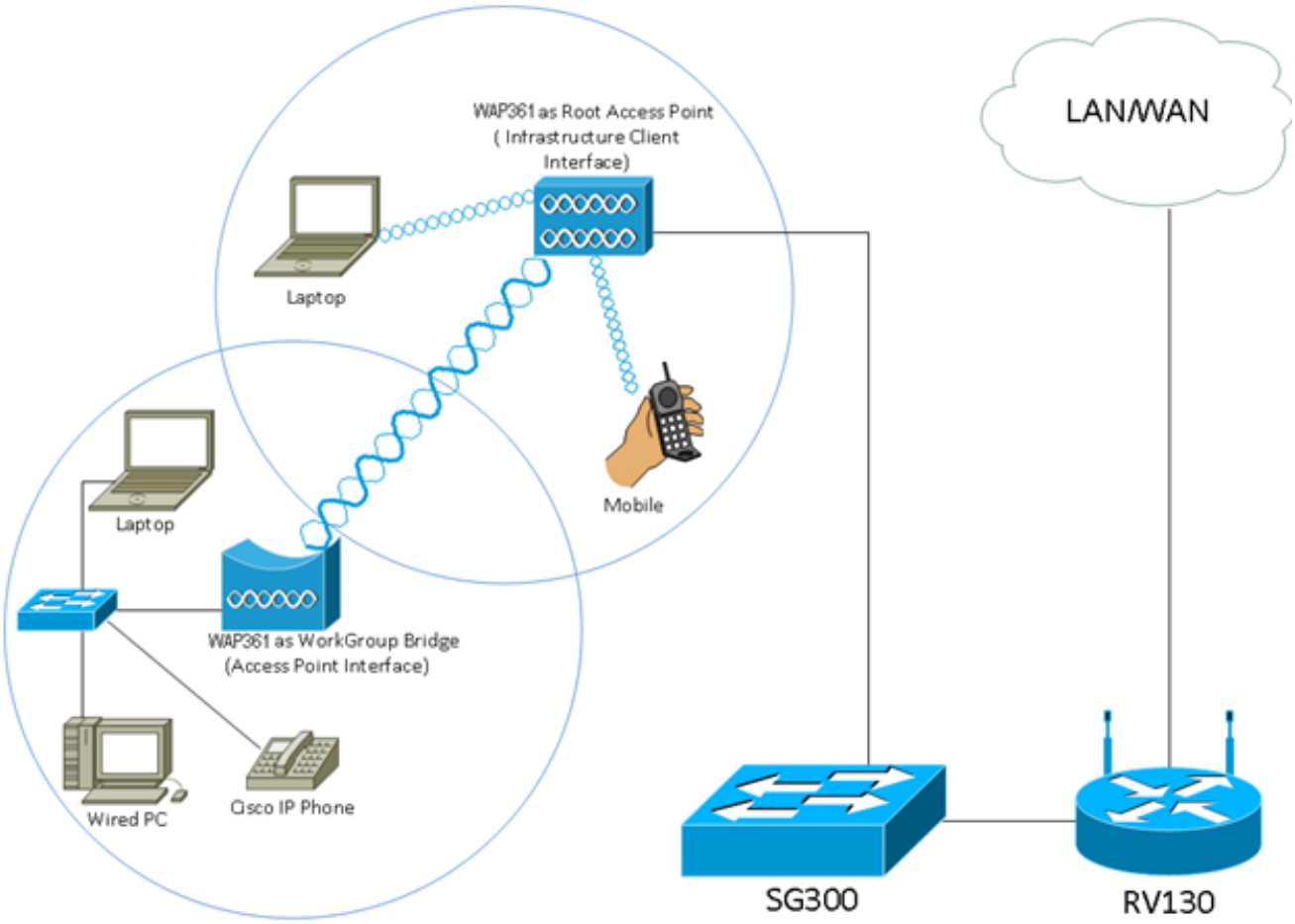
Configuration du pont de groupe de travail sur un point d'accès sans fil (WAP)

Objectif

La fonction de pont de groupe de travail permet au point d'accès sans fil (WAP) de relier le trafic entre un client distant et le réseau local sans fil (LAN) qui est connecté en 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 de groupe de travail permet aux périphériques qui n'ont que des connexions filaires de se connecter à un réseau sans fil. Le mode pont de groupe de travail est recommandé comme solution de rechange lorsque la fonction de système de distribution sans fil (WDS) n'est pas disponible.



Remarque : la topologie ci-dessus illustre un exemple de modèle de pont de groupe de travail. Les périphériques filaires sont attachés à un commutateur, qui se connecte à l'interface LAN du WAP. Le WAP agit comme une interface de point d'accès et se connecte à l'interface d'infrastructure.

Cet article vise à vous montrer comment configurer le pont de groupe de travail entre deux WAP.

Périphériques pertinents

- Série WAP100
- Série WAP300
- Série 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

