

# Cisco Business Wireless Access PointでのRADIUSの設定

## 目的

このドキュメントの目的は、Cisco Business Wireless(CBW)Access Point(AP)でRADIUSを設定する方法を示すことです。

## 該当するデバイス|ファームウェアのバージョン

- 140AC ([データシート](#)) | 10.4.1.0 ([最新版をダウンロード](#))
- 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 ([最新のダウンロード](#))

## 概要

CBW APでRADIUSを設定する場合は、正しい場所に来ています。CBW 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。業界最高レベルのパフォーマンスを実現し、安全性と信頼性の高いワイヤレス接続を実現し、堅牢でモバイルなエンドユーザエクスペリエンスを実現します。

Remote Authentication Dial-In User Service(RADIUS)は、デバイスが接続してネットワークサービスを使用するための認証メカニズムです。これは、中央集中型の認証、認可、アカウントिंगの目的で使用されます。RADIUSサーバは、入力されたログインクレデンシャルを使用してユーザのIDを確認することにより、ネットワークへのアクセスを規制します。たとえば、公共のWi-Fiネットワークは大学のキャンパスに設置されます。これらのネットワークにアクセスできるのは、パスワードを持つ受講者だけです。RADIUSサーバは、ユーザが入力したパスワードをチェックし、必要に応じてワイヤレスローカルエリアネットワーク(WLAN)へのアクセスを許可または拒否します。

CBW APでRADIUSを設定する準備ができたら、まず始めましょう。

## 目次

- [CBW APでのRADIUSの設定](#)
- [WLAN の設定](#)
- [確認](#)


## CBW APでのRADIUSの設定

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ユーザー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

有効なユーザ名とパスワードを使用してCBW APにログインします。



# Cisco Business Wireless Access Point

Welcome! Please click the login button to enter your user name and password



#### 手順 2

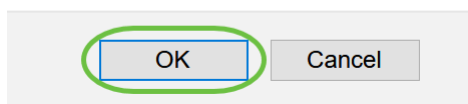
Webユーザインターフェイス(UI)の上部にある双方向矢印アイコンをクリックし、エキスパート

ビューに切り替えます。



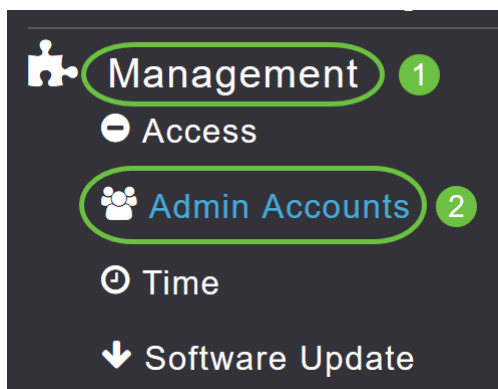
次のポップアップ画面が表示されます。[OK] をクリックして続行します。

Do you want to select Expert View?



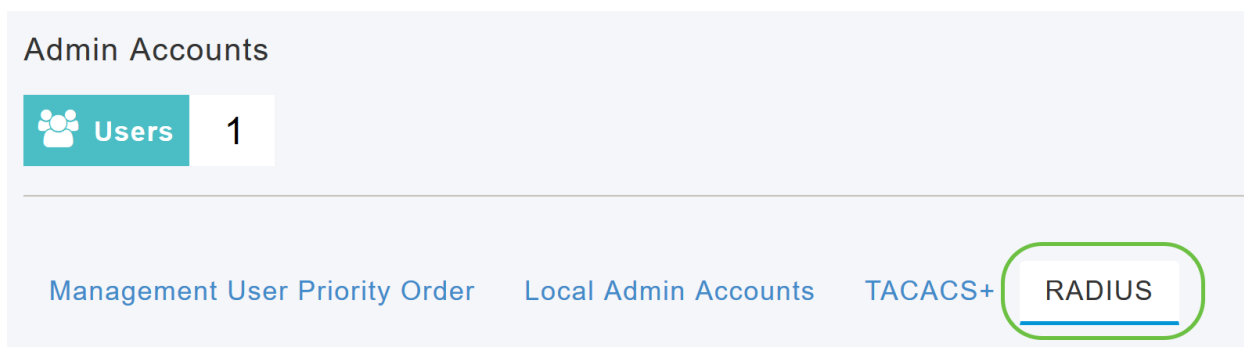
### 手順 3

[Management] > [Admin Accounts]に移動します。



### 手順 4

RADIUSサーバを追加するには、[RADIUS]タブをクリックします。



### 手順 5

[Authentication Call Station ID Type] ドロップダウンリストから、Access-RequestメッセージでRADIUSサーバに送信するオプションを選択します。次のオプションを使用できます。

