CHAPTER 12

Hybrid REAP の設定

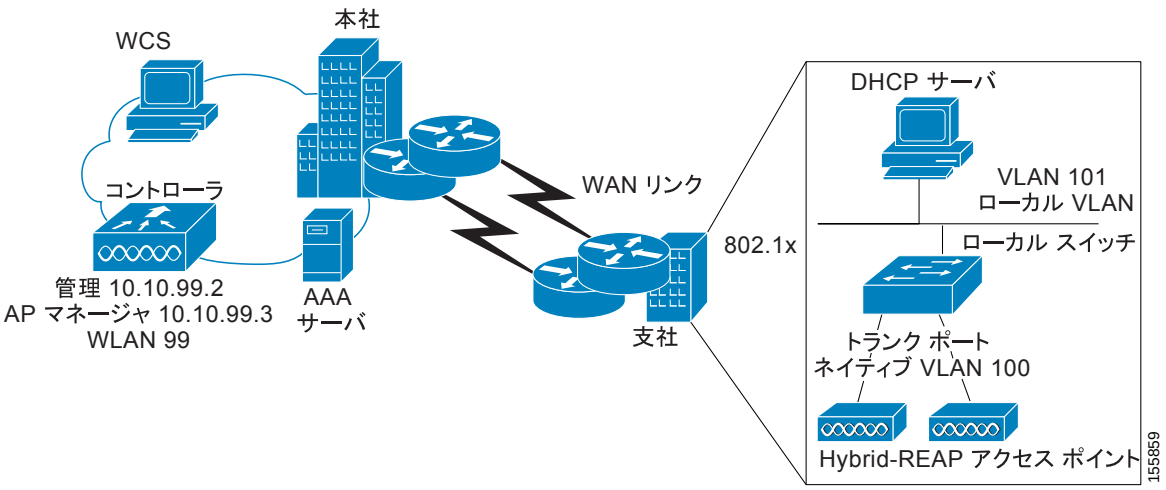
この章では、Hybrid REAP、およびこの機能をコントローラとアクセス ポイント上で設定する方法について説明します。この章の内容は、次のとおりです。

Hybrid REAP の概要

Hybrid REAP は、支社またはリモート オフィスでの展開のための無線ソリューションです。これにより顧客は、各オフィスでコントローラを展開することなく、本社オフィスから Wide Area Network（WAN; ワイドエリア ネットワーク）経由で、支社またはリモート オフィスのアクセス ポイントを設定および制御できるようになります。Hybrid REAP アクセス ポイントは、コントローラへの接続が失われた場合、クライアント データ トラフィックをローカルにスイッチして、ローカルにクライアント認証を行うことができます。コントローラに接続されているときには、トラフィックをコントローラに送り返すこともできます。

Hybrid REAP は、1130AG アクセス ポイントと 1240AG アクセス ポイント、2000 シリーズと 4400 シリーズのコントローラ、Catalyst 3750G 統合型無線 LAN コントローラ スイッチ、Cisco WiSM、およびサービス統合型ルータのコントローラ ネットワーク モジュールでのみサポートされます。図 12-1 は、一般的な Hybrid REAP 展開を示しています。

図 12-1　Hybrid REAP の展開



Hybrid REAP アクセス ポイントは、1 ロケーションにつき何台でも展開できます。ただし、帯域幅は最低でも 128 kbps を維持しながら、ラウンドトリップ遅延は 100 ミリ秒を超えてはならず、Maximum Transmission Unit（MTU; 最大伝送ユニット）は 500 バイトを下回ってはなりません。

Hybrid REAP の認証プロセス

Hybrid REAP アクセス ポイントがブートされると、コントローラを検索します。コントローラが見つかると、コントローラに接続し、最新のソフトウェア イメージと設定をコントローラからダウンロードして、無線を初期化します。スタンドアロン モードで使用するために、不揮発性メモリにダウンロードした設定を保存します。

Hybrid REAP アクセス ポイントは、次のいずれかの方法でコントローラの IP アドレスを認識できます。

- DHCP サーバからアクセス ポイントに IP アドレスが割り当てられている場合、通常の LWAPP ディスカバリ プロセス [レイヤ 3 ブロードキャスト、over-the-air provisioning（OTAP）、DNS、または DHCP オプション 43] を介してコントローラを発見できます。

（注）　OTAP は、購入後初のブート時には動作しません。

- アクセス ポイントに静的 IP アドレスが割り当てられている場合、DHCP オプション 43 以外の LWAPP ディスカバリ プロセス方法のいずれかを介して、コントローラを発見できます。アクセス ポイントで、レイヤ 3 ブロードキャストまたは OTAP を介してコントローラが見つからない場合、DNS 名前解決を使用することをお勧めします。DNS の場合、DNS サーバを認識している静的 IP アドレスを持つ任意のアクセス ポイントは、最低 1 つのコントローラを見つけることができます。
- LWAPP ディスカバリ メカニズムが使用可能でないリモート ネットワークからアクセス ポイントによりコントローラを見つける場合、プライミングを使用できます。この方法を使用すると、アクセス ポイントの接続先のコントローラを（アクセス ポイントの CLI により）指定できます。

