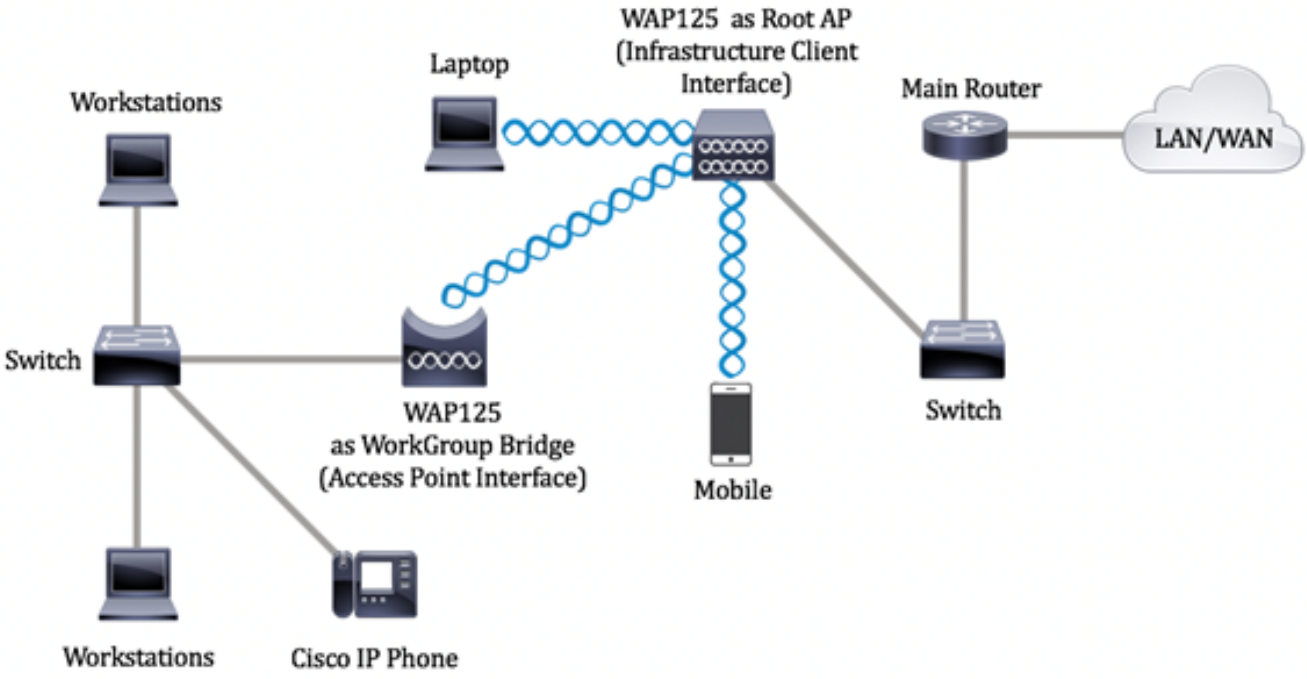
Configurer les paramètres du pont de groupe de travail sur les points d'accès WAP125 ou WAP581

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.

La topologie ci-dessous illustre un exemple de modèle WorkGroup Bridge. Les périphériques filaires sont raccordés à un commutateur, qui se connecte à l'interface LAN du WAP. Dans l'exemple ci-dessous, le WAP125 agit comme une interface de point d'accès qui se connecte à l'interface client de l'infrastructure.



Cet article explique comment configurer les paramètres du pont de groupe de travail entre deux points d'accès sans fil.

Périphériques pertinents

- WAP125
- WAP581

Version du logiciel

- 1.0.0.4 - WAP581
- 1.0.0.5 - WAP125

Configurer les paramètres du pont du groupe de travail

Avant de configurer le pont de groupe de travail sur le périphérique WAP, prenez note des consignes suivantes :

- Tous les périphériques WAP participant au pont WorkGroup doivent avoir les paramètres identiques suivants :

- Radio

- Mode IEEE 802.11

- Bande passante du canal

- Canal (Auto n'est pas recommandé)

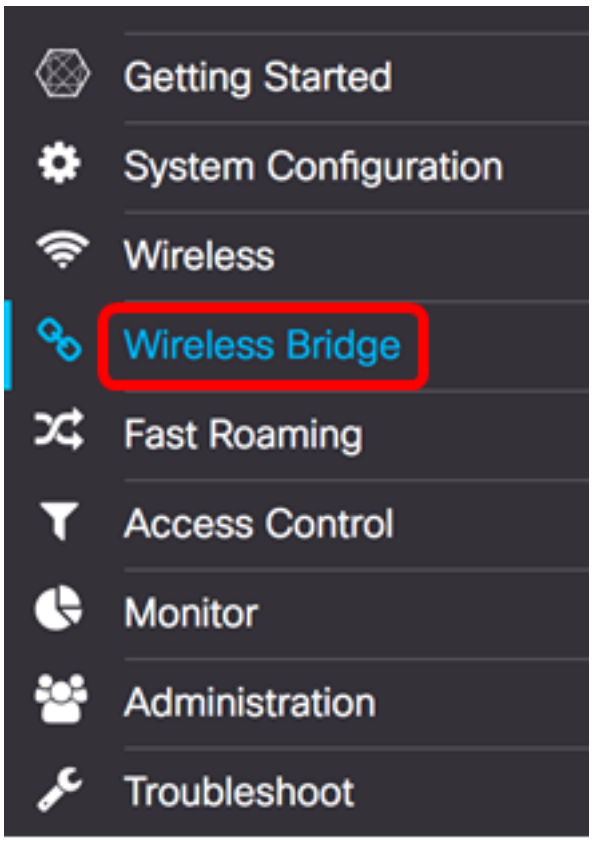
Note: Pour savoir comment configurer ces paramètres sur WAP125, cliquez ici pour obtenir des instructions. Pour WAP581, cliquez ici.

