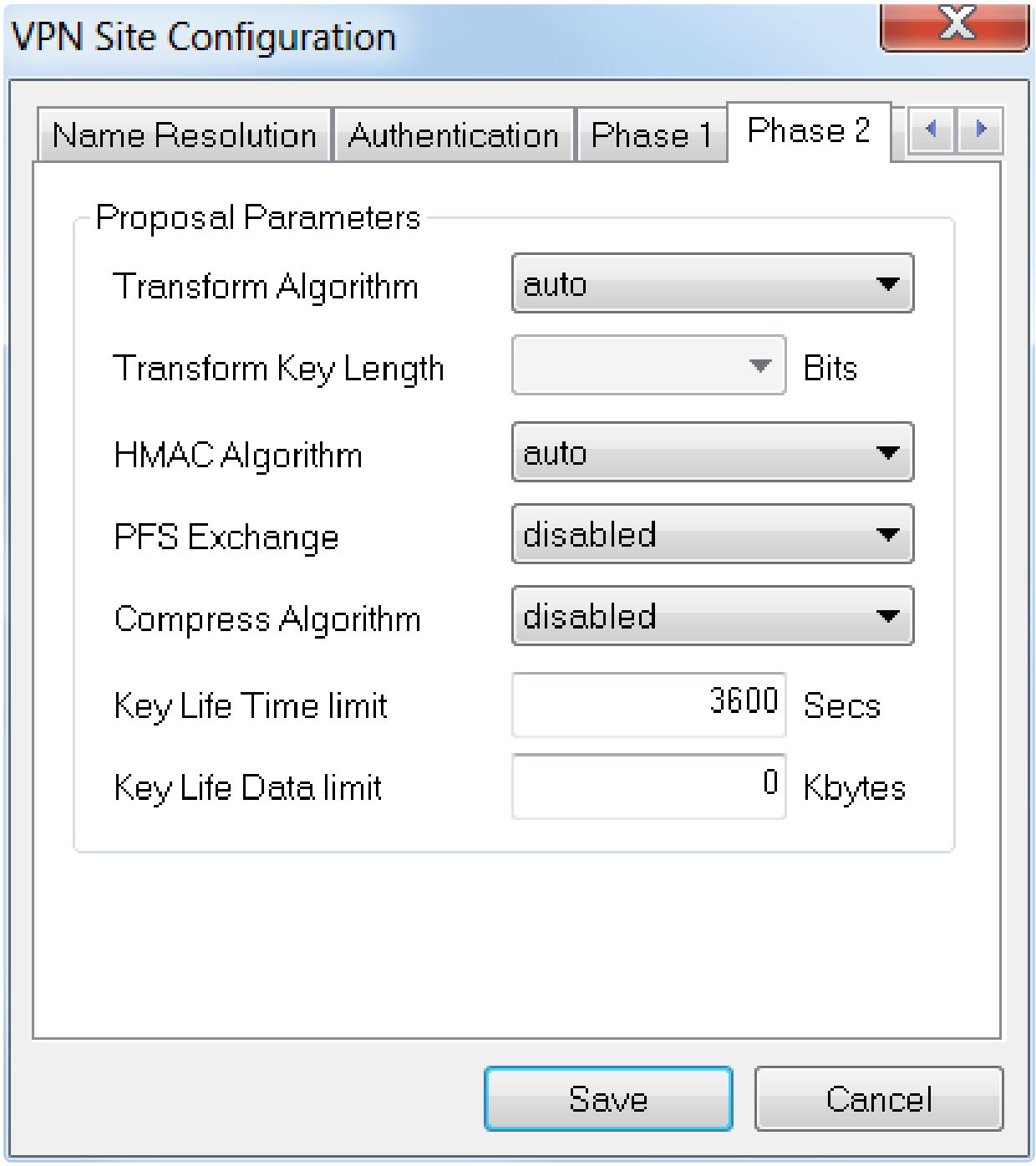
- Type d'échange : Agressif
- Échange DH : groupe 2
- Algorithme de chiffrement : Auto
- Algorithme de hachage : Auto



Étape 9

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

- Algorithme de transformation : Auto
- Algorithme HMAC : Auto
- PFS Exchange : désactivé
- Algorithme de compression : Désactivé

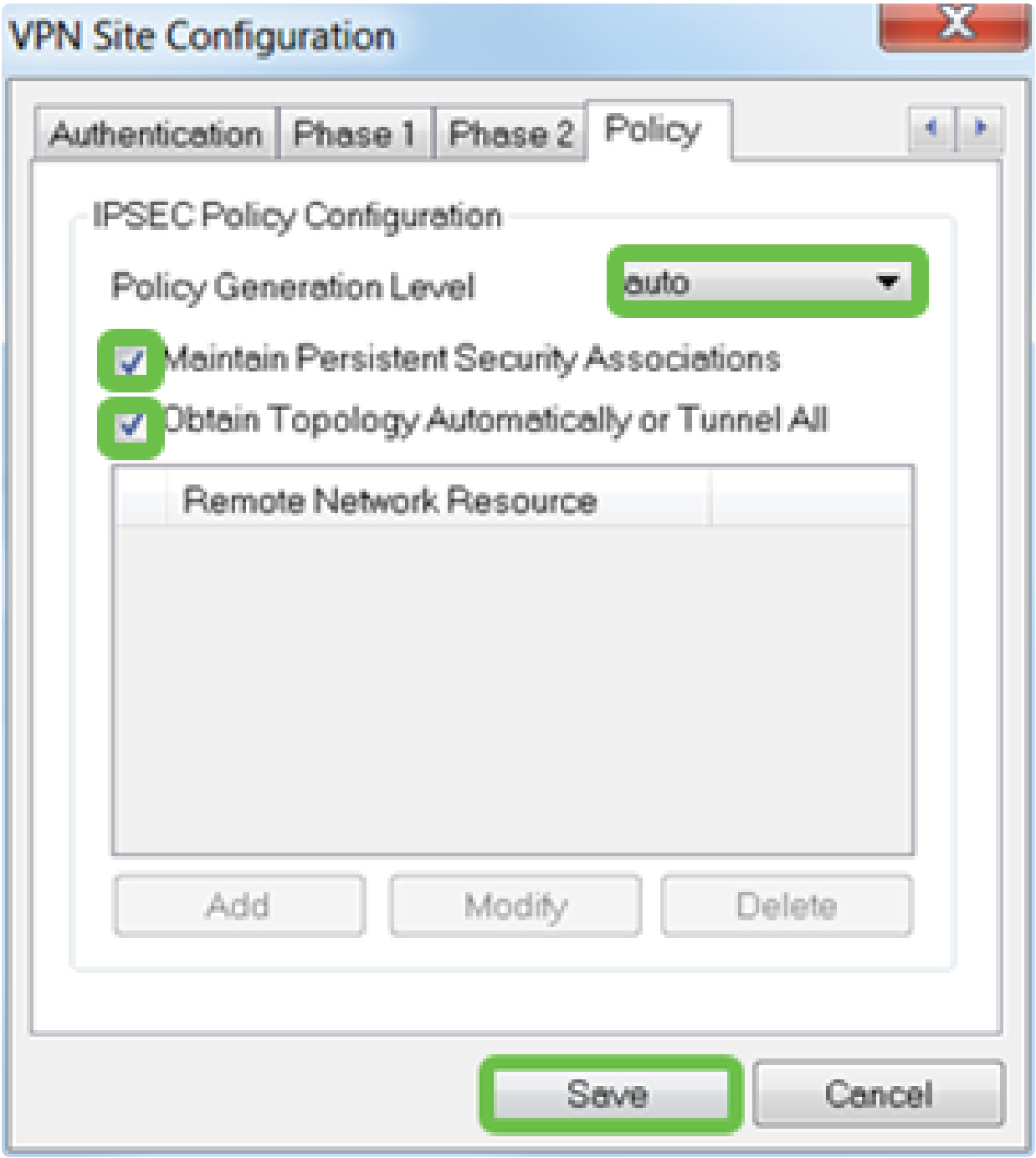


Étape 10

Pour l'exemple de l'onglet Policy, nous avons utilisé les paramètres suivants :

- Niveau de génération de stratégie : Auto
- Gérer les associations de sécurité persistantes : coché
- Obtenir la topologie automatiquement ou Tunnel All : coché

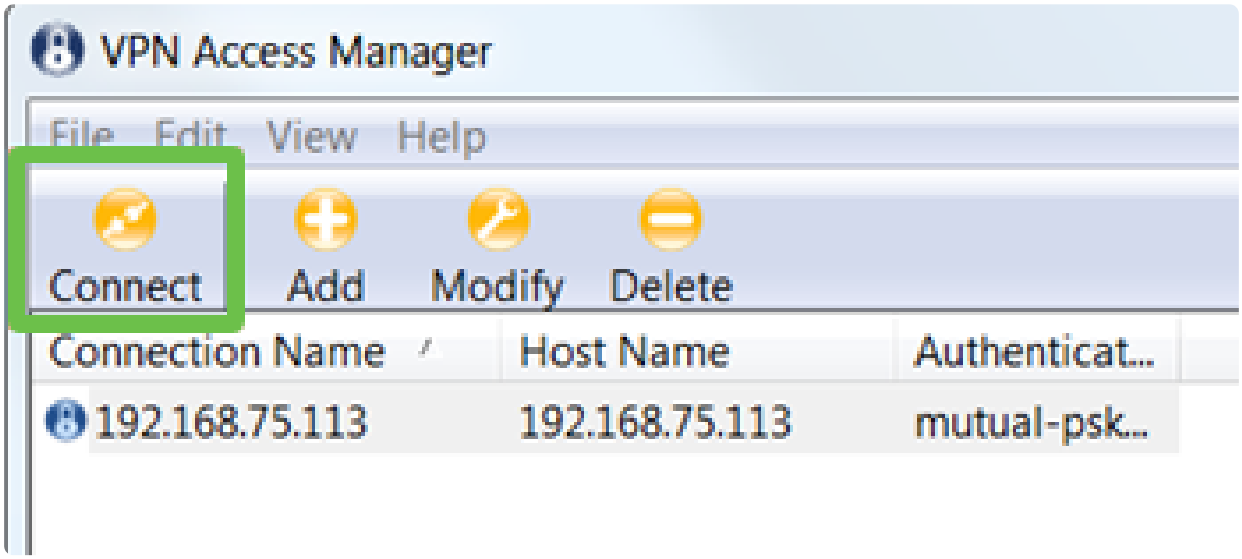
Puisque nous avons configuré la transmission tunnel partagée sur le RV345P, nous n'avons pas besoin de la configurer ici.



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.



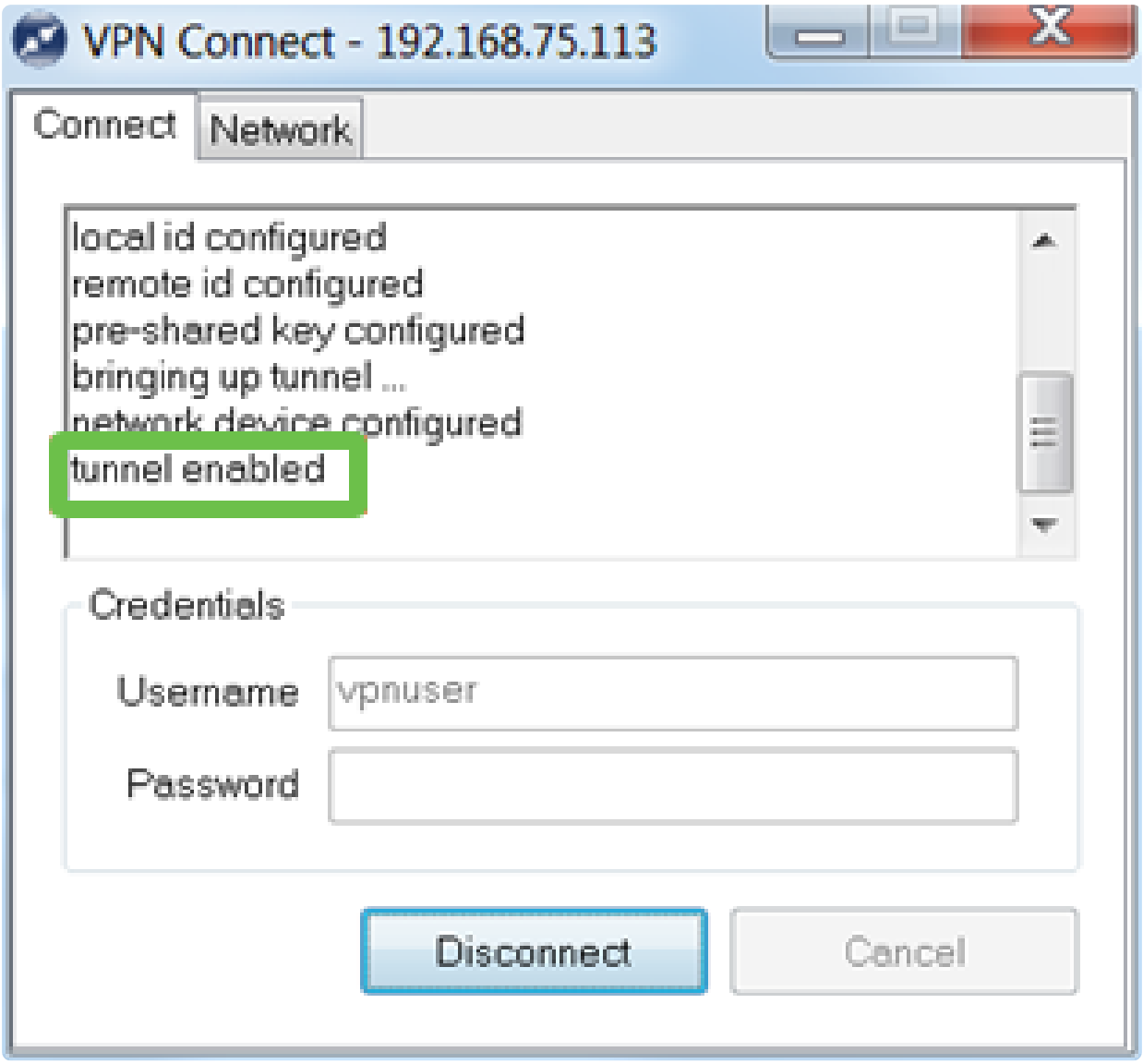
Étape 12

Dans la fenêtre VPN Connect qui s'affiche, 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.



ⓘ Note: Shrew Soft a été utilisé comme exemple dans cette configuration.

Shrew Soft n'étant pas un produit Cisco, veuillez contacter ce tiers si vous avez besoin d'assistance technique.

Autres options VPN

Il existe d'autres options pour l'utilisation d'un VPN. Cliquez sur les liens suivants pour plus d'informations :

- Utiliser le client VPN GreenBow pour se connecter au routeur de la gamme RV34x

- Configuration d'un client VPN pour télétravailleurs 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 IPsec (Internet Protocol Security) sur un routeur de la gamme RV34x
- Configuration des paramètres WAN L2TP sur le routeur RV34x
- Configuration d'un VPN site à site sur le RV34x

Configurations supplémentaires sur le routeur RV345P

Configuration des VLAN (facultatif)

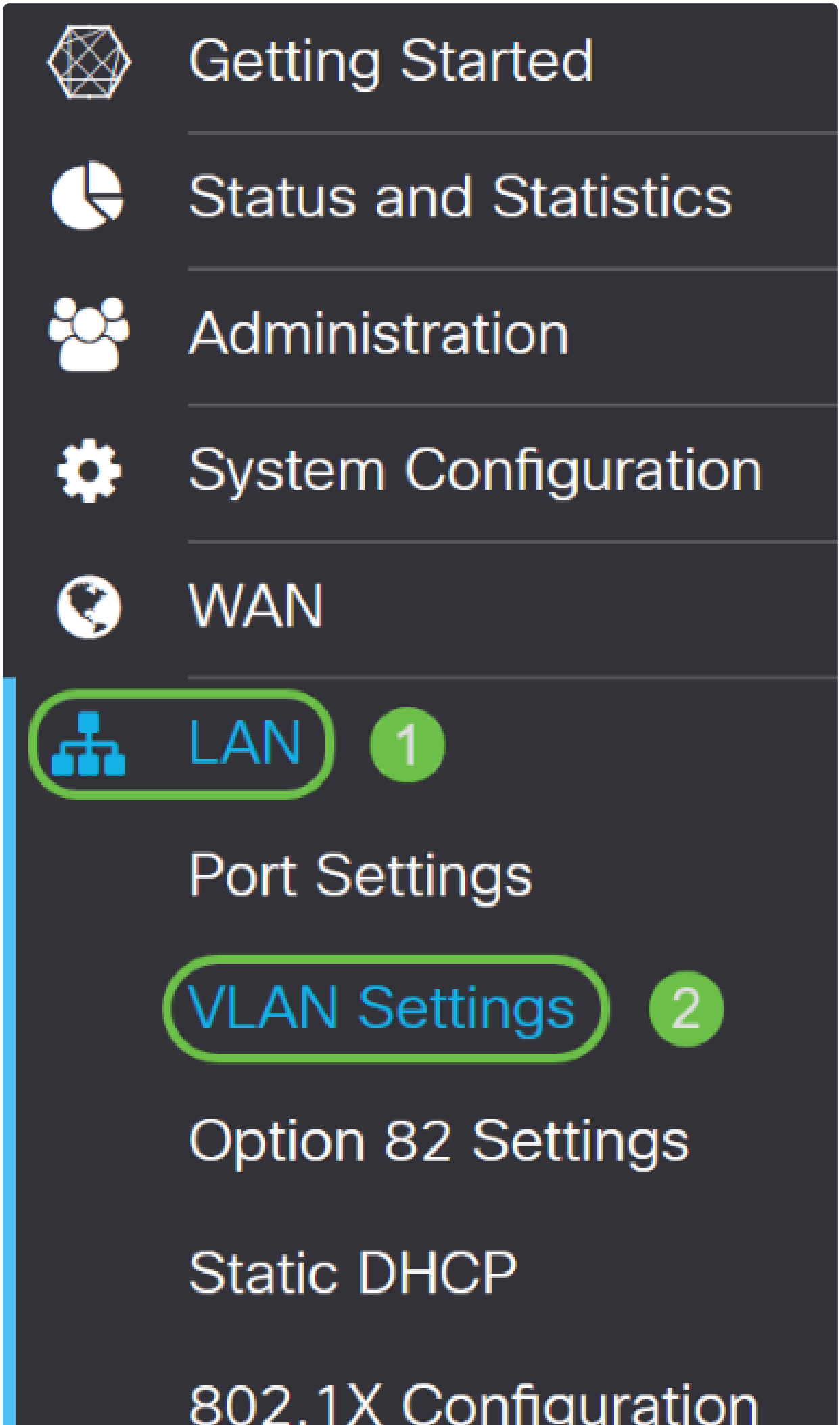
Un réseau local virtuel (VLAN) vous permet de segmenter logiquement un réseau local (LAN) en différents domaines de diffusion. Dans les scénarios où des données sensibles peuvent être diffusées sur un réseau, des VLAN peuvent être créés pour améliorer la sécurité en dirigeant une diffusion sur un VLAN spécifique. Les VLAN peuvent également être utilisés pour améliorer les performances en réduisant le besoin d'acheminer 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 conseillées et les conseils de sécurité pour obtenir des conseils supplémentaires.

Si vous ne souhaitez pas créer de VLAN, passez à la section suivante.

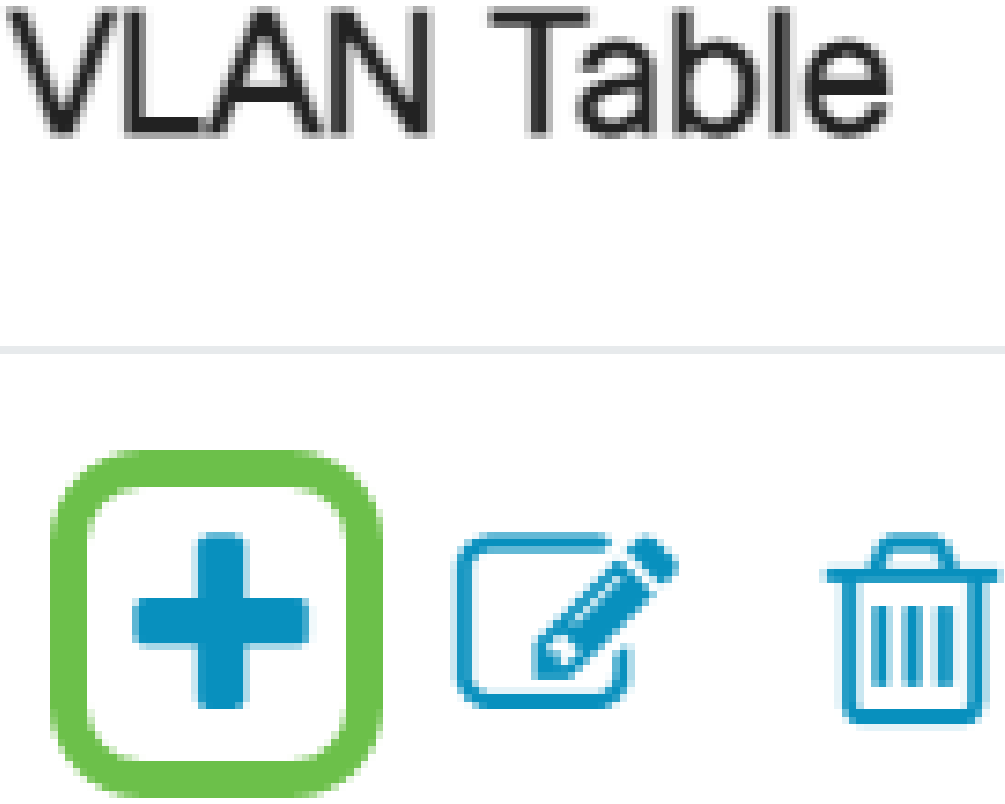
Étape 1

Accédez à LAN > VLAN Settings.


Getting Started
Status and Statistics
Administration
System Configuration
WAN
LAN
1
Port Settings
VLAN Settings
2
Option 82 Settings
Static DHCP
802.1X Configuration

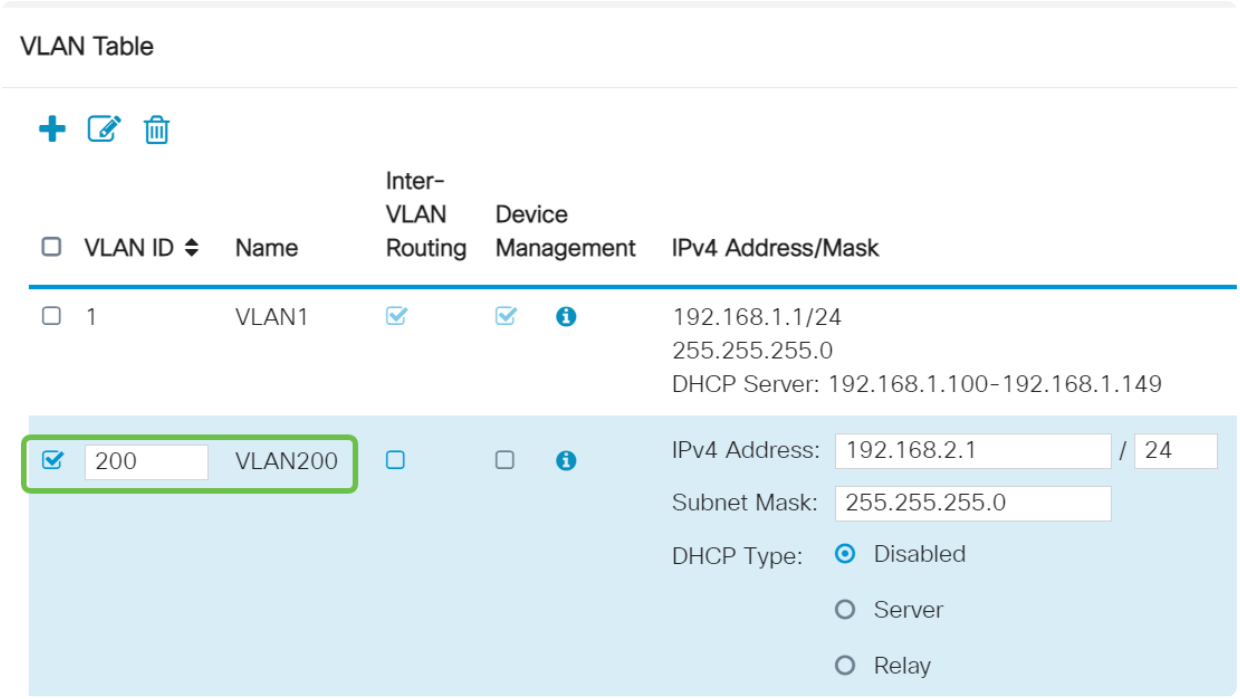
Étape 2

Cliquez sur l'icône d'ajout pour créer un nouveau VLAN.



Étape 3

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



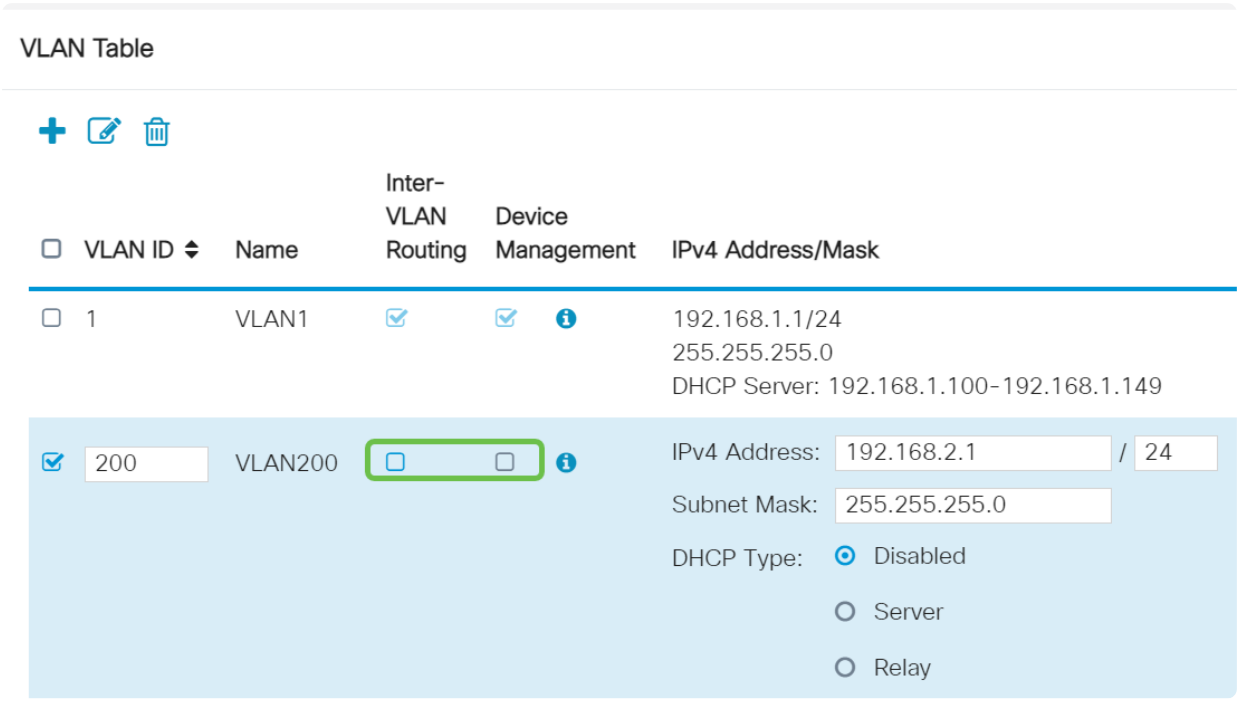
Étape 4

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.

En général, cette méthode n'est pas recommandée pour les réseaux invités, car vous souhaiterez isoler les utilisateurs invités, car elle laisse les VLAN moins sécurisés. Il peut parfois être nécessaire pour les VLAN d'effectuer un routage entre eux. Si c'est le cas, consultez Routage inter-VLAN sur un routeur RV34x avec restrictions ACL ciblées pour configurer le trafic spécifique que vous autorisez entre les VLAN.

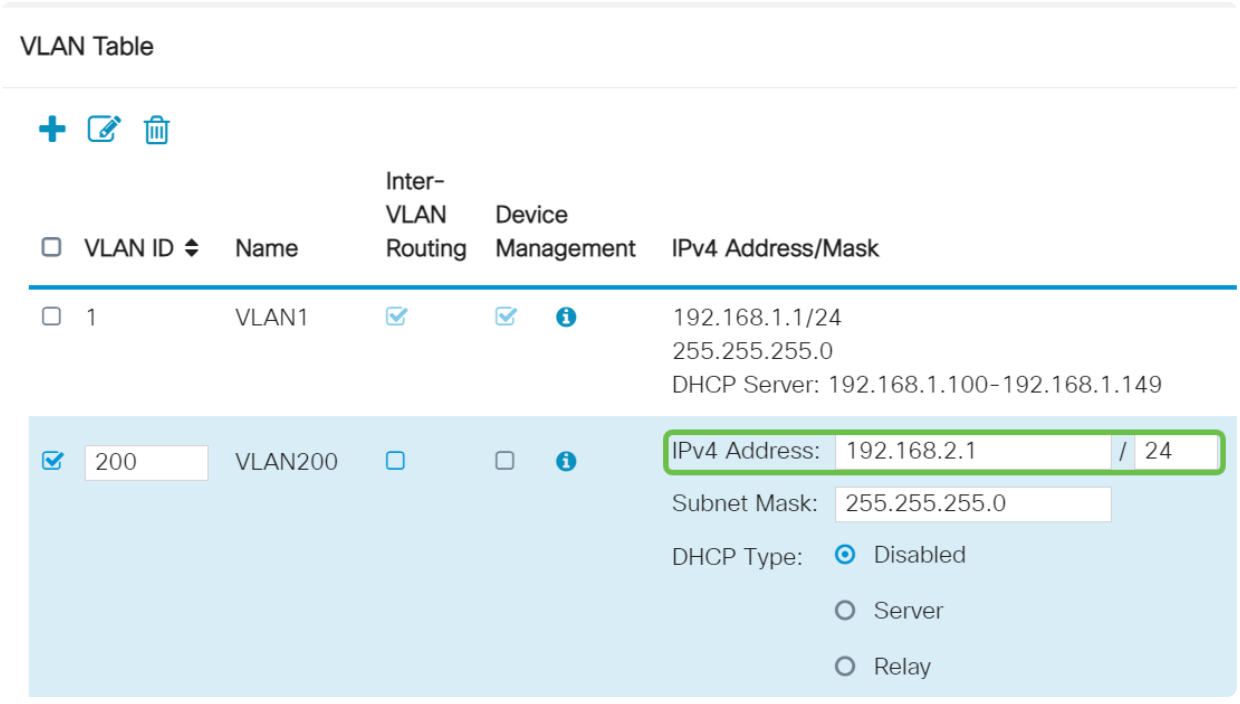
Device Management est le logiciel qui vous permet d'utiliser votre navigateur pour vous connecter à l'interface utilisateur Web du RV345P, à partir du VLAN, et gérer le RV345P. Cette option doit également être désactivée sur les réseaux invités.

Dans cet exemple, nous n'avons pas activé le routage inter-VLAN ou la gestion des périphériques pour maintenir le VLAN plus sécurisé.



Étape 5

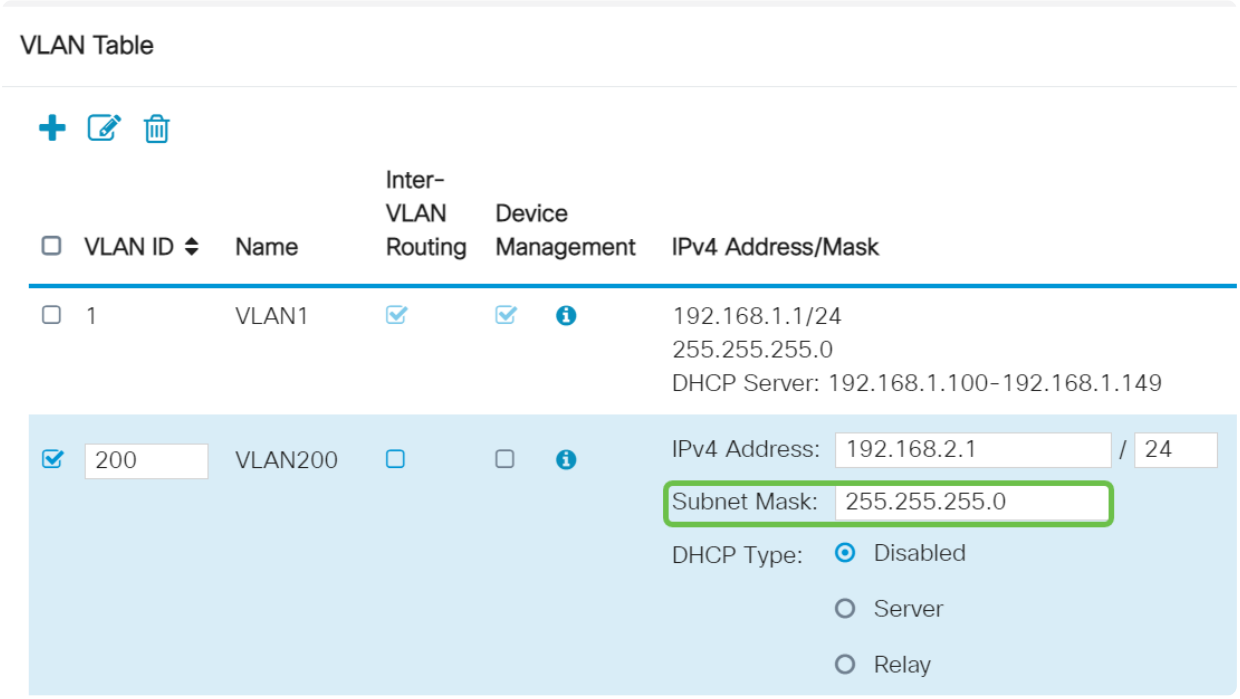
L'adresse IPv4 privée est automatiquement renseignée dans le champ IP Address. Vous pouvez régler ce paramètre si vous le souhaitez. Dans cet exemple, le sous-réseau a 192.168.2.100-192.168.2.149 adresses IP disponibles pour DHCP. 192.168.2.1-192.168.2.99 et 192.168.2.150-192.168.2.254 sont disponibles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



Étape 6

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

Pour cette démonstration, nous allons laisser le masque de sous-réseau comme 255.255.255.0 ou /24.



