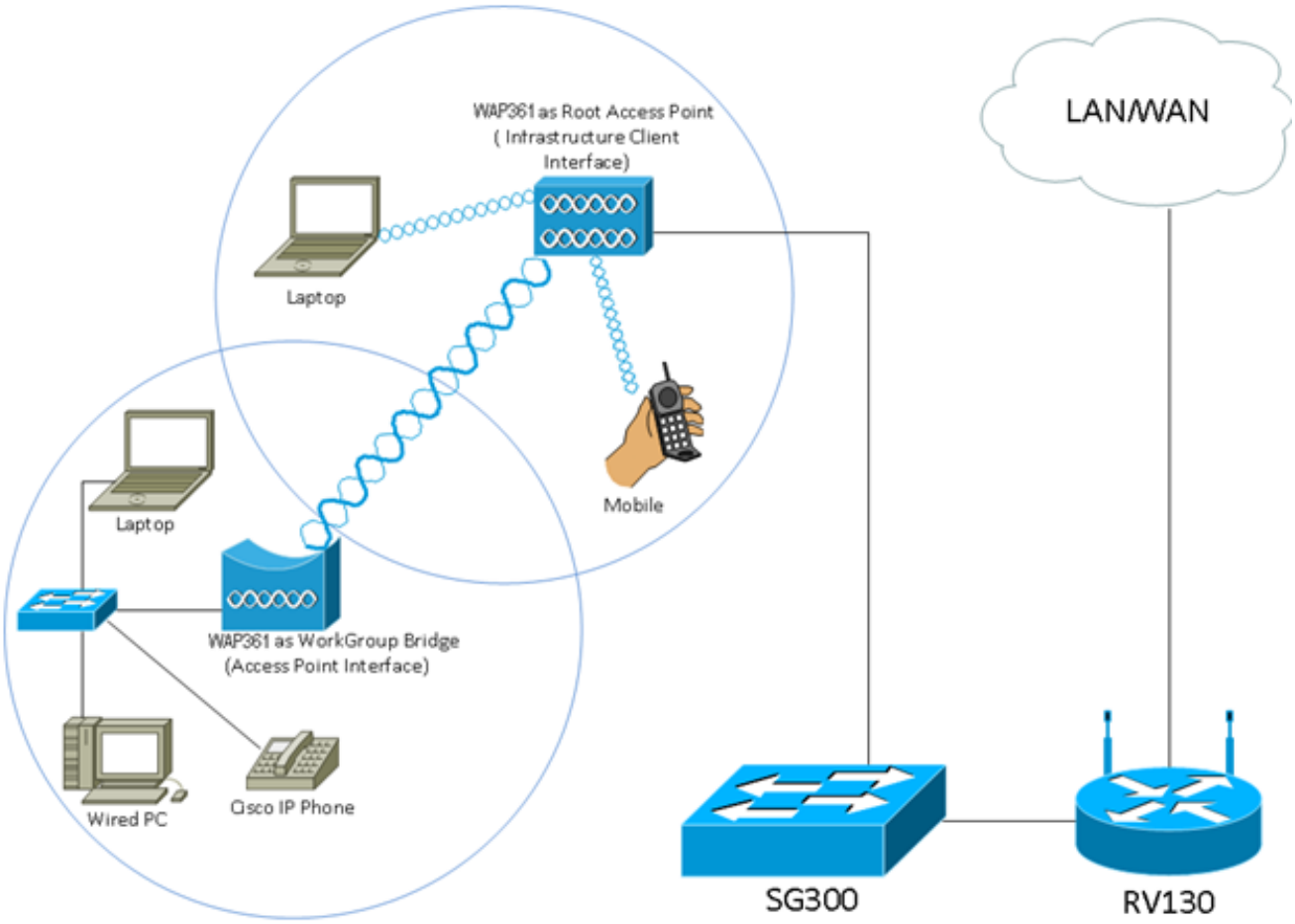
Configurer le pont de groupe de travail sur un point d'accès sans fil (WAP)

Objectif

La fonctionnalité WorkGroup Bridge permet au point d'accès sans fil (WAP) de relier le trafic entre un client distant et le réseau local (LAN) sans fil connecté au mode pont de groupe de travail. Le périphérique WAP associé à l'interface distante est appelé interface de point d'accès, tandis que le périphérique WAP associé au réseau local sans fil est appelé interface d'infrastructure. Le pont WorkGroup permet aux périphériques qui ne disposent que de connexions câblées de se connecter à un réseau sans fil. Le mode pont de groupe de travail est recommandé comme alternative lorsque la fonctionnalité Wireless Distribution System (WDS) n'est pas disponible.



Note: La topologie ci-dessus illustre un exemple de modèle WorkGroup Bridge. Les périphériques filaires sont raccordés à un commutateur, qui se connecte à l'interface LAN du WAP. Le WAP agit comme une interface de point d'accès, se connecte à l'interface d'infrastructure.

Cet article vise à vous montrer comment configurer le pont WorkGroup entre deux WAP.

Périphériques pertinents

- Gamme WAP100
- Gamme WAP300
- Gamme WAP500

Version du logiciel

- 1.0.0.17 : WAP571, WAP571E
- 1.0.1.7 - WAP150, WAP361
- 1.0.2.5 - WAP131, WAP351
- 1.0.6.5 - WAP121, WAP321
- 1.2.1.3 - WAP551, WAP561
- 1.3.0.3 - WAP371

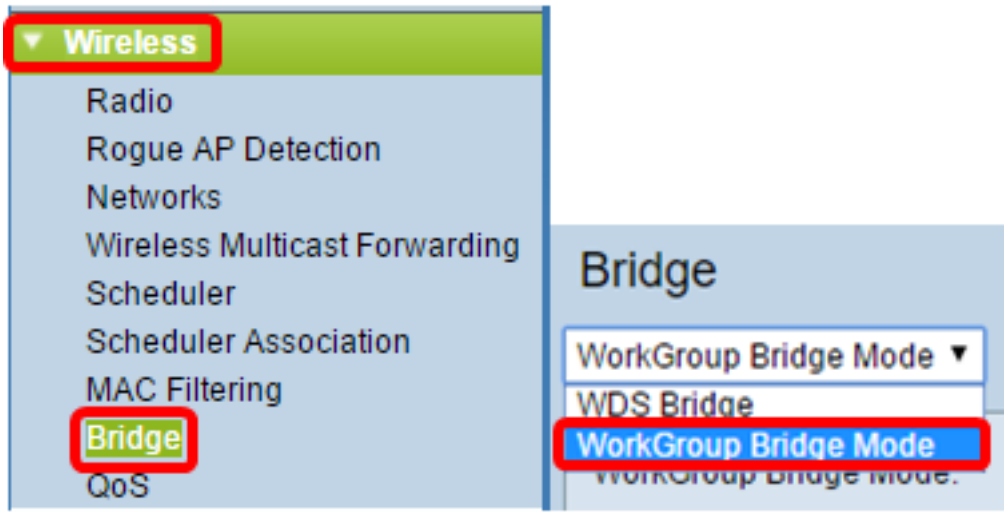
Configurer le pont de groupe de travail

Interface client d'infrastructure

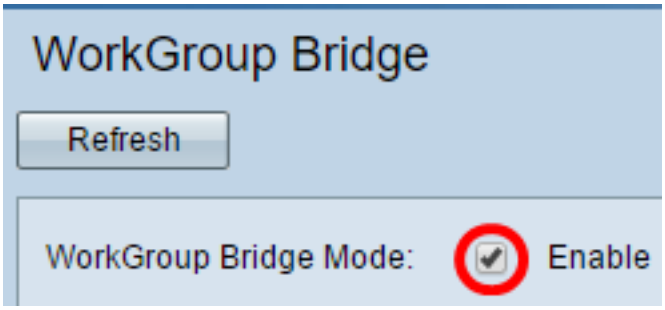
Étape 1. Connectez-vous à l'utilitaire Web du WAP et choisissez **Wireless > WorkGroup Bridge**.