- Le mode WorkGroup Bridge prend actuellement en charge uniquement le trafic IPv4.
- Le mode Pont de groupe de travail n'est pas pris en charge dans une configuration par point unique. Si vous avez des points d'accès WAP581, désactivez d'abord SPS ou le clustering avant de configurer les paramètres du pont de groupe de travail. Pour savoir comment configurer les paramètres SPS sur votre WAP, cliquez ici.

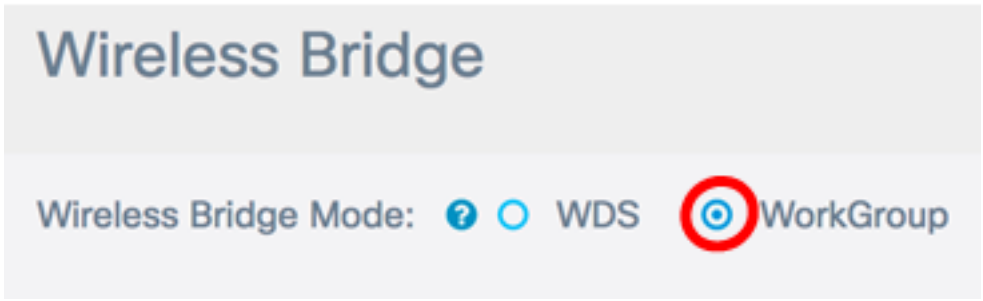
Configurer l'interface client de l'infrastructure

Étape 1. Connectez-vous à l'utilitaire Web du WAP, puis sélectionnez **Wireless Bridge**.

Note: Les options disponibles peuvent varier en fonction du modèle exact de votre périphérique. Dans cet exemple, WAP125 est utilisé.



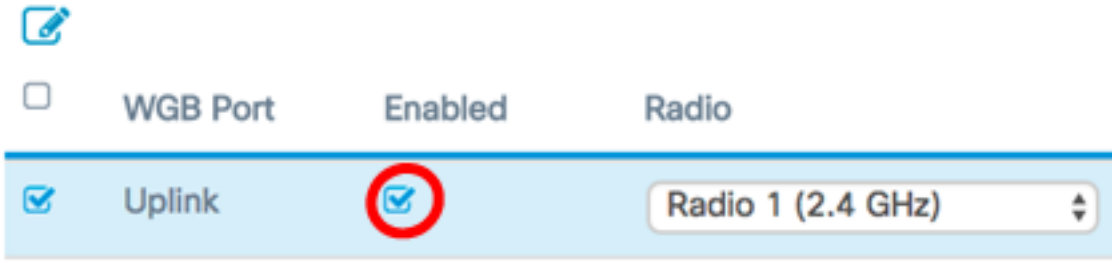
Étape 2. Cliquez sur la case d'option **Groupe de travail**.



Étape 3. Cochez la case **Uplink**.

Étape 4. Cliquez sur l'icône **Modifier**.

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



Étape 6. Sélectionnez 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.

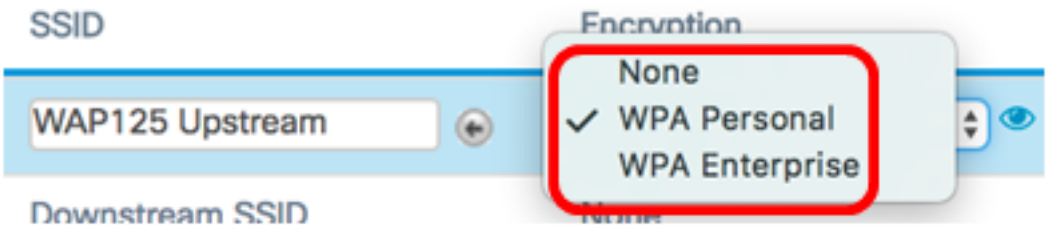
Note: Dans cet exemple, Radio 2 (5 GHz) est sélectionné.

Étape 7. Entrez le nom SSID (Service Set Identifier) dans le champ *SSID*. 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: Dans cet exemple, WAP125 Upstream est utilisé.

