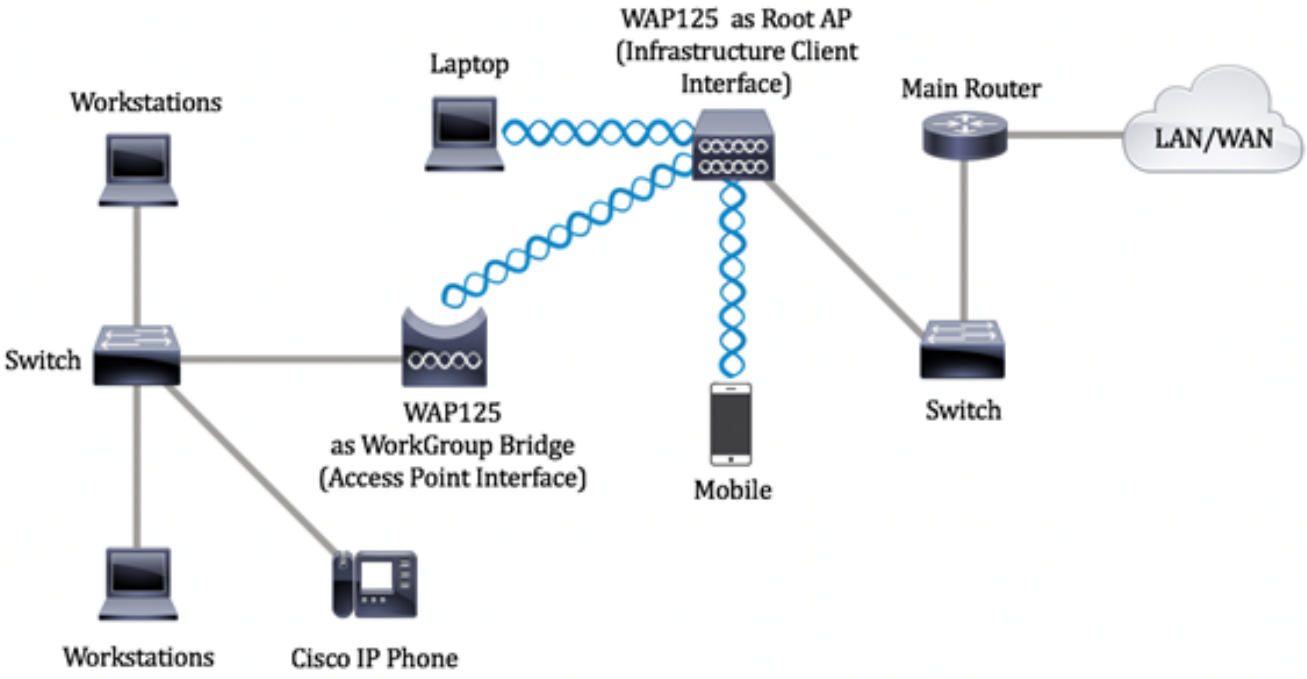
Configurez les configurations de pont de groupe de travail sur les Points d'accès WAP125 ou WAP581

Objectif

La caractéristique de pont de groupe de travail permet au point d'accès sans fil (WAP) de jeter un pont sur le trafic entre un client distant et le réseau local sans fil (RÉSEAU LOCAL) qui est connecté au mode de pont de groupe de travail. Le périphérique WAP associé avec l'interface distante est connu comme interface de Point d'accès, alors que le périphérique WAP associé avec le RÉSEAU LOCAL Sans fil est connu comme interface d'infrastructure. Le pont de groupe de travail permet les périphériques qui font seulement se connecter des connexions câblées à un réseau Sans fil. Le mode de pont de groupe de travail est recommandé comme alternative quand la caractéristique du Wireless Distribution System (WDS) est indisponible.

La topologie ci-dessous illustre un modèle de pont de groupe de travail témoin. Des périphériques de câble sont attachés à un commutateur, qui se connecte à l'interface de RÉSEAU LOCAL du WAP. Dans l'exemple ci-dessous, le WAP125 agit en tant qu'interface de Point d'accès qui se connecte à l'interface client d'infrastructure.



Cet article prévoit des instructions sur la façon dont configurer des configurations de pont de groupe de travail entre deux points d'accès sans fil.

Périphériques applicables

- WAP125
- WAP581

Version de logiciel

- 1.0.0.4 — WAP581
- 1.0.0.5 — WAP125

Configurez les configurations de pont de groupe de travail

Avant que vous configuriez la passerelle de groupe de travail sur le périphérique WAP, notez ces instructions :

- Tous les périphériques WAP participant au pont de groupe de travail doivent avoir les configurations identiques suivantes :

- Radio

- Mode d'IEEE 802.11

- Bande passante de la Manche

- La Manche (l'automatique n'est pas recommandé)

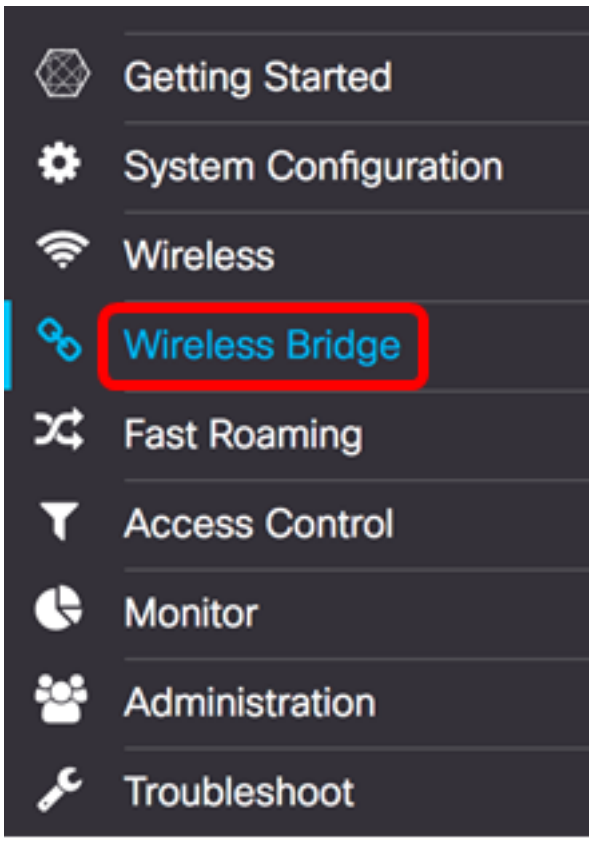
Remarque: Pour apprendre comment configurer ces configurations sur WAP125, a cliquez ici pour des instructions. Pour WAP581, a cliquez ici.