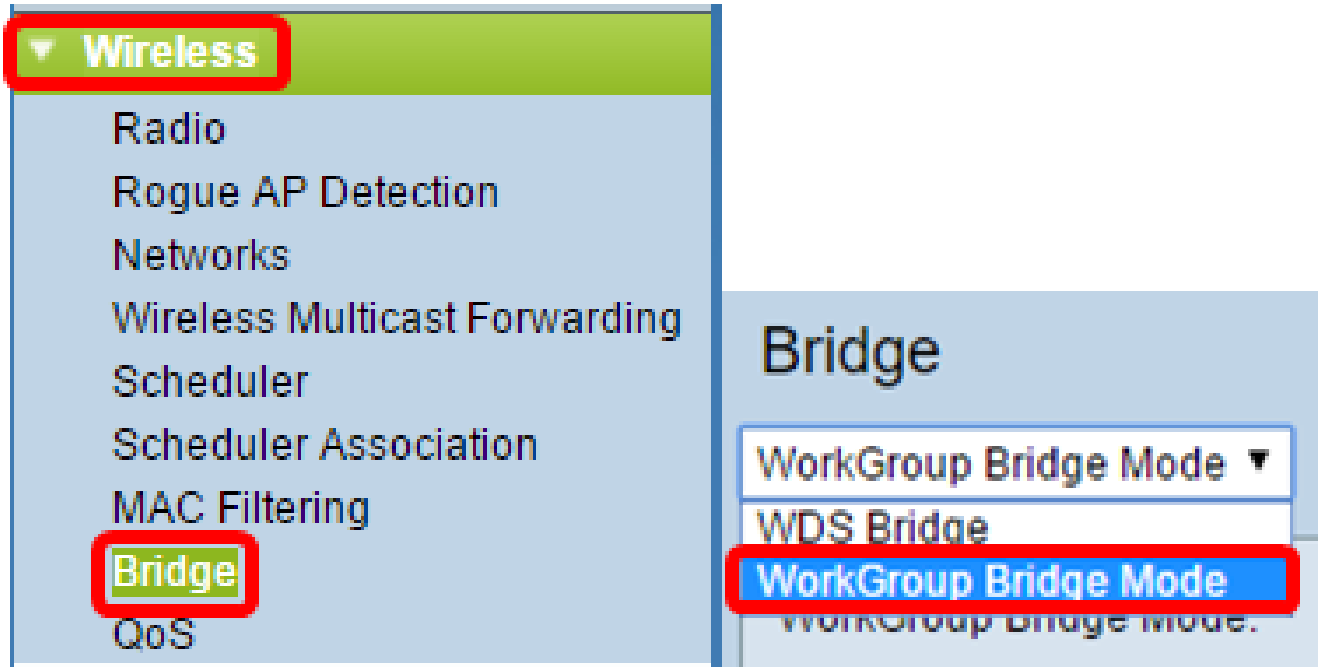
Interface client d'infrastructure

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

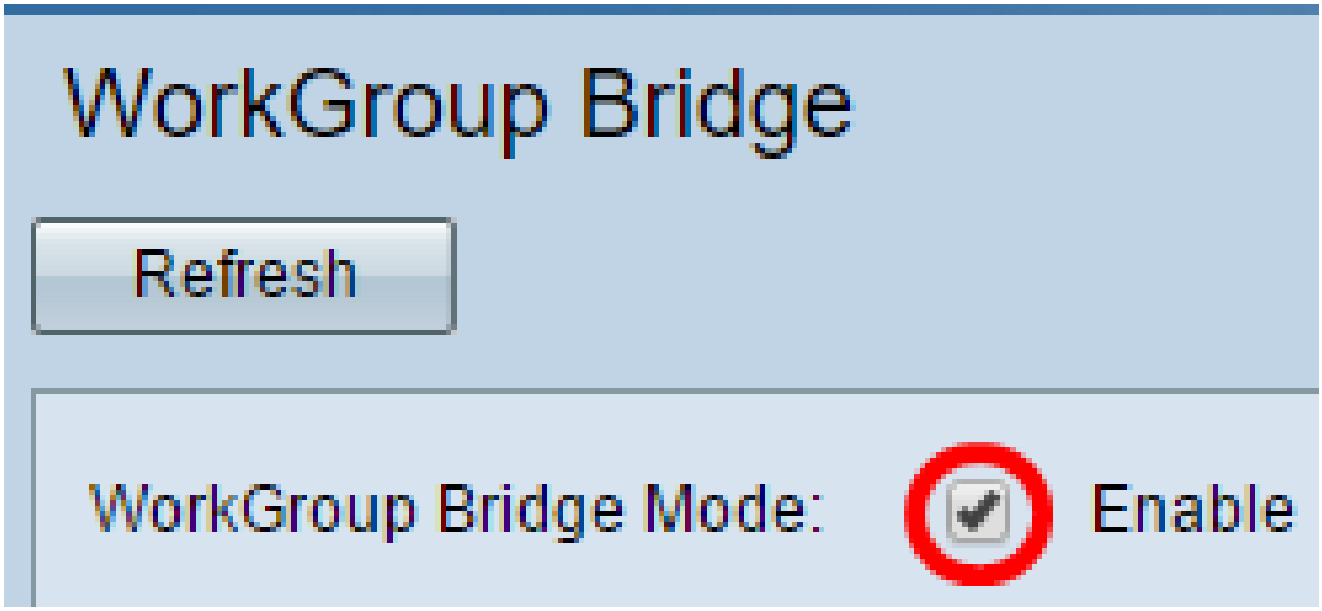
Remarque : les options de menu peuvent varier en fonction du modèle du périphérique que vous utilisez. Sauf indication contraire, les images ci-dessous proviennent du WAP361.



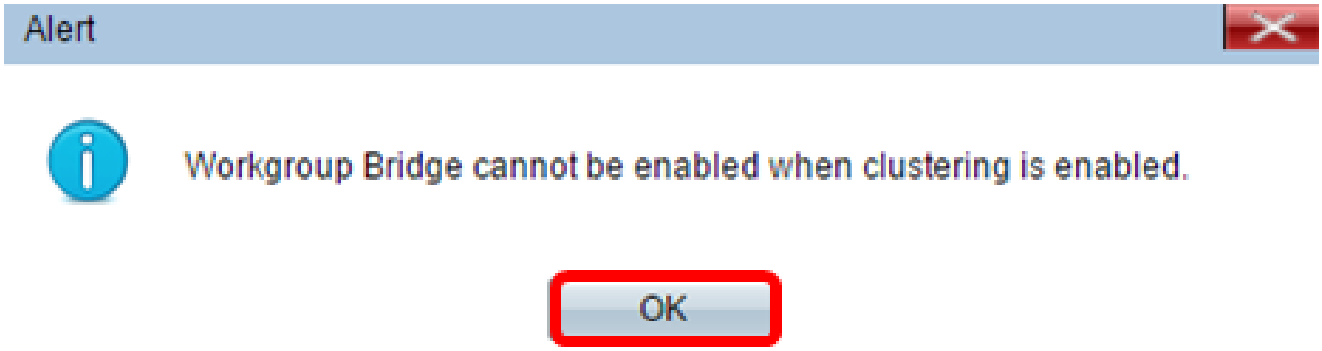
Pour WAP571 et WAP571E, choisissez Wireless > Bridge > WorkGroup Bridge Mode.



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

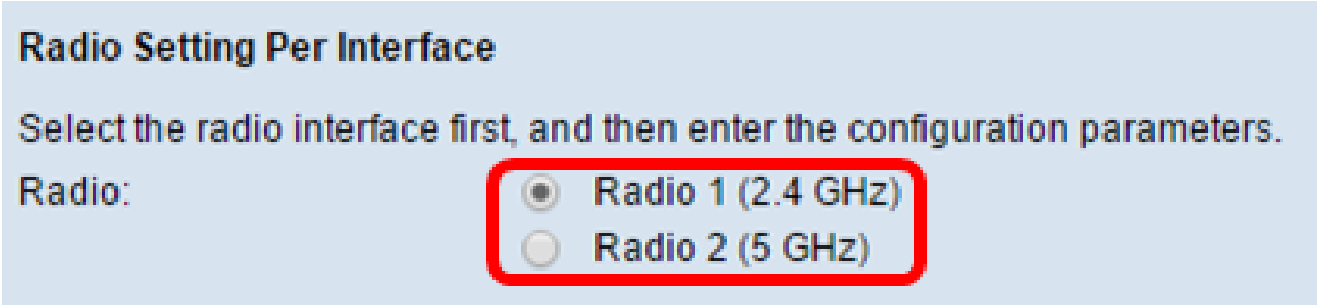


Remarque : si la mise en grappe est activée sur le WAP, une fenêtre contextuelle vous avertit de la désactiver pour que le pont de groupe de travail fonctionne. Cliquez sur OK pour continuer. Pour désactiver le clustering, choisissez Single Point Setup dans le volet de navigation, puis choisissez Access Points > Disable Single Point Setup.



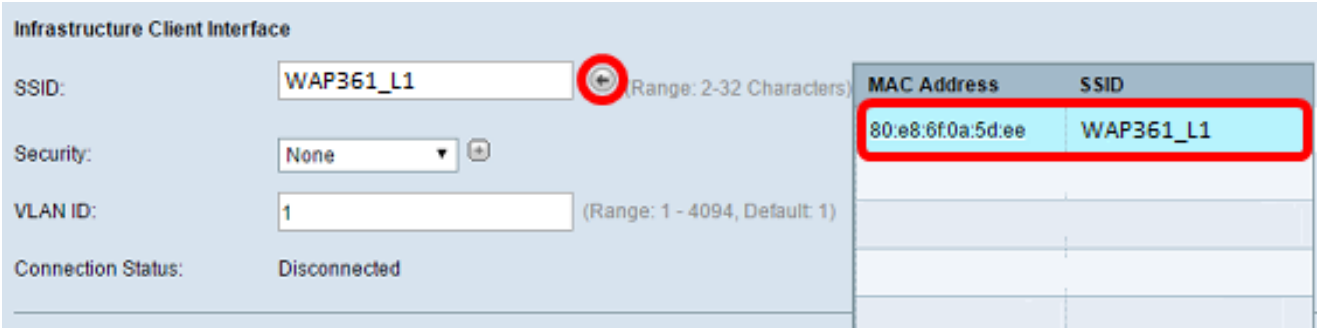
Étape 3. Cliquez sur l'interface radio du pont de groupe de travail. Lorsque vous configurez une radio en tant que pont de groupe de travail, l'autre radio reste opérationnelle. Les interfaces radio correspondent aux bandes de fréquences radio du WAP. Le WAP est équipé pour diffuser sur deux interfaces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

Remarque : cette étape concerne uniquement les WAP suivants avec double bande : WAP131, WAP150, WAP351, WAP361, WAP371, WAP561, WAP571, WAP571E. Pour cet exemple, Radio 1 est choisi.



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 des voisins. Il s'agit de la connexion entre le périphérique et le client distant. Vous pouvez saisir entre 2 et 32 caractères pour le SSID du client d'infrastructure.

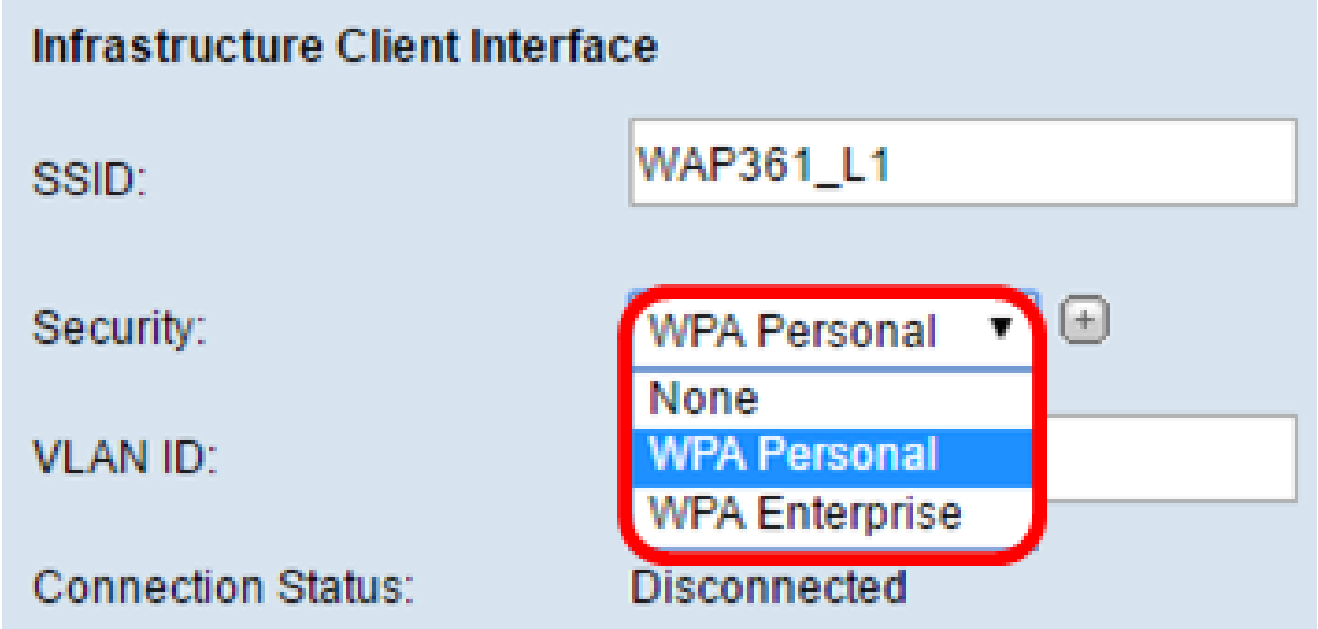
Remarque : il est important d'activer la détection des points d'accès non autorisés. Pour en savoir plus sur l'activation de cette fonctionnalité, cliquez ici. Dans cet exemple, vous cliquez sur la flèche pour choisir WAP361_L1 comme SSID de l'interface client d'infrastructure.