Note: La flèche en regard de SSID est disponible pour l'analyse SSID. Cette fonctionnalité est désactivée par défaut et n'est activée que si la détection des points d'accès est activée dans la détection des points d'accès indésirables, qui est également désactivée par défaut.

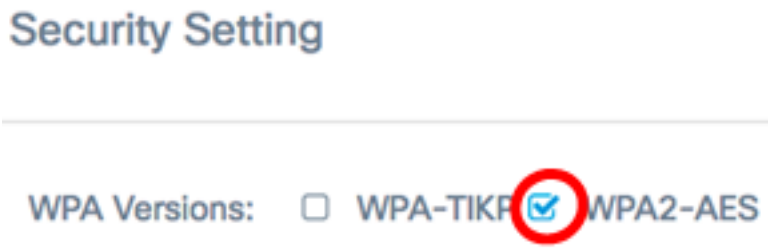
Étape 8. Sélectionnez le type de sécurité à authentifier en tant que station client sur le périphérique WAP en amont dans la liste déroulante Cryptage. Les options sont les suivantes :



- Aucun — Ouvrir ou pas de sécurité. Il s'agit de la configuration par défaut. Si cette option est sélectionnée, passez à l'étape 22.
- 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.
- 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 12 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.

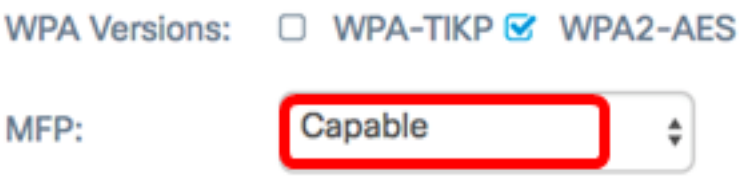
Étape 9. Cliquez sur l' icône et cochez la case WPA-TKIP ou WPA2-AES pour déterminer le type de cryptage WPA que l'interface client d'infrastructure utilisera.



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.

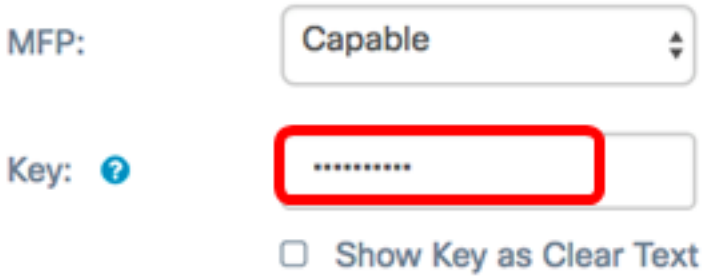
Étape 10. (Facultatif) Si vous avez coché WPA2-AES à l'étape 9, choisissez une option dans la liste déroulante Management Frame Protection (MFP), que vous souhaitiez que le WAP exige ou non des trames protégées. Pour en savoir plus sur la MFP, cliquez ici. Les options sont les suivantes :

- 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.

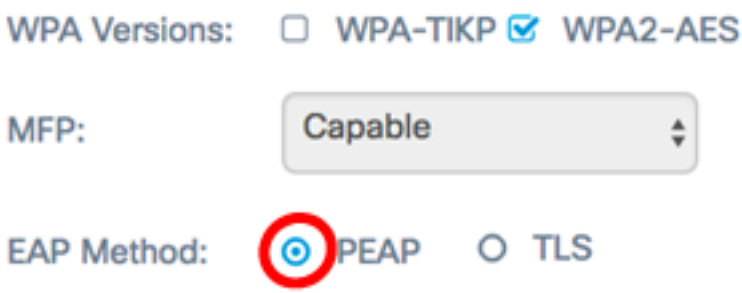
Étape 11. Entrez la clé de chiffrement WPA dans le champ *Key*. La clé doit comporter entre 8 et 63 caractères. Il s'agit d'une combinaison de lettres, de chiffres et de caractères spéciaux. Il s'agit du mot de passe utilisé pour la première connexion au réseau sans fil. Passez ensuite à l'étape 21.



Étape 12. Si vous avez choisi WPA Enterprise à l'étape 8, cliquez sur une case d'option pour la méthode EAP.

Les options disponibles sont définies comme suit :

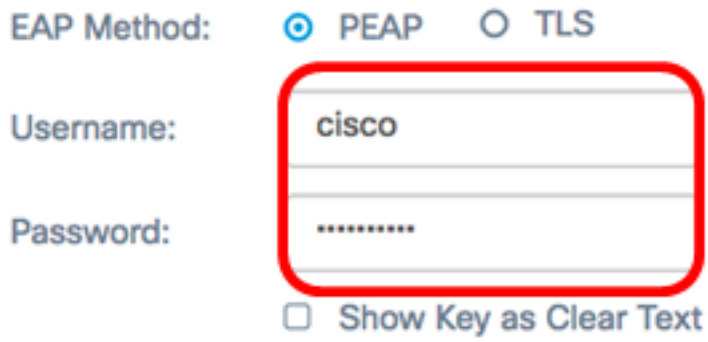
- PEAP : ce protocole donne à chaque utilisateur sans fil des noms d'utilisateur et des mots de passe individuels WAP prenant en charge les normes de cryptage AES. Puisque le PEAP est une méthode de sécurité basée sur un mot de passe, votre sécurité Wi-Fi est basée sur les informations d'identification 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. Si vous choisissez cette option, passez à l'étape 14.