Note: Les options de menu peuvent varier en fonction du modèle du périphérique que vous utilisez. Sauf indication contraire, les images ci-dessous proviennent du WAP361.

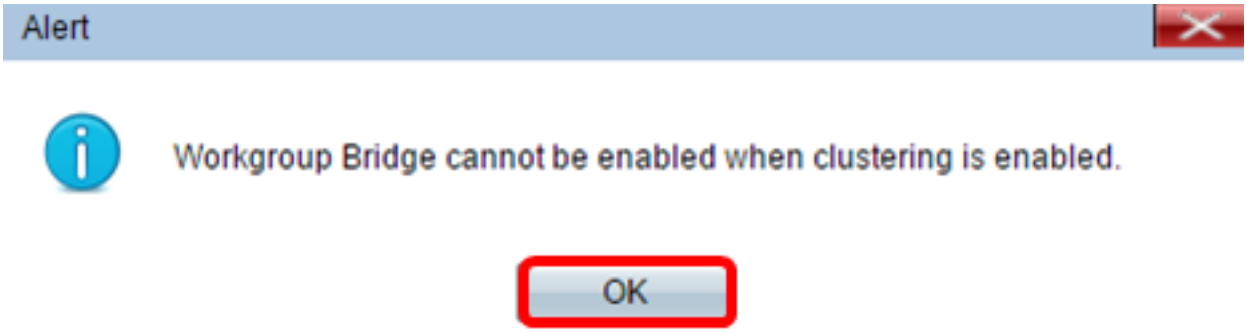
Pour WAP571 et WAP571E, choisissez **Wireless > Bridge > WorkGroup Bridge Mode**.



Étape 2. Cochez la case **Activer le** mode pont du groupe de travail.

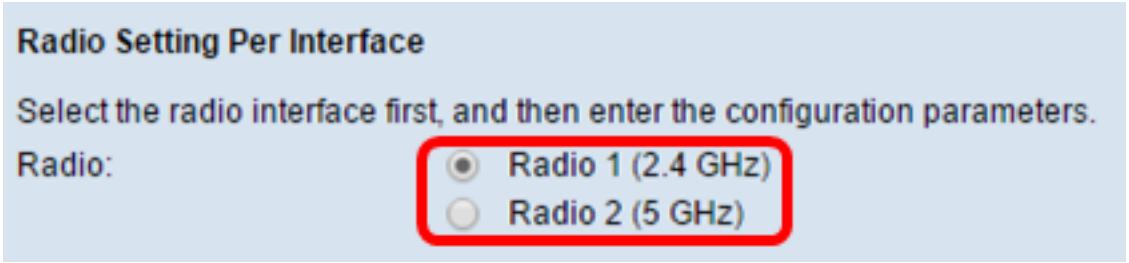


Note: Si le clustering est activé sur le WAP, une fenêtre contextuelle vous avertit de désactiver le clustering afin que le pont WorkGroup fonctionne. Cliquez sur **OK pour continuer.** Pour désactiver la mise en grappe, choisissez **Configuration par point unique** dans le volet de navigation, puis choisissez **Points d'accès > Désactiver la configuration par point unique**.



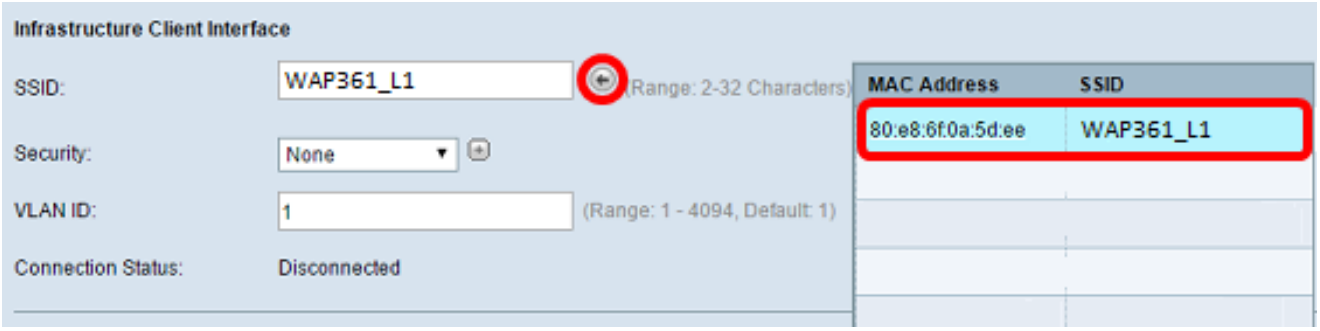
Étape 3. Cliquez sur l'interface radio du pont Groupe de travail. Lorsque vous configurez une radio en tant que pont de groupe de travail, l'autre radio reste opérationnelle. Les interfaces radio correspondent aux bandes de fréquences radio du WAP. Le WAP est équipé pour diffuser sur deux interfaces radio différentes. La configuration des paramètres d'une interface radio n'affecte pas l'autre. Les options d'interface radio peuvent varier en fonction du modèle WAP. Certains WAP affichent Radio 1 comme 2,4 GHz tandis que d'autres ont Radio 2 comme 2,4 GHz.

Note: Cette étape concerne uniquement les WAP suivants avec double bande : WAP131, WAP150, WAP351, WAP361, WAP371, WAP561, WAP571, WAP571E. Dans cet exemple, Radio 1 est sélectionné.



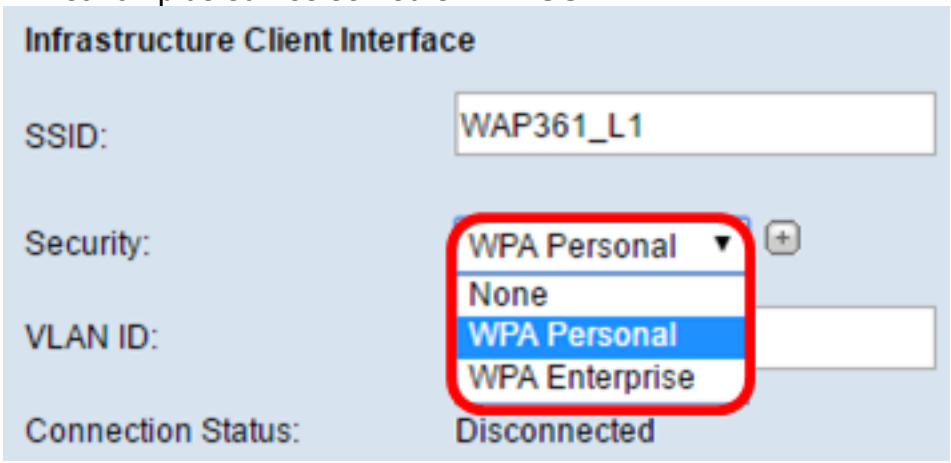
Étape 4. Entrez le nom SSID (Service Set Identifier) dans le champ *SSID* ou cliquez sur le bouton fléché en regard du champ pour rechercher les voisins. Cela sert de connexion entre le périphérique et le client distant. Vous pouvez saisir 2 à 32 caractères pour le SSID du client d'infrastructure.

