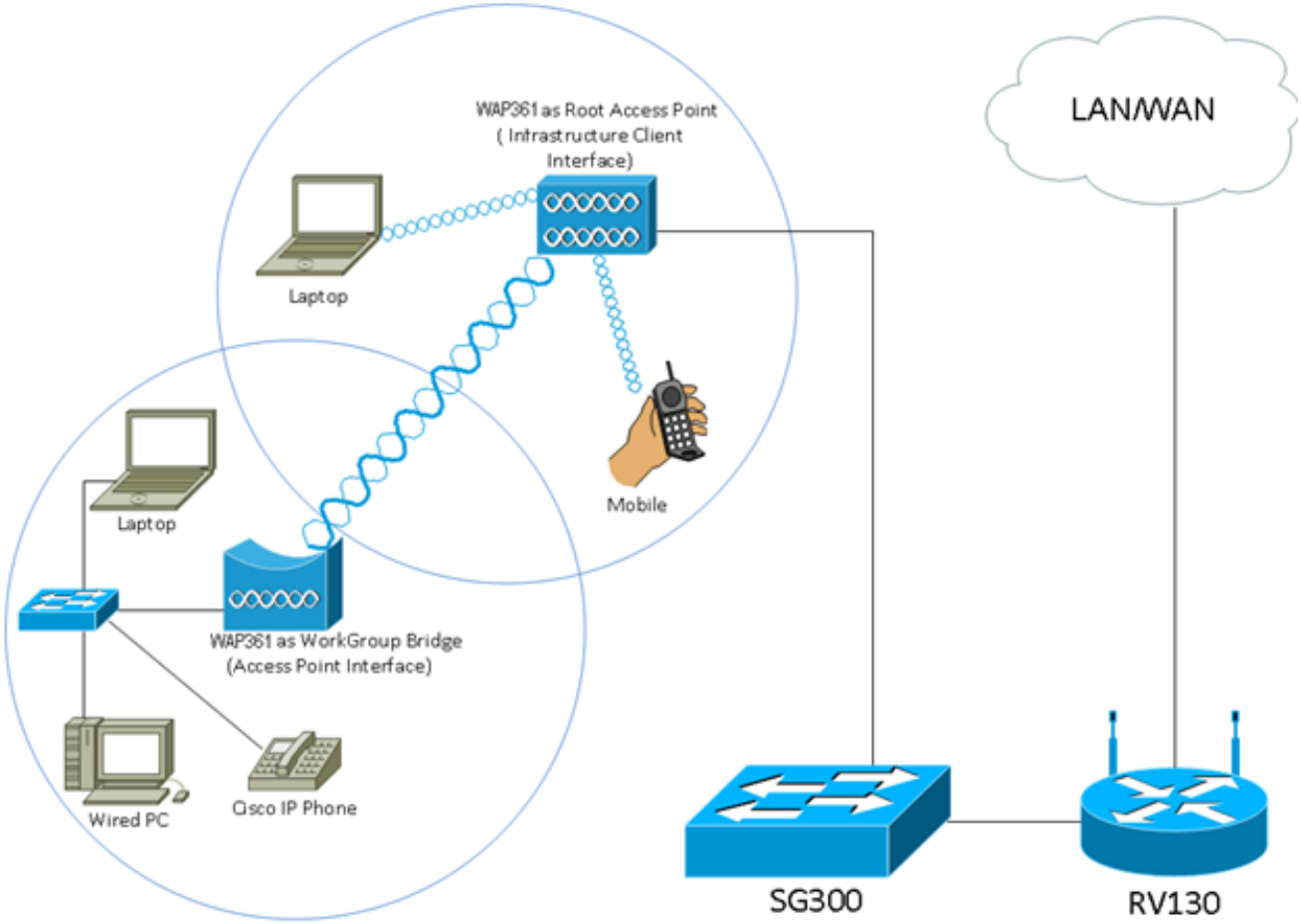
تكوين جسر مجموعة العمل على نقطة وصول لاسلكية (WAP)

الهدف

تتيح ميزة "جسر مجموعة العمل" لنقطة الوصول اللاسلكية (WAP) إمكانية توصيل حركة مرور البيانات بين عميل بعيد وشبكة المنطقة المحلية اللاسلكية (LAN) المتصلة بوضع جسر مجموعة العمل. يعرف جهاز WAP المرتبط بالواجهة البعيدة واجهة نقطة الوصول، بينما يعرف جهاز WAP المرتبط بشبكة LAN اللاسلكية واجهة بنية أساسية. يتيح جسر مجموعة العمل للأجهزة التي لها توصيلات سلكية فقط التوصيل بشبكة لاسلكية. يوصى بوضع جسر مجموعة العمل كبديل عندما تكون ميزة نظام التوزيع اللاسلكي (WDS) غير متوفرة.



ملاحظة: توضح المخطط أعلاه نموذج جسر مجموعة العمل. يتم ربط الأجهزة السلكية بمحول، يتصل بواجهة شبكة LAN الخاصة ب WAP. يعمل WAP كواجهة لنقطة الوصول، ويتصل بواجهة البنية الأساسية.

يهدف هذا المقال إلى شرح كيفية إنشاء جسر مجموعة العمل بين WAPs.

الأجهزة القابلة للتطبيق

- WAP100 Series
- WAP300 Series
- WAP500 Series

إصدار البرامج

- 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

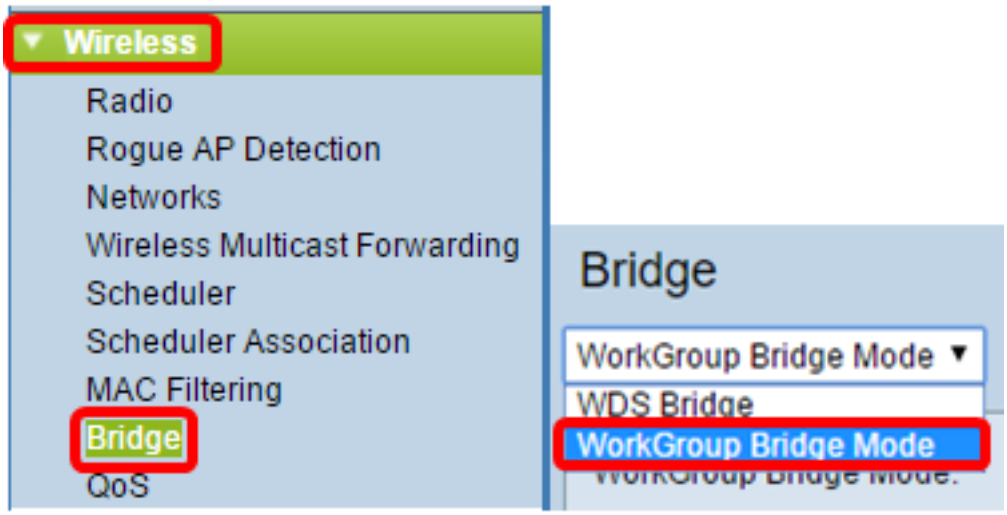
تكوين جسر مجموعة العمل

واجهة عميل Infrastructure

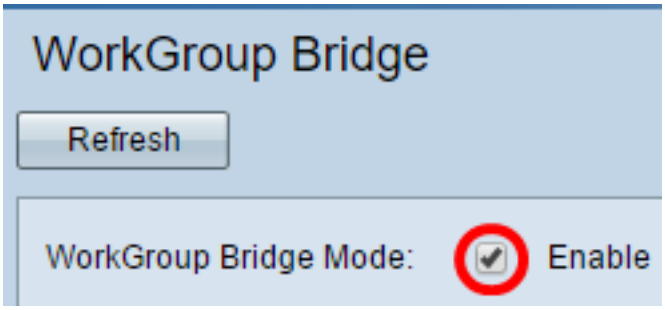
الخطوة 1. سجل الدخول إلى الأداة المساعدة المستندة إلى الويب في WAP واختر **لاسلكي > جسر مجموعة العمل**.

