

# Configuration d'un VAP sur WAP351, WAP131 et WAP371

## Objectif

Les points d'accès virtuels (VAP) segmentent le réseau local sans fil en plusieurs domaines de diffusion qui sont l'équivalent sans fil des VLAN Ethernet. Les points d'accès virtuels simulent plusieurs points d'accès dans un périphérique WAP physique. Jusqu'à quatre points d'accès virtuels sont pris en charge sur le Cisco WAP131 et jusqu'à huit points d'accès virtuels sont pris en charge sur les points d'accès Cisco WAP351 et WAP371.

L'objectif de ce document est de vous montrer comment configurer un VAP sur les points d'accès WAP351, WAP131 et WAP371.

## Périphériques pertinents

- WAP351

- WAP131

- WAP371

## Version du logiciel

- V1.0.0.39 (WAP351)

- V1.0.0.39 (WAP131)

- V1.2.0.2 (WAP371)

## Ajouter et configurer un VAP

**Note:** Chaque VAP est identifié par un SSID (Service Set Identifier) configuré par l'utilisateur. Plusieurs VAP ne peuvent pas avoir le même nom SSID.

**Note:** Pour que votre réseau sans fil fonctionne, la radio à laquelle votre VAP configuré est associé doit être activée et correctement configurée. Reportez-vous à [Configuration des paramètres radio de base sur le WAP131 et le WAP351](#) ou [Configuration des paramètres radio de base sur le WAP371](#) pour plus d'informations

Étape 1. Connectez-vous à l'utilitaire de configuration Web et accédez à **Wireless > Networks**. La page *Réseaux* s'affiche :

Networks

Select the radio interface first, and then enter the configuration parameters.

Radio:  Radio 1 (2.4 GHz)  
 Radio 2 (5 GHz)

Virtual Access Points (SSIDs)									
	VAP No.	Enable	VLAN ID	SSID Name	SSID Broadcast	Security	MAC Filter	Channel Isolation	
<input type="checkbox"/>	0	<input checked="" type="checkbox"/>	1	discosb	<input checked="" type="checkbox"/>	None	Disabled	<input type="checkbox"/>	

Add Edit Delete

Save

Étape 2. Dans le champ *Radio*, sélectionnez la case d'option de la radio sans fil sur laquelle vous souhaitez configurer des VAP.

Select the radio interface first, and then enter the configuration parameters.

Radio:  Radio 1 (2.4 GHz)  
 Radio 2 (5 GHz)

Virtual Access Points (SSIDs)									
	VAP No.	Enable	VLAN ID	SSID Name	SSID Broadcast	Security	MAC Filter	Channel Isolation	
<input type="checkbox"/>	0	<input checked="" type="checkbox"/>	1	discosb	<input checked="" type="checkbox"/>	None	Disabled	<input type="checkbox"/>	

Add Edit Delete

Étape 3. Pour ajouter un nouveau VAP, cliquez sur **Ajouter**. Un nouveau VAP apparaîtra dans le tableau.

Select the radio interface first, and then enter the configuration parameters.

Radio:  Radio 1 (2.4 GHz)  
 Radio 2 (5 GHz)

Virtual Access Points (SSIDs)									
	VAP No.	Enable	VLAN ID	SSID Name	SSID Broadcast	Security	MAC Filter	Channel Isolation	
<input type="checkbox"/>	0	<input checked="" type="checkbox"/>	1	discosb	<input checked="" type="checkbox"/>	None	Disabled	<input type="checkbox"/>	

Add Edit Delete

**Note:** Le WAP131 prend en charge jusqu'à 4 VAP, tandis que les WAP371 et WAP351 prennent en charge jusqu'à 8 VAP.

Étape 4. Pour commencer à modifier un VAP, activez la case à cocher située à l'extrême gauche de l'entrée du tableau, puis cliquez sur **Modifier**. Cela vous permettra de modifier les champs grisés du VAP que vous avez sélectionné.

Select the radio interface first, and then enter the configuration parameters.

Radio:  Radio 1 (2.4 GHz)  
 Radio 2 (5 GHz)

Virtual Access Points (SSIDs)									
	VAP No.	Enable	VLAN ID	SSID Name	SSID Broadcast	Security	MAC Filter	Channel Isolation	
<input type="checkbox"/>	0	<input checked="" type="checkbox"/>	1	discosb	<input checked="" type="checkbox"/>	None	Disabled	<input type="checkbox"/>	
<input checked="" type="checkbox"/>	1	<input checked="" type="checkbox"/>	1		<input checked="" type="checkbox"/>	None	Disabled	<input type="checkbox"/>	

Add Edit Delete

Étape 5. Pour activer l'utilisation du VAP, assurez-vous que la case *Activer* est cochée.

Select the radio interface first, and then enter the configuration parameters.

Radio:  Radio 1 (2.4 GHz)  
 Radio 2 (5 GHz)

Virtual Access Points (SSIDs)								
VAP No.	Enable	VLAN ID <a href="#">Add New VLAN</a>	SSID Name	SSID Broadcast	Security	MAC Filter	Channel Isolation	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	1	discosb	<input checked="" type="checkbox"/>	None	Disabled	<input type="checkbox"/>	
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1		<input checked="" type="checkbox"/>	None	Disabled	<input type="checkbox"/>	

Add Edit Delete

Étape 6. Dans le champ *ID VLAN*, spécifiez l'ID VLAN que vous souhaitez associer au VAP. Si vous utilisez le WAP131 ou le WAP371, saisissez l'ID de VLAN. La valeur maximale que vous pouvez saisir est 4094.

Select the radio interface first, and then enter the configuration parameters.

