Configuration des paramètres sans fil de base sur le RV215W

Objectif

Les réseaux sans fil sont des réseaux informatiques qui ne sont pas connectés par des câbles. Un réseau local sans fil (WLAN) est un type de réseau sans fil qui relie plusieurs périphériques sur une courte distance grâce à l'utilisation de la communication radio.

Cet article explique comment configurer les paramètres sans fil de base sur le routeur RV215W, y compris la configuration de la sécurité réseau.

Indice

· Paramètres généraux
· Modifier la table sans fil
· Désactiver la sécurité
· Configuration de la sécurité WEP
· Configuration de la sécurité WPA personnel
· Configuration de la sécurité WPA entreprise
· Configuration de la sécurité mixte WPA2-Personal/WPA2-Personal
· Configuration de la sécurité mixte WPA2-Enterprise/WPA2-Enterprise
· Modifier le filtrage MAC
· Accès à l'heure
· Modifier le réseau invité
· Configuration de la méthode WPS 1
· Configuration de la méthode WPS 2
· Configuration de la méthode WPS 3

Périphériques pertinents

•RV215W

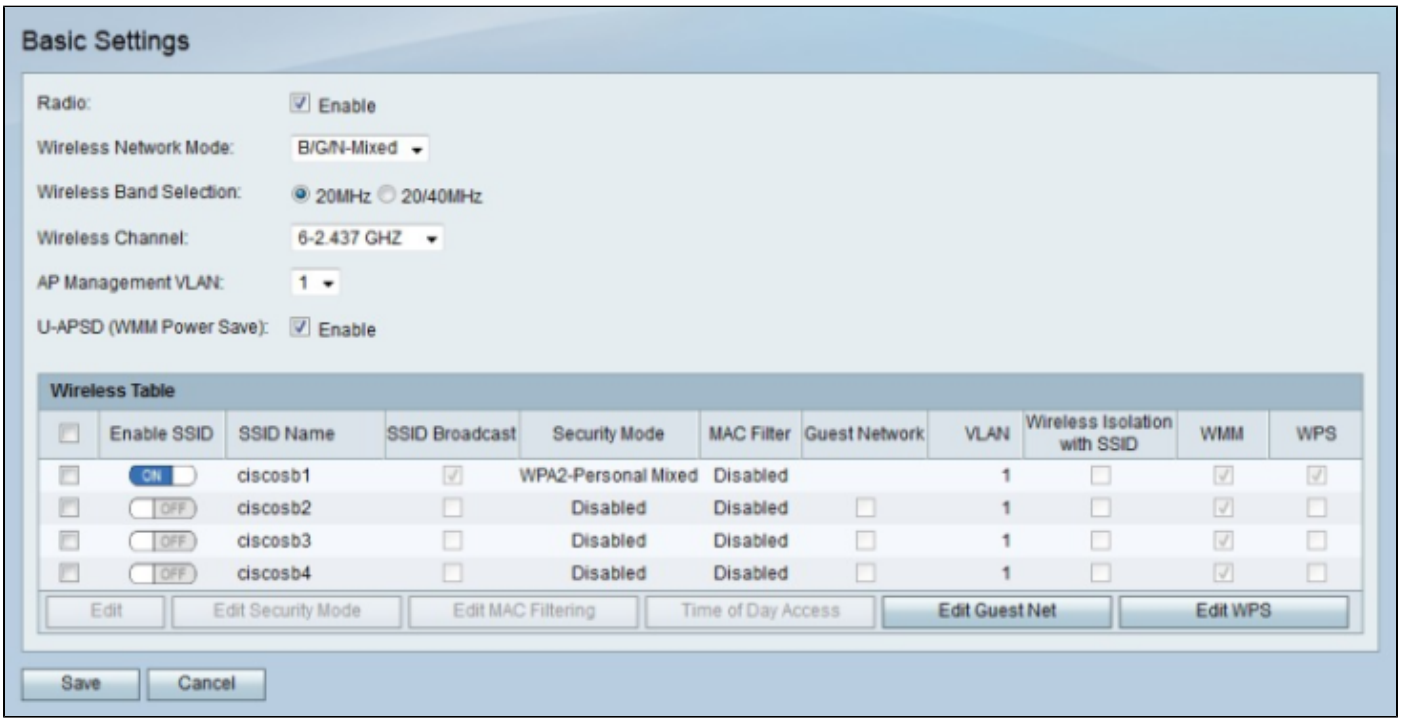
Version du logiciel

•1.1.0.5

Configuration des paramètres de base

Paramètres généraux

Étape 1. Connectez-vous à l'utilitaire de configuration Web et choisissez Wireless > Basic Settings. La page Basic Settings s'ouvre :



Étape 2. Cochez Enable dans le champ Radio pour activer la radio sans fil.

Étape 3. Dans la liste déroulante Wireless Network Mode, sélectionnez le mode sans fil.

· B/G/N-Mixed : le réseau contient une combinaison de périphériques sans fil B, G et N.

· B-Only : le réseau ne contient que des périphériques sans fil B.

· G-Only : le réseau ne contient que des périphériques sans fil G.

· N-Only : le réseau ne contient que des périphériques sans fil N.

· B/G-Mixed : le réseau contient une combinaison de périphériques sans fil B et G.

· G/N Mixed : le réseau contient une combinaison de périphériques sans fil G et sans fil N.

Étape 4. Si le mode réseau contient des périphériques sans fil N, cliquez sur la case d’option correspondant à la bande passante souhaitée du signal sans fil dans le champ Wireless Band Selection (Sélection de bande sans fil). Plus la bande passante est élevée, plus la quantité de données que le signal peut transporter est importante.

· 20 MHz — Fréquence standard d'un signal sans fil.

· 20/40 MHz — Utilise automatiquement un signal de 20 MHz et de 40 MHz. Un signal de 40 MHz fournit plus de bande passante, mais est sujet à davantage d'interférences. Cette option est utilisée uniquement si les périphériques sans fil connectés sont compatibles avec la fréquence 40 MHz.

Étape 5. Dans la liste déroulante Wireless Channel (Canal sans fil), sélectionnez un canal sans fil pour la radio. Sélectionnez un canal qui n'est pas actuellement utilisé par les réseaux voisins.

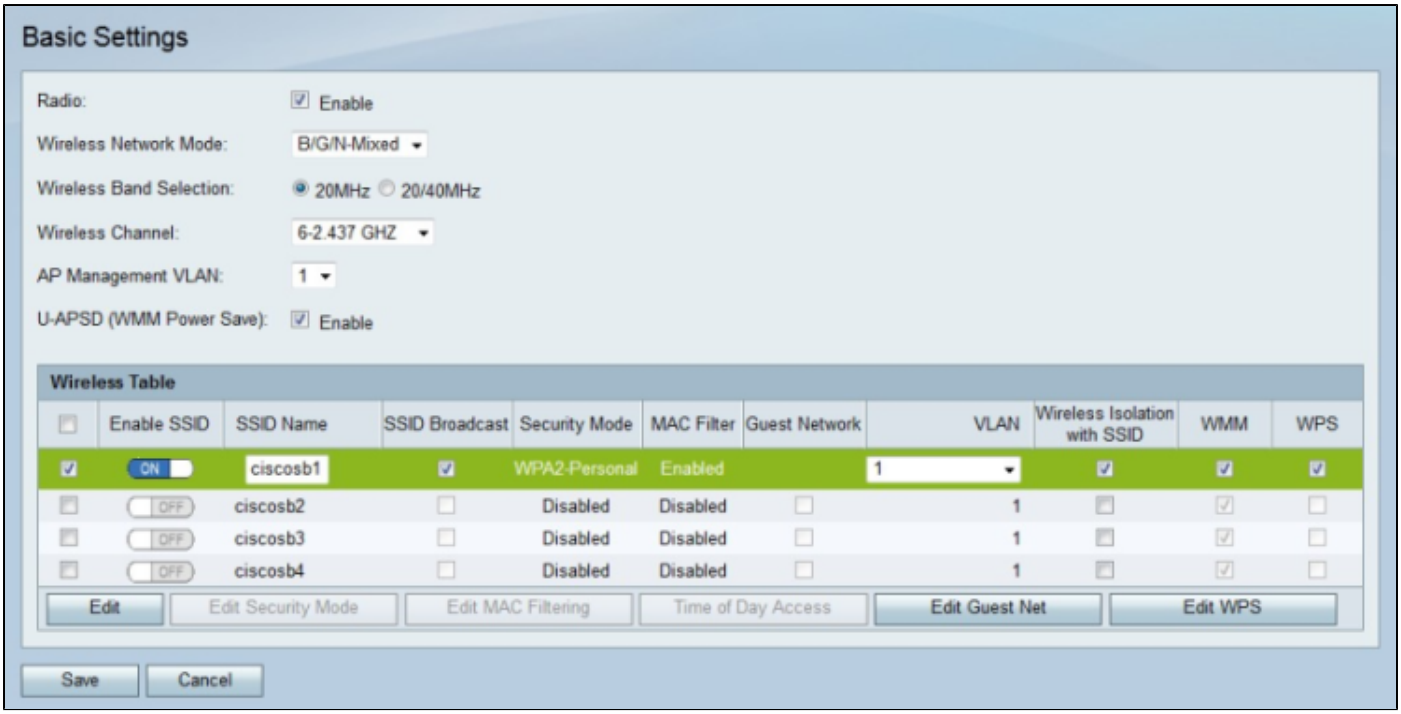
Étape 6. Dans la liste déroulante AP Management VLAN, sélectionnez un VLAN qui doit devenir le VLAN de gestion.

Étape 7. (Facultatif) Cochez Enable dans le champ U-APSD pour activer la remise automatique non planifiée de l'alimentation (U-APSD). U-APSD est une fonctionnalité qui permet à la radio d'économiser de l'énergie. Cependant, U-APSD peut réduire les performances de débit de la radio.

