AP グループ

AP グループを設定するための前提条件

次に、コントローラ でアクセス ポイント グループを作成するための前提条件を示します。

- VLAN またはサブネットにサービスを提供するルータ上で、必要なアクセス コントロール リスト（ACL）を定義する必要があります。
- アクセス ポイント グループ VLAN では、マルチキャスト トラフィックがサポートされます。ただし、クライアントがあるアクセス ポイントから別のアクセス ポイントにローミングする場合、IGMP スヌーピングが有効になっていないと、クライアントによってマルチキャスト トラフィックの受信が停止されることがあります。

アクセス ポイント グループの設定の制約事項

- AP グループ テーブル内の WLAN に対するインターフェイス マッピングが、WLAN インターフェイスと同じであるとします。WLANインターフェイスが変更されると、APグループ テーブル内の WLAN に対するインターフェイス マッピングも新しい WLAN インターフェイスに変わります。

  AP グループ テーブル内の WLAN に対するインターフェイス マッピングが、WLAN に定義されたインターフェイスと異なるとします。WLANインターフェイスが変更されても、

AP グループ テーブル内の WLAN に対するインターフェイス マッピングは新しい WLAN インターフェイスに変わりません。

- コントローラ 上の設定をクリアすると、アクセス ポイント グループのすべてが非表示となります。ただし、デフォルトのアクセス ポイント グループである「default-group」（自動的に作成される）は例外です。
- デフォルトのアクセス ポイント グループには、最大 16 の WLAN を関連付けることができます。デフォルトのアクセス ポイント グループの WLAN ID は、16 以下である必要があります。大規模なデフォルトのアクセス ポイント グループ内で ID が 16 以上の WLAN が作成されると、WLAN SSID はブロードキャストされません。デフォルトのアクセス ポイント グループのすべての WLAN ID で ID が 16 以下であることが必要です。16 を超える ID を含む WLAN は、カスタム アクセス ポイント グループに割り当てることができます。
- OfficeExtend アクセス ポイントはすべて同じアクセス ポイント グループ内にあり、このグループに含まれる WLAN は最大 15 個にする必要があります。アクセス ポイント グループ内の OfficeExtend アクセス ポイントを持つコントローラ は、パーソナルな SSID に対して割り当てられる WLAN が 1 つであるため、接続されている各 OfficeExtend アクセス ポイントに最大 15 個の WLAN しか公開しません。

（注） アクセス ポイント グループ内の OfficeExtend アクセス ポイントを持つコントローラ は、パーソナルな SSID に対して割り当てられる WLAN が 1 つであるため、接続されている各 OfficeExtend アクセス ポイントに最大 15 の WLAN を公開します。

- 同じ AP グループと同じ FlexConnect グループに属しているメッシュ ツリー（同じセクター）内のすべての フレックス + ブリッジ AP は WLAN-VLAN マッピングを正しく継承するように設定することをお勧めします。
- AP グループに新しい WLAN を追加すると常に無線リセットが発生し、接続状態になっているクライアントは認証が解除され、再接続する必要があります。AP グループの WLAN 設定の追加や変更は、停止を防ぐためにメンテナンス時にのみ行うことをお勧めします。
- 設定可能な AP グループの数は、Cisco WLC の ap-count ライセンスの数までです。たとえば、Cisco WLC に 5 つの ap-count ライセンスがある場合、設定できる AP グループの最大数は 5（デフォルトの AP グループを含む）です。

アクセス ポイント グループについて

コントローラ 上に最大 512 の WLAN を作成した後では、さまざまなアクセス ポイントに WLAN を選択的に公開（アクセス ポイント グループを使用して）することで、ワイヤレス ネットワークをより適切に管理できます。一般的な展開では、WLAN 上のすべてのユーザはコントローラ上の 1 つのインターフェイスにマップされます。したがって、WLAN に接続しているすべての

ユーザは、同じサブネットまたは VLAN に存在します。しかし、複数のインターフェイス間で負荷を分散すること、またはアクセス ポイント グループを作成して、個々の部門（たとえばマーケティング部門）などの特定の条件に基づくグループユーザへと負荷を分配することを選択できます。さらに、ネットワーク管理を簡素化するために、これらのアクセス ポイント グループを別個の VLAN で設定できます。

