

Portkonfiguration mit RLANs in einem CBW-Netzwerk

Ziel

Ziel dieses Artikels ist es, ein Remote Local Area Network (RLAN)-Netzwerk zu erstellen und Ports und Access Point-Gruppen auf einem Cisco Business Wireless (CBW) Primary Access Point (AP) zuzuweisen.

Unterstützte Geräte | Softwareversion

- 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

CBW APs basieren auf 802.11 a/b/g/n/ac (Wave 2) mit internen Antennen. Diese APs unterstützen den neuesten 802.11ac Wave 2-Standard für höhere Leistung, besseren Zugriff und Netzwerke mit höherer Dichte.

Die in diesem Artikel genannten Access Points der Serien 145AC und 240AC können in einem herkömmlichen oder Mesh-Netzwerk verwendet werden. In diesem Artikel werden die Geräte für ein herkömmliches Wireless-Netzwerk verwendet.

Weitere Informationen zu Mesh-Netzwerken finden Sie unter [Cisco Business: Willkommen bei Wireless Mesh Networking](#).

Wenn Sie die Portkonfiguration in einem Mesh-Netzwerk bevorzugen, lesen Sie das Dokument [Configure Ethernet Ports of Cisco Business Wireless Access Point in Mesh Mode](#).

In einem herkömmlichen Wireless-Netzwerk wird ein RLAN für die Authentifizierung von kabelgebundenen Clients mithilfe des primären Access Points verwendet. Sobald der kabelgebundene Client erfolgreich zum primären Access Point hinzukommt, schalten die LAN-Ports den Datenverkehr zwischen zentralen oder lokalen Switching-Modi um. Der Datenverkehr vom kabelgebundenen Client wird als Wireless-Client-Datenverkehr behandelt.

Das RLAN sendet die Authentifizierungsanfrage, um den kabelgebundenen Client zu authentifizieren. Die Authentifizierung des kabelgebundenen Clients in einem RLAN ähnelt dem zentralen authentifizierten Wireless-Client.

Wenn Sie nur ein Virtual Local Area Network (VLAN) benötigen, müssen Sie kein RLAN konfigurieren. Ein RLAN ist standardmäßig im WAP enthalten, natives VLAN 1. Es verfügt über offene Sicherheit, und alle Ports sind diesem RLAN standardmäßig zugewiesen.

Wenn Sie mit den verwendeten Begriffen nicht vertraut sind, lesen Sie [Cisco Business: Glossar neuer Begriffe](#).

RLANs funktionieren in einem Mesh-Netzwerk nicht. Mesh ist standardmäßig nicht aktiviert. Wenn der Access Point also nicht zuvor im Mesh-Modus ausgeführt wurde, ist er auf "Go" festgelegt.


Konfigurationsschritte

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://\[ipaddress\]](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 Tooltip, 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

Schalten Sie den Access Point ein, wenn er nicht bereits eingeschaltet ist. Überprüfen Sie den Status der Leuchtanzeigen. Wenn die LED-Anzeige grün blinkt, fahren Sie mit dem nächsten Schritt fort.

Das Booten des Access Points dauert etwa 8-10 Minuten. Die LED blinkt in mehreren Mustern grün, wechselt schnell durch grün, rot und orange, bevor sie wieder grün wird. Die Farbintensität und die Farbe der LED können geringfügig variieren.

