



Cisco Wi-Fi インターフェイスモジュール（WIM）設定ガイド

最終更新：2025年1月26日

シスコシステムズ合同会社

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

<http://www.cisco.com/jp>

お問い合わせ先：シスココンタクトセンター
0120-092-255（フリーコール、携帯・PHS含む）

電話受付時間：平日 10:00～12:00、13:00～17:00

<http://www.cisco.com/jp/go/contactcenter/>



目次

第 1 章

Cisco Wi-Fi インターフェイスモジュールの概要 1

Cisco Wi-Fi インターフェイスモジュール (WIM) の概要 1

ハードウェアの概要 1

ソフトウェアの概要 4

関連資料 6

第 2 章

IR1800 ルータのワイヤレス接続 7

IR1800 設定の概要 7

WIM モジュール管理コマンド 8

通常のルータブートアップ 8

WIM モジュールの非アクティブ化と再アクティブ化 9

工場出荷時の状態へのリセット 9

WIM の電源オフ 10

ルータコンソールを介した WIM との接続 11

デフォルト WIM パスワード 12

WIM イメージタイプの決定 13

第 3 章

WIM のファームウェアのアップグレード 15

ファームウェアをアップグレードするための前提条件 15

EWC AP ファームウェアのアップグレード 17

AP コマンドライン インターフェイス (CLI) を使用したファームウェアのアップグレード
18

17.9 から 17.11.1 以降の UIW イメージへのアップグレード 19

17.11 UIW および CAPWAP イメージのホストルータへのダウンロード 20

17.9 から CAPWAP 17.11 へのアップグレード	20
UIW 17.11 イメージのインストール	22
IOS XE 17.11 から IOS XE 17.12 以降への UIW イメージのアップグレード	24
イメージのダウングレード	25

第 4 章**モード間の変換 27**

Wi-Fi モードの変換	27
変換を始める前に	28
IOS XE 17.11.1 より前の Wi-Fi モードの変換	29
CAPWAP モードから EWC モードへの変換	29
CAPWAP モードから EWC モードへの変換手順	29
CAPWAP モードから WGB モードへの変換	30
WGB モードから CAPWAP モードへの変換	31
EWC モードから CAPWAP モードへの変換	31
EWC モードから CAPWAP モードへの変換手順	32
IOS XE 17.11.1 以降での Wi-Fi モードの変換	32
AP モードと EWC モード間の変換	32
CAPWAP モードから WGB モードへの変換	33
WGB モードから CAPWAP モードへの変換	33

第 5 章**WIM の一般的な展開モード 35**

一般的な導入シナリオ	35
Control And Provisioning of Wireless Access Points (CAPWAP)	36
IR1800 で CAPWAP アクセスポイント構成を設定するための前提条件	36
IR1800 での CAPWAP アクセスポイント構成設定手順	36
アクセスポイントの設定と配置	38
ワークグループブリッジ (WGB)	38
IR1800 で WGB を設定するための前提条件	39
WGB の設定と展開	40
uWGB の設定と展開	42
uWGB 設定例	43

uWGB または WGB アップリンクとルート AP モードの無線機の同時使用	44
無線機の同時使用に必要なルータ設定	46
無線インターフェイスの WGB/uWGB モードおよびルート AP モードへの設定	49
uWGB をアップリンクバックホールとして使用する場合のルート AP の無線機設定例	51
WGB ルート AP での Web 認証	54
Web 認証の概要	54
Web 認証プロセス	55
Web 認証設定の前提条件	55
Web 認証の制限事項	56
Web 認証の設定	56
WGB 設定のインポートとエクスポート	59
Web 認証の確認	59
Cisco Embedded Wireless Controller (EWC)	61
IR1800 で EWC アクセスポイントを設定するための前提条件	62
Day 0 プロビジョニングを使用した EWC の設定	63
Cisco Embedded Wireless Controller (EWC) 対応アクセスポイントのネットワークへの接続	64
EWC モードの WebUI 管理	64
Day 0 Over-The-Air WebUI セットアップウィザードを使用したプロビジョニング	64
EWC WebUI へのログイン	65

第 6 章	フレキシブルアンテナポート	67
	フレキシブルアンテナポート	67
	CAPWAP AP 用フレキシブルアンテナポートの設定	68
	WGB 用フレキシブルアンテナポートの設定	69



第 1 章

Cisco Wi-Fi インターフェイスモジュールの概要

この章は、次の項で構成されています。

- [Cisco Wi-Fi インターフェイスモジュール \(WIM\) の概要 \(1 ページ\)](#)
- [ハードウェアの概要 \(1 ページ\)](#)
- [ソフトウェアの概要 \(4 ページ\)](#)
- [関連資料 \(6 ページ\)](#)

Cisco Wi-Fi インターフェイスモジュール (WIM) の概要

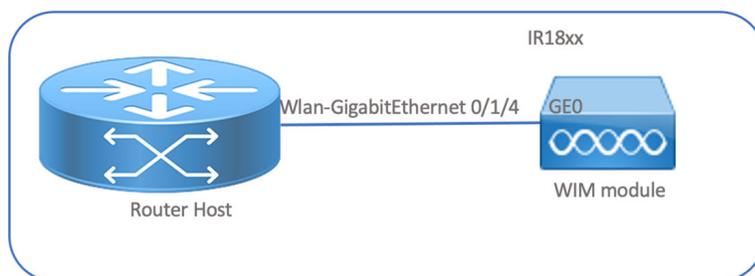
このセクションでは、Cisco Wi-Fi インターフェイスモジュール (WIM) の概要について説明します。PID は WP-WIFI6-x です。ここで、x は規制ドメインを示します。

WIM のハイライトは次のとおりです。

- Cisco Catalyst IR1800 シリーズ用 802.11ax プラガブルモジュール
- Wi-Fi-6 (802.11ax) 、2 X 2 MIMO (2 つの空間ストリームに対応)
- 広範な動作温度範囲
- ただし、Field Replaceable Unit (FRU) は、OIR (活性挿抜) をサポートしていません
- 外部 RP-SMA アンテナコネクタにより多様な RF カバレッジに対応可能
- フレキシブルアンテナポート機能のサポート
- Cisco AP 9105AXI がベース

ハードウェアの概要

次の図は、WIM の制御パスとデータパスを示しています。有線インターフェイスは、IR1800 シリーズ スイッチポート (名前は wlan-GigabitEthernet 0/1/4) に接続されています。



次の図は、WIM の前面パネルを示しています。

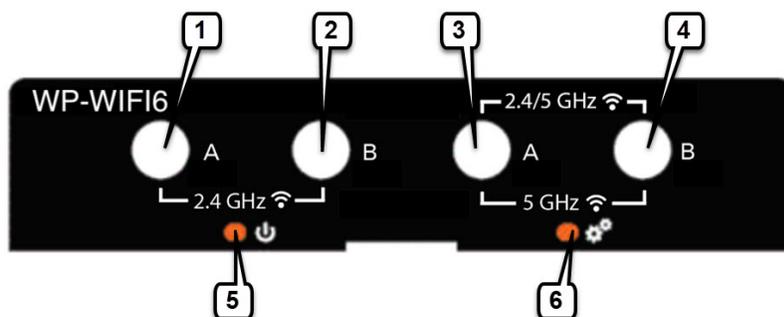


表 1: WIM 前面パネル

アイテム	説明
1	フレキシブルアンテナポートがデュアルバンドモードに設定されている場合は無効です（デフォルト）。 フレキシブルアンテナポートがシングルバンドモードに設定されている場合は 2.4 GHz。
2	フレキシブルアンテナポートがデュアルバンドモードに設定されている場合は無効です（デフォルト）。 フレキシブルアンテナポートがシングルバンドモードに設定されている場合は 2.4 GHz。
3	フレキシブルアンテナポートがデュアルバンドモードに設定されている場合は 2.4/5 GHz（デフォルト）。 フレキシブルアンテナポートがシングルバンドモードに設定されている場合は 5 GHz のみ。
4	フレキシブルアンテナポートがデュアルバンドモードに設定されている場合は 2.4/5 GHz（デフォルト）。 フレキシブルアンテナポートがシングルバンドモードに設定されている場合は 5 GHz のみ。
5	有効 LED

アイテム	説明
6	Wi-Fi LED



(注) 詳細については、[フレキシブルアンテナポート \(67 ページ\)](#) を参照してください。

次の表で、有効な LED について説明します。

LED ステータス	説明
消灯	電力なし
黄色	電源は入っていますが、モジュールはまだ機能していません
緑色	モジュールは完全に機能しています。

次の表で、Wi-Fi の LED について説明します。



(注) LED ステータス情報は、無線機の同時使用モードには適用されません。無線機の同時使用時のルート AP + ワイヤレスクライアントには、デフォルトの LED 動作 (赤/緑の交互点滅) が表示されます。

LED ステータス	ステータスタイプ	説明
緑色の点灯	アソシエーションの状態	正常な動作状態ですが、ワイヤレスクライアントの関連付けがありません。
青色の点灯	アソシエーションの状態	<ul style="list-style-type: none"> • WP-WIFI6 (CAPWAP モード) : WLC に登録されたインフラ AP、AP に接続されたクライアント • WP-WIFI6 (UIW WGB) : 1 : インフラ AP に登録された WGB 2 : 両方の無線機がルート AP (二番目の無線機) + ワイヤレスクライアントが接続済み : NA
緑色の点灯	ブートローダの状態	ブートローダを実行中。
緑色の点滅	ブートローダの状態	ブートローダエラー、署名検証エラー。
青色の点滅	動作状態	ソフトウェアのアップグレード中。

LED ステータス	ステータスタイプ	説明
緑色と赤色の交互の点滅	動作状態	検出/接続プロセスが進行中
赤色、消灯、緑色、消灯、青色、消灯の繰り返し	アクセスポイントのオペレーティングシステムエラー	一般的な警告。インライン電力不足。

ソフトウェアの概要

WIM は、IR1800 シリーズの 4 つすべてのモデルでサポートされます。

サポートされる機能は、WIM ソフトウェアで実行されるバージョンに応じて異なります。IR1800 ルータのソフトウェアは、IOS-XE バージョン 17.7.1 以降を実行している必要があります。WIM で使用可能な機能は、ルータの IOS XE ソフトウェアバージョンで使用可能な機能と、WIM が実行されているモードによって異なります。次の表に詳細を示します。

表 2: 機能マトリックス

ルータの IOS XE リリース	WIM の IOS XE リリース	機能	WIM ソフトウェアイメージタイプ
17.7.1 以降		サポートされる 3 つのモード:	
	17.6.1 ~ 17.10.x	Control And Provisioning of Wireless Access Points (CAPWAP)	ap1g8-k9w8
	17.6.1 ~ 17.10.x	Cisco Embedded Wireless Controller (EWC)	C9800-AP-iosxe-wlc.bin
	17.6.1 ~ 17.10.x	ワークグループブリッジ (WGB)	ap1g8-k9w8

ルータの IOS XE リリース	WIM の IOS XE リリース	機能	WIM ソフトウェアイメージタイプ
17.7.1 以降	17.11.1 以降	<p>Unified Industrial Wireless (UIW) ソフトウェアイメージタイプが導入され、次がサポートされます。</p> <ul style="list-style-type: none"> UIW : WGB モードのサポートが ap1g8-k9w8 から ap1g8t-k9c1 に移行 UIW : WGB アップリンクとルート AP モードの無線機の同時使用 UIW : デュアルルート AP モードの無線機の同時使用 <p>UIW イメージの詳細については、17.9 から 17.11.1 以降の UIW イメージへのアップグレード を参照してください。</p> <p>(注) ap1g8-k9w8 での WGB モードは、17.11.1 以降では廃止となっています。</p>	ap1g8t-k9c1

機能セットは AP 9105AXI と同様です。『[Feature Matrix for Cisco Wireless Access Points](#)』[英語]を参照してください。

各種 WIM ソフトウェアについては、「[ソフトウェアのダウンロード](#)」ページを参照してください。

発注情報

Cisco Commerce 構成では、Wi-Fi ソフトウェアは、異なるイメージタイプにバンドルされた 3 種類の構成でご利用いただけます。WIM モジュールは、構成に合わせて事前にインストールされたイメージバンドルを含めて出荷されます。

- SW-WPWIFI6-EWC : デフォルトを EWC アクセスポイントとする C9800-AP-iosxe-wlc.bin + ap1g8-k9w8 イメージバンドル (EWC + CAPWAP)
- SW-WPWIFI6-CW : デフォルトを CAPWAP アクセスポイントとする ap1g8-k9w8 + ap1g8t-k9c1 イメージバンドル (CAPWAP + UIW WGB)
- SW-WPWIFI6-WGB : デフォルトを WGB アクセスポイントとする ap1g8-k9w8 + ap1g8t-k9c1 イメージバンドル (CAPWAP + UIW WGB)

WIM は、プログラムされたイメージバンドルの機能の範囲内で、各種イメージを起動し、AP タイプを変換してさまざまな動作モードをサポートできます。詳細については、変換の項を参照してください。EWC と WGB は排他的です。



ヒント シスコは、一般的な展開の用途に応じて選択したイメージバンドルが事前にインストールされた状態になるよう Wi-Fi ソフトウェアを注文することを推奨しています。

関連資料

設置シナリオに応じて、アクセスポイントで設定できるさまざまなオプションがあります。関連するドキュメントは、次の場所から入手できます。

[Cisco Catalyst 9100 ファミリアccessポイント](#)

[Cisco Wireless Controller Configuration Guide](#)

[Cisco Embedded Wireless Controller on Catalyst Access Points FAQ \[英語\]](#)

[Cisco Catalyst 9800 Series Configuration Best Practices](#)

[Cisco Wave 2 Access Points as Workgroup Bridges \[英語\]](#)

[Cisco Industrial Wireless Workgroup Bridge and Universal WGB Deployment Guide \[英語\]](#)



第 2 章

IR1800 ルータのワイヤレス接続

この章では、Cisco Catalyst IR1800 高耐久性シリーズ ルータの内部スイッチインターフェイスおよびモジュール管理に対する、Wi-Fi カードの設定方法について説明します。

この章は、次の項で構成されています。

- [IR1800 設定の概要 \(7 ページ\)](#)
- [WIM モジュール管理コマンド \(8 ページ\)](#)
- [通常のルータブートアップ \(8 ページ\)](#)
- [WIM モジュールの非アクティブ化と再アクティブ化 \(9 ページ\)](#)
- [工場出荷時の状態へのリセット \(9 ページ\)](#)
- [WIM の電源オフ \(10 ページ\)](#)
- [ルータコンソールを介した WIM との接続 \(11 ページ\)](#)
- [デフォルト WIM パスワード \(12 ページ\)](#)
- [WIM イメージタイプの決定 \(13 ページ\)](#)

IR1800 設定の概要

次に、製品設定の詳細の一部を示します。

- モジュールはサブスロット 0/3 に固定されています。
- AP と通信するための Wi-Fi インターフェイスは W10/1/4 と呼ばれます。
- デフォルトでは、W10/1/4 は VLAN 1 内に配置されます。
 - DHCP プールが VLAN1 上に設定されている場合、AP (および関連するクライアント) は IP アドレスを取得します。
- モジュールはホットスワップ非対応ですが、現場交換は可能です。
- モジュール挿入後にホストルータを手動でリロードする必要があります。

WIM モジュール管理コマンド

IOS XE ルータのコンソールから、モジュールのステータスを表示するために使用するコマンドは次のとおりです。

- show platform
- show inventory
- show hw-module subslot 0/3 attribute
- show logging

IOS XE ルータのコンソールからモジュールを設定するために使用するコマンドは、次のとおりです。

- hw-module subslot 0/3 maintenance enable | disable
- hw-module subslot 0/3 stop | start | reload [force]
- hw-module subslot 0/3 error-recovery password_reset
- hw-module session 0/3

通常のルータブートアップ

ホストルータがリロードされると同時に Wi-Fi モジュールの電源がオンになります。ホストが Wi-Fi モジュールから [ready] 信号を受信すると、Wi-Fi モジュールの状態が [booting] から [ok] に変わります。次に例を示します。

```
#show platform
Chassis type: IR1835-K9
Slot      Type                State                Insert time (ago)
-----
0         IR1835-K9           ok                   15:25:47
0/0      IR1835-1x1GE       ok                   15:23:37
0/1      IR1835-ES-4        ok                   15:23:36
0/3      WP-WIFI6-B         ok                   00:00:07
R0       IR1835-K9           ok, active          15:25:47
F0       IR1835-K9           ok, active          15:25:47
P0       PWR-12V             ok                   15:23:59
GE-POE   Unknown             ok                   15:23:59

# show logging
Apr  6 18:05:41.992 CST: %IOSXE_OIR-6-INSSPA: SPA inserted in subslot 0/3
Apr  6 18:05:54.886 CST: new extended attributes received from iomd(slot 0 bay 3 board 0)
Apr  6 18:05:55.226 CST: %SPA_OIR-6-ONLINECARD: SPA (WP-WIFI6) online in subslot 0/3
```

