Cisco CMX ビジター接続に対する接続およびエンゲージ コンフィギュレーション ガイド

リリース 8.0
2014 年 8 月

Cisco Systems, Inc.
www.cisco.com

シスコは世界各国 200 箇所にオフィスを開設しています。
住所、電話番号、FAX 番号は
以下のシスコ Web サイトをご覧ください。
www.cisco.com/go/offices.

Text Part Number: OL-31277-01-J

【注意】シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。

本書は、米国シスコシステムズ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動 / 変更されている場合がありますことをご了承ください。
あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。

また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

Cisco CMX ビジター接続に対する接続およびエンゲージ コンフィギュレーション ガイド

目 次

はじめに

ここでは、『Cisco CMX Connect and Engage Configuration Guide for Visitor Connect, *Release 8.0*』の対象読者、目的、表記法について説明します。また、他のマニュアルの入手方法についても説明します。この章は、次の項で構成されています。

対象読者

このマニュアルは、Cisco CMX Connect and Engage アプリケーションを使用するマーケティングおよび IT スタッフを対象としています。

目的

このマニュアルには、ビジター接続のために MX Connect and Engage アプリケーションを管理するのに必要な情報が記載されています。

表記法

このマニュアルでは、次の表記法を使用しています。

表記法	説明
太字	コマンド、キーワード、およびユーザが入力するテキストは**太字**で記載されます。
イタリック体	文書のタイトル、新規用語、強調する用語、およびユーザが値を指定する引数は、*イタリック体*で示しています。
[ ]	角カッコの中の要素は、省略可能です。
{x | y | z }	必ずいずれか 1 つを選択しなければならない必須キーワードは、波カッコで囲み、縦棒で区切って示しています。

[x | y | z]	いずれか 1 つを選択できる省略可能なキーワードは、角カッコで囲み、縦棒で区切って示しています。
string	引用符を付けない一組の文字。string の前後には引用符を使用しません。引用符を使用すると、その引用符も含めて string とみなされます。
courier フォント	システムが表示する端末セッションおよび情報は、courier フォントで示しています。
< >	パスワードのように出力されない文字は、山カッコで囲んで示しています。
[ ]	システム プロンプトに対するデフォルトの応答は、角カッコで囲んで示しています。
!、#	コードの先頭に感嘆符（!）またはポンド記号（#）がある場合には、コメント行であることを示します。

（注） 「*注釈*」です。役立つ情報やこのマニュアルに記載されていない参照資料を紹介しています。

関連資料

これらのマニュアルには、シスコ ワイヤレスに関する詳細な情報が記載されています。

- Cisco Mobility Services Engine のドキュメント：
  http://www.cisco.com/c/en/us/support/wireless/mobility-services-engine/tsd-products-support-series-home.html
- Cisco Prime Infrastructure のドキュメント：
  http://www.cisco.com/en/US/products/ps12239/products_documentation_roadmaps_list.html
- Cisco ワイヤレス LAN コントローラのドキュメント：
  http://www.cisco.com/c/en/us/support/wireless/5500-series-wireless-controllers/products-installation-and-configuration-guides-list.html
- Cisco Wireless Mesh Access Points, Design, and Deployment Guide：
  http://www.cisco.com/c/en/us/support/wireless/aironet-1550-series/products-implementation-design-guides-list.html

シスコ ワイヤレス ソリューションに関するユーザ マニュアルにアクセスするには、このリンクをクリックしてください。

http://www.cisco.com/cisco/web/psa/default.html?mode=prod

マニュアルの入手方法およびテクニカル サポート

マニュアルの入手方法、テクニカル サポート、その他の有用な情報について、次の URL で、毎月更新される『*What's New in Cisco Product Documentation（Cisco 製品資料の更新情報）*』を参照してください。シスコの新規および改訂版の技術マニュアルの一覧も示されています。
http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html

『*What's New in Cisco Product Documentation（Cisco 製品資料の更新情報）*』は、シスコの新規および改訂版の技術マニュアルの一覧も示し、RSS フィードとして購読できます。また、リーダー アプリケーションを使用してコンテンツをデスクトップに配信することもできます。RSS フィードは無料のサービスです。

概要

コネクテッド モバイル エクスペリエンスの概要

Cisco コネクテッド モバイル エクスペリエンス（CMX）は、施設内のモバイル デバイスを検出、接続、およびエンゲージするためのモバイル ソフトウェア ソリューションのスイートです。CMX ソリューションは、モバイル エンド ユーザに対してパーソナライズされたモバイル エクスペリエンスを作成し、ロケーションベースのサービスで運用効率を高めるのに役立ちます。

CMX ソリューションには、以下の機能があります。

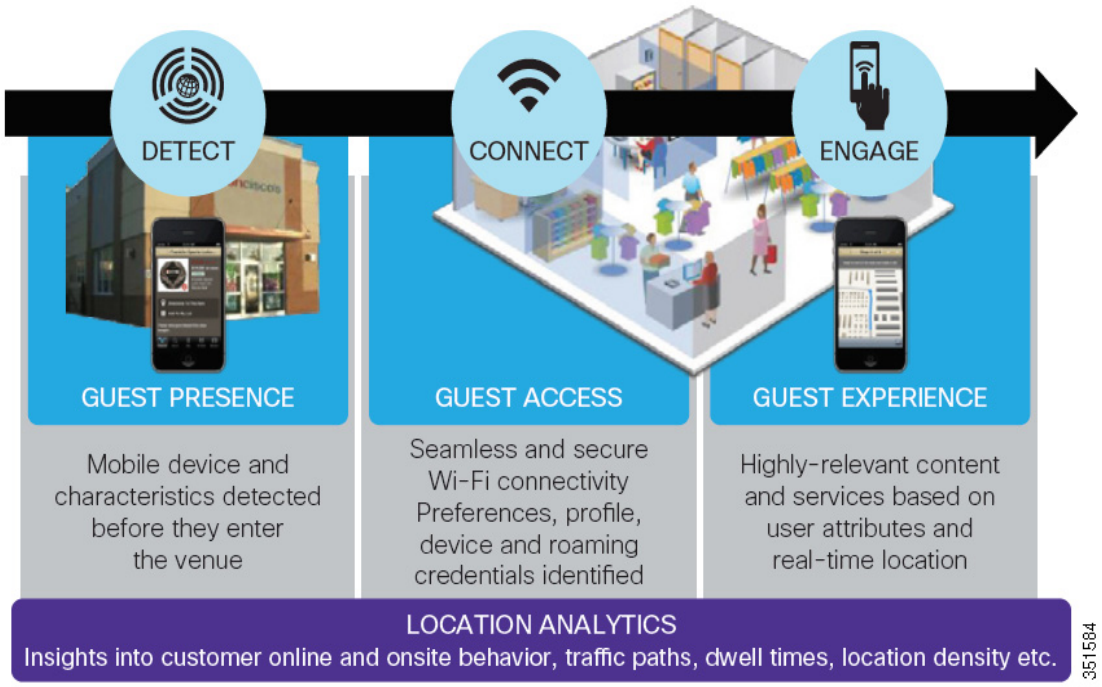
- 検出：デバイスがロケーションに近づくとすぐに、モバイル デバイスのワイヤレス信号を検出します。
- 接続：接続はゲストのポータルで、ゲスト用のスプラッシュ ページを設計することができます。
- エンゲージ：ビジターが一度 Wi-Fi にアクセスすると、そのビジターに、アドバタイズメントまたはパーソナライズされたコンテンツを提供することができます。これにより、お客様とリアルタイムで付加価値の高い関係を築くことができます。

次に、CMX ソリューションの利点を示します。

- パーソナライズされた関連性の高いコンテンツを提供することにより、お客様のエンゲージメントを向上させる。
- トラフィック フローを使用して製品やサービスをより正確に位置づけすることで、施設での効率を向上させる。

下の図は、このプロセスの概要を示しています。

図 1-1　　検出、接続、およびエンゲージ



シスコ ワイヤレス コンポーネント

シスコ ワイヤレスは、従業員の生産性の向上、コラボレーションの強化、および顧客への対応を改善するワイヤレス ソリューションとして設計されています。シスコ ワイヤレスはユニファイド ネットワークです。これは、大企業および商用ワイヤレス LAN ユーザが直面するセキュリティ、導入、管理、および制御の問題に対応します。

次にユニファイド ネットワークのコンポーネントを示します。

- Cisco Prime Infrastructure（PI）：Cisco Prime Network Control System（NCS）のワイヤレス機能と Cisco Prime LAN Management Solution（LMS）の有線機能を組み合せます。
- Cisco ワイヤレス LAN コントローラ（WLC）：ビジネス クラスの WLAN を効果的および確実に管理するために必要なものを可視化しネットワーク管理者が制御できるようにして、Mobility Services Engine を使って作業できるようにします。
- アクセス ポイント（AP）：ワイヤレス デバイスを有線ネットワークに接続し、ユビキタスなネットワーク アクセスを提供します。
- Mobility Services Engine（MSE）：ネットワーク上のさまざまな場所にあるインテリジェンスを統合して、ビジネス モビリティ アプリケーションの提供を可能にして最適化する、一連の付加価値ネットワーク サービス。

ビジター接続に対する CMX 接続およびエンゲージの概要

Cisco CMX ビジター接続は Mobility Services Engine（MSE）、Cisco ワイヤレス LAN コントローラ（WLC）、および Lightweight アクセス ポイント（AP）に基づくゲスト アクセス ソリューションです。ビジター接続は、直観的でシンプルなロケーションを認識するゲスト キャプティブ ポータルで、ビジターに対してカスタム オンボーディングのエクスペリエンスを作成することができます。これはモバイルおよびラップトップの両方のユーザに最適なエクスペリエンスを提供するように設計されています。

CMX ビジター接続が機能するためには、施設のオーナーは、Prime Infrastructure の CMX 接続およびエンゲージ サービスを有効にする必要があります。

施設のオーナーは、ビジターのエクスペリエンスを向上させるために、複数のスプラッシュ テンプレートを作成し、それをさまざまなロケーションに割り当てることによって、ロケーションに特有のスプラッシュ ページとアドバタイズメントをカスタマイズします。

スプラッシュ ページでは、ビジター接続は以下のカスタマイズをサポートしています。

- ページの背景
- HTML テキストを使用したページのヘッダーとフッター
- ダイナミック入力フィールド
- ご利用条件
- アドバタイズメント プラグイン
- スプラッシュ ページ間の移動後の URL のリダイレクト
- Facebook、Linkedin および Google+ などのソーシャル認証プラグイン

施設のビジターは、次の手順を実行して、施設の Wi-Fi にアクセスできます。

- 名前、電話番号、電子メールなどの必要な情報を提供することにより、施設のオーナーの Wi-Fi に登録する。これは 1 回の登録になります。

（注） ビジター接続は、新しいユーザを繰り返しアクセスするユーザと区別し、繰り返しアクセスするユーザに対する登録ページをスキップします。

- 利用条件を受け入れる。
- （任意）施設のオーナーによって事前に定義されているアドバタイズメントまたはアナウンスを参照する。

（任意）ソーシャル認証ページにログインする。

第 2 章

使用する前に

ビジター接続の接続およびエンゲージを設定するための手順

表 2-1　ビジター接続の接続およびエンゲージを設定するための手順

プロセス	説明
1. Prime Infrastructure をセットアップおよび開始する	次の URL を参照してください。 http://www.cisco.com/c/en/us/td/docs/net_mgmt/prime/infrastructure/2-0/quickstart/guide/cpi_qsg.html
2. Prime Infrastructure ユーザ インターフェイスへログインする	次の URL を参照してください。 http://www.cisco.com/c/en/us/td/docs/net_mgmt/prime/infrastructure/2-0/quickstart/guide/cpi_qsg.html#pgfId-42039
3. ライセンスを追加する	次の URL を参照してください。 http://www.cisco.com/c/en/us/td/docs/net_mgmt/prime/infrastructure/2-0/administrator/guide/PIAdminBook/licensing.html
4. Prime Infrastructure でマップを作成する	次の URL を参照してください。 http://www.cisco.com/c/en/us/td/docs/wireless/prime_infrastructure/2-0/configuration/guide/pi_20_cg/maps.html#wp1670968
5. Mobility Services Engine を Prime Infrastructure へ追加する	次の URL を参照してください。 http://www.cisco.com/c/en/us/td/docs/wireless/mse/7-6/MSE_CAS/7_6_MSE_CAS/7_4_MSE_CAS_chapter_010.html#ID136
6. ネットワーク設計と Mobility Services Engine を同期する	次の URL を参照してください。 http://www.cisco.com/c/en/us/td/docs/wireless/mse/7-6/MSE_CAS/7_6_MSE_CAS/7_4_MSE_CAS_chapter_011.html#ID20

表 2-1　ビジター接続の接続およびエンゲージを設定するための手順

プロセス	説明
7. Wireless LAN Controllers（WLC）と Mobility Services Engine を同期する	次の URL を参照してください。 http://www.cisco.com/c/en/us/td/docs/wireless/mse/7-6/MSE_CAS/7_6_MSE_CAS/7_4_MSE_CAS_chapter_011.html#ID64
8. MSE 追跡パラメータと履歴パラメータを設定する	次の URL を参照してください。 http://www.cisco.com/c/en/us/td/docs/wireless/mse/7-6/MSE_CAS/7_6_MSE_CAS/7_4_MSE_CAS_chapter_010.html#ID136
9. Prime Infrastructure で MSE サービスを有効化する	次の URL を参照してください。MSE サービスを有効にする
10. ロケーションまたは Context Aware Service MSE を MSE の接続およびエンゲージに関連付ける	次の URL を参照してください。ロケーションまたは CAS MSE を MSE の接続およびエンゲージと関連付ける
11. CMX Connect and Engage ユーザ インターフェイスにログインする	次の URL を参照してください。CMX Connect and Engage ユーザ インターフェイスにログインする

MSE サービスを有効にする

MSE サービスを有効にするには、次の手順を実行します。

ステップ 1　MSE の admin ユーザ インターフェイスを起動します。

MSE の admin ユーザ インターフェイスを起動するには、Web ブラウザに `https://mseip/mseui` と入力するか、または **[Services > Mobility Services Engines]** ページで [MSE name] リンクをクリックして、Cisco Prime Infrastructure（PI）から起動することができます。MSE の admin UI は、**[Administration > User Preference]** ページで [MSE Admin View] チェックボックスをオンにしたときのみ表示されます。

ステップ 2　ユーザ名とパスワードを入力して **[Sign In]** をクリックします。

MSE Admin UI のホーム ページが表示されます。使用できる MSE サービスはすべて、ホーム ページの [Services] グループ ボックスの下に一覧で表示されます。

ステップ 3　**[CMX Connect & Engage Service]** を有効にします。

ステップ 4　**[Save]** をクリックします。

ロケーションまたは CAS MSE を MSE の接続およびエンゲージと関連付ける

ロケーションまたは Context Aware Service（CAS）MSE を MSE の接続およびエンゲージと関連付けるには、次の手順を実行します。

ステップ 1　MSE の admin UI にログインします。

ステップ 2　**[CONFIGURATION]** をクリックします。

ステップ 3　左側のサイドバー メニューから **[CONNECT AND ENGAGE] > [Setup]** を選択します。

（注）　[Connect and Engage] メニューは、CMX の接続とエンゲージ サービスを有効にしている場合のみ表示されます。

ステップ 4　接続およびエンゲージと使用するロケーション MSE を追加するには、**[Add CAS MSE]** をクリックして、次のように設定します。

- [MSE Name] テキストボックスに、ロケーション MSE の名前を入力します。
- [MSE IP address] テキストボックスに、MSE の IP アドレスを入力します。
- [Username] テキストボックスにユーザ名を入力します。
- [Password] テキスト ボックスにパスワードを入力します。
- **[Save]** をクリックします。