（注）　アクセス ポイントがコントローラを見つける方法の詳細は、第 7 章または次の URL からアクセスできる『Controller Deployment Guide』を参照してください。
http://wnbu-tme/docs/Controller_DG_1.3_External.pdf

Hybrid REAP アクセス ポイントがコントローラに到達できるとき（接続モードと呼ばれます）、コントローラはクライアント認証を支援します。Hybrid REAP アクセス ポイントがコントローラにアクセスできないとき、アクセス ポイントはスタンドアロン モードに入り、独自にクライアントを認証します。

（注）　アクセス ポイント上の LED は、デバイスが異なる Hybrid REAP モードに入るときに変化します。LED パターンの情報については、アクセス ポイントのハードウェア インストール ガイドを参照してください。

クライアントが Hybrid REAP アクセス ポイントにアソシエートするとき、アクセス ポイントではすべての認証メッセージをコントローラに送信し、WLAN 設定に応じて、クライアント データ パケットをローカルにスイッチする（ローカル スイッチング）か、コントローラに送信（中央スイッチング）します。クライアント認証（オープン、共有、EAP、Web 認証、および NAC）とデータ パケットに関して、WLAN は、コントローラ接続の設定と状態に応じて、次のいずれかの状態になります。

- **中央認証、中央スイッチング**：コントローラがクライアント認証を処理し、すべてのクライアント データはコントローラにトンネルを通じて戻されます。この状態は接続モードでのみ有効です。
- **中央認証、ローカル スイッチング**：コントローラがクライアント認証を処理し、Hybrid REAP アクセス ポイントがデータ パケットをローカルにスイッチします。クライアントが認証に成功した後、コントローラは新しいペイロードと共に設定コマンドを送信し、Hybrid REAP アクセス ポイントに対して、ローカルにデータ パケットのスイッチを始めるように指示します。このメッセージはクライアントごとに送信されます。この状態は接続モードにのみ適用されます。
- **ローカル認証、ローカル スイッチング**：Hybrid REAP アクセス ポイントがクライアント認証を処理し、クライアント データ パケットをローカルにスイッチします。この状態はスタンドアロン モードでのみ有効です。
- **認証ダウン、スイッチング ダウン**：WLAN が既存クライアントをアソシエート解除し、ビーコン応答とプローブ応答の送信を停止します。この状態はスタンドアロン モードでのみ有効です。
- **認証ダウン、ローカル スイッチング**：WLAN が認証を試みる新しいクライアントをすべて拒否しますが、既存クライアントを保持するために、ビーコン応答とプローブ応答を送信し続けます。この状態はスタンドアロン モードでのみ有効です。

Hybrid REAP アクセス ポイントがスタンドアロン モードに入ると、オープン、共有、WPA-PSK、または WPA2-PSK 認証に対して設定されている WLAN は、「ローカル認証、ローカル スイッチング」状態に入り、新しいクライアント認証を続行します。その他の WLAN は、「認証ダウン、スイッチング ダウン」状態（WLAN が中央スイッチングに対して設定されている場合）または「認証ダウン、ローカル スイッチング」状態（WLAN がローカル スイッチングに対して設定されている場合）のいずれかに入ります。

Hybrid REAP アクセス ポイントがスタンドアロン モードに入ると、中央でスイッチされる WLAN 上にあるすべてのクライアントをアソシエート解除します。802.1x または Web 認証 WLAN の場合、既存クライアントはアソシエート解除されませんが、Hybrid REAP アクセス ポイントはアソシエートされているクライアントの数がゼロ（0）に達すると、ビーコン応答の送信を停止します。また、802.1x または Web 認証 WLAN にアソシエートしている新しいクライアントにアソシエート解除メッセージを送信します。802.1x 認証、NAC、および Web 認証（ゲスト アクセス）などのコントローラ依存アクティビティは無効化され、アクセス ポイントからコントローラに Intrusion Detection System（IDS; 侵入検知システム）レポートは送信されません。さらに、ほとんどの Radio Resource Management（RRM）機能（ネイバー ディスカバリ、ノイズ、干渉、ロード、およびカバレッジ測定、ネイバー リストの使用、不正阻止および検出）は無効化されます。ただし、Hybrid REAP アクセス ポイントは、スタンドアロン モードで動的周波数選択をサポートします。

（注） コントローラが、Network Access Control(NAC; ネットワーク アクセス コントロール) に対して設定されている場合、クライアントはアクセス ポイントが接続モードにある場合にのみアソシエートできます。NAC が有効化されている場合、正常に動作しない（または検疫された）VLAN を作成する必要があります。これは、WLAN がローカル スイッチングに対して設定されている場合でも VLAN に割り当てられている任意のクライアントのデータ トラフィックがコントローラを経由するようにするためです。クライアントが検疫 VLAN に割り当てられると、クライアントのすべてのデータ パケットは中央でスイッチされます。検疫 VLAN の作成については、「動的インターフェイスの設定」の項（P. 3-18）を参照してください。

Hybrid REAP アクセス ポイントは、スタンドアロン モードに入った後も、クライアントの接続を維持します。ただし、アクセス ポイントがコントローラとの接続を再確立すると、すべてのクライアントをアソシエート解除して、コントローラからの新しい設定情報を適用し、クライアントの接続を再度許可します。

