CHAPTER 4

キャプティブ ポータル ルールの定義

キャプティブ ポータル ルールにより、キャプティブ ポータルの表示および SSID に接続している顧客のインターネット プロビジョニングを管理できます。

キャプティブ ポータル ルールを使用して、次の方法で、キャプティブ ポータルの表示およびインターネット プロビジョニングを管理できます。

- キャプティブ ポータルの表示:ルールに応じてフィルタリングされた顧客が、ルールに応じて設定された SSID に接続すると、キャプティブ ポータルが表示されます。顧客は必要な認証の手順が完了すると、ポータルのメニュー項目をクリックして、インターネットにアクセスできます。顧客のロケーション、アクセス数、顧客が属するタグ、ユーザのロケーションへのアクセス数、アクセスの時間などに基づき、顧客に合ったさまざまなキャプティブ ポータルを表示するように設定できます。
- 直接インターネット アクセス:ルールに応じてフィルタリングされた顧客が、ルールに応じて設定された SSID に接続すると、認証プロセスなしで、インターネットが即座にプロビジョニングされます。この場合、キャプティブ ポータルは表示されません。
- インターネット アクセスの拒否:ルールに応じてフィルタリングされた顧客が SSID に接続しようとすると、インターネットが拒否されて接続を確立できません。

また、キャプティブ ポータル ルールにより、次の操作を行うことができます。

- ルールのフィルタリングに基づいて、タグを作成または既存のタグを変更します。
- 外部 API へのキャプティブ ポータルにサインインする顧客の詳細を送信します。

キャプティブ ポータル ルールでは、定義された条件が満たされているときに実行するアクションを設定できます。ロケーション、タグ、顧客のアクセスの数や時間、アプリケーションのステータスなど、さまざまなパラメータに基づいて、ルールに応じて顧客をフィルタリングできます。

この章では、キャプティブ ポータル ルールを作成する方法について説明します。

キャプティブ ポータル ルールの作成

キャプティブ ポータル ルールを作成するには、次の手順を実行します。

1. アクセス ポイントのモードの設定、ワイヤレス LAN コントローラ(WLC)での SSID および ACL の作成(4-2 ページ)
2. インターネット プロビジョニングおよび RADIUS 認証に関する CUWN の設定(4-2 ページ)
3. WiFi Engage へのアクセス(3-2 ページ)
4. 手動での SSID のインポート(4-3 ページ)
5. ロケーション階層の定義(3-2 ページ)

6. ポータルの作成（4-4 ページ）
7. タグの作成（4-5 ページ）
8. キャプティブ ポータル ルールの定義（4-5 ページ）

（注）　キャプティブ ポータルを設定するには、CUWN アカウント（MSE/CMX と WLC）および WiFi Engage アカウントが必要です。CUWN プロパティは、ワイヤレス LAN コントローラ（WLC）で設定されます。

アクセス ポイントのモードの設定、ワイヤレス LAN コントローラ（WLC）での SSID および ACL の作成

キャプティブ ポータル ルールを作成するには、まずアクセス ポイントのモードを定義し、ワイヤレス LAN コントローラで SSID と ACL を作成します。キャプティブ ポータルの設定に必要な WLC の設定の詳細については、「ワイヤレス LAN コントローラの設定」セクション（4-11 ページ）を参照してください。

インターネット プロビジョニングおよび RADIUS 認証に関する CUWN の設定

ポータルにセキュリティのその他の層を提供するために、WiFi Engage はキャプティブ ポータルのインターネット プロビジョニングに対する RADIUS 認証をサポートします。また、インターネット プロビジョニングを管理するには、CUWN に特定の設定が必要です。キャプティブ ポータル ルールを使用するには、CUWN で次の設定を行う必要があります。

ステップ 1　WLC のクレデンシャルで WLC にログインします。

ステップ 2　WLC のメイン ウィンドウで、[Security]タブをクリックします。

ステップ 3　[Radius] > [Authentication]の順に選択します。

ステップ 4　[New]をクリックします。

ステップ 5　表示された [New] ページで、サーバの IP アドレス、ポート番号、秘密鍵などの認証用の RADIUS サーバの詳細を入力し、[Server Status] に [Enabled]を選択し、[Apply] をクリックします。

- Port Number：1812

注　WiFi Engage の RADIUS サーバだけを設定できます。RADIUS サーバの IP アドレスと秘密鍵については、Cisco EMSP のサポート チームに連絡する必要があります。

ステップ 6　[Radius] > [Accounting]の順に選択します

ステップ 7　[New]をクリックします。

ステップ 8　表示された [New] ページで、サーバの IP アドレス、ポート番号、秘密鍵などのアカウンティング用の RADIUS サーバの詳細を入力し、[Server Status] に [Enabled]を選択し、[Apply] をクリックします。

- Port Number: 1813

注　WiFi Engage の RADIUS サーバだけを設定できます。RADIUS サーバの IP アドレスと秘密鍵については、Cisco EMSP のサポート チームに連絡する必要があります。

