Konfigurieren von RADIUS in Cisco Business Wireless Access Point

Ziel

In diesem Dokument wird erläutert, wie Sie RADIUS in Cisco Business Wireless Access Point (CBW) konfigurieren.

Unterstützte Geräte | Firmware-Version

- 140AC (Datenblatt) | 10.4.1.0 (Laden Sie die aktuelle Version herunter)
- 145AC (Datenblatt) | 10.4.1.0 (Laden Sie die aktuelle Version herunter)
- 240AC (Datenblatt) | 10.4.1.0 (Laden Sie die aktuelle Version herunter)

Einführung

Wenn Sie RADIUS in Ihrem CBW AP konfigurieren möchten, sind Sie hier genau richtig! Die CBW APs unterstützen den neuesten 802.11ac Wave 2-Standard für höhere Leistung, besseren Zugriff und Netzwerke mit höherer Dichte. Sie bieten branchenführende Leistung mit hochsicheren und zuverlässigen Wireless-Verbindungen für eine robuste mobile Endbenutzerumgebung.

Der Remote Authentication Dial-In User Service (RADIUS) ist ein Authentifizierungsmechanismus für Geräte, die eine Verbindung mit einem Netzwerkdienst herstellen und diesen verwenden. Sie wird für zentralisierte Authentifizierungs-, Autorisierungs- und Abrechnungszwecke verwendet. Ein RADIUS-Server regelt den Zugriff auf das Netzwerk, indem er die Identität der Benutzer mithilfe der eingegebenen Anmeldeinformationen überprüft. So wird beispielsweise ein öffentliches Wi-Fi-Netzwerk auf einem Universitätsgelände installiert. Nur Schüler mit Passwort können auf diese Netzwerke zugreifen. Der RADIUS-Server überprüft die von den Benutzern eingegebenen Kennwörter und gewährt bzw. verweigert den Zugriff auf das Wireless Local Area Network (WLAN).

Wenn Sie bereit sind, RADIUS auf Ihrem CBW-Zugangspunkt zu konfigurieren, lassen Sie uns anfangen!

Inhalt

Konfigurieren von RADIUS in Ihrem CBW AP

In diesem umblätterten Abschnitt finden Sie Tipps für Anfänger.

Anmeldung

Melden Sie sich bei der Webbenutzeroberfläche des primären Access Points an. Öffnen Sie dazu einen Webbrowser, und geben Sie https://ciscobusiness.cisco ein. Möglicherweise erhalten Sie eine Warnung, bevor Sie fortfahren. Geben Sie Ihre Anmeldeinformationen ein. Sie können auch

auf den primären Access Point zugreifen, indem Sie https://[ipaddress] (des primären Access Points) in einen Webbrowser eingeben.

Quick-Info

Wenn Sie Fragen zu einem Feld in der Benutzeroberfläche haben, suchen Sie nach einem Tooltipp, der wie folgt aussieht:

Probleme beim Auffinden des Symbols "Hauptmenü erweitern"?

Navigieren Sie zum Menü auf der linken Seite des Bildschirms. Wenn Sie die Menütaste nicht sehen, klicken Sie auf dieses Symbol, um das Menü auf der Seitenleiste zu öffnen.

Cisco Business-App

Diese Geräte verfügen über begleitende Apps, die einige Verwaltungsfunktionen mit der Webbenutzeroberfläche teilen. Nicht alle Funktionen der Webbenutzeroberfläche sind in der App verfügbar.

iOS-App herunterladen Android-App herunterladen

Häufig gestellte Fragen

Wenn Sie immer noch offene Fragen haben, können Sie sich unser Dokument mit häufig gestellten Fragen ansehen. Häufig gestellte Fragen

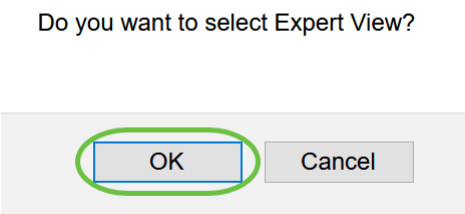
Schritt 1

Melden Sie sich mit einem gültigen Benutzernamen und Kennwort beim CBW AP an.

Schritt 2

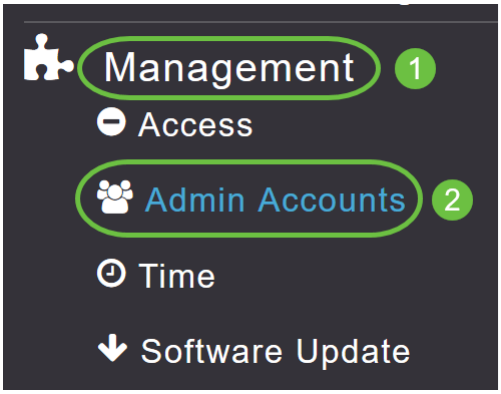
Klicken Sie auf das **bidirektionale Pfeil** oben auf der Webbenutzeroberfläche, um *zur Expertenansicht* zu *wechseln*.

Sie sehen den folgenden Popup-Bildschirm. Klicken Sie auf **OK**, um fortzufahren.



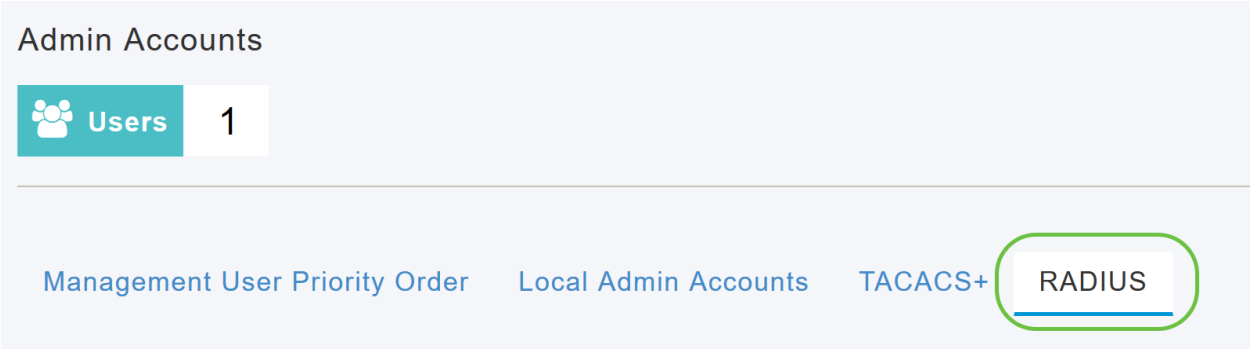
Schritt 3

Navigieren Sie zu **Verwaltung > Administratorkonten**.



Schritt 4

Um die RADIUS-Server hinzuzufügen, klicken Sie auf die Registerkarte **RADIUS**.