（注） アクセス ポイント グループからアクセスポイントを削除すると、そのアクセス ポイントの設定は保存されません。

アクセス ポイント グループの設定

手順

ステップ 1 適切な動的インターフェイスを設定し、必要な VLAN にマップします。

たとえば、「アクセス ポイント グループについて」の項で説明するネットワークを設定するには、コントローラに VLAN 61、62、および 63 の動的インターフェイスを作成します。動的インターフェイスを設定する方法の詳細については、「動的インターフェイスの設定」の項を参照してください。

ステップ 2 アクセス ポイント グループを作成します。「アクセス ポイント グループの作成」の項を参照してください。

ステップ 3 RF プロファイルを作成します。「RF プロファイルの作成」の項を参照してください。

ステップ 4 適切なアクセス ポイント グループにアクセス ポイントを割り当てます。「アクセス ポイント グループの作成」の項を参照してください。

ステップ 5 AP グループの RF プロファイルを適用します。「AP グループへの RF プロファイルの適用」の項を参照してください。

アクセス ポイント グループの作成（GUI）

手順

ステップ 1 [WLANs] > [Advanced] > [AP Groups] の順に選択して、[AP Groups] ページを開きます。

このページには、コントローラで現在作成されているすべてのアクセス ポイント グループが表示されます。デフォルトでは、アクセス ポイントは、他のアクセス ポイント グループに割り当てられない限り、すべて、デフォルトのアクセス ポイント グループ「default-group」に属します。

（注） コントローラによってデフォルトのアクセス ポイント グループが作成され、その中に、最初の 16 の WLAN（1 ～ 16 の ID を持つ WLAN、設定された WLAN の数が 16 に満たない場合は、さらに少なくなる）が自動的に入力されます。このデフォルトのグループは変更できません（このグループに WLAN を追加したり、このグループから WLAN を削除することはできません）。先頭の 16 の WLAN が追加または削除されるたびに、グループの内容は動的に更新されます。アクセス ポイントは、アクセス ポイント グループに属していない場合には、デフォルト グループに割り当てられ、そのデフォルト グループ内の WLAN を使用します。アクセス ポイントは、未定義のアクセス ポイント グループ名を有するコントローラと join した場合、そのグループ名を保持しますが、default-group アクセス ポイント グループ内の WLAN を使用します。

ステップ 2 [Add Group] をクリックして、新しいアクセス ポイント グループを作成します。[Add New AP Group] のセクションがページ上部に表示されます。

ステップ 3 [AP Group Name] テキスト ボックスに、グループの名前を入力します。

ステップ 4 [Description] テキスト ボックスに、グループの説明を入力します。

ステップ 5 [NAS-ID] テキスト ボックスに、AP グループのネットワーク アクセス サーバの ID を入力します。

ステップ 6 [Add] をクリックします。新たに作成したアクセス ポイント グループが、[AP Groups] ページのアクセス ポイント グループのリストに表示されます。

（注） このグループを削除するには、そのグループの青いドロップダウンの矢印の上にカーソルを置いて、[Remove] を選択します。1 つ以上のアクセス ポイントで使用しているアクセス ポイント グループを削除しようとすると、エラー メッセージが表示されます。コントローラ ソフトウェア リリース 6.0 以降では、アクセス ポイント グループを削除する前に、そのグループ内のすべてのアクセス ポイントを別のグループに移動させます。以前のリリースのように、アクセス ポイントが default-group アクセス ポイント グループに移動されることはありません。

ステップ 7 グループの名前をクリックして、この新しいグループを編集します。[AP Groups > Edit (General)] ページが表示されます。

ステップ 8 このアクセス ポイント グループの説明を変更するには、[AP Group Description] テキスト ボックスに新しいテキストを入力して、[Apply] をクリックします。

ステップ 9 [WLANs] タブを選択して、[AP Groups > Edit (WLANs)] ページを開きます。このページでは、このアクセス ポイント グループに現在割り当てられている WLAN が表示されます。

ステップ 10 [Add New] をクリックして、このアクセス ポイント グループに WLAN を割り当てます。[Add New] のセクションがページ上部に表示されます。

ステップ 11 [WLAN SSID] ドロップダウン リストから、この WLAN の SSID を選択します。

ステップ 12 [Interface Name] ドロップダウン リストから、アクセス ポイント グループをマップするインターフェイスを選択します。Network Admission Control（NAC;ネットワーク アドミッション コントロール）のアウトオブバンドのサポートを有効にする場合は、検疫 VLAN を選択します。