Étape 7

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

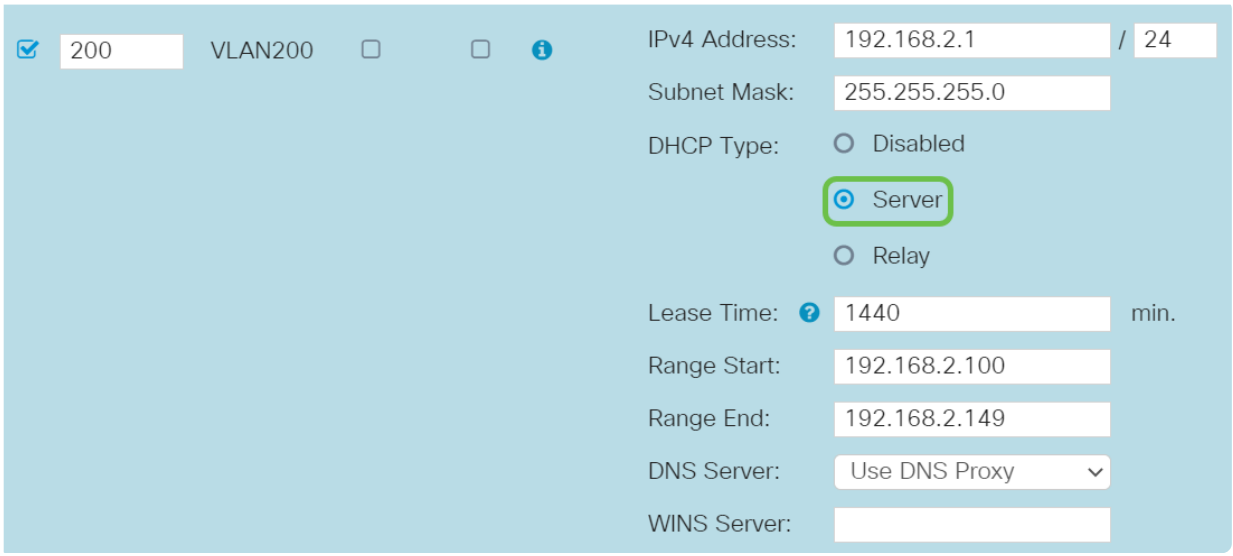
Disabled : désactive le serveur DHCP IPv4 sur le VLAN. Ceci est recommandé dans un environnement de test. Dans ce scénario, toutes les adresses IP doivent être configurées manuellement et toutes les communications doivent être internes.

Serveur : option la plus souvent utilisée.

- Lease Time (Durée du bail) : saisissez une durée comprise entre 5 et 43 200

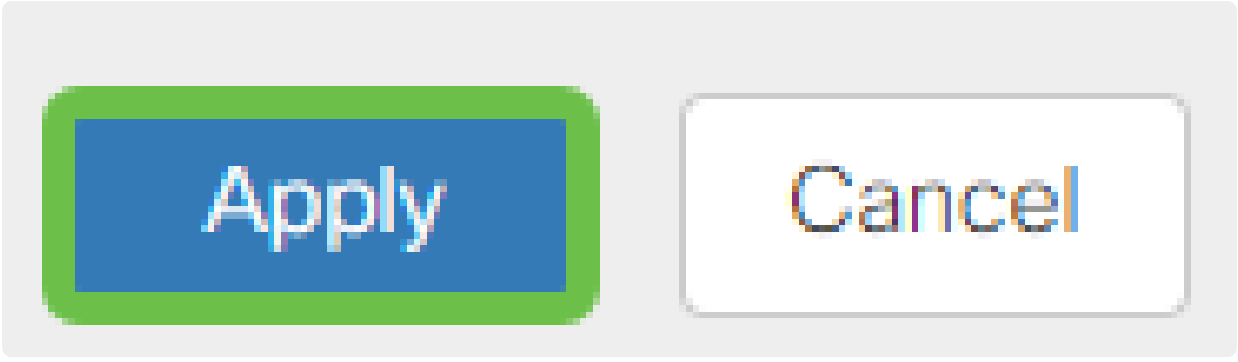
minutes. La valeur par défaut est 1 440 minutes (soit 24 heures).

- Range Start et Range End : saisissez le début et la fin de la plage d'adresses IP pouvant être attribuées dynamiquement.
- DNS Server (Serveur DNS) : sélectionnez cette option pour utiliser le serveur DNS en tant que proxy ou à partir d'un FAI dans la liste déroulante.
- 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 : saisissez 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.



Attribution de VLAN aux ports (facultatif)

16 VLAN peuvent être configurés sur le RV345P, avec un VLAN pour le réseau étendu (WAN). Les VLAN qui ne sont pas sur un port doivent être exclus. Cela permet de conserver 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 configurés en tant que port d'accès ou 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 balisé. Les VLAN dont vous ne voulez pas sur la liaison 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 Untagged.
- Tous les autres VLAN doivent être étiquetés Excluded pour ce port.

Au moins deux VLAN qui partagent un port :

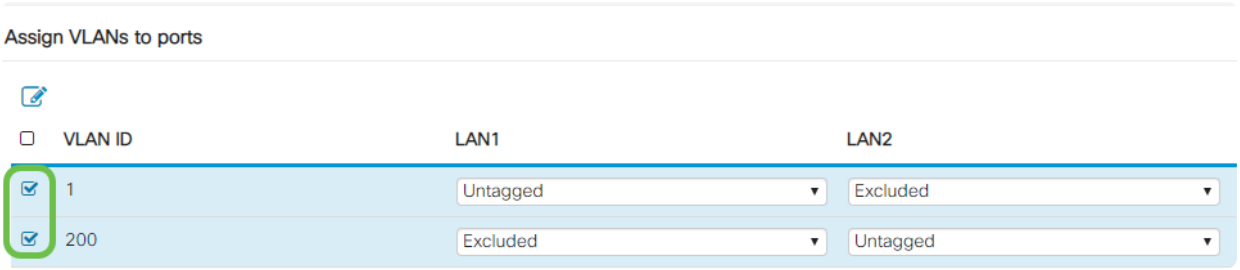
- Considéré comme un port agrégé.
- L'un des VLAN peut être étiqueté Untagged (non balisé).
- Les autres réseaux locaux virtuels qui font partie du port de liaisons doivent être étiquetés Tagged (balisé).
- Les VLAN qui ne font pas partie du port de liaisons doivent être étiquetés Excluded (exclus) pour ce port.

> ⓘ Note: Dans cet exemple, il n'existe pas de trunks.

Étape 1

Sélectionnez les ID de VLAN à modifier.

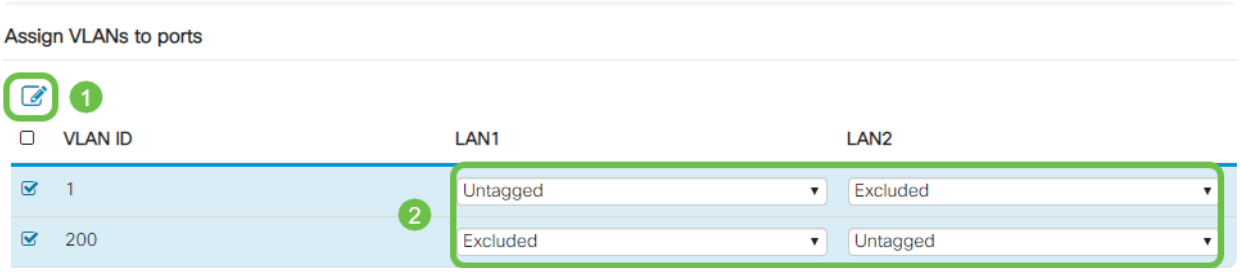
Dans cet exemple, nous avons sélectionné VLAN 1 et VLAN 200.



Étape 2

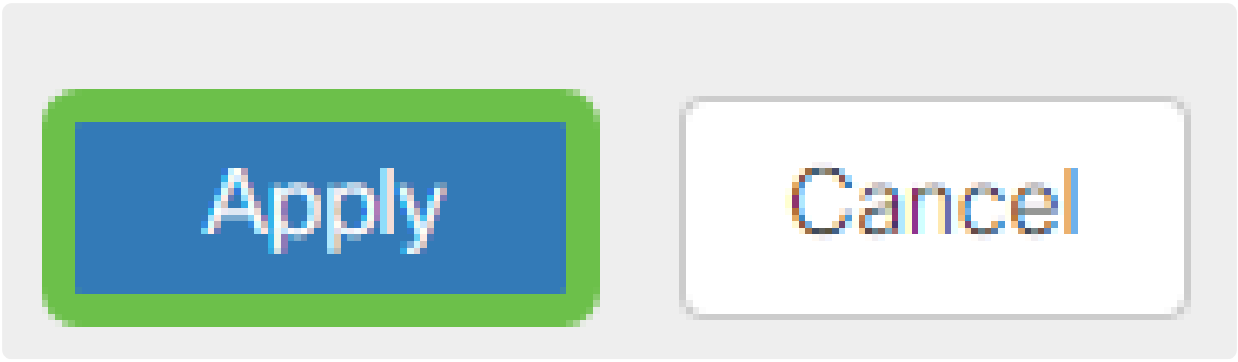
Cliquez sur Edit pour attribuer un VLAN à un port LAN et spécifier chaque paramètre comme Tagged, Untagged ou Excluded.

Dans cet exemple, sur LAN1, nous avons attribué VLAN 1 comme non étiqueté et VLAN 200 comme exclu. Pour le réseau local LAN2, nous avons attribué VLAN 1 comme Excluded et VLAN 200 comme Untagged.



Étape 3

Cliquez sur Apply pour enregistrer la configuration.



Vous devez maintenant avoir correctement créé un nouveau VLAN et configuré les VLAN sur les ports du RV345P. Répétez la procédure pour créer les autres VLAN. Par exemple, VLAN300 serait créé pour Marketing avec un sous-réseau de 192.168.3.x et VLAN400 serait créé pour Accounting avec un sous-réseau de 192.168.4.x.

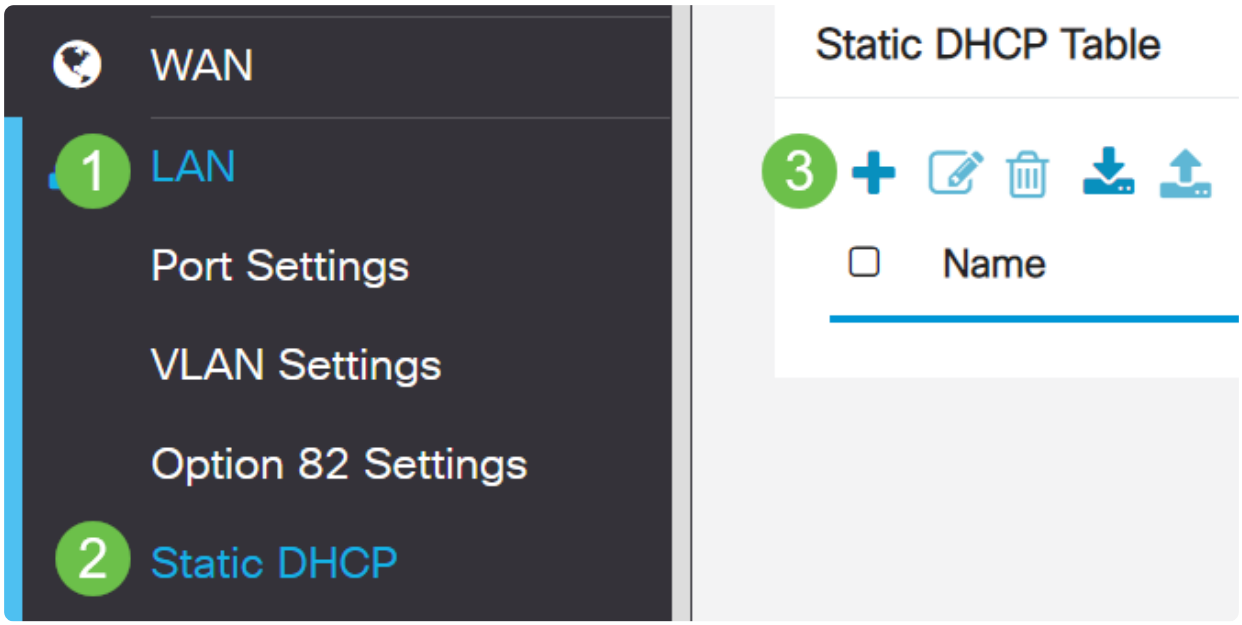
Ajouter une adresse IP statique (facultatif)

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 d'adresses IP statiques, consultez Meilleures pratiques pour la définition d'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.

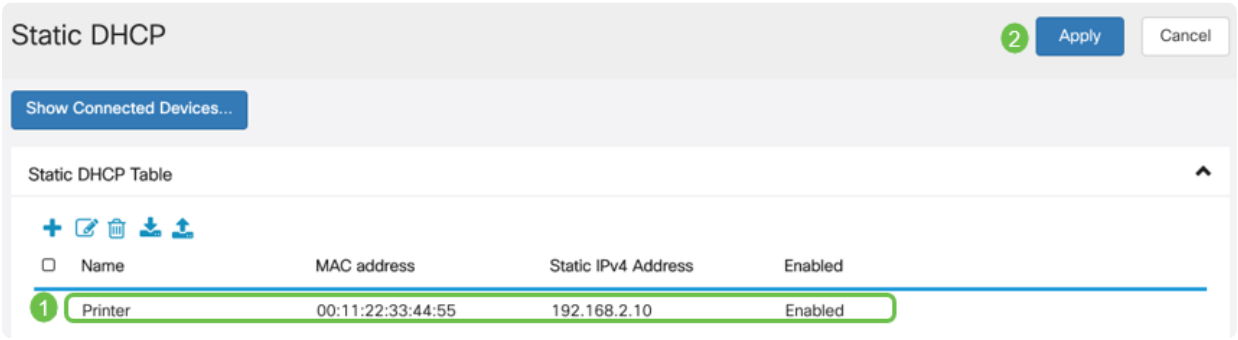
Étape 1

Accédez à LAN > Static DHCP (DHCP statique). Cliquez sur l'icône plus.



Étape 2

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



Gestion des certificats (facultatif)

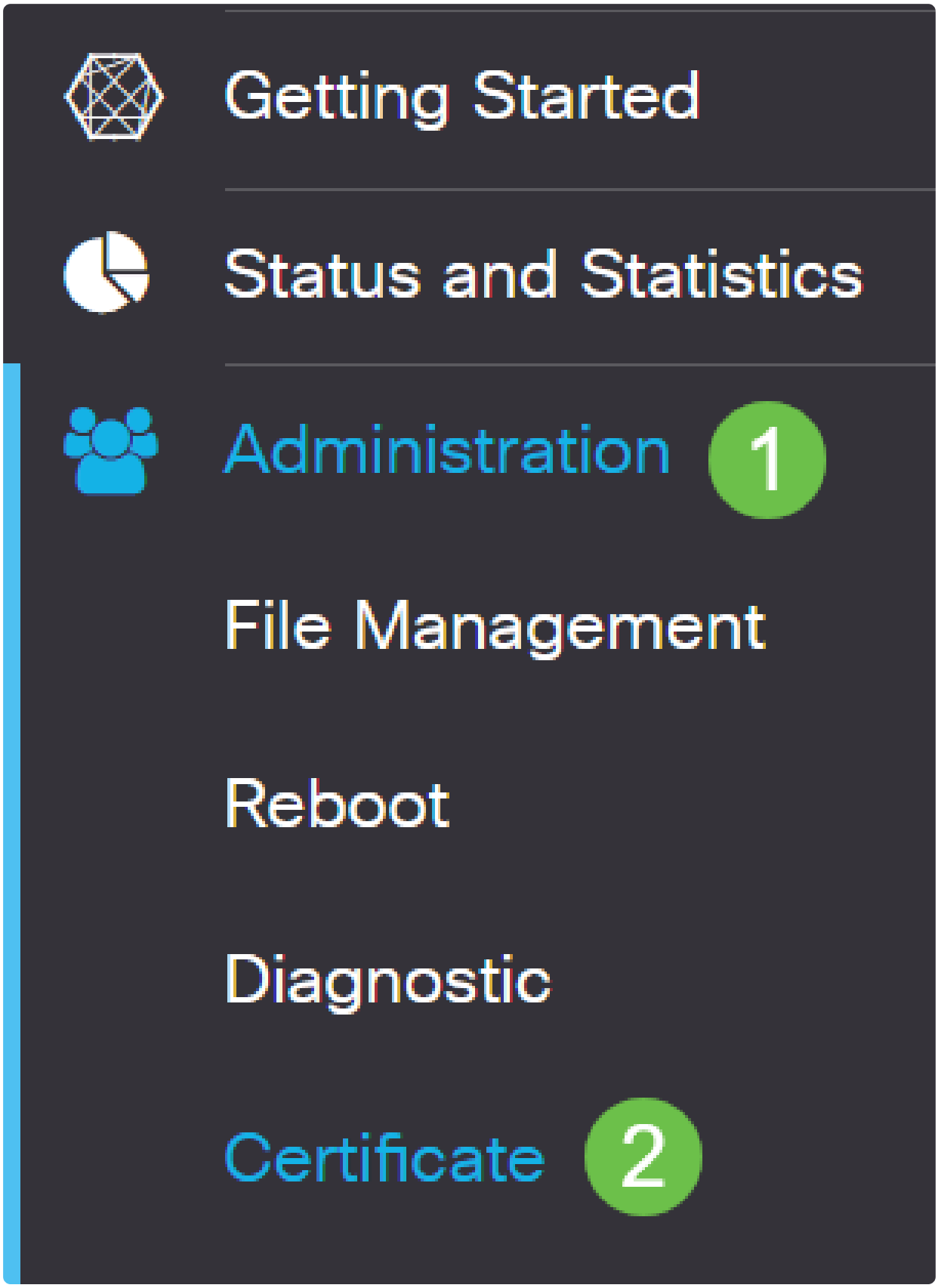
Un certificat numérique certifie la propriété d'une clé publique par le sujet nommé du certificat. Cela permet aux parties de confiance de dépendre des signatures ou des assertions faites par la clé privée qui correspond à la clé publique qui est certifiée. Un routeur peut générer un certificat auto-signé,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

Une autorité de certification (CA) est utilisée pour l'authentification. Les certificats peuvent être achetés à partir de n'importe quel nombre de sites tiers. C'est un moyen officiel de prouver que votre site est sécurisé. Essentiellement, l'autorité de certification est une source fiable qui vérifie que vous êtes une entreprise légitime et que vous pouvez être fiable. Selon vos besoins, un certificat à un coût minimal. Vous êtes extrait par l'autorité de certification, et une fois qu'elle aura vérifié vos informations, elle vous délivrera le certificat. Ce certificat peut être téléchargé en tant que fichier sur votre ordinateur. Vous pouvez ensuite accéder à votre routeur (ou à votre serveur VPN) et l'y télécharger.

Générer un CSR/certificat

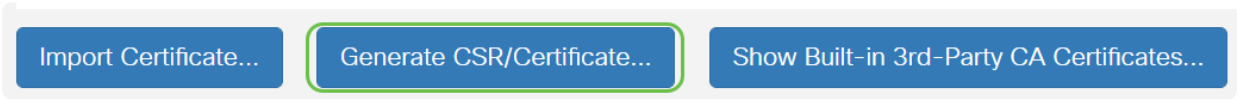
Étape 1

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


Getting Started
Status and Statistics
Administration
1
File Management
Reboot
Diagnostic
Certificate
2

Étape 2

Cliquez sur Generate CSR/Certificate. La page Generate CSR/Certificate (Générer un CSR/certificat) s'affiche.

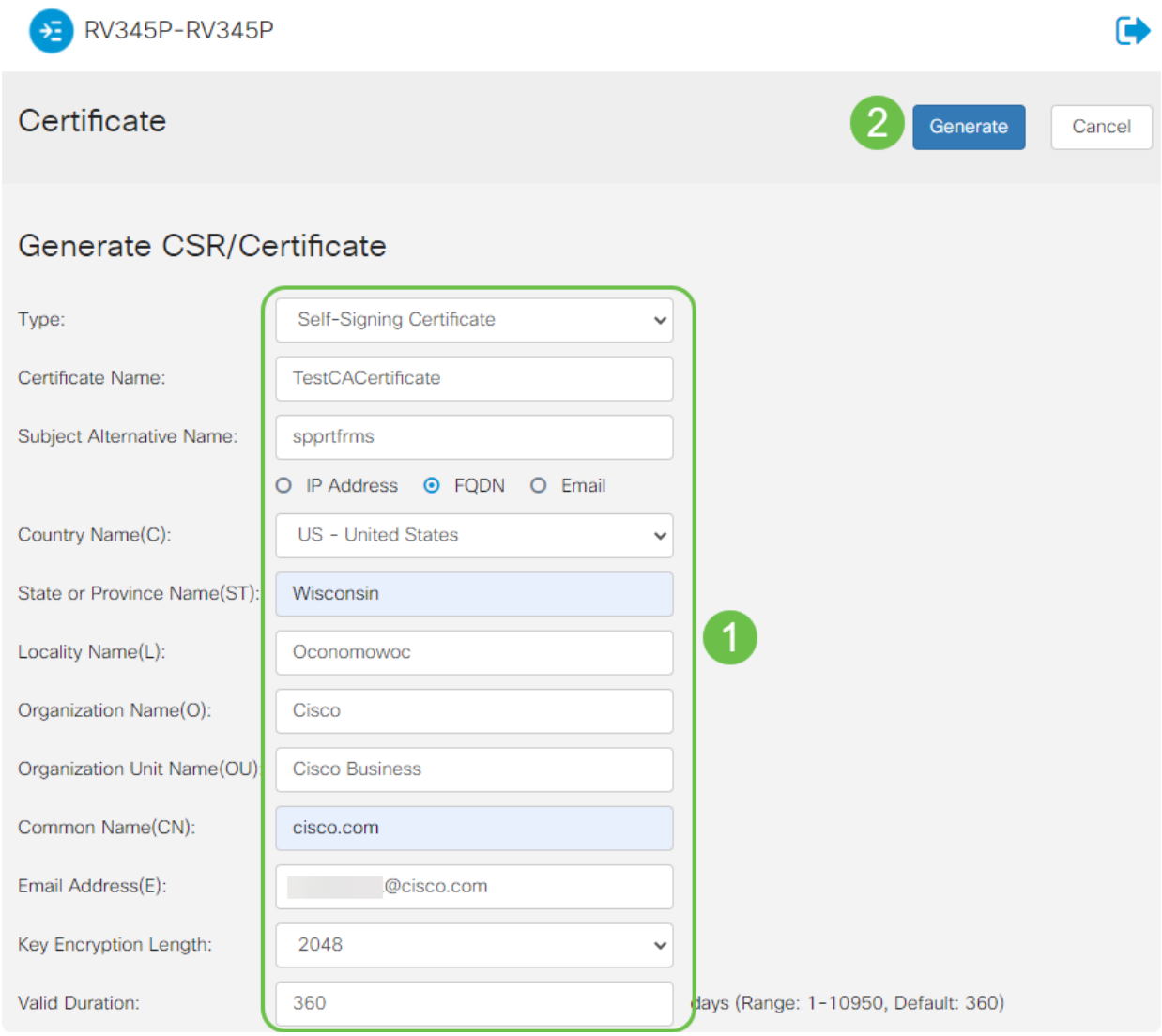


Étape 3

Remplissez les cases avec les éléments suivants :

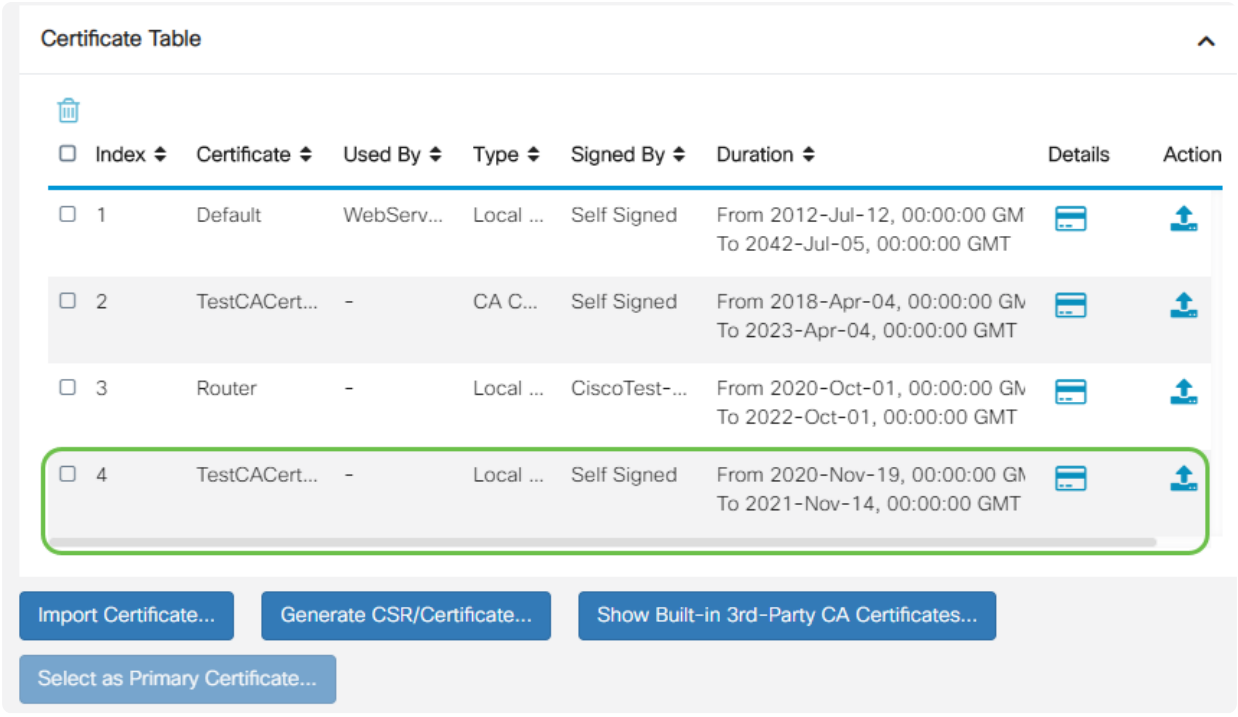
- Sélectionnez le type de certificat approprié
  - Certificat auto-signataire : certificat SSL (Secure Socket Layer) signé par son propre créateur. Ce certificat est moins fiable, car il ne peut pas être annulé si la clé privée est compromise d'une manière ou d'une autre par un pirate.
  - Demande de signature certifiée : il s'agit d'une infrastructure à clé publique (PKI) qui est envoyée à l'autorité de certification pour demander un certificat d'identité numérique. Elle est plus sécurisée que l'auto-signature, 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 ou de caractères spéciaux.
- (Facultatif) Dans la zone Autre nom du sujet, 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)
  - Email : saisissez une adresse e-mail
- Dans le champ Subject Alternative Name, saisissez le nom de domaine complet.
- Sélectionnez le nom du pays dans lequel votre organisation est légalement enregistrée dans la liste déroulante Nom du pays.
- Saisissez le nom ou l'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 située dans le champ Nom de la localité.
- Inscrivez le 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.

- Saisissez un nom dans le champ Nom de l'unité d'organisation pour différencier les divisions au sein d'une organisation.
- Entrez un nom dans le champ Nom commun. 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 importante, 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 Générer.



ⓘ Note: Le certificat généré doit maintenant apparaître dans la table des

certificats.

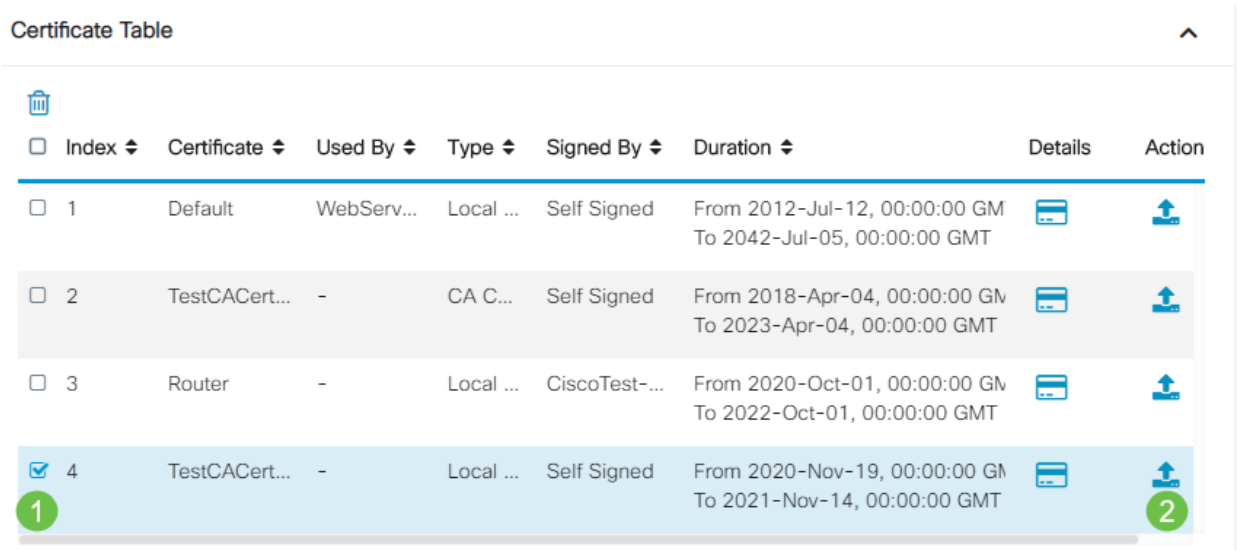


Vous devez maintenant avoir créé un certificat sur le routeur RV345P.

Exporter un certificat

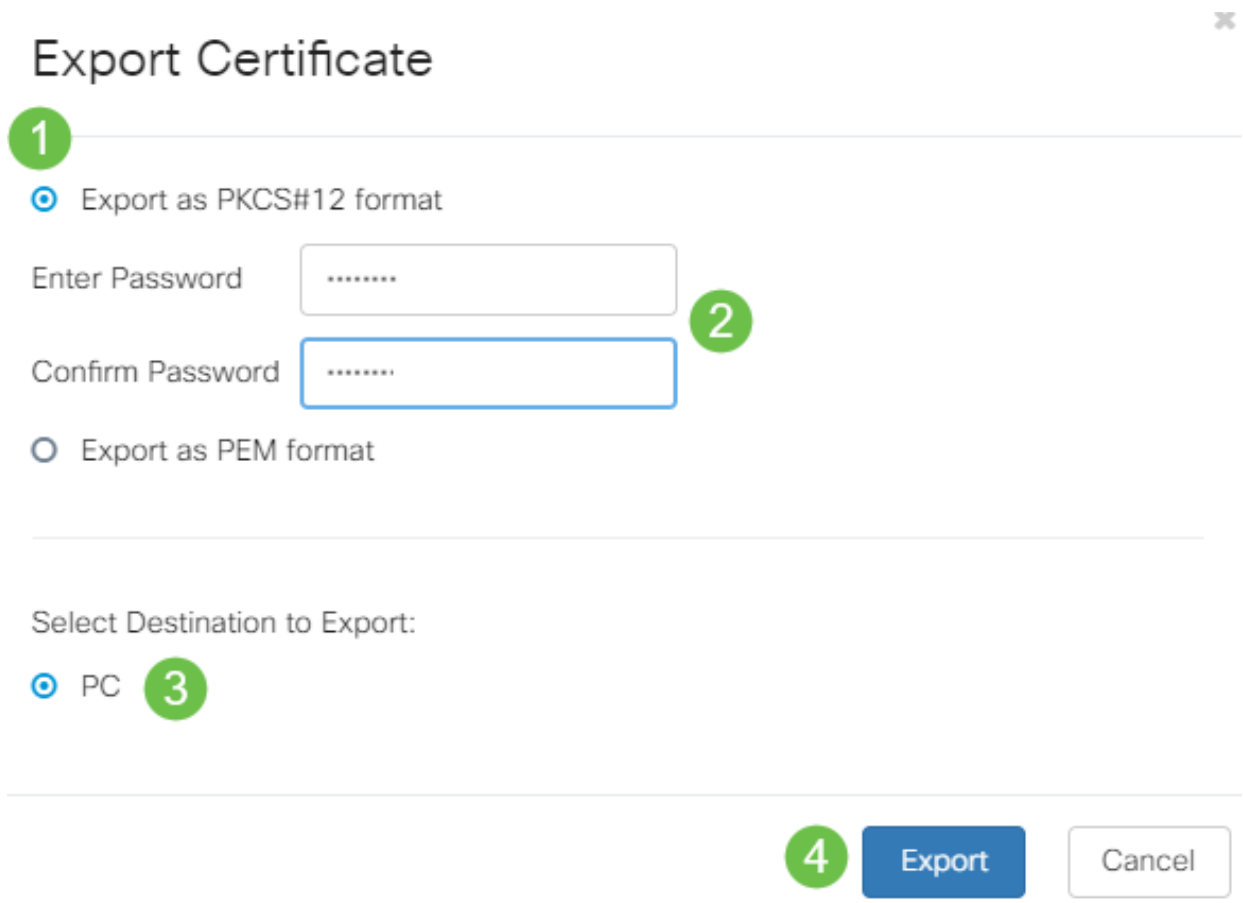
Étape 1

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



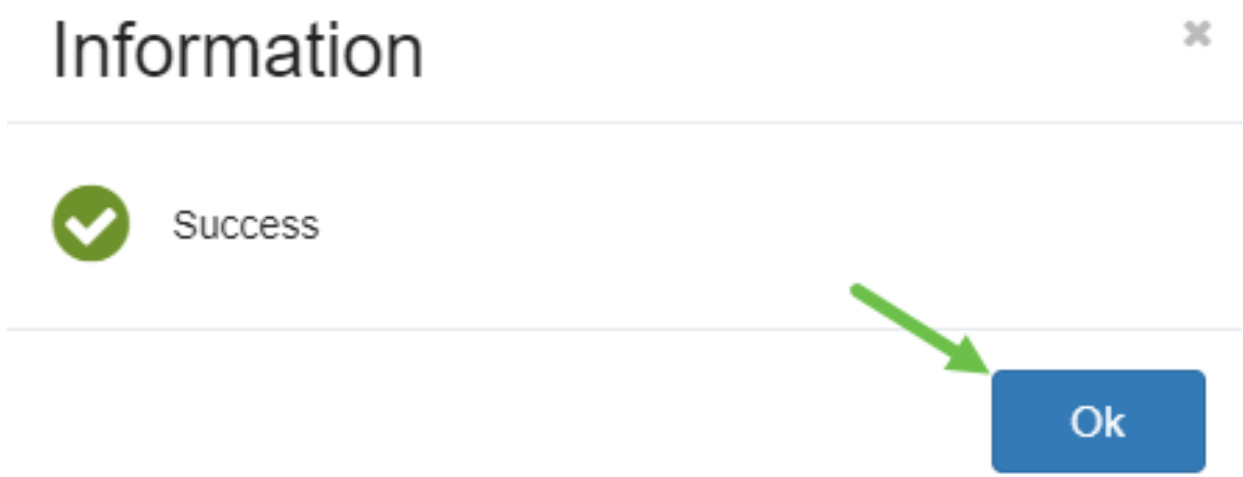
Étape 2

- 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 fourni avec une extension .p12. Un mot de passe sera requis pour chiffrer le fichier afin de le protéger lors de son exportation, de son importation et de sa suppression.
  - PEM — Privacy Enhanced Mail (PEM) est souvent utilisé pour les serveurs Web pour leur capacité à être facilement traduits en données lisibles à l'aide d'un simple éditeur de texte tel que le bloc-notes.
- Si vous avez choisi PEM, cliquez simplement sur Export.
- 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 Select Destination, PC a été sélectionné et est la seule option actuellement disponible.
- Cliquez sur Exporter.