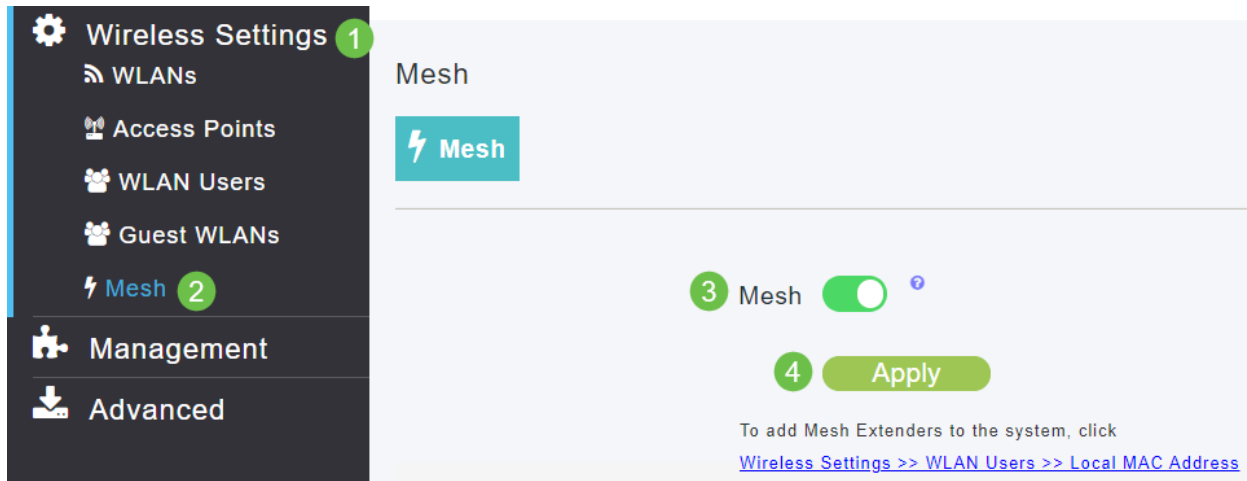
Schritt 2

Melden Sie sich bei der Webbenutzeroberfläche des primären Access Points an. Öffnen Sie 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 darauf zugreifen, indem Sie die IP-Adresse des primären Access Points in einen Webbrowser eingeben.

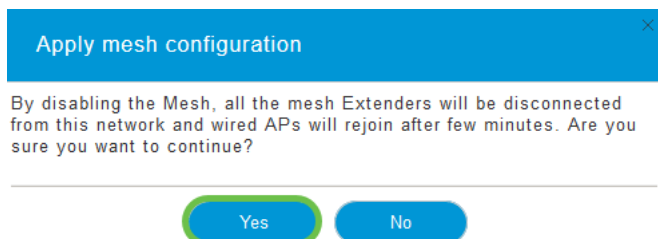
Schritt 3

Der Access Point kann sich nicht im Mesh-Modus befinden, damit ein RLAN funktioniert. Um den Mesh-Modus zu deaktivieren, navigieren Sie zu **Wireless Settings > Mesh (Wireless-Einstellungen > Mesh)**. Wählen Sie diese Option aus, um die Mesh zu deaktivieren. Wenn Ihr Access Point neu ist oder Sie wissen, dass der Mesh-Modus nicht aktiviert ist, können Sie mit [Schritt 7](#) fortfahren.



Schritt 4

Bestätigen Sie, dass Sie den Mesh-Modus deaktivieren möchten, indem Sie auf **Ja** klicken.



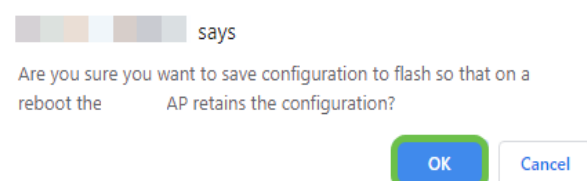
Schritt 5

Speichern Sie Ihre Konfigurationen, indem Sie im rechten oberen Bereich der Webbenutzeroberfläche auf das **Symbol Speichern** klicken.



Schritt 6

Bestätigen Sie die Speichern-Datei, indem Sie auf **OK** klicken. Der Access Point wird neu gestartet. Dieser Vorgang dauert 8 bis 10 Minuten.



Schritt 7

Um ein RLAN zu erstellen, navigieren Sie zu **Wireless Settings > WLANs (Wireless-Einstellungen > WLANs)**. Wählen Sie anschließend **Neues WLAN/RLAN hinzufügen** aus.