Radio:  Radio 1 (2.4 GHz)  
 Radio 2 (5 GHz)

Virtual Access Points (SSIDs)								
VAP No.	Enable	VLAN ID <a href="#">Add New VLAN</a>	SSID Name	SSID Broadcast	Security	MAC Filter	Channel Isolation	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	1	discosb	<input checked="" type="checkbox"/>	None	Disabled	<input type="checkbox"/>	
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1		<input checked="" type="checkbox"/>	None	Disabled	<input type="checkbox"/>	

Add Edit Delete

**Note:** L'ID de VLAN saisi doit exister sur votre réseau et être correctement configuré. Voir [Configuration VLAN sur le point d'accès WAP351](#), [Gestion des ID VLAN balisés et non balisés sur WAP131](#), ou [Gestion des ID VLAN balisés et non balisés sur le WAP371](#) pour plus d'informations.

Étape 7. Saisissez le nom du réseau sans fil dans le champ SSID Name (Nom SSID). Chaque VAP doit avoir un nom SSID unique.

Select the radio interface first, and then enter the configuration parameters.

Radio:  Radio 1 (2.4 GHz)  
 Radio 2 (5 GHz)

Virtual Access Points (SSIDs)								
VAP No.	Enable	VLAN ID <a href="#">Add New VLAN</a>	SSID Name	SSID Broadcast	Security	MAC Filter	Channel Isolation	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	1	discosb	<input checked="" type="checkbox"/>	None	Disabled	<input type="checkbox"/>	
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1	CiscoSBTest	<input checked="" type="checkbox"/>	None	Disabled	<input type="checkbox"/>	

Add Edit Delete

Étape 8. Si vous souhaitez que le nom SSID soit diffusé aux clients, cochez la case *Diffusion SSID*. Le nom SSID sera affiché aux clients sur leur liste de réseaux disponibles.

Select the radio interface first, and then enter the configuration parameters.

Radio:  Radio 1 (2.4 GHz)  
 Radio 2 (5 GHz)

Virtual Access Points (SSIDs)								
VAP No.	Enable	VLAN ID <a href="#">Add New VLAN</a>	SSID Name	SSID Broadcast	Security	MAC Filter	Channel Isolation	
<input type="checkbox"/>	<input checked="" type="checkbox"/>	1	discosb	<input checked="" type="checkbox"/>	None	Disabled	<input type="checkbox"/>	
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1	CiscoSBTest	<input checked="" type="checkbox"/>	None	Disabled	<input type="checkbox"/>	

Add Edit Delete

## Configuration des paramètres de sécurité

Étape 1. Choisissez la méthode d'authentification requise pour la connexion au VAP dans la

liste déroulante *Sécurité*. Si une option autre que **Aucun** est sélectionnée, des champs supplémentaires s'affichent.

Select the radio interface first, and then enter the configuration parameters.

Radio:  Radio 1 (2.4 GHz)  
 Radio 2 (5 GHz)

VAP No.	Enable	VLAN ID <small>Add New VLAN</small>	SSID Name	SSID Broadcast	Security	MAC Filter	Channel Isolation
<input type="checkbox"/>	<input checked="" type="checkbox"/>	1	isco55	<input checked="" type="checkbox"/>	None	Disabled	<input type="checkbox"/>
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1	CiscoSBTest	<input checked="" type="checkbox"/>	None	Disabled	<input type="checkbox"/>

Buttons: Add, Edit, Delete, Save

Security dropdown menu options: None, Static WEP, Dynamic WEP, WPA Personal, WPA Enterprise

Les options disponibles sont les suivantes :

- Aucune
- WEP statique
- WEP dynamique
- WPA personnel
- WPA Enterprise

**Note:** WPA Personal et WPA Enterprise sont les types d'authentification préférés pour une sécurité maximale. Les modes WEP statique et WEP dynamique doivent uniquement être utilisés avec les équipements existants et nécessitent que la radio soit définie sur le mode 802.11a ou 802.11b/g à utiliser. Reportez-vous à [Configuration des paramètres radio de base sur le WAP131 et le WAP351](#) ou [Configuration des paramètres radio de base sur le WAP371](#) pour plus d'informations.

## WEP statique

Le WEP statique est la méthode d'authentification la moins sécurisée. Il chiffre les données du réseau sans fil en fonction d'une clé statique. Il est devenu simple d'obtenir cette clé statique de manière illégitime, de sorte que l'authentification WEP ne doit être utilisée que lorsque nécessaire avec les périphériques existants.

**Note:** Lorsque vous sélectionnez *Static WEP* comme méthode de sécurité, une invite s'affiche et vous indique que votre choix de méthode de sécurité est très peu sécurisé.

Étape 1. Dans la liste déroulante *Transfer Key Index*, sélectionnez l'index de la clé WEP dans la liste des clés ci-dessous que le périphérique utilisera pour chiffrer les données.

Transfer Key Index: 1

Key Length: 2, 3 bits, 4 bits

Key Type:  ASCII,  Hex

WEP Keys: (Required: 26)

1:

2:

3:

4:

Show Key as Clear Text

802.1X Authentication:  Open System  Shared Key

Étape 2. Sélectionnez une case d'option dans le champ *Longueur de clé* pour spécifier si la clé est de 64 bits ou de 128 bits de longueur.

Transfer Key Index: 1

Key Length:  64 bits,  128 bits

Key Type:  ASCII,  Hex

WEP Keys: (Required: 26)

1:

2:

3:

4:

Show Key as Clear Text

802.1X Authentication:  Open System  Shared Key

Étape 3. Dans le champ *Type de clé*, indiquez si vous souhaitez saisir les clés au format ASCII ou hexadécimal. ASCII inclut toutes les lettres, les chiffres et les symboles présents sur le clavier, tandis que le format hexadécimal ne doit utiliser que des chiffres ou des lettres A à F.

Transfer Key Index: 1 ▾

Key Length:  64 bits  
 128 bits

Key Type:  ASCII  
 Hex

WEP Keys: (Required: 26)

1:

2:

3:

4:

Show Key as Clear Text

802.1X Authentication:  Open System  Shared Key

Étape 4. Dans le champ *Clés WEP*, saisissez jusqu'à 4 clés WEP différentes pour votre périphérique. Chaque client qui doit se connecter à ce réseau doit avoir une des mêmes clés WEP dans le même logement spécifié par le périphérique.

