CHAPTER 11

CMX ダッシュボードのビジター接続

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。CMX ビジター接続は、ユーザがビジターに対してカスタム オンボーディング エクスペリエンスを作成することが可能なロケーション対応キャプティブ ポータルです。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。

（注） ページの右上隅にある、CMX ダッシュボード内の [Make a wish] メニューをクリックしてフィードバックを提供してください。機能を無効にするには、Super Admin ロールから [Visitor Connect] 操作を除外します。

キャプティブ ポータルとしてのビジター接続

CMX ビジター接続は、直感的でシンプルなゲスト キャプティブ ポータルで、ゲストのオンボーディングが容易になります。ビジター接続はロケーション認識型で、異なるロケーションまたはゾーンで異なるスプラッシュ テンプレートを使用します。

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 UI の CMX ダッシュボード サービスを有効にする必要があります。

スプラッシュ ページでは、ビジター接続は次の内容のカスタマイズをのサポートします。

- 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
- 利用規約
- アドバタイズメント プラグイン
- Facebook、Linkedin および Google+ などのソーシャル認証プラグイン

施設のオーナーは、次の内容を実行できます。

- 複数のスプラッシュ テンプレートを作成し、それを関心のあるポイント（POI）に割り当てることで、より適したビジター エクスペリエンスを提供するためにロケーション固有のスプラッシュ ページとアドバタイズメントをカスタマイズする。たとえば、ビジターが飲食店街にいる場合、施設のオーナーは食品割引券を PR できます。また、ビジターの場所に応じて、スプラッシュ ページを現地の言語にすることができます。

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。

ここでは、次の内容について説明します。

- 「CMX ビジター接続の前提条件」（P.11-2）.

CMX ビジター接続をセットアップするためのワークフロー

次の表に、CMX 分析システムをセット アップする際に従うべき手順を示します。

表 11-1　CMX ビジター接続をセットアップするためのプロセス

プロセス	説明
1. FlexConnect ACL の設定	詳細については、「FlexConnect ACL の設定」（P.11-3）を参照してください。
2. 認証用の WLAN の設定	詳細については、「Web パススルー認証の WLAN の設定」（P.11-4）を参照してください。
3. 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.11-7）を参照してください。
4. 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.11-9）を参照してください。
5. スプラッシュ ページの作成	詳細については、「スプラッシュ テンプレートの作成」（P.11-11）を参照してください。
6. 関心のあるポイントへのスプラッシュ ページ テンプレートの割り当て	詳細については、「関心のあるポイントまたはフロアへのスプラッシュ ページ テンプレートの割り当て」（P.11-12）を参照してください。

CMX ビジター接続の前提条件

- 「FlexConnect ACL の設定」（P.11-3）
- 「Web パススルー認証の WLAN の設定」（P.11-4）
- 「ソーシャル アプリケーションの設定」（P.11-7）

- 「CMX ビジター接続の設定」（P.11-8）

FlexConnect ACL の設定

Flex モードの展開用にのみ FlexConnect ACL を設定します。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

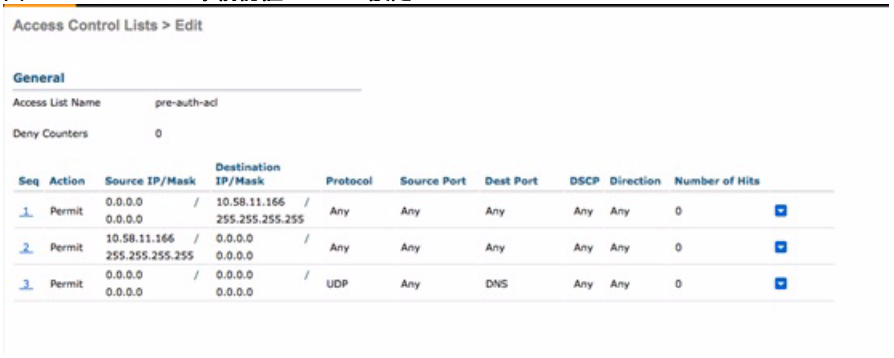
顧客へのネットワーク アクセスを提供するために、Cisco ワイヤレス LAN コントローラ（WLC）上に WLAN を設定する必要があります。これに対して、CMX ビジター接続用 WLAN のレイヤ 3 セキュリティに Web パススルーを設定する必要があります。