The screenshot shows the Cisco Business Wireless management interface. On the left is a dark sidebar with navigation options: Monitoring, Wireless Settings (marked with a green '1'), WLANs (marked with a green '2'), Access Points, WLAN Users, Guest WLANs, Mesh, Management, and Advanced. The main content area is titled 'WLANs' and features two summary cards: 'Active WLANs 1' and 'Active RLANs 1'. Below these is a table with a header 'Add new WLAN/RLAN' (marked with a green '3') and a table with columns: Action, Active, Type, Name, SSID, Security Policy, and Radio Policy. The table contains two rows: one for a WLAN named 'EZ1K' with security policy 'EZ1K' and radio policy 'Personal(WPA2)', and one for an RLAN named 'DEFAULT_RLAN' with security policy 'DEFAULT_RLAN' and radio policy 'Open'.

Schritt 8

Wählen Sie **RLAN** aus. Erstellen Sie einen Namen für das Profil.

The screenshot shows the 'Add new WLAN/RLAN' configuration dialog. It has a blue header bar with the title and a close button. Below the header are four tabs: 'General' (selected), 'RLAN Security', 'VLAN & Firewall', and 'Traffic Shaping'. The 'General' tab contains the following fields: 'Network ID' (dropdown menu with '3' selected), 'Type' (dropdown menu with 'RLAN' selected, marked with a green '1'), 'Profile Name *' (text input field with 'RLAN2' entered, marked with a green '2'), and 'Enable' (toggle switch that is turned on). At the bottom of the dialog are two buttons: 'Apply' and 'Cancel'.

Schritt 9 (Open Security verwenden)

Auf der Registerkarte *RLAN-Sicherheit*. Unter *Sicherheitstyp* können Sie *Öffnen* oder *802.1X* auswählen.

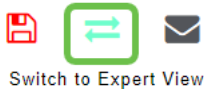
In diesem Beispiel wurde der *Sicherheitstyp* als Standardwert beibehalten.

Klicken Sie auf **Apply** (Anwenden). Dadurch wird dieses Open Security RLAN automatisch aktiviert. Fahren Sie mit [Schritt 11 fort](#).

The screenshot shows the 'Edit RLAN' configuration dialog. It has a blue header bar with the title and a close button. Below the header are four tabs: 'General', 'RLAN Security' (selected), 'VLAN & Firewall', and 'Traffic Shaping'. The 'RLAN Security' tab contains the following fields: 'Guest Network' (toggle switch that is turned off), 'MAC Filtering' (toggle switch that is turned off with a question mark icon), and 'Security Type' (dropdown menu with 'Open' selected, marked with a green '1'). At the bottom of the dialog are two buttons: 'Apply' and 'Cancel'.

Schritt 10a (Verwendung von 802.1X-Sicherheit)

