

Gebruik de setup-wizard op WAP125 of WAP581

Doel

De wizard Instellen is een ingebouwde functie die u kunt gebruiken om u te helpen met de initiële configuratie van een Wireless Access Point (WAP)-apparaat. De wizard maakt het zeer eenvoudig om instellingen te configureren die stapsgewijze instructies geven.

Dit document toont u hoe u WAP125 en WAP581 met de Wizard Setup op het web configuratieprogramma kunt configureren.

Om uw WAP te configureren met behulp van de Setup op een mobiel apparaat, klikt u [hier](#).

Toepasselijke apparaten

- WAP125
- WAP581

Softwareversie

- 1.0.1.3

De installatiewizard gebruiken

Stap 1. Meld u aan bij het web configuratie hulpprogramma van uw WAP door het IP-adres van de WAP in uw webbrowser in te voeren. Als dit uw eerste keer is het configureren van de WAP, is het standaard IP-adres 192.168.1.254.

Opmerking: WAP581 wordt gebruikt in deze handleiding om de Setup-wizard aan te tonen. Het uiterlijk kan afhankelijk van het model verschillen.



Wireless Access Point

cisco

.....

English

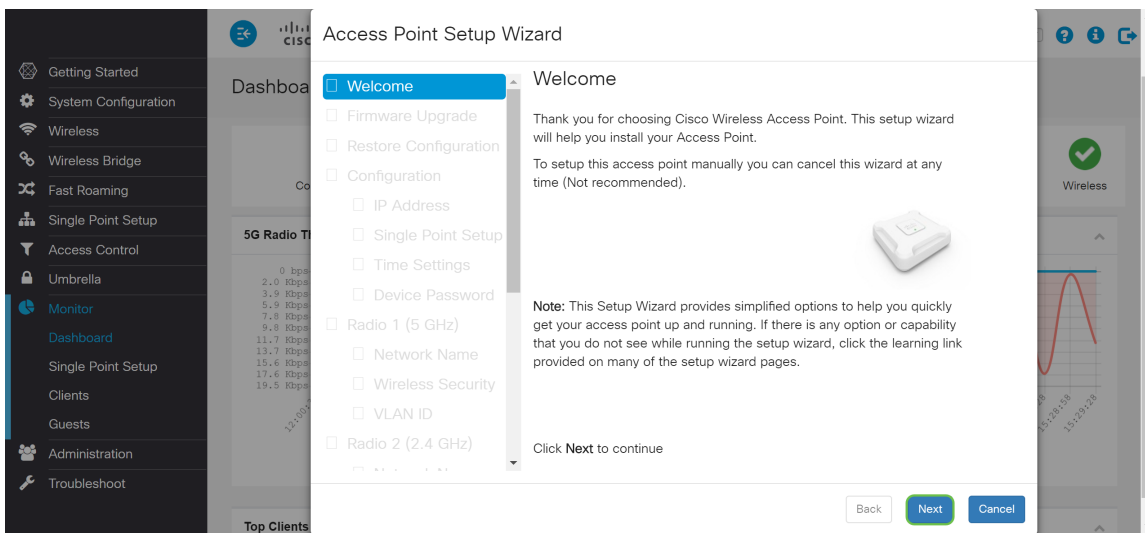


Login

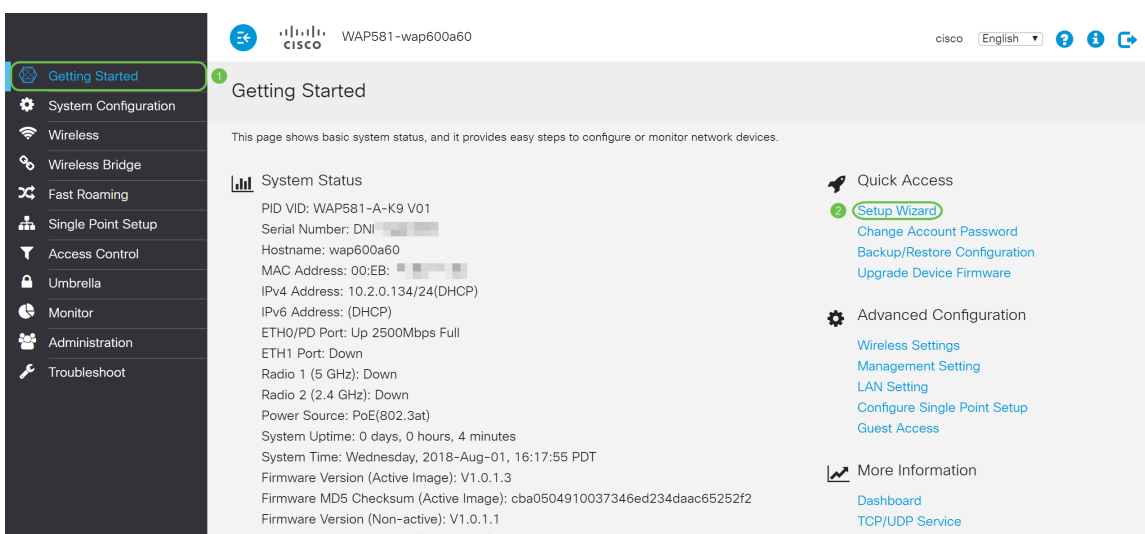
©2017 - 2018 Cisco Systems, Inc. All rights reserved.

Cisco, the Cisco logo, and Cisco Systems are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

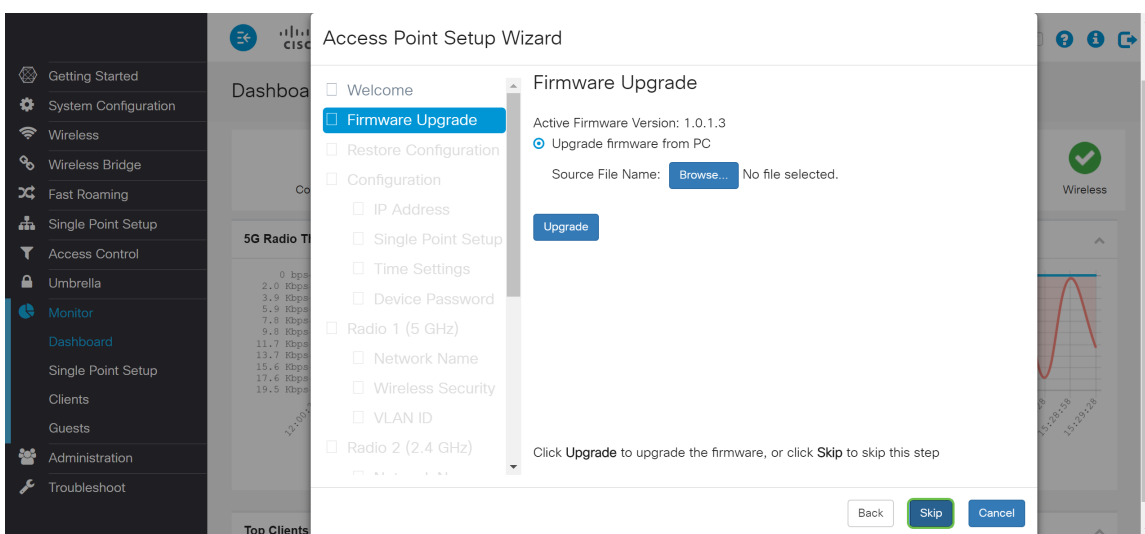
Stap 2. De eerste keer dat u in het access point logt of nadat deze is hersteld naar de standaardinstellingen van de fabriek, verschijnt de *Wizard Access Point Setup*. Klik op **Volgende** om verder te gaan



Opmerking: Als uw WAP al is ingesteld maar u nog steeds toegang wilt hebben tot de *Setup Wizard*, navigeer dan naar **Introductie > Wizard**. Het *Wizard Access Point Setup* verschijnt.