Note: Il est important d'activer la détection des points d'accès indésirables. Pour en savoir plus sur l'activation de cette fonctionnalité, cliquez ici. Dans cet exemple, cliquez sur le bouton fléché pour sélectionner WAP361_L1 comme SSID de l'interface client d'infrastructure.



Étape 5. Dans la zone Infrastructure Client Interface, sélectionnez le type de sécurité à authentifier en tant que station client sur le périphérique WAP en amont dans la liste déroulante Security. Les options sont les suivantes :

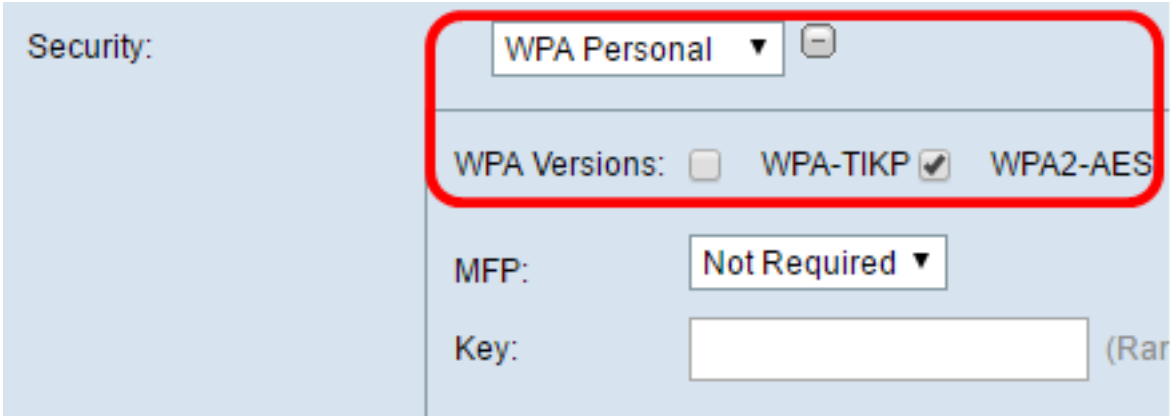
- Aucun — Ouvrir ou pas de sécurité. Il s'agit de la configuration par défaut. Si cette option est sélectionnée, passez à l'étape 18.
- WPA Personal : WPA Personal peut prendre en charge des clés de 8 à 63 caractères. WPA2 est recommandé car il dispose d'une norme de cryptage plus puissante. Passez à l'étape 6 pour configurer.
- WPA Enterprise - WPA Enterprise est plus avancé que WPA Personal et constitue la sécurité recommandée pour l'authentification. Il utilise les protocoles PEAP (Protected Extensible Authentication Protocol) et TLS (Transport Layer Security). Passez à l'étape 9 pour configurer. Ce type de sécurité est souvent utilisé dans un environnement de bureau et nécessite un serveur RADIUS (Remote Authentication Dial-In User Service) configuré. Cliquez ici pour en savoir plus sur les serveurs RADIUS.



Note: Dans cet exemple, WPA Personal est sélectionné.

Étape 6. Cliquez sur le signe **+** et cochez la case WPA-TKIP ou WPA2-AES pour déterminer le type de cryptage WPA que l'interface client de l'infrastructure utilisera.

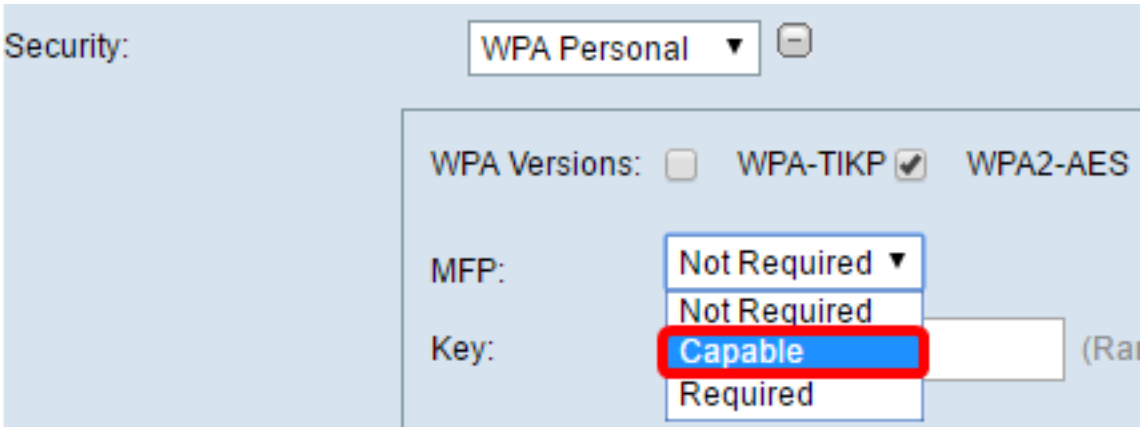
Note: Si tous vos équipements sans fil prennent en charge WPA2, définissez la sécurité du client d'infrastructure sur WPA2-AES. La méthode de cryptage est RC4 pour WPA et Advanced Encryption Standard (AES) pour WPA2. WPA2 est recommandé car il dispose d'une norme de cryptage plus puissante. Dans cet exemple, WPA2-AES est utilisé.



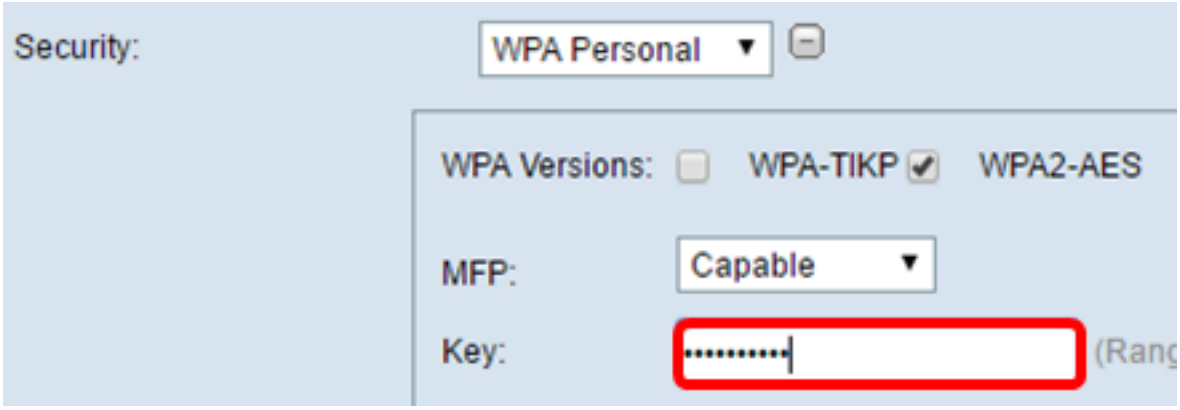
Étape 7. (Facultatif) Si vous avez coché WPA2-AES à l'étape 6, choisissez une option dans la liste déroulante Management Frame Protection (MFP), que vous souhaitiez que le WAP exige ou non des trames protégées. Pour en savoir plus sur la MFP, cliquez ici. Les options sont les suivantes :

- Not Required : désactive la prise en charge du client pour MFP.
- Capable : permet à la fois aux clients compatibles MFP et aux clients qui ne prennent pas en charge MFP de rejoindre le réseau. Il s'agit du paramètre MFP par défaut sur le WAP.
- Obligatoire : les clients ne sont autorisés à s'associer que si MFP est négocié. Si les périphériques ne prennent pas en charge MFP, ils ne sont pas autorisés à se connecter au réseau.

