

Paramètres sans fil de base sur le routeur VPN CVR100W

Objectif

Un réseau local sans fil (WLAN) utilise la communication radio pour connecter des périphériques sans fil à un réseau local. Par exemple, un point d'accès Wi-Fi dans un café. Les réseaux sans fil sont utiles car ils réduisent les coûts de câblage et sont faciles à configurer.

Cet article explique comment configurer les paramètres sans fil de base sur le routeur VPN CVR100W, qui inclut la configuration de la sécurité du réseau. Pour connaître les paramètres sans fil avancés, reportez-vous à l'article [Configuration sans fil avancée sur le routeur VPN CVR100W](#).

Périphérique applicable

Routeur VPN · CVR100W

Version du logiciel

•1.0.1.19

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 :

The screenshot shows the 'Basic Settings' page for the wireless network configuration. The 'Radio' checkbox is checked and labeled 'Enable'. 'Wi-Fi Power' is set to 100%. 'Wireless Network Mode' is set to 'B/G/N-Mixed'. 'Wireless Band Selection' has '20MHz' selected. 'Wireless Channel' is set to 'Auto'. 'AP Management VLAN' is set to '1'. 'U-APSD (WMM Power Save)' is unchecked. Below these settings is a 'Wireless Table' with the following data:

	Enable SSID	SSID Name	SSID Broadcast	Security Mode	MAC Filter	CSC	VLAN	SSID Isolation	WMM	WPS
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Cisco-4D61	<input checked="" type="checkbox"/>	WPA2-Personal	Disabled	<input type="checkbox"/>	1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	cisco-SSID2	<input type="checkbox"/>	Disabled	Disabled	<input type="checkbox"/>	1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	cisco-SSID3	<input type="checkbox"/>	Disabled	Disabled	<input type="checkbox"/>	1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	cisco-guest	<input checked="" type="checkbox"/>	Disabled	Disabled	<input type="checkbox"/>	3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Buttons at the bottom include 'Edit', 'Edit Security Mode', 'Edit MAC Filtering', 'Time of Day Access', 'Edit Guest Net', 'Edit CSC', 'Edit WPS', 'Save', and 'Cancel'.

Étape 2. Cochez la case **Activer** dans le champ Radio pour activer la radio sans fil.

Étape 3. Dans la liste déroulante Wi-Fi Power (Alimentation Wi-Fi), sélectionnez

l'alimentation wi-fi. Cette alimentation wi-fi contrôle la puissance de l'émetteur de la radio wi-fi. Cette fonctionnalité est utile pour réduire ou augmenter la portée du signal. Cette fonction est utilisée pour économiser l'énergie.

- 100 % — Cette option active une puissance d'émetteur radio de 100 %.
- 50 % : cette option permet d'activer une puissance d'émission radio de 50 %.

Étape 4. Dans la liste déroulante Wireless Network Mode (Mode réseau sans fil), sélectionnez le mode sans fil. Cette option est basée sur les fonctionnalités sans fil des périphériques du réseau.

- B/G/N-Mixed : le réseau se compose d'un mélange de périphériques sans fil B, G et N.
- B-Only : le réseau se compose uniquement de périphériques sans fil B.
- G-Only : le réseau se compose uniquement de périphériques sans fil G.
- N-Only : le réseau se compose uniquement de périphériques sans fil N.
- B/G-Mixed : le réseau se compose d'un mélange de périphériques sans fil B et G.
- G/N Mixed : le réseau se compose d'un mélange de périphériques sans fil G et sans fil N.

Étape 5. Si le mode réseau se compose de 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). La bande passante supérieure indique la plus grande quantité de données que le signal peut transporter.

- 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 susceptible d'être plus interféré. Cette option n'est utilisée que si les périphériques sans fil connectés sont compatibles avec la fréquence 40 MHz.

Étape 6. 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. Si plusieurs radios utilisent le même canal, des interférences peuvent se produire.