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。ACL の設定の詳細については、『Cisco Wireless LAN Configuration Guide』を参照してください。

http://www.cisco.com/en/US/products/ps12722/products_installation_and_configuration_guides_list.html

図 11-1　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。

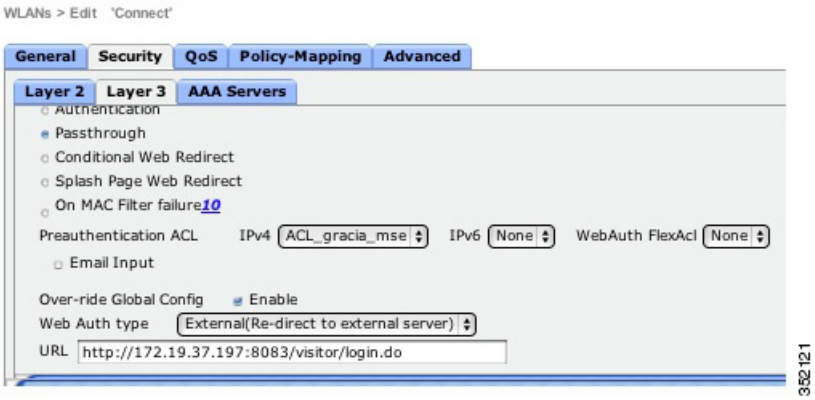
ステップ 5　[Layer 2 Security] ドロップダウン リストから、[None] を選択します。

ステップ 6　[Apply] をクリックします。

図 11-2　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 11-3　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.11-3）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

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には、IOS デバイスに対して 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 disable`

ソーシャル アプリケーションの設定

（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。

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>

ソーシャル アプリケーションの作成方法の詳細については、次のリソースを参照してください。

- Facebook アプリケーション ID と秘密キーについては、次の URL を参照してください。
  http://www.youtube.com/watch?v=orx7bhEBUP4

（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。

- LinkedIn API キーと秘密キーについては、次の URL を参照してください。
  http://www.youtube.com/watch?v=_J2ejcxg6NQ
- Google+ クライアント ID と秘密キーについては、次の URL を参照してください。
  http://www.youtube.com/watch?v=o425vQXpigw

（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 11-4 を参照）。

図 11-4　Google+ 向けのソーシャル アプリケーションの設定

CMX ビジター接続の設定

（注）　スーパー管理者のみが CMX ビジター接続にアクセスできます。

ビジター接続を設定するには、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、[Settings] > [Roles] の順に選択します。

ステップ 2　[Super Admin] をクリックします。

[Select Operations] グループ ボックスが表示されます。

ステップ 3　[Existing Operations] フィールドでビジター接続が使用できることを確認します。このフィールドが使用可能でない場合、[Visitor Connect] をクリックして、[Available Operations] フィールドから強調表示して、[>>]（追加）を選択します。

ステップ 4　[OK] をクリックします。

テンプレート フィールド

[Template Fields] を使用して、さまざまなユーザ入力フィールドのほか、電子メール ID、名前、電話番号などのテンプレートのフィールドを作成できます。

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

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　左側のサイドバーのメニューから、[Visitor Connect] > [Splash Templates] の順に選択します。

ステップ 2　[Create New Splash Template Field] をクリックします。

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。

スプラッシュ 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。

スプラッシュ 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　[OK] をクリックして [Delete Confirmation] グループ ボックスの削除を確定するか、キャンセルして変更を加えずにページを閉じます。

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 アプリケーションの設定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.11-10）
- 「ソーシャル コネクタの編集」（P.11-10）
- 「ソーシャル コネクタの削除」（P.11-10）

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 New Social Connector] 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　[Account] ドロップダウン リストから、アカウントを選択します。