WIM モジュールの非アクティブ化と再アクティブ化

WIM モジュールは、非アクティブ化しなくてもルータから取り外せます。ただし、モジュールを取り外す前に、モジュールを正しい手順で非アクティブにする（または正しい手順で電源をオフにする）ことを推奨します。EXEC モードで次のコマンドを使用します。

1. `hw-module subslot 0/3 stop`



(注) `hw-module subslot 0/3 stop` コマンドを使用してモジュールを非アクティブにした後に、モジュールを再アクティブ化するには、次のいずれかのコマンドを（特権 EXEC モードで）使用します。

2. `hw-module subslot 0/3 start`

3. `hw-module subslot 0/3 reload [force]`

表 3: `hw-module subslot` コマンドオプション

コマンド	説明
<code>reload</code>	指定したモジュールを停止してから再起動します。
<code>stop</code>	モジュールからすべてのインターフェイスを削除し、モジュールの電源をオフにします。
<code>start</code>	指定のスロットに物理的に装着されたモジュールの場合と同様に、モジュールの電源をオンにします。モジュールファームウェアがリブートされ、モジュール初期化シーケンス全体が実行されます。

工場出荷時の状態へのリセット

ユーザーは、ホストルータから次のコマンドを実行して、WIM を初期設定にリセットできます。

```
Router# hw-module subslot 0/3 error-recovery password_reset
```

上記のコマンドは、WIM をメンテナンスモードに設定します。



- (注) **hw-module subslot 0/3 error-recovery password_reset** コマンドを実行すると、AP モジュールが自動的にリロードして設定を復元し、メンテナンスモードを開始します。メンテナンスモードでは、AP モジュールは電源オンモードです。コンソールまたは Web UI を使用して、モジュール設定のリセットを確認します。AP をリロードしてメンテナンスモードを終了するには、**hw-module subslot 0/3 reload force** コマンドを発行する必要があります。

次に、工場出荷時の状態へのリセットシーケンスを示します。

```
Router# hw-module subslot 0/3 error-recovery password_reset
```

1. WIM がリロードされます。
2. WIM はメンテナンスモードに設定され、アウトオブサービスと表示されます。

```
Router# show platform
Chassis type: IR1835-K9
Slot   Type           State           Insert time (ago)
0      IR1835-K9       ok             00:54:57
0/0    IR1835-1K1GE   ok             00:52:49
0/1    IR1835-ES-4    ok             00:52:46
0/3    WP-WIFI6-B     out of service 00:34:24
R0     IR1835-K9      ok, active     00:54:57
FO     IR1835-K9      ok, active     00:54:57
PO     P-R-12V        ok             00:53:09
GE-P06 Unknown        ok             00:53:09
```

ユーザーは約 30 秒待つってから、次のコマンドを使用します。

```
Router# hw-module subslot 0/3 reload force
```

1. WIM がリロードされます。
2. WIM がメンテナンスモードを終了します。WIM が OK 状態になるまで待ちます。

```
Router#show platform
Chassis type: IR1835-K9
Slot   Type           State           Insert time (ago)
0      IR1835-K9       ok             00:56:50
0/0    IR1835-1X1GE   ok             00:54:42
0/1    IR1835-ES-4    ok             00:54:39
0/3    WP-WIFI6-B     ok             00:01:36
```

WIM の電源オフ

WIM が 20 分以内に 5 回リロードされた場合（連続するソフトウェアクラッシュなど）、ホストルータは WIM の電源をオフにします。

```
*Apr 7 10:34:57.412 CST: %SPA_OIR-6-ONLINECARD: SPA (WP-WIFI6) online in subslot 0/3
*Apr 7 10:36:19.021 CST: %SPA_OIR-6-OFFLINECARD: SPA (WP-WIFI6) offline in subslot 0/3
*Apr 7 10:37:59.128 CST: %SPA_OIR-6-ONLINECARD: SPA (WP-WIFI6) online in subslot 0/3
*Apr 7 10:39:18.942 CST: %SPA_OIR-6-OFFLINECARD: SPA (WP-WIFI6) offline in subslot 0/3
*Apr 7 10:41:00.072 CST: %SPA_OIR-6-ONLINECARD: SPA (WP-WIFI6) online in subslot 0/3
*Apr 7 10:42:15.864 CST: %SPA_OIR-6-OFFLINECARD: SPA (WP-WIFI6) offline in subslot 0/3
```

```
*Apr 7 10:43:57.507 CST: %SPA_OIR-6-ONLINECARD: SPA (WP-WIFI6) online in subslot 0/3
*Apr 7 10:45:06.049 CST: %SPA_OIR-6-OFFLINECARD: SPA (WP-WIFI6) offline in subslot 0/3
*Apr 7 10:46:46.167 CST: %SPA_OIR-6-ONLINECARD: SPA (WP-WIFI6) online in subslot 0/3
*Apr 7 10:48:12.425 CST: %SPA_OIR-3-SPA_POWERED_OFF: subslot 0/3: SPA WP-WIFI6 powered
off after 5 failures within 1200 seconds
*Apr 7 10:48:12.425 CST: %SPA_OIR-6-OFFLINECARD: SPA (WP-WIFI6) offline in subslot 0/3
```

```
Router# show platform
Chassis type: IR1835-K9
Slot      Type                State                Insert time (ago)
-----
0         IR1835-K9           ok                  16:45:16
0/0      IR1835-1x1GE       ok                  16:43:06
0/1      IR1835-ES-4        ok                  16:43:05
0/3      WP-WIFI6-B         out of service     00:00:39
R0       IR1835-K9           ok, active         16:45:16
F0       IR1835-K9           ok, active         16:45:16
P0       PWR-12V             ok                  16:43:28
GE-POE   Unknown             ok                  16:43:28
```

ルータコンソールを介した WIM との接続

WIM に接続するには、まずコンソール、SSH プロトコル、または Telnet プロトコルを介してホストルータへの接続を確立します。

次に、ホストルータからアクセスポイントにリダイレクトします。次の例を参照してください。

```
Router# hw-module session 0/3
Establishing session connect to subslot 0/3
To exit, type ^a^q <-This sequence to disconnect is Ctrl-a Ctrl-q
picocom v3.1
port is: /dev/ttyWIFI
flowcontrol: none
baudrate is: 9600
parity: none
databits are: 8
stopbits are: 1
escape is: C-a
local echo is: no
noinit is: no
noreset is: no
hangup is: no
nolock is: yes
send_cmd is: sz -vv
receive_cmd is: rz -vv -E
imap is:
omap is:
emap is: crcrlf,delbs,
logfile is: none
initstring: none
exit_after is: not set
exit is: no
Type [C-a] [C-h] to see available commands
Terminal ready
Username:
```

次の手順を実行して、アクセスポイントから切断します。

```

issue ^a^q <-This sequence to disconnect is Ctrl-a Ctrl-q
Username:
Terminating...
Skipping tty reset...
Thanks for using picocom
Router#

```

デフォルト WIM パスワード

WIM のデフォルトのパスワードは、モードとソフトウェアリリースによって異なります。

WIM CAPWAP AP パスワード

CAPWAP AP のデフォルトのログイン情報は次のとおりです。

- ユーザー名 : **cisco**
- パスワード : **cisco**
- イネーブルパスワード : **cisco**

WIM EWC パスワード

Embedded Wireless Controller のデフォルトのログイン情報は次のとおりです。

- ユーザー名 : **webui**
- パスワード : **cisco**



(注) これらのログイン情報は、Over-the-Air セットアップウィザードへの UI アクセス、または SSH/CLI ベースの Day-0 プロビジョニングで使用できます。

WIM WGB パスワード

WIM の WGB モードのデフォルトパスワードは、ルータと WIM ソフトウェアリリースによって異なります。詳細は次の表に記載します。

表 4:

IR1800 の IOS XE リリース	WIM の IOS XE バージョン	デフォルトパスワード
17.9.x 以前	すべて	ユーザー名 : cisco パスワード : cisco イネーブルパスワード : cisco

IR1800 の IOS XE リリース	WIM の IOS XE バージョン	デフォルトパスワード
17.10.1 以降	17.7.1 以前	ユーザー名 : cisco パスワード : cisco イネーブルパスワード : cisco
	17.8.1 以降	ユーザー名 : Cisco1 パスワード : GigabitEth01! イネーブルパスワード : AppleTree01@

WIM イメージタイプの決定

IOS XE 17.11.1 の AP イメージが導入される前は、Wi-Fi モジュール WGB、CAPWAP イメージ (apl8) を使って AP タイプの変換 (CAPWAP モードまたは WGB モードへの切り替え) を行っていました。

IOS XE 17.11.1 以降には、Unified Industrial Wireless (UIW) イメージと呼ばれる新しいイメージタイプがあります。このイメージは apl8t-k9c1 と呼ばれます。この新しいソフトウェアイメージでは、WGB とルート AP 機能による無線機の同時使用が可能です。

イメージタイプの決定

次のコマンドを使用します。

コマンド	イメージタイプ
AccessPoint# sh version inc AP Cisco AP Software, (apl8)	CAPWAP イメージ
AccessPoint# sh version inc AP Cisco AP Software, (apl8t), C6, RELEASE SOFTWARE.	UIW イメージ
AccessPoint# show version include AP AP Image type: EWC-AP IMAGE AP Configuration: NOT ME OR EWC-AP CAPABLE	EWC イメージ

CAPWAP イメージの実行時に **UIW** イメージがインストールされているかどうかを特定する

次のコマンドを使用します。

コマンド	イメージタイプ
AccessPoint# configure boot mode wgb Image swapping will restore the device to factory settings. Are you sure to proceed? (y/n) n Process Canceled!	UIW イメージがインストールされている
AccessPoint# configure boot mode wgb Error: Unified client image missed.	UIW イメージがインストールされていない



第 3 章

WIM のファームウェアのアップグレード

この章は、次の項で構成されています。

- [ファームウェアをアップグレードするための前提条件 \(15 ページ\)](#)
- [EWC AP ファームウェアのアップグレード \(17 ページ\)](#)
- [AP コマンドラインインターフェイス \(CLI\) を使用したファームウェアのアップグレード \(18 ページ\)](#)
- [17.9 から 17.11.1 以降の UIW イメージへのアップグレード \(19 ページ\)](#)
- [17.11 UIW および CAPWAP イメージのホストルータへのダウンロード \(20 ページ\)](#)
- [17.9 から CAPWAP 17.11 へのアップグレード \(20 ページ\)](#)
- [UIW 17.11 イメージのインストール \(22 ページ\)](#)
- [IOS XE 17.11 から IOS XE 17.12 以降への UIW イメージのアップグレード \(24 ページ\)](#)
- [イメージのダウングレード \(25 ページ\)](#)

ファームウェアをアップグレードするための前提条件



重要 モジュールファームウェアをアップグレードする前に、ルータを IOS XE リリース 17.11.1 以降に更新することを推奨します。

以下の前提条件が整っていることを確認します。

- IR1800 と AP との間にネットワーク接続が必要です。
- AP がイメージを取得するためには、IR1800 の TFTP サーバーが有効になっている必要があります。

IR1800 の設定

次の例を参照してください。

```
Router#sh run int vlan1
Building configuration...
```

```

Current configuration : 60 bytes
!
interface Vlan1
ip address 10.10.10.1 255.255.255.0

interface Wl0/1/4
switchport mode access
switchport access vlan <id>
(In the example above vlan 1 is used)
end

```



(注) vlan id には、<1 ~ 4094> の範囲の任意の値を指定できます。

EWC AP および CAPWAP の IP アドレスを使用した Wi-Fi モジュールの設定

Wi-Fi モジュールをアップグレードまたは変換する際は、IP アドレスが必要です。次の 2 つの方式があります。

1. IR1800 で DHCP サーバーを設定して、Wi-Fi モジュールに IP アドレスを提供する

```

IR1800 Router:
Router#sh run | sec vlan1
ip dhcp pool vlan1
 network 10.10.10.0 255.255.255.0
 default-router 10.10.10.1
Router#

```

WP-WIFI6: Gets ip from IR1800 DHCP server

```

APBCE7.120C.D748#sh ip in br
Interface          IP-Address      Method   Status   Protocol   Speed   Duplex
wired0             10.10.10.2     DHCP    up       up         1000   full
auxiliary-client   unassigned      unset    up       up         n/a    n/a
apr0v0             n/a            n/a     up       up         n/a    n/a
apr1v0             n/a            n/a     up       up         n/a    n/a
APBCE7.120C.D748#

```

2. Wi-Fi モジュールに静的 IP アドレスを設定する

capwap ap ip <ip address> <netmask> <gateway> コマンドを使用します。

```

APBCE7.120C.D748#capwap ap ip 10.10.10.4 255.255.255.0 10.10.10.1
[*12/07/2023 14:01:39.3510] ethernet_port wired0, ip 10.10.10.4, netmask 255.255.255.0,
 gw 10.10.10.1, mtu 1500, bcast 10.10.10.255, dns1 0.0.0.0, is_static true, vid 0,
 static_ip_failover false, dhcp_vlan_failover false

```

```

APBCE7.120C.D748#ping 10.10.10.1

```

```

Sending 5, 100-byte ICMP Echos to 10.10.10.1, timeout is 2 seconds

```

```

PING 10.10.10.1

```

```

!!!!

```

```

Success rate is 100 percent (5/5), round-trip min/avg/max = 0.997/1.100/1.221 ms

```

```

APBCE7.120C.D748#

```

IOS XE 17.13.1 以降を実行する UIW WGB モードの Wi-Fi モジュールの IP アドレス設定

configure ap address ipv4 static <ip address> <netmask> <gateway> コマンドを使用します。次に例を示します。

```
APBCE7.120C.D748#configure ap address ipv4 static 10.10.10.2 255.255.255.0 10.10.10.1
```



(注) ゲートウェイ IP アドレスは、IR1800 ルータ SVI の IP アドレスです。

IOS XE 17.11.x および 17.12.x を実行する UIW WGB モードの Wi-Fi モジュールの IP アドレス設定

IOS XE 17.11.x および 17.12.x を実行しているルータでは、一見すると上記の **configure ap address** コマンド単体で設定できているように見えますが、それだけでは Wi-Fi モジュール上に完全な IP プレゼンスが確立されません。ユニットに「ダミー」の ssid を設定するためには、追加のコマンドが必要です。次のコマンドの実行が前提条件となります。

```
configure ssid-profile dummy ssid dummy authentication open
configure dot11 1 mode wgb ssid dummy
configure dot11 1 enable
configure dot11 1 disable
```



(注) WGB 無線機がすでに設定され、有効になっている場合は、静的 IP アドレスを直接追加できるので、前提条件である上記の手順は必要ありません。

次の例に示すように、Sub-If が「wbridge.x」であることを確認します。

```
WGB#sh datapath command /click/br_router/dump_root_subifs
Root_port BG-ID Hop-Address Sub-If VID VAP Trunk Sec_Trunk Vlan-Trans Learn
Uni-Flood Flood-Age
57 1 BC:E7:12:0C:E4:0F wbridge.0 0 0 true true false false
true 0
```

configure ap address ipv4 static <ip address> <netmask> <gateway> コマンドを使用します。次に例を示します。

```
APBCE7.120C.D748#configure ap address ipv4 static 10.10.10.2 255.255.255.0 10.10.10.1
```

EWC AP ファームウェアのアップグレード

ファームウェアは、EWC モードで、アクセスポイントのコマンドラインインターフェイスまたは WebUI からアップグレードできます。

ここでは、アップグレードの前提条件と、アップグレードの実行手順を説明します。

AP コマンドラインインターフェイス (CLI) を使用したファームウェアのアップグレード

IR1800 ブートフラッシュにイメージファイルを取得するには、セキュアコピーと TFTP 転送の 2 つの方法があります。

イメージをアップグレードする前に、vlan1 と Wi-Fi モジュールに IP アドレスが設定されていることを確認します。[ファームウェアをアップグレードするための前提条件 \(15 ページ\)](#) の項を確認してください。

セキュアコピーを使用する場合

1. イメージファイルを IR1800 ブートフラッシュにコピーします。



(注) セキュアコピー (scp) を使用するには、最初に SSH の設定をセットアップする必要があります。[「Configuring Secure Shell」](#) を参照してください。

```
Router# copy scp: bootflash:
Address or name of remote host []? 192.168.1.2
Source username [xxxxxx]?Enter
Source filename []? /auto/users/<your-image>
Destination filename [<your-image>]?
```

This is a Cisco managed device to be used only for authorized purposes.
Your use is monitored for security, asset protection, and policy compliance.

```
Password: <your-password>
Sending file modes: C0644 208904396 <your-image>
.....
[OK - 208904396 bytes]
208904396 bytes copied in 330.453 secs (632176 bytes/sec)
```