Étape 7. Dans la liste déroulante AP Management VLAN, sélectionnez le VLAN de gestion. Le VLAN de gestion est le VLAN utilisé pour la gestion des périphériques à partir d'un emplacement distant.

Étape 8. (Facultatif) Pour activer la livraison automatique non planifiée de l'alimentation (U-APSD), cochez la case **Activer** dans le champ U-APSD. U-APSD est une fonctionnalité qui permet à la radio de conserver de l'énergie. Cependant, U-APSD peut réduire les performances de débit de la radio.

Étape 9. Cliquez **Save**.

Modifier la table sans fil

Étape 1. Cochez la case du réseau à modifier dans le tableau Wireless.

Wireless Table											
<input type="checkbox"/>	Enable SSID	SSID Name	SSID Broadcast	Security Mode	MAC Filter	CSC	VLAN	SSID Isolation	WMM	WPS	
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Cisco-4D61	<input checked="" type="checkbox"/>	WPA2-Personal	Disabled	<input type="checkbox"/>	1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	<input type="checkbox"/>	cisco-SSID2	<input type="checkbox"/>	Disabled	Disabled	<input type="checkbox"/>	1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
<input type="checkbox"/>	<input type="checkbox"/>	cisco-SSID3	<input type="checkbox"/>	Disabled	Disabled	<input type="checkbox"/>	1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
<input type="checkbox"/>	<input type="checkbox"/>	cisco-guest	<input checked="" type="checkbox"/>	Disabled	Disabled	<input type="checkbox"/>	3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

Étape 2. Cliquez sur **Modifier** pour modifier le réseau spécifié.

Étape 3. Cochez la case **Enable SSID** pour activer le réseau. SSID (Service Set Identifier) est le nom du réseau sans fil.

Étape 4. Dans le champ SSID Name, saisissez le nom du réseau. Tous les périphériques du réseau utilisent ce SSID pour communiquer entre eux.

Étape 5. Cochez la case **SSID Broadcast** pour activer la diffusion sans fil. Lorsque la diffusion SSID est activée, la disponibilité du routeur VPN CVR100W est annoncée aux périphériques sans fil voisins.

Étape 6. (Facultatif) Pour modifier le mode de sécurité, référez-vous à [Modifier le mode de sécurité](#).

Étape 7. (Facultatif) Pour modifier le filtre MAC, référez-vous à [Modifier le filtrage MAC](#).

Étape 8. (Facultatif) Pour activer Cisco Simple Connect (CSC), cochez la case **CSC**. CSC facilite la configuration d'un réseau sans fil et permet une connexion facile des périphériques sans fil au réseau. Le périphérique sans fil utilise CSC pour obtenir le SSID et le mot de passe du réseau, ce qui permet une connexion automatique au réseau. Pour modifier le CSC, reportez-vous à [Modifier le CSC](#).

Note: Le VLAN de Cisco Simple Connect ne peut pas être identique au VLAN actuel ou d'un autre SSID.

Étape 9. Dans la liste déroulante VLAN, sélectionnez le VLAN associé au réseau.

Étape 10. Cochez la case **Isolation SSID** pour empêcher les périphériques du réseau spécifié de communiquer entre eux.

Étape 11. Cochez **WMM** pour activer le mode WMM (Wi-Fi Multimedia) sur le réseau. WMM est utilisé pour améliorer la diffusion multimédia en continu sur des périphériques sans fil. Une priorité plus élevée est accordée au trafic multimédia envoyé via une connexion sans fil lorsque WMM est activé.

Étape 12. Cochez **WPS** pour affecter 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.

Note: Pour configurer WPS sur le routeur VPN CVR100W, reportez-vous à l'article [WiFi Protected Setup \(WPS\) sur le routeur VPN CVR100W](#).

Étape 13. Cliquez sur **Save**.

Modifier le mode de sécurité

Étape 1. Cochez la case du réseau à modifier dans le tableau Wireless.