Étape 5. Dans la zone Infrastructure Client Interface, choisissez 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 : ouvert 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

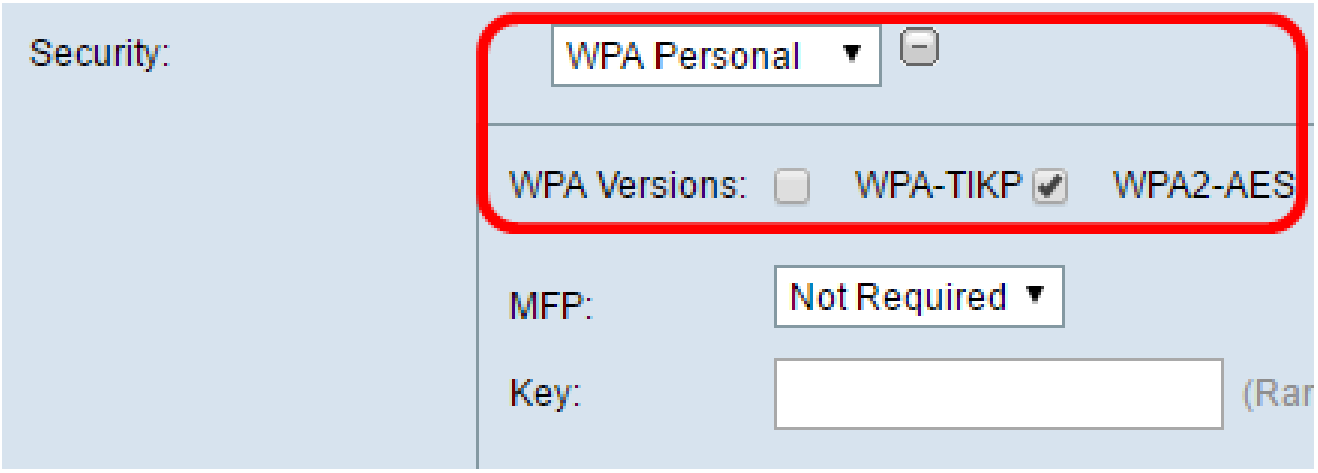
sécurité recommandée pour l'authentification. Il utilise les protocoles PEAP (Protected Extensible Authentication Protocol) et TLS (Transport Layer Security). Passez à l'étape 9 pour configurer. Ce type de sécurité est souvent utilisé dans un environnement de bureau et nécessite la configuration d'un serveur RADIUS (Remote Authentication Dial-In User Service). Cliquez ici pour en savoir plus sur les serveurs RADIUS.



Remarque : dans cet exemple, WPA Personal (WPA personnel) 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.

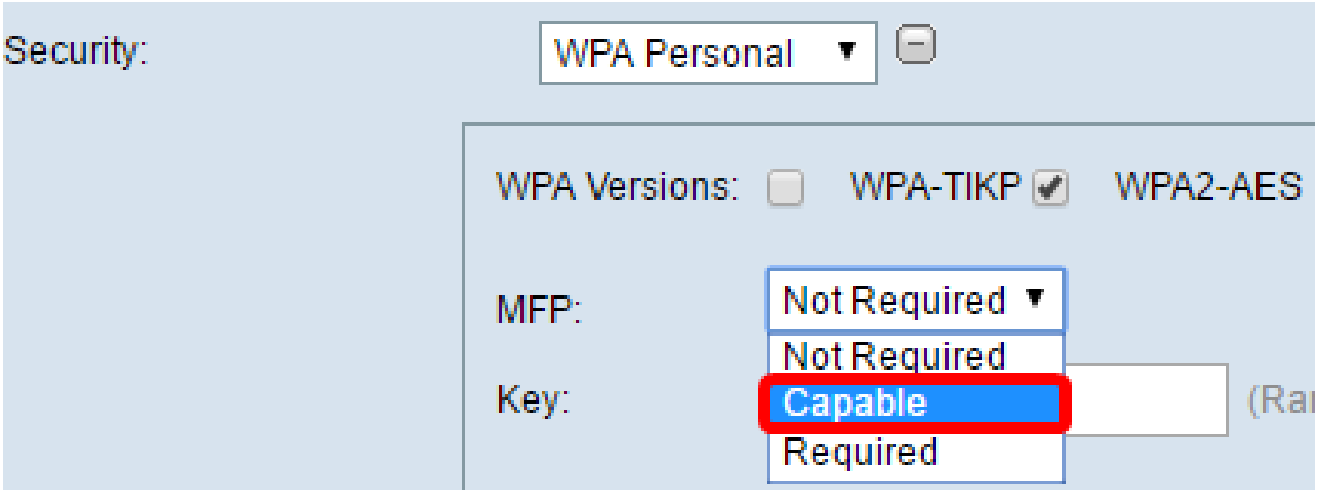
Remarque : si tous vos équipements sans fil prennent en charge WPA2, définissez la sécurité du client d'infrastructure sur WPA2-AES. La méthode de cryptage est RC4 pour WPA et AES (Advanced Encryption Standard) pour WPA2. WPA2 est recommandé car il dispose d'une norme de cryptage plus puissante. Dans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



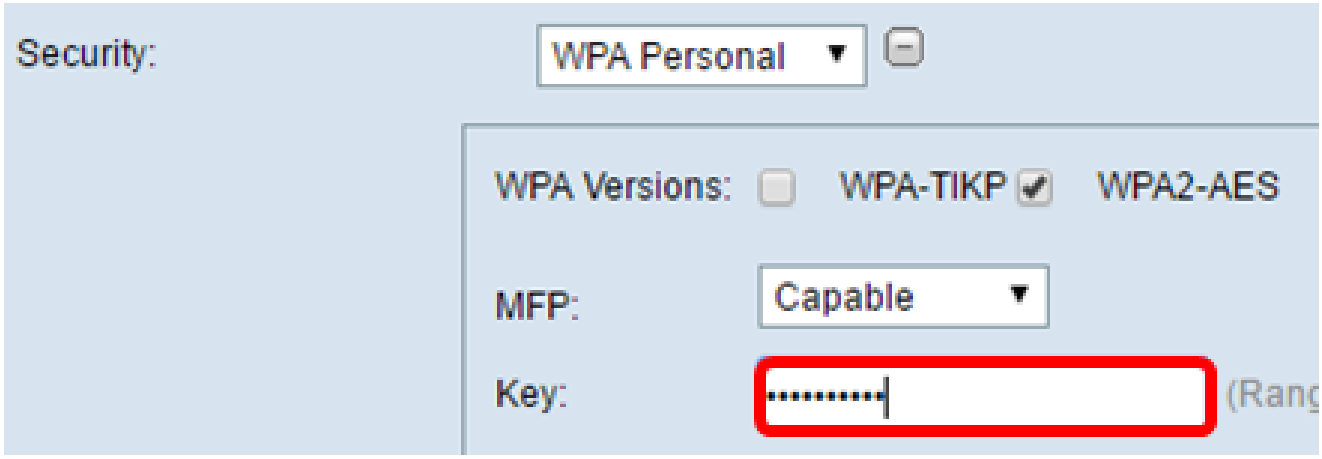
Étape 7. (Facultatif) Si vous avez coché WPA2-AES à l'étape 6, choisissez une option dans la liste déroulante Protection des trames de gestion (MFP) pour savoir si le WAP doit ou non disposer de trames protégées. Pour en savoir plus sur MFP, cliquez ici. Les options sont les suivantes :

- Not Required : désactive la prise en charge du MFP par le client.
- Capable : permet aux clients compatibles MFP et qui ne prennent pas en charge MFP de se connecter au 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.

Remarque : pour cet exemple, Capable est sélectionné.



