Connect and Engage サービス

Connect and Engage サービスの概要

CONNECT&ENGAGE は、カスタマイズ可能なロケーション認識型ゲスト キャプティブ サービスです。これにより、ビジターを対象とした直観的なカスタム オンボーディング エクスペリエンスを作成できます。 このサービスを利用して、ビジターに 2 種類のオンボーディング エクスペリエンスを提供できます。

- Facebook Wi-Fi：
  - 施設の管理者が施設の Facebook ページを、ビジターを対象とした無料 Wi-Fi ホットスポットとして利用できます。
  - ビジターは、施設の Facebook ページにアクセスした後で、無料 Wi-Fi にアクセスできます。
  - デモグラフィック レポートから施設のカスタマー ベースを把握できます。
- カスタム ポータル：
  - 施設の管理者が、カスタマイズしたブランディングおよび広告を使用してゲスト スプラッシュ ページを作成、ホストできます。

- OAuth 2.0 を使用した Facebook、Instagram、Foursquare とのソーシャル ネットワーク認証を提供します。
- OAuth 2.0 ユーザ ソーシャル情報を収集します。

Cisco CMX Connect サービスの新機能の完全なリストについては、次の URL にある『*Release Notes for Cisco CMX 10.2*』の「What's New in This Release」の項を参照してください。

http://www-author.cisco.com/c/en/us/td/docs/wireless/mse/release/notes/cmx_10_2_rn.html

（注） このリリースでは、Location サービスと Presence Analytics サービスを同一の Cisco CMX インスタンスにインストールすることはできません。 したがって、次のいずれかの組み合わせでインストールできます。

- Connect and Engage と Location
- Connect and Engage と Presence Analytics

[Restrictions]

- Cisco CMX Connect の Facebook Wi-Fi 認証機能は、Cisco 5760 ワイヤレス LAN コントローラと Cisco Catalyst 3850 シリーズ スイッチの Cisco IOS XE 3.3.x SE、Cisco IOS XE 3.6.x E、Cisco IOS XE 3.7.x E ではサポートされていません。
- Cisco CMX 10.1 から 10.2 にアップグレードした後で、ブラウザのキャッシュをクリアしてから Cisco CMX Connect UI を起動する必要があります。 この作業を行わないと、ポータルがアップグレードされず、CMX Connect のすべての機能が正しく機能しません。

Facebook Wi-Fi とカスタム ポータルの比較

表 *1*：*Facebook Wi-Fi* とカスタム ポータルの比較

	Facebook Wi-Fi	**カスタム ポータル**
ランディング ページ	Facebook でホスト（Facebook ページ）	Cisco Connected Mobile Experiences（Cisco CMX）
ソーシャル認証	Facebook のみ	Facebook、Instagram、Foursquare（OAuth 2.0 を使用）
Facebook アプリの権限を求めるポップアップ	No	Yes

	Facebook Wi-Fi	カスタム ポータル
タイムラインへの投稿	ユーザのタイムラインにチェックインが表示される（プライバシー設定によって異なります）	チェックインは使用できない
デモグラフィック データ	Facebook に集約レベルで保存される（有効にするには 30 を超える数のチェックインが必要）	Cisco CMX に保存される（個々のレベル）
デモグラフィック データのエクスポート	No	Yes
顧客プロファイル	• Facebook 広告予算が配賦されているマーケティング チーム、ソーシャル メディア チーム、あるいはこの両方 • 複数の小規模なストアを管理するサービス プロバイダー	データを社内で保持することを希望する IT チームおよびマーケティング チーム
Post Auth URL のサポート	No	Yes

準備作業

ビジネス ページ用の Facebook アカウントを取得している必要があります。 詳細については、組織の Facebook ページの作成, （9 ページ）を参照してください。

Connect ユーザまたは ConnectExperience ユーザの追加

手順

ステップ 1 Cisco Connected Mobile Experiences（Cisco CMX）にログインします。

ステップ 2 [MANAGE] > [Users] を選択します。

ステップ 3 [New User] をクリックします。

ステップ 4 [Add New User] ダイアログボックスに、ユーザの名、姓、ユーザ名、パスワードを入力します。

ステップ 5 [Roles] ドロップダウンリストから、[Connect] または [ConnectExperience] を選択します。

（注） Connect および ConnectExperience ユーザ ロールに対して使用可能な Cisco CMX サービスのアクセス権限については、ユーザ ロールの概要, （4 ページ）を参照してください。

ステップ 6 [Submit] をクリックします。

ユーザ ロールの概要

次の表に、Connect & Engage サービスにアクセスできるユーザ ロールを示します。

表 *2*：ユーザ ロールの概要

ロール	Connect and Engage サービス			Other Services
	ダッシュボード	エクスペリエンス	Settings	
Admin	Read	読み取り/書き込み	読み取り/書き込み	読み取り/書き込み
Connect	Read	読み取り/書き込み	読み取り/書き込み	No
Connect Experience	No	読み取り/書き込み	読み取り*	No