CMX 接続およびエンゲージ システムは、選択したロケーション MSE からマップとロケーションのデータを取得します。

CMX Connect and Engage ユーザ インターフェイスにログインする

CMX Connect & Engage ユーザ インターフェイスにログインするには、次の手順を実行します。

ステップ 1　ユーザ名とパスワードを使用して、MSE の admin UI にログインします。

ステップ 2　[Apps] グループ ボックスで、**[CMX Connect & Engage]** をクリックします。

CMX Connect & Engage ユーザ インターフェイスのログイン ページが表示されます。

ステップ 3　ユーザ名とパスワードを入力します。デフォルトのユーザ名とパスワードは *admin*/*admin* です。

ステップ 4　**[Login]** をクリックします。

第 3 章

ビジターの接続

ビジターの接続を使用してカスタム スプラッシュ ページを作成するためのワークフロー

表 3-1 は、ビジターの接続を使用してカスタム スプラッシュ ページを作成するためのワークフローです。

表 3-1　ビジターの接続を使用してカスタム スプラッシュ ページを作成するためのワークフロー

プロセス	説明
1. カスタム スプラッシュ ページの設定に関する前提条件	詳細については、「カスタム スプラッシュ ページの設定に関する前提条件」（P.3-2）を参照してください。
2. ソーシャル アプリケーションの認証	詳細については、「ソーシャル アプリケーションの設定」（P.3-6）を参照してください。
3. スプラッシュ テンプレート フィールドの作成	詳細については、「スプラッシュ テンプレート フィールドの作成」（P.3-8）を参照してください。
4. スプラッシュ テンプレートの作成	詳細については、「スプラッシュ テンプレートの作成」（P.3-11）を参照してください。
5. スプラッシュ テンプレートのロケーションへの割り当て	詳細については、「スプラッシュ テンプレートのロケーションへの割り当て」（P.3-12）を参照してください。

カスタム スプラッシュ ページの設定に関する前提条件

FlexConnect ACL の設定

Flex モードの展開に対してのみ、FlexFlexConnect ACL を設定する必要があります。FlexConnect ACL を設定するには、次の手順を実行します。

ステップ 1　コントローラ UI から **[Security] > [Access Control Lists] > [FlexConnect Access Control Lists]** の順に選択します。

[FlexConnect ACL] ページが表示されます。このページには、コントローラ上で設定したすべての FlexConnect ACL が一覧表示されます。このページには、対応するコントローラで作成した FlexConnect ACL も表示されます。ACL を削除するには、該当する ACL 名の横にある青のドロップダウン矢印の上にカーソルを移動し、**[Remove]** を選択します。

ステップ 2　[New] をクリックして、新しい ACL を追加します。

[Access Control Lists > New] ページが表示されます。

ステップ 3　**[Access Control List Name]** テキスト ボックスに、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 4　**[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。

[Access Control Lists > Edit] ページが表示されたら、**[Add New Rule]** をクリックします。

[Access Control Lists > Rules > New] ページが表示されます。

ステップ 6　この ACL のルールを次のように設定します。

a. コントローラは各 ACL について最大 64 のルールをサポートします。これらのルールは、1 から 64 の順にリストアップされます。[Sequence] テキスト ボックスで、値（1 ～ 64）を入力し、この ACL に定義されている他のルールに対するこのルールの順番を決定します。

（注）　ルール 1 ～ 4 がすでに定義されている場合にルール 29 を追加すると、これはルール 5 として追加されます。ルールのシーケンス番号を追加または変更した場合は、順序を維持するために他のルールのシーケンス番号が自動的に調整されます。たとえば、ルールのシーケンス番号を 7 から 5 に変更した場合、シーケンス番号 5 および 6 のルールはそれぞれ 6 および 7 へと自動的に番号が変更されます。

b. [Source] 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 を適用するパケットの送信元を指定します。

- **[Any]**：任意の送信元（これはデフォルト値です）。
- **[IP Address]**：特定の送信元。このオプションを選択する場合は、該当するテキスト ボックスに送信元の IP アドレスとネットマスクを入力します。

c. [Destination] 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 を適用するパケットの宛先を指定します。
   - **[Any]：**任意の宛先（これはデフォルト値です）。
   - **[IP Address]：**特定の宛先。このオプションを選択する場合は、テキスト ボックスに宛先の IP アドレスとネットマスクを入力します。

d. [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。使用できるプロトコル 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**
   - **UDP**
   - **[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]：**IP-in-IP パケットを許可または拒否します
   - **[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

（注） [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。

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（アドレス解決プロトコル（ARP）パケットなど）は指定できません。[TCP] または [UDP] を選択すると、[Source Port] および [Destination Port] の 2 つの追加のパラメータが表示されます。これらのパラメータを使用すれば、特定の送信元ポートと宛先ポート、またはポート範囲を選択することができます。ポート オプションは、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によって使用されます。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。

e. **[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。
   - **[Any]：**任意の DSCP（これは、デフォルト値です）
   - **[Specific]：**[DSCP] テキスト ボックスに入力する、0 ～ 63 の特定の DSCP

f. **[Action]** ドロップダウン リストから、**[Deny]** を選択してこの ACL でパケットがブロックされるようにするか、[Permit] を選択してこの ACL でパケットが許可されるようにします。デフォルト値は **[Deny]** です。

g. **[Apply]** をクリックします。

   [Access Control Lists] > [Edit] ページが表示され、この ACL のルールが示されます。

h. この ACL にさらにルールを追加するにはこの手順を繰り返します。

ステップ 7　**[Save Configuration]** をクリックします。

Web パススルー認証の WLAN の設定

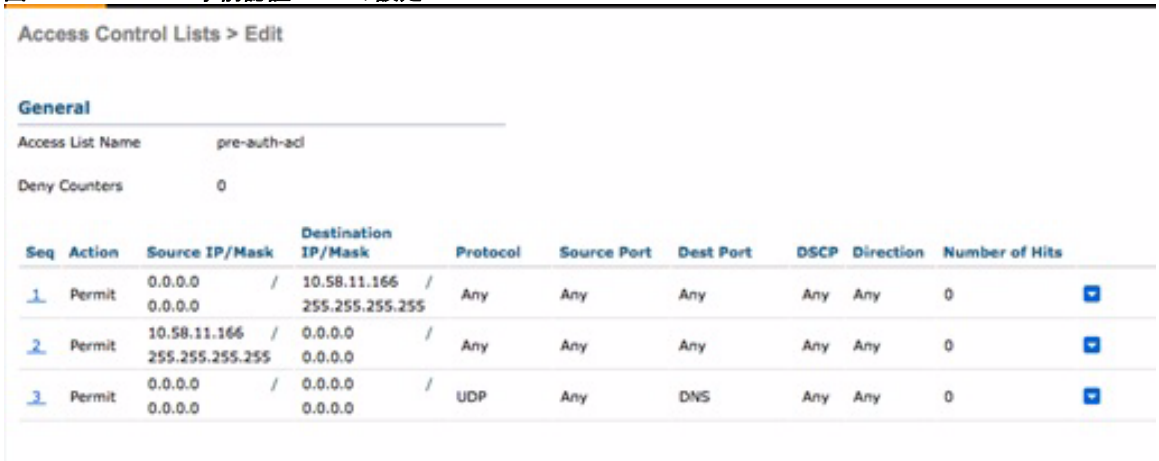
顧客へのネットワーク アクセスを提供するために、Cisco ワイヤレス LAN コントローラ（WLC）上に WLAN を設定する必要があります。これに対して、CMX ビジター接続用 WLAN のレイヤ 3 セキュリティに Web パススルーを設定する必要があります。

Web パススルー構成を設定するには、次の手順を実行します。

ステップ 1　コントローラ UI から事前認証に関するアクセス コントロール リスト（ACL）を定義して、MSE の IP アドレスへのトラフィックを許可し、WENAUTH_REQD 状態のときに DNS を解決できるようにします。他のすべてのトラフィックは、SSID に接続しているクライアントからブロックされます。ACL の設定の詳細については、http://www.cisco.com/en/US/products/ps12722/products_installation_and_configuration_guides_list.html の『Cisco Wireless LAN Configuratioffn Guide』を参照してください。

（注）　Flex 展開には ACL は必要ありません。

図 3-1　事前認証 ACL の設定



ステップ 2　**[WLANs]** を選択して、コントローラ UI から [WLANs] ページを開きます。

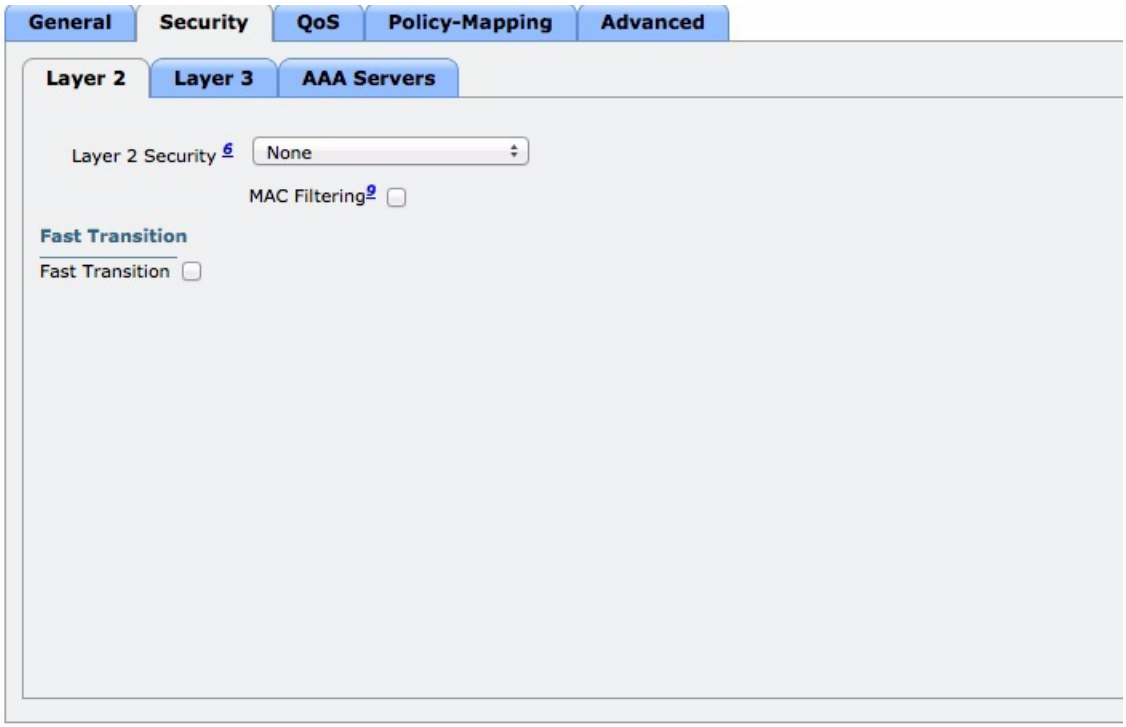
ステップ 3　必要な WLAN の ID 番号をクリックして、[WLANs > Edit] ページを開きます。

ステップ 4　**[Security] > [Layer 2]** タブを選択します。

ステップ 5　[Layer 2 Security] ドロップダウン リストから、**[None]** を選択します。

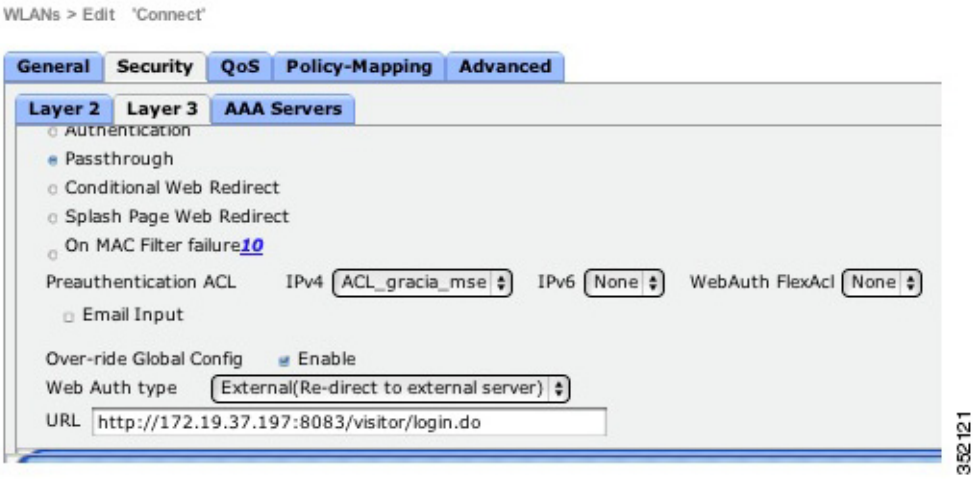
ステップ 6　**[Apply]** をクリックします。

図 3-2　　レイヤ 2 の設定



ステップ 7　[Security] タブおよび [Layer 3] タブを選択して、[WLANs > Edit]（[Security] > [Layer 3]）ページを開きます。

図 3-3　　Web パススルーの設定



ステップ 8　[Web Policy] チェックボックスをオンにします。

ステップ 9　事前認証 ACL を設定して、インターネットのほか、MSE および DNS 解決を除く他のネットワークにクライアントがアクセスすることを制限します。ユーザをコントローラ外部のサイトにリダイレクトするには、[Preauthentication ACL] ドロップダウン リストで設定された ACL を選択します。

アクセス コントロール リスト（ACL）とは、特定のインターフェイスへのアクセスを制限するために使用されるルール セットのことです。Web 認証用に事前認証 ACL を作成できます。事前認証 ACL を使用すると、認証が完了する前に、特定の種類のトラフィックを許可することができます。IPv4 および IPv6 のどちらもサポートされています。IPv6 ACL は、送信元、宛先、送信元ポート、宛先ポートなど、IPv4 ACL と同じオプションをサポートします。

事前認証に対して ACL を定義して、MSE の IP アドレスへのトラフィックを許可し、WENAUTH_REQD 状態のときに DNS を解決できるようにします。他のすべてのトラフィックは、SSID に接続しているクライアントからブロックされます。

事前認証 FlexConnect ACL は、フレックス モードでの展開に必要です。詳細については、「FlexConnect ACL の設定」（P.3-2）を参照してください。

ステップ 10　グローバル認証設定 Web 認証ページを無効にするには、**[Over-ride Global Config]** チェックボックスをオンにします。

ステップ 11　無線ゲスト ユーザ用の Web 認証ページを定義するには、[Web Auth Type] ドロップダウン リストから**[External]** 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。このオプションを選択する場合、[URL] テキスト ボックスに外部サーバの URL も入力する必要があります。

（注）　外部リダイレクト URL は、ビジター接続のキャプティブ ポータル URL を指している必要があります。

ステップ 12　[URL] テキスト ボックスに、スプラッシュ ページの URL を入力します。たとえば、次のように入力できます。*http://<MSE>:8083/visitor/login.do*

（注）　MSE がファイアウォールの背後にある場合、MSE 上で 8083 ポートへのトラフィックを許可するようセキュリティ ルールを変更する必要があります。セキュリティ ルールを変更しないと、スプラッシュ ページがビジターに表示されません。

ステップ 13　**[Apply]** をクリックして、変更を確定します。

ステップ 14　**[Save Configuration]** をクリックして、変更を保存します。

（注）　ビジター接続のリダイレクトでは、iOS デバイスについて WLC 上で特別な設定が必要になります。これは、`config network web-auth captive-bypass enable` コマンドを使用して実行できます。詳細については、http://www.cisco.com/c/en/us/td/docs/wireless/controller/7-4/configuration/guides/consolidated/b_cg74_CONSOLIDATED/b_cg74_CONSOLIDATED_chapter_01010101.html を参照してください。

ソーシャル アプリケーションの設定

ソーシャル認証では、施設のオーナーが Facebook、LinkedIn、および Google+ などのソーシャル ネットワーク プロバイダーでアプリケーションを作成する必要があります。ソーシャル アプリケーションが作成されたら、ビジターを正常に認証するために CMX ビジター接続で必要となるアプリケーション ID と秘密キーを提供します。

