إستخدام معالج الإعداد على WAP125 وأ WAP581

الهدف

معالج الإعداد هو ميزة مدمجة يمكنك إستخدامها لمساعدتك في التكوين الأولي لجهاز نقطة الوصول اللاسلكية (WAP). يسهل معالج الإعداد تكوين الإعدادات لتوفير إرشادات خطوة بخطوة.

يوضح هذا المستند كيفية تكوين WAP125 و WAP581 باستخدام معالج الإعداد على أداة تكوين الويب المساعدة.

لتكوين WAP باستخدام "معالج الإعداد" على جهاز محمول، انقر هنا.

الأجهزة القابلة للتطبيق

- WAP125
- WAP581

إصدار البرامج

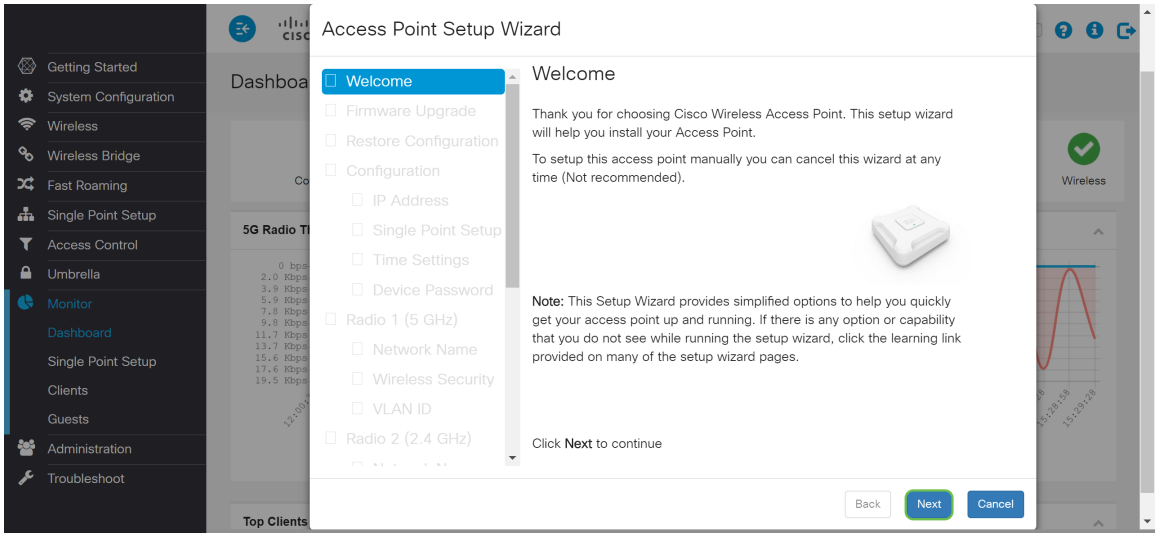
- 1.0.1.3

كيفية إستخدام معالج الإعداد

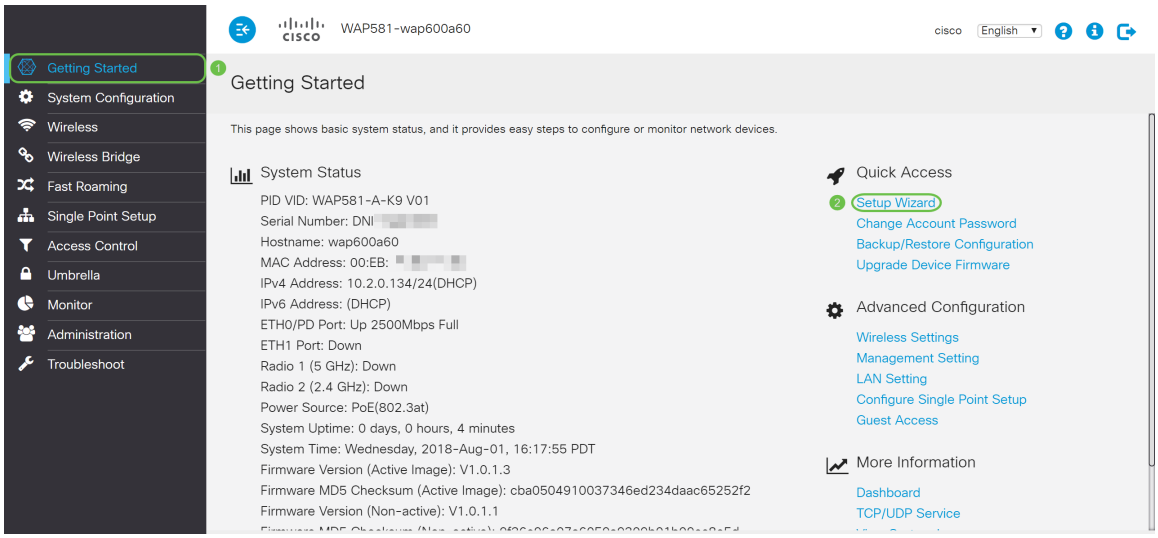
الخطوة 1. سجل الدخول إلى الأداة المساعدة لتكوين الويب في WAP الخاص بك من خلال إدخال عنوان IP الخاص ب WAP في مستعرض الويب الخاص بك. إن هذا هو أول مرة تأتي لك WAP، التقصير عنوان 192.168.1.254.

ملاحظة: يتم إستخدام WAP581 في هذا الدليل لإظهار معالج الإعداد. قد يختلف المظهر حسب النموذج.

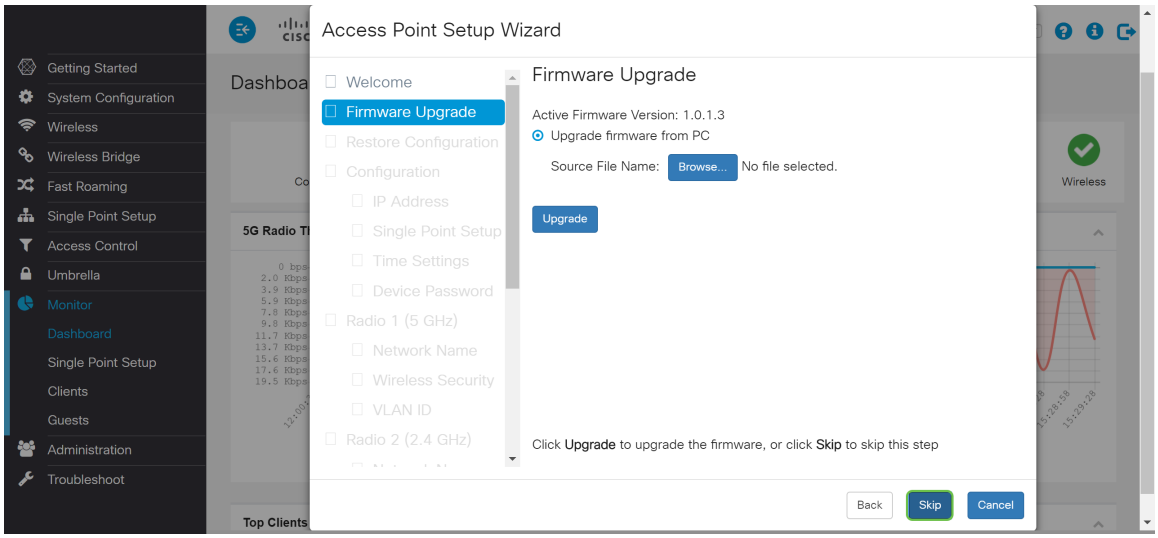
الخطوة 2. في أول مرة تقوم فيها بتسجيل الدخول إلى نقطة الوصول أو بعد إعادة ضبطها إلى إعدادات المصنع الافتراضية، يظهر *معالج إعداد نقطة الوصول*. انقر فوق **التالي** للمتابعة.