Étape 3

Un message indiquant la réussite du téléchargement s'affiche sous le bouton Download (Télécharger). Un fichier commence à être téléchargé dans votre navigateur. Click OK.

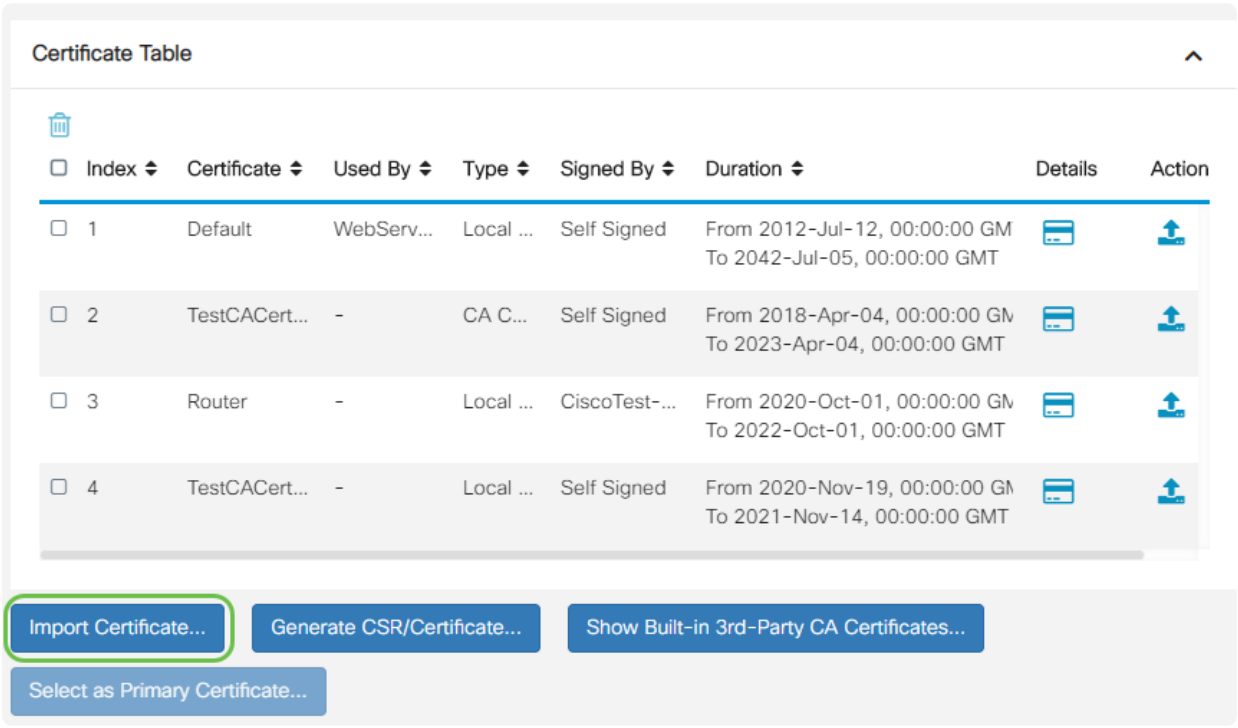


Vous devez maintenant avoir exporté un certificat sur le routeur de la gamme RV345P.

Importer un certificat

Étape 1

Cliquez sur Importer un certificat....



Étape 2

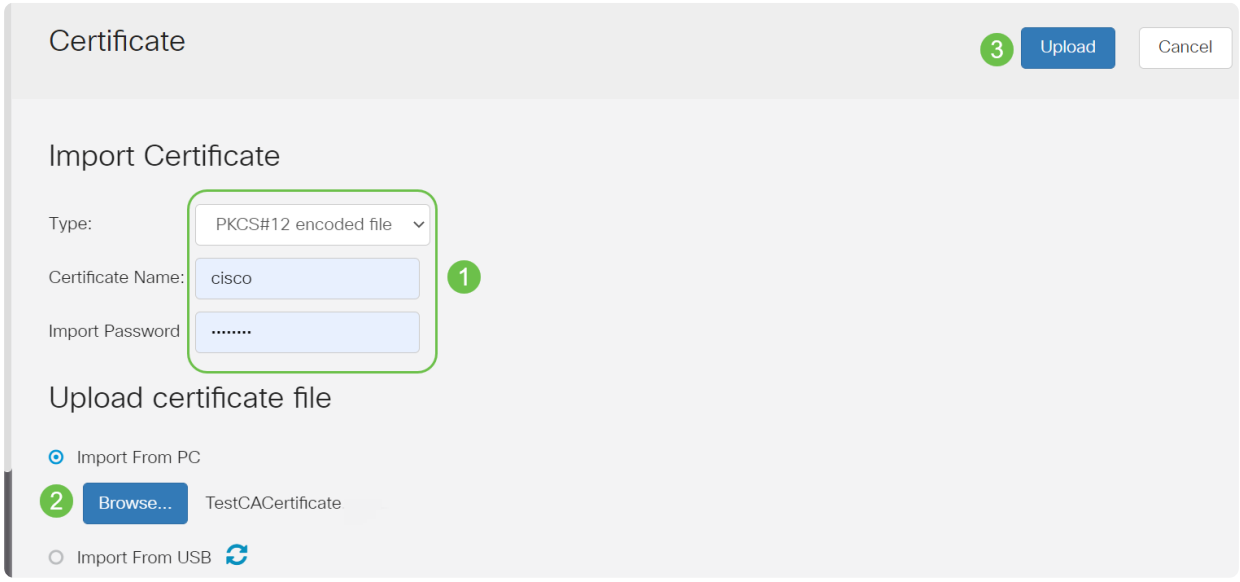
- Sélectionnez le type de certificat à importer dans la liste déroulante. Les options sont les suivantes :
  - Local Certificate : certificat généré sur le routeur.
  - Certificat CA : certificat certifié par une autorité tierce de confiance qui a confirmé que les informations contenues dans le certificat sont correctes.
  - PKCS #12 Encoded file — Public Key Cryptography Standards (PKCS) #12 est un format de stockage d'un certificat de serveur.

- Entrez un nom pour le certificat dans le champ Certificate Name.
- Si vous avez choisi PKCS #12, saisissez un mot de passe pour le fichier dans le

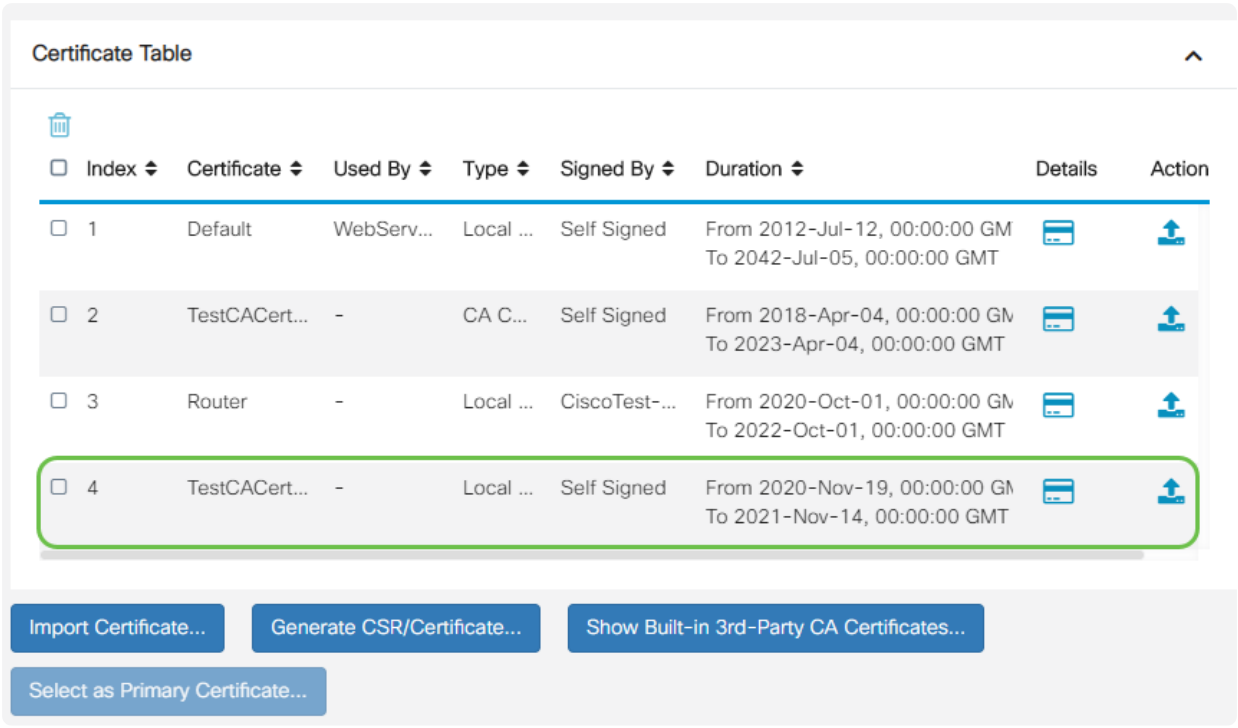
champ Mot de passe d'importation. Sinon, passez à l'étape 3.

- 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 sélectionné Import From USB et que votre périphérique 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 l'opération terminée, vous accédez automatiquement à la page principale du certificat. La table de certificats est renseignée avec le certificat récemment importé.



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

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

Vous souhaitez peut-être configurer un réseau mobile de secours à l'aide d'un dongle et de votre routeur RV345P. Si c'est le cas, vous devriez lire 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 sans fil professionnels Cisco.

Configuration du CBW140AC

CBW140AC prêt à l'emploi

Commencez par brancher un câble Ethernet entre le port PoE de votre CBW140AC et un port PoE du RV345P. Les 4 premiers ports du RV345P peuvent fournir de la technologie PoE, donc n'importe lequel d'entre eux peut être utilisé.

Vérifiez l'état des voyants. Le démarrage du point d'accès prend environ 10 minutes. Le voyant clignote en vert selon plusieurs modèles, alternant rapidement entre le vert, le rouge et l'ambre avant de redevenir vert. Il peut y avoir de petites variations dans l'intensité et la teinte de la couleur des LED d'une unité à l'autre. Lorsque le voyant DEL clignote en vert, passez à l'étape suivante.

Le port de liaison ascendante Ethernet PoE sur le point d'accès principal peut UNIQUEMENT être utilisé pour fournir une liaison ascendante au LAN, et PAS pour se connecter à d'autres périphériques principaux ou d'extension maillée.

Si votre point d'accès n'est pas neuf, prêt à l'emploi, 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 à ce sujet, consultez Comment redémarrer et réinitialiser les paramètres d'usine par défaut sur les routeurs RV345x.

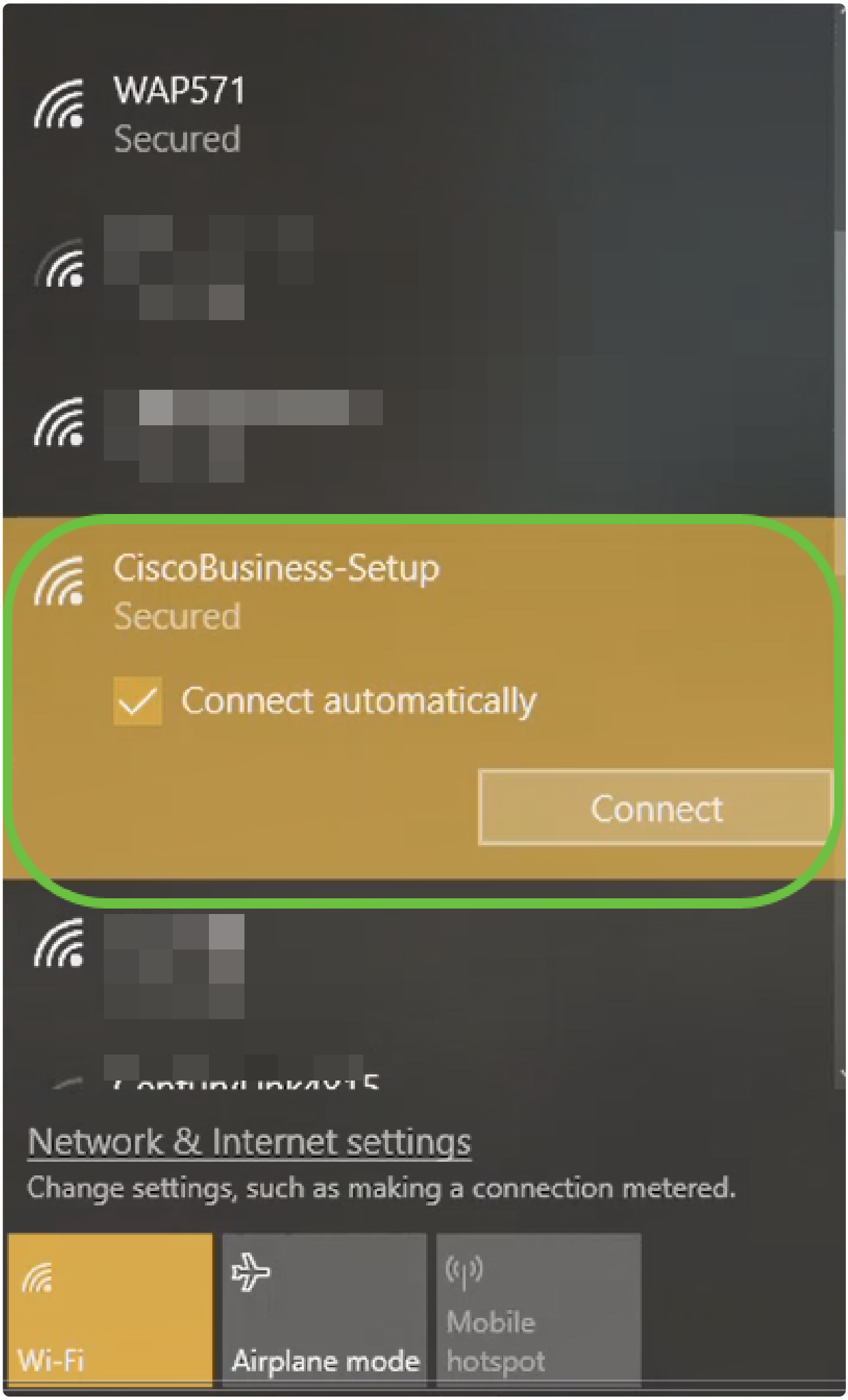
Configuration du point d'accès sans fil principal 140AC sur l'interface utilisateur Web

Vous pouvez configurer le point d'accès à l'aide de l'application mobile ou de l'interface Web. Cet article utilise l'interface utilisateur Web pour la configuration, qui offre plus d'options de configuration, mais est un peu plus compliquée. 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

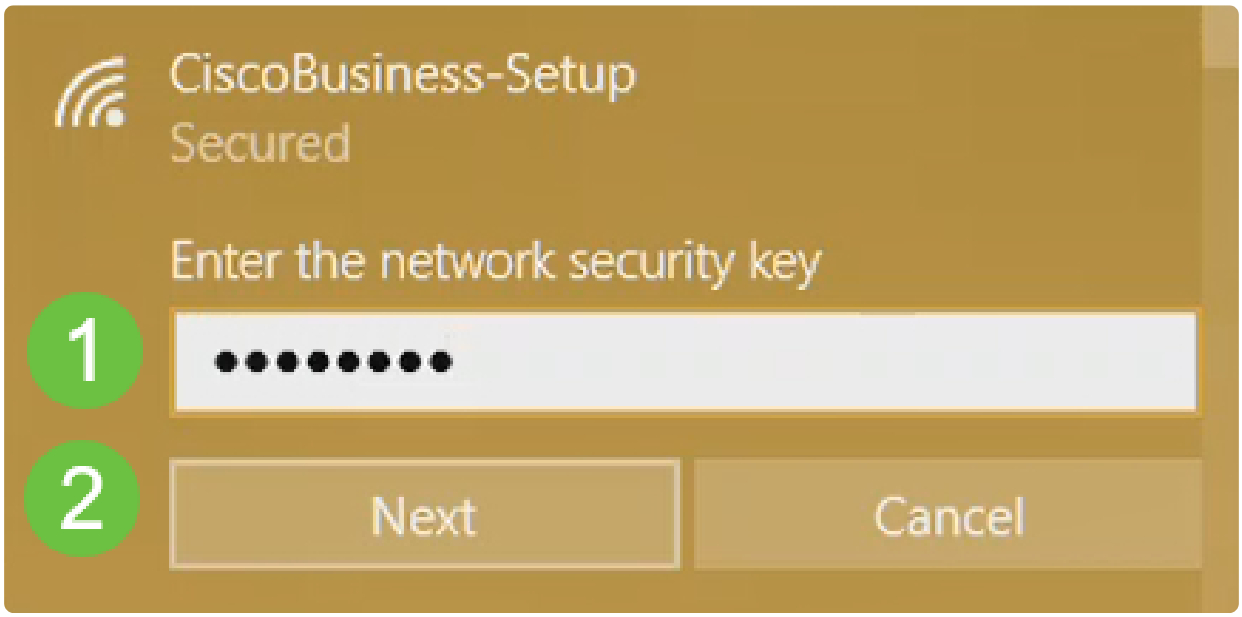
Sur votre PC, cliquez sur l'icône Wi-Fi et choisissez CiscoBusiness-Setup wireless network. Cliquez sur Connect.


WAP571
Secured
CiscoBusiness-Setup
Secured
Connect automatically
Connect
Network & Internet settings
Change settings, such as making a connection metered.
Wi-Fi
Airplane mode
Mobile hotspot

Si votre point d'accès n'est pas neuf, prêt à l'emploi, 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.

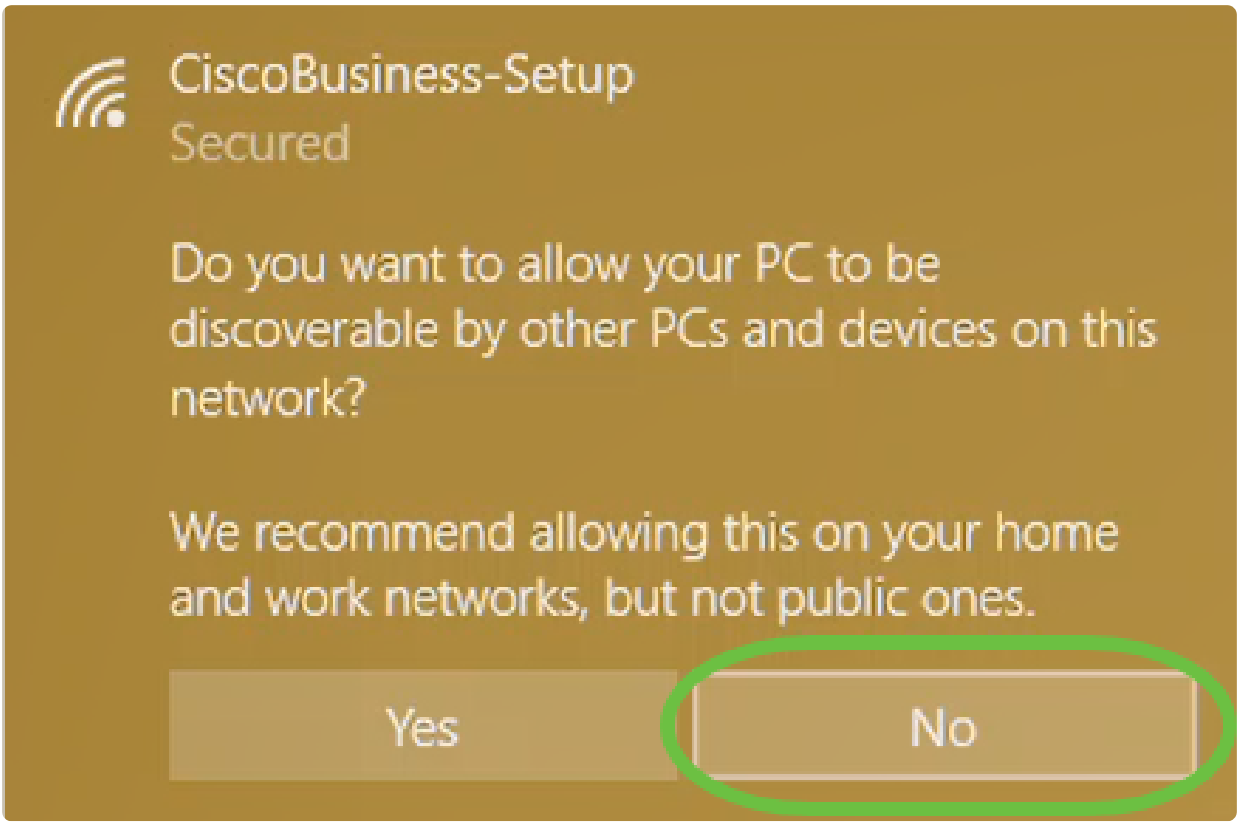
Étape 2

Entrez la phrase de passe cisco123 et cliquez sur Next.



Étape 3

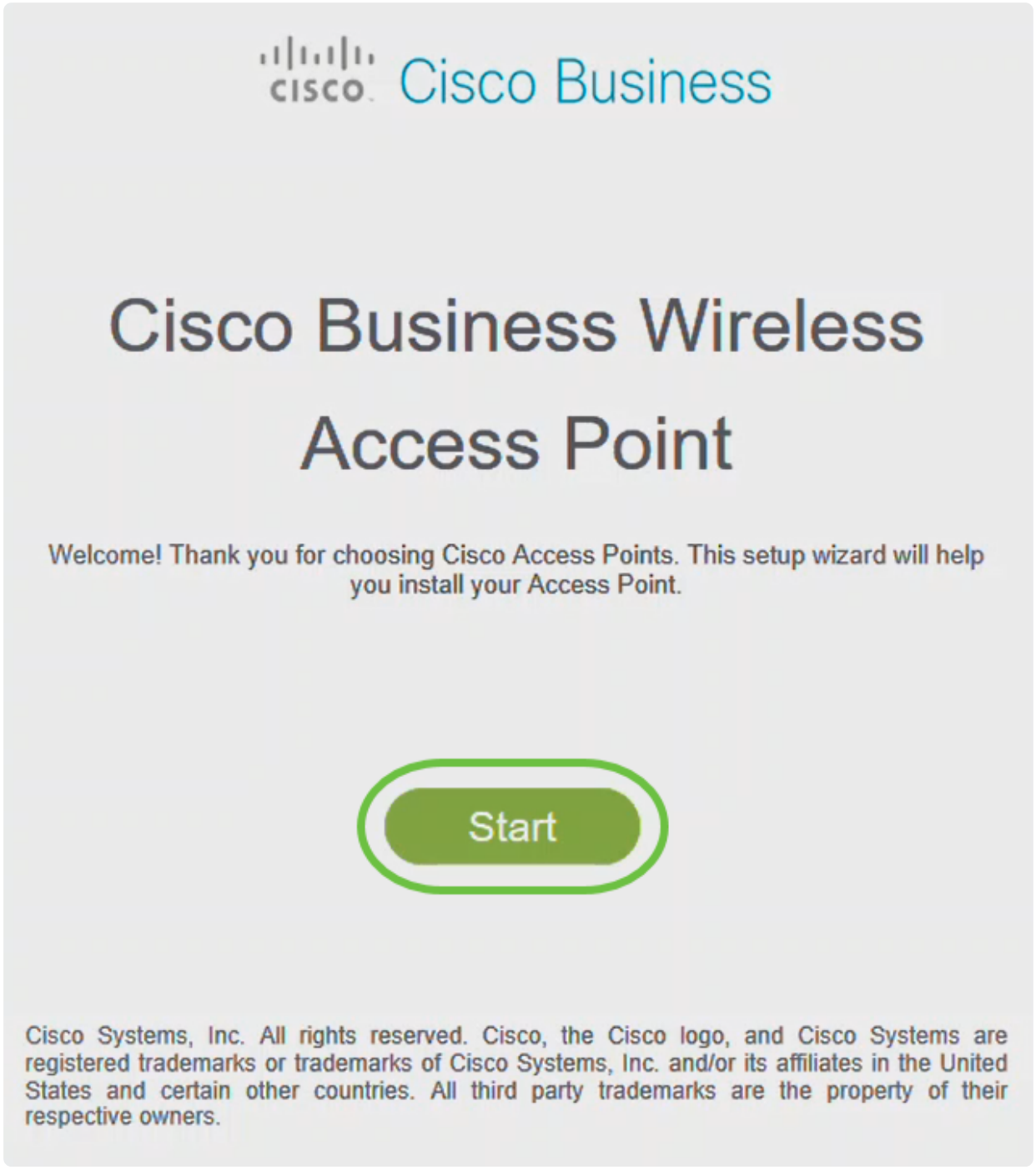
L'écran suivant s'affiche. Comme vous ne pouvez configurer qu'un seul périphérique à la fois, cliquez sur No.



Un seul périphérique peut être connecté au SSID CiscoBusiness-Setup. Si un deuxième 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, il se peut qu'un autre périphérique ait établi la connexion. Redémarrez le point d'accès et réessayez.

Étape 4

Une fois connecté, le navigateur Web doit automatiquement rediriger vers l'assistant de configuration de CBW AP. Si ce n'est pas le cas, 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.



ⓘ Note: Si vous ne voyez pas la page Web, attendez quelques minutes supplémentaires ou rechargez la page. Après cette configuration initiale, vous utiliserez https://ciscobusiness.cisco pour vous connecter. Si votre navigateur Web est renseigné automatiquement avec http://, vous devez taper manuellement le https:// pour y accéder.

Étape 5

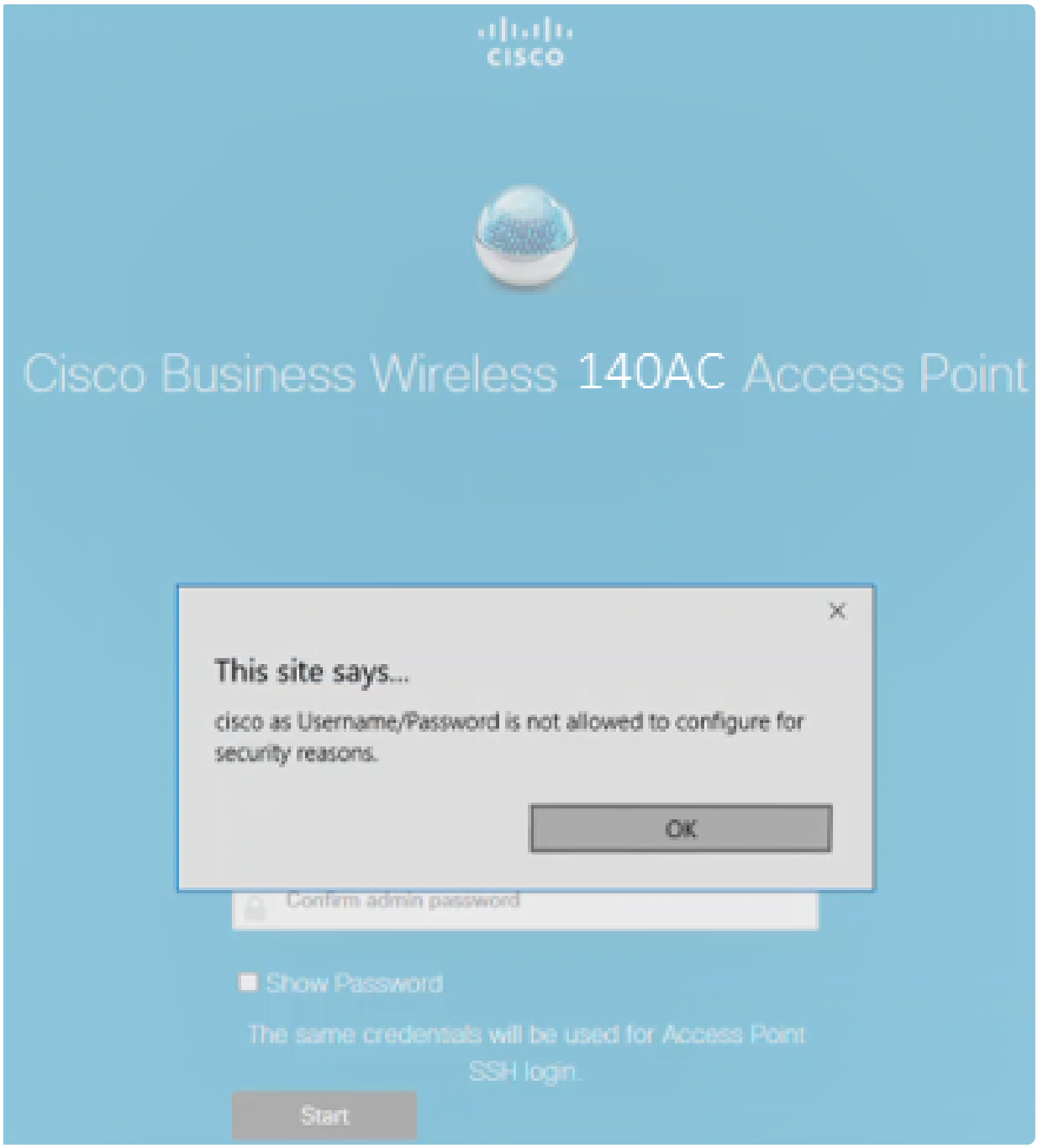
Créez un compte administrateur en saisissant les informations suivantes :

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

Vous pouvez choisir d'afficher le mot de passe en cochant la case en regard de Show Password. Cliquez sur Démarrer.