（注） default-groupアクセス ポイント グループ内のインターフェイス名は、WLANインターフェイスと一致します。

ステップ 13 [SNMP NAC State] チェックボックスをオンして、このアクセス ポイント グループに対するNAC アウトオブバンドのサポートを有効にします。NAC アウトオブバンドのサポートを無効にするには、チェックボックスをオフ（デフォルト値）のままとします。

ステップ 14 [Add] をクリックして、この WLAN をアクセス ポイント グループに追加します。この WLANが、このアクセス ポイント グループに割り当てられている WLAN のリストに表示されます。

（注） このWLANをアクセスポイントグループから削除する場合は、カーソルをこのWLANの青のドロップダウン矢印の上に置いて、[Remove] を選択します。

ステップ 15 ステップ *10* ～ ステップ *14* を繰り返して、このアクセス ポイント グループに WLAN をさらに追加します。

ステップ 16 [APs]タブを選択して、このアクセスポイントグループにアクセスポイントを割り当てます。[AP Groups > Edit]（[APs]）ページには、このグループに現在割り当てられているアクセス ポイントと、グループへの追加が可能なアクセス ポイントが一覧されます。アクセス ポイントがグループに現在割り当てられていない場合、そのアクセス ポイントのグループ名は「default-group」として表示されます。

ステップ 17 アクセス ポイント名の左側にあるチェック ボックスをオンにして [Add APs] をクリックし、このアクセス ポイント グループにアクセス ポイントを追加します。すると、アクセス ポイントが、再ロードされた後に、このアクセス ポイント グループに現在属しているアクセス ポイントのリストに表示されます。AP をあるグループから別のグループに移動する必要がある場合は、AP を再ロードする必要があります。

（注） 使用可能なアクセス ポイントを一度にすべて選択するには、[AP Name] チェックボックスをオンにします。これで、すべてのアクセス ポイントが選択されます。

（注） グループからアクセス ポイントを削除する場合は、アクセス ポイント名の左側のチェックボックスをオンにし、[Remove APs] をクリックします。一度にすべてのアクセス ポイントを選択するには、[AP Name] チェックボックスをオンにします。これで、このグループからすべてのアクセス ポイントが削除されます。

（注） アクセス ポイントが属するアクセス ポイント グループを変更する場合は、[Wireless] > [Access Points] > [All APs] > [ap_name] > [Advanced] タブを選択し、[AP Group Name] ドロップダウン リストから別のアクセス ポイント グループの名前を選択し、[Apply] をクリックします。

ステップ 18 [802.11u] タブで、次のことを実行します。

a) 類似のホットスポットの場所をグループ化するホットスポット グループを選択します。
b) 選択するホットスポットの場所グループに基づく場所タイプを選択します。
c) 新しい場所を追加するには、[Add New Venue] をクリックし、その場所で使用される言語名と、基本サービス セット（BSS）と関連付けられる場所の名前を入力します。この名前は、場所に関する十分な情報を SSID が提供していない場合に使用します。
d) AP グループの動作クラスを選択します。

e) [Apply] をクリックします。

ステップ 19 （注） この手順は次のモジュールに適用されます。

- AoA ベースは、HyperLocation モジュールを使用した AP3600 および AP3700 に適用されます
- PRL ベースは、モジュールのない AP（AP700/AP1700/AP2600/AP2700/AP3600/AP3700）と、NOS モジュールを使用した AP3600 および AP3700 に適用されます

[Locatio] タブで、次の手順を実行します。

a) Hyperlocation を有効または無効にします。

[Enable Hyperlocation] チェックボックスをオンにすると、AP と取り付けられているモジュールに基づいて、異なるロケーション サービス（PRL ベースまたは AoA ベース）が有効になります。

b) [Packet Detection RSSI Minimum (dBm)] の値を入力します。

これは、ロケーション計算で使用するために、データ パケットが WSM モジュールで受信される最小レベルです。デフォルト値は -100 dB です。

ロケーションの計算に強い信号のみを使用する場合は、この値を増やすことをお勧めします。

c) [Scan Count Threshold for Idle Client Detection] の値を入力します。

スキャン数のしきい値は、AP がアイドル状態のクライアントにブロック確認応答要求（BAR）を送信する前に待機するオフチャネル スキャン サイクル数を表します。デフォルト値の 10 は、オフチャネル スキャン サイクル内のチャネル数に応じて、約 40 秒に相当します。

d) NTP サーバの IPv4 アドレスを入力します。

これは、この計算に関係するすべての AP が同期する NTP サーバの IPv4/IPv6 アドレスです。

一般的な WLC インフラストラクチャで使用されるのと同じ NTP サーバを使用することをお勧めします。ロケーションを正確に計算するためには、複数の AP からのスキャンが同期されている必要があります。IPv4 アドレスが必要です。