Note: Dans cet exemple, Capable est sélectionné.



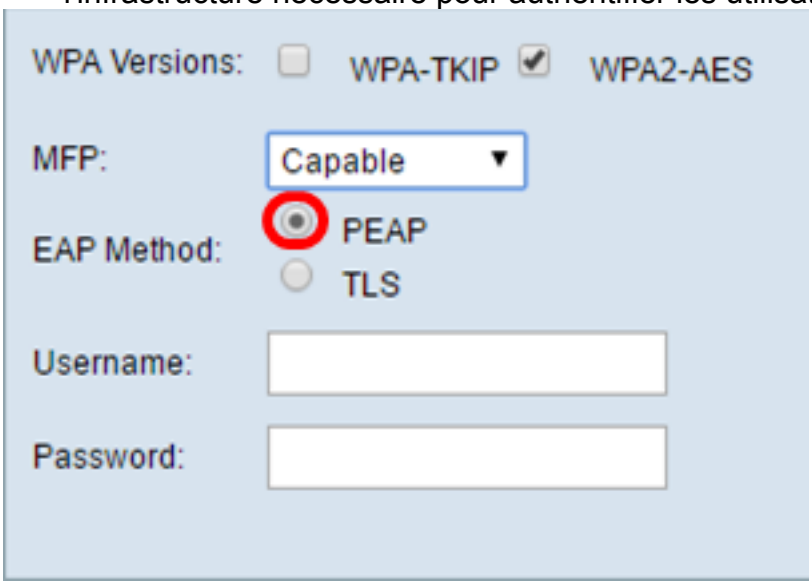
Étape 8. Entrez la clé de chiffrement WPA dans le champ *Key*. La clé doit comporter entre 8 et 63 caractères. Il s'agit d'une combinaison de lettres, de chiffres et de caractères spéciaux. Il s'agit du mot de passe utilisé pour la première connexion au réseau sans fil. Passez ensuite à l'étape 18.



Étape 9. Si vous avez choisi WPA Enterprise à l'étape 5, cliquez sur une case d'option pour la méthode EAP.

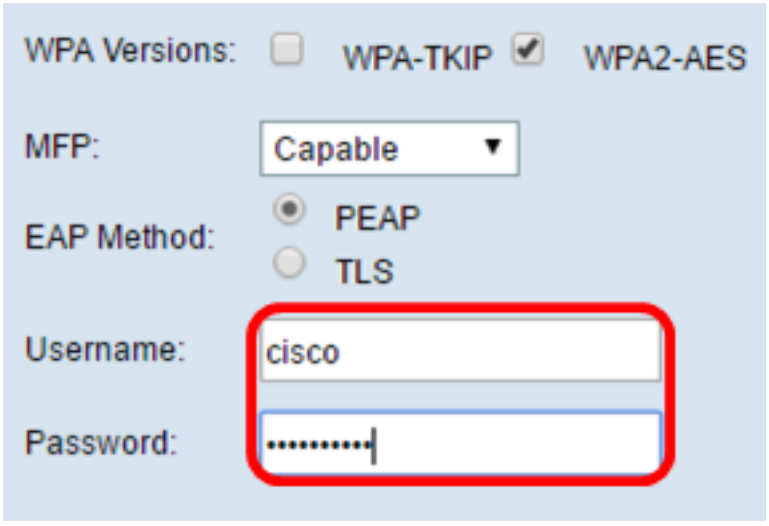
Les options disponibles sont définies comme suit :

- PEAP : ce protocole donne à chaque utilisateur sans fil des noms d'utilisateur et des mots de passe individuels WAP prenant en charge les normes de cryptage AES. Puisque le PEAP est une méthode de sécurité basée sur un mot de passe, votre sécurité Wi-Fi est basée sur les informations d'identification du périphérique du client. Le protocole PEAP peut présenter un risque de sécurité grave si vous avez des mots de passe faibles ou des clients non sécurisés. Il s'appuie sur TLS mais évite l'installation de certificats numériques sur chaque client. Au lieu de cela, il fournit l'authentification par un nom d'utilisateur et un mot de passe.
- TLS : TLS exige que chaque utilisateur dispose d'un certificat supplémentaire pour obtenir l'accès. TLS est plus sécurisé si vous disposez des serveurs supplémentaires et de l'infrastructure nécessaire pour authentifier les utilisateurs sur votre réseau.



Note: Dans cet exemple, le protocole PEAP est choisi.

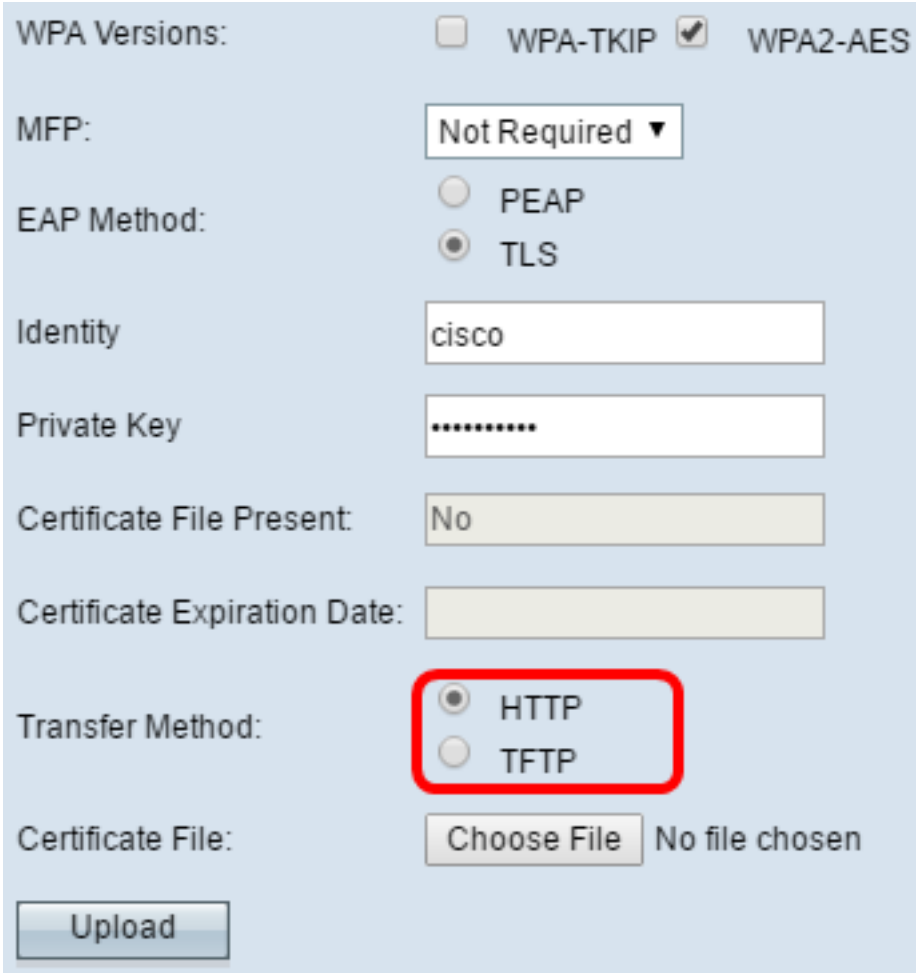
Étape 10. Entrez le nom d'utilisateur et le mot de passe du client d'infrastructure dans les champs *Username* et *Password*. Il s'agit des informations de connexion utilisées pour se connecter à l'interface client de l'infrastructure ; reportez-vous à l'interface client de votre infrastructure pour trouver ces informations. Passez ensuite à l'étape 18.