ステップ 9　WLC のメイン ウィンドウで、[WLANs]タブをクリックします。

ステップ 10　キャプティブ ポータル ルールの SSID の WLAN をクリックします。

ステップ 11　[Security]を選択します。

ステップ 12　[Layer 2] タブで、[MAC Filtering]チェックボックスをオンにします。

ステップ 13　[Layer 3] タブで、次が設定されていることを確認します。

- [Layer 3 security] ドロップダウン リストで、[Web Policy]と [Mac Filter Failure] ラジオ ボタンが選択されています。

（注）　SSID を作成するときに、[Layer 3] でこれらの設定が実行されます。

ステップ 14　[AAA Servers] タブの、[Radius Servers] 領域で、次の手順を実行します。

a. [Authentication Servers] の [Enabled]チェックボックスをオンにします。

b. [Server 1] ドロップダウン リストで、先に定義した RADIUS サーバを選択します。

ステップ 15　[web-auth user] 領域の認証の優先順位に、[Order Used for Authentication] ボックスで、[Radius]を順序の先頭に設定します。

注　[Up] および [Down] ボタンを使用し、順序を並び替えます。

ステップ 16　[Advanced]タブをクリックし、[Allow AAA Override] の [Enabled] チェックボックスをオンにします。

ステップ 17　[Apply]をクリックします。

ステップ 18　ウォールガーデンが ACL に応じて設定されていることを確認します。ウォールガーデンの設定の詳細については、「ワイヤレス LAN コントローラの設定」セクション（4-11 ページ）を参照してください。

WiFi Engage へのアクセス

WiFi Engage へアクセスする手順については、「WiFi Engage へのアクセス」セクション（3-2 ページ）で説明しています。

手動での SSID のインポート

SSID とは、Wi-Fi 経由でインターネットにアクセスするために接続するネットワーク ID のことです。CUWN の SSID のキャプティブ ポータル ルールを作成するには、ワイヤレス LAN コントローラ（WLC）からその SSID を手動でインポートする必要があります。

(注)　CUWN では、SSID を WiFi Engage に手動でインポートする必要があります。WiFi Engage で指定した SSID 名は、WLC で設定されている SSID 名と一致する必要があります。WLC の SSID 名を表示できます。WiFi Engage に SSID を追加するには、最初にワイヤレス LAN コントローラ（WLC）でその SSID を定義する必要があります。WLC で SSID を作成する方法については、「ワイヤレス LAN コントローラの設定」セクション（4-11 ページ）を参照してください。

(注)　SSID は MSE/CMX ではなく WLC で設定されます。

SSID を WiFi Engage に手動でインポートするには、次の手順を実行します。

ステップ 1　WiFi Engage ダッシュボードで [SSIDs]を選択し、[Import] をクリックします。

ステップ 2　[Please Select SSID To Import] ウィンドウで、インポートする必要のある SSID の名前を入力し、[Add SSID]をクリックします。

インポートされた SSID が [SSIDs] ウィンドウに表示されます。

(注)　インポートされた SSID をロードするときには WiFi Engage を CUWN と同期させる必要があるので、ウィンドウを更新してインポートされた SSID を表示することが必要な場合があります。

ロケーション階層の定義

ルールのロケーションを選択するには、ロケーション階層を定義する必要があります。ロケーション階層を定義する手順については、「ロケーション階層の定義」セクション（3-2 ページ）で説明しています。

ポータルの作成

ポータルは、Wi-Fi ユーザが SSID に接続したときに表示されるユーザ インターフェイスです。キャプティブ ポータルを作成し、WiFi Engage から提供されるさまざまなポータル モジュールを使用して、ポータルを強化できます。

ポータルを定義するときに、ポータルを利用可能にする必要があるロケーションを設定することもできます。

(注)　この手順はキャプティブ ポータル ルールのポータルを設定するときにのみ必要です。

ポータルを作成するには、次の手順を実行します。

ステップ 1　WiFi Engage ダッシュボードで、[Portal]を選択し、[Create New] をクリックします。

ステップ 2　表示される [Portal] ウィンドウで、ポータルの名前を [Name]フィールドに入力します。

ステップ 3　すべてのロケーションでポータルを利用可能にする場合は、[This portal will be available in all locations] チェックボックスをオンにします。それ以外の場合は、ポータルを利用可能にする必要があるロケーションを選択します。

ステップ 4　[Create]をクリックします。

ポータル ページでは、左側にポータル モジュールが、右側にポータル プレビューが表示されます。

ステップ 5　ポータル モジュールを使用してポータルに機能を追加します。

（注）　名前や電話番号などの顧客の詳細をキャプチャするには、キャプティブ ポータルに [Data Capture] モジュールを追加します。インターネットをプロビジョニングする前に、データ キャプチャ フォームが顧客に表示されます。キャプチャされた顧客の詳細は、WiFi Engage データベースに保存されます。[Data Capture] モジュールは、Hard SMS with Verification Code および Email 認証タイプで使用できます。

ステップ 6　[Save]をクリックして、各モジュールに加えた変更を保存します。

ステップ 7　ポータルをパブリッシュするには、[Portal] ウィンドウで、ポータルの [Publish]ボタンをクリックします。

タグの作成

キャプティブ ポータル ルールでタグ フィルタを使用するには、タグを作成する必要があります。タグを定義する手順は、「プロファイル ルールを使用したタグの作成または既存のタグへの顧客の追加または除外」セクション（6-1 ページ）で定義されています。