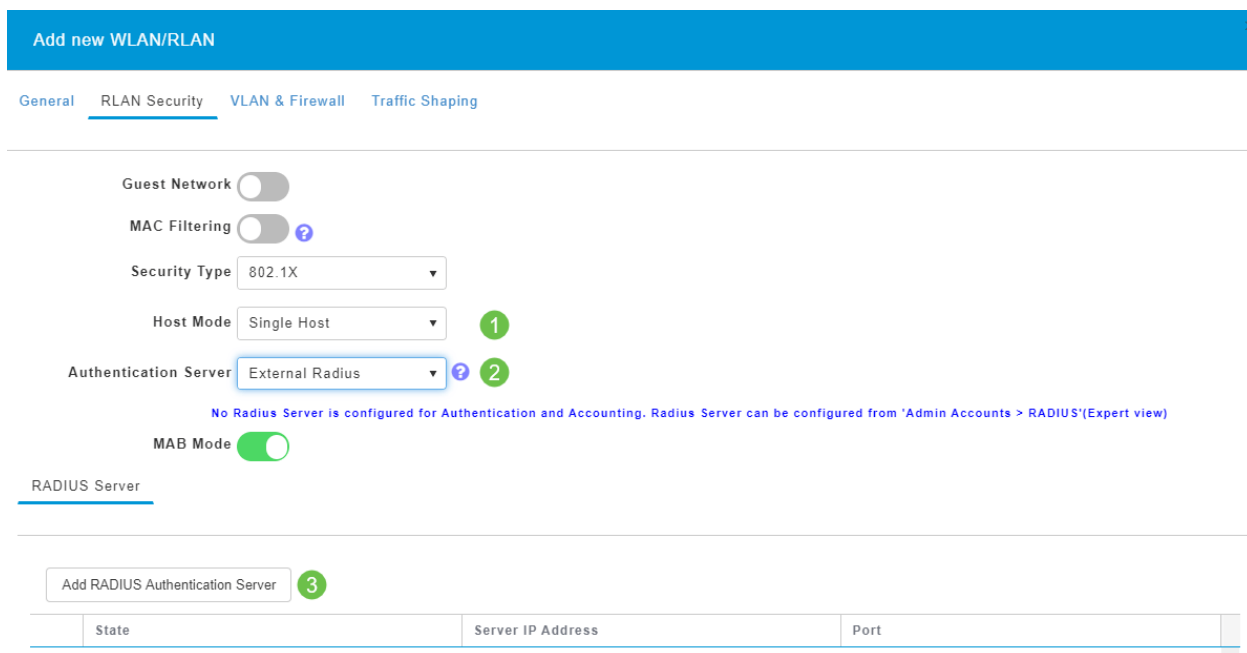
Für die Einrichtung von External Radius muss ein Radius-Server in *Admin-Konten* unter *RADIUS* in *Expert View* konfiguriert sein. Klicken Sie auf das **Pfeilsymbol** oben rechts in der Webbenutzeroberfläche, um zur *Expertenansicht* zu wechseln. Einzelheiten zur Einrichtung eines RADIUS-Servers finden Sie im [Radius-Verzeichnis](#).



Schritt 10b (Verwendung von 802.1X-Sicherheit)

Wenn Sie 802.1X als Sicherheitstyp auswählen, müssen weitere Optionen ausgewählt werden. Sie müssen Folgendes auswählen:

- *Host-Modus* - Einzelhost oder Multi-Host
- *Authentifizierungsserver* - Externer Radius oder AP
- *MAB-Modus* - aktiviert oder deaktiviert. Um MAC-Adressen hinzuzufügen, folgen Sie den Anweisungen im nächsten Schritt.



Add new WLAN/RLAN

General **RLAN Security** VLAN & Firewall Traffic Shaping

Guest Network

MAC Filtering ?

Security Type 802.1X

Host Mode Single Host 1

Authentication Server External Radius 2

No Radius Server is configured for Authentication and Accounting. Radius Server can be configured from 'Admin Accounts > RADIUS'(Expert view)

MAB Mode

RADIUS Server

Add RADIUS Authentication Server 3

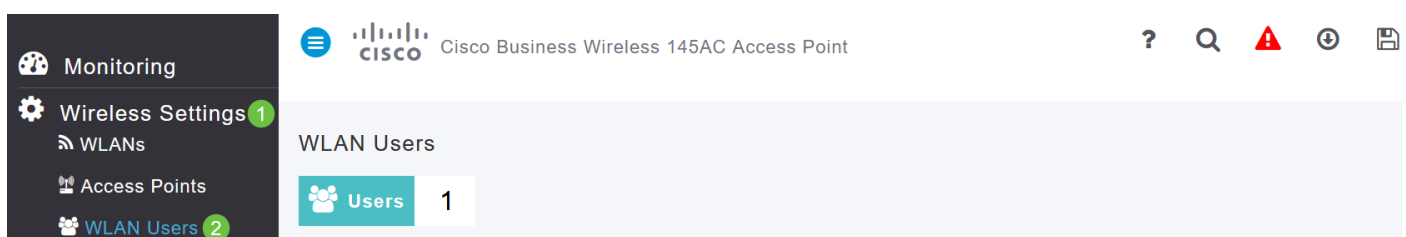
State	Server IP Address	Port
-------	-------------------	------