Étape 11. Si vous avez cliqué sur TLS à l'étape 9, saisissez l'identité et la clé privée du client d'infrastructure dans les champs *Identité* et *Clé privée*.

Étape 12. Dans la zone Méthode de transfert, cliquez sur une case d'option des options suivantes :

- TFTP : le protocole TFTP (Trivial File Transfer Protocol) est une version simplifiée non sécurisée du protocole FTP (File Transfer Protocol). Il est principalement utilisé pour distribuer des logiciels ou authentifier des périphériques parmi les réseaux d'entreprise. Si vous avez cliqué sur TFTP, passez à l'étape 15.
- HTTP : le protocole HTTP (Hypertext Transfer Protocol) fournit un cadre d'authentification de réponse à un défi simple qui peut être utilisé par un client pour fournir un cadre d'authentification.

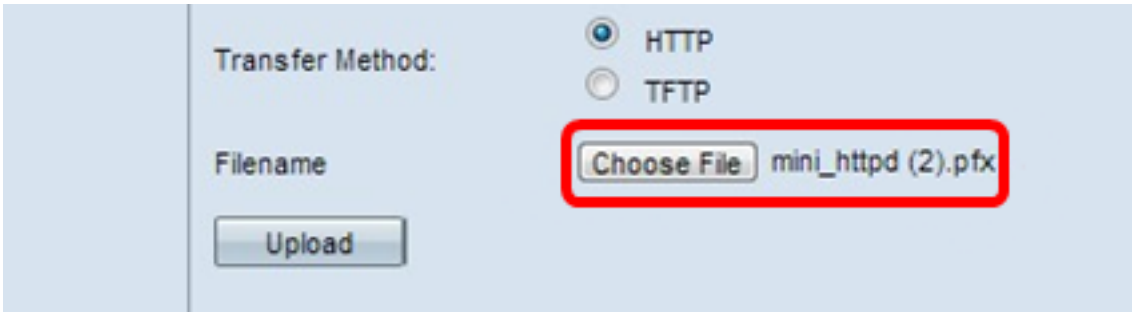


Remarque : Si un fichier de certificat est déjà présent sur le WAP, les champs *Fichier de certificat présent* et Date d'*expiration du certificat* seront déjà remplis avec les informations pertinentes. Sinon, elles seront vides.

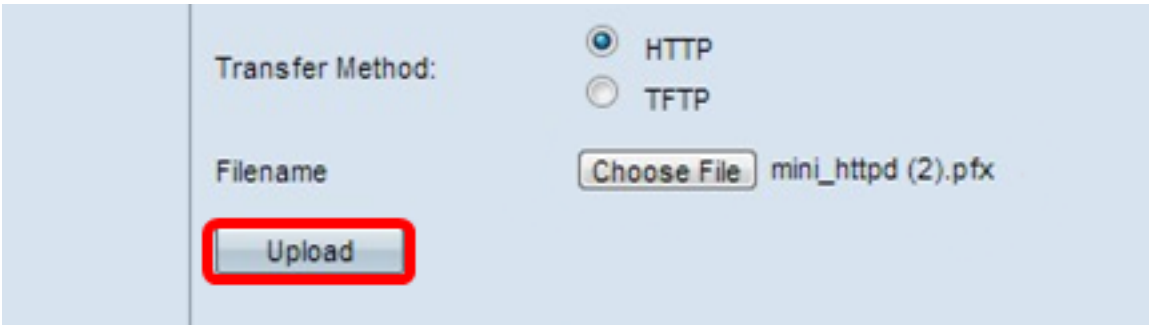
HTTP

Étape 13. Cliquez sur le bouton **Choisir un fichier** pour rechercher et sélectionner un fichier de certificat. Le fichier doit avoir l'extension de fichier de certificat appropriée (par exemple .pem ou .pfx) sinon le fichier ne sera pas accepté.

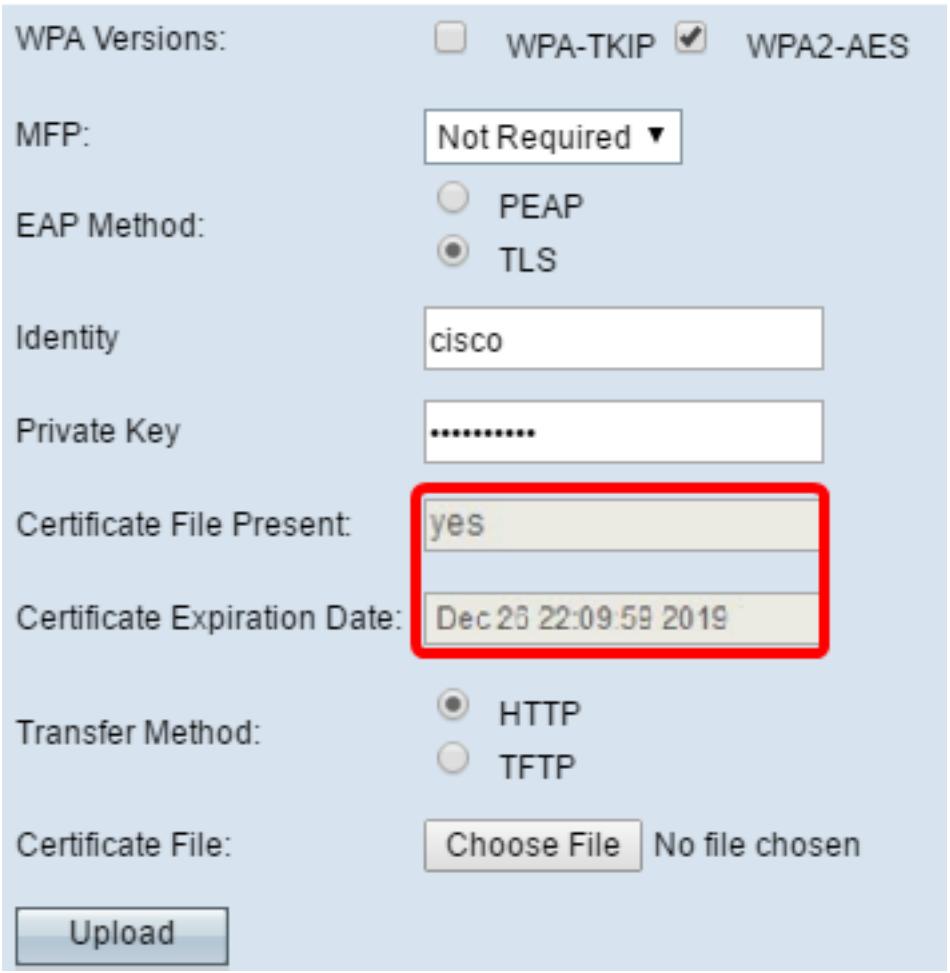
Note: Dans cet exemple, mini_httpd(2).pfx est sélectionné.