Hybrid REAP のガイドライン

Hybrid REAP を使用するときには、次の点に留意してください。

- Hybrid REAP アクセス ポイントは、静的 IP アドレスまたは DHCP アドレスのいずれかで展開できます。DHCP の場合、DHCP サーバはローカルに使用可能であり、ブート時にアクセス ポイントの IP アドレスを提供できる必要があります。
- Hybrid REAP は最大で 4 つの断片化されたパケット、または最低 500 バイトの Maximum Transmission Unit（MTU; 最大伝送ユニット）WAN リンクをサポートします。
- ラウンドトリップ遅延は、アクセス ポイントとコントローラ間で 100 ミリ秒（ms）を超えてはならず、LWAPP コントロール パケットはすべてのその他のトラフィックよりも優先される必要があります。
- コントローラはユニキャスト パケットまたはマルチキャスト パケットの形式でアクセス ポイントにマルチキャスト パケットを送信できます。Hybrid REAP モードで、アクセス ポイントはユニキャスト形式でのみマルチキャスト パケットを受信できます。
- Hybrid REAP は CCKM 完全認証をサポートしますが、CCKM 高速ローミングはサポートしません。
- Hybrid REAP は 1 対 1 の Network Address Translation（NAT; ネットワ ーク アドレス変換）設定をサポートします。また、真のマルチキャストを除くすべての機能に対して、Port Address Translation（PAT; ポート アドレス変換) をサポートします。マルチキャストは、ユニキャスト オプションを使用して設定する場合、NAT 境界全体にわたってサポートされます。
- VPN、PPTP、Fortress 認証、および Cranite 認証は、これらのセキュリティ タイプがアクセス ポイントでローカルにアクセス可能であれば、ローカルにスイッチされるトラフィックに対してサポートされます。
- Hybrid-REAP アクセス ポイントは、複数の SSID をサポートします。詳細は、「CLI を使用して WLAN を作成するには、次のコマンドを使用します。」の項（P. 6-5）を参照してください。

Hybrid REAP の設定

Hybrid REAP を設定するには、提供される順に次の項の指示に従ってください。

リモート サイトでのスイッチの設定

リモート サイトでスイッチを準備する手順は、次のとおりです。

ステップ 1　スイッチ上のトランクまたはアクセス ポートに、Hybrid REAP に対して有効化されるアクセス ポイントを接続します。

（注）　次の設定例は、スイッチ上のトランクに接続されている Hybrid REAP アクセス ポイントを示します。

ステップ 2　Hybrid REAP アクセス ポイントをサポートするようにスイッチを設定するには、次の設定例を参照してください。

この設定例では、Hybrid REAP アクセス ポイントは、ネイティブ VLAN 100 でトランク インターフェイス FastEthernet 1/0/2 に接続されています。アクセス ポイントは、ネイティブ VLAN 上で IP 接続を必要とします。リモート サイトには、VLAN 101 上にローカル サーバとリソースがあります。スイッチ内の両方の VLAN に対して、DHCP プールがローカル スイッチ内に作成されます。最初の DHCP プール（ネイティブ）は、Hybrid REAP アクセス ポイントによって使用され、2 番目の DHCP プール（ローカル スイッチ）は、ローカルにスイッチされている WLAN にアソシエートするときにクライアントによって使用されます。設定例の太字のテキストは、これらの設定を示します。

（注）　この設定例のアドレスは、図示のみを目的としています。使用するアドレスは、アップストリーム ネットワークに収まる必要があります。

ローカル スイッチ設定例：

```
ip dhcp pool NATIVE
   network 10.10.100.0 255.255.255.0
   default-router 10.10.100.1
!
ip dhcp pool LOCAL-SWITCH
   network 10.10.101.0 255.255.255.0
   default-router 10.10.101.1
!
interface FastEthernet1/0/1
 description Uplink port
 no switchport
 ip address 10.10.98.2 255.255.255.0
 spanning-tree portfast
!
interface FastEthernet1/0/2
 description the Access Point port
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 100
 switchport trunk allowed vlan 100,101
 switchport mode trunk
 spanning-tree portfast
!
interface Vlan100
 ip address 10.10.100.1 255.255.255.0
 ip helper-address 10.10.100.1
!
interface Vlan101
 ip address 10.10.101.1 255.255.255.0
 ip helper-address 10.10.101.1
end
```

Hybrid REAP に対するコントローラの設定

この項では、GUI または CLI を使用して Hybrid REAP コントローラを設定する手順について説明します。

GUI を使用した、Hybrid REAP に対するコントローラの設定

Hybrid REAP のコントローラの設定には、中央でスイッチされる WLAN とローカルにスイッチされる WLAN を作成する操作が含まれます。GUI を使用してこれらの WLAN のコントローラを設定するには、この項の手順に従ってください。この手順では、次の 3 つの WLAN を例として使用します。

WLAN	Security	スイッチング	インターフェイス マッピング（VLAN）
employee	WPA1+WPA2	中央	management（中央でスイッチされる VLAN）
employee-local	WPA1+WPA2 (PSK)	Local	101（ローカルにスイッチされる VLAN）
guest-central	Web 認証	中央	management（中央でスイッチされる VLAN）