Étape 8. Cliquez sur Save.

Modifier le tableau sans fil

Étape 1. Connectez-vous à l’utilitaire de configuration Web et choisissez Wireless **>** Basic Settings. La page Basic Settings s'ouvre :



Étape 2. Cochez la case du réseau que vous souhaitez modifier dans le tableau Wireless.

Étape 3. Cliquez sur Edit pour modifier le réseau spécifié.

Étape 4. Cliquez sur le bouton Enable SSID pour activer le réseau. SSID (Service Set Identifier) est le nom du réseau sans fil.

Étape 5. Entrez le nom du réseau dans le champ SSID Name (Nom SSID). Tous les périphériques du réseau doivent utiliser ce SSID pour communiquer entre eux.

Étape 6. Cochez SSID Broadcast pour activer la diffusion sans fil. Le RV215W annonce sa disponibilité aux périphériques sans fil voisins lorsque la diffusion SSID est activée.

Étape 7. Cochez Guest Network pour faire du réseau configuré un réseau invité. Un réseau invité est une petite section d'un réseau conçue pour des utilisateurs temporaires. Cette option permet aux invités d'utiliser le réseau sans avoir à exposer les clés Wi-Fi privées.

Remarque : Le réseau invité ne peut pas être configuré sur le VLAN de gestion AP.

Étape 8. Dans la liste déroulante VLAN, sélectionnez le VLAN associé au réseau.

Étape 9. Vérification de l'isolation sans fil avec SSID pour empêcher les périphériques du réseau spécifié de communiquer entre eux

Étape 10. Cochez la case WMM pour activer le mode WMM (Wi-Fi Multimedia) sur le réseau.

WMM est utilisé pour améliorer la diffusion multimédia en continu sur les périphériques sans fil. WMM donne une priorité plus élevée au trafic multimédia envoyé sur une connexion sans fil.

Étape 11. (Facultatif) Cochez la case WPS pour attribuer le réseau spécifié en tant que réseau WPS (Wi-Fi Protected Setup). WPS est une fonctionnalité qui permet une configuration réseau facile et sécurisée. Cette fonctionnalité permet aux périphériques de se connecter facilement au réseau.

Étape 12. Cliquez sur Save.

Désactiver la sécurité

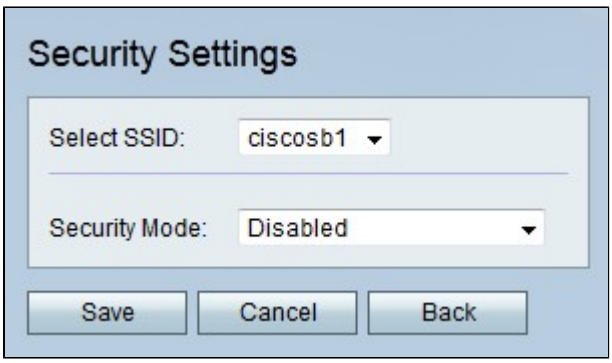
La sécurité sans fil peut être désactivée sur le routeur RV215W pour faciliter l'utilisation lors de la configuration des réseaux de test. Toutefois, il n'est pas recommandé de désactiver la sécurité.

Étape 1. Connectez-vous à l'utilitaire de configuration Web et choisissez Wireless > Basic Settings. La page Basic Settings s'ouvre.

Étape 2. Cochez la case du réseau que vous souhaitez modifier.

Étape 3. Cliquez sur Edit Security Mode pour modifier la sécurité du réseau spécifié. La page Security Settings s'ouvre :

Étape 4. (Facultatif) Dans la liste déroulante Sélectionner le SSID, sélectionnez le SSID pour lequel vous souhaitez configurer la sécurité.



Étape 5. Dans la liste déroulante Security Mode, sélectionnez Disabled. La sécurité est désactivée pour le réseau sans fil.

Étape 6. Cliquez sur Save.

Configuration de la sécurité WEP

WEP (Wired Equivalent Privacy) est un algorithme qui sécurise un réseau sans fil. WEP fournit une méthode de cryptage de base moins sécurisée que WPA. WEP est utilisé lorsque les périphériques réseau connectés ne prennent pas en charge WPA.

Étape 1. Connectez-vous à l'utilitaire de configuration Web et choisissez Wireless > Basic Settings. La page Basic Settings s'ouvre.

Étape 2. Cochez la case du réseau que vous souhaitez modifier.

Étape 3. Cliquez sur Edit Security Mode pour modifier la sécurité du réseau spécifié. La page Security Settings s'ouvre :



Étape 4. (Facultatif) Dans la liste déroulante Sélectionner le SSID, sélectionnez le SSID pour lequel vous souhaitez configurer la sécurité.

Étape 5. Dans la liste déroulante Security Mode, sélectionnez WEP.

Étape 6. Dans la liste déroulante Authentication Type, sélectionnez un type d'authentification pour le réseau sans fil.

· Système ouvert : tout le monde peut s'associer au point d'accès, mais la clé WEP est nécessaire pour acheminer le trafic via le point d'accès du réseau.

· Clé partagée : une clé WEP est nécessaire pour s'associer au point d'accès et pour faire passer le trafic par le point d'accès du réseau.

Étape 7. Dans la liste déroulante Encryption, sélectionnez une méthode de cryptage pour la clé WEP.

· 10/64 bits (10 chiffres hexadécimaux) : fournit une clé de 40 bits.

· 26/128 bits (26 chiffres hexadécimaux) : fournit une clé de 104 bits. Il s'agit du chiffrement le plus sécurisé.

Étape 8. Entrez une phrase de passe de plus de huit caractères dans le champ Passphrase (Phrase de passe).

Étape 9. Cliquez sur Generate pour créer des clés dans les champs Key 1, Key 2, Key 3 et Key 4.

Remarque : Vous pouvez également saisir manuellement des clés dans les champs Clé 1, Clé 2, Clé 3 et Clé 4.

Étape 10. Dans la liste déroulante TX Key, sélectionnez la clé que les utilisateurs doivent saisir pour accéder au réseau sans fil.

Étape 11. (Facultatif) Cochez la case Unmask Password pour afficher les chaînes de caractères des touches.

Étape 12. Cliquez sur Save.

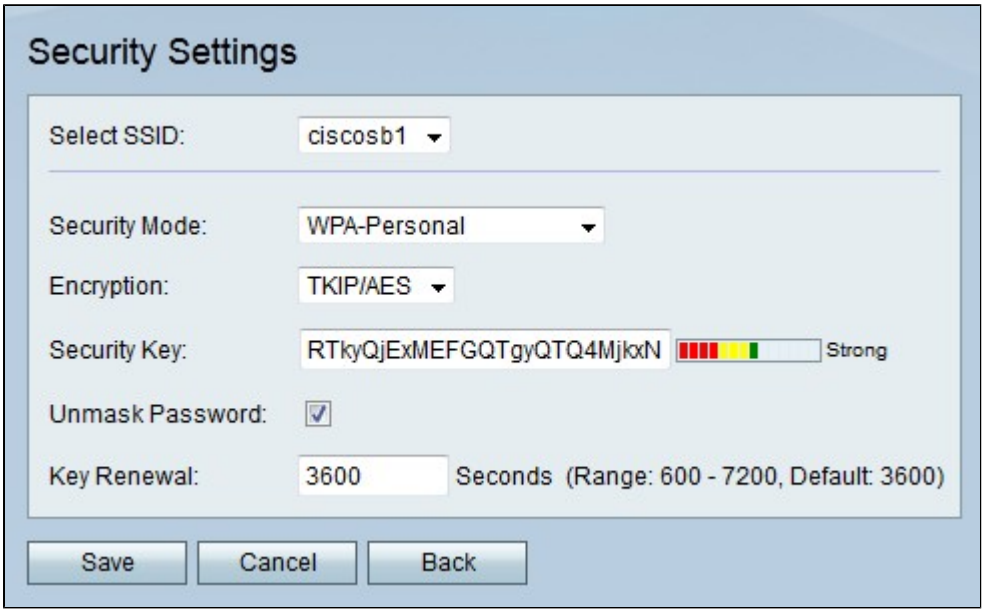
Configuration de la sécurité WPA personnel

La norme WPA (Wi-Fi Protected Access) est une norme de sécurité pour les réseaux sans fil. WPA a été créé pour remplacer WEP en raison de failles de sécurité dans WEP. WPA-Personal est une version de WPA utilisée pour les réseaux comptant seulement quelques utilisateurs. Le mode WPA personnel fournit une clé partagée que chaque utilisateur utilisera pour accéder au réseau sans fil. WPA a été introduit avec les méthodes de cryptage de clé TKIP (Temporal Key Integrity Protocol) et AES (Advanced Encryption Standard). De plus en plus de périphériques réseau prennent en charge le protocole TKIP, mais AES est la méthode de cryptage la plus puissante.

Étape 1. Connectez-vous à l'utilitaire de configuration Web et choisissez Wireless > Basic Settings. La page Basic Settings s'ouvre.

Étape 2. Cochez la case du réseau que vous souhaitez modifier.

Étape 3. Cliquez sur Edit Security Mode pour modifier la sécurité du réseau spécifié. La page Security Settings s'ouvre :



Étape 4. (Facultatif) Dans la liste déroulante Sélectionner le SSID, sélectionnez le SSID pour lequel vous souhaitez configurer la sécurité.

Étape 5. Dans la liste déroulante Security Mode, sélectionnez WPA-Personal.

Étape 6. Dans la liste déroulante Encryption, sélectionnez une méthode de cryptage pour la clé WPA.

· TKIP/AES : cette option est sélectionnée lorsque tous les périphériques connectés au réseau sans fil ne prennent pas en charge AES.

