Cisco Connected Mobile Experiences コンフィギュレーション ガイド、リリース 10.2

初版：2015 年 09 月 23 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

【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。

目 次

第 1 章

はじめに

対象読者

このマニュアルは、Cisco Connected Mobile Experiences（Cisco CMX）サービスを設定するネットワーク管理者を対象としています。

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 *1*：表記法

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 }	どれか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。

表記法	説明
[x | y | z]	どれか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。

ヒント 「問題解決に役立つ情報」です。

注意 「要注意」の意味です。 機器の損傷またはデータ損失を予防するための注意事項が記述されています。

関連資料

Cisco モビリティ サービス エンジンおよび関連製品の詳細については、次の URL を参照してください。

http://www.cisco.com/c/en/us/support/wireless/mobility-services-engine/tsd-products-support-series-h

Cisco Connected Mobile Experiences（Cisco CMX）の詳細については、次の URL を参照してください。

http://www.cisco.com/c/en/us/solutions/enterprise-networks/connected-mobile-experiences/index.html

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、Cisco Bug Search Tool（BST）の使用、サービス要求の送信、追加情報の収集の詳細については、『*What's New in Cisco Product Documentation*』を参照してください。このドキュメントは、http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html から入手できます。

『*What's New in Cisco Product Documentation*』では、シスコの新規および改訂版の技術マニュアルの一覧を、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。

第 2 章

使用する前に

Cisco Connected Mobile Experiences の概要

Cisco モビリティ サービス エンジン（Cisco MSE）は、Cisco Connected Mobile Experiences（Cisco CMX）を導入、実行するためのプラットフォームとして機能します。 Cisco MSE は、物理アプライアンス（ボックス）または仮想アプライアンス（VMware vSphere Client を使用して導入）という 2 種類のモードで提供されます。 Cisco CMX を使用すれば、Cisco ワイヤレス ネットワークと Cisco MSE のロケーション インテリジェンスにより、エンドユーザ向けにパーソナライズしたモバイル 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による業務の効率化を実現することができます。

Cisco CMX の機能の詳細については、次の URL にある『*Release Notes for Cisco CMX, Release 10.2*』を参照してください。

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

Cisco CMX サービスの概要

Cisco CMX では次のサービスにアクセスできます。

- DETECT & LOCATE：Detect & Locate サービスは、Cisco WLC から提供されるデータを使用して、ワイヤレス LAN（WLAN）対応アクセス ポイントにより検出されるワイヤレス デバイスのX,Y位置を（マップの左上を0,0として）高い精度で算出します（一般に、標準ロケーション テクノロジーの場合は +/-5M、90□、ハイパーロケーション テクノロジーの場合は +/-1M、50□）。ただし、ロケーション対応環境に関するシスコのベストプラクティスに従ってアクセス ポイントが展開されている必要があります。 CMX GUI では、以下の物理的な位置を表示できます。
  - 関連付けられているワイヤレス デバイス（デフォルト ビューでは緑色のドットとして表示）
  - 関連付けられていないワイヤレス デバイス（デフォルト ビューでは赤色のドットとして表示）
  - RF 干渉源（照明アイコン）
  - アクセス ポイント（円形）
  - BLE ビーコン（BLE アイコン）
  - アクティブな WiFi RFID タグ（タグ アイコン）

  バックグラウンド マップには次の情報を表示できます。
  - Cisco Prime Infrastructure からインポートされた包含ゾーンと除外ゾーン
  - Cisco CMX で作成された Analytics ゾーン

  また、このロケーション情報が CMX Analytics サービスに渡される場合、このロケーション情報から、敷地内における当日の顧客の移動と行動を把握できます。 Cisco CMX Analytics サービスはデバイス パラメータを判別し、この情報を 6 種類の独自のウィジェットに表示できます。

  インストール時に [Location] を選択した場合、Cisco CMS GUI では次のサービスが表示されます。
  - DETECT & LOCATE：トライアル期間として 120 日間使用できます（CMX 基本/拡張ライセンスを追加しない場合）。
  - ANALYTICS：トライアル期間として120日間使用できます（CMX拡張ライセンスを追加しない場合）。
  - CONNECT & ENGAGE：CMX 基本/拡張ライセンスのいずれかが追加されるまで、トライアル期間として 120 日間使用できます。
  - MANAGE
  - SYSTEM

詳細については、Connect and Engage サービスの概要, （43 ページ）を参照してください。

- ANALYTICS：このサービスは、Wi-Fiデバイスの位置を分析するためのパッケージ化されたデータ分析ツールを提供します。データ可視化エンジンとして機能し、組織がネットワークをビジネス分析のデータ ソースとして使用して、行動パターンとトレンドを理解できるようにします。これにより、組織は来訪者のエクスペリエンスを向上させ、カスタマー サービスを改善する方法を決定できます。

  ANALYTICS サービスでは、6 種類のウィジェットを作成できます。

  - デバイス数（Device Count）
  - 滞在時間（Dwell time）
  - 滞在時間の内訳（Dwell time breakdown）
  - 関連付けられているユーザのレポート（Associated User Report）
  - Path（パス）
  - Correlation（相関）

  詳細については、Cisco CMX Analytics サービス, （23 ページ）を参照してください。

- **CONNECT&ENGAGE**：このサービスは、直感的でシンプルであり、詳細なカスタマイズが可能なロケーション認識型ゲスト サービスを、2 種類のゲスト オンボード エクスペリエンスを提供するキャプティブ ポータルの形式で提供します。

  - Facebook Wi-Fi
  - カスタム ポータル

  詳細については、Connect and Engage サービス, （43 ページ）を参照してください。

- **PRESENCEANALYTICS**：Cisco Presence Analytics サービスは、単一のネットワーク アクセス ポイントであっても、アクセス ポイントとモバイル デバイスとのインタラクションからビジターの存在を検出する新しい分析エンジンです。 ワイヤレス デバイスから送信されるプローブ要求の情報を使用すると、クライアントのプローブ アクティビティを検知するアクセス ポイントが 1 つのみであっても、そのアクセス ポイントのロケーションに基づいて、クライアントの全般的なロケーションを特定できます。 AP が単一であっても、その AP から提供される情報により、Presence Analytics サービスは貴重なビジネス インテリジェンスを作成できます。 Presence Analytics は、受信信号強度表示（RSSI）と、高信号強度の期間から、クライアント デバイスがサイト内にとどまっているか、または単に通過しているだけであるかを判断します。 デバイスがアクセス ポイントに接続していない場合でも、デバイスが信号範囲内にあり、ワイヤレス機能がオンになっていれば、そのデバイスの存在が検出されます。 Presence Analytics が、一連の AP に関するロケーション情報を作成する場合、CMX インスタンスへのマップのインポートも設定も不要であるという点で、管理をシンプルにできます。 Presence Analytics では、特定の AP または一連の AP と物理ロケーションの関連付けを認識することで、特定のロケーションのビジター数（新規ビジターまたはアクセスを繰り返すビジターを問わず）と、各ビジターが AP に物理的に近接した位置で過ごした時間をビジネス上の観点から把握し、デバイスがロケーションを単に通過しただけであるか、または AP による処理対象ロケーション内に実際にとどまっていたどうかを確認することができ

ます。 詳細については、Presence Analytics サービスの概要, （68 ページ）を参照してください。
インストール時に [Presence] を選択した場合、Cisco CMS GUI では次のサービスが表示されます。

- PRESENCE ANALYTICS
- CONNECT & ENGAGE
- MANAGE
- SYSTEM

- **MANAGE**：このサービスでは、ライセンス、ユーザ、ゾーン、ビーコン、および通知を管理できます。 詳細については、Cisco CMX のコンフィギュレーションの管理, （83 ページ）を参照してください。
- **SYSTEM**：このサービスでは、システムの正常性を検証し、パターンとメトリックを確認できます。 詳細については、Cisco CMX のシステム設定の管理, （105 ページ）を参照してください。

Cisco CMX 10.2 でサポートされているすべての新機能のリストについては、次の URL にある『*Release Notes for Cisco CMX 10.2*』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

Cisco CMX 10.2 を設定するための前提条件

Cisco CMX 10.2 を設定するには次のコンポーネントが必要です。

- Cisco Prime Infrastructure 1.3、1.4、または 2.x から（ファイルの形式で）エクスポートされたマップ

（注） Cisco Prime Infrastructure からマップをインポートするのは、Cisco CMX Location サービスを使用する場合だけです。 Presence Analytics サービスを使用する場合は、マップをインポートする必要はありません。これは、Presence Analytics サービスではマップは必要ではなく、Presence Analytics ダッシュボードですべての設定を完了できるためです。

- シスコ ワイヤレス コントローラ（Cisco WLC）7.x または 8.x
- Cisco CMX 10.2 ライセンス（Cisco CMX 10.2 には、すべての機能を利用できる 120 日間の評価ライセンスが付属しています。このライセンスは、Cisco CMX をインストール後、初めて開始するときに有効化されます。 無期限ライセンスの追加については、ライセンスの追加, （84 ページ）を参照してください。）

マップのインポートとシスコ ワイヤレス コントローラ

Cisco CMX は、システムに追加されたシスコ ワイヤレス コントローラ（Cisco WLC）から受信する Network Mobility Services Protocol（NMSP）データを利用します。 ここでは、従うべき手順について説明します。

Cisco Prime Infrastructure マップのエクスポート

Cisco CMX のマップを取得するには、Cisco Prime Infrastructure からマップをエクスポートする必要があります。

手順

ステップ 1 Cisco Prime Infrastructure にログインします。

ステップ 2 [Maps] メニューから [Site Maps] を選択します。

ステップ 3 [Export Maps] を選択して、[Go] をクリックします。

ステップ 4 エクスポートするマップを選択し、[Export] をクリックします。
選択したマップが ImportExport_*xxxx* .tar.gz という名前の圧縮 tar ファイル（例：ImportExport_4575dcc9014d3d88.tar.gz）としてブラウザのダウンロードディレクトリにダウンロードされます。

エクスポートしたマップのコピー

Cisco CMX がアクセスできるサーバのディレクトリに、エクスポートしたマップをコピーするには、Secure Copy Protocol（SCP）を使用します。

マップのインポート

GUI または CLI を使用して、Cisco Prime Infrastructure から Cisco CMX にマップをインポートできます。

インポートされたマップは、Cisco CMX で既存のマップの後に追加されます。 上書きオプションが [Yes] に設定されている場合、Cisco CMX は同名であるが、インポートマップファイルの AesUID が異なるキャンパスが Cisco CMX に存在していることを検出すると、このキャンパスでマップ同期操作を実行します。

CLI を使用してマップをインポートするには、次のいずれかの作業を行います。

- **cmxctlconfigimportmap** または **cmxctl config import** コマンドを使用して、Cisco Prime Infrastructure からすべてのマップを直接インポートする。

- **cmxctlconfigmapsimport--typeFILE--path**<*.tar.gz* ファイルのパス> コマンドを使用して、エクスポートしたマップを Cisco CMX にインポートする。

  Cisco CMX コマンドの詳細については、次の URL にある『*Cisco Connected Mobile Experiences (CMX) Command Reference Guide, Release 10.2*』を参照してください。

  http://www.cisco.com/c/en/us/td/docs/wireless/mse/10-2/cmx_command/guide/cmxcli10.html

GUI を使用してマップをインポートするには、次の作業を行います。

1. Cisco Connected Mobile Experiences（Cisco CMX）にログインします。
2. [SYSTEM Dashboard] をクリックします。
3. ウィンドウの右上隅にある [Gear] アイコンをクリックします。
4. [Controllers and Maps Setup] > [Import] をクリックします。

（注） Cisco CMX 10.2 には [Override Maps] オプションがあります（[SYSTEM] > [Settings]）。デフォルトで、このオプションは有効になっています。このオプションを有効にすると、Cisco CMX マップが、インポートするファイルで定義されているマップに置き換えられます。

CLI からの Cisco WLC の追加

Cisco CMX CLI から Cisco WLC を追加するには、次のいずれかのコマンドを実行します。

- **cmxctlconfigcontrollersadd**
- **cmxctlconfigcontrollersimport[PI/FILE]**

Cisco CMX コマンドの詳細については、次の URL にある『*Cisco Connected Mobile Experiences (CMX) Command Reference Guide, Release 10.2*』を参照してください。

http://www.cisco.com/c/en/us/td/docs/wireless/mse/10-2/cmx_command/guide/cmxcli10.html

Cisco CMX ユーザ インターフェイスへのログイン

手順

ステップ 1 Google Chrome 40 以降を使用して、Cisco CMX ユーザ インターフェイスを起動します。

ステップ 2 ブラウザのアドレス行に、https://*ipaddress* と入力します。ここで、*ipaddress* は、Cisco CMX をインストールしたサーバの IP アドレスです。
Cisco CMX ユーザ インターフェイスに [Login] ウィンドウが表示されます。

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は admin、デフォルトのパスワードは admin です。）

ライセンスの追加と管理

Cisco CMX 10.2 には、すべての機能を利用できる 120 日間の評価ライセンスが付属しています。このライセンスは、Cisco CMX をインストール後、初めて開始するときに有効化されます。

無期限ライセンスの追加については、ライセンスの追加と管理, （11 ページ）を参照してください。

ライセンス取得の詳細については、『Cisco Connected Mobile Experiences (CMX) Version 10 Ordering and Licensing Guide』を参照してください。

Cisco CMX サービスの有効化または無効化

- CLI を使用して Cisco CMX サービスを有効にするには、次のコマンドを実行します。

  cmxctl enable {consul | qlesspyworker | cassandra | iodocs | cache_6382 | cache_6380 | cache_6381 | cache_6383 | cache_6385 | influxdb | metrics | confd | cache_6379 | cache_6378 | haproxy | database | analytics | connect | location | configuration | matlabengine | hyperlocation | nmsplb | agent}

- CLI を使用して Cisco CMX サービスを無効にするには、次のコマンドを実行します。

  cmxctl disable {consul | qlesspyworker | cassandra | iodocs | cache_6382 | cache_6380 | cache_6381 | cache_6383 | cache_6385 | influxdb | metrics | confd | cache_6379 | cache_6378 | haproxy | database | analytics | connect | location | configuration | matlabengine | hyperlocation | nmsplb | agent}

これらのコマンドの詳細については、次の URL にある『*Cisco Connected Mobile Experiences (CMX) Command Reference Guide, Release 10.2*』を参照してください。

http://www.cisco.com/c/en/us/td/docs/wireless/mse/10-2/cmx_command/guide/cmxcli10.html

ユーザの追加とロールの管理

Cisco CMX で **MANAGE** サービスを使用して、ユーザを新規に作成し、ユーザが実行する必要がある作業に基づいてロールをユーザに割り当てることができます。つまり、ロールベース アクセス コントロールを有効にできます。