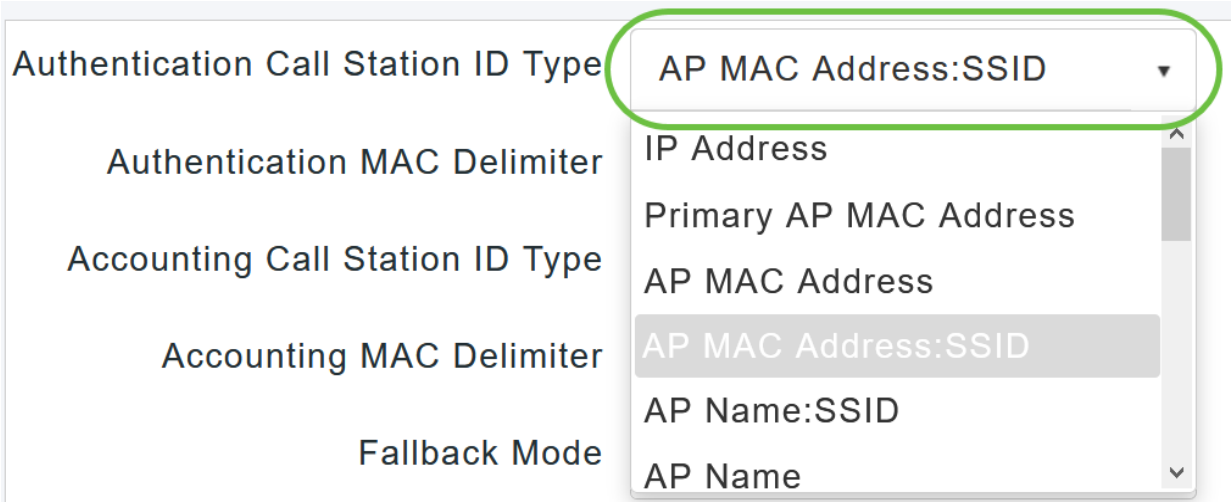


Schritt 5

Wählen Sie aus der Dropdown-Liste *Authentication Call Station ID Type (Authentifizierungs-*

Anrufstation-ID-Typ) die Option aus, die in der Access-Request-Nachricht an den RADIUS-Server gesendet wird. Folgende Optionen sind verfügbar:

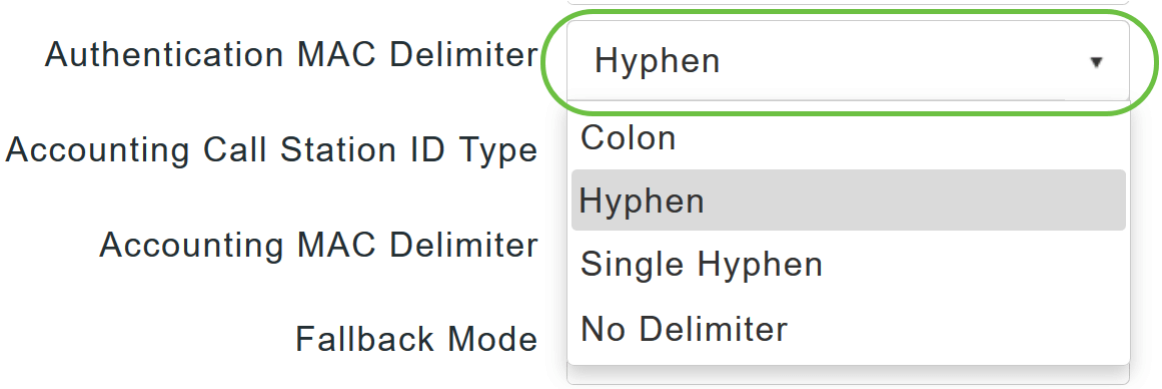
- *IP-Adresse*
- *Primäre AP-MAC-Adresse*
- *AP-MAC-Adresse*
- *AP-MAC-Adresse: SSID*
- *AP-Name:SSID*
- *AP-Name*
- *AP-Gruppe*
- *Flex-Gruppe*
- *AP-Standort*
- *VLAN-ID*
- *AP-Ethernet-MAC-Adresse*
- *AP-Ethernet-MAC-Adresse: SSID*
- *AP-Label-Adresse*
- *AP-Label-Adresse: SSID*
- *AP-MAC: SSID-AP-Gruppe*
- *AP Eth MAC:SSID AP-Gruppe*



Schritt 6

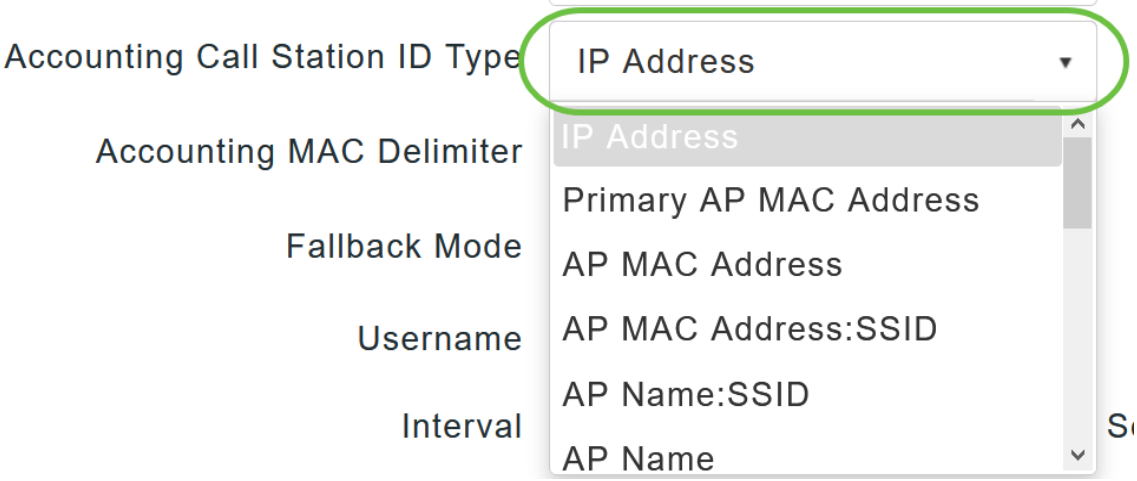
Wählen Sie aus der Dropdown-Liste den *MAC Delimiter für die Authentifizierung* aus. Folgende Optionen sind verfügbar:

- *Doppelpunkt*
- *Bindestrich*
- *Singlestrich*
- *Kein Delimiter*



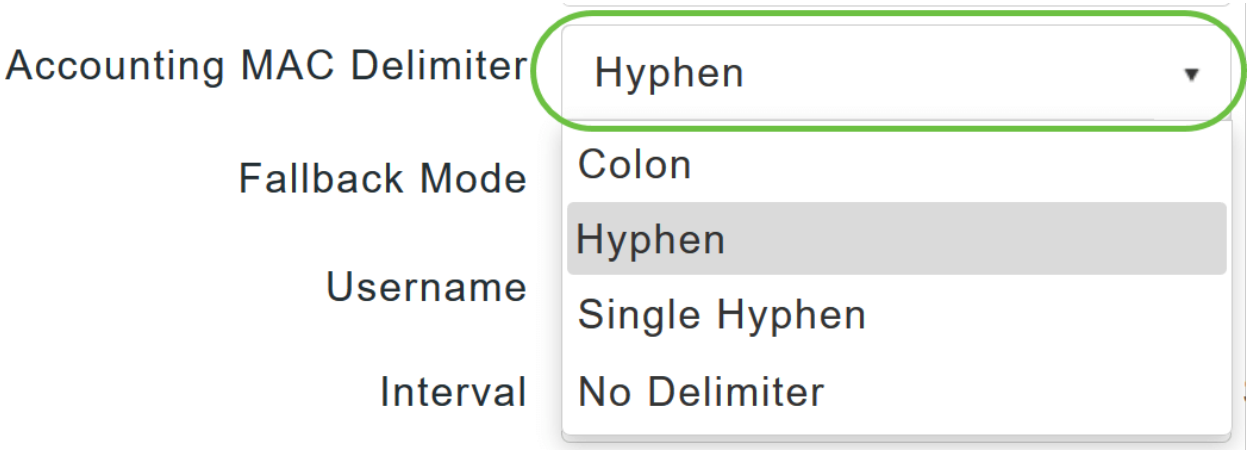
Schritt 7

Wählen Sie aus der Dropdown-Liste den *ID-Typ* der *Buchhaltungsanrufstation* aus.



Schritt 8

Wählen Sie den *MAC Delimiter für die Buchhaltung* aus der Dropdown-Liste aus.



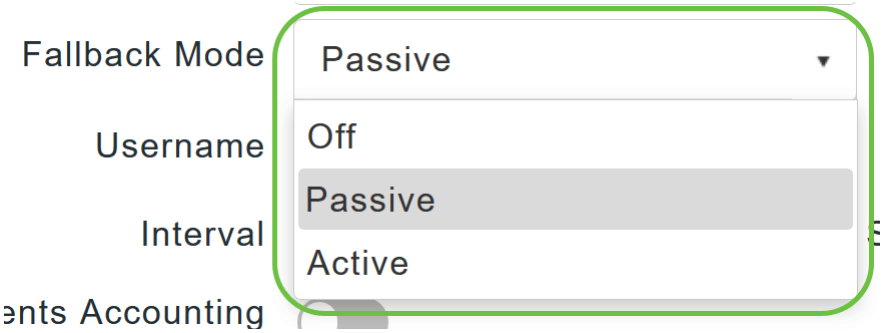
Schritt 9

Geben Sie den RADIUS-Server-*Fallbackmodus* aus der Dropdown-Liste an. Dabei kann es sich um Folgendes handeln:

- *Aus* - Deaktiviert den RADIUS-Serverfallback. Dies ist der Standardwert.
- *Passiv* - Der primäre Access Point kehrt zu einem Server mit einer niedrigeren Priorität von

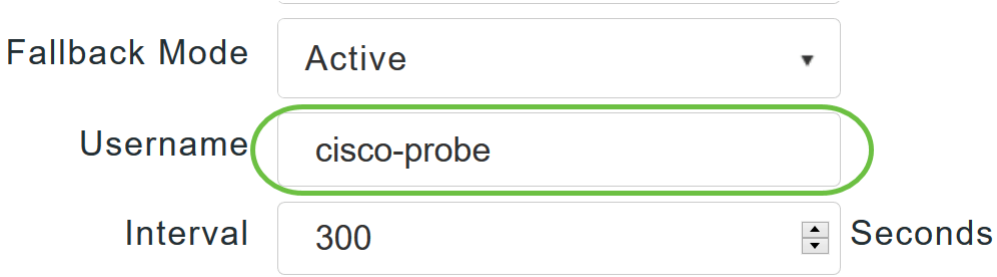
den verfügbaren Backup-Servern zurück, ohne dass externe Überprüfungsmeldungen verwendet werden. Der primäre Zugangspunkt ignoriert alle inaktiven Server für einen bestimmten Zeitraum und versucht es zu einem späteren Zeitpunkt erneut, wenn eine RADIUS-Nachricht gesendet werden muss.

- *Aktiv* - Der primäre Access Point kehrt von den verfügbaren Backup-Servern zu einem Server mit niedrigerer Priorität zurück, indem er anhand von RADIUS-Abfragemeldungen proaktiv feststellt, ob ein als inaktiv markierter Server wieder online ist. Der primäre Access Point ignoriert alle inaktiven Server für alle aktiven RADIUS-Anfragen. Sobald der primäre Server eine Antwort vom wiederhergestellten ACS-Server erhält, sendet der aktive Fall-Back-RADIUS-Server keine Sondennachrichten mehr an den Server, der die aktive Sondenauthentifizierung anfordert.



Schritt 10

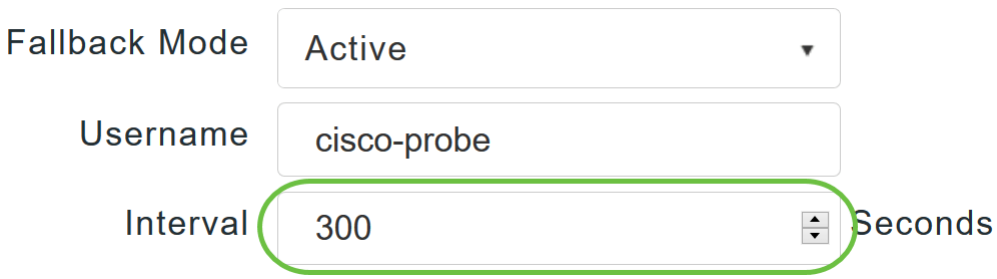
Wenn Sie *Active Fallback Mode (Aktiver Fallback-Modus)* aktiviert haben, geben Sie den Namen für das Senden in die inaktiven Serverproben im Feld *Username (Benutzername) ein*.



Sie können bis zu 16 numerische alphanumerische Zeichen eingeben. Der Standardwert ist **cisco-probe**.

Schritt 11

Wenn Sie den *aktiven Fallbackmodus* aktiviert haben, geben Sie den Wert für das Abfrageintervall (in Sekunden) in das Feld Intervall ein. Das Intervall dient im passiven Modus als inaktive Zeit und im aktiven Modus als Sondierungsintervall.

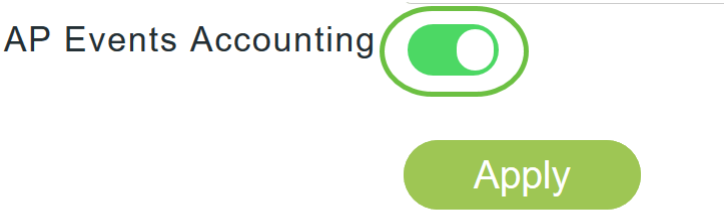


Der gültige Bereich liegt zwischen 180 und 3600 Sekunden, der Standardwert ist **300** Sekunden.

