

Configuration des paramètres de sécurité sans fil sur un WAP

Introduction

La configuration de la sécurité sans fil sur votre point d'accès sans fil (WAP) est essentielle pour protéger votre réseau sans fil contre les intrusions susceptibles de compromettre la confidentialité de vos périphériques sans fil ainsi que la transmission de données sur votre réseau sans fil. Vous pouvez configurer la sécurité sans fil sur votre réseau sans fil en configurant le filtre MAC, le Wi-Fi Protected Access (WPA/WPA2) Personal (WPA/WPA2 personnel) et le WPA/WPA2 Enterprise (WPA/WPA2 entreprise).

Le filtrage MAC permet de filtrer les clients sans fil pour accéder au réseau à l'aide de leurs adresses MAC. Une liste de clients sera configurée pour autoriser ou bloquer les adresses de la liste à accéder au réseau, selon vos préférences. Pour en savoir plus sur le filtrage MAC, cliquez [ici](#).

WPA/WPA2 Personal et WPA/WPA2 Enterprise sont des protocoles de sécurité utilisés pour protéger la confidentialité en chiffrant les données transmises sur le réseau sans fil. WPA/WPA2 est compatible avec les normes IEEE 802.11E et 802.11i. Par rapport au protocole de sécurité WEP (Wired Equivalent Privacy), WPA/WPA2 ont amélioré les fonctions d'authentification et de chiffrement.

WPA/WPA2 Personal (WPA/WPA2 personnel) est destiné à un usage domestique et WPA/WPA2 Enterprise est destiné à un réseau professionnel. WPA/WPA2 Enterprise fournit une sécurité et un contrôle centralisés plus importants sur le réseau que WPA/WPA2 Personal.

Dans ce scénario, la sécurité sans fil va être configurée sur le WAP pour protéger le réseau des intrusions à l'aide des paramètres WPA/WPA2 Personal et Enterprise.

Objectif

Cet article vise à vous montrer comment configurer les protocoles de sécurité WPA/WPA2 Personal et Enterprise pour améliorer la sécurité et la confidentialité de votre réseau sans fil.

Note: Cet article suppose qu'un SSID (Service Set Identifier) ou un WLAN (Wireless Local Area Network) a déjà été créé sur votre WAP.

Périphériques pertinents

- Gamme WAP100
- Gamme WAP300
- Gamme WAP500

Version du logiciel

- 1.0.2.14 - WAP131, WAP351
- 1.0.6.5 - WAP121, WAP321

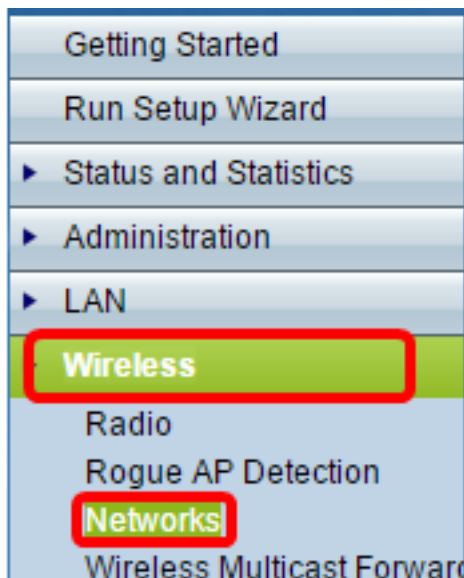
- 1.3.0.4 - WAP371
- 1.1.0.7 - WAP150, WAP361
- 1.2.1.5 - WAP551, WAP561
- 1.0.1.11 - WAP571, WAP571E

