

CBWネットワークのRLANを使用したポート設定

目的

この記事の目的は、リモートローカルエリアネットワーク(RLAN)ネットワークを作成し、Cisco Business Wireless(CBW)プライマリアクセスポイント(AP)でポートとアクセスポイントグループを割り当てることです。

該当するデバイス | ソフトウェアバージョン

- 145AC ([データシート](#)) | 10.4.1.0 ([最新版をダウンロード](#))
- 240AC ([データシート](#)) | 10.4.1.0 ([最新版をダウンロード](#))

概要

CBW APは802.11 a/b/g/n/ac(Wave 2)ベースで、内部アンテナを備えています。これらのAPは、パフォーマンス、アクセス性、高密度ネットワークを実現する最新の802.11ac Wave 2標準をサポートします。

この記事で参照されている145ACおよび240AC APは、従来のネットワークまたはメッシュネットワークで使用できます。この記事では、従来の無線ネットワークに機器を使用します。

メッシュネットワークの基礎を学びたい場合は、[Cisco Business](#)をご覧ください。[ワイヤレスメッシュネットワークへようこそ](#)。

メッシュネットワークでポート設定を行う場合は、「メッシュモードで[Cisco Business Wireless Access Pointのイーサネットポートを設定する](#)」を参照してください。

従来のワイヤレスネットワークでは、RLANはプライマリAPを使用して有線クライアントを認証するために使用されます。有線クライアントがプライマリAPに正常に参加すると、LANポートは中央またはローカルスイッチングモード間でトラフィックをスイッチングします。有線クライアントからのトラフィックは、ワイヤレスクライアントトラフィックとして扱われます。

RLANは、有線クライアントを認証するための認証要求を送信します。RLANでの有線クライアントの認証は、中央の認証済みワイヤレスクライアントに似ています。

必要な仮想ローカルエリアネットワーク(VLAN)が1つだけの場合は、RLANを設定する必要はありません。1つのRLANがデフォルトでAPに到達し、ネイティブVLAN 1がオープンなセキュリティを備え、すべてのポートがデフォルトでこのRLANに割り当てられます。

使用されている用語に慣れていない場合は、[シスコビジネス](#)をご覧ください。[新用語一覧](#)。

RLANはメッシュネットワークでは機能しません。メッシュはデフォルトでは有効になっていないため、APをメッシュモードで実行していた場合を除き、実行するように設定されます。

設定手順

この切り替えセクションでは、初心者のヒントを紹介します。

ログイン

プライマリAPのWebユーザインターフェイス(UI)にログインします。そのためには、Webブラウザを開き、<https://ciscobusiness.cisco>と入力します。続行する前に警告が表示されることがあります。クレデンシャルを入力します。プライマリAPにアクセスするには、Webブラウザに[https://\[ipaddress\]](https://[ipaddress]) (プライマリAPの) と入力します。

ツールのヒント

ユーザインターフェイスのフィールドに関する質問がある場合は、次のようなヒントを確認してください。 

メインメニューの展開アイコンを見つけるのに問題がありますか？

画面左側のメニューに移動します。メニューボタンが表示されない場合は、このアイコンをクリックしてサイドバーメニューを開きます。 

シスコビジネスアプリケーション

これらのデバイスには、Webユーザインターフェイスと一部の管理機能を共有するコンパニオンアプリケーションがあります。Webユーザインターフェイスのすべての機能がアプリで使用できるわけではありません。

[iOSアプリのダウンロード](#) [Androidアプリのダウンロード](#)

よく寄せられる質問 (FAQ)

まだ未回答の質問がある場合は、よく寄せられる質問(FAQ)のドキュメントを確認してください。 [FAQ](#)

手順 1

アクセスポイントがオンになっていない場合は、電源をオンにします。インジケータライトのステータスを確認します。LEDライトが緑色に点滅している場合は、次の手順に進みます。

アクセスポイントの起動には、約8 ~ 10分かかります。LEDは複数のパターンで緑色に点滅し、緑、赤、オレンジが急速に交互に繰り返された後、再び緑色に変わります。LEDの色の強度と色相には小さな変化があります。