以下にユーザのタイプを示します。

- 管理ユーザ：管理ユーザは、Cisco CMX のすべてのサービスと機能（ライセンス タイプに基づく）にアクセスできます。
- その他：管理ユーザはその他のユーザを作成し、作成したユーザにロールを割り当てることができます。

以下に、ユーザに割り当てることができるロールを示します。

- System
- Manage
- Analytics
- Read Only
- Location
- Admin
- ConnectExperience
- Connect

ユーザの作成およびロールの割り当ての詳細については、ユーザの管理, （85 ページ）を参照してください。

Cisco CMX Setup Assistant の使用

Cisco CMX Setup Assistant ポップアップにより、システムを初めて使用する前の基本的な設定手順を実行できます。 Cisco CMX にログインすると、Cisco CMX Setup Assistant が自動的に表示されます。 Cisco CMX Setup Assistant を再起動するには、ヘルプ（  ）アイコンをクリックします。

API の入手

次の API を入手するには、URL https://*cmx-ip-address* /apidocs/ を使用します。

- コンフィギュレーション REST API（Cisco CMX のさまざまな部分を設定するための API）。
- ロケーション ベースの REST API（ビジターのロケーション固有の詳細情報を検出するための API）。
- 分析ベースの REST API（ビジターに関する分析データを検出するための API）。
- 接続ベースの REST API（ユーザ セッション情報を検出するための API）。
- プレゼンス ベースの REST API（ビジターのプレゼンス データを検出するための API）。

第 3 章

Cisco CMX Detect and Locate サービス

Detect and Locate サービスの概要

Cisco Connected Mobile Experiences（Cisco CMX）の **DETECT & LOCATE** サービスでは、導入環境内でデバイスを表示、追跡できます。

DETECT & LOCATE サービスを使用して、キャンパス内のすべてのビルに導入されているすべてのアクセス ポイント（AP）や、各ビルの個々のフロアに導入されている AP を確認できます。また、Wi-Fi タグ、不正な AP、Wi-Fi 干渉源、Bluetooth Low Energy（BLE）ビーコンを検出できます。

初期設定

DETECT & LOCATE サービスを使用するには、次の初期設定を行う必要があります。

- マップのインポート：詳細については、マップのインポート, （9 ページ）を参照してください。
- コントローラの追加：概念については、CLI からの Cisco WLC の追加, （10 ページ）を参照してください。

デバイスの表示または追跡

手順

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

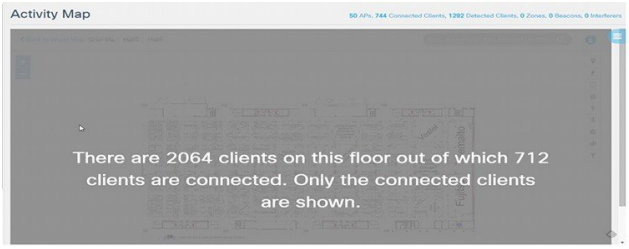
ステップ 2 [DETECT & LOCATE] をクリックします。

ステップ 3 [Activity Map] ウィンドウの左ペインを使用して、目的のビルとフロアに移動します。
[Activity Map] ウィンドウの右側にアイコンのリストが表示されます。

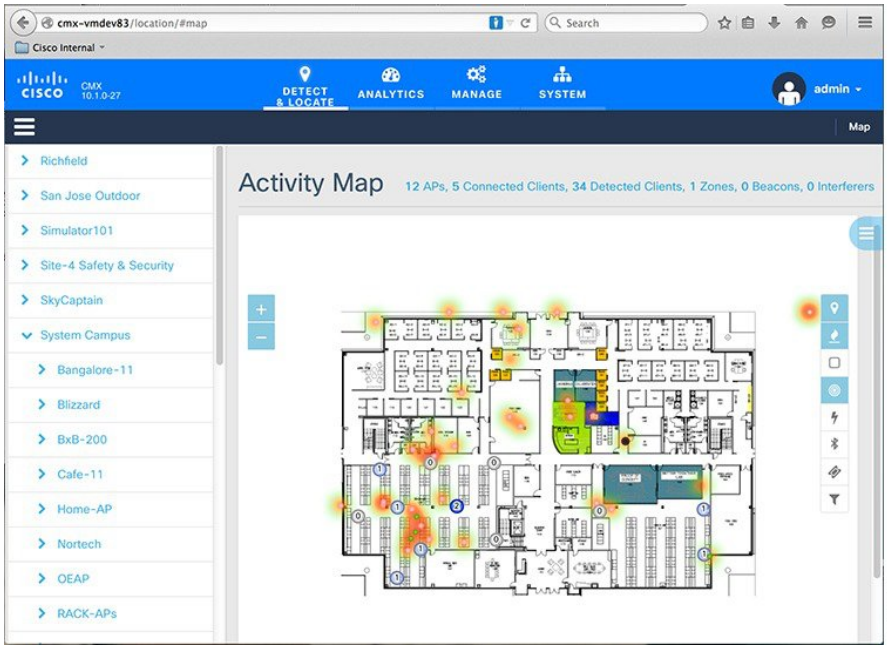
ステップ 4 次のアイコンを任意の組み合わせで選択して、デバイスのビューをカスタマイズします。

[Clients]：[Clients] アイコンをクリックすると、Cisco CMX による追跡対象（接続および検出された）クライアントデバイスがすべて表示または非表示になります。クライアントデバイスは、赤色の点（プローブ中クライアント）または緑色の点（接続クライアント）として表示されます。接続クライアントをクリックすると、そのクライアントが関連付けられている AP（青色の線）が表示され、プローブ中クライアントまたは関連付けられていないクライアントをクリックすると、クライアントの検出に使用される AP（赤色の線）が表示されます。

（注） 一度に表示できるクライアント（接続および検出）の最大数は、2000 です。 この制限を超えると、接続クライアントだけが表示されます。この場合も最大数は2000です（次の図を参照）。 ただし、接続クライアントの合計数も 2000 を超える場合、クライアントは表示されません。 このような場合は、Analytics サービスを使用してクライアント情報を表示することを推奨します。



[Heatmap]：[Heatmap] アイコンをクリックすると、クライアントデバイスのさまざまな集中度のエリアが表示または非表示になります。 次の図に示すように、クライアントデバイスの集中度が高いエリアは明るい赤色で表示されます。



- [Zones]：[Zones] アイコンをクリックすると、特定のフロアのゾーンが表示または非表示になります。

- [Access Point]：[Access Point] アイコンをクリックすると、特定のフロアに導入されているすべてのAPが表示または非表示になります。 APは、中央に番号が入った円オブジェクトとして表示されます。 この番号は、特定のAPに接続しているクライアントの数を示します。

  （注） APをクリックすると、そのAPに接続しているクライアント（青色の線）と、そのAPによって検出されたプローブ中クライアント（赤色の線）が表示されます。
  Cisco Hyperlocation モジュールを Cisco Aironet 3700 および 3600 シリーズ

（注） AP の背面に接続している場合は、1m 未満まで顧客、ビジター、またはアセットの位置を追跡できます。 現在、ハイパーロケーション ソリューションは関連付けられているクライアントでのみ機能します。

- [Interferers]：[Interferers] アイコンをクリックすると、ワイヤレス ネットワークで検出されたすべての RF 干渉源とその影響範囲ゾーンが表示または非表示になります。
- [Beacons]：[Beacons] アイコンをクリックすると、ワイヤレス ネットワークで検出された BLE 送信デバイスが表示または非表示になります。 BLE ビーコンの詳細については、BLE ビーコンの管理, （94 ページ）を参照してください。

  （注） ビーコンは干渉源として検出されます。 ビーコンに関連して発生する一般的な問題の 1 つに、追跡が有効にならないことがあります。 このような場合は、System サービスを使用して追跡の設定を変更できます。 詳細については、デバイスの表示または追跡, （14 ページ）を参照してください。

- [Tags]：[Tags] アイコンをクリックすると、Wi-Fi タグが表示または非表示になります。
- [Filters]：[Connection Status]、[Manufacturer]、および [Service Set Identifier (SSID)] などのパラメータに基づいて、表示するデバイスをフィルタリングするには、[Filters] アイコンをクリックします。
- [Inclusion & Exclusion Regions]：[Inclusion & Exclusion Regions] アイコンをクリックすると、フロアの包含領域と除外領域が表示されます。 包含領域と除外領域は Cisco Prime Infrastructure で作成されます。 Cisco CMX ではこれらの領域を表示できますが、変更することはできません。 包含領域は緑色で示され、除外領域は灰色で示されます。

デバイスの詳細情報の表示

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 [DETECT & LOCATE] をクリックします。

ステップ 3 [Activity Map] ウィンドウの左ペインを使用して、目的のビルとフロアに移動します。
[Activity Map] ウィンドウの右側にアイコンのリストが表示されます。

ステップ 4 目的のデバイス（クライアントデバイス、AP、ビーコンなど）を表示するには、対応するアイコンをクリックします。

ステップ 5 マップ上で該当するデバイスをクリックします。
デバイスの詳細情報（MACアドレス、IPアドレス、ステータスなど）を示すペインが表示されます。

クライアント更新間隔のカスタマイズ

DETECT & LOCATE サービスにより、フロア マップ上のクライアントの位置の更新間隔を設定できます。 更新間隔を使用して、クライアントの位置を判別するためのクライアントの位置のポーリング頻度を設定できます。

手順

ステップ 1 Cisco Connected Mobile Experiences（Cisco CMX）に、管理ユーザまたは Location ロールが付与されているユーザのいずれかとしてログインします。

ステップ 2 [DETECT & LOCATE] をクリックします。

ステップ 3 [Activity Map] ウィンドウの左ペインを使用して、目的のビルとフロアに移動します。
[Activity Map] ウィンドウの右側にアイコンのリストが表示されます。

ステップ 4 [Gear] アイコンをクリックして、クライアントの更新間隔を設定します。
クライアントの更新間隔を示すペインが表示されます。

ステップ 5 + アイコンまたは - アイコンを使用して、クライアントの更新間隔を増減します。 更新間隔は秒単位です。 指定できる範囲は 1 ～ 30 秒です。 デフォルトの更新間隔は 5 秒です。

ステップ 6 [OK] をクリックします。
マップ上にドットで示されるクライアントは、新たに設定された間隔で更新されます。

フィルタを使用したデバイス ビューのカスタマイズ

手順

ステップ 1 Cisco Connected Mobile Experiences（Cisco CMX）に、管理ユーザまたは Location ロールが付与されているユーザのいずれかとしてログインします。

ステップ 2 [DETECT & LOCATE] をクリックします。

ステップ 3 [Activity Map] ウィンドウの左ペインを使用して、目的のビルとフロアに移動します。

[Activity Map] ウィンドウの右側にアイコンのリストが表示されます。

ステップ 4 目的のデバイス（クライアントデバイス、AP、ビーコンなど）を表示するには、対応するアイコンをクリックします。クリックするアイコンが多いほど、有効になるフィルタリング オプションが増えます。

フィルタの追加と削除

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 [DETECT & LOCATE] をクリックします。

ステップ 3 [Activity Map] ウィンドウの左ペインを使用して、目的のビルとフロアに移動します。
[Activity Map] ウィンドウの右側にアイコンのリストが表示されます。

ステップ 4 目的のデバイス（クライアントデバイス、AP、ビーコンなど）を表示するには、対応するアイコンをクリックします。クリックするアイコンが多いほど、有効になるフィルタリング オプションが増えます。

ステップ 5 [Filter] ▼アイコンをクリックします。

ステップ 6 表示される [Filters] ダイアログボックスで、次のパラメータに基づいてクライアント フィルタを追加または削除できます。

- [Connection Status]：[Unassociated] または [Connected]
- [Device Manufacturer Type]：デバイス製造元の名前（Apple、Samsung など）
- [SSID]：デバイスの SSID

デバイスの検索

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 [DETECT & LOCATE] をクリックします。

ステップ 3 [Activity Map] ウィンドウの左ペインを使用して、目的のビルとフロアに移動します。

ステップ 4 [Activity Map] ウィンドウの [Search] フィールドに、目的のデバイスを検索またはフィルタリングするために次のいずれかのパラメータを入力します。

- [MAC Address]：対応するクライアントの MAC アドレスを入力します。このアドレスには小文字を使用し、区切り文字としてコロンを使用します（例：00:a0:22:bc:e2:00）。
- [Device IP Address]：クライアントの IPv4 または IPv6 アドレスをドット形式で入力します（例：10.22.12.212）。
- [SSID]：クライアントの SSID を自由形式のテキストで入力します。
- [Device Manufacturer]：特定の製造元名（Apple、Samsung など）を自由形式のテキストで入力します。
- [Username]：クライアントのユーザ名を自由形式のテキストで入力します。

ロケーション精度テストを使用したクライアントのロケーション精度の測定

Cisco CMX 10.2 では、複数のロケーション ポイントを使用して 1 つのデバイスのロケーション精度テストを実行できます。

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 [DETECT & LOCATE] をクリックします。

ステップ 3 [Activity Map] ウィンドウの左ペインを使用して、目的のビルとフロアに移動します。

ステップ 4 [Activity Map] ウィンドウで、クライアント検索のための検索オプションを選択します。

ステップ 5 該当するクライアントをクリックします。
[Client] ダイアログボックスが表示されます。

ステップ 6 ロケーション精度テストを開始するため、[LOCATION ACCURACY TEST] アイコンをクリックします。

ステップ 7 [Enter a test name] テキストボックスにロケーション精度テストの名前を入力し、Enter を押します。
ダイアログボックスが表示され、マップ上のクライアント デバイスの実際の位置に マーカーを配置するかどうかが確認されます。

ステップ 8 正しい位置にマーカーをドラッグします。

ステップ 9 [Run] をクリックします。
テストは必要に応じて任意の期間にわたって実行できます。 テストの経過時間が表示されます。

ステップ 10 現行ロケーションのテストが完了したら、[Pause] をクリックします。
デバイスを別のロケーションに移動してテストを続行できます（ステップ 8 からステップ 10 を繰り返します）。

ステップ 11 すべてのロケーション ポイントのテストが完了したら、[Finished?] をクリックします。 [View Result] をクリックして、テスト結果を取得します。
10m の精度と平均誤差距離を示すダイアログボックスが表示されます。

ステップ 12 [View accuracy test report] をクリックして、実行した精度テストのリストを表示します。 このレポートでは、テストを再開するか、最新ログまたはすべてのログをダウンロードすることができます。

（注） テストが進行中の場合でも、[View accuracy test report] をクリックしてすべてのテストをモニタできます。 実行中のテストを一時停止するには [Pause] をクリックします。 一時停止したテストを続行するには [Relaunch] をクリックします。 テストを終了し、結果を取得するには [Report] アイコンをクリックします。

