ワイヤレス設定の指定

- WLAN と WLAN ユーザのセットアップ （1 ページ）
- Cisco Mobility Express ネットワーク内のリモート LAN （12 ページ）
- 関連付けられているアクセス ポイントの管理 （14 ページ）
- WLAN ゲスト ユーザのログイン ページの設定 （17 ページ）
- 内部 DHCP サーバの管理 （20 ページ）

WLAN と WLAN ユーザのセットアップ

Cisco Mobility Express ネットワーク内の WLAN について

ワイヤレス ローカル エリア ネットワーク（WLAN）を作成および管理するには、[WLAN Configuration] ウィンドウを使用します。[Wireless Settings] > [WLAN Users] の順に選択します。

[WLAN Configuration] ウィンドウの上部に、アクティブな WLAN の総数が表示されるとともに、マスター AP のコントローラで現在設定されているすべての WLAN が一覧表示されます。この一覧には、各 WLAN に関する次の詳細情報が表示されます。

- WLAN が有効であるか、無効であるか。
- WLAN の名前。
- WLAN のセキュリティ ポリシー。
- WLAN の無線ポリシー。

WLAN のセットアップに関する注意事項と制約事項

- Cisco Mobility Express コントローラには、最大 16 の WLAN を関連付けることができます。ただし、推奨されるのは最大 4 個までです。コントローラは、設定されたすべての WLAN を、接続されているすべての AP に割り当てます。
- 各 WLAN には一意の WLAN ID、一意のプロファイル名、および SSID があります。
- WLAN 名と SSID は 32 文字以内にする必要があります。

- 接続されている各 AP は、[Enabled] 状態の WLAN のみをアドバタイズします。AP は、無効化された WLAN はアドバタイズしません。
- コントローラでは、同じ SSID の WLAN を区別するために、異なる属性が使用されます。
- ピアツーピア ブロッキングは、マルチキャスト トラフィックには適用されません。
- WLAN から VLAN0 へのマッピング、VLAN 1002～1006 のマッピングはできません。
- スタティック IPv4 アドレスを使用するデュアルスタック クライアントはサポートされていません。
- 同じ SSID を使用する複数の WLAN を作成するときには、WLAN ごとに一意のプロファイル名を作成します。

WLAN の追加

ステップ 1 **[Wireless Settings]** > **[WLANs]** の順に選択します。

[WLAN Configuration] ウィンドウが表示されます。

ステップ 2 [Add New WLAN] をクリックします。
[Add New WLAN] ウィンドウが表示されます。

ステップ 3 [General] タブで、次のパラメータを設定します。

- [WLAN ID]：ドロップダウン リストから、この WLAN 用の ID 番号を選択します。
- [Profile Name]：プロファイル名は一意であり、最大 32 文字までです。
- [SSID]：プロファイル名も SSID として機能します。WLAN プロファイル名とは異なる SSID を指定することができます。プロファイル名と同様に、SSID も 32 文字までとし、一意である必要があります。
- [Admin State]：ドロップダウンリストから [Enabled] を選択してこの WLAN を有効にするか、または [Disabled] を選択します。

  デフォルトは [Enabled] です。
- [Radio Policy]：ドロップダウンリストで、次のオプションから選択します。
  - [All]：デュアルバンド（2.4 GHz と 5 GHz）対応のクライアントをサポートするように WLAN を設定します。
  - [2.4 GHz only]：802.11b/g/n 対応のクライアントのみをサポートするように WLAN を設定します。
  - [5 GHz only]：802.11a/n/ac 対応のクライアントのみをサポートするように WLAN を設定します。

  無線ポリシーを使用すると、WLAN に関連付けられているすべての AP の RF 設定を最適化できます。選択した無線ポリシーは、802.11 無線に適用されます。各無線ポリシーでは、WLAN をアドバタイズするスペクトルの部分、つまり、2.5 GHz または 5 GHz、あるいはその両方を指定します。

- [Broadcast SSID]：デフォルトは [Enabled] です。切り替えると、SSID が検出可能になります。それ以外の場合は、SSID は表示されません。
- [Local Profiling]：

ステップ 4 [WLAN Security] タブで、[Security] ドロップダウンリスト リストから次のセキュリティ認証オプションのいずれかを設定します。

- Open：このオプションはオープン認証です。オープン認証では、あらゆるデバイスが認証でき、AP との通信を試行できます。オープン認証を使用すると、あらゆるワイヤレス デバイスが AP に対して認証を実行できます。
- WPA2 Personal：このオプションは、事前共有キー（PSK）を使用する Wi-Fi Protected Access 2 です。WPA2 Personal は、PSK 認証を使用してネットワークを保護するために使用されるメソッドです。PSK は、WLAN セキュリティ ポリシー下のコントローラ AP で設定するだけでなく、クライアントでも設定します。WPA2 Personal は、ネットワーク上の認証サーバを信頼しません。このオプションは、エンタープライズ認証サーバがない場合に使用します。

  このオプションを選択した場合は、[Shared Key] フィールドに PSK を指定し、[Confirm Shared Key] フィールドにもう一度指定して確認します。セキュリティ上の理由により、入力する PSK はアスタリスクで隠されます。表示するには、[Show Shared Key] チェックボックスをオンにします。

- WPA2 Enterprise：このオプションは、ローカル認証サーバまたは RADIUS サーバを使用する Wi-Fi Protected Access 2 です。これがデフォルトのオプションです。

  ローカル認証方式を使用するには、[Authentication Server] ドロップダウン リストで [AP] を選択します。このオプションはローカル EAP 認証方式です。この認証方式では、ユーザとワイヤレスクライアントをローカルで認証できます。マスター AP のコントローラは、認証サーバおよびローカル ユーザ データベースとして機能するため、外部認証サーバに依存する必要がなくなります。

  RADIUS サーバ ベースの認証方式を使用するには、[Authentication Server] ドロップダウン リストで [External Radius] を選択します。RADIUS は、中央管理サーバとの通信を行って、ユーザの認証と WLAN へのアクセス許可を可能にするクライアント/サーバ プロトコルです。RADIUS 認証サーバは最大 2 つまで指定できます。サーバごとに次の詳細を指定する必要があります。