Wireless Table											
<input type="checkbox"/>	Enable SSID	SSID Name	SSID Broadcast	Security Mode	MAC Filter	CSC	VLAN	SSID Isolation	WMM	WPS	
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Cisco-4D61	<input checked="" type="checkbox"/>	WPA2-Personal	Disabled	<input checked="" type="checkbox"/>	1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	<input type="checkbox"/>	cisco-SSID2	<input type="checkbox"/>	Disabled	Disabled	<input type="checkbox"/>	1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
<input type="checkbox"/>	<input type="checkbox"/>	cisco-SSID3	<input type="checkbox"/>	Disabled	Disabled	<input type="checkbox"/>	1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
<input type="checkbox"/>	<input type="checkbox"/>	cisco-guest	<input checked="" type="checkbox"/>	Disabled	Disabled	<input type="checkbox"/>	3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

Buttons: Edit, Edit Security Mode, Edit MAC Filtering, Time of Day Access, Edit Guest Net, Edit CSC, Edit WPS

Étape 2. Cliquez sur **Modifier le mode de sécurité** pour modifier la sécurité du réseau spécifié. La page *Paramètres de sécurité* s'affiche.

Security Settings

Select SSID: Cisco-4D61

Security Mode: WPA2-Personal

Encryption: WEP

Security Key: [] Very Strong

Show Password: []

Key Renewal: [] Range: 600 - 7200, Default: 3600

Buttons: Save, Cancel, Back

Étape 3. (Facultatif) Pour modifier le SSID pour lequel vous souhaitez configurer la sécurité, sélectionnez le SSID souhaité dans la liste déroulante Sélectionner le SSID.

Étape 4. Dans la liste déroulante Security Mode, sélectionnez le mode de sécurité à configurer.

· [Disable Security](#) - Cette option désactive la sécurité sur le routeur VPN CVR100W.

· [WEP Security](#) — WEP (Wired Equivalent Privacy) est un algorithme utilisé pour sécuriser un réseau sans fil. WEP est utilisé pour fournir une méthode de cryptage de base moins sécurisée que WPA. WEP est utilisé lorsque les périphériques réseau connectés ne prennent pas en charge WPA.

· [WPA-Personal Security](#) - Wi-Fi Protected Access (WPA) est une norme de sécurité pour les réseaux sans fil. WPA-Personal est une version de WPA qui est utilisée pour les réseaux composés de quelques utilisateurs. WPA-Personal (WPA personnel) fournit une clé partagée que chaque utilisateur utilise 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).

· [WPA-Enterprise Security](#) - WPA-Enterprise est une version de WPA recommandée pour un réseau composé de nombreux utilisateurs. L'authentification pour accéder au réseau est contrôlée par un serveur RADIUS. Chaque utilisateur connecté reçoit 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).

·[WPA2-Personal Security](#) — WPA2 est une amélioration de WPA et fournit plus de sécurité que WPA. WPA2-Personal (WPA2 personnel) est une version de WPA2 utilisée pour les réseaux avec peu d'utilisateurs. WPA2-Personal est plus sécurisé que WPA2-Personal Mixed. WPA2-Personal (WPA2 personnel) fournit une clé partagée que chaque utilisateur utilise pour accéder au réseau sans fil.

·[WPA2-Personal Mixed Security](#) — WPA2-Personal Mixed est une version de WPA2 qui est utilisée pour les réseaux avec peu d'utilisateurs. WPA2-Personal Mixed prend en charge la rétrocompatibilité pour les périphériques plus anciens qui ne peuvent pas utiliser WPA2. WPA2-Personal Mixed est une connexion moins sécurisée.