テスト レポート テーブルからレポートを削除するには、[Delete] をクリックします。

クライアント再生

クライアント再生機能では、敷地内でクライアントを検出し、クライアントの移動を追跡できます。 一度に 1 つのクライアントのアクティビティを追跡できます。

手順

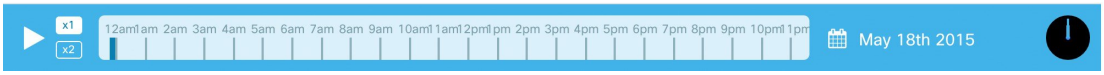
ステップ 1 Cisco Connected Mobile Experiences（Cisco CMX）にログインします。

ステップ 2 [DETECT & LOCATE] をクリックします。

ステップ 3 [Activity Map] ウィンドウの左ペインを使用して、目的のビルとフロアに移動します。

ステップ 4 MAC ID を使用して追跡するクライアントを検索します。
クライアント デバイスの検索方法の詳細については、デバイスの検索, （19 ページ）を参照してください。

ステップ 5 [Client Movement History Playback] アイコン をクリックします。
[Client Playback] ペインが表示されます（以下の図を参照）。



ステップ 6 [Play] アイコンをクリックして、クライアントの再生を開始します。
[Calendar] アイコンをクリックして日付を変更し、特定の日付の再生を表示することもできます。
再生速度を上げるには、[2x] ボタンをクリックします。

Cisco CMX での Hyperlocation の有効化

Cisco Hyperlocation ソリューションは、ソフトウェアおよびハードウェアのイノベーションの組み合わせによって高度なロケーション機能を実現するテクノロジー スイートです。 Cisco CMX リリース 10.2.1 では、Cisco Aironet 3600/3700 アクセス ポイントで使用可能な Angle of Arrival（AoA）テクノロジーと、Hyperlocation モジュールおよび Hyperlocation アンテナがサポートされています。 Cisco CMX は、高度なロケーション アルゴリズムを使用して位相差を抽出し、関連付けられているワイヤレス クライアントの位置を 1 m 以内の精度で正確に検出します。

Cisco Hyperlocation Module with Advanced Security では、Bluetooth Low Energy（BLE）ビーコンもモジュールに統合されています。 お客様は Power over Ethernet やデータセンターからの一元管理などの便利な機能を備えた BLE ビーコンを利用できます。 これにより、現場の IT エンジニアがスマート デバイスのアプリケーションを使用して、BLE ビーコンの状態を検査して回る必要がなくなります。 シスコの Hyperlocation ソリューションでは、仮想 BLE ビーコン技術を採用しています。これによってコンシューマ アプリケーションには単一の Hyperlocation モジュールが 5 つの BLE ビーコンとして表示されます。

Cisco CMX FastLocate テクノロジーにより、接続 WiFi クライアントの位置を迅速に更新できます。 データ パケットとプローブ フレームからの RSSI が使用可能な場合は、この RSSI が位置の計算に使用されます。 これは、中央でスイッチされる WLAN と FlexConnect（ローカルでスイッチされる WLAN）の両方で使用できます。 Cisco Aironet 700、1700、2600/2700、および 3600/3700 AP を Cisco WLC リリース 8.1.123.0 以降と共に使用する場合、これらの AP では CMX FastLocate がサポートされます。

推奨される AP モードを次に示します。

- 拡張ローカル モード：AP はオンカレント チャネルとオフチャネルを状況対応的にスキャンし、データ処理無線に対するパフォーマンスの影響は最大 15% です。
- モニタ モード AP：AP は 2.4 GHz および 5 GHz 帯域でスキャンします。
- モジュラ AP：データ処理無線に影響せずに 2.4 および 5 GHz 帯域での Hyperlocation モジュールまたはワイヤレス セキュリティ モジュール（WSM）スキャン機能を備えた Cisco 3600/3700 AP。

（注）
- FastLocate と Hyperlocation は Cisco CMX 10.2.1 以降でサポートされています。
- Hyperlocation 機能は、Cisco CMX ではデフォルトで有効になっています。
- Hyperlocation および FastLocate 機能は Cisco WLC リリース 8.1.123.0 以降でサポートされています。
- 現在、Hyperlocation に対応した Cisco WLC では、Hyperlocation に対応した Cisco CMX を 1 つだけサポートできます。

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 [SYSTEM] > [Dashboard] を選択します。

ステップ 3 ウィンドウの右上隅にある [Gear] アイコンをクリックします。
[Settings] ウィンドウが表示されます。

ステップ 4 [Location Setup] タブをクリックします。

ステップ 5 [Location Calculation Parameters] ウィンドウで [Enable Hyperlocation] チェックボックスをオンにします。

ステップ 6 Cisco WLC を Cisco CMX に追加します。

ステップ 7 Hyperlocation オプションを有効にする前に Cisco WLC を追加した場合は、NMSPLB サービスを再起動して Hyperlocation を開始します。
NMSPLB サービスを再起動するには、**cmxctl restart nmsplb** コマンドを入力します。

ステップ 8 Cisco CMX による Hyperlocation の処理を停止するには、[Location Parameters] ウィンドウで（[Enable Hyperlocation] チェックボックスをオフにして）Hyperlocation オプションを無効にし、NMSPLB サービスを再起動します。
シスコの Hyperlocation ソリューションの詳細については、次のマニュアルを参照してください。
- 『Release Notes for Cisco Connected Mobile Experiences (CMX)』（リリース 10.2.0 以降）。
- 『Release Notes for Cisco Wireless Controllers and Lightweight Access Points for Cisco Wireless Release 8.1.123.0』
- 『Cisco WLC Configuration Guide』の「Configuring Cisco Hyperlocation in Cisco WLC」の項。
- 『Cisco Aironet Hyperlocation Antenna (AIR-ANT-LOC-01=) Installation Guide』
- Cisco Aironet アクセス ポイント モジュールの設置と取り外し

第 4 章

Cisco CMX Analytics サービス

Analytics サービスの概要

Cisco Connected Mobile Experiences（Cisco CMX）の Analytics サービスには、Wi-Fi デバイスのロケーションを分析するためのデータ分析ツールセットが用意されています。 Analytics サービスにより、組織はデータ ソースとしてネットワークを使用して、ビジターの行動パターンとトレンドを理解できるようになります。これにより、ビジターのエクスペリエンスを向上させ、カスタマー サービスを改善することができます。

Analytics サービスでは、次のことが可能です。

- Wi-Fi デバイスのロケーションを分析します。
- 新規ビジター（初めて認識されるビジター）の数とアクセスを繰り返すビジター（以前の訪問で認識されているビジター）の数、ビジターが敷地に滞在した時間、敷地への訪問頻度を推測します。
- 敷地内を移動し、対話するビジターの行動パターンを詳しく理解します。
- 敷地内部のマーケティングを測定して、ビジネス パフォーマンスを分析します。
- ピーク時に十分な人員を配置すること、適切な信号、十分に活用されていない領域に変更を加えることで、顧客満足度を向上させます。

Analytics ダッシュボード

Analytics サービスのダッシュボードは、特定ゾーン内でのビジターの移動に関連付けられているさまざまなパラメータを可視化し、理解できるように設計されています。 ダッシュボードを毎日使用して、最新のトレンドまたはイベントを調べることができます。 また、要件に応じて、さまざまなウィジェットを使用してダッシュボードをカスタマイズできます。

Analytics ダッシュボードへのアクセス

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 [Analytics] > [Dashboard] を選択します。

ステップ 3 ダッシュボードの左側のペインで、導入階層（ヘテラルキー）を使用して必要なレポートに移動します。 そのレポートに関する詳細がダッシュボードに表示されます。

Analytics ダッシュボードに表示されるデータのフィルタリング

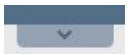
ダッシュボードに表示されるデータはフィルタリングされており、検知されていた期間が 5 分より長く 8 時間未満であるデバイスが表示されます。

滞在時間（ビジターがロケーションに滞在する時間）を変更するには、次の手順を実行します。

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 [Analytics] > [Dashboard] を選択します。

ステップ 3 [Location and Date] ペインの [Expander]  アイコンをクリックします。
[Edit Report] ウィンドウが表示されます。

ステップ 4 [Dwell Threshold] の値を指定します。

Analytics レポート

Analytics ダッシュボードは、特定の敷地内でのビジターの行動パターンを理解し、モニタするためのさまざまなレポートを提供します。

Analytics サービスのレポート機能は、パラメータ化されたテンプレートにより、より定期的なマネージャ向けの情報セットを提供し、特定のゾーンにおいて一定の期間にわたって発生するさまざまなトレンドとパターンを測定します。 新しいレポートの作成や既存のレポートの変更が可能です。

[Device Count] レポートと [Average Dwell Time] レポートの表示

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 [Analytics] > [Dashboard] を選択します。

ステップ 3 分析するロケーション（[Region]、[Building]、[Floor]、[Zone]、または [Tags]）をクリックします。

ステップ 4 [Location andDate] ペインで、レポートの時間枠を選択します。 次のオプションを使用できます。

- [Now]：過去 15 分間のアクティブ デバイスの数。
- [Today]：指定したレポートは本日の値を使用して実行され、結果が表示されます。
- [Yesterday]：指定したレポートは昨日の値を使用して実行され、結果が表示されます。
- [This Week]：指定したレポートは今週の値（月曜日～日曜日）を使用して実行され、結果が表示されます。
- [Last Week]：指定したレポートは先週の値（月曜日～日曜日）を使用して実行され、結果が表示されます。
- [Last 2 Weeks]：指定したレポートは過去 2 週間の値を使用して実行され、結果が表示されます。
- [This Month]：指定したレポートは今月の値を使用して実行され、結果が表示されます。
- [Last Month]：指定したレポートは先月の値を使用して実行され、結果が表示されます。
- [Last 3 Months]：指定したレポートは過去 3 ヵ月の値を使用して実行され、結果が表示されます。
- [This Year]：指定したレポートは今年の値を使用して実行され、結果が表示されます。
- [Last Year]：指定したレポートは昨年の値を使用して実行され、結果が表示されます。
- [Custom Range]：指定したレポートは [Start] および [End] の日付フィールドに指定した日付値を使用して実行されます。

  選択した基準に基づくレポートがダッシュボードに表示されます。レポートには次のウィジェットが含まれています。

- [Visitors] ウィジェット
  - [Device Count] レポートには、ビジターの総数と、アクセスを繰り返すビジターの割合および新規ビジターの割合が表示されます。

- [Dwell Time] レポートには、すべてのビジターの平均滞在時間と、アクセスを繰り返すビジターおよび新規ビジターの滞在時間が表示されます。

- [Compare Data to] ウィジェット：アクセスを繰り返すビジターと新規ビジターの比較結果が表示されます。 次のオプションを使用できます。
  - [Previous]
  - [Average]：現在の期間と前の期間の平均計算から、平均値が算出されます。 [Date]ペインで [This Week] を選択すると、比較対象の前の週は先週になり、先週と今週を対象として平均が算出されます。

- 折れ線グラフと、選択した基準のサマリ ビューと詳細ビューの組み合わせ：次のフィルタ基準を適用して X 軸と Y 軸をカスタマイズできます。
  - [View Unique Devices] または [View Absolute Visits]
  - [Locations]：[Campus]、[Building]、[Floor]、[Zone]、[Zone Tag]
  - [Values]：[Ascending]、[Descending]、[Alphabetical]

カスタム レポートの作成と管理

独自のレポートを作成するには、ロケーション、日付/時刻、各種ウィジェットを選択し、Analytics ダッシュボードでどのように表示するかを決定します。 レポートは左側のペインの [Reports] の下に表示されます。 レポート名をクリックします。ダッシュボードに対応する詳細が表示されます。

（注） ダッシュボードにレポートが表示されない場合は、[Create New Report] ウィンドウが自動的に表示されます。

実行できるカスタム レポート関連の操作を以下に示します。

- カスタム レポートの削除, （30 ページ）

カスタム レポートの作成

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 [Analytics] > [Dashboard] を選択します。

ステップ 3 ダッシュボードの左側のペインで、[Reports] の横の  をクリックします。
[Create New Report] ページが表示されます。

ステップ 4 右側のペインで [Report Type] 行から次のいずれかのオプションを選択します。

- 自動生成（Auto-Generate）
- カスタマイズ（Customized）

ステップ 5 [Focus Area Filter] ドロップダウンリストから、分析するロケーションを選択します。
ロケーション タイプは、[Building]、[Campus]、[Floor]、[Zone] です。

ステップ 6 [Date & Time filters] ドロップダウンリストから、レポート対象の日付と時間の範囲を選択します。

ステップ 7 [Add Widgets]  エリアで [+] をクリックし、レポートに次のウィジェットのいずれかを追加します。

- [Visitor]：ネットワークで検出されたビジターの数を表示します。
- [Average Dwell Time]：特定のロケーションでのビジターの滞在時間を表示します。
- [Correlation]：ロケーション間でのデバイスと訪問の関係を示します。
- [Path]：ビジターがロケーションを訪問する前にいた場所と、訪問後に移動した場所を示します。
- [Associated Status]：ネットワークに関連付けられているビジターと、プローブ中ビジターの数を示します。
- [Dwell Time Breakdown]：選択したエリアの滞在時間の内訳を示します。次に例を示します。
  - 滞在時間が 1 時間未満のビジターの割合は 20% 未満である（20 percent of the visitors stayed less than an hour）
  - 滞在時間が 1 ～ 2 時間のビジターの割合は 50% である（50 percent stayed for 1 to 2 hours）
  - 滞在時間が 2 時間を超えるビジターの割合は 30% である（30 percent stayed for more than 2 hours）

ステップ 8 滞在時間のしきい値を設定できます。 これは、クライアント デバイス（ビジター）が特定のロケーションに滞在する時間です。 [Advanced Widget Filters] エリアで、ドロップダウン オプションから最小時間と最大時間を選択します。

ステップ 9 [Done] をクリックします。
指定したフォーカス エリア フィルタと日付フィルタに基づいて、レポート名が生成されます。新しいレポート名は、左側のペインの [Reports] の下にリストされます。

カスタム レポートの作成後に実行できる作業を次に示します。

- **1** スケジュール設定されたレポートを作成するレポートをクリックします。
  2 表示される [Expander] アイコンをクリックします。
  3 [Clock] アイコン（スケジュール）をクリックして、レポートをスケジュールします。
  4 [SELECT REPORT OPTION] ダイアログボックスで [HTML] または [PDF] を選択します。
  5 [Next] をクリックします。