Étape 14. Cliquez sur **Upload** pour télécharger le fichier de certificat sélectionné. Passez à l'étape 18.



Les champs *Fichier de certificat présent* et *Date d'expiration du certificat* seront mis à jour automatiquement.



TFTP

Étape 15. Si vous avez cliqué sur TFTP à l'étape 12, entrez le nom de fichier du fichier de certificat dans le champ *Nom de fichier*.

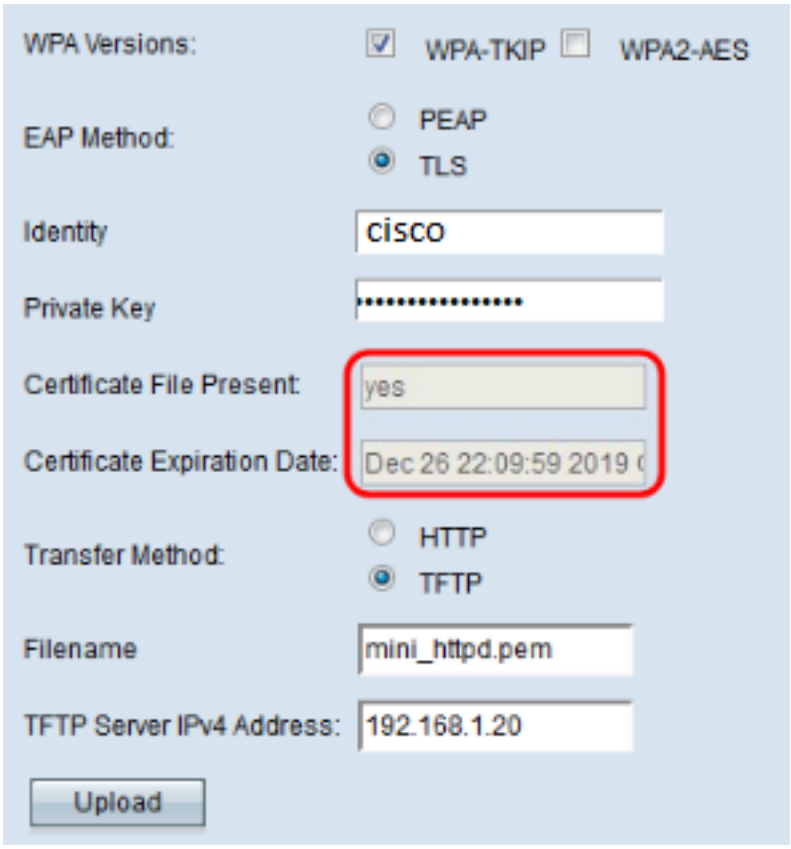
Note: Dans cet exemple, mini_httpd.pem est utilisé.

Étape 16. Entrez l'adresse du serveur TFTP dans le champ *TFTP Server IPv4 Address*.

Note: Dans cet exemple. 192.168.1.20 est utilisé comme adresse du serveur TFTP.

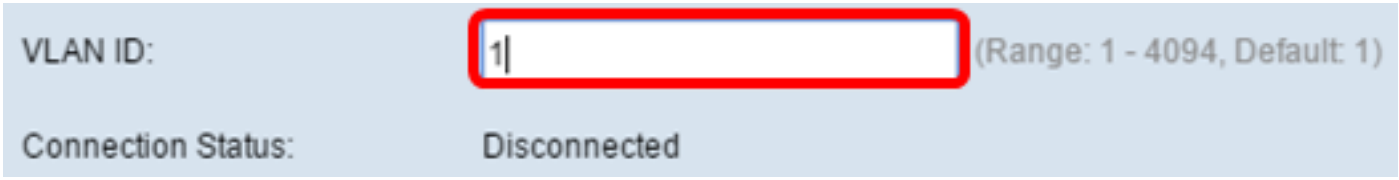
Étape 17. Cliquez sur le bouton **Upload** pour télécharger le fichier de certificat spécifié.

Les champs *Fichier de certificat présent* et *Date d'expiration du certificat* seront mis à jour automatiquement.



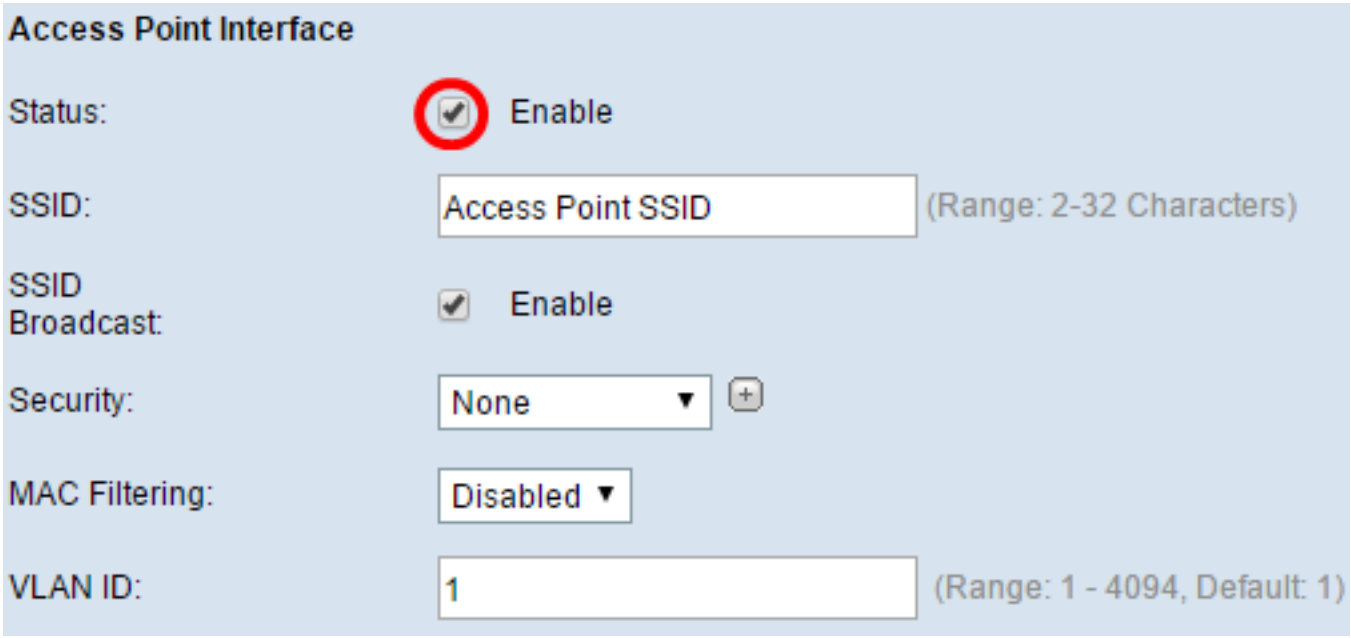
Étape 18. Saisissez l'ID de VLAN de l'interface client de l'infrastructure. 1 est établi par défaut.