手順 2

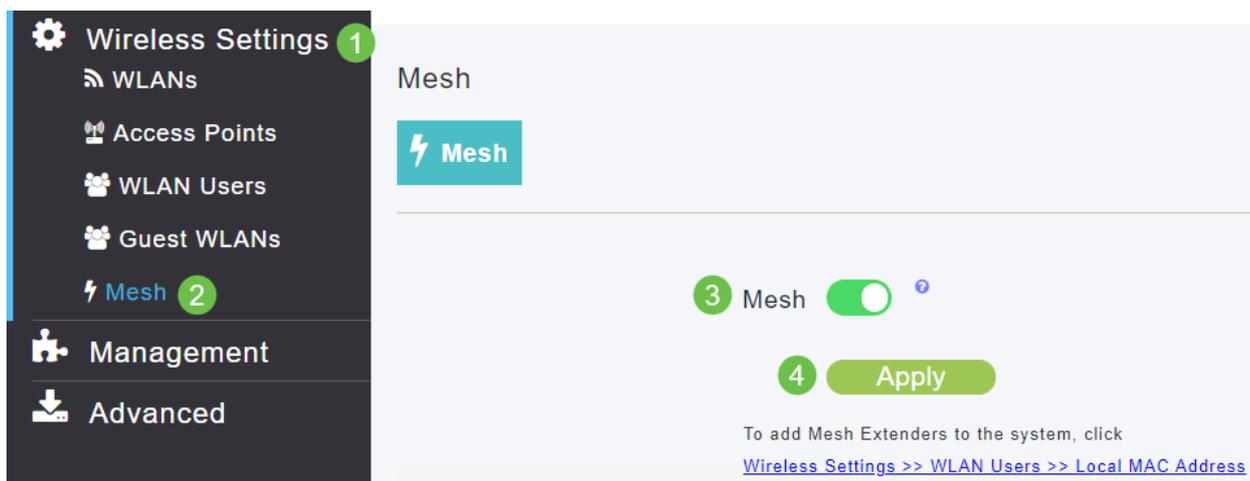
プライマリAPのWebユーザインターフェイス(UI)にログインします。Webブラウザを開き、「<https://ciscobusiness.cisco>」と入力します。続行する前に警告が表示されることがあります。認証情報を入力してください。

また、プライマリAPのIPアドレスをWebブラウザに入力してアクセスすることもできます。

手順 3

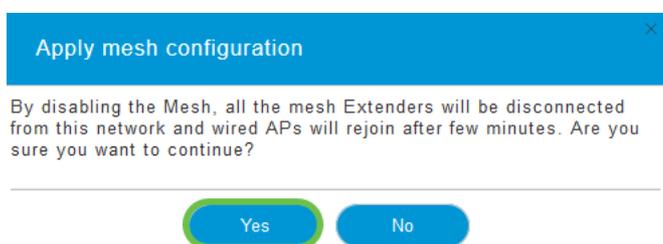
RLANが機能するようにAPをメッシュモードにすることはできません。メッシュモードをオフにするには、[ワイヤレス設定] > [メッシュ]に移動します。メッシュをオフにするには、を選択します。APが新規の場合、またはメッシュモードがオンになっていないことがわかっている場合は、