- Le mode de pont de groupe de travail prend en charge actuellement seulement le trafic d'ipv4.
- Le mode de pont de groupe de travail n'est pas pris en charge à travers une installation unique. Si vous avez les Points d'accès WAP581, désactivez le SPS ou le groupement d'abord avant de configurer les configurations de pont de groupe de travail. Pour des instructions sur la façon dont configurer les configurations SPS sur votre WAP, a cliquez ici.

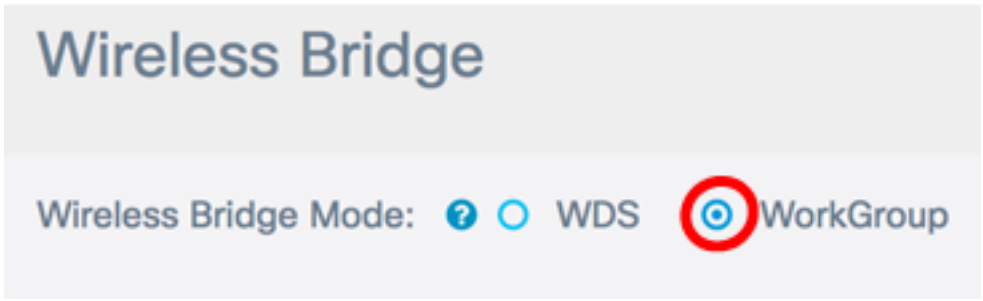
Configurez l'interface client d'infrastructure

Étape 1. La procédure de connexion à l'utilitaire basé sur le WEB du WAP choisissent alors le **pont sans fil**.

Remarque: Les options disponibles peuvent varier selon le modèle exact de votre périphérique. Dans cet exemple, WAP125 est utilisé.



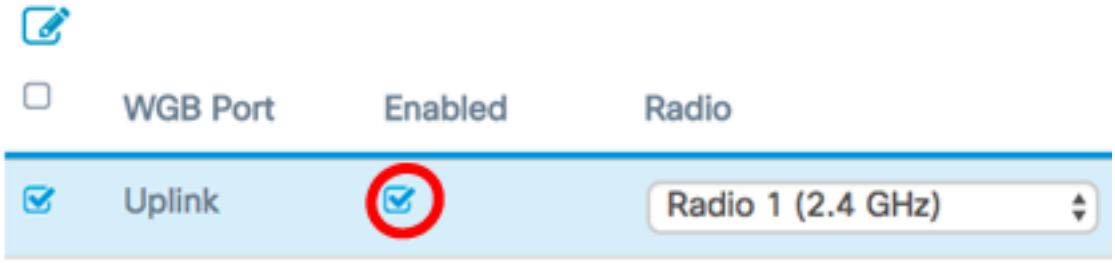
Étape 2. Cliquez sur la case d'option de **groupe de travail**.



Étape 3. Cochez la case de **liaison ascendante**.

Étape 4. Cliquez sur l'icône d'**éditer**.

Étape 5. Cochez la case **activée** pour activer l'interface client d'infrastructure.



Étape 6. Choisissez l'interface par radio pour le pont de groupe de travail. Quand vous configurez une radio comme pont de groupe de travail, l'autre radio reste opérationnelle. Les interfaces par radio correspondent aux bandes de fréquence du WAP. Le WAP est équipé pour annoncer sur deux interfaces par radio différentes. Configurer des configurations pour une interface par radio n'affectera pas l'autre.

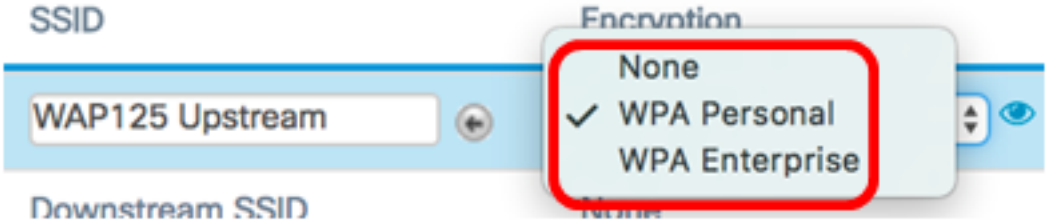
Remarque: Dans cet exemple, la radio 2 (5 gigahertz) est choisie.

Étape 7. Écrivez le nom d'Identifiant SSID (Service Set Identifier) dans le *champ SSID*. Ceci sert de connexion entre le périphérique et le client distant. Vous pouvez écrire 2 à 32 caractères pour le client SSID d'infrastructure.

Remarque: Dans cet exemple, l'en amont WAP125 est utilisé.

Remarque: La flèche à côté du SSID est disponible pour la lecture SSID. Cette caractéristique est désactivée par défaut, et est activée seulement si la détection AP est activée dans la détection escroc AP, qui est également désactivée par défaut.