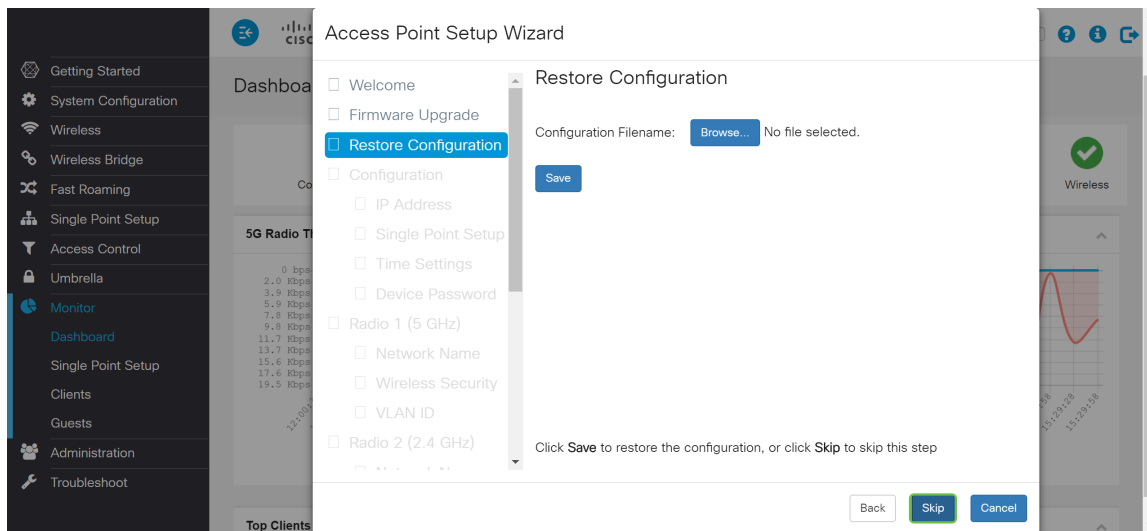


Stap 3. Klik in het venster *Firmware Upgrade* op de **Bladeren...** Selecteer het firmware-bestand naar u wilt upgraden. Druk vervolgens op **upgrade** naar upgrade. Nadat de firmware is bijgewerkt, start het apparaat automatisch opnieuw op en gaat het direct naar de logpagina. In dit voorbeeld, zullen we op **Skip** klikken aangezien we de firmware versie hebben die we willen.



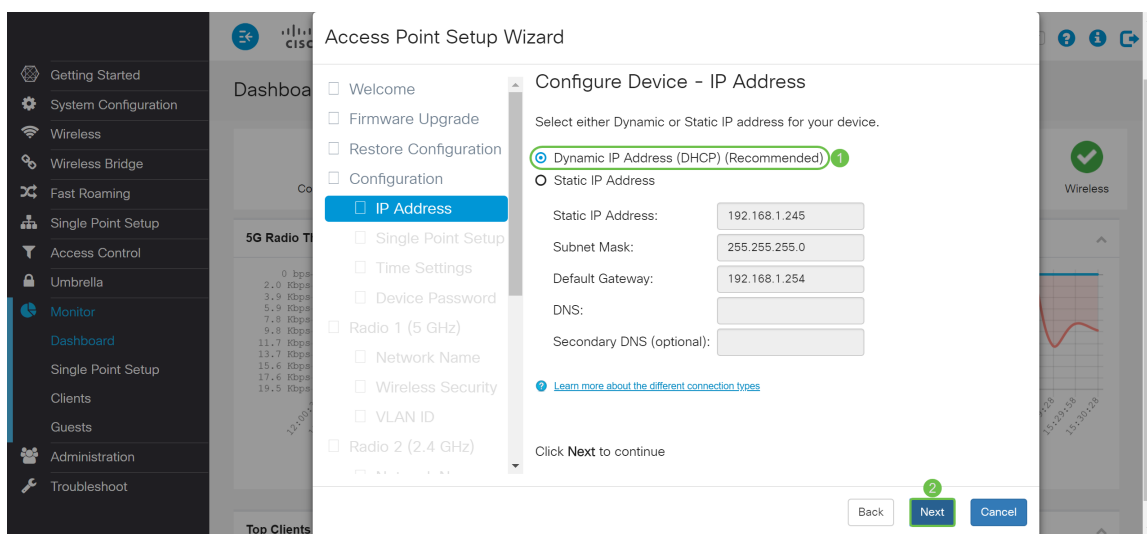
Stap 4. Als u vorige configuratie hebt die u op het apparaat wilt toepassen, klikt u op de knop **Bladeren...** Selecteer de knop in het venster *Configuration* en het configuratiebestand dat u wilt toepassen. Klik vervolgens op **Opslaan** om het configuratiebestand op het apparaat toe te passen. In dit voorbeeld, zullen we op **Skip** klikken.

Opmerking: Wanneer het apparaat de relevante configuratie toepast, wordt u opnieuw opgestart en naar de logpagina verwezen.



Stap 5. In het venster *Apparaat - IP Adres configureren* selecteert u **Dynamic IP Address (DHCP) (Aanbevolen)** om een IP-adres te verkrijgen van een Dynamic Host Configuration Protocol (DHCP) server, of klikt u op **Static IP Address** om het IP-adres handmatig te configureren. Klik vervolgens op **Volgende** om verder te gaan naar de volgende sectie. DHCP biedt configuratieparameters voor internethosts. In dit geval wijst DHCP een IP-adres aan een client voor een beperkte tijd toe of totdat de client het adres expliciet opzegt.

In dit voorbeeld, zullen we **Dynamic IP Address (DHCP) (Aanbevolen)** selecteren.



Stap 6. Single Point Setup biedt een gecentraliseerde methode om draadloze services over meerdere apparaten te beheren en te controleren. Dit zal u in staat stellen om één groep of cluster van uw draadloze apparaten te creëren die u kunt bekijken, opstellen, configureren en beveiligen het draadloze netwerk als één enkele entiteit. Single Point Setup kan kanaalplanning over uw draadloze service vergemakkelijken om radiointerferentie te verminderen en bandbreedte op uw draadloos netwerk te maximaliseren.

Om een nieuwe Single Point Setup van het WAP-apparaat te maken, klikt u op **New Cluster Name** en specificeert u een nieuwe naam. Wanneer u uw apparaten met dezelfde clusternaam configureren en de Single Point Setup-modus op andere WAP-apparaten inschakelen, sluiten zij zich automatisch bij de groep aan.