Schritt 12

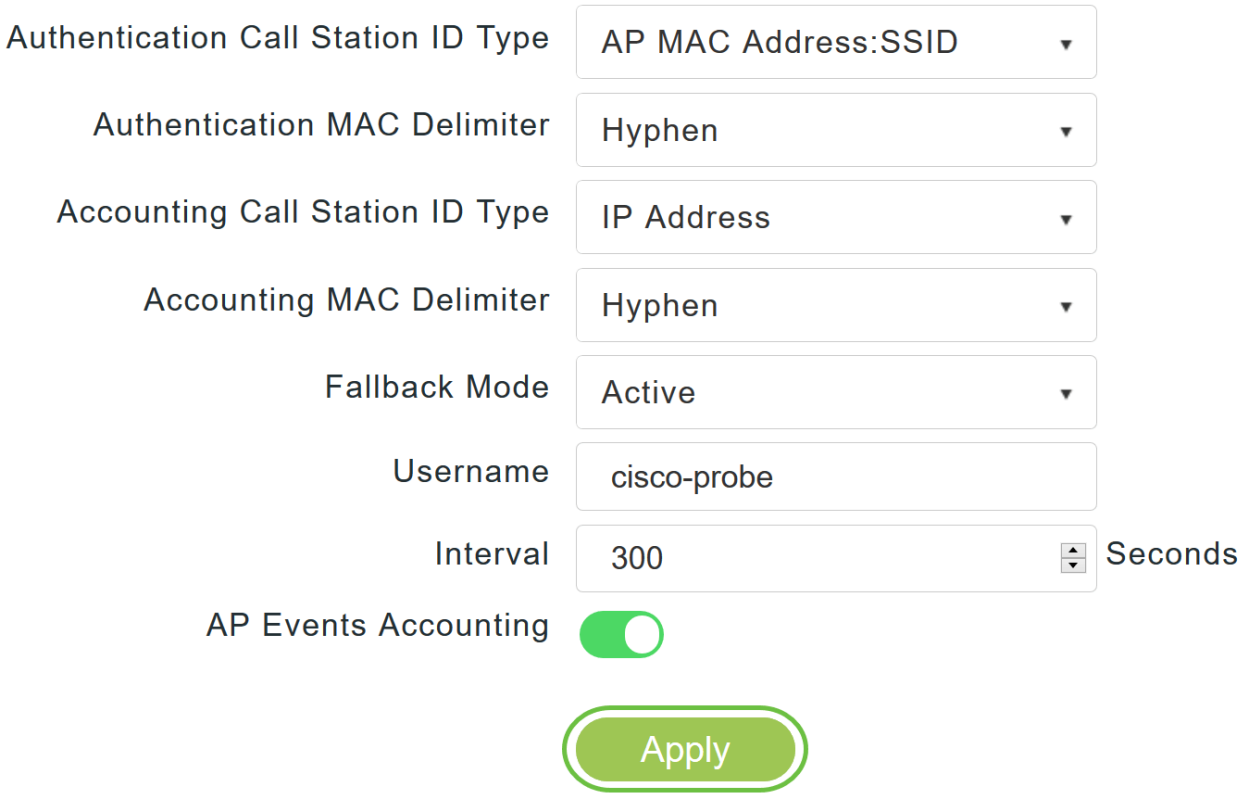
Aktivieren Sie den Schieberegler für die *AP-Ereignisabrechnung*, um das Senden von Abrechnungsanfragen an den RADIUS-Server zu aktivieren.

Bei Netzwerkproblemen schließen sich die APs dem primären Access Point an bzw. trennen ihn von diesem. Durch Aktivieren dieser Option wird sichergestellt, dass diese Ereignisse überwacht und die Accounting-Anforderungen an den RADIUS-Server gesendet werden, um Ihnen bei der Erkennung von Netzwerkproblemen zu helfen.



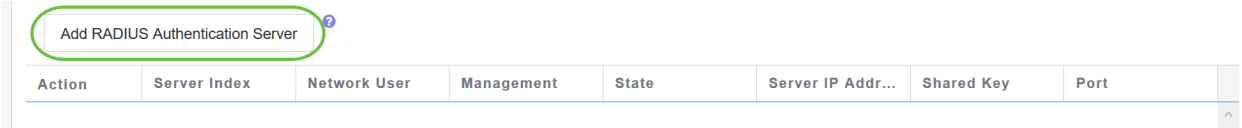
Schritt 13

Klicken Sie auf **Apply** (Anwenden).



Schritt 14

Um den RADIUS-Authentifizierungsserver zu konfigurieren, klicken Sie auf **RADIUS Authentication Server hinzufügen**.