ステップ7に移動できます。



手順 4

[はい]をクリックして、メッシュモードをオフにするかどうかを確認します。



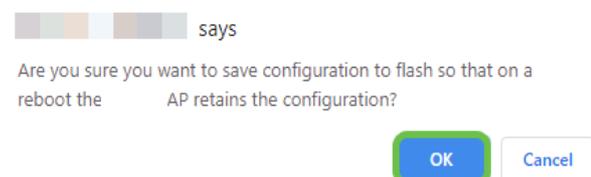
手順 5

Web UI画面の右上のパネルにあるSaveアイコンをクリックして、設定を保存してください。



手順 6

[OK]をクリックして、[保存]を確認します。APがリブートします。この処理には8 ~ 10分かかります。



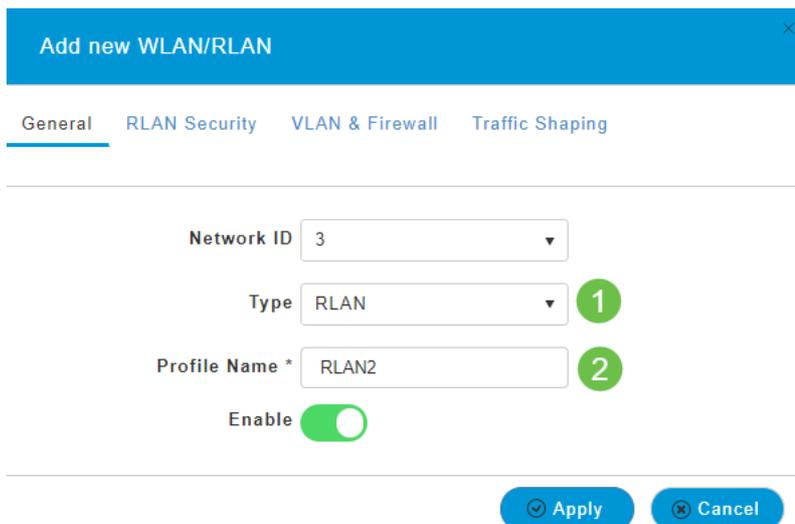
ステップ7

RLANを作成するには、[Wireless Settings] > [WLANs]に移動します。次に、[Add new WLAN/RLAN]を選択します。



手順 8

[RLAN]を選択します。プロファイルの名前を作成します。



Add new WLAN/RLAN

General RLAN Security VLAN & Firewall Traffic Shaping

Network ID 3

Type RLAN 1

Profile Name * RLAN2 2

Enable

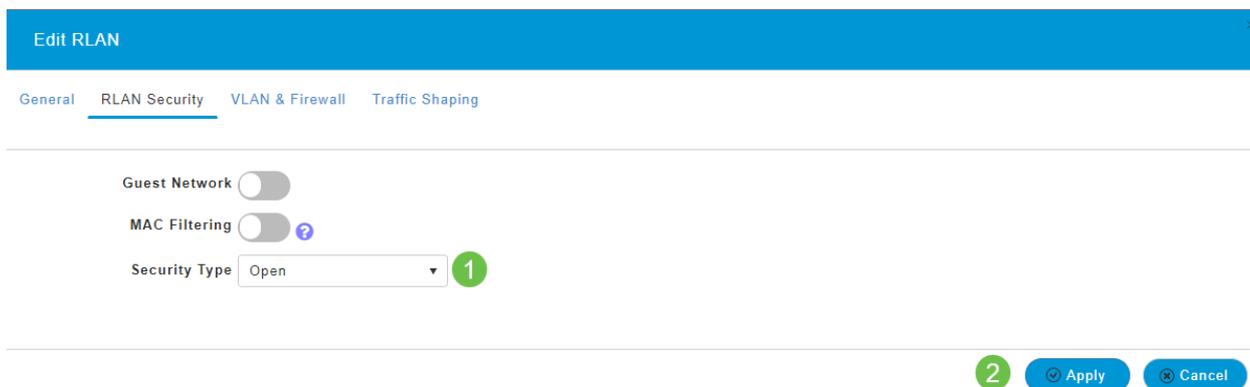
Apply Cancel

ステップ9 (オープンセキュリティの使用)

[RLAN Security]タブの下です。[セキュリティの種類]で、[開く]または[802.1X]を選択できます。

この例では、[Security Type]がデフォルトのままになっています。

[Apply] をクリックします。これにより、このオープンセキュリティRLANが自動的にアクティブ化されます。ステップ 11 に進みます。



Edit RLAN

General RLAN Security VLAN & Firewall Traffic Shaping

Guest Network

MAC Filtering ?