Schritt 11 (optional)

MAB-Modus (MAC Authentication Bypass) bedeutet, dass das Gerät sich nicht authentifizieren muss, wenn unter WLAN-Benutzern eine MAC-Adresse aufgeführt ist. Die aufgelisteten MAC-Adressen können die Authentifizierung umgehen, um entweder automatisch auf das Netzwerk zugreifen oder automatisch ablehnen zu können. Dies ist nützlich, wenn ein IP-Telefon an einen PoE-Port eines Switches angeschlossen wird.

Sie können jede MAC-Adresse auf zwei Arten bezeichnen:

1. *Zulässig* - Das Gerät erhält automatischen Zugriff.
2. *Sperrliste* - Dem Gerät wird automatisch der Zugriff verweigert.



Monitoring

Wireless Settings 1

WLANs

Access Points

WLAN Users 2

Cisco Business Wireless 145AC Access Point

WLAN Users

Users 1

Schritt 12

Auf der Registerkarte *VLAN & Firewall* können Sie *VLAN Tagging* verwenden auswählen und eine *VLAN-ID*-Nummer auswählen.

General **RLAN Security** VLAN & Firewall Traffic Shaping

Client IP Management External DHCP Server ▾

Use VLAN Tagging Yes ▾ **1**

VLAN ID * 5 ▾ **2**

Enable Firewall No ▾

VLAN and Firewall configuration apply to all WLANs and RLANs configured with same VLAN

Apply Cancel

Schritt 13 (optional)

Sie können **Firewall aktivieren**, wenn Sie *Zugriffskontrolllisten (ACLs)* konfigurieren möchten, mit denen Sie den Zugriff für bestimmte IP-Adressen oder VLANs zulassen oder ablehnen können. Dies wird verwendet, wenn jemand eine Verbindung zum Netzwerk-Port-Gerät herstellt.

General **RLAN Security** VLAN & Firewall Traffic Shaping

Client IP Management External DHCP Server ▾

Use VLAN Tagging Yes ▾

VLAN ID * 5 ▾

Enable Firewall Yes ▾ **1**

2

WLAN Post-auth ACL

ACL Name(IPv4) None ▾

ACL Name(IPv6) None ▾

VLAN ACL

ACL Name(IPv4) None ▾

ACL Direction Ingress ▾

Schritt 14 (optional)

Auf der Registerkarte *Traffic Shaping* können Sie das Traffic Shaping konfigurieren, indem Sie die **Application Visibility Control** aktivieren. Dadurch wird die Datenverkehrspriorisierung festgelegt.

General **RLAN Security** VLAN & Firewall **Traffic Shaping**

Application Visibility Control Enabled ▾ **1**

Schritt 15 (optional)

Auf der Registerkarte *Planung* können Sie einen Zeitplan auswählen. Dadurch wird festgelegt, wann der Port mit dem Netzwerk verbunden werden kann.

Add new WLAN/RLAN

General RLAN Security VLAN & Firewall Traffic Shaping **Scheduling**

Schedule WLAN **No Schedule**

When 'No Schedule' is selected, all the below scheduling information would be cleared.