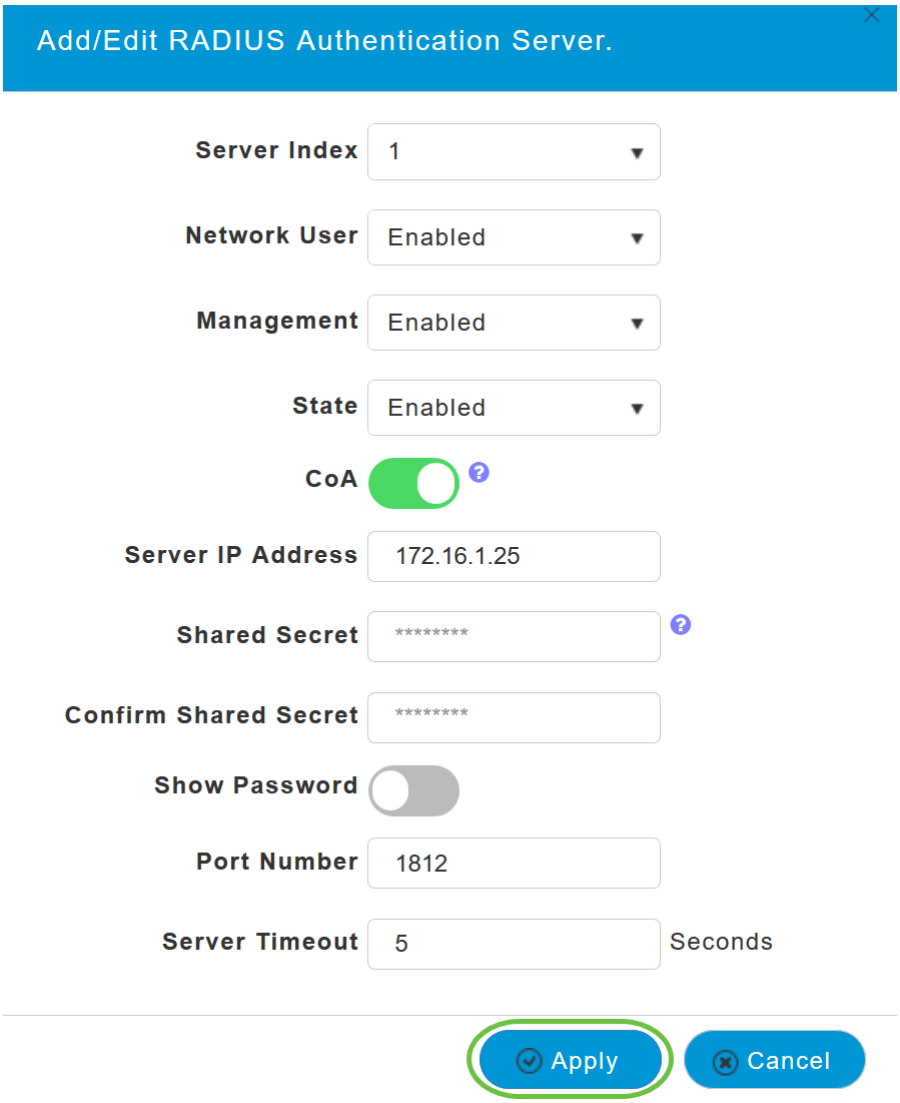


Schritt 15

Konfigurieren Sie im Popup-Fenster *RADIUS-Authentifizierung hinzufügen/bearbeiten* Folgendes:

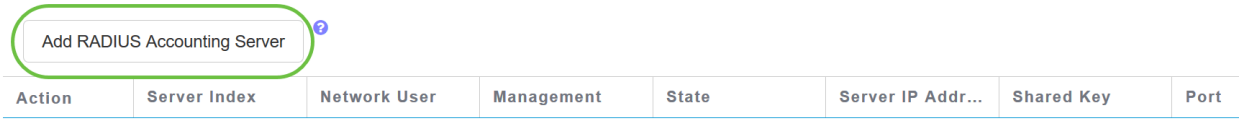
- *Serverindex* - Wählen Sie 1 bis 6 aus.
- *Netzwerkbenutzer*: Aktivieren Sie den Status. Standardmäßig ist diese Option aktiviert.
- *Management*: Aktivieren Sie den Status. Standardmäßig ist diese Option aktiviert.
- *Status*: Aktivieren Sie den Status. Standardmäßig ist diese Option aktiviert.
- *CoA*: Sie können diese Option aktivieren, indem Sie den Schieberegler verschieben.
- *Server-IP-Adresse* - Geben Sie die IPv4-Adresse des RADIUS-Servers ein.
- *Shared Secret* - Geben Sie den gemeinsamen geheimen Schlüssel ein.
- *Portnummer*: Geben Sie die Portnummer ein, die für die Kommunikation mit dem RADIUS-Server verwendet wird.
- *Server Timeout* - Geben Sie das Server-Timeout ein.

Klicken Sie auf **Apply** (Anwenden).



Schritt 16

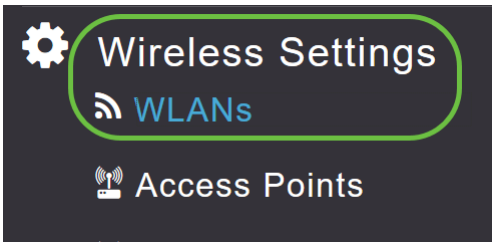
Um *RADIUS Accounting Server* hinzuzufügen, gehen Sie wie in Schritt 15 vor, da die Seite ähnliche Felder enthält.



WLAN konfigurieren

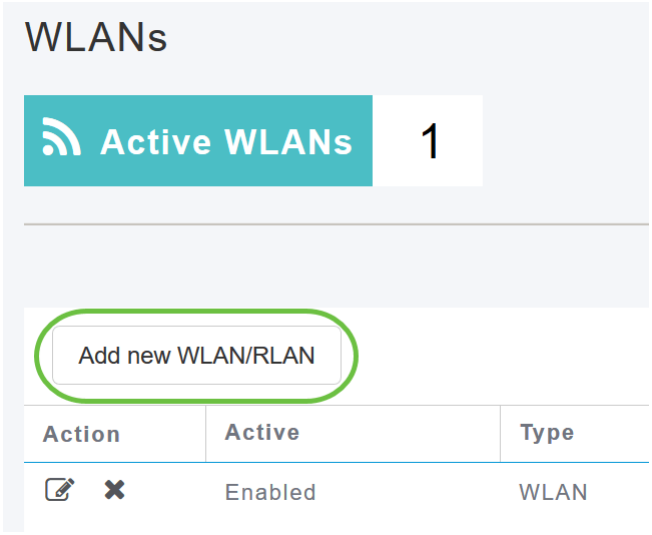
Schritt 1

Um ein WLAN zu konfigurieren, das die WPA2-Authentifizierung mit RADIUS behandelt, navigieren Sie zu **Wireless settings > WLAN**.