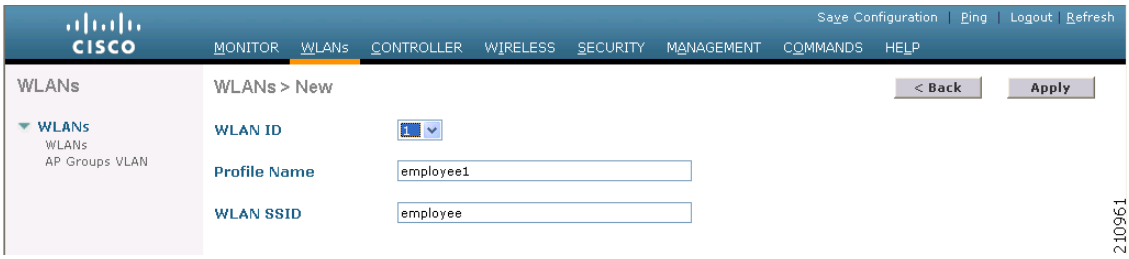
（注）　CLI を使用して Hybrid REAP のコントローラを設定する場合は、「CLI による Hybrid REAP のコントローラの設定」の項（P. 12-10）を参照してください。

ステップ 1　中央でスイッチされる WLAN を作成する手順は次のとおりです。例では、これは最初の WLAN（employee）です。

a. **WLANs** をクリックして、WLANs ページにアクセスします。

b. **New** をクリックして、WLANs > New ページにアクセスします（図 12-2 を参照）。

図 12-2　WLANs > New ページ

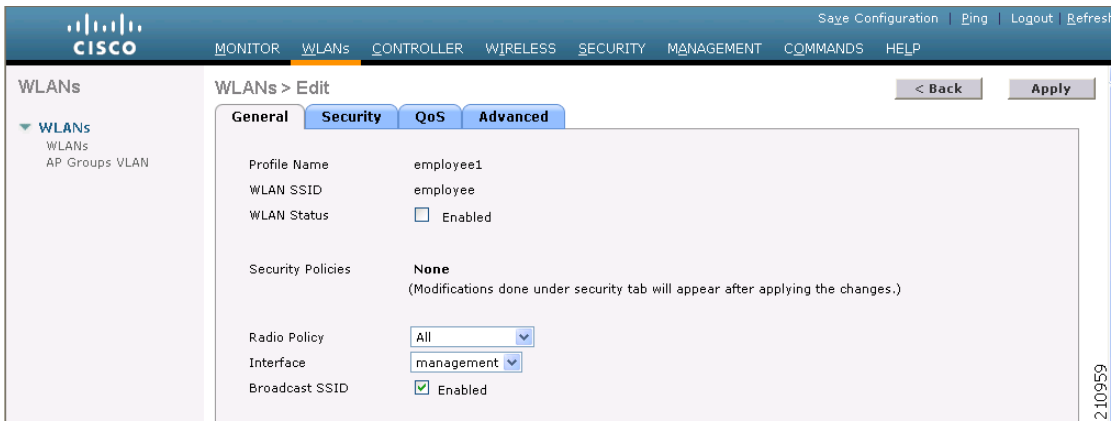


c. Profile Name フィールドで、WLAN に一意のプロファイル名を付けます。

d. WLAN SSID フィールドに WLAN の名前を入力します。

e. **Apply** をクリックして、変更を適用します。WLANs > Edit ページが表示されます（図 12-3 を参照）。

図 12-3　WLANs > Edit ページ



f. WLANs タブ > Edit タブの各設定から、この WLAN に対する設定パラメータを変更します。employee WLAN の例では、Security タブ > Layer 2 タブから Layer 2 Security に **WPA1+WPA2** を選択してから、WPA1+WPA2 パラメータを設定する必要があります。

（注）　General タブの **WLAN Status** チェックボックスをオンすることにより、この WLAN を有効化することを確認してください。

（注）　NAC が有効化されているときに、検疫 VLAN を作成し、この WLAN に対して検疫 VLAN を使用する場合には、General タブの Interface ドロップダウン ボックスから選択することを確認してください。また、Advanced タブの **Allow AAA Override** チェックボックスをオンにして、コントローラが検疫 VLAN 割り当てをチェックするように確認してください。

g. **Apply** をクリックして、変更を適用します。

h. **Save Configuration** をクリックして、変更内容を保存します。

ステップ 2　ローカルにスイッチされる WLAN を作成する手順は次のとおりです。例では、これは 2 番目の WLAN（employee-local）です。

a. ステップ 1 のサブステップに従って、新しい WLAN を作成します。例では、この WLAN には「employee-local」という名前が付けられています。

b. WLANs > Edit ページが表示されたら、この WLAN に対する設定パラメータを変更します。employee WLAN の例では、Security タブ > Layer 2 タブから Layer 2 Security に **WPA1+WPA2** を選択してから、WPA1+WPA2 パラメータを設定する必要があります。PSK 認証キー管理を選択して、事前共有キーを入力することを確認してください。

（注）　General タブの **WLAN Status** チェックボックスをオンすることにより、この WLAN を有効化することを確認してください。さらに、Advanced タブの **H-REAP Local Switching** チェックボックスをオンにして、ローカル スイッチングを確実に有効化してください。ローカル スイッチングを有効化すると、この WLAN をアドバタイズするすべての Hybrid REAP アクセス ポイントは、データ パケットを（コントローラへトンネリングする代わりに）ローカルにスイッチできます。