Apply to all weekdays

Day	Availability	From	To	Availability Bar
Monday	<input type="checkbox"/>	00:00	23:59	0 4 8 12 16 20 24
Tuesday	<input type="checkbox"/>	00:00	23:59	0 4 8 12 16 20 24
Wednesday	<input type="checkbox"/>	00:00	23:59	0 4 8 12 16 20 24
Thursday	<input type="checkbox"/>	00:00	23:59	0 4 8 12 16 20 24
Friday	<input type="checkbox"/>	00:00	23:59	0 4 8 12 16 20 24
Saturday	<input type="checkbox"/>	00:00	23:59	0 4 8 12 16 20 24
Sunday	<input type="checkbox"/>	00:00	23:59	0 4 8 12 16 20 24

Schritt 16 (optional)

Nachdem das RLAN erstellt wurde, können Sie zu **Wireless Settings > Access Point Groups (Wireless-Einstellungen > Access Point-Gruppen)** navigieren. Hier können Sie Gruppen hinzufügen oder bearbeiten. Um diesen Bildschirm anzuzeigen, müssen Sie in der *Expertenansicht* sein, die Sie in [Schritt 10a](#) ausgewählt haben.

Wireless Settings 1

WLANs

Access Points

Access Points Groups 2

WLAN Users

Guest WLANs

Mesh

Management

Services

Advanced

Access Points Groups

Access Points Groups 1

Add new group Refresh

Action AP Group name

Warehouse

default-group

1 1 10 ite

Add new group

