Verwenden des Setup-Assistenten auf dem WAP125 oder WAP581

Ziel

Der Installationsassistent ist eine integrierte Funktion, die Sie bei der Erstkonfiguration eines WAP-Geräts (Wireless Access Point) unterstützen kann. Der Setup-Assistent vereinfacht die Konfiguration von Einstellungen und enthält schrittweise Anweisungen.

In diesem Dokument wird die Konfiguration von WAP125 und WAP581 mithilfe des Setup-Assistenten im Webkonfigurationsprogramm beschrieben.

Klicken Sie hier, um den WAP mithilfe des Setup-Assistenten auf einem Mobilgerät zu konfigurieren.

Anwendbare Geräte

- WAP125
- WAP581

Softwareversion

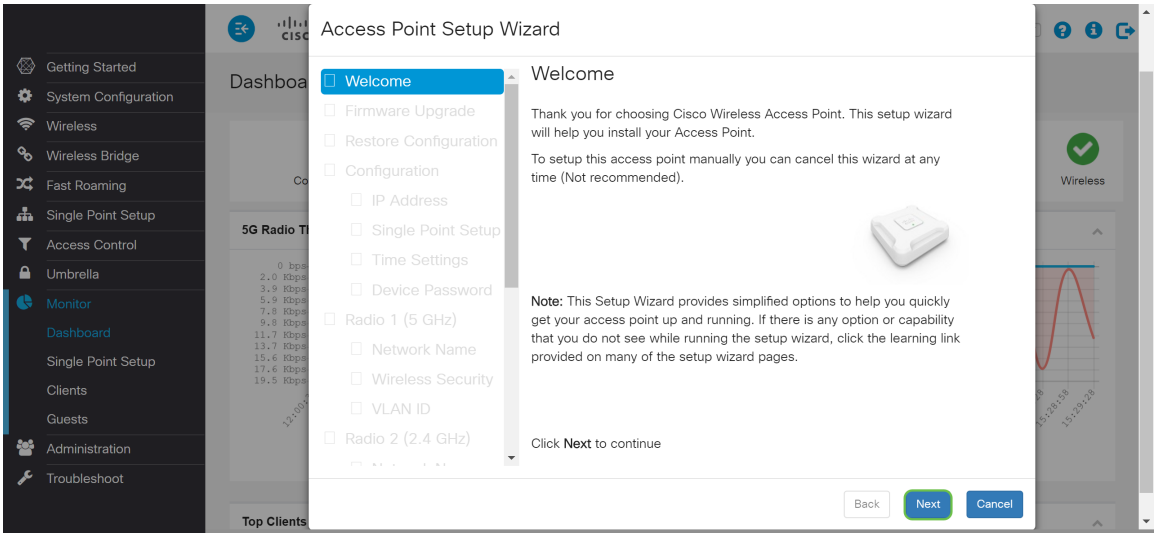
- 1,0/1,3

Verwendung des Installationsassistenten

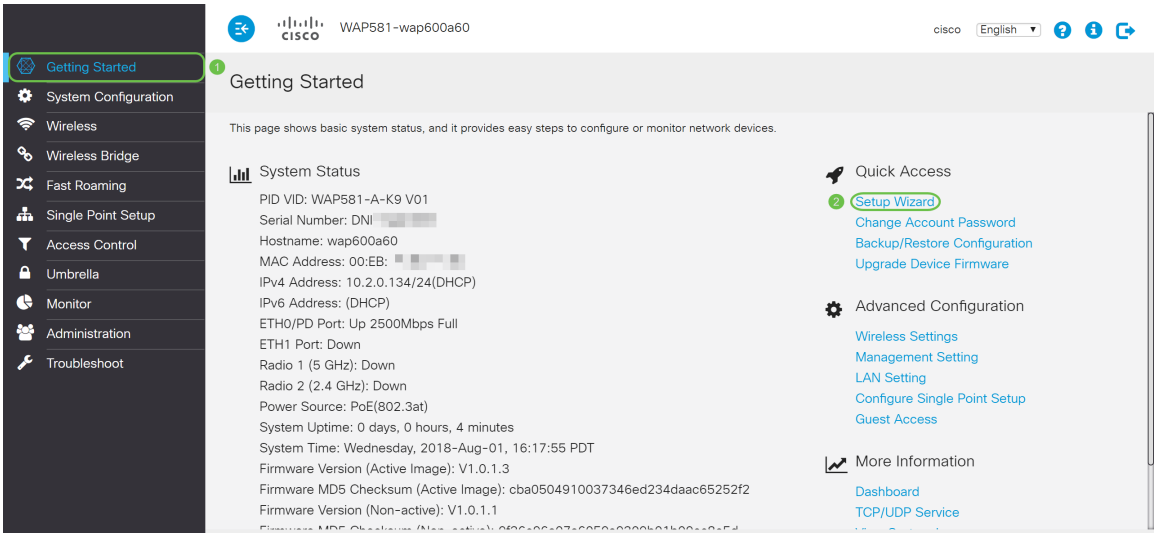
Schritt 1: Melden Sie sich beim Webkonfigurationsprogramm Ihres WAP an, indem Sie die IP-Adresse des WAP in Ihren Webbrowser eingeben. Wenn Sie den WAP zum ersten Mal konfigurieren, lautet die Standard-IP-Adresse 192.168.1.254.

Hinweis: Der WAP581 wird in dieser Anleitung verwendet, um den Setup-Assistenten zu veranschaulichen. Das Aussehen kann je nach Modell variieren.

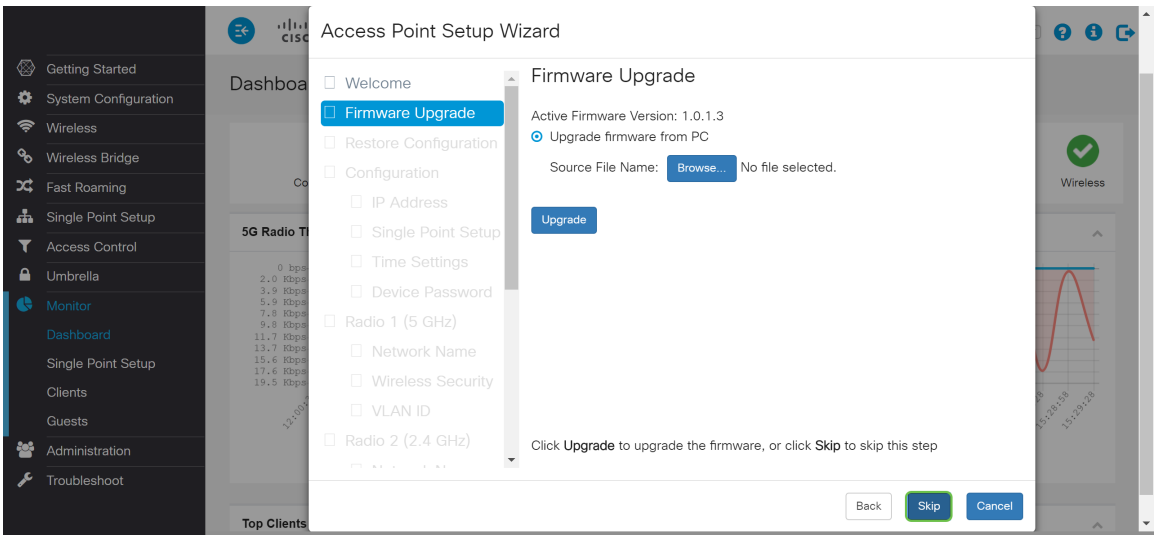
Schritt 2: Bei der ersten Anmeldung am Access Point oder nach dem Zurücksetzen auf die Werkseinstellungen wird der *Access Point Setup Wizard* angezeigt. Klicken Sie auf **Weiter**, um fortzufahren.