Security Type Open 1

2 Apply Cancel

手順10a (802.1Xセキュリティの使用)

外部RADIUSを設定するには、Expert ViewのRADIUSの下でAdmin AccountsでRADIUSサーバを設定する必要があります。Web UIの右上のメニューにある矢印アイコンをクリックして、エキスパートビューに切り替えます。RADIUSサーバの設定の詳細については、RADIUSを確認してください



手順10b (802.1Xセキュリティの使用)

[Security Type]に[802.1X]を選択する場合は、さらに多くのオプションを選択する必要があります。次を選択する必要があります。

- ホストモード: 単一ホストまたは複数ホスト

- 認証サーバ:外部RadiusまたはAP
- MABモード：有効または無効に設定します。MACアドレスを追加するには、次の手順の手順に従います。

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

手順 11 (オプション)

MAC認証バイパス(MAB)モードとは、WLAN Usersの下にMACアドレスがリストされている場合、デバイスの認証は不要であることを意味します。リストされたMACアドレスは、ネットワークへの自動アクセスまたは自動的に拒否される認証をバイパスできます。これは、IP PhoneがスイッチのPoEポートに接続されている場合に便利です。

各MACアドレスには、次の2つの方法のいずれかでラベルを付けることができます。

1. *Allowlisted* : デバイスは自動アクセスを受信します。
2. *Blocklisted* : デバイスは自動的にアクセスを拒否されます。

Monitoring

Wireless Settings 1

WLANs

Access Points

WLAN Users 2

Guest WLANs

Mesh

Management

Advanced

Cisco Business Wireless 145AC Access Point

WLAN Users

Users 1

WLAN Users Local MAC Addresses ?

Search ?

+ Add MAC Address Refresh Number of Blocklist:0 Number of Allowlist:3

Action	MAC Address	Type	Profile Name	Description
3	a4: : :20	Allowlist	Any WLAN/RLAN	CBW145AC-0b20
	4c: : :68	Allowlist	Any WLAN/RLAN	CBW141ACM-7468
	4c: : :1	Allowlist	Any WLAN/RLAN	CBW140AC-cba1

ステップ 12

[VLANとファイアウォール]タブで、[VLANタギングの使用]を選択し、VLAN ID番号を選択します。

手順 13 (オプション)

特定のIPアドレスまたはVLANに対するアクセスを許可または拒否できるアクセスコントロールリスト(ACL)を設定する場合は、[ファイアウォールの有効化]を選択できます。これは、誰かがネットワークポートデバイスに接続してネットワークに接続している場合に使用されます。

General RLAN Security VLAN & Firewall Traffic Shaping

Client IP Management External DHCP Server ▾

Use VLAN Tagging Yes ▾

VLAN ID * 5 ▾

Enable Firewall Yes ▾ 1

WLAN Post-auth ACL

ACL Name(IPv4) None ▾

ACL Name(IPv6) None ▾

VLAN ACL

ACL Name(IPv4) None ▾

ACL Direction Ingress ▾

2

手順 14 (オプション)

[Traffic Shaping]タブの下で、Enabling **Application Visibility Control**を使用してトラフィックシェーピングを設定できます。これにより、トラフィックの優先順位付けが設定されます。

General RLAN Security VLAN & Firewall Traffic Shaping

Application Visibility Control Enabled ▾ 1

AVC Profile RLAN2

Add Rule 2

Action	S.L No.	Application	Action
<			>

Apply Cancel

ステップ 15 (オプション)