ملاحظة: قد تختلف خيارات القائمة حسب طراز الجهاز الذي تستخدمه. الصور التالية مأخوذة من WAP361 ما لم يذكر خلاف ذلك.

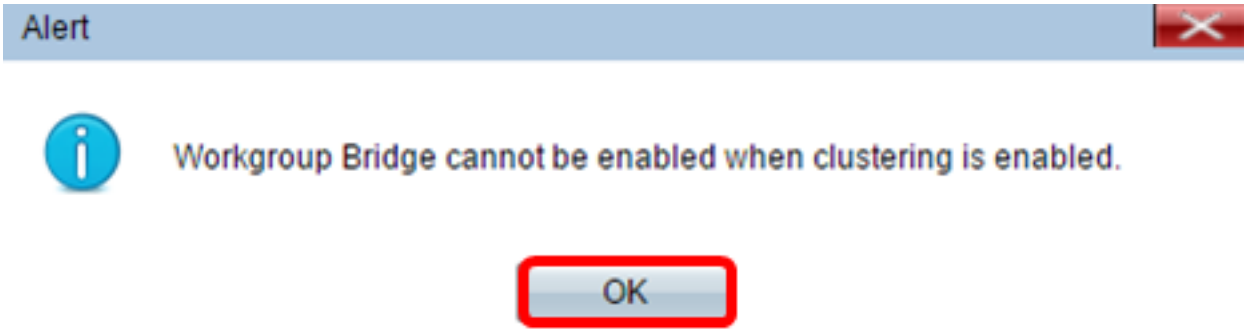
أخترت ل WAP571 و WAP571E، **لاسلكي > جسر > وضع جسر مجموعة العمل**.



الخطوة 2. حدد خانة الاختيار **تمكين** وضع جسر مجموعة العمل.

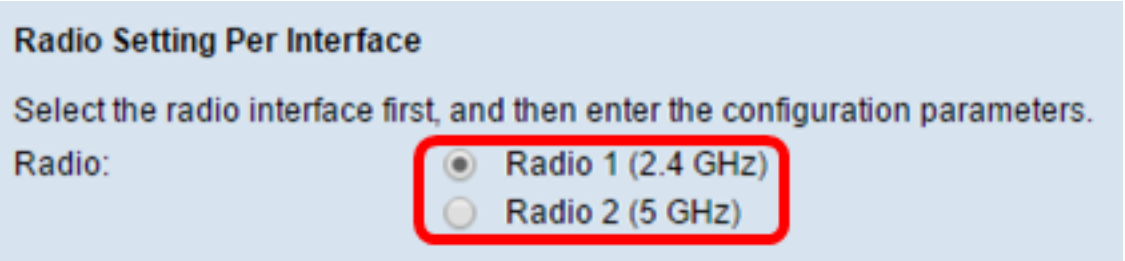


ملاحظة: إذا تم تمكين التجميع على WAP، سيخبرك أحد الإطارات المنبثقة بتعطيل التجميع من أجل عمل جسر مجموعة العمل. انقر فوق **موافق"** للمتابعة. لإيقاف إتاحة التجميع، أختر **إعداد نقطة واحدة** من لوحة التصفح ثم أختر **نقاط الوصول > إيقاف إعداد نقطة واحدة**.



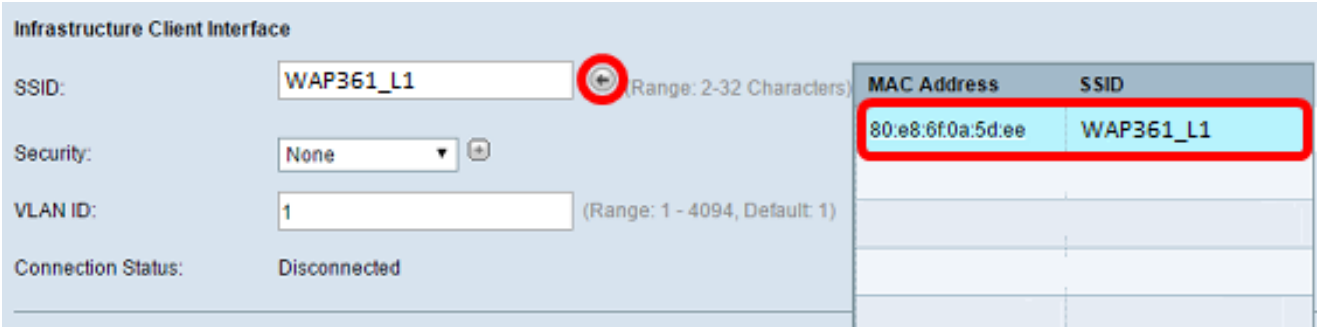
الخطوة 3. انقر فوق واجهة الراديو لجسر مجموعة العمل. عندما تقوم بتكوين أحد الموجهات اللاسلكية كجسر مجموعة عمل، فإن الراديو الآخر يظل يعمل. تتوافق واجهات الراديو مع نطاقات التردد اللاسلكي في WAP. إن WAP مجهز للبث على واجهتي راديو مختلفتين. لن يؤثر تكوين إعدادات لواجهة راديو على الأخرى. قد تختلف خيارات واجهة الراديو حسب نموذج WAP. تظهر بعض نقاط الوصول WAP الراديو 1 على أنه 2. 4 جيجاهيرتز، بينما يكون بعضها ضمن نطاق الراديو 2. 4 جيجاهيرتز.

ملاحظة: هذه الخطوة خاصة فقط بالنقاط WAP التالية ذات النطاق المزدوج: WAP131، WAP150، WAP571E، WAP571، WAP561، WAP371، WAP361، WAP351. على سبيل المثال، يتم إختيار راديو 1.



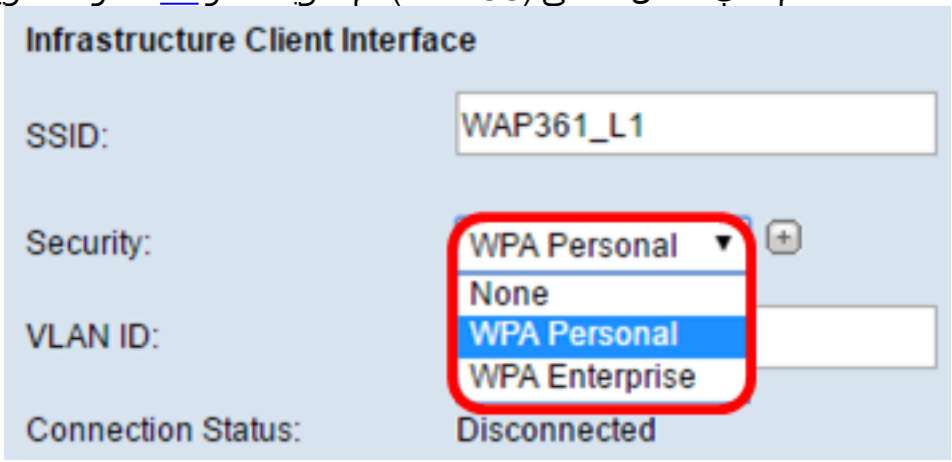
الخطوة 4. أدخل اسم معرف مجموعة الخدمة (SSID) في حقل *SSID* أو انقر فوق زر السهم الموجود بجانب الحقل لإجراء المسح بحثا عن الجيران. يعمل هذا كاتصال بين الجهاز والعميل البعيد. يمكنك إدخال من 2 إلى 32 حرفا لمعرف SSID لعميل البنية الأساسية.