General WLANs Access Points RF Profile Ports

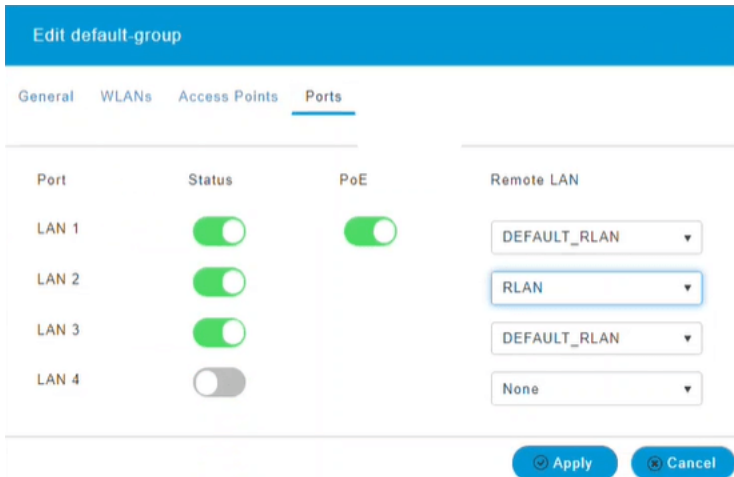
3 AP Group name Warehouse

AP Group description

Apply Cancel

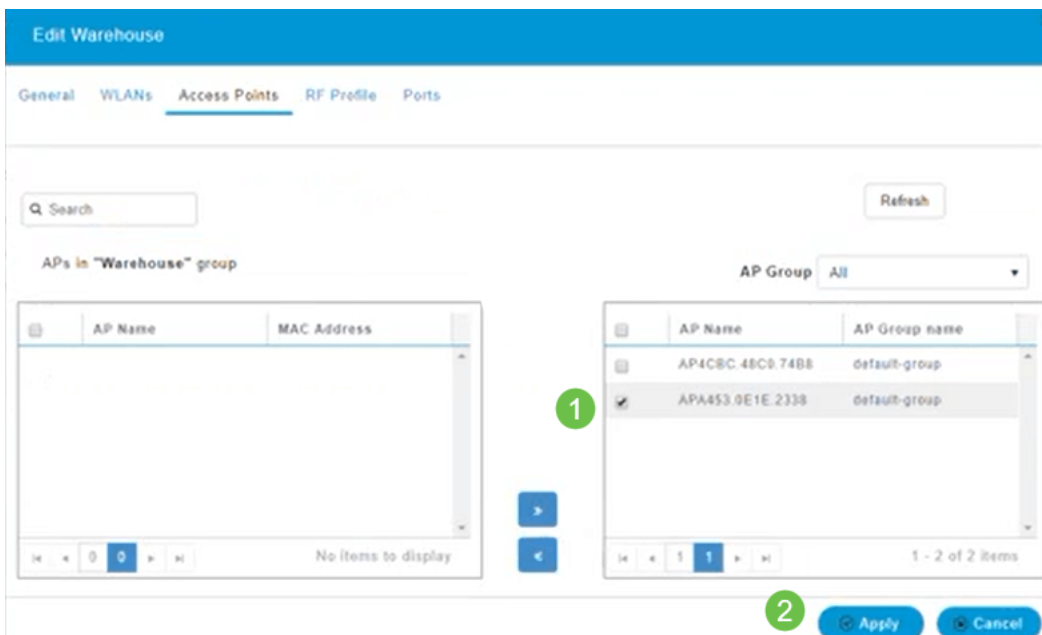
Schritt 17

Auf der Registerkarte *Ports* können Sie die Ports des Access Points bestimmten Remote-LANs zuweisen.



Schritt 18

Auf der Registerkarte *Access Points* müssen Sie dieser Access Point-Gruppe einen bestimmten Access Point zuweisen. Klicken Sie auf **Apply** (Anwenden).



Schritt 19

Wählen Sie zur Bestätigung **Ja** aus.



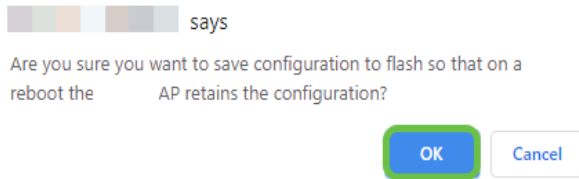
Schritt 20

Speichern Sie Ihre Konfigurationen, indem Sie im rechten oberen Bereich der Webbenutzeroberfläche auf das **Symbol Speichern** klicken.



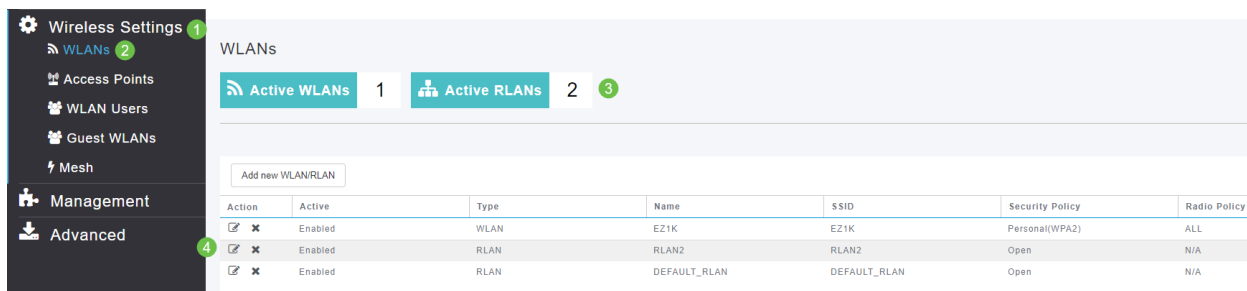
Schritt 21

Bestätigen Sie die Speichern-Datei, indem Sie auf **OK** klicken. Der Access Point wird neu gestartet. Dieser Vorgang dauert 8 bis 10 Minuten.



RLAN anzeigen

Um das von Ihnen erstellte RLAN anzuzeigen, wählen Sie **Wireless Settings > WLANs (Wireless-Einstellungen > WLANs)**. Die Anzahl der aktiven RLANs wird auf 2 erhöht, und das neue RLAN wird aufgelistet.