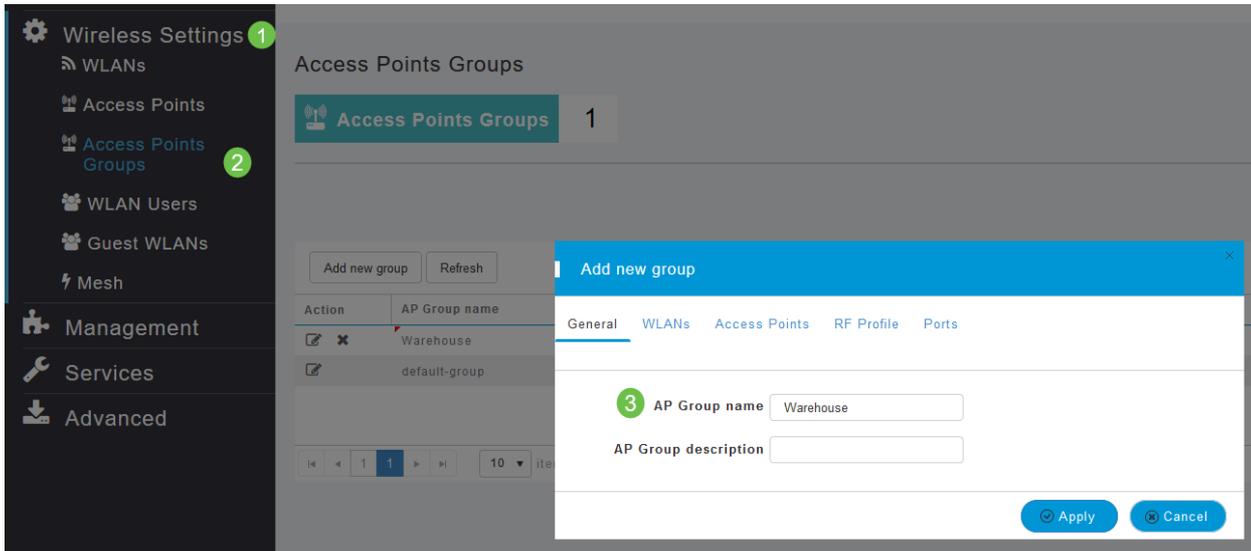
[スケジュール]タブで、スケジュールを選択できます。ポートがネットワークに接続できる時間を設定します。

Add new WLAN/RLAN

General RLAN Security VLAN & Firewall Traffic Shaping Scheduling

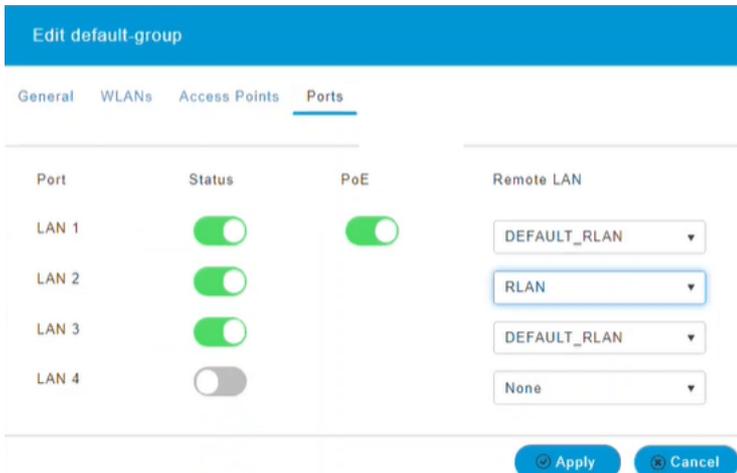
手順 16 (オプション)

RLANが作成されたら、[Wireless Settings] > [Access Point Groups]に移動できます。ここでは、グループを追加または編集できます。この画面を表示するには、手順10aで選択したエキスパートビューに移動する必要があります。