2. IR1800 を SFTP サーバーとして機能するように設定します。

```
ip scp source-interface Vlan1 ! VLAN interface to be modified based on the
configuration
sftp-server bootflash:<your-image>
```

3. AP CLI から AP ファームウェアをアップグレードします。

```
#ap-type ewc-ap sftp://10.10.10.1/aplg8 sftp://10.10.10.1/<your-image>
```

TFTP 転送を使用する場合

1. イメージファイルを IR1800 ブートフラッシュにコピーします。

```
Router# copy tftp: bootflash:
Address or name of remote host []? 192.168.1.2
Source filename []? /auto/users/<your-image>
Destination filename [<your-image>]?
.....
```

```
[OK - 208904396 bytes]
208904396 bytes copied in 330.453 secs (632176 bytes/sec)
```

2. IR1800 を TFTP サーバーとして機能するように設定します。

```
ip tftp source-interface Vlan1 ! VLAN interface to be modified based on the
configuration
tftp-server bootflash:<your-image>
```

3. AP CLI から AP ファームウェアをアップグレードします。

```
#ap-type ewc-ap tftp://10.10.10.1/ap1g8 tftp://10.10.10.1/<your-image>
```

17.9 から 17.11.1 以降の UIW イメージへのアップグレード

IOSXE 17.11.1 以降、イメージアーキテクチャが新しいイメージタイプに変更され、WP-WIFI6 モジュールの Unified Industrial Wireless (UIW) イメージが導入されました。イメージ名は ap1g8t-k9c1 です。従来の CAPWAP (ap1g8-k9w8) イメージに代わって、UIW イメージが WGB 機能を提供します。

UIW イメージがプログラムされていない場合、この章で、Wi-Fi モジュールのフラッシュパーティションに新しいイメージをプログラムするための手順を説明します。

UIW イメージがすでにインストールされている場合は、この章をスキップしてください。

デバイス上に 2 つのタイプのイメージが共存し、各イメージが独立したプライマリパーティションとバックアップパーティションを持ちます。次の表に、IOS XE 17.9 と 17.11 のイメージパーティションの違いを示します。



UIW イメージがサポートされるのは IOS XE 17.11 以降であるため、それより古いイメージ上で動作していて、UIW イメージを一度もインストールしていないデバイスは、次の手順に従ってアップグレードを開始する必要があります。

- [17.11 UIW および CAPWAP イメージのホストルータへのダウンロード](#)
- [17.9 から CAPWAP 17.11 へのアップグレード](#)
- [UIW 17.11 イメージのインストール](#)

17.11 UIW および CAPWAP イメージのホストルータへのダウンロード

アップグレードを開始する前に、必要なイメージを IR1800 にダウンロードします。次のイメージが必要です。

- [17.11 CAPWAP CCO イメージ](#)
- [17.11 UIW CCO イメージ](#)

手順

ステップ 1 イメージをアップグレードする前に、vlan1 と Wi-Fi モジュールに IP アドレスが設定されていることを確認します。[ファームウェアをアップグレードするための前提条件 \(15 ページ\)](#) の項を確認してください。

ステップ 2 イメージを IR1800 の `flash:` ディレクトリに配置します。

a) TFTP ブロックサイズを設定します。

```
IR1800(config)#ip tftp blocksize 8192
```

b) バージョン 17.11 UIW CCO イメージをダウンロードします。

```
IR1800#copy tftp://<TFTP IP>/ap1g8t-k9c1-tar.17.11.0.155.tar flash:
```

c) バージョン 17.11 CAPWAP CCO イメージをダウンロードします。

```
Download 17.11 CAPWAP CCO image:
```

```
IR1800#copy tftp://<TFTP IP>/ap1g8-k9w8-tar.153-3.JPP.tar flash:
```

ステップ 3 IR1800 を TFTP サーバーとして設定します。

```
IR1800(config)#tftp-server bootflash:ap1g8t-k9c1-tar.17.11.0.155.tar
```

```
IR1800(config)#tftp-server bootflash:ap1g8-k9w8-tar.153-3.JPP.tar
```

17.9 から CAPWAP 17.11 へのアップグレード



ヒント 長いコマンド文字列を入力しているときに、さまざまなコンソールメッセージが表示されると、どこまで作業したか分からなくなりがちです。**logging console disable** コマンドを使用し、メッセージの表示を停止できます。

手順

ステップ 1 AP_WIFI6 シェルに移動します。コンソールか SSH を使用して IR1800 にログインした後、**hw-module session 0/3** コマンドを実行して AP_WIFI6 コンソールにリダイレクトできます。次に、**Ctrl-a Ctrl-q** を発行して IR1800 に戻ります。

```
IR1800#hw-module session 0/3
```

ステップ 2 アップグレードを開始する前に、実行中のイメージが常に CAPWAP モードであることを確認します。WorkGroupBridge モードまたは EWC モードで実行している場合は、**ap-type capwap** コマンドを使用して CAPWAP モードに変換します。ap-type を変更すると、Wi-Fi モジュールがリブートします。次の例を参照してください。

a) WorkGroupBridge モード

```
AP_WIFI6#sh running-config | inc Mode
AP Mode          : WorkGroupBridge
```

```
AP_WIFI6#ap-type capwap
```

Note: After rebooting, check the running image is CAPWAP:

```
APE8EB.349C.14F8#sh running-config | inc Mode
AP Mode          : Local
```

b) EWC モード

```
WLC#wireless ewc-ap ap shell username <username>
```

```
AP_WIFI6#ap-type capwap
```

```
AP is the Master AP, system will need a reboot when ap type is changed to CAPWAP
. Do you want to proceed? (y/N)y
```

Note: After rebooting, check the running image is CAPWAP:

```
APE8EB.349C.14F8#sh running-config | inc Mode
AP Mode          : Local (or FlexConnect)
```

ステップ 3 CAPWAP 17.11 イメージを **ap1g8-k9w8** のプライマリパーティション (パーティション 1) にアップグレードします。PING コマンドを使用してネットワークに到達可能であることを確認し、17.11 CAPWAP CCO イメージにアップグレードします。

(注)

ダウンロードとリブートには約 6 分かかります。

```
AP_WIFI6#ping <IP of IR1800 TFTP> For example:192.168.145.77
AP_WIFI6#logging console disable
AP_WIFI6#archive download-sw /reload tftp://<IP of IR1800>/ap1g8-k9w8-tar.153-3.JPP.tar
Starting download AP image tftp://<IP of IR1800 TFTP>/ap1g8-k9w8-tar.153-3.JPP.tar ...
!This may take a few minutes.
!If longer, please abort command, check network and try again.
--O-- # # # #
```

ステップ 4 続いて、CAPWAP の **ap1g8-k9w8** のバックアップパーティション (パーティション 2) をアップグレードします。

PING メッセージを使用してネットワークに到達可能であることを確認し、CLI オプション **no-reload** を使って 17.11 CAPWAP CCO イメージをアップグレードします。次に例を示します。

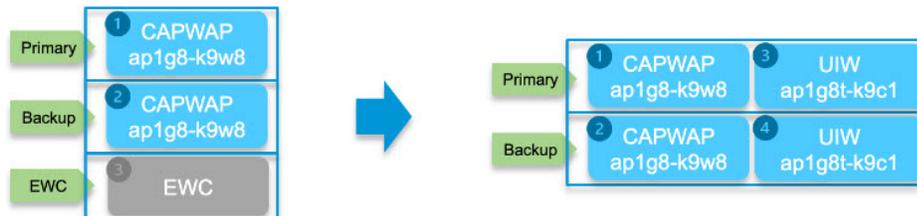
```
AP_WIFI6#ping <IP of IR1800 TFTP or Infra TFTP, for example: 192.168.145.77>
```

```
AP_WIFI6#logging console disable
```

```
AP_WIFI6#archive download-sw /no-reload tftp://<IP of IR1800 TFTP>/ap1g8-k9w8-tar.153-3.JPP.tar
```

UIW 17.11 イメージのインストール

次の手順は、プライマリ UIW パーティションとバックアップ UIW パーティション (3 と 4) のインストール手順を説明したものです。プライマリパーティションとバックアップパーティションの両方が一緒に更新されるため、ステップ 2 は 1 回だけ実行します。次の図を参照してください。



重要 ストレージが限られているため、EWC イメージは完全に削除され、EWC モードに戻すことはできません。



ヒント 長いコマンド文字列を入力しているときに、さまざまなコンソールメッセージが表示されると、どこまで作業したか分からなくなりがちです。**logging console disable** コマンドを使用して、メッセージの表示を停止できます。

手順

ステップ 1 `config boot mode wgb` コマンドを使用して、UIW イメージがすでにプログラムされているかどうかを確認します。

a) コマンドが失敗した場合、UIW イメージはプログラムされていません。ステップ 2 に進みます。

次の例は、UIW イメージがないことを示しています。

```
AP_WIFI6#sh version | inc AP
Cisco AP Software, (ap1g8),
```

```
AP_WIFI6# config boot mode wgb
Error: Unified client image missed.
```

- b) コマンドが成功した場合、UIW イメージはすでにプログラムされています。ステップ 4 に進みます。
次の例は、UIW イメージが存在することを示しています。

```
AP_WIFI6#sh version | inc AP
Cisco AP Software, (aplg8),

AP_WIFI6#config boot mode wgb
Image swapping will restore the device to factory settings.
Are you sure to proceed? (y/n) y
AP starts factory reset...
```

- ステップ 2** CAPWAP 17.11 で、**no-reload** オプションを使用して UIW 17.11 イメージをインストールします。プライマリパーティションとバックアップパーティション（3 と 4）の両方が同時に更新されます。

```
AP_WIFI6#ping <IP of IR1800 TFTP or Infra TFTP>
AP_WIFI6#logging console disable
AP_WIFI6#archive download-sw /no-reload tftp://<IP of IR1800 TFTP>/aplg8t-k9c1-tar.17.11.0.155.tar
*****
Detected field upgrading unified client image by CAPWAP image...
New image will be added into flash, but EWC will be removed.
Are you sure to proceed?(y/n) y
After the upgrade, please remember to switch the mode manually.
Press any key to continue
*****
```

(注)

手順が失敗し、ステータスが **upgrade.sh: INFO: unified client image exists, please try command: config boot mode** の場合、デバイスにすでにプログラムされた UIW イメージがあるためにアップグレードが失敗しています。ステップ 1 に戻ります。

- ステップ 3** UIW がデバイスにインストールされたら、**configure boot mode wgb** CLI を使用してイメージタイプを WGB に変更できます。変更した場合、Wi-Fi モジュールが再起動し、UIW ソフトウェアがロードされ、工場出荷時の状態へのリセットが実行されます。

```
AP_WIFI6#configure boot mode wgb
Image swapping will restore the device to factory settings.
Are you sure to proceed? (y/n) y
AP starts factory reset...
Full Factory Reset triggered: clear all files from storage..
```

- ステップ 4** [デフォルト WIM パスワード \(12 ページ\)](#) で説明したデフォルトのログイン情報でログインします。

- ステップ 5** UIW イメージタイプが **aplg8t** であることを確認します。

```
AP_WIFI6#sh version | inc AP
Cisco AP Software, (aplg8t), C6, RELEASE SOFTWARE
AP Running Image      : 17.11.0.155
```

次のタスク

WGB の基本機能を手動で設定します。詳細については、『[Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide, Cisco IOS XE Dublin 17.11.x](#)』 [英語] を参照してください。

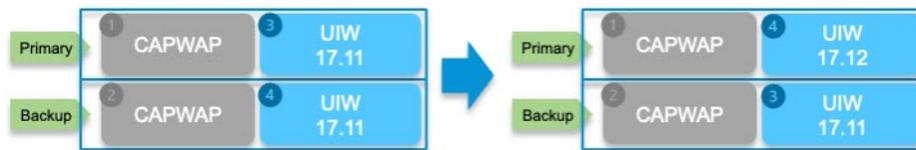
IOS XE 17.11 から IOS XE 17.12 以降への UIW イメージのアップグレード

UIW イメージをアップグレードする前に、実行中のイメージタイプも UIW (ap1g8t-k9c1) であることを確認してください。デバイスに UIW イメージが一度もインストールされておらず、IOS XE 17.11 CAPWAP イメージが実行されていない場合は、[UIW 17.11 イメージのインストール \(22 ページ\)](#) のステップ 3 からアップグレードを開始します。



(注) イメージプログラムでは、CAPWAP から CAPWAP イメージ、UIW から UIW イメージなど、同じイメージタイプのアップグレードのみが許可されます。現在のタイプと異なる場合は、アップグレードする前にイメージタイプを変更します。

プライマリ UIW イメージが新しいバージョンにアップグレードされます。次の 17.12 の例を参照してください。



手順

ステップ 1 デバイスが IOS XE リリース 17.11 UIW イメージを実行していることを確認します。

```
AP_WIFI6#sh version | inc AP
Cisco AP Software, (ap1g8t), C6, RELEASE SOFTWARE
AP Running Image      : 17.11.0.155
```

ステップ 2 IR1800 でローカルに TFTP サーバーを設定します。[17.11 UIW および CAPWAP イメージのホストルータへのダウンロード \(20 ページ\)](#) を参照してください。次に、AP_WIFI6 に静的 IP アドレスを設定します。

```
AP_WIFI6#config ssid default ssid default auth open
AP_WIFI6#config dot11 1 mode wgb ssid default
AP_WIFI6#configure ap address ipv4 static <ip> <netmask> <gateway>
AP_WIFI6#reload
```

ステップ 3 新しい UIW イメージは、**archive** コマンドを使用して古い UIW イメージを直接アップグレードできます。これにより、パーティション 4 のイメージが置き換えられ、プライマリになります。

```
AP_WIFI6#ping <IP of IR1800 TFTP or Infra TFTP> For example 192.168.145.77  
AP_WIFI6#archive download-sw /no-reload tftp://<IP of TFTP>/ap1g8t-k9c1-tar.17.12.1.5.tar
```

重要

archive コマンドを使用すると、任意の UIW イメージから別の UIW イメージにアップグレードできます。バージョンチェックはありません。

イメージのダウングレード

WIM の WGB モードと新たな WGB 機能は、CAPWAP イメージ (ap1g8-k9w8) から UIW イメージ (ap1g8t-k9c1) に移行され、その後サポートされます。



重要 17.10 以前へのダウングレードはサポートされません。



第 4 章

モード間の変換

この章は、次の項で構成されています。

- [Wi-Fi モードの変換 \(27 ページ\)](#)
- [変換を始める前に \(28 ページ\)](#)
- [IOS XE 17.11.1 より前の Wi-Fi モードの変換 \(29 ページ\)](#)
- [IOS XE 17.11.1 以降での Wi-Fi モードの変換 \(32 ページ\)](#)

Wi-Fi モードの変換

シスコに Wi-Fi プラガブルモジュールをご注文いただいた場合、CAPWAP、EWC、および WGB モードを現在 Cisco Commerce Workspace (CCW) で選択できます。希望する展開モードを考慮した上で、それに応じたソフトウェアタイプがインストールされたモジュールをご注文いただくのが一番便利な方法です。

このセクションで説明する手順に従うことで別のモードに変換できますが、一部サポートされないモード変換もありますのでご注意ください。

モジュールのファームウェアのアップグレードと Wi-Fi モードの変換は、IOS XE 17.11.1 以降を実行しているか、17.11.1 より前の IOS XE バージョンを実行しているかによって異なります。ここでは、その両方のシナリオについて説明します。

変換プロセスを開始する前に、実行している WIM イメージのタイプ、バージョン、およびモードを把握しておくことが重要です。次の表を参照してください。

イメージ	サポートされるモード
EWC イメージ (C9800-AP-iosxe-wlc.bin)	EWC モードをサポート
UIW イメージ (ap1g8t-k9c1-tar)	17.11 より WGB モードをサポート
CAPWAP イメージ (ap1g8-k9w8-tar)	17.11 以降の CAPWAP モードのみをサポート
CAPWAP イメージ (ap1g8-k8w8-tar)	CAPWAP をサポート WGB モードをサポート (17.10 まで)

変換を始める前に

変換を適切に実行するには、変換を実行する前に、次の手順に従って現在の WIM イメージのタイプ、バージョン、およびモードを確認します。[Wi-Fi モードの変換 \(27 ページ\)](#) の表を参照してください。

手順

ステップ 1 ルータコンソールを介した WIM との接続 (11 ページ)、ログインし、**Enable** と入力して、設定されたユーザー名とパスワードまたはデフォルトパスワードを使用して特権 EXEC モードに移行します。

(注)

EWC 内部アクセスポイントの場合、プライマリ AP CLI を使用するには、コントローラのプロンプトで **wireless ewc-ap ap shell username [AP-username]** と入力し、内部アクセスポイントシェルにログインします。