Hinweis: Wenn Ihr WAP bereits konfiguriert ist, Sie jedoch weiterhin auf den *Installationsassistenten* zugreifen möchten, navigieren Sie zu **Getting Started > Setup Wizard (Erste Schritte > Installationsassistent)**. Das Fenster *Access Point Setup Wizard* (Assistent für Access Point-Einrichtung) wird angezeigt.



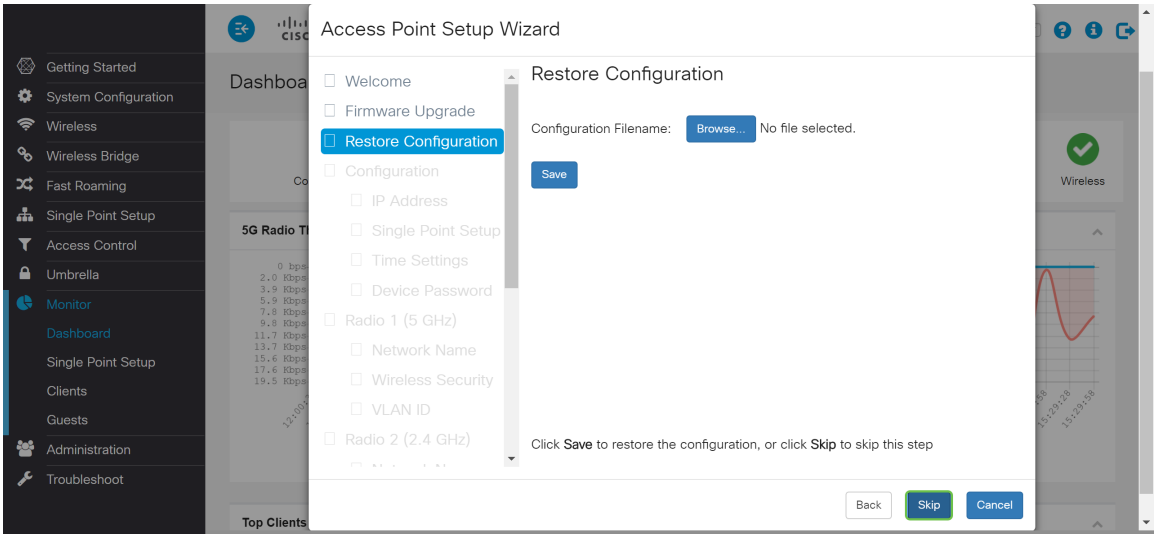
Schritt 3: Klicken Sie im Fenster *Firmware-Aktualisierung* auf **Durchsuchen...** und wählen Sie die Firmware-Datei aus, auf die Sie aktualisieren möchten. Drücken Sie anschließend **Upgrade**, um ein Upgrade auf die Firmware durchzuführen. Nach dem Aktualisieren der Firmware wird das Gerät automatisch neu gestartet und führt die Anmeldeseite durch. In diesem Beispiel klicken wir auf **Überspringen**, da wir die gewünschte Firmware-Version haben.



Schritt 4: Wenn Sie bereits eine Konfiguration vorgenommen haben, die Sie auf das Gerät

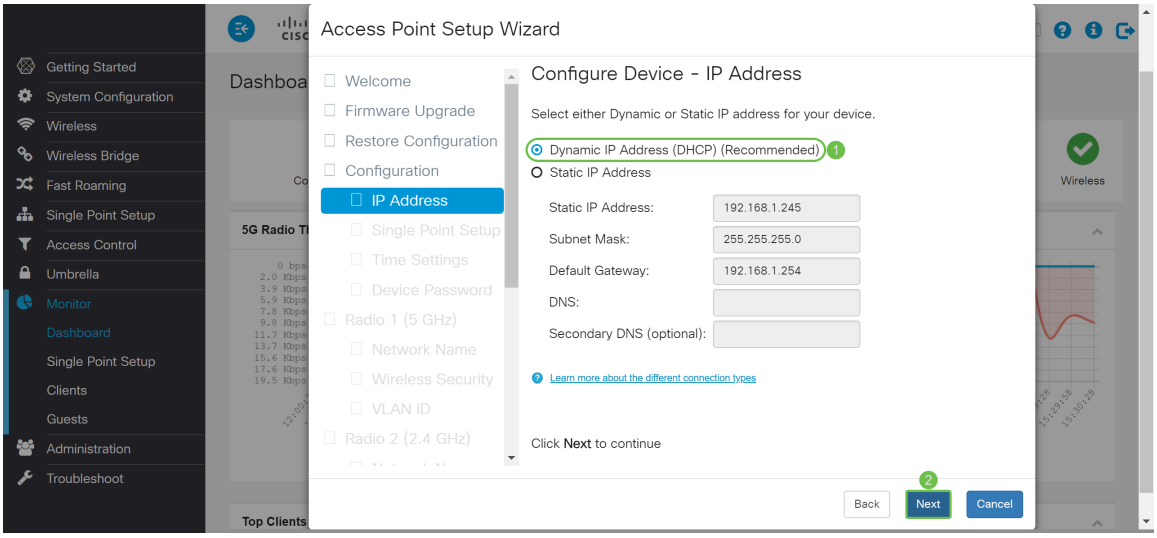
anwenden möchten, klicken Sie auf **Durchsuchen...** im Fenster *Konfiguration wiederherstellen* und die Konfigurationsdatei auswählen, die Sie anwenden möchten. Klicken Sie anschließend auf **Speichern**, um die Konfigurationsdatei auf das Gerät anzuwenden. In diesem Beispiel klicken wir auf **Überspringen**.

Hinweis: Wenn das Gerät die entsprechende Konfiguration anwendet, wird es neu gestartet und führt Sie zur Anmeldeseite.



Schritt 5: Wählen Sie im Fenster *Configure Device - IP Address (Gerät konfigurieren - IP-Adresse)* die *Option* **Dynamic IP Address (DHCP) (Recommended) (Dynamic IP Address) (DHCP) (Empfohlen))** um eine IP-Adresse von einem Dynamic Host Configuration Protocol (DHCP)-Server abzurufen, oder klicken Sie auf **Static IP Address**, um die IP-Adresse manuell zu konfigurieren. Klicken Sie anschließend auf **Weiter**, um mit dem nächsten Abschnitt fortzufahren. DHCP stellt Konfigurationsparameter für Internet-Hosts bereit. In diesem Fall weist der DHCP-Client einem Client eine IP-Adresse für einen begrenzten Zeitraum zu oder bis der Client die Adresse explizit aufgibt.

In diesem Beispiel wählen wir **Dynamic IP Address (DHCP) (Empfohlen)** aus.



Schritt 6: Die Single-Point-Einrichtung bietet eine zentralisierte Methode zur Verwaltung und Steuerung von Wireless-Services auf mehreren Geräten. So können Sie eine einzelne Gruppe oder einen Cluster Ihrer Wireless-Geräte erstellen, die Sie als eine Einheit anzeigen, bereitstellen, konfigurieren und sichern können. Die Single-Point-Einrichtung erleichtert die Planung von Kanälen im gesamten Wireless-Dienst, um Funkstörungen zu reduzieren und die Bandbreite im Wireless-Netzwerk zu maximieren.