（注）　Hybrid REAP アクセス ポイントの場合、H-REAP ローカル スイッチングに対して設定されている WLAN のコントローラでのインターフェイス マッピングは、デフォルト VLAN タギングとしてアクセス ポイントで継承されます。これは、SSID 別、Hybrid REAP アクセス ポイント別に容易に変更できます。Hybrid REAP 以外のアクセス ポイントでは、すべてのトラフィックがコントローラへトンネリングで戻され、VLAN タギングは各 WLAN のインターフェイス マッピングによって要求されます。

c. **Apply** をクリックして、変更を適用します。

d. **Save Configuration** をクリックして、変更内容を保存します。

ステップ 3　ゲスト アクセスに使用される中央スイッチの WLAN も作成する場合は、次の手順に従ってください。例では、これは 3 番目の WLAN（guest-central）です。中央サイトからの保護されていないゲスト トラフィックに対する企業データ ポリシーを施行できるように、ゲスト トラフィックをコントローラにトンネリングする必要のある場合があります。

（注）　第 9 章は、ゲスト ユーザー アカウントの作成に関する詳細について説明します。

a. ステップ 1 のサブステップに従って、新しい WLAN を作成します。例では、この WLAN には「employee-local」という名前が付けられています。

b. WLANs > Edit ページが表示されたら、この WLAN に対する設定パラメータを変更します。employee WLAN の例では、Security > Layer 2 タブと Security > Layer 3 タブから Layer 2 Security および Layer 3 Security の両方に **None** を選択し、**Web Policy** チェックボックスをオンにして、Layer 3 タブで **Authentication** が選択されていることを確認する必要があります。

（注）　外部 Web サーバを使用している場合には、WLAN 上でサーバに対する事前認証 Access Control List （ACL; アクセス コントロール リスト）を設定し、Layer 3 タブでこの ACL を WLAN 事前認証 ACL として選択する必要があります。ACL の詳細は、第 5 章を参照してください。

（注）　General タブの **WLAN Status** チェックボックスをオンすることにより、この WLAN を有効化することを確認してください。

c. **Apply** をクリックして、変更を適用します。

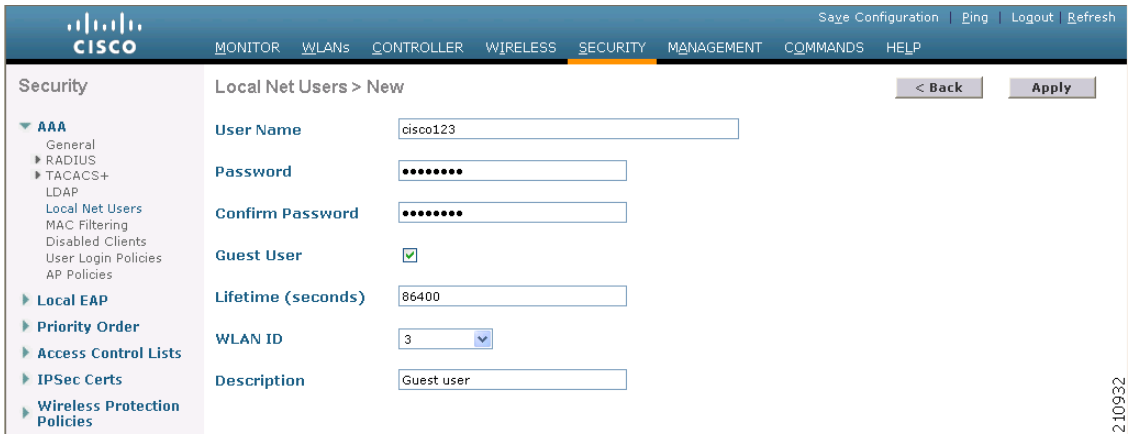
d. **Save Configuration** をクリックして、変更内容を保存します。

e. ゲスト ユーザがこの WLAN に初めてアクセスするときに表示されるログイン ページのコンテンツと外観をカスタマイズする場合は、第 5 章の指示に従ってください。

f. この WLAN にローカル ユーザを追加するには、**Security** > **AAA** > **Local Net Users** をクリックしてください。

g. Local Net Users ページが表示されたら、**New** をクリックします。Local Net Users > New ページが表示されます（図 12-4 を参照）。

図 12-4　Local Net Users > New ページ



h. User Name フィールドと Password フィールドに、ローカル ユーザのユーザ名とパスワードを入力します。

i. Confirm Password フィールドに、パスワードを再度入力します。

j. **Guest User** チェックボックスをオンにして、このローカル ユーザ アカウントを有効にします。

k. Lifetime フィールドに、このユーザ アカウントをアクティブにする時間（秒数）を入力します。

l. WLAN ID フィールドに、ローカル ユーザによってアクセスされる WLAN の数を入力します。

m. Description フィールドに、ローカル ユーザを説明するタイトル（「ゲスト ユーザ」など）を入力します。

n. **Apply** をクリックして、変更を適用します。

o. **Save Configuration** をクリックして、変更内容を保存します。

ステップ 4　「Hybrid REAP のアクセス ポイントの設定」の項（P. 12-11）へ移動して、Hybrid REAP に対する最大 6 台までのアクセス ポイントを設定します。