ステップ 2 [WIM イメージタイプの決定 \(13 ページ\)](#) で説明されているコマンドを使用して、WIM の現在のイメージタイプを取得します。イメージタイプは、CAPWAP、UIW、および EWC-AP のいずれかである必要があります。

ステップ 3 次のように、イメージタイプに応じた CLI を使用して、WIM の現在のバージョンを確認します。

- a) イメージタイプが CAPWAP および UIW の場合は、WIM で **show version | inc Running** コマンドを使用してバージョンを取得します。

```
AP#show version | inc Running
AP Running Image      : 17.11.0.100  <-version number 17.11
```

- b) イメージタイプが EWC-AP の場合は、WIM で **show version | inc Cisco IOS XE Software** コマンドを使用してバージョンを取得します。

```
AP#show version | inc Cisco IOS XE Software
Cisco IOS XE Software, Version BLD_V179_xxxx.  <-version number:17.9
```

ステップ 4 WIM で **show running-config | inc AP** コマンドを使用してモードを確認します。

- a) WGB モードの場合、**AP Mode : WorkGroupBridge** が出力に表示されます。

```
APE8EB.349C.1510#show running config | inc AP
AP Name      : APBCE7.120C.D850
AP Mode      : WorkGroupBridge
```

- b) CAPWAP AP モードの場合、**Local** または **FlexConnect** が出力に表示されます。

```
APBCE7.120C.D658#show running-config | inc AP
AP Name      : APBCE7.120C.D658
AP Mode      : FlexConnect
```



- (注) 上記の手順を使用してソフトウェアのバージョンとモードを確認したら、次の対応する変換の項に進めます。

iOS XE 17.11.1 より前の Wi-Fi モードの変換

この項の内容は、次のとおりです。

- [CAPWAP モードから EWC モードへの変換 \(29 ページ\)](#)
- [CAPWAP モードから WGB モードへの変換 \(30 ページ\)](#)
- [WGB モードから CAPWAP モードへの変換 \(31 ページ\)](#)
- [EWC モードから CAPWAP モードへの変換 \(31 ページ\)](#)

CAPWAP モードから EWC モードへの変換

この変換は、CAPWAP イメージを含む WIM があり、その WIM を Embedded Wireless Controller ベースのネットワークに展開する場合に必要です。これを行うには、CAPWAP AP を Embedded Wireless Controller に変換する必要があります。

CAPWAP イメージを含む WIM を Embedded Wireless Controller 対応イメージに変換するには、次の変換手順に従ってコントローライメージをダウンロードします。詳細については、[EWC ホワイトペーパーの「変換」の項](#)を参照してください。

CAPWAP モードから EWC モードへの変換手順

手順

- ステップ 1** ルータコンソールを介した WIM との接続 ([11 ページ](#))、ログインし、**Enable** と入力して、設定された CAPWAP AP のユーザー名とパスワードを使用して特権 EXEC モードに移行するか、[デフォルト WIM パスワード \(12 ページ\)](#) を使用します。
- ステップ 2** `show version | include AP` コマンドを使用して、EWC イメージがすでに WIM にプログラムされているかどうかを確認します。

EWC イメージがプログラムされている場合は、次の出力が表示されます。

```
APE8EB.349C.1510#show version | include AP
Cisco AP Software, (aplg8),
APE8EB.349C.1510 uptime is 1 days, 13 hours, 07 minutes
AP Running Image      : 17.13.0.98
AP Image type        : EWC-AP IMAGE
```

EWC イメージが存在しない場合は、次の出力が表示されます。

```
APBCE7.120C.DAD8# show version | include AP
AP Image type      : EWC-AP IMAGE
AP Configuration  : NOT ME OR EWC-AP CAPABLE
APBCE7.120C.DAD8#
```

(注)

イメージが存在しない場合は、次のサブステップに従って、イメージを IR1800 bootflash: またはリモート TFTP サーバーにコピーします。

- a) EWC イメージファイルをダウンロードして解凍します。
- b) 必要なイメージ (**C9800-AP-iosxe-wlc.bin**) とそれぞれの AP イメージ (**ap1g8**) をリモート TFTP サーバーにコピーします。
- c) または、IR1800 をローカル TFTP サーバーとして使用する場合は、IR1800 で次の追加コマンドを実行します。

次の例を使用して、EWC および AP イメージファイルを IR1800 bootflash: にコピーします。

```
IR1800#copy tftp://<TFTP IP>/C9800-AP-iosxe-wlc.bin flash:
IR1800#copy tftp://<TFTP IP>/ap1g8 flash:
```

IR1800 で TFTP サーバーを設定します。たとえば、VLAN100 インターフェイスに接続されている AP などです。

```
IR1800# config term
ip tftp source-interface Vlan100
tftp-server bootflash:C9800-AP-iosxe-wlc.bin tftp-server bootflash:ap1g8
```

ステップ3 変換プロセスを開始します。

- a) WIM で AP イメージが使用可能な場合は、次の手順を実行します。

```
AP# ap-type ewc-ap tftp://<image>
```

- b) show version の出力を確認しても AP イメージが表示されない場合、それは、その AP が CAPWAP イメージで動作していることを意味します。変換を行うには、次のコマンドを実行します。**ap-typeEWC tftp://<TFTP Server IP>/ap1g8 tftp://<TFTP Server IP>/C9800-AP-iosxe-wlc.bin**。次に例を示します。

```
AP-console#ap-type ewc-ap tftp://192.168.72.11/ap1g8 tftp://192.168.72.11/C9800-AP-iosxe-wlc.bin
Starting download eWLC image tftp://192.168.72.11/C9800-AP-iosxe-wlc.bin
It may take a few minutes. If longer, please abort command, check network and try again.
```

```
##### 100.0%
```

APが再起動したら、新しいモードの設定を実行する必要があります。「[Cisco Embedded Wireless Controller \(EWC\)](#)」の項を参照してください。

CAPWAP モードから WGB モードへの変換

ワークグループブリッジ (WGB) モードへの変換では、アクセスポイントは、別のアクセスポイントにクライアントとしてアソシエートされ、イーサネットポートに接続されたデバイスにネットワーク接続を提供します。

CAPWAP から WGB モードへの変換

次の手順を実行します。

1. ルータコンソールを介した [WIM との接続](#) (11 ページ)、ログインし、**Enable** と入力して、設定された CAPWAP AP のユーザー名とパスワードを使用して特権 EXEC モードに移行するか、[デフォルト WIM パスワード](#) (12 ページ) を使用します。
2. 次のコマンドを使用して、WIM で CAPWAP AP を WGB モードに変換します。

```
APBCE7.120C.DAA8#ap-type workgroup-bridge
WGB is a wireless client that serve as nonroot ap for wired clients.
AP is the Master/CAPWAP AP, system will need a reboot when ap type is changed to
WGB. Do you want to proceed? (y/N): y
```
3. AP が再起動したら、新しいモードの設定を実行する必要があります。[ワークグループブリッジ \(WGB\)](#) を参照してください。

WGB モードから CAPWAP モードへの変換

この変換は、WIM をワークグループブリッジモードから Embedded Wireless Controller ネットワーク以外のネットワークに移行する場合、または AP をプライマリ AP 選定プロセスの対象外にする場合に必要です。

WGB モードから CAPWAP モードへの変換手順

1. ルータコンソールを介した [WIM との接続](#) (11 ページ)、ログインし、**Enable** と入力して、設定された CAPWAP AP のユーザー名とパスワードを使用して特権 EXEC モードに移行するか、[デフォルト WIM パスワード](#) (12 ページ) を使用します。
2. **ap-type capwap** コマンドを使用して、WIM で CAPWAP AP を WGB モードに変換します。次の例を参照してください。

```
APBCE7.120C.DAA8#ap-type capwap
AP serving in WGB mode, system will reboot when ap type is changed to CAPWAP. Do you
want to proceed? (y/N): y
```
3. WGB が再起動し、WGB の設定がクリアされます。AP が起動し、CAPWAP 接続プロセスが開始されます。

EWC モードから CAPWAP モードへの変換

Embedded Wireless Controller (EWC) 対応アクセスポイントをアプライアンスまたは vWLC ベースの環境に移行する場合、次の手順に従い、CLI を使って WIM で変換を実行します。

その他の変換ワークフローと詳細な手順については、[EWC ホワイトペーパーの「変換」の項](#)を参照してください。

EWC モードから CAPWAP モードへの変換手順

手順

- ステップ 1** ルータコンソールを介した WIM との接続 (11 ページ)、ログインし、**Enable** と入力して、設定された CAPWAP AP のユーザー名とパスワードを使用して特権 EXEC モードに移行するか、**デフォルト WIM パスワード** (12 ページ) を使用します。
- ステップ 2** 内部 AP CLI を使用するには、コントローラのプロンプトで **wireless ewc-ap ap shell username [AP-username]** と入力し、内部アクセスポイントシェルにログインします。
- ステップ 3** **ap-type capwap** コマンドを実行します。これにより、AP がリロードされ、AP と EWC パーティションの両方が完全に工場出荷時の状態にリセットされ、アクセスポイントはプライマリ選定プロセスの対象外となります。次の例を参照してください。

```
WLC#wireless ewc-ap ap shell username Cisco
The authenticity of host '192.168.129.1 (192.168.129.1)' can't be established.
ECDSA key fingerprint is SHA256:xxxxxxx
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.129.1' (ECDSA) to the list of known hosts.
Cisco@192.168.129.1's password:

AP#ap-type capwap
APBCE7.120C.D760#ap-type capwap
AP is the Master AP, system will need a reboot when ap type is changed to CAPWAP.
Do you want to proceed? (y/N) Y
```

IOS XE 17.11.1 以降での Wi-Fi モードの変換

IOS XE 17.11.1 以降、UIW イメージの導入により、WP-WIFI6 モジュールの WGB モードのサポートが強化され、対応するモード変換で新しい CLI が使用されるようになりました。

モジュールは、現在のイメージバンドルに基づいて、次の 2 つの固有の変換シナリオをサポートします。

- プログラムされた UIW イメージを使用しない EWC と CAPWAP AP モード間の変換
- プログラムされた UIW イメージを使用した CAPWAP AP モードと WGB モード間の変換

WP-WIFI6 モジュールに UIW イメージがプログラムされている場合、EWC モードに変換できなくなります。

AP モードと EWC モード間の変換

WP-WIFI6 モジュールが UIW イメージでプログラムされているかどうかを確認するには、**WIM イメージタイプの決定** (13 ページ) の項を参照してください。



- (注) AP モードと EWC モード間の変換は、事前インストール済みの EWC+CAPWAP イメージバンドルでのみ許可されます。

以前に WIM に UIW イメージがプログラムされていない場合は、同じ手順に従って EWC モードと AP モードを切り替えます。

- [CAPWAP モードから EWC モードへの変換](#)
- [EWC モードから CAPWAP モードへの変換](#)

CAPWAP モードから WGB モードへの変換

この変換は、IOS XE 17.11 以降で、CAPWAP AP モードからワークグループブリッジモードに変換する場合に必要です。まず、[UIW 17.11 イメージのインストール \(22 ページ\)](#) の手順に従ってください。

WP-WIFI6 モジュールコンソールで **config boot mode wgb** コマンドを使用します。

変換の手順

1. ルータコンソールを介した [WIM との接続 \(11 ページ\)](#)、ログインし、**Enable** と入力して、設定された CAPWAP AP のユーザー名とパスワードを使用して特権 EXEC モードに移行するか、[デフォルト WIM パスワード \(12 ページ\)](#) を使用します。
2. **config boot mode wgb** コマンドを使用して、WIM で CAPWAP AP を WGB モードに変換します。次の例を参照してください。

```
AP_WIFI6# config boot mode wgb
Image swapping will restore the device to factory settings.
Are you sure to proceed? (y/n) y
AP starts factory reset...
```

3. AP が再起動したら、新しいモードの設定を実行する必要があります。「[ワークグループブリッジ \(WGB\)](#)」の項を参照してください。

WGB モードから CAPWAP モードへの変換

この変換は、AP をワークグループブリッジモードからワイヤレスコントローラネットワークに移行する場合に必要です。

変換の手順

1. ルータコンソールを介した [WIM との接続 \(11 ページ\)](#)、ログインし、**Enable** と入力して、設定された CAPWAP AP のユーザー名とパスワードを使用して特権 EXEC モードに移行するか、[デフォルト WIM パスワード \(12 ページ\)](#) を使用します。

2. **config boot mode capwap** コマンドを使用して、WIM で CAPWAP AP を WGB モードに変換します。次の例を参照してください。

```
AP_WIFI6# config boot mode capwap
Image swapping will restore the device to factory settings.
Are you sure to proceed? (y/n) y
AP starts factory reset...
```

3. WGB が再起動し、WGB の設定がクリアされます。AP が起動し、CAPWAP 接続プロセスが開始されます。



第 5 章

WIM の一般的な展開モード

この章は、次の項で構成されています。

- 一般的な導入シナリオ (35 ページ)
- Control And Provisioning of Wireless Access Points (CAPWAP) (36 ページ)
- ワークグループブリッジ (WGB) (38 ページ)
- uWGB または WGB アップリンクとルート AP モードの無線機の同時使用 (44 ページ)
- Cisco Embedded Wireless Controller (EWC) (61 ページ)

一般的な導入シナリオ

ここでは、WIM の展開に関する一般的なシナリオをいくつか説明します。

ワイヤレスインターフェイス モジュールは、機能面で [Cisco Catalyst シリーズ 9105AXI アクセスポイント](#) とよく似ています。

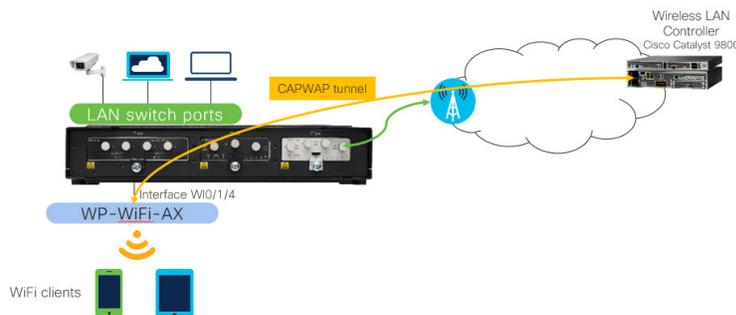
ホストルータのワイヤレス挿入モジュールとして、ワイヤレスアクセスポイント (CAPWAP APモード) として機能する WIM モジュールのプロビジョニングをサポートできます。これにより、ルータは Wi-Fi ワイヤレスクライアントにネットワークアクセスを提供でき、同時に中央ワイヤレスコントローラによって AP 機能を管理できます。AP 機能を管理するための中央ワイヤレスコントローラを展開しない場合は、EWC モードで WIM を展開できます。この場合、ホストルータはワイヤレスクライアントにネットワークアクセスを提供でき、同時にローカル EWC コントローラによって AP 機能を管理できます。

WGB モードで動作するように WIM をプロビジョニングすると、ホストルータの設定により、Wi-Fi ワイヤレス接続をバックホールリンク候補として使用できます。17.11.1 UIW ソフトウェアの機能拡張により、ホストルータは 1 つの無線機を WGB バックホール用に、もう 1 つの無線機をワイヤレス クライアント アクセス用に使用できるようになります。

Control And Provisioning of Wireless Access Points (CAPWAP)

アクセスポイントでは、コントローラとネットワーク上のその他のワイヤレスアクセスポイント間の通信に、標準の Control and Provisioning of Wireless Access Points Protocol (CAPWAP) を使用します。アクセスポイントの役割を果たす WP-WIFI6 は、有線 LAN に直接接続され、無線ユーザーへの接続ポイントとして機能します。

CAPWAP モードに使用されるイメージは ap1g8-k9w8 です。



IR1800 で CAPWAP アクセスポイント構成を設定するための前提条件

アクセスポイントをネットワークでアクティブにするには、コントローラがそのアクセスポイントを検出する必要があります。CAPWAP はレイヤ 2 をサポートしていません。アクセスポイントでは、レイヤ 3、DHCP、DNS、または IP サブネットのブロードキャストを使用して IP アドレスを取得し、コントローラを検出する必要があります。

ここでは、WIM CAPWAP AP がコントローラと通信するための、DHCP サーバーとルータの SVI インターフェイスの基本設定を示します。追加の NAT、ドメインネームシステム (DNS)、およびその他のルーティング設定の変更については、[IR1800 設定ガイド \[英語\]](#) を参照してください。



(注) AP がすでに CAPWAP モードになっている場合、AP はリブートしません。AP が EWC または WGB モードの場合、モードが CAPWAP に変更されてから AP がリブートします。