* [SMS]、[Number of Devices]、および [Time to Expire] の場合は書き込み権限。

Connect and Engage の設定

[Connect Settings] ウィンドウを表示するには、Cisco CMX に管理ユーザとしてログインし、[CONNECT & ENGAGE] > [Settings] を選択します。

Connect の設定

次のデータ保持設定を使用できます。

- [User Retention Period]：この値は、ユーザが再接続しない場合にユーザ エントリをデータ ストアで保持する期間を示します。 デフォルトのユーザ保持期間の値は 180 日間です。 システム容量に達した場合、[User Retention Period] に指定した値に達していなくても、最も古いエントリが削除されます。 これにより、システムが引き続き新しいユーザに対応できるようになります。
- [Statistics Retention Period]：統計情報は、各ロケーションで毎日 1 回計算されます。 このテキスト ボックスに指定した値よりも前に計算された統計情報エントリは消去されます。 範囲は 7 ～ 1000 日です。 デフォルトの保持期間の値は 365 日です。

- [SMS: Number of Devices]：1 つの SMS コードを使用できるデバイスの合計です。 指定できる範囲は 1 ～ 10 ユーザです。 デフォルト値は 3 ユーザです。
- [SMS: Time to expire]（分単位）：この値は、SMS コードをアクティブに維持する期間を示します。 指定できる範囲は 3 ～ 1440 分です。 デフォルト値は 15 分です。

Connect & Engage では、ユーザ保持期間に基づいてユーザがプルーニングされます。 このタスクは、サーバ時刻で毎日午前 3 時に 1 回実行されます。 最大ユーザ数を超えた場合は、新しいユーザを追加できるようにするため、保持期間内にある古いユーザがプルーニングされます。 ユーザデータが失われないようにするために、次の作業を行うことを推奨します。

- データを Cisco CMX から定期的にエクスポートします。
- 最大容量に達するまでの推定日数に基づいて保存期間を調整します。この推定日数は、使用パターンに基づいて算出されます。使用パターンは、システムがしばらく稼働してから確立されます。

CMX Connect デバッグ ツールの使用

CMX Connect デバッグ ツールを使用すると、MAC アドレスに基づいてクライアント レコードを削除できます。

（注） デバッグ ツールはデバッグ目的でのみ使用してください。

手順

ステップ 1 Cisco Connected Mobile Experiences（Cisco CMX）にログインします。

ステップ 2 [CONNECT & ENGAGE] > [Settings] を選択します。

ステップ 3 [Debugging Tools] タブをクリックします。

ステップ 4 [Delete User Tool] エリアで、MAC アドレスに基づいてレコードを削除するユーザの MAC アドレスを入力します。

ステップ 5 [DELETE USER] をクリックします。

Connect Experiences

概要

Connect Experiences を使用して、2 種類のゲスト オンボード エクスペリエンスのいずれかを選択できます。

Facebook Wi-Fi

Facebook Wi-Fi 機能は、シンプルかつ高速なゲスト アクセス ソリューションを組織に提供します。 Cisco CMX for Facebook Wi-Fi を導入すると、組織には次のようなメリットがあります。

- ゲストを施設の Facebook ページに誘導することで、各自のキャプティブ ポータルの設計にかかる時間と労力を節約する。
- Facebook ログインを使用して Wi-Fi に接続したビジターから収集した集約ソーシャル データを確認し、ソーシャル メディア マーケティング戦略を調整する。

Facebook Wi-Fi は、Cisco ワイヤレス コントローラ（Cisco WLC）の WLAN Web パススルー認証に基づいています。 Cisco WLC は HTTP トラフィックを傍受し、クライアント ブラウザを Cisco CMX へリダイレクトします。 Cisco CMX はクライアント ロケーションを検出し、クライアント ブラウザのロケーションを、設定されたロケーション固有の Facebook ページにリダイレクトします。 Facebook のサインインとチェックインが成功すると、Cisco CMX は、クライアント ブラウザを特定の Facebook ページへリダイレクトします。

Facebook Wi-Fi の設定の詳細については、Facebook Wi-Fi ポータルの設定, （7 ページ）を参照してください。

カスタム ポータル

カスタム ポータルでは次の作業を行うことができます。

- ロケーション固有のスプラッシュ ページの作成
- スプラッシュ ページを使用したブランディングの一貫性の確立
- 顧客サインイン ページからの登録情報の所有。これにより、キャプティブ ポータルが、後で電子メール マーケティングを使用して実施するターゲット マーケティングのデータ ソースとなります。

カスタム ポータルの設定については、カスタム ポータルの設定, （10 ページ）を参照してください。

Facebook Wi-Fi ポータルの設定

Facebook Wi-Fi ポータルの設定では、次の作業を行います。

1. シスコ ワイヤレス コントローラでのアクセス コントロール リストの設定, （7 ページ）
2. Web パススルー認証の WLAN の設定, （8 ページ）
3. 組織の Facebook ページの作成, （9 ページ）
4. システムのデフォルト Facebook ページの割り当て, （10 ページ）
5. ロケーション固有の Facebook ページの割り当て, （10 ページ）