  - [RADIUS IP]：RADIUS サーバの IPv4 アドレス。
  - [RADIUS Port]：RADIUS サーバの通信ポートを入力します。デフォルト値は 1812 です。
  - [Shared Secret]：RADIUS サーバで使用する秘密キーを ASCII 形式で入力します。

- Guest：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。この WLAN をゲスト ユーザ アクセス専用に設定するには、[Security] に [Guest] を選択します。

  ゲスト ユーザの認証を設定するには、[Guest Type] ドロップダウンリストで次のいずれかのオプションを選択します。

  - WPA2 Personal：このオプションは、事前共有キー（PSK）を使用する Wi-Fi Protected Access 2 です。WPA2 Personal は、PSK 認証を使用してネットワークを保護するために使用されるメソッドです。PSK は、WLAN セキュリティ ポリシー下のコントローラ AP で設定するだけでなく、クライアントでも設定します。WPA2 Personal は、ネットワーク上の認証サーバを信頼しません。このオプションは、エンタープライズ認証サーバがない場合に使用します。

このオプションを選択した場合は、[Passphrase] フィールドに PSK を指定し、[Confirm **Passphrase**] フィールドにもう一度指定して確認します。セキュリティ上の理由により、入力する PSK はアスタリスクで隠されます。表示するには、[Show Passphrase] チェックボックスをオンにします。

- [Captive Portal (AP)]：次の**キャプティブ ポータル タイプ**のいずれかをユーザに提示するキャプティブ ポータルを設定するには、このオプションを選択します。
  - [Require Username and Password]：これはデフォルト オプションです。この WLAN のゲスト ユーザに指定できるユーザ名とパスワードを使用してゲストを認証するには、[Wireless Settings] > [WLAN Users] でこのオプションを選択します。詳細については、WLAN ユーザの表示と管理 （8 ページ）を参照してください。
  - [Web Consent]：表示された利用規約をゲストが受け入れたときに、WLAN へのアクセスを許可するには、このオプションを選択します。これでユーザは、ユーザ名とパスワードを入力しなくても WLAN にアクセスできます。
  - [Require Email Address]：ゲスト ユーザが WLAN にアクセスしようとしたときに、電子メールアドレスの入力を求めるには、このオプションを選択します。有効な電子メールアドレスが入力されたら、アクセス権を付与します。これでユーザは、ユーザ名とパスワードを入力しなくても WLAN にアクセスできます。
- [Captive Portal (External Web Server)]：ネットワーク外の Web サーバを使用して外部キャプティブ ポータル認証を取得するには、このオプションを選択します。また、[Site URL] フィールドにサーバの URL を指定します。
- [CMX Guest Connect]：Cisco CMX Connect を使用してゲストを認証するには、このオプションを選択します。また、[Site URL] フィールドに CMX クラウド サイトの URL を指定します。

ステップ 5 [VLAN & Firewall] タブで [Use VLAN Tagging] ドロップダウン リストから [Yes] を選択し、パケットの VLAN タギングを有効にします。その後、タギングに使用する [VLAN ID] をドロップダウン リストから選択します。デフォルトでは VLAN タギングは無効です。

VLAN タギングを有効にすると、パケットが属する VLAN（仮想ローカル エリア ネットワーク）を識別するために、選択した VLAN ID がパケット ヘッダーに挿入されます。これによりコントローラは、VLAN ID を使用して、ブロードキャスト パケットの送信先 VLAN を判別できるため、VLAN 間でトラフィックが分離されます。

ステップ 6 VLAN タギングを有効にするように選択した場合は、アクセス コントロール リスト（ACL）に基づいて WLAN のファイアウォールを有効にするためのオプションを選択できます。ACL は次のいずれかの目的で使用されるルール セットです。1 つの目的は、特定の WLAN へのアクセスを制限して、ワイヤレス クライアントとの間で送受信されるデータ トラフィックを制御すること、もう 1 つの目的は、コントローラ CPU へのアクセスを制限して、CPU を宛先とするすべてのトラフィックを制御することです。

ACL ベースのファイアウォールを有効にするには、次の手順に従います。

1. [Enable Firewall] ドロップダウン リストで [Yes] を選択します。
2. [ACL Name] フィールドに、新しい ACL の名前を入力します。最大 32 文字の英数字を入力できます。ACL 名は固有の名前でなければなりません。

3. [Apply] をクリックします。
4. ACL のルールを設定するには、[Add Rule] をクリックします。

ACL ルールは VLAN に適用されることに注意してください。複数の WLAN で同じ VLAN を使用できるので、VLAN に適用されている ACL ルールがあればそれが継承されます。

この ACL のルールを次のように設定します。

1. [Action] ドロップダウン リストから、この ACL によってパケットがブロックされるようにする場合は [Deny] を選択し、この ACL によってパケットが許可されるようにする場合は [Permit] を選択します。デフォルトの設定は [Permit] です。コントローラは ACL の IP パケットのみを許可または拒否できます。他のタイプのパケット（ARP パケットなど）は指定できません。
2. [Protocol] ドロップダウン リストから、この ACL に使用する IP パケットのプロトコル ID を選択します。プロトコル オプションは次のとおりです。
   - [Any]：任意のプロトコル（これはデフォルト値です）
   - [TCP]：トランスミッション コントロール プロトコル
   - [UDP]：ユーザ データグラム プロトコル
   - [ICMP]：インターネット制御メッセージ プロトコル