Étape 8. Saisissez la clé de cryptage WPA dans le champ Key (Clé). 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 lors de la première connexion au réseau sans fil. Passez ensuite à l'étape 18.



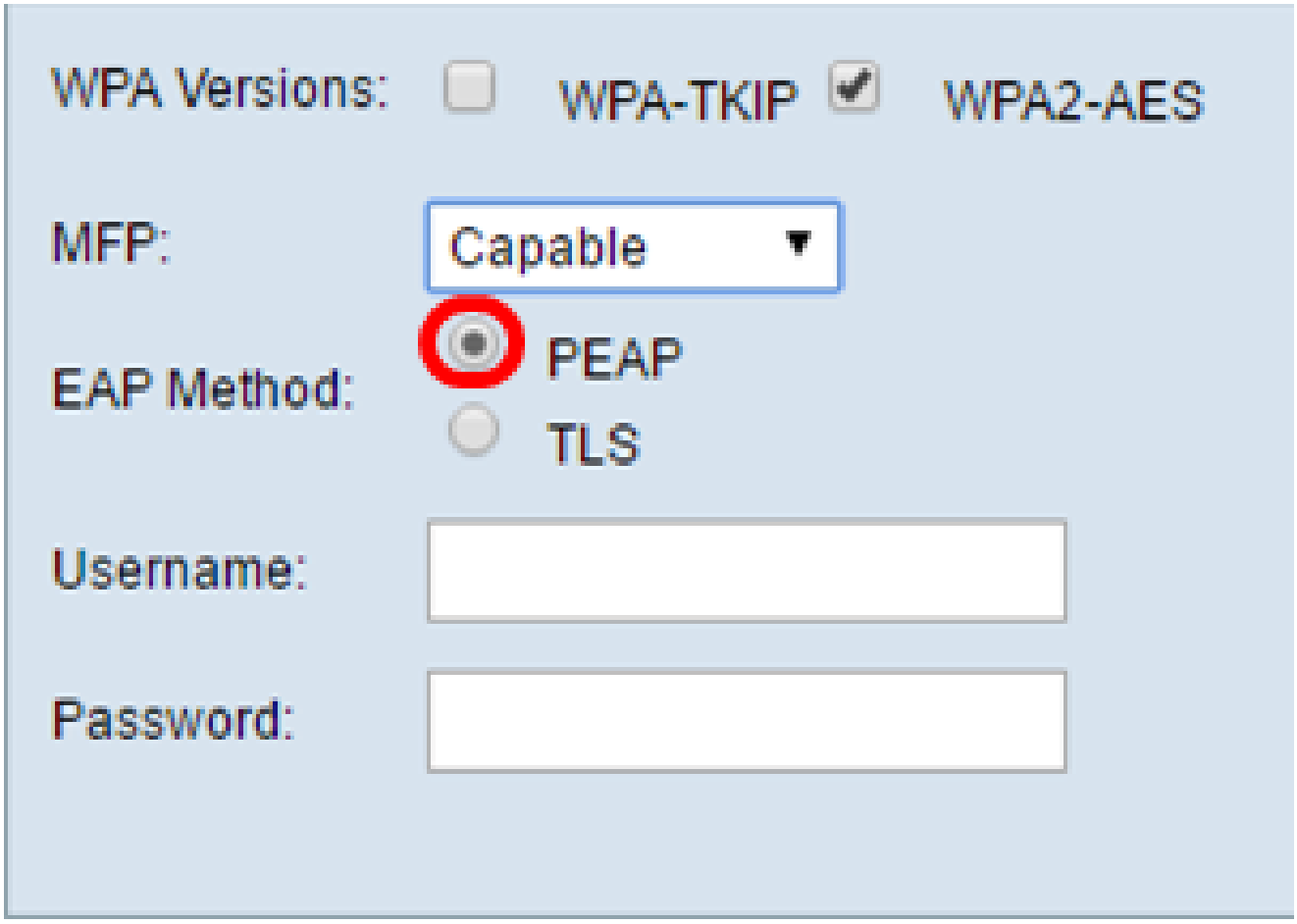
Étape 9. Si vous avez choisi WPA Enterprise à l'étape 5, cliquez sur une case d'option pour la méthode EAP.

Les options disponibles sont définies comme suit :

- PEAP : ce protocole attribue à chaque utilisateur sans fil des noms d'utilisateur et des mots de passe individuels WAP prenant en charge les normes de cryptage AES. Comme le protocole 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

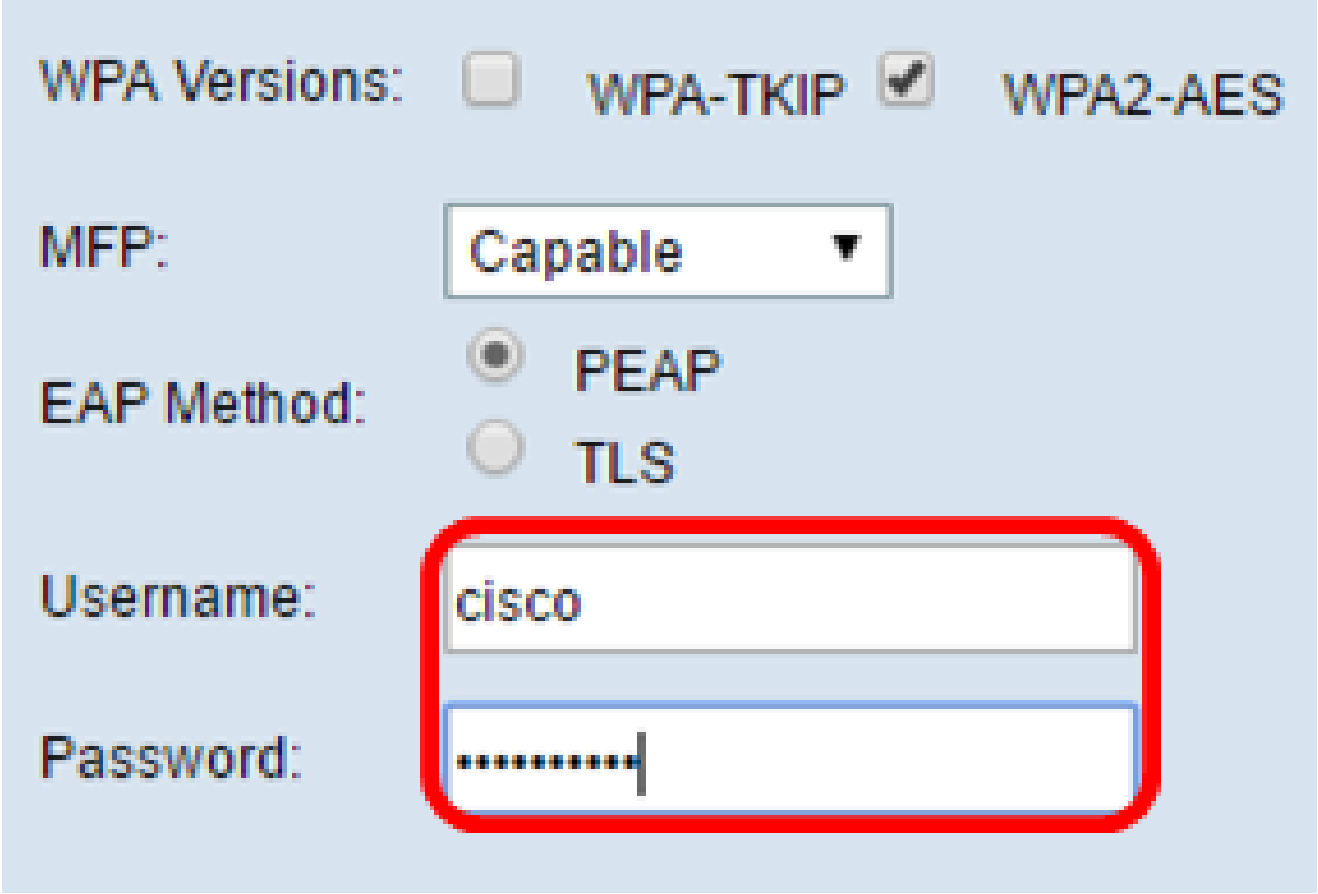
client. Le protocole PEAP peut présenter un risque de sécurité potentiellement grave si vous avez des mots de passe faibles ou des clients non sécurisés. Il s'appuie sur TLS mais évite l'installation de certificats numériques sur chaque client. Au lieu de cela, il fournit une authentification par un nom d'utilisateur et un mot de passe.

- TLS : TLS exige que chaque utilisateur dispose d'un certificat supplémentaire pour pouvoir accéder à l'application. TLS est plus sécurisé si vous disposez des serveurs supplémentaires et de l'infrastructure nécessaire pour authentifier les utilisateurs sur votre réseau.