· AES : cette option est préférable si tous les périphériques connectés aux périphériques sans fil prennent en charge AES.

Étape 7. Entrez une clé de sécurité dans le champ Clé de sécurité.

Étape 8. (Facultatif) Cochez la case Unmask Password pour afficher la chaîne de caractères de la clé.

Étape 9. Entrez une heure dans le champ Key Renewal (Renouvellement de clé). Il s'agit de la durée pendant laquelle le routeur RV215W utilisera la clé avant d'en générer une nouvelle.

Étape 10. Cliquez sur Save.

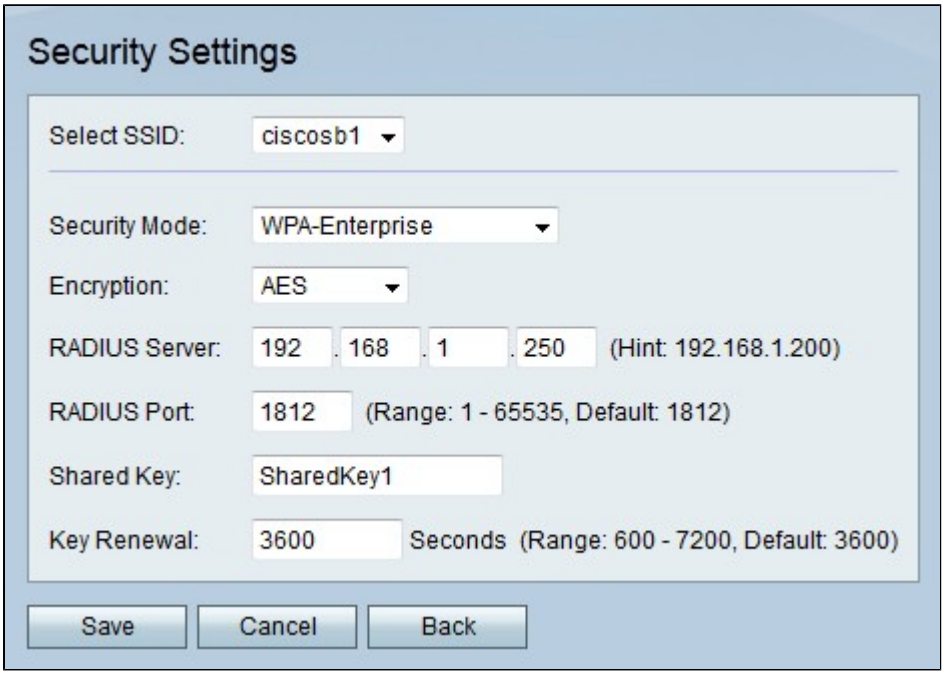
Configuration de la sécurité WPA-Enterprise

La norme WPA (Wi-Fi Protected Access) est une norme de sécurité pour les réseaux sans fil. WPA a été créé pour remplacer WEP en raison de failles de sécurité dans WEP. WPA-Enterprise est une version de WPA recommandée pour un réseau comportant de nombreux utilisateurs, par exemple une entreprise. L'authentification utilisée pour obtenir l'accès est contrôlée par un serveur RADIUS. Cela signifie que chaque utilisateur connecté recevra une clé unique pour accéder au réseau sans fil. WPA a été introduit avec les méthodes de cryptage de clé TKIP (Temporal Key Integrity Protocol) et AES (Advanced Encryption Standard). De plus en plus de périphériques réseau prennent en charge le protocole TKIP, mais AES est la méthode de cryptage la plus puissante.

Étape 1. Connectez-vous à l'utilitaire de configuration Web et choisissez Wireless > Basic Settings. La page Basic Settings s'ouvre.

Étape 2. Cochez la case du réseau que vous souhaitez modifier.

Étape 3. Cliquez sur Edit Security Mode pour modifier la sécurité du réseau spécifié. La page Security Settings s'ouvre :



Étape 4. (Facultatif) Dans la liste déroulante Sélectionner le SSID, sélectionnez le SSID pour

lequel vous souhaitez configurer la sécurité.

Étape 5. Dans la liste déroulante Security Mode, sélectionnez WPA-Enterprise.

Étape 6. Dans la liste déroulante Encryption, sélectionnez une méthode de cryptage pour la clé WPA.

· TKIP/AES : cette option est sélectionnée lorsque tous les périphériques connectés au réseau sans fil ne prennent pas en charge AES.

· AES : cette option est préférable si tous les périphériques connectés aux périphériques sans fil prennent en charge AES.

Étape 7. Entrez l’adresse IP du serveur RADIUS dans le champ RADIUS Server.

Étape 8. Entrez le numéro de port utilisé pour accéder au serveur RADIUS dans le champ RADIUS Port.

Étape 9. Entrez la clé pré-partagée pour les utilisateurs sans fil dans le champ Shared Key (Clé partagée). Une clé pré-partagée est une clé utilisée par tous les utilisateurs. La fonctionnalité de clé prépartagée est une fonctionnalité de sécurité ajoutée à l'authentification RADIUS.

Étape 10. Entrez une heure dans le champ Key Renewal (Renouvellement de clé). Il s'agit de la durée pendant laquelle le routeur RV215W utilisera la clé avant d'en générer une nouvelle.

Étape 11. Cliquez sur Save.

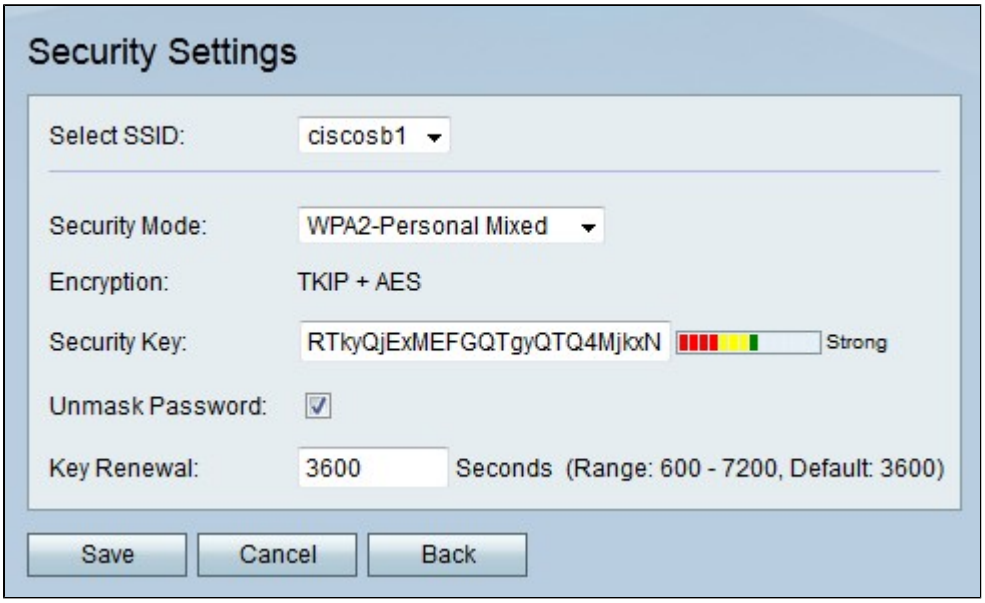
Configuration de la sécurité mixte WPA2-Personal/WPA2-Personal

La norme WPA2 (Wi-Fi Protected Access 2) est une norme de sécurité pour les réseaux sans fil. WPA2 est une amélioration de WPA. WPA2 offre plus de sécurité que WPA, mais WPA2 nécessite plus de puissance de traitement. WPA2-Personal/WPA2-Personal Mixed sont des versions de WPA2 utilisées pour les réseaux comptant peu d'utilisateurs. WPA2-Personal Mixed est conçu pour assurer la compatibilité descendante des périphériques plus anciens qui ne sont pas capables d’utiliser WPA2. Si possible, n’utilisez pas WPA2-Personal Mixed, car il offre une connexion moins sécurisée. WPA2-Personal (WPA2 personnel) fournit une clé partagée que chaque utilisateur utilisera pour accéder au réseau sans fil. WPA2 utilise les méthodes de cryptage TKIP (Temporal Key Integrity Protocol) et AES (Advanced Encryption Standard). De plus en plus de périphériques réseau prennent en charge le protocole TKIP, mais AES est la méthode de cryptage la plus puissante.

Étape 1. Connectez-vous à l'utilitaire de configuration Web et choisissez Wireless > Basic Settings. La page Basic Settings s'ouvre.

Étape 2. Cochez la case du réseau que vous souhaitez modifier.

Étape 3. Cliquez sur Edit Security Mode pour modifier la sécurité du réseau spécifié. La page Security Settings s'ouvre :



Étape 4. (Facultatif) Dans la liste déroulante Sélectionner le SSID, sélectionnez le SSID pour lequel vous souhaitez configurer la sécurité.

Étape 5. Dans la liste déroulante Security Mode, sélectionnez WPA2-Personal ou WPA2-Personal Mixed. WPA2-Personal (WPA2 personnel) est utilisé lorsque tous les périphériques du réseau sans fil prennent en charge AES. WPA2-Personal Mixed est utilisé lorsque tous les périphériques ne prennent pas en charge AES.

Remarque : Le type de cryptage utilisé par la méthode de sécurité est affiché dans le champ Encryption (Cryptage).

Étape 6. Entrez une clé de sécurité dans le champ Clé de sécurité.

Étape 7. (Facultatif) Cochez la case Unmask Password pour afficher les chaînes de caractères de la clé.

Étape 8. Entrez une heure dans le champ Key Renewal (Renouvellement de clé). Il s'agit de la durée pendant laquelle le routeur RV215W utilisera la clé avant d'en générer une nouvelle.

Étape 9. Cliquez sur Save.

