ワイヤレス ネットワークの作成

WLAN

Cisco Mobility Express ソリューションは最大 16 個の WLAN をサポートします。各 WLAN には、一意の WLAN ID（1 ～ 16）、一意のプロファイル名、SSID が割り当てられます。また、異なるセキュリティ ポリシーを割り当てることもできます。

アクセス ポイントは、すべてのアクティブな WLAN SSID をブロードキャストし、WLAN ごとに定義するポリシーを適用します。

Cisco Mobility Express ソリューションでは、いくつかの WLAN セキュリティ オプションがサポートされます。主なオプションは次のとおりです。

1. Open
2. WPA2 パーソナル

3. WPA2 エンタープライズ（外部 RADIUS、AP）

ゲスト WLAN については、いくつかの機能がサポートされます。

1. CMX ゲスト接続
2. WPA2 パーソナル
3. キャプティブ ポータル（AP）
4. キャプティブ ポータル（外部 Web サーバ）

従業員 WLAN の作成

WPA2 パーソナルを使用した従業員 WLAN の作成

手順

ステップ 1 [Wireless Settings] > [WLANs] に移動してから、[Add new WLAN] ボタンをクリックします。[Add new WLAN] ウィンドウがポップアップ表示されます。

ステップ 2 [Add new WLAN] ウィンドウの [General] ページで、以下を設定します。

a) **プロファイル名**を入力します。
b) **SSID** を入力します。

ステップ 3 [WLAN Security] をクリックし、以下を設定します。

a) [Security] で *WPA2* パーソナルを選択します。
b) **パスフレーズ**を入力し、**パスフレーズ** を確認します。

ステップ 4 [Apply] をクリックします。

WPA2 エンタープライズおよび外部 RADIUS サーバを使用した従業員 WLAN の作成

手順

ステップ 1 [Wireless Settings] > [WLANs] に移動して、[Add new WLAN] ボタンをクリックします。[Add new WLAN] ウィンドウがポップアップ表示されます。

ステップ 2 [Add new WLAN] ウィンドウの [General] ページで、以下を設定します。

a) **プロファイル名**を入力します。

b) **SSID** を入力します。

ステップ 3 [WLAN Security] をクリックし、以下を設定します。

a) [Security Type] で **WPA2 エンタープライズ**を選択します。

b) [Authentication Server] で**[External Radius]** を選択します。

ステップ 4 RADIUS サーバを追加し、以下を設定します。

- RADIUS IP を入力します
- RADIUS ポートを入力します
- Shared Secret を入力します
- [tick] アイコンをクリックします

ステップ 5 [Apply] をクリックします。

WPA2エンタープライズおよび認証サーバとしてAPを使用した従業員WLANの作成

手順

ステップ 1 [Wireless Settings] > [WLANs] に移動して、[Add new WLAN] ボタンをクリックします。[Add new WLAN] ウィンドウがポップアップ表示されます。

ステップ 2 [Add new WLAN] ウィンドウの [General] ページで、以下を設定します。

a) **プロファイル名**を入力します。

b) **SSID** を入力します。

ステップ 3 [WLAN Security] をクリックし、以下を設定します。

a) [Security] で **WPA2 エンタープライズ**を選択します。

b) [Authentication Server] で **AP** を選択します。

（注） APは、コントローラ機能を実行しているマスターAPです。この使用例では、コントローラは認証サーバであるため、ローカル WLAN ユーザ アカウントは、クライアントの接続するコントローラに存在する必要があります。

ステップ 4 [Apply] をクリックします。

WPA2 エンタープライズ/外部 RADIUS および MAC フィルタリングを使用した従業員 WLAN の作成

手順

ステップ 1 [Wireless Settings] > [WLANs] に移動して、[Add new WLAN] ボタンをクリックします。[Add new WLAN] ウィンドウがポップアップ表示されます。

ステップ 2 [Add new WLAN] ウィンドウの [General] タブで、以下を設定します。

- **プロファイル名**を入力します。
- **SSID** を入力します。

ステップ 3 [WLAN Security] タブをクリックし、以下を設定します。

- [MAC Filtering] を有効にします
- [Security Type] で [WPA2 Enterprise] を選択します。
- [Authentication Server] で [External RADIUS] を選択します。
- ドロップダウン リストから [RADIUS Compatibility] を選択します
- ドロップダウン リストから [MAC Delimiter] を選択します

ステップ 4 RADIUS サーバを追加し、以下を設定します。

- **RADIUS IP** を入力します
- **RADIUS ポート**を入力します
- **Shared Secret** を入力します
- [tick] アイコンをクリックします。