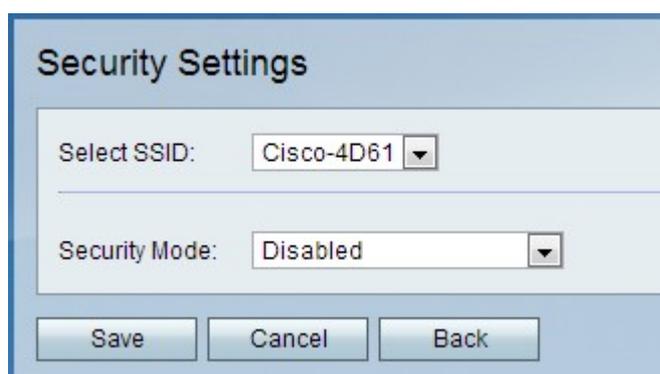
·[WPA2-Enterprise Security](#) — WPA2-Enterprise est une version de WPA2 qui est utilisée pour les réseaux avec de nombreux utilisateurs. WPA2-Enterprise est plus sécurisé que WPA2-Enterprise Mixed. L'authentification utilisée pour obtenir l'accès est contrôlée par un serveur RADIUS. Cela signifie que chaque utilisateur connecté se verra attribuer une clé unique pour accéder au réseau sans fil.

·[WPA2-Enterprise Mixed Security](#) — WPA2-Enterprise Mixed est une version de WPA2 utilisée pour les réseaux avec de nombreux utilisateurs. WPA2-Enterprise Mixed prend en charge la rétrocompatibilité pour les périphériques plus anciens qui ne peuvent pas utiliser WPA2. WPA2-Enterprise Mixed fournit une connexion moins sécurisée que WPA2-Enterprise. L'authentification utilisée pour obtenir l'accès est contrôlée par un serveur RADIUS. Cela signifie que chaque utilisateur connecté se verra attribuer une clé unique pour accéder au réseau sans fil.

Désactiver la sécurité

La sécurité sans fil peut être désactivée sur le routeur VPN CVR100W pour faciliter l'utilisation lors de la configuration des réseaux de test.

Note: Il n'est pas recommandé de désactiver la sécurité.



The image shows a web-based configuration interface for a Cisco router. The title is "Security Settings". There are two main configuration fields: "Select SSID:" with a dropdown menu showing "Cisco-4D61", and "Security Mode:" with a dropdown menu showing "Disabled". At the bottom of the form, there are three buttons: "Save", "Cancel", and "Back".

Étape 1. Dans la liste déroulante Security Mode, sélectionnez **Disabled**. La sécurité est désactivée pour le réseau sans fil.

Étape 2. Cliquez sur **Save**.

Configuration de la sécurité WEP

Security Settings

Select SSID: Cisco-4D61

Security Mode: WEP

Authentication Type: Open System (Default: Open System)

Encryption: 10/64-bit(10 hex digits)

Passphrase: Passphrase1

Key 1:

Key 2:

Key 3:

Key 4:

TX Key: 1

Show Password:

Étape 1. Dans la liste déroulante Security Mode, sélectionnez **WEP**.

Étape 2. Dans la liste déroulante Authentication Type, sélectionnez un type d'authentification pour le réseau sans fil.

·système ouvert : tout périphérique réseau peut s'associer au point d'accès, mais la clé WEP est nécessaire pour transmettre le trafic via le point d'accès.

·Shared Key : une clé WEP est nécessaire pour s'associer au point d'accès. Il est également utilisé pour acheminer le trafic via le point d'accès.

Étape 3. Dans la liste déroulante Encryption (Cryptage), sélectionnez une méthode de cryptage pour la clé WEP.

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

·26/128 bits (26 chiffres hexadécimaux) : fournit une clé 104 bits. Cette option est plus sécurisée.

Étape 4. Dans le champ Passphrase (Phrase de passe), saisissez une phrase de passe supérieure à huit caractères. Une phrase de passe est utile pour faciliter la mémorisation des paramètres de sécurité du réseau.

Étape 5. Cliquez sur **Generate** pour créer des clés dans les champs Key 1, Key 2, Key 3 et Key 4.