IR1800 での CAPWAP アクセスポイント構成設定手順

次のステップを実行します。

ステップ	コマンドまたはアクション	目的
ステップ 1	<p>ip dhcp pool name</p> <p>network ip address subnet mask</p> <p>default-router ip address</p> <p>dns-server ip address</p> <p>option 43 hex <value></p> <p>例 :</p> <pre>Router(config)#ip dhcp pool wireless Router(dhcp-config)#network 10.10.10.0 255.255.255.0 Router(dhcp-config)#default-router 10.10.10.1 Router(dhcp-config)#dns-server 192.0.2.1 Router(dhcp-config)#option 43 hex f108c0a80a05c0a80a14</pre>	<p>スイッチ仮想インターフェイス (SVI) に使用される IP アドレスの DHCP サーバーアドレスプールを作成します。ステップ 4 を参照してください。</p> <p>プールのデフォルトゲートウェイとドメインネームシステム (DNS) サーバーアドレスを割り当てます。</p>
ステップ 2	<p>interface GigabitEthernet slot/subslot/port</p> <p>ip address dhcp</p> <p>ip nat outside</p> <p>例 :</p> <pre>Router(config)#interface GigabitEthernet 0/0/0 Router(config-if)#ip address dhcp Router(config-if)#ip nat outside</pre>	<p>ルータのアップリンク WAN ポートの IP アドレスを設定し、NAT コマンドを使用してインターフェイスを外部ネットワークに接続します。</p>
ステップ 3	<p>interface Wlan-GigabitEthernet slot/subslot/port</p> <p>switchport mode trunk</p> <p>switchport trunk native vlan number</p> <p>例 :</p> <pre>Router(config)#interface Wlan-GigabitEthernet 0/1/4 Router(config-if)#switchport mode trunk Router(config-if)#switchport trunk native vlan 10</pre>	<p>WIM 内部スイッチインターフェイスのスイッチポートモードとネイティブ VLAN を設定します。ネイティブ VLAN は AP 管理 VLAN である必要があります。</p>
ステップ 4	<p>interface vlan number</p> <p>description <name></p> <p>ip address ip-address subnet_mask</p> <p>ip nat inside</p> <p>例 :</p> <pre>Router(config)#interface vlan 10 Router(config-if)#description Wireless Router(config-if)#ip address 10.10.10.1 255.255.255.0 Router(config)#ip nat inside</pre>	<p>スイッチ仮想インターフェイス (SVI) を作成し、DHCP プールから IP アドレスを割り当て、インターフェイスを内部ネットワークに接続します。</p>

ステップ	コマンドまたはアクション	目的
ステップ 5	ip route 10.10.10.10 10.10.10.10 default gateway ip-address 例 : Router(config)# ip route 10.10.10.10 10.10.10.10 192.0.2.1	すべてのトラフィックをルータのデフォルトゲートウェイに転送します。
ステップ 6	ip nat inside source list number interface GigabitEthernet slot/subslot/port overload ip access-list standard number number permit ip address wildcard mask 例 : Router(config)# ip nat inside source list 10 interface GigabitEthernet 0/0/0 overload Router(config)# ip access-list standard 10 Router(config)# 10 permit 10.10.10.0 0.0.0.255	アクセスリストを指定して、動的送信元変換を確立します。 トラフィックを許可または拒否する ACL を作成します。

アクセスポイントの設定と配置

ワイヤレス インターフェイス モジュールが CAPWAP モードで実行されている場合、モジュールに IP アドレスが設定されると、Cisco 9800 シリーズなどの WLC を介して通信し、管理されます。設定プロセスは、コントローラで行います。

CAPWAP とシスコ ワイヤレス LAN の詳細については、次の資料を参照してください。

- [Configure DHCP OPTION 43 for Lightweight Access Points Guide \[英語\]](#)
- [Cisco Catalyst 9800 Series Configuration Best Practices](#)
- [Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide, Cisco IOS XE Bengaluru 17.6.x \[英語\]](#)

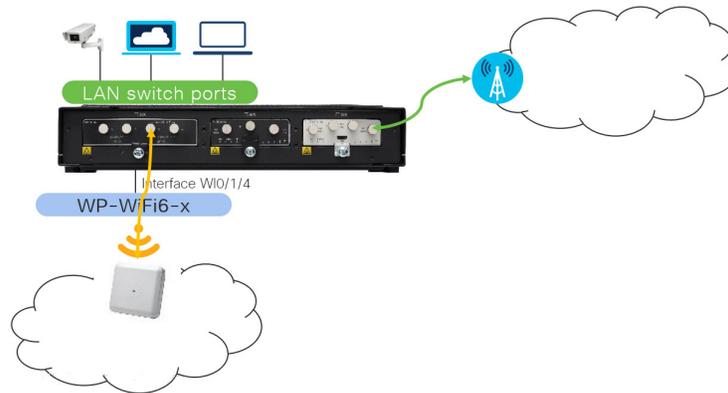
ワークグループブリッジ (WGB)

ワークグループブリッジ (WGB) のシナリオでは、次のことが可能になります。

- 低コスト、高速 Wi-Fi アップリンク
- 1 つの無線機のみで uWGB または WGB モードでの動作が許可される
- WGB は最大 20 の有線クライアントをサポート
- uWGB は単一のクライアント MAC アドレスをサポート (W10/1/4 が、バックホールリンクである Wi-Fi のルーテッドインターフェイスである設定における、VLAN10 インターフェイスなど)



重要 IR1800 の WGB モードは、固定型の展開でのみ推奨されます。



ワークグループブリッジモードは、インフラストラクチャ Wi-Fi を介したデータオフロードに使用される特殊なモードです。このモードで実行中の WIM は、ワイヤレスステーションのように動作します。通常、（ギガビットポートを介して WIM に接続されている）有線クライアントをワイヤレスインフラストラクチャにブリッジするために使用されます。

このモードを使用するシナリオの例として、IR1800 の有線イーサネットポートに接続されているカメラやその他のデバイスに Wi-Fi バックホールを提供する場合があります。WGB モードは、ワイヤレスインフラストラクチャがシスコ製であることが前提条件となりますので、ご注意ください。

Cisco IOS-XE リリース 17.8.1 以降、WIM でユニバーサル WGB モードがサポートされます。

ユニバーサル WGB (uWGB) は、uWGB に接続された有線クライアントとシスコおよびシスコ以外のワイヤレスネットワークを含むワイヤレスインフラストラクチャとの間のワイヤレスブリッジとして機能する WGB 機能の補完モードです。

WGB および uWGB の設定の詳細については、次を参照してください。

[Cisco Wave 2 Access Points as Workgroup Bridges \[英語\]](#)

[Cisco Industrial Wireless Workgroup Bridge and Universal WGB Deployment Guide \[英語\]](#)

IR1800 で WGB を設定するための前提条件

ここでは、有線クライアントとインフラストラクチャ Wi-Fi トラフィックをブリッジする IR1800 の基本設定を示します。NAT、ACL、およびその他特定の設定については、[IR1800 設定ガイド \[英語\]](#) を参照してください。

ステップ	コマンドまたはアクション	目的
ステップ 1	vlan number-number 例 : <pre>Router (config) #vlan 2001-2002</pre>	さまざまな有線クライアントトラフィック用 VLAN として固有の VLAN を作成します。 有線クライアントプリンタ用の VLAN 2001。 ビデオカメラ用の VLAN 2002。
ステップ 2	interface Wlan-GigabitEthernet slot/subslot/port switchport mode trunk switchport trunk allowed vlan number 例 : <pre>Router (config) #interface Wlan-GigabitEthernet 0/1/4 Router (config-if) #switchport mode trunk Router (config-if) #switchport trunk allowed vlan 2001-2002</pre>	Wlan-GigabitEthernet コマンドを使用して、内部スイッチインターフェイスの Wi-Fi カードを接続します。スイッチポートモードと、許可された有線クライアントトラフィック VLAN パススルーを設定します。
ステップ 3	interface GigabitEthernet slot/subslot/port description name switchport mode trunk switchport trunk native vlan number interface GigabitEthernet slot/subslot/port description name switchport mode access switchport access vlan number 例 : <pre>Router (config) #interface GigabitEthernet 0/1/0 Router (config-if) #description Printer Router (config-if) #switchport mode trunk Router (config-if) #switchport trunk native vlan 2001 Router (config) #interface GigabitEthernet 0/1/1 Router (config-if) #description Camera Router (config-if) #switchport mode access Router (config-if) #switchport access vlan 2002</pre>	有線クライアント接続ポートごとにスイッチポートモードと VLAN を設定します。

WGB の設定と展開

ここでは、WP-WIFI6 モジュールに必要な最低限の WGB CLI 設定を示します。[モード間の変換 \(27 ページ\)](#) のガイダンスに従って、まず WP-WIFI6 モジュールを WGB で起動します。WGB の詳細な設定については、『[Cisco Industrial Wireless Workgroup Bridge and Universal WGB Deployment Guide](#)』 [英語] を参照してください。

手順

ステップ1 SSID プロファイルを設定します。

例：

```
WIM-WGB# configure ssid-profile Test ssid Free authentication psk cisco12345 key-management wpa2
```

ステップ2 無線インターフェイスを WGB モードに設定し、SSID プロファイルをマッピングします。ワイヤレスインフラストラクチャにより規定された認証を選択します。

例：

```
WIM-WGB# configure dot11Radio 1 mode wgb ssid-profile Test
WIM-WGB# configure dot11Radio 1 encryption mode ciphers aes-ccm
WIM-WGB# configure dot11Radio 1 enable
```

ステップ3 未使用の無線機をルート AP として設定し、オフにします。本稿執筆時点では、WGB は単一の無線機を使用します。

例：

```
WIM-WGB# configure dot11Radio 0 mode root-ap
WIM-WGB# configure dot11Radio 0 disable
WIM-WGB# configure wgb antenna band mode single
```

ステップ4 WIM で **show configuration** を使用して、WGB の基本設定を確認します。

例：

```
WIM-WGB# show configuration
AP Name : WIM-WGB
AP Mode : WorkGroupBridge
SSH State : Enabled
AP Username : Ciscot
Syslog Host : 0.0.0.0
```

```
Radio and WLAN-Profile mapping:-
```

```
=====
Radio ID Radio Mode SSID-Profile SSID Authentication
-----
1 WGB Test Free PSK
```

```
Radio configurations:-
```

```
=====
Radio Id : 0
Admin state : DISABLED
Mode : RootAP
Radio Id : 1
Admin state : ENABLED
Mode : WGB
```

```
WGB specific configuration:-
```

```
=====
WGB Radio Id : 1
Mode State : Enable
SSID Profile : Test
```

```
Antenna Band Mode : Single
```

ステップ 5 WIM で `show wgb dot11 associations` コマンドを使用して、WGB アソシエーションの **Uplink State** と **RSSI** を確認します。

例：

```
WIM-WGB# show wgb dot11 associations

Uplink Radio ID : 1
Uplink Radio MAC : BC:E7:12:0C:FF:6F
SSID Name : Free
Connected Duration : 0 hours, 0 minutes, 5 seconds
Parent AP Name : AP60E6.F0D4.4E34
Parent AP MAC : 60:E6:F0:D4:4A:6A
Uplink State : CONNECTED
Auth Type : PSK
Key management Type : WPA2
Dot11 type : 11ax
Channel : 124
Bandwidth : 40 MHz
Current Datarate : 6 Mbps
Max Datarate : 573 Mbps
RSSI : 40
IP : 192.168.56.107/24
Default Gateway : 192.168.56.1
DNS Server1 : 192.168.71.2
Domain : iottest.local
IPV6 : ::/128
Assoc timeout : 5000 Msec
Auth timeout : 5000 Msec
Dhcp timeout : 60 Sec
Country-code : US
```

ステップ 6 WIM で `show wgb bridge` コマンドを使用して、ブリッジテーブルから WGB の **wired client mac**、**IP**、**vlan id** を確認します。

例：

```
WIM-WGB# show wgb bridge
***Client ip table entries***
mac vap port vlan_id seen_ip confirm_ago fast_brg
60:E6:F0:D4:4A:6A 0 wbridg1 0 0.0.0.0 24.082000 true
E4:62:C4:49:96:F4 0 wired0 2256 192.168.56.108 6.668000 true
```

uWGB の設定と展開

ここでは、WP-WIFI6 モジュールに必要な最低限の uWGB 設定を示します。[モード間の変換 \(27 ページ\)](#) に記載されている手順に従って、まず WP-WIFI6 モジュールを WGB で起動します。uWGB の詳細な設定については、『[Cisco Industrial Wireless Workgroup Bridge and Universal WGB Deployment Guide](#)』[英語] を参照してください。

0/3 へのセッションを開始したら、`show configuration` を確認します。次の内容を参照してください。

- 2.4GHz 無線機 (dot11 radio 0) がオフになっている
- 5GHz 無線機 (dot11 radio 1) がサードパーティの AP に接続するように設定されている



(注) 2.4GHz または 5GHz のいずれかを uWGB モードに設定できます。

次に、サードパーティアプリケーションに接続するための uWGB 設定手順の概要を示します。

手順

ステップ 1 SSID プロファイルを設定します。

例：

```
configure ssid-profile Test ssid Free authentication psk cisco12345 key-management wpa2
```

ステップ 2 無線インターフェイスを uWGB モードに設定し、SSID プロファイルをマッピングします。ワイヤレス インフラストラクチャにより規定された認証を選択します。次の例では、c44d.849b.0a8c は、インフラからアドレスを取得する uWGB 有線クライアントデバイスの MAC アドレスです。

例：

```
configure dot11radio 1 mode uwgb c44d.849b.0a8c ssid-profile Test
configure dot11radio 1 encryption mode ciphers aes-ccm
configure dot11radio 1 enable
```

ステップ 3 未使用の無線機をルート AP として設定し、オフにします。本稿執筆時点では、uWGB は単一の無線機を使用します。

例：

```
configure dot11radio 0 mode root-ap
configure dot11radio 0 disable
```

uWGB 設定例

次に、uWGB の設定例を示します。

```
APBCE7.120C.DAA8#show config
AP Name           : APBCE7.120C.DAA8
AP Mode           : WorkGroupBridge
CDP State         : Enabled
Watchdog monitoring : Enabled
SSH State         : Disabled
AP Username       : Cisco
Session Timeout   : 300
```

Radio and WLAN-Profile mapping:

```
=====
Radio ID   Radio Mode   SSID-Profile   SSID   Authentication
1          UWGB           Test           Free   PSK
```

Radio Configuration:

```
Radio Id       : 0
Admin state    : DISABLED
Mode           : RootAP
Beacon Period  : 100 mSec
```

```

Radio Id          : 1
  Admin state     : ENABLED
  Mode            : UWGB
  Uclient mac     : C44D.849B.0A8C
  Current state   : WGB
  UClient timeout : 0 Sec
  Dot11 type      : 11ax
  Encryption mode : AES128

```

WGB specific configuration:

```

=====
WGB Radio Id      : NA
  Mode State      : NA
  SSID Profile    : NA
UWGB Radio Id     : 1
  Mode Enable     : Enable
  SSID Profile    : Test
  Uclient MAC Address: C44D.849B.0A8C

```

IR1800 に接続されている有線デバイスを確認します。

#show wgb bridge

```

***Client ip table entries***
mac vap          port  vlan_id  seen_ip      confirm_ago  fast_brg
10:DD:B1:CE:B2:E6  0    wired0   192.168.10.25 0.016000    true

```

アソシエーションを確認します。次の例では、uWGB ステータスを表示するためには、クライアントが接続されている必要があります。有線クライアントからまたは有線クライアントへのトラフィックがない場合は、WGB にフォールバックします。

#show wgb dot11 associations

```

Uplink Radio ID   : 1
Uplink Radio MAC  : BC:E7:12:0C:F1:CF
SSID Name         : Free
Parent AP MAC     : 08:02:8E:8D:52:9A
Uplink State      : CONNECTED
Auth Type         : PSK
Key management Type : WPA2
Uclient mac       : C4:4D:84:9B:0A:8C
Current state     : UWGB
Uclient timeout   : 60 Sec
Dot11 type        : 11ac
Channel           : 36
Bandwidth         : 80 MHz
Current Datarate  : 433 Mbps
Max Datarate      : 1200 Mbps
RSSI              : 53
IP                : 0.0.0.0
IPV6              : ::/128
Assoc timeout     : 5000 Msec
Auth timeout      : 5000 Msec
Dhcp timeout      : 60 Sec