シスコ ワイヤレス コントローラでのアクセス コントロール リストの設定

手順

ステップ 1 Cisco CMX に関連付けらているシスコ ワイヤレス コントローラ（Cisco WLC）の Web UI 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 [Access Control Lists] ウィンドウで [New] をクリックし、アクセス コントロール リスト（ACL）を追加します。

ステップ 4 [Access Control Lists] > [Edit] ウィンドウに、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。

ステップ 5 ACL タイプとして [IPv4] または [IPv6] を選択します。

ステップ 6 [Apply] をクリックします

ステップ 7 [Access Control Lists] ウィンドウで、新しい ACL の名前をクリックします。

ステップ 8 [Access Control Lists] > [Edit] ウィンドウで、[Add New Rule] をクリックします。
[Access Control Lists] > [Rules] > [New] ウィンドウが表示されます。

ステップ 9 ACL を次の表の内容に従って設定します。

表 *3* : *Facebook Wi-Fi* ポータルの *ACL*

順序番号	Action	送信元 IP/ Mask	宛先 IP Mask	プロトコル	送信元ポート	Destination Port	DSCP	方向
1	Permit	0.0.0.0/ 0.0.0.0	0.0.0.0/ 0.0.0.0	TCP	HTTPS	いずれか（Any）	いずれか（Any）	いずれか（Any）
2	Permit	0.0.0.0/ 0.0.0.0	0.0.0.0/ 0.0.0.0	TCP	いずれか（Any）	HTTPS	いずれか（Any）	いずれか（Any）

順序番号	Action	送信元 IP/ Mask	宛先 IP Mask	プロトコル	送信元ポート	Destination Port	DSCP	方向
3	Permit	MSE_IP/ 255.255.255.255	0.0.0.0/ 0.0.0.0	TCP	HTTP	いずれか（Any）	いずれか（Any）	いずれか（Any）
4	Permit	0.0.0.0/ 0.0.0.0	MSE_IP/ 255.255.255.255	TCP	いずれか（Any）	HTTP	いずれか（Any）	いずれか（Any）

Web パススルー認証の WLAN の設定

（注） Cisco CMX 10.2 へのアップグレード完了後、または Cisco CMX 10.2 の新規インストール完了後は、デフォルトで sslmode が有効になっています。 したがって、HTTP リダイレクトが必要な場合は sslmode を無効にする必要があります。 このようにしない場合は、WLC SSID の設定で https://<CMX>/… を設定する必要があります。

ユーザにネットワーク アクセスを付与するには、Cisco WLC でワイヤレス LAN（WLAN）を設定する必要があります。このため、Connect & Engage 向けに WLAN のレイヤ 3 セキュリティで Web パススルーを設定する必要があります。

手順

ステップ 1 Cisco WLC の Web UI で [WLANs] をクリックします。

ステップ 2 [WLANs] ウィンドウで、対応する WLAN ID をクリックします。

ステップ 3 [WLANs] > [Edit] ウィンドウで [SECURITY] > [Layer 2] を選択します。

ステップ 4 [Layer 2 Security] ドロップダウン リストから、[None] を選択します。

ステップ 5 [Apply] をクリックします

ステップ 6 [Layer 3] タブで [Layer 3 Security] ドロップダウン リストから [Web Policy] を選択します。

ステップ 7 Web パススルーについて、[Passthrough] を選択します。

ステップ 8 シスコ ワイヤレス コントローラでのアクセス コントロール リストの設定, （7 ページ）で説明する手順に従って定義した**事前認証 ACL** を選択します。

ステップ 9 グローバル認証および Web 認証ページを上書きするために、[Over-ride Global Config] チェックボックスをオンにします。

ステップ 10 ワイヤレス ゲスト ユーザ用の Web 認証ページを定義するために、[Web Auth Type] ドロップダウン リストから [External (Re-direct to external server)] を選択します。
これは、認証のためにクライアントを外部サーバにリダイレクトします。

ステップ 11 [URL] フィールドに、Facebook Wi-Fi ページの URL を入力します。 外部リダイレクション URL は、Facebook Wi-Fi 用の Cisco CMX 上のポータルを指している必要があります。次に例を示します。

例：

```
http://<CMX>/fbwifi/forward
```

ステップ 12 このサービス セット識別子（SSID）を有効にします。

ステップ 13 [Apply] をクリックします

ステップ 14 [Save Configuration] をクリックします。

（注） Connect & Engage のリダイレクションでは、Apple iOS デバイス向けに Cisco WLC 上で特殊な設定が必要です。 Cisco WLC CLI を使用して **configgetworkweb-authcaptive-bypassenable** コマンドを入力します。詳細については、http://www.cisco.com/c/en/us/td/docs/wireless/controller/8-0/command-reference/b_cr80/b_cr80_chapter_010.html#wp2423541535. を参照してください。

組織の Facebook ページの作成

組織の Facebook ページを作成するには、Facebook で提示される手順に従います。 Facebook ページを作成するには、https://www.facebook.com/pages/create.phpを参照してください。