CLI による Hybrid REAP のコントローラの設定

次のコマンドを使用して、Hybrid REAP のコントローラを設定します。

- **config wlan h-reap local-switch** <WLAN ID> **disable**：中央スイッチングに対して WLAN を設定します。
- **config wlan h-reap local-switch** <WLAN ID> **disable**：中央スイッチングに対して WLAN を設定します。これはデフォルト値です。

（注）　「Hybrid REAP のアクセス ポイントの設定」の項（P. 12-11）へ移動して、Hybrid REAP に対する最大 6 台までのアクセス ポイントを設定します。

次のコマンドを使用して、Hybrid REAP 情報を取得します。

- **show ap config general** *Cisco_AP*：VLAN 設定を表示します。
- **show wlan wlan_id**：WLAN がローカルにスイッチされているか、中央でスイッチされているかを表示します。
- **show client detail** *client_mac*：クライアントがローカルにスイッチされているか、中央でスイッチされているかを表示します。

次のコマンドを使用して、デバッグ情報を取得します。

- **debug lwapp events enable**：LWAPP イベントに関するデバッグ情報を提供します。
- **debug lwapp error enable**：LWAPP エラーに関するデバッグ情報を提供します。
- **debug pem state enable**：Policy Manager ステート マシンに関するデバッグ情報を提供します。
- **debug pem events enable**：Policy Manager イベントに関するデバッグ情報を提供します。
- **debug dhcp packet enable**：DHCP パケットに関するデバッグ情報を提供します。
- **debug dhcp message enable**：DHCP エラー メッセージに関するデバッグ情報を提供します。.