ステップ 5 [Apply] をクリックします。

WLAN でのセントラル Web 認証サポート

ユーザは Web 認証 SSID に接続します。実際にはオープンな MAC フィルタリングであり、レイヤ 3 セキュリティではありません。

1. ユーザがブラウザを開きます。
2. WLC がゲスト ポータルにリダイレクトします。
3. ユーザがポータルで認証されます。

4. ISEが、ユーザが有効であることをコントローラに示すためのRADIUS認可変更（CoA-UDP ポート 1700）を送信し、最終的にアクセス コントロール リスト（ACL）などの RADIUS 属性をプッシュします。

WLAN でのセントラル Web 認証サポート

セントラル Web 認証を使用すると、ゲスト ユーザは、ポータルにリダイレクトされてからデバイス登録やセルフプロビジョニングを実施することで、ネットワークにアクセスできるようになります。CWA のフローには、次の処理が含まれます。

1. ユーザはWeb認証SSIDに接続します。実際にはオープンなMACフィルタリングであり、レイヤ 3 セキュリティではありません。
2. ユーザがブラウザを開きます。
3. WLC がゲスト ポータルにリダイレクトします。
4. ユーザがポータルで認証されます。
5. ISEが、ユーザが有効であることをコントローラに示すためのRADIUS認可変更（CoA-UDP ポート 1700）を送信し、最終的にアクセス コントロール リスト（ACL）などの RADIUS 属性をプッシュします。

セントラル Web 認証方式の WLAN を作成するには、次の手順に従います。

手順

ステップ 1 [Wireless Settings] > [WLANs] に移動し、[Add new WLAN/RLAN] をクリックします。

ステップ 2 [Security Type] で [Central Web Auth] を選択します。

ステップ 3 [Add the RADIUS Authentication Server] をクリックし、デバイス登録用のポータルをホストしているサーバを追加します。

ステップ 4 [Apply] をクリックします。

（注） CWA WLAN 作成の一環として、事前認証 ACL が自動的に作成され、AAA オーバーライド、CoA、ISE NAC が WLAN で有効になります。

（注） CWA を機能させるには、さらに ISE を設定する必要があります。

ゲスト WLAN の作成

Cisco Mobility Express コントローラは、ゲスト ユーザ専用の WLAN でゲスト ユーザ アクセスを提供できます。WLANをゲストユーザアクセス専用に設定するために、[WLAN Security] タブの下の [Guest Network] を有効にします。

CMX Connect のキャプティブ ポータルを使用したゲスト WLAN の作成

手順

ステップ 1 [Wireless Settings] > [WLANs] に移動して、[Add new WLAN] ボタンをクリックします。[Add new WLAN] ウィンドウがポップアップ表示されます。

ステップ 2 [Add new WLAN] ウィンドウの [General] タブで、以下を設定します。

- **プロファイル名**を入力します。
- **SSID** を入力します。

ステップ 3 [WLAN Security] タブの下の [Guest Network] を有効にします。

ステップ 4 [Captive Portal] で **CMX Connect** を選択します。

ステップ 5 **キャプティブ ポータルの URL** を入力します。

（注） キャプティブ ポータルの URL は、https://yya7lc.cmxcisco.com/visitor/login 形式にする必要があります。**yya7lc** は CMX Cloud のアカウント ID です。

ステップ 6 [Apply] をクリックします。

（注） 追加の手順が、キャプティブ ポータル、アクセス ポイントがあるサイトおよびサイトに関連付けられているキャプティブ ポータルを作成するために CMX Cloud 側で必要です。

内部スプラッシュ ページを使用したゲスト WLAN の作成

ゲスト WLAN に接続しているクライアントのオンボードに使用できる Mobility Express コントローラにビルトインされた内部スプラッシュ ページがあります。この内部スプラッシュ ページでは、カスタマイズされたバンドルをアップロードしてページをカスタマイズすることもできます。カスタマイズされた内部スプラッシュ ページをアップロードするには、[Wireless Settings] > [Guest WLANs] に移動します。[Page Type] で **[Customized]** を選択し、[Upload] ボタンをクリックして、カスタマイズされたページのバンドルをアップロードします。

内部スプラッシュ ページのために、Cisco Mobility Express は**アクセス タイプ**の複数のオプションをサポートします。サポートされているアクセス タイプは次のとおりです。

1. ローカル ユーザ アカウント
2. Web 許諾
3. 電子メール アドレス
4. RADIUS
5. WPA2 パーソナル

手順

ステップ 1 [Wireless Settings] > [WLANs] に移動して、[Add new WLAN] ボタンをクリックします。[Add new WLAN] ウィンドウがポップアップ表示されます。