Transfer Key Index: 1 ▾

Key Length:  64 bits  
 128 bits

Key Type:  ASCII  
 Hex

WEP Keys: (Required: 26)

1:

2:

3:

4:

Show Key as Clear Text

802.1X Authentication:  Open System  Shared Key

Étape 5. (Facultatif) Activez la case à cocher dans le champ *Afficher la clé comme texte clair*, si vous affichez les chaînes de caractères des clés.

Transfer Key Index: 1 ▾

Key Length:  64 bits  
 128 bits

Key Type:  ASCII  
 Hex

WEP Keys: (Required: 26)

1: ABCDFE123456789ABCDE34251  
2: ABEDC43C2A1B56CD7AE494A56  
3: BB4C56AD3E12CB78A9234BD23  
4: BEE59A4C5D3E5B7B8AD23169B

Show Key as Clear Text

802.1X Authentication:  Open System  Shared Key

**Remarque :** Lorsque vous utilisez un autre micrologiciel sur les points d'accès WAP351, WAP131 ou WAP371, le champ *Afficher la clé en clair* peut être manquant.

Étape 6. Dans le champ *Authentification 802.1X*, spécifiez l'algorithme d'authentification à utiliser en sélectionnant les options *Open System* et/ou *Shared Key*. L'algorithme d'authentification définit la méthode utilisée pour déterminer si une station client est autorisée à s'associer au périphérique WAP lorsque le mode de sécurité WEP statique est le mode de sécurité.

Transfer Key Index: 1 ▾

Key Length:  64 bits  
 128 bits

Key Type:  ASCII  
 Hex

WEP Keys: (Required: 26)

1: .....  
2: .....  
3: .....  
4: .....

Show Key as Clear Text

802.1X Authentication:  Open System  Shared Key

Les options disponibles sont définies comme suit :

·système ouvert : l'authentification permet à n'importe quelle station cliente de s'associer au périphérique WAP, que cette station cliente possède ou non la clé WEP correcte. Cet algorithme est utilisé en texte brut, en mode IEEE 802.1X et en mode WPA. Lorsque l'algorithme d'authentification est défini sur *Open System*, tout client peut s'associer au périphérique WAP.

·Shared Key : l'authentification nécessite que la station cliente dispose de la clé WEP correcte pour s'associer au périphérique WAP. Lorsque l'algorithme d'authentification est

défini sur *Shared Key*, une station avec une clé WEP incorrecte ne peut pas s'associer au périphérique WAP.

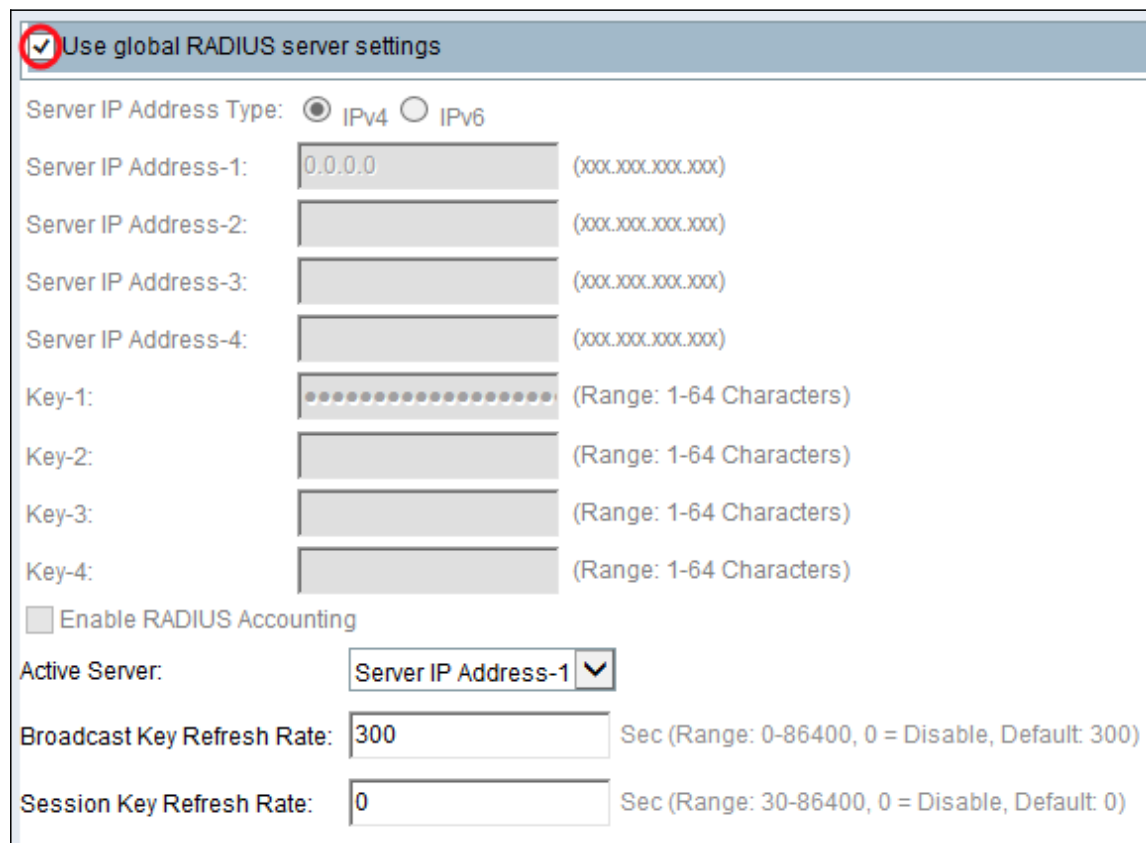
·système ouvert et clé partagée : lorsque vous avez sélectionné les deux algorithmes d'authentification, les stations clientes configurées pour utiliser le protocole WEP en mode clé partagée doivent avoir une clé WEP valide afin de s'associer au périphérique WAP. En outre, les stations clientes configurées pour utiliser WEP comme système ouvert (le mode de clé partagée n'est pas activé) peuvent s'associer au périphérique WAP même si elles ne possèdent pas la clé WEP correcte.