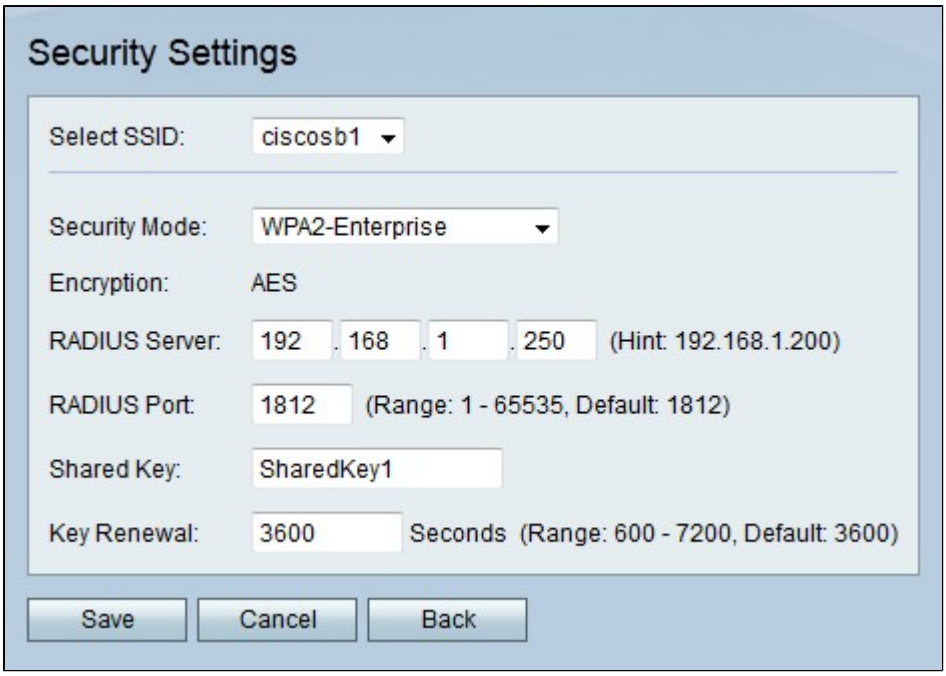
Configuration de la sécurité mixte WPA2-Enterprise/WPA2-Enterprise

La norme WPA2 (Wi-Fi Protected Access 2) est une norme de sécurité pour les réseaux sans fil. WPA2 est une amélioration de WPA. WPA2 offre plus de sécurité que WPA, mais WPA2 nécessite plus de puissance de traitement. WPA2-Enterprise/WPA2-Enterprise Mixed sont des versions de WPA2 utilisées pour les réseaux comportant de nombreux utilisateurs, tels qu'une entreprise. WPA2-Enterprise Mixed est conçu pour assurer la compatibilité descendante des périphériques plus anciens qui ne sont pas capables d'utiliser WPA2. Si possible, n'utilisez pas WPA2-Enterprise Mixed car il fournit une connexion moins sécurisée. L'authentification permettant de déterminer si un utilisateur obtient l'accès est contrôlée par un serveur RADIUS. Cela signifie que chaque utilisateur connecté recevra une clé unique pour accéder au réseau sans fil. WPA2 utilise les méthodes de cryptage TKIP (Temporal Key Integrity Protocol) et AES (Advanced Encryption Standard). De plus en plus de périphériques réseau prennent en charge le protocole TKIP, mais AES est la méthode de cryptage la plus puissante.

Étape 1. Connectez-vous à l'utilitaire de configuration Web et choisissez Wireless > Basic Settings. La page Basic Settings s'ouvre.

Étape 2. Cochez la case du réseau que vous souhaitez modifier.

Étape 3. Cliquez sur Edit Security Mode pour modifier la sécurité du réseau spécifié. La page Security Settings s'ouvre :



Étape 4. (Facultatif) Dans la liste déroulante Sélectionner le SSID, sélectionnez le SSID pour lequel vous souhaitez configurer la sécurité.

Étape 5. Dans la liste déroulante Security Mode, sélectionnez WPA2-Enterprise ou WPA2-Enterprise Mixed. WPA2-Enterprise (WPA2 entreprise) est utilisé lorsque tous les périphériques du réseau sans fil prennent en charge AES. WPA2-Enterprise Mixed est utilisé lorsque tous les périphériques ne prennent pas en charge AES.

Remarque : Le type de cryptage utilisé par la méthode de sécurité est affiché dans le champ Encryption (Cryptage).

Étape 6. Entrez l’adresse IP du serveur RADIUS dans le champ RADIUS Server.

Étape 7. Entrez le port utilisé pour accéder au serveur RADIUS dans le champ RADIUS Port.

Étape 8. Entrez la clé pré-partagée pour les utilisateurs sans fil dans le champ Shared Key (Clé partagée). Une clé pré-partagée est une clé utilisée par tous les utilisateurs. La fonctionnalité de clé prépartagée est une fonctionnalité de sécurité ajoutée à l'authentification RADIUS.

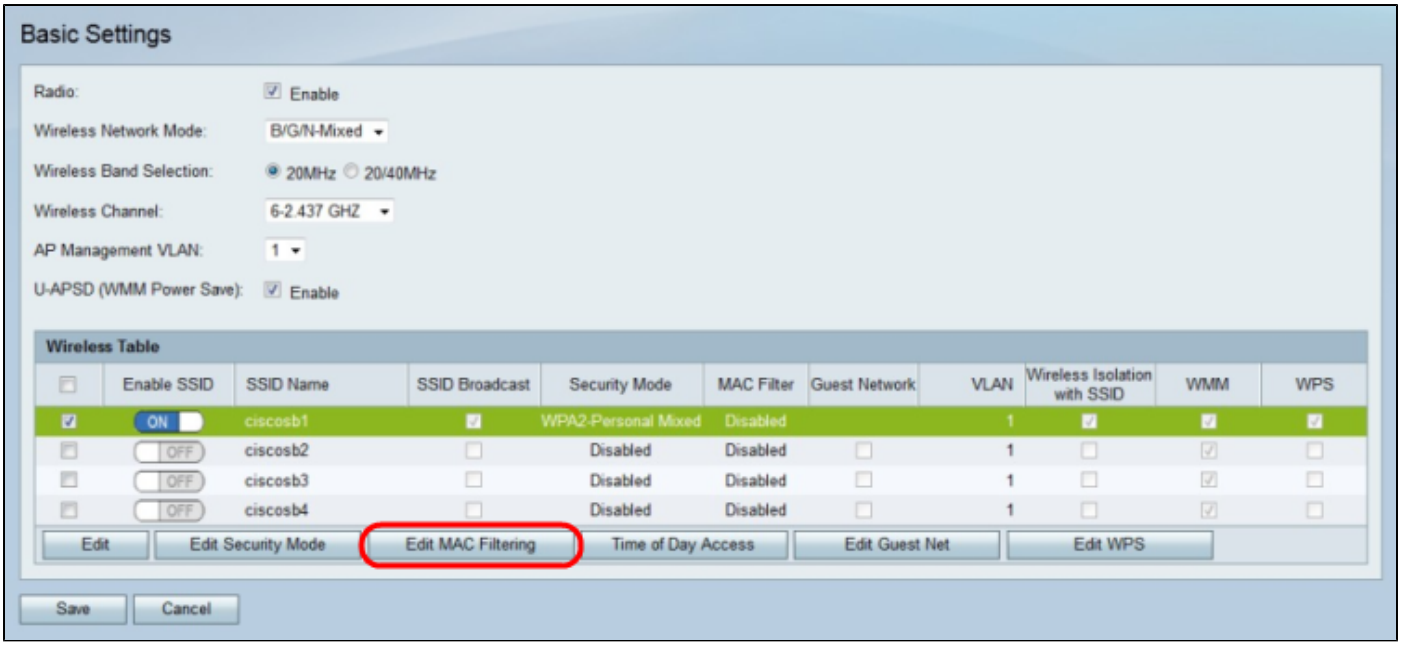
Étape 9. Entrez une heure dans le champ Key Renewal (Renouvellement de clé). Il s'agit de la durée pendant laquelle le routeur RV215W utilisera la clé avant d'en générer une nouvelle.

Étape 10. Cliquez sur Save.