ステップ 2 [Add new WLAN] ウィンドウの [General] タブで、以下を設定します。

- プロファイル名を入力します。
- SSID を入力します。

ステップ 3 [WLAN Security] タブの下の [Guest Network] を有効にします。

ステップ 4 [Captive Portal] で**内部スプラッシュ ページ**を選択します。

ステップ 5 必要に応じて、次の**アクセス タイプ**のうちの 1 つを選択します。

1. **ローカル ユーザ アカウント**：スプラッシュ ページは、ネットワーク アクセスを許可する前に、コントローラによって認証する必要があるユーザ名とパスワードの入力をユーザに表示します。ローカル WLAN ユーザは、ゲスト クライアントが接続するコントローラで作成する必要があります。
2. **Web 許諾**：スプラッシュ ページは、ネットワーク アクセスが許可される前に許諾をユーザに表示します。
3. **電子メール アドレス**：スプラッシュ ページは、ネットワーク アクセスが許可される前に電子メール アドレスの入力をユーザに表示します。
4. **RADIUS**：スプラッシュ ページは、ネットワーク アクセスが許可される前に RADIUS サーバで認証する必要があるユーザ名とパスワードの入力をユーザに表示します。[Access Type] で **RADIUS** を選択し、RADIUS サーバの設定を入力します。
5. **WPA2 パーソナル**：これは、L2 + L3 の例（Web 許諾）です。レイヤ 2 PSK セキュリティ認証が最初に行われ、次に、ネットワーク アクセスが許可される前にスプラッシュ ページが許諾をユーザに表示します。[Access Type] で **WPA2 パーソナル**を選択し、**パスフレーズ**を入力します。

ステップ 6 [Apply] をクリックします。

外部スプラッシュ ページを使用したゲスト WLAN の作成

外部スプラッシュ ページは、外部 Web サーバに存在します。内部スプラッシュ ページと同様に、Cisco Mobility Express は、外部スプラッシュ ページを使用して**アクセス タイプ**の複数のオプションをサポートします。サポートしているアクセス タイプは次のとおりです。

1. ローカル ユーザ アカウント
2. Web 許諾

3. 電子メール アドレス
4. RADIUS
5. WPA2 パーソナル

手順

ステップ 1 [Wireless Settings] > [WLANs] に移動して、[Add new WLAN] ボタンをクリックします。[Add new WLAN] ウィンドウがポップアップ表示されます。

ステップ 2 [Add new WLAN] ウィンドウの [General] タブで、以下を設定します。

- **プロファイル名**を入力します。
- **SSID** を入力します。

ステップ 3 [WLAN Security] タブの下の [Guest Network] を有効にします。

ステップ 4 [Captive Portal] で**外部スプラッシュ ページ**を選択します。

ステップ 5 必要に応じて、次の**アクセス タイプ**のうちの 1 つを選択します。

1. **ローカル ユーザ アカウント**：スプラッシュ ページは、ネットワーク アクセスを許可する前に、コントローラによって認証する必要があるユーザ名とパスワードの入力をユーザに表示します。ローカル WLAN ユーザは、ゲスト クライアントが接続するコントローラで作成する必要があります。
2. **Web 許諾**：スプラッシュ ページは、ネットワーク アクセスが許可される前に許諾をユーザに表示します。
3. **電子メール アドレス**：スプラッシュ ページは、ネットワーク アクセスが許可される前に電子メール アドレスの入力をユーザに表示します。
4. **RADIUS**：スプラッシュ ページは、ネットワーク アクセスが許可される前に RADIUS サーバで認証する必要があるユーザ名とパスワードの入力をユーザに表示します。[Access Type] で **RADIUS** を選択し、RADIUS サーバの設定を入力します。
5. **WPA2 パーソナル**：これは、L2 + L3 の例（Web 許諾）です。レイヤ 2 PSK セキュリティ認証が最初に行われ、次に、ネットワーク アクセスが許可される前にスプラッシュ ページが許諾をユーザに表示します。[Access Type] で **WPA2 パーソナル**を選択し、**パスフレーズ**を入力します。

ステップ 6 [Apply] をクリックします。

ウォールド ガーデン（DNS 事前認証 ACL）

クライアントがゲスト WLAN に接続した際、通常、スプラッシュ ページまたはゲスト ポータルは、認証が成功するまでインターネットアクセスをブロックするように設定されています。認証を完了させるためには、アクセスを許可する Web サイトの特定のドメインと IP アドレスを追加する必要があります。