  - [HTML Report]：HTML 形式のレポートをスケジュールできます。
    - レポート送信先の受信者の電子メール アドレスを入力します。
    - レポートを生成する必要がある期間の開始日時を入力します。
    - レポートの実行頻度（[One Time]、[Daily]、または [Weekly]）を選択します。
  - [PDF Report]：PDF 形式のレポートをスケジュールできます。 PDF レポートのパラメータをカスタマイズできます。
    - [Header] テキストボックスに、PDF レポートのヘッダーを指定します。
    - [Select a Logo] をクリックし、PDF レポートのロゴを選択します。 ロゴは左、中央、右のいずれかに配置できます。
    - コメントを指定する場合は、[Add your comments here] テキスト ボックスにコメントを入力します。
    - [Footer] テキスト ボックスに、PDF レポートのフッターを指定します。
    - レポート送信先の受信者の電子メール アドレスを入力します。
    - レポートを生成する必要がある期間の開始日時を入力します。
    - レポートの実行頻度（[One Time]、[Daily]、または [Weekly]）を選択します。

- [Print a Report]：レポートを印刷します。
  1 印刷するレポートをクリックします。
  2 表示される [Expander] アイコンをクリックします。
  3 レポートを印刷するため、[Print] アイコンをクリックします。

4 [SELECT REPORT OPTION] ダイアログボックスで [HTML] または [PDF] を選択します。

5 [Next] をクリックします。

- [View Scheduled Report Manager]：スケジュール設定されたレポートを表示するには、[Analytics] > [Schedule] を選択します。 [Scheduled Report Manager] ページに、次の情報が表示されます。
  - [Report ID]：レポート ID を示します。
  - [Report Title]：レポートのタイトルを示します。
  - [Username]：スケジュール設定されたレポートを作成したユーザを示します。
  - [Start From]：レポートの実行スケジュールの開始日時を示します。
  - [Recipients]：受信者の電子メール アドレスを示します。
  - [Type]：レポートのタイプ（HTML または PDF）を示します。
  - [History]：[View] をクリックして、スケジュール設定されたレポートの履歴を表示します。
  - [Actions]：スケジュール設定されたレポートを変更するには [Modify] をクリックし、削除するには、[Delete] をクリックします。

スケジュール設定されたカスタム レポートの作成

カスタム レポートを作成し、組織に合ったロゴ、テキスト、ヘッダー、フッターをレポートに追加します。 レポートを、カスタマイズされた頻度で特定の受信者を対象にスケジュール設定できます。

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 [Analytics] > [Dashboard] を選択します。

ステップ 3 ダッシュボードの左側のペインでレポート名を展開し、[Schedule] をクリックします。
[SELECT REPORT OPTION] ダイアログボックスが表示されます。 次のオプションを使用できます。

- [HTML Report]
- [PDF Report]

ステップ 4 必要なレポートの種類に対応するオプション ボタンをクリックし、[Next] をクリックします。
PDF オプションを選択した場合、次のカスタマイズ オプションを利用できます。

- [Header]：ヘッダーをレポートに追加し、名前を指定します。 右矢印キー、上矢印キー、左矢印キーを使用してヘッダー テキストの位置をカスタマイズできます。
- [Logo]：[Logo] アイコンをクリックしてレポートにロゴを追加します。 選択できるデフォルトのロゴがいくつかあります。 また、[Upload a Logo] をクリックしてロゴをアップロードすることもできます。
- [Comment]：レポートに関するコメントを追加します。このためには、[Add your comments Here] フィールドにテキストを入力します。 レポートのセクションを移動するには、セクション内の各種コンポーネントの左側にある 上矢印キーまたは下矢印キーをクリックします。
- [Footer]：レポート下部にフッター テキストを追加します。

ステップ 5 [Next] をクリックします。
[Schedule Report] ウィジェットが表示されます。

ステップ 6 レポート送信先の受信者の電子メール アドレスを入力します。

ステップ 7 レポートを生成する必要がある期間の開始日時を入力します。

ステップ 8 レポートの実行頻度（[One Time]、[Daily]、または [Weekly]）を選択します。

ステップ 9 [Schedule] をクリックします。

カスタム レポートの削除

自分が作成したカスタム レポートはすべて削除できます。

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 [Analytics] > [Dashboard] を選択します。

ステップ 3 ダッシュボード の左側のペインで、カーソルをレポートに合わせ、[Delete] アイコンをクリックします。

カスタム ウィジェット

カスタム ウィジェットでは、分析の目的に適した特定のアクティビティを表示、分析できます。たとえば、関心対象ゾーンでのビジター（クライアント）のアクティビティに重点を置くウィジェットを作成できます。 カスタム ウィジェットは、ビジターのアクティビティに関連するデータだけを収集、表示し、このデータを分析、解釈できるようにします。 カスタム ウィジェットの情報から、クライアント アクティビティに基づく有効な意思決定を行うことができます。

（注） カスタム ウィジェットを生成できるのは上級ユーザだけです。

[Visitors] ウィジェット

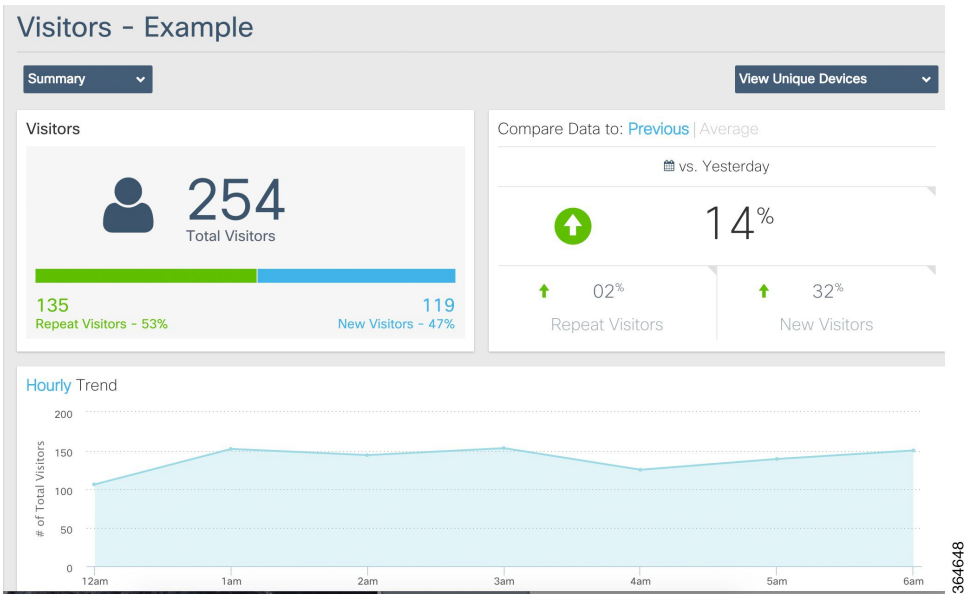
[Visitors] ウィジェットは、フォーカスエリアにおけるビジター（クライアントデバイス）に関する詳細なサマリを表示します。

[Visitors] ウィジェットは、次の形式で表示できます。

- [Summary]：これはデフォルト ビューです。 このビューは、[Visitors]、[Compare Data to] 、および [Hourly Trend] の各グラフで構成されています。 新規ビジターとアクセスを繰り返すビジターの内訳も表示されます。 [Compare Data to] グラフには、当日と前日の比較データが表示されます。 また、現在のデータを 1 日あたりの平均ビジター数と比較することもできます。 アクセスを繰り返すビジターと新規ビジターの内訳は、パーセントでも表示されます。 グラフには、午前 12 時から午後 12 時までの間の 1 時間あたりのビジター数が表示されます。
- [Chart]：折れ線グラフと、合計ビジター数（Y 軸）および特定の時間におけるアクティビティ（X 軸）のサマリ ビューが表示されます。 次のビューに基づいてグラフを設定できます。
  - [View Unique Devices] または [View Absolute Visits]
  - [Locations]：[Campus]、[Building]、[Floor]、[Zone]、[By Hour]
  - [Values]：[Ascending]、[Descending]、[Alphabetical]

  Y 軸の値には、ビジター数と合計ビジター数に対する割合を交互に表示できます。 折れ線上の任意の点にカーソルを合わせると、そのインスタンスでの接続とプローブに関するデータが表示されます。
- [Table]：ビジター数属性が表形式で表示されます。

  各ビューでは次のトレンドを使用できます。
  - ユニークデバイスの表示（View Unique Devices）
  - 絶対訪問の表示（View Absolute Visits）



[Average Dwell Time] ウィジェット

[Average Dwell Time] ウィジェットには、特定のロケーションでのビジター（クライアント デバイス）の滞在時間に関する詳細なサマリが表示されます。

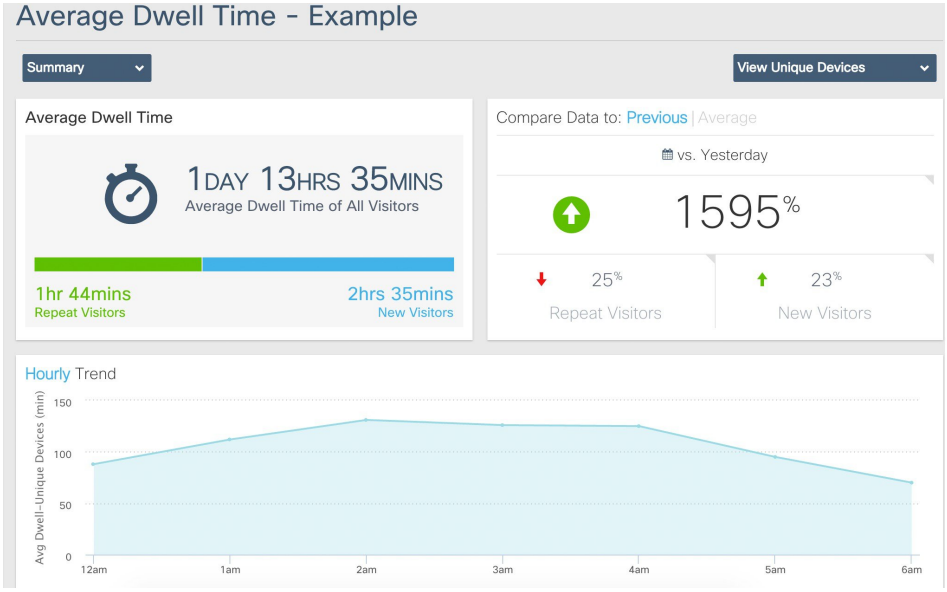
平均滞在時間は次の形式で表示できます。

- [Summary]：これはデフォルト ビューです。 サマリ ビューには [Average Dwell Time]、[Compare Data to]、および [Daily Trend] の各グラフが表示されます。 新規ビジターとアクセスを繰り返すビジターの内訳も表示されます。 [Compare Data to] グラフには、当日と前日の比較データが表示されます。 また、現在のデータを 1 日あたりの平均ビジター数と比較することもできます。 アクセスを繰り返すビジターと新規ビジターの内訳は、パーセントでも表示されます。 グラフには、午前 12 時から午後 12 時までの間の 1 時間あたりのビジター数が表示されます。
- [Chart]：折れ線グラフと、合計ビジター数（Y 軸）および特定の時間におけるアクティビティ（X 軸）のサマリ ビューが表示されます。 次のビューに基づいてグラフを設定できます。
  - [View Unique Devices] または [View Visits]
  - [Locations]：[Campus]、[Building]、[Floor]、[Zone]、[Day]、[Hour of Day]、[Hour]、[Region]、[Tag] のいずれかの値を使用してフィルタリングできます。
  - [Sort order]：[Ascending]、[Descending]、[Alphabetical]
- [Table]：ビジター数属性が表形式で表示されます。 次の詳細情報を表示できます。
  - 場所
  - 上位エリア

- Day
- 時刻
- 滞在時間

各ビューでは次のトレンドを使用できます。

- ユニークデバイスの表示（View Unique Devices）
- 絶対訪問の表示（View Absolute Visits）



[Dwell Time Breakdown] ウィジェット

[Dwell Time Breakdown] ウィジェットには、選択したエリアの滞在時間の分布が表示されます。

[Dwell Time Breakdown] は次の形式で表示できます。

- [Summary]：これはデフォルト ビューです。 サマリ ビューには [Dwell Time Breakdown]、[Compare Data to]、および [Daily Trend] の各グラフが表示されます。 滞在時間の内訳は、次の範囲で表示されます。
  - 0 ～ 5 分
  - 5 ～ 20 分
  - 20 ～ 60 分
  - 60 ～ 120 分
  - > 120 分

- [Chart]：折れ線グラフと、時間範囲 0 ～ 5 分、5 ～ 20 分、20 ～ 60 分、60 ～ 120 分、および > 120 分での滞在時間の内訳のサマリ ビューです。 次のビューに基づいてグラフを設定できます。
  - [View Unique Devices] または [View Visits]
  - [Locations]：[Campus]、[Building]、[Floor]、[Zone]、[Day]、[Hour of Day]、[Hour]、[Region]、[Tag] のいずれかの値を使用してフィルタリングできます。
  - [Sort order]：[Ascending]、[Descending]、[Alphabetical]

- [Table]：0 ～ 5 分、5 ～ 20 分、20 ～ 60 分、60 ～ 120 分、および > 120 分の時間範囲での滞在時間の内訳に関する情報を表示する表形式のビューです。

（注） このビューでは、テーブル内のレコードを検索できます。 [Search] テキスト ボックスはテーブルの上にあります。

[Correlation] ウィジェット

（注） Cisco CMX 10.2 の [Correlation] ウィジェットは、Cisco CMX リリース 10.1 では [Crossover] ウィジェットと呼ばれていました。

[Correlation] ウィジェットには、2 つのロケーション間でのクライアント デバイスの相間に関する詳細なサマリが表示されます。 相関データから、2 つのゾーン間の関係を判断できます。 ゾーン間の相関が低い場合は、2 つのゾーン間のアクセスが欠落していることを示します。 たとえば、ショッピング モールの飲食店街と映画館の間では相関が高いことを期待できます。 [Correlation] ウィジェットは、次の形式で表示できます。

- [Correlation]：ゾーン間の相関をインタラクティブなグラフィックで表示します。 フォーカス エリア、ビル、または絶対デバイスとユニーク デバイスの比較に基づいてフィルタリングすることで、ゾーン間の相関を設定できます。
- [Table]：次のカラムからなるテーブルにデータが表形式で表示されます。
  - [Area]：相関が設定されているゾーン。
  - [Grouping]：相関データの収集対象であるフォーカス エリア。
  - [Correlation]：ゾーン（[Area] カラム）とフォーカス エリアの間の相関データ（パーセント）。