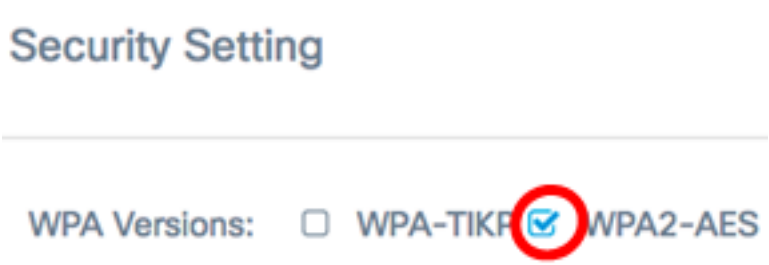
Étape 8. Choisissez le type de Sécurité pour authentifier comme station client sur le périphérique de l'en amont WAP de la liste déroulante de cryptage. Les options sont :



- Aucun — Ouvrez-vous ou aucune Sécurité. Il s'agit de la configuration par défaut. Si ceci est choisi, ignorez à l'étape 22.
- WPA personnel — Le WPA personnel peut prendre en charge des clés des caractères de la longueur 8-63. Le WPA2 est recommandé car il a une norme de chiffrement plus puissante.
- WPA Enterprise — Le WPA Enterprise est plus avancé que le WPA personnel et est la Sécurité recommandée pour l'authentification. Il utilise le Protected Extensible Authentication Protocol (PEAP) et le Transport Layer Security (TLS). Saut à l'étape 12 à configurer. Ce type de Sécurité est employé souvent dans un environnement de bureau et a besoin d'un serveur de Service RADIUS (Remote Authentication Dial-In User Service) configuré. A cliquez ici pour connaître plus des serveurs de RADIUS.

Remarque: Dans cet exemple, le WPA personnel est choisi.

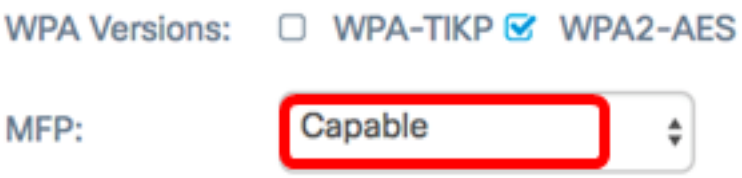
Étape 9. Cliquez sur l'icône et cochez la case WPA-TKIP ou WPA2-AES pour déterminer quel genre de chiffrement WPA l'interface client d'infrastructure utilisera.



Remarque: Si tout votre support d'équipement sans fil WPA2, plaçait la Sécurité de client d'infrastructure à WPA2-AES. La méthode de cryptage est RC4 pour le WPA et le Norme AES (Advanced Encryption Standard) pour le WPA2. Le WPA2 est recommandé car il a une norme de chiffrement plus puissante. Dans cet exemple, WPA2-AES est utilisé.

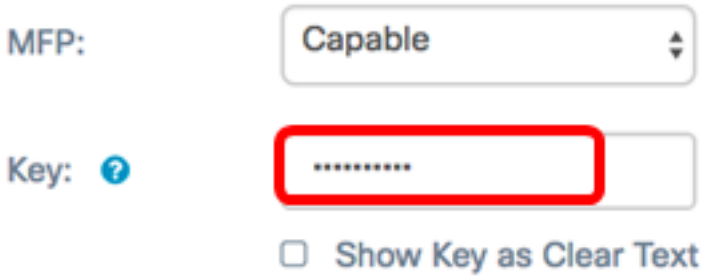
Étape 10. (facultative) si vous vérifiiez WPA2-AES dans l'étape 9, choisissent une option de la liste déroulante du Management Frame Protection (MFP), que vous vouliez que le WAP exige d'avoir les trames protégées ou pas. Pour se renseigner plus sur MFP, a cliquez ici. Les options sont :

- Non requis — Désactive le soutien de client de MFP.
- Capable — Permet MFP-capables et les clients qui ne prennent en charge pas MFP pour joindre le réseau. C'est la configuration du par défaut MFP sur le WAP.
- Requis — On permet à des des clients pour s'associer seulement si MFP est négocié. Si les périphériques ne prennent en charge pas MFP, on ne leur permet pas pour joindre le réseau.



Remarque: Dans cet exemple, capable est choisi.

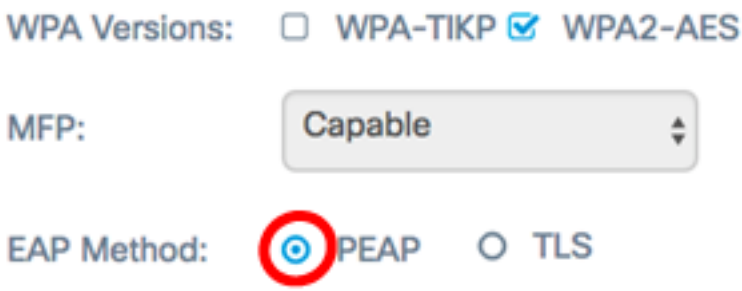
Étape 11. Introduisez la clé de chiffrement WPA dans la zone de tri. La clé doit être 8-63 caractères longs. C'est une combinaison des lettres, des nombres, et des caractères particuliers. C'est le mot de passe qui est utilisé en se connectant au réseau Sans fil pour la première fois. Puis, saut à l'étape 21.



Étape 12. Si vous choisissiez le WPA Enterprise dans l'étape 8, cliquez sur une case d'option pour la méthode d'EAP.

Les options disponibles sont définies comme suit :

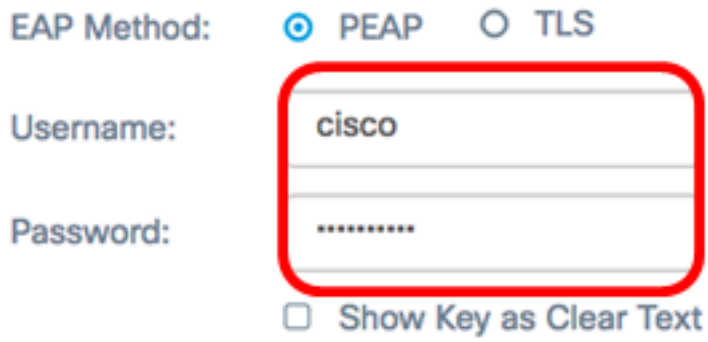
- PEAP — Ce protocole donne chaque utilisateur de sans fil sous les différents noms d'utilisateur et mot de passe WAP qui prennent en charge des normes de chiffrement AES. Puisque le PEAP est une méthode de Sécurité basée par mot de passe, votre sécurité wifi est basée sur les qualifications de périphérique du client. Le PEAP peut poser potentiellement un risque de sécurité élevé si vous avez des mots de passe faible ou des clients sans garantie. Il se fonde sur le TLS mais évite l'installation des Certificats numériques sur chaque client. Au lieu de cela, il fournit l'authentification par un nom d'utilisateur et mot de passe.
- TLS — Le TLS exige de chaque utilisateur d'avoir un certificat supplémentaire pour accorder l'accès. Le TLS est plus sécurisés si vous avez les serveurs supplémentaires et l'infrastructure nécessaire pour authentifier des utilisateurs dans votre réseau. Si vous choisissez cette option, ignorez à l'étape 14.