Configurer les paramètres de sécurité sans fil

Configuration de WPA/WPA2 Personal

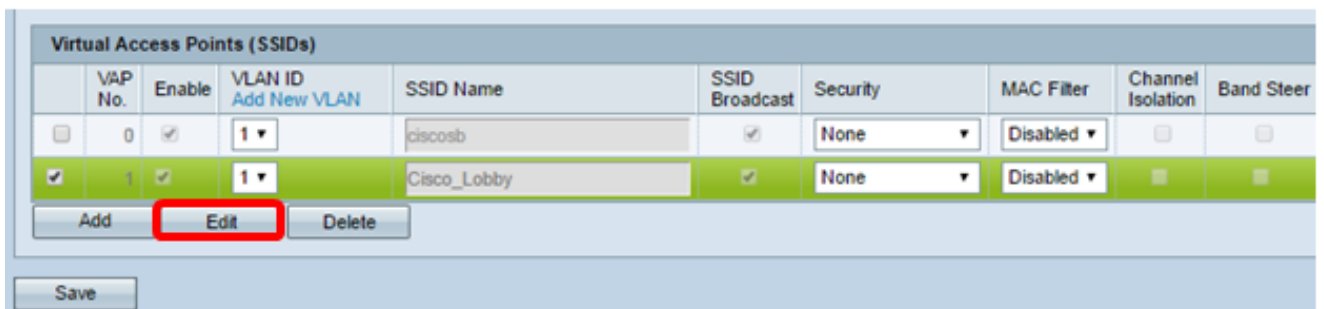
Étape 1. Connectez-vous à l'utilitaire Web de votre point d'accès et sélectionnez **Wireless > Networks**.

Note: Dans l'image ci-dessous, l'utilitaire Web du WAP361 est utilisé comme exemple. Les options de menu peuvent varier en fonction du modèle de votre périphérique.



Étape 2. Dans la zone Virtual Access Points (SSIDs), cochez la case du SSID que vous souhaitez configurer et cliquez sur **Edit**.

Note: Dans cet exemple, VAP1 est sélectionné.



Étape 3. Cliquez sur **WPA Personal** dans la liste déroulante Security.

Virtual Access Points (SSIDs)							
	VAP No.	Enable	VLAN ID <small>Add New VLAN</small>	SSID Name	SSID Broadcast	Security	
<input type="checkbox"/>	0	<input checked="" type="checkbox"/>	1	ciscosb	<input checked="" type="checkbox"/>	None	
<input checked="" type="checkbox"/>	1	<input checked="" type="checkbox"/>	1	Cisco_Lobby	<input checked="" type="checkbox"/>	None	<div style="border: 2px solid red; padding: 2px;"> None None WPA Personal WPA Enterprise </div>

Étape 4. Activez la case à cocher WPA version (WPA-TKIP ou WPA2-AES). Deux peuvent être choisis en même temps.

- WPA-TKIP — Outil Wi-Fi Protected Access-Temporal Key Integrity. Le réseau dispose de certaines stations clientes qui prennent uniquement en charge le protocole de sécurité WPA et TKIP d'origine. Notez que le choix uniquement de WPA-TKIP pour le point d'accès n'est pas autorisé conformément à la dernière exigence de Wi-Fi Alliance.
- WPA2-AES - Wi-Fi Protected Access - Advanced Encryption Standard. Toutes les stations clientes du réseau prennent en charge le protocole de chiffrement/sécurité WPA2 et AES-CCMP. Cette version WPA offre la meilleure sécurité selon la norme IEEE 802.11i. Conformément à la dernière exigence de Wi-Fi Alliance, le WAP doit toujours prendre en charge ce mode.

Note: Dans cet exemple, les deux cases à cocher sont cochées.

WPA Versions: WPA-TKIP WPA2-AES

Key: (Range: 8-63 Characters)

Show Key as Clear Text

Key Strength Meter: Below Minimum

Broadcast Key Refresh Rate Sec (Range: 0-86400, 0 =

Étape 5. Créez un mot de passe composé de 8 à 63 caractères et saisissez-le dans le champ *Clé*.

WPA Versions: WPA-TKIP WPA2-AES

Key: (Range: 8-63 Characters)

Show Key as Clear Text


Key Strength Meter: Strong

Note: Vous pouvez cocher la case **Afficher la clé en texte clair** pour afficher le mot de passe que vous avez créé.