ملاحظة: إذا كان WAP الخاص بك تم تكوينه بالفعل لكنك ما زلت تريد الوصول إلى *معالج الإعداد*، انتقل إلى **بدء التشغيل > معالج الإعداد**. سوف يظهر إطار *معالج إعداد نقطة الوصول*.

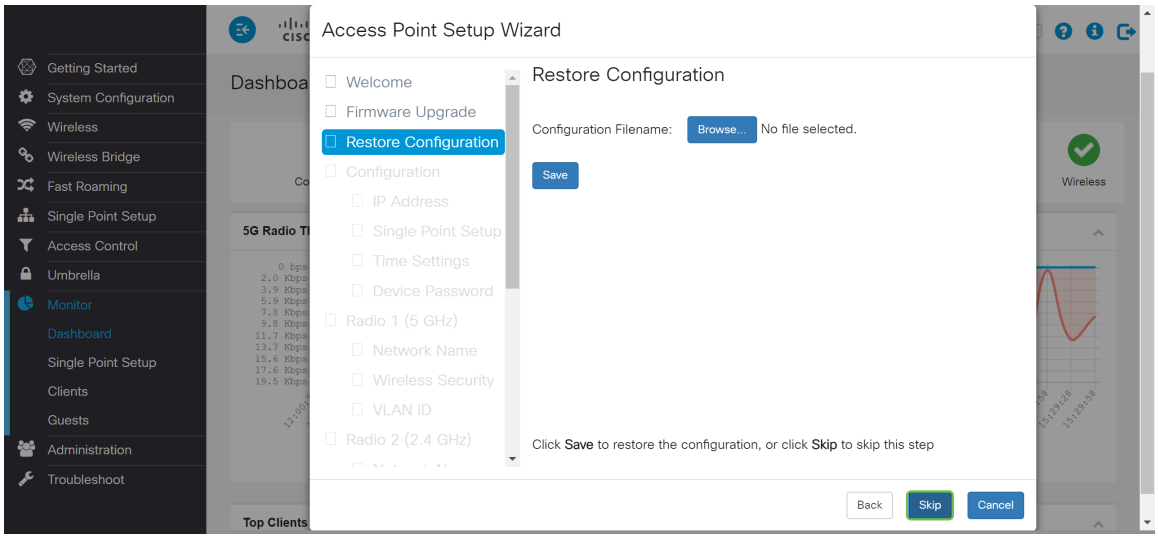


الخطوة 3. في إطار *ترقية البرامج الثابتة*، انقر فوق **إستعراض...** ثم حدد ملف البرامج الثابتة التي تريد الترقية إليها. ثم اضغط على **ترقية** للترقية إلى هذا البرنامج الثابت. بمجرد ترقية البرامج الثابتة، ستتم إعادة تشغيل الجهاز تلقائيا ومباشرة إلى صفحة تسجيل الدخول. في هذا المثال، سنقوم بالنقر فوق **Skip** نظرا لوجود إصدار البرامج الثابتة الذي نريده.



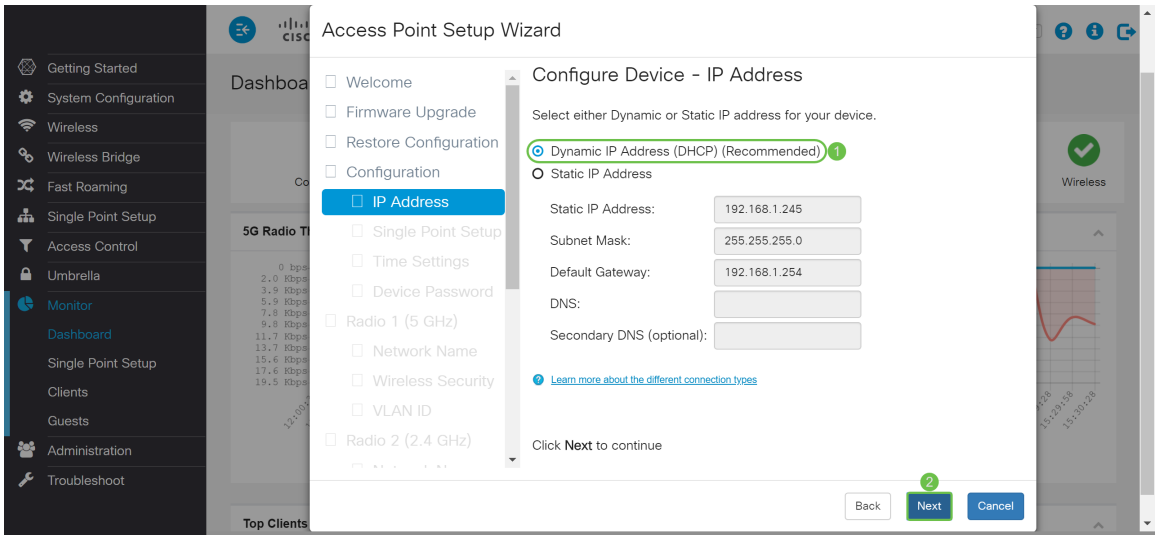
الخطوة 4. إذا كان لديك تكوين سابق تريد تطبيقه على الجهاز، فانقر فوق **إستعراض...** زر في نافذة *إستعادة تشكيل* وحدد التشكيل مبرد أن أنت تريد أن يطبق. ثم انقر فوق **حفظ** لتطبيق ملف التكوين على الجهاز. في هذا المثال، سننقر على **تخطي**.

ملاحظة: عندما يطبق الجهاز التكوين المناسب، فإنه سيعيد التمهيد ويوجهك إلى صفحة تسجيل الدخول.



الخطوة 5. في نافذة *تكوين الجهاز - عنوان IP*، حدد **عنوان IP الديناميكي (DHCP) (مستحسن)** للحصول على عنوان IP من خادم بروتوكول التكوين الديناميكي للمضيف (DHCP)، أو انقر فوق **عنوان IP الثابت** لتكوين عنوان IP يدويا. ثم انقر فوق **التالي** للمتابعة إلى القسم التالي. يوفر DHCP معلمات التكوين لمضيفي الإنترنت. في هذه الحالة، يقوم بروتوكول DHCP بتعيين عنوان IP لعميل لفترة محدودة من الوقت أو حتى يتخلى العميل عن العنوان بشكل صريح.

في هذا المثال، سنقوم بتحديد **عنوان IP الديناميكي (DHCP) (مستحسن)**.



الخطوة 6. يوفر إعداد نقطة واحدة طريقة مركزية لإدارة الخدمات اللاسلكية والتحكم فيها عبر أجهزة متعددة. سيتيح لك ذلك إنشاء مجموعة واحدة أو مجموعة واحدة من أجهزتك اللاسلكية يمكنك عرض الشبكة اللاسلكية ونشرها وتكوينها وتأمينها ككيان واحد. يمكن لإعداد نقطة واحدة المساعدة على تسهيل تخطيط القناة في خدمتك اللاسلكية لتقليل تداخل الراديو وزيادة عرض النطاق الترددي على شبكتك اللاسلكية إلى الحد الأقصى.