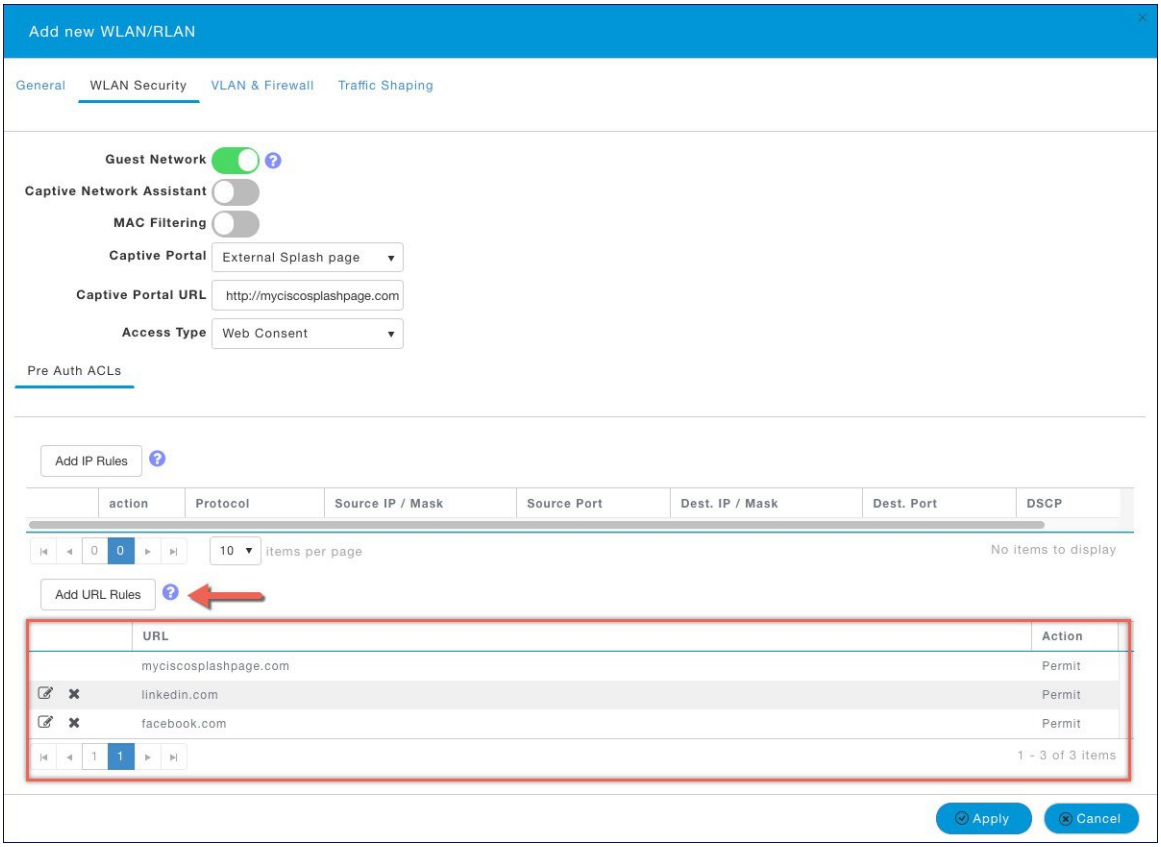
リリース 8.7 以降では、WLAN 上に DNS 事前認証 ACL と IPv4 ベースの事前認証 ACL を設定できます。1 つの ACL につき最大 20 の URL ルールがサポートされます。各 URL の長さは最大 255 文字です。URL ではワイルドカードもサポートされています。

手順

ステップ 1 [Wireless Settings] > [WLANs] > [Add new WLAN/RLAN] に移動します。

ステップ 2 [General] タブで、必要に応じて WLAN の値を入力します。

ステップ 3 [WLAN Security] タブで、[Guest Network] を有効にします。[External Splash Page] として [Captive Portal] を選択し、[Captive Portal URL] を入力します。[Access Type] として [Web Consent] を選択します。[DNS Pre-Auth ACLs] を追加するには、[Add URL Rules] ボタンをクリックし、許可または拒否する URL を追加します。



ステップ 4 [Apply] をクリックします。

Web 認証の内部スプラッシュ ページ

Cisco Mobility Express は、デフォルトの内部ゲスト ポータルをサポートします。ユーザがインポートできるカスタマイズされた内部ゲストポータルもサポートします。

デフォルトの内部ゲスト ポータルの使用

デフォルトのゲスト ポータル ページを使用したり、カスタマイズされたゲスト ポータル ページをインポートするには、以下の手順に従います。

手順

ステップ 1 [Wireless Settings] > [Guest WLANs] に移動します。

ステップ 2 ゲスト WLAN ページで以下を設定します。

- **Page Type**：[Internal]（デフォルト）を選択します
- **Preview**：[Preview] ボタンをクリックして、ページをプレビューできます。
- **Display Cisco Logo**：デフォルト ページの右上隅に表示されるシスコ ロゴを非表示にするには、[No] を選択します。このフィールドは、デフォルトで [Yes] に設定されています。
- **Redirect URL After Login**：ログイン後にゲスト ユーザを特定の URL（企業 URL など）にリダイレクトするには、このテキスト ボックスに必要な URL を入力します。最大 254 文字を入力することができます。
- **Page Headline**：ログイン ページに独自のヘッドラインを表示するには、このテキスト ボックスに必要なテキストを入力します。最大 127 文字を入力することができます。デフォルトのヘッドラインは、「Welcome to the Cisco Wireless Network」です。
- **Page Message**：ログイン ページで独自のメッセージを表示するには、このテキスト ボックスに必要なテキストを入力します。最大 2047 文字を入力することができます。デフォルトのメッセージは、「Cisco is pleased to provide the Wireless LAN infrastructure for your network.Please login and put your air space to work.」です。

ステップ 3 [Apply] をクリックします。

カスタマイズされた内部ゲスト ポールの使用

カスタマイズされたゲスト ポータルをゲスト ユーザに表示する必要がある場合、編集した後に Cisco Mobility Express コントローラにインポートできるサンプルページを Cisco.com からダウンロードできます。ページを編集し、Cisco Mobility Express コントローラへのアップロードの準備ができた後、次の手順に従います。