（注）　この手順はキャプティブ ポータル ルールでタグ フィルタを使用するときにのみ必要です。

キャプティブ ポータル ルールの定義

CUWN 設定、ロケーション階層などの前提条件を満たした後、キャプティブ ポータル ルールを定義できます。前提条件は、ルールで使用するフィルタによって異なります。

顧客のロケーション、顧客がオプトイン ユーザかどうか、顧客が属するタグ、顧客のアクセス回数、顧客のデバイスのアプリケーションの状態などに基づいて、ルールを適用する顧客をフィルタリングできます。ロケーションまたはそのロケーションに関連付けられているメタデータに基づいて、ルールが適用されるロケーションをフィルタリングできます。指定された時間内に指定したロケーションへの顧客によるアクセス回数に基づき、ルールを適用できます。また、特定の期間だけ、特定の曜日だけ、および特定の時間だけ、ルールを適用するように設定できます。キャプティブ ポータル ルールにより、ルールに応じてフィルタリングされた顧客が SSID に接続する際に、直接インターネット接続を提供するように設定することもできます。この場合、キャプティブ ポータルは表示されませんが、顧客はインターネットへアクセスできるようになります。また、ルールに応じてフィルタリングされた顧客にインターネット アクセスを拒否するようにも設定できます。

キャプティブ ポータル ルールを使用して、新しいタグを作成、またはルールに応じてフィルタリングされた顧客の既存のタグを変更できます。キャプティブ ポータル ルールはまた、ルールに応じて設定されている SSID に接続されている顧客の詳細を外部 API へ送信します。

ポータルを表示するキャプティブ ポータル ルールを作成するには、次の手順を実行します。

ステップ 1　WiFi Engage ダッシュボードで、[Proximity Rules] > [Captive Portal Rule]の順に選択します。

ステップ 2　[Create a new rule]をクリックします。

ステップ 3　[Rule Name] テキスト フィールドに、キャプティブ ポータル ルールの名前を入力します。

ステップ 4　[Sense] 領域で、次の手順を実行します。

a. [When a user is on] の後のドロップダウン リストから、[WiFi]を選択します。

b. [and connected to] の後のドロップダウン リストから、キャプティブ ポータルを表示する SSID を選択します。

（注）　SSID は SSID をインポートした場合にのみ選択することができます。SSID のインポートの詳細については、「手動での SSID のインポート」セクション（4-3 ページ）を参照してください。

ステップ 5　[Location] 領域で、ルールを適用するロケーションを指定します。

ロケーション階層全体、1 つまたは複数の MSE、キャンパス、グループ、ビルディング、フロア、ゾーンにルールを適用するように設定できます。ロケーション階層の作成の詳細については、「ロケーション階層の定義」セクション（3-2 ページ）を参照してください。

また、選択したロケーション、またはその親や子のロケーションに定義されているメタデータに基づいてロケーションをフィルタリングできます。ロケーションに対するメタデータの設定の詳細については、「ロケーション要素のメタデータの定義」セクション（3-7 ページ）を参照してください。特定のメタデータのロケーションにルールを適用するか、または特定のメタデータのロケーションを除外することができます。

ルールを適用するロケーションを指定するには、次の手順を実行します。

a. [Add Locations]ボタンをクリックします。

b. 表示される [Choose Location] ウィンドウで、キャプティブ ポータル ルールを適用するロケーションを選択します。

c. [OK]をクリックします。

特定のメタデータのロケーションにルールを適用するには、次の手順を実行します。

a. [Filterby Metadata] チェックボックスをオンにします。

b. [Filter] 領域で、[Add Metadata] ボタンをクリックします。

[Choose Location Metadata] ウィンドウが表示されます。

c. ドロップダウン リストから、メタデータの変数を選択し、隣接フィールドに変数の値を選択します。

d. [OK]をクリックします。

特定のメタデータのロケーションを除外するには、次の手順を実行します。

a. [Filterby Metadata] チェックボックスをオンにします。

b. [Exclude] 領域で、[Add Metadata] ボタンをクリックします。

[Choose Location Metadata] ウィンドウが表示されます。

c. ドロップダウン リストから、メタデータの変数を選択し、隣接フィールドに変数の値を選択します。

d. [OK]をクリックします。

ステップ 6　[IDENTIFY] 領域には、ポータルを表示する顧客のタイプを指定します。

(注)　顧客がオプトイン ユーザかどうか、顧客が属するタグ、顧客のアクセス回数、顧客のデバイスのアプリケーションの状態などに基づいてルールを適用する顧客をフィルタリングできます。これらのフィルタをすべて適用することも、要件に応じて一部を適用することもできます。

キャプティブ ポータル ルールが適用される顧客を指定するには、次の手順を実行します。

a. オプトイン ステータスにより顧客をフィルタリングする場合、[Filter by OptIn Status] チェックボックスをオンにし、[Only for] ドロップダウン リストから、オプトイン ユーザまたは非オプトイン ユーザのどちらをフィルタリングするかを選択します。

注　オプトイン ユーザの詳細については、「オプトイン ユーザ」セクション（6-6 ページ）を参照してください。

b. タグに基づいて顧客をフィルタリングするには、[Filter by Tags]チェックボックスをオンにします。

注　2 つの異なる方法でタグをフィルタリングできます。ルールを適用する必要のあるタグを指定することも、ルールを適用しないタグを指定することもできます。要件に基づいて、最適なフィルタリング方法を選択できます。たとえば、1 つのタグを除くすべてのタグの顧客にルールを適用する場合、除外オプションを選択し、ルールを適用しない特定のタグを指定する方法が簡単です。