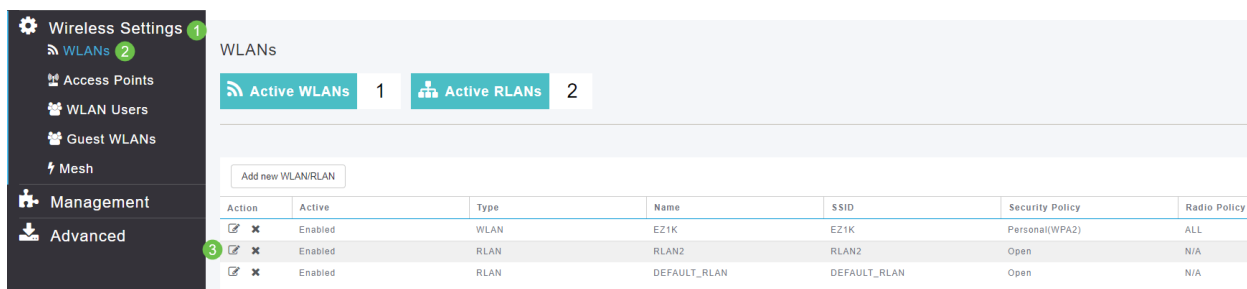


RLAN bearbeiten

Wenn Sie am Ende der Einrichtung des RLANs auf **Apply** geklickt haben, wird das RLAN automatisch aktiviert. Wenn Sie das RLAN deaktivieren oder andere Änderungen vornehmen müssen, gehen Sie wie folgt vor:

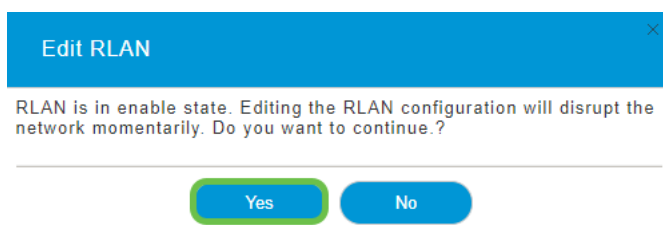
Schritt 1

Wählen Sie **Wireless Settings > WLANs** aus. Klicken Sie auf das **Bearbeitungssymbol**.



Schritt 2

Sie erhalten eine Popup-Meldung, dass die Bearbeitung des RLANs das Netzwerk vorübergehend stört. Bestätigen Sie, dass Sie fortfahren möchten, indem Sie auf **Ja** klicken.



Schritt 3 (Aktivieren/Deaktivieren)

Wählen Sie im Fenster **WLAN/RLAN bearbeiten** unter **Allgemein** die Option **Aktiviert** oder **Deaktiviert** aus, um das RLAN zu aktivieren/deaktivieren. Klicken Sie auf **Apply** (Anwenden).

The screenshot shows the 'Edit RLAN' window with the following settings:

- Network ID: 3
- Type: RLAN
- Profile Name *: RLAN2
- Enable: (marked with a green circle '1')

At the bottom, there are 'Apply' and 'Cancel' buttons. The 'Apply' button is marked with a green circle '2'.

Schritt 4 (Bearbeiten anderer Einstellungen)

Navigieren Sie zu den Registerkarten *RLAN-Sicherheit*, *VLAN und Firewall* oder *Traffic Shaping*, wenn Sie Einstellungen ändern müssen. Klicken Sie nach den Änderungen auf **Übernehmen**.

The screenshot shows the 'Edit RLAN' window with the 'RLAN Security' tab selected. The settings are:

- Guest Network: (marked with a green circle '1')
- MAC Filtering: (marked with a green circle '1')
- Security Type: Open

At the bottom, there are 'Apply' and 'Cancel' buttons. The 'Apply' button is marked with a green circle '2'.

Schritt 5

Speichern Sie Ihre Konfigurationen, indem Sie im rechten oberen Bereich der Webbenutzeroberfläche auf das **Symbol Speichern** klicken.



Fazit

Sie haben jetzt ein RLAN in Ihrem CBW-Netzwerk erstellt. Genießen Sie alles, und fühlen Sie sich frei, mehr hinzuzufügen, wenn es Ihre Anforderungen erfüllt.

[Häufig gestellte Fragen](#) [Radius](#) [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](#) [Willkommen bei CBW Mesh Networking](#) [Gastnetzwerk mit E-Mail-Authentifizierung und RADIUS-Accounting](#) [Fehlerbehebung](#) [Verwenden eines Draytek-Routers mit CBW](#)