Étape 7. Cliquez **Save**.

## WEP dynamique

Le protocole WEP dynamique fait référence à la combinaison de la technologie 802.1x et du protocole EAP (Extensible Authentication Protocol). Ce mode nécessite l'utilisation d'un serveur RADIUS externe pour authentifier les utilisateurs. Le périphérique WAP nécessite un serveur RADIUS qui prend en charge EAP, tel que Microsoft Internet Authentication Server. Pour fonctionner avec les clients Microsoft Windows, le serveur d'authentification doit prendre en charge les protocoles PEAP (Protected EAP) et MSCHAP v2. Vous pouvez utiliser n'importe quelle méthode d'authentification prise en charge par le mode IEEE 802.1X, y compris les certificats, Kerberos et l'authentification par clé publique, mais vous devez configurer les stations clientes pour qu'elles utilisent la même méthode d'authentification que celle utilisée par le périphérique WAP.

Étape 1. Par défaut, la case *Utiliser les paramètres globaux du serveur RADIUS* est cochée. Décochez la case si vous voulez configurer le VAP pour qu'il utilise un autre ensemble de serveurs RADIUS. Sinon, passez à l'étape 8.



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 2. Dans le champ *Type d'adresse IP du serveur*, sélectionnez le type d'adresse IP du



serveur utilisé par votre périphérique WAP. Les options sont *IPv4* ou *IPv6*. IPv4 utilise des nombres binaires de 32 bits représentés en notation décimale à point. IPv6 utilise des nombres hexadécimaux et des deux-points pour représenter un nombre binaire de 128 bits. Le périphérique WAP contacte uniquement le ou les serveurs RADIUS pour le type d'adresse que vous avez sélectionné dans ce champ. Si vous choisissez IPv6, passez à l'étape 4.

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 3. Si vous avez sélectionné **IPv4** à l'étape 2, entrez l'adresse IP du serveur RADIUS que tous les VAP utilisent par défaut. Passez ensuite à l'étape 5.

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)

**Note:** Vous pouvez avoir jusqu'à trois adresses de serveur RADIUS de sauvegarde IPv4. Si l'authentification échoue avec le serveur principal, chaque serveur de sauvegarde configuré est essayé en séquence.

Étape 4. Si vous avez sélectionné **IPv6** à l'étape 2, saisissez l'adresse IPv6 du serveur RADIUS global principal.

The screenshot shows a configuration window for RADIUS server settings. At the top, there is a checkbox labeled "Use global RADIUS server settings" which is unchecked. Below this, the "Server IP Address Type" is set to "IPv6" (indicated by a selected radio button). There are four input fields for "Server IPv6 Address-1" through "Server IPv6 Address-4", each followed by a placeholder "(xxxxCxxxxCxxxxCxxxxCxxxxCxxxxCxxxxCxxxxCxxxx)". The first address field, "2001:DB8:1234:abcd::", is highlighted with a red rectangular box. Below the address fields are four "Key" fields, labeled "Key-1" through "Key-4", each with a text input area and a "(Range: 1-64 Characters)" label. The "Key-1" field contains a series of black dots. At the bottom, there is an unchecked checkbox for "Enable RADIUS Accounting". Below that is an "Active Server:" dropdown menu currently set to "Server IP Address-1". Finally, there are two numeric input fields: "Broadcast Key Refresh Rate" set to "300" and "Session Key Refresh Rate" set to "0", both with "(Range: 0-86400, 0 = Disable, Default: 300)" and "(Range: 30-86400, 0 = Disable, Default: 0)" labels respectively.

**Note:** Vous pouvez avoir jusqu'à trois adresses de serveur RADIUS de sauvegarde IPv6. Si l'authentification échoue avec le serveur principal, chaque serveur de sauvegarde configuré est essayé en séquence.

Étape 5. Dans le champ *Key-1*, saisissez la clé secrète partagée que le périphérique WAP utilise pour s'authentifier auprès du serveur RADIUS principal.

Use global RADIUS server settings

Server IP Address Type:  IPv4  IPv6

Server IP Address-1: 192.168.10.23 (xxx.xxx.xxx.xxx)

Server IP Address-2: 192.168.11.1 (xxx.xxx.xxx.xxx)

Server IP Address-3: 192.168.12.2 (xxx.xxx.xxx.xxx)

Server IP Address-4: 192.168.13.3 (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: Server IP Address-1

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

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

Étape 6. Dans les champs *Key-2* to *Key-4*, saisissez la clé RADIUS associée aux serveurs RADIUS de sauvegarde configurés. L'adresse IP du serveur 2 utilise *Key-2*, l'adresse IP du serveur 3 utilise *Key-3* et l'adresse IP du serveur 4 utilise *Key-4*.

Use global RADIUS server settings

Server IP Address Type:  IPv4  IPv6

Server IP Address-1: 192.168.10.23 (xxx.xxx.xxx.xxx)

Server IP Address-2: 192.168.11.1 (xxx.xxx.xxx.xxx)

Server IP Address-3: 192.168.12.2 (xxx.xxx.xxx.xxx)

Server IP Address-4: 192.168.13.3 (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: Server IP Address-1

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

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

Étape 7. (Facultatif) Dans le champ *Activer la comptabilité RADIUS*, cochez la case si vous voulez activer le suivi et la mesure des ressources consommées par un utilisateur particulier. L'activation de la comptabilité RADIUS permet de suivre l'heure système et la quantité de données transmises et reçues. Les informations seront stockées dans le serveur Radius. Ceci sera activé pour le serveur RADIUS principal et tous les serveurs de sauvegarde.