各ビューでは次のトレンドを使用できます。

- ユニークデバイスの表示（View Unique Devices）
- 絶対訪問の表示（View Absolute Visits）

[Path Analysis] ウィジェット

[Path Analysis] ウィジェットでは、ビジター（クライアント デバイス）がフォーカス ロケーションの訪問前と訪問後に辿った経路が分析され、その経路がグラフィカルに表示されます。

- 緑色（左）の側は、デバイスの移動元ロケーション（例：フォーカス ゾーンに入る直前にいたロケーション）を示します。
- 青色（右）の側は、デバイスの移動先ロケーション（例：フォーカス ゾーンを出た直後に移動したロケーション）を示します。

フォーカスの上にカーソルを合わせると、次のパーセント値に基づく内訳が表示されます。

- フォーカス ゾーンで開始または終了した経路の割合（□）。
- フォーカス ゾーンに到着した経路またはフォーカス ゾーンを離れた経路の割合（□）。

緑色のセクションにカーソルを合わせると、このゾーンから開始してフォーカス ゾーンに入った経路の数が表示されます。

青色のセクションにカーソルを合わせると、フォーカス ゾーンから開始してこのゾーンで終了した経路の数が表示されます。

[Associated Status] ウィジェット

[Associated Status] ウィジェットには、ネットワークに関連付けられているクライアントの数と、ネットワークをプローブしているクライアントに関する詳細なサマリが表示されます。

- [Detected]：ネットワークをプローブ中にネットワークの AP により検出されたクライアント デバイスを指します。
- [Connected]：レポートで選択されている期間内に 1 回以上 AP との接続を確立したクライアント デバイスを指します。

（注） 定義されているデータ セット全体に基づいてすべてのパスが算出されますが、スペースの制約上、ウィジェットには（パーセンテージに基づく）上位 15 パスだけが表示されます。 [Edit Widget] リンクを使用すると、データ プールの収集元のヘテラルキー レベルを定義し、このウィジェットの特定のフォーカスを定義することができます。 これにより、レポートに複数のウィジェットを追加し、2 つのゾーンを並べて比較できます。

関連付けステータスは、次の形式で表示できます。

- [Summary]：これはデフォルト ビューです。 [Summary] ビューは、[Associated Status]、[Compare Data to]、および [Hourly Trend] の各グラフで構成されています。
- [Chart]：折れ線グラフと、関連付けられているクライアントとプローブ中クライアントのサマリ。 このビューを切り替え、関連付けられているクライアントのパーセンテージとクライ

アント合計数を表示することができます。X軸は、ロケーションまたは時刻のいずれかに基づきます。 折れ線グラフと、選択した基準のサマリ ビューと詳細ビューの組み合わせも使用可能です。 次のフィルタ基準を適用して X 軸と Y 軸をカスタマイズできます。

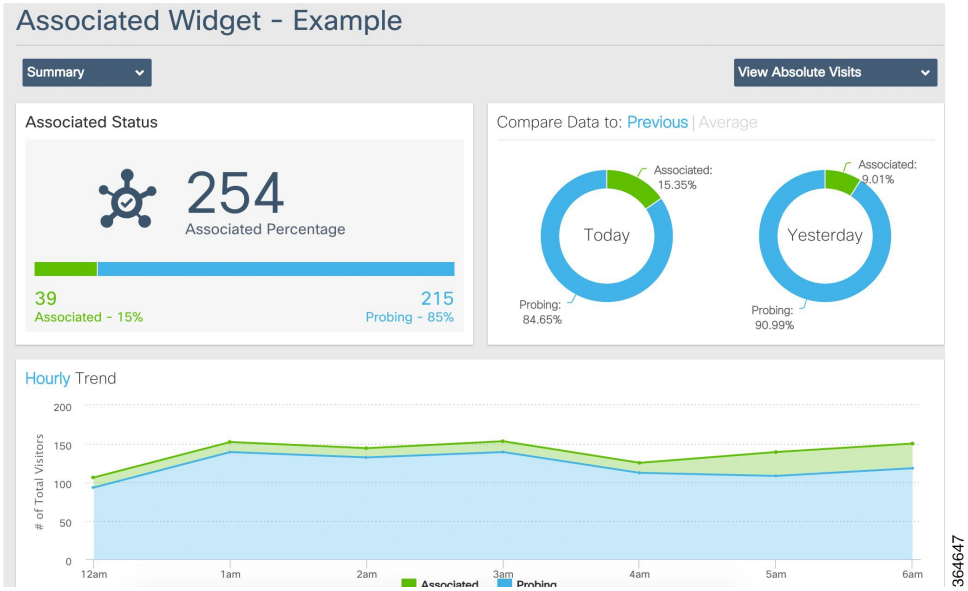
- [View Unique Devices] または [View Absolute Visits]
- [Locations]：[Campus]、[Building]、[Floor]、[Zone]、[By Hour]
- [Values]：[Ascending]、[Descending]、[Alphabetical]

折れ線上の任意の点にマウス ポインタを合わせると、そのインスタンスでの接続とプローブに関するデータが表示されます。

- [Table]：クライアントの接続属性と検出属性が表形式で表示されます。

各ビューでは次のトレンドを使用できます。

- ユニークデバイスの表示（View Unique Devices）
- 絶対訪問の表示（View Absolute Visits）



カスタム ウィジェットの作成

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 [Analytics] > [Dashboard] を選択します。

ステップ 3 ダッシュボードの左側のパネルで、[Custom Reports] の横の [Add] アイコンをクリックします。
[Create New Report] ウィンドウが表示されます。

ステップ 4 右側のペインの [Report Type] ウィジェット行から [Customized] を選択します。

ステップ 5 [Focus Area Filter] ドロップダウン リストから、分析するロケーションを選択します。
ロケーション タイプは [Building]、[Campus]、[Floor]、[Zone] です。

ステップ 6 [Date & Time filters] ドロップダウン リストから、レポートを実行する日付と時間の範囲を選択します。
[Add Widget] エリアの下部にあるドットをクリックし、次のオプション セットにスクロールします。 1 つのウィジェットにまとめる複数のウィジェットを選択します。

ステップ 7 [Add Widgets] エリアで [Add+] アイコンをクリックし、レポートに次のウィジェットのいずれかを追加します。
[Add Widget] エリアの下部にあるドットをクリックし、次のオプション セットにスクロールします。 1 つのウィジェットにまとめる複数のウィジェットを選択します。

ステップ 8 滞在時間のしきい値を設定できます。 これは、クライアント デバイス（ビジター）が特定のロケーションに滞在する時間です。 [Advanced Widget Filters] エリアで、ドロップダウン オプションから最小時間と最大時間を選択します。

ステップ 9 [Done] をクリックします。
ウィジェットが作成されます。

ステップ 10 レポートに付けるレポート タイトルをクリックします。

ステップ 11 [Save] をクリックします。

ソーシャル メディア分析

CMX 10.2 では、ソーシャル メディアから収集したデータを使用して、意思決定能力向上のための分析を提供できるようになりました。企業は自社のオンライン レピュテーションを分析し、イベントやサービスに関する肯定的なコメントと否定的なコメントのトレンドを確認できます。

たとえば、レストランのマネージャはオンライン レピュテーションを分析し、レストランのサービスに関する肯定的なコメントと否定的なコメントのトレンドを確認できます。 また、一定期間、特定のロケーション、および 1 日のうちの特定の時間における情報を確認するためのデータ

を設定することもできます。 この情報により、提供するサービスについて情報に基づいた意思決定を行うことができます。

現在、ソーシャル メディア分析（SMA）ではTwitterからの投稿がサポートされています。 また、Cisco CMX は Twitter サーバに対して API コールを実行できる必要があります。

ユーザは SMA 設定ページでハッシュタグを設定できます。これにより、SMA は設定されたハッシュタグを含むツイートを取得し、ソーシャル メディア分析エンジン パイプラインに挿入します。 SMA ダッシュボードには、ソーシャル メディア分析とトレンドの詳細が表示されます。

ソーシャル メディア分析の設定

Twitter ハンドルの設定

手順

ステップ 1 Twitter ユーザ アカウントを作成します。

a) ブラウザで http://twitter.com にログインします。
b) サインアップ ページで、氏名、電子メール、パスワードを入力します。
c) サインアップ手順を完了します。

ステップ 2 ユーザ アカウントのクレデンシャルを使用して Twitter アプリを作成します。

a) https://apps.twitter.com/ にログインします。
b) 新しいアプリケーションを作成するため、[Create New App] ボタンをクリックします。
c) 組織に関する必要な情報を入力します。
d) 開発者契約に同意し、アプリケーションを作成します。

ステップ 3 アプリケーションの作成後に、[Keys and Access tokens] タブからアプリケーションのコンシューマ キーとコンシューマ秘密キーを取得します。

Cisco CMX SMA の初期プロビジョニング

- Twitter クレデンシャルを使用して SMA をプロビジョニングするために、**cmxctl config sma twitter** コマンドを入力します。
  Cisco CMX コマンドの詳細については、『Cisco Connected Mobile Experiences (CMX) Command Reference Guide, Release 10.2』を参照してください。

プロキシ設定

- システムがプロキシの背後にある場合は、プロキシを使用するように SMA を設定するために、**cmxctl config sma proxy** コマンドを入力します。

ハッシュタグの設定

SMAは、ハッシュタグに基づいてTwitterからツイートを取得します。 これは、製品、ロケーション、関連コンテキストなどの名前です。 たとえば、レストランのハッシュタグとして、「#olivegarden」や「#applebee」などのようにレストラン名を使用できます。

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 [Analytics] > [Social] を選択します。

ステップ3 [Social analytics] ページで [Gear] アイコンをクリックし、ソーシャル メディア分析を設定します。
すべてのビルのハッシュタグをロードするには、[Location] ドロップダウン リストから [All] を選択できます。

[Configure Hash tag] ウィンドウが表示されます。

ステップ4 ビジネスに関連するロケーション固有のハッシュタグを入力して、[Add] ボタンをクリックします。

ステップ5 [Social] タブをクリックして、[Social analytics] ウィンドウに戻ります。
ハッシュタグの設定後にCisco CMXがツイートを取り込んでダッシュボードに結果を表示するまで1 ～ 2時間かかることがあります。

ソーシャル メディア分析の表示

SMAダッシュボードには、設定されたハッシュタグに関する詳細なソーシャルメディア分析が表示されます。 ロケーションと日時範囲に基づいて結果をフィルタリングできます。 また、さまざまな業務時間の統計情報を確認することもできます。

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 [Analytics] > [Social] を選択します。

ステップ3 表示するデータをフィルタリングします。 次のオプションを使用できます。

- [Location]：ソーシャル メディア データの取得元ロケーションを選択します。 複数のロケーションを選択できます。
- [Date]：ソーシャル分析データを取得する期間を選択します。

- [Today]：このドロップダウン リストから、必要な期間を選択します（[Today]、[Yesterday]、[Last Week]、[Last 2 Weeks]、[This Month]、[Last Month]、[Last 3 Month]、[This Year]、[Last Year]）。
- [All Day]：このドロップダウン リストから、ソーシャル メディア データを取得する時間枠を選択します。 オプションは、[All Day]、[Morning (5am-9am)]、[Business Hours (9am-5pm)]、[Evening(5pm-9pm)]、および [Custom Time] です。

SMA ダッシュボードには次の情報が表示されます。

- [Hashtags]：このセクションには、統計が参照するハッシュタグが表示されます。
- [Statistics]：統計データには、ロケーションに関する情報（[total posts]、[photos]、[reposts]、[likes]、[dislikes]、[neutral]）が含まれています。 グラフィカル表現には、選択された条件に基づいてトレンドを示す折れ線グラフが含まれます。
- [Details]：詳細なデータには、[photos reposts]、[likes]、[dislikes]、[neutral] が含まれます。 詳細を数値で示す積み重ねグラフが表示されます。

ヒートマップ分析の実行

ヒートマップは、クライアントの移動をグラフィカルに表示できます。ヒートマップではデバイスが多数集中しているエリアが赤色で示され、アクティビティが少ないエリアが青色で示されます。

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 [Analytics] > [Heatmap] を選択します。

ステップ 3 [Activity Heatmap] ウィンドウで、[Date] アイコンをクリックし、日付を選択します。

ステップ 4 [Time] アイコンをクリックし、時刻を表示または非表示にします。

ステップ 5 次のオプションから選択します。

- [Campus] ドロップダウン リストから、ヒートマップ分析を実行するキャンパスを選択します。 ドロップダウン リストには、Cisco CMX と同期しているすべてのキャンパスが含まれています。
- [Building] ドロップダウン リストから、この分析を実行するビルを選択します。 このドロップダウン リストには、Cisco CMX と同期しているすべてのビルが含まれています。
- [Floor] ドロップダウン リストから、この分析を実行するフロアを選択します。

ステップ 6 [Heatmap] アイコンをクリックしてヒートマップ分散を表示し、[Zone] アイコンをクリックしてゾーンを表示します。

ステップ 7 [Zoom in (+)] ボタンをクリックしてマップのビューを拡大するか、[Zoom out (-)] ボタンをクリックしてマップのビューを縮小します。

ステップ 8 [Realtime] をクリックしてヒートマップ データを表示します。

ステップ 9 [Playback] をクリックして、選択した日付のクライアントの移動を再生します。

スケジュール マネージャの使用

[Schedule Manager] ウィンドウを表示するには、Cisco CMX にログインし、[Analytics] > [Schedule] を選択します。 [Schedule Manager] ウィンドウが表示されます。このウィンドウには次の情報が表示されます。

- [Report ID]：スケジュール設定されたレポートのレポート ID を示します。
- [Report Title]：レポートのタイトルを示します。
- [Start From]：受信者へのレポートの電子メール送信を開始する日を示します。
- [Recipients]：受信者の電子メール アドレスを示します。
- [History]：過去のレポートのステータスを示します。
- [Actions]：スケジュール設定されたレポートを削除するには、[Delete] をクリックします。

業種設定

業種設定機能では、レポート生成で使用する階層の各レベルに関連付けられている名前を変更できます。 階層レベルの名前を変更できますが、既存の要素は、作成後に名前を変更することはできません。 このプロセスでの名前変更はグローバルであり、すべてのユーザに影響します。

業種設定の管理に関する詳細については、業種設定機能の管理, （99 ページ）を参照してください。

第 5 章

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 *2* : ***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, （51 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, （46 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 *3* : 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, （49 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, （52 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, （49 ページ）
2. Web パススルー認証の WLAN の設定, （50 ページ）
3. 組織の Facebook ページの作成, （51 ページ）
4. システムのデフォルト Facebook ページの割り当て, （52 ページ）
5. ロケーション固有の Facebook ページの割り当て, （52 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 *4* : *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, （49 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, （60 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 *5*：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 *6*：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, （49 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 *7*：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 *8*：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	—