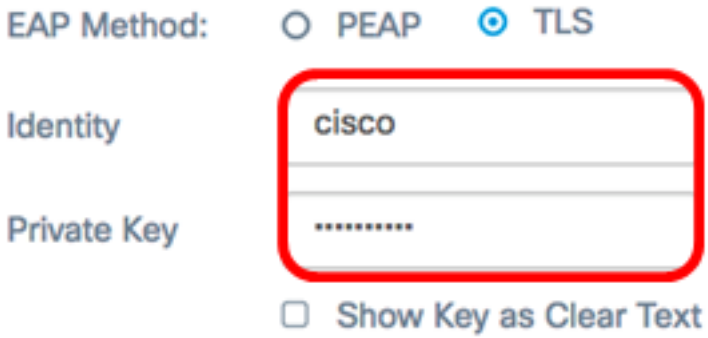
Remarque: Pour cet exemple, le PEAP est choisi.

Étape 13. Écrivez le nom d'utilisateur et mot de passe pour le client d'infrastructure dans les domaines de nom d'utilisateur et mot de passe. C'est l'information de connexion qui est utilisée pour se connecter à l'interface client d'infrastructure ; référez-vous à votre interface

client d'infrastructure pour trouver ces informations. Puis, saut à l'étape 21.

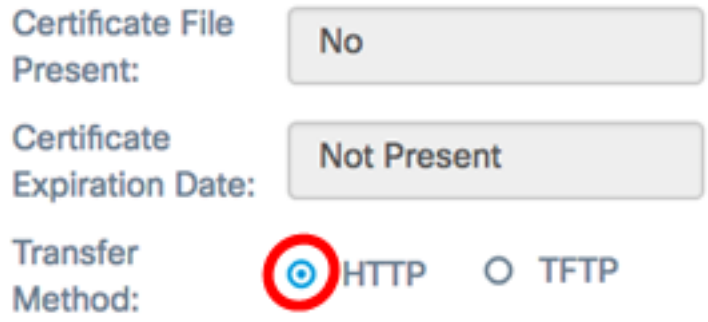


Étape 14. Si vous cliquiez sur le TLS dans l'étape 12, introduisez l'identité et la clé privée du client d'infrastructure dans l'identité et les zones de tri privées.



Étape 15. Dans la zone de méthode de transfert, cliquez sur une case d'option des options suivantes :

- TFTP — Le Protocole TFTP (Trivial File Transfer Protocol) est une version sans garantie simplifiée de Protocole FTP (File Transfer Protocol). Il est principalement utilisé pour distribuer le logiciel ou pour authentifier des périphériques parmi des réseaux d'entreprise. Si vous cliquiez sur le TFTP, ignorez à l'étape 18.
- HTTP — Le Protocole HTTP (Hypertext Transfer Protocol) fournit un cadre simple d'authentification de défi-réponse qui peut être utilisé par un client pour fournir le cadre d'authentification.



Remarque: Si un fichier du certificat est déjà présent sur le WAP, les gisements de date d'expiration de présent de fichier du certificat et de certificat déjà seront complétés d'informations pertinentes. Autrement, ils seront vides.

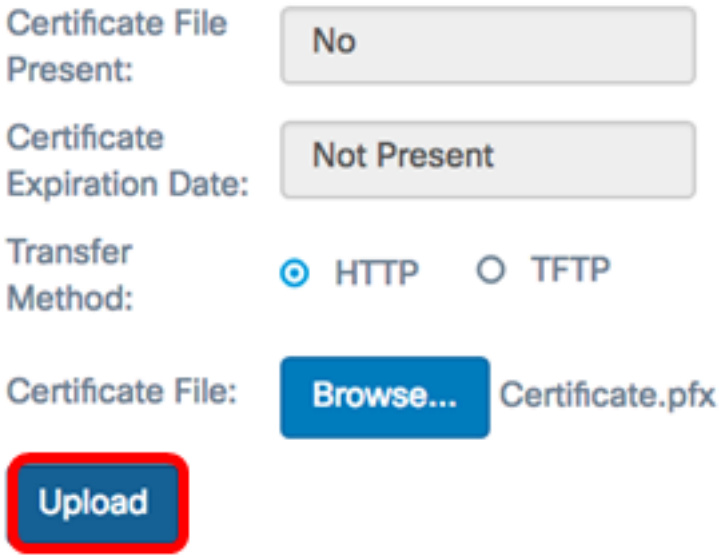
HTTP

Étape 16. Cliquez sur le **bouton Parcourir** pour trouver et sélectionner un fichier du certificat.

Le fichier doit avoir l'extension de fichier du certificat appropriée (telle que .pem ou .pfx) autrement, le fichier ne sera pas reçu.

Remarque: Dans cet exemple, Certificate.pfx est choisi.

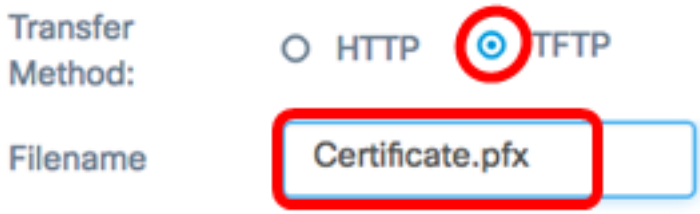
Étape 17. Cliquez sur Upload pour télécharger le fichier du certificat sélectionné. Saut à l' étape 21.