     [ESP]：IP カプセル化セキュリティ ペイロード
   - [AH]：認証ヘッダー
   - [GRE]：Generic Routing Encapsulation
   - [IP in IP]：Internet Protocol（IP）in IP（IP-in-IP パケットのみを許可または拒否）
   - [Eth Over IP]：Ethernet-over-Internet プロトコル
   - [OSPF]：Open Shortest Path First
   - [Other]：その他の Internet Assigned Numbers Authority（IANA）プロトコル[Other] を選択する場合は、[Protocol] テキスト ボックスに目的のプロトコルの番号を入力します。使用可能なプロトコルのリストは IANA Web サイトで確認できます。
3. **[宛先**IP / Mask（Dest. IP / Mask）] フィールドに、特定の宛先の IP アドレスとネットマスクを入力します。
4. [TCP] または [UDP] を選択した場合は、[Destination Port] を指定する必要があります。この宛先ポートは、ネットワーキング スタックとのデータ送受信をするアプリケーションが使用できます。一部のポートは、Telnet、SSH、HTTP など特定のアプリケーション用に指定されています。
5. [DSCP] ドロップダウン リストから次のオプションのいずれかを選択して、この ACL の Differentiated Service Code Point（DSCP）値を指定します。[DSCP] は、インターネット上の QoS を定義するために使用できる IP ヘッダー テキスト ボックスです。次のオプションを選択できます。
   - [Any]：任意の DSCP（これは、デフォルト値です）

- [Specific]：DSCP 編集ボックスに入力する、0 ～ 63 の特定の DSCP

6. [Apply] アイコンをクリックして、変更を確定します。

ステップ 7 Quality of Service（QoS）とは、選択したネットワーク トラフィックにさまざまなテクノロジーに渡る優れたサービスを提供する、ネットワークの機能を意味します。QoS の主要な目的は、専用の帯域幅の確保、ジッターおよび遅延の制御（ある種のリアルタイム トラフィックや対話型トラフィックで必要）、および損失特性の改善などを優先的に処理することです。

Cisco Mobility Express コントローラでは次の 4 つの QoS レベルがサポートされています。[QoS] タブの [QoS] ドロップダウン リストで、次のいずれかの QoS レベルを選択します。

- Platinum (Voice)：無線を介して転送される音声のために高品質のサービスを保証します。
- Gold (Video)：高品質のビデオ アプリケーションをサポートします。
- Silver (Best Effort)：クライアントの通常の帯域幅をサポートします。
- Bronze (Background)：ゲスト サービス用の最小の帯域幅を提供します。

ステップ 8 [Application Visibility] は、Network-Based Application Recognition（NBAR2）エンジンを使用してアプリケーションを分類し、ワイヤレスネットワークにアプリケーションレベルの可視性を提供します。[Application Visibility] により、コントローラは 1000 個を超えるアプリケーションの検出と認識、リアルタイム分析の実行、ネットワークの輻輳とネットワーク リンクの使用状況のモニタができます。この機能は、**[Monitoring]** > **[Network Summary]** にある [Applications By Usage] 統計を提供します。

[Application Visibility] を有効にするには、[Application Visibility] ドロップダウン リストから [Enabled]（デフォルト オプション）を選択します。有効にしない場合は、[Disabled] を選択します。

ステップ 9 [Apply] をクリックします。

次のタスク

この時点で、この WLAN のユーザ アカウントを作成または編集できます。WLAN ユーザの表示と管理 （8 ページ）を参照してください。

WLAN の有効化と無効化

ステップ 1 [Wireless Settings] > [WLANs] の順に選択します。
[WLAN Configuration] ウィンドウが表示されます。

ステップ 2 有効または無効にする WLAN の横にある [Edit] アイコンをクリックします。
[Edit WLAN] ウィンドウが表示されます。

ステップ 3 **[General]** > **[Admin State]** の順に選択し、必要に応じて [Enabled] または [Disabled] を選択します。

ステップ 4 [Apply] をクリックします。

（注） WLAN を新規作成または既存の WLAN を編集した後で [Apply] をクリックすると、以前有効だったか無効だったかに関係なく、必ず WLAN が有効になります。

WLAN の編集と削除

[Wireless Settings] > **[WLANs]** の順に選択します。表示されるウィンドウで、次のいずれかの操作を実行します。

- WLAN を編集するには、その隣にある [Edit] アイコンをクリックします。
- WLAN を削除するには、その隣にある [Delete] アイコンをクリックします。

WLAN ごとのクライアント数の制限

マスター AP に応じて、Cisco Mobility Express は WLAN ごとに最大 100 の AP と、2,000 の クライアントをサポートします。Cisco Mobility Express ネットワーク上のクライアント数を制限するには、次を実行します。

始める前に

ステップ 1 [Expert] ビューで、**[Wireless Settings]** > **[WLANs]** に移動します。

[WLAN/RLAN Configuration] ウィンドウが表示されます。

ステップ 2 [Add New WLAN/RLAN] をクリックします。

既存の WLAN のクライアントの制限を変更するには、[WLAN/RLAN] テーブルの特定の WLAN に移動し、[Edit] アイコンをクリックします。

[Add New WLAN/RLAN] ウィンドウが表示されます。

ステップ 3 [Advanced] タブで、[Maximum Allowed Clients] の特定の値を対応するドロップダウンリストから選択するか、または入力します。

ステップ 4 [Apply] をクリックして、変更内容を保存します。

[WLAN/RLAN Configuration] ウィンドウが表示されます。

選択した WLAN が、指定したクライアントの最大数で設定されています。

AP 無線あたりのクライアント数の制限

Cisco Mobility Express は、単一の AP 無線上で最大 200 の接続クライアントをサポートします。シスコ ワイヤレス リリース 8.7 以降、この制限は以下を実行することによって変更できます。

始める前に

ステップ 1 [Expert] ビューで、**[Wireless Settings]** > **[WLANs]** に移動します。

[WLAN/RLAN Configuration] ウィンドウが表示されます。

ステップ 2 [Add New WLAN/RLAN] をクリックします。

既存の WLAN の AP 無線ごとの最大クライアント制限を変更するには、[WLAN/RLAN] テーブル内の特定の WLAN に移動し、[Edit] アイコンをクリックします。

[Add New WLAN/RLAN] ウィンドウが表示されます。

ステップ 3 [Advanced] タブで、[Maximum Allowed Clients Per AP Radio] の特定の値を対応するドロップダウンリストから選択するか、または入力します。