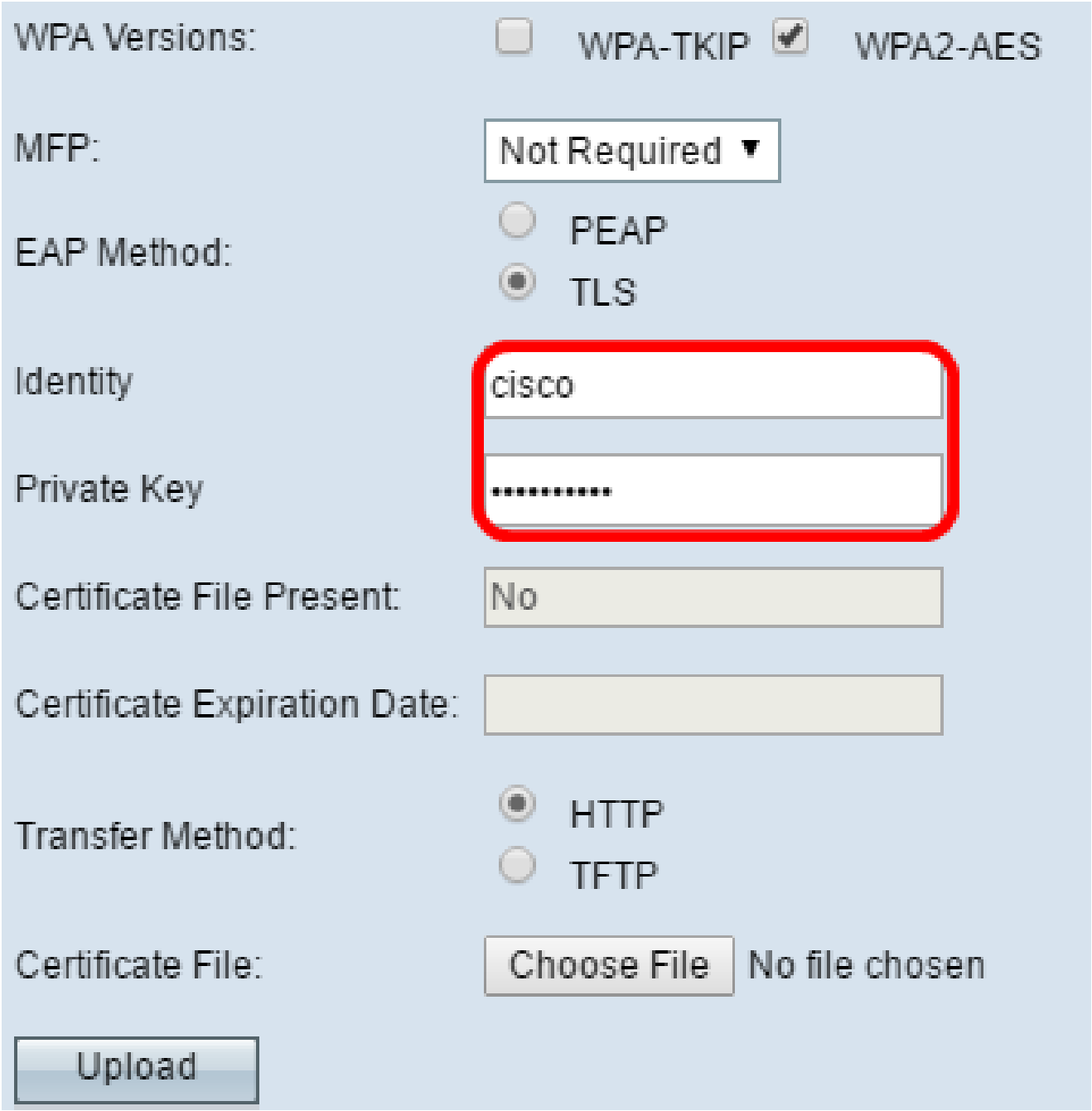


Remarque : pour cet exemple, le protocole PEAP est choisi.

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 du client d'infrastructure. Pour obtenir ces informations, reportez-vous à l'interface de votre client d'infrastructure. Passez ensuite à l'étape 18.

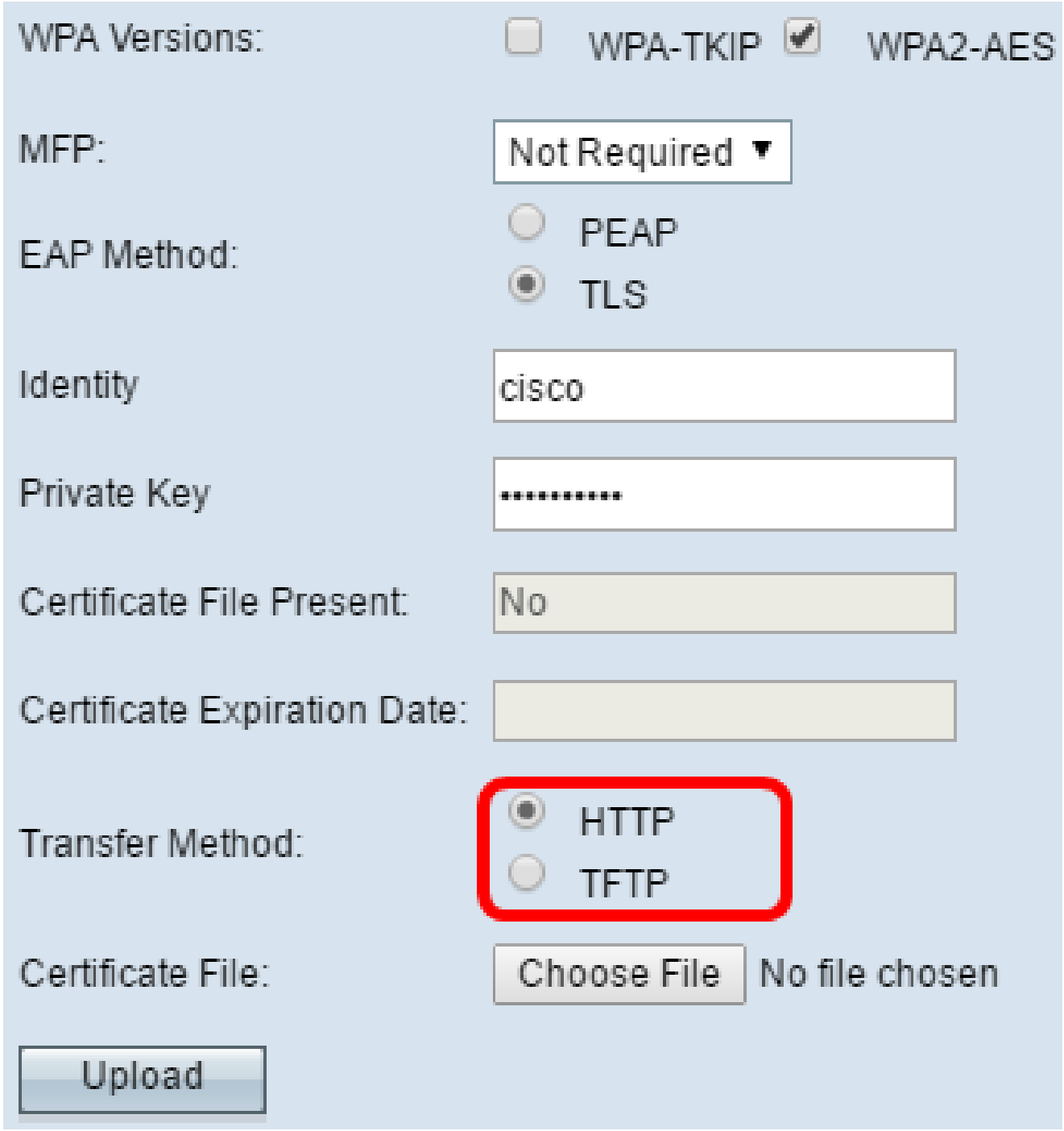


Étape 11. Si vous avez cliqué sur TLS à l'étape 9, entrez l'identité et la clé privée du client d'infrastructure dans les champs Identity et Private Key.



Étape 12. Dans la zone Méthode de transfert, cliquez sur une case d'option parmi les 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 sur 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 par stimulation/réponse 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 Certificate File Present et Certificate Expiration Date seront déjà renseignés avec les informations pertinentes. Dans le cas contraire, elles seront vides.