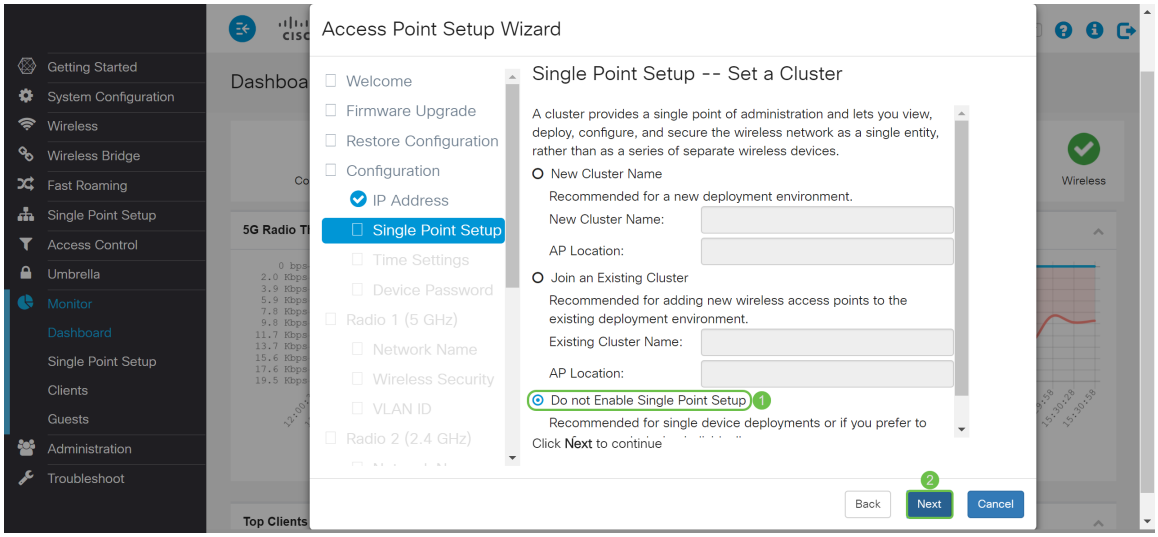
لإنشاء إعداد نقطة واحدة جديد لجهاز WAP، انقر فوق **اسم نظام مجموعة جديد** وحدد اسما جديدا. عندما تقوم بتكوين أجهزتك بنفس اسم نظام المجموعة وتمكن وضع إعداد النقطة المفردة على أجهزة WAP الأخرى، فإنها تنضم للمجموعة تلقائيا.

إذا كان لديك نظام مجموعة بالفعل على شبكتك، فيمكنك إضافة هذا الجهاز إليه بالنقر فوق **الانضمام إلى نظام مجموعة موجود**، ثم أدخل **اسم نظام المجموعة الموجود**. يقوم WAP بتكوين باقي الإعدادات استنادا إلى نظام المجموعة. انقر فوق **التالي** وقم بالتصديق على تأكيد الانضمام إلى نظام المجموعة. انقر فوق **إرسال** للانضمام إلى نظام المجموعة. بعد اكتمال التكوين، انقر فوق **إنهاء** للخروج من *معالج الإعداد*.

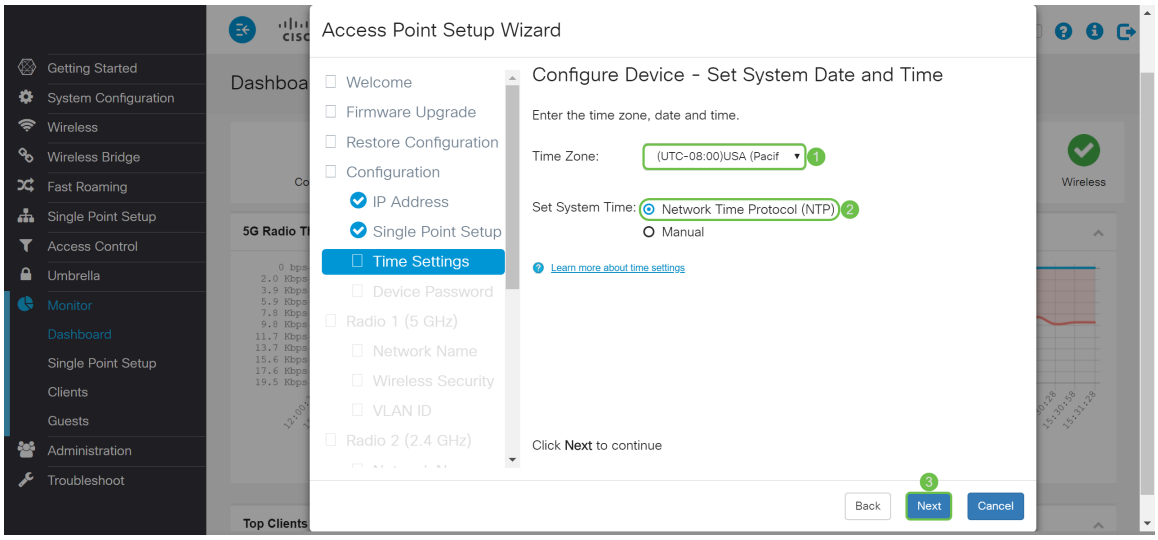
ملاحظة: يمكنك إدخال موقع نقطة الوصول في حقل **موقع نقطة الوصول** لتلاحظ الموقع الفعلي لجهاز WAP.

إذا كنت لا تريد أن يشارك هذا الجهاز في إعداد نقطة واحدة في هذا الوقت، انقر فوق **عدم تمكين إعداد نقطة واحدة**.

في هذا المثال، سنقوم بتحديد **عدم تمكين إعداد نقطة واحدة**. ثم انقر فوق **التالي** للاستمرار إلى القسم التالي.



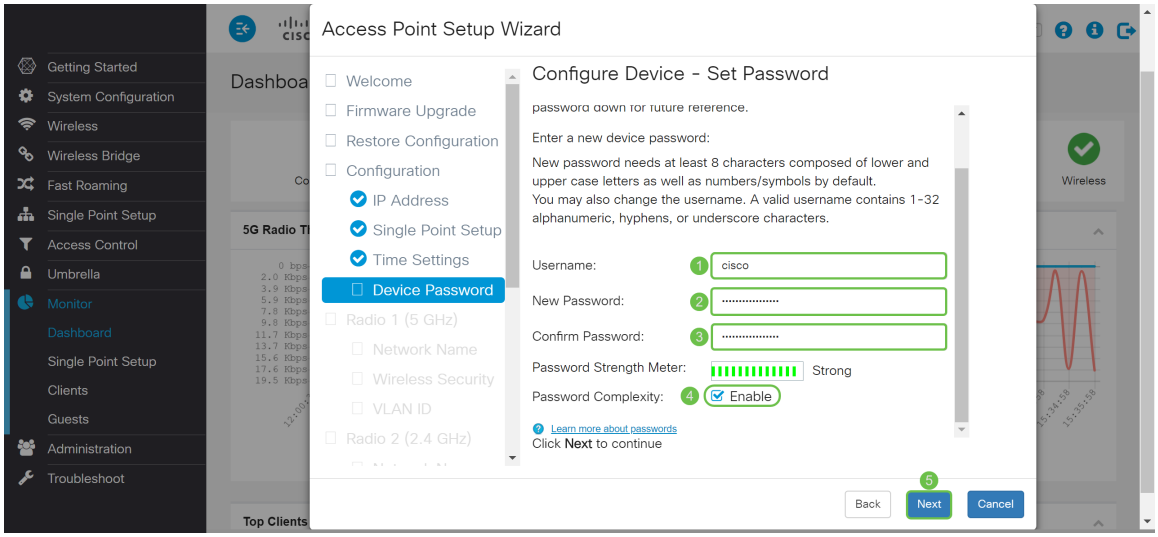
الخطوة 7. في نافذة *تكوين الجهاز - تعيين تاريخ النظام ووقته*، أختر **المنطقة الزمنية**، ثم حدد ما إذا كنت تريد أن يحصل وقت النظام لديك تلقائيا على إعداد الوقت من خادم **بروتوكول وقت الشبكة (NTP)** أو حدد **يدويا** لتكوين إعدادات الوقت يدويا. توفر ساعة النظام خدمة ختم الوقت المتزامن مع الشبكة لسجلات الرسائل. يمكن تكوين ساعة النظام يدويا أو كعميل NTP يحصل على بيانات النقر من خادم. انقر فوق **التالي** لمتابعة *معالج الإعداد*.