Modifier le filtrage MAC

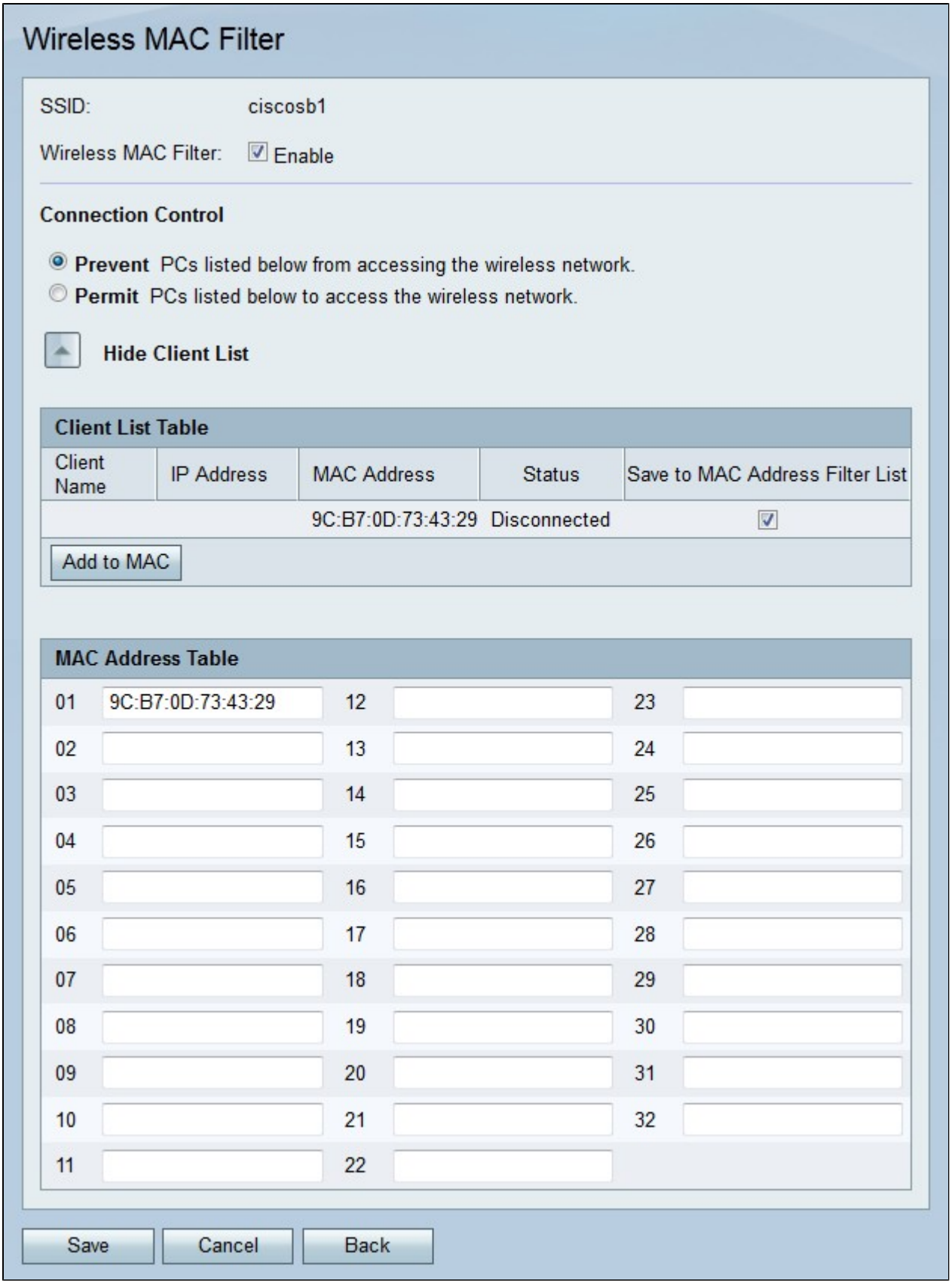
Le filtrage MAC permet d'autoriser ou de refuser l'accès au réseau sans fil en fonction de l'adresse MAC du périphérique connecté.

Étape 1. Connectez-vous à l’utilitaire de configuration Web et choisissez Wireless **>** Basic Settings. La page Basic Settings s'ouvre :



Étape 2. Cochez la case du réseau que vous souhaitez modifier.

Étape 3. Cliquez sur Edit MAC Filtering pour créer une liste de contrôle d’accès MAC pour le réseau spécifié. La page Wireless MAC Filter s'ouvre :



Étape 4. Cochez Enable pour activer le filtrage MAC sur le réseau.

Étape 5. Cliquez sur la case d'option correspondant au type de liste souhaité dans le champ Contrôle de connexion.

· Prevent PCs : empêche les ordinateurs dont les adresses MAC sont répertoriées d’accéder au réseau.

· Permit PCs : permet aux ordinateurs dotés des adresses MAC répertoriées d'accéder au réseau.

Étape 6. Entrez les adresses MAC souhaitées dans la table d’adresses MAC.

Étape 7. Cliquez sur Save.

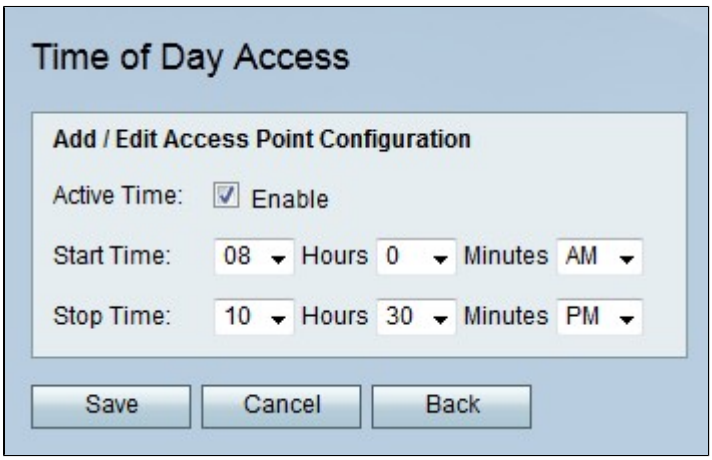
Accès à l'heure

La fonction d'accès à l'heure du jour est utilisée pour autoriser uniquement l'accès aux utilisateurs en fonction d'une planification configurée.

Étape 1. Connectez-vous à l’utilitaire de configuration Web et choisissez Wireless > Basic Settings. La page Basic Settings s'ouvre :

Étape 2. Cochez la case du réseau que vous souhaitez modifier.

Étape 3. Cliquez sur Time of Day Access pour configurer quand les utilisateurs peuvent accéder au réseau spécifié. La page Time of Day Access s'ouvre :



Étape 4. Cochez Enable dans le champ Active Time pour activer l’accès à l’heure du jour pour le réseau.

Étape 5. Entrez l’heure à laquelle l’accès au réseau commence dans le champ Heure de début.

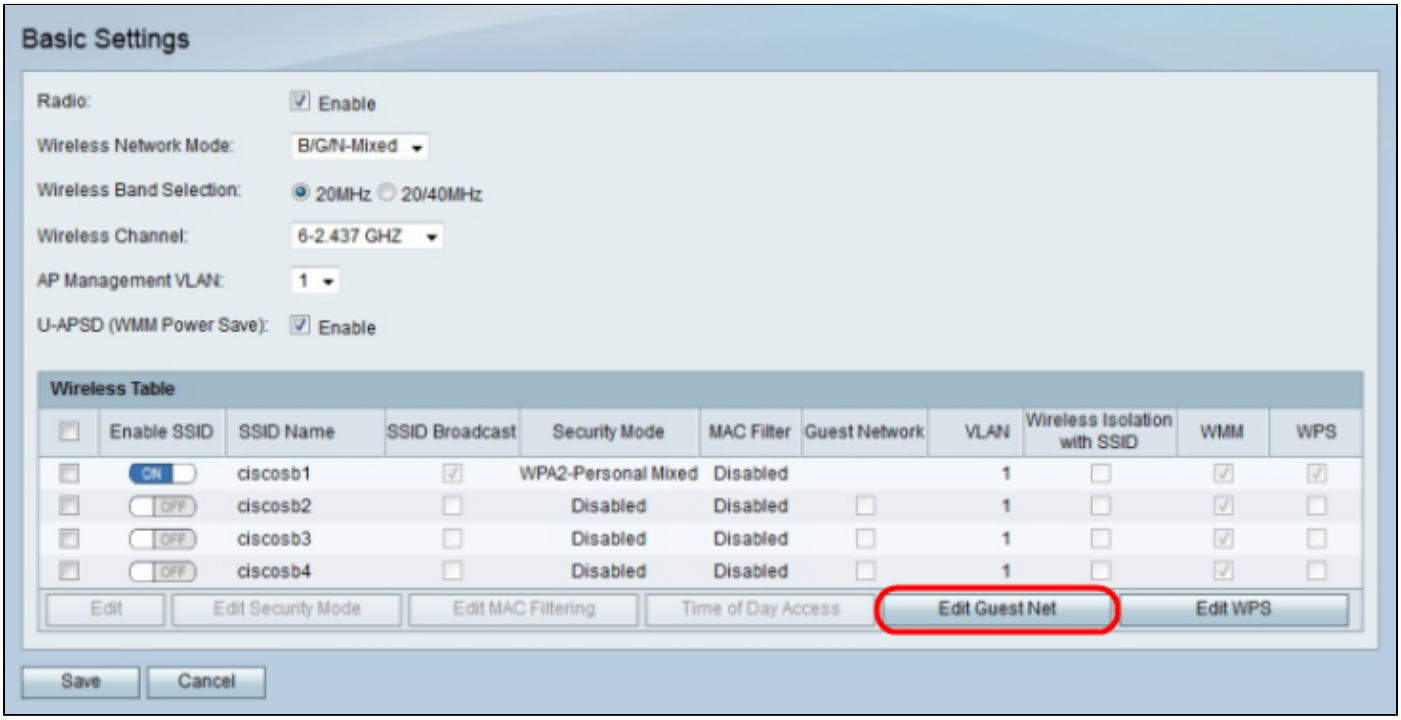
Étape 6. Entrez l’heure à laquelle l’accès au réseau se termine dans le champ Heure d’arrêt.

Étape 7. Cliquez sur Save.