システムのデフォルト Facebook ページの割り当て

手順

ステップ 1 Cisco Connected Mobile Experiences（Cisco CMX）にログインします。

ステップ 2 [CONNECT & ENGAGE] > [Connect Experiences] を選択します。

ステップ 3 [Facebook Wi-Fi] カラムで [Assign Default] をクリックします。
[Facebook Wi-Fi Configuration] オプションが新しいブラウザ タブに表示されます。

ステップ 4 次の作業を行います。

a) ページを選択します。
b) [Bypass Mode] を選択します。
c) [Session Length] を選択します。
d) 追加の利用規約が必要な場合は、オプションの [Terms of Service] をクリックします。
e) [Save Settings] をクリックします。

ロケーション固有の Facebook ページの割り当て

システムのデフォルト ページを設定したら、ロケーション固有の Facebook ページを割り当てることができます。

手順

ステップ 1 特定のキャンパス、ビル、フロア、またはゾーンを選択してクリックするか、または [Gear]  アイコンにカーソルを合わせます。

ステップ 2 [Assign New] をクリックします。

カスタム ポータルの設定

カスタム ポータル ページを作成するときには、次の 4 種類のテンプレートを使用できます。

- [Registration Form]：このテンプレートには次の要素が含まれています。
  - ロゴまたは画像
  - ビジターの名前、電子メール アドレス、および電話番号を指定する登録フォーム
  - 利用規約

- [Submit] ボタン
  電話番号を指定するときに、SMS 経由で通知を受け取るため [SMS Auth] チェックボックスをオンにします。 詳細については、 SMS 認証, （18 ページ）

- [Social Login]：このテンプレートには次の要素が含まれています。
  - ロゴまたは画像
  - ソーシャル ログイン要素。Facebook、Instagram、および Foursquare の 3 つのオプションがあります。
    ソーシャル ログイン要素により、ソーシャル OAuth 2.0 を使用したビジターのオンボーディングが可能になります。

- [Social & Registration Login]：このテンプレートには、[Social Login] 要素と [Registration Form] 要素の両方が含まれています。
- [SMS Form]：このテンプレートでは、SMS 認証用ポータルを作成できます。 ポータルに [Registration Form] 要素があることを確認するか、必要に応じてこの要素を追加します。 この要素で必要となるのは電話番号フィールドだけですが、必要に応じて他のフィールドを追加できます。 登録フォームでは、SMS 対応デバイスで認証コードを受信し、SMS 非対応デバイスで認証コードを入力することができます。
- [Custom]：このテンプレートは空白であり、独自のテンプレートを新規に作成できます。

選択したテンプレートによって、追加できる要素のタイプが限定されることはありません。たとえば、[Social Login] テンプレートが選択されている場合、いつでもこのテンプレートを変更して、代わりに [Registration Form] の要素を使用することができます。

カスタム ポータルの設計時に使用できるオプションを次に示します。

- ウィンドウの左側にカスタム ポータルのプレビューが表示され、ウィンドウの右側にポータルとその要素を編集するためのオプションが表示されます。

（注） モバイル、PC、およびタブレットのカスタム ポータルのプレビューを確認できます。

- [CONTENT] タブでは、ポータル要素を追加、編集できます。 要素をクリックしてポータルの領域をプレビューし、要素の設定を編集します。
- [BACKGROUND] タブでは次の操作を行うことができます。
  - 画像ライブラリから画像をアップロードする。
  - ポータルの背景色と不透明度を指定する。
- [THEMES] タブでは、ポータルのテーマを指定できます。

- [Languages] タブでは、必要な言語を選択できます。 言語を追加するには、[Select language] ドロップダウン リストから必要な言語を選択し、[Add to list] をクリックします。 詳細については、 カスタム ポータルでの多言語サポートの有効化

シスコ ワイヤレス コントローラでのアクセス コントロール リストの設定

手順

ステップ 1 Cisco CMX に関連付けらているシスコ ワイヤレス コントローラ（Cisco WLC）の Web UI 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 [Access Control Lists] ウィンドウで [New] をクリックし、アクセス コントロール リスト（ACL）を追加します。
[Access Control Lists] > [New] ウィンドウが表示されます。

ステップ 4 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。

ステップ 5 ACL タイプとして [IPv4] または [IPv6] を選択します。

ステップ 6 [Apply] をクリックします
[Access Control Lists] ページが表示されます。

ステップ 7 新しい ACL の名前をクリックします。

ステップ 8 [Add New Rule] をクリックします。
[Access Control Lists] > [Rules] > [New] ウィンドウが表示されます。

ステップ 9 ACL を次のいずれかの表の内容に従って設定します。

表 *4*：登録フィールドだけを使用した *ACL* の設定（ソーシャル ネットワーク ログインなし）

順序番号	Action	送信元 IP/ Mask	宛先 IP Mask	プロトコル	送信元ポート	Destination Port	DSCP	方向
1	Permit	MSE_IP/ 255.255.255.255	0.0.0.0/ 0.0.0.0	TCP	HTTP	いずれか（Any）	いずれか（Any）	いずれか（Any）
2	Permit	0.0.0.0/ 0.0.0.0	MSE_IP/ 255.255.255.255	TCP	いずれか（Any）	HTTP	いずれか（Any）	いずれか（Any）

