Paramètres de sécurité SSID sur le routeur RV110W

Objectif

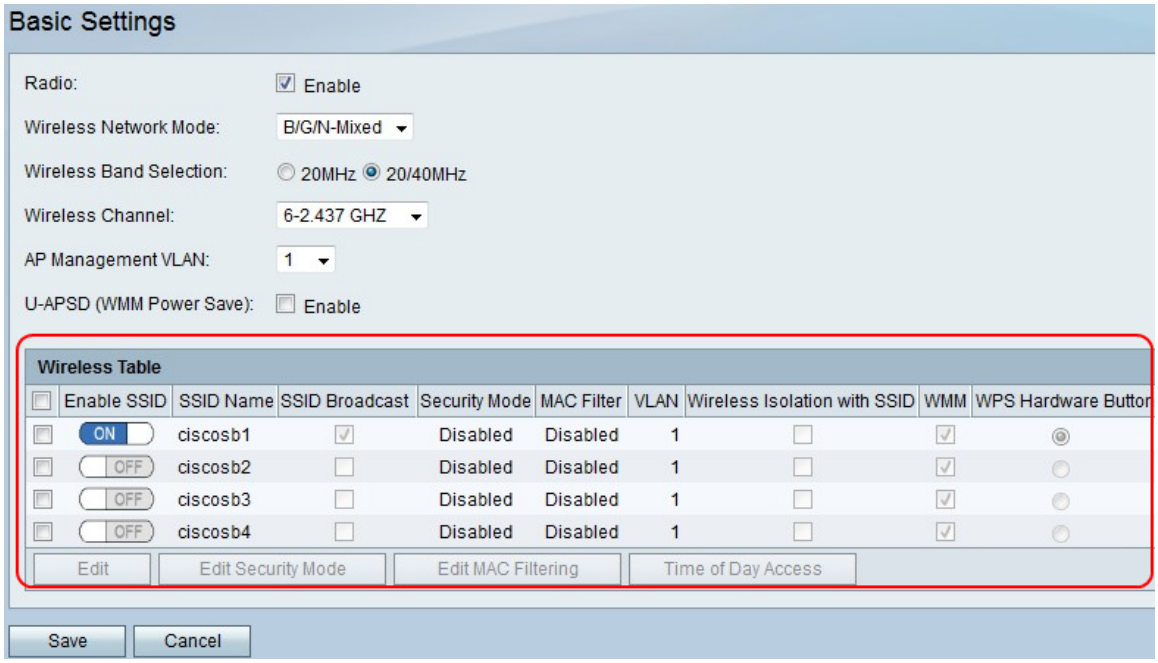
Les modes de sécurité offrent une protection pour un réseau sans fil. Différents SSID (Service Set ID) peuvent avoir différents modes de sécurité. Les SSID peuvent exécuter différentes fonctions pour le réseau ; par conséquent, les SSID peuvent nécessiter différentes mesures de sécurité. Cet article explique comment configurer les paramètres de sécurité pour un SSID sur le RV110W.

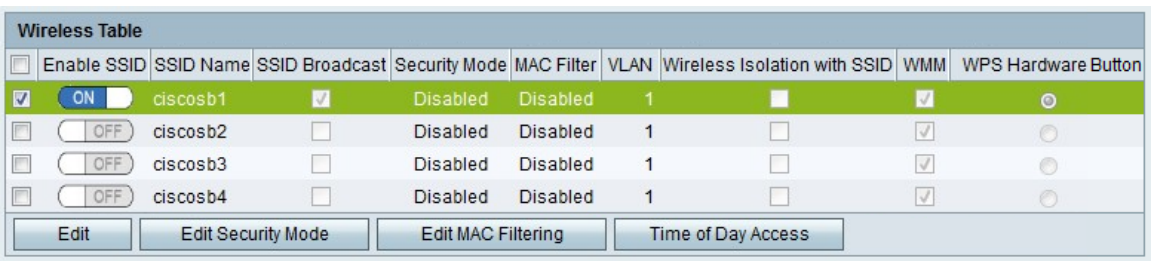
Périphériques pertinents

- RV110W

Étapes de procédure

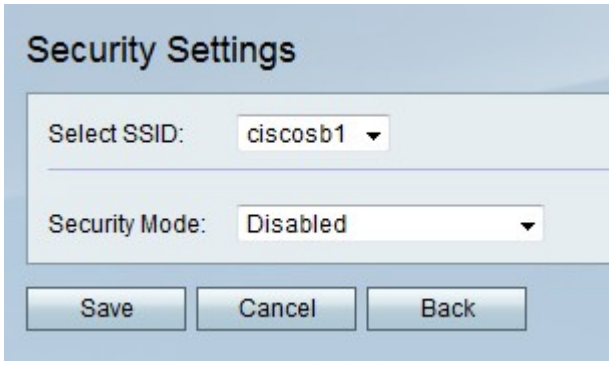
Étape 1. Utilisez l'utilitaire de configuration Web pour sélectionner **Wireless > Basic Settings**.