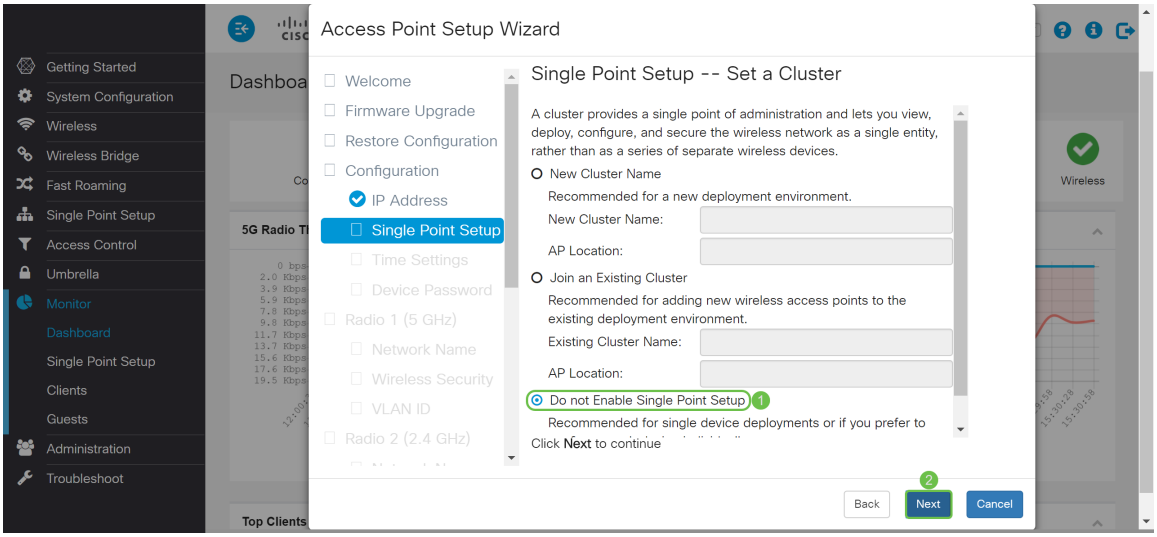
Um eine neue Single-Point-Einrichtung für das WAP-Gerät zu erstellen, klicken Sie auf **Neuer Cluster-Name** und geben Sie einen neuen Namen an. Wenn Sie Ihre Geräte mit demselben Cluster-Namen konfigurieren und den Single-Point-Setup-Modus auf anderen WAP-Geräten aktivieren, werden sie automatisch der Gruppe hinzugefügt.

Wenn Sie bereits einen Cluster in Ihrem Netzwerk haben, können Sie dieses Gerät hinzufügen, indem Sie auf **An bestehendem Cluster beitreten** klicken und dann den **vorhandenen Cluster-Namen** eingeben. Der WAP konfiguriert die übrigen Einstellungen basierend auf dem Cluster. Klicken Sie auf **Weiter** und bestätigen Sie die Bestätigung, dem Cluster beizutreten. Klicken Sie auf **Senden**, um dem Cluster beizutreten. Wenn die Konfiguration abgeschlossen ist, klicken Sie auf **Fertig stellen**, um den *Installationsassistenten* zu beenden.

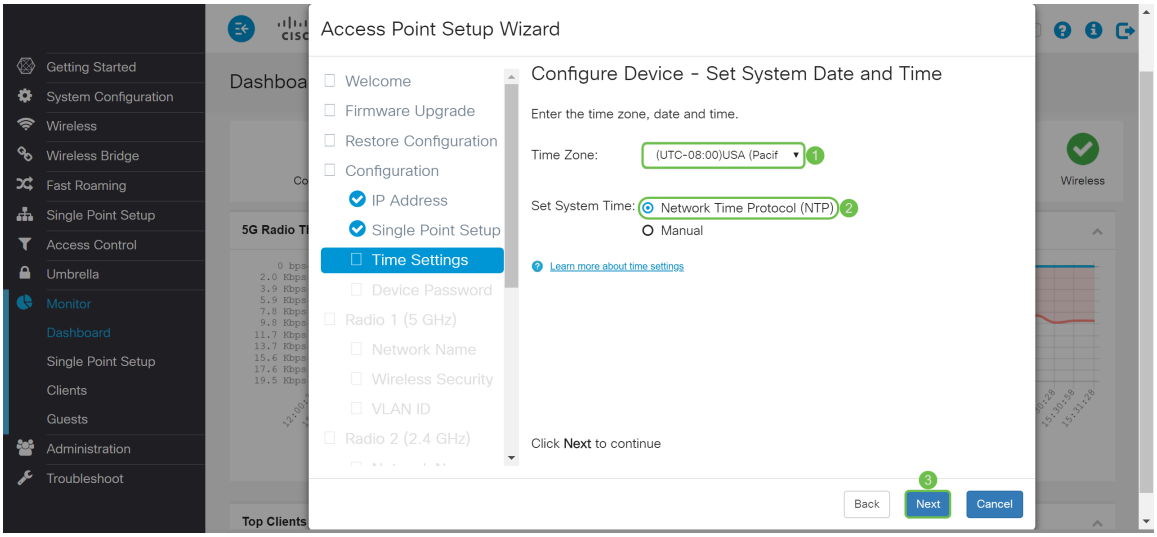
Hinweis: Sie können den Access Point-Standort im Feld **AP Location** eingeben, um den physischen Standort des WAP-Geräts anzuzeigen.

Wenn dieses Gerät derzeit nicht an einer Single-Point-Einrichtung teilnehmen soll, klicken Sie auf **Single-Point-Einrichtung nicht aktivieren**.

In diesem Beispiel wählen Sie **Single-Point-Einrichtung nicht aktivieren aus**. Klicken Sie anschließend auf **Weiter**, um mit dem nächsten Abschnitt fortzufahren.



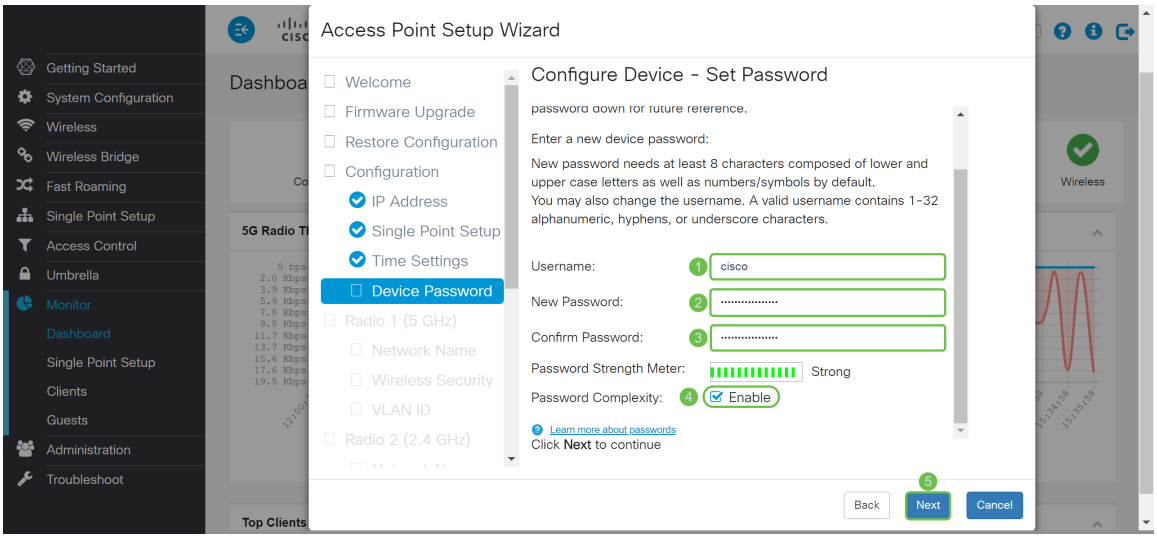
Schritt 7: Wählen Sie im Fenster *Gerät konfigurieren - Systemdatum und -zeit festlegen* die **Zeitzone aus**, und wählen Sie dann aus, ob die Systemzeit automatisch die Zeiteinstellung von einem **NTP-**Server abruft oder **Manuell** auswählen soll, um die Zeiteinstellungen manuell zu konfigurieren. Eine Systemuhr bietet einen netzwerksynchronisierten Zeitstempeldienst für die Nachrichtenprotokolle. Die Systemuhr kann manuell oder als NTP-Client konfiguriert werden, der die Klickdaten von einem Server abruft. Klicken Sie auf **Weiter**, um den *Installationsassistenten* fortzusetzen.