または

表 *5*：ソーシャル ネットワーク ログインを使用した *ACL* の設定

順序番号	Action	送信元 IP/ Mask	宛先 IP Mask	プロトコル	送信元ポート	Destination Port	DSCP	方向
1	Permit	0.0.0.0/ 0.0.0.0	0.0.0.0/ 0.0.0.0	TCP	HTTPS	いずれか（Any）	いずれか（Any）	いずれか（Any）
2	Permit	0.0.0.0/ 0.0.0.0	0.0.0.0/ 0.0.0.0	TCP	いずれか（Any）	HTTPS	いずれか（Any）	いずれか（Any）
3	Permit	MSE_IP/ 255.255.255.255	0.0.0.0/ 0.0.0.0	TCP	HTTP	いずれか（Any）	いずれか（Any）	いずれか（Any）
4	Permit	0.0.0.0/ 0.0.0.0	MSE_IP/ 255255255255	TCP	いずれか（Any）	HTTP	いずれか（Any）	いずれか（Any）

Web パススルー認証の WLAN の設定

（注） Cisco CMX 10.2 へのアップグレード完了後、または Cisco CMX 10.2 の新規インストール完了後は、デフォルトで sslmode が有効になっています。 したがって、HTTP リダイレクトが必要な場合は sslmodeを無効にする必要があります。 このようにしない場合は、WLC SSID の設定で https://<CMX>/… を設定する必要があります。

ユーザにネットワーク アクセスを付与するには、Cisco WLC でワイヤレス LAN（WLAN）を設定する必要があります。このため、Connect & Engage サービス向けに WLAN のレイヤ 3 セキュリティで Web パススルーを設定する必要があります。

手順

ステップ 1 Cisco WLC の Web UI で [WLANs] を選択します。

ステップ 2 [WLANs] ウィンドウで、対応する WLAN ID をクリックします。

ステップ 3 [WLANs] > [Edit] ウィンドウで [SECURITY] > [Layer 2] を選択します。

ステップ 4 [Layer 2 Security] ドロップダウン リストから、[None] を選択します。

ステップ 5 [Apply] をクリックします

ステップ 6 [Layer 3] タブで [Layer 3 Security] ドロップダウン リストから [Web Policy] を選択します。

ステップ 7 Web パススルーについて、[Passthrough] ラジオボタンを選択します。

ステップ 8 シスコ ワイヤレス コントローラでのアクセス コントロール リストの設定, （7 ページ）で説明する手順に従って定義した**事前認証 ACL** を選択します。

ステップ 9 グローバル認証設定 Web 認証ページを上書きするには、[Over-ride Global Config] チェックボックスをオンにします。

ステップ 10 ワイヤレス ゲスト ユーザ用の Web 認証ページを定義するために、[Web Auth Type] ドロップダウン リストから [External (Re-direct to external server)] を選択します。
これは、認証のためにクライアントを外部サーバにリダイレクトします。

ステップ 11 [URL] フィールドに、カスタム ポータルの URL を入力します。 外部リダイレクション URL は、カスタム ポータル用の Cisco CMX 上のポータルを指している必要があります。次に例を示します。

例：

```
http://<CMX>/visitor/login
```

ステップ 12 このサービス セット識別子（SSID）を有効にします。

ステップ 13 [Apply] をクリックします

ステップ 14 [Save Configuration] をクリックします。

（注） Connect & Engage のリダイレクションでは、Apple iOS デバイス向けに Cisco WLC 上で特殊な設定が必要です。 これを実行するには、Cisco WLC CLI を使用して **configgetworkweb-authcaptive-bypassenable** コマンドを入力します。詳細については、http://www.cisco.com/c/en/us/td/docs/wireless/controller/8-0/command-reference/b_cr80/b_cr80_chapter_010.html#wp2423541535. を参照してください。

デフォルトのカスタム ポータル ページの作成

手順

ステップ 1 管理ユーザとして Cisco CMX にログインします。
ステップ 2 [CONNECT & ENGAGE] > [Connect Experiences] を選択します。
ステップ 3 [Custom Cisco CMXs] で [Create Default] をクリックします。
ステップ 4 [Portal Title] フィールドに、カスタム ポータルの名前を入力します。
ステップ 5 使用するテンプレートをクリックし、[Next] をクリックします。
ステップ 6 要件に基づいてテンプレートを設計します。
ステップ 7 [Save] をクリックします。

ロケーション固有のカスタム ポータル ページの割り当て

システムのデフォルト ポータルを設定した後、ロケーション固有のカスタム ポータル ページを割り当てることができます。

手順

ステップ 1 対応するカスタムポータルドロップダウンリストから、特定のキャンパス、ビル、フロア、またはゾーンを選択します。
ステップ 2 [Create New] をクリックし、新規ポータルを作成してそのロケーションに割り当てます。 あるいは、そのロケーションに既存のポータルを割り当てます。