Hybrid REAP のアクセス ポイントの設定

この項では、コントローラの GUI または CLI を使用して Hybrid REAP のアクセス ポイントを設定する手順について説明します。

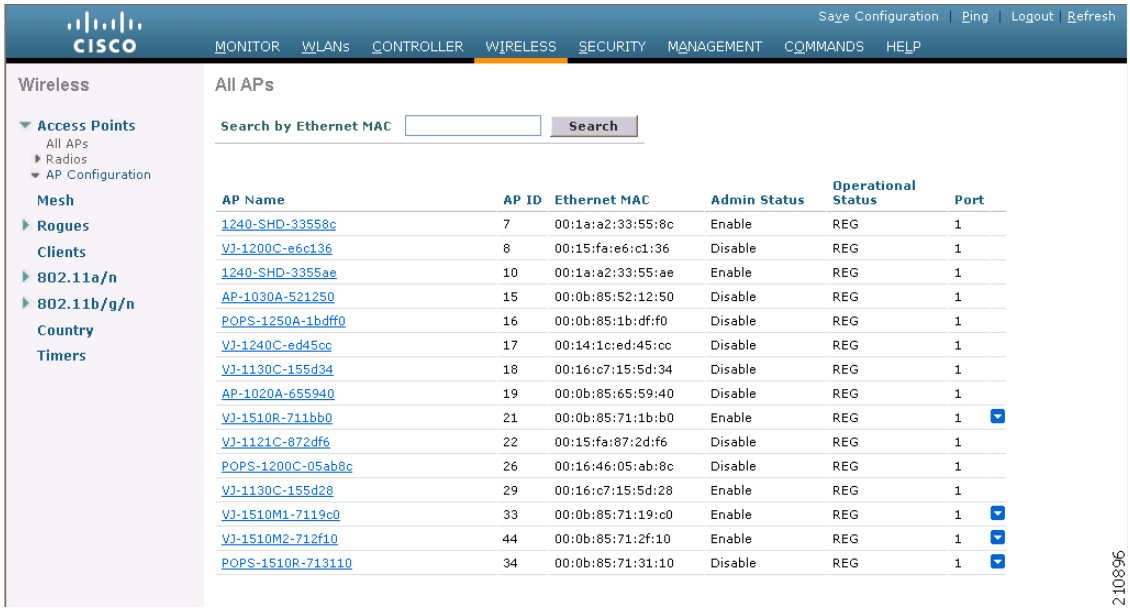
GUI を使用した Hybrid REAP のアクセス ポイントの設定

コントローラの GUI を使用して Hybrid REAP のアクセス ポイントを設定する手順は、次のとおりです。

ステップ 1　アクセス ポイントが物理的にネットワークに追加されていることを確認します。

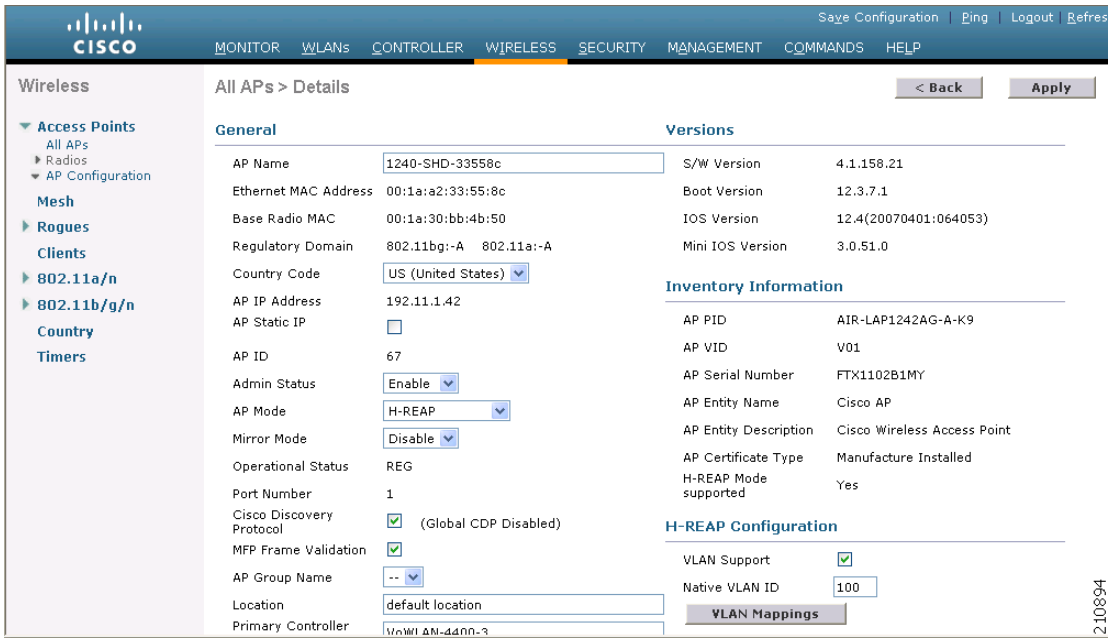
ステップ 2　**Wireless** をクリックして、All APs ページにアクセスします（図 12-5 を参照）。

図 12-5　All APs ページ



ステップ 3　目的のアクセス ポイントの名前をクリックします。All APs > Details ページが表示されます（図 12-6 を参照）。

図 12-6　All APs > Details ページ



Inventory Information の下の最後のパラメータは、このアクセス ポイントを Hybrid REAP に対して設定できるかどうかを示します。1130AG アクセス ポイントと 1240AG アクセス ポイントのみが、Hybrid REAP をサポートします。

ステップ 4　このアクセス ポイントに対して Hybrid REAP を有効化するには、AP Mode ドロップダウン ボックスから **H-REAP** を選択します。

ステップ 5　**Apply** をクリックして変更を適用し、アクセス ポイントをリブートさせます。

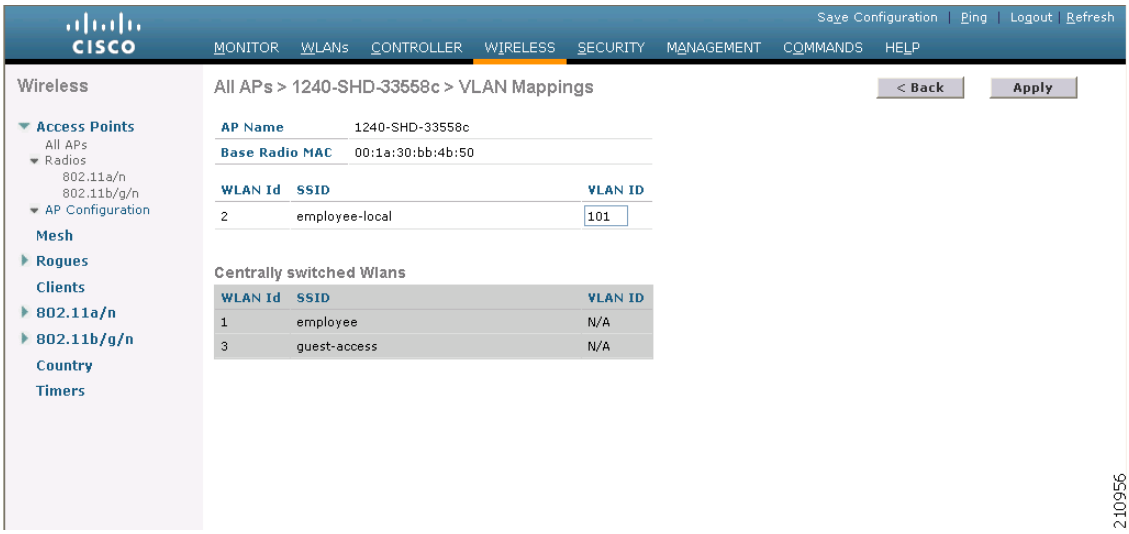
ステップ 6　H-REAP Configuration の下で、**VLAN Support** チェックボックスをオンにし、**Native VLAN ID** フィールドに、リモート ネットワーク上のネイティブ VLAN の数（100 など）を入力します。

（注）　デフォルトで、VLAN は Hybrid REAP アクセス ポイント上では有効化されていません。Hybrid REAP が有効化されると、アクセス ポイントは WLAN にアソシエートされている VLAN ID を継承します。この設定はアクセス ポイントで保存され、接続応答が成功した後に受信されます。デフォルトで、ネイティブ VLAN は 1 です。VLAN が有効化されたドメインで、Hybrid REAP アクセス ポイントごとにネイティブ VLAN を 1 つ設定する必要があります。そうしないと、アクセス ポイントはコントローラとのパケットの送受信ができません。

ステップ 7　**Apply** をクリックして、変更を適用します。イーサネット ポートがリセットされる間、アクセス ポイントは一時的にコントローラへの接続を失います。