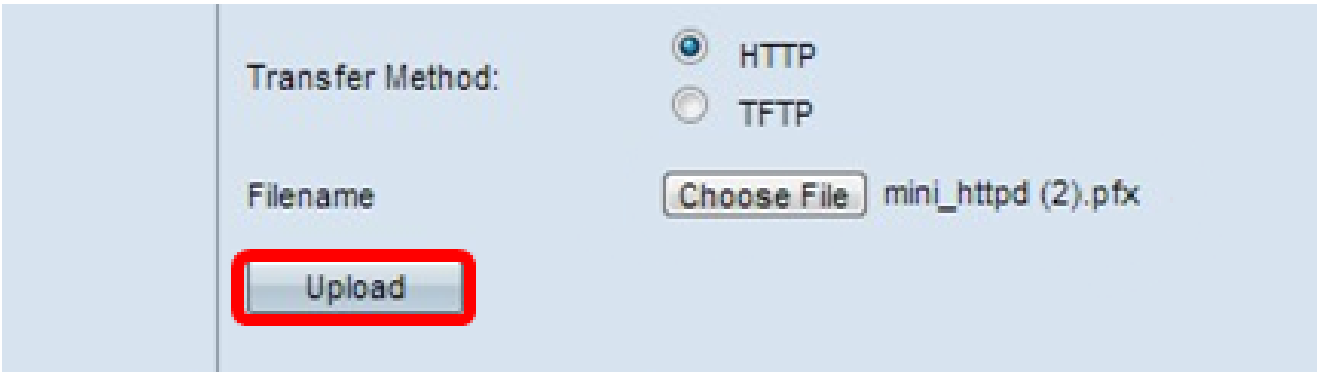
HTTP

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 (telle que .pem ou .pfx) sinon, le fichier ne sera pas accepté.

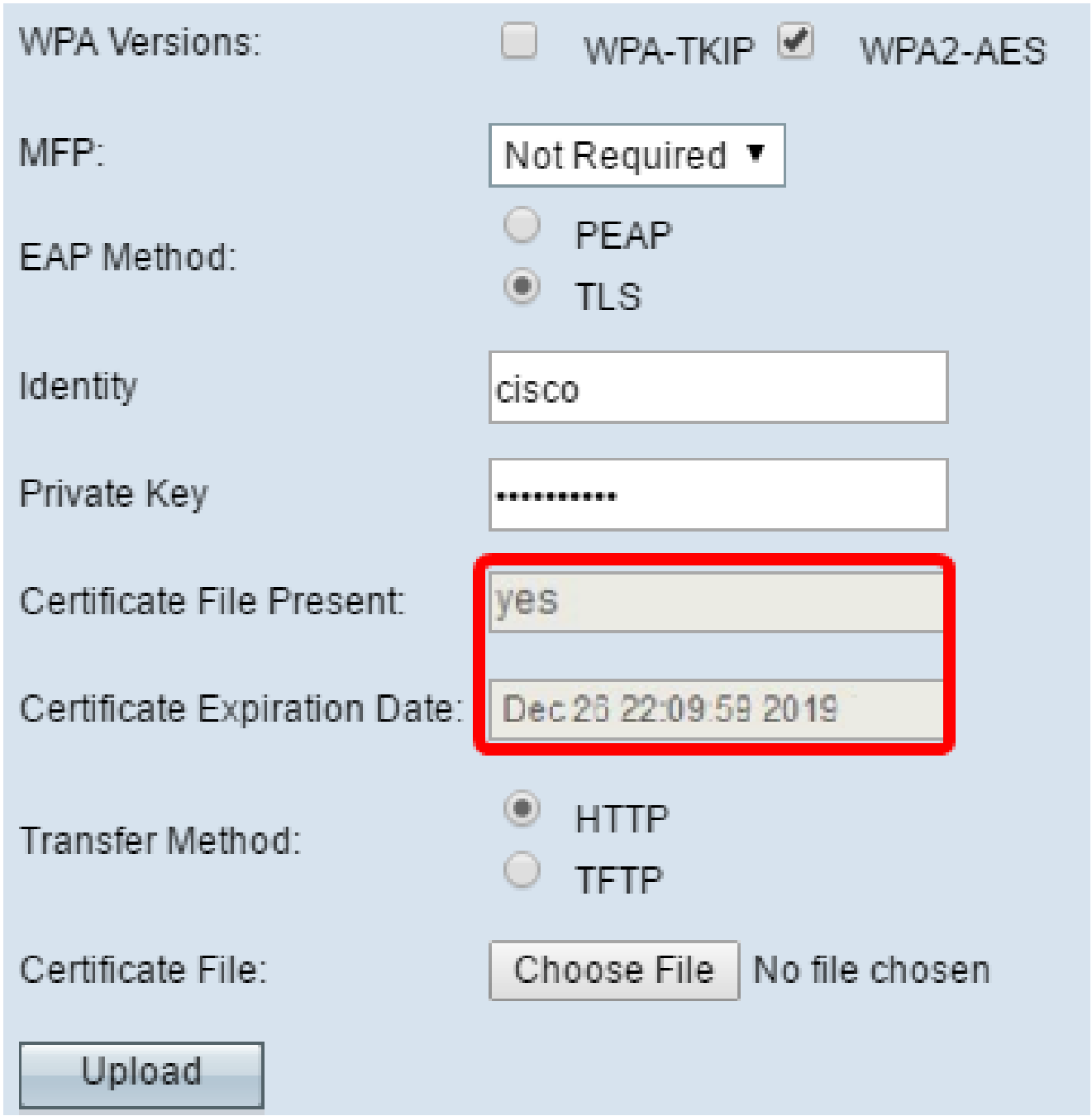
Remarque : dans cet exemple, mini_httpd(2).pfx est choisi.



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



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



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 Filename.

Remarque : dans cet exemple, mini_httpd.pem est utilisé.



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

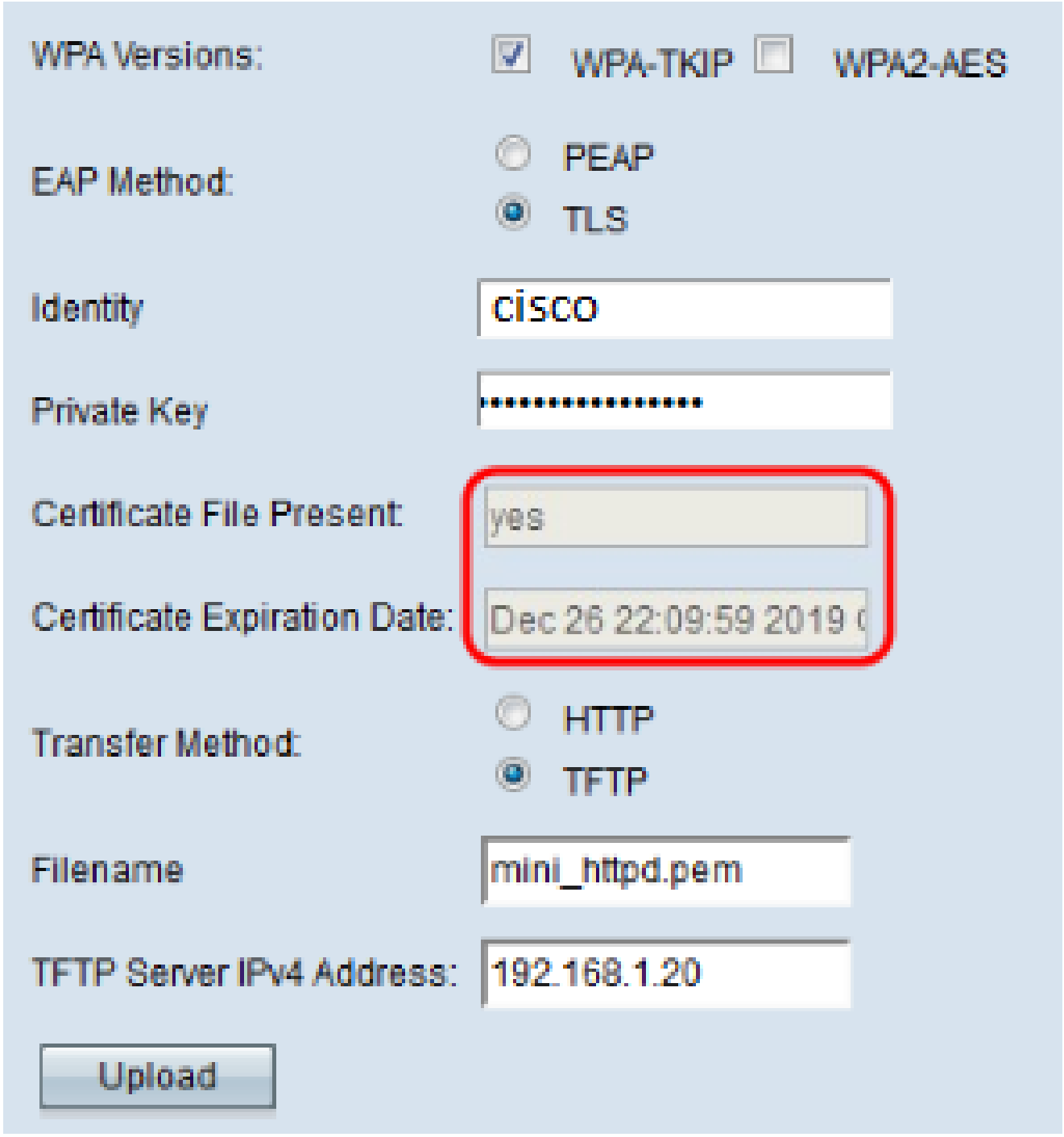
Remarque : dans cet exemple. 192.168.1.20 est utilisée comme adresse du serveur TFTP.