カスタム ポータルの多言語サポートの有効化

Cisco CMX には言語翻訳エンジンは含まれていません。 管理者は各言語ページを個別に編集し、すべてのテキスト エントリを手動で翻訳する必要があります。

（注） ポータル ページ翻訳は、右から左へ記述する言語（ヘブライ語やアラビア語）ではサポートされていません。

1 つのポータル ページで複数のページをサポートするには、各ページを有効にする前に、必要な言語をページに追加する必要があります。 多言語サポートは、ポータルの作成時に追加できます。 英語以外の言語を無効にできます。あるいは、英語以外の言語の翻訳が完了した時点で言語を 1 つずつ再度有効にできます。

多言語サポートを有効にするには、管理ユーザが次の作業を行う必要があります。

- ポータルを作成します。
- サポートする必要がある言語を追加します。
  - 言語を追加するには、ポータル エディタ内にある [Languages] タブをクリックします。ドロップダウンから言語を選択し、[Add Language] をクリックします。 有効になっている言語（選択されている言語）だけが使用されます。
- 有効な各言語の翻訳を提供します。
  - 現在表示されているポータルの翻訳を変更するには、ポータル エディタのプレビュー エリアの上にあるドロップダウン リストから、別の言語を選択します。
  - ほとんどの要素の翻訳はポータルに固有です。つまり、あるポータルでテキスト要素を翻訳しても、別のポータルのテキスト要素には影響しません。
  - ただし、登録フィールドの翻訳はすべてのポータルで共有されます。 あるポータルで特定のフィールドを変更すると、他のすべてのポータルでもそのフィールドが変更されます。
- ライブ ビューを使用して翻訳が正しいことを確認し、各言語を切り替えて翻訳を検証し、ポータルを保存します。

エンド ユーザに対してスプラッシュ ページを表示するときに、Cisco CMX はブラウザの設定から、エンドユーザの最優先言語を判別します。 次に、表示可能な優先言語が選択され、その言語でのポータルが表示されます。 エンド ユーザはスプラッシュ ページの右上隅にあるドロップダウン リストを使用して、別の言語を手動で選択できます。

エンド ユーザ デバイスには事前に定義されている言語があります。 優先言語のリストが HTTP ヘッダーの一部として渡されます。 Cisco CMX は HTTP ヘッダーを分析し、表示可能な翻訳の中で最も近い翻訳でポータルを表示します。

たとえば、ユーザが英語、スペイン語、フランス語をこの順序で優先言語として設定しており、ポータルで表示可能な翻訳がロシア語、スペイン語、イタリア語、ドイツ語だけである場合、スペイン語が表示されます。これは、表示可能な言語の中ではスペイン語が最優先言語であるためです。

別の言語でポータルを表示するには、ポータルのユーザは [Language] ドロップダウン リストを使用して、表示可能な翻訳のリストから選択できます。

サイトの Connect ポータル ページの設定

ポータルを作成したら、次の手順でそのポータルをサイトに割り当てることができます。

手順

ステップ 1 [Connect & Engage] > [Connect Experiences] を選択します。
ステップ 2 [Post Auth URL] カラムで、ポータルに割り当てるサイトの [Assign Default] をクリックします。
ステップ 3 [Post Auth URL for <site name>] ダイアログボックスに、post Auth URL を入力します。

サイトの Connect クライアントの表示

サイトの Connect クライアントを表示するには、次の手順を実行します。

手順

ステップ 1 [Connect & Engage] > [Dashboard] を選択します。
ステップ 2 [Location] ドロップダウン リストから、[Sites] を選択します。
ステップ 3 [Select a Location] ドロップダウン リストから、サイトを選択します。
ステップ 4 [Interval] ドロップダウン リストから、間隔を選択します。

Cisco CMX Connect からの HTTPS でのポータル ページの提供

Cisco CMX Connect から HTTPS でポータル ページを提供するには、次の手順を実行します。

手順

ステップ 1 Cisco MSE CLI で次のコマンドを入力して、SSL モードを有効にします。
cmxctl node sslmode enable

ステップ 2 SSL モードを有効にしたら、次の手順に従って SSL 証明書をインストール:
a) 必要なパスに .pem ファイルをダウンロードします。
b) 次のコマンドを入力します。
cmxctl node sslmode enable pem <パス>
新しい pem ファイルのパスを指定できます。 デフォルトの場所は /opt/haproxy/ssl/host.pem です。

ステップ 3 Cisco WLC（[WLANs] > [SECURITY] > [Layer 3]）で、URL に HTTP ではなく HTTPS を使用します。 たとえば http:/<IP address>/visitor/login の代わりに https://<IP address>/visitor/login を入力します。