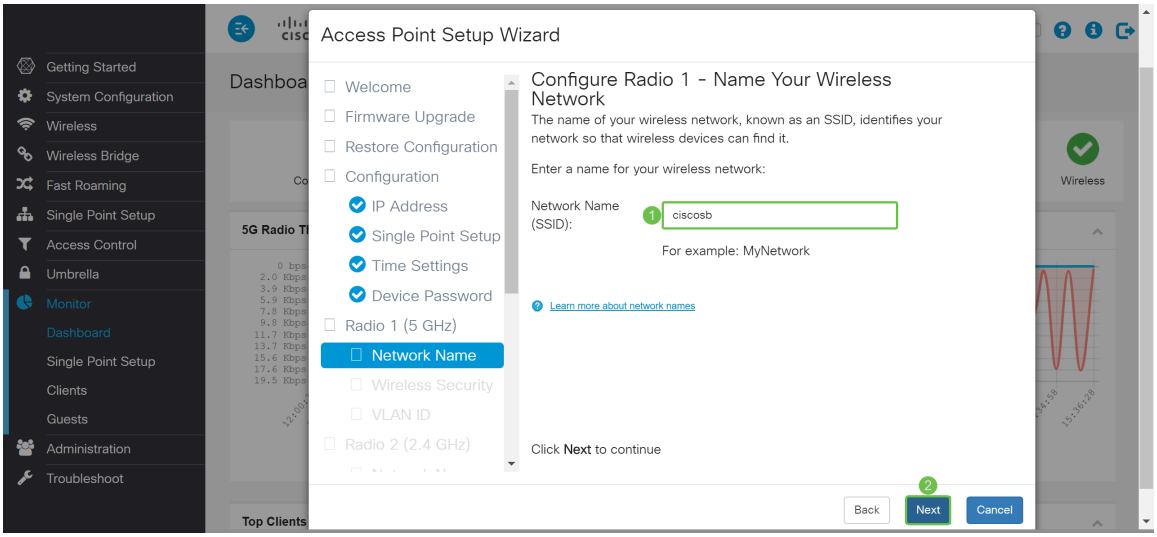
Schritt 8: Geben Sie einen neuen **Benutzernamen** in das Feld *Benutzername ein*. Standardmäßig lautet der Benutzername cisco. Geben Sie ein **neues Kennwort** für den *Benutzernamen ein*. Geben Sie dann erneut **Neues Kennwort** im Feld *Kennwort bestätigen ein*. Sie können die *Kennwortkomplexität* deaktivieren, um die Kennwortsicherheitsregeln zu deaktivieren. Es wird jedoch dringend empfohlen, die Kennwortsicherheitsregeln zu aktivieren. Das neue Kennwort muss den folgenden Komplexitätseinstellungen entsprechen:

- unterscheidet sich vom Benutzernamen.
- unterscheidet sich vom aktuellen Kennwort.
- Mindestens acht Zeichen lang.
- Enthält Zeichen aus mindestens drei Zeichenklassen (Großbuchstaben, Kleinbuchstaben, Zahlen und Sonderzeichen sind auf einer Standardtastatur verfügbar).

Klicken Sie anschließend auf **Weiter**, um *Radio 1* zu konfigurieren.



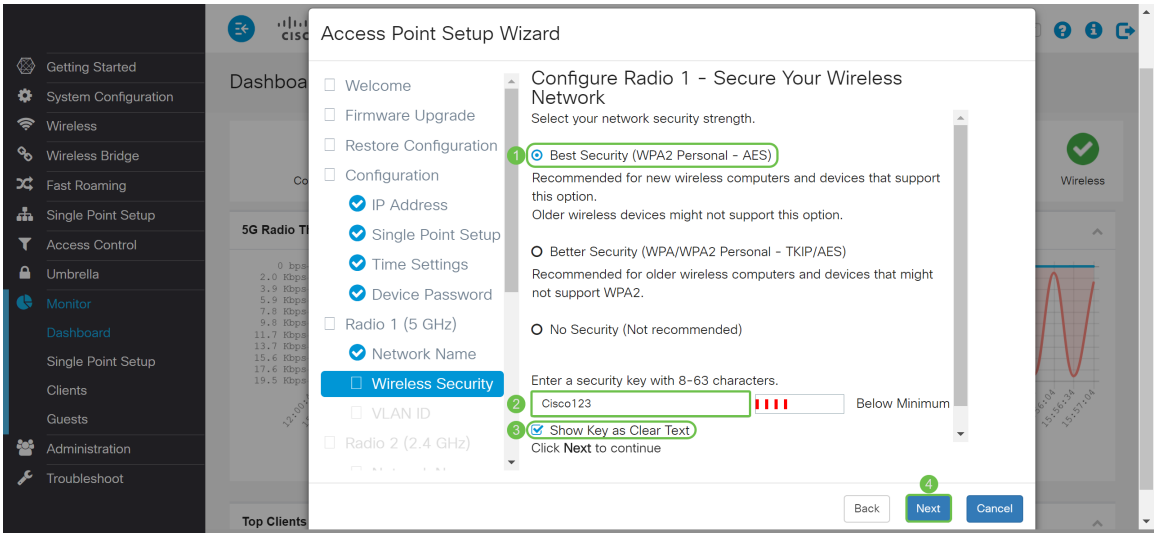
Schritt 9: Geben Sie im *Netzwerknamen (SSID)* einen Namen für Ihr Wireless-Netzwerk ein. So können Sie Ihr Netzwerk leichter identifizieren, sodass es von Wireless-Geräten gefunden werden kann. Standardmäßig wird **ciscosb** als Netzwerkname verwendet. Klicken Sie anschließend auf **Weiter**, um mit dem nächsten Abschnitt fortzufahren.



Schritt 10: Klicken Sie auf das Optionsfeld für die Netzwerksicherheit, die Sie auf Ihr Wireless-Netzwerk anwenden möchten. Geben Sie dann das Kennwort für Ihr Netzwerk im Feld *Sicherheitsschlüssel ein*. Um das Kennwort während der Eingabe anzuzeigen, aktivieren Sie das Kontrollkästchen **Schlüssel als** Text löschen. Klicken Sie auf **Weiter**, um fortzufahren.

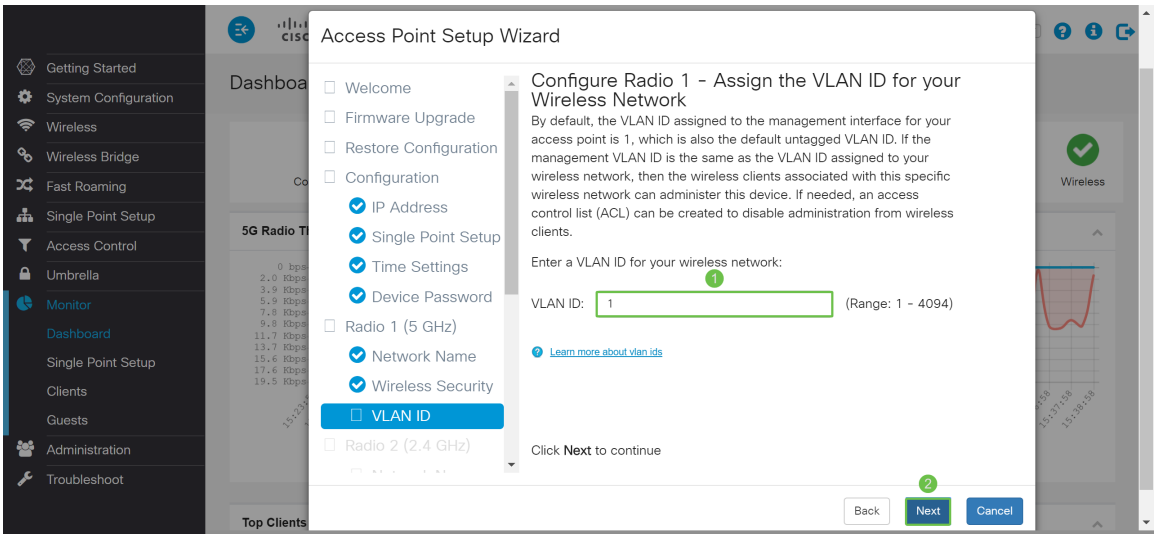
Hinweis: Wenn das Netzwerk über eine Mischung von Clients verfügt, von denen einige WPA2 und andere nur das ursprüngliche WPA unterstützen, wählen Sie beides (WPA/WPA2) aus. Dadurch können sowohl WPA- als auch WPA2-Client-Stationen eine Verbindung herstellen und authentifizieren. Für Clients, die diese Funktion unterstützen, wird jedoch das robustere WPA2 verwendet. Diese WPA-Konfiguration ermöglicht mehr Interoperabilität anstelle einiger Sicherheitsfunktionen.