ソーシャル アプリケーションの作成時に、施設のオーナーは次の情報を提供する必要があります。

- 認可されたリダイレクト URL：*http://<mse>:8083/visitor/social.do*
- Javascript API ドメイン：*http://<mse>*

注意　Google、Facebook、および Linkedin ではワークフローを頻繁に変更する可能性があります。このため、ソーシャル メディア サイトで提供される公開情報を使用するか、Google でソーシャル アプリケーションの作成方法に関する最新の公開情報を検索してください。

- Facebook のアプリケーション リンク：https://developers.facebook.com/apps

（注）　Facebook アプリケーション ID と秘密キーの作成時に、[Facebook Developers] ページから [Sandbox Mode] を無効にします。

（注）　アプリケーションが Public（公開）使用に有効になっていることを確認してください。有効になっていない場合は、認証が失敗します。

- LinkedIn アプリケーションのリンク：https://www.linkedin.com/secure/developer
- Google+ アプリケーションのリンク：https://console.developers.google.com/project

スプラッシュ テンプレートの作成フローの一部として、ソーシャル コネクタを作成することができます。詳細については、「スプラッシュ テンプレートの設定」を参照してください。

（注）　クライアント認証は、MSE にプライベート IP アドレスがあり、MSE の IP アドレスがソーシャル アプリケーション設定で使用されている場合に失敗します。問題を修正するには、MSE の DNS 名を割り当て、ソーシャル アプリケーション設定で、MSE の IP アドレスではなく、MSE の DNS 名を使用します。MSE の DNS 名がゲスト SSID 設定で外部ポータル URL として確実に使用されるようにします。

（注）　CMX ビジター接続のスプラッシュ テンプレートのセットアップに必要な API キーを取得するために、Google Cloud Storage JSON API を有効にする必要があります。これをアクティブにするには、[Services] タブの [Google Cloud Storage JSON API] の隣にある **[Activate]** をクリックします（図 3-4 を参照）。

図 3-4　Google+ 向けのソーシャル アプリケーションの設定

スプラッシュ テンプレートの設定

スプラッシュ テンプレートでは、ゲスト ポータル用のスプラッシュ ページを設計することができます。スプラッシュ テンプレートの作成に関連する手順は次のとおりです。

- （任意）テンプレート フィールドの作成：詳細は「テンプレート フィールド」を参照してください。
- （任意）ソーシャル コネクタの作成：「ソーシャル コネクタ」を参照してください。
- スプラッシュ テンプレートの作成：「スプラッシュ テンプレート」
- スプラッシュ テンプレートの割り当て：「スプラッシュ テンプレートのロケーションへの割り当て」

テンプレート フィールド

テンプレート フィールドを使用して、登録時にビジターの情報を収集します。テンプレート フィールドには、名前、性別、電話番号などを含めることができます。

ここでは、次の内容について説明します。

- 「スプラッシュ テンプレート フィールドの作成」（P.3-8）
- 「テンプレート フィールドの編集」（P.3-9）
- 「テンプレート フィールドの削除」（P.3-9）

スプラッシュ テンプレート フィールドの作成

スプラッシュ テンプレート フィールドを作成するには、次の手順を実行します。

ステップ 1　左側のサイドバー メニューから、**[Visitor Connect] > [Template Fields]** の順に選択します。

ステップ 2　**[Create]** をクリックします。

[Add/Edit Splash Template] フィールドが表示されます。

ステップ 3　[Name] テキスト ボックスに作成するフィールドの名前を入力します。

ステップ 4　フィールド タイプを選択します。**[Text]** および **[List]**

ステップ 5　**[Submit]** をクリックして変更内容を適用するか、または **[Cancel]** をクリックしてフィールドの作成を廃棄します。

[Splash Template Fields] グループ ボックスに、新しく追加されたフィールドが表示されます。

テンプレート フィールドの編集

スプラッシュ テンプレート フィールドを編集するには、次の手順を実行します。

ステップ 1　左側のサイドバーのメニューから、**[Visitor Connect] > [Template Fields]** の順に選択します。

ステップ 2　[Splash Template Fields] グループ ボックスで編集するフィールドを強調表示し、**[Edit]** をクリックします。

ステップ 3　[Add/Edit Splash Template Field] グループ ボックスで必要な変更を行い、**[Submit]** をクリックします。

テンプレート フィールドの削除

スプラッシュ テンプレート フィールドを削除するには、次の手順を実行します。

ステップ 1　左側のサイドバーのメニューから、**[Visitor Connect] > [Template Fields]** の順に選択します。

ステップ 2　[Splash Template Fields] グループ ボックスで削除するフィールドを強調表示し、**[Delete]** をクリックします。

ステップ 3　削除を確定する場合は [Delete Confirmation] グループ ボックスで **[OK]** をクリックし、変更を行わずにページを閉じる場合は **[Close]** をクリックします。

ソーシャル コネクタ

ビジター接続を使用すると、施設のオーナーはソーシャル ネットワーク認証を使用して、顧客に Wi-Fi アクセスを提供することができます。これには、施設のオーナーが Facebook、Google+、LinkedIn などのソーシャル ネットワーク サイトでアプリケーションを作成する必要があります。詳細については、ソーシャル コネクタのセットアップを参照してください。

（注）　ソーシャル コネクタを作成するために、Facebook、Google+、および LinkedIn のサイトを使用できます。ビジターはこれらのコネクタのどれかに対するクレデンシャルを使用できます。

- 「ソーシャル コネクタの設定」（P.3-10）
- 「ソーシャル コネクタ エントリの編集」（P.3-10）
- 「ソーシャル コネクタの削除」（P.3-10）

ソーシャル コネクタの設定

ソーシャル コネクタ メニューを使用して、複数のソーシャル コネクタを作成できます。ソーシャル コネクタを設定するには、次の手順を実行します。

ステップ 1　左側のサイドバーのメニューから、**[Visitor Connect] > [Social Connector]** の順に選択します。

ステップ 2　**[Create]** をクリックします。

[Add/Edit Social Connectors] グループ ボックスが表示されます。

ステップ 3　[Connector Name] テキスト ボックスに、ソーシャル コネクタ名を入力します。最大 10 個のソーシャル コネクタを作成できます。

ステップ 4　Facebook の認証を提供するには、Facebook アプリケーションを作成した後で受信した Facebook APP ID を [Facebook] テキストボックスに入力します。

ステップ 5　LinkedIn の認証を提供するには、受信した LinkedIn API キーを [Linkedin] テキストボックスに入力します。

ステップ 6　Google+ の認証を提供するには、Google API クライアント ID と Google API キーを [Google+] テキストボックスに入力します。

ステップ 7　**[Submit]** をクリックします。

ソーシャル コネクタ エントリの編集

ソーシャル コネクタ エントリを編集するには、次の手順を実行します。

ステップ 1　左側のサイドバーのメニューから、**[Visitor Connect] > [Social Connector]** の順に選択します。

ステップ 2　[Social Connectors] グループ ボックスのソーシャル コネクタ エントリをクリックして強調表示し、**[Edit]** をクリックします。

ステップ 3　[Add/Edit Social Connectors] グループ ボックスで必要な変更を行い、**[Submit]** をクリックします。

ソーシャル コネクタの削除

ソーシャル コネクタを削除するには、次の手順を実行します。

ステップ 1　左側のサイドバーのメニューから、**[Visitor Connect] > [Social Connector]** の順に選択します。

ステップ 2　[Social Connectors] グループ ボックスのソーシャル コネクタ エントリをクリックして強調表示し、**[Delete]** をクリックします。

ステップ 3　**[OK]** をクリックして削除を確定するか、**[Close]** をクリックして、変更を加えずにページを閉じます。

スプラッシュ テンプレート

異なるロケーションまたはゾーンを扱うために、ロケーション認識のスプラッシュ テンプレートを作成できます。複数のスプラッシュ テンプレートを作成し、それをさまざまな関心のあるポイントに割り当てることができます。

- 「スプラッシュ テンプレートの作成」（P.3-11）
- 「スプラッシュ テンプレートのロケーションへの割り当て」（P.3-12）

スプラッシュ テンプレートの作成

スプラッシュ テンプレートを作成するには、次の手順を実行します。

ステップ 1　左側のサイドバー メニューから **[Visitor Connect]** を選択します。

[Splash Template Configuration] ページが表示されます。

ステップ 2　[Splash Templates] グループ ボックスで **[Create]** をクリックします。

[Add/Edit Splash Template] ウィザードが表示されます。

ステップ 3　[Template Name] テキストに、スプラッシュ ページの名前を入力します。

ステップ 4　[Background] ドロップダウン リストから、スプラッシュ ページに対して事前に設定されている背景を選択します。好みの背景を設定するには、[Template Background] ドロップリストから [Custom] を選択し、**[Click to upload an image]** をクリックして、スプラッシュ ページの背景のイメージをアップロードします。

ステップ 5　[Form Fields] リストから、スプラッシュ ページに含めるフィールドを選択します。**[Visitor Connect] > [Template Fields] > [Create]** メニューを使用して、すでにテンプレート フィールドを作成している場合は、フィールドが表示されます。テンプレート フィールドを作成していない場合は、**[Create Template Fields]** をクリックして「スプラッシュ テンプレート フィールドの作成」（P.3-8）に記載されている手順を実行します。

ステップ 6　[Form Fields] リストで選択したスプラッシュ フィールドの詳細を入力します。[List] のテンプレート フィールド タイプには、提供する選択肢のリストを入力します。

ステップ 7　[Terms&Conditions] テキストボックスで、スプラッシュ ページに表示する条件を入力します。

ステップ 8　[Header] テキスト ボックスに、顧客向けのようこそメッセージを入力します。たとえば「XYZ ショッピング センターへようこそ」と入力できます。

ステップ 9　[Footer] テキスト ボックスに、免責事項を入力できます。

ステップ 10　**[Next]** をクリックして、スプラッシュ ページに表示するアドバタイズメントを入力します。

ステップ 11　[Ad Script] テキスト ボックスに、アドバタイズメントのサーバまたはスタティック HTML ページ、または動画グラフィックスを使用した HTML ページを指す html スクリプトを入力します。

これは、YouTube の URL を指しているサンプル広告の設定です。どのような HTML も提供することができます。

```
<iframe width="100%" height="100%" src="//www.youtube.com/embed/imW392e6XR0"
frameborder="0" allowfullscreen></iframe>.
```

（注）　アドバタイズメントは、任意です。アドバタイズメントで URL を指定しなければ、ゲストのオンボーディング時にアドバタイズメント ページがスキップされます。

ステップ 12　**[Next]** をクリックして、ビジターのログイン用のソーシャル認証を設定します。

（注）　ソーシャル認証は、任意です。ソーシャル コネクタを選ばなければ、ゲストのオンボーディング時に [Social Authentication] ページがスキップされます。

ステップ 13　[Header] テキスト ボックスに、ソーシャル認証ページで表示する情報を入力します。たとえば、「おめでとうございます。XYZ 社の Wi-Fi ネットワークにいらっしゃいます」と入力できます。

ステップ 14　[Social Connector] ドロップダウン リストから、ソーシャル コネクタを選択します。**[Visitor Connect] > [Social Connectors]** メニューを使用してすでにソーシャル コネクタを作成している場合は、ソーシャル コネクタ フィールドが表示されます。作成していない場合、**[Create Social Connectors]** をクリックし、「ソーシャル コネクタの設定」（P.3-10）に記載されている手順を実行します。

ステップ 15　[Social Auth] チェックボックスから該当する認証タイプを選択します。

ステップ 16　[Footer] テキスト ボックスに情報を入力します。

ステップ 17　**[Submit]** をクリックします。

ステップ 18　認証が正常に終了した後で、ユーザを特定のページにリダイレクトするには、[Redirect URL] テキストボックスに URL を入力します。

スプラッシュ テンプレートのロケーションへの割り当て

スプラッシュ テンプレートを、マップ内の 1 つ以上のロケーションに割り当てることができます。これによって、施設のオーナーは顧客に「ロケーションを意識した」ネットワーク アクセスを提供できます。

スプラッシュ テンプレートをフロアに割り当てるには、次の手順を実行します。

ステップ 1　左側のサイドバー メニューから、**[Maps]** を選択します。

（注）　PI から、マップが更新されたことを確認します。詳細については、Prime Infrastructure からのマップの更新を参照してください。

ステップ 2　右側のペインで、**[Maps] > [System Campus] >** *[desired Building]* **>** *[desired Floor]* を選択します。

（注）　ビルディングがフロアに適用されるだけでなく、この継承関係はロケーションのすべての層に適用されます。

（注）　ビルディングにスプラッシュ テンプレートを割り当てると、そのビルディングに定義されているすべてのフロアがスプラッシュ テンプレートを継承します。ビルディングとフロアの両方で定義したスプラッシュ テンプレートがある場合、フロア スプラッシュ テンプレートが使用されます。

ステップ 3　[Visitor Connect Splash Template] ドロップダウン リストから、選択したフロアに割り当てるスプラッシュ ページ テンプレートを選択します。

ステップ 4　**[Submit]** をクリックします。

Prime Infrastructure からのマップの更新

PI でキャンパス、ビルディング、またはフロアを修正する場合は、CMX Connect & Engage で更新する必要があります。Prime Infrastructure からマップを更新するには、次の手順を実行します。

ステップ 1　左側のサイドバー メニューから、**[Maps]** を選択します。

ステップ 2　右側のペインで **[Update Maps from PI]** をクリックします。

ステップ 3　[Update Confirmation] ダイアログボックスで **[OK]** をクリックします。

ビジター接続のレポート

ビジターの詳細情報のモニタリング

ビジターの詳細情報をモニタするには、次の手順を実行します。

ステップ 1　左側のサイドバー メニューから **[Summary]** を選択します。

ステップ 2　ビジターの詳細をモニタするには、右側のペインで **[Visitor Connect]** タブをクリックします。

- [Visitor Connect] で接続された新しいビジターおよびビジターの合計について、時間単位で傾向を表示するには、**[Hourly]** をクリックして、開始日時と終了日時を選択します。

図 3-5　新しいビジターの時間別傾向

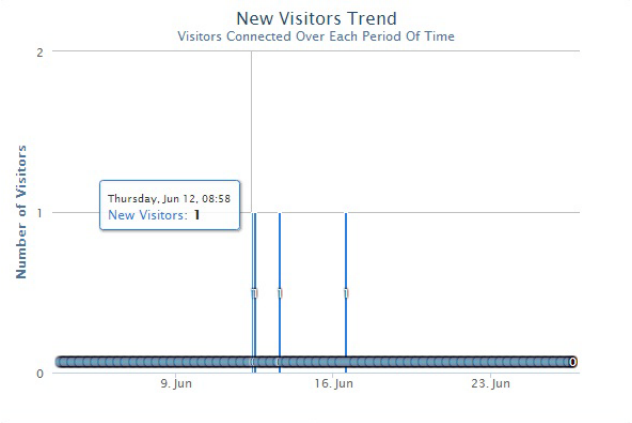
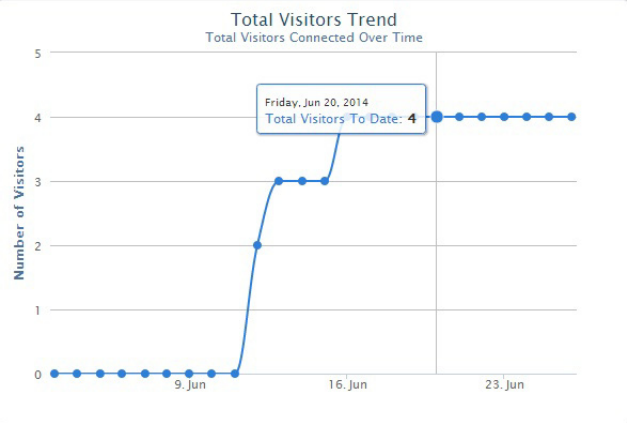