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)

**Note:** Si vous avez activé la comptabilité RADIUS, elle est activée pour le serveur RADIUS principal et tous les serveurs de sauvegarde

Étape 8. Sélectionnez le premier serveur actif dans le champ *Serveur actif*. Cela permet de sélectionner manuellement le serveur RADIUS actif, plutôt que de demander au périphérique WAP de tenter de contacter chaque serveur configuré dans l'ordre et de choisir le premier serveur actif.

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 9. Dans le champ *Broadcast Key Refresh Rate*, saisissez l'intervalle au cours duquel la clé de diffusion (groupe) est actualisée pour les clients associés à ce VAP. 300 secondes sont établies par défaut.

Use global RADIUS server settings

Server IP Address Type:  IPv4  IPv6

Server IP Address-1: 192.168.10.23 (xxx.xxx.xxx.xxx)

Server IP Address-2: 192.168.11.1 (xxx.xxx.xxx.xxx)

Server IP Address-3: 192.168.12.2 (xxx.xxx.xxx.xxx)

Server IP Address-4: 192.168.13.3 (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: Server IP Address-1

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

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

Étape 10. Dans le champ *Session Key Refresh Rate*, saisissez l'intervalle auquel le périphérique WAP actualise la clé de session (monodiffusion) pour chaque client associé au VAP. 0 est établi par défaut.

Use global RADIUS server settings

Server IP Address Type:  IPv4  IPv6

Server IP Address-1: 192.168.10.23 (xxx.xxx.xxx.xxx)

Server IP Address-2: 192.168.11.1 (xxx.xxx.xxx.xxx)

Server IP Address-3: 192.168.12.2 (xxx.xxx.xxx.xxx)

Server IP Address-4: 192.168.13.3 (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: Server IP Address-1

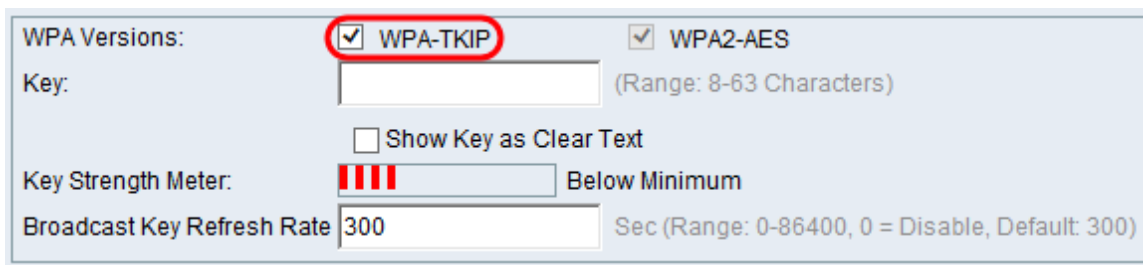
Broadcast Key Refresh Rate: 300 Sec (Range: 0-86400, 0 = Disable, Default: 300)

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

## WPA personnel

WPA Personal est une norme Wi-Fi Alliance IEEE 802.11i, qui inclut le chiffrement AES-CCMP et TKIP. WPA utilise une clé prépartagée (PSK) au lieu d'utiliser IEEE 802.1X et EAP comme utilisé en mode de sécurité WPA d'entreprise. La clé PSK est utilisée pour une vérification initiale des informations d'identification uniquement. WPA est également appelé WPA-PSK. Ce mode de sécurité est rétrocompatible pour les clients sans fil qui prennent en charge le WPA d'origine.

Étape 1. Dans le champ *WPA Versions*, cochez la case *WPA-TKIP* si vous souhaitez activer WPA-TKIP. WPA-TKIP et WPA2-AES peuvent être activés simultanément. Le WAP prend toujours en charge WPA2-AES, de sorte que vous ne pourrez pas le configurer.



The screenshot shows a configuration window for WPA security. Under 'WPA Versions', both 'WPA-TKIP' and 'WPA2-AES' are checked. The 'Key' field is empty, and the 'Key Strength Meter' shows four red bars, indicating a strength 'Below Minimum'. The 'Broadcast Key Refresh Rate' is set to 300 seconds.

Les options disponibles sont définies comme suit :

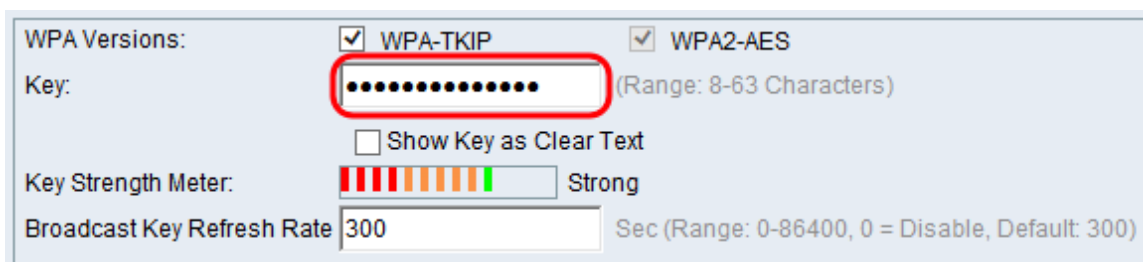
·WPA-TKIP : le réseau dispose de certaines stations clientes qui prennent uniquement en charge le protocole de sécurité WPA et TKIP d'origine. Selon les dernières exigences de WiFi Alliance, il n'est pas recommandé de choisir uniquement WPA-TKIP.

·WPA2-AES — 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. Selon la dernière exigence de WiFi Alliance, le point d'accès doit toujours prendre en charge ce mode.