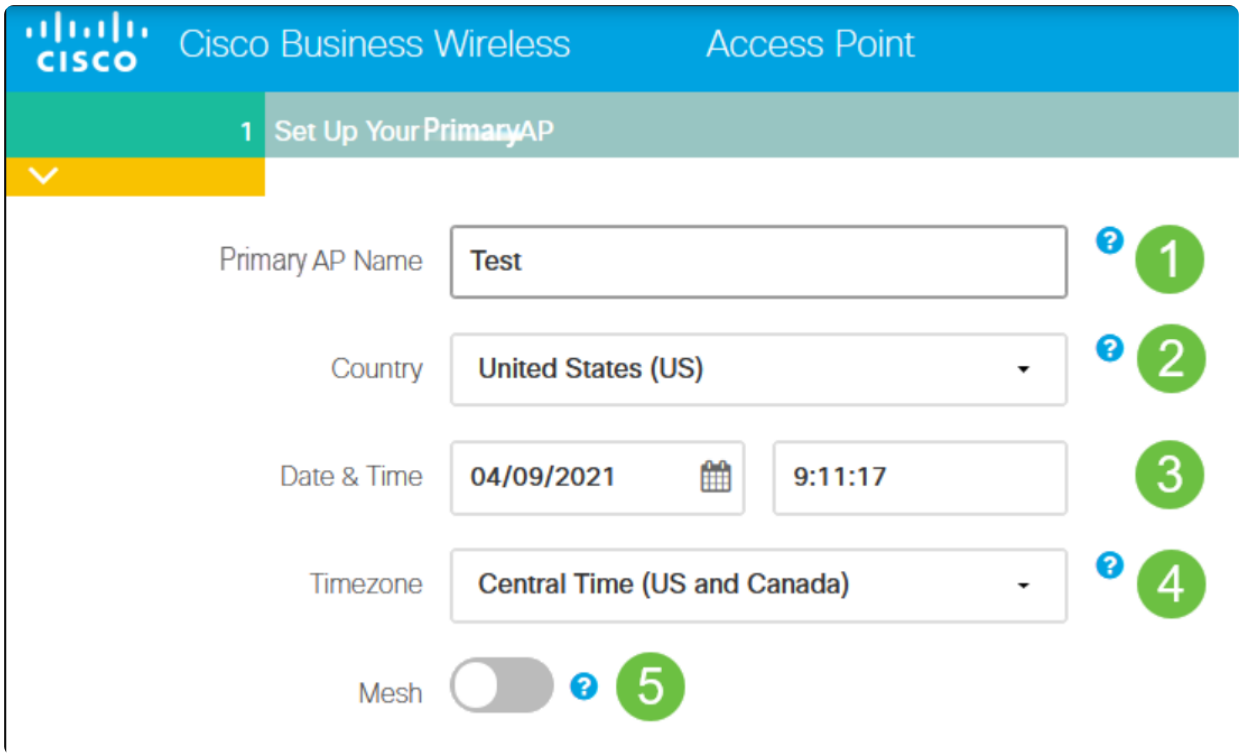
N'utilisez pas cisco, ni ses variantes dans les champs de nom d'utilisateur ou de mot de passe. Si vous le faites, vous obtiendrez un message d'erreur comme indiqué ci-dessous.



Étape 6

Configurez votre point d'accès principal en saisissant ce qui suit :

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



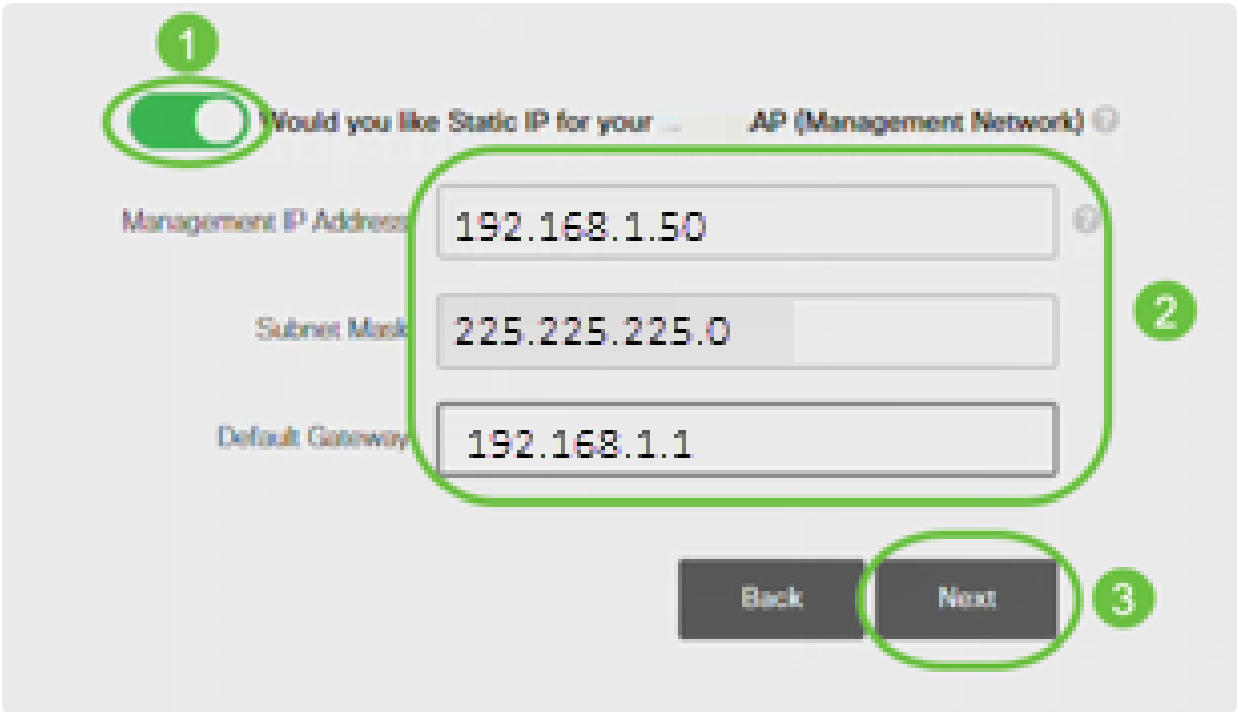
Le maillage ne doit être activé que si vous prévoyez de créer un réseau maillé. Par défaut, elle est désactivée.

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 les informations suivantes :

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

Cliquez sur Next (Suivant).



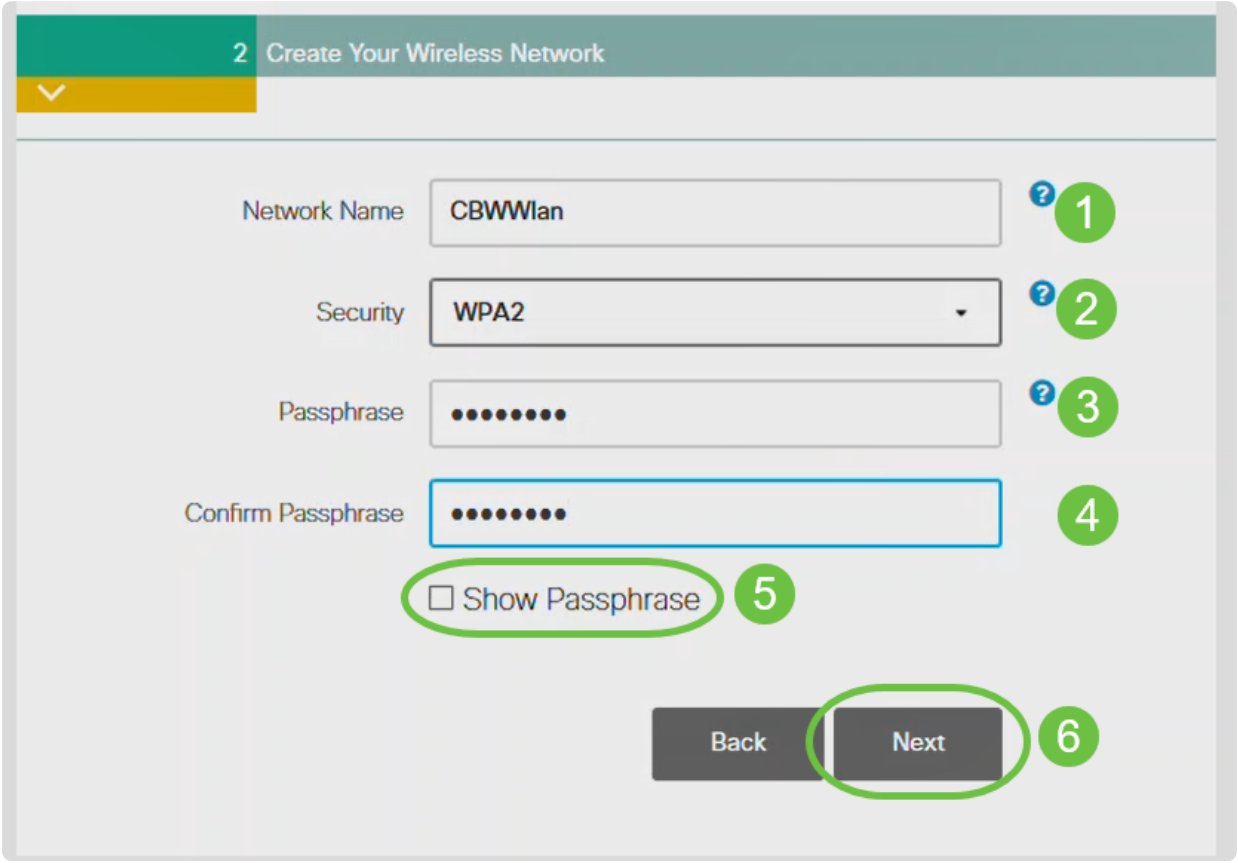
Par défaut, cette option est désactivée.

Étape 8

Créez vos réseaux sans fil en saisissant ce qui suit :

- Nom du réseau
- Choisir la sécurité
- Phrase De Passe
- Confirmer la phrase secrète
- (Facultatif) Cochez la case Afficher la phrase de passe.

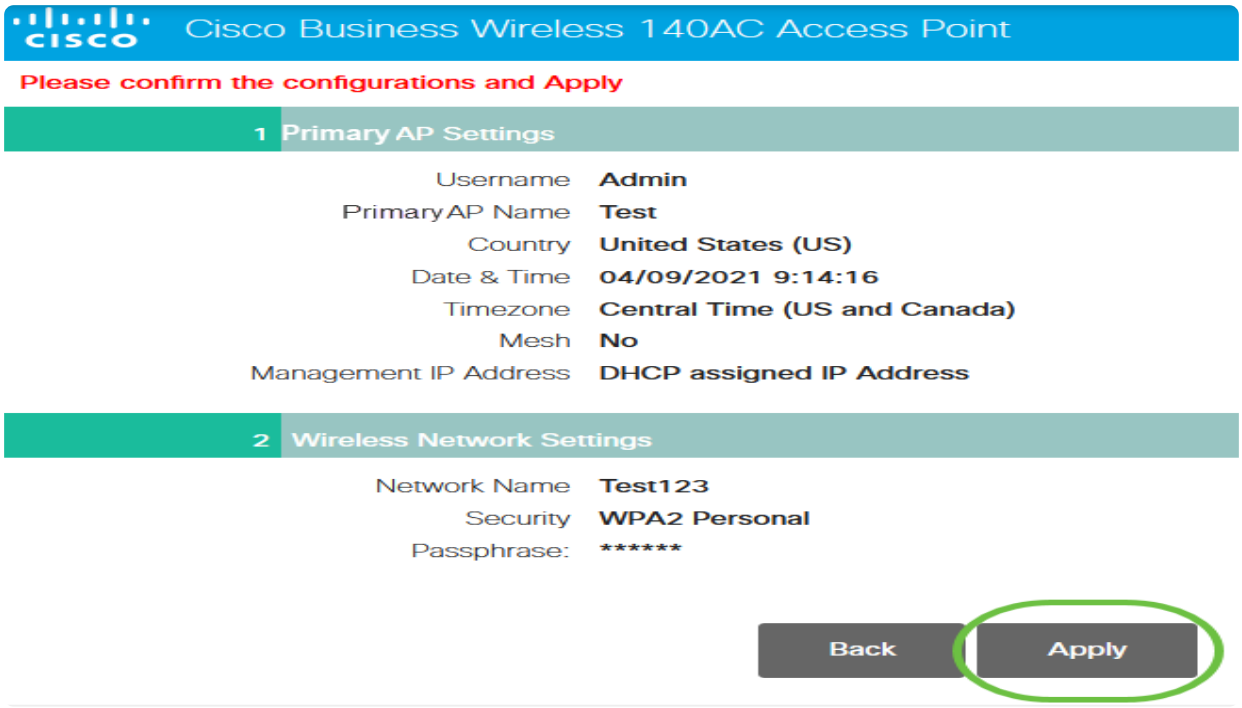
Cliquez sur Next (Suivant).



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

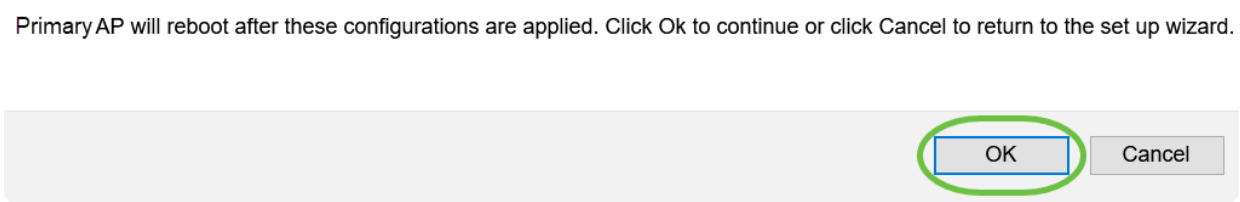
Étape 9

Confirmez les paramètres et cliquez sur Apply.

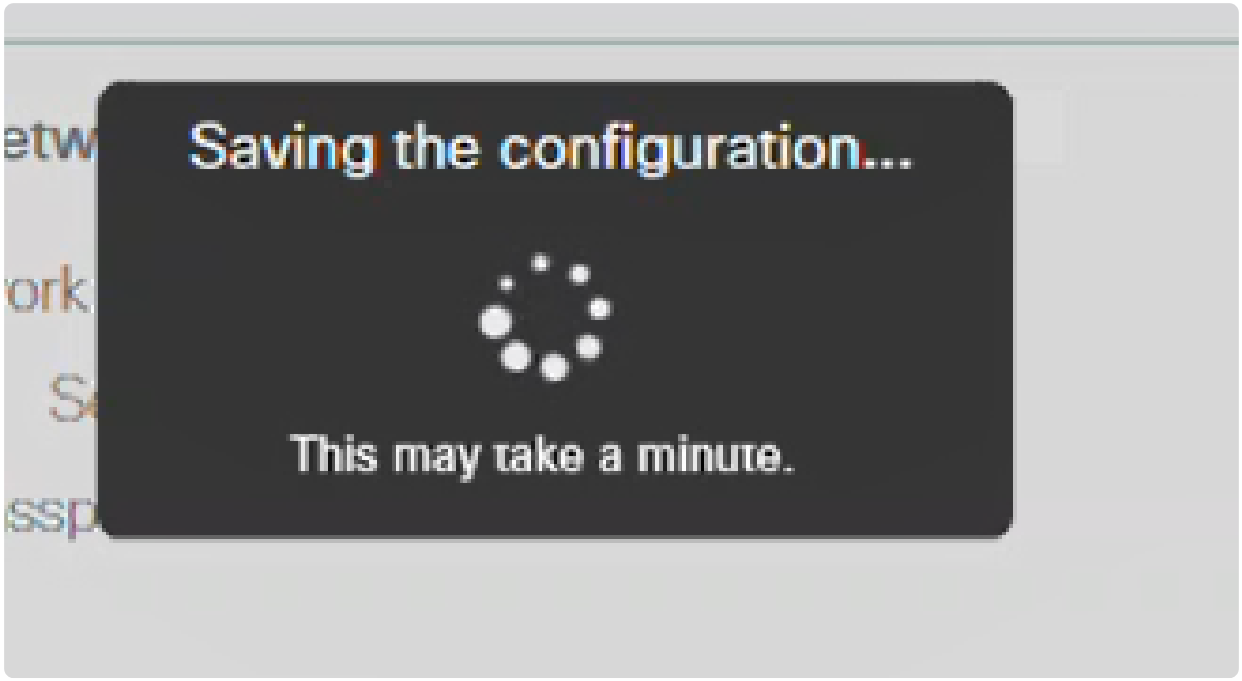


Étape 10

Cliquez sur OK pour appliquer les paramètres.



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

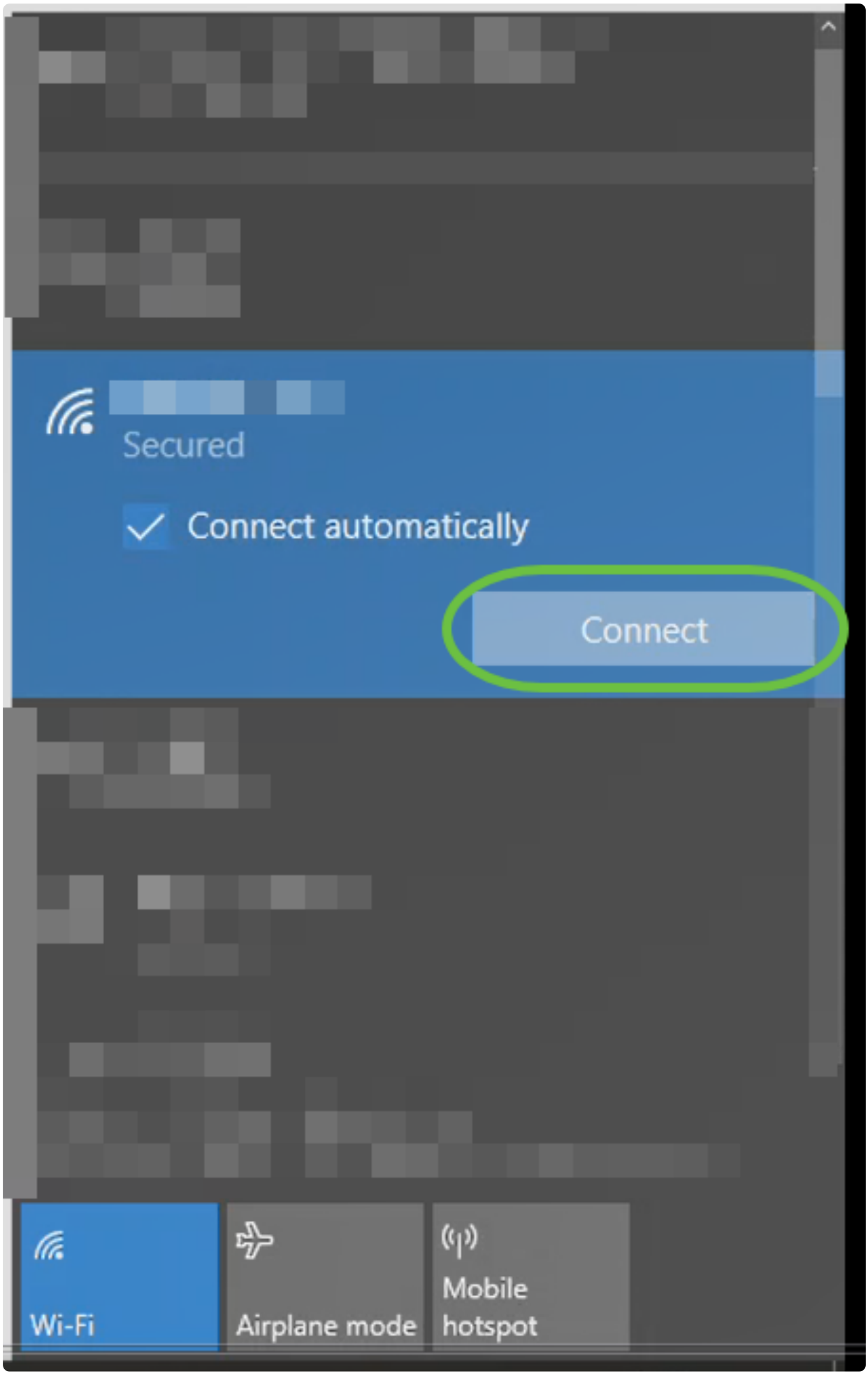


Au cours du redémarrage, le voyant du point d'accès passe par plusieurs modèles de couleurs. Lorsque le voyant est vert et clignote, passez à l'étape suivante. Si le voyant ne passe pas le modèle rouge clignotant, cela indique qu'il n'y a pas de serveur DHCP dans votre réseau. Assurez-vous que le point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

Étape 11

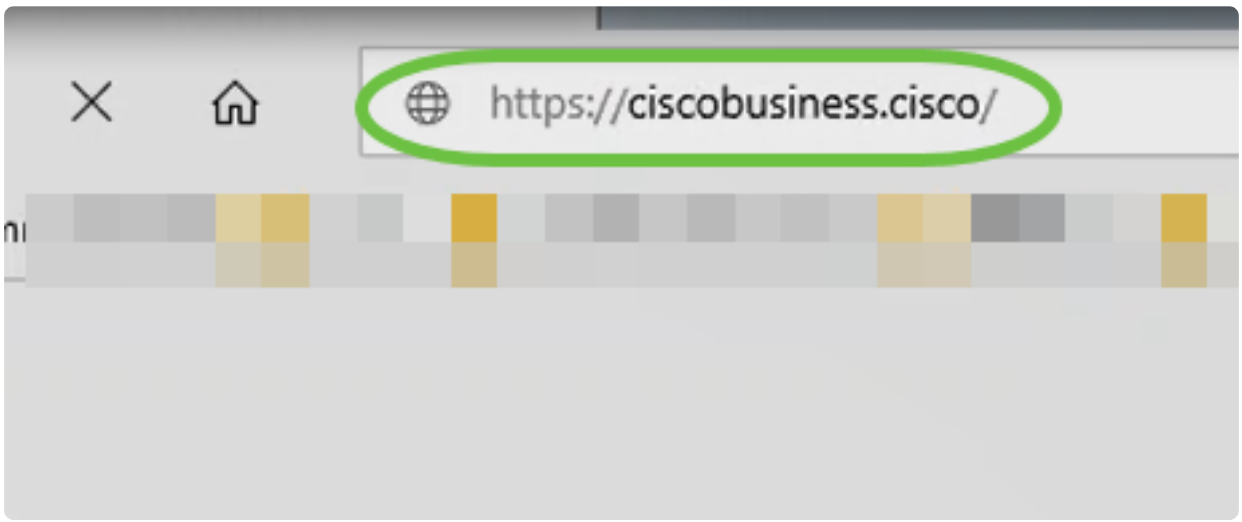
Accédez aux options sans fil de votre ordinateur et sélectionnez le réseau que vous avez configuré. Cliquez sur Connect.

Le SSID CiscoBusiness-Setup disparaît après le redémarrage.


Secured
Connect automatically
Connect
Wi-Fi
Airplane mode
Mobile hotspot

Étape 12

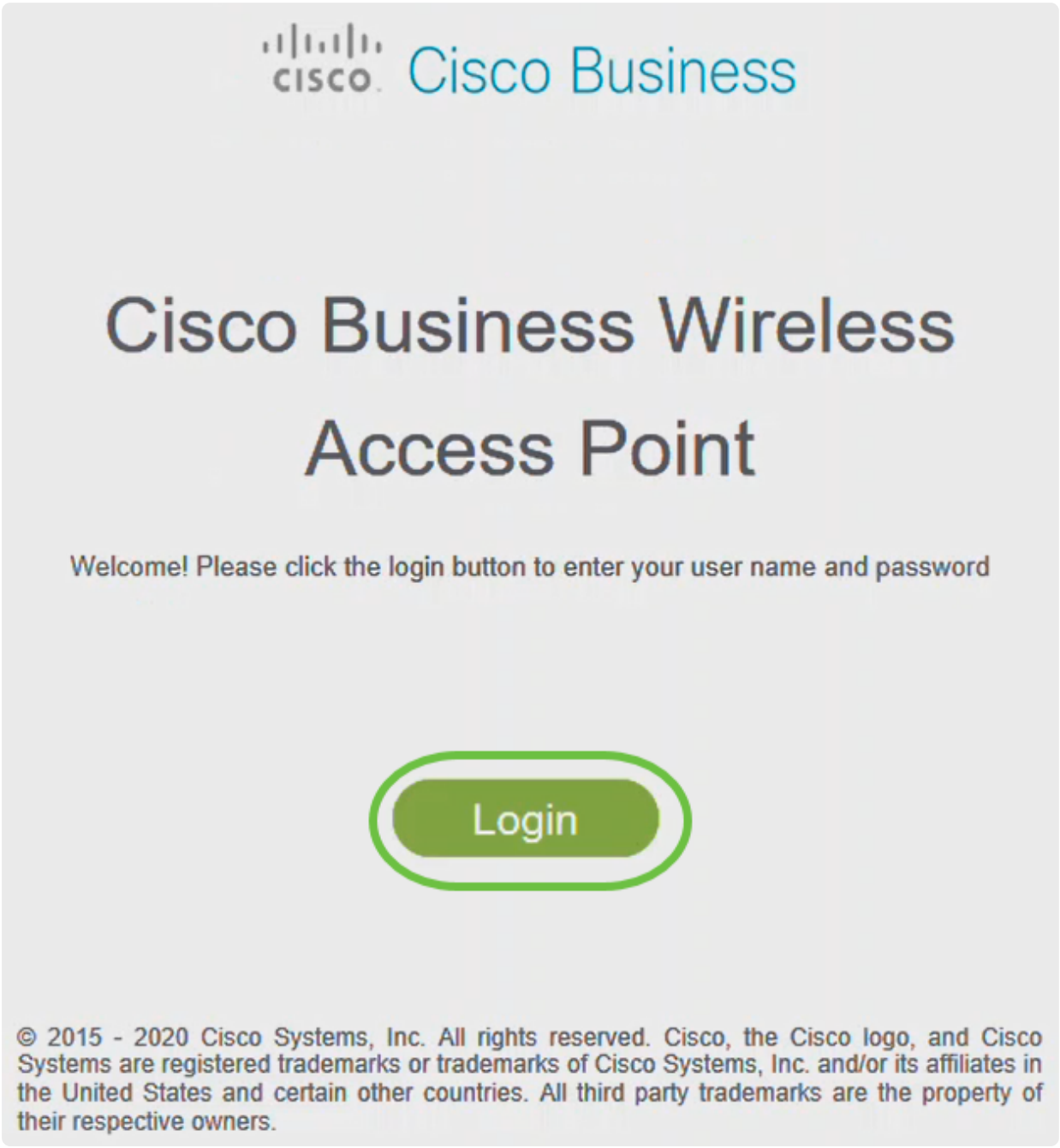
Ouvrez un navigateur Web et tapez https://[adresse IP du point d'accès CBW]. Vous pouvez également taper https://ciscobusiness.cisco dans la barre d'adresse et appuyer sur Entrée.



ⓘ Note: Assurez-vous que vous tapez https et non http à cette étape.

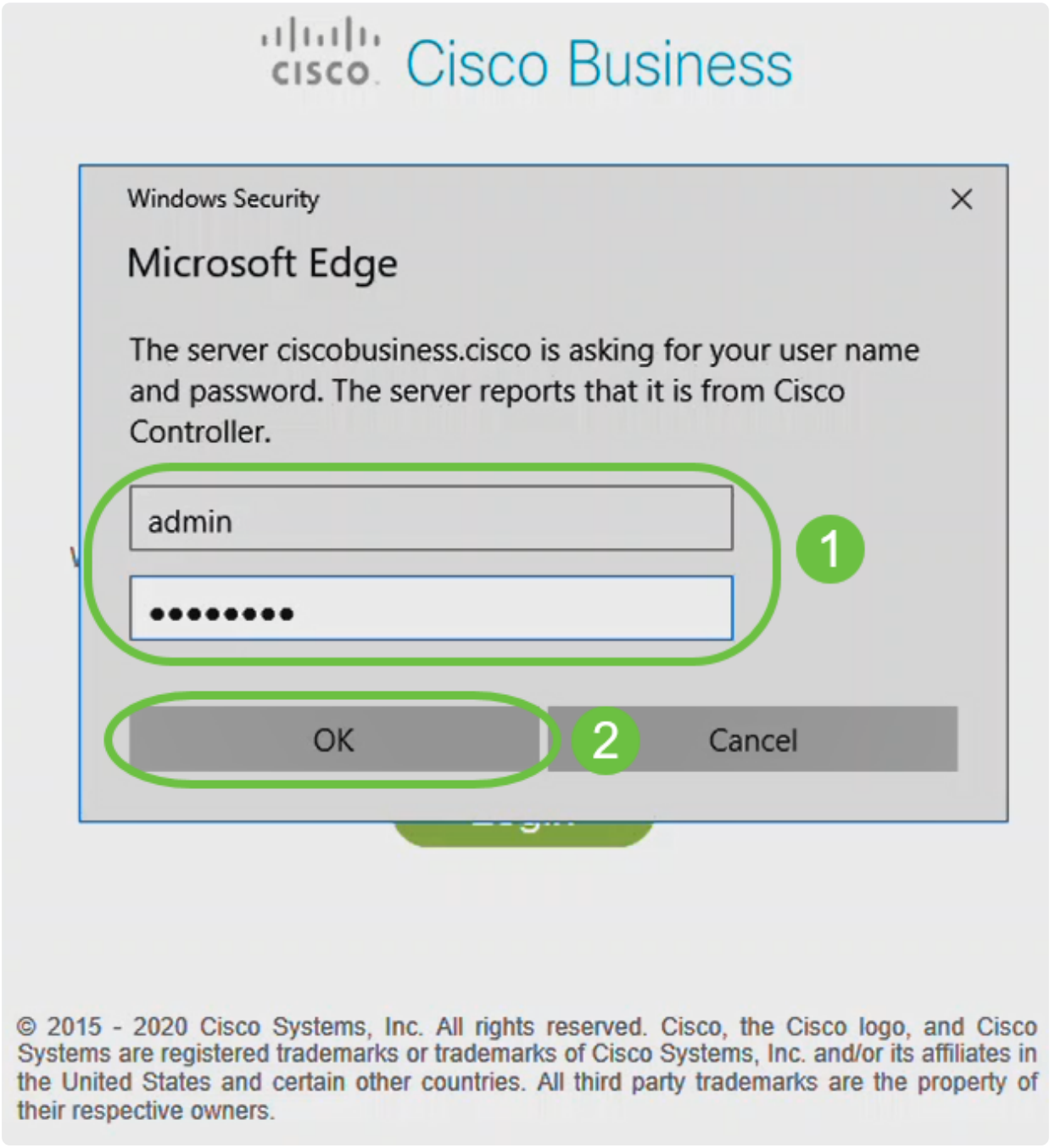
Étape 13

Cliquez sur Connexion.



Étape 14

Connectez-vous en utilisant les informations d'identification configurées. Click OK.



Étape 15

Vous pourrez accéder à la page de l'interface utilisateur Web 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. Il s'agit du 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 dispose d'un VPN intégré qui se connecte automatiquement sans notification. Cette option 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 que vous avez effectué la configuration initiale, assurez-vous que https:// is est utilisé si vous vous connectez à ciscobusiness.cisco ou en entrant l'adresse IP dans votre navigateur Web. En fonction de vos paramètres, votre ordinateur peut avoir été automatiquement renseigné avec http:// since, 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 utilisateur Web ou les problèmes de navigateur pendant l'utilisation de l'AP, dans le navigateur Web (Firefox dans ce cas) cliquez sur le menu Ouvrir, allez à Aide > Informations de dépannage et cliquez sur Actualiser Firefox.

Configuration des extendeurs de réseau maillé CBW142ACM à l'aide de l'interface utilisateur Web

Vous êtes dans la partie domestique de la configuration de ce réseau, il vous suffit d'ajouter vos extendeurs de maillage !

Étape 1

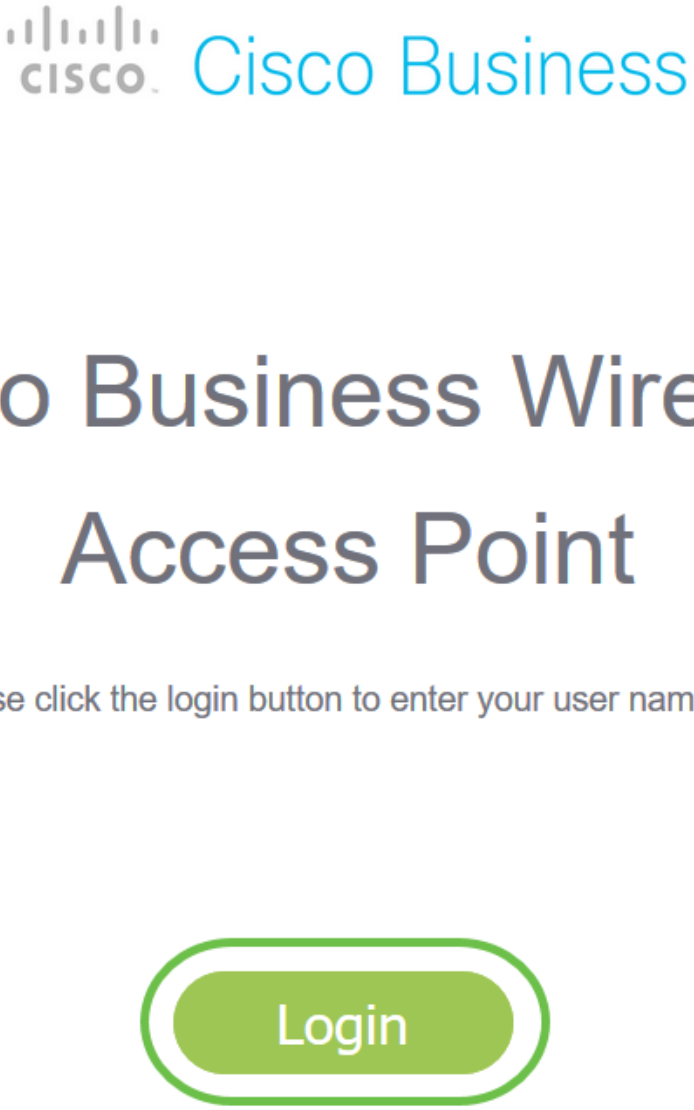
Branchez les deux extenseurs de maillage sur le mur aux emplacements sélectionnés. Notez l'adresse MAC de chaque extendeur de réseau maillé.

Étape 2

Attendez environ 10 minutes que les unités Mesh Extender démarrent.