Étape 2. Dans le tableau Wireless, cochez la case d'un SSID pour lequel vous souhaitez modifier les paramètres de sécurité.

Étape 3. Cliquez sur **Modifier le mode de sécurité**. La page *Paramètres de sécurité s'*affiche.



Étape 4. Dans le menu déroulant Sélectionner le SSID, sélectionnez un SSID pour lequel vous souhaitez modifier les paramètres de sécurité.

Désactiver le mode de sécurité

Cette procédure montre comment désactiver le mode de sécurité d'un SSID qui ne nécessite aucune information de sécurité pour utiliser le SSID.

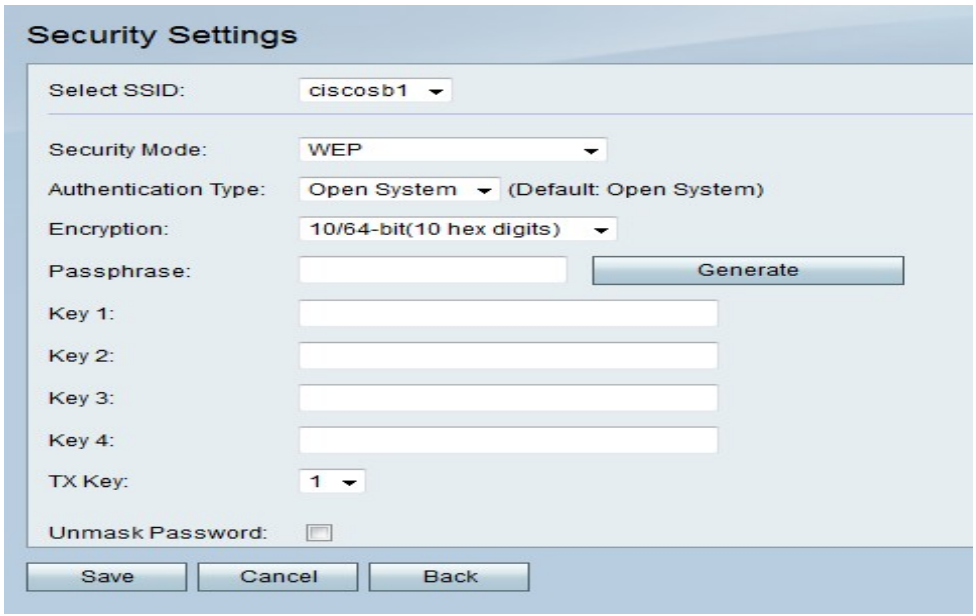
Étape 1. Dans le menu déroulant Security Mode, sélectionnez **Disabled**.

Étape 2. Cliquez sur **Enregistrer** pour enregistrer les modifications, **Annuler** pour les annuler ou **Précédent** pour revenir à la page précédente.

Mode de sécurité WEP

Cette procédure montre comment définir le mode WEP (Wired Equivalent Privacy) comme mode de sécurité d'un SSID. Le mode WEP n'est pas le mode de sécurité le plus sécurisé, mais il peut être la seule option si certains périphériques réseau ne prennent pas en charge le mode WPA.

Étape 1. Dans le menu déroulant Security Mode, sélectionnez **WEP**.



Étape 2. Dans le menu déroulant Authentication Type, sélectionnez une option.

- Open System : cette option est plus directe et plus sécurisée que l'authentification par clé partagée.

- Shared Key : cette option est moins sécurisée que Open System.

Étape 3. Dans le menu déroulant Cryptage, choisissez 10/64 bits (10 chiffres hexadécimaux), qui utilise une clé 40 bits, ou 26/128 bits (26 chiffres hexadécimaux), qui utilise une clé 104 bits.

Étape 4. Dans le champ Passphrase (Phrase de passe), saisissez une phrase de passe comportant des lettres et des chiffres d'au moins 8 caractères.