ステップ 8　**VLAN Mappings** をクリックして、All APs > *Access Point Name* > VLAN Mappings ページにアクセスします（図 12-7 を参照）。

図 12-7　All APs > Access Point Name > VLAN Mappings ページ



ステップ 9　ローカル スイッチング（この例では、VLAN 101）を行っているときにクライアントが IP アドレスを取得する VLAN の数を VLAN ID フィールドに入力します。

ステップ 10　**Apply** をクリックして、変更を適用します。

ステップ 11　**Save Configuration** をクリックして、変更内容を保存します。

ステップ 12　リモート サイトで、Hybrid REAP に対して設定する必要があるすべての追加のアクセス ポイントについて、この手順を繰り返します。

CLI を使用した Hybrid REAP に対するアクセス ポイントの設定

次のコマンドを使用して、Hybrid REAP に対するアクセス ポイントを設定します。

- **config ap mode h-reap** *Cisco_AP*：このアクセス ポイントに対する Hybrid REAP を有効化します。
- **config ap h-reap vlan wlan** <WLAN ID> <VLAN ID> *Cisco_AP*：VLAN ID をこの Hybrid REAP アクセス ポイントに割り当てることができます。デフォルトで、アクセス ポイントは WLAN にアソシエートされている VLAN ID を継承します。
- **config ap h-reap vlan** {**enable** | **disable**} *Cisco_AP*：この Hybrid REAP アクセス ポイントに対して VLAN タギングを有効化または無効化します。デフォルトで、VLAN タギングは有効化されていません。VLAN タギングが Hybrid REAP アクセス ポイント上で有効化されると、ローカル スイッチングに対する WLAN は、コントローラで割り当てられている VLAN を継承します。
- **config ap h-reap vlan wlan** <VLAN ID> *Cisco_AP*：この Hybrid REAP アクセス ポイントに対するネイティブ VLAN を設定できます。デフォルトで、VLAN はネイティブ VLAN に設定されています。（VLAN タギングが有効化されているとき）Hybrid REAP アクセス ポイントごとにネイティブ VLAN を 1 つ設定する必要があります。アクセス ポイントが接続されているスイッチポートに、対応するネイティブ VLAN も設定されていることを確認します。Hybrid REAP アクセス ポイントのネイティブ VLAN 設定と、アップストリーム スイッチポートのネイティブ VLAN が一致しない場合、アクセス ポイントではコントローラとの間のパケット送受信ができません。

Hybrid REAP アクセス ポイント上で次のコマンドを使用して、ステータス情報を取得します。

- **show lwapp reap status**：Hybrid REAP アクセス ポイントのステータス（connected または standalone）を表示します。
- **show lwapp reap association**：このアクセス ポイントおよび SSID にアソシエートされているクライアントのリストを表示します。

Hybrid REAP アクセス ポイント上で次のコマンドを使用して、デバッグ情報を取得します。

- **debug lwapp reap**：一般的な Hybrid REAP アクティビティを表示します。
- **debug lwapp reap mgmt**：クライアント認証メッセージとアソシエーション メッセージを表示します。
- **debug lwapp reap load**：Hybrid REAP アクセス ポイントがスタンドアロン モードでブートされるときに役立つ、ペイロード アクティビティを表示します。
- **debug dot11 mgmt interface**：802.11 管理インターフェイス イベントを表示します。
- **debug dot11 mgmt msg**：802.11 管理メッセージを表示します。
- **debug dot11 mgmt ssid**：SSID 管理イベントを示します。
- **debug dot11 mgmt state-machine**：802.11 ステート マシンを表示します。
- **debug dot11 mgmt station**：クライアント イベントを表示します。

クライアント デバイスの WLAN への接続

「Hybrid REAP に対するコントローラの設定」の項（P. 12-6）で作成した WLAN に接続するためのプロファイルを作成するには、クライアント デバイスで次の手順に従ってください。

例では、クライアント上で 3 つプロファイルを作成することになります。

1. 「employee」WLAN へ接続するには、PEAP-MSCHAPV2 認証で WPA/WPA2 を使用するクライアント プロファイルを作成します。クライアントは認証されると、コントローラの管理 VLAN から IP アドレスを取得します。
2. 「local-employee」WLAN へ接続するには、WPA/WPA2-PSK 認証を使用するクライアント プロファイルを作成します。クライアントは認証されると、ローカル スイッチ上の VLAN 101 から IP アドレスを取得します。
3. 「guest-central」WLAN へ接続するには、オープン認証を使用するクライアント プロファイルを作成します。クライアントは認証されると、アクセス ポイントにとってローカルのネットワーク上にある VLAN 101 から、IP アドレスを取得します。クライアントが接続すると、ローカル ユーザは、Web ブラウザに任意の http アドレスを入力できます。ユーザは、Web 認証プロセスを完了するために、自動的にコントローラへダイレクトされます。Web ログイン ページが表示されると、ユーザはユーザ名とパスワードを入力します。

クライアントのデータ トラフィックがローカルに、または中央でスイッチされていることを確認するには、コントローラの GUI で、**Monitor** > **Clients** をクリックし、必要なクライアントの **Detail** リンクをクリックして、AP Properties の下の Data Switching パラメータを確認します。