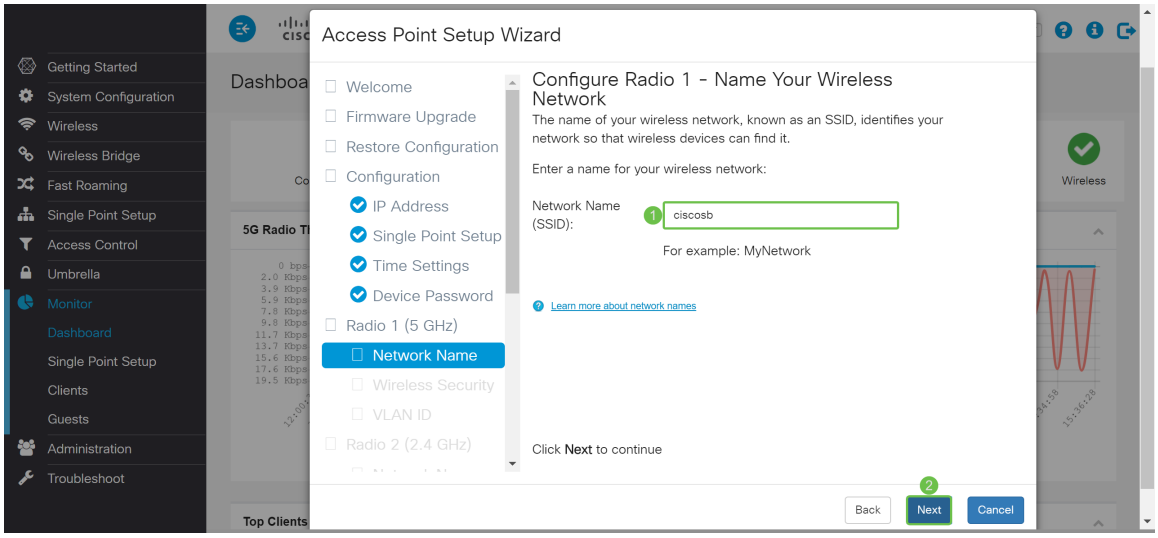
الخطوة 8. دخلت **username** جديد في *ال username* مجال، افتراضيا ال username يكون cisco. دخلت **كلمة جديد** ل *ال username*. بعد ذلك أدخل **كلمة المرور الجديدة** مرة أخرى في حقل *تأكيد كلمة المرور*. أنت يستطيع أن يلغي *تدقيق كلمة تعقيد* أن يعجز الكلمة أمن قاعدة. ومع ذلك، نوصي بشدة بتمكين قواعد أمان كلمة المرور. الكلمة جديد ينبغي طابقت إلى التالي تعقيد عملية إعداد:

- مختلف عن اسم المستخدم.
- مختلف من الكلمة حالي.
- تلقيت طول أدنى من ثمانية رمز.
- يحتوي على حروف من على الأقل فئة ثلاثة حروف (حروف كبيرة، حروف صغيرة، أرقام، وحروف خاصة متوفرة على لوحة مفاتيح قياسية).

ثم انقر على **التالي** لتكوين *الراديو 1*.



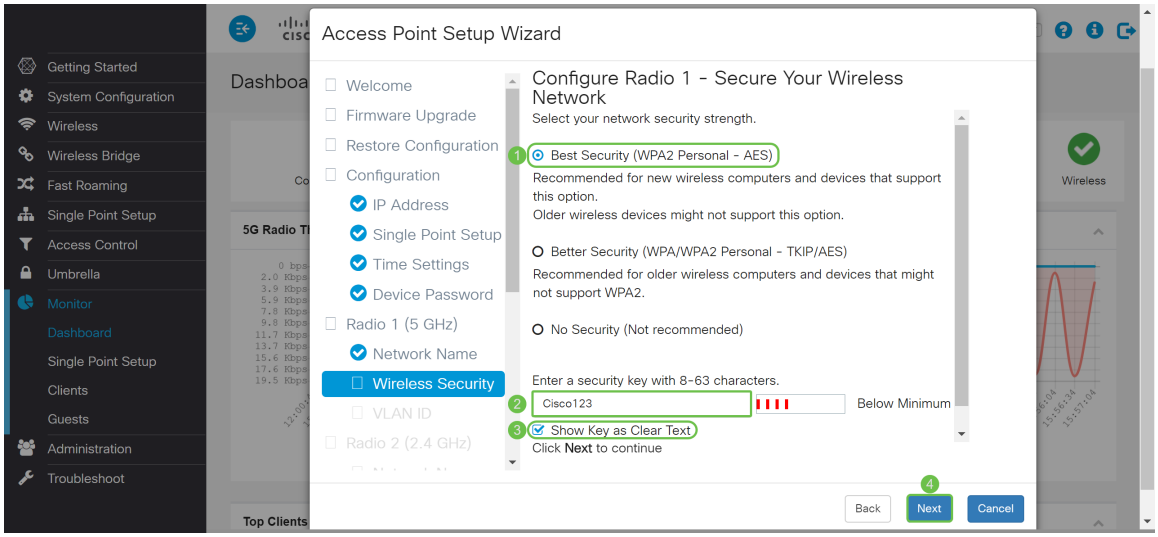
الخطوة 9. أدخل اسما للشبكة اللاسلكية في *اسم الشبكة (SSID)*. سيساعد ذلك في التعرف على الشبكة حتى تتمكن الأجهزة اللاسلكية من العثور عليها. افتراضيا، يتم إستخدام **CiscoSB** كاسم الشبكة. ثم انقر فوق **التالي** للاستمرار إلى القسم التالي.



الخطوة 10. انقر على زر الاختيار المطابق لأمان الشبكة الذي تريد تطبيقه على الشبكة اللاسلكية. ثم أدخل كلمة المرور لشبكتك في حقل *مفتاح الأمان*. لترى كلمة المرور وأنت تكتب، حدد خانة الاختيار **إظهار المفتاح كنص واضح**. انقر فوق **التالي** للمتابعة.

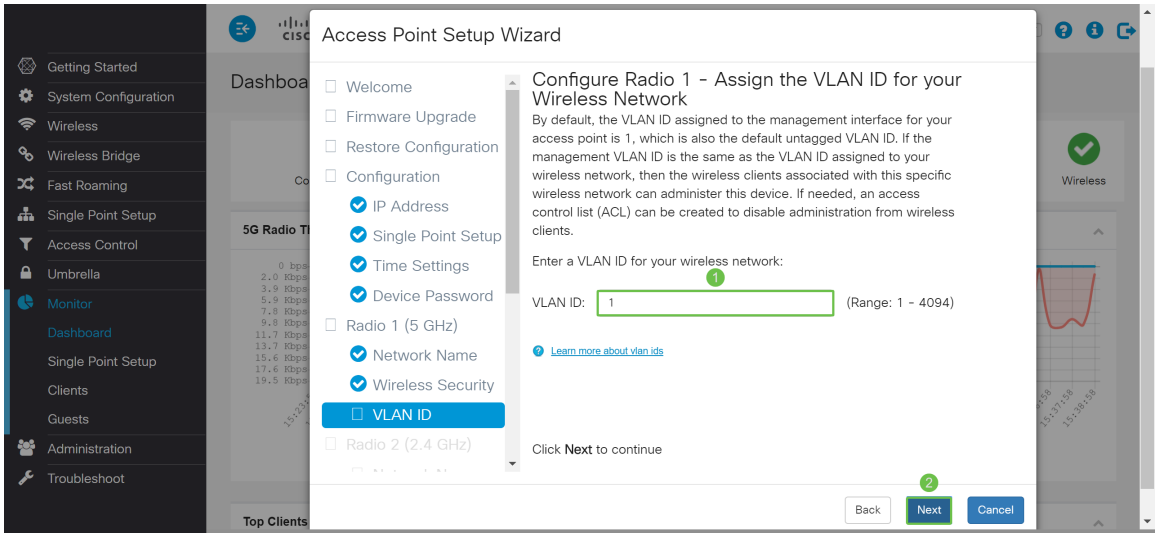
ملاحظة: إذا كانت الشبكة تحتوي على خليط من العملاء، يدعم بعضهم WPA2 ويدعم آخرون WPA الأصلي فقط، فحدد كلا (WPA/WPA2). يتيح ذلك لمحطات عملاء WPA و WPA2 الاقتران والمصادقة، لكنه يستخدم WPA2 الأكثر قوة للعميل الذي يدعمها. يتيح تكوين WPA هذا المزيد من قابلية التشغيل البيني بدلا من بعض التأمين.