Étape 5. Cliquez sur **Generate** pour créer quatre clés WEP dans les champs Key (Clé) ou saisissez manuellement les clés WEP dans les champs Key (Clé).

Étape 6. Dans le menu déroulant TX Key, sélectionnez le numéro de champ Key de la clé WEP que vous souhaitez utiliser comme clé partagée.

Étape 7. Cochez la case **Démasquer le mot de passe** si vous voulez révéler les caractères de mot de passe.

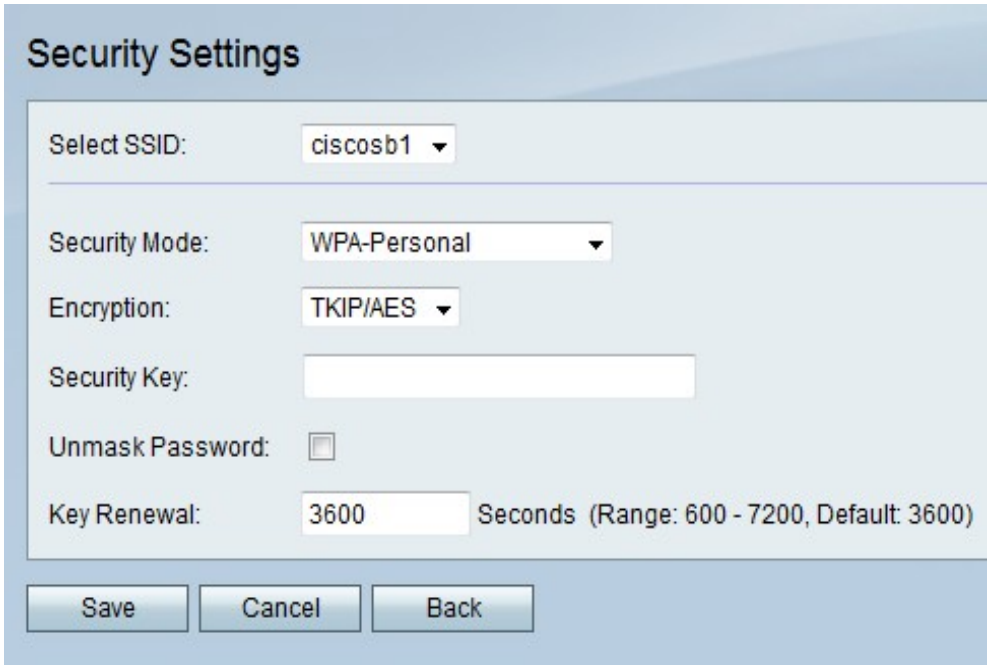
Étape 8. Cliquez sur **Enregistrer** pour enregistrer les modifications, **Annuler** pour les annuler ou **Précédent** pour revenir à la page précédente.

Mode de sécurité mixte WPA-Personal, WPA2-Personal et WPA2-Personal

Le mode WPA (Wi-Fi Protected Access) est un mode de sécurité plus puissant que le mode WEP. WPA-Personal peut utiliser le protocole TKIP (Temporal Key Integrity Protocol) ou AES (Advanced Encryption Standard) pour le chiffrement. WPA2-Personal utilise uniquement AES pour le chiffrement et une clé prépartagée (PSK) pour l'authentification. WPA2-Personal Mixed prend en charge les clients WPA et WPA2 et utilise AES et PSK. Cette procédure montre comment configurer WPA-Personal, WPA2-Personal ou WPA2-Personal Mixed comme mode de sécurité pour un SSID.

Étape 1. Dans le menu déroulant Security Mode, sélectionnez une option.

- WPA-Personal : cette option prend en charge AES et TKIP.
- WPA2-Personal : cette option prend en charge AES et PSK.
- WPA2-Personal Mixed : cette option prend en charge les clients WPA et WPA2.



Étape 2. Si vous choisissez WPA-Personal (WPA personnel), choisissez un type de cryptage dans le menu déroulant Encryption (Cryptage).

- TKIP/AES - Cette option est compatible avec les périphériques plus anciens qui ne prennent pas en charge AES.
- AES : cette option est plus sécurisée que TKIP/AES.

Étape 3. Dans le champ Security Key, saisissez une phrase de lettres et de chiffres qui restreint l'accès au réseau.

Étape 4. Cochez la case **Démasquer le mot de passe** si vous voulez révéler les caractères de mot de passe.