- 選択したタグの顧客にルールが適用されるようにタグを含めるには、[Add Tags] ボタンを使用して「含め」ます。
- 除外したタグの顧客にルールを適用しないようにするには、[Add Tags]ボタンを使用して「除外」します。

タグ フィルタの使用の詳細については、「タグによるフィルタリング」セクション（6-5 ページ）を参照してください。

c. 選択したロケーションの顧客のアクセスの数に基づいて顧客をフィルタリングするには、[Filter by Previous Visits]チェックボックスをオンにします。

[Add Locations]ボタンをクリックします。[Choose location] ウィンドウで、フィルタリングについて検討する必要がある顧客のアクセス先を選択します。次のフィールドで、フィルタリング対象のアクセス数と時間を指定します。自分で設定できるアクセスと時間の詳細については、「通知基準」セクション（5-18 ページ）を参照してください。

d. 顧客のアプリケーションのステータスに基づいて顧客をフィルタリングするには、[Filter by App Status]チェックボックスをオンにします。[Filter by the users who] ドロップダウン リストから、ルールを適用できるアプリケーションのステータスを選択します。

ステップ 7　[Schedule] 領域で、ルールを適用する期間を指定します。

a. [Set a time range for the rule] チェックボックスをオンにし、表示されるフィールドに、キャプティブ ポータル ルールを適用する時間範囲を指定します。

b. [Set a date range for the rule] チェックボックスをオンにし、表示されるフィールドに、キャプティブ ポータル ルールを適用する期間の開始日と終了日を指定します。

c. 特定の曜日にだけルールを適用するには、[Filter by days of the week] チェックボックスをオンにし、表示される曜日のリストから、ルールを適用する曜日を選択します。

ステップ 8　[Actions] 領域で、前述の条件が満たされたときに実行する操作を設定します。

a. ルールに応じてフィルタリングされた顧客のインターネットのプロビジョニングを管理するには、次から必要なオプションを選択してください。

- Show CaptivePortal：キャプティブ ポータル ルールに応じてフィルタリングされた顧客が、ルールを設定した SSID に接続するときに、キャプティブ ポータルを表示するには、このオプションを選択します。[Show them Portal] ドロップダウン リストから、このルールで定義された条件が満たされているときに表示するキャプティブ ポータルを選択します。選択したロケーションに作成したポータルを選択することができます。ポータルの作成の詳細については、「ポータルの作成」セクション（4-4 ページ）を参照してください。
- Seamlessly ProvisionInternet：顧客が SSID に接続するとすぐに顧客にインターネットを提供するには、このオプションを選択します。この場合、顧客は認証の手順を実行する必要がありません。[Seamlessly Provision Internet] オプションを使用するには、WLC で必要な設定が行われていることを確認します。WLC で必要な設定の詳細については、「インターネット プロビジョニングおよび RADIUS 認証に関する CUWN の設定」セクション（4-2 ページ）を参照してください。
  - [Session Duration] フィールドには、各接続にインターネット アクセスを提供する期間を指定します。
  - [Bandwidth Limit] フィールドで、提供する帯域幅を選択します。1 tbps の最大帯域幅を選択できます。

注　ワイヤレス ネットワークが CUWN の場合、ルール/ポリシー名は不要です。

- DenyInternet：顧客が SSID に接続しようとしたときに、ルールに応じてフィルタリングされた顧客にインターネットを拒否するには、このオプションを選択します。この場合、顧客は SSID への接続が許可されません。

b. このキャプティブ ポータル ルールに基づいてフィルタリングされた顧客にタグを作成する、または、フィルタリングされた顧客を既存のルールに追加または削除するには、[Add Tags]ボタンをクリックします。タグ フィルタの使用の詳細については、「タグによるフィルタリング」セクション（6-5 ページ）を参照してください。

c. 外部 API に通知を送信するには、[Trigger API] チェックボックスをオンにします。

- [Method] ドロップダウン リストから、API をトリガーするメソッドを選択します。

注　API URI またはメソッド パラメータにスマート リンク変数を追加することで、通知メッセージに顧客の詳細を追加できます。

  - Get：get メソッドを使用して API に通知を送信します。このメソッドを選択すると、要求パラメータを指定できる追加のフィールドが表示され、顧客の名、姓、携帯番号などの追加情報を通知に含めることができます。API で定義された要求パラメータのキーを追加し、スマート リンクを使用して、これらの値を指定できます。値はハードコード値または変数のどちらでもかまいません。隣接する [Add Variable] ドロップダウン リストを使用するか、または値フィールドに「$」を入力して、スマート リンク変数を追加できます。スマート リンクの詳細については、「Smart Link」セクション（7-42 ページ）を参照してください。[add]ボタンを使用して、さらに「get パラメータ」を追加できます。