図 3-6　すべてのビジターの時間別傾向

- 新しいビジターおよびすべてのビジターの日単位の傾向を表示するには、**[Daily]** をクリックし、開始日と終了日を選択します。

図 3-7　新しいビジターの日別傾向

図 3-8　すべてのビジターの日別傾向



- 新しいビジターおよびすべてのビジターの週単位の傾向を表示するには、**[Weekly]** をクリックし、開始日と終了日を選択します。

図 3-9　新しいビジターの週別傾向

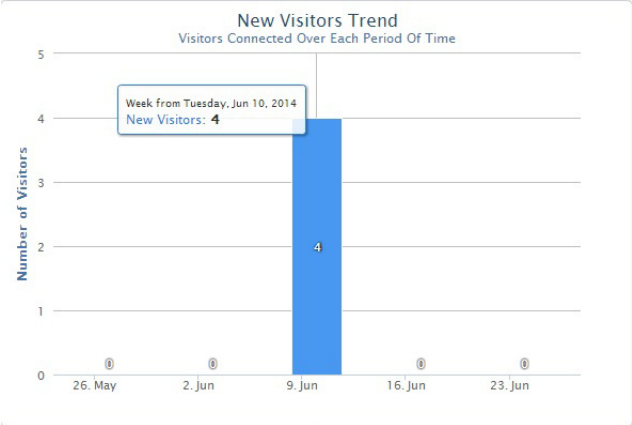
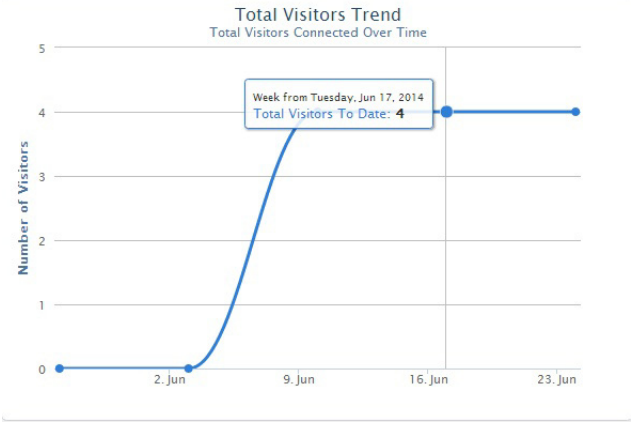


図 3-10　すべてのビジターの週別傾向



- 新しいビジターおよびすべてのビジターの月単位の傾向を表示するには、**[Monthly]** をクリックし、月を選択します。

図 3-11　新しいビジターの月別傾向

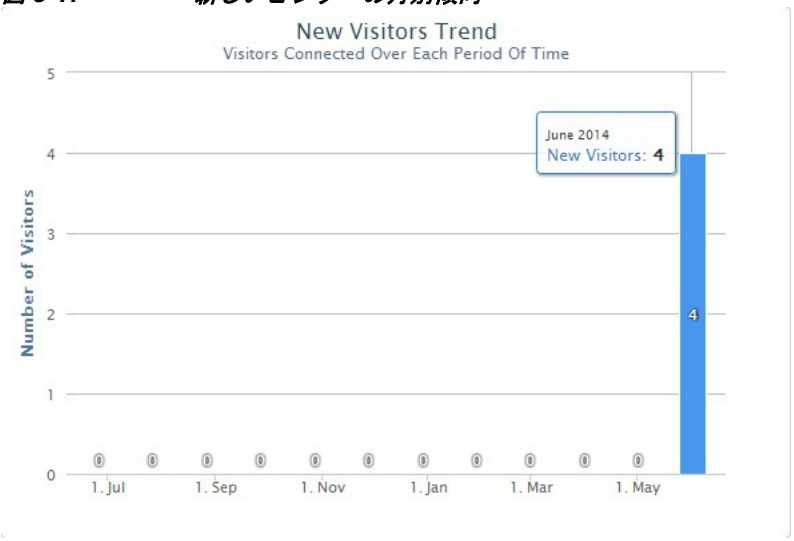
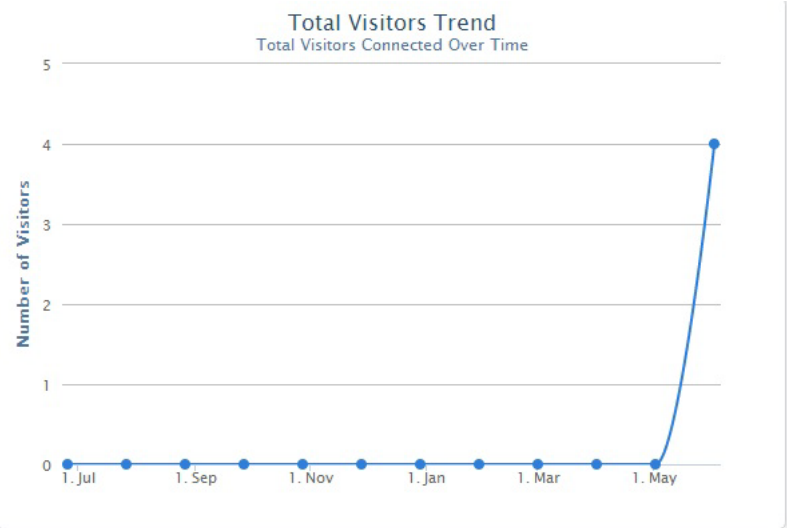


図 3-12　　すべてのビジターの月別傾向



ステップ 3　ページの下部の [Active Visitors] の表は、スプラッシュ テンプレートの設定に基づいて、アクティブなビジターに関する登録情報を一覧で示しています。表のこの情報は、ソートおよびフィルタリングできます。

ステップ 4　アクティブなビジターのすべての詳細情報をエクスポートするには、**[Export to CSV] > [Export Active Visitors]** をクリックします。ビジターのすべての詳細情報をエクスポートするには、**[Export to CSV] > [Export All Visitors]** をクリックします。

ビジターのポリシー設定

ビジターのポリシーにより、MSE はさまざまなタイプのビジターを区別することができます。ビジターのポリシーを使用すると、ユーザのタイプごとにネットワークの使用制限を定義できます。使用できるユーザ グループは次のとおりです。

- 基本ユーザ：ユーザが [Visitor Connect splash] ページにリダイレクトされると、そのユーザには、ソーシャル ネットワーク ID でログインするオプションが付与されます。ビジターがソーシャル ネットワーク ID を使用してログインしない場合、そのユーザは基本グループに配置されます。ビジターに使用制限を割り当てることができます。その日の使用制限に達すると、ビジターは次の日にログインするよう要求されます。これは、使用のカウントが午前 0 時（00.00）に始まるためです。デフォルトの使用制限は 300 MB です。
- ソーシャル ユーザ：ビジターがソーシャル ネットワーク ID でログインした場合、そのユーザはソーシャル グループに配置されます。このグループには、Wi-Fi Facebook ユーザも含まれます。デフォルトでは、デフォルトの使用制限は 1 日 3 GB です。

（注）　ビジターのポリシー設定は、ビジター接続と Facebook Wi-Fi の両方に適用されます。

ビジター ポリシーの有効化とユーザ グループの編集

ビジター ポリシーを有効にしてユーザ グループを編集するには、次の手順を実行します。

ステップ 1　左側のサイドバー メニューから **[Visitor Policy]** を選択します。

ステップ 2　[Visitor Policy] グループ ボックスの **[Enable]** をクリックします。

ステップ 3　使用制限を編集するには、**[Edit]** アイコン、または [Usage Cap number] をクリックします。

ステップ 4　使用率の値を保存するには、[outside] をクリックします。

CMX Facebook Wi-Fi

CMX Facebook Wi-Fi の概要

Facebook Wi-Fi では、お客様が Facebook ページを Wi-Fi キャプティブ ページとして使用することができます。これにより、お客様は自身の Facebook アカウントにチェックインした後で、自身のモバイル デバイスからフリー Wi-Fi へアクセスすることが可能になります。Facebook Wi-Fi は、企業が顧客についてより多くのことを知るうえで有用です。

CMX Facebook Wi-Fi は Wireless LAN Controllers（WLC）上の WLAN Web パススルー認証に基づいています。コントローラは HTTP/HTTPs のトラフィックを傍受し、クライアント ブラウザを MSE へリダイレクトします。MSE はクライアントの場所を見つけて、クライアント ブラウザの場所を、事前に設定された場所の特定の 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、MSE 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。

CMX Facebook Wi-Fi の機能

- シンプルで無料の Wi-Fi
- In-venue プロモーション
- デモグラフィック データの提供 : Facebook の統計情報およびデモグラフィック データの収集方法の詳細については、http://www.slideshare.net/EmergenceMedia/facebook-demographics-user-statistics-emergence-media を参照してください。
- ブランド露出の向上

（注） OVA を実装していて、MSE 向けに移行する場合は、MSE の展開のみ必要で、OVA のセットアップおよび Policy Based Routing（PBR）は必要ありません。

表 4-1　Facebook Wi-Fi とビジター接続 OAuthentication の違い

Facebook Wi-Fi	ビジター接続と Facebook OAuthentication
シスコと Facebook 間の特殊なプロトコルを使用する。	Web 認証で広く使用されている一般的なプロトコルを使用する。
クライアントは Facebook 認証なしで Web にアクセスできない。	リリース 8.0 のビジター接続（カスタマイズされたゲスト ポータル）では、クライアントは Facebook 認証なしで Web にアクセスできる。
クライアントは、Facebook でホストされるゲスト ログイン ページを提供される。	リリース 8.0 のビジター接続（カスタマイズされたゲスト ポータル）では、クライアントは、CMX でホストされるカスタマイズされたポータルを提供され、Facebook でそれを認証する。

CMX Facebook Wi-Fi のワークフロー

表 4-2 に、CMX Facebook Wi-Fi を設定する手順について説明します。

表 4-2　CMX Facebook Wi-Fi のセットアップのワークフロー

プロセス	説明
1. アクセス コントロール リストの設定	次の URL を参照してください。アクセス コントロール リストの設定
2. 認証用の WLAN の設定	次の URL を参照してください。Web パススルー認証の WLAN の設定
3. Facebook ページの作成	次の URL を参照してください。組織の Facebook ページの作成
4. デフォルトの Facebook ページの作成およびペアリング	次の URL を参照してください。デフォルトの Facebook ページのペアリング
5. MSE と特別なロケーションを Facebook ページとペアリングする	次の URL を参照してください。ロケーションと Facebook ページのペアリング

アクセス コントロール リストの設定

Facebook Wi-Fi 用のアクセス コントロール リスト（ACL）を設定するには、次の手順を実行します。

ステップ 1　[Controller UI] から、**[Security]** > **[Access Control Lists]** > *[Access Control Name]* リンクを選択します。

ステップ 2　**[New]** をクリックして、新しい ACL を追加します。[Access Control Lists > New] ページが表示されます。

ステップ 3　[Access Control List Name] テキスト ボックスに、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 4　ACL タイプを選択します。IPv4 と IPv6 の 2 つの ACL のタイプがサポートされています。

ステップ 5　**[Apply]** をクリックします。[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　[Access Control Lists > Edit] ページが表示されたら、**[Add New Rule]** をクリックします。[Access Control Lists > Rules > New] ページが表示されます。

ステップ 7　この ACL のルールを次のように設定します。

a. コントローラは各 ACL について最大 64 のルールをサポートします。これらのルールは、1 から 64 の順にリストアップされます。[Sequence] テキスト ボックスで、値（1 ～ 64）を入力し、この ACL に定義されている他のルールに対するこのルールの順番を決定します。

（注）　ルール 1 ～ 4 がすでに定義されている場合にルール 29 を追加すると、これはルール 5 として追加されます。ルールのシーケンス番号を追加または変更した場合は、順序を維持するために他のルールのシーケンス番号が調整されます。たとえば、ルールのシーケンス番号を 7 から 5 に変更した場合、シーケンス番号 5 および 6 のルールはそれぞれ 6 および 7 へと自動的に番号が変更されます。

b. [Source] 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 を適用するパケットの送信元を指定します。

- **[Any]：**任意の送信元（これはデフォルト値です）。
- **[IP Address]：**特定の送信元。このオプションを選択する場合は、テキスト ボックスに送信元の IP アドレスとネットマスクを入力します。IPv6 ACL を設定している場合は、テキスト ボックスに宛先の IPv6 アドレスとプレフィックスの長さを入力します。

c. [Destination] 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 を適用するパケットの宛先を指定します。

- **[Any]：**任意の宛先（これはデフォルト値です）。
- **[IP Address]：**特定の宛先。このオプションを選択する場合は、テキスト ボックスに宛先の IP アドレスとネットマスクを入力します。IPv6 ACL を設定している場合は、テキスト ボックスに宛先の IPv6 アドレスとプレフィックスの長さを入力します。

d. [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/ICMPv6]：**インターネット制御メッセージ プロトコル

（注）　ICMPv6 は IPv6 ACL でのみ使用可能です。

- **[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

（注）　[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。

ステップ 8　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。

e. 前の手順で [TCP] または [UDP] を選択すると、[Source Port] および [Destination Port] の 2 つのパラメータも追加で表示されます。これらのパラメータを使用すれば、特定の送信元ポートと宛先ポート、またはポート範囲を選択することができます。ポート オプションは、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によって使用されます。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。

（注）　ACL タイプに基づく送信元および宛先ポート。

f. [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。

- **[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

g. [Direction] 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 を適用するトラフィックの方向を指定します。

- **[Any]：**任意の方向（これはデフォルト値です）
- **[Inbound]：**クライアントから
- **[Outbound]：**クライアントへ

（注）　この ACL をコントローラ CPU に適用する予定の場合、パケットの方向は重要ではないので常に「Any」です。

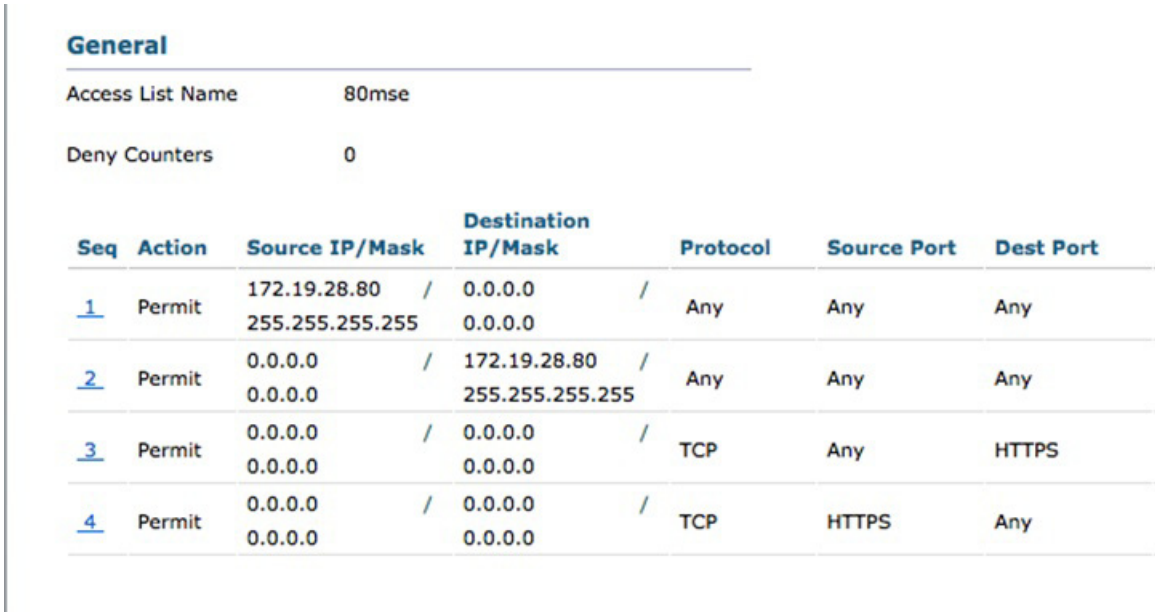
h. **[Action]** ドロップダウン リストから、[Deny] を選択してこの ACL でパケットがブロックされるようにするか、[Permit] を選択してこの ACL でパケットが許可されるようにします。デフォルト値は [Deny] です。

i. [Apply] をクリックして、変更を確定します。[Access Control Lists > Edit] ページが再表示され、この ACL のルールが示されます。
[Deny Counters] フィールドには、パケットが明示的拒否 ACL ルールに一致した回数が表示されます。**[Number of Hits]** フィールドには、パケットが ACL ルールに一致した回数が表示されます。これらのフィールドを有効にするには、[Access Control Lists] ページ上で ACL カウンタを有効にする必要があります。