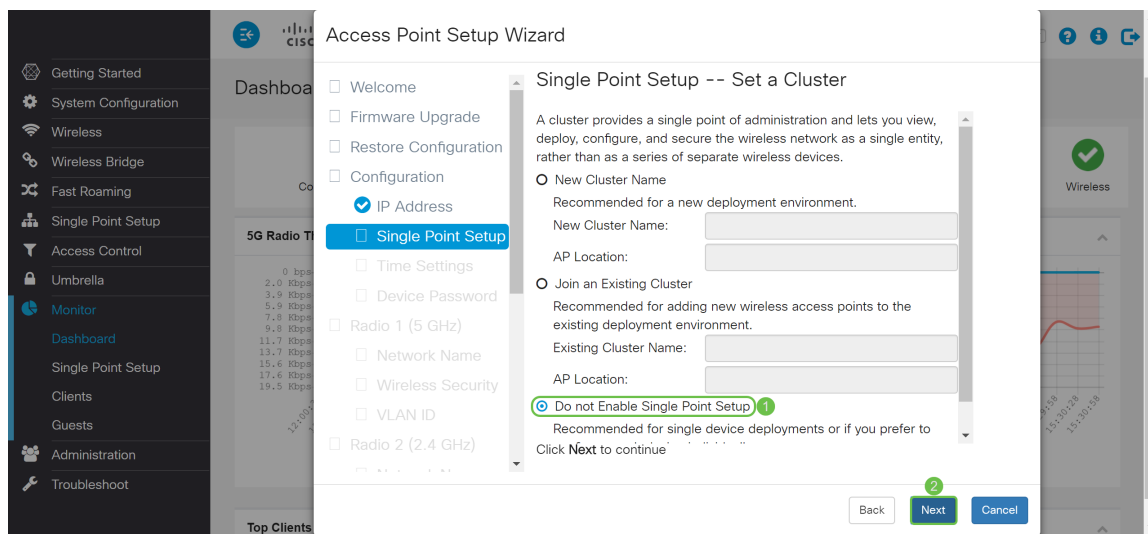
Als u al een cluster op uw netwerk hebt, kunt u dit apparaat aan het toevoegen door op

Samenvoegen in een bestaande cluster te klikken en dan de **bestaande clusternaam** in te voeren. WAP vormt de rest van de instellingen op basis van het cluster. Klik op **Volgende** en bevestig de bevestiging om zich bij het cluster aan te sluiten. Klik op **Inzenden** om zich bij het cluster aan te sluiten. Klik nadat de configuratie is voltooid op **Voltoeien** om de *installatiewizard* te verlaten.

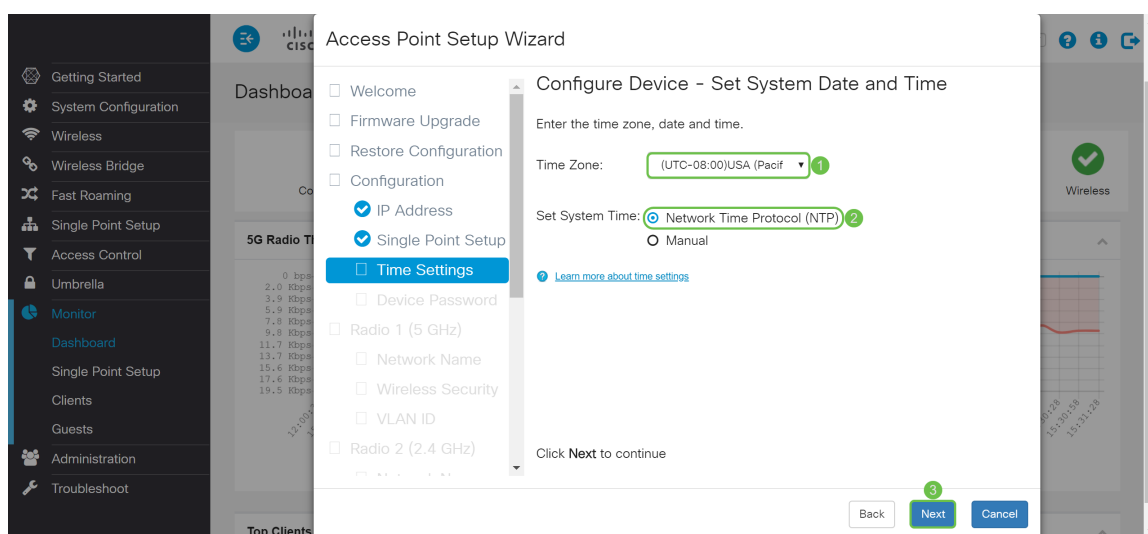
Opmerking: U kunt de locatie van het access point in het veld **AP Locatie** invoeren om nota te nemen van de fysieke locatie van het WAP-apparaat.

Als u wilt dat dit apparaat momenteel niet aan een Single Point Setup deelneemt, klikt u op **Geen Single Point Setup** inschakelen.

In dit voorbeeld selecteert u **Niet Single Point Setup** inschakelen. Klik vervolgens op **Volgende** om verder te gaan naar de volgende sectie.



Stap 7. In het venster *Machine configureren - Datum en tijd instellen*, kiest u uw **tijdzone** en selecteert u vervolgens of u de tijd wilt die uw systeem nodig heeft om automatisch de tijdsinstelling te verkrijgen op een **NTP-server (Network Time Protocol)** of selecteert u **Handmatig** om de tijdsinstellingen handmatig te configureren. Een systeemklok biedt een netwerk-gesynchroniseerde tijd-stempeling service voor de berichtloggen. De systeemklok kan handmatig worden ingesteld of als een NTP-client die de muisklikken van een server verkrijgt. Klik op **Next** om door te gaan met de *Setup-wizard*.

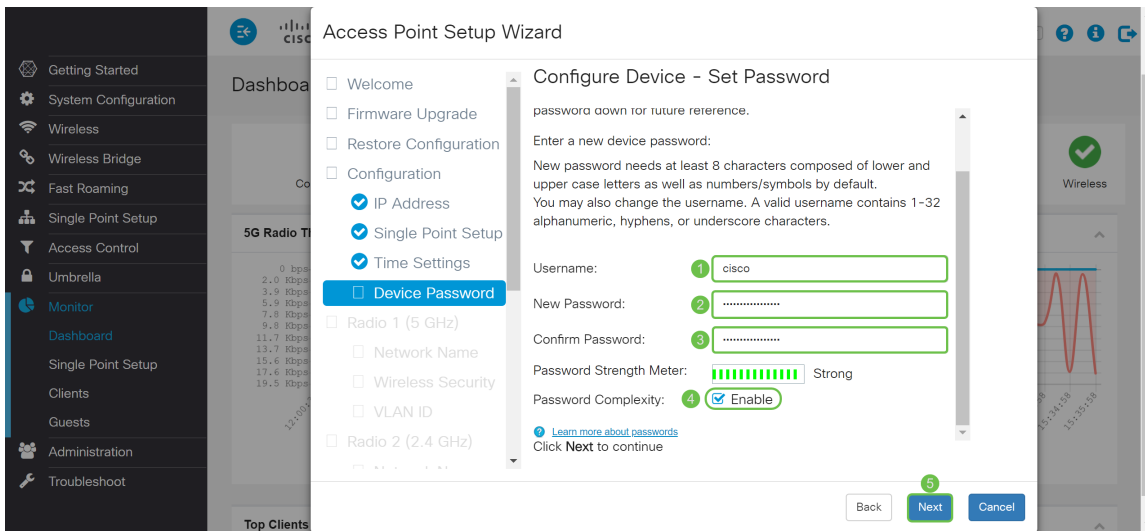


Stap 8. Voer een nieuwe **gebruikersnaam** in in het veld *Gebruikersnaam*, standaard is de gebruikersnaam Cisco. Voer een **nieuw wachtwoord** in voor de *gebruikersnaam*. Typ het **nieuwe wachtwoord** vervolgens opnieuw in het veld *Wachtwoord bevestigen*. U kunt de