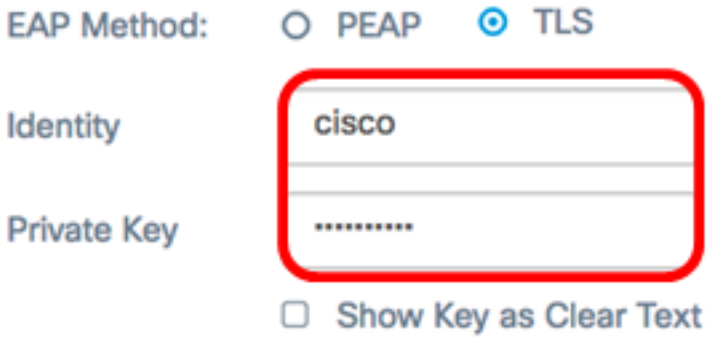
Note: Dans cet exemple, le protocole PEAP est choisi.

Étape 13. Saisissez 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 21.

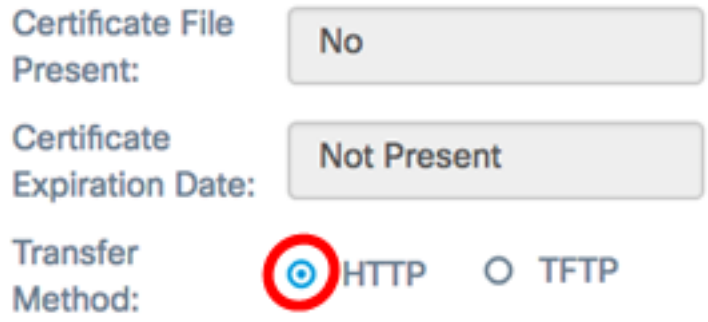


Étape 14. Si vous avez cliqué sur TLS à l'étape 12, saisissez l'identité et la clé privée du client d'infrastructure dans les champs Identité et Clé privée.



Étape 15. 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 18.
- 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.



Note: Si un fichier de certificat est déjà présent sur le WAP, les champs Certificate File Present and Certificate Expiration Date (Fichier de certificat présent et Date d'expiration du certificat) sont déjà renseignés avec les informations pertinentes. Sinon, elles seront vides.

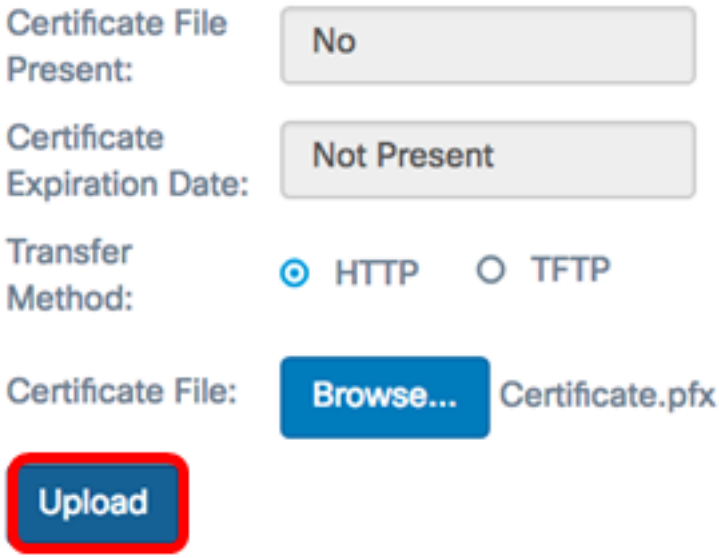
HTTP

Étape 16. Cliquez sur le bouton **Parcourir** 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, Certificate.pfx est sélectionné.

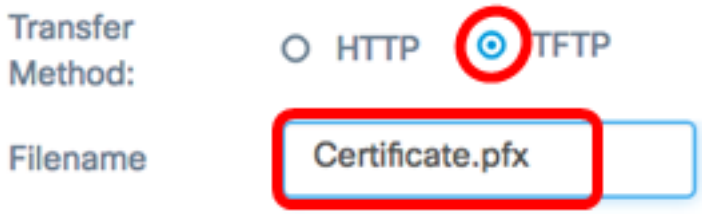
Étape 17. Cliquez sur **Upload** pour télécharger le fichier de certificat sélectionné. Passez à l'étape 21.



Les champs Certificate File Present et Certificate Expiration Date seront mis à jour automatiquement.

TFTP

Étape 18. (Facultatif) Si vous avez cliqué sur TFTP à l'étape 15, entrez le nom de fichier du fichier de certificat dans le champ *Nom de fichier*.



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

Étape 19. Entrez l'adresse du serveur TFTP dans le champ *TFTP Server IPv4 Address*.