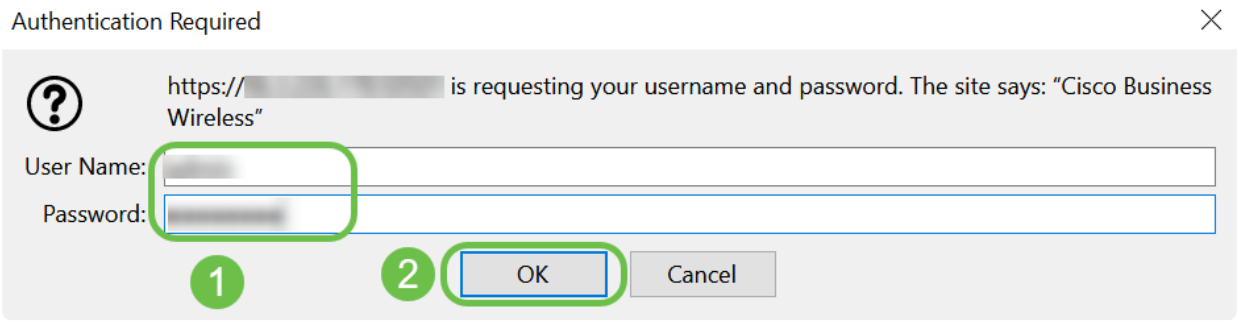
Étape 3

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



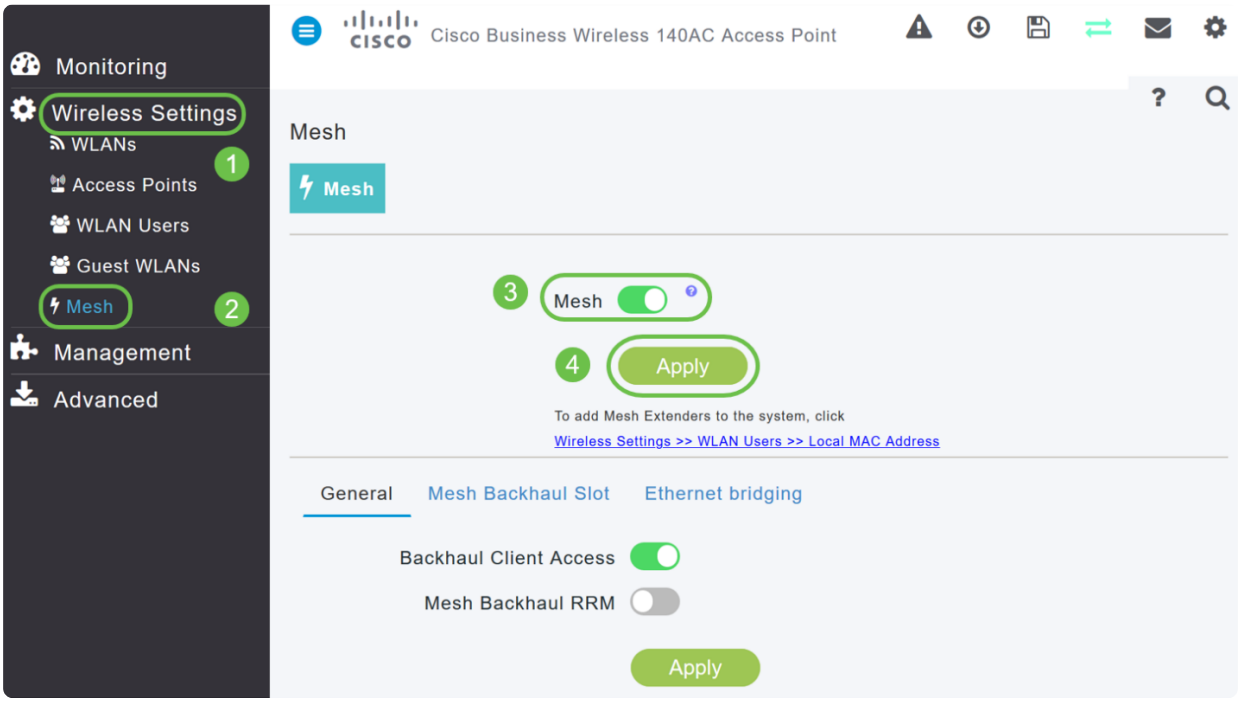
Étape 4

Entrez vos identifiants de nom d'utilisateur et de mot de passe 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.

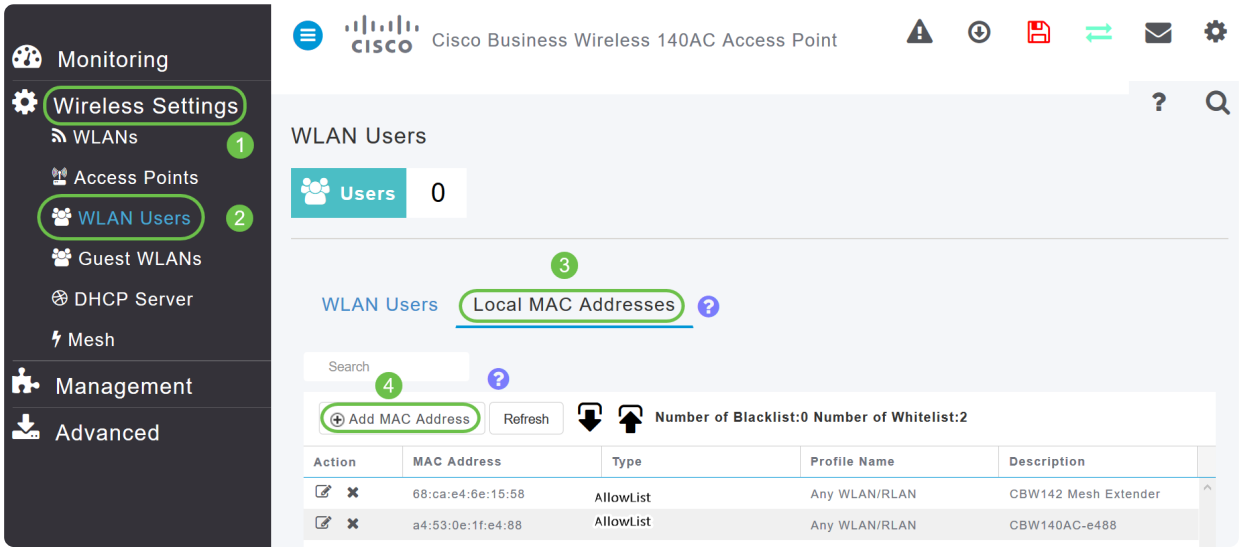


Étape 6

Si le maillage n'était pas déjà activé, le WAP devra peut-être effectuer un redémarrage. Une fenêtre contextuelle apparaît pour effectuer un redémarrage. Confirmer. Cela prendra environ 10 minutes. Lors d'un redémarrage, le voyant clignote en vert selon plusieurs schémas, alternant rapidement entre le vert, le rouge et l'orange avant de redevenir vert. Il peut y avoir de petites variations dans l'intensité et la teinte de la couleur des LED d'une unité à l'autre.

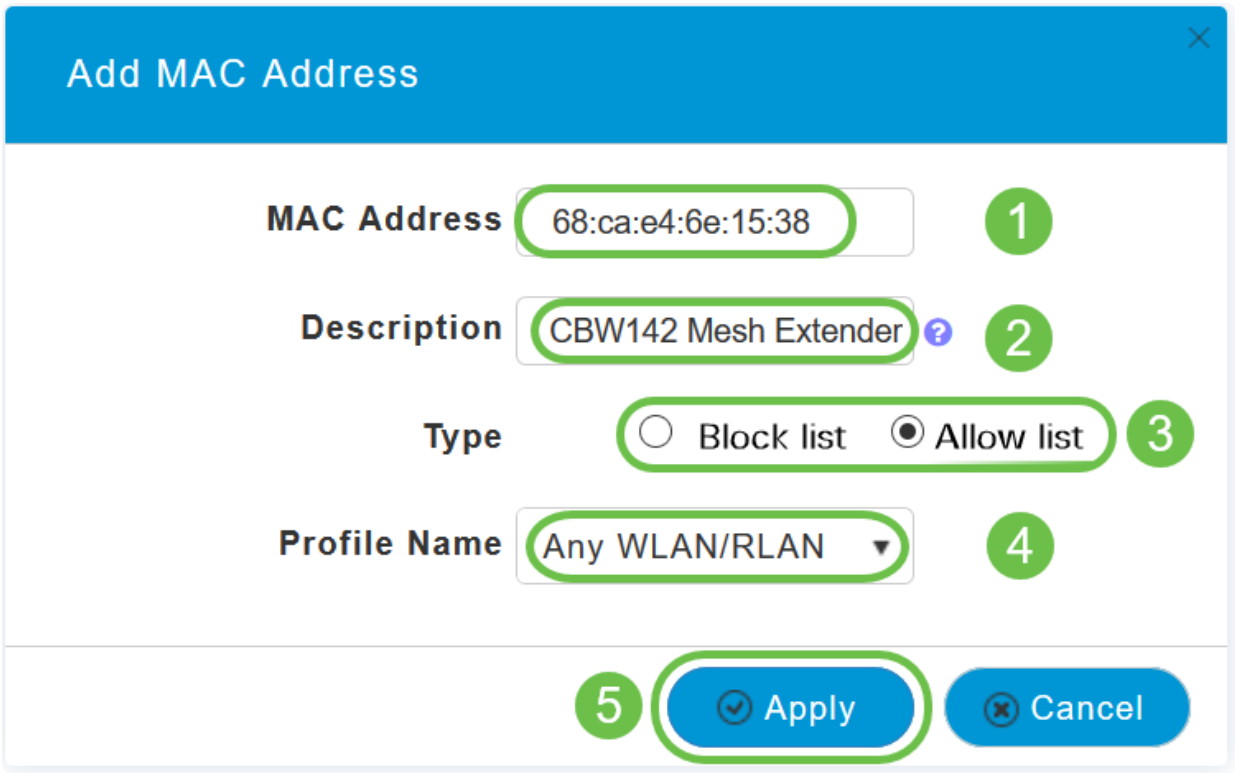
Étape 7

Accédez à Wireless Settings > WLAN Users > Local MAC Addresses. Cliquez sur Add MAC Address.



Étape 8

Saisissez l'adresse MAC et la description du périphérique Mesh Extender. Sélectionnez la liste Type autorisé. Sélectionnez le nom du profil dans le menu déroulant. Cliquez sur Apply.



Étape 9

Assurez-vous d'enregistrer toutes vos configurations en appuyant sur l'icône d'enregistrement sur le volet supérieur droit de l'écran.



Répétez l' pour chaque extendeur de maillage.

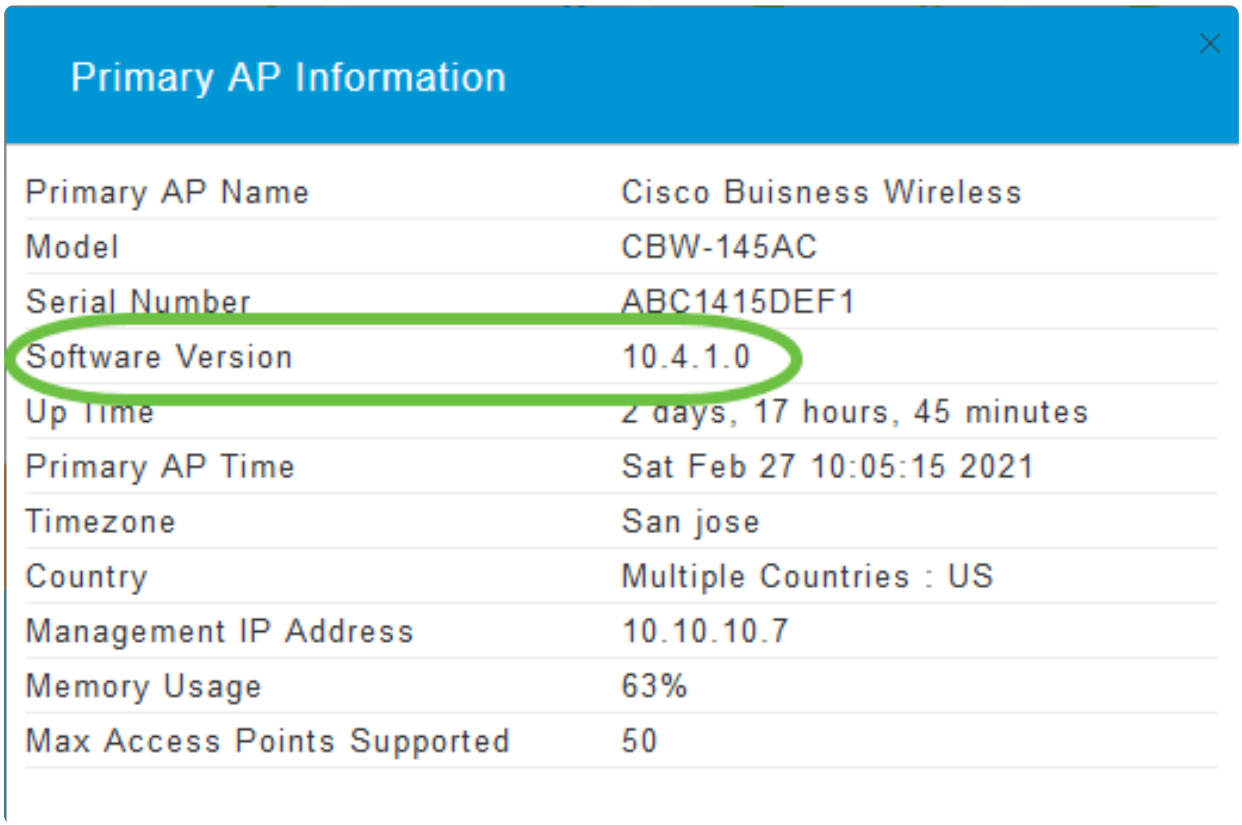
Vérifier et mettre à jour le logiciel via l'interface utilisateur Web

Ne passez pas à côté de cette étape importante ! Il existe quelques méthodes de mise à jour du logiciel, mais les étapes ci-dessous sont recommandées comme étant les plus simples 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.

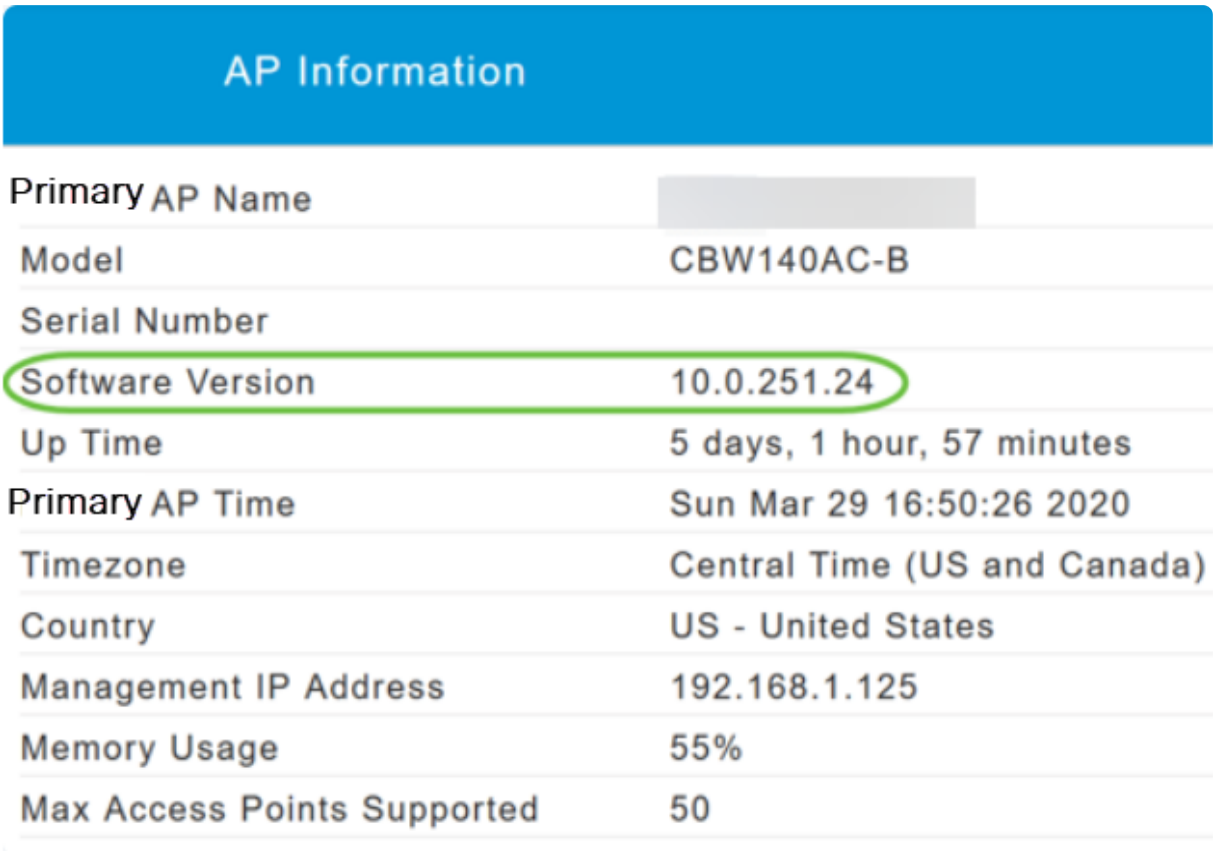
Étape 1

Cliquez sur l'icône de roue dentée dans le coin supérieur droit de l'interface Web, puis cliquez sur Informations sur le point d'accès principal.



Étape 2

Comparez la version en cours d'exécution à la dernière version du logiciel. Fermez la fenêtre lorsque vous savez si vous devez mettre à jour le logiciel.

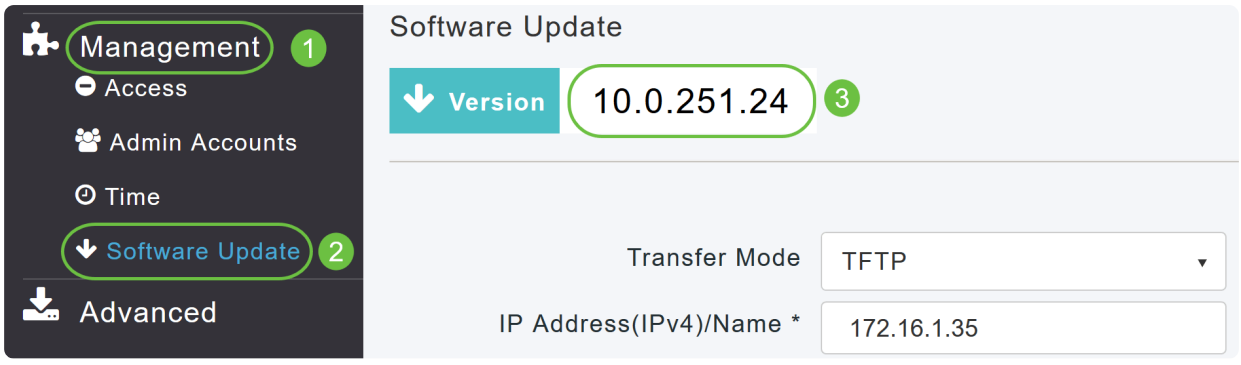


Si vous exécutez la dernière version du logiciel, vous pouvez passer à la section Create WLANs.

Étape 3

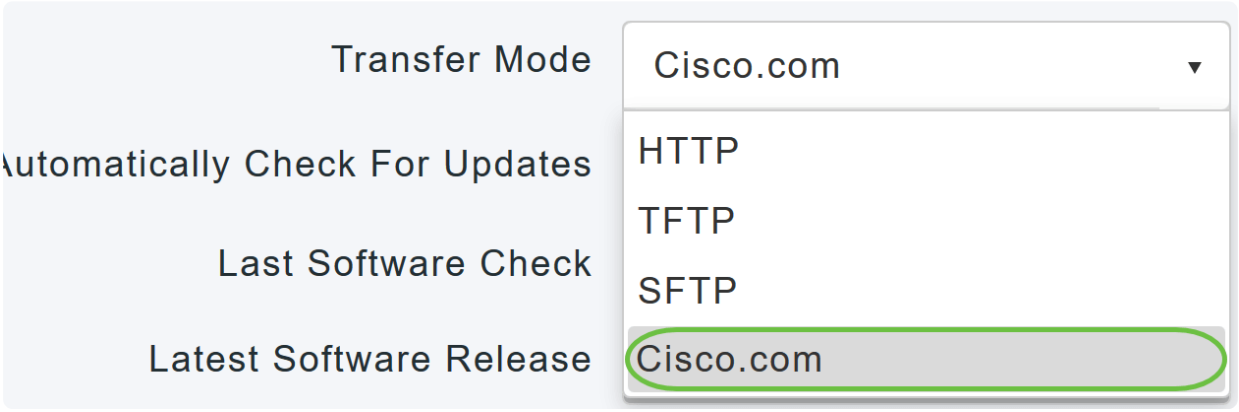
Choisissez Management > Software Update dans le menu.

La fenêtre Software Update s'affiche avec le numéro de version actuelle du logiciel répertorié en haut.



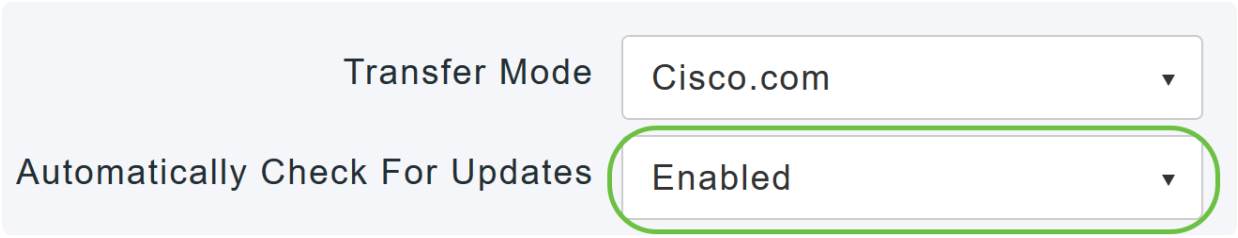
Vous pouvez mettre à jour le logiciel CBW AP et les configurations actuelles sur le point d'accès principal ne seront pas supprimées.

Dans la liste déroulante Transfer Mode, sélectionnez Cisco.com.



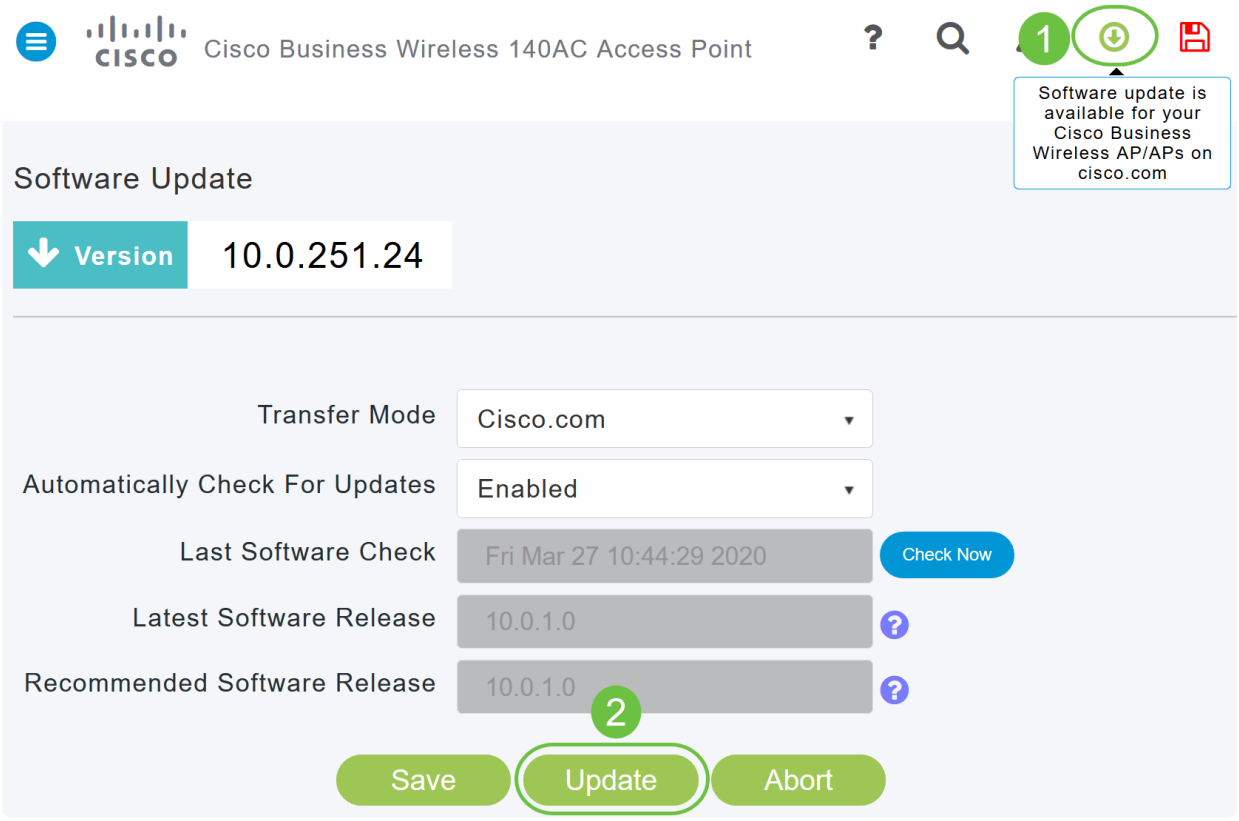
Étape 4

Pour configurer le point d'accès principal pour qu'il vérifie automatiquement les mises à jour logicielles, sélectionnez Enabled dans la liste déroulante Automatically Check for Updates. Ceci est activé par défaut.



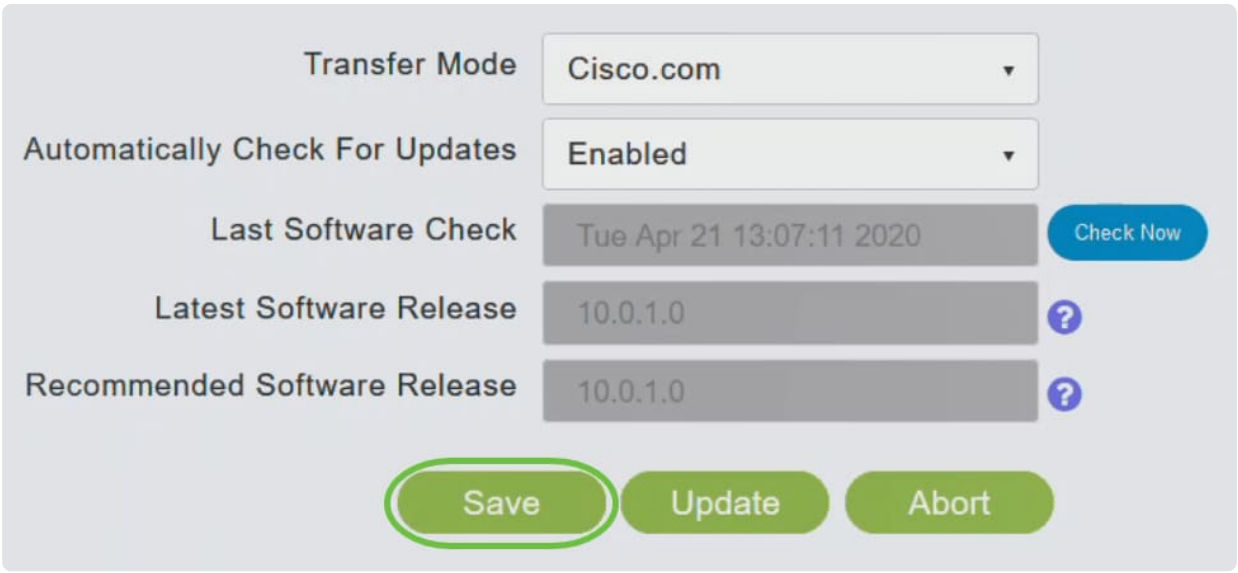
Lorsqu'une vérification logicielle est effectuée et qu'une mise à jour logicielle plus récente ou recommandée est disponible sur Cisco.com, alors :

- L'icône Alerte de mise à jour logicielle dans le coin supérieur droit de l'interface utilisateur Web sera verte (ou grise). Cliquez sur l'icône pour accéder à la page Software Update.
- Le bouton Mettre à jour situé au bas de la page Mise à jour logicielle est activé.

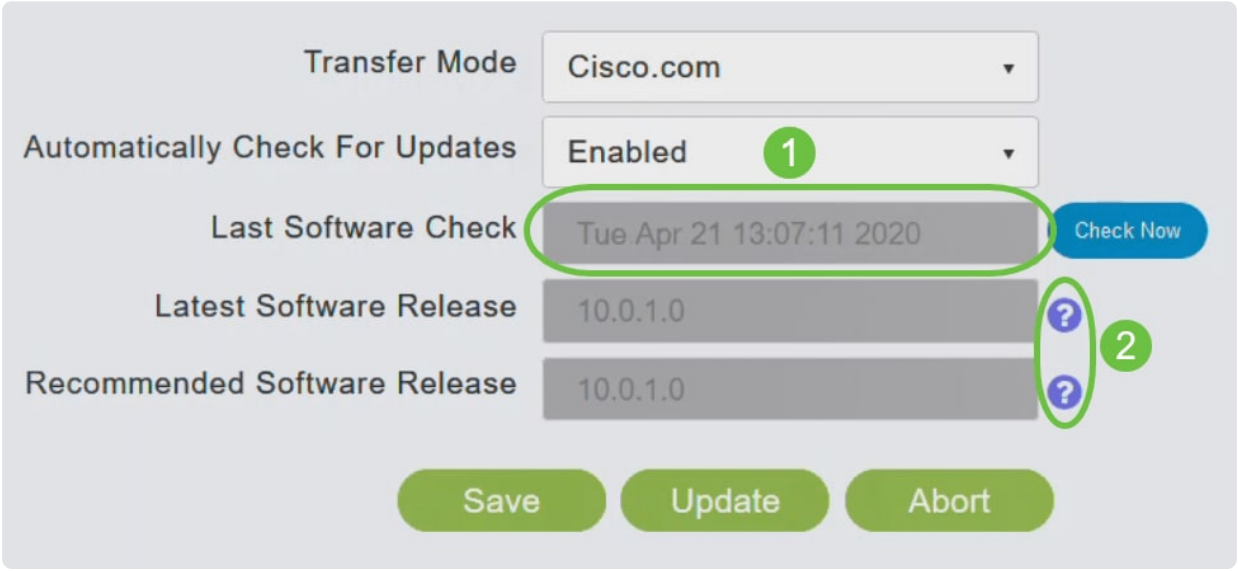


Étape 5

Cliquez sur Save. Cette opération enregistre les entrées ou les modifications que vous avez effectuées en mode Transfert et en mode Rechercher automatiquement les mises à jour.

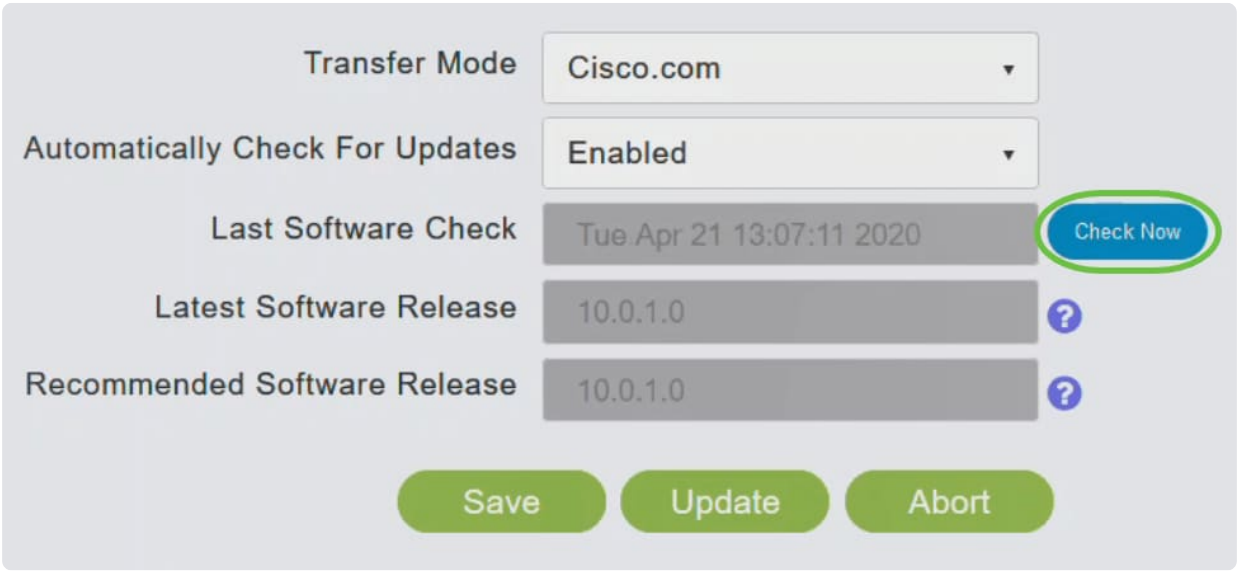


Le champ Dernière vérification logicielle affiche l'horodatage de la dernière vérification logicielle automatique ou manuelle. Vous pouvez afficher les notes des versions affichées en cliquant sur l'icône en forme de point d'interrogation située en regard.