- Post Form：post form メソッドを使用して API に通知を送信します。このメソッドを選択すると、form パラメータを指定できる追加のフィールドが表示され、顧客の名、姓、携帯番号などの追加情報を通知に含めることができます。API に定義されている form パラメータのキーを追加し、それらの値を指定できます。値は、ハードコード値または変数のどちらでもかまいません。隣接する [Add Variable] ドロップダウン リストを使用するか、または値フィールドに「$」を入力して、form パラメータ変数として変数を追加できます。スマート リンクの詳細については、「Smart Link」セクション（7-42 ページ）を参照してください。[add] ボタンを使用して、さらに「form パラメータ」を追加できます。
- Post Json：post json メソッドを使用して API に通知を送信します。このメソッドを選択すると、API に通知メッセージとして送信する json データを指定できるテキスト ボックスが表示されます。API で定義されるさまざまな json フィールドの json 値を指定できます。値はハードコード値または変数のどちらでもかまいません。隣接する [Add Variable] ドロップダウン リストを使用するか、またはテキスト ボックスに「$」を入力して、json 値として変数を追加できます。スマート リンクの詳細については、「Smart Link」セクション（7-42 ページ）を参照してください。
- Post Body：post body メソッドを使用して API に通知を送信します。このメソッドを選択すると、API に送信する通知に含める必要がある内容を指定できる追加のフィールドが表示されます。

- [URI] テキスト フィールドに、API の URI を入力します。スマート リンクを使用して通知メッセージに顧客の詳細を含めることができます。[Add Variable] ドロップダウン リストをクリックするか、テキスト ボックスに「$」を入力して変数を表示します。スマート リンクの詳細については、「Smart Link」セクション（7-42 ページ）を参照してください

注　ポータルの [Data Capture] モジュールを使用してキャプチャするように設定されたこれらのスマート リンク変数だけが通知に含まれます。

（注）　ルールの概要がページの右側に表示されます。

ステップ 9　[Save]をクリックします。

ルールは [Captive Portal Rules] ページに表示されます。

ステップ 10　ルールの右端の [Make Rule Live]アイコンをクリックします。

キャプティブ ポータル ルールがパブリッシュされます。

例

XYZ は、モバイル ストアからスーパーマーケットまで、さまざまな事業のストリームラインに関わっているビジネス グループです。XYZ はニューヨークの各地に 5 軒のモバイル ストアと 4 軒のスーパーマーケットを展開しています。ニューヨークの XYZ の SSID は XYZID です。XYZ は顧客が XYZ のスーパーマーケットから XYZID に接続すると、スーパーマーケットのさまざまな品目が利用可能なオファーを表示する、キャプティブ ポータル C1 を表示したいと考えています。同様に、キャプティブ ポータル C2 は、XYZ のモバイル ストアから XYZID に接続する顧客に表示される必要があります。キャプティブ ポータルは、オプトインではないユーザに表示される必要があります。

スーパー マーケットのロケーション：L1、L2、L3、L4、L5

モバイル ストアのロケーション：L7、L8、L9、L10

前述のシナリオを実現するには、次の手順を実行します。

ステップ 1　WLC で、アクセスポイントのモードを定義し、ACL を作成し、SSID の XYZID を作成します。WLC 設定の詳細については、ワイヤレス LAN コントローラの設定（4-11 ページ）を参照してください。

ステップ 2　WiFi Engage にログインします。

ステップ 3　[Import SSID] オプションを使用して、WiFi Engage に XYZID を追加します。

ステップ 4　XYZ のロケーション階層を作成します。ロケーション階層では、ニューヨークの XYZ のすべてのスーパーマーケットとモバイル ストアが、ロケーション [New York] の下のロケーション要素として定義される必要があります。キーが[StoreType]、値が [SM]の、ロケーション L1、L2、L3、L4、L5 のロケーション メタデータを追加します。キーが[StoreType]、値が [MS]の、ロケーション L7、L8、L9、L10 のロケーション メタデータを追加します。ロケーション メタデータの定義の詳細については、「ロケーション要素のメタデータの定義」セクション（3-7 ページ）を参照してください。

ステップ 5　スーパーマーケットのポータル **C1** と、モバイル ストアのポータル **C2** を作成します。ポータルの作成の詳細については、「ポータルの作成」セクション（4-4 ページ）を参照してください。

ステップ 6　WiFi Engage ダッシュボードで、[Proximity Rules] > [Captive Portal Rule]の順に選択します。

ステップ 7　[Create a new rule]をクリックします。

ステップ 8　[RULE NAME] フィールドに、キャプティブ ポータル ルールの名前 **R1** を入力します。

ステップ 9　[When a user is on] ドロップダウン リストから [WiFi]を、[and connected to] ドロップダウン リストから [XYZID] を選択します。

ステップ 10　[Locations] 領域で、次の手順を実行します。

a. [Add Locations]ボタンをクリックし、表示される [Choose Location] ウィンドウで、ニューヨークのロケーションを選択し、[OK] をクリックします。

b. [Filter by metadata] チェックボックスをオンにし、フィルタの [Add Metadata]ボタンをクリックします。

c. [Choose Location Metadata] ウィンドウで、キーに [StoreType]を選択し、値に [SM] を選択します。

注　ロケーション メタデータ「StoreType」は、ロケーション「New York」の下にあるロケーションに定義されているため、[Choose Location Metadata] ウィンドウで選択することができます。