Note: Dans cet exemple, l'ID de VLAN par défaut est utilisé.



Interface de point d'accès

Étape 1. Cochez la case **Activer** l'état pour activer le pontage sur l'interface du point d'accès.

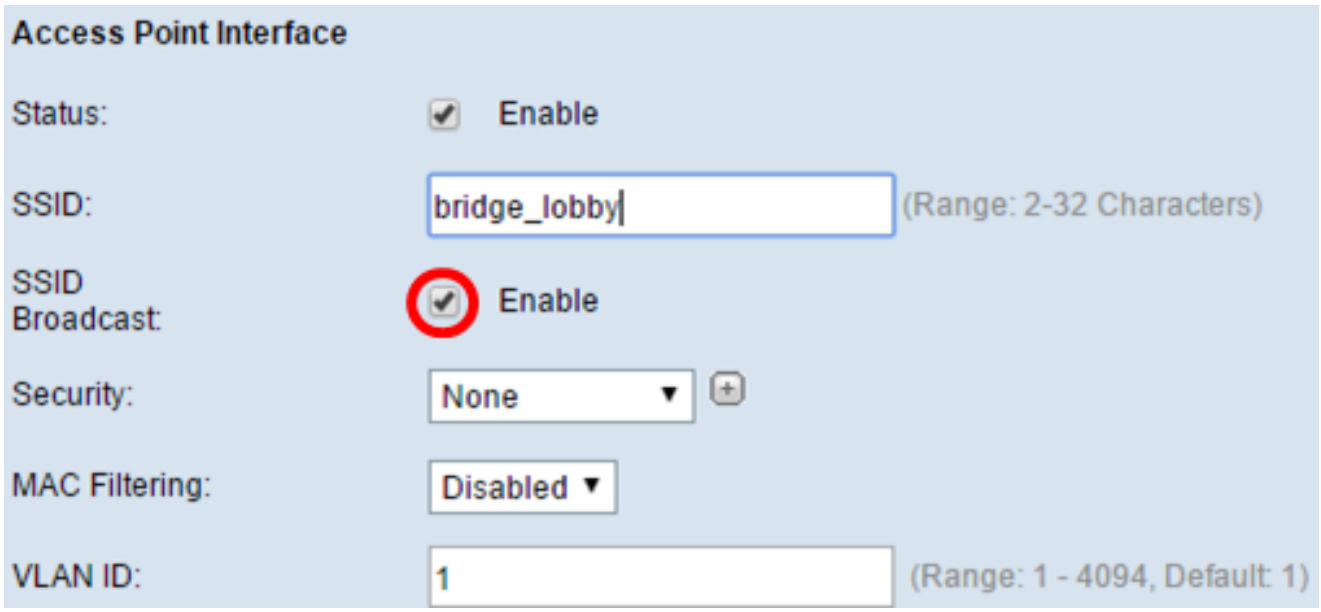


Étape 2. Entrez le SSID du point d'accès dans le champ *SSID*. La longueur du SSID doit

être comprise entre 2 et 32 caractères. La valeur par défaut est le SSID du point d'accès.

Note: Dans cet exemple, le SSID utilisé est bridge_hall.

Étape 3. (Facultatif) Si vous ne voulez pas diffuser le SSID, décochez la case **Activer la** diffusion SSID. Cela rendra le point d'accès invisible pour ceux qui recherchent des points d'accès sans fil ; elle ne peut être connectée qu'à une personne qui connaît déjà le SSID. La diffusion SSID est activée par défaut.

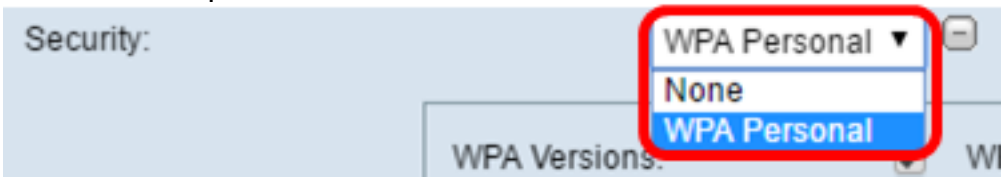


Étape 4. Sélectionnez le type de sécurité à utiliser pour authentifier les stations clientes en aval sur le WAP dans la liste déroulante Sécurité.

Les options disponibles sont définies comme suit :

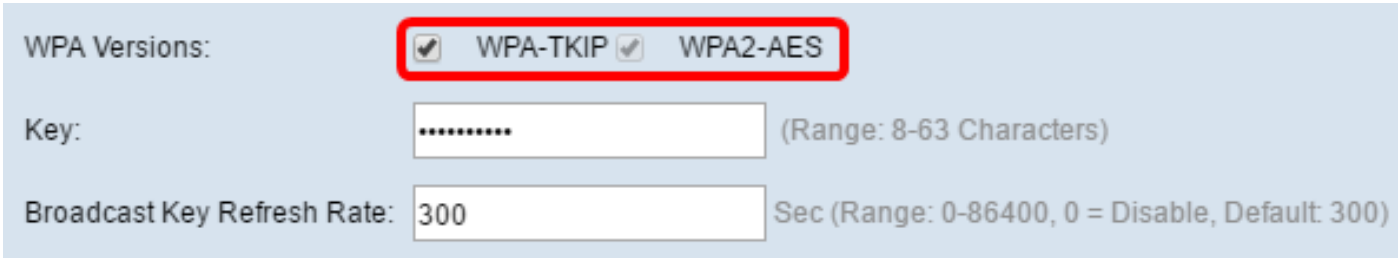
- Aucun — Ouvrir ou pas de sécurité. C'est la valeur par défaut. Passez à l'étape 10 si vous choisissez cette option.
- WPA Personal : WPA (Wi-Fi Protected Access) Personal peut prendre en charge des clés de 8 à 63 caractères. La méthode de chiffrement est TKIP ou Counter Cipher Mode avec le protocole CCMP (Block Chaining Message Authentication Code Protocol). WPA2 avec CCMP

est recommandé car il possède une norme de cryptage plus puissante, AES (Advanced Encryption Standard), par rapport au protocole TKIP (Temporal Key Integrity Protocol) qui utilise uniquement une norme RC4 64 bits.