ステップ 5　[Facebook APP ID] テキスト ボックスで Facebook アプリケーションを作成した後で、受信した Facebook APP ID を入力します。

ステップ 6　[Linkedin API Key] テキスト ボックスで受信した LinkedIn API ID を入力します。

ステップ 7　[Google API Client ID] テキスト ボックスに Google クライアント ID を入力します。

ステップ 8　[Google API Key] テキスト ボックスに Google API キーを入力します。

ステップ 9　[Submit] をクリックします。

ソーシャル コネクタの編集

ソーシャル コネクタを編集するには、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、キャンセル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.11-11）
- 「関心のあるポイントまたはフロアへのスプラッシュ ページ テンプレートの割り当て」（P.11-12）

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

ステップ 2　[Create New Splash Template] 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　[Template Background] ドロップダウン リストから、スプラッシュ ページの事前定義された背景を選択します。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。これらは、[Splash Template Fields] メニューを使用して作成したフィールドです。

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 and Conditions] テキスト ボックスに、スプラッシュ ページを表示する利用条件を入力します。

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。たとえば、「これは補足的な Wi-Fi ネットワークで、データは保存されません」と入力できます。

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。

次の内容は、YouTube の URL を指すアドバタイズメント設定の例です。<iframe width="853" height="480" sword//www.youtube.com/embed/uIDx3eUZ-vw" 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。これは、[Visitor Connect] > [Social Connectors] で作成したコネクタのリストです。

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。

関心のあるポイントまたはフロアへのスプラッシュ ページ テンプレートの割り当て

特定のスプラッシュ ページ テンプレートを関心のあるポイントまたはフロア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。

フロアにスプラッシュ ページ テンプレートを割り当てるには、次の手順を実行します。

ステップ 1　左側のサイドバーのメニューから [Points of Interest] を選択します。

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

（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　[Edit Floor] をクリックします。

ステップ 4　[Splash Template] ドロップダウン リストから、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 5　[Submit] をクリックします。

ビジター接続のレポート

ビジターの詳細の監視

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　左側のサイドバーのメニューから [Reports] を選択します。

[Services]、[Message]、および [Domain Metrics]、[Visitor Connect] タブが表示されます。

ステップ 2　ビジターの詳細を監視するには、[Visitor Connect] をクリックします。

- ビジター接続で接続された新しいビジターおよびすべてのビジターの時間単位の傾向を表示するには、[Hourly] をクリックし、開始日時と終了日時を選択します。

図 11-5　新しいビジターの時間別傾向

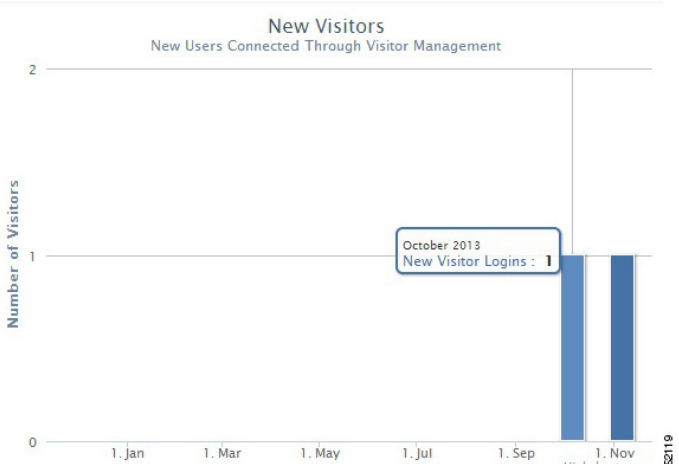
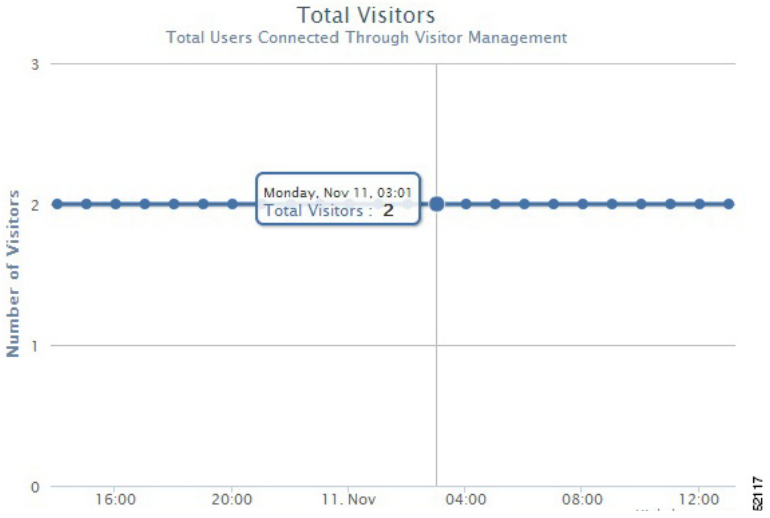