ステップ 4 [Apply] をクリックして、変更内容を保存します。

[WLAN/RLAN Configuration] ウィンドウが表示されます。

選択した WLAN が AP 無線に接続可能な改訂したクライアントの最大数で設定されます。

WLAN ユーザの表示と管理

WLAN ユーザを表示、管理するには、**[Wireless Settings]** > **[WLAN Users]** の順に選択します。

[WLAN Users] ウィンドウが表示され、コントローラ上で構成されている WLAN ユーザの総数が表示されます。さらに、ネットワーク上のすべての WLAN ユーザおよび各ユーザに関する次の詳細情報が表示されます。

- User name：WLAN ユーザの名前。
- Guest user：このチェックボックスをオンにした場合、ユーザは作成時から 86400 秒間（24 時間）のみ有効となるゲスト ユーザ アカウントとなります。
- WLAN Profile：このユーザが接続できる WLAN。
- Password：WLAN への接続時に使用するパスワード。
- Description：ユーザに関する詳細またはコメント。

ローカル サーバ設定を使用して、WPA2 Enterprise のみの WLAN ユーザを表示および管理できます。ワイヤレス クライアントが Cisco Mobility Express ワイヤレス ネットワークを使用するには、ネットワーク内の WLAN に接続する必要があります。ワイヤレスクライアントが WLAN に接続するには、その WLAN に設定されたユーザ クレデンシャルを使用する必要があります。この WLAN で [Security Policy] として [WPA2 Personal] が使用されている場合、ユーザはコントローラ AP 上のその WLAN に設定された該当する WPA2 PSK を入力する必要があります。[Security Policy] が [WPA2-Enterprise] に設定されている場合、ユーザは、RADIUS ユーザ デー

タベースで設定されている有効なユーザアイデンティティとそれに対応するパスワードを入力する必要があります。

WLAN ユーザの追加

WLAN ユーザを追加するには、[Add WLAN User] をクリックしてから、次の詳細情報を入力します。

- User name：WLAN ユーザ アカウントの名前を指定します。
- Guest user：ゲスト WLAN ユーザ アカウントにする場合は、このチェックボックスをオンにします。さらに [Lifetime] フィールドに、このアカウントが有効であり続ける時間数を作成時からの秒数で指定できます。デフォルト値は 86400 秒（24 時間）です。ライフタイム値は 60 秒～ 31536000 秒（つまり 1 分~ 1 年）の範囲内で指定できます。
- WLAN Profile：このユーザが接続できる WLAN を選択します。ドロップダウン リストから特定の WLAN から選択するか、[Any WLAN] を選択して、コントローラ上にセットアップされているすべての WLAN 用にこのアカウントを適用します。

  このドロップダウン リストには、[Wireless Settings] > [WLANs] で設定した WLAN が表示されます。
- Password：WLAN への接続時に使用するパスワード。
- Description：ユーザに関する詳細またはコメント。

WLAN ユーザの編集

WLAN ユーザを編集するには、詳細を編集する WLAN ユーザの横にある [Edit] アイコンをクリックし、必要な変更を加えます。

WLAN ユーザの削除

WLAN ユーザを削除するには、削除する WLAN ユーザの横にある [Delete] アイコンをクリックしてから、確認ダイアログボックスで [Ok] をクリックします。

双方向帯域幅レート制限

Cisco Mobility Express ネットワーク上でクライアント デバイス、WLAN、および BSSID のスループットの制限を定義できます。双方向レート制限によって、ネットワーク帯域幅がすべてのユーザに平等に分配されます。Cisco Mobility Express ネットワーク上のクライアント デバイス、WLAN、および BSSID に双方向帯域幅レート制限を設定するには、次の手順を実行します。

- クライアントごとの双方向レートの制限 （10 ページ）
- BSSID ごとの双方向レートの制限 （10 ページ）
- WLAN ごとの双方向レートの制限 （11 ページ）

クライアントごとの双方向レートの制限

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

[WLAN/RLAN Configuration] ウィンドウが表示されます。

ステップ 2 [Add New WLAN/RLAN] をクリックします。

既存の WLAN の双方向レート制限を変更するには、テーブル内の特定の WLAN に移動し、[Edit] アイコンをクリックします。

[Add New WLAN/RLAN] ウィンドウが表示されます。

ステップ 3 [Traffic Shaping] タブで、クライアントごとのダウンストリームとアップストリームの制限に特定の値を選択するか、または入力します。

[Standard] ビューで、対応するスライダーを移動して、次のように特定の値を選択します（Mbps 単位）。

- **[Per-client downstream bandwidth limit]**
- **[Per-client upstream bandwidth limit]**

[Expert] ビューで、[Rate limits per client] セクションの下にある次のフィールドに特定の値を指定します（kbps 単位）。

- **[Average downstream bandwidth limit]**
- **[Average real-time downstream bandwidth limit]**
- **[Average upstream bandwidth limit]**
- **[Average real-time upstream bandwidth limit]**

ステップ 4 [Apply] をクリックして、変更内容を保存します。

[WLAN/RLAN Configuration] ウィンドウが表示されます。

新しい設定に従って、双方向帯域幅はクライアント デバイスごとに制限されています。

BSSID ごとの双方向レートの制限

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

[WLAN/RLAN Configuration] ウィンドウが表示されます。

ステップ 2 [Add New WLAN/RLAN] をクリックします。

既存の WLAN の双方向レート制限を変更するには、テーブル内の特定の WLAN に移動し、[Edit] アイコンをクリックします。

[Add New WLAN/RLAN] ウィンドウが表示されます。

ステップ 3 [Traffic Shaping] タブで、BSSID ごとのダウンストリームとアップストリームの制限に特定の値を選択するか、または入力します。

[Standard] ビューで、対応するスライダーを移動して、次のように特定の値を選択します（Mbps 単位）。

- **[Per-BSSID downstream bandwidth limit]**
- **[Per-BSSID upstream bandwidth limit]**

[Expert] ビューで、[Rate limits per BSSID] セクションの下にある次のフィールドに特定の値を指定します（kbps 単位）。

- **[Average downstream bandwidth limit]**
- **[Average real-time downstream bandwidth limit]**
- **[Average upstream bandwidth limit]**
- **[Average real-time upstream bandwidth limit]**