Note: Vous pouvez également saisir manuellement des clés dans les champs Key 1, Key 2,

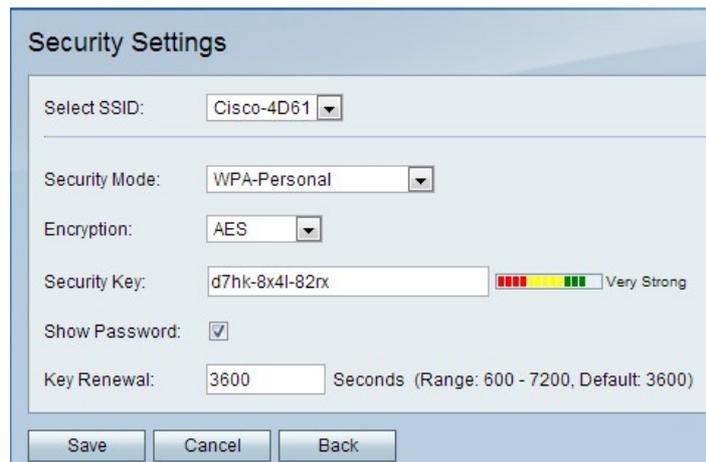
Key 3 et Key 4.

Étape 6. Dans la liste déroulante TX Key (Clé de transmission), sélectionnez la clé que les utilisateurs doivent saisir pour accéder au réseau sans fil.

Étape 7. (Facultatif) Cochez la case **Afficher le mot de passe** pour afficher les chaînes de caractères des clés.

Étape 8. Cliquez **Save**.

Configuration de la sécurité WPA-Personal



The screenshot shows a 'Security Settings' window with the following fields and options:

- Select SSID: Cisco-4D61
- Security Mode: WPA-Personal
- Encryption: AES
- Security Key: d7hk-8x4l-82rx (with a strength indicator showing 'Very Strong')
- Show Password:
- Key Renewal: 3600 Seconds (Range: 600 - 7200, Default: 3600)

Buttons at the bottom: Save, Cancel, Back.

Étape 1. Dans la liste déroulante Security Mode, sélectionnez **WPA-Personal**.

Étape 2. Dans la liste déroulante Encryption (Cryptage), sélectionnez une méthode de cryptage pour la clé WPA.

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

- AES : cette option est préférable si tous les périphériques connectés au réseau sans fil prennent en charge AES.

Étape 3. Saisissez une clé de sécurité dans le champ Security Key. La clé de sécurité est une phrase de passe composée de lettres et de chiffres. Les périphériques utilisent la clé de sécurité pour se connecter au réseau.

Étape 4. (Facultatif) Pour afficher la chaîne de caractères de la clé, cochez la case **Afficher le mot de passe**.

Étape 5. Dans le champ Key Renewal (Renouvellement de clé), saisissez la durée en secondes pendant laquelle le routeur VPN CVR100W utilise la clé avant d'en générer une nouvelle.

Étape 6. Cliquez **Save**.

Configuration de la sécurité WPA-Enterprise

Security Settings

Select SSID: Cisco-4D61

Security Mode: WPA-Enterprise

Encryption: AES

RADIUS Server: 192 . 168 . 1 . 220 (Hint: 192.168.1.200)

RADIUS Port: 1812 (Range: 1 - 65535, Default: 1812)

Shared Key: SharedKey1

Key Renewal: 3600 Seconds (Range: 600 - 7200, Default: 3600)

Save Cancel Back

Étape 1. Dans la liste déroulante Security Mode, sélectionnez **WPA-Enterprise**.

Étape 2. Dans la liste déroulante Encryption (Cryptage), sélectionnez une méthode de cryptage pour la clé WPA.

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

·AES : cette option est préférable si tous les périphériques connectés au réseau sans fil prennent en charge 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 utilisé pour accéder au serveur RADIUS.

Étape 5. Dans le champ Shared Key (Clé partagée), saisissez la clé prépartagée pour les utilisateurs sans fil. Une clé pré-partagée est une clé utilisée par tous les utilisateurs. La fonction de clé pré-partagée est une fonction de sécurité ajoutée.