```

uWGB または WGB アップリンクとルート AP モードの無線機の同時使用

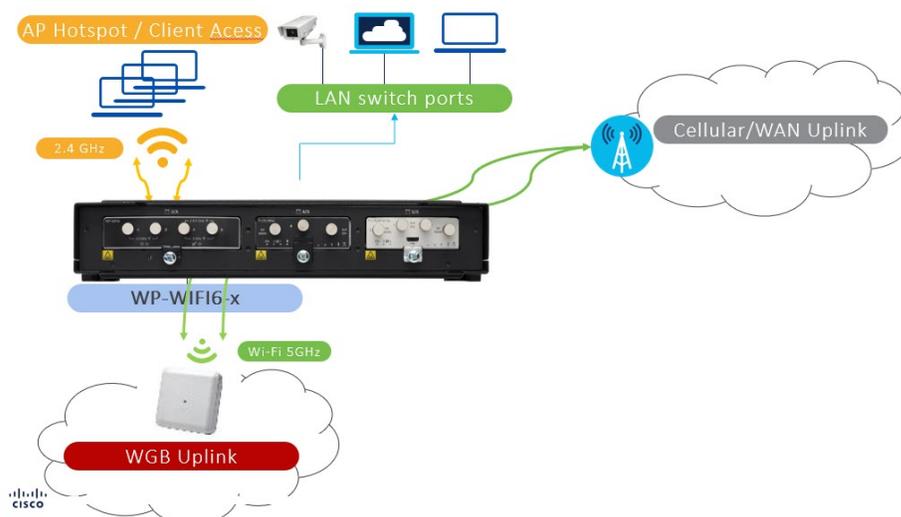
Cisco IOS XE 17.11.1 では、新たな Unified Industrial Wireless イメージ (ap1g8t-k9c1) による WGB アップリンクとルート AP モードの無線機の同時使用機能が導入されました。1 つ目の無

線機を WGB アップリンク（2.4G または 5G）に設定し、2 つ目の無線機をローカル ワイヤレス クライアント用の WGB ルート AP モード（ホットスポット Wi-Fi とも呼ばれる）に設定して個別にサービスを提供するか、両方の無線機をルート AP モードに設定できます。

17.14.1 以降、Wi-Fi モジュールは無線機の同時使用に対応し、一方の無線機は uWGB モードのアップリンクバックホールとして機能し、もう一方はルート AP 無線機として機能します。

この機能により、WLAN-VLAN マッピングが異なるワイヤレス クライアント トラフィックを内部イーサネットポートにブリッジできます。IR1800 ルータは、用途と設定に応じて、これらのワイヤレス クライアント トラフィックを異なるアップリンクにルーティングおよび転送します。

一般的な用例については、次の図を参照してください。



ルート AP 無線機（2 つ目の無線機）に接続されたワイヤレスクライアントのトラフィックフロー：

- クライアントにサービスを提供する無線機のトラフィックは、ワイヤレスバックホールに直接ブリッジされません。
- ワイヤレスクライアントのトラフィックは、内部 `gig0` を介して統合ルータにブリッジされます。
- ワイヤレスクライアントは、ルータの内部 DHCP サーバーから DHCP を介して IP アドレスを取得します。
- その後、ルータを NAT/ip ルートで設定して、それに応じてワイヤレスクライアントからインフラストラクチャネットワークにパケットをルーティングし、トラフィックを転送できます（用途による）。

無線機の同時使用が対応するシナリオとワイヤレスクライアント数の上限：

Wi-Fi モジュールの端末接続を担っている無線機に関連づけられ認証されたワイヤレスクライアントは、それらがローカルに接続されてることから、インフラのルート AP には決して更新されません。

1. シナリオ 1

- 無線機 0：WGB モードに設定中。ステータス：Disabled（アップリンク無線機が無効）
- 無線機 1：ルート AP モード。最大 100 のワイヤレスクライアントを接続可能

2. シナリオ 2

- 無線機 0：WGB モードに設定中。ステータス：Enabled（アップリンクが有効）
- 無線機 1：ルート AP モード。100 のワイヤレスクライアントをサポート

3. シナリオ 3

- 無線機 0：ルート AP モード。100 のワイヤレスクライアントをサポート
- 無線機 1：ルート AP モード。100 のワイヤレスクライアントをサポート



(注) 上記のシナリオでは、ルート AP 無線機と WGB アップリンク無線機は、要件に応じて無線機 0 または無線機 1 に設定できます。

無線機の同時使用に必要なルータ設定

ここでは、必要な設定を表示するためのコマンドの例を示します。

IR1800 でのアップリンク VLAN の設定：

アップリンク VLAN に固有の MAC 設定は、WP-WIFI6 への（および WP-WIFI6 からの）パケットのトラバース効率を高めるため、IR1800 では必須の設定です。次に、例を示します。

```
interface Vlan119          ->This is the interface that can carry the data from local
network to the infrastructure n/w.
mac-address c014.fe60.ef8d ->unique mac address configuration
ip address dhcp            ->Uplink VLAN gets ip from infra via DHCP
ip nat outside             ->This config should be done to NAT the downlink/wireless
client traffic from vlan 4094 to vlan 119
```



(注) Gig0/0/0 MAC アドレス +4 によって、固有の MAC アドレスが作られます。

アップリンクに uWGB を使用する場合は、uWGB 設定 CLI の実行時に、[wired client mac] として固有の MAC アドレスを指定する必要があります。

```
configure dot11radio <0/1> mode uwgb <c014.fe60.ef8d> ssid-profile <ssid profile name>
```

MAC アドレスを取得するには、**show int GigabitEthernet0/0/0** コマンドを使用します。

```
Router#show int GigabitEthernet0/0/0
GigabitEthernet0/0/0 is administratively down, line protocol is down
  Hardware is IR1821-1x1GE, address is c014.fe60.ef80 (bia c014.fe60.ef80)
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive not supported
  Full Duplex, 1000Mbps, link type is auto, media type is Auto Select
  output flow-control is unsupported, input flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 no buffer
    Received 0 broadcasts (0 IP multicasts)
    0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
    0 watchdog, 0 multicast, 0 pause input
    0 packets output, 0 bytes, 0 underruns
    Output 0 broadcasts (0 IP multicasts)
    0 output errors, 0 collisions, 0 interface resets
    0 unknown protocol drops
    0 babbles, 0 late collision, 0 deferred
    0 lost carrier, 0 no carrier, 0 pause output
    0 output buffer failures, 0 output buffers swapped out
Router#
```

次に、WGB ブリッジテーブルの出力例を示します。

```
AP84EB.EF55.1438#sh wgb bridge
***Client ip table entries***
mac vap          port  vlan_id  seen_ip          confirm_ago      fast_brg
A0:E7:0B:D5:99:95 12    apr0v12  4094 192.168.94.13  158.708000      true
76:68:82:01:86:C9 13    apr0v13  4094 192.168.94.2   0.000000        true
C0:14:FE:60:EF:8D 0     wired0   0    10.119.119.229 1.814000        true
```



(注) ブリッジテーブルエントリでは、アップリンク VLAN (119) に基づく SVI/有線クライアントと、ダウンリンク VLAN に基づくワイヤレスクライアントのみが学習されます。ダウンリンク VLAN (4094) に基づく SVI アドレスは、ここでは学習されません。IR1800 に設定されたアップリンク VLAN (VLAN 119) は、ネイティブ VLAN であるため、VLAN ID 「0」として学習されます。

IR1800 でのダウンリンク VLAN の設定 :

次の例を参照してください。

```
interface Vlan4094          ->Downlink VLAN for wireless client traffic
 ip address 192.168.94.1 255.255.255.0
 ip nat inside              ->Should be provided in the local network VLAN to communicate
                             with infrastructure VLAN
```

ダウンリンク VLAN インターフェイスの DHCP プール設定 :

次の例を参照してください。

```
ip dhcp pool vlan4094 -> Downlink VLAN's are the used for wireless client (Root ap:
WLAN-VLAN mapping)
 network 192.168.94.0 255.255.255.0
 default-router 192.168.94.1
 dns-server 8.8.8.8
```

W10/1/4 ポート設定 :

次に、W10/1/4 ポートの設定例を示します。AP をルータに接続する内部 Gig0 ポートです。

```
interface Wlan-GigabitEthernet0/1/4
 switchport trunk native vlan 119
 switchport trunk allowed vlan 119,4094
 switchport mode trunk
```



-
- (注) vlan 119 は WBG アップリンク VLAN、vlan 4094 はワイヤレスクライアントのトラフィックに使用されるダウンリンク VLAN です。
-

NAT ACL の設定 :

次に、NAT ACL ルールを作成するための設定例を示します。

```
ip access-list extended NAT_ACL
 10 permit ip 192.168.94.0 0.0.0.255 any
//subnet of Downlink VLAN 4094 interface
 route-map RM_WGB_ACL permit 10 ->Used for Routing table mapping
 match ip address NAT_ACL        ->NAT list used for translation
 match interface Vlan119         ->NAT interface (infrastructure VLAN)
```

外部ネットワークと通信するためのルートマップ :

```
ip nat inside source route-map RM_WGB_ACL interface Vlan119 overload
```



-
- (注) その他のルータトポロジのシナリオについては、『[Cisco Connected Mass Transit System Implementation Guide \(Cisco Validated Design\)](#)』を参照してください。
-

無線インターフェイスの WGB/uWGB モードおよびルート AP モードへの設定

ワイヤレスクライアントのサポートには、さまざまな項目の管理設定が必要です。この機能をサポートするには、次の CLI を使用します。

CAPWAP モードからユニファイド WGB モードに設定する

次のコマンドを使用します。

```
configure boot mode wgb
```

無線インターフェイスで WGB アップリンクまたはルート AP の SSID を設定する

次のコマンドを使用します。

```
configure ssid-profile <profile-name> ssid <ssid-name>  
authentication <auth-type> key-management <key-mgmt>
```

無線機を WGB モードに設定する

次のコマンドを使用します。

```
configure dot11Radio <0|1> mode wgb ssid-profile <ssid profile name>  
configure dot11Radio <0|1> enable
```

無線機を uWGB モードに設定する

次のコマンドを使用します。

```
configure dot11Radio<0|1>mode uwgb <client mac> ssid-profile<ssid profile name>
```



- (注) <client mac> - uWGB がアップリンクの場合、uWGB 設定 CLI の実行時に、ルータ SVI または PC 有線クライアント MAC 固有の MAC アドレスを <wired client mac> として指定できます。

アップリンクバックホールが uWGB モードの場合に同時ルート AP 無線機モードを機能させるには、CLI でルータスイッチ仮想インターフェイス (SVI) 固有の MAC アドレスを「wired client mac」として指定します。この手順により、Wi-Fi モジュールが uWGB モードに設定されている間、ルータ SVI が IP アドレスを取得できるようになります。ルータ SVI はアップリンク VLAN になり、IP ルーティングまたは NAT 設定が適用されると、ワイヤレスクライアントなどのダウンリンク VLAN からのパケットを転送できるようになります。

詳細については、「無線機の同時使用に必要なルータ設定」を参照してください。

無線機をルート AP モードに設定する

次のコマンドを使用します。

```
configure dot11Radio <0|1> mode root-ap
```

SSID を VLAN ID を含めてルート AP モードの無線インターフェイスにマッピングする

次のコマンドを使用します。

```
configure dot11Radio <0|1> wlan add <profile-name> <wlan id> wlan <vlan-id>
```



- (注) 上記のコマンドでは、クライアントにサービスを提供する無線機での VLAN の作成が wired0 にブリッジされるため、ワイヤレスクライアントからのトラフィックがルータに直接転送されます。WLAN ID の範囲は 2 ~ 16 です (最大 15 の WLAN をサポート)。

ルート AP 関連の設定は、ルート AP 無線機を切り替えてはじめて保存され、有効になります。

WGB のブロードキャストタギングが有効になっている場合、ルート AP はワイヤレスクライアント接続をサポートできません。ブロードキャストタギング設定は、デフォルトで無効になります。

```
configure dot11Radio <0|1> wlan delete <profile-name>
```

ルート AP 無線インターフェイスの SSID をブロードキャストするよう無線チャンネルを設定する

次のコマンドを使用します。

```
configure dot11Radio <0|1> channel <channel number> <width>
```



- (注) 設定済みのチャンネルでレーダーが検出された場合、そのチャンネルは自動的に変更され、設定したチャンネルには戻りません。

無線インターフェイスのアンテナの設定

次のコマンドを使用します。

```
configure dot11Radio <0|1> antenna <dot11 antenna a/ab>
```

QoS プロファイルを設定して SSID プロファイルにアタッチする (オプション)

次のコマンドを使用します。

```
configure qos profile <qos-prof-name> <bronze|gold|platinum|silver> configure ssid-profile <profile-name> ssid <ssid> qos profile <qos-prof-name>
```

802.11 のタイプの有効化または無効化

次のコマンドを使用します。

```
configure dot11radio <slot-id> 802.11ax <enable/disable>
configure dot11radio <slot-id> 802.11n <enable/disable>
configure dot11radio <slot-id> 802.11ac <enable/disable>
```

出力制限とチャンネルのスイッチ数の設定

次のコマンドを使用します。

```
configure dot11radio <slot-id> 802.11h power-constraint <value> channel-switch-count <value>
```

無線インターフェイスの tx-power の設定

次のコマンドを使用します。

```
configure dot11Radio <0|1> tx-power <1-8>
```

uWGB をアップリンクバックホールとして使用する場合のルート AP の無線機設定例

次に、uWGB をアップリンクバックホールとして使用する場合のルート AP の無線機設定例を示します。

WIFI module uWGB configuration:

```
=====
AP6879.0974.F728#sh running-config
AP Name : AP6879.0974.F728
AP Mode : WorkGroupBridge
CDP State : Enabled
Watchdog monitoring : Enabled
SSH State : Enabled
AP Username : admin
Session Timeout : 0
WGB Trace : Disabled
Syslog Host : 0.0.0.0
```

Radio and WLAN-Profile mapping:-

```
=====
Radio ID Radio Mode SSID-Profile SSID
Authentication
0 RootAP root_wlan root_wlan
OPEN
1 UWGB Test Test
OPEN
```

Radio configurations:-

```
=====
Radio Id : 0
Admin state : ENABLED
Mode : RootAP
Spatial Stream : AUTO
Mgmt Frame Retries : 15
Channel(Band) : 1 (20)
Beacon Period : 100 mSec
Tx Power : 1
802.11ac : Disabled
802.11ax : Enabled
802.11n : Enabled
Encryption mode : AES128
Radio Id : 1
Admin state : ENABLED
Mode : UWGB
Spatial Stream : AUTO
Mgmt Frame Retries : 15
Uclient mac : C014.FE60.EF8D
```

```

Current state : UWGB
UClient timeout : 0 Sec
Dot11 type : 11ax
11v BSS-Neighbor : Disabled
A-MPDU priority : 0x3f
A-MPDU subframe number : 255
RTS Protection : 2347(default)
Rx-SOP Threshold : AUTO
Radio profile : NA
Encryption mode : AES128

```

List of Root-AP SSID-Profiles:

```

=====
Radio id : 0, SSID-Profile_8 : root_wlan

```

WGB specific configuration:-

```

=====
WGB Radio Id : NA
Mode State : NA
SSID Profile : NA
UWGB Radio Id : 1
Mode Enable : Enable
SSID Profile : Test
Uclient MAC Address: C014.FE60.EF8D

```

Password Policy configured:-

```

=====
password policy : Enable
password minimum length : 8
password lifetime : Disable
Upper Case Required : 1
Lower Case Required : 1
Digit Required : 1
Special Character Required : 1

Rx Beacon Missing Action : Enable
Rx Beacon Missing Count : 100
Packet retries Action : Reconnect
Packet retries Value : 64
RSSI Threshold Value : 70 dBm
Threshold timeout : 5 Sec
HSR-Scan status : Disable
Auth response timeout : 5000 Msec
Assoc response timeout : 5000 Msec
11v neighbor query timeout : 10 sec
WGB channel scan timeout : 20 Msec
Dhcp response timeout : 60 Sec
EAP timeout : 3 sec
Bridge table aging-time : 300 Sec
Probe pak data rate type : NA
Probe pak data rate : 0
Antenna Band Mode : Dual
Broadcast tagging : Disable
Wired Client 802.1x Auth : Disable
IGMP querier IP address : ::
Offchan scan status : Disable

```

Total configurations size on different structure:-

```

=====
Total channels : 0
Total SSID-Profiles : 3
Total Root-AP SSID-Profile : 1

```

```
Total EAP Profiles : 0
Total QOS Profiles : 0
Total dot1x credentials : 0
Total PKI truspoints : 0
Total bridge groups : 0
```

Total SSID profiles configured are:

```
=====
SSID-Profile : Test
SSID Name : Test
SSID Profile path : /data/platform/wbridge/Test
Auth type : OPEN
DTIM Period : 1
QOS profile :
SSID-Profile : root_wlan
SSID Name : root_wlan
SSID Profile path : /data/platform/wbridge/root_wlan
Auth type : OPEN
DTIM Period : 1
QOS profile :
```

L2NAT Configuration are:

```
=====
Status: disabled
Default Vlan: 0
The Number of L2nat Rules: 0
Dir Inside Outside Vlan
```