（注） シスコの Hyperlocation ソリューションの詳細については、このマニュアルを参照してください。

ステップ 20 [RF Profiles] タブで、802.11a および 802.11b 無線を使用する AP の RF プロファイルを選択し、[Apply] をクリックします。
AP プロファイルを適用すると、AP グループに関連付けられているすべての AP がリブートされます。

ステップ 21 [Save Configuration] をクリックします。

アクセス ポイント グループの作成（CLI）

手順

ステップ 1 アクセス ポイント グループを作成するには、次のコマンドを入力します。

config wlan apgroup add *group_name*

（注） アクセス ポイント グループを削除するには、**config wlan apgroup delete** *group_name* コマンドを入力します。1つ以上のアクセスポイントで使用しているアクセス ポイント グループを削除しようとすると、エラー メッセージが表示されます。コントローラ ソフトウェア リリース6.0以降では、アクセスポイントグループを削除する前に、そのグループ内のすべてのアクセスポイントを別のグループに移動させます。以前のリリースのように、アクセス ポイントが default-group アクセス ポイント グループに移動されることはありません。グループ内のアクセスポイントを表示するには、**show wlan apgroups** コマンドを入力します。アクセス ポイントを別のグループに移動するには、**config ap group-name** *group_name Cisco_AP* コマンドを入力します。

ステップ 2 アクセス ポイント グループに説明を追加するには、次のコマンドを入力します。

config wlan apgroup description *group_name description*

ステップ 3 アクセス ポイント グループに WLAN を割り当てるには、次のコマンドを入力します。

config wlan apgroup interface-mapping add *group_name wlan_id interface_name*

（注） アクセス ポイント グループから WLAN を削除するには、**config wlan apgroup interface-mapping delete** *group_name wlan_id* コマンドを入力します。

ステップ 4 このアクセス ポイント グループに対して、NAC アウトオブバンドのサポートを有効または無効にするには、次のコマンドを入力します。

config wlan apgroup nac {**enable** | **disable**}*group_name wlan_id*

ステップ 5 次のコマンドを入力して、アクセス ポイント グループで WLAN 無線ポリシーを設定します。

config wlan apgroup wlan-radio-policy *apgroup_name wlan_id* {**802.11a-only** | **802.11bg** | **802.11g-only** | **all**}