- Beste Sicherheit (Wi-Fi Protected Access 2 (WPA2) Personal - Advanced Encryption Standard (AES)) Alle Client-Stationen im Netzwerk unterstützen den WPA2- und den Advanced Encryption Standard-Verschlüsselungsalgorithmus unter Verwendung des Counter Mode mit dem Cipher Block Chaining Message Authentication Code Protocol (AES-CCMP)-Verschlüsselungsprotokoll/-Sicherheitsprotokoll. Dies bietet die beste Sicherheit gemäß IEEE 802.11i-Standard. Gemäß den neuesten Anforderungen der Wi-Fi Alliance muss der Access Point diesen Modus ständig unterstützen.
- Höhere Sicherheit (WPA/WPA2 Personal - TKIP/AES) WPA Personal ist ein IEEE802.11i-Standard der Wi-Fi Alliance, der AES-CCMP- und TKIP-Verschlüsselung umfasst. Sie bietet Sicherheit, wenn ältere Wireless-Geräte das ursprüngliche WPA unterstützen, die neuere WPA2 jedoch nicht unterstützen.
- Keine Sicherheit (nicht empfohlen) Für das Wireless-Netzwerk ist kein Kennwort erforderlich, und jeder kann darauf zugreifen.

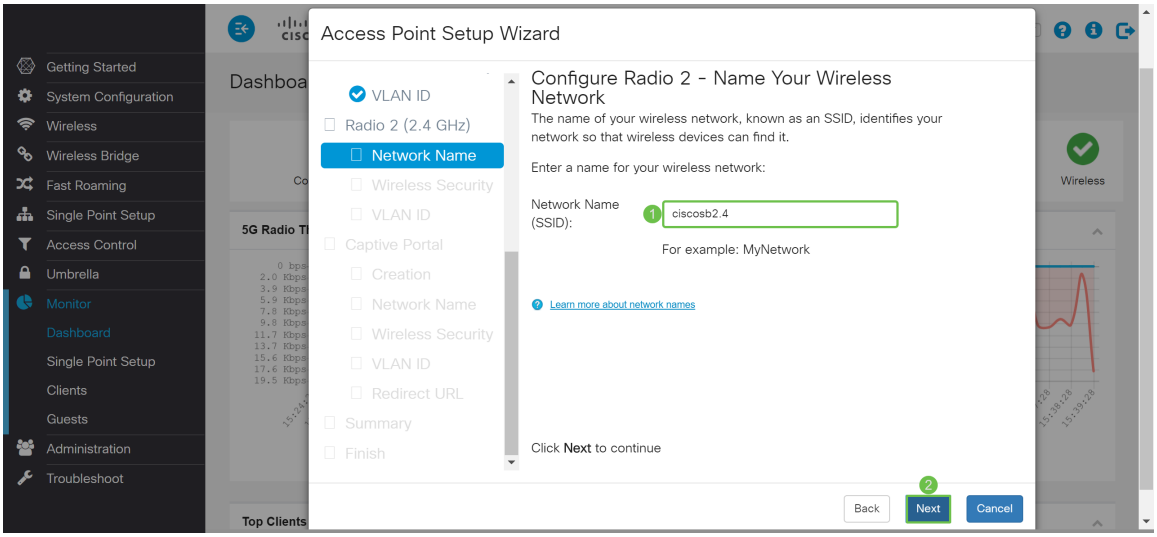


Schritt 11: Geben Sie im Feld *VLAN ID* die ID-Nummer des VLAN ein, zu dem das *Radio 1 (5 GHz)* gehören soll. In diesem Beispiel belassen wir die *VLAN-ID* als 1. Klicken Sie auf **Weiter**, um *Radio 2 (2,4 GHz)* zu konfigurieren.

Hinweis: Es wird empfohlen, dem Wireless-Datenverkehr eine andere VLAN-ID als die Standard-ID (1) zuzuweisen, um diese vom Management-Datenverkehr in VLAN 1 zu trennen. Klicken Sie hier, um mehr über Virtual Access Points (VAPs) zu erfahren.



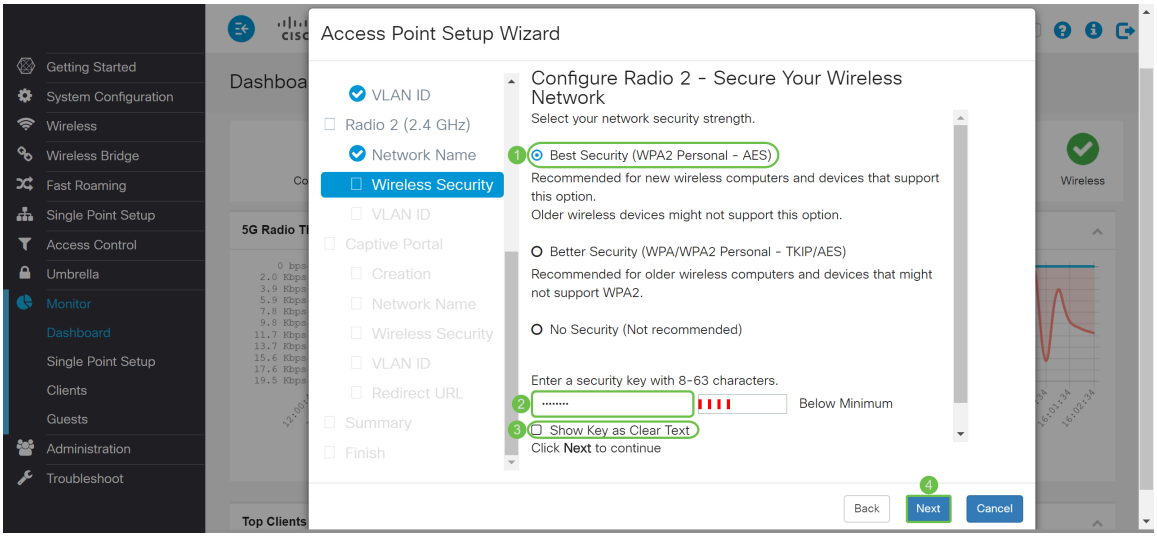
Schritt 12: Geben Sie im Feld *Netzwerkname (SSID)* einen neuen Netzwerknamen ein. Standardmäßig wird **ciscosb** verwendet. Der Netzwerkname wird als SSID bezeichnet. Er identifiziert Ihr Netzwerk, damit die Wireless-Geräte ihn finden können. In diesem Beispiel wurde **ciscosb2.4** verwendet, um den 5-GHz-Netzwerknamen zu unterscheiden. Klicken Sie auf **Weiter**, um die Wireless-Sicherheit für *Radio 2 (2,4 GHz)* zu konfigurieren.



Schritt 13: Klicken Sie auf das Optionsfeld für die Netzwerksicherheit, die Sie auf Ihr Wireless-Netzwerk anwenden möchten. Geben Sie dann das Kennwort für Ihr Netzwerk im Feld *Sicherheitsschlüssel ein*. Um das Kennwort während der Eingabe anzuzeigen, aktivieren Sie das Kontrollkästchen **Schlüssel als** Text löschen. Die **Option Schlüssel als Klartext anzeigen** ist standardmäßig aktiviert. Klicken Sie auf **Weiter**, um fortzufahren.