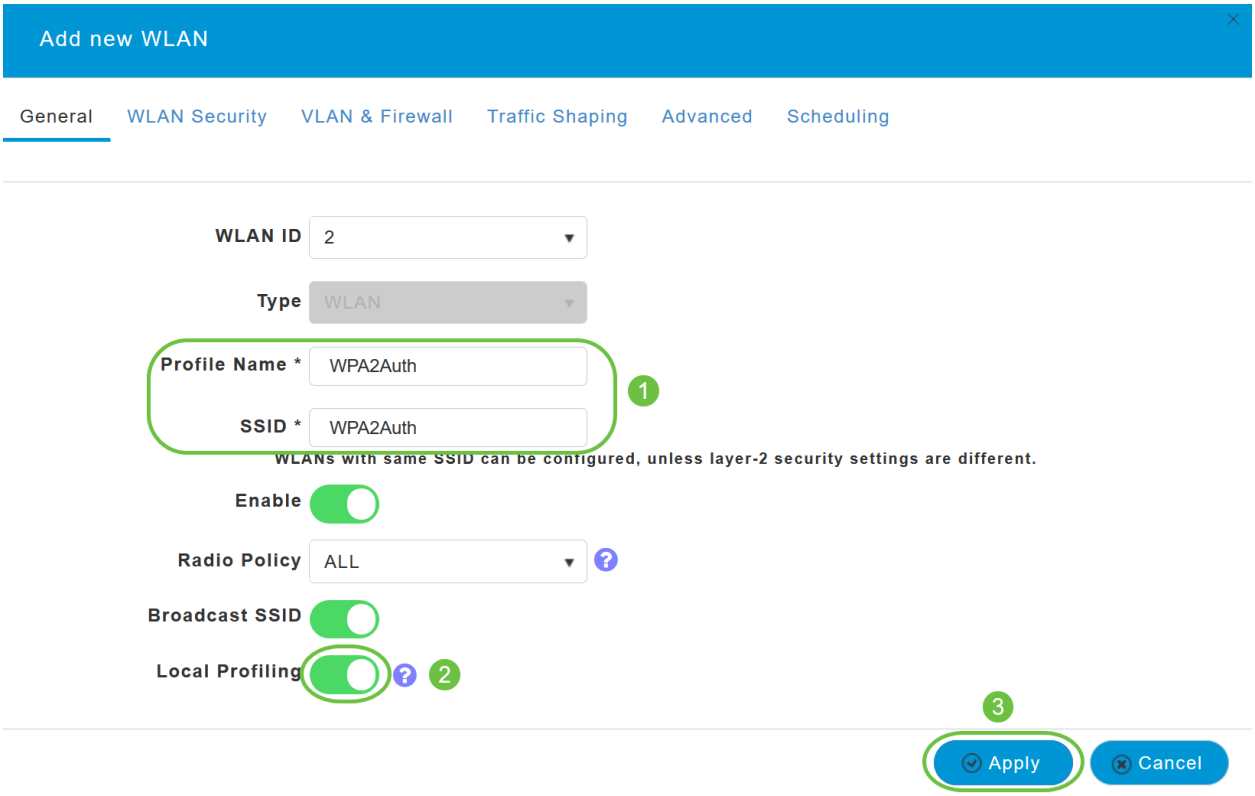
Schritt 2

Klicken Sie auf **Neues WLAN/RLAN hinzufügen**.



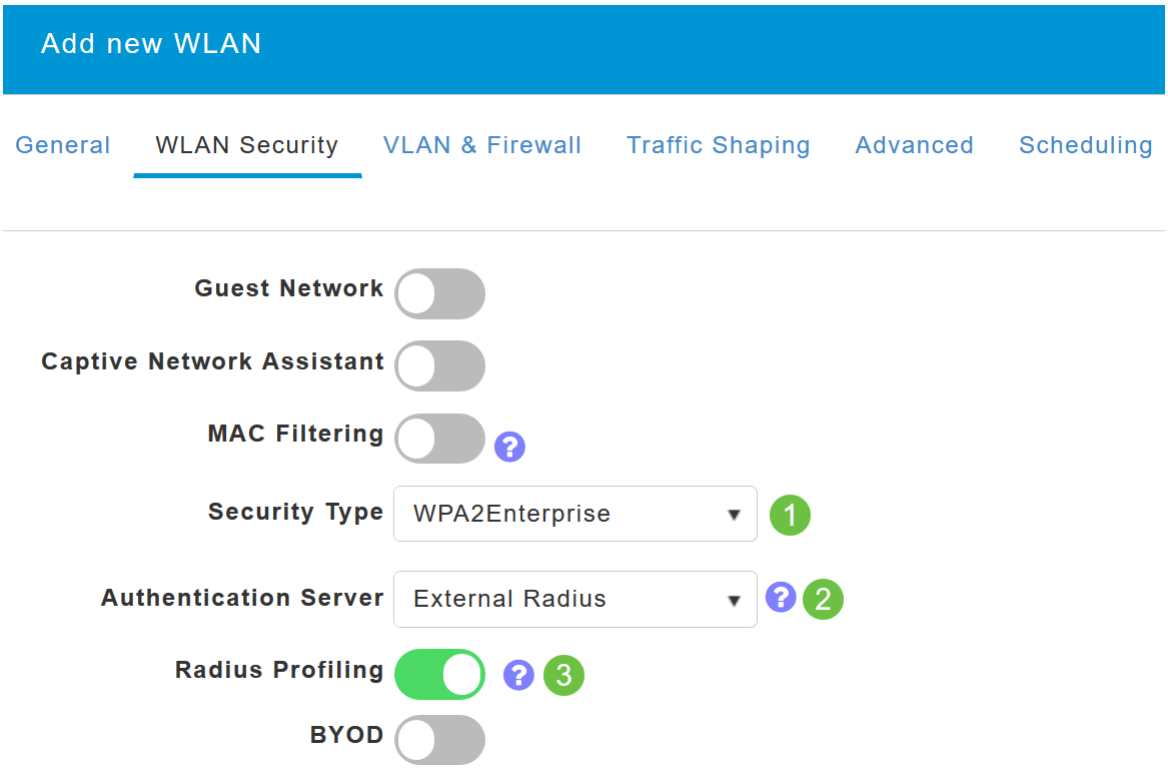
Schritt 3

Geben Sie auf der Registerkarte *Allgemein* den *Profilnamen ein*. Das *SSID*-Feld wird automatisch ausgefüllt. Sie können *Lokale Profilerstellung* aktivieren. Klicken Sie auf **Apply** (Anwenden).



Schritt 4

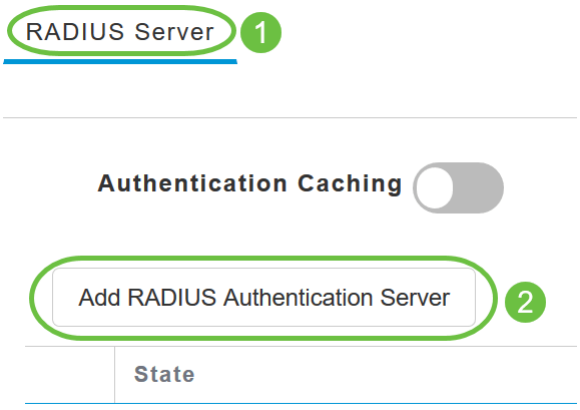
Navigieren Sie zur Registerkarte *WLAN-Sicherheit*. Wählen Sie im Dropdown-Menü *Sicherheitstyp* die Option **WPA2Enterprise aus**. Wählen Sie **External Radius** als *Authentifizierungsserver aus*. Sie können *Radius Profiling* aktivieren.



Schritt 5

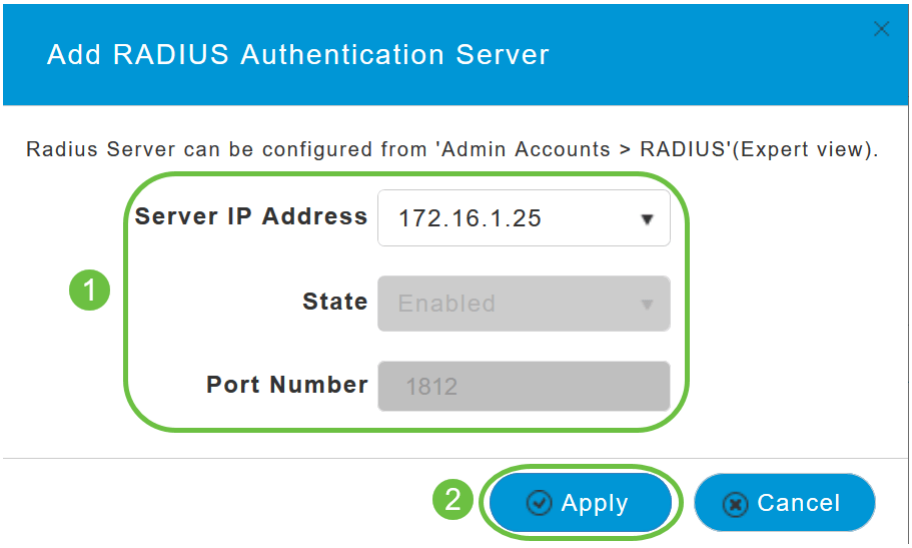
Navigieren Sie zum Abschnitt *RADIUS Server*. Klicken Sie auf **RADIUS Authentication Server**

hinzufügen.