ステップ 4 [Apply] をクリックして、変更内容を保存します。

[WLAN/RLAN Configuration] ウィンドウが表示されます。

新しい設定に従って、双方向帯域幅は BSSID ごとに制限されています。

WLAN ごとの双方向レートの制限

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

[WLAN/RLAN Configuration] ウィンドウが表示されます。

ステップ 2 [Add New WLAN/RLAN] をクリックします。

既存の WLAN の双方向レート制限を変更するには、テーブル内の特定の WLAN に移動し、[Edit] アイコンをクリックします。

[Add New WLAN/RLAN] ウィンドウが表示されます。

ステップ 3 [Traffic Shaping] タブで、WLAN ごとのダウンストリームとアップストリームの制限に特定の値を選択するか、または入力します。

[Standard] ビューで、対応するスライダーを移動して、次のように特定の値を選択します（Mbps 単位）。

- **[Per-WLAN downstream bandwidth limit]**
- **[Per-WLAN upstream bandwidth limit]**

[Expert] ビューで、[Rate limits per WLAN] セクションの下にある次のフィールドに特定の値を指定します（kbps 単位）。

- **[Average downstream bandwidth limit]**

- **[Average real-time downstream bandwidth limit]**
- **[Average upstream bandwidth limit]**
- **[Average real-time upstream bandwidth limit]**

ステップ 4 [Apply] をクリックして、変更内容を保存します。

[WLAN/RLAN Configuration] ウィンドウが表示されます。

新たに指定された値に従って、双方向帯域幅は WLAN で制限されるようになります。

Cisco Mobility Express ネットワーク内のリモート LAN

[WLAN/RLAN Configuration] ウィンドウを通じてリモート ローカル エリア ネットワーク（RLAN）を作成し、管理できます。このウィンドウへは **[Wireless Settings]** > **[WLANs]** でアクセスできます。RLAN では、1810W や1815W のような Cisco AP 上で有線ポートを管理できます。

Cisco Mobility Express ネットワーク上で RLAN 機能を有効にするには、次のタスクを指定された順序で実行します。

- RLAN を作成します。
- AP グループを作成します。
- RLAN を AP グループに関連付けます。
- （管理する必要がある有線ポートを備えた）AP をAP グループに追加します
- 有線 ポートを RLAN に関連付けます。

リモート LAN の作成

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

このウィンドウには、Cisco Mobility Express コントローラ上に設定されているすべての WLAN とリモート LAN のカウントが表示されます。また、設定された WLAN と RLAN の詳細を示すテーブルも表示されます。

各リモート LAN については、プロファイル**名**、管理状態、**タイプ**（RLAN）、および**セキュリティ ポリシー**を確認できます。WLAN およびリモート LAN を表示するテーブルが複数ページに及ぶ場合、ページ番号のリンクをクリックすると、それらのページにアクセスできます。

[WLAN/RLAN Configuration] ウィンドウが表示されます。

ステップ 2 [Add New WLAN/RLAN] をクリックします。

[Add New WLAN/RLAN] ウィンドウが表示されます。

ステップ 3 [WLANs] を選択して、[WLANs] ページを開きます。

このページでは、コントローラ上で現在設定されているすべての WLAN およびリモート LAN が表示されます。各 WLAN について、WLAN/リモート LAN ID、プロファイル名、タイプ、SSID、ステータス、およびセキュリティ ポリシーを表示できます。

WLAN/リモート LAN の合計数がページの右上隅に表示されます。WLAN/リモート LAN のリストが複数ページに渡る場合は、ページ番号のリンクをクリックすることで、目的のページにアクセスできます。

（注） リモート LAN を削除する場合は、カーソルを目的の WLAN の青いドロップダウン矢印の上に置いて、[Remove] を選択するか、または行の左側のチェックボックスをオンにして、ドロップダウン リストから [Remove Selected] を選択し、[Go] をクリックします。決定を確認するメッセージが表示されます。作業を続行すると、割り当てられているアクセス ポイント グループおよびアクセス ポイント無線からそのリモート LAN が削除されます。

ステップ 4 ドロップダウン リストから [Create New] を選択し、[Go] をクリックして新規の Remote-LAN を作成します。[WLANs > New] ページが表示されます。

ステップ 5 [Type] ドロップダウン リストから、[Remote LAN] を選択してリモート LAN を作成します。

ステップ 6 [Profile Name] テキスト ボックスに、このリモート WLAN に割り当てるプロファイル名に対する最大 32 文字の英数字を入力します。プロファイル名は固有である必要があります。

ステップ 7 [WLAN ID] ドロップダウン リストから、この WLAN の ID 番号を選択します。

ステップ 8 [Apply] をクリックして、変更を確定します。[WLANs > Edit] ページが表示されます。

（注） 編集する WLAN の ID 番号をクリックすることにより、[WLANs] ページから [WLANs > Edit] ページを開くこともできます。

ステップ 9 [General] タブ、[Security] タブ、および [Advanced] タブ上でパラメータを使用してこのリモート LAN を設定します。特定の機能を設定する手順については、この章の後の項を参照してください。

ステップ 10 [General] タブの [Status] チェックボックスをオンにして、このリモート LAN を有効にします。リモート LAN に対する設定変更が終了するまで、チェックボックスをオフにしておいてください。

（注） また、[WLANs] ページから、有効化または無効化する ID の左側のチェック ボックスをオンにして、ドロップダウンリストから [Enable Selected] または [Disable Selected] を選択し、[Go] をクリックすることでも、リモート LAN を有効化または無効化できます。

ステップ 11 [Apply] をクリックして、変更を確定します。

ステップ 12 [Save Configuration] をクリックして、変更を保存します。

関連付けられているアクセス ポイントの管理

[Wireless Settings] > **[Access Points]** の順に選択します。[Access Points Administration] ウィンドウが表示されます。ウィンドウの上部には、コントローラに関連付けられている AP の数とともに、次の詳細情報が表示されます。

- Manage：次のアイコンが表示され、AP がプライマリ コントローラ（マスター AP）として動作しているのか、従属 AP として動作しているのかが示されます。