·WPA-TKIP et WPA2-AES : si le réseau comporte un mélange de clients, dont certains prennent en charge WPA2 et d'autres qui ne prennent en charge que le WPA d'origine, cochez les deux cases. Ce paramètre permet aux stations client WPA et WPA2 de s'associer et de s'authentifier, mais utilise le WPA2 plus robuste pour les clients qui le prennent en charge. Cette configuration WPA permet une plus grande interopérabilité au lieu d'une certaine sécurité.

**Note:** Les clients WPA doivent avoir une de ces clés (une clé TKIP valide ou une clé AES-CCMP valide) pour pouvoir s'associer au périphérique WAP.

Étape 2. Dans le champ *Key*, saisissez la clé secrète partagée pour la sécurité WPA Personal. Saisissez au moins 8 caractères et un maximum de 63 caractères.



The screenshot shows the same configuration window as before, but now the 'Key' field contains ten black dots, indicating a password has been entered. The 'Key Strength Meter' now shows seven bars (four red, three orange, one green), indicating a strength of 'Strong'.

**Note:** Les caractères acceptés comprennent les lettres alphabétiques majuscules et minuscules, les chiffres et les symboles spéciaux (?!\@#\$\$%^&\*).

Étape 3. (Facultatif) Cochez la case *Afficher la clé en texte clair* si vous voulez que le texte que vous tapez soit visible. La case est décochée par défaut.

WPA Versions:  WPA-TKIP  WPA2-AES

Key:  (Range: 8-63 Characters)

Show Key as Clear Text

Key Strength Meter: Strong

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

**Remarque :** Lorsque vous utilisez un autre micrologiciel sur les points d'accès WAP351, WAP131 ou WAP371, le champ *Afficher la clé en clair* peut être manquant.

**Note:** Le champ *Key Strength Meter* indique où le périphérique WAP vérifie la clé en fonction de critères de complexité tels que le nombre de types différents de caractères utilisés et la durée de validité de la clé. Si la fonction de contrôle de la complexité WPA-PSK est activée, la clé n'est pas acceptée, sauf si elle répond aux critères minimaux. Pour plus d'informations sur la complexité WPA-PSK, référez-vous à [Configuration de la complexité du mot de passe pour les WAP131, WAP351 et WAP371](#).

WPA Versions:  WPA-TKIP  WPA2-AES

Key:  (Range: 8-63 Characters)

Show Key as Clear Text

Key Strength Meter: Strong

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

Étape 4. Dans le champ *Broadcast Key Refresh Rate*, saisissez l'intervalle au cours duquel la clé de diffusion (groupe) est actualisée pour les clients associés à ce VAP. 300 secondes sont établies par défaut.

WPA Versions:  WPA-TKIP  WPA2-AES

Key:  (Range: 8-63 Characters)

Show Key as Clear Text

Key Strength Meter: Strong

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

## WPA Enterprise

WPA Enterprise with RADIUS est une implémentation de la norme IEEE 802.11i de Wi-Fi Alliance, qui inclut le cryptage CCMP (AES) et TKIP. Le mode Entreprise nécessite l'utilisation d'un serveur RADIUS pour authentifier les utilisateurs. Le mode de sécurité est rétrocompatible avec les clients sans fil qui prennent en charge le WPA d'origine.

**Note:** Le mode VLAN dynamique est activé par défaut, ce qui permet au serveur d'authentification RADIUS de décider quel VLAN est utilisé pour les stations.

Étape 1. Dans le champ *WPA Versions*, cochez la case pour les types de stations clientes à prendre en charge. Ils sont tous activés par défaut. Le point d'accès doit prendre en charge WPA2-AES tout le temps afin que vous ne puissiez pas le configurer.



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)

Les options disponibles sont définies comme suit :

- WPA-TKIP : le réseau dispose de certaines stations clientes qui prennent uniquement en charge les protocoles de sécurité WPA et TKIP d'origine. Notez que la sélection uniquement de WPA-TKIP pour le point d'accès n'est pas autorisée conformément à la dernière exigence de WiFi Alliance.

- WPA2-AES — Toutes les stations clientes du réseau prennent en charge la version WPA2 et le protocole de chiffrement/sécurité AES-CCMP. Cette version WPA fournit 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.

- Activer la pré-authentification : si vous choisissez uniquement WPA2 ou WPA et WPA2 comme version WPA, vous pouvez activer la pré-authentification pour les clients WPA2. 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 WAP. Cette option ne s'applique pas si vous avez sélectionné WPA pour les versions WPA, car le WPA d'origine ne prend pas en charge cette fonctionnalité.

**Note:** Les stations clientes configurées pour utiliser WPA avec RADIUS doivent avoir une des adresses et clés suivantes : Une adresse IP TKIP RADIUS ou CCMP (AES) valide et une clé RADIUS.

Étape 2. Par défaut, la case *Utiliser les paramètres globaux du serveur RADIUS* est cochée. Décochez la case si vous voulez configurer le VAP pour qu'il utilise un autre ensemble de serveurs RADIUS. Sinon, passez à l'étape 9.



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 3. Dans le champ *Type d'adresse IP du serveur*, sélectionnez le type d'adresse IP du serveur utilisé par votre périphérique WAP. Les options sont *IPv4* ou *IPv6*. IPv4 utilise des nombres binaires de 32 bits représentés en notation décimale à point. IPv6 utilise des nombres hexadécimaux et des deux-points pour représenter un nombre binaire de 128 bits. Le périphérique WAP contacte uniquement le ou les serveurs RADIUS pour le type d'adresse que vous avez sélectionné dans ce champ.

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 4. Si vous avez sélectionné **IPv4** à l'étape 2, entrez l'adresse IP du serveur RADIUS que tous les VAP utilisent par défaut. Passez ensuite à l'étape 6.

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)

**Note:** Vous pouvez avoir jusqu'à trois adresses de serveur RADIUS de sauvegarde IPv4. Si l'authentification échoue avec le serveur principal, chaque serveur de sauvegarde configuré est essayé en séquence.