ملاحظة: من المهم تمكين اكتشاف نقاط الوصول المخادعة. لمعرفة المزيد حول كيفية تمكين الميزة المذكورة، انقر هنا. على سبيل المثال، يتم النقر فوق زر السهم لاختيار WAP361_L1 كمعرف SSID لواجهة عميل البنية الأساسية.



الخطوة 5. في منطقة "واجهة عميل البنية الأساسية"، أختر نوع الأمان المراد مصادقته كمحطة عميل على جهاز WAP للتدفق من القائمة المنسدلة أمان. الخيارات هي:

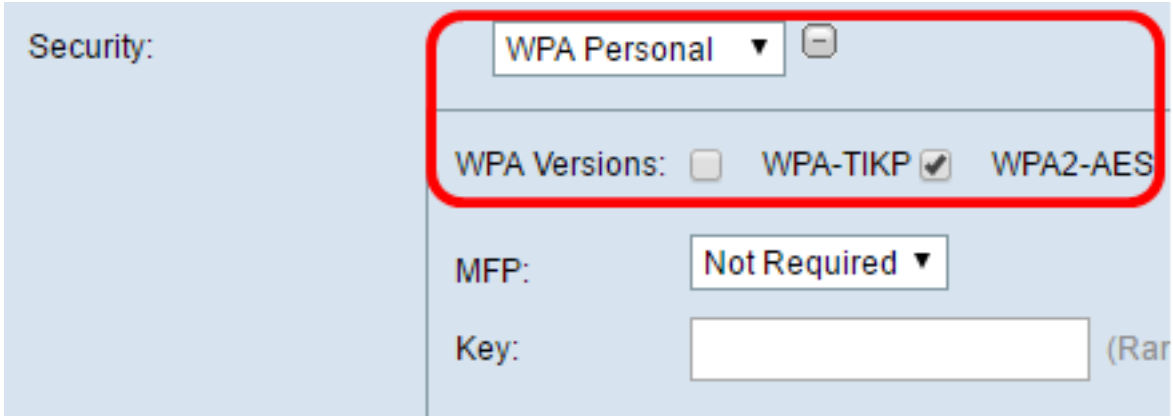
- لا شيء — تأمين مفتوح أو بلا. هذا هو الإعداد الافتراضي. إذا تم إختيار هذا الخيار، فقم بالتخطي إلى الخطوة 18.
- WPA شخصي — يمكن WPA شخصي دعم مفاتيح طولها 8-63 حرفا. يوصى باستخدام معيار WPA2 لأنه يحتوي على معيار تشفير أكثر فعالية. تخطي الخطوة 6 للتكوين.
- WPA Enterprise — WPA Enterprise أكثر تقدما من WPA Personal وهو التأمين الموصى به للمصادقة. وهو يستخدم بروتوكول المصادقة المتوسع المحمي (PEAP) وأمان طبقة النقل (TLS). تخطي الخطوة 9 للتكوين. غالبا ما يتم إستخدام هذا النوع من الأمان في بيئة مكتب ويحتاج إلى خادم خدمة مصادقة عن بعد لمستخدم طلب اتصال هاتفي (RADIUS) تم تكوينه. انقر هنا لمعرفة المزيد حول خوادم RADIUS.



ملاحظة: في هذا المثال، يتم إختيار WPA Personal.

الخطوة 6. انقر فوق + وحدد خانة الاختيار WPA-TKIP أو WPA2-AES لتحديد نوع تشفير WPA الذي ستستخدمه واجهة عميل البنية الأساسية.

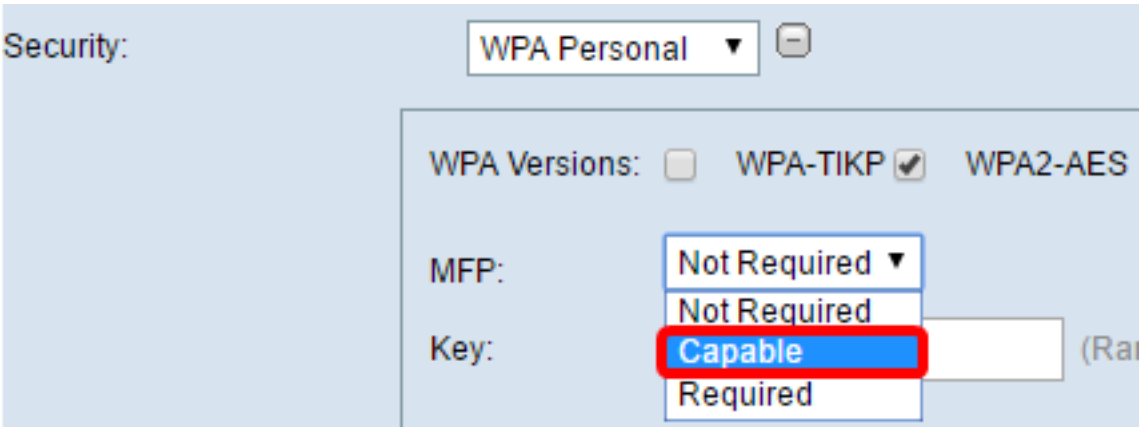
ملاحظة: إذا كانت جميع المعدات اللاسلكية الخاصة بك تدعم WPA2، فقم بتعيين أمان عميل البنية الأساسية على WPA2-AES. أسلوب التشفير هو RC4 ل WPA ومعيار التشفير المتقدم (AES) ل WPA2. يوصى باستخدام معيار WPA2 لأنه يحتوي على معيار تشفير أكثر فعالية. على سبيل المثال، يتم إستخدام WPA2-AES.