- أفضل تأمين (Wi-Fi Protected Access 2 (WPA2) شخصي - معيار التشفير المتقدم (AES) تدعم جميع محطات العميل الموجودة على الشبكة خوارزمية التشفير القياسي WPA2 وخوارزمية التشفير المتقدم باستخدام وضع العداد مع بروتوكول تشفير تشفير كود مصادقة الرسائل (AES-CCMP) الخاص بربط مجموعات التشفير. وهذا يوفر أفضل مستوى أمان وفقا لمعايير IEEE 802.11i. طبقا لأحدث متطلبات تحالف Wi-Fi، يجب على نقطة الوصول دعم هذا الوضع طوال الوقت.
- أمان أفضل (WPA/WPA2 شخصي - WPA Personal (TKIP/AES هو مقياس Wi-Fi Alliance الذي يتضمن تشفير AES-CCMP و TKIP. يوفر التأمين عندما تكون هناك أجهزة لاسلكية قديمة تدعم WPA الأصلي لكنها لا تدعم WPA2 الأحدث.
- لا يوجد أمان (غير مستحسن) لا تتطلب الشبكة اللاسلكية كلمة مرور ويمكن لأي شخص الوصول إليها.

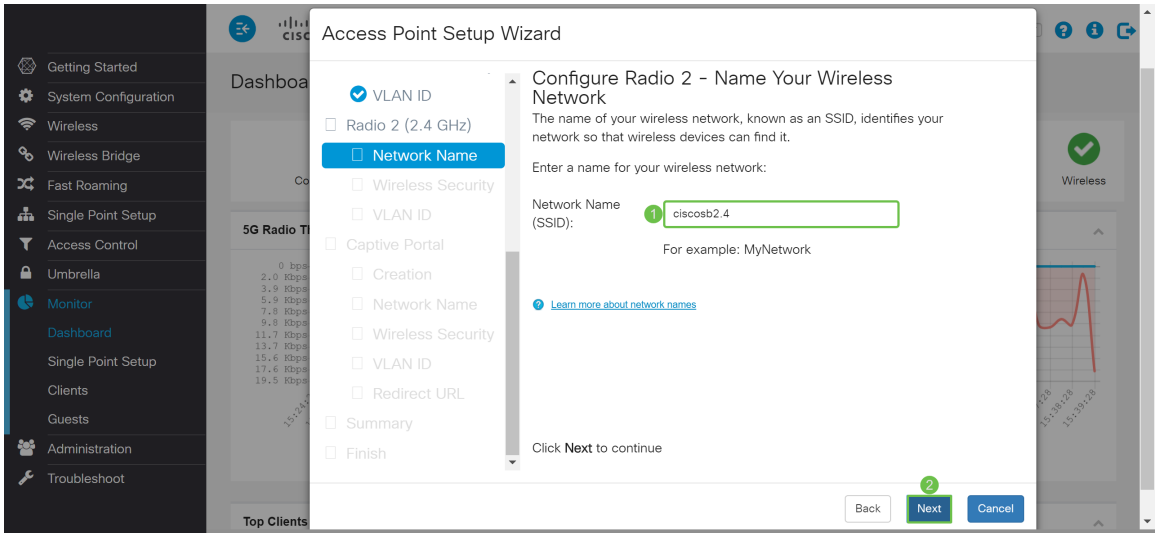


الخطوة 11. في حقل *معرف شبكة VLAN*، أدخل رقم معرف شبكة VLAN التي تريد أن ينتمي إليها *الراديو 1 (5 جيجاهرتز)*. في هذا المثال، سنترك *معرف شبكة VLAN* باسم 1. طقطقت **بعد ذلك** أن يشكل *لاسلكي 2 (2. 4 جيجاهيرتز)*.

ملاحظة: نوصي بتعيين معرف VLAN مختلف من الافتراضي (1) إلى حركة مرور البيانات اللاسلكية، لفصلها عن حركة مرور الإدارة على شبكة VLAN رقم 1. انقر هنا لمعرفة المزيد حول نقاط الوصول الظاهرية (VAPs).



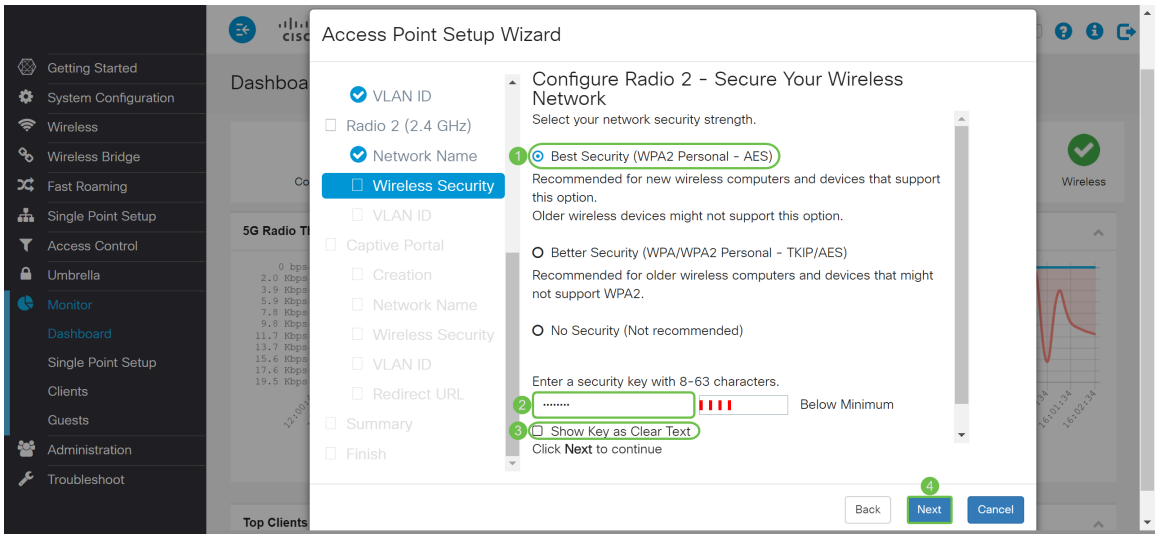
الخطوة 12. أدخل اسم شبكة جديد في حقل *اسم الشبكة (SSID)*. بشكل افتراضي يتم إستخدام **CiscoSB**. يعرف اسم الشبكة باسم SSID، وهو يعرف شبكتك حتى تتمكن الأجهزة اللاسلكية من العثور عليها. في هذا المثال، تم إستخدام **CiscoSB2.4** للتمييز بين اسم الشبكة بسرعة 5 جيجاهرتز. طقطقت **بعد ذلك** أن يشكل التأمين اللاسلكي *للراديو 2 (2. 4 جيجاهيرتز)*.



الخطوة 13. انقر على زر الاختيار المطابق لأمان الشبكة الذي تريد تطبيقه على الشبكة اللاسلكية. ثم أدخل كلمة المرور لشبكتك في حقل *مفتاح الأمان*. لترى كلمة المرور وأنت تكتب، حدد خانة الاختيار **إظهار المفتاح كنص واضح**. يتم تحديد **مفتاح العرض كنص واضح** بشكل افتراضي. انقر فوق **التالي** للمتابعة.