第 6 章

Cisco CMX Presence Analytics サービス

• Presence Analytics のテーマの変更，81 ページ

Presence Analytics サービスの概要

Cisco Connected Mobile Experiences（Cisco CMX）の Presence Analytics サービスでは、小規模な導入環境（アクセス ポイント（AP）が 1 ～ 2 つだけの導入環境を含む）を運用する組織が、ワイヤレス テクノロジーを使用して顧客の行動を調査できます。

Cisco CMX Presence Analytics サービスは、AP を使用して、ビジターのモバイル デバイスの受信信号強度表示（RSSI）からビジターのプレゼンスを検出する、包括的な分析およびエンゲージメント プラットフォームです。 AP は、クライアント モバイル デバイスが指定された信号範囲内に存在し、かつモバイルデバイスでワイヤレスオプション（ネットワークに接続していないデバイスでもワイヤレスで検出できる機能）が有効になっている限り、ワイヤレス関連付けの状態に関係なくこれらのクライアント モバイル デバイスを検出します。

PRESENCEANALYTICSDashboard を使用して、特定のサイトでさまざまなクライアント モバイル デバイスの以下の重要業績評価指標（KPI）を確認できます。

- ビジター（Visitors）
- 平均滞在時間（Average Response Time）
- Peak Hour
- 通過者からビジターへのコンバージョン率（Passerby-to-visitor conversion rate）
- AP により検出された最も多いクライアント モバイル デバイスの製造元（Manufacturers of popular client mobile devices detected by AP）

これらの KPI は、現在の日付から 180 日以内の任意の期間（日、週、月、またはカスタム）で表示できます。 特定の日や週末のデータを表示するか、または 1 ヵ月にわたるトレンドを表示するように、表示内容をカスタマイズすることもできます。

Presence Analytics サービスのインストール

Presence Analytics サービスと Location サービスを同じボックスで実行することはできません。 したがって、初期インストール時に Location サービスまたは Presence Analytics サービスのいずれかを選択する必要があります。

Presence Analytics サービスの利点

- 小規模な導入環境（AP が 1 ～ 2 つだけの導入環境を含む）を運用する組織が、顧客の行動を把握できるようになります。
- さまざまなロケーション間での顧客のモバイル環境での行動を把握し、その情報からカスタマー エクスペリエンスを強化します。

- ロケーション統計情報に基づいて、さまざまなサイトにおける顧客エンゲージメントと顧客ロイヤルティを測定します。
- サイト間でビジターのトレンドを比較し、マーケティングアクションの効果を測定します。

初期設定

Cisco CMX Presence Analytics サービスを使用するには、Cisco MSE 仮想アプライアンスのインストール時に [Presence] オプションを選択します。 詳細については、『*Cisco MSE Virtual Appliance Installation Guide for Cisco CMX Release 10.2*』の「Installing a Cisco MSE Virtual Appliance」の項を参照してください。 インストールが完了したら、次の操作を行います。

- コントローラを追加します。
- サイトを追加します。
- AP を追加します。

Presence Analytics ダッシュボード

Presence Analytics ダッシュボードには以下のグラフが含まれています。

表 *9*：*Presence Analytics* のグラフ

グラフ	説明
インサイト（Insights）	特定の週または月における重要なインサイト（最もビジーな日、最もビジーな時間、ピーク日、ピーク カウントなど）を表示します。 （注） インサイト データにより、現在のサイトのメトリックを、前週または前月と比較できます。 これは、集計期間中にすべてのサイトを対象として日単位で計算されます。
Proximity	特定のサイトでの通過者、ビジター、接続デバイスなどの情報を時間単位（1 日または過去 3 日の場合）または日単位で表示します。
近接分布（Proximity Distribution）	通過者またはビジターなどに関する情報と、特定の期間における特定のサイトの接続率（%）を表示します。

グラフ	説明
滞在時間	時間別または日別のビジターの滞在レベルを表示します。 次の滞在レベルを表示できます。 5 ～ 30 分：サイトでの滞在時間が 5 ～ 30 分のビジター。 30 ～ 60 分：サイトでの滞在時間が 30 ～ 60 分のビジター。 1 ～ 5 時間：サイトでの滞在時間が 1 ～ 5 時間のビジター。 5 ～ 8 時間：サイトでの滞在時間が 5 ～ 8 時間のビジター。 8+時間：サイトでの滞在時間が 8 時間を超えるビジター。
滞在時間の分布	特定の期間における特定のサイトでのビジター滞在レベルの割合を表示します。
アクセスを繰り返すビジター	アクセスを繰り返すビジターを時間別または日別で表示します。アクセスを繰り返すビジターの次のカテゴリを確認できます。 [Daily]：選択されているサイトに、過去 7 日間のうち 5 日以上アクセスしたビジター。 [Weekly]：選択されているサイトに、過去 4 週間のうち 2 週間以上アクセスしたビジター。 [First Time]：選択されているサイトに初めてアクセスしたビジター。 [Occasional]：毎日、毎週、初回のいずれでもないビジター。 [Yesterday]：前日にサイトにアクセスしたビジター。
アクセスを繰り返すビジターの分布（Repeat Visitors Distribution）	アクセスを繰り返すビジターの分布の割合（%）を示します。

サイトの追加

新しいサイトを個別に追加するか、または.CSV形式のサイトのリストをアップロードして一括で追加することができます。

新しいサイトを追加するには、次のいずれかの方法を使用します。

- サイトを個別に追加する。 詳細については、個別のサイトの追加, （71 ページ）を参照してください。
- 複数のサイトを一括で追加する。 詳細については、サイトの一括での追加, （72 ページ）を参照してください。
- AP からサイトを作成する。 この方法では、管理者が AP を名前でフィルタリングし、新しいサイトに直接追加することでサイトを作成できます。 詳細については、サイトへの AP の追加, （74 ページ）を参照してください。

個別のサイトの追加

サイトを個別に追加するには、次の手順を実行します。

手順

ステップ 1 Cisco CMX にログインします。

ステップ 2 [PRESENCE ANALYTICS] > [MANAGE] を選択します。

ステップ 3 [Sites] タブをクリックします。

ステップ 4 [Add Site] をクリックします。

ステップ 5 [Name] フィールドに、サイトの名前を入力します。

ステップ 6 [Address] フィールドに、サイトのアドレスを入力します。

ステップ 7 クライアント デバイスがサイト内にとどまっているか、または単に通過しているだけであるかを判別するため、[Signal Strength Threshold] を設定します。 青色の円形ボタンを移動して、[Visitor Signal Threshold] と [Ignore Signal Threshold] の値を指定します。サイトに対して定義される 2 つの RSSI しきい値は、下限（デフォルトは -95 dBm）と上限（デフォルトは 65 dBm）です。

- RSSI が下限しきい値（デフォルトは - 95 dBm）よりも低いクライアントは破棄されます。
- RSSI が下限しきい値よりも高いクライアントは「通過中」として分類されます。
- 過去 20 分間のうち *x* 分（デフォルトは 5 分）以上にわたって RSSI が上限しきい値を超えているクライアントは、ビジターとして分類されます。
- サイト内の AP に関連付けられているクライアントは、そのサイトのビジターとして分類されます。

ステップ 8 [Configure the Minimum Dwell Time For Visitor (minutes)] フィールドに、ビジターの最小滞在時間を指定します。

ステップ 9 [Save] をクリックします。

サイトの一括での追加

手順

ステップ 1 Cisco CMX にログインします。

ステップ 2 [PRESENCE ANALYTICS] > [MANAGE] を選択します。

ステップ 3 [Import] をクリックします。

ステップ 4 [Sites] の下の [Browse] をクリックします。
[File Upload] ダイアログボックスが表示されます。

（注） サイト情報をインポートするためにアップロードするファイルは、.csv 形式である必要があります。

ステップ 5 アップロードする CSV ファイル（サイトのリストが含まれているファイル）の場所に移動し、[Open] をクリックします。 サイトの詳細情報を正しくインポートするため、サイトの情報をサイト名,アドレス,*RSSI* 上限しきい値,*RSSI* 下限しきい値,滞在時間（分数）の形式で、この順序で保存してください（例：*TestSite,123MainStreetCityCAUS,-65,-95,5*）。

ステップ 6 [Import] をクリックします。
一連の新しいサイトが作成され、[PRESENCE ANALYTICS] > [MANAGE] の下にあるサイトのテーブルに追加されます。

使用可能なサイトの表示

手順

ステップ 1 Cisco CMX にログインします。

ステップ 2 [PRESENCE ANALYTICS] > [MANAGE] を選択します。

ステップ 3 [Sites] タブに、使用可能なサイトのリストが表形式で表示されます。このリストはサイト名のアルファベット順にソートされています。[Sites] テーブルの表示をカスタマイズするには、[Location]、[Timezone]、または [AP count] に基づいてソートします。

既存のサイトの編集

手順

ステップ 1 Cisco CMX にログインします。

ステップ 2 [PRESENCE ANALYTICS] > [MANAGE] を選択します。

ステップ 3 [Sites] で、使用可能なサイトのテーブルに表示されている該当するサイトの名前をクリックします。
ダイアログボックスが表示されます。

ステップ 4 サイトの [Name]、[Address]、[Signal Strength Threshold] の制限、または [Minimum Dwell Time for Visitor] を編集します。

ステップ 5 [Save] をクリックします。

既存のサイトの削除

手順

ステップ 1 Cisco CMX にログインします。

ステップ 2 [PRESENCE ANALYTICS] > [MANAGE] を選択します。

ステップ 3 [Sites] で、削除するサイトのチェックボックスをオンにします。

ステップ 4 [Delete] をクリックします。
サイトを削除しようとすると、確認ダイアログボックスが表示されます。[OK] をクリックして、削除アクションを確認します。

（注） 使用可能なすべてのサイトを同時に削除する場合は、ヘッダー行のチェックボックスをオンにし、[Delete] をクリックします。

サイトの検索

手順

ステップ 1 Cisco CMX にログインします。

ステップ 2 [PRESENCE ANALYTICS] > [MANAGE] > [Sites] を選択します。

ステップ 3 ウィンドウ右上隅の [Search] フィールドにサイト名を入力し、Return キーを押します。 指定したサイトがすでに [PRESENCE ANALYTICS] に追加されている場合は、検索結果にそのサイトが表示されます。

AP の追加

新しい AP を個別に追加するか、または .CSV 形式の AP のリストをアップロードして一括で追加することができます。

マップの有無にかかわらず、次のいずれかの方法で新しい AP を追加できます。

- AP を個別に追加する：個々の AP を特定のサイトに追加します。 詳細については、サイトへの AP の追加, （74 ページ）を参照してください。
- 複数の AP を一括で追加する：.CSV 形式の AP のリストをインポートして、複数の AP を一括で追加します。 詳細については、AP の一括での追加, （75 ページ）を参照してください。

サイトへの AP の追加

（注） AP リストが表示されない場合は、[System] > [Settings] ウィンドウを使用して、WLC のコミュニティ ストリングを更新する必要があります。 AP 情報は SNMP を使用して WLC から取得されます。

手順

ステップ 1 Cisco CMX にログインします。

ステップ 2 AP を個別にサイトに追加するには、次の手順を実行します。

a) [PRESENCE ANALYTICS] > [MANAGE] > [Sites] を選択します。
b) 使用可能なサイトのテーブルで、新しい AP を関連付けるサイトの名前をクリックします。
c) [AP count] の横の [Details] アイコンをクリックします。

使用可能な AP のリストが表形式で表示されます。

d) 追加して指定のサイトに関連付ける AP の MAC アドレスを入力します。
e) [Add] をクリックします。
指定した AP が追加され、指定のサイトに関連付けられます。

ステップ 3 1 つ以上の AP を 1 つのサイトに追加するには、次の手順を実行します。

a) [PRESENCE ANALYTICS] > [MANAGE] > [Access Points] を選択します。
b) [APs by Controller] ドロップダウン リストから、サイトに追加する AP を選択します。
ドロップダウン リストからすべてのサイトを選択するには、**Ctrl+a** キーまたは **Command+a** キーを使用します。
c) AP を選択したら [Close] をクリックします。
使用可能な AP の中から選択した AP の数がドロップダウンリストに表示されます（例：[8 of 160 selected]）。
d) [Add to Site] をクリックします。
e) 選択した AP の追加先となるサイトを選択します。
f) [Add] をクリックします。
選択した AP が指定のサイトに追加され、このサイトに関連付けられます。

このページからサイトを作成するには、[Create Site] をクリックします。

ステップ 4 [Controller AP list] の下の [Download CSV] をクリックして .CSV ファイルをダウンロードし、AP の欠落しているサイト名を追加し、[Import] タブからファイルをもう一度インポートします。
CSV の形式：無線 MAC アドレス,イーサネット MAC アドレス,名前,サイト名,サイト アドレス

例：aa:bb:cc:dd:ee:ff,bb:cc:dd:ee:ff:11,AP-1,Site-1,123 Main St City CA US

AP の一括での追加

1 つのサイトに複数の AP を一括で追加するには、次の手順を実行します。

手順

ステップ 1 Cisco CMX にログインします。
ステップ 2 [PRESENCE ANALYTICS] > [MANAGE] > [Import] を選択します。
ステップ 3 [AP] の下の [Browse] をクリックします。
[File Upload] ダイアログボックスが表示されます。
ステップ 4 アップロードする .CSV ファイル（APのリストが含まれているファイル）の場所に移動し、[Open] をクリックします。

AP の詳細情報を正しくインポートするため、AP の情報を無線 *MAC* アドレス,イーサネット *MAC* アドレス,名前,サイト名,サイト アドレスの形式で、この順序で保存してください（例：*aa:bb:cc:dd:ee:ff,bb:cc:dd:ee:ff:11,AP-1,Site-1,123MainStCityCAUS*）。

ステップ 5 [Import] をクリックします。
一連の新しい AP が作成され、追加されます。

AP の削除

手順

ステップ 1 Cisco CMX にログインします。

ステップ 2 [PRESENCE ANALYTICS] > [MANAGE] > [Sites] を選択します。

ステップ 3 使用可能なサイトのテーブルで、削除して対応する AP の関連付けを解除するサイトの名前をクリックします。
ダイアログボックスが表示されます。

ステップ 4 [AP count] の横の [Details] アイコンをクリックします。
使用可能な AP のリストが表形式で表示されます。

ステップ 5 削除する AP の横にある [Delete] アイコンをクリックします。

指定した期間のサイトの詳細情報の表示

手順

ステップ 1 Cisco CMX にログインします。

ステップ 2 [PRESENCE ANALYTICS] をクリックします。

ステップ 3 [SITE] 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 [Date] ドロップダウン リストから期間を選択します。 次のオプションの中から選択できます。