Les gisements de date d'expiration de présent et de certificat de fichier du certificat seront mis à jour automatiquement.

TFTP

Étape 18. (Facultatif) si vous cliquiez sur le TFTP dans l'étape 15, écrivez le nom du fichier du fichier du certificat dans le *champ Filename*.



Remarque: Dans cet exemple, Certificate.pfx est utilisé.

Étape 19. Introduisez l'adresse du serveur TFTP dans le domaine d'*ipv4 addres de serveur TFTP*.

Remarque: Dans cet exemple. 192.168.100.108 est utilisé comme adresse du serveur TFTP.

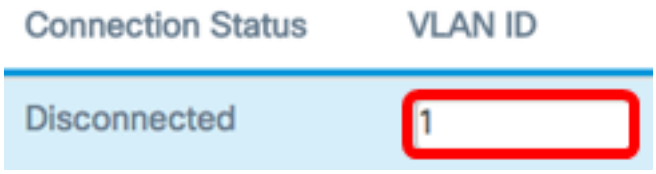
Étape 20. Cliquez sur le bouton de **téléchargement** pour télécharger le fichier du certificat spécifié.

Les gisements de date d'expiration de présent et de certificat de fichier du certificat seront mis à jour automatiquement.

Étape 21. Cliquez sur OK pour fermer la fenêtre Configuration de la sécurité.

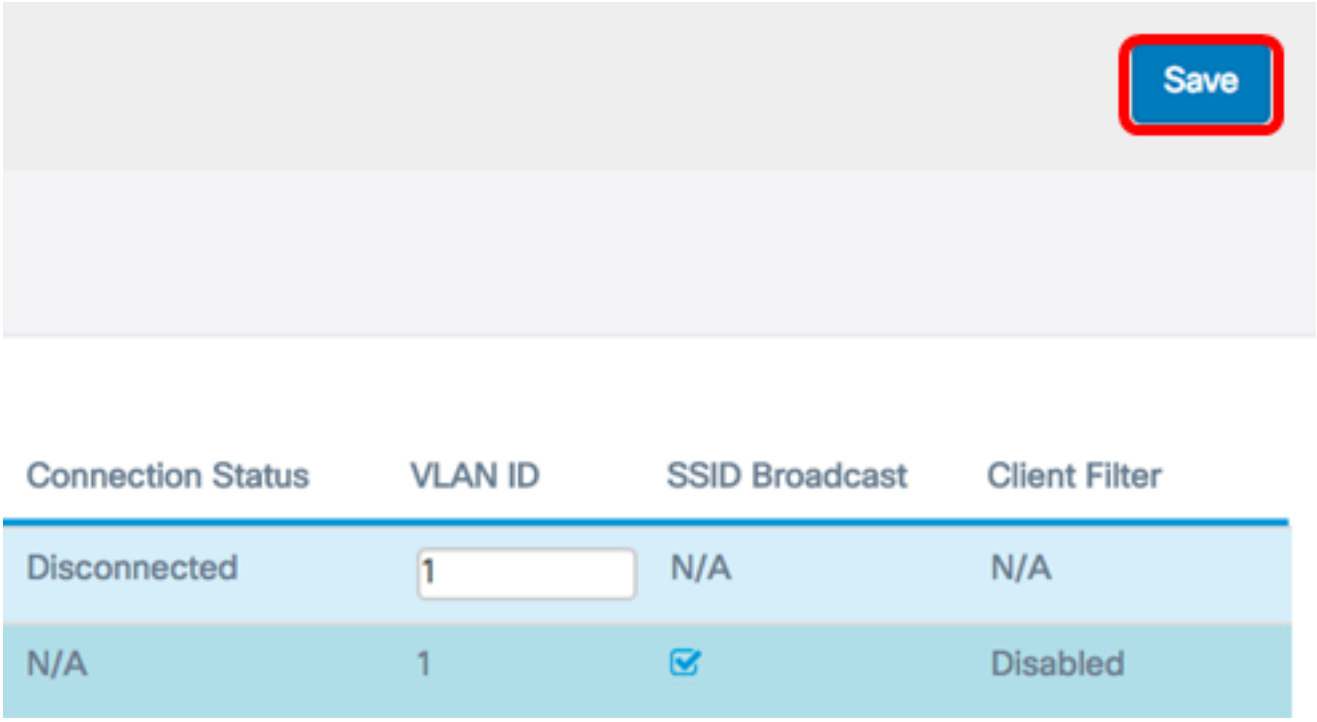
La région d'état de la connexion indique si le WAP est connecté au périphérique de l'en amont WAP.

Étape 22. Écrivez l'ID DE VLAN pour l'interface client d'infrastructure. 1 est établi par défaut.



Remarque: Pour cet exemple, l'ID DE VLAN par défaut est utilisé.

Étape 23. **Sauvegarde de** clic pour sauvegarder les configurations configurées.