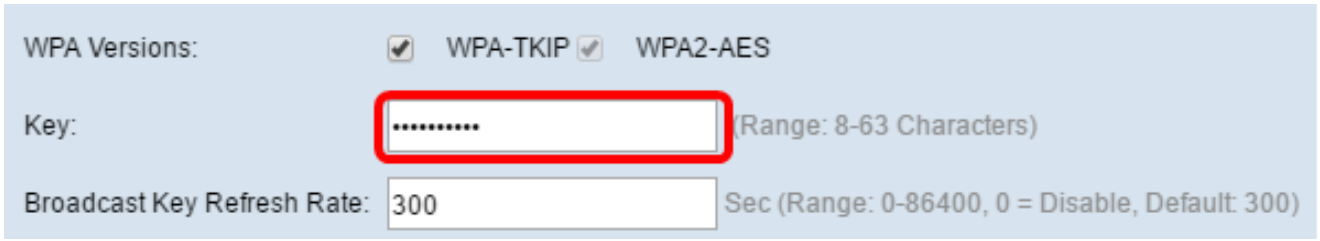


Étape 5. Cochez la case **WPA-TKIP** ou **WPA2-AES** pour déterminer le type de cryptage WPA que l'interface de point d'accès utilisera. Ils sont activés par défaut.

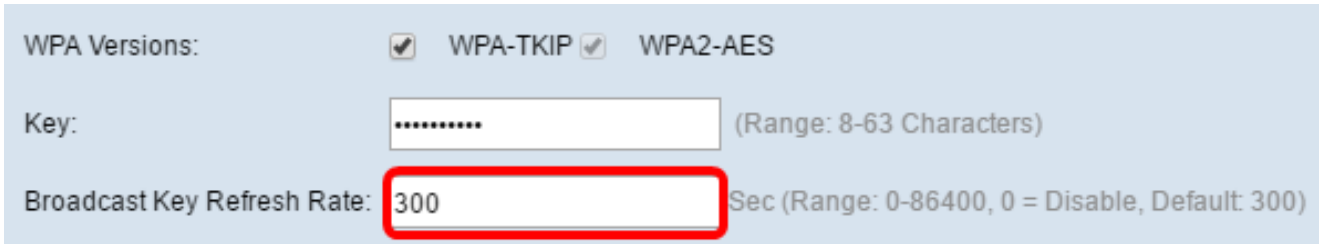
Note: Si tous vos équipements sans fil prennent en charge WPA2, définissez la sécurité du client d'infrastructure sur WPA2-AES. La méthode de cryptage est RC4 pour WPA et Advanced Encryption Standard (AES) pour WPA2. WPA2 est recommandé car il dispose d'une norme de cryptage plus puissante. Dans cet exemple, WPA2-AES est utilisé.



Étape 6. Entrez la clé WPA partagée dans le champ *Key*. La clé doit comporter entre 8 et 63 caractères et peut inclure des caractères alphanumériques, des majuscules et des minuscules ainsi que des caractères spéciaux.



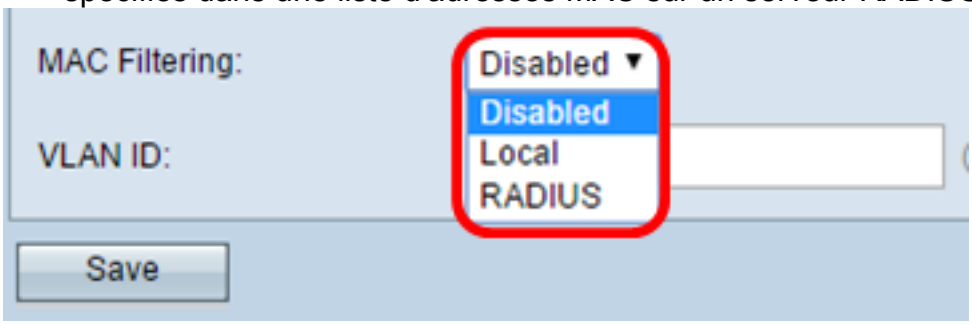
Étape 7. Entrez le taux dans le champ *Broadcast Key Refresh Rate*. La fréquence d'actualisation de la clé de diffusion spécifie l'intervalle auquel la clé de sécurité est actualisée pour les clients associés à ce point d'accès. Le taux doit être compris entre 0 et 86 400, la valeur 0 désactivant la fonction. Il est défini par défaut à 300.



Étape 8. Sélectionnez le type de filtrage MAC que vous souhaitez configurer pour l'interface de point d'accès dans la liste déroulante MAC Filtering. Lorsqu'elle est activée, l'accès au WAP est accordé ou refusé aux utilisateurs en fonction de l'adresse MAC du client qu'ils utilisent.

Les options disponibles sont définies comme suit :

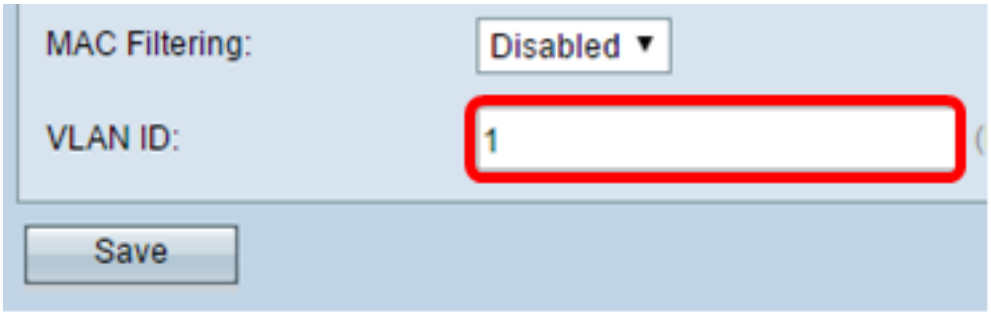
- Disabled : tous les clients peuvent accéder au réseau en amont. C'est la valeur par défaut.
- Local : l'ensemble de clients qui peuvent accéder au réseau en amont est limité aux clients spécifiés dans une liste d'adresses MAC définie localement.
- RADIUS : l'ensemble de clients pouvant accéder au réseau en amont est limité aux clients spécifiés dans une liste d'adresses MAC sur un serveur RADIUS.



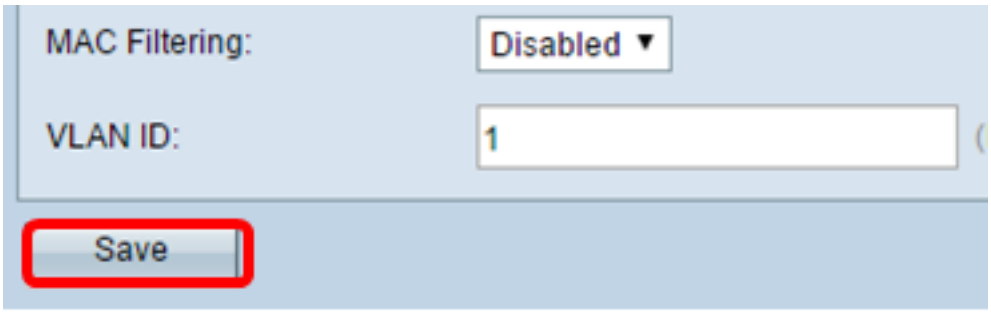
Note: Dans cet exemple, Désactivé est sélectionné.

Étape 9. Entrez l'ID de VLAN dans le champ *ID de VLAN* de l'interface de point d'accès.

Remarque : pour permettre le pontage des paquets, la configuration VLAN de l'interface de point d'accès et de l'interface filaire doit correspondre à celle de l'interface client de l'infrastructure.



Étape 10. Cliquez sur **Enregistrer** pour enregistrer vos modifications.



Vous devez maintenant avoir correctement configuré un pont de groupe de travail sur un point d'accès sans fil.