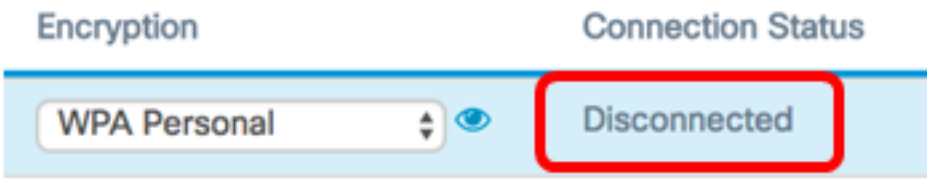
Note: Dans cet exemple. 192.168.100.108 est utilisé comme adresse du serveur TFTP.

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

Les champs Certificate File Present et Certificate Expiration Date seront mis à jour automatiquement.

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

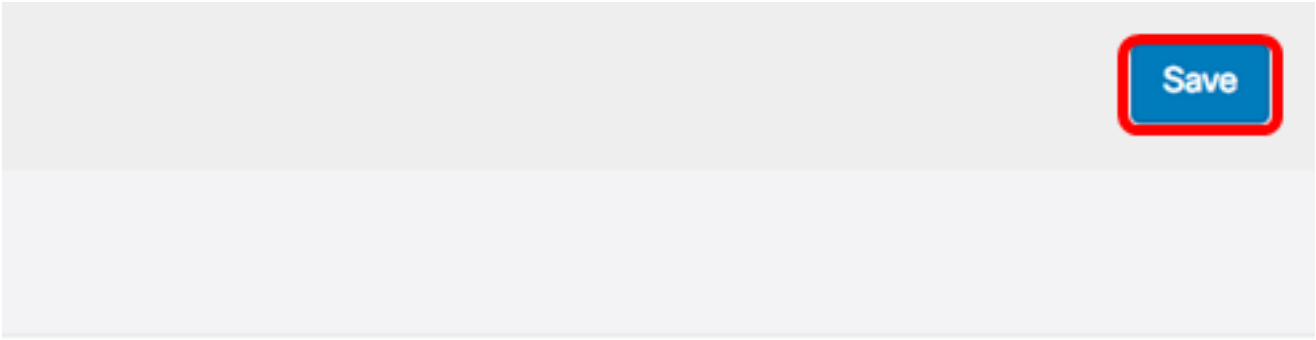
La zone État de la connexion indique si le WAP est connecté au périphérique WAP en amont.

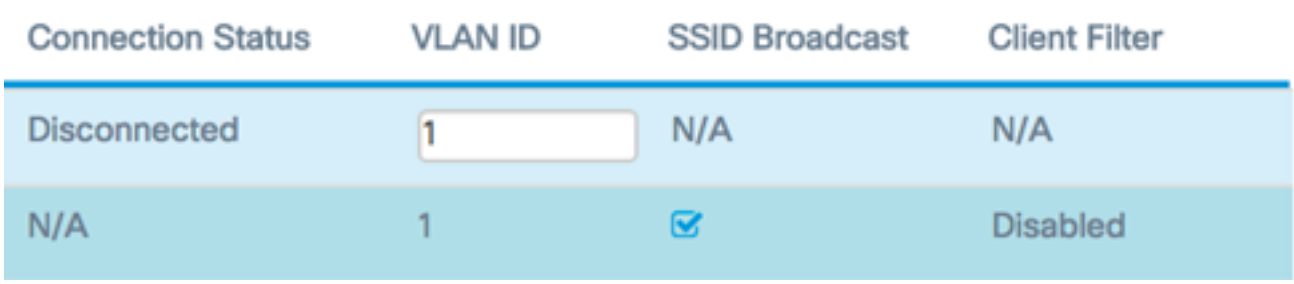


Étape 22. Saisissez l'ID de VLAN de l'interface client de l'infrastructure. 1 est établi par défaut.

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

Étape 23. Cliquez sur **Save** pour enregistrer les paramètres configurés.



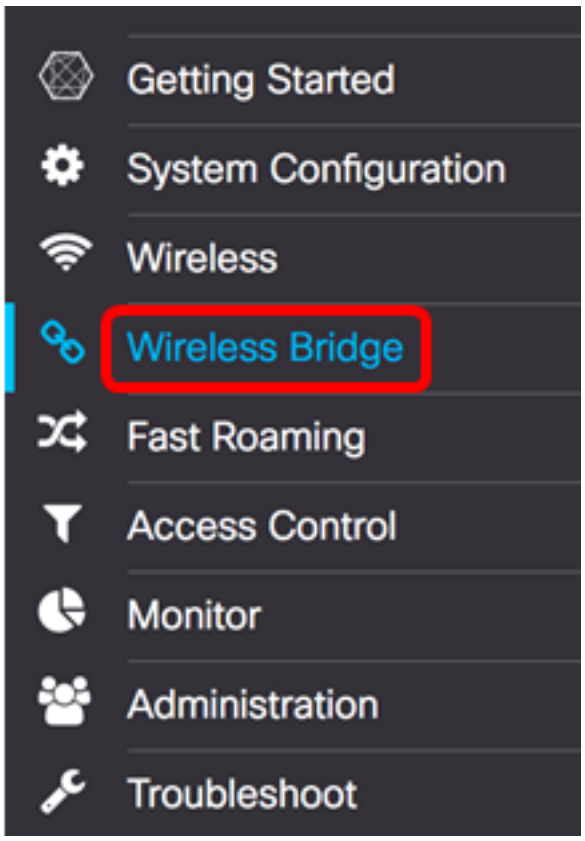


Vous devez maintenant avoir correctement configuré les paramètres d'interface client de l'infrastructure sur votre WAP.