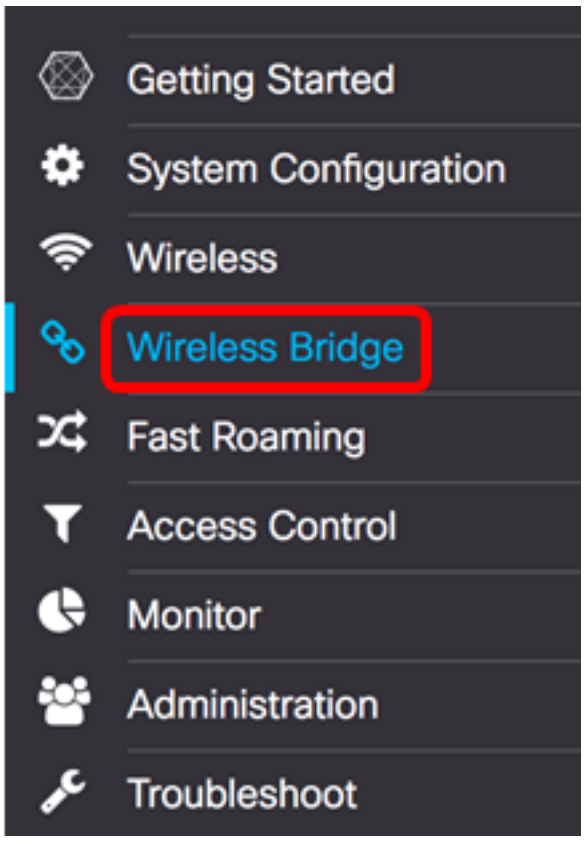


Vous devriez avoir maintenant avec succès configuré les configurations d'interface client d'infrastructure sur votre WAP.

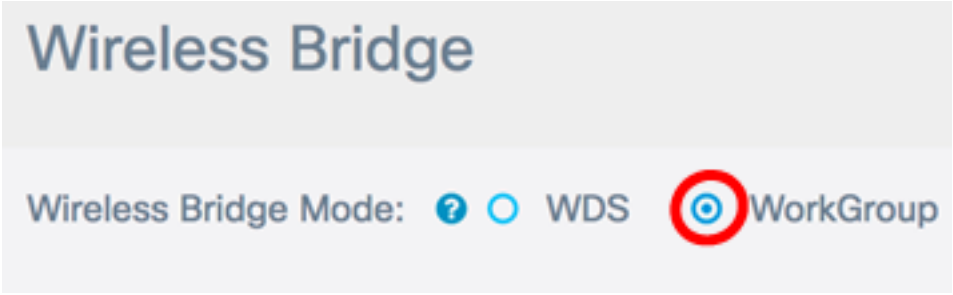
Configurez l'interface client de Point d'accès

Étape 1. La procédure de connexion à l'utilitaire basé sur le WEB du WAP choisissent alors le **pont sans fil**.

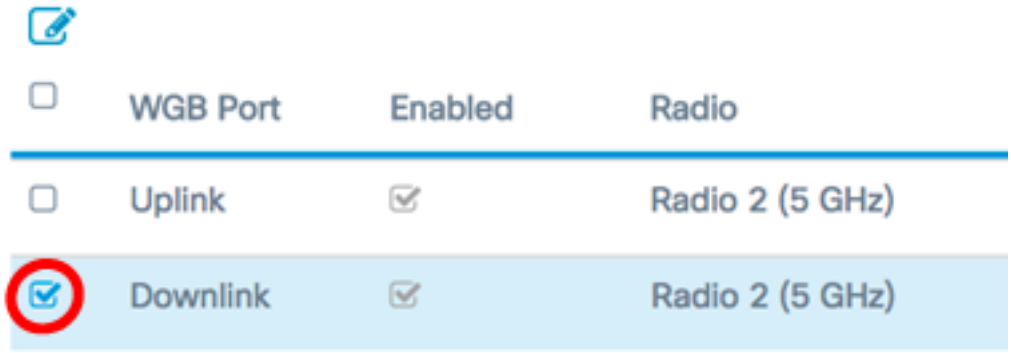
Remarque: Les options disponibles peuvent varier selon le modèle exact de votre périphérique. Dans cet exemple, WAP125 est utilisé.



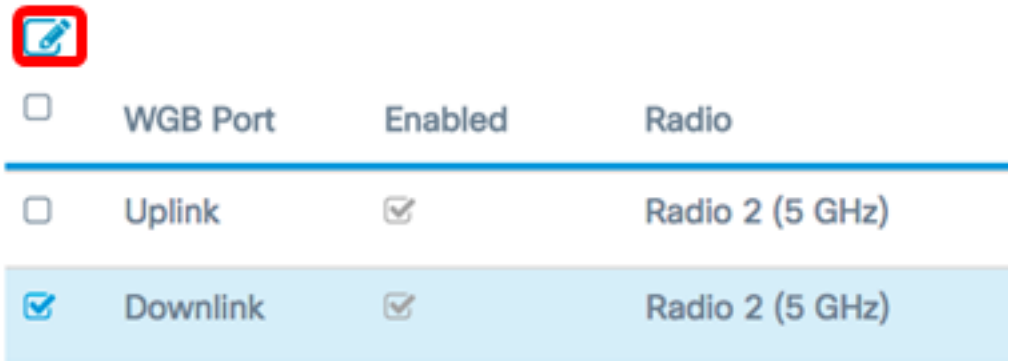
Étape 2. Cliquez sur la case d'option de **groupe de travail**.



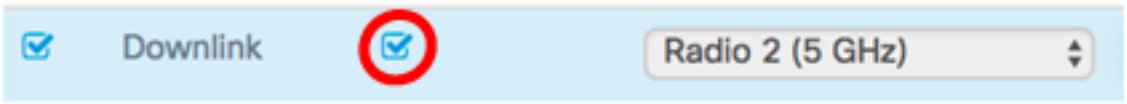
Étape 3. Cochez la case de **liaison descendante**.



Étape 4. Cliquez sur le bouton d'**éditer**.



Étape 5. Cochez la case **activée** pour activer la transition sur l'interface de Point d'accès.



Étape 6. Écrivez le SSID pour le Point d'accès dans le *champ SSID*. La longueur SSID doit être entre 2 à 32 caractères. Le par défaut est l'en aval SSID.

Remarque: Pour cet exemple, le SSID utilisé est l'en aval WAP125.

Étape 7. Choisissez le type de Sécurité pour authentifier les stations client en aval au WAP de la liste déroulante de Sécurité.