（注）　ルールを編集する場合は、希望のルールのシーケンス番号をクリックし、[Access Control Lists > Rules > Edit] ページを開きます。ルールを削除するには、該当するルールの青いドロップダウン矢印の上にカーソルを置き、**[Remove]** を選択します。

次に、認証の前のアクセスについて選択するさまざまなオプションを示します。

- Allow HTTPs traffic only before authentication and block all the traffic：
  - このオプションを選択するには、[Source Port] または [Dest Port] の値が HTTPs であるシーケンス番号をクリックします。[Access Control Lists > Rules > Edit] ページが表示されます。ここで [Action] ドロップダウン リストから **[Permit]** を選択し、**[Apply]** をクリックします。



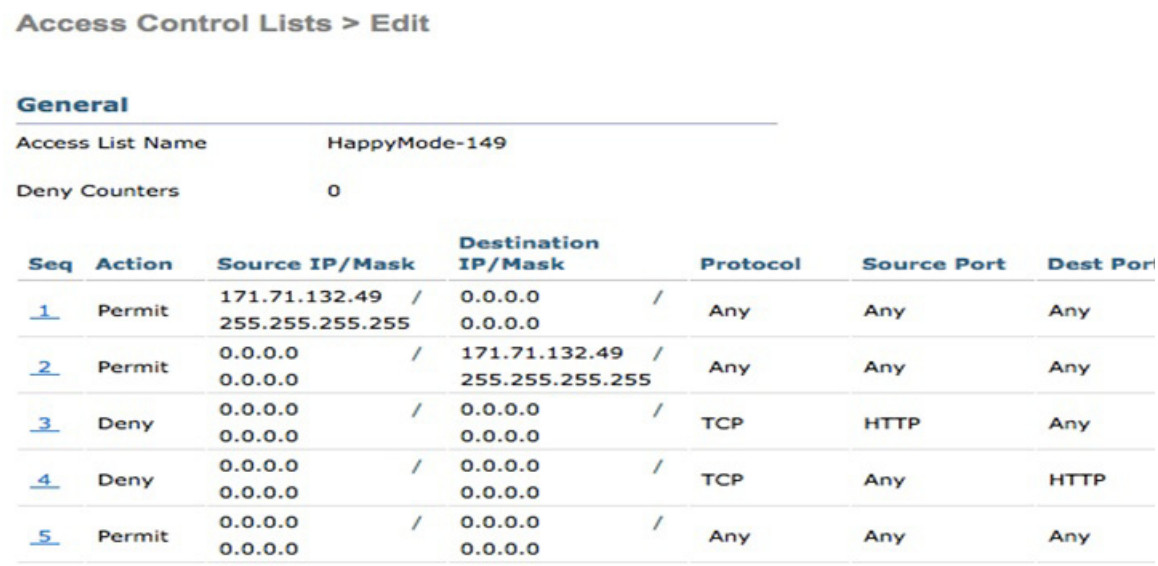
General

Access List Name　80mse

Deny Counters　0

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port
1	Permit	172.19.28.80 / 255.255.255.255	0.0.0.0 / 0.0.0.0	Any	Any	Any
2	Permit	0.0.0.0 / 0.0.0.0	172.19.28.80 / 255.255.255.255	Any	Any	Any
3	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	TCP	Any	HTTPS
4	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	TCP	HTTPS	Any

- Allow all the traffic before authentication and intercept HTTP only：
  - HTTP を傍受するには、[Source Port] または [Dest Port] の値が HTTP であるシーケンス番号をクリックします。[Access Control Lists > Rules > Edit] ページが表示されます。ここで [Action] ドロップダウン リストから **[Deny]** を選択し、**[Apply]** をクリックします。



Access Control Lists > Edit

General

Access List Name　HappyMode-149

Deny Counters　0

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port
1	Permit	171.71.132.49 / 255.255.255.255	0.0.0.0 / 0.0.0.0	Any	Any	Any
2	Permit	0.0.0.0 / 0.0.0.0	171.71.132.49 / 255.255.255.255	Any	Any	Any
3	Deny	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	TCP	HTTP	Any
4	Deny	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	TCP	Any	HTTP
5	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any

ステップ 9　**[Save Configuration]** をクリックして、変更を保存します。

ステップ 10　さらに ACL を追加するにはこの手順を繰り返します。

Web パススルー認証の WLAN の設定

顧客へのネットワーク アクセスを提供するために、Cisco ワイヤレス LAN コントローラ（WLC）上に WLAN を設定する必要があります。これに対して、CMX ビジター接続用 WLAN のレイヤ 3 セキュリティに Web パススルーを設定する必要があります。

Web パススルー構成を設定するには、次の手順を実行します。

ステップ 1　**[WLANs]** を選択して、コントローラ UI から [WLANs] ページを開きます。

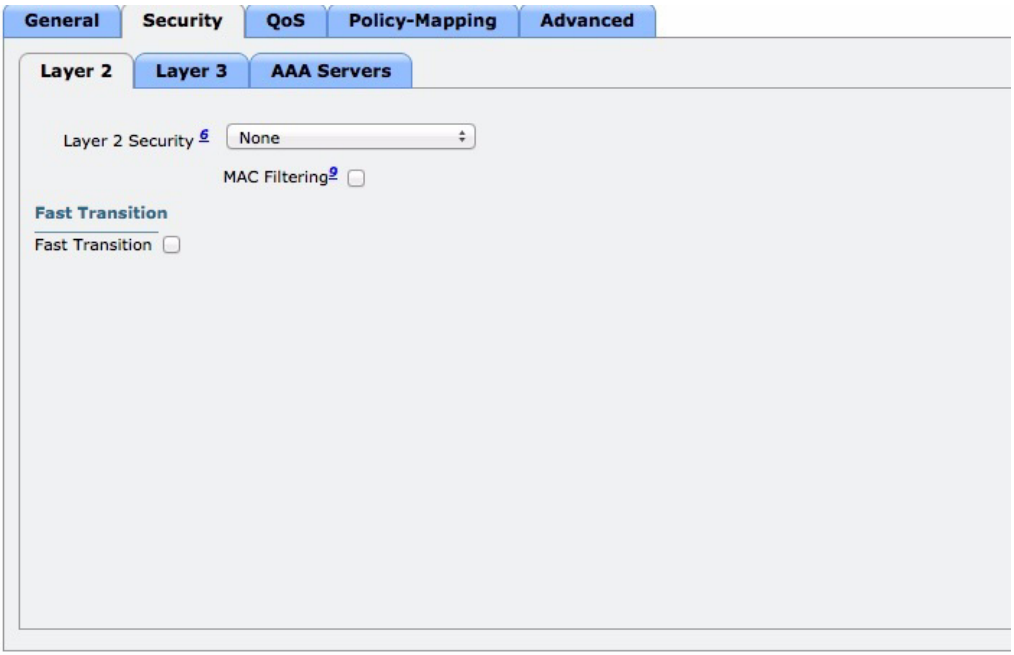
ステップ 2　必要な WLAN の ID 番号をクリックして、[WLANs > Edit] ページを開きます。

ステップ 3　**[Security] > [Layer 2]** タブを選択します。

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。

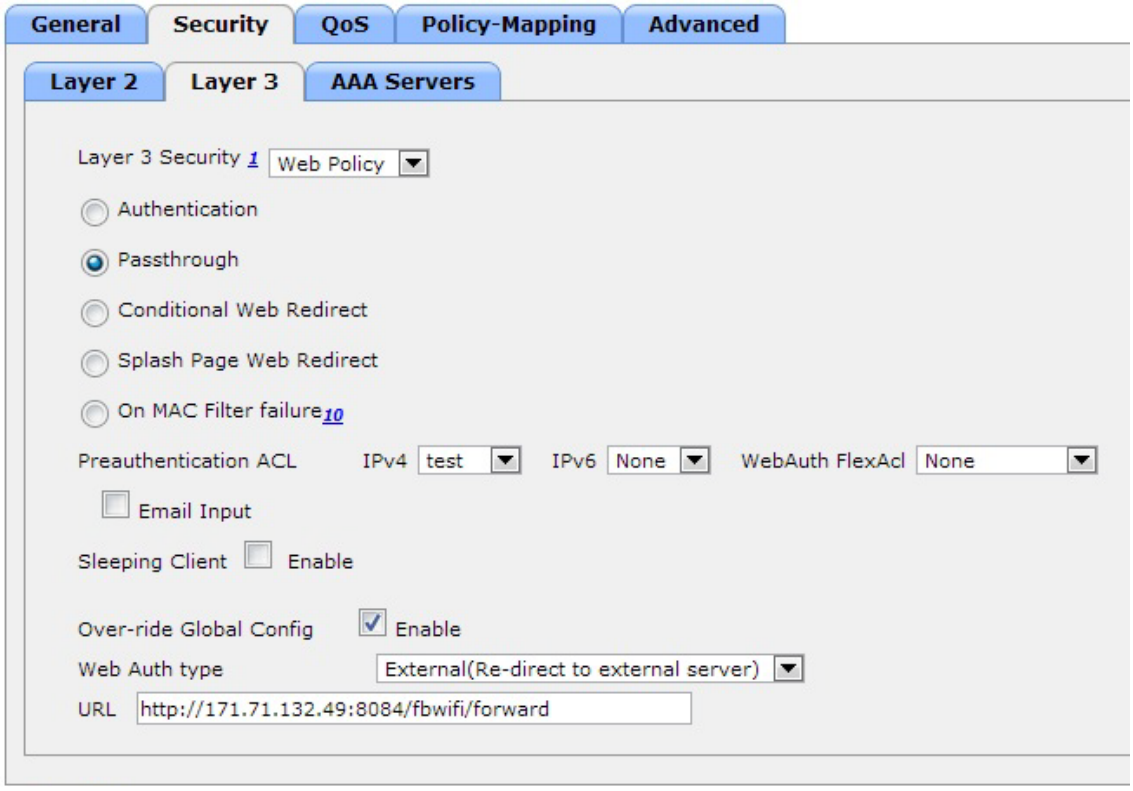
ステップ 5　**[Apply]** をクリックします。

図 4-1　　レイヤ 2 の設定



ステップ 6　[Security] タブおよび [Layer 3] タブを選択して、[WLANs > Edit]（[Security] > [Layer 3]）ページを開きます。

図 4-2　　Web パススルーの設定



ステップ 7　[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 8　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 9　グローバル認証設定 Web 認証ページを無効にするには、**[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には、[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。このオプションを選択する場合、[URL] テキスト ボックスに外部サーバの URL も入力する必要があります。

ステップ 11　[URL] テキストボックスに、[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 MSE 上のポータルを指している必要があります。たとえば、次のように入力できます。*http://<MSE>:8084/fbwifi/forward*

（注）　MSE がファイアウォールの背後にある場合、MSE 上で 8084 ポートへのトラフィックを許可するようセキュリティ ルールを変更する必要があります。セキュリティ ルールを変更しないと、スプラッシュ ページがビジターに表示されません。

ステップ 12　この SSID を有効にします。

ステップ 13　**[Apply]** をクリックして、変更を確定します。

ステップ 14　**[Save Configuration]** をクリックして、変更を保存します。

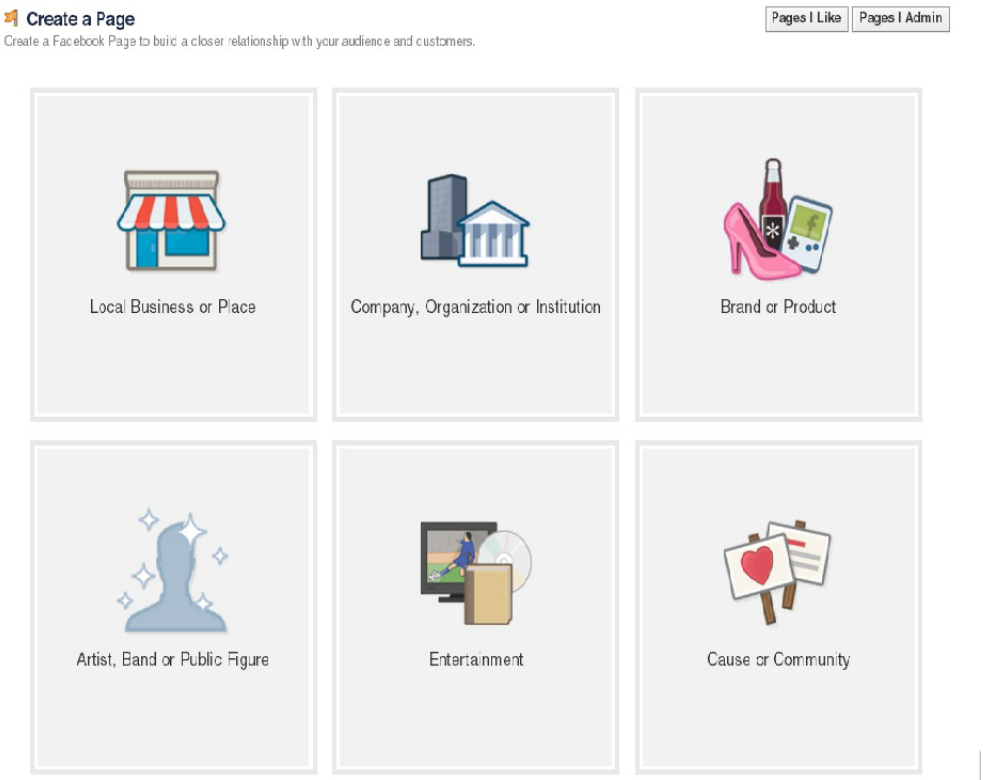
（注）　ビジター接続のリダイレクトでは、iOS デバイスについて WLC 上で特別な設定が必要になります。次のコマンドを使用して実行できます。`config network web-auth captive-bypass enable`