図 11-6　すべてのビジターの時間別傾向



- 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 11-7　新しいビジターの日別傾向

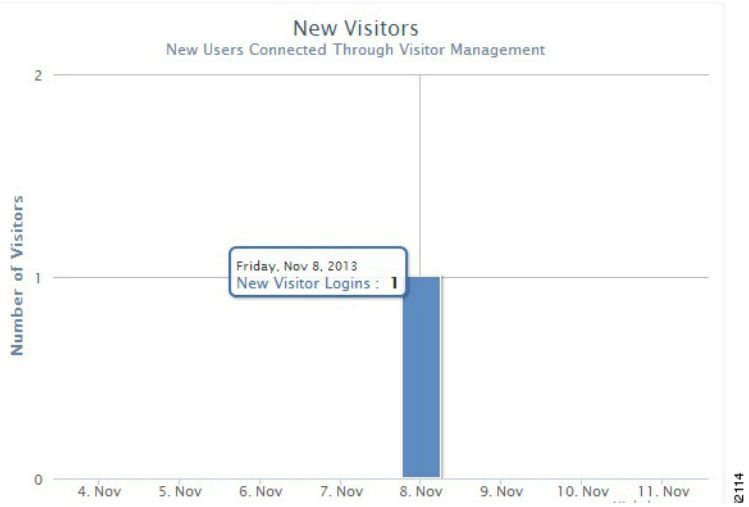
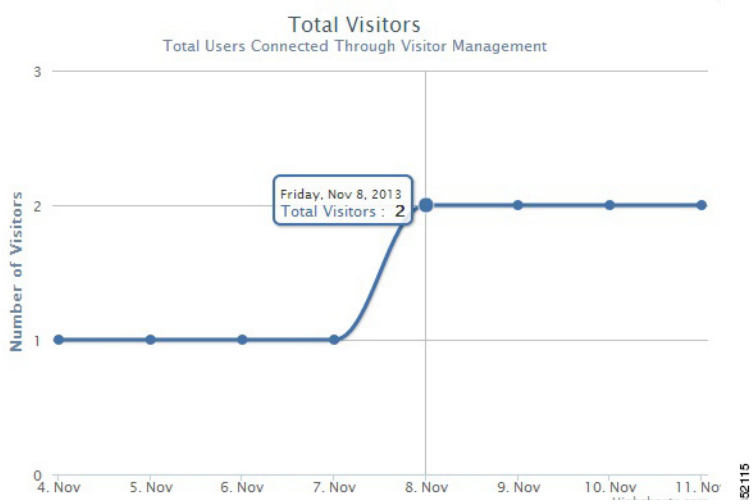