- iSCSIポータルの

- プライマリAP MACアドレス
- AP MACアドレス
- AP MACアドレス : SSID
- AP名 : SSID
- AP名
- APグループ
- Flex Group
- APの場所
- VLAN ID
- APイーサネットMACアドレス
- APイーサネットMACアドレス : SSID
- APラベルアドレス
- APラベルアドレス : SSID
- AP MAC:SSID APグループ
- AP Eth MAC:SSID APグループ

Authentication Call Station ID Type AP MAC Address:SSID

Authentication MAC Delimiter IP Address

Accounting Call Station ID Type Primary AP MAC Address

Accounting MAC Delimiter AP MAC Address

Fallback Mode AP MAC Address:SSID

AP Name:SSID

AP Name

## 手順 6

ドロップダウンリストから[Authentication MAC Delimiter]を選択します。次のオプションがあります。

- コロン
- ハイフン
- シングルハイフン
- 区切り文字なし

Authentication MAC Delimiter Hyphen

Accounting Call Station ID Type Colon

Accounting MAC Delimiter Hyphen

Fallback Mode Single Hyphen

No Delimiter

## ステップ7

ドロップダウンリストから[Accounting Call Station ID Type]を選択します。

Accounting Call Station ID Type

Accounting MAC Delimiter

Fallback Mode

Username

Interval

## 手順 8

ドロップダウンリストから[Accounting MAC Delimiter]を選択します。

Accounting MAC Delimiter

Fallback Mode

Username

Interval

## 手順 9

ドロップダウンリストからRADIUSサーバのフォールバックモードを指定します。次のいずれかになります。

- *Off*:RADIUSサーバのフォールバックを無効にします。これがデフォルト値です。
- *Passive* : プライマリAPを、余分なプローブメッセージを使用せずに、使用可能なバックアップサーバから低い優先度のサーバに戻します。プライマリAPは、ある期間、非アクティブなサーバをすべて無視し、RADIUSメッセージを送信する必要がある場合は後で再試行します。
- *Active*:RADIUSプローブメッセージを使用して、非アクティブとマークされたサーバがオンラインに戻ったかどうかを予防的に判断することにより、プライマリAPが使用可能なバックアップサーバから低い優先度のサーバに戻ります。プライマリAPは、すべてのアクティブなRADIUS要求に対して、非アクティブなサーバをすべて無視します。プライマリサーバがリカバリされたACSサーバから応答を受信すると、アクティブフォールバックRADIUSサーバはアクティブプローブ認証を要求するサーバにプローブメッセージを送信しなくなります。

Fallback Mode

Username

Interval

Events Accounting

### 手順 10

アクティブフォールバックモードを有効にした場合は、[ユーザ名]フィールドに、非アクティブサーバプロブに送信する名前を入力します。

Fallback Mode

Username

Interval  Seconds

英数字は最大16文字まで入力できます。デフォルト値はcisco-probeです。

### 手順 11

アクティブ・フォールバク・モードを有効にした場合は、[間隔]フィールドにプローブ間隔の値(秒)を入力します。この間隔は、パッシブモードでは非アクティブ時間として機能し、アクティブモードではプローブ間隔として機能します。

Fallback Mode

Username

Interval  Seconds

有効な範囲は180 ~ 3600秒で、デフォルト値は300秒です。

### ステップ 12

AP Events Accountingスライダー・ボタンを有効にして、RADIUSサーバへのアカウントリング要求の送信をアクティブにします。

ネットワークの問題が発生している間、APはプライマリAPに参加/参加しません。このオプションを有効にすると、これらのイベントが監視され、ネットワークの問題を検出するためにアカウントリング要求がRADIUSサーバに送信されます。