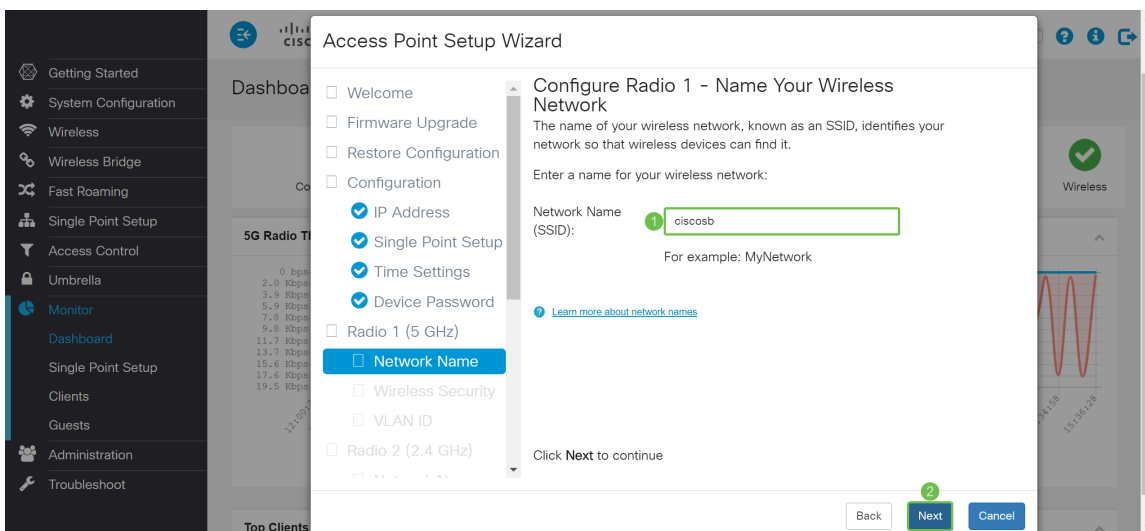
Wachtwoordcomplexiteit niet controleren om de wachtwoordbeveiligingsregels uit te schakelen. We raden echter sterk aan om de wachtwoordbeveiligingsregels aan te houden. Het nieuwe wachtwoord moet voldoen aan de volgende complexiteit-instellingen:

- Is anders dan de gebruikersnaam.
- Dit is niet hetzelfde wachtwoord als het huidige wachtwoord.
- Heeft een minimumlengte van acht tekens.
- Bevat tekens van ten minste drie tekenklassen (hoofdletters, kleine letters, getallen en speciale tekens die op een standaardtoetsenbord beschikbaar zijn).

Klik vervolgens op **Next** om *Radio 1* te configureren.



Stap 9. Voer een naam voor uw draadloze netwerk in in de *naam* van het *netwerk (SSID)*. Dit zal helpen uw netwerk te identificeren zodat draadloze apparaten het kunnen vinden. Standaard wordt **ciscosb** gebruikt als de netwerknaam. Klik vervolgens op **Volgende** om verder te gaan naar de volgende sectie.

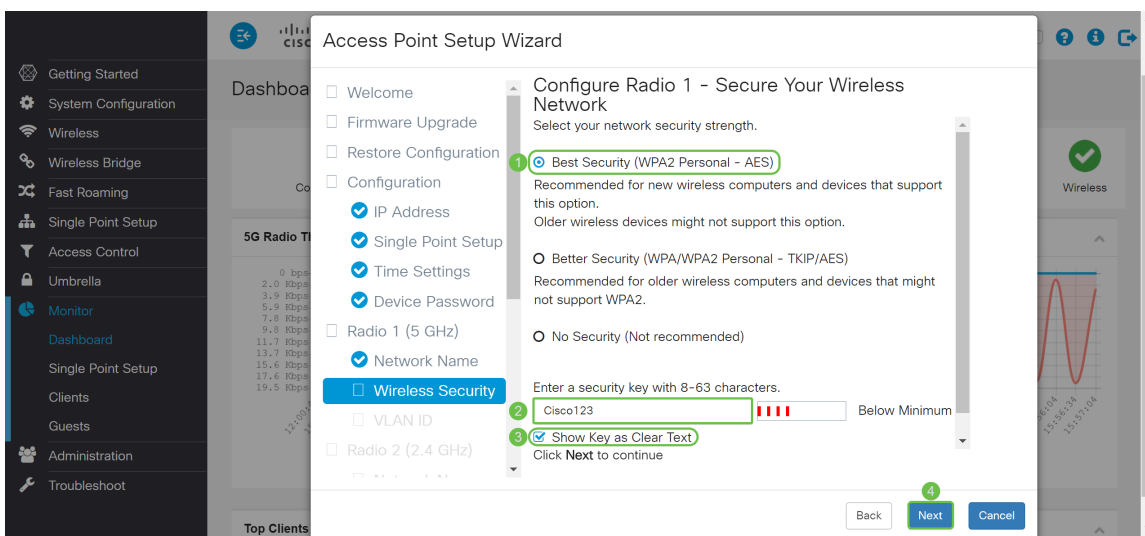


Stap 10. Klik op de radioknop die overeenkomt met de netwerkbeveiliging die u op uw draadloos netwerk wilt toepassen. Typ het wachtwoord voor het netwerk in het veld *Security Key*. Als u het wachtwoord wilt zien zoals u typt, controleert u de **sleutel tonen** als het vakje **Tekst wissen**. Klik op **Volgende** om verder te gaan

Opmerking: Als het netwerk een mix van klanten heeft, waarvan sommige steun voor WAP2 en anderen die slechts het oorspronkelijke WAP ondersteunen, selecteer beiden (WAP/WAP2). Dit laat zowel de de client van WAP als van WAP2 associëren en authenticatie verklaren, maar gebruikt de robuustere WAP2 voor client die het steunt. Deze configuratie maakt meer interoperabiliteit

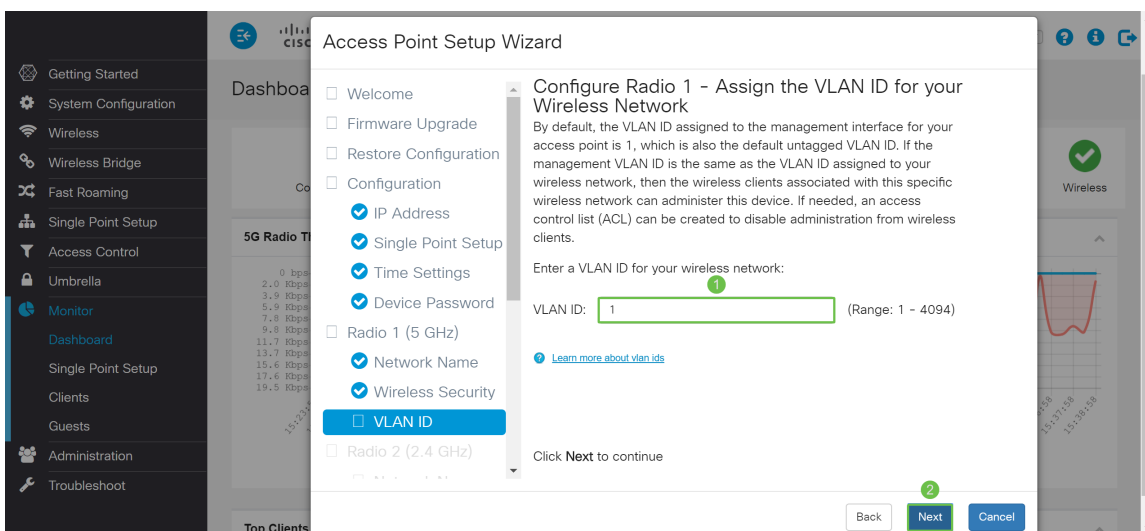
mogelijk in plaats van enige beveiliging.