Étape 5. Si vous avez sélectionné **IPv6** à l'étape 2, saisissez l'adresse IPv6 du serveur RADIUS global principal.

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

Use global RADIUS server settings

Server IP Address Type:  IPv4  IPv6

Server IPv6 Address-1: 2001:DB8:1234:abcd:: (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx)

Server IPv6 Address-2: 2002:DB8:1234:abcd:: (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx)

Server IPv6 Address-3: 2003:DB8:1234:abcd:: (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx)

Server IPv6 Address-4: 2004:DB8:1234:abcd:: (xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx)

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: Server IP Address-1 ▼

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

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

**Note:** Vous pouvez avoir jusqu'à trois adresses de serveur RADIUS de sauvegarde IPv6. Si l'authentification échoue avec le serveur principal, chaque serveur de sauvegarde configuré est essayé en séquence.

Étape 6. Dans le champ *Key-1*, saisissez la clé secrète partagée que le périphérique WAP utilise pour s'authentifier auprès du serveur RADIUS principal.

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. Dans les champs *Key-2* to *Key-4*, saisissez la clé RADIUS associée aux serveurs RADIUS de sauvegarde configurés. L'adresse IP du serveur 2 utilise *Key-2*, l'adresse IP du serveur 3 utilise *Key-3* et l'adresse IP du serveur 4 utilise *Key-4*.

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. (Facultatif) Dans le champ *Activer la comptabilité RADIUS*, cochez la case si vous voulez activer le suivi et la mesure des ressources consommées par un utilisateur particulier.

L'activation de la comptabilité RADIUS vous permettra de suivre l'heure système d'un utilisateur donné et la quantité de données transmises et reçues.

WPA Versions: <input checked="" type="checkbox"/> WPA-TKIP <input checked="" type="checkbox"/> WPA2-AES	
<input checked="" type="checkbox"/> Enable pre-authentication	
<input type="checkbox"/> Use global RADIUS server settings	
Server IP Address Type:	<input checked="" type="radio"/> IPv4 <input type="radio"/> IPv6
Server IP Address-1:	<input type="text" value="192.168.10.23"/> (xxx.xxx.xxx.xxx)
Server IP Address-2:	<input type="text" value="192.168.10.24"/> (xxx.xxx.xxx.xxx)
Server IP Address-3:	<input type="text" value="192.168.10.25"/> (xxx.xxx.xxx.xxx)
Server IP Address-4:	<input type="text" value="192.168.10.26"/> (xxx.xxx.xxx.xxx)
Key-1:	<input type="text" value="••••••••"/> (Range: 1-64 Characters)
Key-2:	<input type="text" value="••••••••"/> (Range: 1-64 Characters)
Key-3:	<input type="text" value="••••~••••"/> (Range: 1-64 Characters)
Key-4:	<input type="text" value="••••••••"/> (Range: 1-64 Characters)
<input checked="" type="checkbox"/> Enable RADIUS Accounting	
Active Server:	<input type="text" value="Server IP Address-1"/> ▼
Broadcast Key Refresh Rate:	<input type="text" value="300"/> Sec (Range: 0-86400, 0 = Disable, Default: 300)
Session Key Refresh Rate:	<input type="text" value="0"/> Sec (Range: 30-86400, 0 = Disable, Default: 0)

**Note:** Si vous avez activé la comptabilité RADIUS, elle est activée pour le serveur RADIUS principal et tous les serveurs de sauvegarde.

Étape 9. Sélectionnez le premier serveur actif dans le champ *Serveur actif*. Cela permet de sélectionner manuellement le serveur RADIUS actif, plutôt que de demander au périphérique WAP de contacter chaque serveur configuré dans l'ordre.

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: Server IP Address-1  
Server IP Address-2  
Server IP Address-3  
Server IP Address-4

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. Dans le champ *Broadcast Key Refresh Rate*, saisissez l'intervalle au cours duquel la clé de diffusion (groupe) est actualisée pour les clients associés à ce VAP. 300 secondes sont établies par défaut.

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

Étape 11. Dans le champ *Session Key Refresh Rate*, saisissez l'intervalle auquel le périphérique WAP actualise les clés de session (monodiffusion) pour chaque client associé

au VAP. 0 est établi par défaut.

WPA Versions:  WPA-TKIP  WPA2-AES  
 Enable pre-authentication  
 Use global RADIUS server settings

Server IP Address Type:  IPv4  IPv6

Server IP Address-1: 192.168.10.23 (xxx.xxx.xxx.xxx)  
Server IP Address-2: 192.168.10.24 (xxx.xxx.xxx.xxx)  
Server IP Address-3: 192.168.10.25 (xxx.xxx.xxx.xxx)  
Server IP Address-4: 192.168.10.26 (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: Server IP Address-1

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

## Filtre MAC

Le filtre MAC spécifie si les stations qui peuvent accéder à ce VAP sont limitées à une liste globale d'adresses MAC configurée.

Étape 1. Dans la liste déroulante *Filtre MAC*, sélectionnez le type de filtrage MAC souhaité.

Select the radio interface first, and then enter the configuration parameters.

Radio:  Radio 1 (2.4 GHz)  Radio 2 (5 GHz)

VAP No.	Enable	VLAN ID	SSID Name	SSID Broadcast	Security	MAC Filter	Channel Isolation
<input type="checkbox"/> 0	<input checked="" type="checkbox"/>	1	DISCOFD	<input checked="" type="checkbox"/>	None	Disabled	<input type="checkbox"/>
<input checked="" type="checkbox"/> 1	<input checked="" type="checkbox"/>	1	CiscoSBTest	<input checked="" type="checkbox"/>	None	Disabled Local RADIUS	<input type="checkbox"/>

Add Edit Delete

Les options disponibles sont définies comme suit :

·Désactivé : n'utilise pas le filtrage MAC.