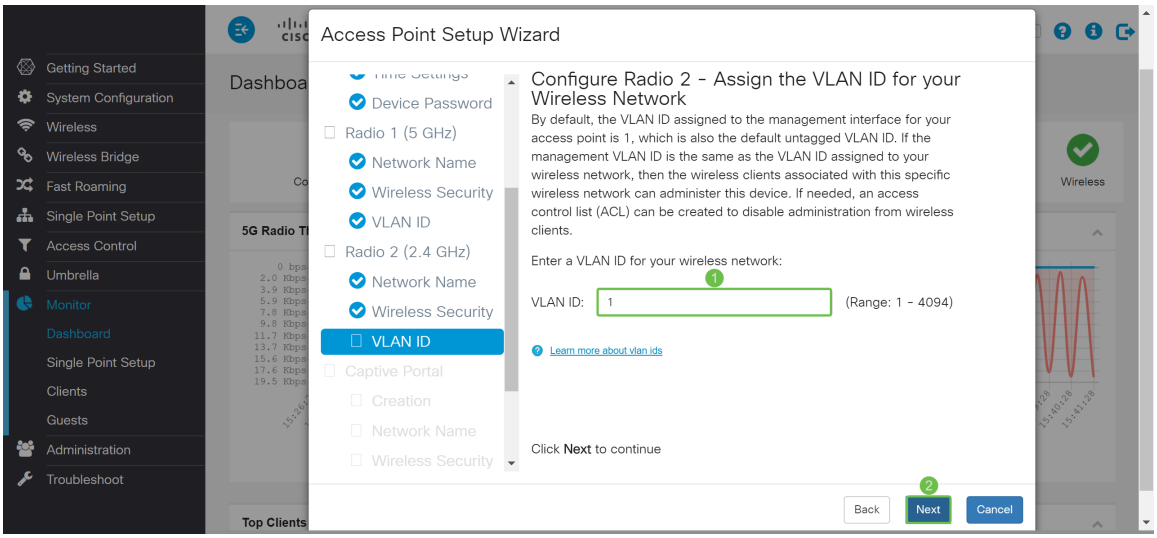
Hinweis: Wenn das Netzwerk über eine Mischung von Clients verfügt, von denen einige WPA2 und andere nur das ursprüngliche WPA unterstützen, wählen Sie beides (WPA/WPA2) aus. Dadurch können sowohl WPA- als auch WPA2-Client-Stationen eine Verbindung herstellen und authentifizieren. Für Clients, die diese Funktion unterstützen, wird jedoch das robustere WPA2 verwendet. Diese WPA-Konfiguration ermöglicht mehr Interoperabilität anstelle einiger Sicherheitsfunktionen.

- Beste Sicherheit (Wi-Fi Protected Access 2 (WPA2) Personal - Advanced Encryption Standard (AES)) Alle Client-Stationen im Netzwerk unterstützen den WPA2- und den Advanced Encryption Standard-Verschlüsselungsalgorithmus unter Verwendung des Counter Mode mit dem Cipher Block Chaining Message Authentication Code Protocol (AES-CCMP)-Verschlüsselungsprotokoll/-Sicherheitsprotokoll. Dies bietet die beste Sicherheit gemäß IEEE 802.11i-Standard. Gemäß den neuesten Anforderungen der Wi-Fi Alliance muss der Access Point diesen Modus ständig unterstützen.
- Höhere Sicherheit (WPA/WPA2 Personal - TKIP/AES) WPA Personal ist ein IEEE802.11i-Standard der Wi-Fi Alliance, der AES-CCMP- und TKIP-Verschlüsselung umfasst. Sie bietet Sicherheit, wenn ältere Wireless-Geräte das ursprüngliche WPA unterstützen, die neuere WPA2 jedoch nicht unterstützen.
- Keine Sicherheit (nicht empfohlen) Für das Wireless-Netzwerk ist kein Kennwort erforderlich, und jeder kann darauf zugreifen.

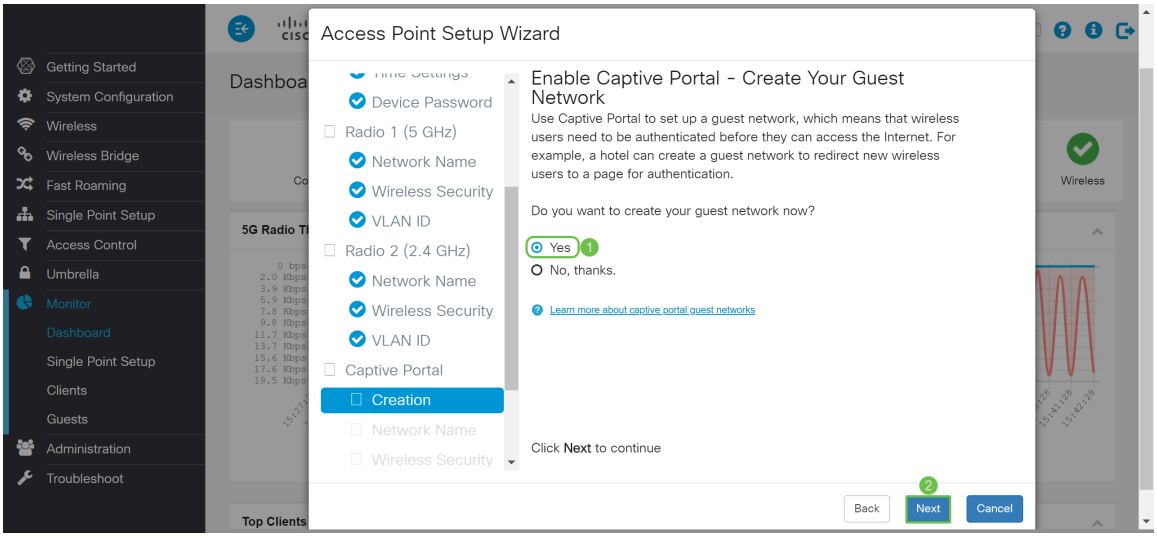


Schritt 14: Geben Sie im Feld *VLAN ID* die ID-Nummer des VLAN ein, zu dem das *Radio 1 (2,4 GHz)* gehören soll. In diesem Beispiel wird der Standardwert 1 als *VLAN-ID* verwendet. Klicken Sie auf **Weiter**, um *Captive Portal* zu konfigurieren.

Hinweis: Es wird empfohlen, dem Wireless-Datenverkehr eine andere VLAN-ID als die Standard-ID (1) zuzuweisen, um diese vom Management-Datenverkehr in VLAN 1 zu trennen. Klicken Sie hier, um mehr über Virtual Access Points (VAPs) zu erfahren.