Ethernet Port Native VLAN Configuration are:

```
=====
Ethernet Port: 0
Status: disabled
Native VLAN ID: 0
Ethernet Port: 1
Status: disabled
Native VLAN ID: 0
```

Total QoS Mapping profiles configured are:

```
=====
Number of QoS Mapping Profiles: 0
```

Configuration command list:

```
=====
### WGB Running config - Hostname: AP6879.0974.F728 ###
configure ap management add username admin password $1$khxfBj0qAAV4gFMFboJcg. s
ecret $1$khxfBj0qAAV4gFMFboJcg.
configure ssid-profile Test ssid Test authentication open
configure ssid-profile root_wlan ssid root_wlan authentication open
configure dot11Radio 1 mode uwgb C014.FE60.EF8D ssid-profile Test
configure dot11Radio 1 enable
configure wgb mobile period 5 70
configure dot11Radio 0 mode root-ap
configure dot11Radio 0 wlan add root_wlan 8 vlan 10
configure dot11Radio 0 encryption mode ciphers aes-ccm
configure dot11Radio 0 antenna ab-antenna
configure dot11Radio 0 channel 7 20
configure dot11Radio 0 802.11ac disable
configure dot11Radio 0 tx-power 1
configure dot11Radio 0 enable
configure dot11Radio 1 encryption mode ciphers aes-ccm
configure dot11Radio 1 tx-power 1
```

WGB ルート AP での Web 認証

Web 認証の概要

Web 認証は、ゲストアクセスネットワークを設定するためのレイヤ3セキュリティ機能の役割を果たします。ワイヤレスクライアントの Web ブラウザを介して認証され、ユーザープロフィールを作成せずにオープン SSID に接続できます。

Cisco IOS XE リリース 17.15.1 以降では、WGB ルート AP で Web 認証を設定およびカスタマイズできます。Web 認証を設定すると、WP-WIFI6 の WGB ルート AP でキャプティブポータルがアクティブ化されます。Web ポータルの利用規約に同意して、インターネットにアクセスします。

Web 認証の設定により、デフォルトの Web ページまたはカスタマイズされた Web ページのいずれかを使用できます。

次の図は、デフォルトのキャプティブポータルページです。

図 1: デフォルトのキャプティブポータルページ



また、次のように Web 認証をカスタマイズできます。

- キャプティブポータル Web ページに同意した後で、希望する URL をリダイレクトする。
- カスタマイズした同意 Web ページを WIM にコピーし、WGB ルート AP の Web 認証に使用する。
- キャプティブポータル Web ページのカスタム仮想インターフェイス IP アドレスを割り当てる。
- キャプティブポータル Web ページで利用規約に同意する前に、特定のインターネット接続先にアクセスするための事前認証アクセス制御リスト (ACL) ルールを追加する。

たとえば、現在のキャプティブポータル Web ページに外部 Web サイトの広告を表示する場合などです。



- (注) Web 認証は、Android、iOS、macOS、および Windows ワイヤレスクライアントをサポートします。

Web 認証プロセス

1. **Wi-Fi への接続**：ホットスポット SSID を選択し、パブリック Wi-Fi ネットワークに接続して、デバイスで接続を確立します。
2. **キャプティブポータルの検出**：デバイスは、SSID に接続すると、関連付けられたキャプティブポータルを自動的に検出します。
3. **Web 認証のアクティブ化**：デバイスは Web ブラウザをアクティブ化し、特定の同意 Web ページを表示します。
4. **認証の完了**：Web 認証ページの手順を読んで理解したら、同意 Web ページの [Agree & Connect] ボタンをクリックしてサービス利用規約に同意します。
5. **インターネットへのアクセス**：キャプティブポータルアシスタントから求められる手順を完了すると、ネットワーク経由でインターネットにアクセスできるようになります。



- (注) クライアントキャッシュ：Web 認証の完了後 5 分以内に再接続する場合は、デバイスによって同意ページがバイパスされます。

Web 認証設定の前提条件

Wi-Fi モジュールとルータを設定するには、次の手順を実行します。

手順

- ステップ 1 無線インターフェイスを WGB モードおよびルート AP モードに設定します。[無線インターフェイスの WGB/uWGB モードおよびルート AP モードへの設定 \(49 ページ\)](#) を参照してください。
- ステップ 2 ルータに無線機の同時使用を設定します。[無線機の同時使用に必要なルータ設定 \(46 ページ\)](#) を参照してください。
- ステップ 3 WGB の静的 IP アドレスに ping を実行するように、ルータの IP サービスレベル契約 (SLA) を設定します。

```
Device(config)#ip sla number
```

例：

```
Router(config)#ip sla 10
Router(config-ip-sla)#icmp-echo 192.0.2.1 source-interface Vlan4094
Router(config-ip-sla-echo)#frequency 5
Router(config)#ip sla schedule 10 start-time now
```

(注)

- 192.0.2.1 は WGB の静的 IP アドレスで、Vlan4094 はルータと WGB の間で通信するためのダウンリンク VLAN です。
- ルータの IP SLA は、WGB の静的 IP アドレスに ping を実行します。
- WGB ルート AP に静的 IP アドレスが割り当てられている場合は、リロード後に ping を実行するか、WGB から ping を開始して、WGB の静的 IP アドレスをアクティブ化する必要があります。これを行わないと、Web 認証ページが正常に表示されません。
- ルータの IP SLA 設定によって WGB の静的 IP アドレスがアクティブ化され、手動で ping を行わなくても Web 認証ページがポップアップ表示されます。

Web 認証の制限事項

Web 認証は、事前認証アクセス制御リスト (ACL) の IPv4 アドレスと IP アドレスだけをサポートするように設計されています。完全修飾ドメイン名 (FQDN) ACL はサポートされません。

リダイレクト URL の設定は、Android クライアントでは必須です。

Web 認証の設定

Web 認証の有効化

AP で、次の手順を実行して Web 認証を設定します。

手順

ステップ 1 コマンドを実行して、HTTPd サービスを有効にします。

```
Device#configure ap http enable
```

(注)

デフォルトでは、HTTPd サービスは有効になっています。 **configure ap http disable** コマンドを実行して、HTTPd サービスを無効化します。

ステップ 2 コマンドを実行して、Web 認証を有効にします。

```
Device#configure webauth enable
```

(注)

configure webauth disable コマンドを実行して、Web 認証を無効にします。

ステップ3 コマンドを実行して、ルート AP WLAN の Web 認証を設定します。

```
Device#configure dot11Radio {0|1} wlan add <profile-name> <wlan id> wlan <vlan id> webauth
{default_webpage/customized_webpage}
```

(注)

デフォルトの Web ページは、webauthpassthrough.html です。必要に応じて、カスタム Web ページを使用できます。

カスタム Web ページが WGB にアップロードされていない場合、AP は警告を出力し、デフォルトの Web ページを使用します。

例：

次に、デフォルトおよびカスタム Web ページの設定例を示します。

- デフォルト Web ページ：

```
Device#configure dot11Radio 1 wlan add WebAuth 4 vlan 4094 webauth default_webpage
```

- カスタム Web ページ：

```
Device#configure dot11Radio 1 wlan add WebAuth-customize 5 vlan 4094 webauth customized_webpage
```

Web 認証設定のカスタマイズ

AP で、次の手順を実行して Web 認証設定をカスタマイズします。

手順

ステップ1 サーバーから WIM ストレージにカスタマイズする Web ページをコピーします。

```
Device#copy webpage {tftp|sftp}://<server-ip>[/dir]/[filename]
```

```
Device#copy webpage scp://username@<server-ip>[:port]/dir/[filename]
```

(注)

.tar ファイルまたは HTML ファイルをコピーできます。.tar ファイルのサイズは 10 MB を超えてはいけません。

例：

```
Device#copy webpage scp://root@100.10.10.3:/tftpboot/userid/WebAuth/wp_wifi6_web.tar
copy "scp://root@100.10.10.3:/tftpboot/userid/WebAuth/wp_wifi6_web.tar" to
"/storage/webauth/customized_webpage" (Y/N)Y
root@100.10.10.3's password:
wp_wifi6_web.tar                               100% 30KB 6.4MB/s 00:00
[*04/24/2024 08:27:34.1830] wp_wifi6_web/
[*04/24/2024 08:27:34.1830] wp_wifi6_web/logo.jpg
[*04/24/2024 08:27:34.1830] wp_wifi6_web/webauth.css
[*04/24/2024 08:27:34.1830] wp_wifi6_web/reg_customized_webpage.html
[*04/24/2024 08:27:34.1840] % Customized webpage will use wp_wifi6_web/reg_customized_webpage.html
as index.html
```

ストレージパス (/storage/webauth/customized_webpage/) にファイルを保存します。tar パッケージをこのディレクトリに抽出し、HTML ページの名前を index.html に変更します。

ステップ 2 リダイレクト URL を設定します。

```
Device#configure webauth redirect-url {customized|default} RedirectURL
```

例 :

```
Device#configure webauth redirect-url customized https://www.example.com/
```

(注)

カスタムリダイレクト URL を削除するには、**configure webauth redirect-url default** コマンドを使用します。

ステップ 3 Web 認証インターフェイスで仮想インターフェイスを設定します。

```
Device# configure interface webauth address ipv4 static<interface_ip> <netmask>
```

例 :

```
Device#configure interface webauth address ipv4 static 10.10.10.10 255.255.255.255
```

(注)

デフォルトでは、Web 認証インターフェイスは IP アドレス 1.1.1.1 を使用します。これは仮想インターフェイス IP (同意ページの Web サイトの IP アドレス) です。

ステップ 4 事前認証 ACL を設定します。

```
Device#configure webauthpreauth-acl add <aclrules>
```

例 :

```
Device#configure webauth preauth-acl add "allow true and dst 192.168.93.1 mask 255.255.255.0 and ip proto 6"
```

ACL ルールのフォーマットの例を次に示します。

- {allow/deny} {icmp/tcp/udp}
- {allow/deny} {icmp/tcp/udp} {src/dst} <> [mask] <>
- {allow/deny} true {and/or} {src/dst} <> [mask] <>
- {allow/deny} true {and/or} {src/dst} <> [mask] <> {and/or} {ip proto <>}
- {allow/deny} true
- {allow/deny} all
- {allow/deny} true {and/or} {tcp/udp} {src/dst} port <>

(注)

- 事前認証 ACL は、クライアントが WEBAUTH_REQD 状態になるとアクティブ化されます。
- ACL ルールの最大長は 255 文字です。ACL エントリの件数に制限はありません。
- 事前認証 ACL を削除するには、**configure webauth pre-authentication acl delete** コマンドを実行します。

- 事前認証 ACL を削除すると、すべての事前認証 ACL エントリがクリアされます。

WGB 設定のインポートとエクスポート

既存の WGB と同様の設定を作成する場合は、既存の WGB の稼働中の設定をサーバーにアップロードしてから、新たに展開した WGB にダウンロードします。

設定をサーバーにアップロードするには、次のコマンドを使用します。

```
Device#copy configuration upload {sftp|tftp|scp:} // ip-address [directory] [file-name]
```

展開内のすべての WGB にサンプル設定をダウンロードするには、次のコマンドを使用します。

```
Device#copy configuration download {sftp|tftp|scp:} // ip-address [directory] [file-name]
```

copy configuration download コマンドを実行すると、実行後にアクセスポイントが再起動します。インポートされた設定は、再起動後に有効になります。

Web 認証の確認

Web 認証

Web 認証の設定を確認するには、次の例に示すように **show webauth** を使用します。

```
Device#show webauth
```

```
WEBAUTH Configuration are:
=====
HTTP Status: enabled
Webauth Status: enabled
Webauth Redirect-URL: https://www.example.com/
Webauth Preauth-ACL: allow true and dst 198.51.100.1 mask 255.255.255.0 and ip proto 6,
  allow icmp dst 198.51.100.1 mask 255.255.255.0, allow icmp src 198.51.100.1 mask
255.255.255.0
Customized Webpage Exists: Yes
Customized Webpage MD5 HASH: 05ff0f8944e5466e484c342cba6fc403
```

Web 認証の現在のステータス

ルート AP WLAN ステータスを表示するには、次の例に示すように **show controller dot11radio {0|1} wlan** を使用します。

```
Device#show controllers dot11Radio 1 wlan
```

```
aprlv0      Link encap:Ethernet  HWaddr 68:79:09:B8:03:8F
            UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
            RX packets:0 errors:0 dropped:0 overruns:0 frame:60425858
            TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
            Interrupt:38
```

```
radio vap id          mac          ssid state ml_enabled          mld
webauth
```

```

1      3 68:79:09:B8:03:8C      WebAuth  UP      No 00:00:00:00:00:00
Yes
1      4 68:79:09:B8:03:8B  WebAuth-customize  UP      No 00:00:00:00:00:00
Yes

NON_ML
  intf TxData TxUC TxMBC TxBytes TxFail TxDcrd RxData RxUC RxMBC RxBytes RxErr stats_ago
aprlv3 3051 2976   75 2376573   919    0 2902 2556  346 575037   0 4.196000
aprlv4  427  402   25 289034    31    0  460  344  116  70123   0 4.196000
ML
  intf TxData TxUC TxMBC TxBytes TxFail TxDcrd RxData RxUC RxMBC RxBytes RxErr stats_ago
aprlv3     0    0    0     0     0     0     0     0     0     0     0     0 4.196000
aprlv4     0    0    0     0     0     0     0     0     0     0     0     0 4.196000

Vlan BSSID Pri/U/M EncryPolicy Key0 Key1 Key2 Key3 iGTK          SSIDs MFP
2290 38C   3 3 3      NONE                DIS              WebAuth  0
2290 38B   3 3 3      NONE                DIS      WebAuth-customize  0

VAP-ID          SSID Bridging Type
3              WebAuth Local-Switched
4  WebAuth-customize Local-Switched

```

Web 認証クライアントのステータス

クライアントの Web 認証ステータスを表示するには、次の例に示すように **show controller dot11radio {0|1} client** を使用します。

```
Device#show controllers dot11Radio 1 client
```

```

          mac radio vap aid          state encr  Maxrate Assoc Cap is_wgb_wired
wgb_mac_addr is_mld_sta is_webauth webauth_cached
BC:6E:E2:67:CD:9D   1   3   2  WEBAUTH_REQD OPEN MCS112SS   HE  HE           false
00:00:00:00:00:00           No           Yes           No
00:50:54:27:A2:9F   1   3   1    FWD OPEN MCS112SS   HE  HE           false
00:00:00:00:00:00           No           Yes           Yes

```

```
APAP6879.0974.FD08#show client summary
```

```
Radio Driver client Summary:
```

```
=====
```

```
aprlv3
```

```
-----
```

```

STA BC:6E:E2:67:CD:9D
  chanspec 153 (0xd099)
  state: AUTHENTICATED ASSOCIATED AUTHORIZED
  per antenna rssi of last rx data frame: -34 -34 0 0
  per antenna average rssi of rx data frames: -34 -33 0 0
  per antenna noise floor: -82 -84 0 0
smoothed rssi: -33
tx nrate
he mcs 9 Nss 2 Tx Exp 0 bw20 ldpc 2xLTF GI 1.6us auto
rx nrate
he mcs 9 Nss 2 Tx Exp 0 bw20 ldpc 4xLTF GI 3.2us auto

```

```
aprlv4
```

```
-----
```

```
WCP client Summary:
```

```
=====
```

```

          mac radio vap aid          state encr  Maxrate Assoc Cap is_wgb_wired
wgb_mac_addr is_mld_sta is_webauth webauth_cached
BC:6E:E2:67:CD:9D   1   3   2  WEBAUTH_REQD OPEN MCS112SS   HE  HE           false

```

```

00:00:00:00:00:00      No      Yes      No

Assoc time:
=====
                mac      assoc_time
BC:6E:E2:67:CD:9D 00d:00h:04m:08s

```



(注) 同意ページで同意するまでは、クライアントの状態は [WEBAUTH_REQD] であり、Web 認証が完了すると、クライアントの状態は [FWD] (転送) に変わります。