ステップ 11　[Identify] 領域で、[Filter by OptIn Status] チェックボックスをオンにし、[Only for] ドロップダウン リストから[not Opted In Users] を選択します。

ステップ 12　[Schedule] 領域で、[Set a date range for the rule] チェックボックスをオンにし、開始日に今日の日付を、終了日に今年の最後の日付を指定します。

ステップ 13　[Actions] 領域で、[Show them Portal] ドロップダウン リストから [C1]を選択します。

ステップ 14　[Save]をクリックします。

ルールは [Captive Rules] ページでパブリッシュされます。

ステップ 15　[Captive Rules] ページの [Make Rule Live]アイコンをクリックして、ルールをパブリッシュします。

ステップ 16　同様に、ロケーション メタデータ キーが[StoreType]、値が [MS]、キャプティブ ポータルが [C2]の、別のルール **R2** を、モバイル グループ用に作成します。

これで、顧客が XYZ のスーパーマーケットにアクセスして XYZID に接続すると、**C1** が表示されます。同じ顧客が XYZ のモバイル ストアから XYZID に接続すると、**C2** が表示されます。

ワイヤレス LAN コントローラの設定

CUWN の設定は WLC で行われます。ローカルと flexconnect モードの WLC の設定は異なります。

- WiFi Engage を使用するためのローカル モード設定（4-11 ページ）
- WiFi Engage を使用するための FlexConnect モードの設定（4-14 ページ）

（注）　設定は、WLC で行われ、これは Enterprise Mobility Services Platform の一部ではありません。またこのマニュアル内のメニュー パス、タブに指定された名前、ウィンドウ、オプションなどが変更されることがあります。

（注）　SSID と ACL は MSE/CMX ではなく WLC で作成されます。

WiFi Engage を使用するためのローカル モード設定

ローカル モードで WiFi Engage を使用するように WLC を設定するには、次の手順を実行します。

1. アクセス ポイントのローカル モードを設定する（4-11 ページ）
2. アクセス コントロール リストの作成（4-11 ページ）
3. CUWN で SSID を作成する（4-12 ページ）
4. 仮想インターフェイスの設定（4-13 ページ）

アクセス ポイントのローカル モードを設定する

アクセス ポイントのローカル モードを設定するには、次の手順を実行します。

ステップ 1　WLC のクレデンシャルで WLC にログインします。

ステップ 2　WLC のメイン ウィンドウで、[WIRELESS]タブをクリックします。
すべてのアクセス ポイントが一覧表示されます。

ステップ 3　モードをローカルに設定するアクセス ポイントをクリックします。

ステップ 4　[General]タブをクリックします。

ステップ 5　[AP Mode] ドロップダウン リストから、[local]を選択して、[Apply] をクリックします。

アクセス コントロール リストの作成

アクセス コントロール リストを作成するには、次の手順を行います。

ステップ 1　WLC のクレデンシャルで WLC にログインします。

ステップ 2　[Security] > [Access Control Lists] > [Access Control Lists]を選択します。

ステップ 3　ACL を追加するには、[New]をクリックします。

ステップ 4　表示される [New] ページに次の情報を入力します。

a. [Access Control List Name] フィールドに新しい ACL の名前を入力します。

注　最大 32 文字の英数字を入力できます。

b. ACL タイプとして [IPv4]を選択します。

c. [Apply]をクリックします。

ステップ 5　[Access Control Lists] ページが再度表示されたら、新しい ACL の名前をクリックします。

ステップ 6　表示される [Edit] ページで、[Add New Rule]をクリックします。

[Rules > New] ページが表示されます。

ステップ 7　必要なウォールガーデンの範囲にこの ACL のルールを設定します。

ウォールガーデンの範囲を表示するには、WiFi Engage で [SSIDs] ウィンドウの [Configuration Instructions] リンクをクリックします。

ACL ルールを定義するときには、次のように値を設定します。

- **Direction**: Any
- **Protocol**: Any
- **Source Port Range**: 0-65535
- **Destination Port Range**: 0-65535
- **DSCP**: Any
- **Action**: Permit

CUWN で SSID を作成する

(注)　SSID は MSE/CMX ではなく WLC で作成されます。

WLC で SSID を作成するには、次の手順を実行します。

ステップ 1　WLC のメイン ウィンドウで、[WLANs]タブをクリックします。

ステップ 2　WLAN を作成するには、ページの右端にあるドロップダウン リストで [Create New]を選択し、[Go] をクリックします。

ステップ 3　表示される [New] ページで、[Type]、[Profile Name]、[SSID] などの WLAN の詳細を入力します。

ステップ 4　[Apply]をクリックします。

[SSID Name] ページが表示されます。

ステップ 5　[General] タブでは、[Broadcast SSID] チェックボックスをオフにします。

ステップ 6　[Security] > [Layer 2]を選択し、[Layer 2 Security] を [None] に設定します。

ステップ 7　[Layer 3]タブで、次を設定します。

a. [Layer 3 security] ドロップダウン リストから、[Web Policy]を選択します。

b. [On Mac Filter Failure]ラジオ ボタンを選択します。

c. [Preauthentication ACL] 領域で、[IPv4] ドロップダウン リストから、先に定義した ACL を選択します。

d. [Sleeping Client] の [Enable] チェックボックスをオンにします。

e. [Override Global Config] の [Enable] チェックボックスをオンにします。

f. [Web Auth Type] ドロップダウン リストから [External (Redirect to External Server)]を選択します。

g. 表示される [URL] フィールドに、WiFi Engage のスプラッシュ URL を入力します。

CUWN アカウントのスプラッシュ URL を表示するには、WiFi Engage で、[SSIDs] ウィンドウの [Configuration Instructions] リンクをクリックします。