組織の Facebook ページの作成

Facebook ページを作成するには、次の手順を実行します。

ステップ 1　https://www.facebook.com/pages/create に移動します。

次のページが表示されます。



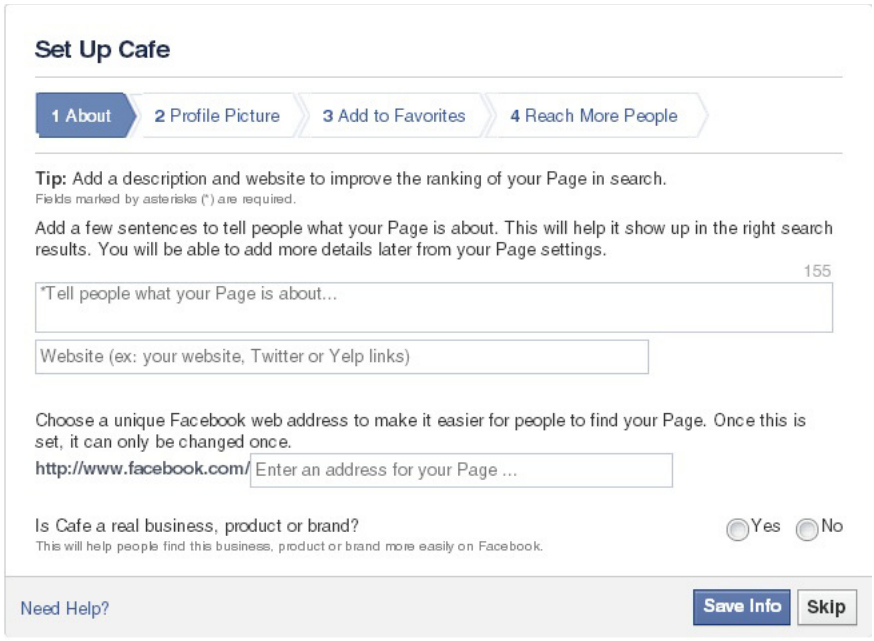
ステップ 2　ページ カテゴリをクリックします。

ステップ 3　[Choose a category] ドロップダウン メニューで、具体的なカテゴリを選択し、必要な情報を入力します。

ステップ 4　**[I agree to Facebook Pages terms]** の隣のチェックボックスをオンにします。

ステップ 5　**[Get Started]** をクリックします。

Set Up ウィザードが表示されます。



ステップ 6　Set Up ウィザードで提示される指示に従ってページを完成させるか、**[Skip]** をクリックして、作成したページへアクセスします。

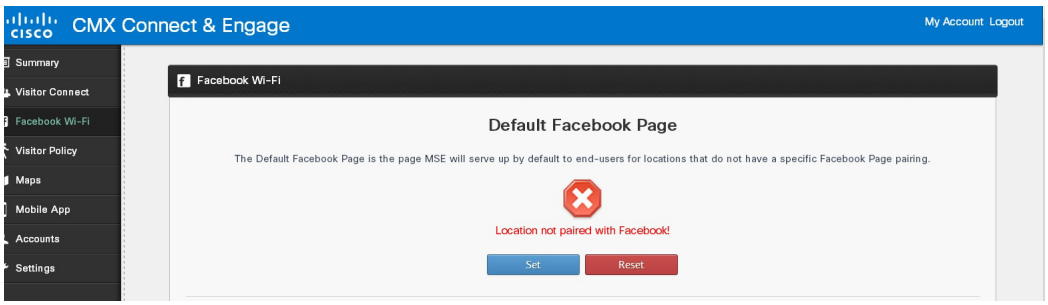
デフォルトの Facebook ページのペアリング

MSE は、特定の Facebook ページのペアリングを持っていないロケーションに対して、または MSE がクライアントを見つけられない場合に、デフォルトの Facebook ページを表示します。

デフォルトの Facebook ページを作成するには、次の手順を実行します。

ステップ 1　左側のサイドバー メニューで **[Facebook Wi-Fi]** を選択します。

右側のペインに [Facebook Wi-Fi] ページが表示されます。



ステップ 2　[Default Facebook] ページで **[Set]** をクリックします。

[Facebook Wi-Fi Configuration] ページが表示されます。

（注）　[Facebook Wi-Fi Configuration] ページは、有効な Facebook ページが作成されている場合のみ表示されます。

ステップ 3　[Select a Page] ドロップダウン リストから適切な Facebook ページを選択します。このページは、ペアリングされた Facebook ページを持たないすべてのロケーションに対して表示されます。

ステップ 4　[Bypass Mode] オプションで、Facebook アカウントを持たないゲスト ユーザに対して、**[Skip check-in link]** または **[Require Wi-Fi code]** ラジオボタンを選択できます。

ステップ 5　[Session Length] ドロップダウン リストから、顧客がチェックインした後で Wi-Fi 接続を保持する期間を選択します。

ステップ 6　[You've Set Up Facebook Wi-Fi] の確認のダイアログボックスで **[Okay]** をクリックします。

ステップ 7　[CMX Connect &Engage Dashboard] に切り替えます。

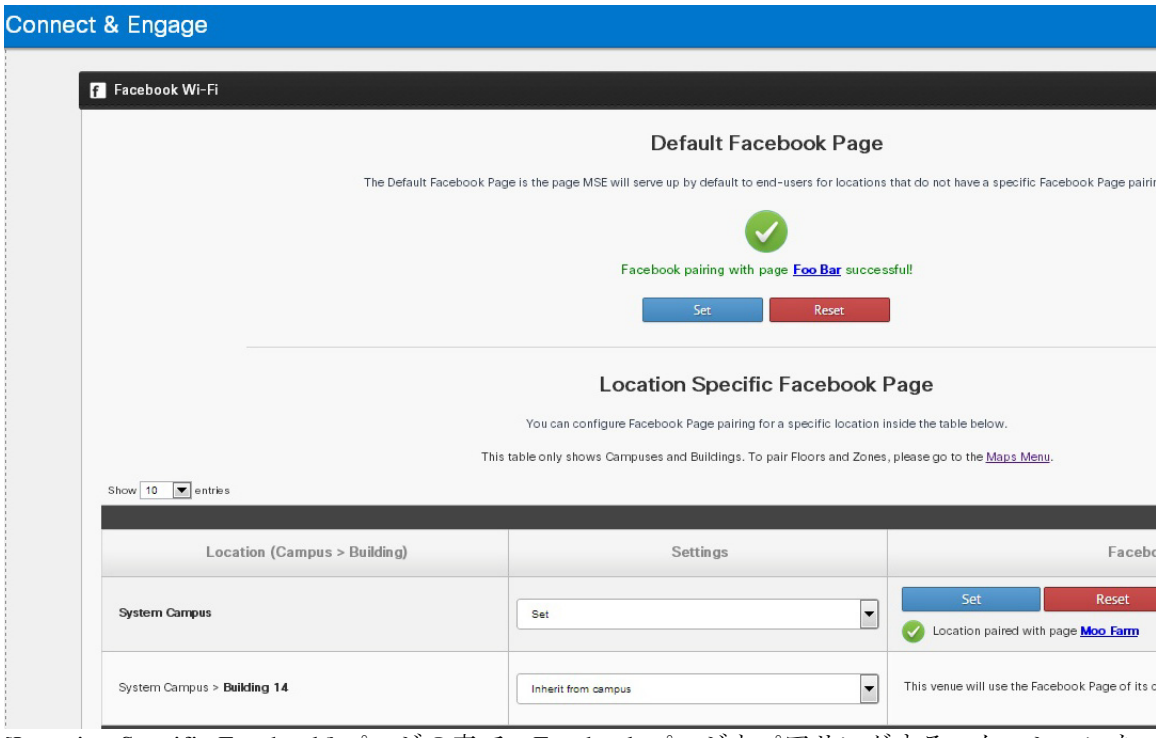
ロケーションと Facebook ページのペアリング

異なるロケーションに対して異なる Facebook ページを設定できます。

ビルディングおよびキャンパスと Facebook ページのペアリング

特定のロケーションを Facebook ページとペアリングするには、次の手順を実行します。

ステップ 1　左側のサイドバー メニューで **[Facebook Wi-Fi]** を選択します。



ステップ 2　[Location Specific Facebook] ページの表で、Facebook ページとペアリングするロケーションをハイライトし、[Settings] ドロップダウン リストから [Default]、[Set] または [Inherit] を選択します。キャンパスで使用できるオプションは **[Default]** と **[Set]** です。ビルディングで使用できるオプションは **[Inherit]** と [Set] です。

- Default：キャンパスは、デフォルトのロケーションを継承します。
- Set：キャンパスとビルディングの両方にペアリングをセットアップすることができます。
- Inherit：ビルディングは、キャンパスのロケーションを継承します。

ステップ 3　**[Set]** をクリックします。

[Facebook Wi-Fi Configuration] ページが表示されます。

ステップ 4　[Select a Page] ドロップダウン リストに、作成されているすべてのページが一覧で表示されます。[Select a Page] ドロップダウン リストから、ロケーションに関連付けるページを選択します。

ステップ 5　[You've Set Up Facebook Wi-Fi] の確認のダイアログボックスで **[Okay]** をクリックします。

ステップ 6　[CMX Connect &Engage Dashboard] に切り替えます。

ゾーンおよびフロアと Facebook ページのペアリング

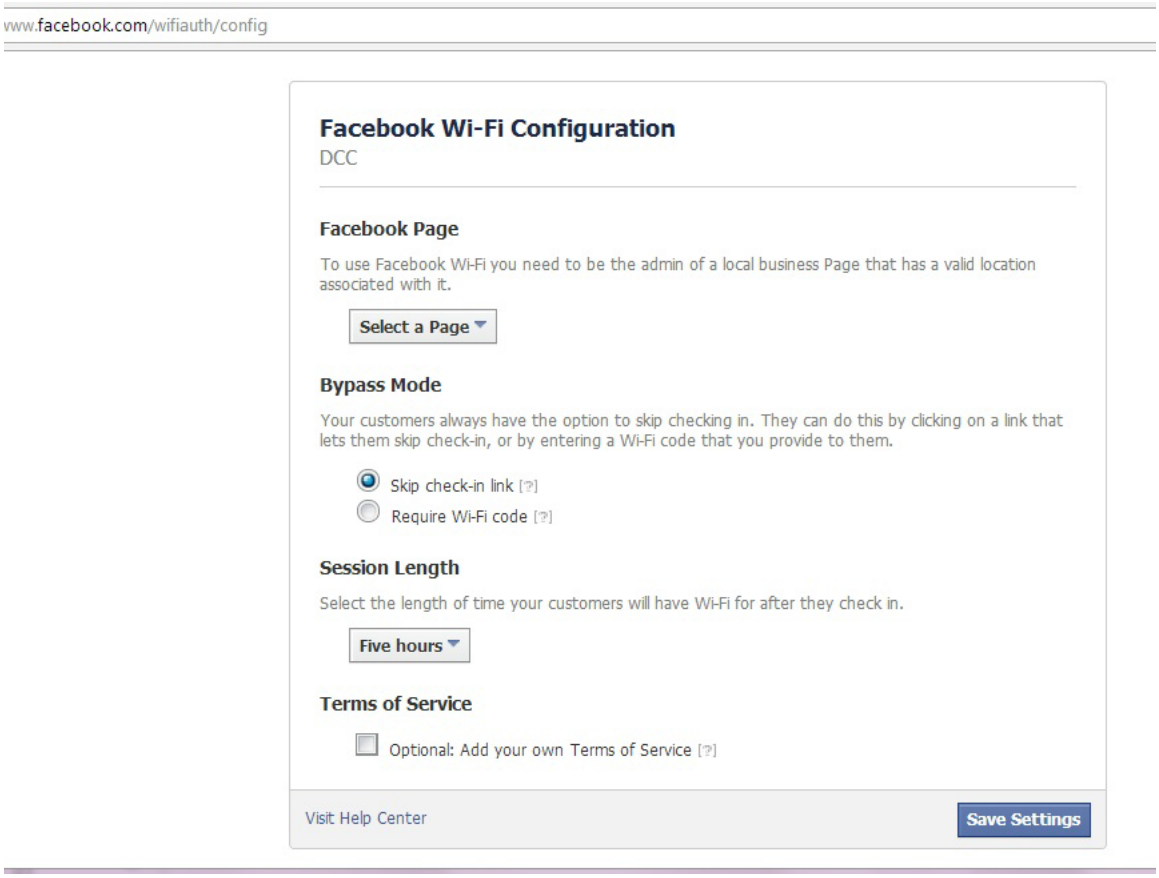
ゾーンまたはフロアを Facebook ページとペアリングするには、次の手順を実行します。

ステップ 1　左側のサイドバー メニューから、**[Maps]** を選択します。

ステップ 2　[Maps] > [System Campus] を選択し、次の手順を実行します。

- 施設と Facebook のページをペアにするには、**[Maps] > [System Campus] > [*Venue*]** を選択して **[Pair with Facebook]** をクリックします。
- フロアと Facebook のページをペアリングするには、**[Maps] > [System Campus] > [*Floor*]** を選択して **[Pair with Facebook]** をクリックします。
- ゾーンと Facebook のページをペアリングするには、**[Maps] > [System Campus] > [*Zone*]** を選択して **[Pair with Facebook]** をクリックします。

[Facebook Wi-Fi Configuration] ページが表示されます。



ステップ 3　「ビルディングおよびキャンパスと Facebook ページのペアリング」（P.4-11）のステップ 3 からステップ 6 までを実行します。

CMX Facebook Wi-Fi レポート

ビジターの詳細情報のモニタリング

ビジターの詳細を監視するには、次の手順を実行します。

ステップ 1　左側のサイドバー メニューから **[Summary]** を選択します。

ステップ 2　ビジターの詳細をモニタするには、右側のペインで **[Facebook Wi-Fi]** タブをクリックします。

- [Visitor Connect] で接続された新しいビジターおよびビジターの合計について、時間単位で傾向を表示するには、**[Hourly]** をクリックして、開始日時と終了日時を選択します。

図 4-3　新しいビジターの時間別傾向

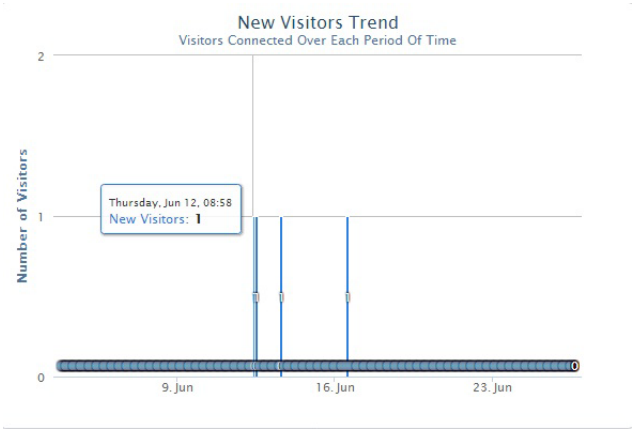


図 4-4　すべてのビジターの時間別傾向

- 新しいビジターおよびすべてのビジターの日単位の傾向を表示するには、**[Daily]** をクリックし、開始日と終了日を選択します。

図 4-5　新しいビジターの日別傾向

図 4-6　すべてのビジターの日別傾向

- 新しいビジターおよびすべてのビジターの週単位の傾向を表示するには、**[Weekly]** をクリックし、開始日と終了日を選択します。

図 4-7　新しいビジターの週別傾向

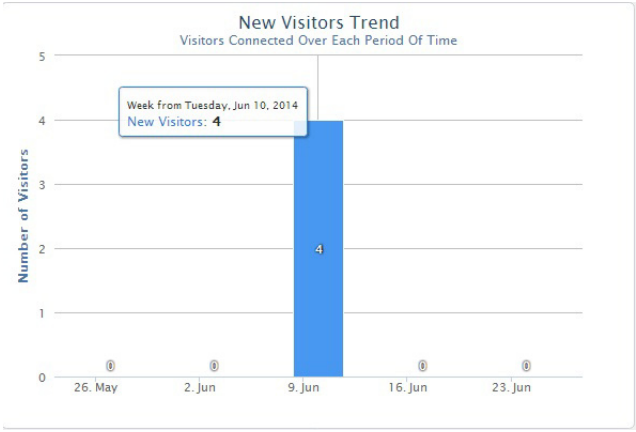
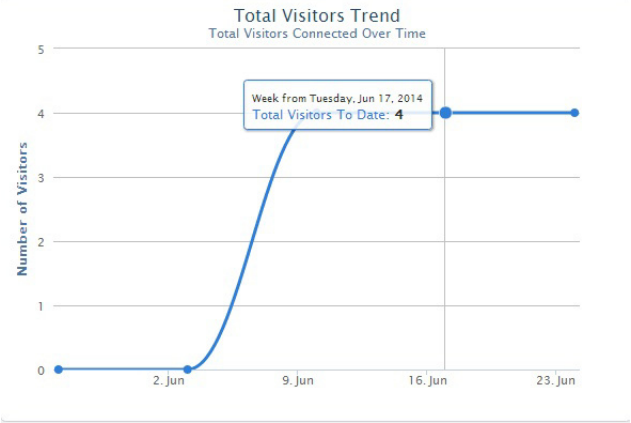