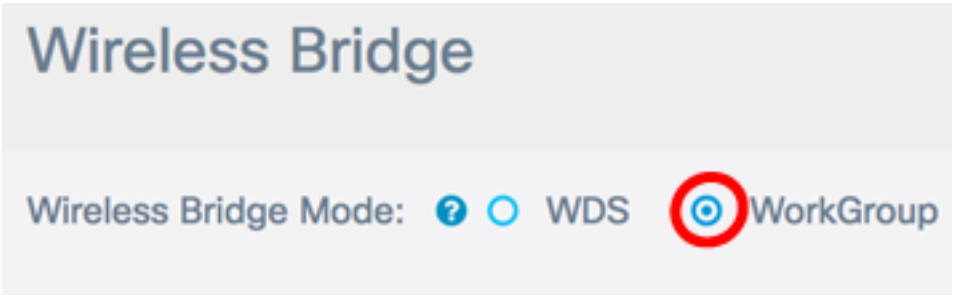
Configurer l'interface client du point d'accès

Étape 1. Connectez-vous à l'utilitaire Web du WAP, puis sélectionnez **Wireless Bridge**.

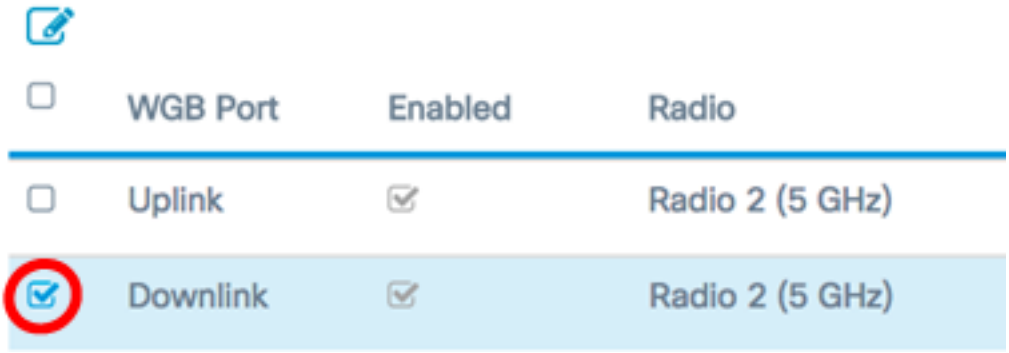
Note: Les options disponibles peuvent varier en fonction du modèle exact de votre périphérique. Dans cet exemple, WAP125 est utilisé.



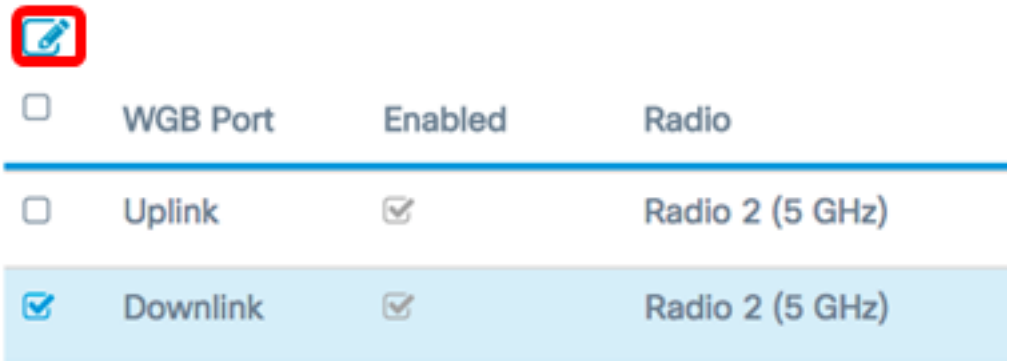
Étape 2. Cliquez sur la case d'option **Groupe de travail**.



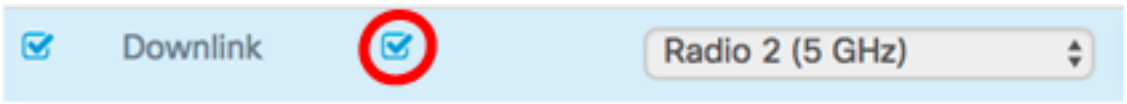
Étape 3. Cochez la case **Downlink**.



Étape 4. Cliquez sur le bouton **Edit.**



Étape 5. Cochez la case **Enabled** pour activer le pontage sur l'interface du point d'accès.