Étape 6. Dans le champ Key Renewal (Renouvellement de clé), saisissez la durée en secondes pendant laquelle le routeur VPN CVR100W utilise la clé avant d'en générer une nouvelle.

Étape 7. Cliquez **Save**.

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

Security Settings

Select SSID: Cisco-4D61

Security Mode: WPA2-Personal Mixed

Encryption: TKIP + AES

Security Key: d7hk-8x4l-82rx ■■■■ ■■ Very Strong

Show Password:

Key Renewal: 3600 Seconds (Range: 600 - 7200, Default: 3600)

Save Cancel Back

Étape 1. Dans la liste déroulante Security Mode, sélectionnez **WPA2-Personal** ou **WPA2-Personal Mixed**.

Note: WPA2-Personal (WPA2 personnel) est utilisé lorsque tous les périphériques du réseau sans fil prennent en charge AES. WPA2-Personal Mixed est utilisé lorsque les périphériques du réseau ne prennent pas tous en charge AES. Le type de chiffrement utilisé par la méthode de sécurité s'affiche dans le champ Encryption (Cryptage).

Étape 2. Dans le champ Security Key, saisissez une clé de sécurité. La clé de sécurité est une phrase de passe composée de lettres et de chiffres. Les périphériques utilisent la clé de sécurité pour se connecter au réseau.

Étape 3. (Facultatif) Pour afficher les chaînes de caractères de la clé, cochez la case **Afficher le mot de passe**.

Étape 4. Dans le champ Key Renewal (Renouvellement de clé), saisissez la durée en secondes pendant laquelle le routeur VPN CVR100W utilise la clé avant d'en générer une nouvelle.

Étape 5. Cliquez **Save**.

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

Security Settings

Select SSID: Cisco-4D61

Security Mode: WPA2-Enterprise Mixed

Encryption: TKIP + AES

RADIUS Server: 192 . 168 . 1 . 220 (Hint: 192.168.1.200)

RADIUS Port: 1812 (Range: 1 - 65535, Default: 1812)

Shared Key: Sharedkey1

Key Renewal: 3600 Seconds (Range: 600 - 7200, Default: 3600)

Save Cancel Back

Étape 1. Dans la liste déroulante Security Mode, sélectionnez **WPA2-Enterprise** ou **WPA2-Enterprise Mixed**.

Note: WPA2-Enterprise est utilisé lorsque tous les périphériques du réseau sans fil prennent en charge AES. WPA2-Enterprise Mixed est utilisé lorsque les périphériques du réseau ne prennent pas tous en charge AES. Le type de chiffrement utilisé par la méthode de sécurité s'affiche dans le champ Encryption (Cryptage).

Étape 2. Dans le champ RADIUS Server, saisissez l'adresse IP du serveur RADIUS.

Étape 3. Dans le champ Port RADIUS, saisissez le numéro de port utilisé pour accéder au serveur RADIUS.

Étape 4. Dans le champ Shared Key (Clé partagée), saisissez la clé prépartagée pour les utilisateurs sans fil. Une clé pré-partagée est une clé utilisée par tous les utilisateurs. La fonction de clé pré-partagée est une fonction de sécurité ajoutée.

Étape 5. Dans le champ Key Renewal (Renouvellement de clé), saisissez la durée en secondes pendant laquelle le routeur VPN CVR100W utilise la clé avant d'en générer une nouvelle.

Étape 6. Cliquez **Save**.

Modifier le filtrage MAC

Le filtrage MAC est utilisé pour autoriser ou refuser l'accès au réseau sans fil en fonction de l'adresse MAC du périphérique de connexion.