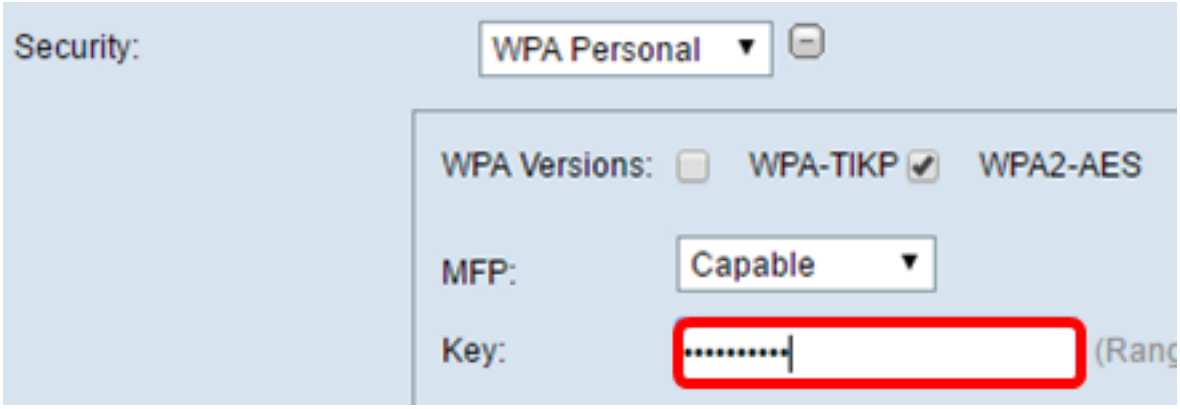
خطوة 7. (إختياري) إذا فحصت WPA2-AES في خطوة 6، أختر خيار من الإدارة إطار حماية (MFP) قائمة منسدلة إذا أنت تريد أن ال WAP أن يتطلب أن يتلقى إطار محمي أو لا. لمعرفة المزيد حول MFP، انقر هنا. الخيارات هي:

- غير مطلوب — تعطيل دعم العميل ل MFP.
- إمكانية — تسمح لكل من الأجهزة القابلة للتوصيل متعدد الطبقات (MFP) والعملاء الذين لا يدعمون MFP بالانضمام إلى الشبكة. هذا هو إعداد MFP الافتراضي على WAP.
- مطلوب - لا يسمح للعملاء بالاقتران إلا إذا تم التفاوض على MFP. إذا كانت الأجهزة لا تدعم MFP، لا يسمح لها بالانضمام إلى الشبكة.

ملاحظة: على سبيل المثال، يتم إختيار قادر.



الخطوة 8. أدخل مفتاح تشفير WPA في حقل *المفتاح*. يجب أن يتراوح طول المفتاح بين 8 و 63 حرفا. هذه تركيبة من الحروف، الأرقام، والحروف الخاصة. هي كلمة المرور التي تستخدم لأول مرة عند التوصيل بالشبكة اللاسلكية. ثم، تخطي الخطوة 18.



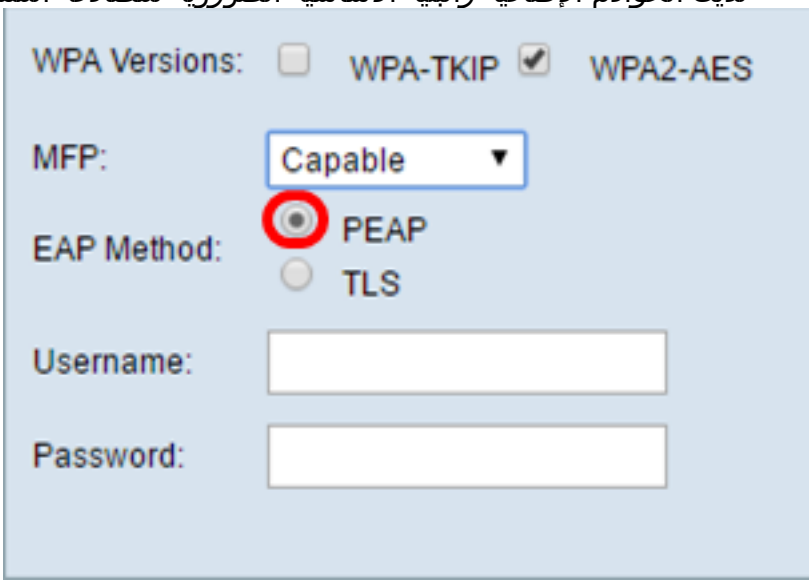
الخطوة 9. إذا أخترت WPA مؤسسي في خطوة 5، انقر زر انتقاء لطريقة EAP.

يتم تحديد الخيارات المتاحة على النحو التالي:

- PEAP — يعطي هذا البروتوكول كل مستخدم لاسلكي تحت WAP أسماء المستخدمين وكلمات المرور الفردية

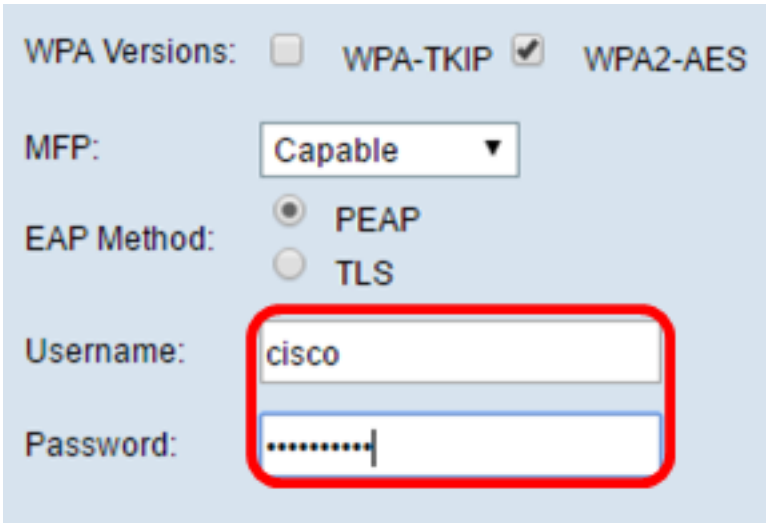
التي تدعم معايير التشفير AES. بما أن PEAP هو أسلوب تأمين قائم على كلمة المرور، فإن تأمين Wi-Fi يعتمد على مسوغات الجهاز الخاصة بالعميل. يمكن أن يشكل PEAP خطرا أمنيا خطيرا إن كان لديك كلمات مرور ضعيفة أو عملاء غير آمنين. ويعتمد على TLS ولكنه يتجنب تثبيت الشهادات الرقمية على كل عميل. وبدلا من ذلك، فإنه يوفر المصادقة من خلال اسم مستخدم وكلمة مرور.

- TLS — يتطلب TLS أن يكون لكل مستخدم شهادة إضافية ليتم منحه حق الوصول. يكون TLS أكثر أمانا إذا كان لديك الخوادم الإضافية والبنية الأساسية الضرورية لمصادقة المستخدمين في شبكتك.



ملاحظة: على سبيل المثال، يتم إختيار PEAP.