手順

ステップ 1 [Wireless Settings] > [Guest WLANs] に移動します。

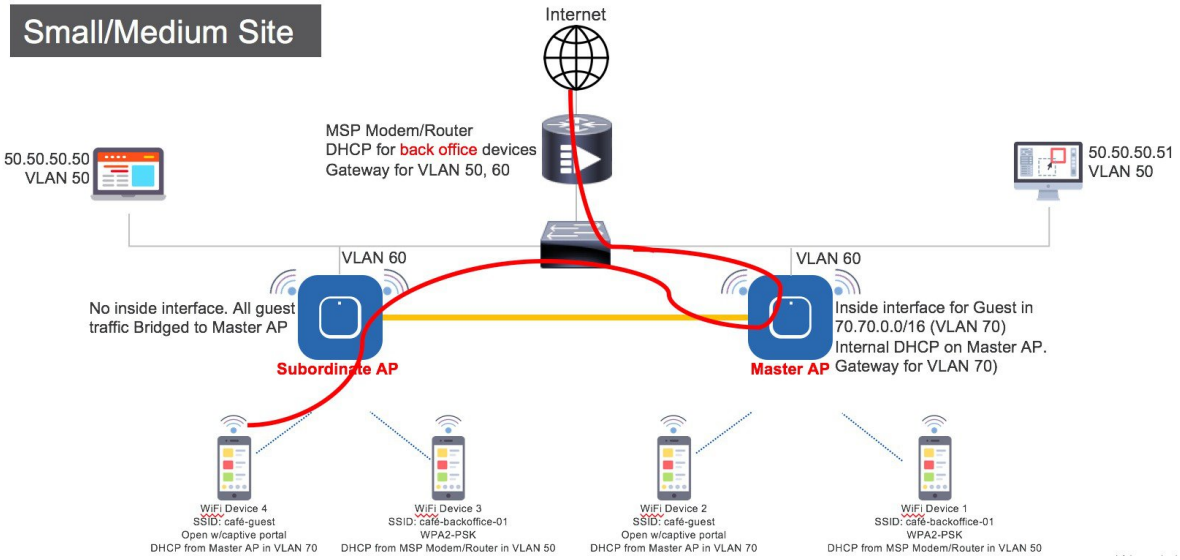
ステップ 2 ゲスト WLAN ページで以下を設定します。

- **Page Type**：**[Customized]** を選択します。
- **Customized page Bundle**：[Upload] ボタンをクリックして、カスタマイズされたページのバンドルを Mobility Express コントローラにアップロードします。
- **Preview**：[Preview] ボタンをクリックして、ゲスト ポータルをプレビューできます。
- **Redirect URL After Login**：ログイン後にゲスト ユーザを特定の URL（企業 URL など）にリダイレクトするには、このテキスト ボックスに必要な URL を入力します。最大 254 文字を入力することができます。

ステップ 3 [Apply] をクリックします。

ゲスト WLAN での集中型 NAT

マネージド サービス プロバイダは、1 つのサイトで 1 ～ 70 台の AP があり、同時に 300 以上のワイヤレス クライアントが接続するようなホテルや小売店に対してマネージド Wi-Fi サービスを提供します。このような場所では WAN 接続が制限されるため総スループットが通常、250 Mbps を下回ります。クライアントに対して外部 DHCP サーバを使用することは、規模の制限があるため、業務用のデバイスおよびクライアントに限定されます。ゲスト デバイスの場合、ゲストのすべてのトラフィックをマスター アクセス ポイント経由でルーティングできるように、マスター AP の内部 DHCP サーバの使用が期待されます。



ゲスト WLAN で集中型 NAT を設定するには、以下の手順に従います。

手順

ステップ 1 NAT 処理される WLAN のための DHCP プールを追加します。スコープを作成するには、[Wireless Settings] > [DHCP Server] > [Add new Pool] に移動します。[Add DHCP Pool] ウィンドウがポップアップ表示されます。[Add DHCP Pool] ウィンドウで、以下を設定します。

- WLAN のための **DHCP プール名**を入力します
- [Pool Status] を有効にします
- WLAN の **VLAN ID** を入力します
- DHCP クライアントの**リース期間**を入力します。デフォルトは 1 Day です
- [Network/Mask] を入力します
- DHCP プールの**開始 IP** を入力します
- DHCP プールの**終了 IP** を入力します
- DHCP プールの**デフォルト ゲートウェイ**を入力します

  （注） 集中型 NAT に接続するクライアント デバイス用のスコープの場合は、**デフォルト ゲートウェイ**として **Mobility Express コントローラ**を選択する必要があります。

- DHCP プールの**ドメイン名**（オプション）を入力します
- **ネーム サーバ**のために、必要に応じて [User Defined] を選択し、ネーム サーバの IP アドレスを入力します。OpenDNS ネーム サーバの IP アドレスが自動的に入力されている場合は OpenDNS を選択します。

- [Apply] をクリックします。

ステップ 2 WLAN を作成するには、[Wireless Settings] > [WLANs] に移動します。[Add new WLAN] または [Edit WLAN] ウィンドウで、[VLAN and Firewall] タブをクリックし、以下を設定します。