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

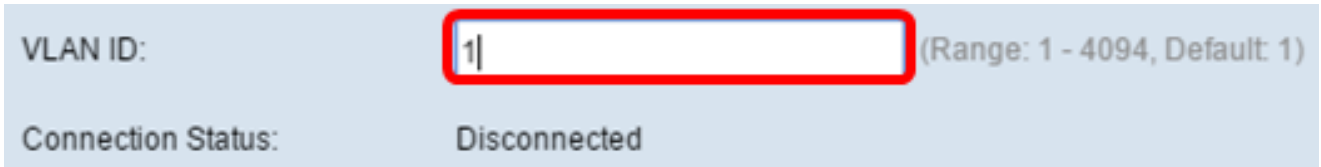


Les champs Certificate File Present et Certificate Expiration Date seront automatiquement mis à jour.



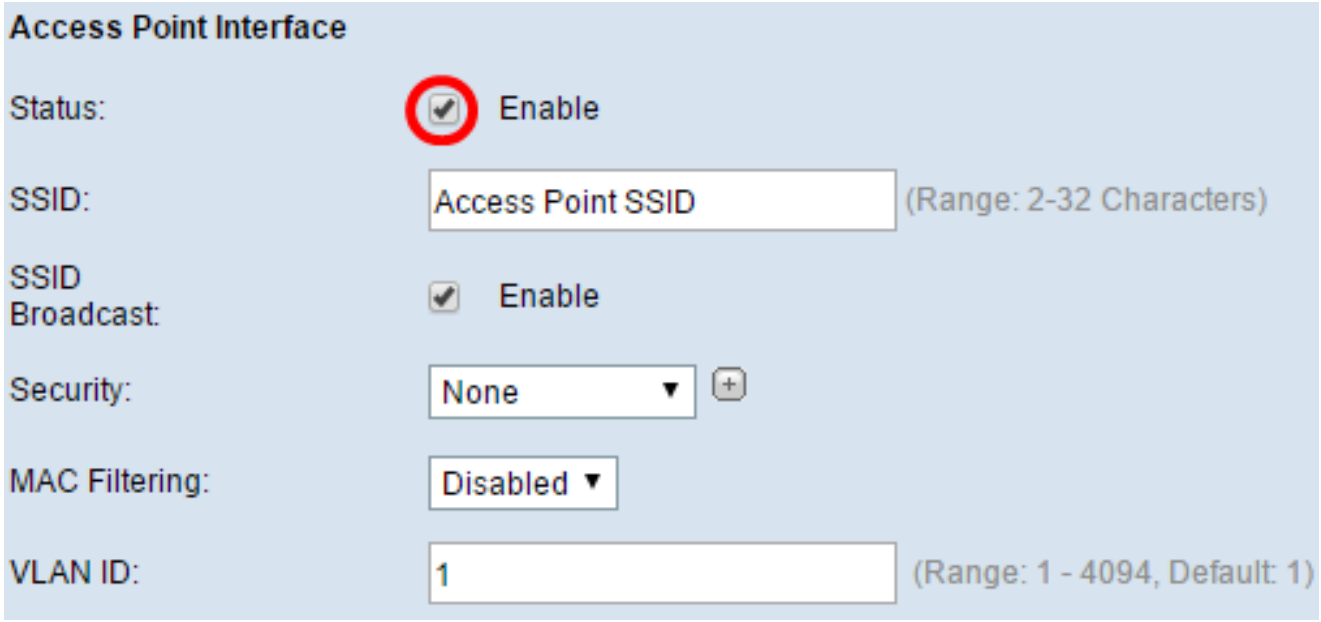
Étape 18. Saisissez l'ID de VLAN pour l'interface client de l'infrastructure. 1 est établi par défaut.

Remarque : pour cet exemple, l'ID de VLAN par défaut est utilisé.



Interface du point d'accès

Étape 1. Cochez la case Enable Status pour activer le pontage sur l'interface du point d'accès.

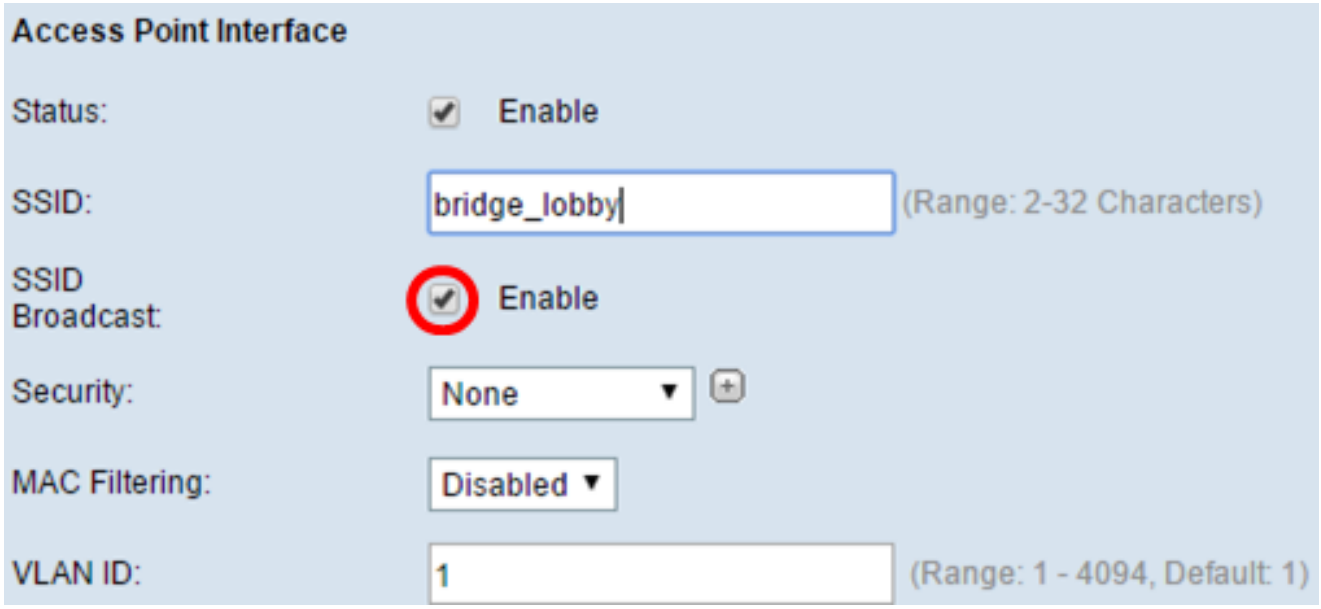


Étape 2. Saisissez le SSID du point d'accès dans le champ SSID. La longueur du SSID doit être comprise entre 2 et 32 caractères. La valeur par défaut est le SSID du point d'accès.

Remarque : pour cet exemple, le SSID utilisé est bridge_lobby.



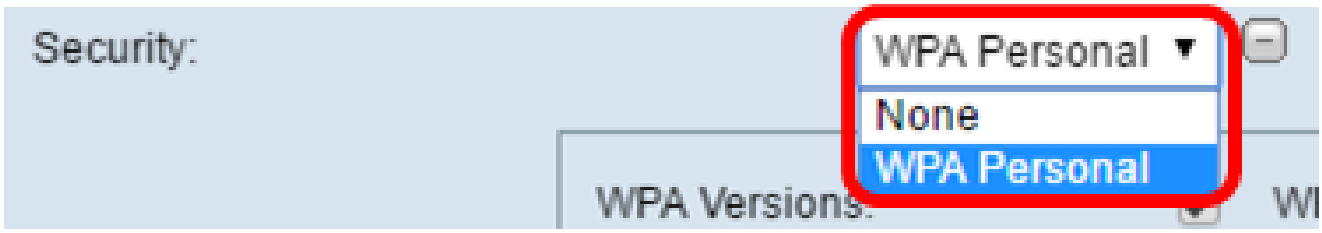
Étape 3. (Facultatif) Si vous ne souhaitez pas diffuser le SSID, décochez la case Enable SSID Broadcast. Cela rendra le point d'accès invisible pour ceux qui recherchent des points d'accès sans fil ; il ne peut être connecté que par une personne qui connaît déjà le SSID. La diffusion SSID est activée par défaut.



Étape 4. Sélectionnez le type de sécurité permettant d'authentifier les stations clientes en aval auprès du WAP dans la liste déroulante Security.