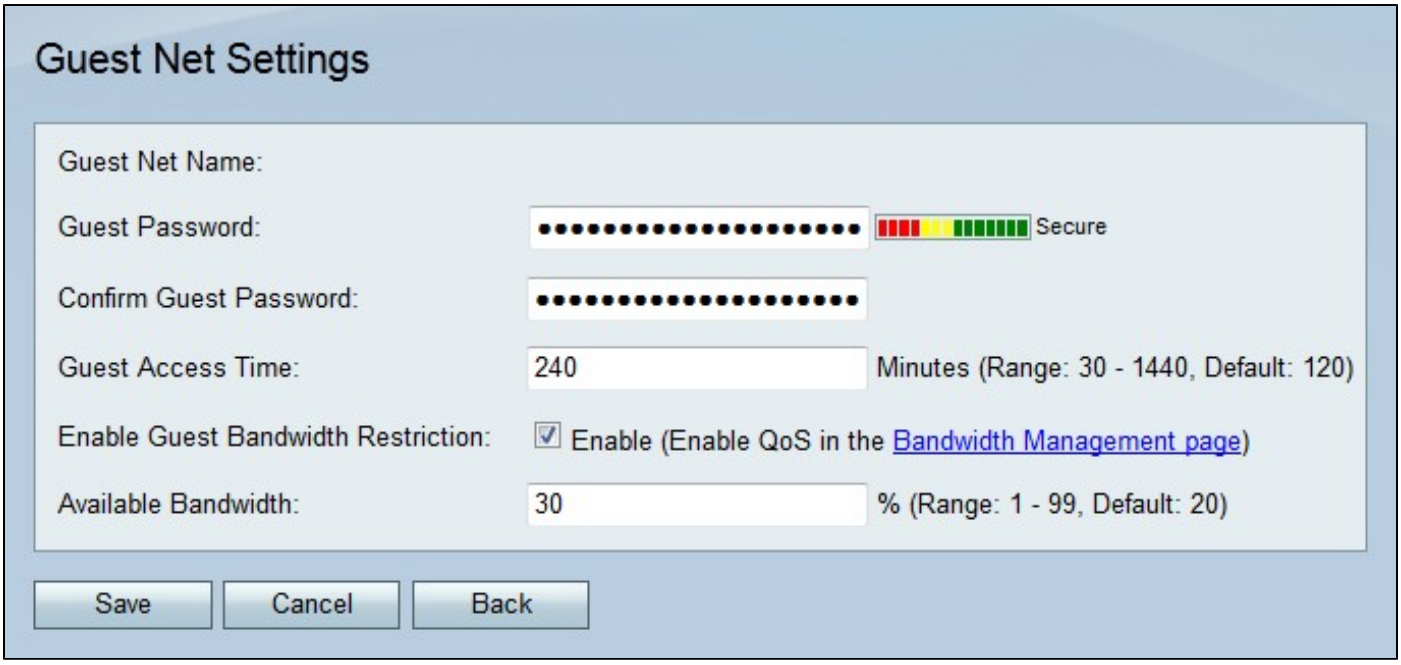
Modifier le réseau invité

Un réseau invité est une petite section d'un réseau conçue pour des utilisateurs temporaires. Il permet aux invités d'utiliser le réseau sans avoir à exposer des clés Wi-Fi privées. Un réseau invité peut être configuré pour limiter le temps d'accès et l'utilisation de la bande passante d'un utilisateur.

Étape 1. Connectez-vous à l'utilitaire de configuration Web et choisissez Wireless > Basic Settings. La page Basic Settings s'ouvre :



Étape 2. Cliquez sur Edit Guest Network pour configurer le réseau invité. La page Guest Net Settings s'ouvre :



Étape 3. Entrez un mot de passe que les utilisateurs utiliseront pour entrer le réseau invité dans le champ Mot de passe invité.

Étape 4. Entrez à nouveau le mot de passe que les utilisateurs utiliseront pour entrer le réseau invité dans le champ Confirmer le mot de passe invité.

Étape 5. Entrez l'heure à laquelle les utilisateurs sont autorisés à rester connectés au réseau invité dans le champ Guest Access Time.

Étape 6. Cochez la case Enable Guest Bandwidth Restriction pour limiter la quantité de bande passante que le réseau invité reçoit.

Remarque : La gestion de la bande passante doit être activée sur la page Gestion de la bande passante.

Étape 7. Entrez le pourcentage de bande passante qui doit être disponible pour le réseau invité dans le champ Bande passante disponible.

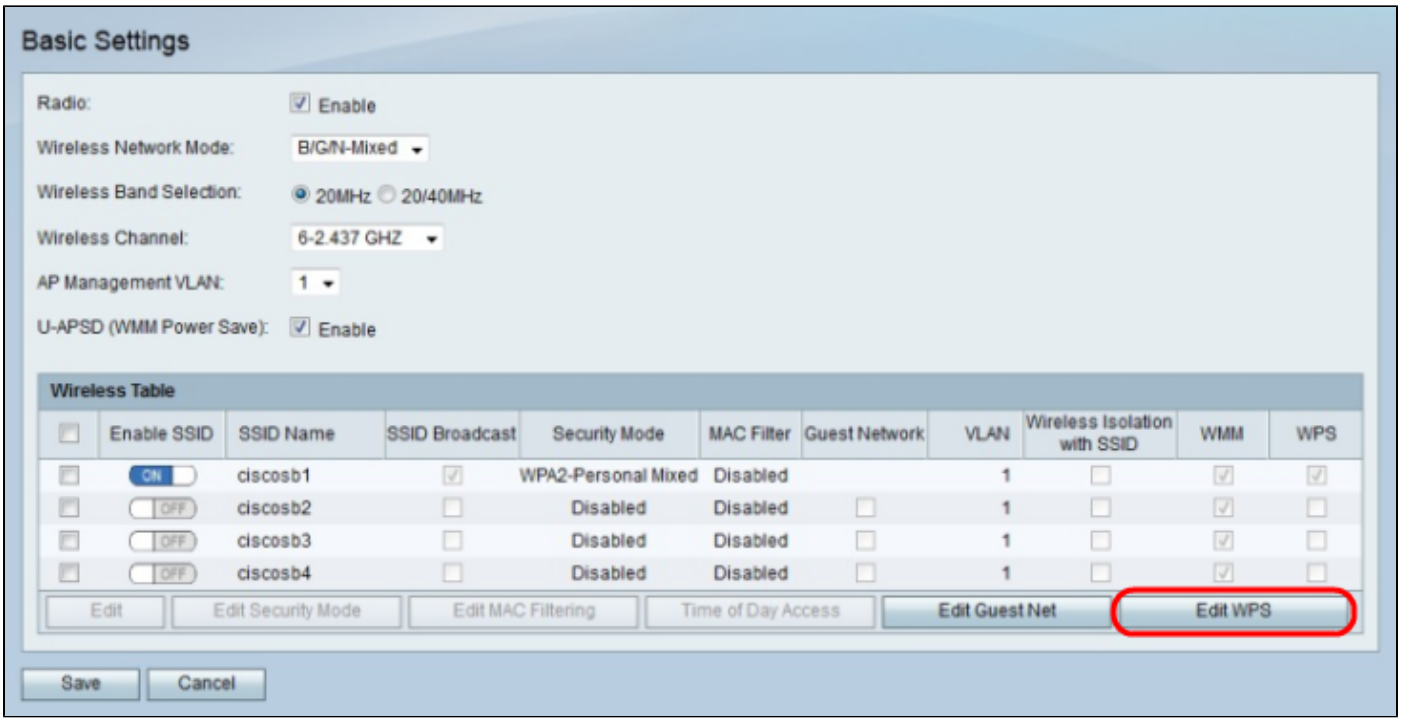
Étape 8. Cliquez sur Save.

Configuration de la méthode WPS 1

La fonction Wi-Fi Protected Setup (WPS) permet de configurer un réseau sans fil de manière simple et sécurisée. Pour se connecter à WPS, le périphérique de connexion doit prendre en charge WPS et être compatible avec la sécurité WPA. La première méthode de configuration est une méthode simple qui nécessite d'appuyer sur le bouton WPS du RV215W et sur le bouton du

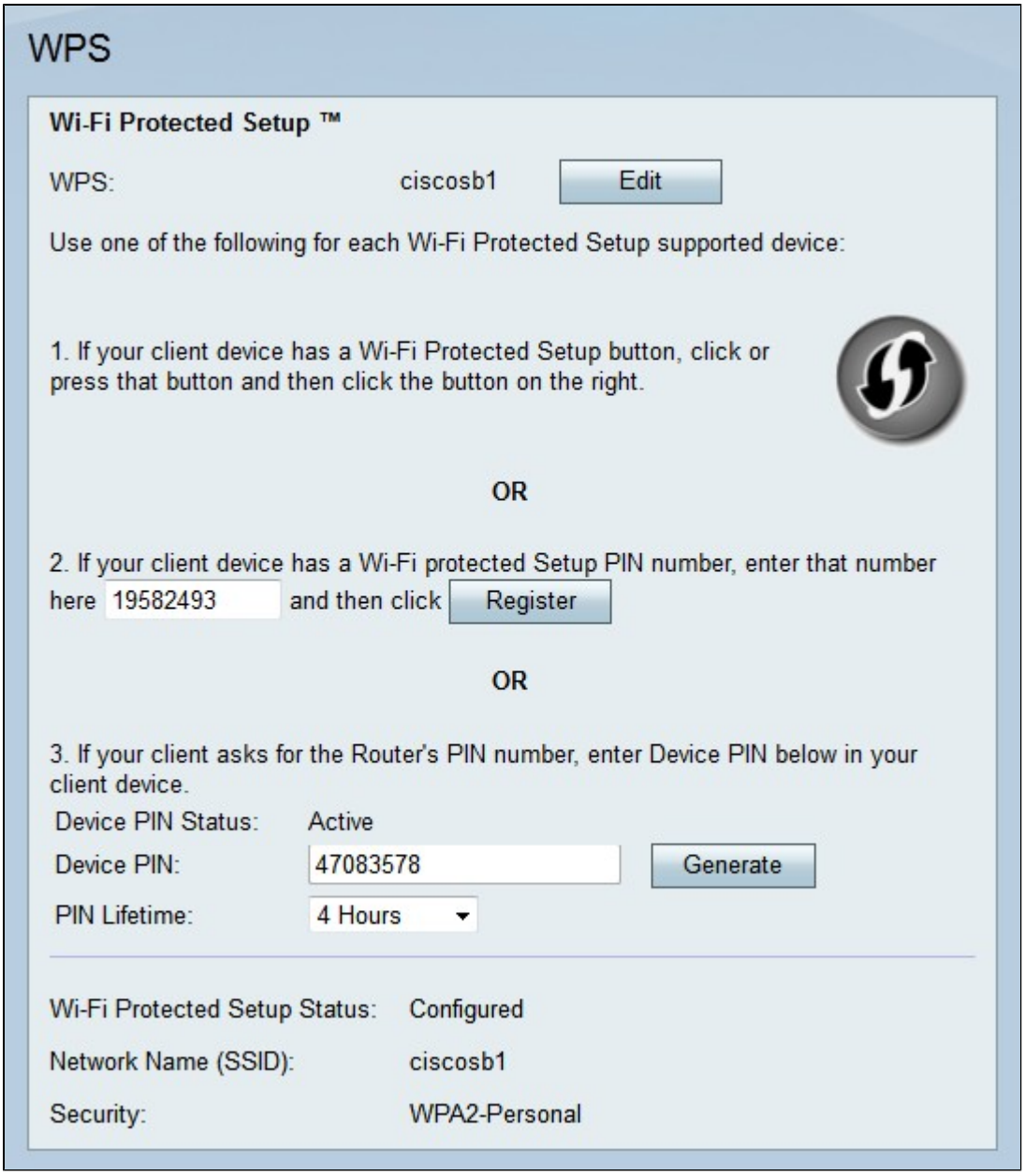
périphérique client. Une fois les deux boutons enfoncés, le périphérique client est connecté au réseau WPS.