（注） クライアントが SSID に接続している間に SSL モードを有効にするため、証明書を受け入れる必要があります。

SMS 認証

接続している個人の識別情報を提供するため、Cisco CMX 10.2 にはカスタム ポータルに SMS ベースの認証を追加する機能があります。 現在この機能は SMS 認証の目的で Twilio アカウントのみと統合します。 各自の Twilio アカウントを作成します（https://www.twilio.com/user/account/settings を参照）。 また、この機能では SMS 対応デバイスがネットワークにアクセスできるようにしておく必要があります。

適切に設定されている事前認証 ACL がない場合、ワイヤレス クライアントは SMS メッセージに含まれているリンクを使用して Cisco CMX に認証コードを戻すことができないため、WebAuth が必要な状態のままになります。

この機能を使用するには、既存のポータルを編集するか、またはテンプレートを使用して SMS 認証を使用する新しいポータルを作成します。 作成できる Twilio アカウントは 1 つだけですが、アカウントに複数の電話番号を関連付けることができるので、同じアカウントを複数のポータルで使用できます。ただし各ポータルで Twilio アカウントに関連付けることができる電話番号は 1 つだけです。 ポータルと設定されている Twilio アカウントの関連付けを解除するには、[Reset] ボタンを使用します。

[Twilio Configuration] エリアで設定する発信元番号を Twilio から購入する必要があります。 既存の番号は使用できません。

手順

ステップ 1 ポータルに [Registration Form] 要素があることを確認するか、必要に応じてこの要素を追加します。

ステップ 2 必ず電話番号フィールドを指定してください。ただし、他のフィールドを必要に応じて追加することもできます。

ステップ 3 [Registration Form] エリアで、[SMS Auth] チェックボックスをオンにします。
登録フォームでは、SMS 対応デバイスで認証コードを受信し、SMS 非対応デバイスで認証コードを入力することができます。

ステップ 4 [Edit] アイコン（[SMS Auth] チェックボックスの横）を選択し、Twilio アカウントの情報を入力します。

ステップ 5 [Twilio Configuration] エリアで、次のパラメータを入力します。
[Twilio Configuration] フィールドの横の [Edit] ボタンをクリックして、Twilio アカウント情報にアクセスできます。

a) [Twilio Account ID] に ID を入力します。 これは、Twilio アカウントを識別する 34 文字の文字列です。
b) [Twilio Auth Token] に値を入力します。

c) [From Number] を入力します。 この番号は、Twilio から購入します。 既存の電話番号は使用できません。

d) [Create] をクリックします。
設定されている Twilio アカウントとポータルの関連付けを解除する（コネクタを削除する）には、[Reset] ボタンをクリックします。

ステップ 6 [Save] をクリックします。

Connect and Engage ダッシュボード

Connect & Engage ダッシュボードを表示するには、Cisco CMX にログインし、[CONNECT & ENGAGE] >[Dashboard] を選択します。

[Connect & Engage Dashboard] ウィンドウに、サマリー レポートと 2 つの履歴レポートが表示されます。

ページ上部のナビゲーション バーを使用して、レポートのロケーションと間隔を指定します。

ロケーションは次のレベルで構成されています。

- グローバル
- キャンパス（Campuses）
- ビル（Buildings）
- フロア（Floor）
- ゾーン
- サイト

[Connect & Engage Dashboard] ウィンドウの [Interval] ドロップダウンリストから、履歴レポートの生成対象期間を選択できます。

- 過去 7 日間（Last 7 Days）（デフォルト）
- 過去 8 日（Last 28 Days）
- 過去 365 日（Last 365 Days）

概要情報

概要情報は、当日のユーザの使用状況情報を示します。 使用する時刻はサーバ時刻であり、Web ブラウザの時刻ではないことに注意してください。

履歴情報

Connect & Engage ダッシュボードには履歴情報が表示されます。

- [New and Repeat Visitors]：新規ビジターとは、初めて認識されたユーザです。 アクセスを繰り返すビジターとは、以前の訪問で認識されているユーザです。
- [Network Usage]：ネットワーク使用量とは、すべてのビジターによってアップロード/ダウンロードされたデータの合計量です。
- [Pages Served vs Submitted]：ページの表示回数とは、ポータル ページがビジターのデバイスで表示された回数です。 ページの送信回数とは、ポータル ページがビジターによって送信された回数です。
- [SMS Sent vs Authenticated]：送信 SMS とは、送信されたテキストの合計数です。 認証 SMS とは、ビジターを正しく認証するために使用されたテキストの数です。
- [Languages Used]：使用言語とは、各言語を使用して認証されたビジターの数です。

履歴レポートでは、レポートに表示するグラフのタイプを選択できます。

- Area Chart
- Line Chart
- 縦棒グラフ

ビジター検索

Connect & Engage ダッシュボードには検索オプションがあります。次の検索タイプを実行できます。

- Advanced Search
- すべてのビジターのエクスポート（Export All Visitors）

ビジターを検索するには、[Visitor Search] フィールドに検索語（名前、電子メールアドレスなど）を入力します。

その他の情報

- 検索テーブルでは、ページあたり最大 50 件のクライアントのプレビューが表示されます。
- 検索結果全体を .CSV ファイルにエクスポートできます。
- 検索時間範囲は Web ブラウザの時刻ではなく Cisco CMX のシステム時刻に基づいています。
- 部分検索がサポートされていますが、ワイルドカード（*）はサポートされていません。
- 詳細検索は、次のパラメータに基づいて実行できます。