- [Client IP Management] で [Mobility Express Controller] を選択します
- [Peer to Peer Block] をチェックして、その WLAN に接続している 2 つのクライアント間の通信を無効にします
- **ネイティブ VLAN ID** を入力します。
- Mobility Express コントローラでゲスト クライアント用に作成された **DHCP スコープ**を選択します

（注） ：この WLAN のための VLAN は、AP が接続しているすべてのスイッチ ポートで設定する必要があります。

ステップ 3 [Apply] をクリックします。

WLAN ユーザの管理

Cisco Mobility Express はローカル ユーザ アカウントの作成をサポートします。このユーザは、AP を認証サーバとして設定しセキュリティとして WPA2 エンタープライズを使用するように設定されている WLAN、または**ローカル ユーザ アカウント**としての**アクセス タイプ**と内部または外部スプラッシュ ページを使用するように設定されているゲスト WLAN のために認証されます。

ローカル ユーザ アカウントを作成するには、以下の手順に従います。

手順

ステップ 1 [Wireless Settings] > [WLAN Users] に移動して、[Add WLAN User] ボタンをクリックします。

ステップ 2 WLAN ユーザとして以下を設定します。

- **User Name**：ユーザ名を入力します。
- **Guest User**：ゲスト ユーザの場合、[Guest User] チェックボックスを有効にします。
- **Lifetime**：ゲスト ユーザの場合、ユーザ アカウントの有効性を定義します。デフォルトは、作成時から 86400 秒（または 24 時間）です。
- **WLAN Profile**：ユーザが接続する WLAN を選択します。
- **Password**：ユーザ アカウントのパスワードを入力します。
- **Description**：ユーザ アカウントに関する詳細またはコメント。

• [tick] アイコンをクリックします。

WLAN での最大クライアント数の設定

Mobility Express は、最大 100 AP と 2000 クライアントをサポートします。1 つの WLAN に接続できるクライアントの最大数を制限するには、次の手順に従います。

手順

ステップ 1 [Expert View] を有効にします。

ステップ 2 [Wireless Settings] > [WLANs] > [Add new WLAN/RLAN] に移動します。

ステップ 3 [Advanced] タブで、[Maximum Allowed Clients] の値を入力するか、またはドロップダウン リストから数を選択します。

ステップ 4 [Apply] をクリックします。

AP Radio ごとの最大クライアント数の設定

Mobility Express は、radio ごとに最大 200 クライアントまでサポートします。radio に接続できるクライアントの最大数を制限するには、次の手順に従います。

手順

ステップ 1 [Expert View] を有効にします。

ステップ 2 [Wireless Settings] > [WLANs] > [Add new WLAN/RLAN] に移動します。

ステップ 3 [Advanced] タブで、[Maximum Allowed Clients per AP Radio] の値を入力します。

ステップ 4 [Apply] をクリックします。

WLAN での AAA オーバーライド

WLAN の AAA オーバーライド オプションを使用すると、WLAN で ID ネットワーキングを設定できます。ID ネットワーキングでは、AAA サーバから返された RADIUS 属性に基づいて、各 WLAN に、VLAN、アクセス コントロール リスト（ACL）、および Quality of Service（QoS）を適用できます。

手順

ステップ 1 [Expert View] を有効にします。

ステップ 2 [Wireless Settings] > [WLANs] > [Add new WLAN/RLAN] に移動します。

ステップ 3 [Advanced] タブで、[Allow AAA Override] を有効にします。

ステップ 4 [Apply] をクリックします。

双方向レート制限

AireOS 8.7 から、双方向レート制限が次の単位でサポートされます。

- クライアント単位
- BSSID 単位
- WLAN 単位

手順

ステップ 1 [Expert View] を有効にします。

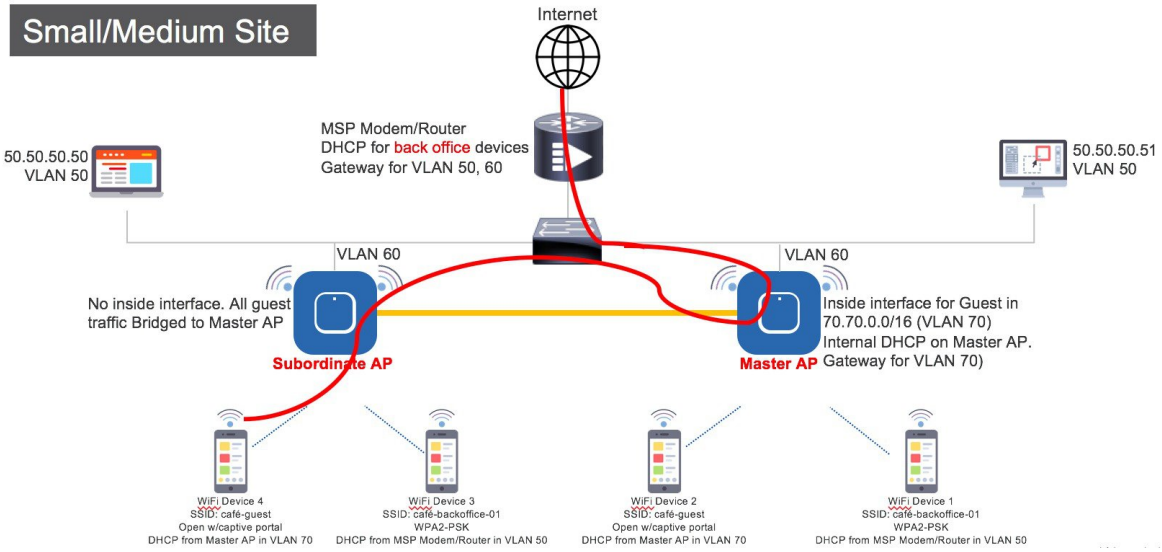
ステップ 2 [Wireless Settings] > [WLANs] > [Add new WLAN/RLAN] に移動します。