注　また、スプラッシュ URL として スタジオ URL を設定できます。キャプティブ ポータル URL としてのスタジオ URL の設定の詳細については、「Enterprise Mobility Services Platform Studio URL のキャプティブ ポータル URL としての設定」セクション（7-26 ページ）を参照してください。

h. [Apply]をクリックします。

ステップ 8　[Advanced]タブをクリックします。

ステップ 9　[Enable Session Timeout] フィールドに、**1800** と入力して [Apply] をクリックします。

ステップ 10　[General] タブで、[Status] および [Broadcast SSID] オプションの [Enabled] チェックボックスをオンにし、SSID を有効にします。

ステップ 11　コマンド プロンプトで次のコマンドを実行して、キャプティブ バイパスを無効にします。その後、WLC を再起動します。

config network web-auth captive-bypass disable

ステップ 12　[Management] > [HTTP-HTTPS]を選択します。

ステップ 13　表示される [HTTP-HTTPS configuration] ページで、次を実行します。

a. [HTTP Access] ドロップダウン リストから、[Disabled]を選択します。

b. [HTTPS Access] ドロップダウン リストから、[Enabled]を選択します。

c. [WebAuth SecureWeb] ドロップダウン リストから、[Disabled]を選択します。

d. [Apply]をクリックします。

ステップ 14　[Security] >[Web Auth] > [Web Login Page] の順に選択し、[Redirect URL after login] フィールドが空白であることを確認します。

（注）　[Management] タブに変更を加えた場合は、変更を反映するために WLC を再起動します。

仮想インターフェイスの設定

仮想インターフェイスを設定するには、次の手順を実行します。

ステップ 1　[Controller]> [Interfaces] の順に選択します。

ステップ 2　[Virtual]リンクをクリックします。

ステップ 3　表示される[Interfaces > Edit] ページで、次のパラメータを入力します。

a. [IP address] フィールドに、未割り当ておよび未使用のゲートウェイ IP アドレス（存在する場合）を入力します。

b. [DNS Host Name] フィールドに、DNS ホスト名（存在する場合）を入力します。

注　理想的には、このフィールドは空白になります。

注　接続して Web 認証を確立するには、DNS サーバは常に仮想インターフェイスをポイントしている必要があります。仮想インターフェイスに DNS ホスト名が設定されている場合は、クライアントが使用する DNS サーバ上で同じ DNS ホスト名が設定されている必要があります。

c. [Apply]をクリックします。

（注）　仮想インターフェイスに変更を加えた場合は、変更を反映するために WLC を再起動します。

WiFi Engage を使用するための FlexConnect モードの設定

中央スイッチまたはローカル スイッチのモードに FlexConnect を設定できます。

FlexConnect 中央スイッチ モード

FlexConnect 中央スイッチ モードで WiFi Engage を使用するように WLC を設定するには、次の手順を実行します。

1. アクセス ポイントの FlexConnect モードを設定する（4-14 ページ）。
2. FlexConnect 中央スイッチ モードのアクセス コントロール リストの作成（4-15 ページ）
3. FlexConnect 中央スイッチ モードの CUWN での SSID の作成（4-15 ページ）
4. 仮想インターフェイスの設定（4-13 ページ）

FlexConnect ローカル スイッチ モード

FlexConnect ローカル スイッチ モードで WiFi Engage を使用するように WLC を設定するには、次の手順を実行します。

1. アクセス ポイントの FlexConnect モードを設定する（4-14 ページ）
2. FlexConnect のローカル スイッチ モードでのアクセス コントロール リストの作成（4-15 ページ）
3. FlexConnect のローカル スイッチ モードの CUWN での SSID の作成（4-16 ページ）
4. 仮想インターフェイスの設定（4-13 ページ）

アクセス ポイントの FlexConnect モードを設定する

この設定は、FlexConnect 中央スイッチおよびローカル スイッチ モードに適用されます。アクセスポイントに FlexConnect 中央スイッチ モードを設定するには、次の手順を実行します。

ステップ 1　WLC のメイン ウィンドウで、[WIRELESS]タブをクリックします。

すべてのアクセス ポイントが一覧表示されます。

注　アクセス ポイントの詳細については、ワイヤレス LAN コントローラのユーザ ガイドを参照してください。

ステップ 2　モードを FlexConnect に設定するアクセス ポイントをクリックします。

ステップ 3　[General]タブをクリックします。

ステップ 4　[AP Mode] ドロップダウン リストから [FlexConnect]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します。

FlexConnect 中央スイッチ モードのアクセス コントロール リストの作成

ローカル モードの場合と同じ手順を使用して、アクセス コントロール リストを作成します。詳細については、「アクセス コントロール リストの作成」セクション（4-11 ページ）を参照してください。