Étape 6. 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 en aval.

Note: Pour cet exemple, le SSID utilisé est WAP125 Downstream.

Étape 7. 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 13 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 8. (Facultatif) Cochez la case WPA-TKIP pour déterminer le chiffrement WPA-TKIP que l'interface du point d'accès utilisera. Ceci est activé par défaut.

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

Étape 9. Saisissez la clé WPA partagée dans le champ Key (Clé). 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 10. Saisissez 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.

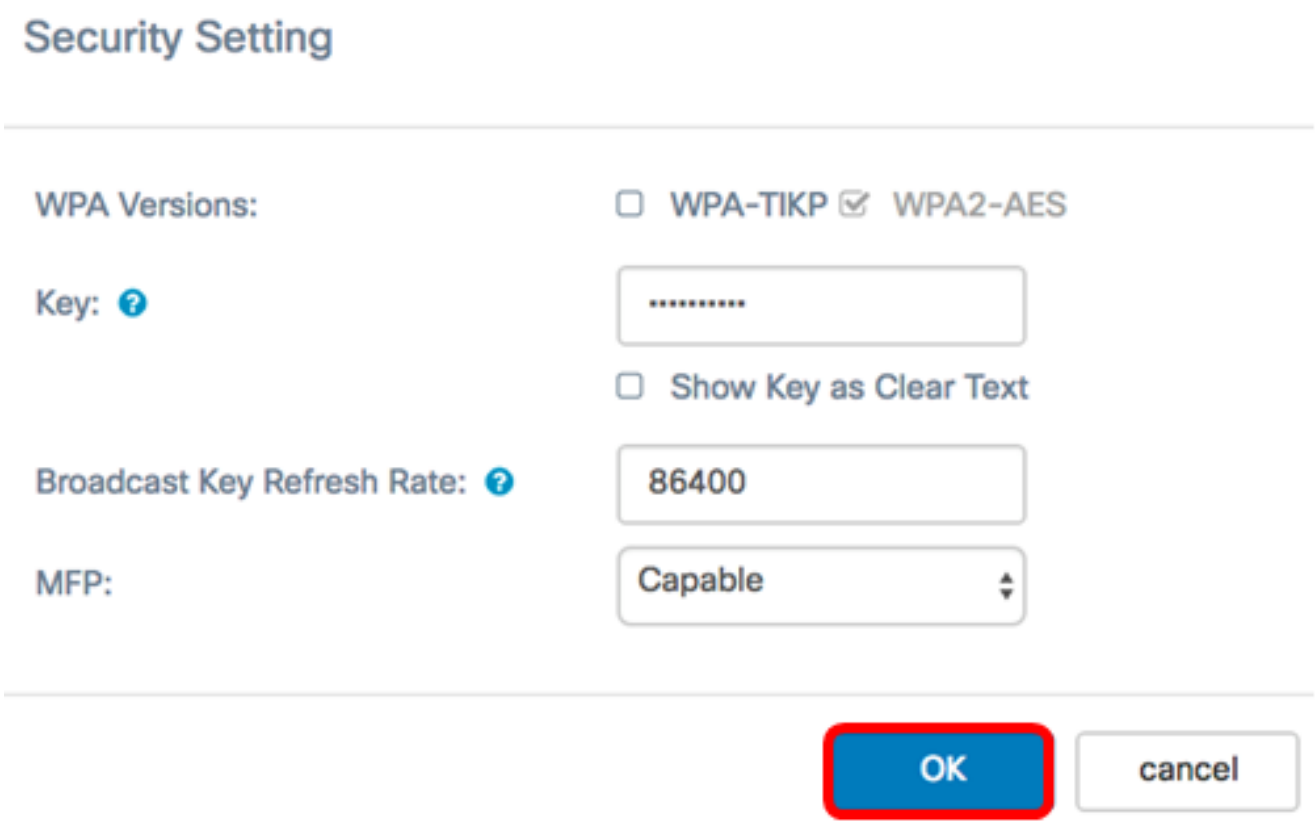
Note: Dans cet exemple, 86400 est utilisé.

Étape 11. Choisissez une option dans la liste déroulante MFP si vous voulez que le WAP exige ou non des trames protégées. Pour en savoir plus sur la MFP, cliquez ici. Les options sont les suivantes :

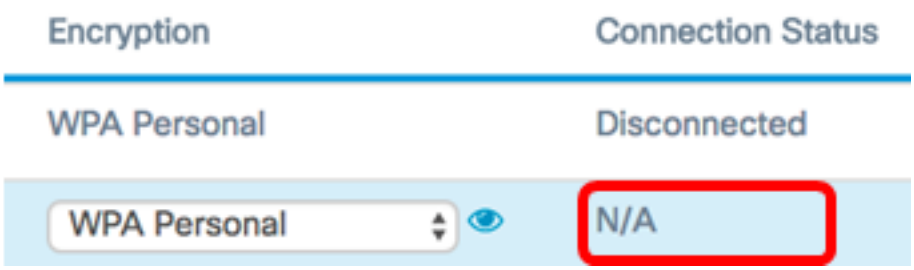
- Not Required : désactive la prise en charge du client pour MFP.
- Capable : permet à la fois aux clients compatibles MFP et aux clients qui ne prennent pas en charge MFP de rejoindre le réseau. Il s'agit du paramètre MFP par défaut sur le WAP.
- Obligatoire : les clients ne sont autorisés à s'associer 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 12. Cliquez sur **OK** pour enregistrer les paramètres de sécurité.