- [Today]
- [Yesterday]
- [Last 3 Days]
- [Last 7 Days]
- Last 30 Days

- [This Month]
- [Last Month]
- [Custom]：日付範囲を指定して [Change] をクリックします。 [FROM] フィールドと [TO] フィールドに日付を yyyy-mm-dd 形式で手動で入力するか、または該当するカレンダーから日付を選択します。 これらのカレンダーは、[Custom] を選択するか、[FROM] フィールドまたは [TO] フィールドをクリックすると、表示されます。 ウィンドウが更新され、選択内容に基づいてサイトの KPI が表示されます。

  （注） [FROM] フィールドと [TO] フィールドで同じ日付を選択すると、単一の日を選択できます。

KPI サマリの表示

ウィンドウ上部に表示される次の KPI ボタンのいずれかをクリックすると、サイトでのビジターの行動の詳細が表示されます。

- [Visitors]：サイト内の AP に関連付けられているクライアントは、サイトのビジターとして分類されます。
- [Average Dwell Time]：ロケーションにおけるすべてのビジターの平均滞在時間または待機時間。
- [Peak Hour]：ロケーションで検出されたビジターの数が最も多かった時間。
- [Conversion Rate]：コンバージョン率は、ビジターになった通過者の割合です。これは、ビジター数/（ビジター数 + 通過者数）X 100 として算出されます。
- [Top Device Maker]：AP により検出された最も多いクライアント モバイル デバイスのデバイス製造元。

特定のサイトのデバイスプロキシミティ、数、分布の表示

手順

ステップ 1 Cisco CMX にログインします。
ステップ 2 [PRESENCE ANALYTICS] をクリックします。
ステップ 3 [SITE] 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 [Date] ドロップダウン リストから期間を選択または指定します。

ウィンドウが更新され、選択内容に基づいてサイトの詳細情報が表示されます。

ステップ 5 [Proximity] または [Proximity Duration] グラフ内で該当する要素をクリックします。指定した期間中の選択したサイトでの通過者、ビジター、接続デバイスの 1 時間ごとの内訳が表示されます。

（注） **ステップ 4** で選択した期間が 1 日よりも長い場合は、[Proximity] グラフの要素をクリックすると、特定の日付での選択したサイトの詳細情報が表示されます。

レポートの電子メール送信

手順

ステップ 1 Cisco CMX にログインします。

ステップ 2 [PRESENCE ANALYTICS] をクリックします。

ステップ 3 [Email] アイコンをクリックします。

ステップ 4 受信者の電子メール アドレスを入力します。

ステップ 5 メモがある場合は入力します。

ステップ 6 [Send] をクリックします。
この電子メールを後で送信する場合は、[Schedule] チェックボックスをオンにし、スケジュール パラメータ（[Start From]（日時）、[Frequency]（[Daily] または [Weekly] など）を入力し、[Schedule] をもう一度クリックします。

レポートの印刷

手順

ステップ 1 Cisco CMX にログインします。

ステップ 2 [PRESENCE ANALYTICS] をクリックします。

ステップ 3 [Printer] アイコンをクリックします。

ステップ 4 プリンタ設定を指定します。

ステップ 5 [OK] をクリックします。

PDF レポートの生成

（注） PDF レポートのロゴをカスタマイズできます。 アーカイブ済みのレポートを表示するには、[PRESENCE ANALYTICS] > [MANAGE] > [Reports] を選択します。

手順

ステップ 1 Cisco CMX にログインします。

ステップ 2 [PRESENCE ANALYTICS] をクリックします。

ステップ 3 [PDF Report] アイコンをクリックします。

ステップ 4 PDF レポートのメモがある場合は入力します。

ステップ 5 受信者の電子メール アドレス（オプション）を入力します。 レポートの受信者が複数いる場合は、電子メール アドレスをコンマで区切って入力します。

ステップ 6 [Submit] をクリックします。
PDF レポートを将来の日付でスケジュールする場合は、[Schedule] チェックボックスをオンにし、スケジュール パラメータ（[Start From]（日時）、[Frequency]（[Daily] または [Weekly]）など）を入力し、[Schedule] をクリックします。

レポートの管理

Presence Analytics サービスでは、スケジュール設定されたレポートと生成されたレポートを管理できます。 また、生成される PDF レポートに表示するロゴをカスタマイズできます。

[Reports] ウィンドウには、次のエリアがあります。

- [Report Logo]：PDF レポートのロゴとして使用可能な画像ファイルをアップロードできます。
- [Scheduled Reports]：すでにスケジュール設定されているレポート（電子メールまたは PDF）を変更または削除できます。
- [Generated PDF Reports]：生成済み PDF レポートをダウンロードまたは削除できます。

  - レポートのロゴをアップロードするには、次の手順を実行します。
    a) Cisco CMX にログインします。
    b) [PRESENCE ANALYTICS] > [MANAGE] をクリックします。
    c) [Reports] をクリックします。
    d) [Report Logo] エリアで [Browse] をクリックし、レポート ロゴとしてアップロードする画像ファイルを選択します。

e) [Upload] をクリックします。

- スケジュール設定されたレポートを編集または削除するには、次の手順を実行します。
  a) Cisco CMX にログインします。
  b) [PRESENCE ANALYTICS] > [MANAGE] をクリックします。
  c) [Reports] をクリックします。
  d) [Scheduled Reports] エリアの [Link] カラムの [Edit] または [Delete] をクリックします。スケジュール設定されたレポートを編集することを選択すると、[EDIT SCHEDULED REPORT] ウィンドウに既存のスケジュールの詳細が表示され、必要に応じて変更できます。

- 生成済み PDF レポートをダウンロードまたは削除するには、次の手順を実行します。
  a) Cisco CMX にログインします。
  b) [PRESENCE ANALYTICS] > [MANAGE] をクリックします。
  c) [Reports] をクリックします。
  d) [Generated Reports] エリアの [Link] カラムの [Download] または [Delete] をクリックします。

フィルタ パラメータの指定

[Filter Parameters] タブでは、特定の SSID、MAC アドレス、または定義されている期間からのデータを除外できます。

手順

ステップ 1 Cisco CMX にログインします。
ステップ 2 [PRESENCE ANALYTICS] > [MANAGE] > [Filters] を選択します。
ステップ 3 データを除外するため、[Enable Exclusion Filters] チェックボックスをオンにします。
ステップ 4 [Save] をクリックします。

グローバル サイトの有効化

グローバル サイトを有効にすると、すべての個別サイトの既存データが 1 つの大きなサイトにまとめられます。これにより、すべてのサイトのデータを一度に確認できます。 グローバルサイトのタイムゾーンを指定する必要があります。このタイムゾーンは、個々のすべてのサイトのタイム ゾーンを上書きします。 すべての分析は、グローバル サイトに定義されているタイム ゾーンのコンテキストになります。

手順

ステップ 1 Cisco CMX にログインします。
ステップ 2 [PRESENCE ANALYTICS] > [MANAGE] > [Global Sites] を選択します。
ステップ 3 [Enable Global Site] チェックボックスをオンにします。
ステップ 4 [Site Name]、[Address]、および [Time Zone] を指定します。
ステップ 5 [Save] をクリックします。

サイト グループの作成

サイト グループにより、複数サイト（例：同一タイムゾーンのすべてのサイト）からの情報を分析目的で結合できます。

手順

ステップ 1 Cisco CMX にログインします。
ステップ 2 [PRESENCE ANALYTICS] > [MANAGE] > [Site Groups] を選択します。
ステップ 3 [Create Group] をクリックします。
ステップ 4 [Group Name]、[Address]、[Timezone]、[Sites] を指定します。
ステップ 5 [Save] をクリックします。

Presence Analytics のテーマの変更

手順

ステップ 1 Cisco CMX にログインします。
ステップ 2 [PRESENCE ANALYTICS] をクリックします。
ステップ 3 [THEMES] アイコンをクリックします。
ステップ 4 目的のテーマを選択します。

第 7 章

CiscoCMXのコンフィギュレーションの管理

Manage サービスの概要

Cisco Connected Mobile Experiences（Cisco CMX）の MANAGE サービスは次のタブで構成されています。これらのタブでは、次に示す設定をはじめとする Cisco CMX の設定を効率的に管理できます。

- [Locations]：ロケーションのゾーンとタグを管理、追加できます。
- [BLE Beacons]：Bluetooth Low Energy（BLE）ビーコンを管理、追加できます。
- [Notifications]：電子メール通知と HTTP 通知を管理、追加できます。
- [Licenses]：ライセンスを管理、追加できます。
- [Users]：ユーザを管理、追加できます。

（注） Manage サービスのすべてのタスクは、該当するユーザ ロールが割り当てられているユーザだけが実行できます。 ユーザ ロールの詳細については、ユーザ ロール，（85 ページ）を参照してください。

ライセンスの管理

Cisco Connected Mobile Experiences（Cisco CMX）システムのライセンスのリストを表示するには、Cisco CMX にログインし、[MANAGE] > [Licenses] を選択します。 [Licenses] ウィンドウに、ライセンスのリストが表示されます。

Cisco CMX を運用するために必要なライセンスについては、『Cisco CMX 10.2 Ordering and Licensing Guide』を参照してください。

（注） Cisco CMX リリース 10.2 には、すべての機能を利用できる 120 日間の評価ライセンスが付属しています。 Cisco CMX に接続しているすべてのアクセス ポイント（AP）もライセンスを取得する必要があります。

ライセンスの追加

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] > [Licenses] を選択します。

ステップ 3 [Licenses] ウィンドウで、[See Installed Licenses] をクリックし、インストールされているライセンスのリストを表示します。

ステップ 4 [Add License] をクリックします。
[UPLOAD LICENSE] ダイアログボックスが表示されます。

ステップ 5 [Browse] をクリックして対応するライセンス ファイルを選択し、[Upload] をクリックします。

ライセンスの削除

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] > [Licenses] を選択します。

ステップ 3 [Licenses] ウィンドウで、[See Installed Licenses] をクリックし、インストールされているライセンスのリストを表示します。

ステップ 4 削除するライセンスの隣にある [Action] カラムで [Delete] をクリックします。

[DELETE LICENSE] ダイアログボックスが表示されます。

ステップ 5 [DELETE LICENSE] をクリックして、削除を実行します。

ユーザの管理

Cisco Connected Mobile Experiences（Cisco CMX）には、デフォルトの管理ユーザ アカウントとパスワードが付属しています。 管理ユーザは他のユーザを追加、編集、および削除できます。

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。
[Users] ウィンドウが表示されます。このウィンドウには現行ユーザがすべて表示されます。

ステップ 3 テーブル下部にある [New User] をクリックします。
[Add New User] ダイアログボックスが表示されます。

ステップ 4 詳細を入力し、[Roles] ドロップダウン リストからそのユーザに割り当てる 1 つ以上のロールを選択します。
選択可能なロールについては「ユーザ ロール」を参照してください。

ステップ 5 [Submit] をクリックします。`

ユーザ ロール

Cisco Connected Mobile Experiences（Cisco CMX）システムには、該当ライセンスを所有しているかどうかに応じて、以下のサービスが含まれます。

- SYSTEM サービス（Cisco CMX Base ライセンスに含まれる）
- MANAGE サービス（Cisco CMX Base ライセンスに含まれる）
- DETECT & LOCATE サービス（Cisco CMX Base ライセンスに含まれる）
- CONNECT & ENGAGE サービス（Cisco CMX Base ライセンスに含まれる）
- ANALYTICS サービス（Cisco CMX Advanced ライセンスにのみ含まれる、Cisco CMX Base ライセンスには含まれない）

Cisco CMX でユーザを設定するときに、各ユーザに対して 1 つ以上のロールを選択できます。 各ロールは、ご利用のライセンスに含まれている 1 つ以上のサービスへのアクセス権限を提供します。

各ロールに関連付けられているアクセス権限の説明については、次の表を参照してください。

表 *10*：ユーザ ロールに関連付けられているアクセス権限

ロール	アクセス権限
Admin	すべてのサービスへの読み取り/書き込みアクセス権
システム	SYSTEM サービスへの読み取り/書き込みアクセス権
Manage	MANAGE サービスへの読み取り/書き込みアクセス権
場所	DETECT & LOCATE サービスへの読み取り/書き込みアクセス権
分析[ぶんせき]	ANALYTICS サービスへの読み取り/書き込みアクセス権
Connect	CONNECT & ENGAGE サービスへの読み取り/書き込みアクセス権
Connect Experience	• CONNECT & ENGAGE サービスの Connect Experience への読み取り/書き込みアクセス権 • CONNECT & ENGAGE サービスのすべての設定への読み取り専用アクセス権 • CONNECT & ENGAGE サービスのダッシュボードへはアクセスできません
Read Only	すべてのサービスへの読み取り専用アクセス。

（注）

- ユーザに割り当てることができるロールは、System、Manage、Location、Analytics、および Connect です。 これにより、ユーザは管理ユーザとして機能できます。 管理ユーザは非管理ユーザを削除できますが、非管理ユーザが管理ユーザを削除することはできません。
- 管理ユーザを削除できるのは他の管理ユーザだけです。

デフォルト admin パスワードの変更

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。
[Users] ウィンドウが表示されます。このウィンドウでは、新規ユーザを追加し、既存ユーザのロールを変更することができます。

ステップ 3 管理ユーザの隣にある [Action] カラムの [Edit] をクリックします。
これにより、その管理ユーザの [EDIT USER] ダイアログボックスが表示されます。

ステップ 4 デフォルトの初期設定 admin パスワードを変更します。

ステップ 5 [Submit] をクリックします。`

ユーザ情報の編集

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。
[Users] ウィンドウが表示されます。このウィンドウには現行ユーザがすべて表示されます。

ステップ 3 詳細情報を編集するユーザの隣にある [Actions] カラムで、[Edit] をクリックします。
[EDIT USER] ダイアログボックスが表示されます。

ステップ 4 ユーザの詳細情報を編集します。 ユーザ名は編集できないことに注意してください。
ユーザ ロールの詳細については、ユーザ ロール，（85 ページ）を参照してください。

ステップ 5 [Submit] をクリックします。`

ユーザの削除

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 詳細情報を削除するユーザの隣にある [Actions] カラムで、[Delete] をクリックします。

[DELETE USER] 確認ダイアログボックスが表示されます。

ステップ 4 [DELETE USER] をクリックして、削除を実行します。

ロケーション マップでの境界とゾーンの管理

境界とは、クライアントが常にその内部に存在する包括的なゾーンです。 個々のゾーンが境界の内部にあります。

- キャンパス、ビル、フロア、ゾーンの詳細情報の表示
- 境界の作成
- 境界の削除
- 境界の編集
- ゾーンの作成
- ゾーンの削除
- ゾーンの編集

キャンパス、ビル、フロア、ゾーンの詳細情報の表示

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] > [Locations] を選択します。

ステップ 3 表示されるウィンドウの左側のペインで、表示するエリアに応じて [Campus]、[Building]、[Floor]、または [Zone] をクリックします。
選択したエリアに対応する項目がボックスとして表示されます。