Local : utilise la liste d'authentification MAC que vous configurez dans la section Filtrage MAC pour en savoir plus sur le filtrage MAC, reportez-vous à [Comment configurer le filtrage MAC sur les WAP351 et WAP131](#).

·RADIUS : utilise la liste d'authentification MAC sur un serveur RADIUS externe.

## Isolement du canal

Lorsque l'isolement de canal est désactivé, les clients sans fil peuvent communiquer entre eux normalement en envoyant du trafic via le périphérique WAP. Lorsqu'il est activé, le

périphérique WAP bloque la communication entre les clients sans fil sur le même VAP. Le périphérique WAP autorise toujours le trafic de données entre ses clients sans fil et les périphériques câblés sur le réseau, via une liaison WDS, et avec d'autres clients sans fil associés à un VAP différent, mais pas entre les clients sans fil.

Étape 1. Dans le champ *Isolation de canal*, cochez la case si vous voulez activer l'Isolation de canal.

Select the radio interface first, and then enter the configuration parameters.

Radio:  Radio 1 (2.4 GHz)  Radio 2 (5 GHz)

VAP No.	Enable	VLAN ID <small>Add New VLAN</small>	SSID Name	SSID Broadcast	Security	MAC Filter	Channel Isolation
0	<input checked="" type="checkbox"/>	1	discosb	<input checked="" type="checkbox"/>	None	Disabled	<input type="checkbox"/>
1	<input checked="" type="checkbox"/>	1	CiscoSBTest	<input checked="" type="checkbox"/>	None	Disabled	<input checked="" type="checkbox"/>

Add Edit Delete

Étape 2. Cliquez **Save**.

**Note:** Une fois les nouveaux paramètres enregistrés, les processus correspondants peuvent être arrêtés et redémarrés. Lorsque cette condition se produit, le périphérique WAP peut perdre la connectivité. Nous vous recommandons de modifier les paramètres du périphérique WAP lorsqu'une perte de connectivité affectera le moins vos clients sans fil.

## Régleur de bande

Band Steer est uniquement disponible sur le WAP371. Band Steer utilise efficacement la bande 5 GHz en orientant les clients pris en charge b bande de la bande 2,4 GHz vers la bande 5 GHz. Cela libère la bande 2,4 GHz pour une utilisation par un périphérique hérité qui ne prend pas en charge la double radio.

**Note:** Les radios 5 GHz et 2,4 GHz doivent toutes deux être activées pour utiliser Band Steer. Pour plus d'informations sur l'activation des radios, référez-vous à [Comment configurer les paramètres radio de base sur le WAP371](#).

Étape 1. Band Steer est configuré par VAP et doit être activé sur les deux radios. Si vous souhaitez activer l'indicateur de bande, cochez la case du champ Indicateur de bande.

Select the radio interface first, and then enter the configuration parameters.

Radio:  Radio 1 (5 GHz)  Radio 2 (2.4 GHz)

VAP No.	Enable	VLAN ID	SSID Name	SSID Broadcast	Security	MAC Filter	Channel Isolation	Band Steer
0	<input checked="" type="checkbox"/>	1	discosb	<input checked="" type="checkbox"/>	WPA Personal	Disabled	<input type="checkbox"/>	<input type="checkbox"/>
1	<input checked="" type="checkbox"/>	1	CiscoSBTest	<input checked="" type="checkbox"/>	None	Disabled	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Add Edit Delete

**Note:** Band Steer n'est pas encouragé sur les points d'accès virtuels avec un trafic voix ou vidéo sensible au temps. Même si la radio 5 GHz utilise moins de bande passante, elle tente d'orienter les clients vers cette radio.

Étape 2. Cliquez **Save**.

## Suppression d'un VAP

Étape 1. Cochez la case du VAP à supprimer.



Select the radio interface first, and then enter the configuration parameters.

Radio:  Radio 1 (2.4 GHz)  
 Radio 2 (5 GHz)

Virtual Access Points (SSIDs)									
VAP No.	Enable	VLAN ID	SSID Name	SSID Broadcast	Security	MAC Filter	Channel Isolation		
<input type="checkbox"/>	<input checked="" type="checkbox"/>	1	discosb	<input checked="" type="checkbox"/>	WPA Personal	Disabled	<input type="checkbox"/>		
<a href="#">Show Details</a>									
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1	CiscoSBTest	<input checked="" type="checkbox"/>	WPA Personal	Disabled	<input type="checkbox"/>		
<a href="#">Show Details</a>									

Étape 2. Cliquez sur **Supprimer** pour supprimer le VAP.

Select the radio interface first, and then enter the configuration parameters.

Radio:  Radio 1 (2.4 GHz)  
 Radio 2 (5 GHz)

Virtual Access Points (SSIDs)									
VAP No.	Enable	VLAN ID	SSID Name	SSID Broadcast	Security	MAC Filter	Channel Isolation		
<input type="checkbox"/>	<input checked="" type="checkbox"/>	1	discosb	<input checked="" type="checkbox"/>	WPA Personal	Disabled	<input type="checkbox"/>		
<a href="#">Show Details</a>									
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1	CiscoSBTest	<input checked="" type="checkbox"/>	WPA Personal	Disabled	<input type="checkbox"/>		
<a href="#">Show Details</a>									

Étape 3. Cliquez sur **Enregistrer** pour enregistrer définitivement votre suppression.

Select the radio interface first, and then enter the configuration parameters.

Radio:  Radio 1 (2.4 GHz)  
 Radio 2 (5 GHz)

Virtual Access Points (SSIDs)									
VAP No.	Enable	VLAN ID	SSID Name	SSID Broadcast	Security	MAC Filter	Channel Isolation		
<input type="checkbox"/>	<input checked="" type="checkbox"/>	1	discosb	<input checked="" type="checkbox"/>	None	Disabled	<input type="checkbox"/>		