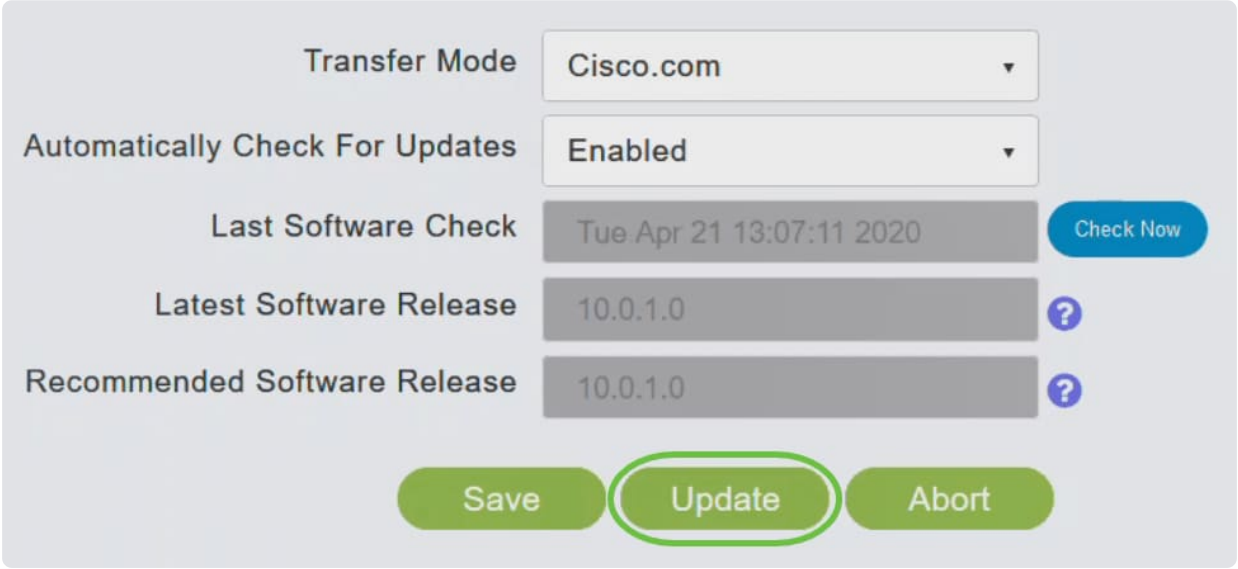
Étape 6

Vous pouvez exécuter manuellement une vérification du logiciel à tout moment en cliquant sur Vérifier maintenant.



Étape 7

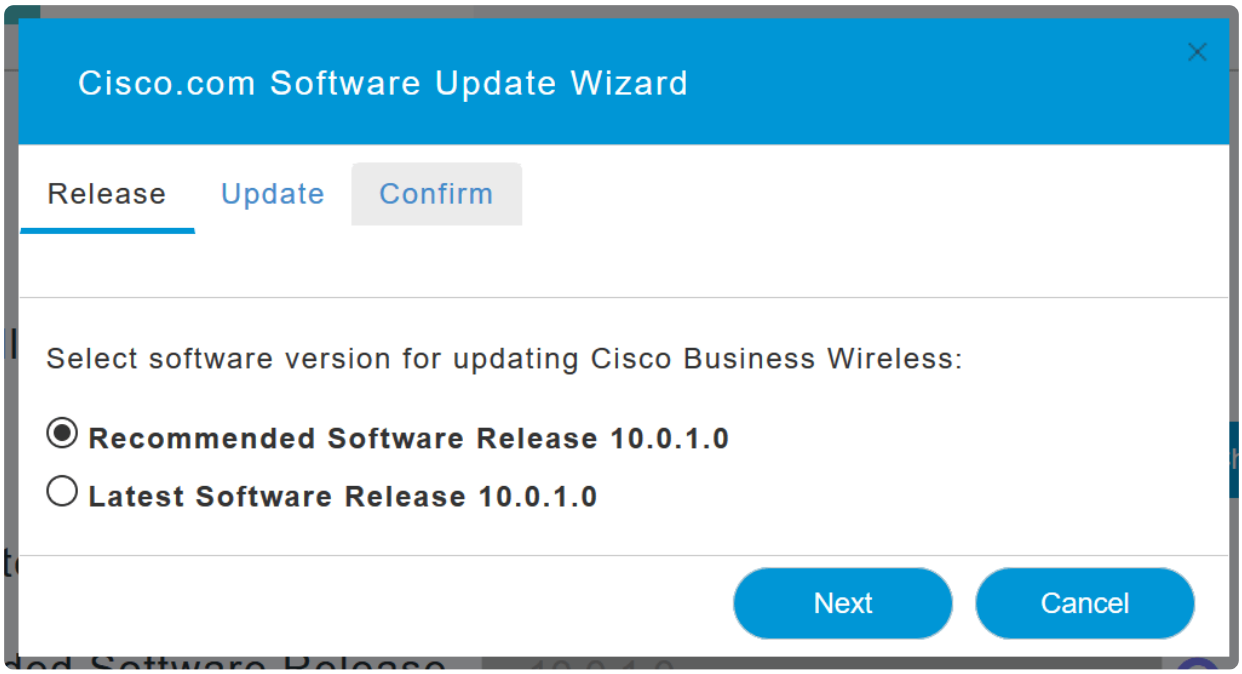
Pour poursuivre la mise à jour logicielle, cliquez sur Update.



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

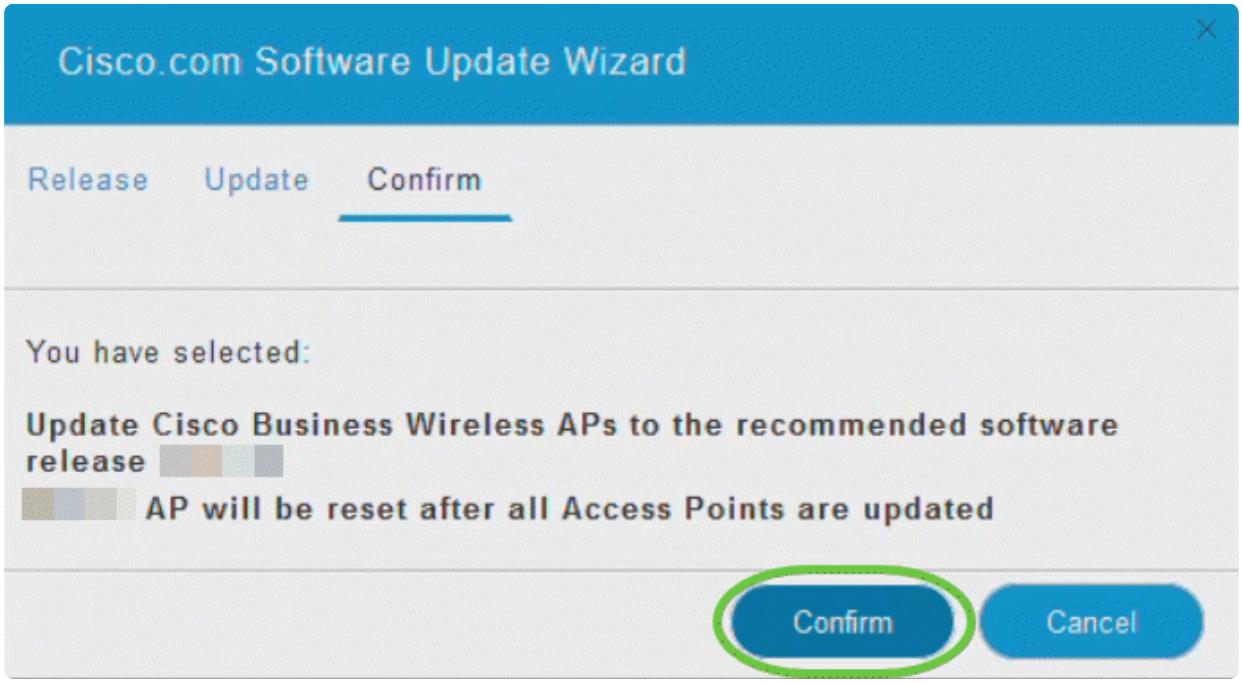
- Onglet Release (Version) : indiquez si vous souhaitez effectuer une mise à jour vers la version logicielle recommandée ou la dernière version logicielle.
- Onglet Mise à jour - Spécifiez quand les points d'accès doivent être réinitialisés. Vous pouvez choisir de le faire immédiatement ou de le programmer pour une heure ultérieure. 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 - Confirmez 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 sélectionnant Wireless Settings > WLANs. Sélectionnez ensuite Add new WLAN/RLAN.



Étape 2

Sous l'onglet General, saisissez les informations suivantes :

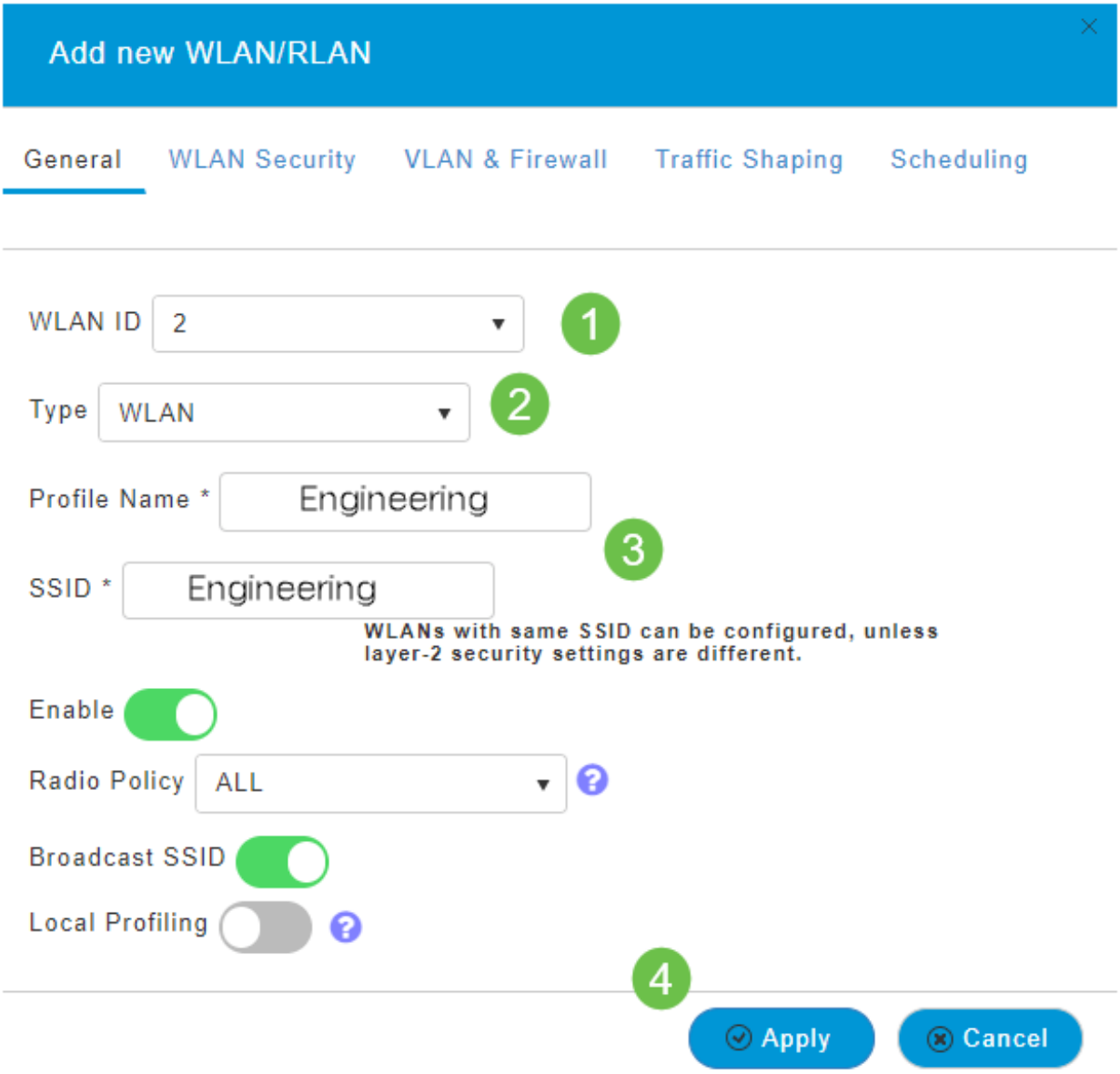
- WLAN ID : sélectionnez un numéro pour le WLAN
- Type : sélectionnez WLAN
- Profile Name (Nom du profil) : lorsque vous entrez un nom, le SSID est automatiquement renseigné avec le même nom. Le nom doit être unique et ne doit pas dépasser 31 caractères.

Les champs suivants ont été conservés comme champs par défaut dans cet exemple, mais des explications sont répertoriées au cas où vous souhaiteriez les configurer différemment.

- SSID : le nom du profil fait également office de SSID. Vous pouvez changer cela si vous le souhaitez. Le nom doit être unique et ne doit pas dépasser 31 caractères.

- Enable (Activer) : cette option doit rester activée pour que le réseau local sans fil fonctionne.
- Politique radio : en règle générale, vous devez choisir All pour que les clients 2,4 GHz et 5 GHz puissent accéder au réseau.
- Broadcast SSID (SSID de diffusion) : vous souhaitez généralement que le SSID soit découvert afin de le laisser activé.
- Profilage local : vous devez uniquement activer cette option pour afficher le système d'exploitation exécuté sur le client ou pour afficher le nom d'utilisateur.

Cliquez sur Apply.



Étape 3

Vous accédez à l'onglet WLAN Security (Sécurité WLAN).

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

- Le réseau invité, l'assistant réseau captif et le filtrage MAC sont restés 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) - ASCII. Cette option correspond à Wi-Fi Protected Access 2 avec clé prépartagée (PSK).

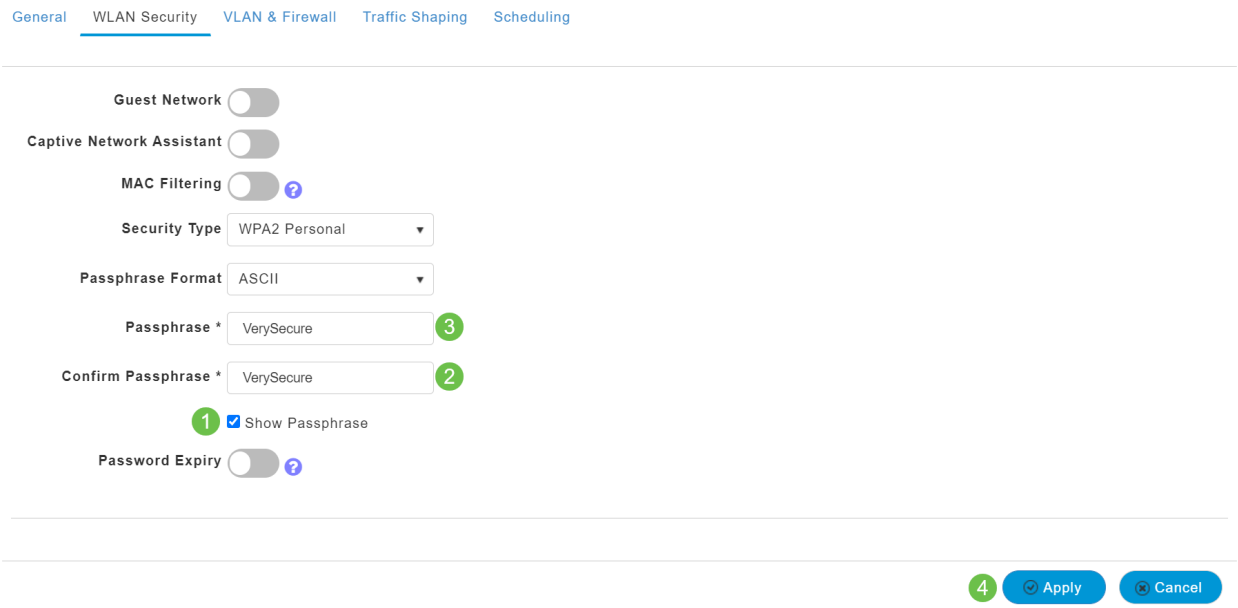
WPA2 Personal (WPA2 personnel) est une méthode utilisée pour sécuriser votre réseau à l'aide d'une authentification PSK. La clé PSK est configurée séparément sur le point d'accès principal, sous la stratégie de sécurité WLAN, et sur le client. WPA2 Personal (WPA2 personnel) ne dépend pas d'un serveur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

- Format de la phrase de passe : ASCII est conservé par défaut.

Les champs suivants ont été saisis dans ce scénario :

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

Cliquez sur Apply. Cette opération active automatiquement le nouveau WLAN.



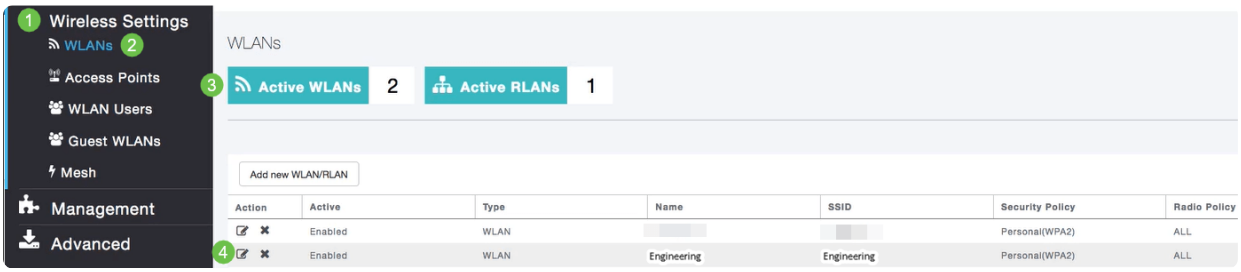
Étape 4

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



Étape 5

Pour afficher le WLAN que vous avez créé, sélectionnez Wireless Settings > WLANs. Vous verrez le nombre de WLAN actifs élevé à 2, et le nouveau WLAN s'affiche.



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

Configurations sans fil en option

Toutes les configurations de base sont désormais définies et prêtes à être déployées. 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 d'application (facultatif)
- Profilage client (facultatif)
- Je suis prêt à conclure et à commencer à utiliser mon réseau !

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

Un WLAN invité donne accès à votre réseau sans fil professionnel Cisco.

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 sélectionnant Wireless Settings > WLANs. Sélectionnez ensuite Add new WLAN/RLAN.



Étape 3

Sous l'onglet General, 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.

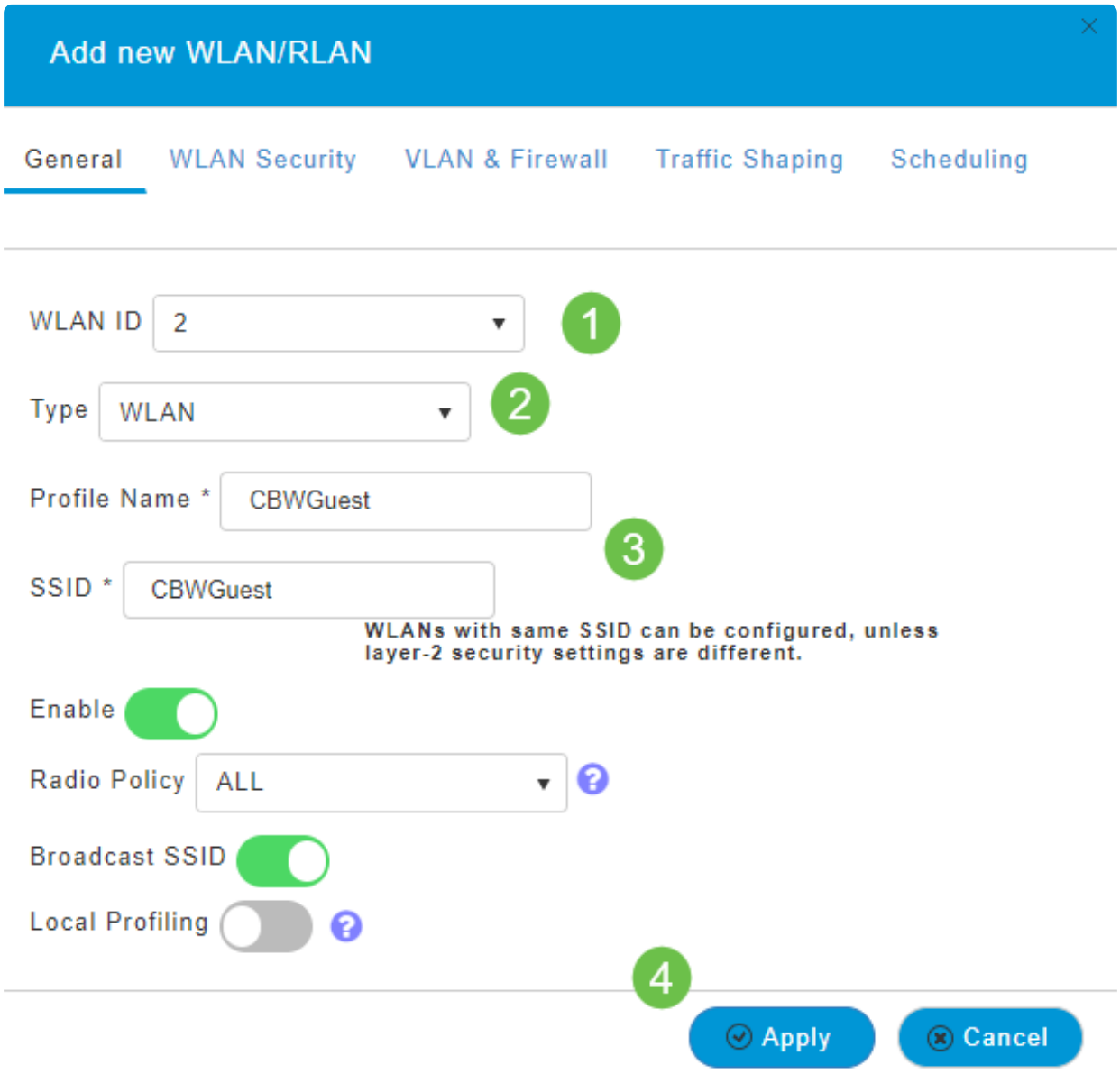
Les champs suivants ont été conservés comme champs par défaut dans cet exemple, mais des explications sont répertoriées au cas où vous souhaiteriez les configurer différemment.

- SSID : le nom du profil agit également comme SSID. Vous pouvez changer cela si vous le souhaitez. Le nom doit être unique et ne doit pas dépasser 31 caractères.
- Enable : cette option doit rester activée pour que le réseau local sans fil fonctionne.
- Politique radio - En règle générale, vous souhaitez conserver la valeur All (Tous) afin que les clients 2,4 GHz et 5 GHz puissent accéder au réseau.
- Broadcast SSID : vous souhaitez généralement que le SSID soit découvert afin de le

laisser comme Enabled.

- Profilage local : vous ne souhaitez activer cette option que pour afficher le système d'exploitation exécuté sur le client ou pour afficher le nom d'utilisateur.

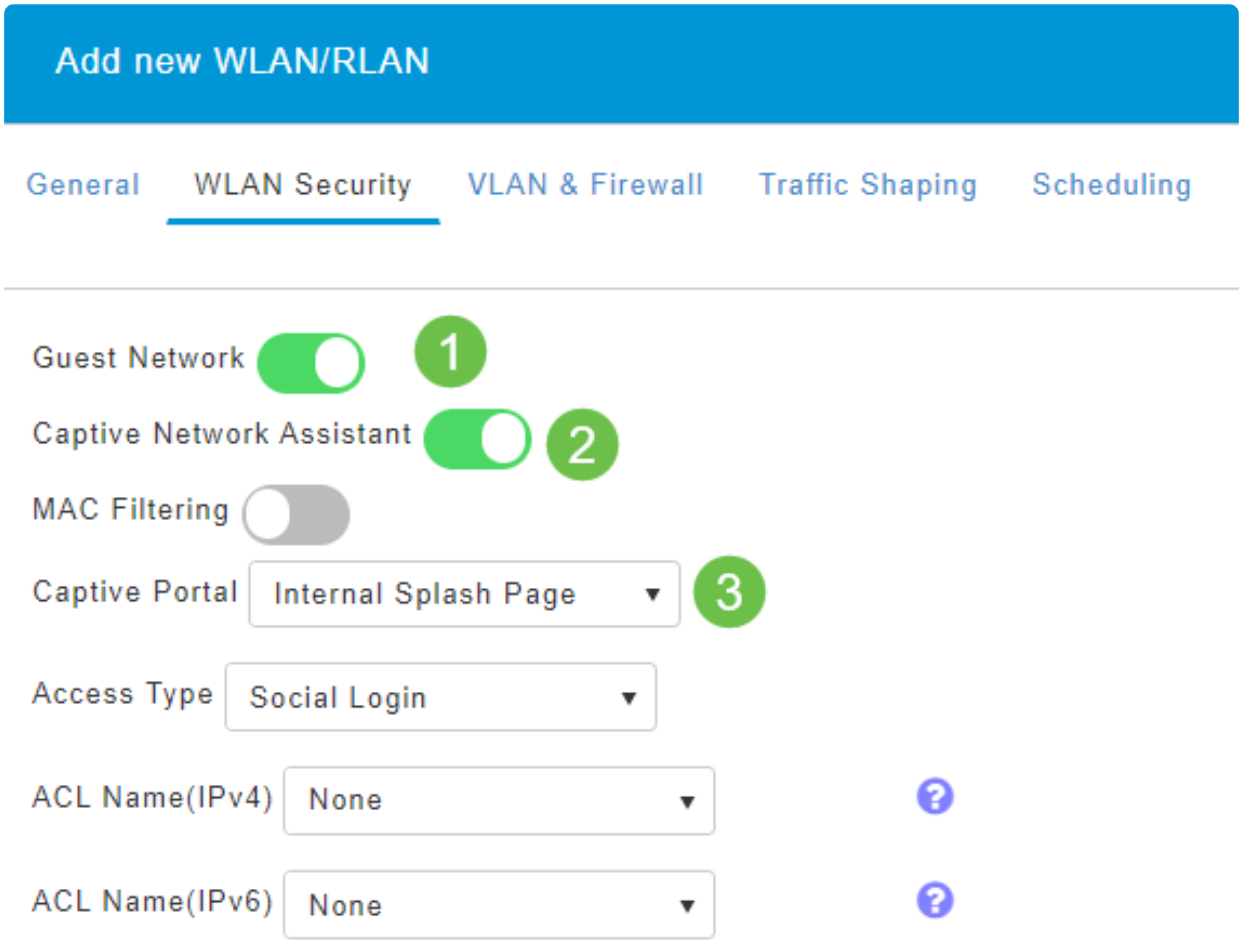
Cliquez sur Apply.



Étape 4

Vous accédez à l'onglet WLAN Security (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 activer cette fonction. Cette fonctionnalité détecte la présence d'un portail captif en envoyant une requête Web lors de la connexion à un réseau sans fil. Cette demande est adressée à un Uniform Resource Locator (URL) pour les modèles d'iPhone et si une réponse est reçue, l'accès Internet est supposé disponible et aucune autre interaction n'est requise. Si aucune réponse n'est reçue, l'accès à Internet est alors supposé 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. Le CNA peut se rompre lors de la redirection vers un portail captif ISE (Identity Services Engine). Le point d'accès principal empêche ce pseudo-navigateur de s'afficher.
- Portail captif : ce champ n'est visible que lorsque l'option Réseau invité est activée. Permet de spécifier le type de portail Web pouvant être utilisé à des fins d'authentification. Sélectionnez Internal Splash Page (Page d'accueil interne) pour utiliser l'authentification par défaut basée sur le portail Web Cisco. Sélectionnez External Splash Page (Page d'accueil externe) si vous souhaitez utiliser une authentification de portail captive à l'aide d'un serveur Web externe à 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 Social login activé sera créé. Une fois que l'utilisateur se connecte à ce WLAN invité, il est redirigé vers la page de connexion par défaut de Cisco où il peut trouver les boutons de connexion pour Google et Facebook. L'utilisateur peut se connecter à l'aide de son compte Google ou Facebook pour accéder à Internet.

Étape 5

Dans le même onglet, sélectionnez un type d'accès dans le menu déroulant. Dans cet exemple, Social Login a été sélectionné. Il s'agit de l'option qui permet aux invités d'utiliser leurs identifiants Google ou Facebook pour s'authentifier et accéder au réseau.

Les autres options du type d'accès sont les suivantes :

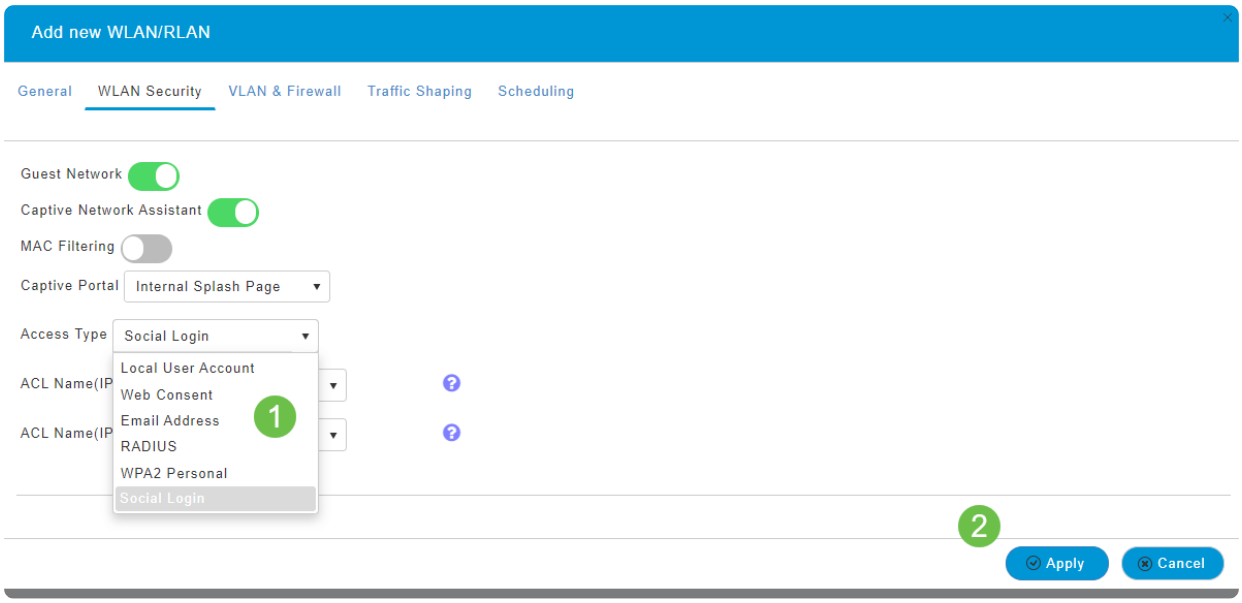
- Local User Account - Option par défaut. Choisissez cette option pour authentifier les invités en utilisant le nom d'utilisateur et le mot de passe que vous pouvez spécifier pour les utilisateurs invités de ce WLAN, sous Paramètres sans fil > Utilisateurs WLAN. Voici un exemple de la page de démarrage interne par défaut.



Vous pouvez personnaliser ceci en naviguant à Wireless Settings > Guest WLANs. À partir de là, vous pouvez saisir un titre de page 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 et 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

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



Vous venez de créer un réseau invité disponible sur votre réseau CBW. Vos invités apprécieront la commodité.

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

Le profilage est un sous-ensemble de fonctionnalités qui permettent de mettre en oeuvre une stratégie organisationnelle. Il vous permet de faire correspondre et de hiérarchiser les types de trafic. Comme les règles prennent des décisions sur la façon de classer ou d'abandonner le trafic. Le système sans fil Cisco Business Mesh permet le profilage des applications et des clients. L'accès à un réseau en tant qu'utilisateur commence par de nombreux échanges d'informations, dont le type de trafic. La politique interrompt le flux de trafic pour diriger le chemin, tout comme un organigramme. D'autres types de fonctionnalités de stratégie incluent l'accès invité, les listes de contrôle d'accès et la QoS.

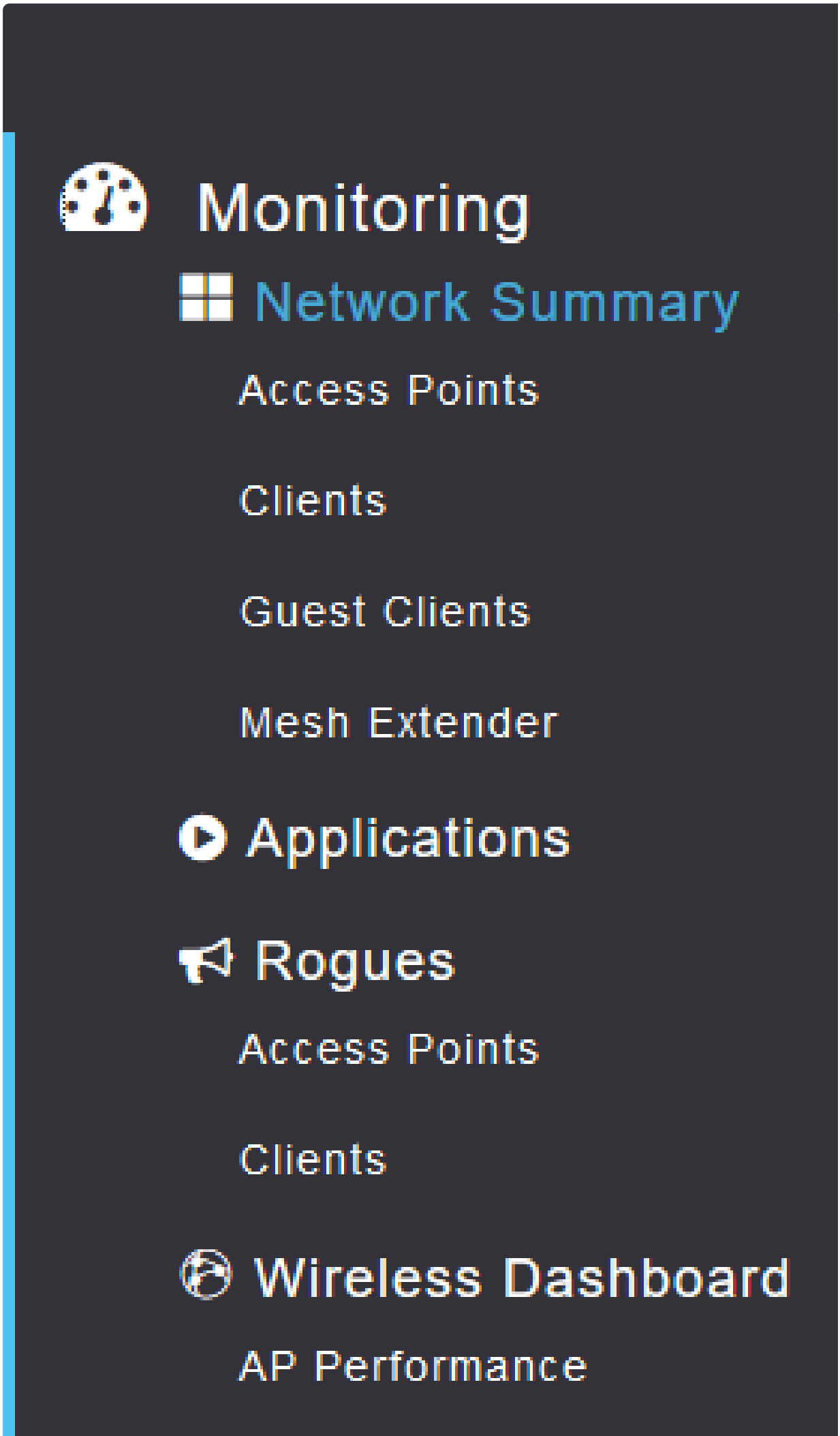
Étape 1

Naviguez jusqu'au menu situé à gauche de l'écran si la barre de menus de gauche n'apparaît pas.