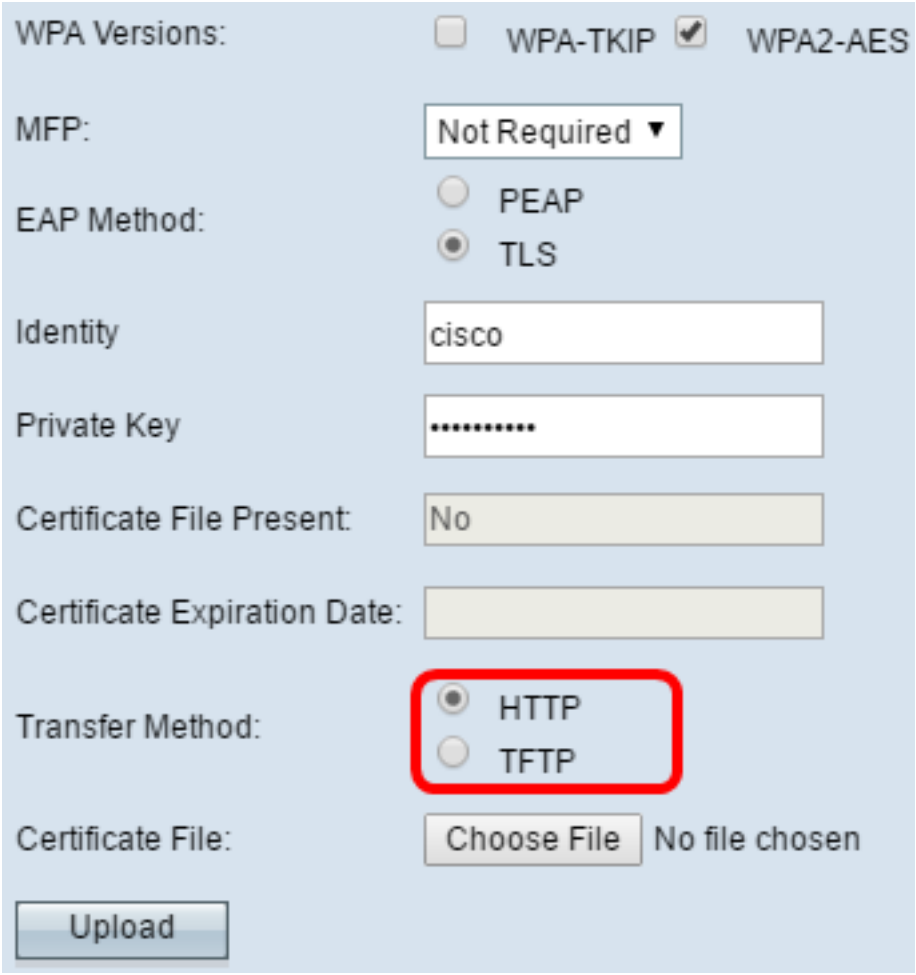
الخطوة 10. أدخل اسم المستخدم وكلمة المرور لعميل البنية الأساسية في حقلي *اسم المستخدم* وكلمة *المرور*. هذه هي معلومات تسجيل الدخول التي يتم إستخدامها للاتصال بواجهة عميل البنية الأساسية، ارجع إلى واجهة عميل البنية الأساسية لديك للعثور على هذه المعلومات. ثم، تخطى الخطوة 18.



الخطوة 11. إذا نقرت فوق TLS في الخطوة 9، فأدخل الهوية والمفتاح الخاص لعميل البنية الأساسية في حقلي *الهوية والمفتاح الخاص*.

الخطوة 12. في منطقة طريقة النقل، انقر زر انتقاء للخيارات التالية:

- TFTP — بروتوكول نقل الملفات المبسط (TFTP) هو إصدار مبسط غير آمن لبروتوكول نقل الملفات (FTP). ويتم إستخدامها بشكل أساسي لتوزيع البرامج أو الأجهزة المصادق عليها بين شبكات الشركات. إذا قمت بالنقر فوق TFTP، فقم بالتخطي إلى الخطوة 15.
- HTTP — يوفر بروتوكول نقل النص التشعبي (HTTP) إطار عمل مصادقة بسيط لاستجابة التحدي يمكن إستخدامه من قبل العميل لتوفير إطار عمل المصادقة.



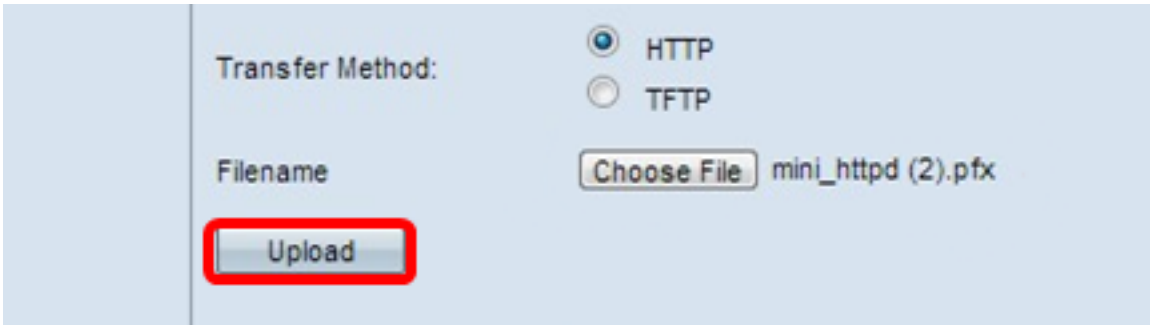
ملاحظة: إذا كان ملف الشهادة موجودا بالفعل على WAP، فسيتم ملء حقلي *ملف الشهادة* الحالي و*تاريخ انتهاء صلاحية الشهادة* بالمعلومات ذات الصلة. وإلا فإنها ستكون فارغة.

HTTP

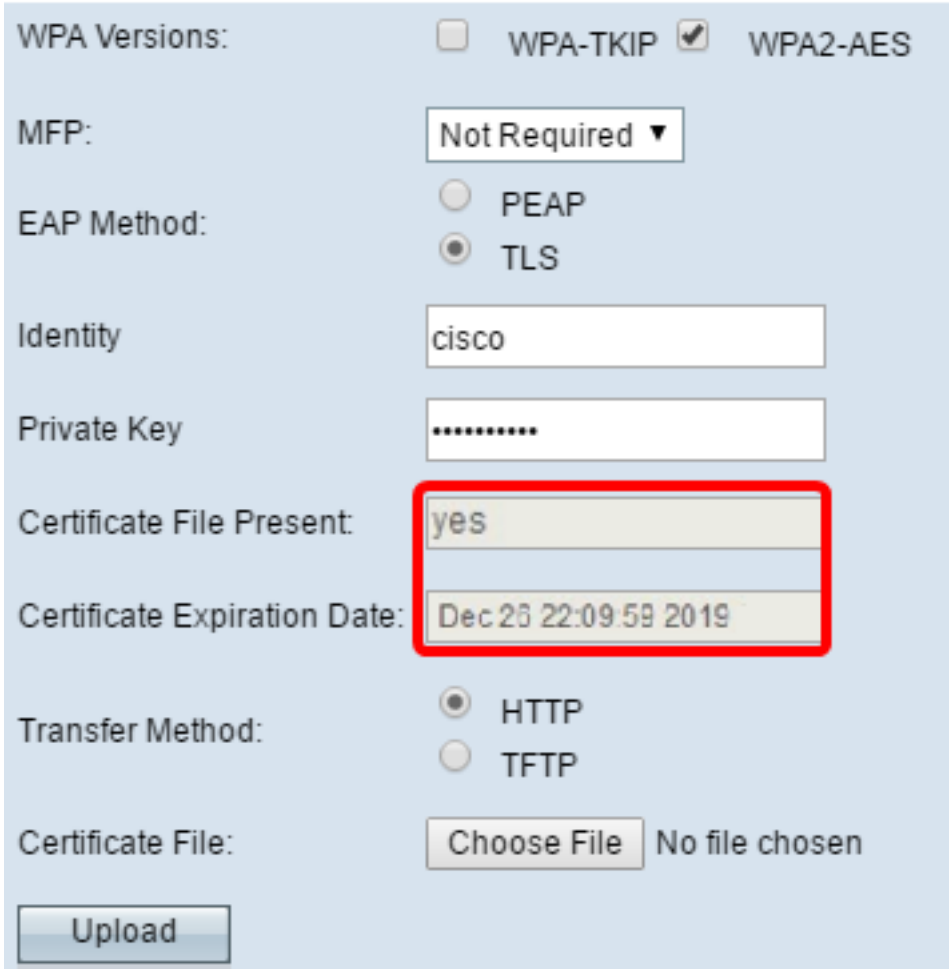
الخطوة 13. انقر زر **إختيار ملف** للعثور على ملف ترخيص وتحديده. يجب أن يحتوي الملف على ملحق ملف الشهادة المناسب (مثل .pem أو .pfx) وإلا فلن يتم قبول الملف.