FlexConnect 中央スイッチ モードの CUWN での SSID の作成

ローカル モードの場合と同じ手順で SSID を作成します。詳細については、「CUWN で SSID を作成する」セクション（4-12 ページ）を参照してください。

FlexConnect のローカル スイッチ モードでのアクセス コントロール リストの作成

FlexConnect のローカル スイッチ モードでのアクセス コントロール リストを作成するには、次の手順を実行します。

ステップ 1　WLC のクレデンシャルで WLC にログインします。

ステップ 2　[Security] > [Access Control Lists] > [FlexConnect ACLs]の順に選択します。

ステップ 3　ACL を追加するには、[New]をクリックします。

ステップ 4　表示される [New] ページに次の情報を入力します。

a.　[Access Control List Name] テキスト フィールドに新しい ACL の名前を入力します。

注　最大 32 文字の英数字を入力できます。

b.　[Apply]をクリックします。

ステップ 5　[Access Control Lists] ページが再度表示されたら、新しい ACL の名前をクリックします。

ステップ 6　表示される [Edit] ページで、[Add New Rule]をクリックします。

[Rules > New] ページが表示されます。

ステップ 7　必要なウォールガーデンの範囲にこの ACL のルールを設定します。

ウォールガーデンの範囲を表示するには、WiFi Engage で [SSIDs] ウィンドウの [Configuration Instructions] リンクをクリックします。

ACL ルールを定義するときには、次のように値を設定します。

- **Direction**：Any
- **Protocol**：Any
- **Source Port Range**：0-65535
- **Destination Port Range**：0-65535
- **DSCP**：Any
- **Action**：Permit

FlexConnect のローカル スイッチ モードの CUWN での SSID の作成

（注）　SSID は MSE/CMX ではなく WLC で作成されます。

FlexConnect のローカル スイッチ モードの CUWN で SSID を作成するには、次の手順を実行します。

ステップ 1　WLC のメイン ウィンドウで、[WLANs]タブをクリックします。

ステップ 2　WLAN を作成するには、ページの右端にあるドロップダウン リストで [Create New]を選択し、[Go] をクリックします。

ステップ 3　表示される [New] ページで、[Type]、[Profile Name]、[SSID] などの WLAN の詳細を入力します。

ステップ 4　[Apply]をクリックします。

[SSID Name] ページが表示されます。

ステップ 5　[General] タブでは、[Broadcast SSID] チェックボックスをオフにします。

ステップ 6　[Security] > [Layer 2]を選択し、[Layer 2 Security] を [None] に設定します。

ステップ 7　[Layer 3]タブで、次を設定します。

a. [Layer 3 security] ドロップダウン リストから、[Web Policy]を選択します。

b. [On Mac Filter Failure]ラジオ ボタンを選択します。

c. [Preauthentication ACL] 領域で、[WebAuth FlexACL] ドロップダウン リストから、事前に定義されている ACL を選択します。

d. [Sleeping Client] の [Enable] チェックボックスをオンにします。

注　Web 認証に成功したゲスト アクセスを持つクライアントは、ログイン ページから別の認証プロセスを実行せずにスリープおよび復帰することを許可されています。再認証が必要になるまでスリープ状態にあるクライアントが記録される期間を設定できます。有効な範囲は 1 時間から 720 時間（30 日）で、デフォルトは 12 時間です。これがセッション タイムアウトと同じになるのが理想的です。

e. [Override Global Config] の [Enable] チェックボックスをオンにします。

f. [Web Auth Type] ドロップダウン リストから、[External]を選択します。

g. 表示される [URL] フィールドに、WiFi Engage のスプラッシュ URL を入力します。

CUWN アカウントのスプラッシュ URL を表示するには、WiFi Engage で、[SSIDs] ウィンドウの [Configuration Instructions] リンクをクリックします。

注　また、スプラッシュ URL として スタジオ URL を設定できます。キャプティブ ポータル URL としてのスタジオ URL の設定の詳細については、「Enterprise Mobility Services Platform Studio URL のキャプティブ ポータル URL としての設定」セクション（7-26 ページ）を参照してください。

h. [Apply]をクリックします。

ステップ 8　[Advanced]タブをクリックします。

ステップ 9　[Enable Session Timeout] フィールドに「**1800**」と入力します。

ステップ 10　[FlexConnect] 領域で、FlexConnect のローカル スイッチに [Enabled]チェックボックスをオンにし、[Apply] をクリックします。

ステップ 11　[General] タブで、[Status] および [Broadcast SSID] オプションの [Enabled] チェックボックスをオンにし、SSID を有効にします。

ステップ 12　コマンド プロンプトで次のコマンドを実行して、キャプティブ バイパスを無効にします。その後、WLC を再起動します。

config network web-auth captive-bypass disable

ステップ 13　[Management] > [HTTP-HTTPS]を選択します。

ステップ 14　表示される [HTTP-HTTPS configuration] ページで、次を実行します。

a. [HTTP Access] ドロップダウン リストから、[Disabled]を選択します。

b. [HTTPS Access] ドロップダウン リストから、[Enabled]を選択します。

c. [WebAuth SecureWeb] ドロップダウン リストから、[Disabled]を選択します。

d. [Apply]をクリックします。

ステップ 15　[Security]>[Web Auth] > [Web Login Page] の順に選択し、[Redirect URL after login] フィールドが空白であることを確認します。