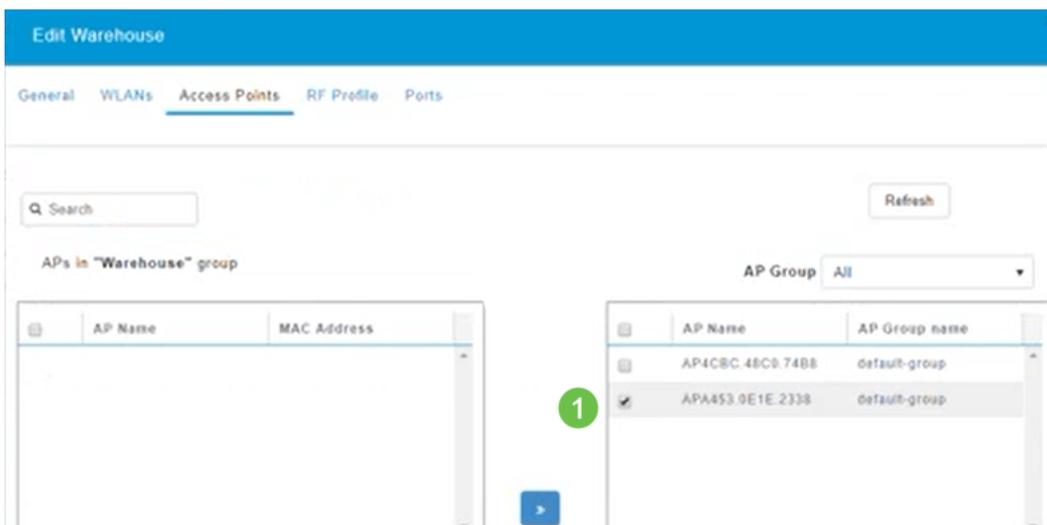
手順 17

[Ports]タブで、APのポートを特定のリモートLANに割り当てることができます。



ステップ 18

[Access Points]タブで、特定のアクセスポイントをそのアクセスポイントグループに割り当てる必要があります。[Apply] をクリックします。



ステップ 19

[はい]を選択して確認します。



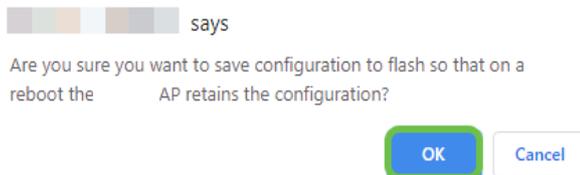
ステップ 20

Web UI画面の右上のパネルにあるSaveアイコンをクリックして、設定を保存してください。



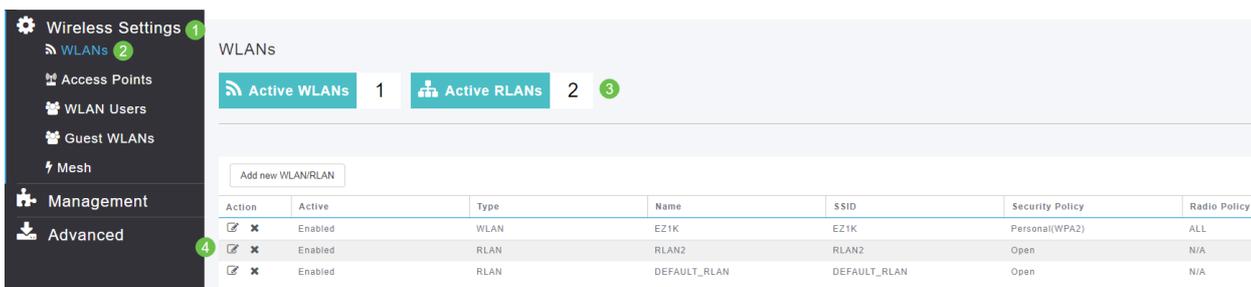
ステップ 21

[OK]をクリックして、[保存]を確認します。APがリブートします。この処理には8 ~ 10分かかります。



RLANの表示

作成したRLANを表示するには、[ワイヤレス設定] > [WLANs]を選択します。アクティブRLANの数が2に増え、新しいRLANがリストされます。

A screenshot of the "Wireless Settings" page, specifically the "WLANs" section. The left sidebar shows "Wireless Settings" (1), "WLANs" (2), "Access Points", "WLAN Users", "Guest WLANs", "Mesh", "Management", and "Advanced" (4). The main content area shows "WLANs" with "Active WLANs" (1) and "Active RLANs" (2) (3). Below this is a table with columns: Action, Active, Type, Name, SSID, Security Policy, and Radio Policy. The table contains three rows: a WLAN named "EZ1K", an RLAN named "RLAN2", and a default RLAN named "DEFAULT_RLAN".