ملاحظة: في هذا المثال، يتم إختيار mini_httpd(2).pfx.

الخطوة 14. انقر على **تحميل** لتحميل ملف الشهادة المحدد. تخطي الخطوة 18.



سيتم تحديث حقلي *ملف الشهادة الموجود* و*تاريخ انتهاء الشهادة* تلقائيا.



TFTP

الخطوة 15. إذا نقرت TFTP في الخطوة 12، أدخل اسم الملف الخاص بملف الترخيص في حقل *اسم الملف*.

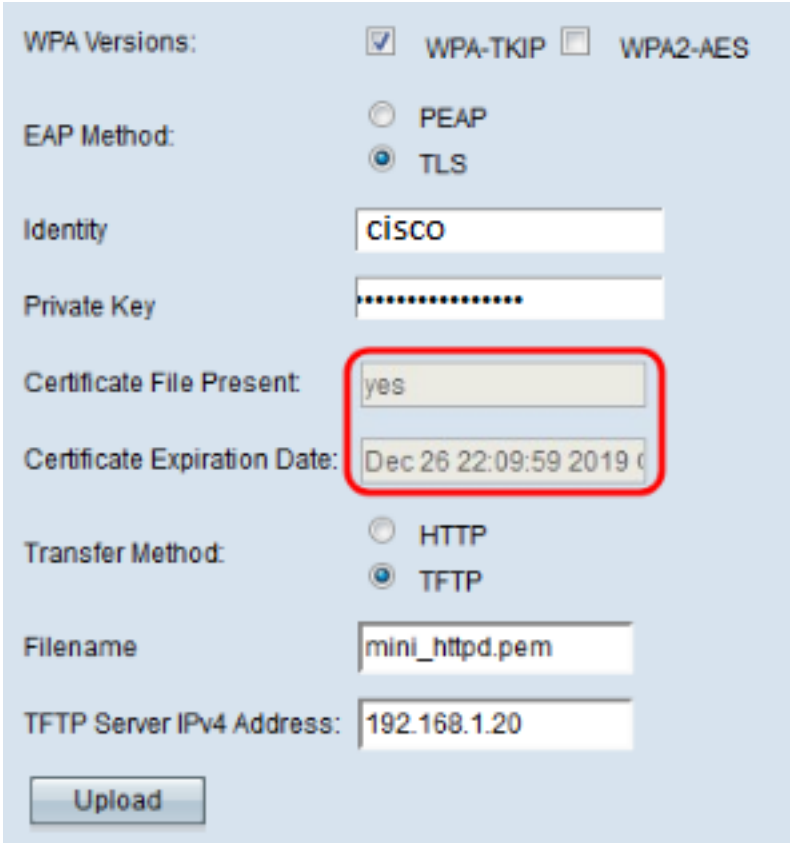
ملاحظة: في هذا المثال، يتم إستخدام mini_httpd.pem.

الخطوة 16. دخلت ال TFTP نادل عنوان في *ال TFTP نادل عنوان* مجال.

ملاحظة: في هذا المثال. يتم إستخدام 192.168.1.20 كعنوان خادم TFTP.

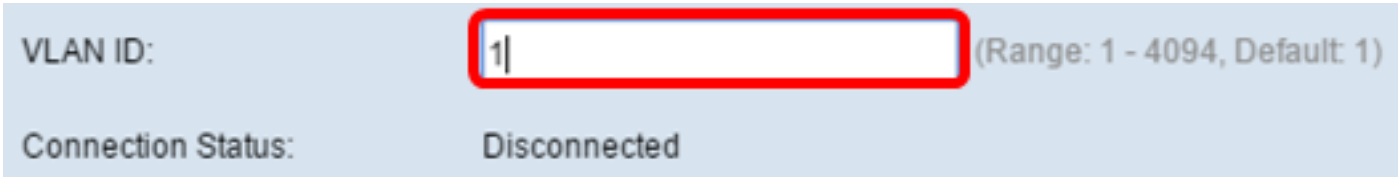
الخطوة 17. انقر على زر **تحميل** لتحميل ملف الشهادة المحدد.

سيتم تحديث حقلي *ملف الشهادة الموجود* و*تاريخ انتهاء الشهادة* تلقائيا.



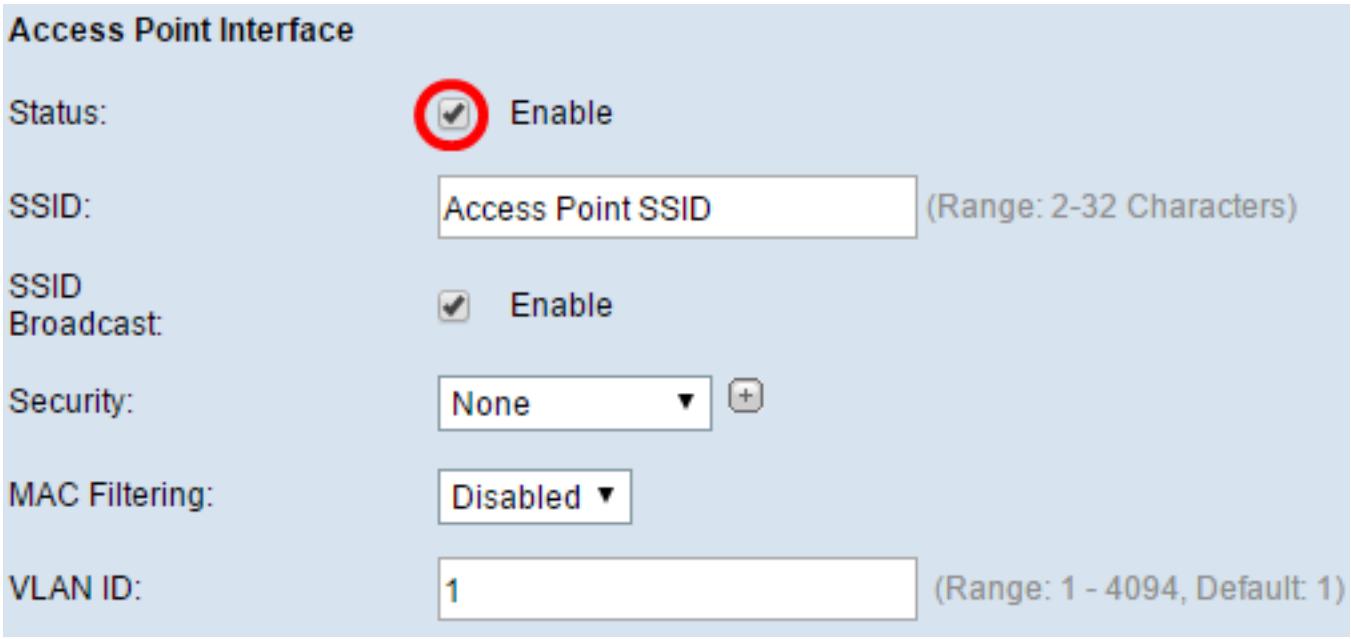
الخطوة 18. أدخل معرف VLAN لواجهة عميل البنية الأساسية. الافتراضي هو 1.

ملاحظة: لهذا المثال، يتم إستخدام معرف شبكة VLAN الافتراضي.