Étape 1. Connectez-vous à l'utilitaire de configuration Web et choisissez Wireless > Basic Settings. La page Basic Settings s'ouvre :



Étape 2. Cliquez sur Edit WPS pour configurer WPS. La page WPS s'ouvre :

Remarque : La page WPS est également accessible via Wireless > WPS.



Étape 3. Cliquez sur Edit pour choisir le réseau sans fil sur lequel activer WPS.



Étape 4. Cliquez sur le bouton WPS sur la page WPS.

Étape 5. Cliquez sur le bouton WPS sur le périphérique client ou sur un écran d'utilitaire du périphérique client pour connecter le périphérique client au réseau WPS.

Les champs suivants affichent des informations sur la configuration WPS.

· Wi-Fi Protected Setup Status : état de la configuration WPS.

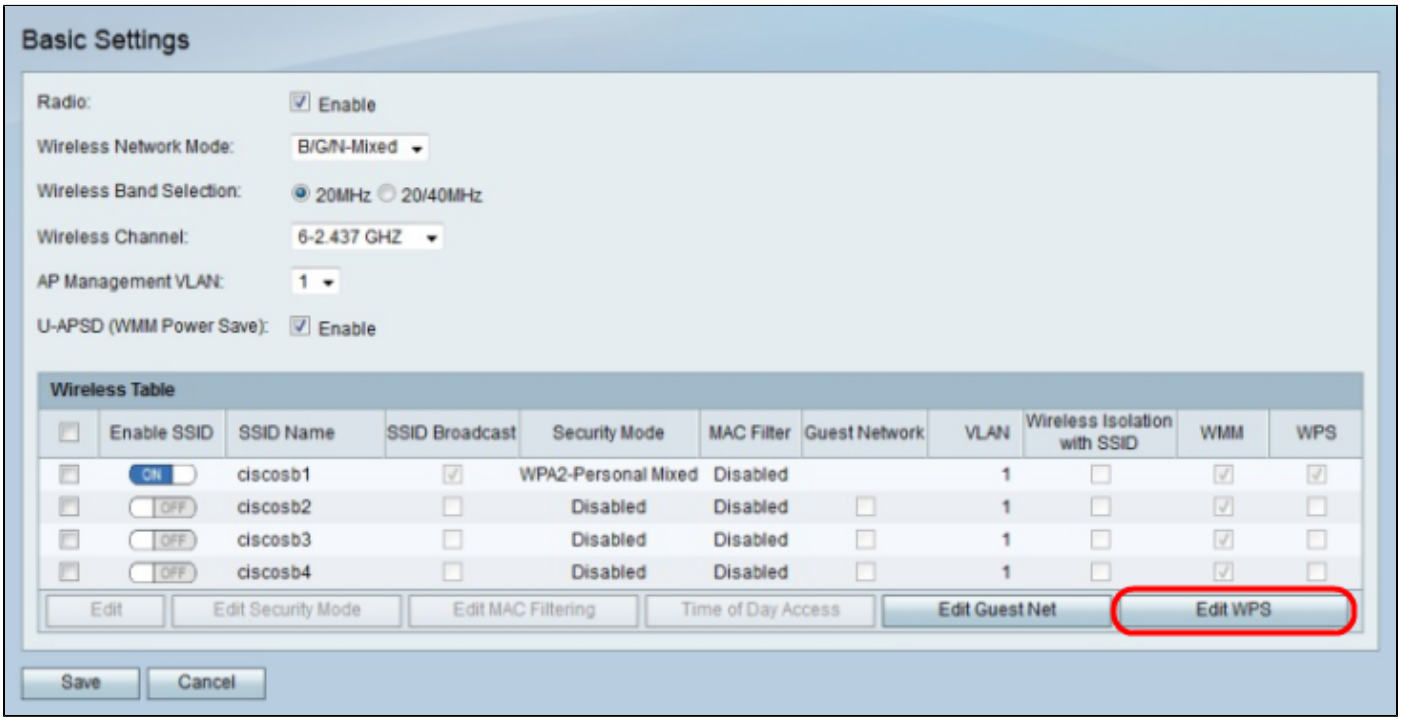
· Network Name (SSID) : nom de réseau attribué à la configuration WPS par le routeur RV215W.

· WPA2-Personal : type de sécurité utilisé par la configuration WPS.

Configuration de la méthode WPS 2

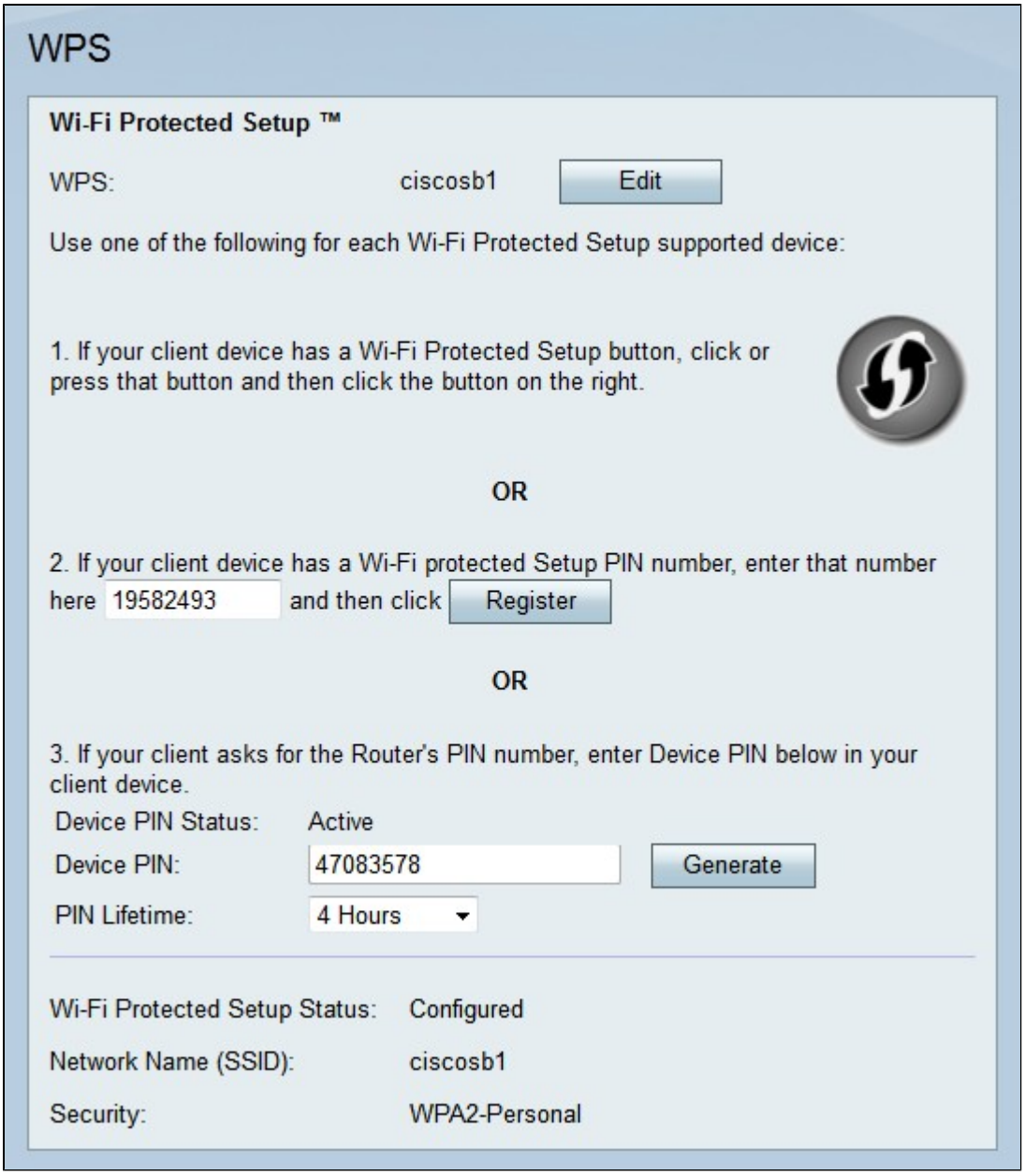
La fonction Wi-Fi Protected Setup (WPS) permet de configurer un réseau sans fil de manière simple et sécurisée. Pour se connecter à WPS, le périphérique de connexion doit prendre en charge WPS et être compatible avec la sécurité WPA. La deuxième méthode nécessite le code PIN du périphérique client. Une fois le code PIN saisi sur la page WPS, le périphérique client se connecte au réseau WPS.