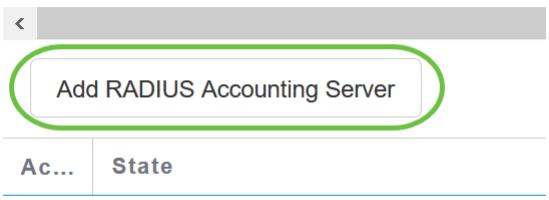
Schritt 6

Überprüfen Sie die Details des von Ihnen konfigurierten RADIUS-Authentifizierungsservers, und klicken Sie auf **Übernehmen**.



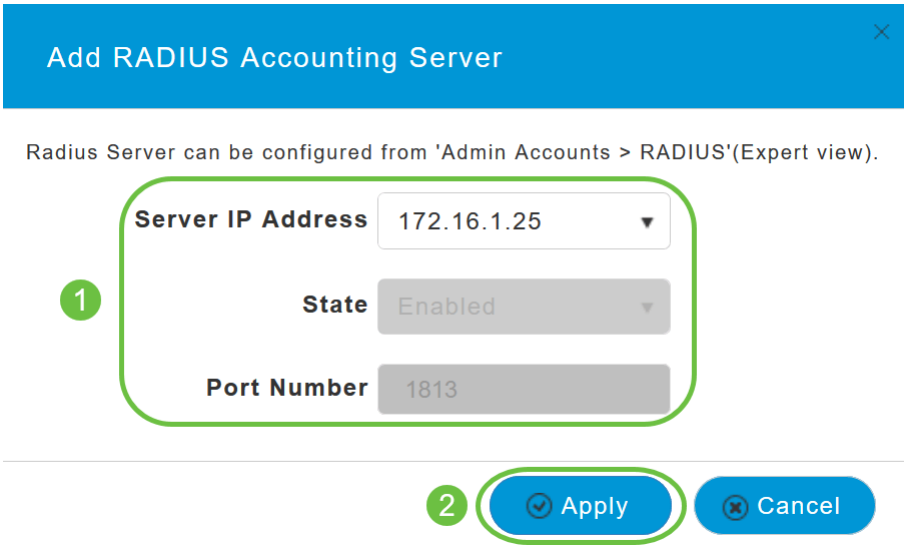
Schritt 7

Klicken Sie auf **RADIUS Accounting Server hinzufügen**.



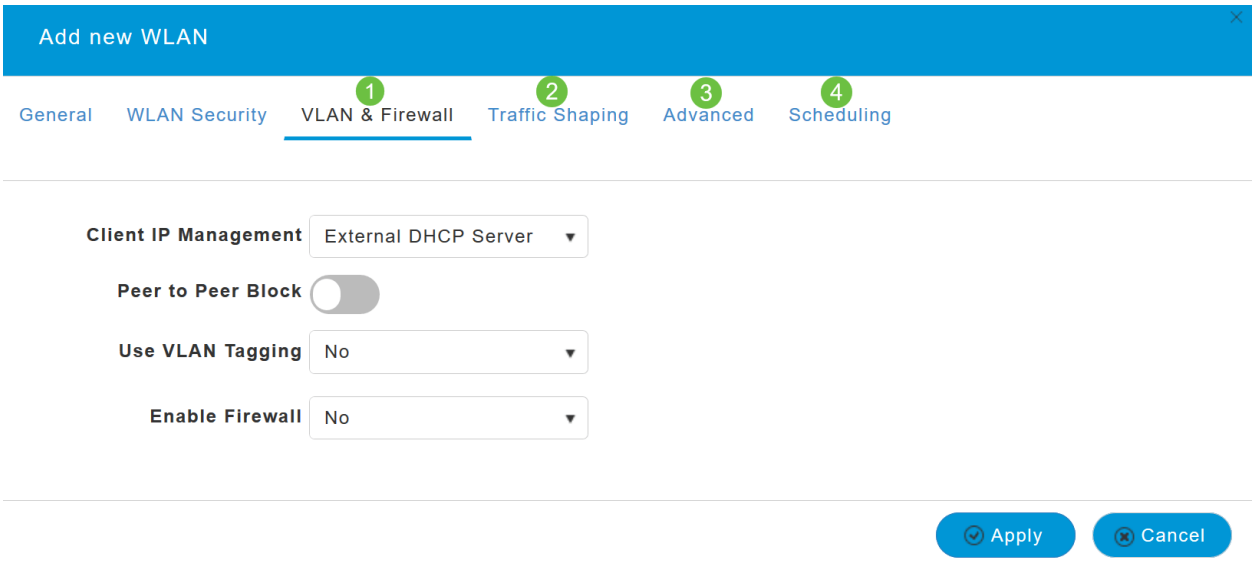
Schritt 8

Überprüfen Sie die Details des von Ihnen konfigurierten RADIUS Accounting Server, und klicken Sie auf **Apply**.



Schritt 9

Navigieren Sie zu den Registerkarten *VLAN & Firewall*, *Traffic Shaping*, *Advanced* und *Scheduling* , um die Einstellungen entsprechend Ihren Netzwerkeinstellungen zu konfigurieren. Klicken Sie auf **Apply** (Anwenden).

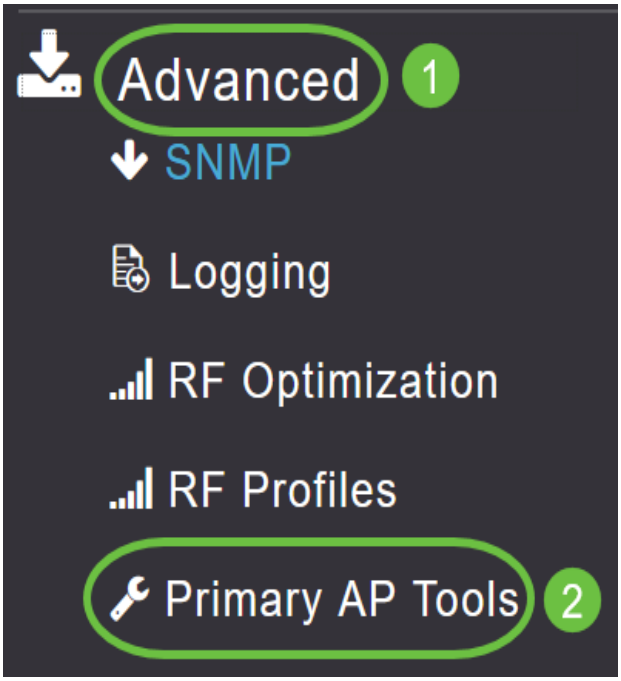


Überprüfung

Gehen Sie wie folgt vor, um die RADIUS-Authentifizierung zu testen:

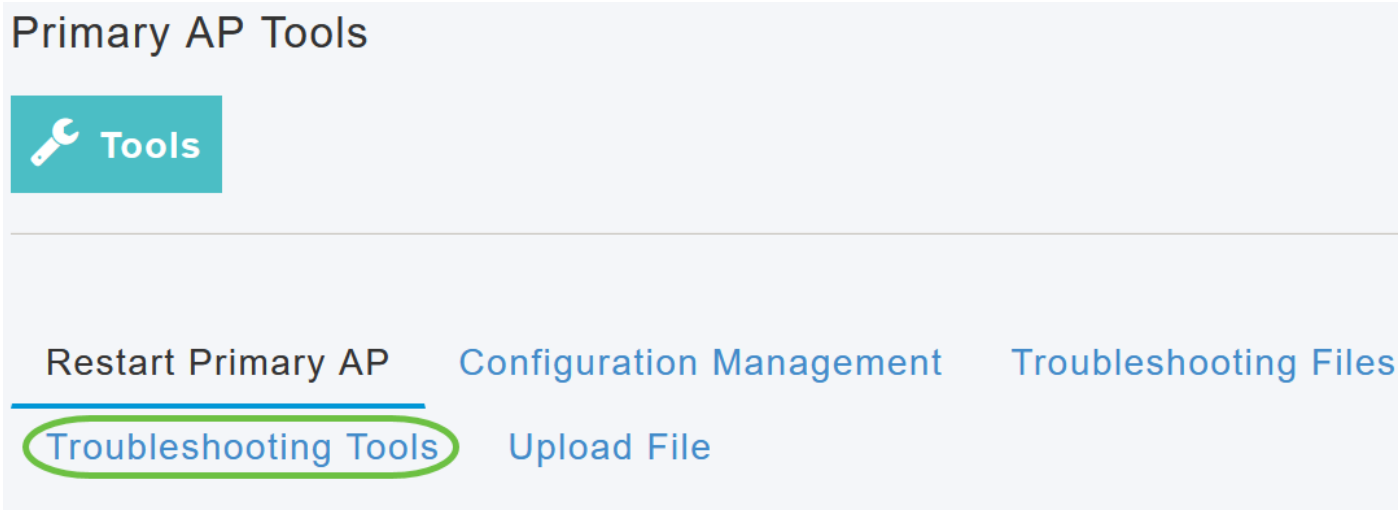
Schritt 1

Navigieren Sie zu **Erweitert > Primäre AP-Tools**.



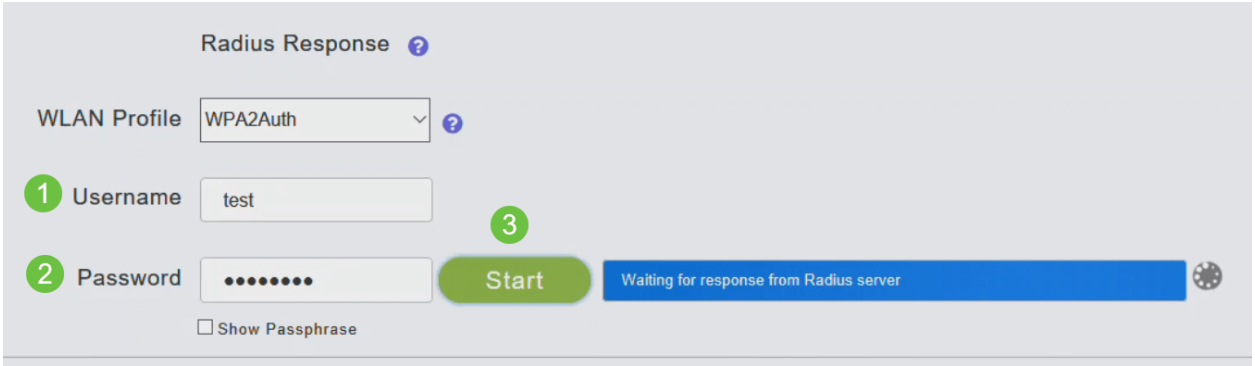
Schritt 2

Klicken Sie auf **Tools zur Fehlerbehebung**.



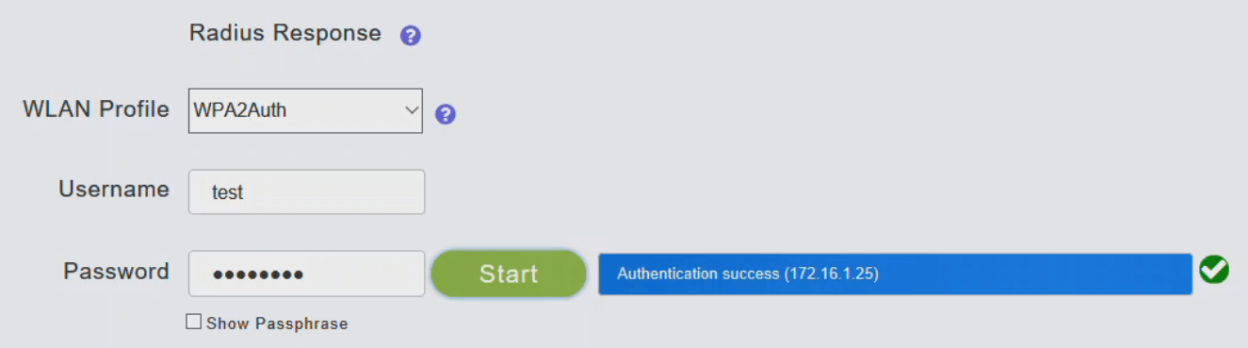
Schritt 3

Geben Sie im Abschnitt *Radius Response* den *Benutzernamen* und das *Kennwort* für das zuvor konfigurierte WLAN-Profil ein, und klicken Sie auf **Start**.



Schritt 4

Nachdem die Überprüfung erfolgreich abgeschlossen wurde, wird auf Ihrem Bildschirm die folgende Benachrichtigung angezeigt.



Fazit

Da hast du es! Nun haben Sie gelernt, wie Sie RADIUS auf Ihrem CBW AP konfigurieren. Weitere erweiterte Konfigurationen finden Sie im *Cisco Business Wireless Access Point Administration Guide.*

Häufig gestellte Fragen Firmware-Upgrade RLANs Erstellung von Anwendungsprofilen Client-Profilerstellung Primäre AP-Tools Umbrella WLAN-Benutzer Protokollieren Traffic Shaping Schurken Störungsquelle Konfigurationsverwaltung Mesh-Modus für die Portkonfiguration