WPA Versions: WPA-TKIP WPA2-AES

Key: (Range: 8-63 Characters)

Show Key as Clear Text

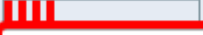
Key Strength Meter:  Strong

Étape 6. (Facultatif) Dans le champ *Broadcast Key Refresh Rate*, saisissez une valeur ou l'intervalle d'actualisation de la clé de diffusion (groupe) pour les clients associés à ce VAP. La valeur par défaut est 300 secondes et la plage valide est comprise entre 0 et 86 400 secondes. La valeur 0 indique que la clé de diffusion n'est pas actualisée.

WPA Versions: WPA-TKIP WPA2-AES

Key: (Range: 8-63 Characters)

Show Key as Clear Text

Key Strength Meter:  Session Key Refresh Rate

Broadcast Key Refresh Rate Sec (Range: 0-86400, 0 = Disable, Default: 300)

Étape 7. Click Save.

Virtual Access Points (SSIDs)				
	VAP No.	Enable	VLAN ID <small>Add New VLAN</small>	SSID Name
<input type="checkbox"/>	0	<input checked="" type="checkbox"/>	1	ciscosb
<input checked="" type="checkbox"/>	1	<input checked="" type="checkbox"/>	1	Cisco_Lobby

Add Edit Delete

Save

Vous avez maintenant configuré WPA Personal sur votre WAP.

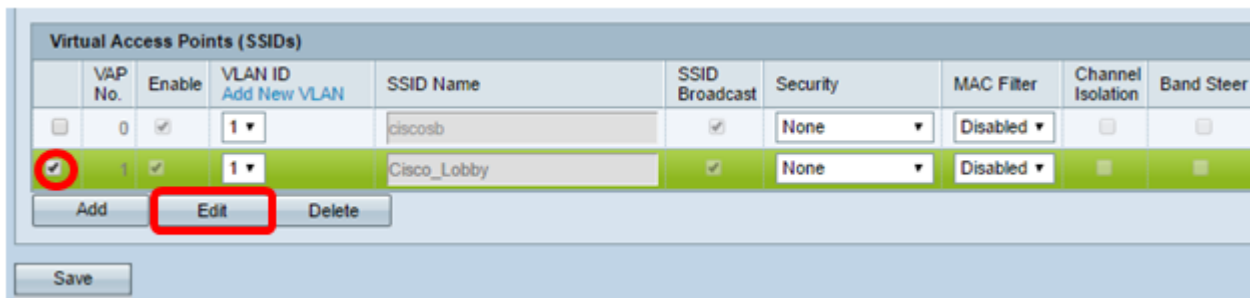
Configuration de WPA/WPA2 Enterprise

Étape 1. Connectez-vous à l'utilitaire Web de votre point d'accès et sélectionnez **Wireless > Networks**.

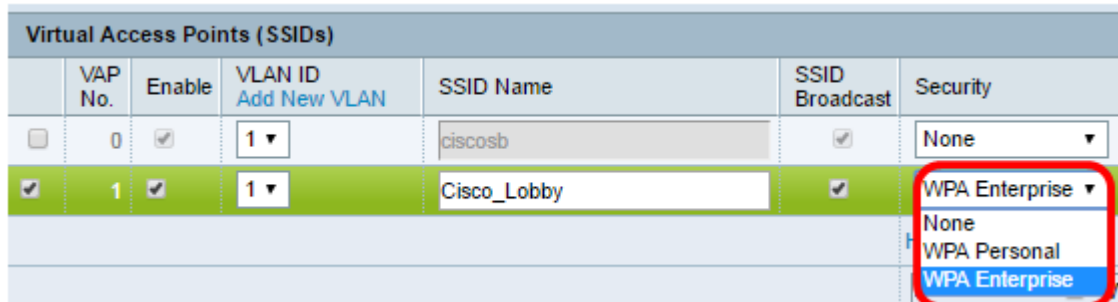
Note: Dans l'image ci-dessous, l'utilitaire Web du WAP361 est utilisé comme exemple.

- Getting Started
- Run Setup Wizard
- ▶ Status and Statistics
- ▶ Administration
- ▶ LAN
- Wireless**
- Radio
- Rogue AP Detection
- Networks**
- Wireless Multicast Forward

Étape 2. Dans la zone Virtual Access Points (SSIDs), vérifiez le SSID que vous souhaitez configurer et cliquez sur le bouton **Edit** situé en dessous.