- すべて（All）
- MAC
- Facebook での名前（Facebook Name）
- Facebook での性別（Facebook Gender）
- Facebook でのロケール（Facebook Locale）
- Facebook でのタイムゾーン（Facebook Timezone）
- Facebook での友達（Facebook Friends）
- Foursquare での名前（Foursquare Name）
- Foursquare での電子メール（Foursquare Email）
- Instagram での名前（Instagram Name）
- Instagram での電子メール（Instagram Email）
- 登録フォームの電子メール（Registration Form Email）
- 登録フォームの性別（Registration Form Gender）
- 登録フォームの名前（Registration Form Name）
- 登録フォームの電話番号（Registration Form Phone Number）

Connect and Engage ライブラリの使用

Connect & Engage ライブラリを表示するには、Cisco CMX にログインし、[CONNECT & ENGAGE] > [Library] を選択します。

- [Portal Library]：作成したポータル（ドラフトおよび完成済みポータルの両方）が示されます。 [Portal Library] では、以下の操作を実行できます。
  - 編集：作成中のポータルを編集します。
  - コピー：ポータルをコピー（複製）できます。
  - 表示：ポータルを表示できます。
  - 削除：ポータルを削除できます。
- [Templates Library]：各自のポータルを作成するときに使用できる事前定義のテンプレートが含まれています。 次のテンプレートを使用できます。
  - [Registration Form]
  - [Social Login]
  - [Social or Registration Login]
  - [SMS Form]

- Custom

- [Image Library]：画像ライブラリにより、インポートした画像を複数のポータルで使用できます。 画像はアップロード時に縮小拡大されるため、アップロードする画像のサイズ制限はありません。 アップロードが完了した画像は、組み込みの画像エディタを使用して回転、クロップ、縦横比変更を行うことができます。 [Image Library] では、以下の操作を実行できます。
  - 追加：新規画像を追加できます。 画像が縮小され、画像のサムネイル ビューが作成されます。
  - 表示：画像をプレビューできます。 画像をプレビューするときに、クロップ、サイズ変更、縦横比変更を行うことができます。 画像エディタで変更を行ったら、[Save] と [Close] をクリックして、画像を [Image Library] にコピーするか、または既存の画像を上書きします。
  - 削除：[Image Library] から画像を削除できます。

デバイスとブラウザのマトリックス

デバイスとブラウザのマトリックス：Connect and Engage

次の表に、カスタム ポータルのコンテキストでの Connect & Engage についてテストが完了しているデバイスおよびブラウザを示します。

表 *6*：デバイスとブラウザのマトリックス：カスタム ポータルの *Connect and Engage*

デバイスと名前	OS Version	デフォルト ブラウザとバージョン	Remarks
Google Nexus 7	4.3	Google Chrome 32.0.1700.99	—
Amazon Kindle	13.3.2.2	Silk 1.0.454.220	—
Apple iPad	7.0	Safari 7.0	—
Apple iPhone	6.1(3)	Safari 6.0	—
Apple Macbook Pro	10.8.4	Safari 6.0	—
Samsung（Snow OS）	33.0.1750.152	Google Chrome 33.0.1750.152	—
Apple iPad Mini	7.0	Safari 7.0	—

デバイスと名前	OS Version	デフォルトブラウザとバージョン	Remarks
Microsoft Windows タブレット	Windows RT 8.1	Internet Explorer 11	ソーシャルコネクタの問題
Samsung	4.2.2	デフォルト ブラウザ	—

デバイスとブラウザのマトリックス：Facebook WiFi

（注） Social OAuth を採用しているポータル ページは、Mozilla Firefox ブラウザでは正しく機能しません。

次の表に、Facebook Wi-Fi についてテストが完了しているデバイスおよびブラウザを示します。

表 *7*：デバイスとブラウザのマトリックス：*Facebook WiFi*

デバイスと名前	OS Version	デフォルトブラウザとバージョン	他のブラウザとバージョン
Google Nexus 7	4.3	Google Chrome 32.0.1700.99	—
Amazon Kindle	13.3.2.2	Silk 1.0.454.220	—
Apple iPad	7.0	Safari 7.0	—
Apple iPhone	6.1(3)	Safari 6.0	—
Apple Macbook Pro	10.8.4	Safari 6.0	—
Samsung（Snow OS）	33.0.1750.152	Google Chrome 33.0.1750.152	—
Apple iPad Mini	7.0	Safari 7.0	Google Chrome 34.0.1874.114
Microsoft Windows タブレット	4.2.2	Internet Explorer 11	—
Samsung	4.2.2	デフォルト ブラウザ	—
One+ 電話	5.0.1	Google Chrome	—

デバイスと名前	OS Version	デフォルトブラウザとバージョン	他のブラウザとバージョン
Amazon Reader	5.6.2.1	デフォルト ブラウザ	—