Basic Settings

Radio: Enable

Wi-Fi Power: 100%

Wireless Network Mode: B/G/N-Mixed

Wireless Band Selection: 20MHz 20/40MHz

Wireless Channel: Auto

AP Management VLAN: 1

U-APSD (WMM Power Save): Enable

<input type="checkbox"/>	Enable SSID	SSID Name	SSID Broadcast	Security Mode	MAC Filter	CSC	VLAN	SSID Isolation	WMM	WPS
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Cisco-4D61	<input checked="" type="checkbox"/>	WPA2-Personal	Disabled	<input type="checkbox"/>	1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	cisco-SSID2	<input type="checkbox"/>	Disabled	Disabled	<input type="checkbox"/>	1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	cisco-SSID3	<input type="checkbox"/>	Disabled	Disabled	<input type="checkbox"/>	1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	cisco-guest	<input checked="" type="checkbox"/>	Disabled	Disabled	<input type="checkbox"/>	3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Buttons: Edit, **Edit Security Mode**, Edit MAC Filtering, Time of Day Access, Edit Guest Net, Edit CSC, Edit WPS

Buttons: Save, Cancel

Étape 1. Cochez la case du réseau à modifier.

Étape 2. 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 :

Wireless MAC Filtering

SSID Name: Cisco-4D61

Wireless MAC Filtering: Enable

Connection Control

Prevent PCs listed below from accessing the wireless network.

Permit PCs listed below to access the wireless network.

Show Client List

MAC Address Table					
01	1A:2B:3C:4D:5E:6F	12		23	
02		13		24	
03		14		25	
04		15		26	
05		16		27	
06		17		28	
07		18		29	
08		19		30	
09		20		31	
10		21		32	
11		22			

Buttons: Save, Cancel, Back

Étape 3. Cochez **Enable** pour activer le filtrage MAC sur le réseau.

Étape 4. Sélectionnez la case d'option correspondant au type de liste souhaité dans le champ Connection Control.

-Prevent PCs : empêche les ordinateurs dotés des adresses MAC répertoriées d'accéder au réseau.

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

Étape 5. Dans la table d'adresses MAC, saisissez les adresses MAC souhaitées.

Étape 6. Cliquez **Save**.

Accès à l'heure du jour

La fonction Accès à l'heure du jour permet d'autoriser l'accès aux utilisateurs en fonction d'un planning configuré.

Wireless Table										
<input type="checkbox"/>	Enable SSID	SSID Name	SSID Broadcast	Security Mode	MAC Filter	CSC	VLAN	SSID Isolation	WMM	WPS
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Cisco-4D61	<input checked="" type="checkbox"/>	WPA2-Personal	Disabled	<input checked="" type="checkbox"/>	1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	cisco-SSID2	<input type="checkbox"/>	Disabled	Disabled	<input type="checkbox"/>	1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	cisco-SSID3	<input type="checkbox"/>	Disabled	Disabled	<input type="checkbox"/>	1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	cisco-guest	<input checked="" type="checkbox"/>	Disabled	Disabled	<input type="checkbox"/>	3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Buttons: Edit, Edit Security Mode, Edit MAC Filtering, **Time of Day Access**, Edit Guest Net, Edit CSC, Edit WPS

Étape 1. Cochez la case du réseau à modifier.

Étape 2. Cliquez sur **Accès à l'heure du jour** pour configurer quand les utilisateurs peuvent accéder au réseau spécifié. La page *Accès à l'heure du jour* s'ouvre :

Time of Day Access

Add / Edit Access Point Configuration

Active Time: Enable

Start Time: 03 Hours 0 Minutes AM

Stop Time: 12 Hours 0 Minutes AM

Buttons: Save, Cancel, Back

Étape 3. Cochez **Enable** dans le champ Active Time pour activer l'accès à l'heure du jour pour le réseau.

Étape 4. Dans le champ Start Time (Heure de début), saisissez l'heure à laquelle commence l'accès au réseau.

Étape 5. Dans le champ Stop Time, saisissez l'heure à laquelle l'accès au réseau se termine.

Étape 6. Cliquez **Save**.

Modifier le réseau invité

Un réseau invité est une section d'un réseau conçue pour les utilisateurs temporaires. Permet aux invités d'accéder au réseau sans avoir à exposer les 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.