- Persoonlijke security (Wi-Fi beschermde Access 2) - geavanceerde encryptie-standaard (AES) Alle clientstations op de netwerkondersteuning van WAP2 en Advanced Encryption Standard Encryption met behulp van Counter Mode met Cipher Block Chaining Message Authentication Protocol (AES-CCMP)-algoritme/beveiligingsprotocol. Dit biedt de beste beveiliging volgens de IEEE 802.11i-standaard. Volgens de laatste Wi-Fi Alliance-eis moet AP deze modus voortdurend ondersteunen.
- Persoonlijke beveiliging (WAP/WAP2) - TKIP/AES Persoonlijk ben ik een Wi-Fi Alliance IEEE802.11i standaard, die AES-CCMP en TKIP-encryptie omvat. Het biedt beveiliging wanneer er oudere draadloze apparaten zijn die het oorspronkelijke WAP ondersteunen maar het nieuwere WAP2 niet ondersteunen.
- Geen beveiliging (niet aanbevolen) Draadloos netwerk heeft geen wachtwoord nodig en is toegankelijk voor iedereen.



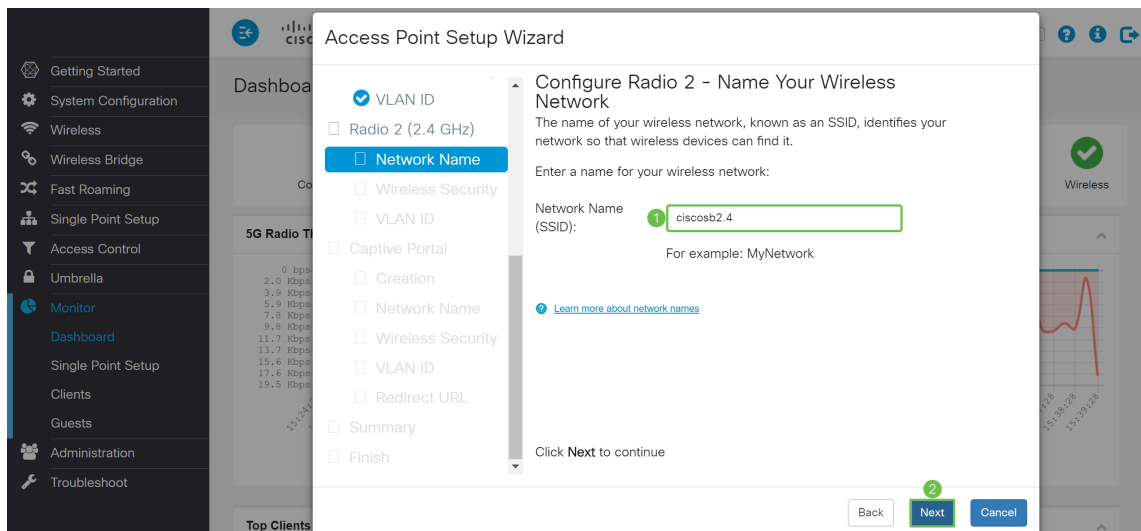
Stap 1. In het veld *VLAN-id* voert u het ID-nummer in van het VLAN dat u wilt dat *Radio 1 (5 GHz)* tot u behoort. In dit voorbeeld laten we de *VLAN-ID* als 1 achter. Klik op **Next** om *Radio 2 (2,4 GHz)* te configureren.

Opmerking: Wij raden u aan een andere VLAN-id van de standaard (1) toe te wijzen aan het draadloze verkeer, om deze van het beheerverkeer op VLAN 1 te scheiden. Klik [hier](#) om meer over Virtual Access Point (VAP's) te weten te komen.



Stap 12. Voer een nieuwe netwerknaam in het veld *Netwerknaam (SSID)*. Standaard wordt

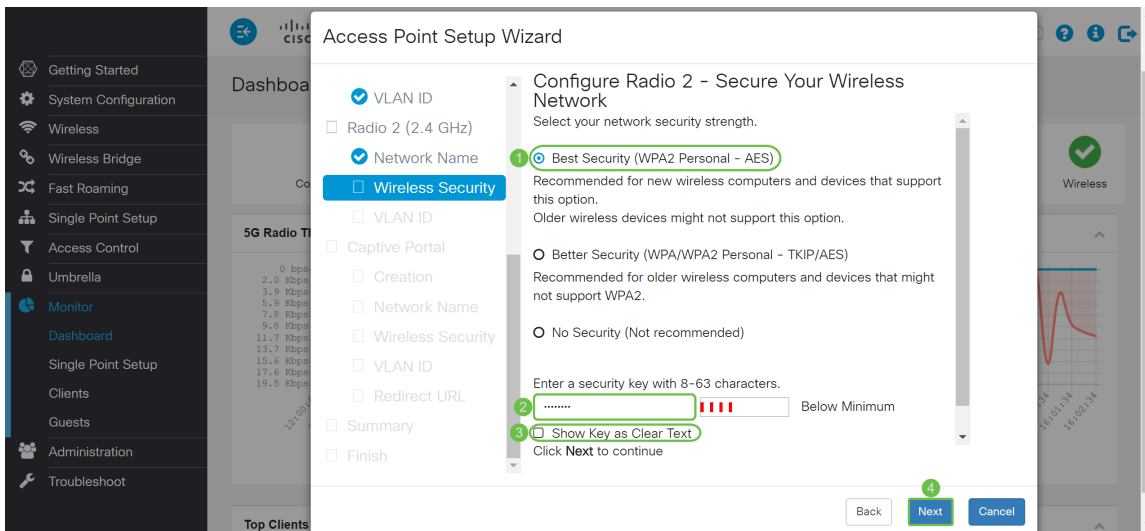
ciscosb gebruikt. De naam van het netwerk is bekend als SSID, het identificeert uw netwerk zodat de draadloze apparaten het kunnen vinden. In dit voorbeeld werd **ciscosb2.4** gebruikt om de 5 GHz netwerknaam te differentiëren. Klik op **Next** om de draadloze beveiliging van *Radio 2 (2,4 GHz)* te configureren.