  図 *1*：プライマリ コントローラ（マスター *AP*）アイコン

  図 *2*：従属 *AP* アイコン

- Location：AP の場所。
- Name：AP の名前。
- IP Address：AP の IP アドレス。
- AP MAC：AP の MAC アドレス。
- Up Time：AP がコントローラに関連付けられている時間の長さ。
- AP Model：アクセス ポイントのモデル番号。

（注） AP が AP グループに参加するとき、または AP グループの RF プロファイルが変更されたときに AP の CAPWAP プロセスが再起動され、すべての AP の再起動が回避されます。新しい CAPWAP 再起動ペイロードが AP に送信され、CAPWAP プロセスのみが再起動されます。応答として、AP では新しい AP グループまたは RF プロファイルに固有の新しい設定を受信します。コントローラへの AP の接続が失われ、AP がネットワークをリロードして再度参加します。

アクセス ポイントの管理

ステップ 1 **[Wireless Settings]** > **[Access Points]** の順に選択します。

[Access Points Administration] ウィンドウが表示されます。コントローラに関連付けられている AP のみを管理できます。

ステップ 2 管理する AP の横にある [Edit] アイコンをクリックします。
[Edit] ウィンドウが表示され、[General] タブが表示されます。

ステップ 3 [General] タブでは、次の AP パラメータを編集できます。

- [Operating Mode] および [Make me Controller]：マスター AP の場合、[Operating Mode] フィールドに *AP* と コントローラが表示されます。関連付けられている他の AP の場合、このフィールドには [AP Only] と表示されます。

  [Make me Controller] ボタンは、マスターの選定プロセスに含めることができる下位 AP に対してのみ使用できます。この AP をマスター AP にするには、このボタンをクリックします。

- IP Configuration：AP の IP アドレスがネットワーク上の DHCP サーバによって割り当てられるようにするには、[Obtain from DHCP] を選択します。静的 IP アドレスを使用する場合は、[Static IP] を選択します。静的 IP アドレスを使用する選択をした場合は、[IP Address]、[Subnet Mask]、および [Gateway] フィールドを編集できます。

- AP Name：AP の名前を編集します。これはフリー テキスト フィールドです。

- Location：AP の場所を編集します。これはフリー テキスト フィールドです。

[General] タブには次の編集できない AP パラメータも表示されます。

- AP MAC address
- AP Model number
- アクセス ポイントの [IP Address]（[Obtain from DHCP] を選択した場合のみ編集不可）。
- [Subnet mask]（[Obtain from DHCP] を選択した場合のみ編集不可）。
- [Gateway]（[Obtain from DHCP] を選択した場合のみ編集不可）。

ステップ 4 （マスター AP の場合のみ）[Controller] タブでは、統合された Mobility Express ワイヤレス LAN コントローラの次のコントローラ パラメータを手動で編集できます。

- [IP Address]：この IP アドレスは、コントローラの Web インターフェイスへのログイン URL を決定します。URL の形式は *https://<ip address>* です。この IP アドレスを変更すると、ログイン URL も変更されます。
- **[サブネット マスク（Subnet Mask）]**
- **[Country Code]**

ステップ 5 [Radio 1] タブおよび [Radio 2] タブでは、次のパラメータを設定できます。

（注） [Radio 1] タブは、Cisco Aironet 3800 シリーズと 2800 シリーズの AP を除き、すべての AP の 2.4 GHz（802.11 b/g/n）無線に相当します。これらの AP では、2.4 GHz（802.11 b/g/n）または 5 GHz（802.11a/n/ac）のいずれかに設定できます。[Radio 2] タブはすべての AP の 5 GHz（802.11a/n/ac）無線のみに相当します。

また、無線タブ名は、カッコ内に運用無線帯域も示しています。

パラメータ	説明	
[Admin Mode]	AP 上で対応する無線を有効または無効にします。	
[Band]	[Radio 1] にのみ表示されます。デフォルトでは、2.4 GHz に設定されています。3800 シリーズと 2800 シリーズの AP の場合は、5 GHz に変更できます。	
[Channel]	2.4 GHz の場合、これを [Automatic] に設定するか、1 ～ 11 の値を設定します。 [Automatic] を選択すると、動的チャネル割り当てが有効になります。つまり、マスター AP の制御下にある各 AP にチャネルが動的に割り当てられます。これにより、隣接する AP が同じチャネル上でブロードキャストされることがなくなり、干渉などの通信の問題を回避できます。2.4 GHz 無線の場合、米国では 11 チャネルが提供され、米国以外の国や地域では最大 14 チャネルが提供されます。ただし、隣接する AP で使用される場合、非オーバーラップと見なすことができるのは、1-6-11 のみです。 特定の値を割り当てると、その AP にチャネルが静的に割り当てられます。	5 GHz の場合、これは [Automatic]、36、40、44、48、52、56、60、64、100、104、108、112、116、132、136、140、149、153、157、161、または 165 に設定できます。 5 GHz の無線の場合は、最大 23 の非オーバーラップ チャネルが提供されます。 特定の値を割り当てると、その AP にチャネルが静的に割り当てられます。
[Channel Width]	2.4 GHz のチャネル幅は 20 MHzにしか設定できません。	チャネル ボンディングを使用する場合、5 GHz のチャネル幅は [Automatic]、あるいは 20、40、または 80 MHz に設定できます。 チャネル ボンディングは、1 つの無線ストリーム用のチャネルを 2 つまたは 4 つのグループに分けます。これにより、速度とスループットが向上します。2.4 GHz のチャネル数が不十分である場合は、複数の非オーバーラップチャネルを有効にするためにチャネル ボンディングを使用することはできません。

パラメータ	説明
[Transmit Power]	[Automatic] に設定するか、または 1 ～ 8 の値を設定できます。 これは対数目盛の送信電力、つまり AP で使用される伝送エネルギーです。[1] が最高、[2] が [1] の半分、[3] が [1] の 1/4 となり、以下同様に減少していきます。 [Automatic] を選択すると、受信側の変動する信号レベルに基づいて、無線のトランスミッタ電力が調整されます。これによりトランスミッタは、フェーディング条件が発生した場合に、ほとんどの時間、最大電力未満で動作できるようになります。これが最大値に到達するまで、送信電力が必要に応じて増加します。