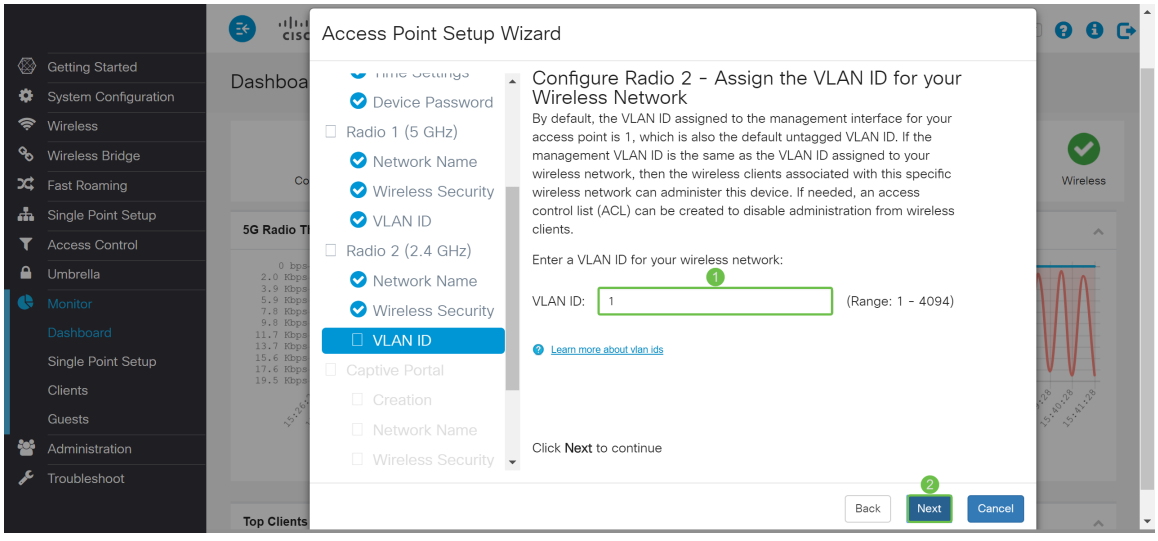
ملاحظة: إذا كانت الشبكة تحتوي على خليط من العملاء، يدعم بعضهم WPA2 ويدعم آخرون WPA الأصلي فقط، فحدد كلا (WPA/WPA2). وهذا يتيح لمحطات عملاء WPA و WPA2 الاقتران والمصادقة، إلا أنه يستخدم WPA2 الأكثر قوة للعملاء الذين يدعمونها. يتيح تكوين WPA هذا المزيد من قابلية التشغيل البيني بدلا من بعض التأمين.

- أفضل تأمين (Wi-Fi Protected Access 2 (WPA2) شخصي - معيار التشفير المتقدم (AES) تدعم جميع محطات العميل الموجودة على الشبكة خوارزمية التشفير القياسي WPA2 وخوارزمية التشفير المتقدم باستخدام وضع العداد مع بروتوكول تشفير تشفير كود مصادقة الرسائل (AES-CCMP) الخاص بربط مجموعات التشفير. وهذا يوفر أفضل مستوى أمان وفقا لمعايير IEEE 802.11i. طبقا لأحدث متطلبات تحالف Wi-Fi، يجب على نقطة الوصول دعم هذا الوضع طوال الوقت.
- أمان أفضل (WPA/WPA2 شخصي - WPA Personal (TKIP/AES هو مقياس Wi-Fi Alliance IEEE802.11i الذي يتضمن تشفير AES-CCMP و TKIP. يوفر التأمين عندما تكون هناك أجهزة لاسلكية قديمة تدعم WPA الأصلي لكنها لا تدعم WPA2 الأحدث.
- لا يوجد أمان (غير مستحسن) لا تتطلب الشبكة اللاسلكية كلمة مرور ويمكن لأي شخص الوصول إليها.

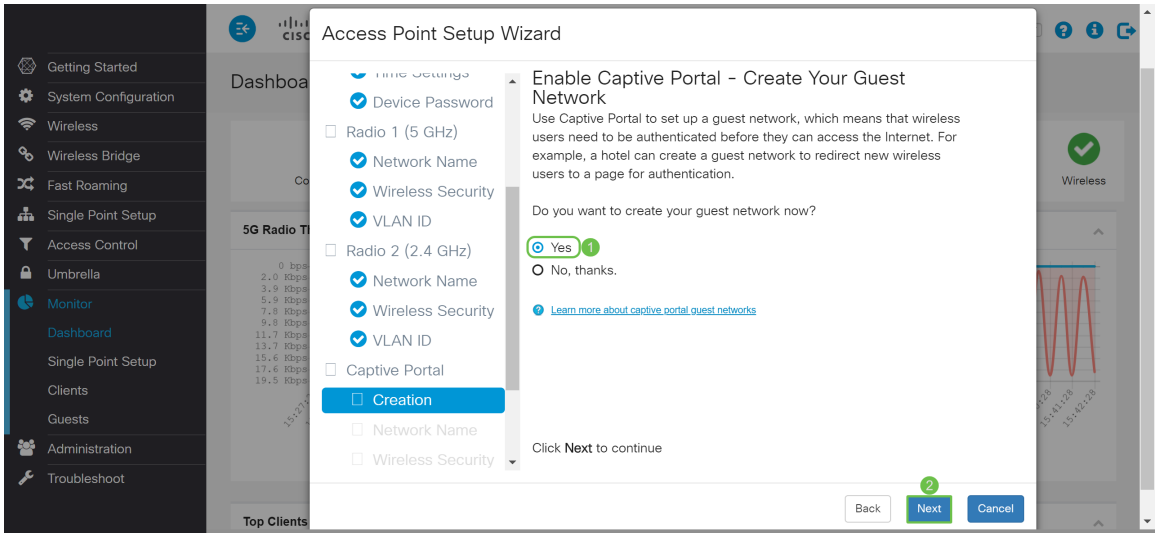


الخطوة 14. في حقل معرف *شبكة VLAN*، أدخل رقم معرف شبكة VLAN التي تريد أن ينتمي إليها *الراديو 1 (2.4 جيجاهرتز)*. في هذا المثال، سنستخدم القيمة الافتراضية ل 1 كمعرف *VLAN* الخاص بنا. طقطقت **بعد ذلك** أن يشكل *أسير مدخل*.

ملاحظة: نوصي بتعيين معرف VLAN مختلف من الافتراضي (1) إلى حركة مرور البيانات اللاسلكية، لفصلها عن حركة مرور الإدارة على شبكة VLAN رقم 1. انقر هنا لمعرفة المزيد حول نقاط الوصول الظاهرية (VAPs).