Stap 13. Klik op de radioknop die overeenkomt met de netwerkbeveiliging die u op uw draadloos netwerk wilt toepassen. Typ het wachtwoord voor het netwerk in het veld *Security Key*. Als u het wachtwoord wilt zien zoals u typt, controleert u de **slutel tonen** als het vakje **Tekst wissen**. De **Toon-toets** als **Clear Tekst** is standaard ingeschakeld. Klik op **Volgende** om verder te gaan

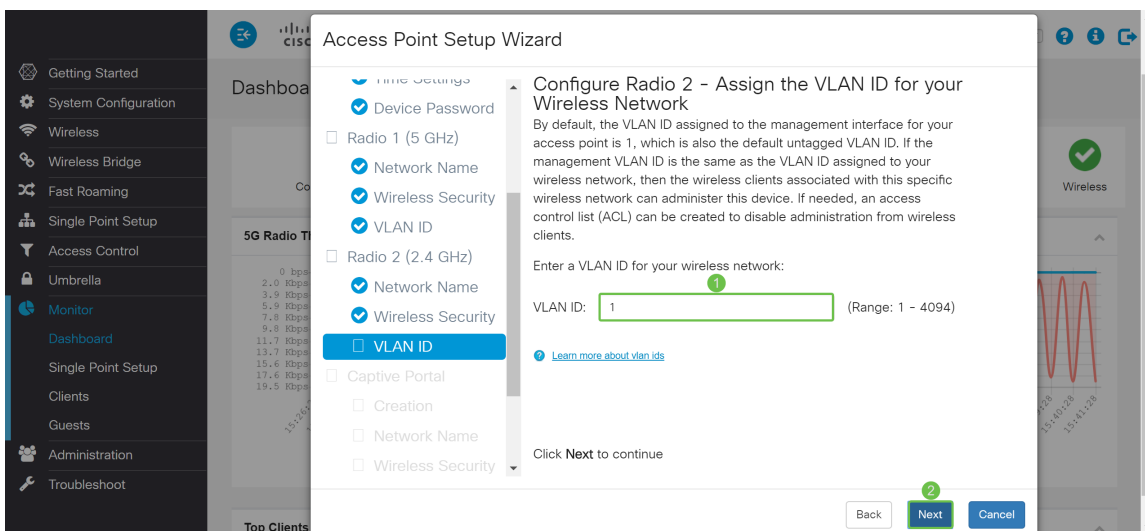
Opmerking: Als het netwerk een mix van klanten heeft, waarvan sommige steun voor WAP2 en anderen die slechts het oorspronkelijke WAP ondersteunen, selecteer beiden (WAP/WAP2). Dit laat zowel WAP- als WAP2 clientstations associëren en authenticeren, maar gebruikt de robuustere WAP2 voor klanten die dit ondersteunen. Deze configuratie maakt meer interoperabiliteit mogelijk in plaats van enige beveiliging.

- **Persoonlijke security (Wi-Fi beschermde Access 2)** - geavanceerde encryptie-standaard (AES) Alle clientstations op de netwerkondersteuning van WAP2 en Advanced Encryption Standard Encryption met behulp van Counter Mode met Cipher Block Chaining Message Authentication Protocol (AES-CCMP)-algoritme/beveiligingsprotocol. Dit biedt de beste beveiliging volgens de IEEE 802.11i-standaard. Volgens de laatste Wi-Fi Alliance-eis moet AP deze modus voortdurend ondersteunen.
- **Persoonlijke beveiliging (WAP/WAP2)** - TKIP/AES Persoonlijk ben ik een Wi-Fi Alliance IEEE802.11i standaard, die AES-CCMP en TKIP-encryptie omvat. Het biedt beveiliging wanneer er oudere draadloze apparaten zijn die het oorspronkelijke WAP ondersteunen maar het nieuwere WAP2 niet ondersteunen.
- **Geen beveiliging (niet aanbevolen)** Draadloos netwerk heeft geen wachtwoord nodig en is toegankelijk voor iedereen.

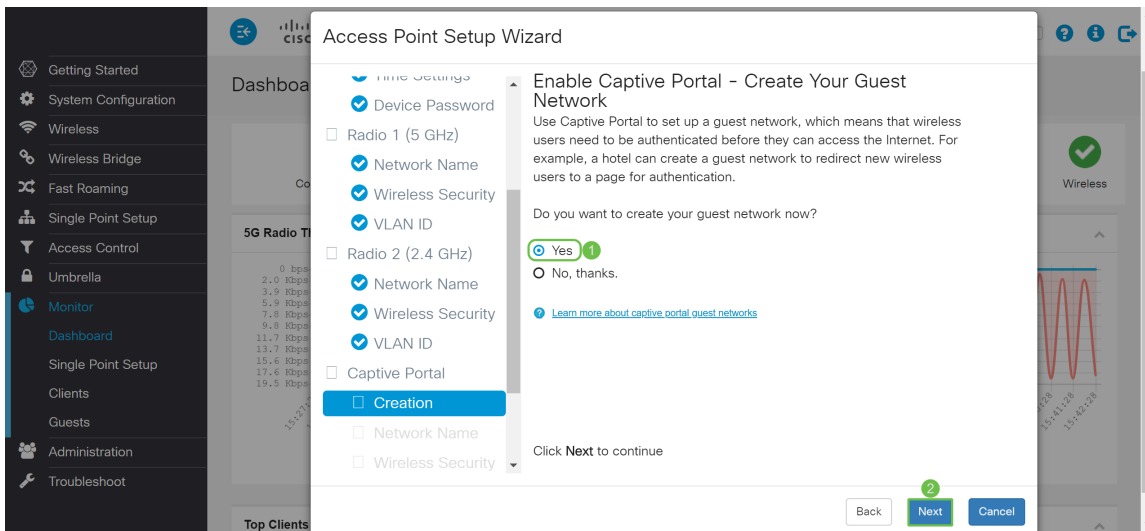


Stap 14. In het veld *VLAN-id* voert u het ID-nummer van het VLAN in waarvan u wilt dat *Radio 1 (2.4 GHz)* tot u behoort. In dit voorbeeld, zullen we de standaardwaarde van 1 als onze *VLAN ID* gebruiken. Klik op **Next** om *Captive Portal* te configureren.

Opmerking: Wij raden u aan een andere VLAN-id van de standaard (1) toe te wijzen aan het draadloze verkeer, om deze van het beheerverkeer op VLAN 1 te scheiden. Klik [hier](#) om meer over Virtual Access Point (VAP's) te weten te komen.