ステップ 3 [Traffic Shaping] タブで、必要に応じてレート制限を設定します。

ステップ 4 [Apply] をクリックします。

WLAN での集中型 NAT

マネージド サービス プロバイダは、1 つのサイトで 1 ～ 70 台の AP があり、同時に 300 以上のワイヤレス クライアントが接続するようなホテルや小売店に対してマネージド Wi-Fi サービスを提供します。このような場所では WAN 接続が制限されるため総スループットが通常、250 Mbps を下回ります。クライアントに対して外部 DHCP サーバを使用することは、規模の制限があるため、業務用のデバイスおよびクライアントに限定されます。ゲストデバイスの場合、ゲストのすべてのトラフィックをマスター アクセス ポイント経由でルーティングできるように、マスター AP の内部 DHCP サーバの使用が期待されます。



WLAN で集中型 NAT を設定するには、以下の手順に従います。

手順

ステップ 1 NAT 処理される WLAN のための DHCP プールを追加します。スコープを作成するには、[Wireless Settings] > [DHCP Server] > [Add new Pool] に移動します。[Add DHCP Pool] ウィンドウがポップアップ表示されます。[Add DHCP Pool] ウィンドウで、以下を設定します。

- WLAN のための **DHCP プール名**を入力します
- [Pool Status] を有効にします
- WLAN の **VLAN ID** を入力します
- DHCP クライアントの**リース期間**を入力します。デフォルトは 1 Day です
- [Network/Mask] を入力します
- DHCP プールの**開始 IP** を入力します
- DHCP プールの**終了 IP** を入力します
- DHCP プールの**デフォルト ゲートウェイ**を入力します

  （注） 集中型 NAT に接続するクライアント デバイス用のスコープの場合は、**デフォルト ゲートウェイ**として **Mobility Express コントローラ**を選択する必要があります。

- DHCP プールの**ドメイン名**（オプション）を入力します。
- **ネーム サーバ**のために、必要に応じて [User Defined] を選択し、ネーム サーバの IP アドレスを入力します。OpenDNS ネーム サーバの IP アドレスが自動的に入力されている場合は OpenDNS を選択します。

- [Apply] をクリックします。

（注） DHCP プールを作成する際に、集中型 NAT 用に設定された WLAN にこのスコープを使用する必要がある場合は、**デフォルト ゲートウェイ**として **Mobility Express コントローラ**を選択する**必要があります**。

ステップ 2 WLAN を作成するには、[Wireless Settings] > [WLANs] に移動します。[Add new WLAN] または [Edit WLAN] ウィンドウで、[VLAN and Firewall] タブをクリックし、以下を設定します。

- [Client IP Management] で [Mobility Express Controller] を選択します
- [Peer to Peer Block] をチェックして、その WLAN に接続している 2 つのクライアント間の通信を無効にします
- **ネイティブ VLAN ID** を入力します。
- ゲスト クライアント用に作成した **DHCP スコープ**を選択します。

（注） この WLAN のための VLAN は、AP が接続しているすべてのスイッチ ポートで設定する必要があります。

ステップ 3 [Apply] をクリックします。

WLAN でのローカル MAC フィルタリングのための MAC の追加

Cisco Mobility Express は、コントローラの WLAN での設定、および外部 RADIUS を使用して、MAC フィルタリングをサポートします。コントローラに MAC アドレスを追加して、ホワイトリストまたはブラックリストのいずれかに記載できます。コントローラへ MAC アドレスを追加するには、以下の手順に従います。

手順

ステップ 1 [Wireless Settings] > [WLAN Users] に移動して、[Local MAC Addresses] をクリックします。

ステップ 2 [Add MAC Address] をクリックします。

ステップ 3 [Add MAC Address] ウィンドウで、以下を設定します。

- **MAC Address**：デバイスの MAC アドレスを入力します
- **Description**：説明を入力します
- **Type**：この MAC がホワイトリストまたはブラックリストのいずれになるかを選択します
- **Profile Name**：ユーザが接続する WLAN を選択します