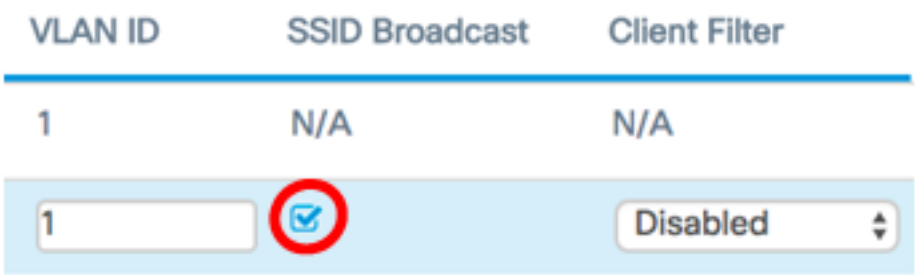
La zone État de la connexion indique Non applicable ou S/O.



Étape 13. Saisissez l'ID VLAN dans le champ VLAN ID de l'interface du point d'accès.

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

Étape 14. Cochez la case SSID Broadcast (Diffusion SSID) si vous voulez que le SSID en aval soit diffusé. La diffusion SSID est activée par défaut.



Étape 15. 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

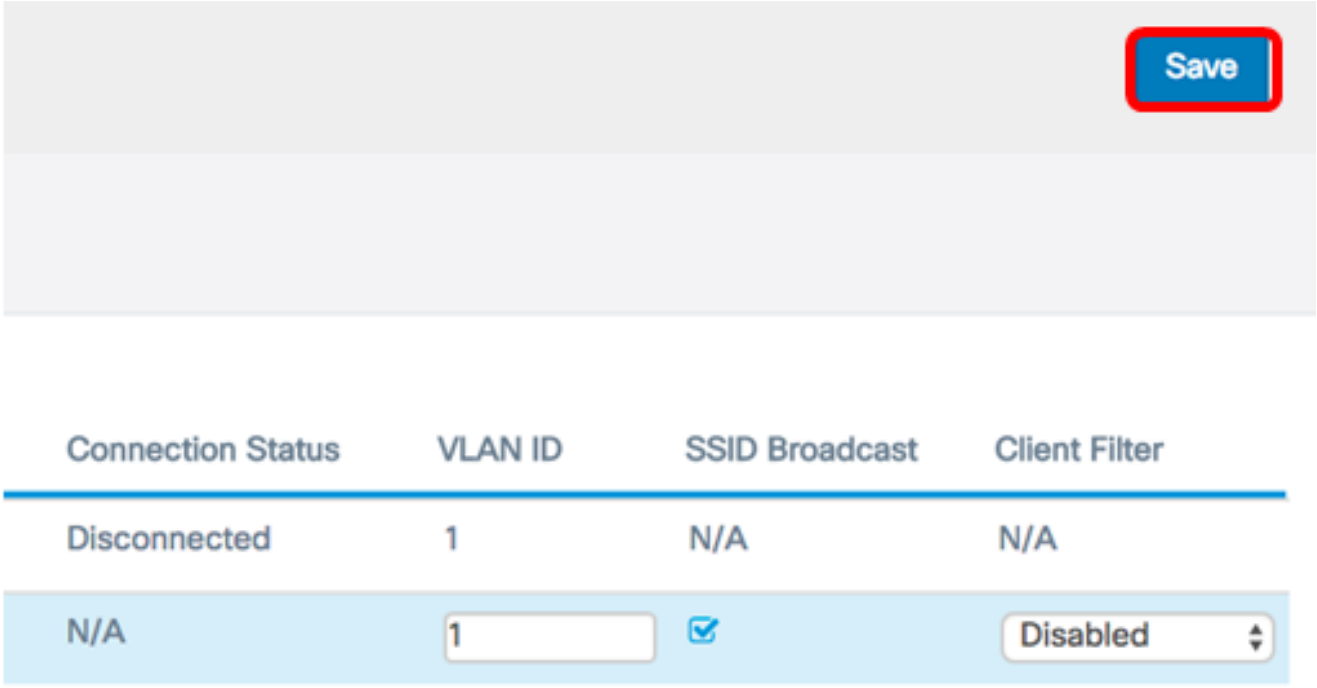
WAP est accordé ou refusé aux utilisateurs en fonction de l'adresse MAC du client qu'ils utilisent.

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 16. Cliquez sur **Enregistrer** pour enregistrer vos modifications.



Vous devez maintenant avoir correctement configuré les paramètres du pont de groupe de travail sur vos points d'accès sans fil.