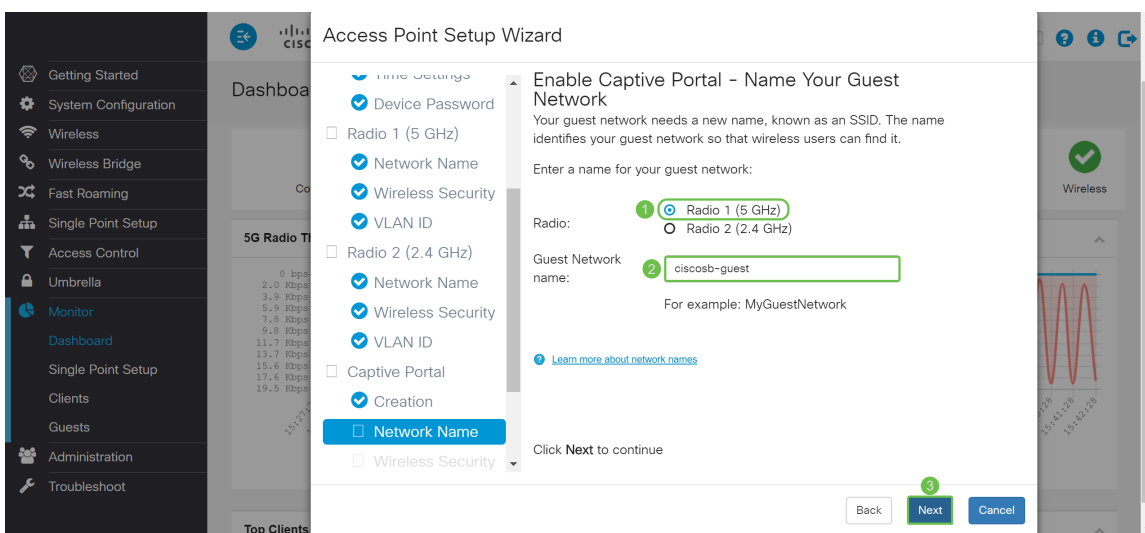


Stap 15. (Optioneel) Een gastnetwerk is niet vereist. Klik op de radioknop **Ja** als u een gastnetwerk wilt creëren. Klik op de radioknop **Geen** of als u geen gastnetwerk wilt maken en skip naar [Stap 20](#). Klik op de knop **Volgende** om verder te gaan.



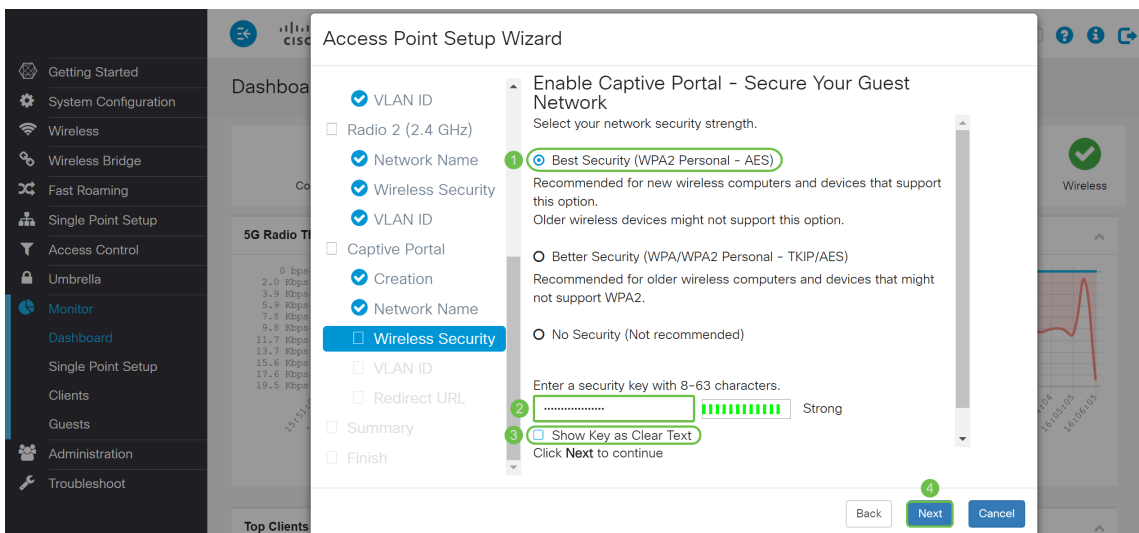
Stap 16. (Optioneel) Selecteer de radioknop die overeenkomt met de *radio* waarin u het gastnetwerk wilt plaatsen. Voer vervolgens een netwerknaam in het veld *Naam* van het *netwerk* uit. Klik op **Next** om de *draadloze security* instellingen voor het *gastnetwerk* te configureren.

In dit voorbeeld, zullen we **Radio 1 (5 GHz)** als onze *Radio* selecteren en de standaard netwerknaam als **ciscosb-gast** verlaten zodat uw mobiele gastgebruikers de netwerknaam kunnen vinden.

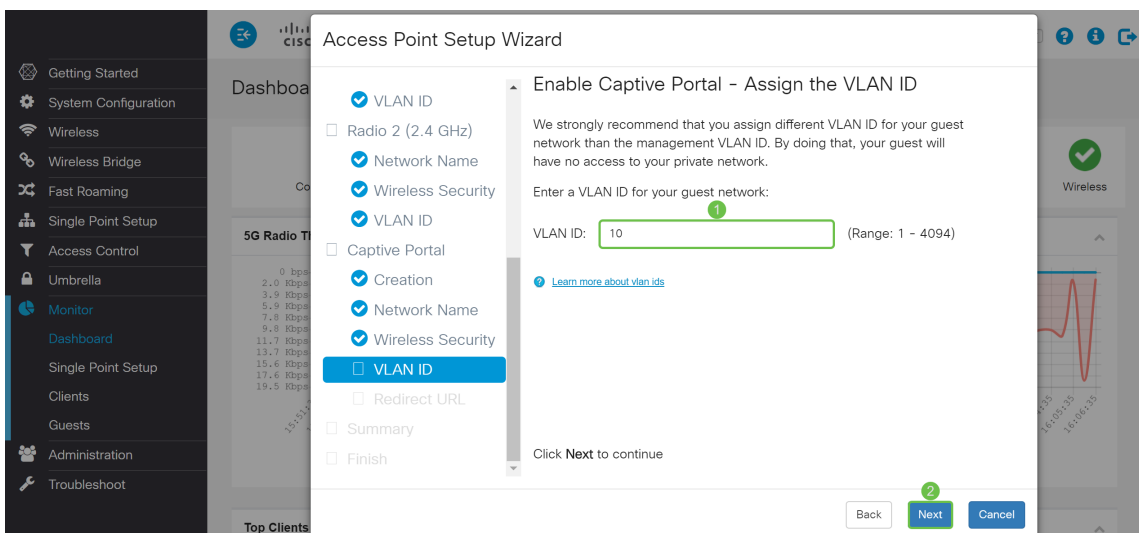


Stap 17. (Optioneel) Selecteer de radioknop die overeenkomt met de netwerkbeveiliging die u op uw gastnetwerk wilt toepassen. Typ indien van toepassing een wachtwoord voor het gastnetwerk in het veld *Security Key*. Als u **sleutel wilt tonen als tekst wissen**, schakelt u het aanvinkvakje in om de beveiligingstoets als illustratie weer te geven. Dit is standaard ingeschakeld. Klik op **Volgende** om verder te gaan. De opties voor netwerkbeveiliging zijn:

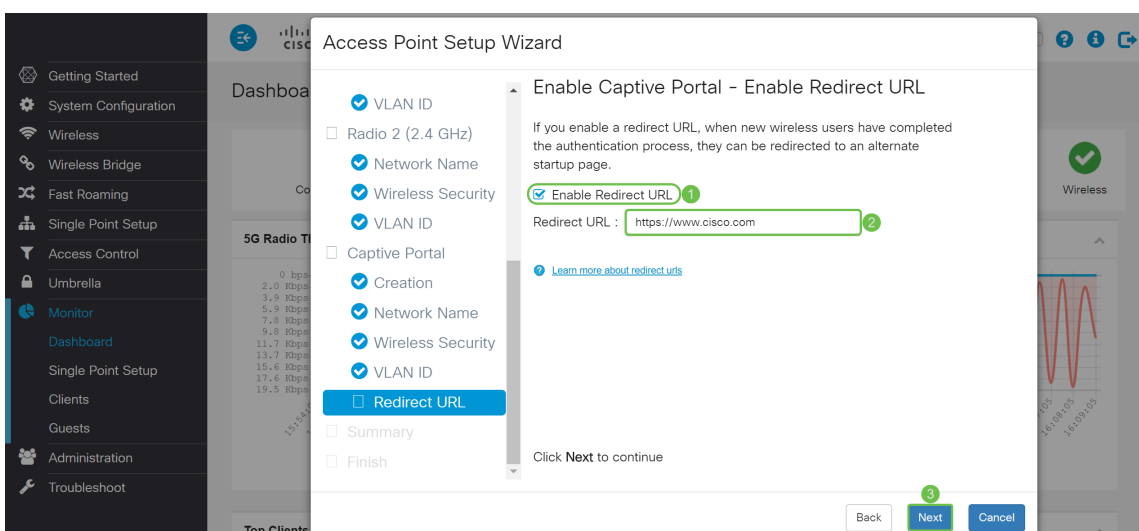
- Best Security (WAP2 Persoonlijk - AES) - Aanbevolen voor nieuwe draadloze computers en apparaten die deze optie ondersteunen.
- Betere beveiliging (WAP/WAP2 Persoonlijk - TKIP/AES) - Aanbevolen voor oudere draadloze computers en apparaten die WAP2 niet kunnen ondersteunen.
- Geen beveiliging (niet aanbevolen) - Dit is de standaardselectie.



Stap 18. (Optioneel) Specificeer een *VLAN-id* voor het gastnetwerk. De id-id van het gastnetwerk VLAN zou van het beheer VLAN-id moeten verschillen. In dit voorbeeld, gebruikten we *VLAN ID 10* als onze VLAN ID voor het gastnetwerk. Klik op **Volgende** om de *URL* omleiden voor het gastnetwerk te configureren.

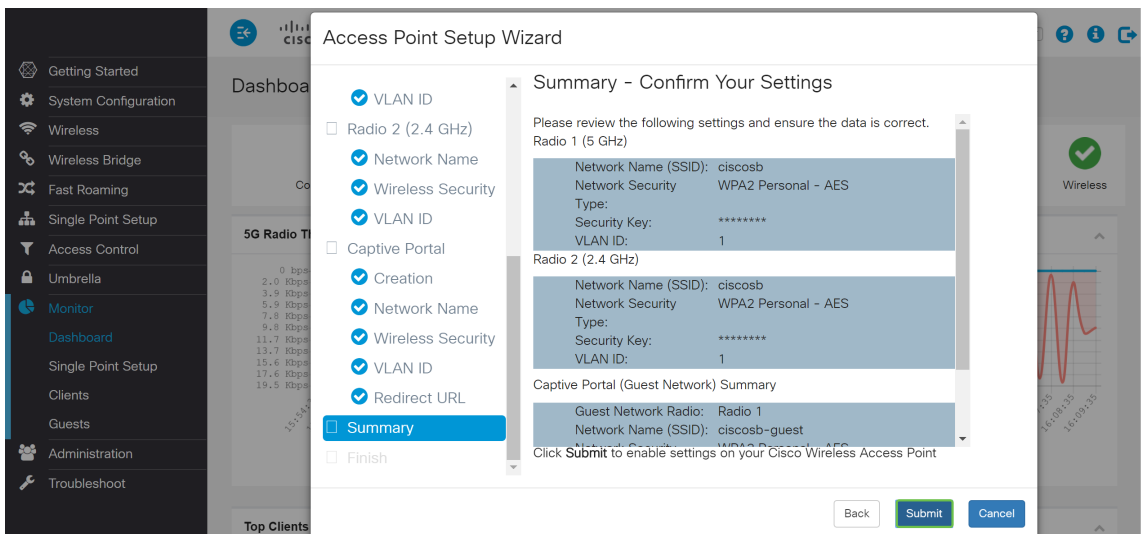


Stap 19. (Optioneel) Controleer het vakje **URL omleiden** om nieuwe draadloze gebruikers te omleiden naar een alternatieve startpagina. Voer een Full Qualified Domain Name (FQDN) of IP-adres in in het veld *Redirect URL* (inclusief *http://* of *https://*). Klik vervolgens op **Volgende** om verder te gaan naar de pagina *Samenvatting*.

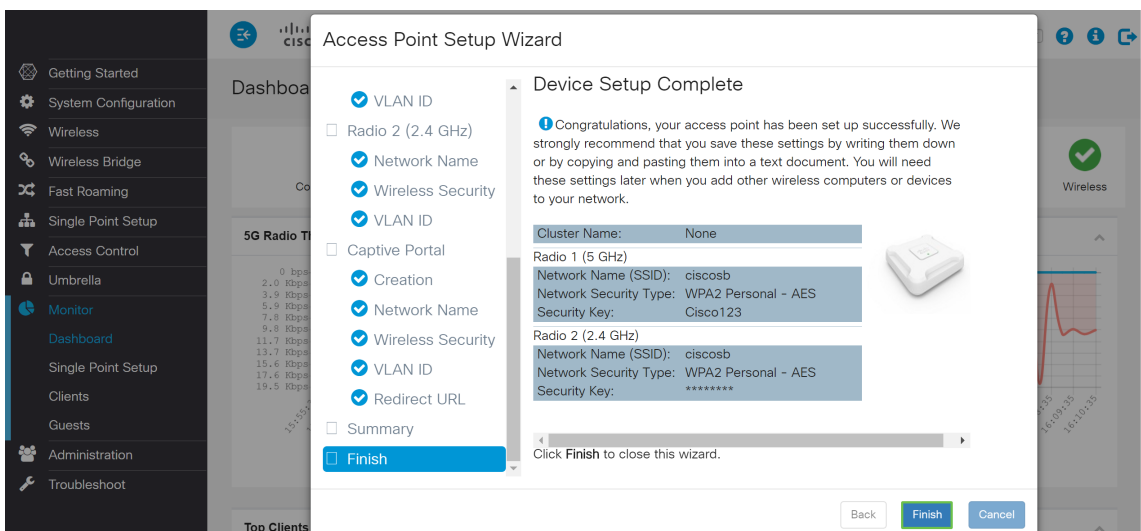


Stap 20. In de *samenvatting - Bevestig uw pagina met instellingen* en controleer de instellingen die u hebt ingesteld. Klik op de knop **Terug** om een of meer instellingen opnieuw te configureren.

Als u op **Annuleren** klikt, worden alle instellingen teruggegeven aan de vorige of standaardwaarden. Als uw configuraties correct zijn, klikt u op **Indienen**. Uw instellingen worden opgeslagen en er verschijnt een bevestigingsvenster.



Stap 21. Zodra uw instellingen zijn geconfigureerd, verschijnt de *volledige* pagina van de *installatie* om u te laten weten dat uw access point met succes is ingesteld. Klik op **Voltooien** en u moet met het nieuwe wachtwoord opnieuw inloggen.



Conclusie

U hebt uw WAP nu met de Setup Wizard ingesteld. U dient uw SSID's te zien die u net hebt ingesteld in uw lijst met Wi-Fi-netwerken. Om de andere functies op uw WAP te kunnen configureren moet u opnieuw inloggen.