واجهة نقطة الوصول

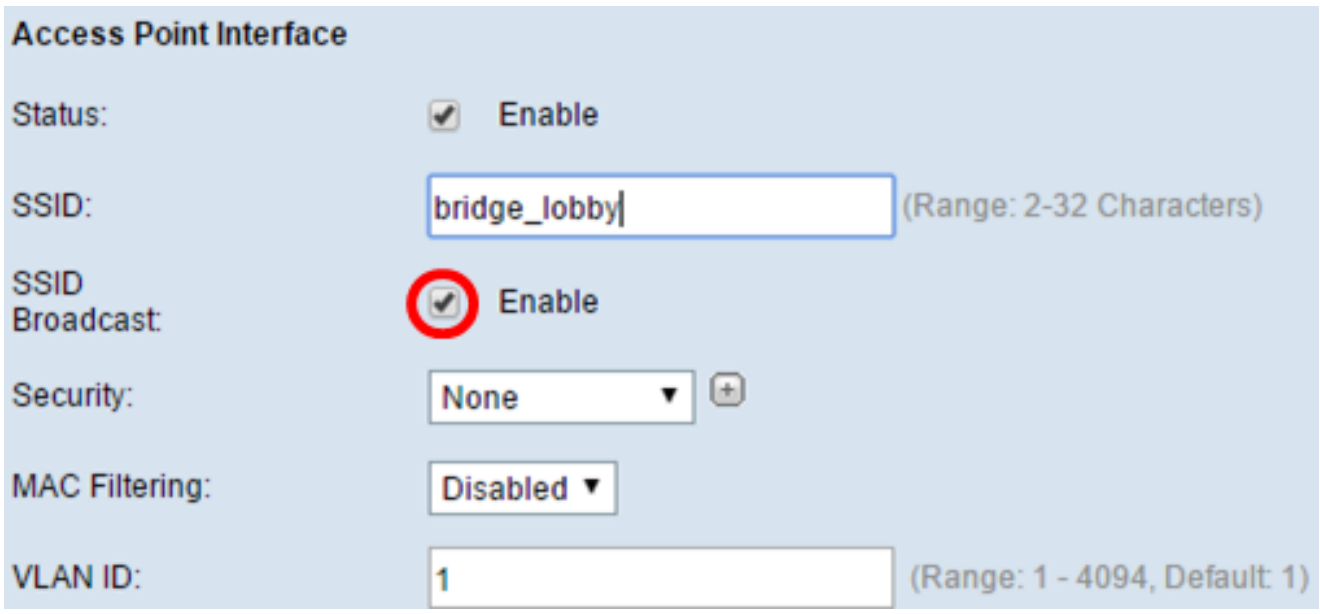
الخطوة 1. حدد خانة الاختيار **تمكين** الحالة لتمكين التوصيل على واجهة نقطة الوصول.



الخطوة 2. أدخل SSID لنقطة الوصول في حقل *SSID*. يجب أن يتراوح طول SSID بين 2 و 32 حرفا. التقصير هو SSID لنقطة الوصول.

ملاحظة: على سبيل المثال، SSID المستخدم هو bridge_lobby.

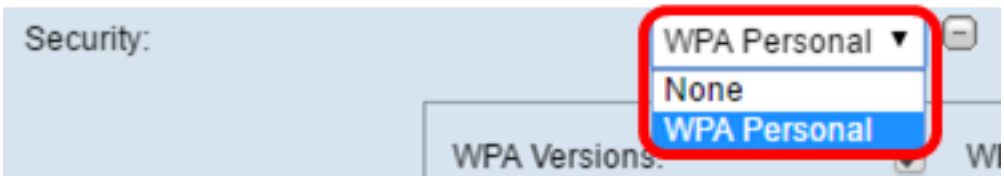
الخطوة 3. (إختياري) إذا كنت لا تريد بث SSID، فقم بإلغاء تحديد خانة الاختيار **تمكين** بث SSID. وبذلك تصبح نقطة الوصول غير مرئية بالنسبة لمن يبحثون عن نقاط وصول لاسلكية، ولا يمكن توصيلها إلا من خلال شخص يعرف مسبقا SSID. يتم تمكين بث SSID بشكل افتراضي.



الخطوة 4. أختر نوع الأمان لمصادقة محطات عميل تدفق البيانات من الخادم إلى WAP من القائمة المنسدلة أمان.

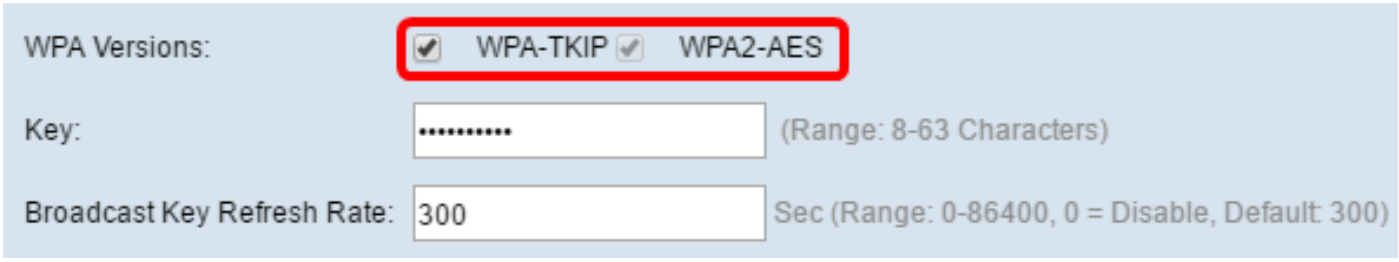
يتم تحديد الخيارات المتاحة على النحو التالي:

- بلا — فتح أو لا يوجد تأمين. هذه هي القيمة الافتراضية. تخطي الخطوة 10 إذا أخترت هذا.
- WPA شخصي — يمكن ل (Wi-Fi Protected Access (WPA الشخصي دعم مفاتيح يتراوح طولها من 8 إلى 63 حرفا. أسلوب التشفير هو إما TKIP أو وضع التشفير العكسي مع بروتوكول مصادقة رمز رسالة تقسيم الكتلة (CCMP). يوصى باستخدام WPA2 مع CCMP لأنه يحتوي على معيار تشفير أكثر قوة، وهو معيار التشفير المتقدم (AES)، مقارنة ببروتوكول سلامة المفاتيح المؤقتة (TKIP) الذي يستخدم معيار 64 بت فقط RC4.

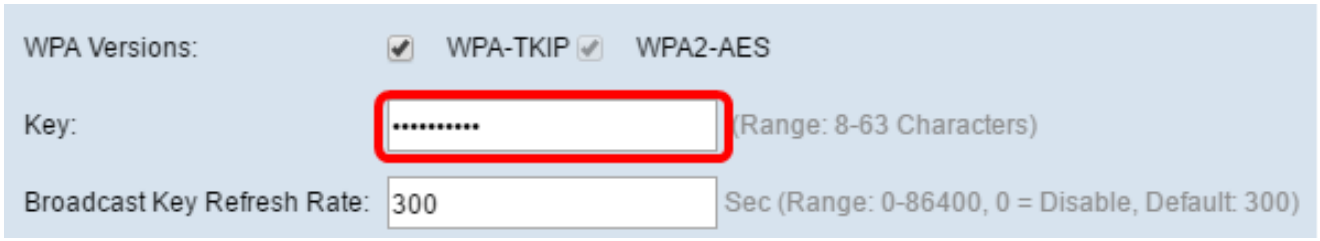


الخطوة 5. حدد خانة الاختيار **WPA-TKIP** أو **WPA2-AES** لتحديد نوع تشفير WPA الذي ستستخدمه واجهة نقطة الوصول. هذا مكنت افتراضيا.