図 11-8　すべてのビジターの日別傾向



- 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 11-9　新しいビジターの週別傾向

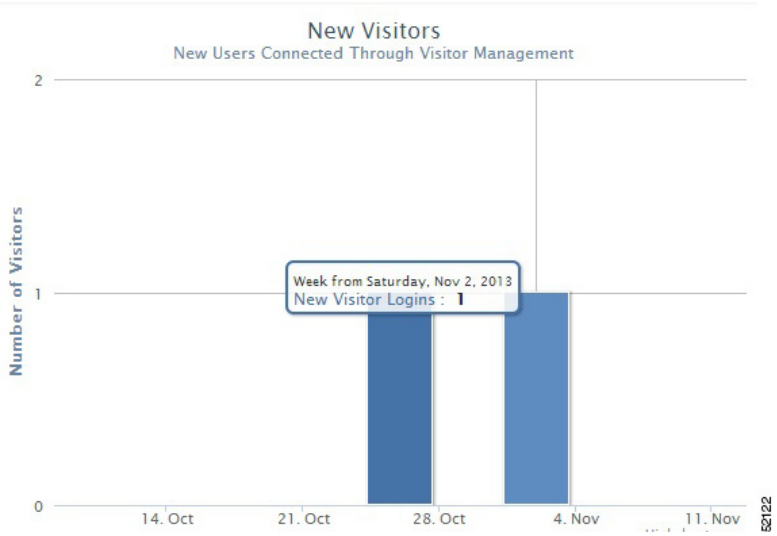


図 11-10　すべてのビジターの週別傾向

- 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 11-11　新しいビジターの月別傾向

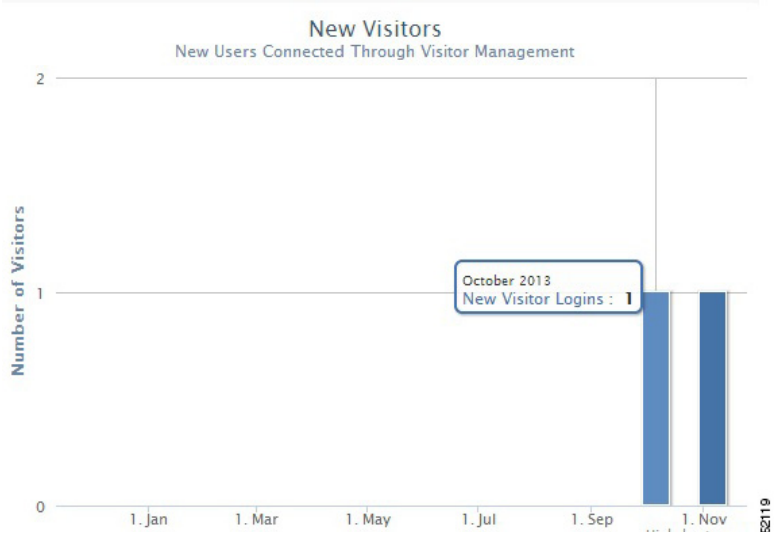
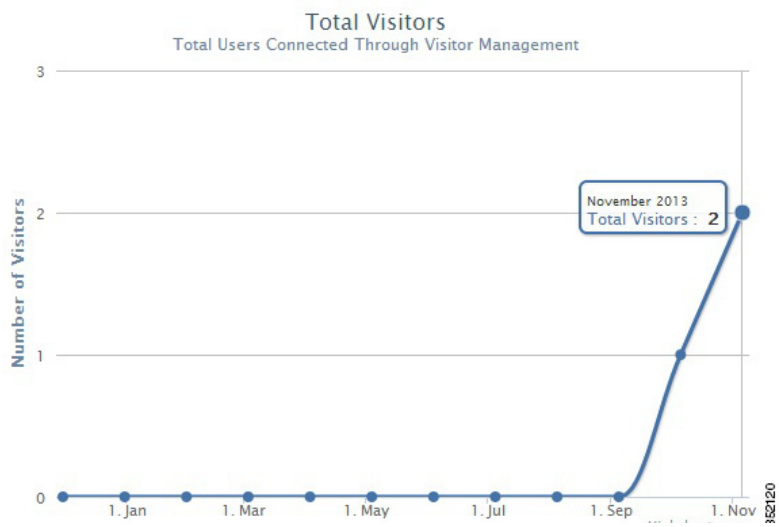


図 11-12　すべてのビジターの月別傾向



ステップ 3　ページの下部にある表は、スプラッシュ テンプレート設定に基づいたアクティブ ビジターに関する登録情報を示します。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　[Export to CSV] をクリックして、ビジターの詳細をエクスポートします。