Étape 3. Choisissez **WPA Enterprise** dans la liste déroulante Sécurité.



Étape 4. Choisissez la version WPA (WPA-TKIP, WPA2-AES et Enable pre-authentication).

- Enable pre-authentication : si vous choisissez WPA2-AES uniquement ou WPA-TKIP et WPA2-AES comme version WPA, vous pouvez activer la pré-authentification pour les clients WPA2-AES. Cochez cette option si vous voulez que les clients sans fil WPA2 envoient les paquets de pré-authentification. Les informations de pré-authentification sont relayées à partir du périphérique WAP que le client utilise actuellement vers le périphérique WAP cible. L'activation de cette fonctionnalité peut accélérer l'authentification des clients itinérants qui se connectent à plusieurs points d'accès (AP).

Note: Cette option ne s'applique pas si vous avez sélectionné WPA-TKIP pour les versions WPA, car le WPA d'origine ne prend pas en charge cette fonctionnalité.

Hide Details

WPA Versions: WPA-TKIP WPA2-AES
 Enable pre-authentication

Use global RADIUS server settings

Server IP Address Type: IPv4 IPv6

Server IP Address-1: (xxx.xxx.xxx.xxx)
 Server IP Address-2: (xxx.xxx.xxx.xxx)
 Server IP Address-3: (xxx.xxx.xxx.xxx)
 Server IP Address-4: (xxx.xxx.xxx.xxx)

Key-1: (Range: 1 - 64 Characters)
 Key-2: (Range: 1 - 64 Characters)
 Key-3: (Range: 1 - 64 Characters)
 Key-4: (Range: 1 - 64 Characters)

Enable RADIUS Accounting

Active Server:

Broadcast Key Refresh Rate: Sec (Range: 0-86400, 0 = Disable, Default: 300)
 Session Key Refresh Rate: Sec (Range: 30-86400, 0 = Disable, Default: 0)

Étape 5. (Facultatif) Décochez la case **Utiliser les paramètres globaux du serveur RADIUS** pour modifier les paramètres.

WPA Versions: WPA-TKIP WPA2-AES
 Enable pre-authentication

Use global RADIUS server settings

Server IP Address Type: IPv4 IPv6

Server IP Address-1: (xxx.xxx.xxx.xxx)
 Server IP Address-2: (xxx.xxx.xxx.xxx)
 Server IP Address-3: (xxx.xxx.xxx.xxx)
 Server IP Address-4: (xxx.xxx.xxx.xxx)

Key-1: (Range: 1 - 64 Characters)
 Key-2: (Range: 1 - 64 Characters)
 Key-3: (Range: 1 - 64 Characters)
 Key-4: (Range: 1 - 64 Characters)

Enable RADIUS Accounting

Active Server:

Broadcast Key Refresh Rate: Sec (Range: 0-86400, 0 = Disable, Default: 300)
 Session Key Refresh Rate: Sec (Range: 30-86400, 0 = Disable, Default: 0)

Étape 6. (Facultatif) Activez la case d'option correspondant au **type d'adresse IP** du serveur approprié.

Note: Dans cet exemple, IPv4 est choisi.

WPA Versions: WPA-TKIP WPA2-AES
 Enable pre-authentication

Use global RADIUS server settings

Server IP Address Type: IPv4 IPv6

Server IP Address-1: (xxx.xxx.xxx.xxx)
Server IP Address-2: (xxx.xxx.xxx.xxx)
Server IP Address-3: (xxx.xxx.xxx.xxx)
Server IP Address-4: (xxx.xxx.xxx.xxx)

Key-1: (Range: 1 - 64 Characters)
Key-2: (Range: 1 - 64 Characters)
Key-3: (Range: 1 - 64 Characters)
Key-4: (Range: 1 - 64 Characters)

Enable RADIUS Accounting

Active Server: ▼

Broadcast Key Refresh Rate: Sec (Range: 0-86400, 0 = Disable, Default: 300)
Session Key Refresh Rate: Sec (Range: 30-86400, 0 = Disable, Default: 0)

Étape 7. Entrez l'adresse IP du serveur RADIUS dans le champ *Adresse IP du serveur*.