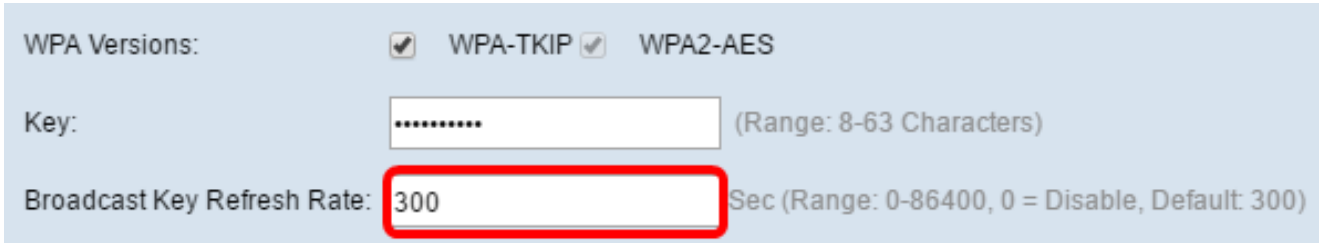
ملاحظة: إذا كانت جميع المعدات اللاسلكية الخاصة بك تدعم WPA2، فقم بتعيين أمان عميل البنية الأساسية على WPA2-AES. أسلوب التشفير هو RC4 ل WPA ومعيار التشفير المتقدم (AES) ل WPA2. يوصى باستخدام معيار WPA2 لأنه يحتوي على معيار تشفير أكثر فعالية. على سبيل المثال، يتم إستخدام WPA2-AES.



الخطوة 6. أدخل مفتاح WPA المشترك في حقل *المفتاح*. يجب أن يتراوح طول المفتاح بين 8 و 63 حرفا ويمكن أن يتضمن أحرف أبجدية رقمية وحروف كبيرة وأسفل ورموز خاصة.



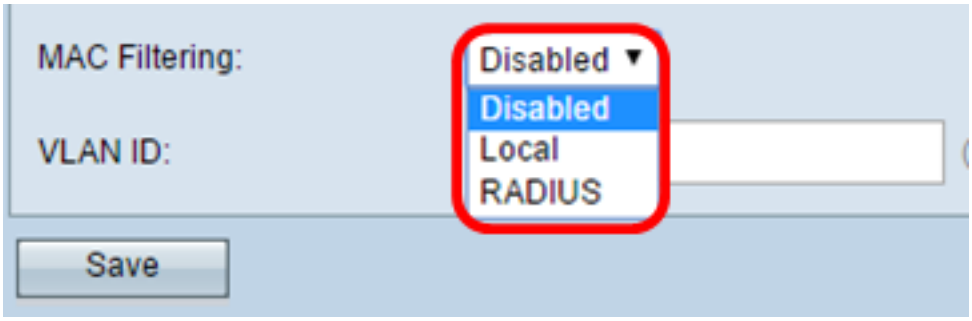
الخطوة 7. أدخل المعدل في حقل *تحديث مفتاح البث*. يحدد معدل تحديث مفتاح البث الفاصل الزمني الذي يتم فيه تحديث مفتاح الأمان للعملاء المقترنين بنقطة الوصول هذه. يجب أن يكون المعدل بين 0-86400، مع قيمة 0 لتعطيل الميزة. الافتراضي هو 300.



الخطوة 8. أختر نوع تصفية MAC الذي تريد تكوينه لواجهة نقطة الوصول من القائمة المنسدلة لتصفية MAC. عند تمكين هذا الخيار، يتم منح المستخدمين أو رفض الوصول إلى WAP استنادا إلى عنوان MAC الخاص بالعميل الذي يستخدمونه.

يتم تحديد الخيارات المتاحة على النحو التالي:

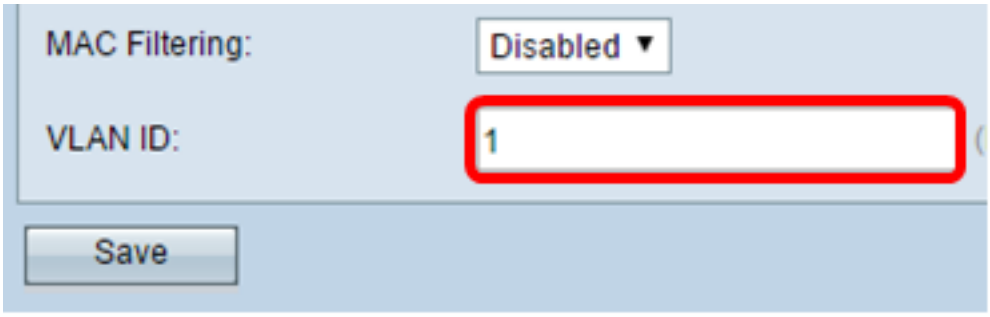
- معطل — يمكن لجميع العملاء الوصول إلى شبكة الخادم. هذه هي القيمة الافتراضية.
- محلي — قيدت مجموعة العملاء الذين يمكنهم الوصول إلى شبكة الخادم إلى العملاء المحددين في قائمة عناوين MAC المعرفة محليا.
- RADIUS — تقتصر مجموعة العملاء الذين يمكنهم الوصول إلى شبكة الخادم على العملاء المحددين في قائمة عناوين MAC على خادم RADIUS.



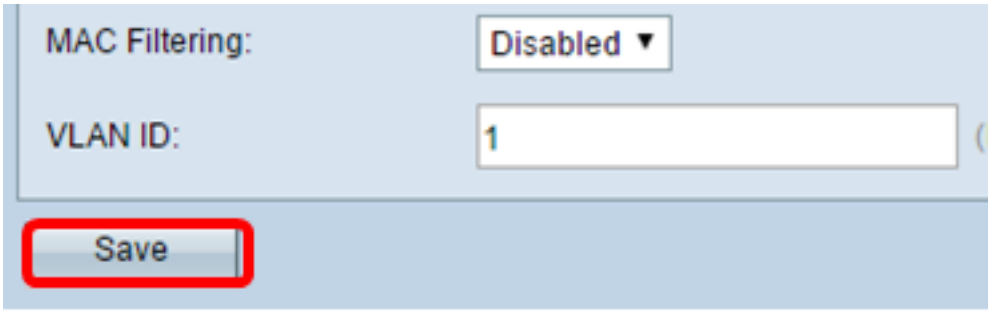
ملاحظة: على سبيل المثال، يتم إختيار "معطل".

الخطوة 9. أدخل معرف شبكة VLAN في حقل *معرف شبكة VLAN* لواجهة نقطة الوصول.

ملاحظة: للسماح بجسر الحزم، يجب أن يتطابق تكوين شبكة VLAN لواجهة نقطة الوصول والواجهة السلكية مع تكوين واجهة عميل البنية الأساسية.



الخطوة 10. انقر فوق **حفظ** لحفظ التغييرات.



يجب أن تكون قد انتهيت الآن من تكوين جسر مجموعة عمل بنجاح على نقطة وصول لاسلكية.

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).