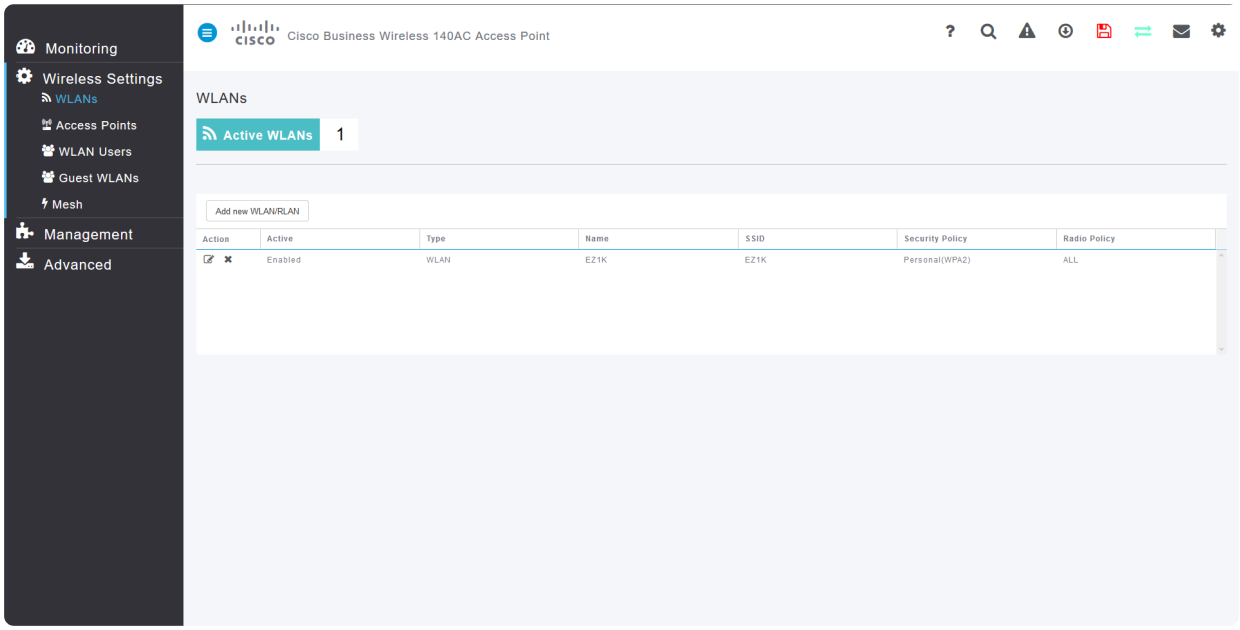


Étape 2

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

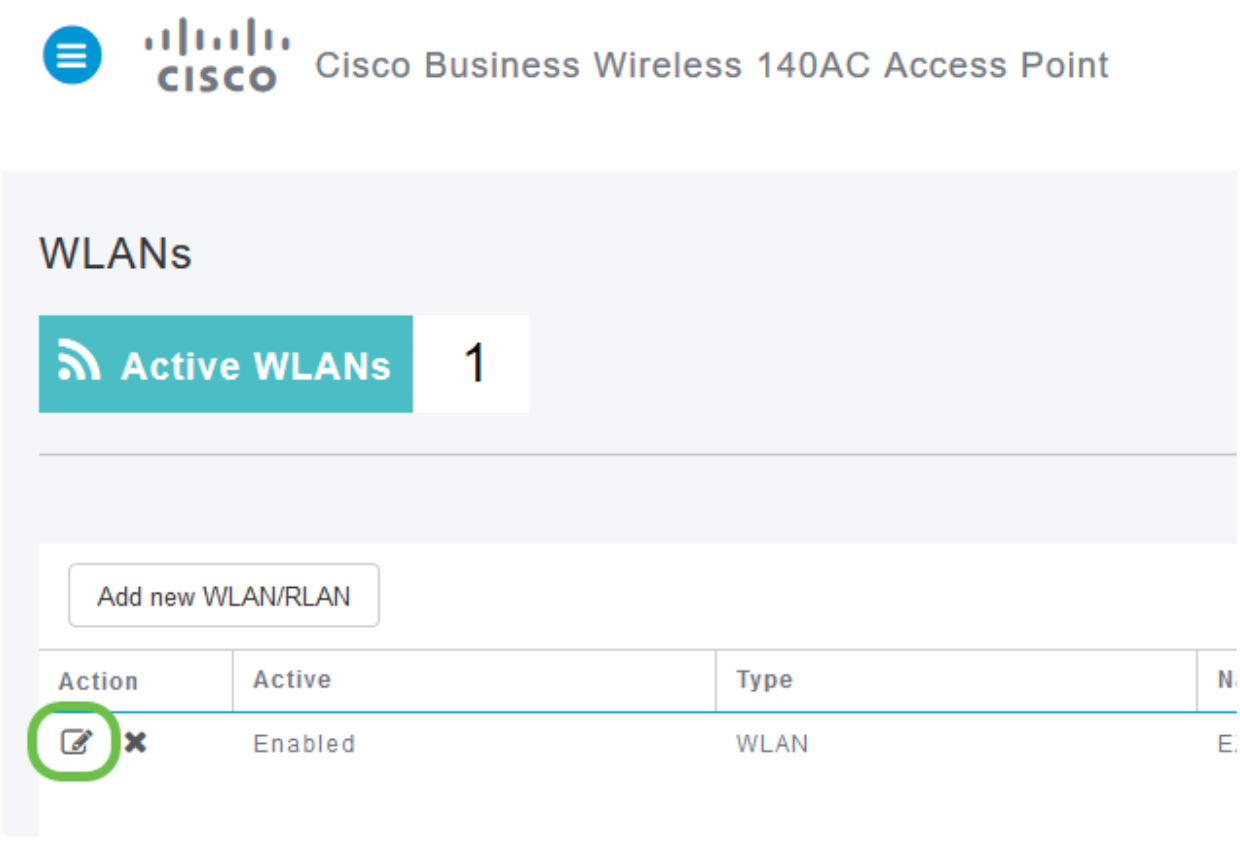

Monitoring
Network Summary
Access Points
Clients
Guest Clients
Mesh Extender
Applications
Rogues
Access Points
Clients
Wireless Dashboard
AP Performance

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

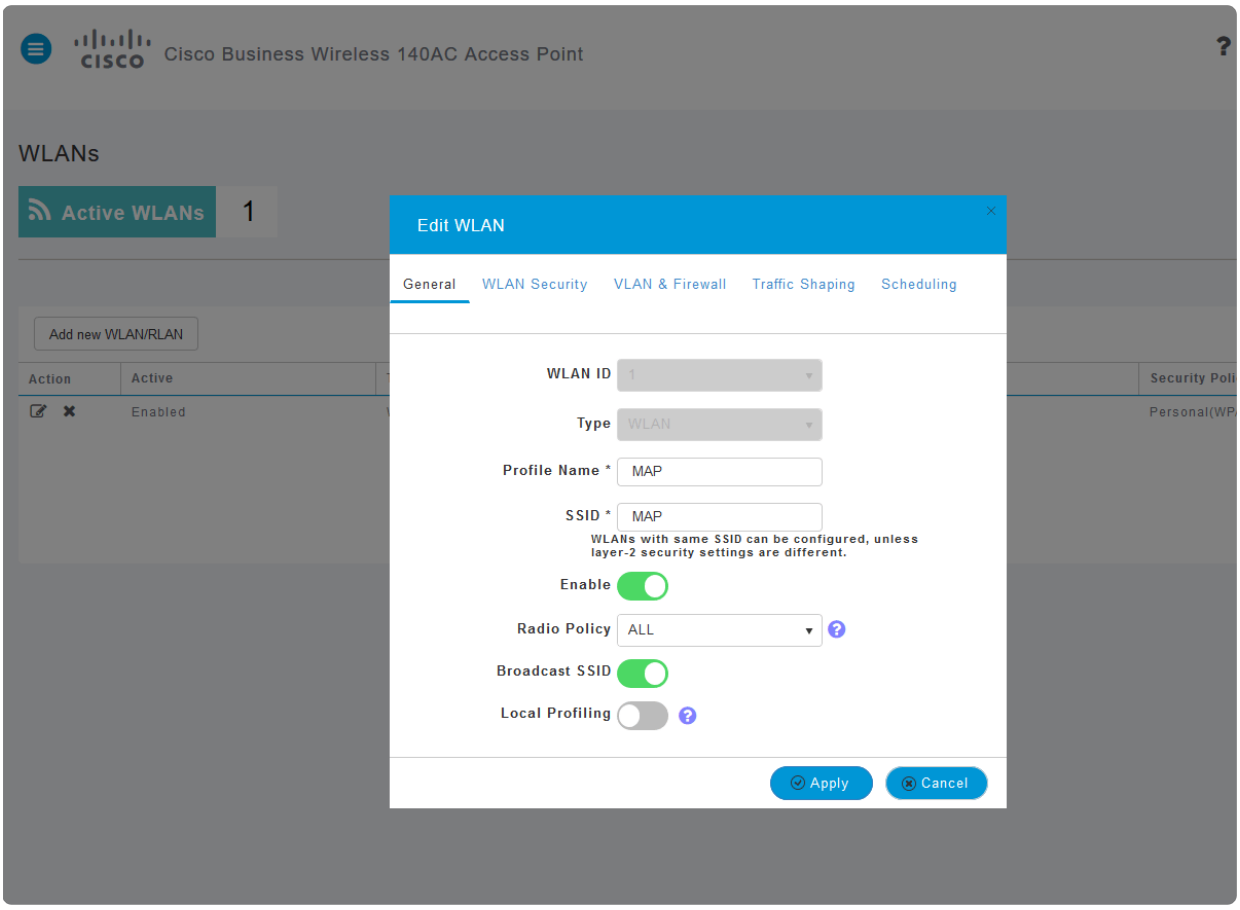


Étape 3

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

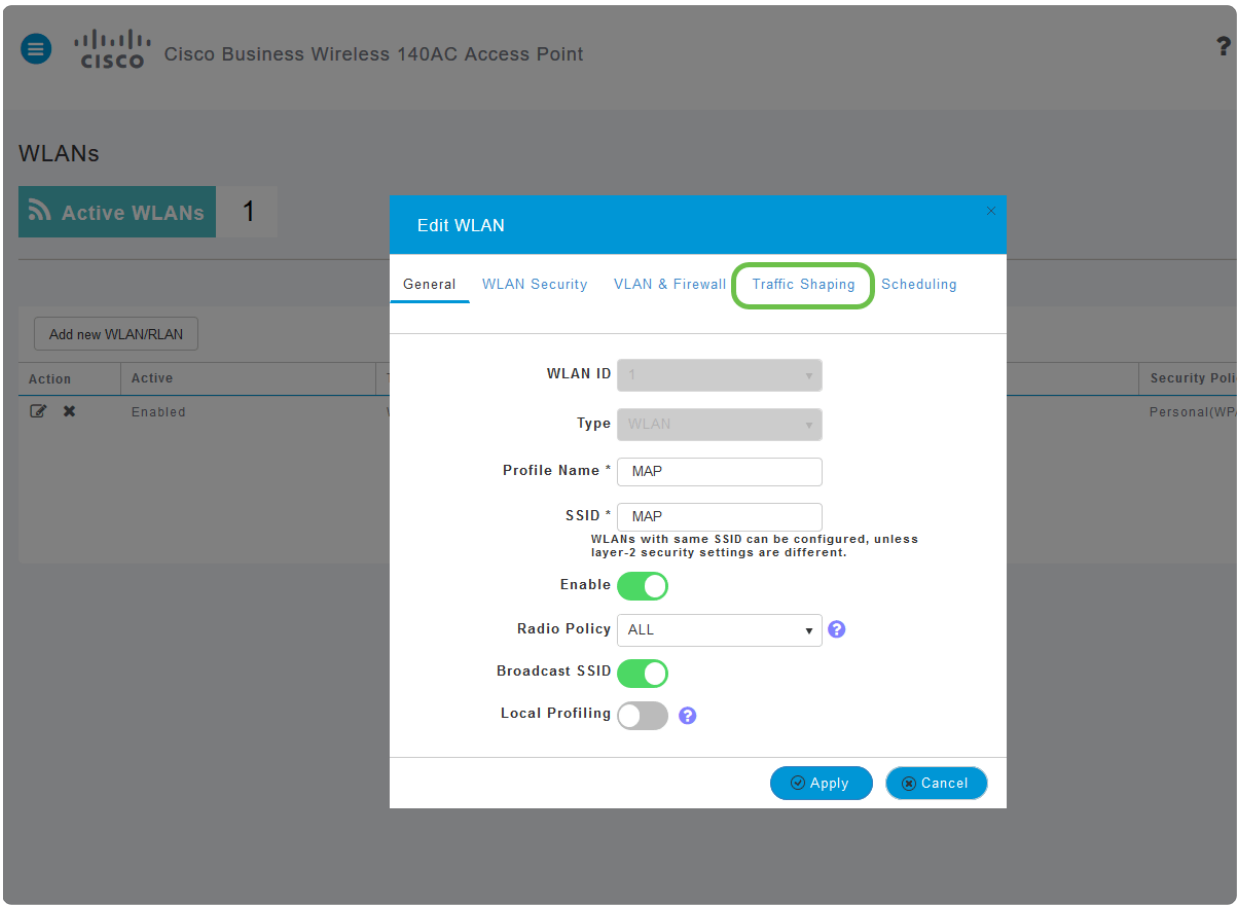


Depuis que vous avez récemment ajouté le WLAN, votre page Edit WLAN peut apparaître comme suit :

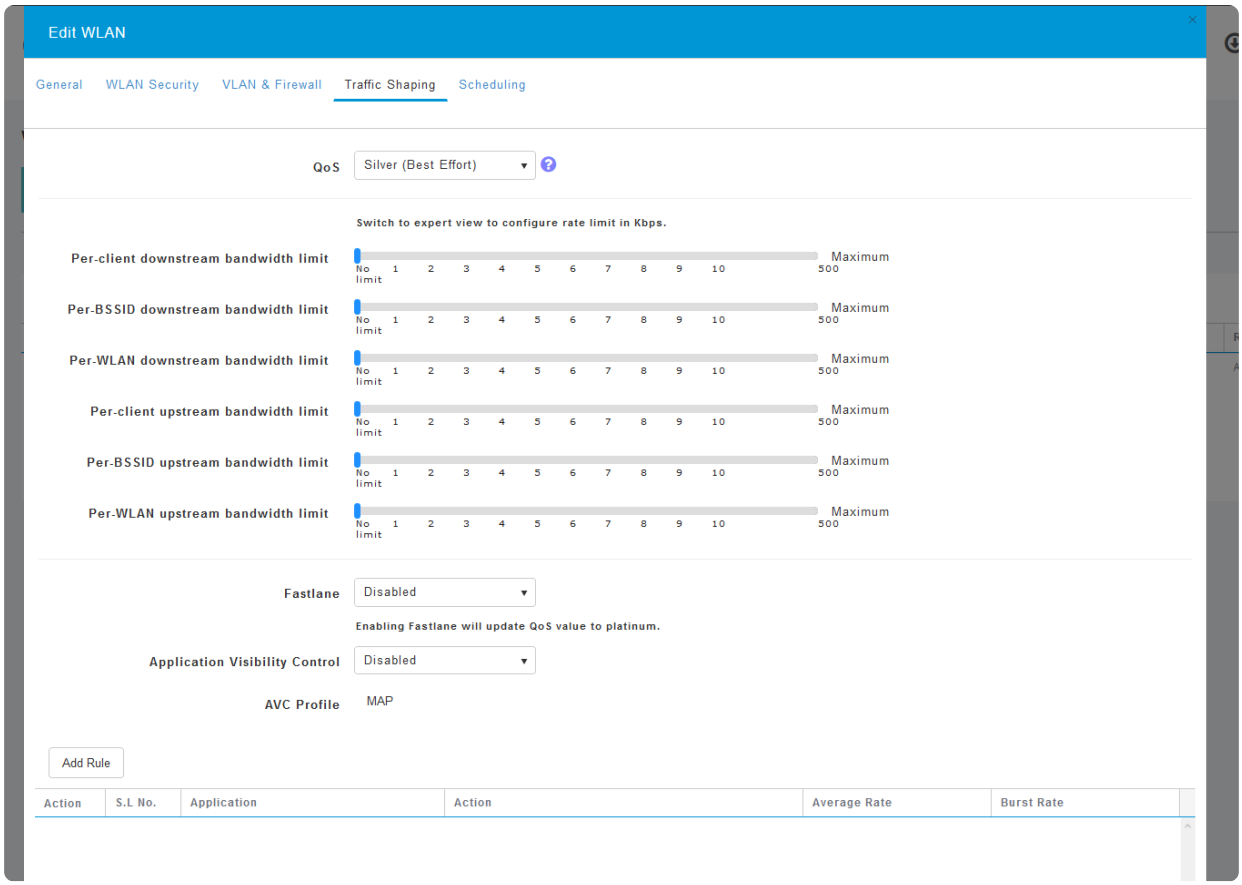


Étape 4

Accédez à l'onglet Traffic Shaping en cliquant dessus.

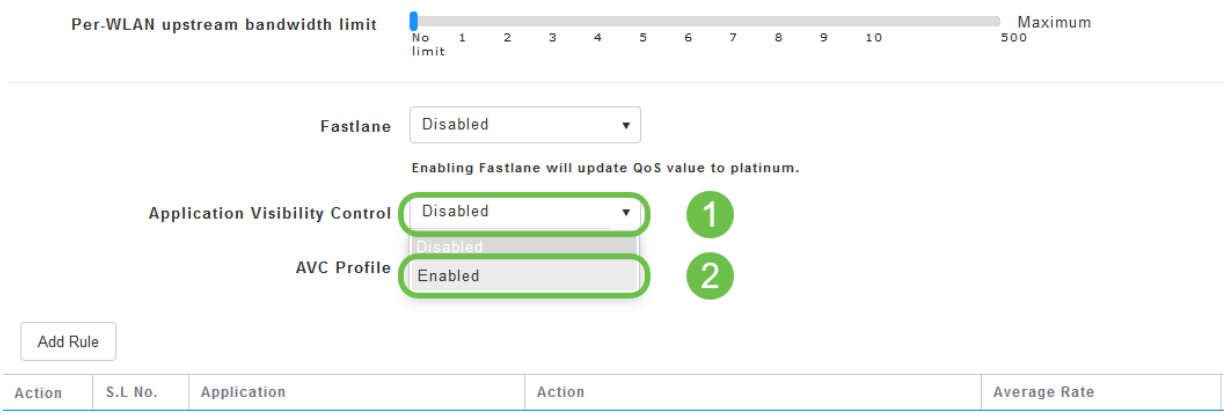


Votre écran peut s'afficher comme suit :



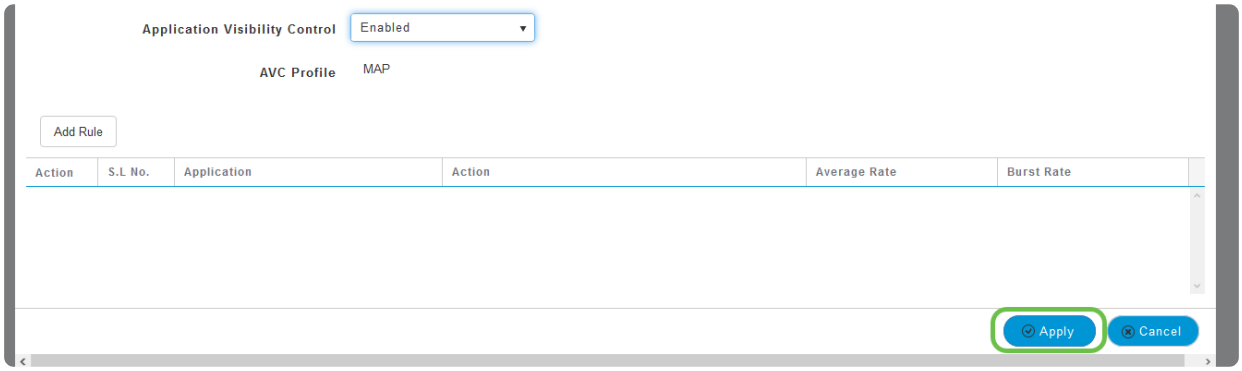
Étape 5

Vers le bas de la page, vous trouverez la fonctionnalité Contrôle de la visibilité des applications. Cette option est désactivée par défaut. Cliquez sur la liste déroulante et sélectionnez Enabled.



Étape 6

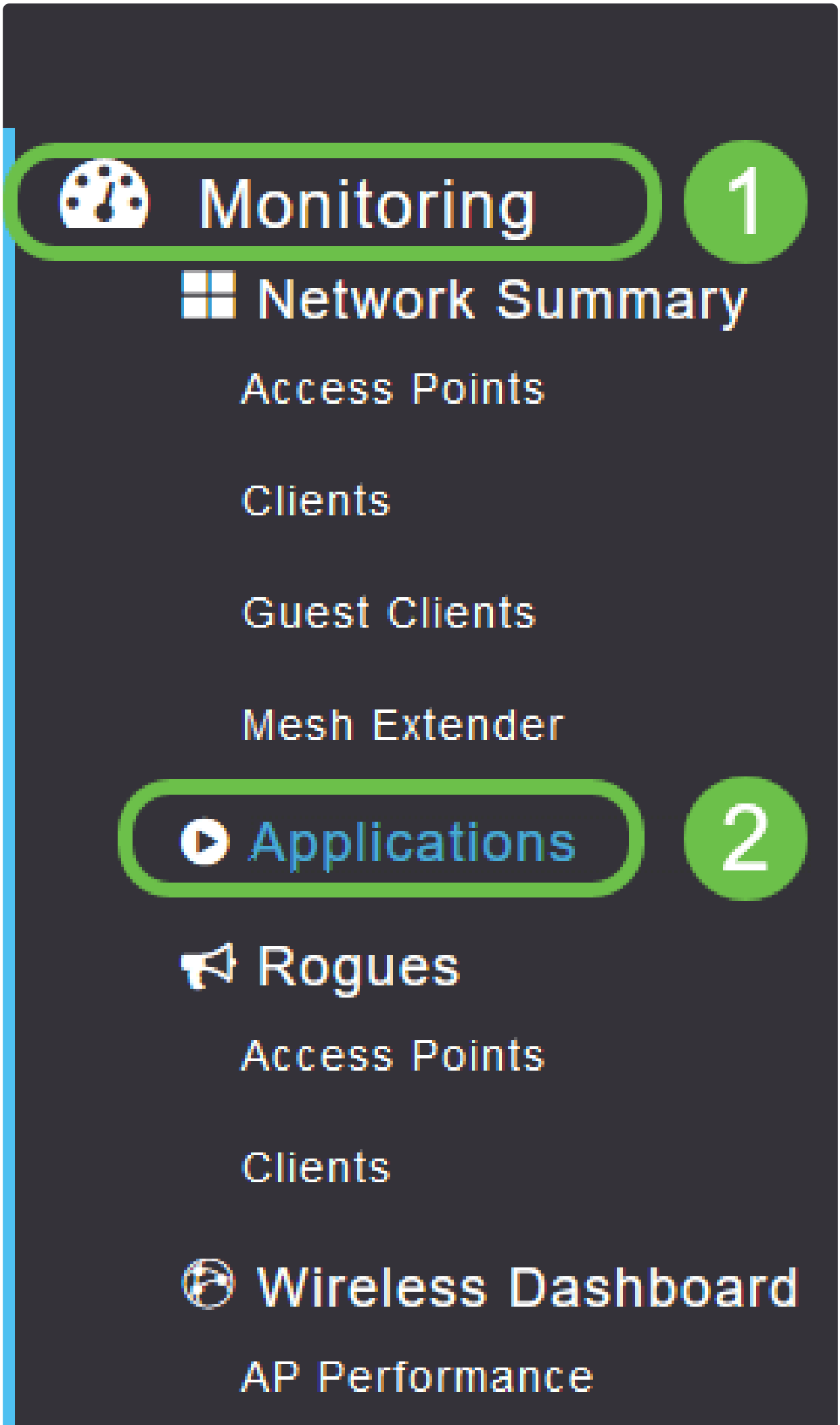
Cliquez sur le bouton Apply.



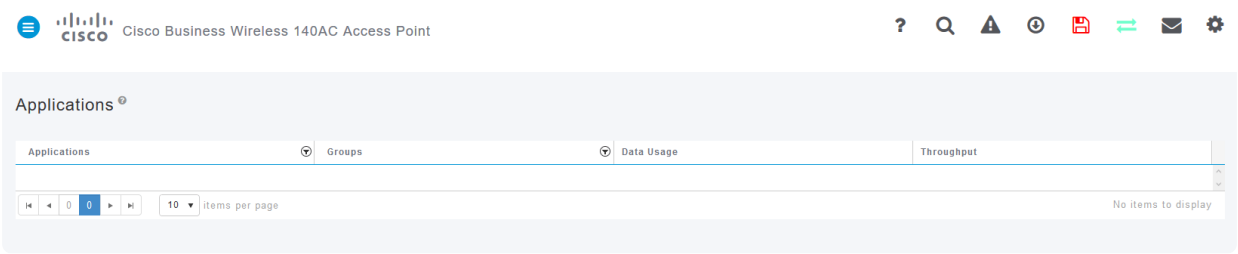
Ce paramètre doit être activé, sinon la fonctionnalité ne fonctionnera pas.

Étape 7

Cliquez sur le bouton Cancel (Annuler) pour fermer le sous-menu WLAN. Cliquez ensuite sur le menu Monitoring dans la barre de menus de gauche. Lorsque vous le pouvez, cliquez sur l'élément de menu Applications.


Monitoring
1
Network Summary
Access Points
Clients
Guest Clients
Mesh Extender
Applications
2
Rogues
Access Points
Clients
Wireless Dashboard
AP Performance

Si vous n'avez pas de trafic vers une source quelconque, votre page sera vide, 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 utilisée par ce service dans son ensemble
- Débit : quantité de bande passante utilisée par l'application

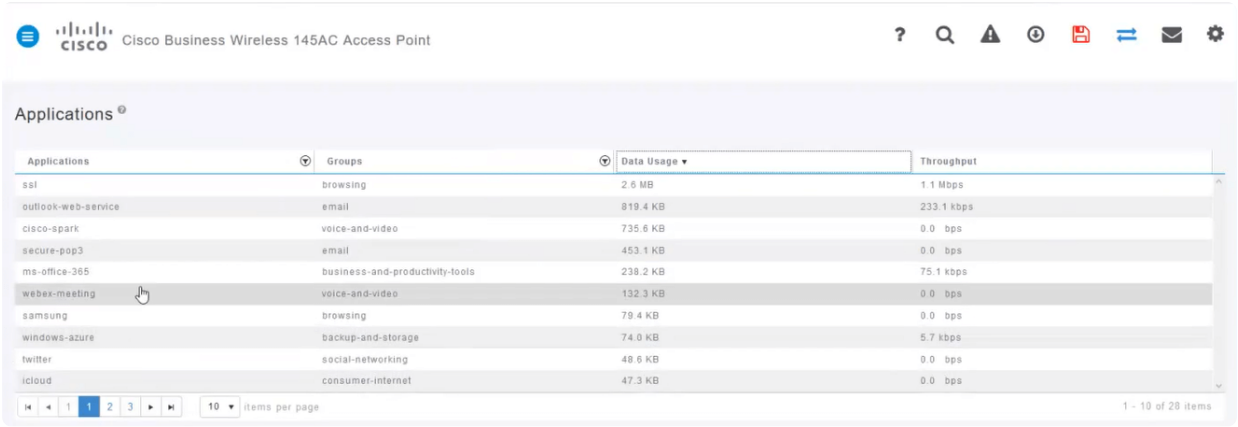
Vous pouvez cliquer sur les onglets pour effectuer un tri du plus grand au plus petit, ce qui peut vous aider à identifier les plus grands consommateurs de ressources réseau.

Cette fonctionnalité est très puissante pour gérer vos ressources WLAN de manière granulaire. Vous trouverez ci-dessous certains des groupes et types d'applications les plus courants. Votre liste est susceptible d'en inclure beaucoup d'autres, y compris les groupes et 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
- Mises à jour de logiciels
    - EX : Google-Play, IOS
- Messagerie instantanée
    - EX : Hangouts, Messages

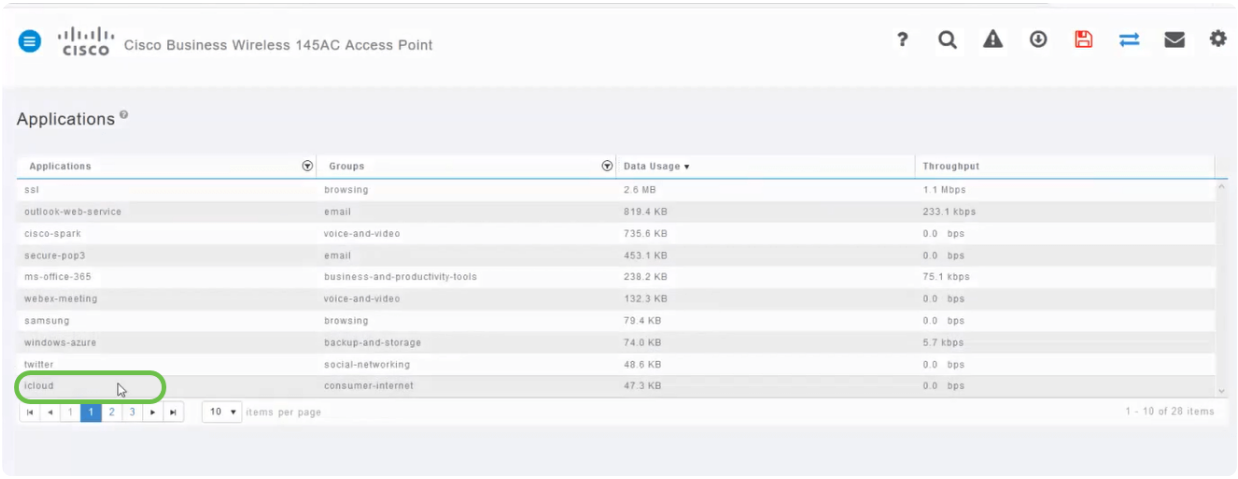
Voici un exemple de ce à quoi la page ressemblera une fois remplie.



Vous pouvez cliquer sur chaque en-tête de table pour effectuer le tri, ce qui est particulièrement utile pour les champs Utilisation des données et Débit.