（注） リリース 8.0 では、AP グループの WLAN 無線ポリシー設定をアップロードまたはダウンロード時に保存できます。

ステップ 6 アクセス ポイントをアクセス ポイント グループに割り当てるには、次のコマンドを入力します。

config ap group-name *group_name Cisco_AP*

（注） アクセス ポイント グループからアクセス ポイントを削除するには、このコマンドを再度入力して、そのアクセス ポイントを別のグループに割り当てます。

ステップ 7 AP グループのホットスポットを設定するには、次のコマンドを入力します。

config wlan apgroup hotspot {**venue** | **operating-class**}

ステップ 8 次のコマンドを入力して、変更を保存します。

save config

アクセス ポイント グループの表示（CLI）

アクセス ポイント グループについて情報を表示する、またはトラブルシューティングするには、次のコマンドを使用します。

- コントローラのすべてのアクセス ポイント グループのリストを表示するには、次のコマンドを入力します。

  show wlan apgroups

- アクセス ポイント グループに割り当てられている各 WLAN の BSSID を表示するには、次のコマンドを入力します。

  show ap wlan {**802.11a** | **802.11b**} *Cisco_AP*

- アクセス ポイント グループに対して有効になっている WLAN の数を表示するには、次のコマンドを入力します。

  show ap config {**802.11a** | **802.11b**} *Cisco_AP*

- アクセス ポイント グループのデバッグを有効または無効にするには、次のコマンドを入力します。

  debug group {**enable** | **disable**}

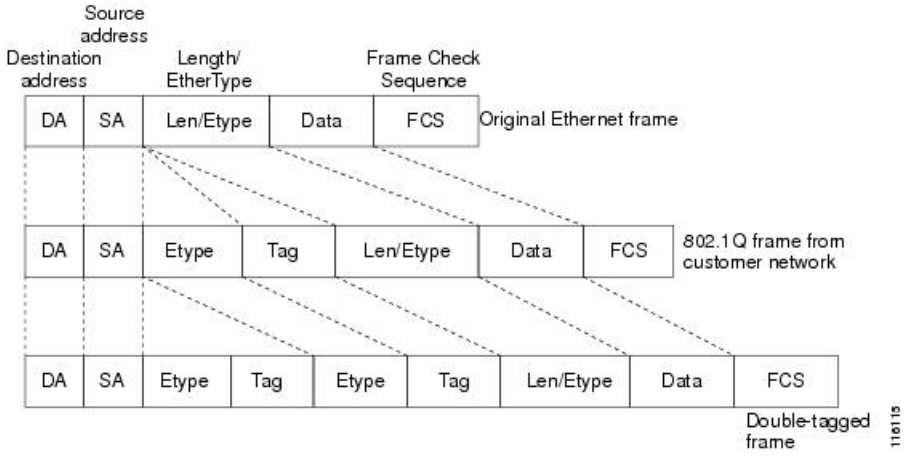
802.1Q-in-Q VLAN タギング

802.1Q-in-Q VLAN タギングの情報

クライアントごとに一意の VLAN ID 範囲を割り当てると、4096 VLAN という制限を超える可能性があります。802.1Q-in-Q VLAN タグ機能は、別の 802.1Q VLAN タグ内に 802.1Q VLAN タギングをカプセル化します。外部タグは AP グループに基づいて割り当てられ、内部 VLAN ID は AAA サーバによって動的に割り当てられます。

802.1Q-in-Q機能を使用すれば、単一のVLANで複数のVLANをサポートできます。802.1Q-in-Q機能では、VLAN ID を保存しながら、複数の VLAN のトラフィックを分離できます。下の図は、タグなし、802.1Q タグ付き、および802.1Q-in-Q タグ付きのイーサネット フレームを示しています。

図 *1 :* タグなし、*802.1Q* タグ付き、および *802.1Q-in-Q* タグ付きのイーサネット フレーム



802.1Q-in-Q VLAN タギングの制約事項

- IGMP スヌーピングを無効にするまで、マルチキャストは有効にできません。
- 802.1Q-in-Q VLAN タギングは、レイヤ 2 およびレイヤ 3 のコントローラ内ローミング、およびレイヤ 2 コントローラ間ローミングでのみサポートされます。レイヤ 3 コントローラ間ローミングはサポートされません。
- 0x8100 は、802.1Q-in-Q イーサネット フレームの [Ether Type] フィールドに対してのみサポートされている値です。
- 中央でスイッチされるパケットでのみ、802.1Q-in-Q VLAN タギングを有効にすることができます。
- 802.1Q-in-Q VLAN タギングについては、IPv6 DHCP パケットではなく、IPv4 DHCP パケットのみ有効にすることができます。
- tunnel-type である IETF 属性は、C-VLAN のオーバーライドに必要です。
- C-VLAN は tunnel-private-group-ID /tunnel-type および tunnel-private-group-id で設定できます。

802.1Q-in-Q VLAN タギングの設定（GUI）

手順

ステップ 1 **[WLANs]** > **[Advanced]** > **[AP Groups]** の順に選択して、[AP Groups] ページを開きます。

ステップ 2 [AP Group Name] をクリックして、対応する [AP Groups > Edit] ページを開きます。

ステップ 3 [General] タブをクリックして、802.1Q-in-Q VLAN タギングの詳細を設定します。

ステップ 4 [Enable Client Traffic QinQ] チェックボックスをオンにして、AP グループの 802.1Q-in-Q VLAN タギングを有効にします。

ステップ 5 [Enable DHCPv4 QinQ] チェックボックスをオンにして、AP グループの IPv4 DHCP パケットの 802.1Q-in-Q VLAN タギングを有効にします。

ステップ 6 [QinQ Service VLAN ID] テキスト ボックスに、802.1Q-in-Q VLAN タギングの VLAN ID を入力します。

ステップ 7 [Apply] をクリックします。

802.1Q-in-Q VLAN タギングの設定（CLI）

手順

ステップ 1 次のコマンドを入力して、AP グループの 802.1Q-in-Q VLAN タギングを有効または無効にします。

config wlan apgroup qinq tagging client-traffic *apgroup_name* {**enable** | **disable**}

デフォルトでは、AP グループのクライアント トラフィックの 802.1Q-in-Q VLAN タギングは無効です。

ステップ 2 次のコマンドを入力して、 AP グループのサービス VLAN を設定します。

config wlan apgroup qinq service-vlan *apgroup_name vlan_id*

ステップ 3 次のコマンドを入力して、 AP グループのクライアント トラフィックの IPv4 DHCP パケットを有効または無効にします。

config wlan apgroup qinq tagging dhcp-v4 *apgroup_name* {**enable** | **disable**}