Les options disponibles sont définies comme suit :

- Aucun — Ouvrez-vous ou aucune Sécurité. C'est la valeur par défaut. Ignorez à l'étape 13 si vous choisissez cette option.
- WPA personnel — Le Protocole WPA (Wi-Fi Protected Access) personnel peut prendre en charge des clés de 8 à 63 caractères longs. La méthode de cryptage est TKIP ou mode de chiffrement de compteur avec le code Protocol (CCMP) d'authentification de message d'enchaînement de bloc. Le WPA2 avec CCMP est recommandé car il a une norme de chiffrement plus puissante, Norme AES (Advanced Encryption Standard), comparé au Protocole TKIP (Temporal Key Integrity Protocol) qui utilise seulement une norme RC4 64-bit.

Contrôle (facultatif) d'étape 8. la case WPA-TKIP pour déterminer le cryptage WPA-TKIP que l'interface de Point d'accès l'utilisera. Ceci est activé par défaut.

Remarque: WPA-AES est grisé et ne peut pas être désactivé. Dans cet exemple, WPA-TKIP est décoché.

Étape 9. Introduisez la clé WPA partagée dans la zone de tri. La clé doit être 8-63 caractères longs et peut inclure des caractères alphanumériques, des majuscules et minuscules, et des caractères particuliers.

Étape 10. Écrivez le débit dans le domaine de fréquence d'actualisation principale d'émission. La fréquence d'actualisation de clé d'émission spécifie l'intervalle auquel la clé de Sécurité est régénérée pour des clients associés à ce Point d'accès. Le débit doit être entre 0-86400, avec une valeur de 0 désactivant la caractéristique.

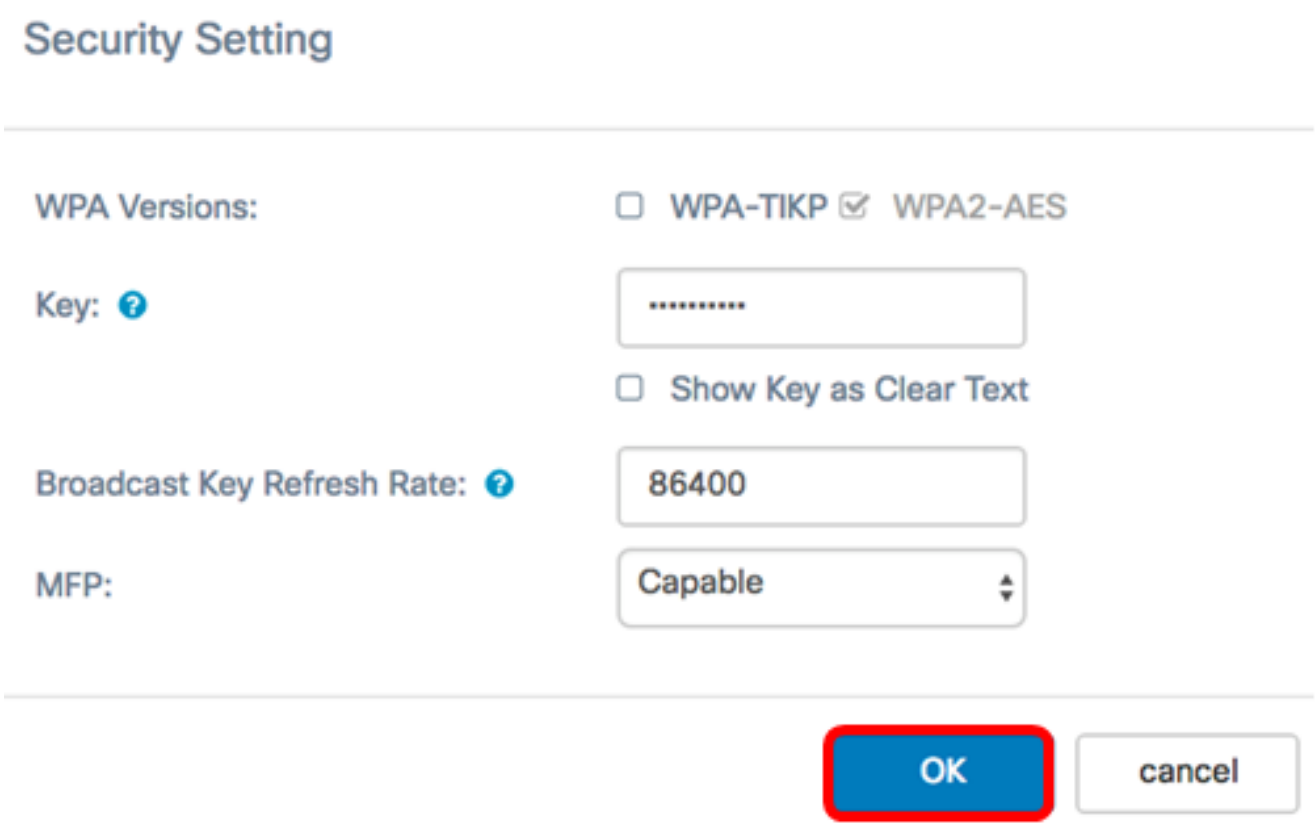
Remarque: Dans cet exemple, 86400 est utilisés.

Étape 11. Choisissez une option de la liste déroulante MFP, que vous vouliez que le WAP exige d'avoir les trames protégées ou pas. Pour se renseigner plus sur MFP, a cliquez ici. Les options sont :

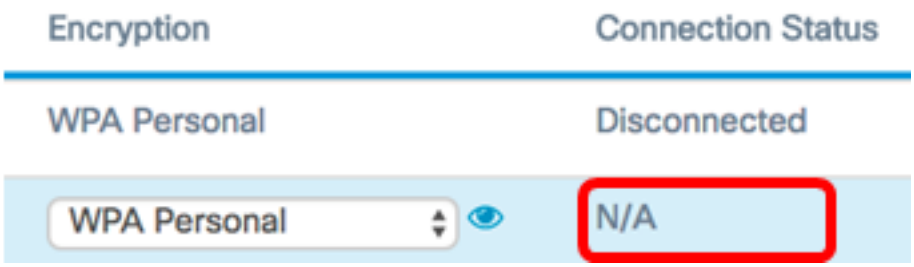
- Non requis — Désactive le soutien de client de MFP.
- Capable — Permet MFP-capables et les clients qui ne prennent en charge pas MFP pour joindre le réseau. C'est la configuration du par défaut MFP sur le WAP.
- Requis — On permet à des des clients pour s'associer seulement si MFP est négocié. Si les périphériques ne prennent en charge pas MFP, on ne leur permet pas pour joindre le réseau.