図 4-8　すべてのビジターの週別傾向



- 新しいビジターおよびすべてのビジターの月単位の傾向を表示するには、**[Monthly]** をクリックし、月を選択します。

図 4-9　新しいビジターの月別傾向

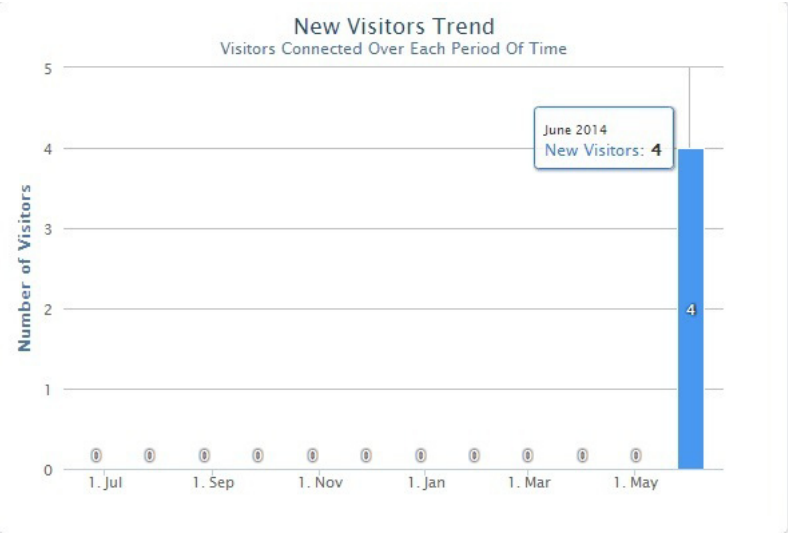
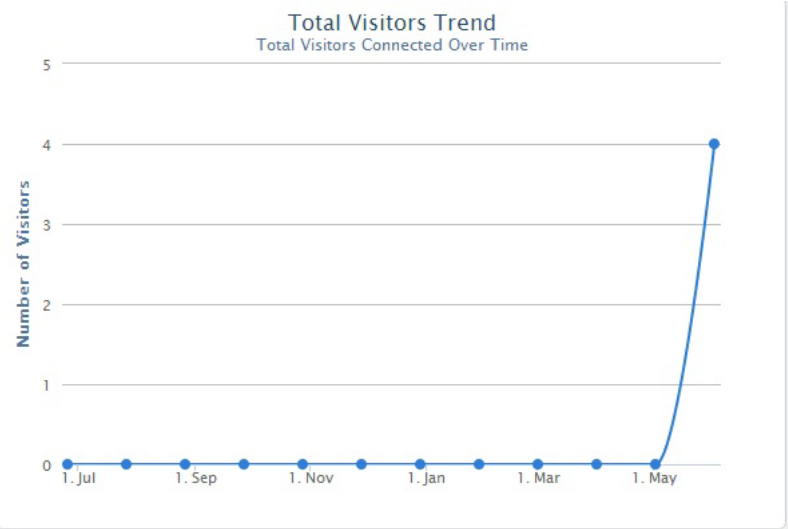


図 4-10　すべてのビジターの月別傾向



ステップ 3　ページの下部の [Active Visitors] テーブルには、ビジターの接続または Facebook Wi-Fi のいずれかのサービスで登録されたビジターの情報が表示されます。表のこの情報は、ソートおよびフィルタリングできます。

ステップ 4　アクティブなビジターのすべての詳細情報をエクスポートするには、**[Export to CSV] > [Export Active Visitors]** をクリックします。ビジターのすべての詳細情報をエクスポートするには、**[Export to CSV] > [Export All Visitors]** をクリックします。

ソーシャル コネクタのセットアップ

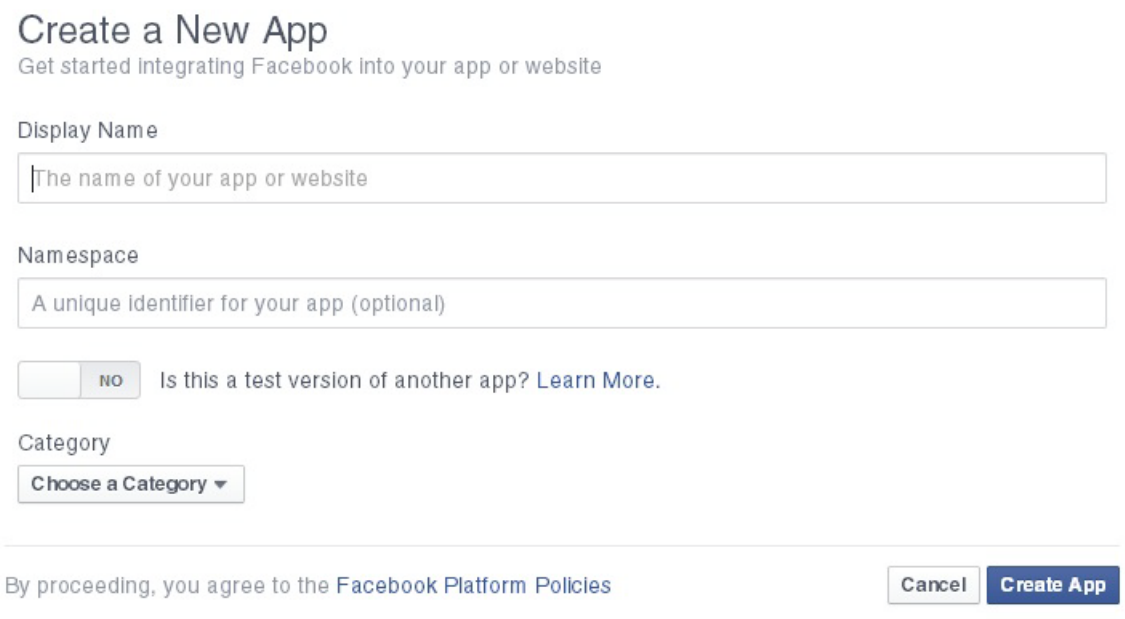
Facebook アプリケーションのセットアップ

Facebook アプリケーションをセットアップするには、次の手順を実行します。

ステップ 1 https://developers.facebook.com にアクセスし、Facebook のユーザ名とパスワードでサインインします。

ステップ 2 **[Apps] > [Create a New Apps]** を選択します。

[Create a New App] ポップアップ ウィンドウが表示されます。



ステップ 3 [Display Name] テキストボックスにアプリケーションの名前を入力します。

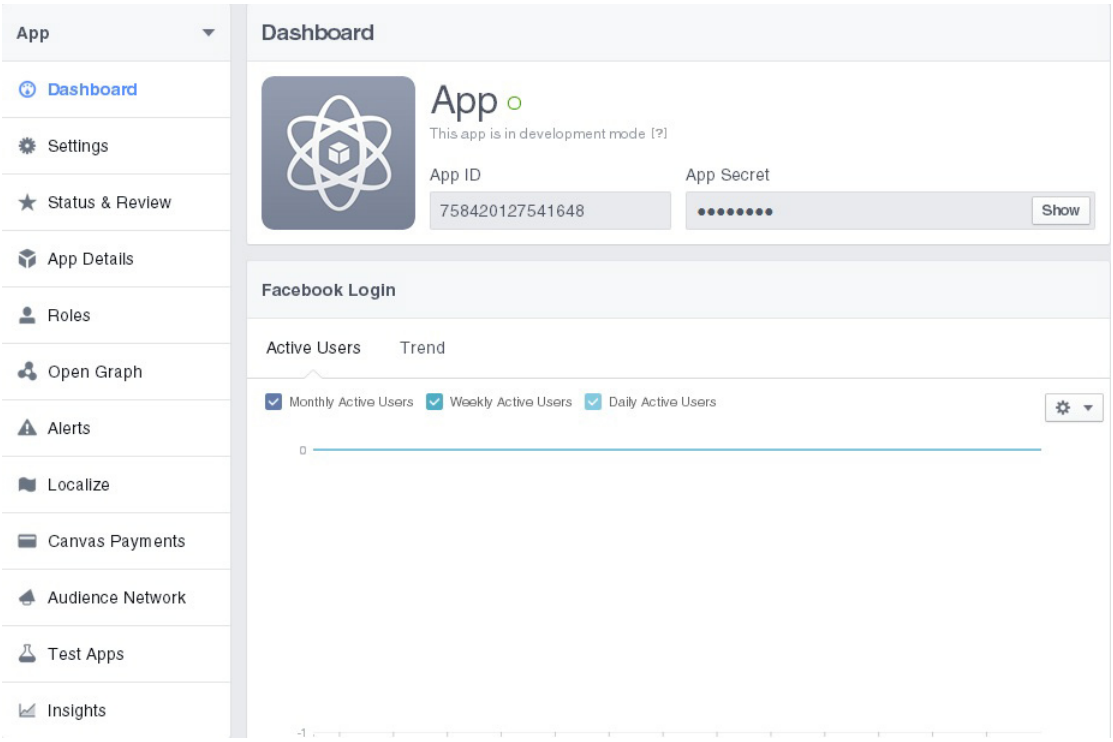
ステップ 4　[Category] ドロップダウン リストからカテゴリを選択します。

ステップ 5　**[Create App]** をクリックします。

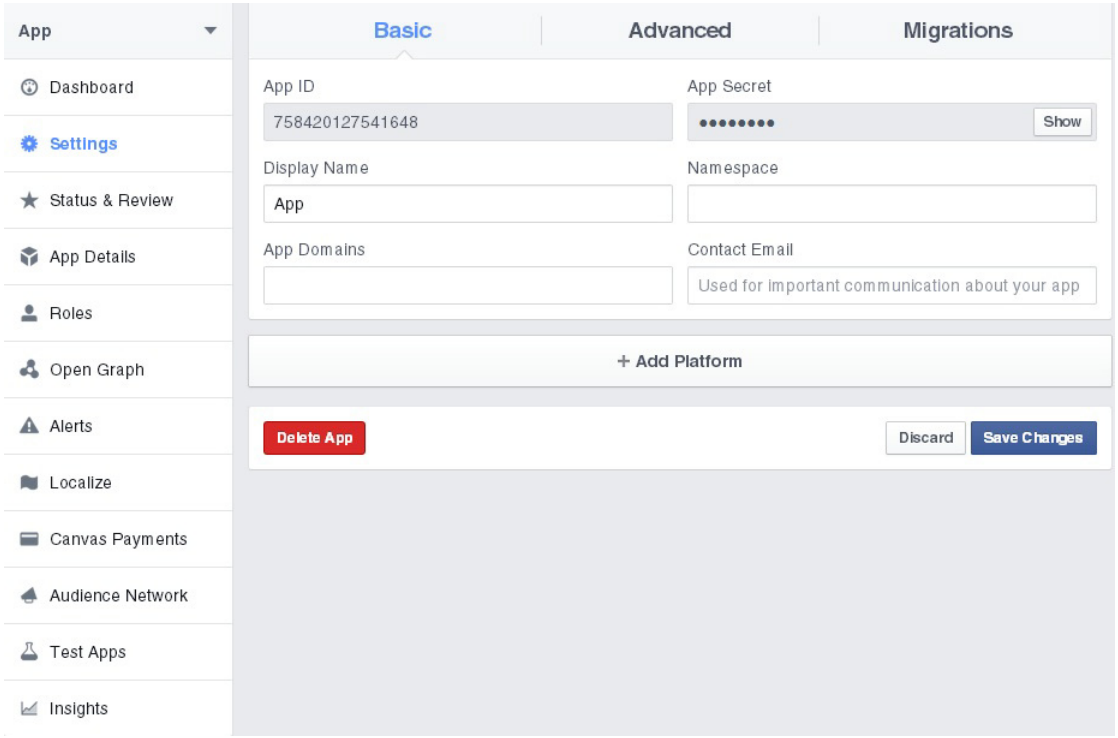
[Security Check] ポップアップ ウィンドウが表示されます。

ステップ 6　セキュリティに関して確認してから、**[Submit]** をクリックします。

[Dashboard] タブに [App ID] と [App Secret] が表示されます。

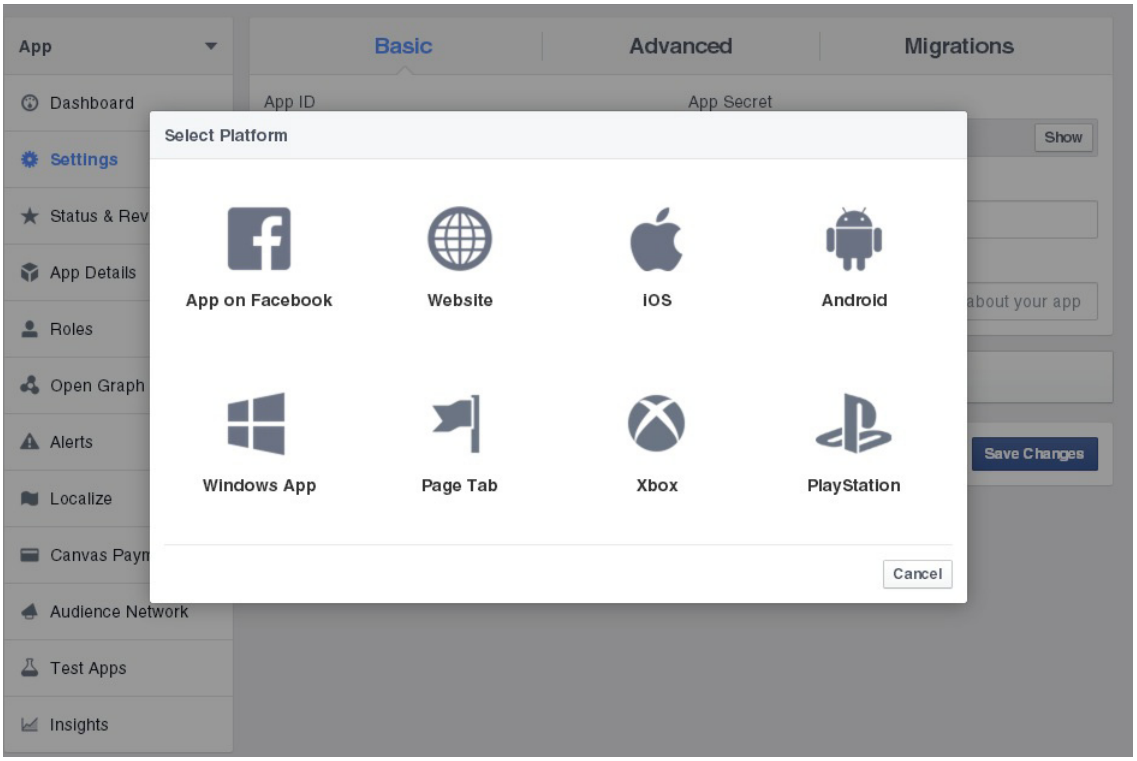


ステップ 7　左側のサイドバー メニューから **[Settings]** を選択します。

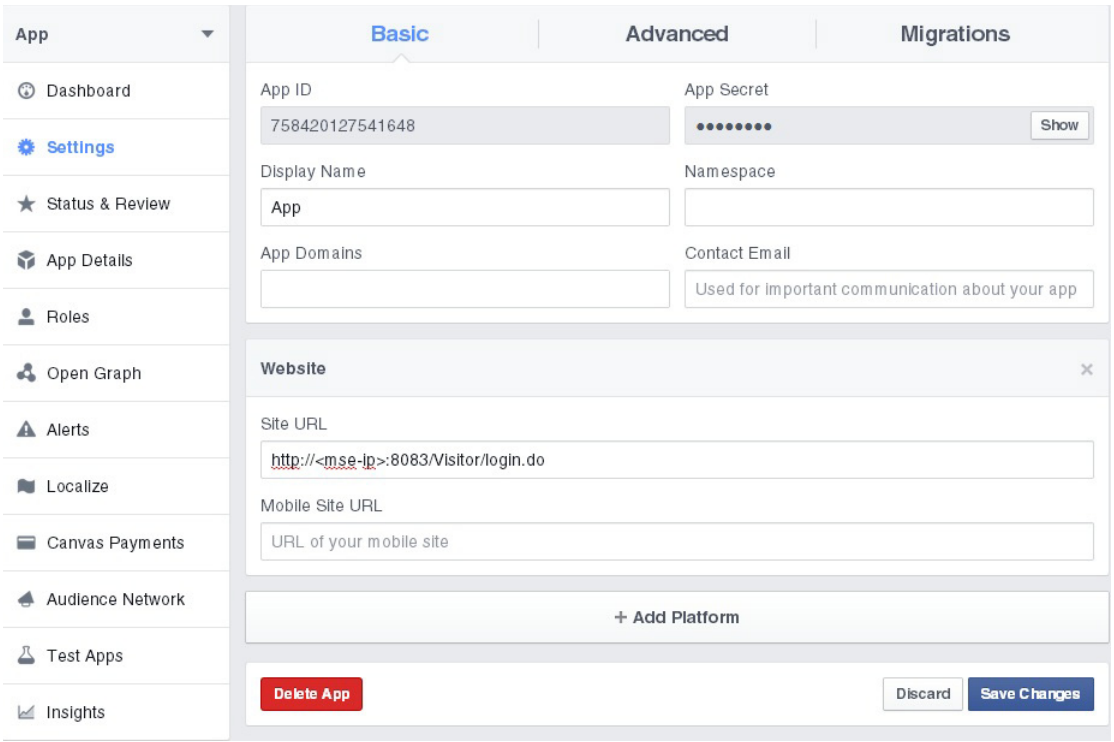


ステップ 8　[Contact Email] テキストボックスの [Email ID] を入力します。このメール ID は、アプリケーションのすべての通信に使用されます。