Note: Pour cet exemple, 192.168.1.101 est utilisé.

WPA Versions: WPA-TKIP WPA2-AES
 Enable pre-authentication

Use global RADIUS server settings

Server IP Address Type: IPv4 IPv6

Server IP Address-1: (xxx.xxx.xxx.xxx)
Server IP Address-2: (xxx.xxx.xxx.xxx)
Server IP Address-3: (xxx.xxx.xxx.xxx)
Server IP Address-4: (xxx.xxx.xxx.xxx)

Key-1: (Range: 1 - 64 Characters)
Key-2: (Range: 1 - 64 Characters)
Key-3: (Range: 1 - 64 Characters)
Key-4: (Range: 1 - 64 Characters)

Enable RADIUS Accounting

Active Server: ▼

Broadcast Key Refresh Rate: Sec (Range: 0-86400, 0 = Disable, Default: 300)
Session Key Refresh Rate: Sec (Range: 30-86400, 0 = Disable, Default: 0)

Étape 8. Dans le champ *Key*, saisissez la clé de mot de passe correspondant à votre serveur RADIUS que le WAP utilise pour s'authentifier auprès du serveur RADIUS. Vous pouvez utiliser entre 1 et 64 caractères alphanumériques et spéciaux standard.

Note: Les clés sont sensibles à la casse et doivent correspondre à la clé configurée sur le serveur RADIUS.

Étape 9. (Facultatif) Répétez les étapes 7 à 8 pour chaque serveur RADIUS de votre réseau avec lequel vous voulez que le WAP communique.

WPA Versions: WPA-TKIP WPA2-AES
 Enable pre-authentication

Use global RADIUS server settings

Server IP Address Type: IPv4 IPv6

Server IP Address-1: (xxx.xxx.xxx.xxx)
Server IP Address-2: (xxx.xxx.xxx.xxx)
Server IP Address-3: (xxx.xxx.xxx.xxx)
Server IP Address-4: (xxx.xxx.xxx.xxx)

Key-1: (Range: 1 - 64 Characters)
Key-2: (Range: 1 - 64 Characters)
Key-3: (Range: 1 - 64 Characters)
Key-4: (Range: 1 - 64 Characters)

Enable RADIUS Accounting

Active Server: ▾

Broadcast Key Refresh Rate: Sec (Range: 0-86400, 0 = Disable, Default: 300)
Session Key Refresh Rate: Sec (Range: 30-86400, 0 = Disable, Default: 0)

Étape 10. (Facultatif) Cochez la case **EnableRADIUS Accounting** pour activer le suivi et la mesure des ressources consommées par un utilisateur (temps système, quantité de données transmises). L'activation de cette fonctionnalité permettra la comptabilisation RADIUS des serveurs principal et de sauvegarde.

WPA Versions: WPA-TKIP WPA2-AES
 Enable pre-authentication

Use global RADIUS server settings

Server IP Address Type: IPv4 IPv6


Server IP Address-1: (xxx.xxx.xxx.xxx)
Server IP Address-2: (xxx.xxx.xxx.xxx)
Server IP Address-3: (xxx.xxx.xxx.xxx)
Server IP Address-4: (xxx.xxx.xxx.xxx)

Key-1: (Range: 1 - 64 Characters)
Key-2: (Range: 1 - 64 Characters)
Key-3: (Range: 1 - 64 Characters)
Key-4: (Range: 1 - 64 Characters)

Enable RADIUS Accounting

Active Server: ▼

Broadcast Key Refresh Rate: Sec (Range: 0-86400, 0 = Disable, Default: 300)
Session Key Refresh Rate: Sec (Range: 30-86400, 0 = Disable, Default: 0)

Étape 11. Cliquez sur .

Vous avez maintenant correctement configuré la sécurité WPA/WPA2 Enterprise sur votre WAP.