ステップ 6 [Apply] をクリックして変更を保存し、終了します。

WLAN ゲスト ユーザのログイン ページの設定

開始する前に、次の手順を実行してゲストユーザにネットワークへのアクセスを提供します。

1. ゲスト ユーザにアクセスを提供する新しい WLAN をセットアップするか、既存の WLAN を選択します。

   また、特定の WLAN をゲスト アクセス専用としてセットアップすることもできます。これを行うには、その WLAN の [WLAN Security] を [Guest] に設定します。詳細については、WLAN の追加 （2 ページ）を参照してください。

2. ゲスト ユーザ アカウントをセットアップします。[Wireless Settings] > [WLAN Users] の順に選択し、[Guest User] チェックボックスをオンにしてアカウントをセットアップします。詳細については、WLAN ユーザの表示と管理 （8 ページ）を参照してください。

WLAN のゲスト ユーザには、次のログイン ページ オプションを表示できます。

- わずかな変更オプションを備えたシンプルで必要最低限のデフォルトのログイン ページ。これを設定するには、デフォルトのログイン ページの設定 （17 ページ）を参照してください。
- コントローラにアップロードされたカスタマイズされたログイン ページ。これを設定するには、カスタマイズされたログイン ページの設定 （18 ページ）を参照してください。

デフォルトのログイン ページの設定

設定が不要なデフォルトのログインページにはシスコロゴとシスコ独自のテキストが含まれています。このデフォルトのログイン ページをここで説明するように変更できます。

ステップ 1 **[Wireless Settings]** > **[Guest WLAN]** の順に選択します。

[Guest WLAN] ページが表示されます。ネットワーク上にセットアップ済みのゲスト WLAN の数がページ上部に表示されます。

ステップ 2 デフォルトのログイン ページを使用するには、[Page Type] ドロップダウンリストで [Internal] を選択します。

ステップ 3 次のパラメータを設定して、デフォルトの内部ログイン ページを変更します。

- [Display Cisco Logo]：このフィールドはデフォルトで [Yes] に設定されています。デフォルト ウィンドウの右上に表示されるシスコの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。ただし、他のロゴを表示するためのオプションはありません。
- [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場合は、このフィールドにリダイレクト先の 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]：デフォルトのヘッドラインは「*Welcome to the Cisco Wireless Network*」です。ログイン ページに独自のヘッドラインを表示するには、このフィールドにヘッドライン文字列を入力します。最大 127 文字を入力することができます。
- [ページ メッセージ（Page Message）]：デフォルトのメッセージは「 シスコはお客様のネットワークに無線*LAN*インフラストラクチャを提供します。を開始するにはログインしてエア スペースを入力してください。（Cisco is pleased to provide the Wireless LAN infrastructure for your network. Please login and put your air space to work.）」です。ログイン ページに独自のメッセージを表示するには、このフィールドにメッセージ（2047 文字まで）を入力します。

ステップ 4 [Apply] をクリックします。

カスタマイズされたログイン ページの設定

コンピュータにカスタム ログイン ページを作成し、そのページとイメージ ファイルを .TAR ファイルに圧縮した後、コントローラにアップロードすることができます。アップロードは HTTP を介して行われます。

（注） コントローラの設定を保存する時点では、コントローラにダンロードし、保存した Web 認証バンドルなどの余分なファイルやコンポーネントは含まれません。そのため、そのようなファイルのコピーを手動で外部にバックアップします。

（注） Cisco TAC はカスタム Web 認証バンドルを作成する責任を負いません。

始める前に

- コンピュータ上でカスタム ログイン ページを作成して、以下を確認します。
  - ログイン ページの名前を **`login.html`** とします。コントローラは、この名前に基づいて Web 認証 URL を作成します。Web 認証バンドルの展開後にこのファイルが見つからない場合、そのバンドルは破棄され、エラー メッセージが表示されます。
  - このページには 6 つ以上のエレメント（HTML、CSS、およびイメージ）を含めないでください。これは、内部コントローラの Web サーバが実装する DoS 保護メカニズムにより、各クライアントが開く同時 TCP 接続が負荷に応じて最大 5 つに制限されるためです。ページに多くの要素が含まれていて、ブラウザによる DoS 保護の処理方法によっては、ページのロードが遅くなることがある場合、一部のブラウザでは、同時に 5 つを超える TCP セッションが開かれようとします。
  - ユーザ名とパスワード用のテキスト ボックスを含めます。
  - 元の URL からアクション URL を抽出して、ページに設定する。
  - リターン ステータス コードをデコードするスクリプトを提供する。
  - メインページで使用されるすべてのパス（たとえば、イメージへの参照など）が相対パスであること。
  - バンドル内のすべてのファイル名が 30 文字以内であること。
- ページとイメージファイルを TAR ファイルに圧縮します。ファイルの最大許容サイズは、非圧縮の状態で 1 MB です。

  シスコは、GNU 標準に準拠しているアプリケーションを使用して .TAR ファイル（Web 認証バンドルとも呼ばれる）を圧縮することをお勧めします。GNU に準拠していない .TAR 圧縮アプリケーションで Web 認証バンドルをロードすると、コントローラはバンドル内のファイルを抽出できません。

  .TAR ファイルはコントローラのファイル システムに未展開ファイルとして入力されます。

（注） 前述の前提要件に準拠していないカスタマイズされた複雑な Web 認証バンドルがある場合、シスコは外部 Web サーバでそれをホストすることをお勧めします。(..)を参照してください。

ステップ 1 **[Wireless Settings]** > **[Guest WLAN]** の順に選択します。

[Guest WLAN] ページが表示されます。ネットワーク上にセットアップ済みのゲスト WLAN の数がページ上部に表示されます。

ステップ 2 カスタマイズしたログイン ページをコントローラにアップロードするには、[Page Type] ドロップダウンリストで [Customized] を選択します。