（注） DHCPv4 トラフィックの 802.1Q-in-Q タギングを有効にする前に、クライアント トラフィックの 802.1Q-in-Q タギングを有効にする必要があります。

デフォルトでは、AP グループの DHCPv4 トラフィックの 802.1Q-in-Q VLAN タギングは無効です。

ステップ 4 次のコマンドを入力して、AP グループの EAP for Global System for Mobile Communications (GSM) Subscriber Identity Module（EAP-SIM）、または EAP for Authentication and Key Agreement 認証クライアント トラフィックの 802.1Q-in-Q VLAN タギングを有効または無効にします。

config wlan apgroup qinq tagging eap-sim-aka *apgroup_name* {**enable** | **disable**}

クライアント トラフィックの 802.1Q-in-Q タギングを有効にすると、EAP for Authentication and Key Agreement（EAP-AKA）および EAP-SIM トラフィックの 802.1Q-in-Q タギング が有効になります。

ステップ 5 次のコマンドを入力して、802.1Q-in-Q VLAN タギングが有効かどうかを確認します。

show wlan apgroups

```
(Cisco Controller) >show wlan apgroups
Total Number of AP Groups..................... 5


Site Name..................................... CT_builing1
Site Description.............................. APs for CT Building1
Venue Group Code.............................. Unspecified
Venue Type Code............................... Unspecified

NAS-identifier................................ CTB1
Client Traffic QinQ Enable.................... TRUE
DHCPv4 QinQ Enable............................ TRUE
AP Operating Class............................ Not-configured
```

AP グループのキャプティブ ポータルの設定

この機能を使用すると、AP グループに基づき同じ SSID に対して、複数の Web 認証 URL（外部のキャプティブ URL を含む）を設定できます。デフォルトの設定では、グローバル URL が認証に使用されます。オーバーライド オプションは、WLAN および AP グループ レベルで使用できます。

優先順位は次のとおりです。

1. AP Group
2. WLAN
3. グローバル コンフィギュレーション

次の表に、コントローラに設定されているオーバーライド オプションに基づいた URL 認証マトリックスを示します。

表 *1* : オーバーライドの設定に基づいた認証 *URL*

WLAN レベルでグローバル	AP グループ レベルでグローバル	カスタム認証 URL
Enabled	Enabled	グローバルに設定されている URL
無効	イネーブル	WLAN に設定されている URL
イネーブル	無効	AP グループ レベルに設定されている URL
無効	ディセーブル	AP グループ レベルに設定されている URL

AP グループのキャプティブ ポータルの設定の制約事項

- この設定は、スタンドアロン コントローラでのみサポートされています。
- エクスポート アンカー設定はサポートされていません。

AP グループのキャプティブ ポータルの設定（GUI）

手順

ステップ 1 **[WLANs]** > **[Advanced]** > **[AP Groups]** の順に選択して、[AP Groups] ページを開きます。

ステップ 2 AP グループ名をクリックして、対応する **[AP Group]** > **[Edit]** ページを開きます。

ステップ 3 カスタム認証 web サイトを有効にする**カスタム Web オーバーライド-グローバル**のチェックボックスをオンにします。

（注） デフォルトの AP グループでこのオプションを有効にすることはできません。

ステップ 4 [External Web auth URL] フィールドに、認証 URL を入力します。

ステップ 5 設定を保存します。

AP グループのキャプティブ ポータルの設定（CLI）

手順

- 次のコマンドを入力して、 AP グループのカスタム Web を設定します。

  config wlan apgroup custom-web global *ap-groupname* {**enable | disable**}

- 次のコマンドを入力して、AP グループの外部 Web 認証 URL を設定します。

  config wlan apgroup custom-web ext-webauth-url { **add** *apgroupname ext web* 認証 *url* | **delete** *apgroupname*}

- 次のコマンドを入力して、WLAN の AP グループの設定を表示します。

  show wlan apgroups

- 次のコマンドを入力して、最大 10 クライアントのデバッグを有効にします。

  debug client *mac-addr*

- 次のコマンドを入力して、クライアントの Web 認証のリダイレクトのデバッグを有効または無効にします。

  debug web-auth redirect {**enable | disable**} **mac** *mac-addr*