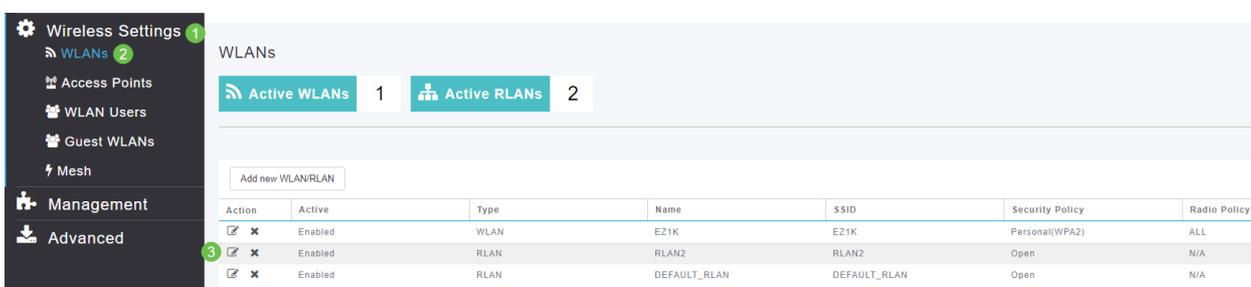
Action	Active	Type	Name	SSID	Security Policy	Radio Policy
<input checked="" type="checkbox"/> <input type="checkbox"/>	Enabled	WLAN	EZ1K	EZ1K	Personal(WPA2)	ALL
<input checked="" type="checkbox"/> <input type="checkbox"/>	Enabled	RLAN	RLAN2	RLAN2	Open	N/A
<input checked="" type="checkbox"/> <input type="checkbox"/>	Enabled	RLAN	DEFAULT_RLAN	DEFAULT_RLAN	Open	N/A

RLANの編集

RLANの設定の終わりに[Apply]をクリックすると、RLANが自動的にアクティブになります。RLANを無効にするか、その他の変更を行う必要がある場合は、次の簡単な手順に従います。

手順 1

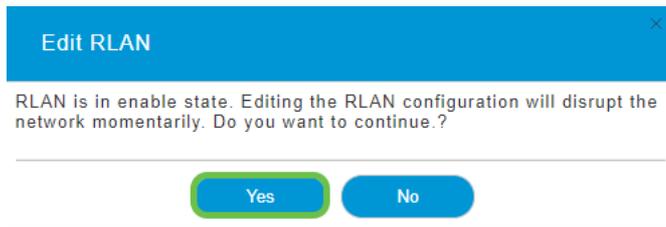
[Wireless Settings] > [WLANs]を選択します。編集アイコンをクリックします。

A screenshot of the "Wireless Settings" page, specifically the "WLANs" section. The left sidebar shows "Wireless Settings" (1), "WLANs" (2), "Access Points", "WLAN Users", "Guest WLANs", "Mesh", "Management", and "Advanced" (4). The main content area shows "WLANs" with "Active WLANs" (1) and "Active RLANs" (2). Below this is a table with columns: Action, Active, Type, Name, SSID, Security Policy, and Radio Policy. The table contains three rows: a WLAN named "EZ1K", an RLAN named "RLAN2", and a default RLAN named "DEFAULT_RLAN".

Action	Active	Type	Name	SSID	Security Policy	Radio Policy
<input checked="" type="checkbox"/> <input type="checkbox"/>	Enabled	WLAN	EZ1K	EZ1K	Personal(WPA2)	ALL
<input checked="" type="checkbox"/> <input type="checkbox"/>	Enabled	RLAN	RLAN2	RLAN2	Open	N/A
<input checked="" type="checkbox"/> <input type="checkbox"/>	Enabled	RLAN	DEFAULT_RLAN	DEFAULT_RLAN	Open	N/A