AP Events Accounting



Apply

### 手順 13

[Apply] をクリックします。

Authentication Call Station ID Type	AP MAC Address:SSID	▼
Authentication MAC Delimiter	Hyphen	▼
Accounting Call Station ID Type	IP Address	▼
Accounting MAC Delimiter	Hyphen	▼
Fallback Mode	Active	▼
Username	cisco-probe	
Interval	300	Seconds
AP Events Accounting	<input checked="" type="checkbox"/>	

Apply

### ステップ 14

RADIUS認証サーバーを構成するには、「Add RADIUS Authentication Server」をクリックします。

Add RADIUS Authentication Server

Action	Server Index	Network User	Management	State	Server IP Addr...	Shared Key	Port
--------	--------------	--------------	------------	-------	-------------------	------------	------

### ステップ 15

[Add/Edit RADIUS Authentication]ポップアップウィンドウで、次のように設定します。

- サーバインデックス – 1から6を選択
- Network User : 状態を有効にします。デフォルトでは[Enabled]です
- 管理 : 状態を有効にします。デフォルトでは[Enabled]です
- State : 状態を有効にします。デフォルトでは[Enabled]です
- CoA : スライダボタンを動かすことで、このオプションを有効にできます
- Server IP Address:RADIUSサーバのIPv4アドレスを入力します

- *Shared Secret* : 共有秘密を入力します
- *Port Number*:RADIUSサーバとの通信に使用されるポート番号を入力します。
- *Server Timeout* : サーバタイムアウトを入力します

[Apply] をクリックします。

Add/Edit RADIUS Authentication Server. ✕

Server Index

Network User

Management

State

CoA

Server IP Address

Shared Secret

Confirm Shared Secret

Show Password

Port Number

Server Timeout  Seconds

---

✔ Apply
✕ Cancel

## ステップ 16

RADIUSアカウントिंगサーバを追加するには、ステップ15と同じ手順を実行します。ページに同様のフィールドが含まれているためです。

Add RADIUS Accounting Server

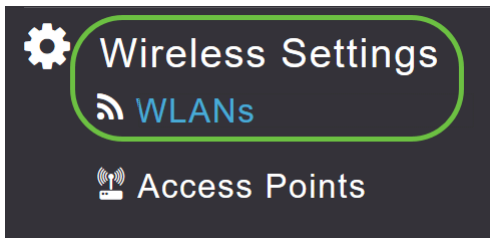
Action	Server Index	Network User	Management	State	Server IP Addr...	Shared Key	Port

## WLAN の設定

### 手順 1

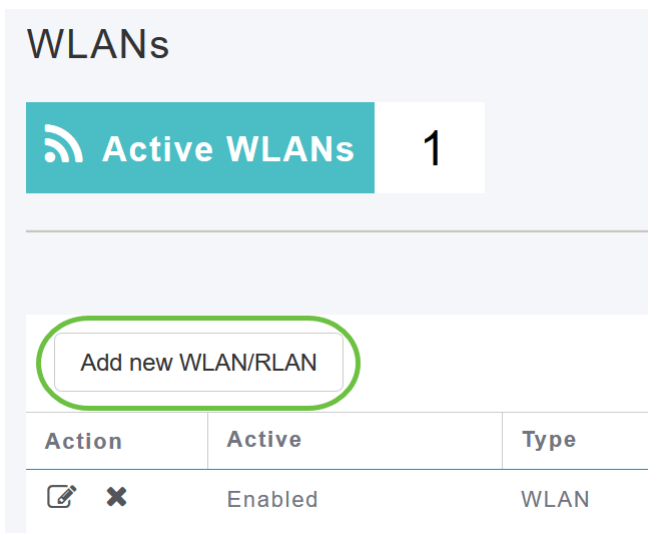
RADIUSを使用してWPA2認証を処理するWLANを設定するには、[Wireless settings] > [WLAN]に移動します。