Étape 5. Dans le champ Key Renewal (Renouvellement de clé), saisissez la fréquence en secondes à laquelle le réseau renouvelle la clé.

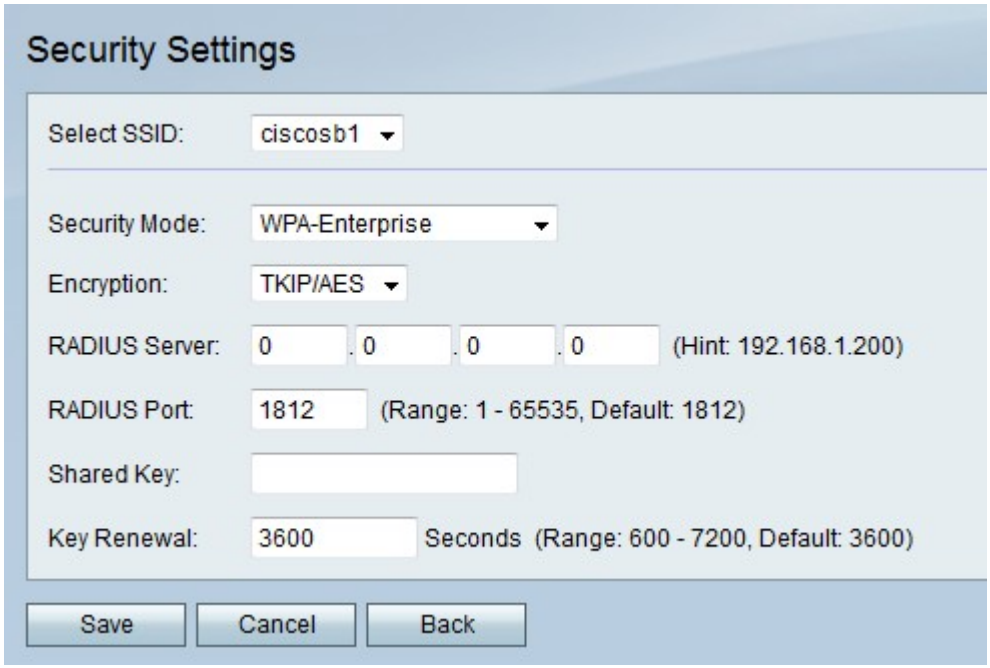
Étape 6. Cliquez sur **Enregistrer** pour enregistrer les modifications, **Annuler** pour les annuler ou **Précédent** pour revenir à la page précédente.

Mode de sécurité mixte WPA-Enterprise, WPA2-Enterprise et WPA2-Enterprise

Les modes de sécurité d'entreprise utilisent l'authentification serveur RADIUS (Remote Authentication Dial In User Service). RADIUS est un protocole réseau qui utilise un serveur distinct et le trafic en provenance et à destination du réseau doit passer par le serveur RADIUS. Cette procédure montre comment configurer WPA-Enterprise, WPA2-Enterprise ou WPA2-Enterprise Mixed comme mode de sécurité pour un SSID.

Étape 1. Dans le menu déroulant Security Mode, sélectionnez une option.

- WPA-Enterprise : cette option utilise RADIUS, AES et TKIP.
- WPA2-Enterprise : cette option utilise RADIUS, AES et PSK.
- WPA2-Enterprise Mixed : cette option utilise RADIUS et prend en charge les clients WPA et WPA2.



Étape 2. Si vous choisissez WPA-Enterprise, choisissez un type de cryptage dans le menu déroulant Encryption (Cryptage).

- TKIP/AES - Cette option est compatible avec les périphériques plus anciens qui ne prennent pas en charge AES.
- AES : cette option est plus sécurisée que TKIP/AES.

Étape 3. Dans le champ RADIUS Server, saisissez l'adresse IP du serveur RADIUS.

Étape 4. Dans le champ Port RADIUS, saisissez le numéro de port sur lequel le réseau accède au serveur RADIUS.

Étape 5. Dans le champ Shared Key (Clé partagée), saisissez une phrase de lettres et de chiffres qui restreint l'accès au réseau.

Étape 6. Dans le champ Key Renewal (Renouvellement de clé), saisissez la fréquence en secondes à laquelle le réseau renouvelle la clé.

Étape 7. Cliquez sur **Enregistrer** pour enregistrer les modifications, **Annuler** pour les annuler ou **Précédent** pour revenir à la page précédente.