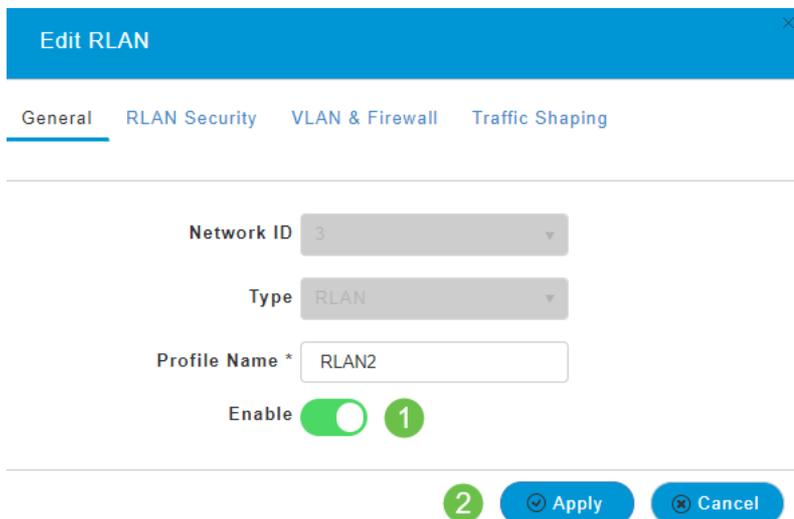
手順 2

RLANを編集すると、ネットワークが一時的に中断されることを通知するポップアップが表示されます。[はい]をクリックして、続行することを確認します。



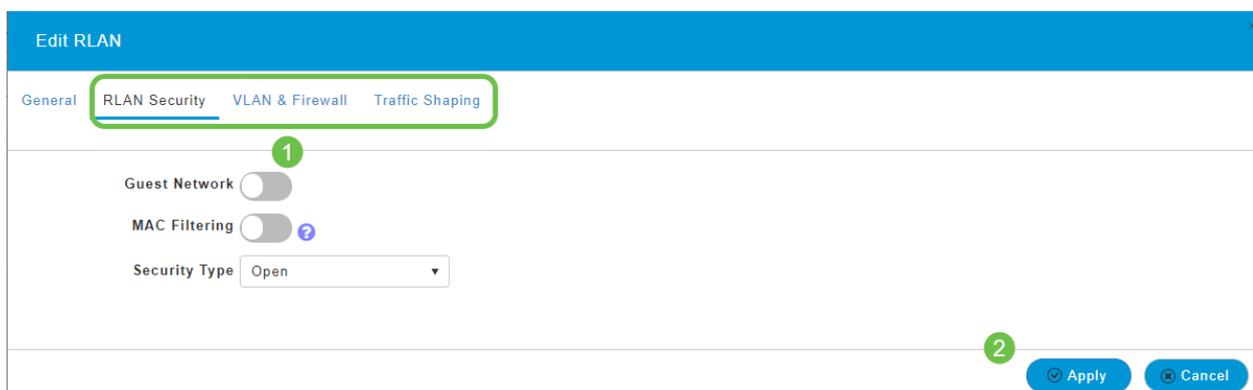
ステップ3 (有効/無効)

[Edit WLAN/RLAN]ウィンドウの[General]で、[Enabled] または[Disabled] を選択してRLANを有効/無効にします。[Apply] をクリックします。



ステップ4 (他の設定の編集)

設定を変更する必要がある場合は、[RLAN Security]、[VLAN & Firewall]、または[Traffic Shaping] タブに移動します。変更を加えたら、[Apply]をクリックします。



手順 5

Web UI画面の右上のパネルにあるSaveアイコンをクリックして、設定を保存してください。



結論

これで、CBWネットワークにRLANが作成されました。お楽しみください。必要に応じて追加することもできます。

[よく寄せられる質問 \(FAQ\)](#) [Radius Firmware Upgrade](#) [RLAN アプリケーションのプロファイリング](#) [クライアントプロファイリング](#) [プライマリAPツール](#) [Umbrella WLANユーザ](#) [Logging](#) [トラブルシューティング](#) [Rogues](#) [干渉源](#) [構成管理](#) [ポート設定](#) [メッシュモード](#) [CBWメッシュネットワーク](#) [へようこそ](#) [電子メール認証とRADIUSアカウントिंगを使用したゲストネットワーク](#) [トラブルシューティング](#) [CBWでのDraytekルータの使用](#)