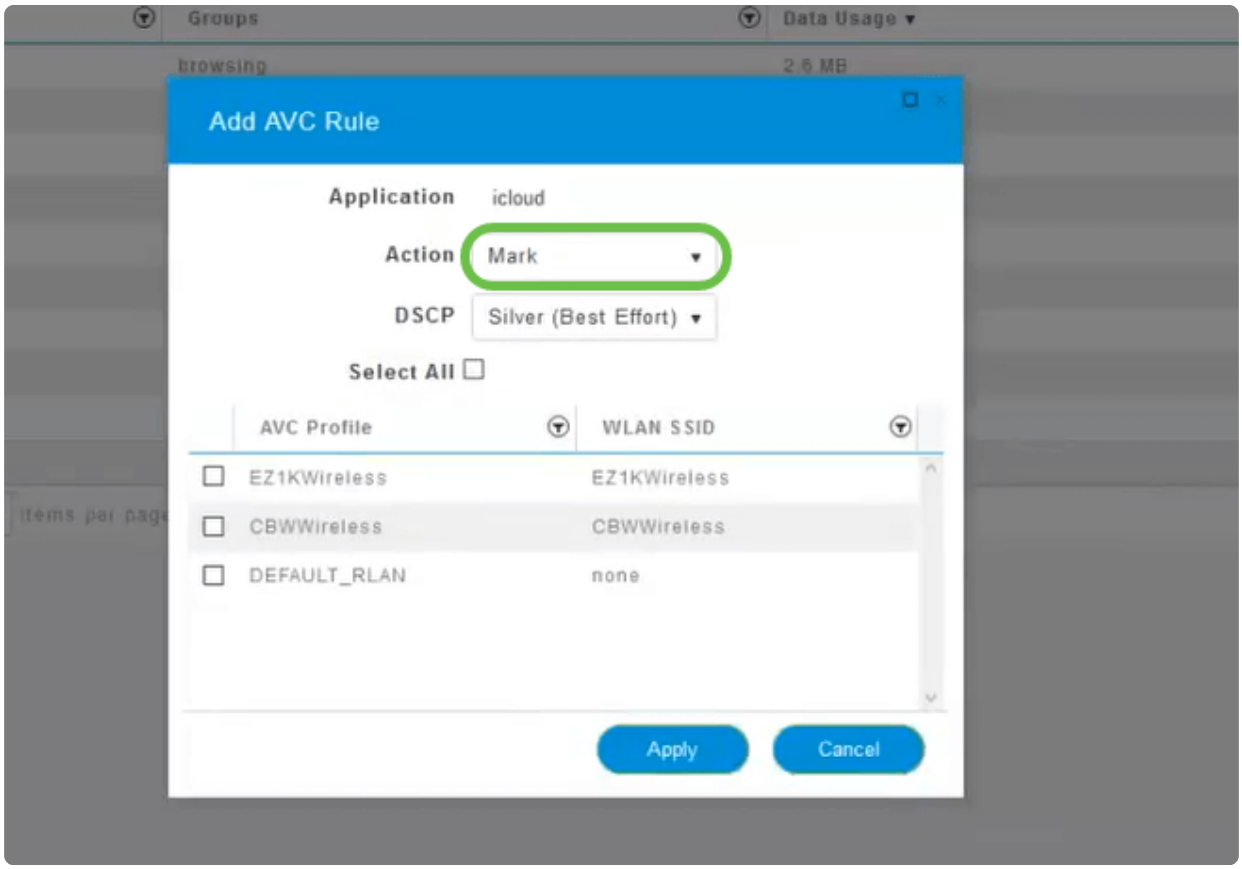
Étape 8

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



Étape 9

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



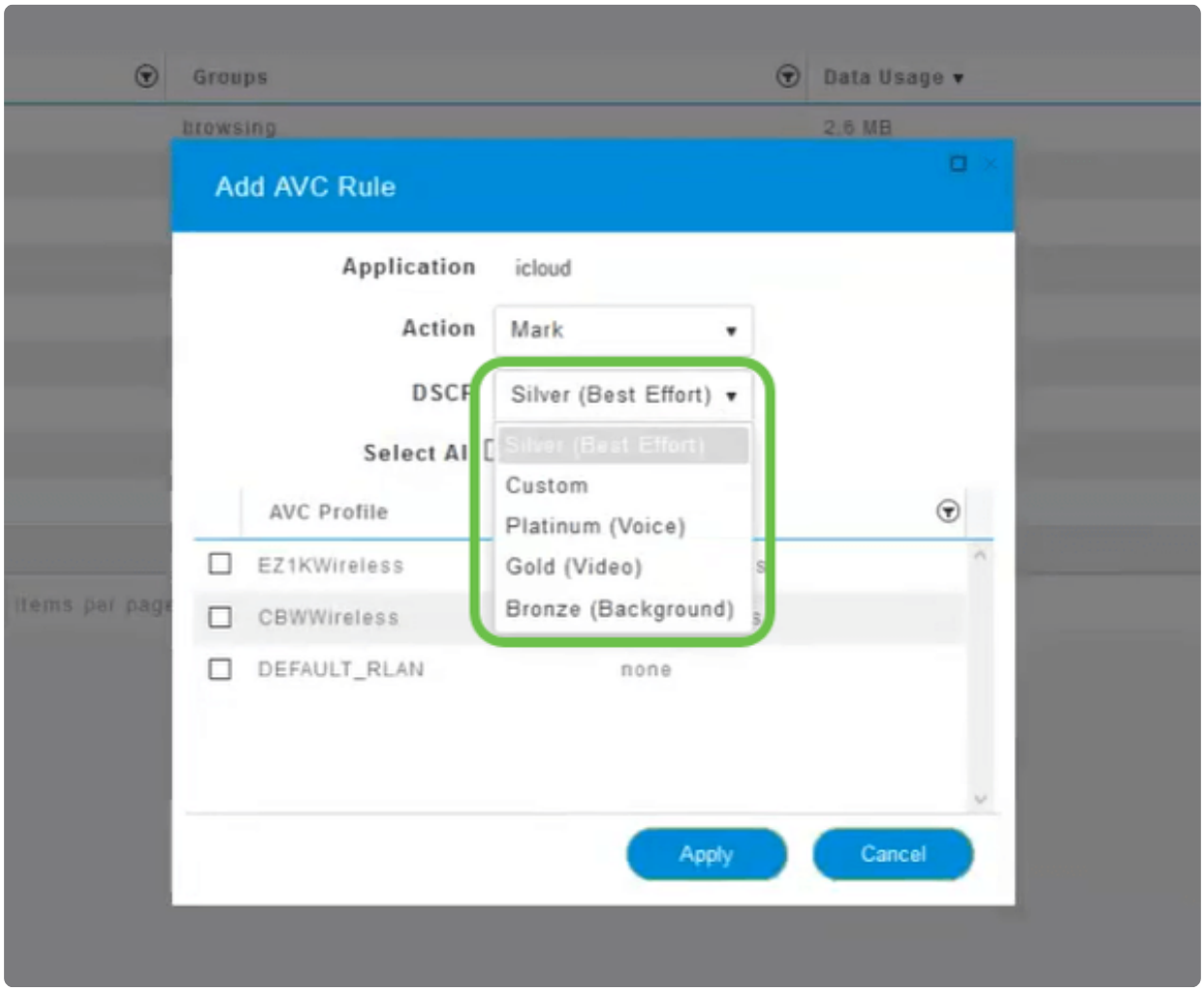
Pour cet exemple, nous laissons cette option à Mark.

Mesures à prendre concernant le trafic

- Marquer : place le type de trafic dans l'un des niveaux DSCP (Differentiated Services Code Point) 3, qui détermine le nombre de ressources disponibles pour le type d'application
- Abandonner - Ne rien faire, mais rejeter le trafic
- Rate Limit (Limite de débit) : permet de définir le débit moyen, le débit en rafale (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 pour le trafic à marquer. Ces options

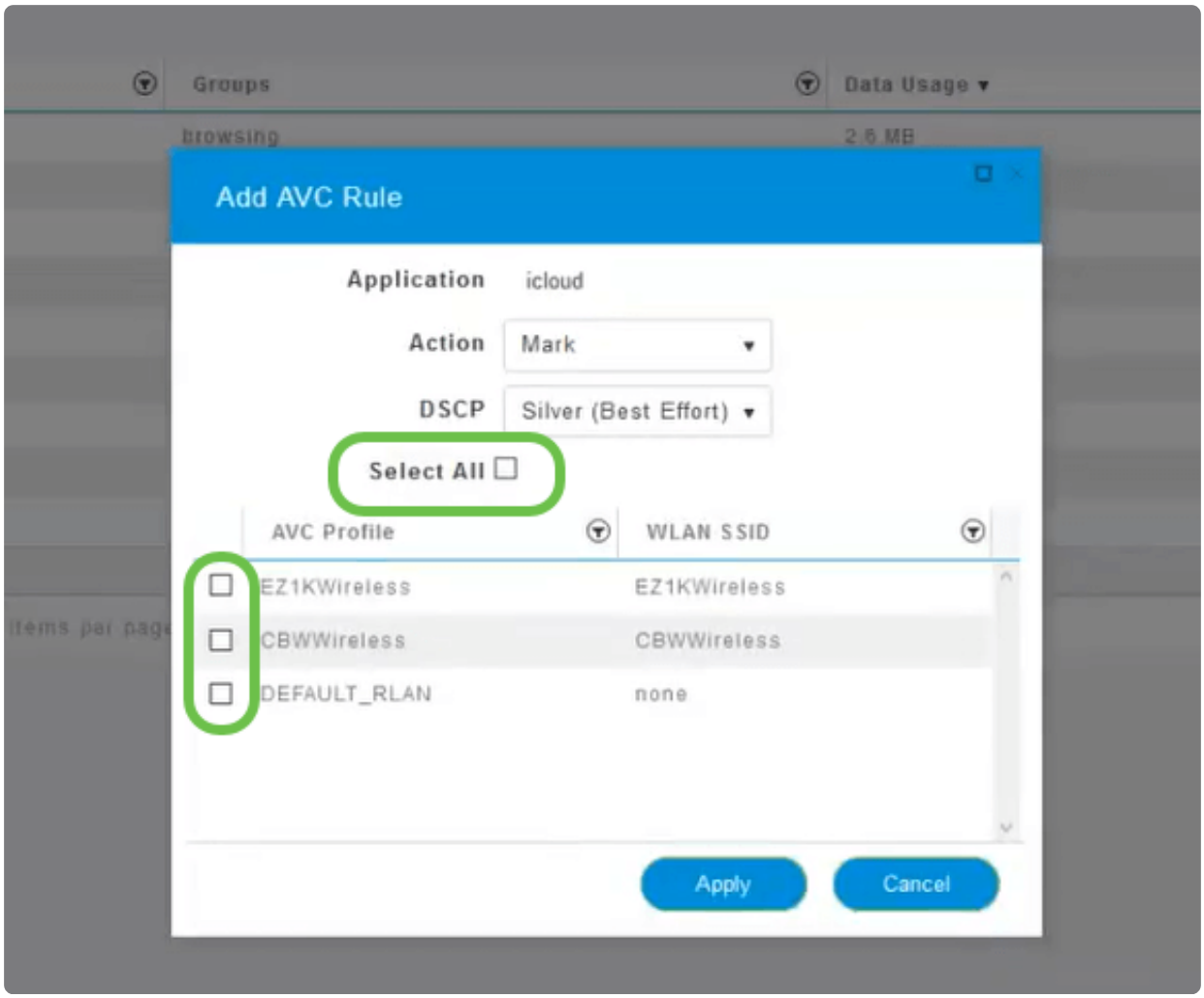
passent d'un nombre réduit de ressources à un nombre plus important de ressources disponibles pour le type de trafic que vous modifiez.

- Bronze (arrière-plan) - Moins
- Argent (au mieux)
- Gold (vidéo)
- Platinum (voix) Plus
- Personnalisé - Jeu 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 d'une priorité inférieure pour le trafic SSL peut affecter votre expérience de navigation.

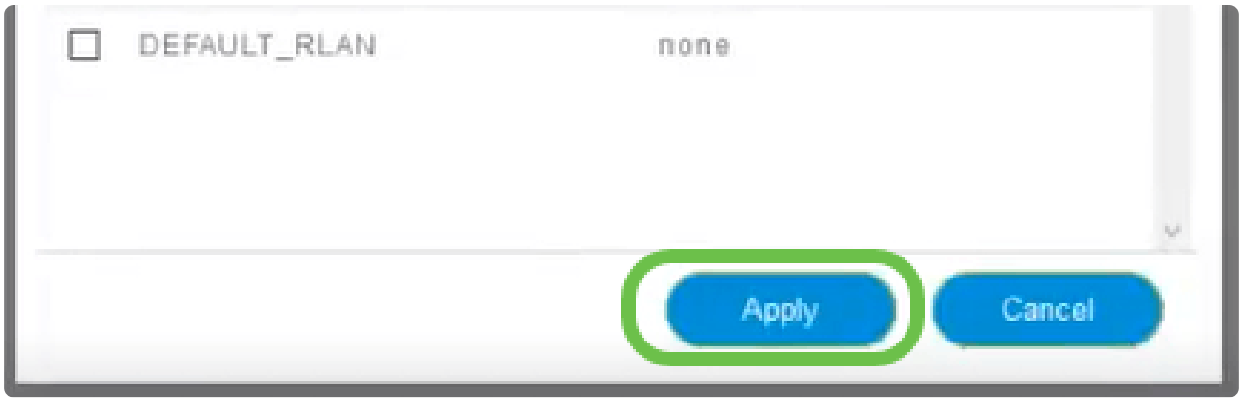
Étape 11

Sélectionnez maintenant le SSID individuel que vous souhaitez exécuter cette stratégie ou cliquez sur Select All.



Étape 12

Cliquez maintenant sur Apply pour commencer cette stratégie.



Deux cas où cela pourrait s'appliquer :

- Les invités/utilisateurs diffusent en continu 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 volumineuses pendant les heures de bureau peut être déclassé ou limité.

Tu l'as fait ! Le profilage d'application est un outil très puissant qui peut être activé en activant également le profilage client, 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 client est désactivé. Ces informations peuvent inclure :

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

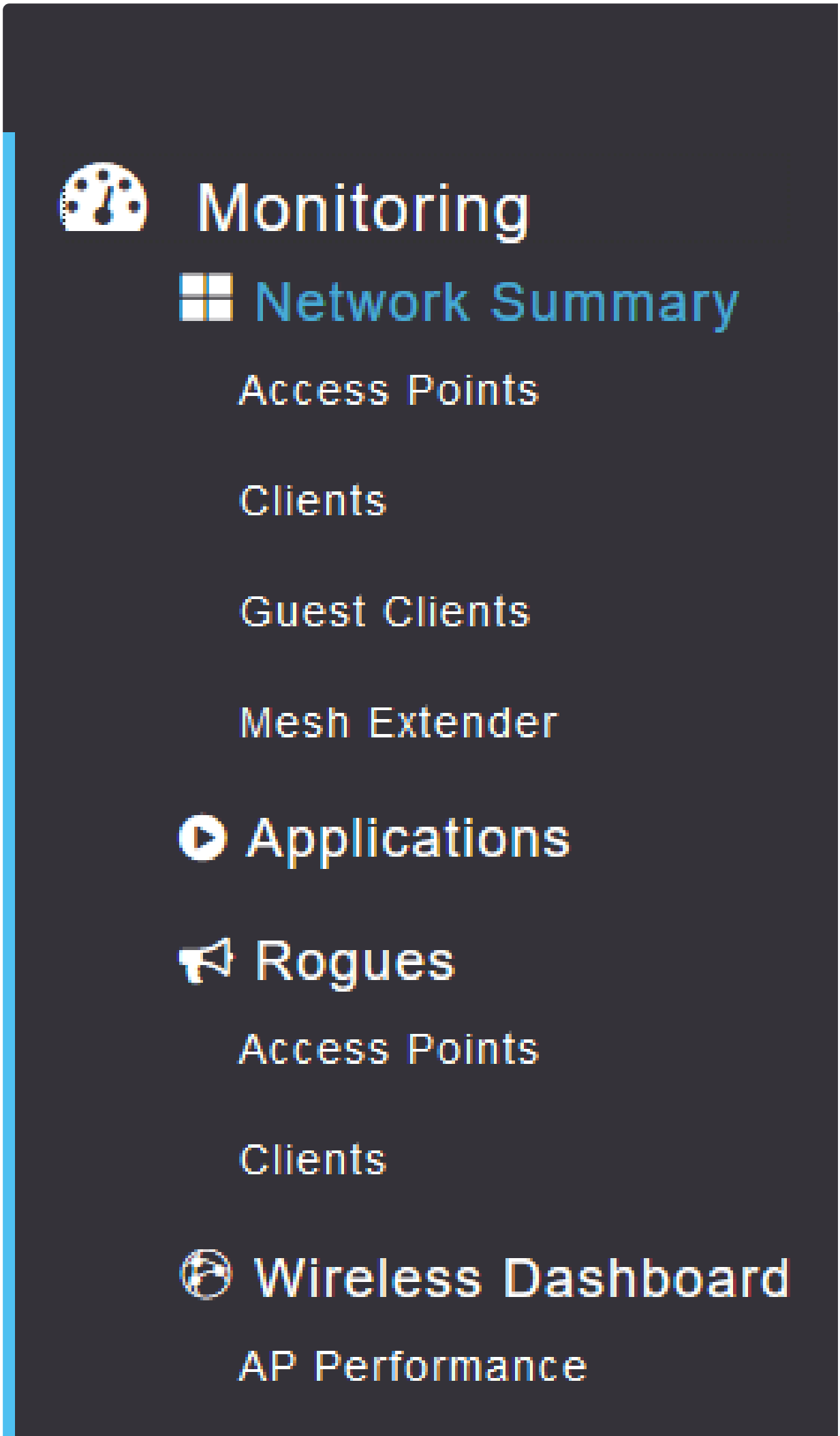
Les statistiques relatives à ces clients incluent la quantité de données utilisées et le débit.

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

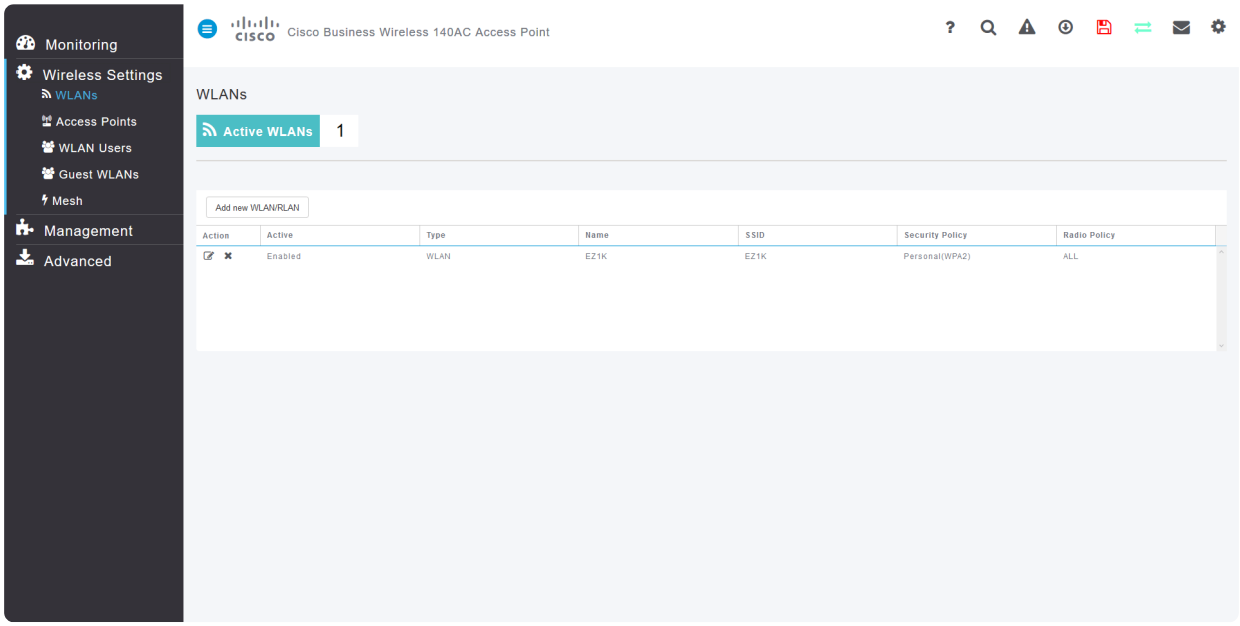
Une fois activé, les détails du client de votre réseau sont disponibles dans la section Surveillance de l'interface utilisateur Web.

Étape 1

Cliquez sur Wireless Settings.

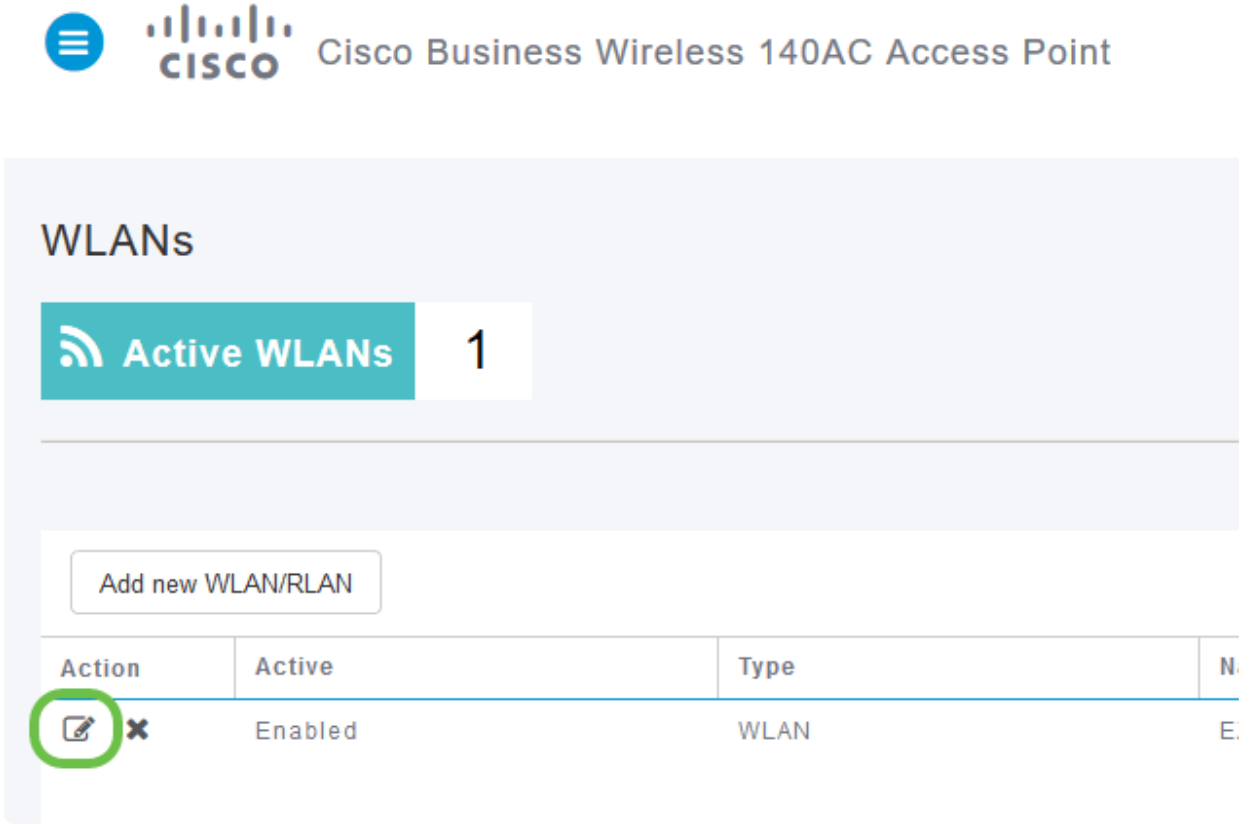

Monitoring
Network Summary
Access Points
Clients
Guest Clients
Mesh Extender
Applications
Rogues
Access Points
Clients
Wireless Dashboard
AP Performance

Le tableau ci-dessous est similaire à celui qui s'affiche lorsque vous cliquez sur le lien Wireless Settings (Paramètres sans fil) :



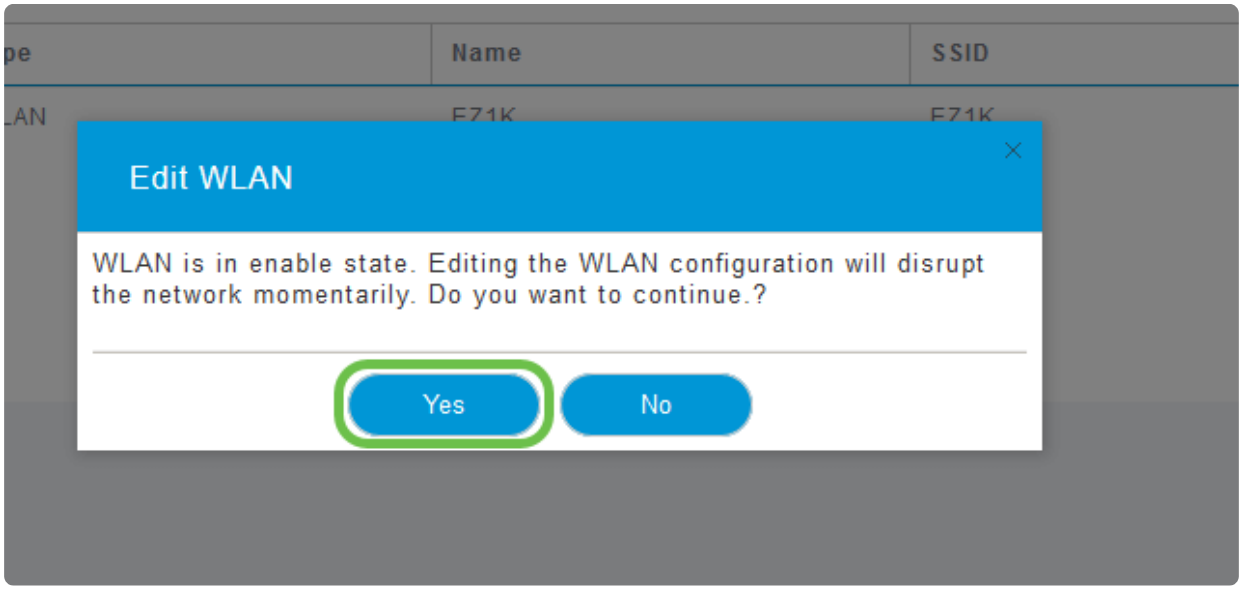
Étape 2

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



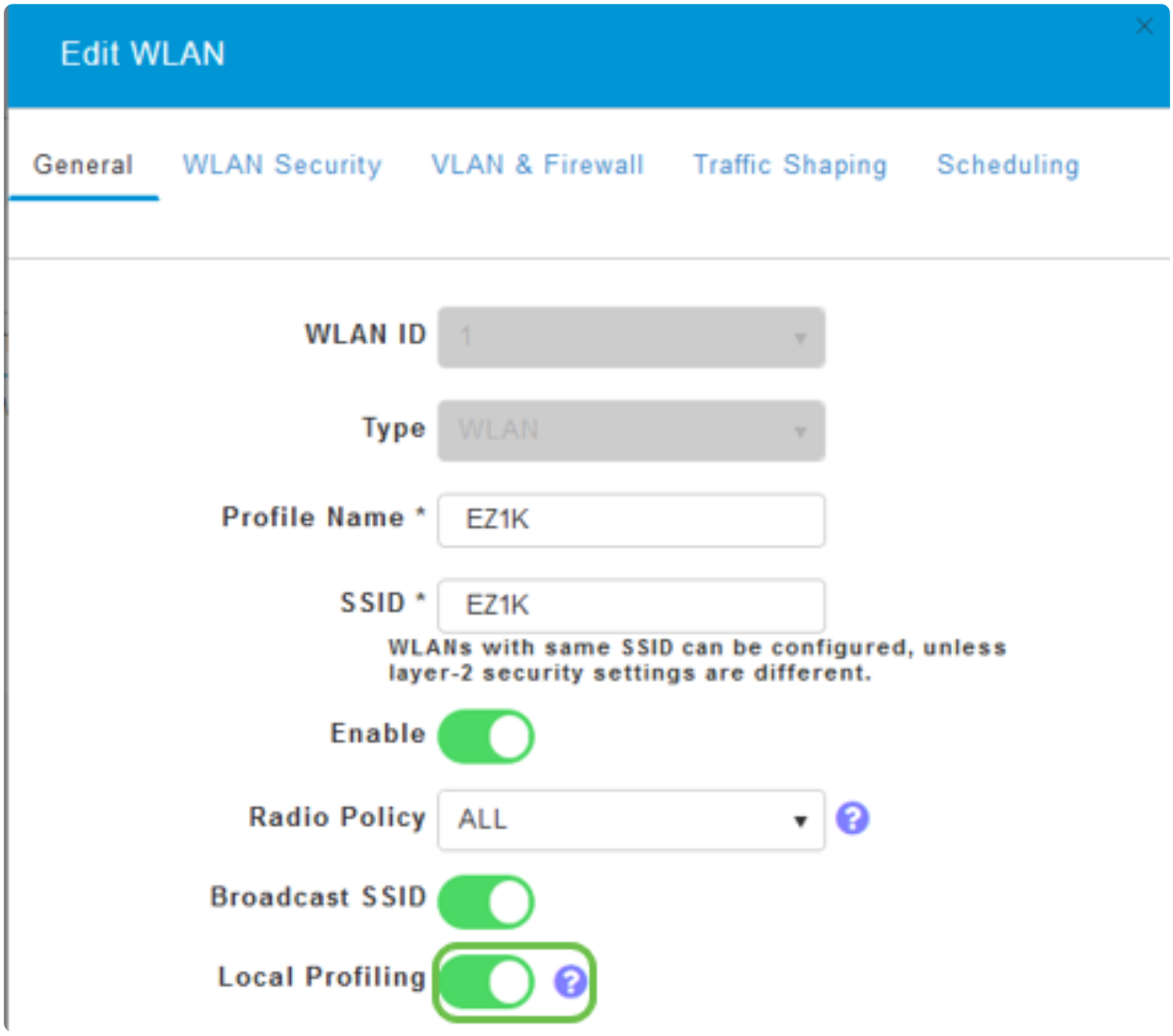
Étape 3

Un menu contextuel peut être similaire à celui ci-dessous. Ce message important peut affecter temporairement le service sur votre réseau. Cliquez sur Yes pour avancer.



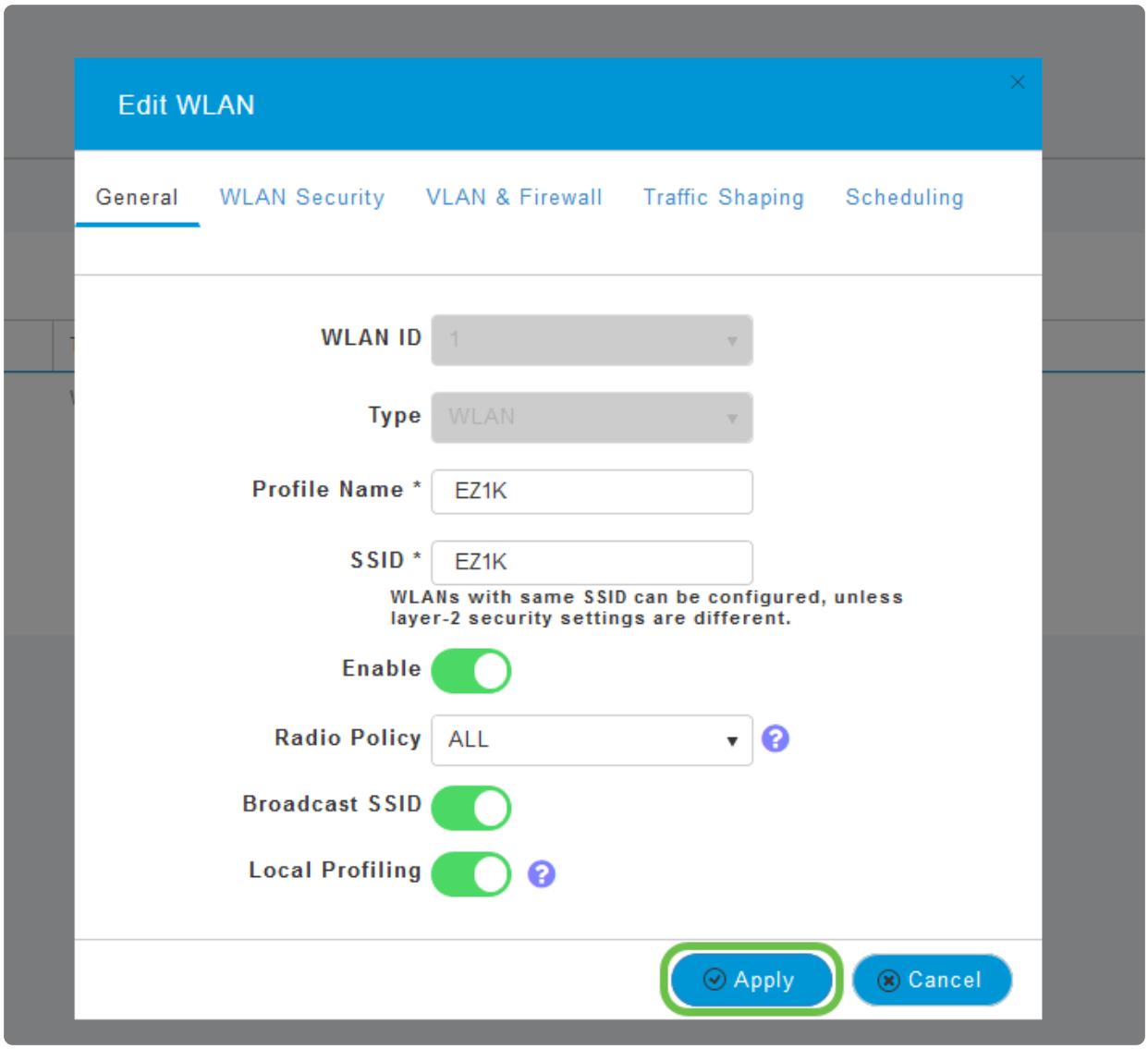
Étape 4

Activez ou désactivez le profilage client en cliquant sur le bouton bascule Profilage local.



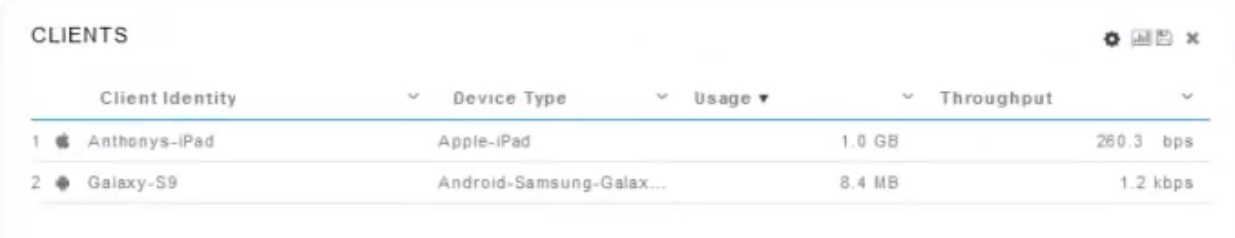
Étape 5

Cliquez sur Apply.



Étape 6

Cliquez sur l'élément de menu de la section Surveillance sur le côté 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 géniale, prenez une minute pour fêter ça et ensuite allez au travail !

Nous voulons ce qu'il y a de mieux pour nos clients. Si vous avez des commentaires ou des suggestions à ce sujet, veuillez nous envoyer un courriel à l'équipe responsable du contenu de Cisco.

Si vous souhaitez lire d'autres articles et documentations, consultez les pages d'assistance de votre matériel :

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

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

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