ステップ 9　右側のペインの **[+Add Platform]** をクリックし、アプリケーションのプラットフォームを選択します。

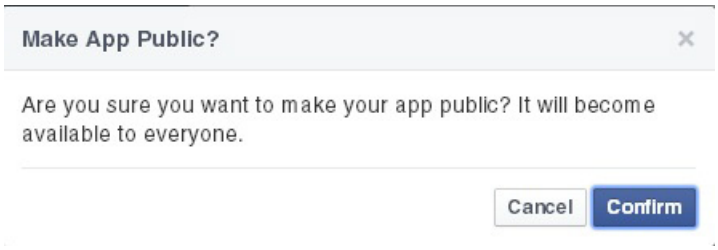


ステップ 10　右側のペインに [Website] グループ ボックスが表示されます。ここでサイトの URL を入力できます。



ステップ 11　左側のサイドバー メニューから **[Status & Review]** を選択します。

ステップ 12　すべてのユーザがアプリケーションを使用できるようにするには、**[YES]** をクリックします。
[Make App Public] ポップアップ ウィンドウで [Confirm] をクリックします。



ステップ 13　**[Start a Submission]** をクリックします。

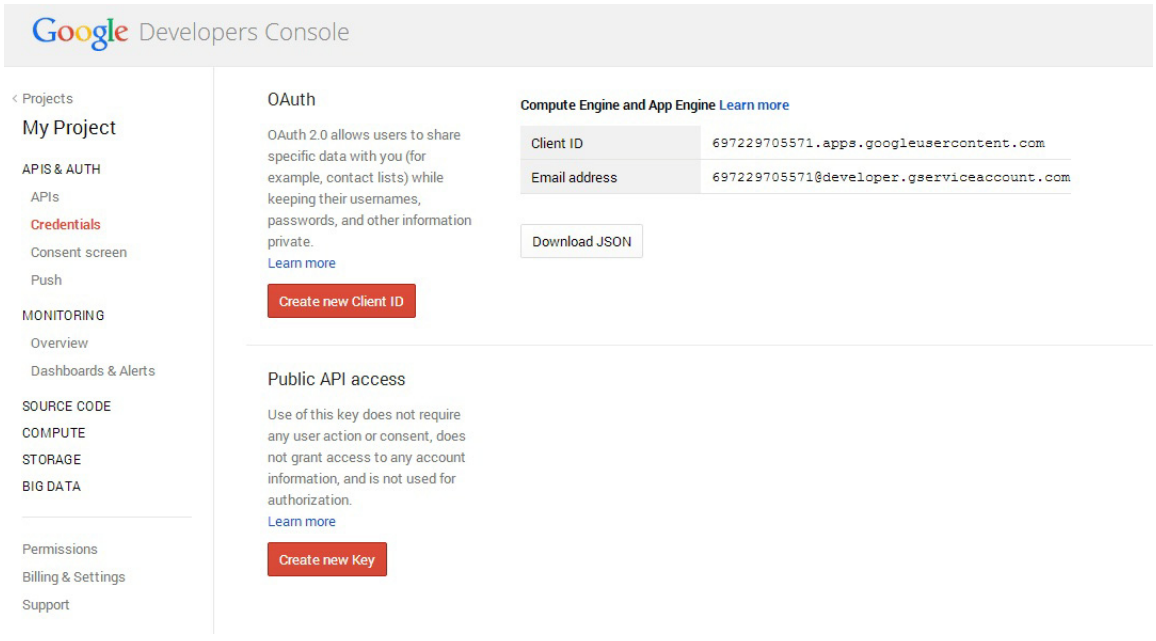
Google アプリケーションのセットアップ

Google アプリケーションをセットアップするには、次の手順を実行します。

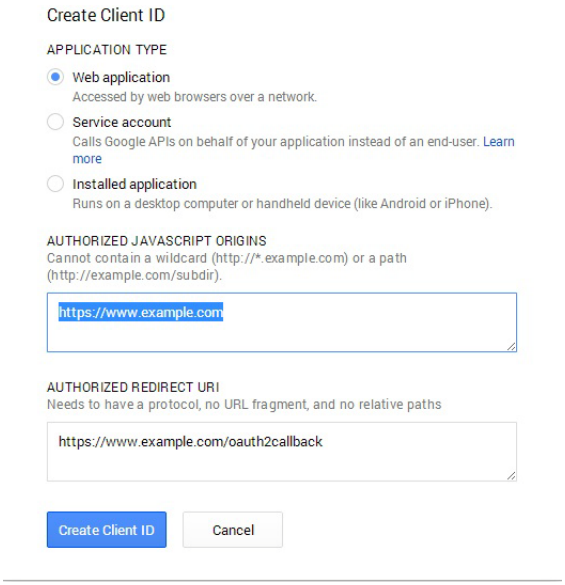
ステップ 1　https://code.google.com/apis/console にアクセスして API Console にアクセスします。

ステップ 2　ユーザ名とパスワードを使用して Google アカウントへログインします。

ステップ 3　[My Project] サイドバー メニューから **[APIS & AUTH] > [APIs] > [Credentials]** を選択します。



ステップ 4　**[Create new Client ID]** をクリックします。
[Create Client ID] ページが表示されます。



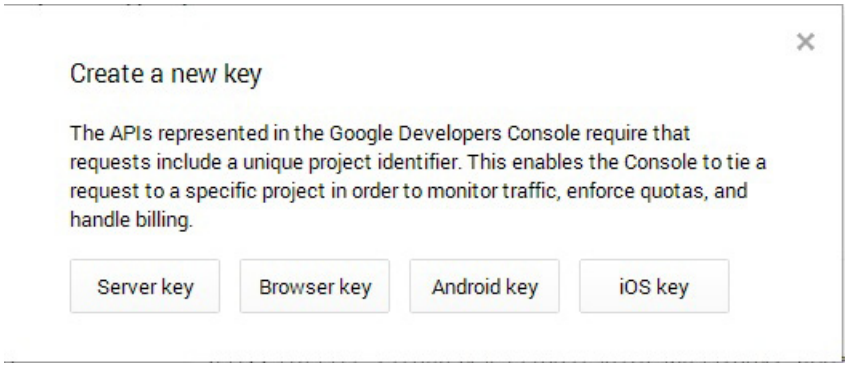
ステップ 5　アプリケーションのタイプとして Web アプリケーションを選択します。

ステップ 6　[AUTHORIZED JAVASCRIPT ORIGINS] テキストボックスに MSE の IP アドレスを入力します。

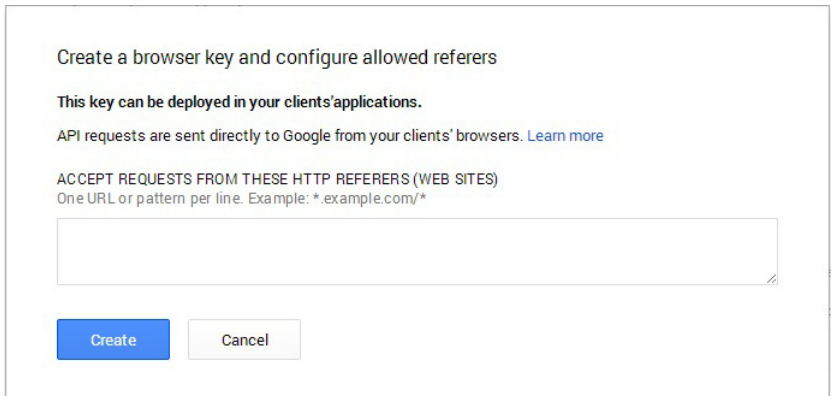
ステップ 7　**[Create Client ID]** をクリックします。

Web アプリケーションのクライアント ID が作成されます。

ステップ 8　**[Create new Key]** をクリックします。



ステップ 9　**[Browse Key]** をクリックします。



ステップ 10　[ACCEPIT REQUESTS FROM THESE HTTP REFERERS (WEB SITES)] テキストボックスに MSE の IP アドレスを入力して [Create] をクリックします。

新しいキーが作成されます。クライアント アプリケーションでの展開にこのキーを使用することができます。

ステップ 11　左側の [My Project] サイドバー メニューから [Consent Screen] をクリックします。

ステップ 12　[PRODUCT NAME] テキストボックスに製品名を入力します。

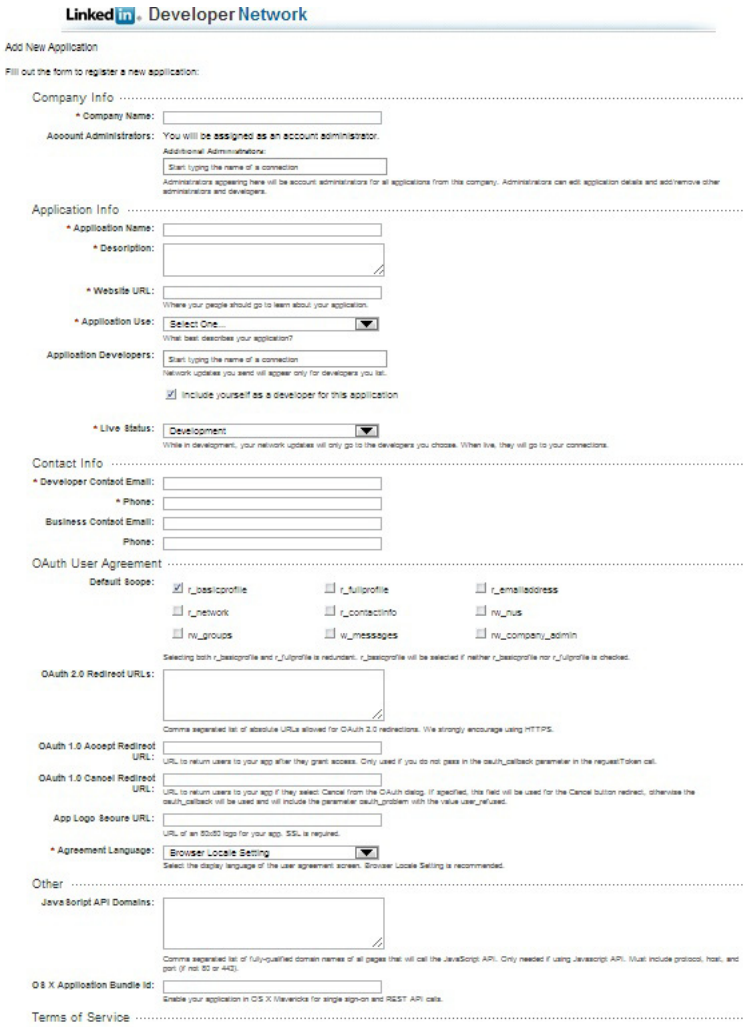
ステップ 13　**[Save]** をクリックします。

Linkedin アプリケーションのセットアップ

Linkedin アプリケーションをセットアップするには、次の手順を実行します。

ステップ 1　https://www.linkedin.com/secure/developer にアクセスして、Linkedin Developer ネットワークを起動します。

ステップ 2　**[Add New Application]** をクリックします。



ステップ 3　新しいアプリケーションを登録するには、application.form の必須フィールドをすべて入力します。

- [Company Info] セクションで以下の内容を指定します。
  - Company Name
  - Account Administrators name
- [Application Info] セクションで以下の内容を指定します。
  - Application Name
  - 説明
  - Website URL：MSE の IP アドレスを入力します。たとえば、`http://<mse-ip>:8083/visitor/social.do` のように入力します。
  - Application Use
  - アプリケーション開発者
  - Live Status
- Contact Info
  - Developer Contact Email and Phone

  - Business Contact Email and Phone
- OAuth User Agreement
  - [OAuth 1.0 Accept Redirect URL] には、`https://localhost:8083/visitor/social.do` と入力します。
  - [OAuth 1.0 Cancel Redirect URL] には、`https://localhost:8083/visitor/social.do` と入力します。
- Other
  - [JavaScriptAPI Domains] テキストボックスに、`http://<mse-ip>:8083` と入力します。

ステップ 4　**[Add Application]** をクリックします。

アプリケーションが登録され、新しく登録されたアプリケーションの API キーおよび秘密キーが表示されます。

デバイス ブラウザのマトリクス

ビジター接続のデバイス ブラウザ マトリクス

次に、ビジター接続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 B-1　　ビジター接続のデバイス ブラウザ マトリクス

モデル番号	Version	ブラウザ	デフォルト ブラウザのバージョン	Remarks
Nexus 7	4.3	Google Chrome	32.0.1700.99	—
Kindle	13.3.2.2	Silk	1.0.454.220	ソーシャル コネクタの問題
iPad（大）	7.0	Safari	7.0	
iPhone	6.1(3)	Safari	6.0	
Macbook Pro	10.8.4	Safari	6.0	
Samsung（Snow OS）	33.0.1750.152	Google Chrome	33.0.1750.152	
iPad（小）	7.0	Safari	7.0	
Windows タブレット	Windows RT 8.1	Internet Explorer[InternetExplorer]	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		

Facebook WiFi 用のデバイスのブラウザ マトリクス

次に、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 B-2　Facebook WiFi 用のデバイスのブラウザ マトリクス

モデル番号	version	ブラウザ	デフォルト ブラウザのバージョン	他のブラウザ	version
Nexus 7	4.3	Google Chrome	32.0.1700.99		
Kindle	13.3.2.2	Silk	1.0.454.220		
iPad（大）	7.0	Safari	7.0		
iPhone	6.1(3)	Safari	6.0		
Macbook Pro	10.8.4	Safari	6.0		
Samsung（snow OS）	33.0.1750.152	Google Chrome	33.0.1750.152		
iPad（小）	7.0	Safari	7.0	Chrome	34.0.1874.114
Windows タブレット	Windows RT 8.1	Internet Explorer[InternetExplorer]	11		
Samsung	4.2.2	デフォルト ブラウザ			

索 引

C

F

G

H

L

M

P

W

あ