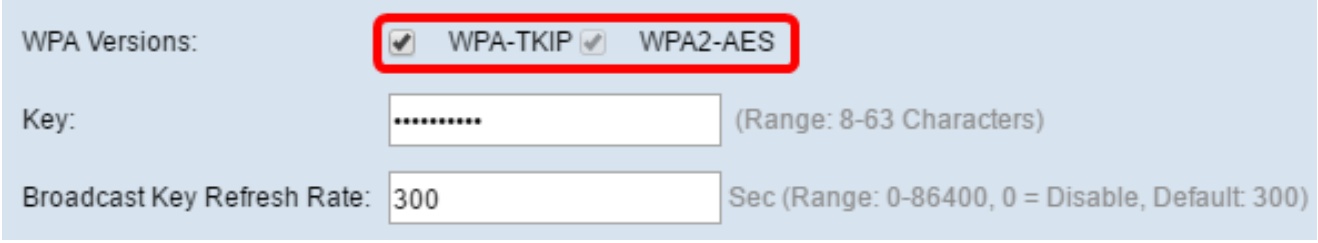
Les options disponibles sont définies comme suit :

- Aucun : ouvert ou sans sécurité. C'est la valeur par défaut. Passez à l'étape 10 si vous choisissez ceci.
- WPA Personal (WPA personnel) : la fonction WPA (Wi-Fi Protected Access) Personal peut prendre en charge des clés de 8 à 63 caractères. La méthode de cryptage est soit TKIP, soit le mode de cryptage de compteur avec le protocole CCMP (Block Chaining Message Authentication Code Protocol). WPA2 avec CCMP est recommandé car il dispose d'une norme de cryptage plus puissante, Advanced Encryption Standard (AES), par rapport au protocole TKIP (Temporal Key Integrity Protocol) qui utilise uniquement une norme RC4 64 bits.

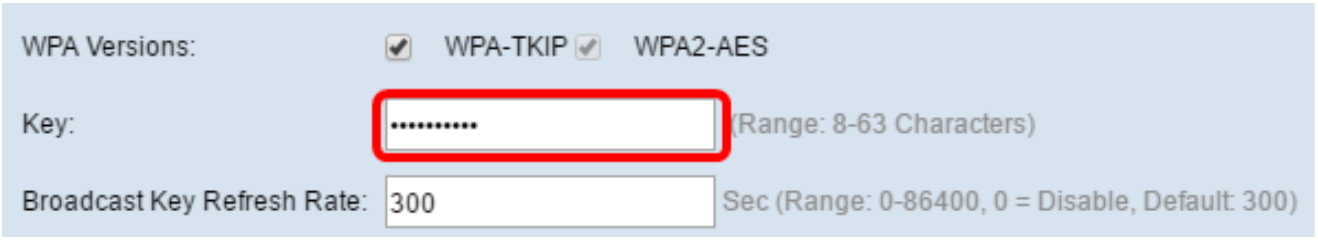


Étape 5. Cochez la case WPA-TKIP ou WPA2-AES pour déterminer le type de cryptage WPA que l'interface du point d'accès utilisera. Ils sont activés par défaut.

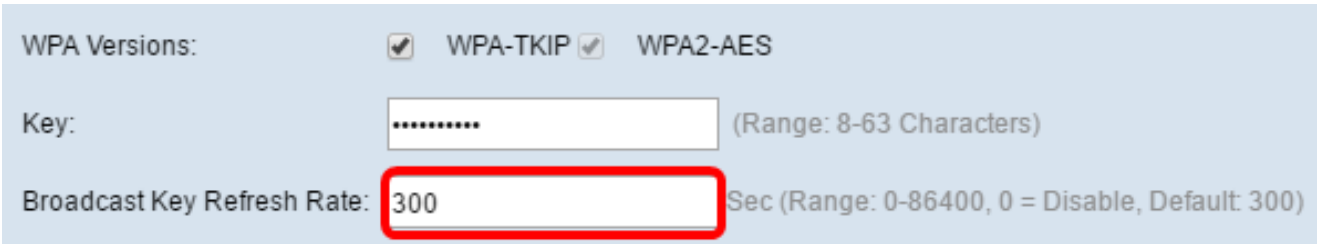
Remarque : si tous vos équipements sans fil prennent en charge WPA2, définissez la sécurité du client d'infrastructure sur WPA2-AES. La méthode de cryptage est RC4 pour WPA et AES (Advanced Encryption Standard) pour WPA2. WPA2 est recommandé car il dispose d'une norme de cryptage plus puissante. Dans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



Étape 6. Saisissez 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.



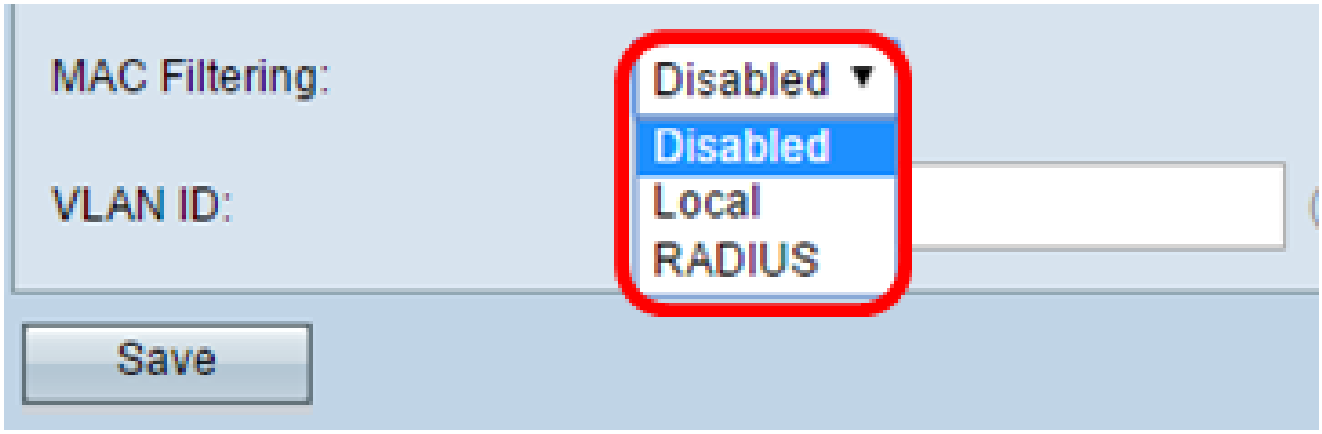
Étape 7. Saisissez le taux dans le champ Taux de rafraîchissement de la clé de diffusion. La fréquence d'actualisation de la clé de diffusion spécifie l'intervalle auquel la clé de sécurité est actualisée pour les clients associés à ce point d'accès. Le taux doit être compris entre 0 et 86400, la valeur 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 du point d'accès dans la liste déroulante Filtrage MAC. 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 des clients pouvant accéder au réseau en amont est limité aux clients spécifiés dans une liste d'adresses MAC définie localement.
- RADIUS : l'ensemble des clients pouvant accéder au réseau en amont est limité aux clients spécifiés dans une liste d'adresses MAC sur un serveur RADIUS.



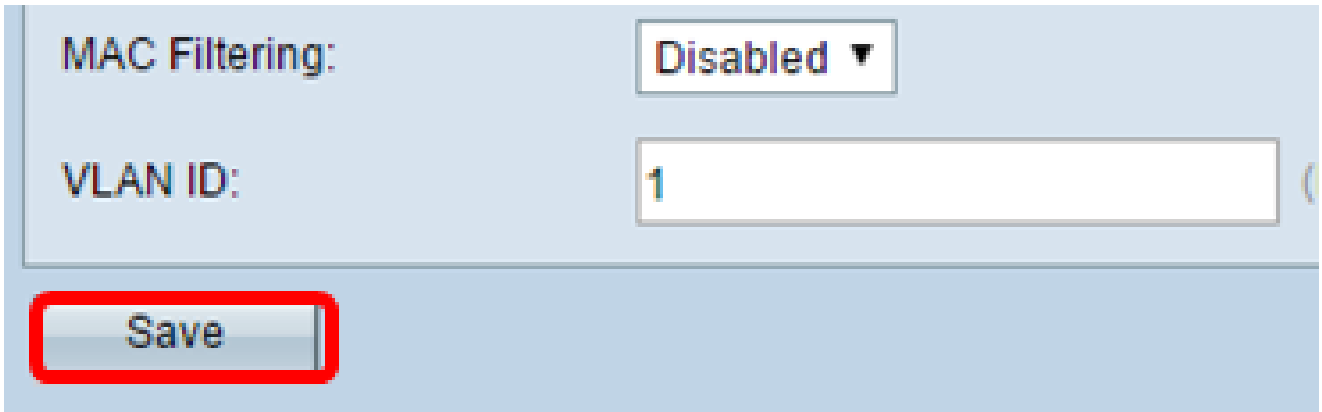
Remarque : pour cet exemple, Disabled est sélectionné.

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

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



Étape 10. Cliquez sur Save pour enregistrer vos modifications.



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

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.