Basic Settings

Radio: Enable

Wi-Fi Power: 100%

Wireless Network Mode: B/G/N-Mixed

Wireless Band Selection: 20MHz 20/40MHz

Wireless Channel: Auto

AP Management VLAN: 1

U-APSD (WMM Power Save): Enable

<input type="checkbox"/>	Enable SSID	SSID Name	SSID Broadcast	Security Mode	MAC Filter	CSC	VLAN	SSID Isolation	WMM	WPS
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Cisco-4D61	<input checked="" type="checkbox"/>	WPA2-Personal	Disabled	<input type="checkbox"/>	1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	cisco-SSID2	<input type="checkbox"/>	Disabled	Disabled	<input type="checkbox"/>	1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	cisco-SSID3	<input type="checkbox"/>	Disabled	Disabled	<input type="checkbox"/>	1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input checked="" type="checkbox"/>	<input type="checkbox"/>	cisco-guest	<input checked="" type="checkbox"/>	Disabled	Disabled	<input type="checkbox"/>	3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Étape 1. Cliquez sur **Edit Guest Network** pour configurer le réseau invité. La page *Guest Net Settings* s'ouvre :

Guest Net Settings

Guest Net Name: guest

Guest Password:

Hide Password:

Lease Time: 120 Minutes

Total Guest Allowed: 5

Étape 2. Dans le champ Guest Password (Mot de passe invité), saisissez un mot de passe que les utilisateurs utiliseront pour accéder au réseau invité.

Étape 3. (Facultatif) Pour masquer le mot de passe sur la page, cochez la case dans le champ Masquer le mot de passe.

Étape 4. Dans le champ Lease Time (Durée du bail), saisissez l'heure en minutes pendant laquelle les utilisateurs sont autorisés à rester connectés au réseau invité.

Étape 5. Dans la liste déroulante Total Guest Allowed, sélectionnez le nombre total d'invités autorisés.

Étape 6. Cliquez **Save**.

Modifier CSC

CSC facilite la configuration d'un réseau sans fil et permet une connexion facile des périphériques sans fil au réseau. Le périphérique sans fil utilise CSC pour obtenir le SSID et

le mot de passe du réseau, ce qui permet une connexion automatique au réseau.

Wireless Table										
<input type="checkbox"/>	Enable SSID	SSID Name	SSID Broadcast	Security Mode	MAC Filter	CSC	VLAN	SSID Isolation	WMM	WPS
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Cisco-4D61	<input checked="" type="checkbox"/>	WPA2-Personal	Disabled	<input type="checkbox"/>	1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Cisco-1	<input checked="" type="checkbox"/>	Disabled	Disabled	<input checked="" type="checkbox"/>	5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	cisco-SSID3	<input type="checkbox"/>	Disabled	Disabled	<input type="checkbox"/>	1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	<input type="checkbox"/>	cisco-guest	<input checked="" type="checkbox"/>	Disabled	Disabled	<input type="checkbox"/>	3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Buttons: Edit, Edit Security Mode, Edit MAC Filtering, Time of Day Access, Edit Guest Net, **Edit CSC**, Edit WPS

Étape 1. Cochez la case du réseau à modifier.

Étape 2. Cliquez sur **Edit CSC** pour modifier Cisco Simple Connect.

Étape 3. Cochez la case CSC.

Étape 4. Dans la liste déroulante VLAN, sélectionnez le VLAN utilisé pour CSC.

Note: Le VLAN Cisco Simple Connect ne peut pas être identique au VLAN SSID actuel ou autre. Pour créer un nouveau VLAN, reportez-vous à l'article [Appartenance VLAN sur le routeur CVR100W](#).

Note: CSC ne peut prendre effet que sur le système de distribution sans fil (WDS) sur SSID1. Reportez-vous à l'article [Wireless Distribution System \(WDS\) sur le routeur CVR100W](#).

Étape 5. Cliquez sur **Save**.