Étape 1. Connectez-vous à l'utilitaire de configuration Web et choisissez Wireless > Basic Settings. La page Basic Settings s'ouvre :



Étape 2. Cliquez sur Edit WPS pour configurer WPS. La page WPS s'ouvre :

Remarque : La page WPS est également accessible via Wireless > WPS.



Étape 3. Cliquez sur Edit pour choisir le réseau sans fil sur lequel activer WPS.

Étape 4. Entrez le code PIN du périphérique client.

Étape 5. Cliquez sur Register pour créer le réseau WPS.

Les champs suivants affichent des informations sur la configuration WPS.

· Wi-Fi Protected Setup Status : état de la configuration WPS.

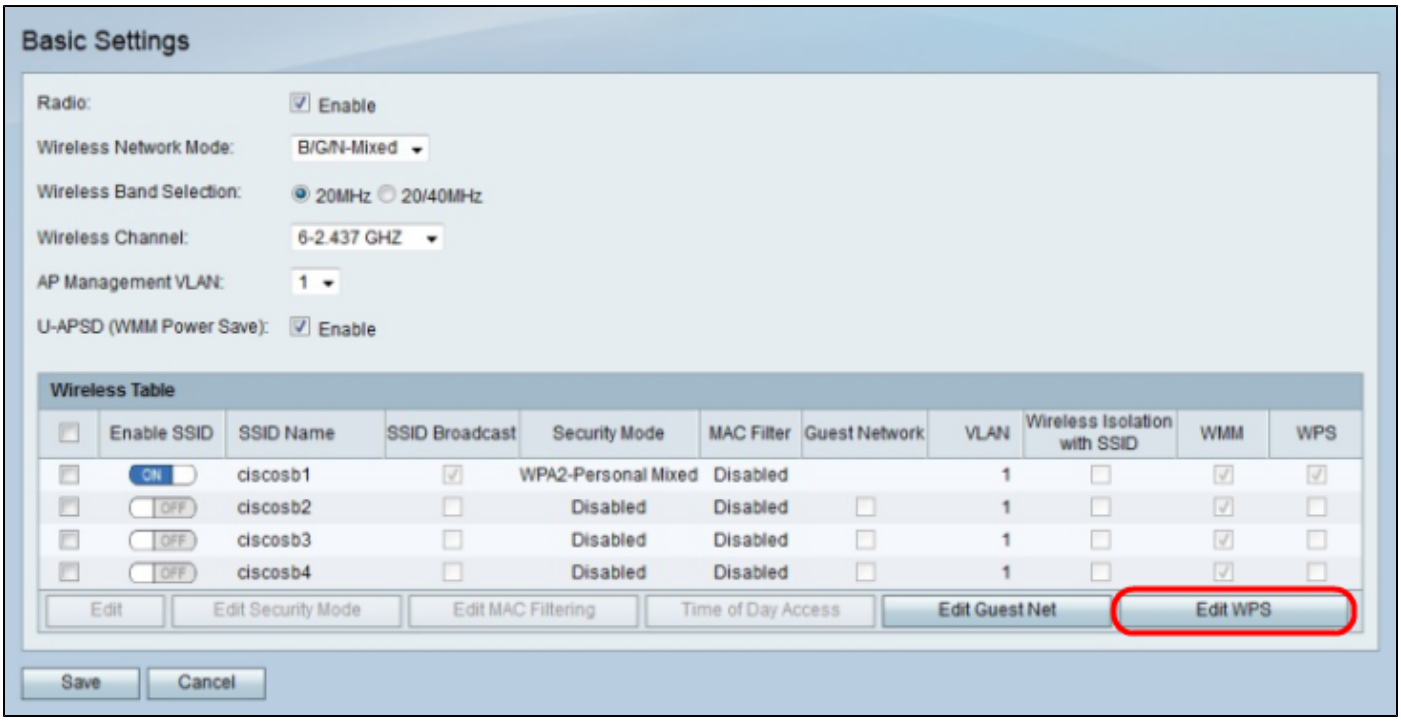
· Network Name (SSID) : nom de réseau attribué à la configuration WPS par le routeur RV215W.

· WPA2-Personal : type de sécurité utilisé par la configuration WPS.

Configuration de la méthode WPS 3

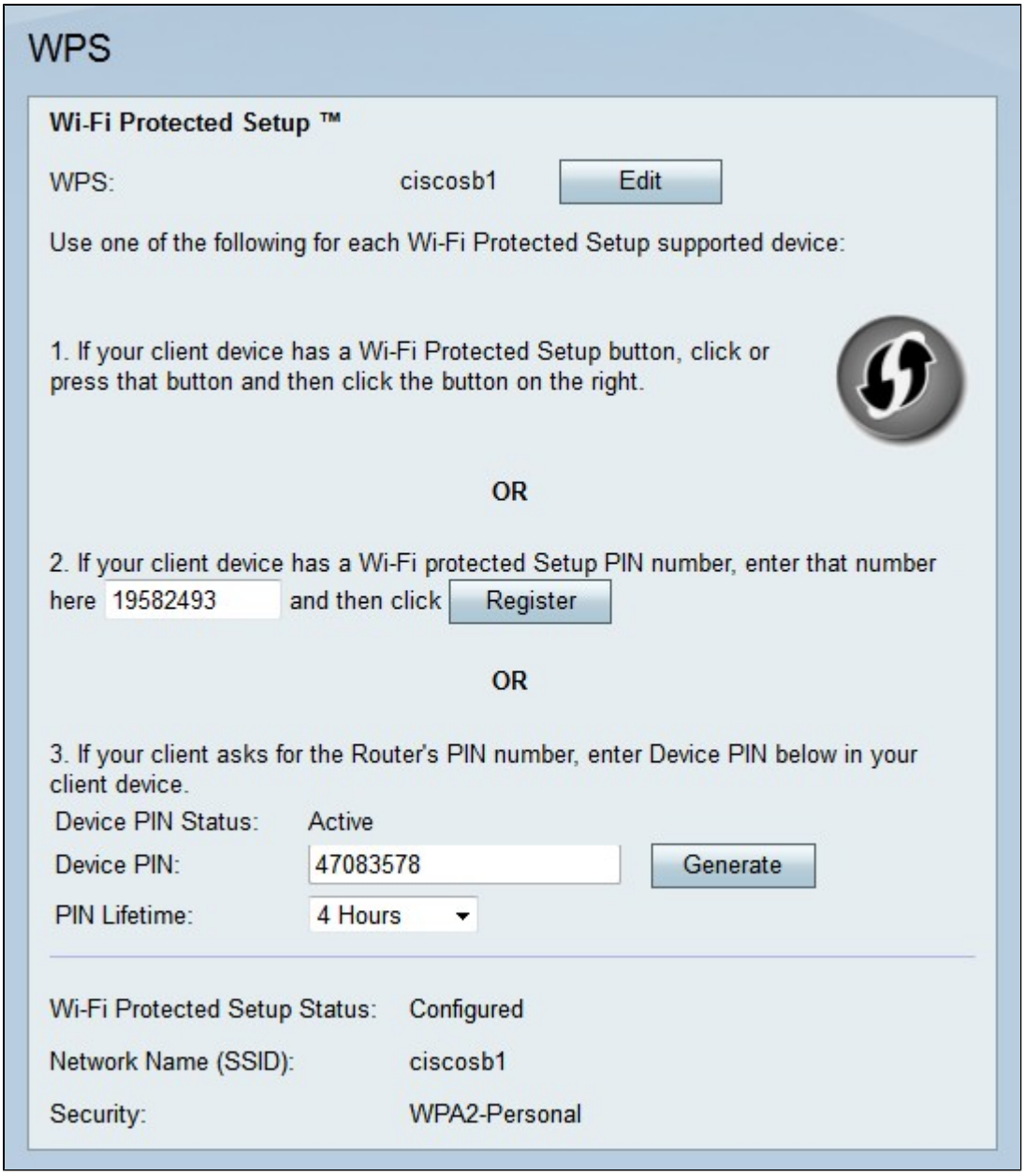
La fonction Wi-Fi Protected Setup (WPS) permet de configurer un réseau sans fil de manière simple et sécurisée. Pour se connecter à WPS, le périphérique de connexion doit prendre en charge WPS et être compatible avec la sécurité WPA. La troisième méthode exige que l'utilisateur saisisse le code PIN du RV215W sur la page de configuration WPS du périphérique client.

Étape 1. Connectez-vous à l'utilitaire de configuration Web et choisissez Wireless > Basic Settings. La page Basic Settings s'ouvre :



Étape 2. Cliquez sur Edit WPS pour configurer WPS. La page WPS s'ouvre :

Remarque : La page WPS est également accessible via Wireless > WPS.



Étape 3. Cliquez sur Edit pour choisir le réseau sans fil sur lequel activer WPS.

Étape 4. Cliquez sur Generate pour générer un code PIN pour le routeur RV215W.

Étape 5. Dans la liste déroulante Durée de vie du PIN, sélectionnez la durée écoulée avant la génération d'un nouveau PIN.

Étape 6. Entrez le code PIN RV215W indiqué dans la configuration du périphérique client. Le périphérique client se connecte au réseau WPS.

Les champs suivants affichent des informations sur la configuration WPS.

· Wi-Fi Protected Setup Status : état de la configuration WPS.

· Network Name (SSID) : nom de réseau attribué à la configuration WPS par le routeur RV215W.

· WPA2-Personal : type de sécurité utilisé par la configuration WPS.

Si vous souhaitez consulter toute autre documentation sur le routeur RV215W, cliquez ici.

Visionner une vidéo connexe à cet article...

Cliquez ici pour consulter les autres discussions techniques (Tech Talks) de Cisco

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.