ステップ 4 [Apply] をクリックします。

WLAN Passpoint のサポート

リリース 8.5 から、Cisco Mobility Express では WLAN での Passpoint サポートが追加されています。IEEE 802.11u ベースのネットワーク情報をサポートするアクセス ポイントと、WiFi Alliance で認定された電話クライアント デバイスは連携して動作し、Passpoint 機能をサポートします。

802.11u 対応電話クライアント デバイスは、802.11u 対応 AP/Cisco Mobility Express コントローラから pre-association の際に収集された情報に基づき、ターゲット AP を検出し、選択します。電話クライアント デバイスは、デバイス内の設定ファイルに含まれるホーム OI 情報、レルム名やドメイン名などのプロビジョニング前のネットワーク情報を持ちます。さらに、電話クライアント デバイスは、挿入された SIM/USIM カードから得た IMSI データを使用してホーム ネットワーク情報を取得することもできます。

802.11u 対応 AP は、ホット スポットの所有者の詳細、ローミング パートナー、レルム リスト、3GPP セルラー情報、ドメイン名を含むさまざまな情報のリストを提供します。レルム リストは、レルム名と、関連する EAP 認証タイプ マッピングのリストも提供します。この情報を知ることは、正しい EAP 資格情報の交換を行うために、電話クライアント デバイスにとって必要不可欠です。

WLAN 設定で、単一 SSID と複数 SSID は必要な Passpoint 情報と共に設定されます。この追加の Passpoint 情報は、ビーコンまたはプローブ応答情報に追加され、Passpoint 対応の電話クライアント デバイスが AP を検出し、クエリを実行してさらなる情報を取得できるようにします。クエリ処理中に ANQP-Access Network Query プロトコルと呼ばれる標準プロトコル形式が使用されます。ここでは、プロトコルは、標準的な 2 ウェイまたは 4 ウェイ ハンドシェイク プロセスを記述し、AP と ANQP サーバから十分な情報を取得して、電話クライアント デバイスが認証され接続される最適な AP を決定します。このハンドシェイク プロセスは、GAS-Generic Advertisement Service プロトコルと呼ばれ、IEEE 802.11u 標準で定義されています。

Passpoint を設定するには、以下の手順に従います。

手順

ステップ 1 Cisco Mobility Express で [Expert View] を有効にします。 [Expert View] は次に示すように、Cisco Mobility Express WebUI のトップ バナーで使用可能です。これにより、WLAN の [802.11u] と [Hotspot 2.0] タブが有効になります。

ステップ 2 WLAN の 802.11u および Hotspot 2.0 を設定するには、[Wireless Setting] > [WLANs] に移動します。[Add new WLAN] または [Edit WLAN] ウィンドウで、[802.11u] タブおよび [Hotspot 2.0] タブをクリックし、関連する設定を入力します。

ステップ 3 [Apply] をクリックします。

Mobility Express での RLAN サポート

リリース 8.7 以降では、Cisco Mobility Express で RLAN を作成し、1810W および 1815W の有線ポートを管理できます。

Mobility Express はデータ トラフィックのローカル スイッチングをサポートしているため、RLAN データ トラフィックもローカルでスイッチされます。次の例では、802.1x 認証を使用してローカル スイッチング用の RLAN を設定し、有線アクセス用の AIR-AP1815W 上のイーサネット LAN ポートに関連付けます。設定タスクは次のとおりです。

1. 802.1x 認証を使用して RLAN を作成します。
2. AP グループを作成し、RLAN を AP グループに関連付けてから AP を AP グループに追加し、最後に有線ポートを RLAN に関連付けます。

802.1x 認証を使用して RLAN を作成するには、次の手順に従います。

手順

ステップ 1 [Wireless Settings] > [WLANs] に移動し、[Add new WLAN/RLAN] ボタンをクリックします。

ステップ 2 [General] タブで、[Type] ドロップダウンリストから [RLAN] を選択します。

ステップ 3 [Profile Name] を入力します。

ステップ 4 [RLAN Security] で、[Security Type] に [802.1x] を選択します。

ステップ 5 有線クライアントに 802.1x 認証を使用するので、[Add RADIUS Authentication Server] をクリックして RADIUS サーバを入力します。

ステップ 6 [VLAN & Firewall] タブで、[Use VLAN Tagging] を有効にし、データ トラフィックに使用する ID を [Native VLAN ID] と [VLAN ID] に入力します。

ステップ 7 [Apply] をクリックします。

AP グループの作成および AP グループへの 1815W の追加

AP グループを作成し、AP グループに 1815W を追加するには、次の手順に従います。

手順

ステップ 1 [Wireless Settings] > [Access Point Groups] に移動して、[Add new group] ボタンをクリックします。

ステップ 2 [General] タブで、[AP Group Name] と [AP Group Description] を入力します。

ステップ 3 [WLANs] タブで、[Add new WLAN/RLAN] ボタンをクリックし、AP グループに追加する RLAN を選択します。

ステップ 4 [Access Points] タブで、この AP グループに追加するウォール プレート AP を選択します。

ステップ 5 [Ports] タブで、必要な LAN ポートを有効にし、そのポート用の RLAN を選択します。

ステップ 6 [Apply] をクリックします。