ステップ 3 [Upload] をクリックし、カスタマイズした Web 認証バンドルの .TAR ファイルを参照してアップロードします。

ステップ 4 ログイン後にユーザを特定の URL（会社の URL など）にダイレクトさせる場合、[Redirect URL After Login] テキスト ボックスにその 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 5 [Apply] をクリックします。

[Preview] をクリックして、カスタマイズされた Web 認証ログイン ページを表示します。

内部 DHCP サーバの管理

Cisco Mobility Express コントローラには、内部 DHCP サーバが含まれています。このサーバは、それに関連付けられているネットワーク デバイスに割り当てられた DHCP アドレスを管理します。クライアントデバイスに割り当てられたIPアドレスはリブートすると失われます。これにより、複数のクライアント デバイスで IP アドレスを再利用できるようになります。IP アドレスの競合を解決するには、クライアント デバイスが既存の IP アドレスを解放し、新しいアドレスを要求する必要があります。

シスコ ワイヤレス リリース 8.3 以降、Cisco Mobility Express の Web インターフェイスを使用して内部 DHCP サーバを設定できます。

DHCP プールの追加

ステップ 1 **[Wireless Settings]** > **[DHCP Server]** を選択します。

[DHCP Configuration] ウィンドウが表示されます。

ステップ 2 [Add New Pool] をクリックします。

[Add DHCP Pool] ウィンドウが表示されます。

ステップ 3 [Pool Name] フィールドに、特定の名前を入力します。

DHCP プール名は、次の条件を満たしている必要があります。

ステップ 4 [Active] ドロップダウンリストから [Enabled] または [Disabled] のいずれかを選択します。

デフォルト設定では [Disabled] になっています。

ステップ 5 [VLAN ID] フィールドに、DHCP プールの VLAN ID を入力します。

（注） [Management Network] チェックボックスを選択し、Cisco Mobility Express コントローラの管理インターフェイス IP アドレスを DHCP サーバの IP アドレスとして設定します。

ステップ 6 [Network/Mask] フィールドに、ネットワークの IP アドレスとサブネットマスクを指定します。

ステップ 7 [Start IP] フィールドに、ネットワークの開始 IP アドレスを指定します。

ステップ 8 [End IP] フィールドに、ネットワークの終了 IP アドレス を指定します。

ステップ 9 [Default Gateway] フィールドに、ネットワークへのデフォルト ゲートウェイの IP アドレスを指定します。

（注） デフォルトのゲスト、開始 IP アドレス、および終了 IP アドレスは同じサブネット内にある必要があります。

ステップ 10 [Domain Name] フィールドに、特定の名前を入力します。

ドメイン名は、次の条件を満たしている必要があります。

ステップ 11 [Name Servers] ドロップダウンリストから、[OpenDNS] または [User Defined] のいずれかを選択します。

デフォルトの設定は [OpenDNS] です。

ステップ 12 表示されたフィールドにネーム サーバの IP アドレスを入力します。

DHCP プールの編集

ステップ 1 **[Wireless Settings]** > **[DHCP Server]** を選択します。

[DHCP Configuration] ウィンドウが表示されます。

ステップ 2 詳細を変更する DHCP プールが含まれている行で [edit_icon.gif] アイコンをクリックします。

DHCP プール テーブル内の特定の行が編集可能になります（または、[Edit DHCP Pool] ウィンドウが表示されます）。

ステップ 3 [DHCP Pool] テーブルで、特定の変更をインラインします（または、[Edit DHCP Pool] ウィンドウに表示します）。

ステップ 4 [Apply] をクリックします。

[DHCP Pool] テーブルが更新され、更新したエントリがこのテーブルに表示されます。

DHCP プールの削除

ステップ 1 **[Wireless Settings]** > **[DHCP Server]** を選択します。

[DHCP Configuration] ウィンドウが表示されます。

ステップ 2 削除する DHCP プールが含まれている行で [X] アイコンをクリックします。

警告メッセージが表示されます。

ステップ 3 ポップアップ ウィンドウで [Yes] をクリックします。

[DHCP Pool] テーブルが更新され、削除したエントリがこのテーブルから削除されます。

DHCP リースの詳細の表示

ステップ 1 **[Wireless Settings]** > **[DHCP Server]** を選択します。

[DHCP Configuration] ウィンドウが表示されます。

ステップ 2 [DHCP Pool] テーブルに下にある [DHCP Leases] をクリックします。

[DHCP Pool Information] ウィンドウが表示されます。このウィンドウでは、ホスト名、その MAC アドレス、割り当てられている IP アドレス、リースの有効期限の詳細など、詳細情報を表示できます。

（注） [DHCP Pool Information] テーブルの対応するエントリでホストへのリースを削除することで、特定の IP アドレスを開放できます。

リース IP アドレスの詳細のエクスポート

ステップ 1 **[Wireless Settings]** > **[DHCP Server]** を選択します。

[DHCP Configuration] ウィンドウが表示されます。

ステップ 2 [DHCP Pool] テーブルに下にある [DHCP Leases] をクリックします。

[DHCP Pool Information] ウィンドウが表示されます。

ステップ 3 [DHCP Pool Information] テーブルに下にある [Export] をクリックします。

ステップ 4 リース IP アドレスと対応するホストの詳細をエクスポートする形式を選択します。

リース IP アドレスの開放

ステップ 1 **[Wireless Settings]** > **[DHCP Server]** を選択します。

[DHCP Configuration] ウィンドウが表示されます。

ステップ 2 [DHCP Pool] テーブルに下にある [DHCP Leases] をクリックします。

[DHCP Pool Information] ウィンドウが表示されます。

ステップ 3 削除するリース IP アドレスが割り当てられたホストを含む行で、[release_icon.gif] アイコンをクリックします。

警告メッセージが表示されます。

ステップ 4 [DHCP Pool Information] テーブルの対応するエントリでリースを削除することで、特定の IP アドレスを開放できます。

ステップ 5 ポップアップ ウィンドウで [Yes] をクリックします。

[DHCP Pool Information] テーブルが更新され、削除したエントリがこのテーブルから削除されます。