Remarque: Pour cet exemple, capable est choisi.

Étape 12. Cliquez sur OK pour sauvegarder les paramètres de sécurité.



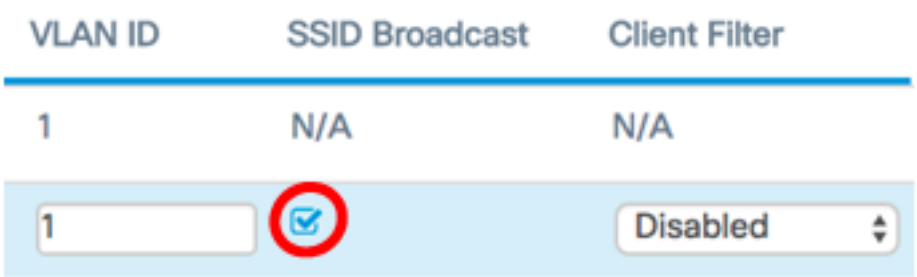
La région d'état de la connexion indique le pas applicable ou le NON APPLICABLE.



Étape 13. Écrivez l'ID DE VLAN dans le domaine d'ID DE VLAN pour l'interface de Point d'accès.

Remarque: Pour permettre la transition des paquets, la configuration VLAN pour l'interface de Point d'accès et l'interface de câble devrait apparier cela de l'interface client d'infrastructure.

Étape 14. Cochez la case de diffusion SSID si vous voulez que l'en aval SSID soit émission. La diffusion SSID est activée par défaut.



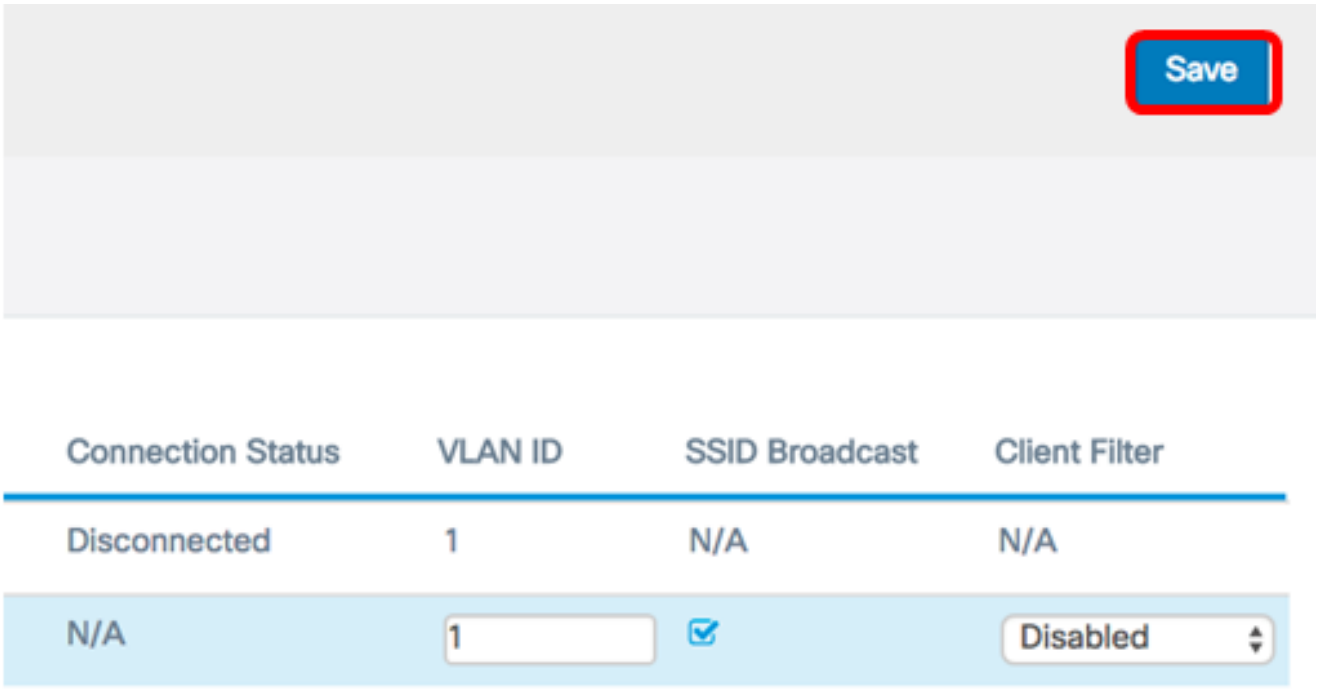
Étape 15. Choisissez le type de filtrage MAC que vous souhaitez configurer pour l'interface de Point d'accès de la liste déroulante de filtrage MAC. Une fois activés, on accorde des utilisateurs ou l'accès refusé au WAP sont basés sur l'adresse MAC du client qu'ils les utilisent.

Les options disponibles sont définies comme suit :

- Handicapé — Tous les clients peuvent accéder au réseau en amont. C'est la valeur par défaut.
- Gens du pays — L'ensemble de clients qui peuvent accéder au réseau en amont est limité aux clients spécifiés dans une liste localement définie d'adresse MAC.
- RADIUS — L'ensemble de clients qui peuvent accéder au réseau en amont est limité aux clients spécifiés dans une liste d'adresse MAC sur un serveur de RADIUS.

Remarque: Dans cet exemple, le handicapé est choisi.

Étape 16. **Sauvegarde de** clic pour sauvegarder vos modifications.



Vous devriez avoir maintenant avec succès configuré les configurations de pont de groupe de travail sur vos points d'accès sans fil.