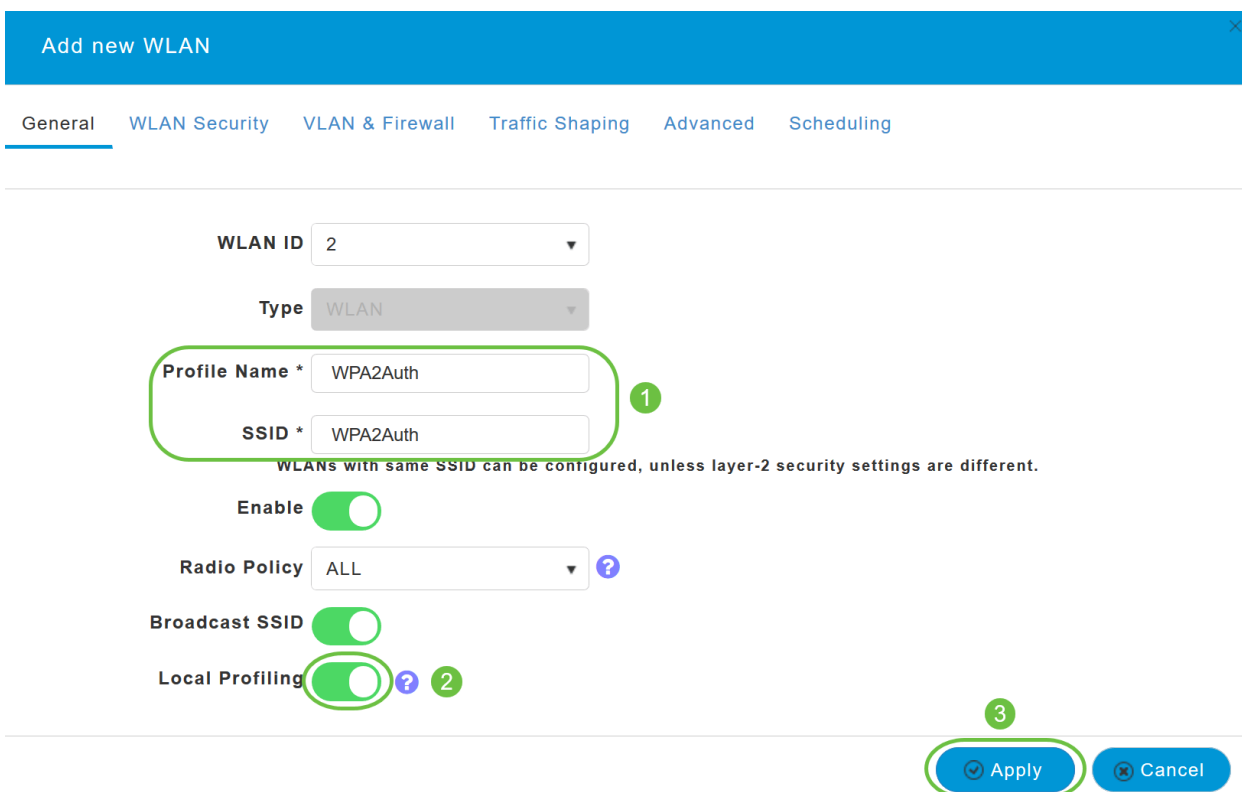
## 手順 2

Add New WLAN/RLANをクリックします。



## 手順 3

[全般]タブで、[プロファイル名]を入力します。[SSID]フィールドが自動的に入力されます。ローカルプロファイリングを有効にすることを選択できます。[Apply] をクリックします。



## 手順 4

[WLAN Security]タブに移動します。[セキュリティの種類]ドロップダウンメニューから、[WPA2Enterprise]を選択します。認証サーバとして[External Radius]を選択します。RADIUSプロファイリングを有効にすることを選択できます。

Add new WLAN

General WLAN Security VLAN & Firewall Traffic Shaping Advanced Scheduling

---

Guest Network

Captive Network Assistant

MAC Filtering  ?