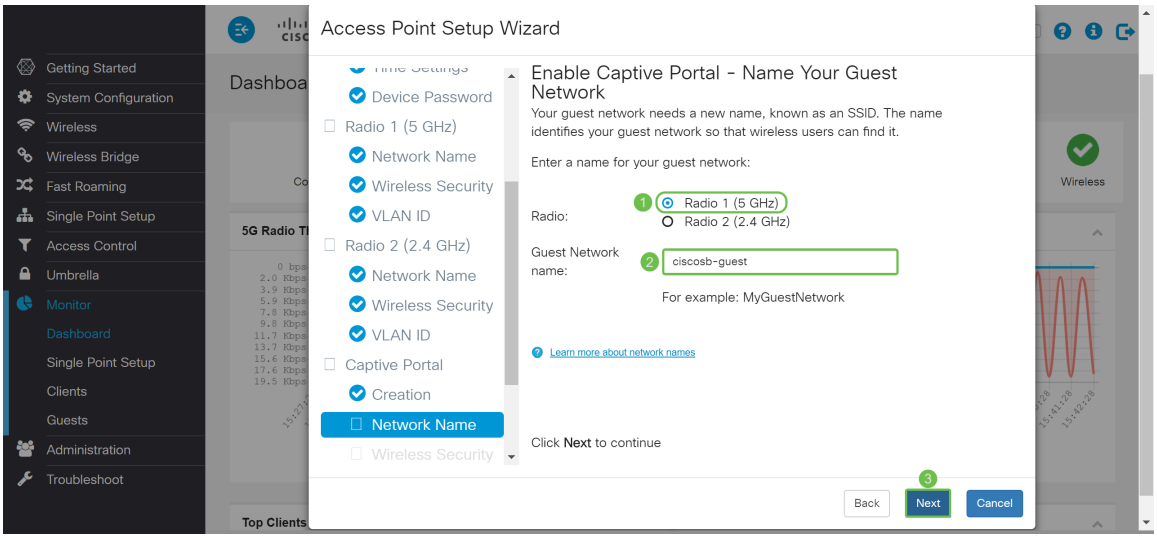


Schritt 15: (Optional) Ein Gastnetzwerk ist nicht erforderlich. Klicken Sie auf das Optionsfeld **Ja**, wenn Sie ein Gastnetzwerk erstellen möchten. Klicken Sie auf das Optionsfeld **Nein**, wenn Sie kein Gastnetzwerk erstellen möchten, und fahren Sie mit Schritt 20 fort. Klicken Sie auf die Schaltfläche **Weiter**, um fortzufahren.



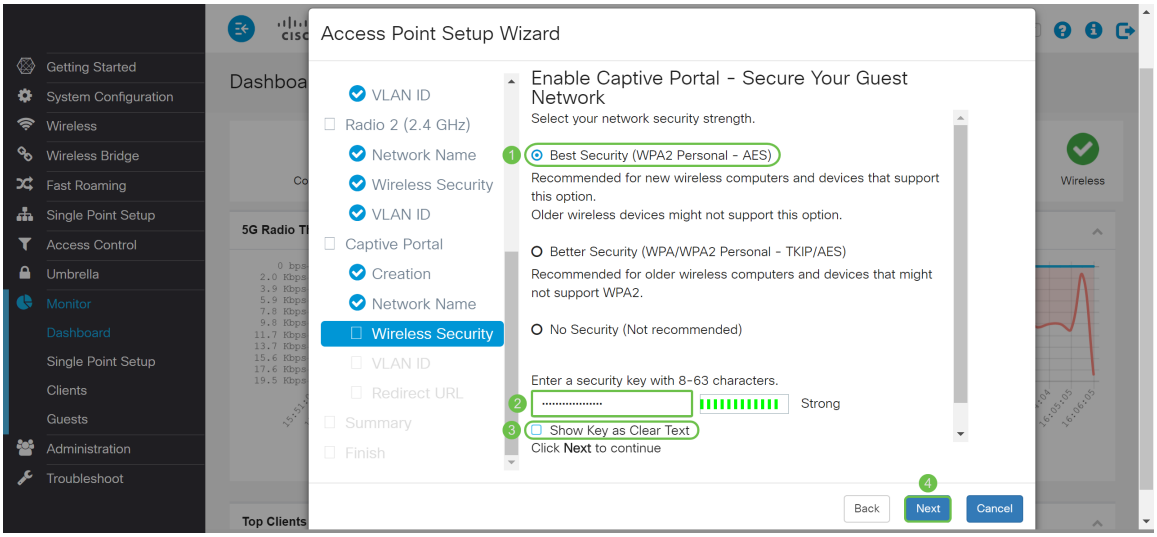
Schritt 16: (Optional) Wählen Sie das Optionsfeld aus, das dem *Radio* (*Funkmodul)* entspricht, in dem Sie das Gastnetzwerk platzieren möchten. Erstellen Sie dann im Feld *Gastnetzwerk* einen Netzwerknamen. Klicken Sie auf **Weiter**, um die *Wireless*-Sicherheitseinstellungen für das *Gastnetzwerk* zu konfigurieren.

In diesem Beispiel wählen wir **Radio 1 (5 GHz)** als unser *Radio aus* und belassen den Standard-Netzwerknamen als **ciscosb-guest,** damit Ihre Wireless-Gastbenutzer den Netzwerknamen finden können.

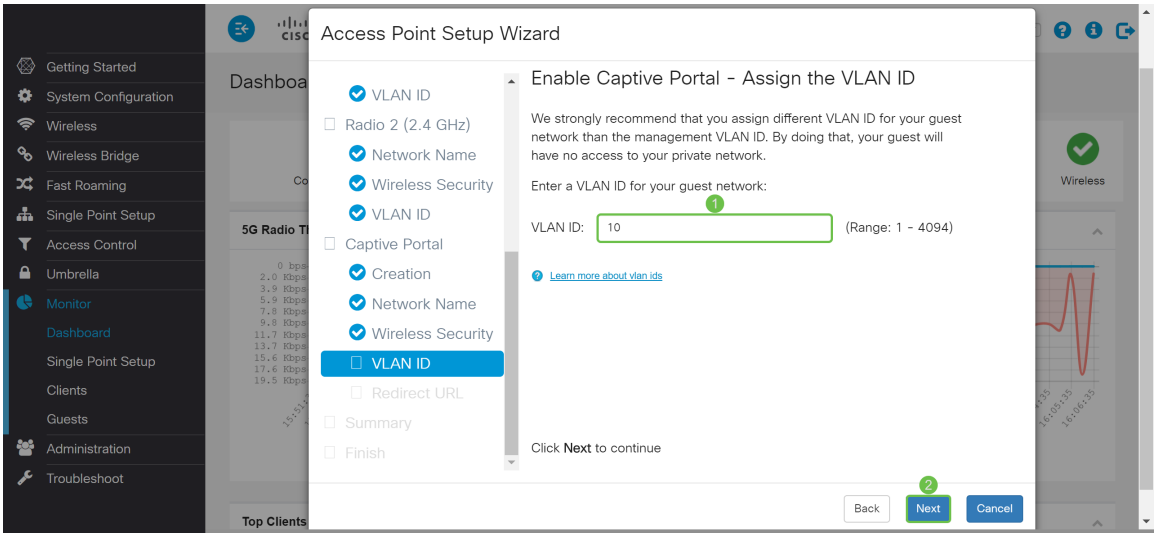


Schritt 17: (Optional) Wählen Sie das Optionsfeld aus, das der Netzwerksicherheit entspricht, die Sie auf Ihr Gastnetzwerk anwenden möchten. Geben Sie dann ggf. ein Kennwort für das Gastnetzwerk in das *Sicherheitsschlüsselfeld ein*. Um **Schlüssel als Klartext anzeigen**, aktivieren Sie das Kontrollkästchen, um den Sicherheitsschlüssel als Klartext anzuzeigen. Dies ist standardmäßig aktiviert. Klicken Sie auf **Weiter**, um fortzufahren. Die Netzwerksicherheitsoptionen sind:

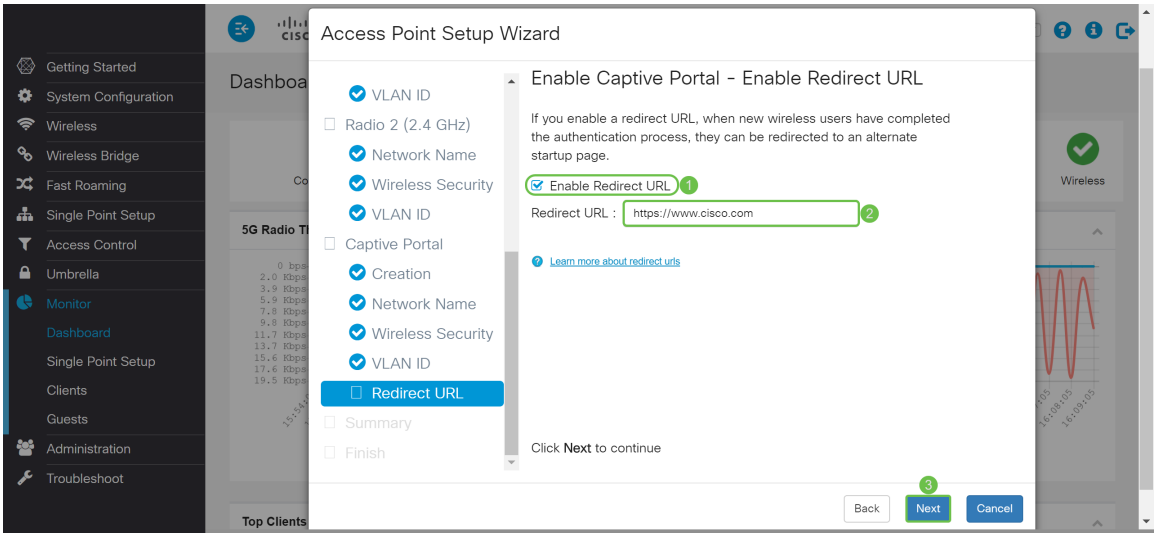
- Best Security (WPA2 Personal - AES) - Empfohlen für neue Wireless-Computer und -Geräte, die diese Option unterstützen.
- Starke Sicherheit (WPA/WPA2 Personal - TKIP/AES) - Empfohlen für ältere Wireless-Computer und -Geräte, die WPA2 möglicherweise nicht unterstützen.
- Keine Sicherheit (Nicht empfohlen) - Dies ist die Standardauswahl.



Schritt 18: (Optional) Geben Sie eine *VLAN-ID* für das Gastnetzwerk an. Die VLAN-ID des Gastnetzwerks sollte sich von der Management-VLAN-ID unterscheiden. In diesem Beispiel wurde die *VLAN-ID* **10** als unsere VLAN-ID für das Gastnetzwerk verwendet. Klicken Sie auf **Weiter**, um die *Umleitungs-URL* für das Gastnetzwerk zu konfigurieren.

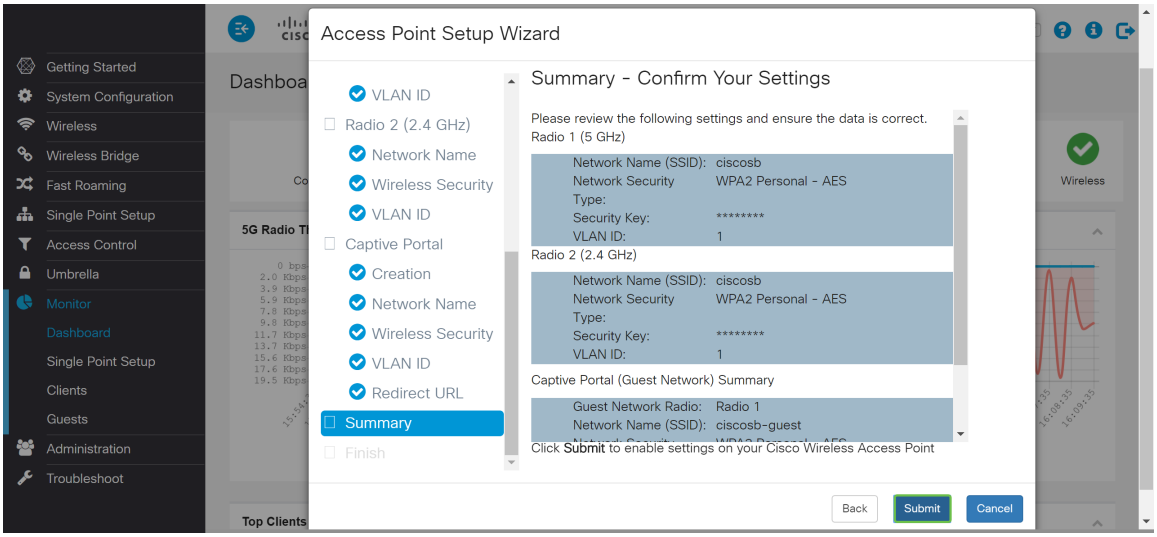


Schritt 19: (Optional) Aktivieren Sie das Kontrollkästchen **Umleitung aktivieren**, um neue Wireless-Benutzer auf eine andere Startseite umzuleiten. Geben Sie einen vollqualifizierten Domänennamen (Fully Qualified Domain Name, FQDN) oder eine IP-Adresse in das Feld *Redirect URL* (einschließlich http:// oder https://) ein. Klicken Sie anschließend auf **Weiter**, um zur *Zusammenfassungsseite* zu gelangen.

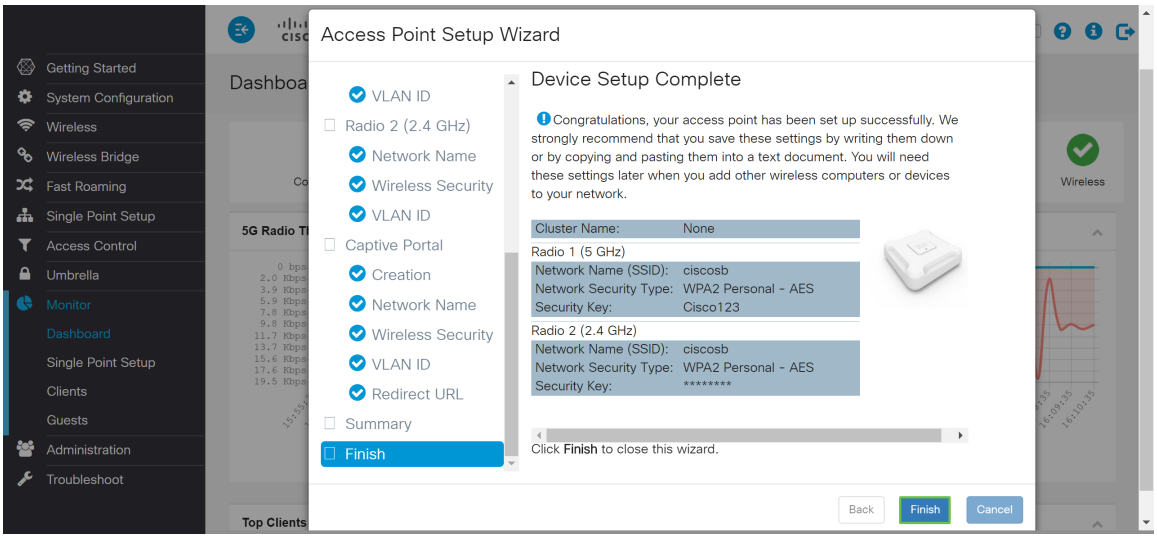


Schritt 20: Überprüfen Sie auf der Seite *Zusammenfassung - Bestätigen Sie Ihre Einstellungen* die

von Ihnen konfigurierten Einstellungen. Klicken Sie auf die Schaltfläche **Zurück**, um eine oder mehrere Einstellungen neu zu konfigurieren. Wenn Sie auf **Abbrechen** klicken, werden alle Einstellungen auf die vorherigen oder Standardwerte zurückgesetzt. Wenn Ihre Konfigurationen korrekt sind, klicken Sie auf **Senden**. Ihre Setup-Einstellungen werden gespeichert, und ein Bestätigungsfenster wird angezeigt.



Schritt 21: Nach der Konfiguration der Einstellungen wird die Seite *Device Setup Complete (Geräte-Setup abgeschlossen)* angezeigt, auf der Sie wissen, dass der Access Point erfolgreich eingerichtet wurde. Klicken Sie auf **Fertig stellen**, um sich erneut mit dem neuen Kennwort anzumelden.



Schlussfolgerung

Sie haben jetzt erfolgreich Ihren WAP mit dem Setup-Assistenten konfiguriert. Sie sollten Ihre soeben konfigurierten SSIDs in Ihrer Liste der Wi-Fi-Netzwerke sehen. Um andere Funktionen auf dem WAP zu konfigurieren, müssen Sie sich erneut anmelden.