事前認証 ACL

クライアントの現在の事前認証 ACL を表示するには、次の例に示すように **show client access-lists pre-auth all client mac-address** を使用します。

```

Device#show client access-lists pre-auth all BC:6E:E2:67:CD:9D
Pre-Auth URL ACLs for Client: BC:6E:E2:67:CD:9D
IPv4 ACL: PREAUTH
IPv6 ACL:
ACTION      URL-LIST
Resolved IPs for Client: BC:6E:E2:67:CD:9D
HIT-COUNT   URL          ACTION      IP-LIST
PREAUTH
rule 0: allow true and dst 198.51.100.1 mask 255.255.255.0 and ip proto 6
rule 1: allow icmp dst 198.51.100.1 mask 255.255.255.0
rule 2: allow icmp src 198.51.100.1 mask 255.255.255.0

No IPv6 ACL found
Redirect URL for client: BC:6E:E2:67:CD:9D

Acl name Quota Bytes left In bytes Out bytes In pkts Out pkts Drops-in Drops-out
PREAUTH 0 0 0 148 0 2 21 201
CLIENT STATE: WEBAUTH_REQD
WEBAUTH_REQUIRED: TRUE
DNS POST AUTH: FALSE
PREAUTH ENABLED: TRUE
POSTAUTH ENABLED: FALSE

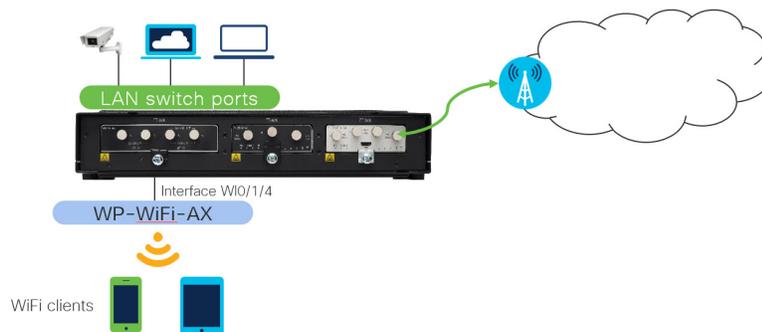
```

Cisco Embedded Wireless Controller (EWC)

Embedded Wireless Controller (EWC) のシナリオでは、次の機能が提供されます。

- 自己管理
- トラフィックのローカルスイッチング
- C9105 + IR1800 の性能に合わせて調整されたカスケード AP を管理できる場合もある
- WebUI 管理
- Cisco Catalyst ワイヤレス モバイル アプリケーション (iPhone/Android)

EWC モードは通常、公共交通機関/運輸の遠隔および移動体資産に使用されます。



ワイヤレスインターフェイスモジュールがEWCモードで実行されている場合、ワイヤレスコントローラかつアクセスポイント（通常、内部APと呼ばれる）として機能します。EWCは、専用ワイヤレスコントローラ（C9800 シリーズなど）と同様の方法で他の AP を管理します。

Cisco EWC ネットワークでは、ワイヤレスコントローラ機能を実行するアクセスポイント（AP）がアクティブ AP として指定されます。このアクティブ AP によって管理される他のアクセスポイントは従属 AP と呼ばれます。

EWC モードに使用されるイメージは C9800-AP-iosxe-wlc.bin です。

アクティブ EWC には以下の 2 つの役割があります。

- ワイヤレス LAN コントローラ（WLC）として機能し、従属 AP を管理および制御する。従属 AP は、クライアントにサービスを提供する中央管理型アクセスポイントとして機能します。
- クライアントにサービスを提供するアクセスポイントとして機能する。

Wi-Fi ランディングページ機能（Web ベース認証）のサポートについては、『[Cisco Embedded Wireless Controller on Catalyst Access Points Configuration Guide](#)』[英語]の「[Web-Based Authentication](#)」の章を参照してください。

Cisco Embedded Wireless Controller の詳細については、次を参照してください。

[Cisco Embedded Wireless Controller on Catalyst Access Points FAQ](#) [英語]

[Cisco Embedded Wireless Controller on Catalyst Access Points \(EWC\) ホワイトペーパー](#)

IR1800 で EWC アクセスポイントを設定するための前提条件

ルータで EWC アクセスポイントを設定する前に、次の前提条件が満たされていることを確認します。

- Cisco Embedded Wireless Controller（EWC）ネットワークのセットアップ時や毎日の運用時に、同じネットワークに他の Cisco Wireless LAN Controller（アプライアンスも仮想も）を実装しないことを推奨します。
- DHCP サーバーは、アクセスポイントおよびクライアントが IP アドレスを取得できるように、ネットワーク上で使用可能である必要があります。

- IR1800 シリーズ ルータに統合された EWC および AP を設定するには、ルータで DHCP サーバー、SVI インターフェイス、および NAT を設定する必要があります。AP の設定に関する詳細は、[IR1800 で CAPWAP アクセスポイント構成を設定するための前提条件 \(36 ページ\)](#) の項を参照してください。
- Embedded Wireless Controller (EWC) では、管理トラフィックはタグなしで、スイッチポートのネイティブ VLAN として設定する必要があります。WIM と WLAN がすべて異なる VLAN 上にある場合は、ルータの WIM 接続ポートをトランクとして設定する必要があります。個々の WLAN のトラフィックはそれぞれの VLAN でローカルにスイッチングされます。次に、異なる VLAN 上の WIM と WLAN を使用したルータ設定を示します。

コマンド	目的
<pre>interface Wlan-GigabitEthernet slot/subslot/port switchport mode trunk switchport trunk native vlan number switchport trunk allowed vlan numbers</pre>	<p>WIM 内部スイッチインターフェイスのスイッチポートモードとネイティブ VLAN を設定します。ネイティブ VLAN 10 は AP 管理 VLAN である必要があります。VLAN 20 および 30 は WLAN トラフィックに使用されます。</p>

次の例を参照してください。

```
Router(config)#interface Wlan-GigabitEthernet 0/1/4
Router(config-if)#switchport mode trunk
Router(config-if)#switchport trunk native vlan 10
Router(config-if)#switchport trunk native vlan 10,20,30
```

Day 0 プロビジョニングを使用した EWC の設定

Day 0 プロビジョニングを使用して AP を設定するには、次の 3 つの方法があります。

1. 「[EWC の導入](#)」 [英語] の手順に従って、SSID を CiscoAirProvision-XXXX に接続します。
2. 携帯電話で Catalyst ワイヤレスアプリケーションを使用して QR コードをスキャンすることもできます。『[User Guide for Cisco Catalyst Wireless Mobile Application](#)』 [英語] の手順に従ってください。
3. 「[Day 0 ウィザードを使用したコントローラの設定 \(CLI\)](#)」 の手順に従うか、「[オプション 1 初期 CLI 設定](#)」 (『[Catalyst 9100 アクセスポイントの Embedded Wireless Controller への変換](#)』内) の手順に従って手動で基本設定を行うことで、CLI を使用して AP を手動で設定できます。

その他の考慮事項は次のとおりです。

- WebUI またはシスコ ワイヤレス モビリティ アプリケーションを使用して初期設定を行う場合は、設定済みの VLAN プール (VLAN10 など) から IP アドレスが取得されるよう、Wi-Fi モジュールをリロードすることが推奨されます。

- WebUI での初期設定は、デフォルトの IP アドレス (192.168.0.1) と異なる IP アドレスを使用し、かつ、その IP アドレスが IR1800 IOS-XE の初期設定用 IP アドレスとも競合した場合には機能しない可能性があります。

Cisco Embedded Wireless Controller (EWC) 対応アクセスポイントのネットワークへの接続

展開に応じて、ルータポートに接続された Embedded Wireless Controller (EWC) 対応アクセスポイントを、アクセスポートまたはトランクポートに設定できます。

アクセスポイントと WLAN がすべて同じネットワーク上にある場合、Embedded Wireless Controller (EWC) 対応アクセスポイントは、次の例に示すように、アクセスモードでルータに接続できます。

```
interface Wlan-GigabitEthernet 0/1/4
switchport access vlan 10
switchport mode access
```

Embedded Wireless Controller (EWC) では、管理トラフィックはタグなしです。アクセスポイントと WLAN がすべて異なる VLAN 上にある場合、Embedded Wireless Controller (EWC) 対応アクセスポイントはスイッチのトランクポートに接続し、個々の WLAN のトラフィックは個々の VLAN でローカルにスイッチングされます。次に示すのは、異なる VLAN でアクセスポイントと WLAN を使用した展開の例です。

```
interface Wlan-GigabitEthernet 0/1/4
switchport trunk native vlan 10
switchport trunk allowed vlan 10,20,30
switchport mode trunk
```

EWC モードの WebUI 管理

ここでは、WebUI を使用して EWC モードで WIM を設定する手順について説明します。

Day 0 Over-The-Air WebUI セットアップウィザードを使用したプロビジョニング

AP が Embedded Wireless Controller (EWC) モードで再起動すると、MAC アドレスの最後の数字で終わるプロビジョニング SSID がブロードキャストされます。PSK パスワードを使用してプロビジョニング SSID に接続できます。

次に、ブラウザを開いて mywifi.cisco.com にリダイレクトすると、AP Web UI に移動します。ユーザー名に **webui**、パスワードに **cisco** と入力します。詳しい Day 0 設定手順は、次のリンクを参照してください。 <https://www.cisco.com/c/en/us/products/collateral/wireless/embedded-wireless-controller-catalyst-access-points/white-paper-c11-743398.html#DeployingtheEWC>



- (注) Embedded Wireless Controller (EWC) 設定ポータルへの Web リダイレクションは、プロビジョニング SSID に接続している場合にのみ機能します。ラップトップが別の Wi-Fi ネットワークまたは有線ネットワークに接続されている場合は機能しません。Day 0 ウィザードプロビジョニングモードのときに EWC IP アドレスを入力しても、有線ネットワークからは AP を設定できません。

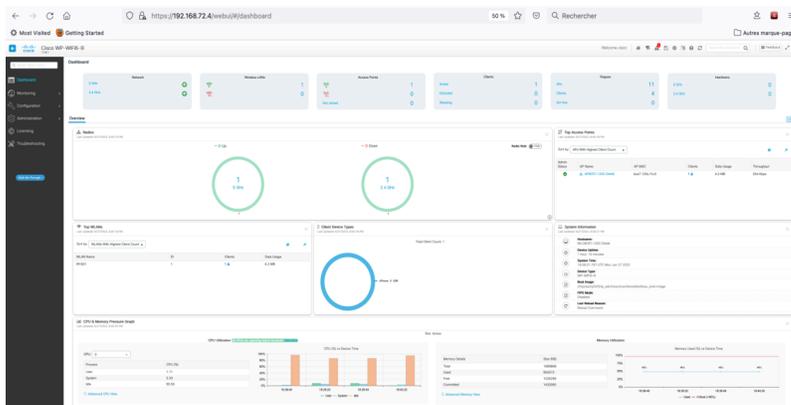
EWC WebUI へのログイン

EWC にログインするには、次の手順を実施します。

手順

ステップ 1 ブラウザから WebUI を開きます。DHCP から割り当てられた IP アドレスを使用します。

ステップ 2 WebUI ダッシュボードが表示されます。



ステップ 3 ワイヤレス LAN コントローラ (WLC) に接続すると、他のアクセスポイントと同様に設定が実行されます。詳細については、次のリソースを参照してください。

[Overview of Cisco Embedded Wireless Controller on Catalyst Access Points \[英語\]](#)

[Cisco Embedded Wireless Controller on Catalyst Access Points Configuration Guide, IOS XE \[英語\]](#)



第 6 章

フレキシブルアンテナポート

この章は、次の項で構成されています。

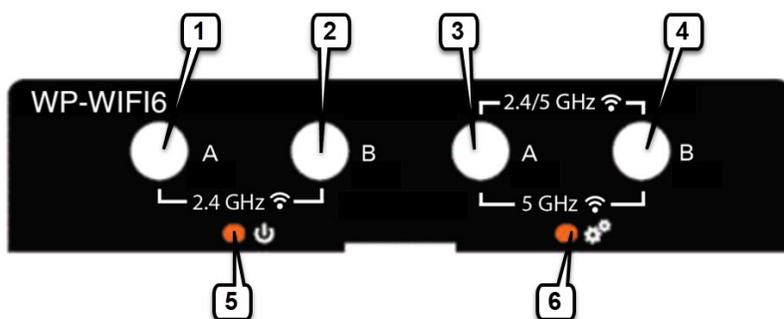
- [フレキシブルアンテナポート \(67 ページ\)](#)
- [CAPWAP AP 用フレキシブルアンテナポートの設定 \(68 ページ\)](#)
- [WGB 用フレキシブルアンテナポートの設定 \(69 ページ\)](#)

フレキシブルアンテナポート

フレキシブルアンテナポート機能により、お客様による無線のカバー範囲のカスタマイズが可能です。CLI コマンドまたは WebUI を使用して、この機能をデュアルバンドモードまたはシングルバンドモードに設定できます。デフォルトはデュアルバンドモードです。

アンテナポートのラベル付けについては、WIM では 2.4G、5G 両方のポストに A と B のラベルを使用します。

WIM の前面パネルを見ると、4 つのアンテナポートが 1 ~ 4 と示されています。5 と 6 は、[ハードウェアの概要 \(1 ページ\)](#) の説明にあるステータス LED です。



デュアルバンドモードでは、デュアルバンドアンテナを右側のアンテナポート 3 と 4 にインストールします。

シングルバンドモードでは、2.4G バンドアンテナを左側のアンテナポート 1 と 2 にインストールし、5G バンドアンテナを右側のアンテナポート 3 と 4 にインストールします。

CAPWAP AP 用フレキシブルアンテナポートの設定

次の2つの手順を使用します。

CLI を使用したコントローラの CAPWAP AP アンテナバンドモードの設定

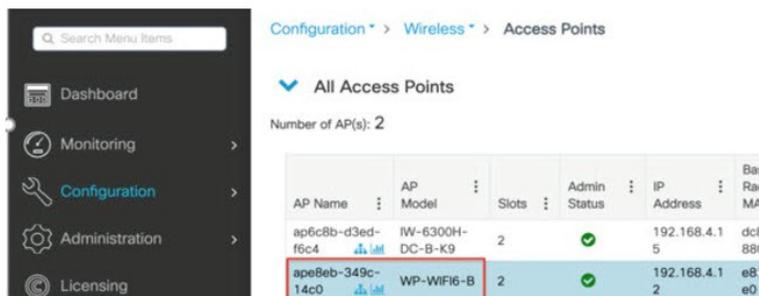
ap name <Cisco AP> **antenna band-mode** [single][dual]

次に例を示します。

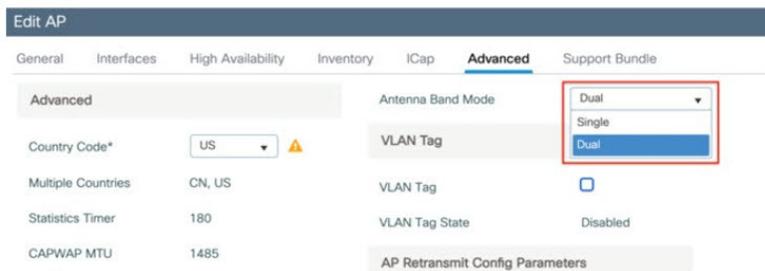
```
ap name ape8eb-349c-14c0 antenna-band-mode ?
dual      Dual band mode
single    Single band mode
```

WebUI を使用したコントローラの CAPWAP AP アンテナバンドモードの設定

1. [Configuration] > [Wireless] > [Access Points] の順に進み、アクセスポイントを選択します。



2. [Edit AP] > [Advanced] の順に選択します。[Antenna Band Mode] を選択し、[Update & Apply to Device] をクリックして AP に設定を保存します。



アンテナバンドモードの確認

次の CLI を使用して、コントローラの CAPWAP AP アンテナバンドモードを確認します。

```
WLC#show ap name <Cisco AP> config general | inc Antenna Band
For example:
WLC#show ap name ape8eb-349c-14c0 config general | inc Antenna Band
Antenna Band Mode: Single
```

次の CLI を使用して、WIM の AP アンテナバンドモードを確認します。バンドモードは、GPIO 値によって表示されます。

```
AP#show capwap client config | inc GPIO
For example:
AP84EB.EF55.1498#show capwap client config | inc GPIO
GPIO_34: 0
GPIO_35: 1
```



(注) GPIO_34:1 および GPIO_35:0 はデュアルバンドモードです。GPIO_34:0 および GPIO_35:1 はシングルバンドモードです。

WGB 用フレキシブルアンテナポートの設定

CLI を使用して WIM の WGB アンテナバンドモードを設定するには、次の例にあるいずれかのオプションを使用します。

```
WGB#configure wgb antenna band mode
    dual    Configure WGB antenna dual band
    single  Configure WGB antenna single band
```

次に例を示します。

```
AP84EB.EF55.1498#configure wgb antenna band mode single
[*10/24/2023 22:55:04.7280] Antenna band mode configuration has been saved successfully

AP84EB.EF55.4E53#configure wgb antenna band mode dual
[*10/24/2023 22:57:14.3470] Antenna band mode configuration has been saved successfully
```

CLI を使って WIM の WGB アンテナバンドモードを確認するには、**show running-config | inc Antenna** CLI を使用します。

```
AP84EB.EF55.1498#show running-config | inc Antenna
Antenna Band Mode          : Single

AP84EB.EF55.4E53#show running-config | inc Antenna
Antenna Band Mode          : Dual
```


翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。