Security Type WPA2Enterprise 1

Authentication Server External Radius ? 2

Radius Profiling  ? 3

BYOD

## 手順 5

[RADIUS Server]セクションに移動します。[Add RADIUS Authentication Server]をクリックします。

RADIUS Server 1

---

Authentication Caching

Add RADIUS Authentication Server 2

State
-------

## 手順 6

設定したRADIUS認証サーバの詳細を確認し、[Apply]をクリックします。

## Add RADIUS Authentication Server

Radius Server can be configured from 'Admin Accounts > RADIUS'(Expert view).

1

Server IP Address	172.16.1.25
State	Enabled
Port Number	1812

2

Apply Cancel

### ステップ7

[Add RADIUS Accounting Server]をクリックします。

<

Add RADIUS Accounting Server

Ac...	State
-------	-------

### 手順 8

設定したRADIUSアカウントングサーバの詳細を確認し、[Apply]をクリックします。

## Add RADIUS Accounting Server

Radius Server can be configured from 'Admin Accounts > RADIUS'(Expert view).

1

Server IP Address	172.16.1.25
State	Enabled
Port Number	1813

2

Apply Cancel

### 手順 9

[VLAN & Firewall]、[Traffic Shaping]、[Advanced]、および[Scheduling] タブに移動し、ネットワーク設定に基づいて設定を行います。[Apply] をクリックします。

Client IP Management External DHCP Server ▾

Peer to Peer Block 

Use VLAN Tagging No ▾

Enable Firewall No ▾

Apply

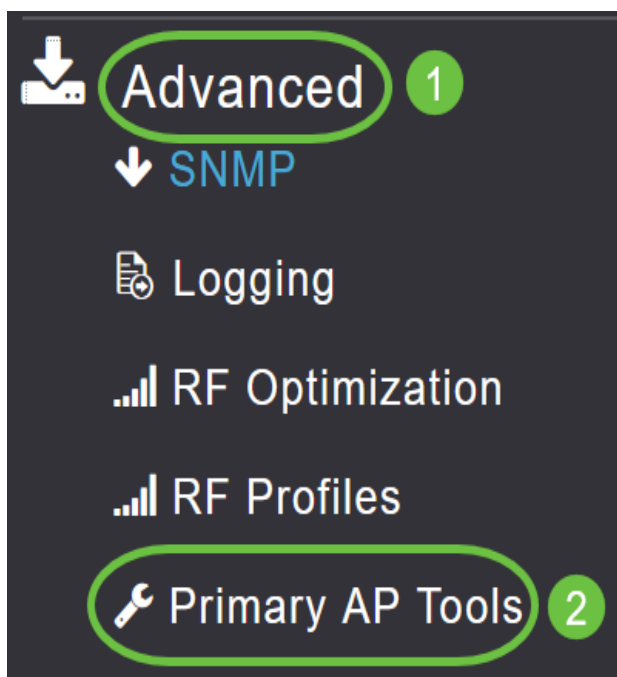
Cancel

## 確認

RADIUS認証をテストするには、次の手順を実行します。

### 手順 1

[Advanced] > [Primary AP Tools]に移動します。



### 手順 2

[Troubleshooting Tools]をクリックします。

## Primary AP Tools



Restart Primary AP

Configuration Management

Troubleshooting Files

Troubleshooting Tools

Upload File

### 手順 3

Radius Responseセクションで、前に設定したWLANプロファイルのUsernameとPasswordを入力し、Startをクリックします。

Radius Response ?

WLAN Profile WPA2Auth ?

1 Username test

2 Password .....

3 Start

Waiting for response from Radius server

Show Passphrase

### 手順 4

検証が正常に完了すると、画面に次の通知が表示されます。

Radius Response ?

WLAN Profile WPA2Auth ?

Username test

Password .....

Start

Authentication success (172.16.1.25)

Show Passphrase

## 結論

そこだ！これで、CBW APでRADIUSを設定する手順が学習されました。詳細な設定については、『Cisco Business Wireless Access Point Administration Guide』を参照してください。

[よく寄せられる質問 \(FAQ\)](#) [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](#) [トラフィックシェーピング](#) [Rogues](#) [干渉源](#) [構成管理](#) [ポート設定](#) [メッシュモード](#)