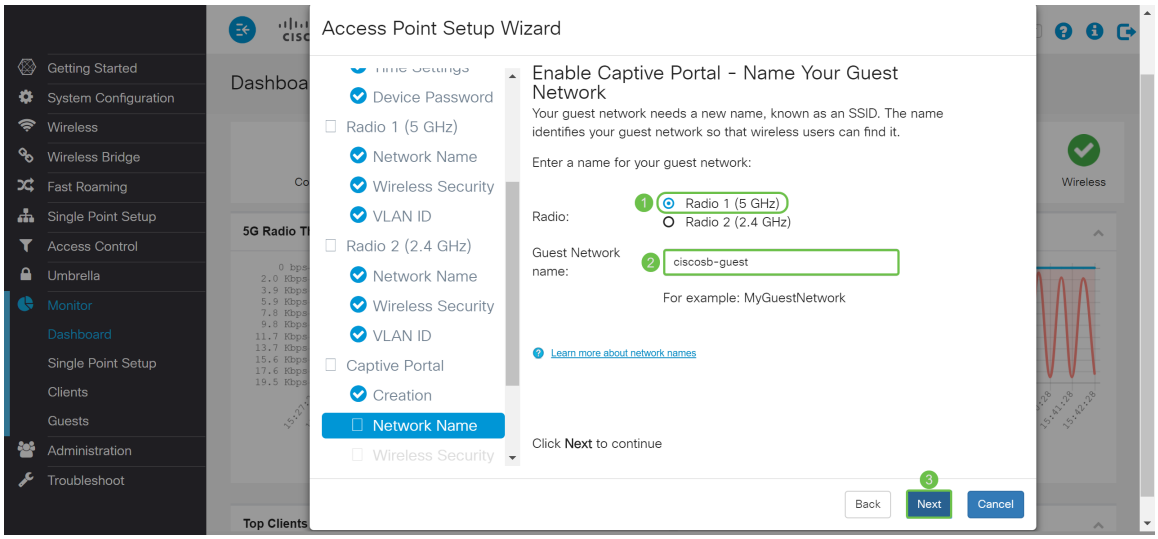


الخطوة 15. (إختياري) لا يلزم وجود شبكة ضيف. انقر على زر الخيار **نعم** إذا كنت تريد إنشاء شبكة ضيف. انقر فوق الزر **لا** لاسلكي إذا كنت لا تريد إنشاء شبكة ضيف وتخطي إلى الخطوة 20. انقر فوق الزر **التالي** للمتابعة.



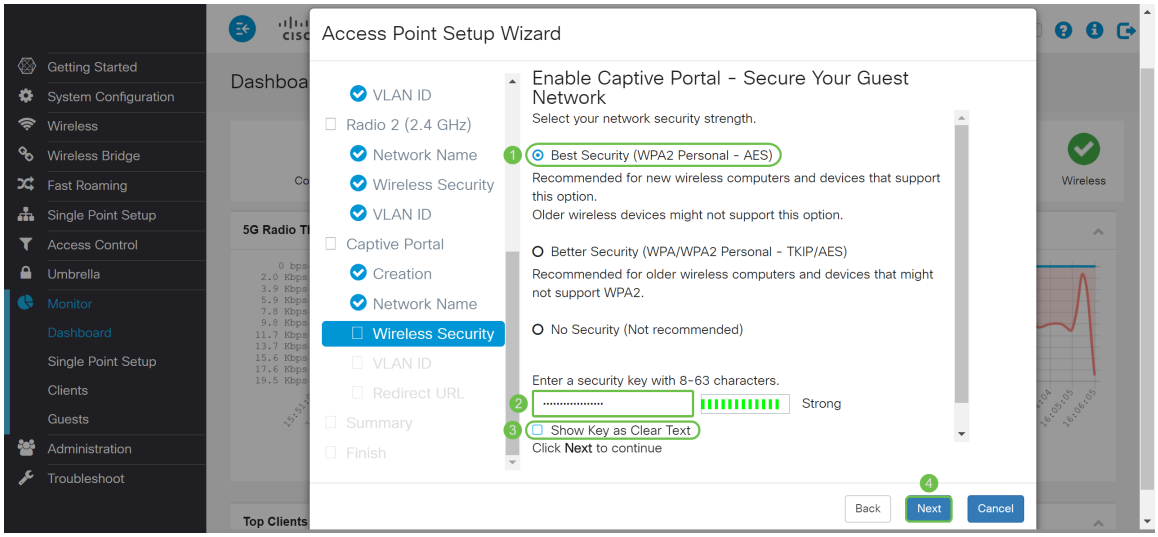
الخطوة 16. (إختياري) حدد زر الراديو الذي يتوافق مع *الراديو* الذي تريد وضع شبكة الضيوف فيه. ثم قم بإنشاء اسم شبكة في حقل *اسم شبكة الضيف*. انقر على **التالي** لتكوين إعدادات *تأمين اللاسلكي لشبكة الضيف*.

في هذا المثال، سنختار **الراديو 1 (5 جيجاهيرتز)** على أنه *الراديو* لدينا ونترك اسم الشبكة الافتراضي على أنه **ciscoSB-guest** حتى يتمكن مستخدمو الضيف اللاسلكي من العثور على اسم الشبكة.

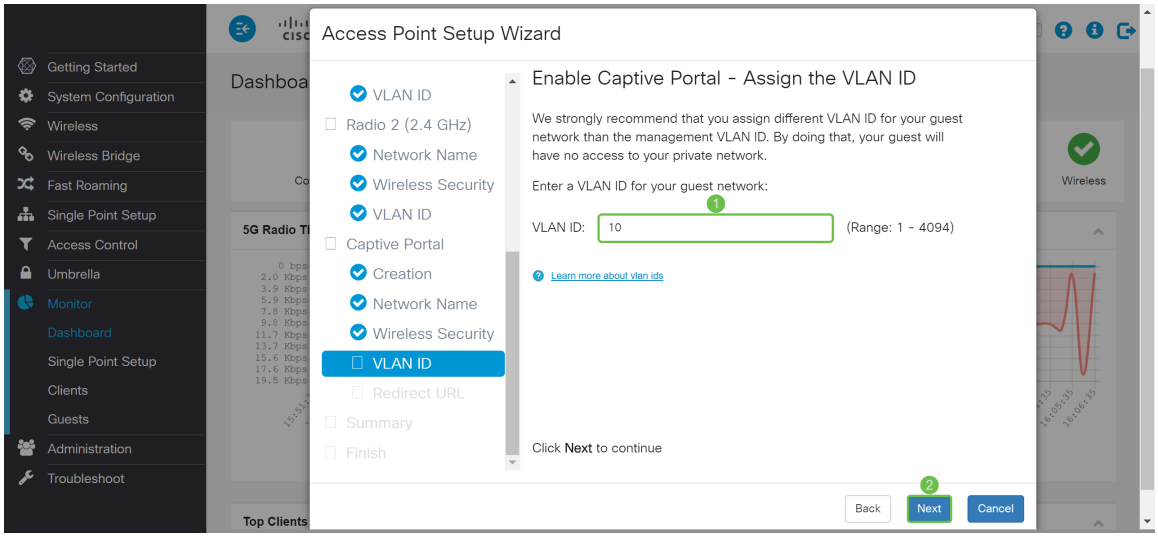


الخطوة 17. (إختياري) حدد زر الراديو الذي يتوافق مع أمان الشبكة الذي تريد تطبيقه على شبكة الضيوف الخاصة بك. ثم أدخل كلمة مرور لشبكة الضيف في حقل *مفتاح الأمان* إذا كان ذلك ممكنا. لإظهار **المفتاح كنص واضح** حدد خانة الاختيار لإظهار مفتاح الأمان كنص عادي. مكنت هذا افتراضيا. انقر فوق **التالي** للمتابعة. خيارات أمان الشبكة هي:

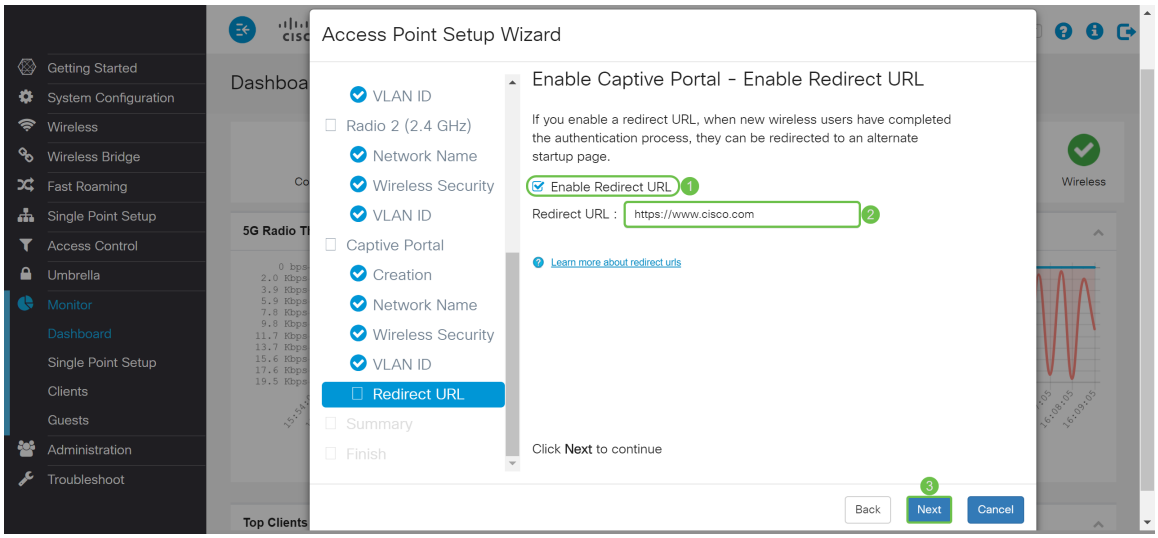
- أفضل تأمين (WPA2 Personal - AES) - ينصح به لأجهزة الكمبيوتر اللاسلكية الجديدة والأجهزة التي تدعم هذا الخيار.
- تأمين أفضل (WPA/WPA2 Personal - TKIP/AES) - ينصح به لأجهزة الكمبيوتر اللاسلكية القديمة والأجهزة التي قد لا تدعم WPA2.
- لا يوجد تأمين (غير مستحسن) - هذا هو التحديد الافتراضي.



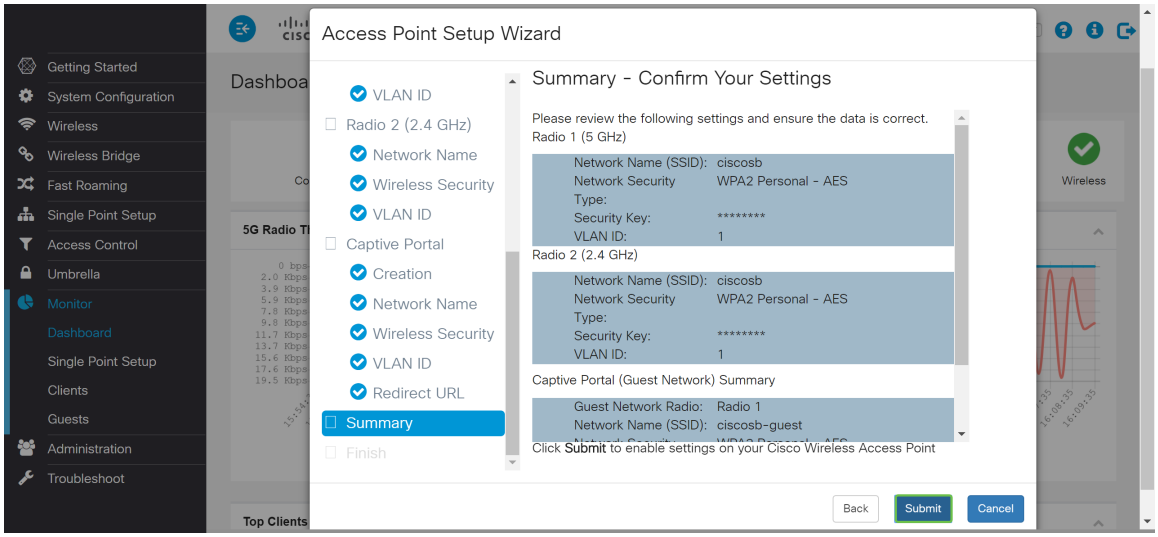
الخطوة 18. (إختياري) حدد *معرف شبكة VLAN* لشبكة الضيف. يجب أن يكون معرف شبكة VLAN الضيف مختلفا عن معرف شبكة VLAN الخاصة بالإدارة. في هذا المثال، إستخدمنا معرف *شبكة VLAN* **رقم 10** كمعرف شبكة VLAN الخاص بنا لشبكة الضيف. طقطقت **بعد ذلك** أن يشكل *ال redirect URL* لشبكة الضيف.



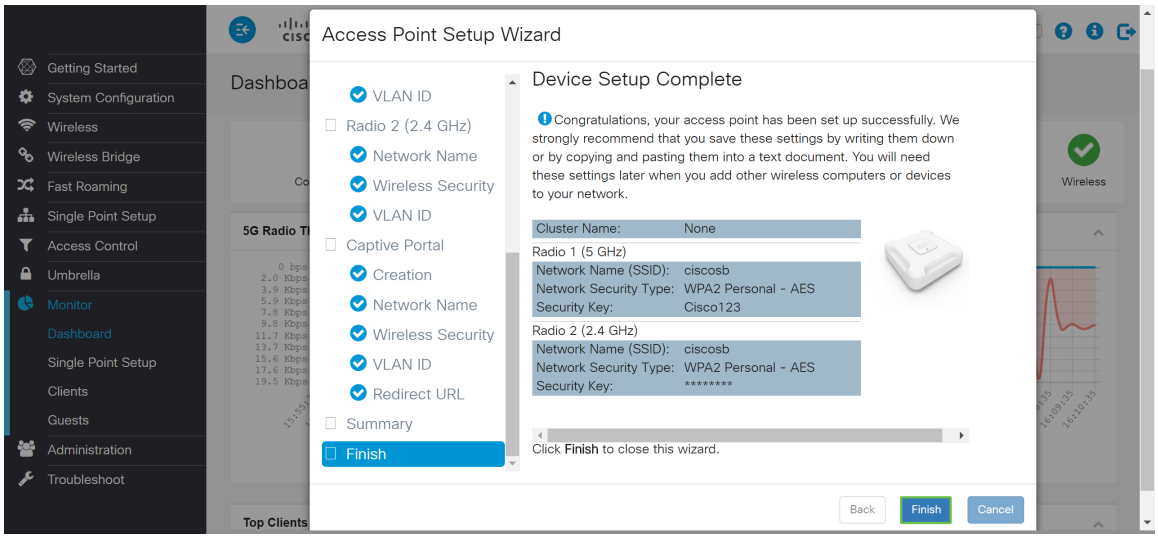
الخطوة 19. (إختياري) حدد خانة الاختيار **تمكين إعادة توجيه عنوان URL** لإعادة توجيه المستخدمين اللاسلكيين الجدد إلى صفحة بدء تشغيل بديلة. أدخل اسم مجال مؤهل بالكامل (FQDN) أو عنوان IP في حقل *عنوان URL لإعادة التوجيه* (بما في ذلك http:// أو https://). ثم انقر فوق **التالي** للمتابعة إلى صفحة *الملخص*.



الخطوة 20. في *الملخص - تأكد من إعداداتك*، راجع الإعدادات التي قمت بتكوينها. انقر فوق الزر **الخلف** لإعادة تكوين إعداد واحد أو أكثر. إذا نقرت فوق **إلغاء الأمر**، يتم إرجاع جميع الإعدادات إلى القيم السابقة أو الافتراضية. إذا كانت التكوينات صحيحة، انقر فوق **إرسال**. يتم حفظ إعدادات الإعداد الخاصة بك وتظهر نافذة تأكيد.



الخطوة 21. بمجرد تكوين إعداداتك، تظهر صفحة *اكتمال إعداد الجهاز* لتعلمك بأنه قد تم إعداد نقطة الوصول بنجاح. انقر فوق **إنهاء"** وسوف يطلب منك تسجيل الدخول مرة أخرى باستخدام كلمة المرور الجديدة.



القرار

لقد قمت الآن بتكوين WAP الخاص بك بنجاح باستخدام معالج الإعداد. يجب أن ترى SSIDs الخاصة بك والتي قمت بتكوينها في قائمة شبكات Wi-Fi. لتكوين ميزات أخرى على WAP الخاص بك، يجب عليك تسجيل الدخول مرة أخرى.

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).