ステップ 4 各項目ボックスの右上隅にある曲がった矢印をクリックして、その項目の詳細情報を表示します。これにより、[Zone Editor] マップ ビューが表示され、このビューにフロア マップが表示されます。

（注） フロア ボックスの右上隅にある曲がった矢印は、[Go to map view] 矢印と呼ばれます。この矢印は、すべてのレベルの項目ボックスで使用可能です。 たとえばビルの場合、1 階のフロアが開きます。 キャンパスの場合、最初のビルの 1 階のフロアが開きます。その後そのキャンパス内の他のビルとフロアに切り替えることができます。

境界の作成

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] > [Locations] を選択します。

ステップ 3 表示されるウィンドウの左側のペインで、[Zone] をクリックします。
[Zone Item] のボックスが表示されます。

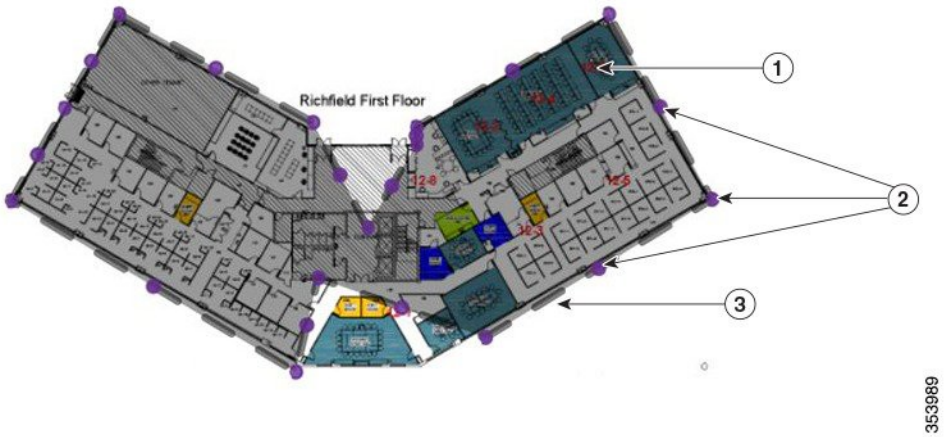
ステップ 4 対応するゾーンのサブゾーンをクリックします。

ステップ 5 [Zone Editor] ウィンドウで [CREATE A PERIMETER] アイコンをクリックします。
カーソルが描画ツールに変化します。

ステップ 6 境界の頂点にする各点をクリックします。 最後の頂点をダブルクリックします。境界の頂点のマーキングが完了し、境界が閉じます。
最後の頂点をダブルクリックすると、[CREATE A PERIMETER] ダイアログボックスが表示されます。

ステップ 7 [Add] をクリックして、境界をフロアに追加します。

図 *1*：境界とその頂点



1	境界で囲まれたエリアを示す濃い灰色の領域。	**3**	境界を示す濃い灰色の線。
2	境界の頂点を示す紫色の点。		

境界の削除

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] > [Locations] を選択します。

ステップ 3 表示されるウィンドウの左側のペインで、[Zone] をクリックします。
[Zone Item] のボックスが表示されます。

ステップ 4 対応するゾーンのサブゾーンをクリックします。

ステップ 5 [Zone Editor] ウィンドウで [Edit Perimeter] アイコンをクリックします。

ステップ 6 削除する境界の内側をクリックします。
境界は灰色で強調表示されます。

ステップ 7 [Trash] アイコンをクリックします。

ステップ 8 [DELETE PERIMETER] 確認ダイアログボックスで、[Confirm] をクリックして境界を削除します。

境界の編集

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] > [Locations] を選択します。

ステップ 3 表示されるウィンドウの左側のペインで、[Zone] をクリックします。
[Zone Item] のボックスが表示されます。

ステップ 4 対応するゾーンのサブゾーンをクリックします。

ステップ 5 [Zone Editor] ウィンドウで [Edit Perimeter] アイコンをクリックします。

ステップ 6 編集する境界の内側をクリックします。
境界は灰色で、頂点は紫色で強調表示されます。

ステップ 7 紫色の頂点をドラッグして、境界の形状を変更します。

ステップ 8 必要な形状になったら、境界の外側をクリックします。 これで新しい形状が保存されます。

ゾーンの作成

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] > [Locations] を選択します。

ステップ 3 表示されるウィンドウの左側のペインで、[Zone] をクリックします。
[Zone Item] のボックスが表示されます。

ステップ 4 対応するゾーンのサブゾーンをクリックします。

ステップ 5 [Zone Editor] ウィンドウで [Draw Polygon Zone] アイコンをクリックします。
カーソルが描画ツールに変化します。

ステップ 6 境界の頂点にする各点をクリックします。 最後の頂点をダブルクリックします。境界の頂点のマーキングが完了し、境界が閉じます。次の図を参照してください。
最後の頂点をダブルクリックすると、[CREATE A NEW ZONE] ダイアログボックスが表示されます。

ステップ 7 [Add] をクリックして、ゾーンを該当するフロアに追加します。
ウィンドウ右側に、このゾーンに関連する [Item] ペインが表示されます。 ドロップダウン リストから既存のタグを追加するか、または新しいタグを追加することができます。

（注） ゾーンをフロア マップの外側に移動すること、またはゾーンを重ね合わせることはできません。 重なり合ったゾーンを作成するには、Cisco Prime Infrastructure を使用します。

図 *2*：ゾーンとその頂点

1	Lab という名前のゾーン。	**3**	ゾーンの頂点を示す紫色の点。
2	境界を示す灰色の線。	**4**	マップの他のゾーン。

ゾーンの削除

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] > [Locations] を選択します。

ステップ 3 表示されるウィンドウの左側のペインで、削除するゾーンに移動します。

ステップ 4 [Trash] アイコンをクリックします。
[DELETE ZONE] 確認ダイアログボックスが表示されます。

ステップ 5 [Confirm] をクリックします。

ゾーンの編集

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] > [Locations] を選択します。

ステップ 3 表示されるウィンドウの左側のペインで、[Zone] をクリックします。
[Zone Item] のボックスが表示されます。

ステップ 4 対応するゾーンのサブゾーンをクリックします。

ステップ 5 [Zone Editor] ウィンドウで [Gear] アイコンをクリックし、ゾーン編集オプションを表示します。

ステップ 6 ゾーンの形状を変更するには、[Pencil] アイコンを使用し、頂点を移動してゾーンの形状を変更します。
[DELETE ZONE] 確認ダイアログボックスが表示されます。

ステップ 7 ゾーンを移動するには、[Hand] アイコンで示されるドラッグ ツールを使ってゾーンをドラッグします。 [Hand] アイコンをクリックし、ゾーン中心へカーソルを移動します。ゾーン中心ではアイコンが [Arrow] アイコンに変わります。 これでゾーンをドラッグできます。

ステップ 8 ゾーンの外側をクリックし、変更内容を保存します。

（注） ゾーンをフロア マップの外側に移動すること、またはゾーンを重ね合わせることはできません。 重なり合ったゾーンを作成するには、Cisco Prime Infrastructure を使用します。

BLE ビーコンの管理

Bluetooth Low Energy（BLE）ビーコンは、近接位置に存在する Bluetooth 対応モバイル デバイスと連携するために使用されます。

（注） Cisco CMX には、アクセス ポイント（AP）を使用してビーコンの現在位置を表示できる機能があります。 Cisco CMX は、ビーコンが不明であるか、または配置が誤っているかどうかを判別できます。

BLE ビーコン機能を使用するには、[MANAGE] > [BLE Beacons] を選択します。 [Beacons Activity Map] ウィンドウが開きます。このウィンドウでは以下の操作を実行できます。

- ビーコンの数と、各ビーコンのステータスと位置を確認する。 ビーコンのステータスは、アイコンの色によって示されます。これについては以下の表に示します。
- 特定のフロアのすべての BLE ビーコンの位置を追跡する。
- フロア マップに BLE ビーコンを配置する。

表 *11*：ビーコンのステータス

ビーコン ステータスアイコン	意味	説明
	未配置（Unplaced）	新しく作成されたが、まだ配置されていないビーコン。 マップの左上隅に配置されます。
緑色のアイコン	既知（Known）	定義され配置されているか、または [Rogue] ステータスから変換されたビーコン。
赤色のアイコン	Missing	ビーコンのネットワーク ステータスが非アクティブであるために [Missing] としてマークされているビーコン。
青色のアイコン	誤配置（Misplaced）	確度範囲外に移動されたビーコン。 たとえば、確度範囲が 1.5 m（5 フィート）であり、検出された現在位置が、設定されている位置の半径 1.5m（5 フィート）よりも外側である場合などです。
黄色のアイコン	不正（Rogue）	新たに検出されたが、[Known] ステータスに変更されていないか、または未定義のビーコン。

マップへのビーコンの追加

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] > [BLE Beacons] を選択します。

ステップ 3 左側のペインで、フロア レベルまでドリルダウンし、ビーコンを追加するフロアをクリックします。

ステップ 4 表示される [Beacons Activity Map] ウィンドウで、[New Beacon] をクリックします。

ステップ 5 表示される [CREATE A NEW BEACON] ダイアログボックスで、ビーコンの詳細を入力して [Add] をクリックします。
新しいビーコンが配置可能な状態でマップの左上隅に表示されます。

ステップ 6 新しいビーコンを、マップ上の目的のロケーションにドラッグします。

ビーコンの削除

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] > [BLE Beacons] を選択します。

ステップ 3 左側のペインで、フロア レベルまでドリルダウンし、ビーコンを追加するフロアをクリックします。

ステップ 4 表示される [Beacons Activity Map] ウィンドウで、削除するビーコンをクリックします。
そのビーコンの詳細情報を示すスライドアウト ペインが表示されます。

ステップ 5 スライドアウト ペインの [Trash] アイコンをクリックし、ビーコンを削除します。

ビーコン名の変更

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] > [BLE Beacons] を選択します。

ステップ 3 左側のペインで、フロア レベルまでドリルダウンし、ビーコンの名前を変更するフロアをクリックします。

ステップ 4 表示される [Beacons Activity Map] ウィンドウで、名前を変更するビーコンをクリックします。そのビーコンの詳細情報を示すスライドアウト ペインが表示されます。

ステップ 5 現在の名前の隣にある [Edit] アイコンをクリックし、名前を変更します。

不正なビーコンから既知のビーコンへの変換

（注） 新たに検出されるビーコンはすべて「不正」としてマークされます。

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] > [BLE Beacons] を選択します。

ステップ 3 左側のペインで、フロア レベルまでドリルダウンし、ビーコンを追加するフロアをクリックします。

ステップ 4 表示される [Beacons Activity Map] ウィンドウで、変換する不正なビーコンをクリックします。そのビーコンの詳細情報を示すスライドアウト ペインが表示されます。

ステップ 5 [Convert to Known] をクリックします。

アプリケーションからの通知の管理

各自のアプリケーションとサードパーティアプリケーションの通知を設定できます。通知機能では以下がサポートされています。

- HTTP レシーバ
- MAC アドレスのスクランブル処理（デフォルトで有効）

- 2 つのメッセージ形式（JSON と XML）
- Alerts
- 受信信号強度インジケータ（RSSI）タグのストリーム通知
- ネットワーク構成変更の通知
- HTTPS 経由での REST 通知

ここでは、実行できる通知関連の作業について説明します。

- 新規通知の作成，（97 ページ）
- 通知の変更，（98 ページ）

新規通知の作成

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] > [Notifications] を選択します。
[Notifications] ウィンドウが表示されます。

ステップ 3 [New Notification] をクリックします。
[CREATE NEW NOTIFICATION] ダイアログボックスが表示されます。

ステップ 4 通知の名前を入力し、詳細情報を入力します。
使用可能な通知タイプの説明については、次の表を参照してください。 詳細情報を指定するときには次の点に注意してください。

- ロケーション階層を選択した場合、階層はその通知の特定のエリア フィルタになります。
- MAC アドレスを入力する場合、MAC アドレスがその通知のフィルタになります。

表 *12*：通知タイプ

通知タイプ	用途
[Association]	クライアントが関連付けまたは関連付け解除されると通知が生成されます。
[Beacon Movement]	BLE ビーコンの移動距離が指定した距離を超えると通知が生成されます。
[Absence]	クライアントが 15 分経過しても検出されない場合に通知が生成されます。

通知タイプ	用途
[Location Update]	デバイスのロケーションの再計算時に通知が生成されます。 [Location Update] 通知は、デバイスを検出するさまざまな AP からの RSSI に基づいています。
[In / Out]	デバイスがロケーション階層の特定のエリア内に移動するか、そのエリアから外へ移動する場合に、通知が生成されます。
[Beacon Absence]	BLE ビーコンが 5 分以上経過しても検出されない場合に通知が生成されます。
[Movement]	デバイスの移動距離が指定した距離を超えると通知が生成されます。
[Area Change]	デバイスの位置がキャンパス、ビル、またはフロア間で変更される場合に、通知が生成されます。
[Stream Notification for RSSI tag]	RSSI タグ通知を有効にします。
[Network Configuration Change]	マップが変更されると通知が生成されます。
[REST Notification over HTTPS]	HTTPS 経由での REST 通知を有効にします。

通知の変更

（注） 管理ユーザ以外のユーザは、各自が作成した通知だけを変更できます。 管理ユーザ以外のユーザは、他のユーザが作成した通知を変更することはできません。

通知に対して行うことができる変更は以下のとおりです。

- 通知の有効化と無効化, （99 ページ）
- 通知の編集, （99 ページ）
- 通知の削除, （99 ページ）

通知の有効化と無効化

通知の作成時に、通知はデフォルトで有効になります。

- 通知を無効にするには、[Notifications] ウィンドウで通知の隣にある [Status] カラムの [Enabled] をクリックします。
  ラベルが [Disabled] に変更され、通知が無効になります。
- 通知を有効にするには、[Notifications] ウィンドウで通知の隣にある [Status] カラムの [Disabled] をクリックします。
  ラベルが [Enabled] に変更され、通知が有効になります。

通知の編集

手順

ステップ 1 通知を編集するには、[Notifications] ウィンドウで通知の隣にある [Actions] カラムの [Edit] をクリックします。
[EDIT NOTIFICATION] ダイアログボックスが表示されます。

ステップ 2 必要に応じて通知の詳細情報を編集します。
（注） 通知の名前は編集できません。

通知の削除

注意 通知削除アクションは即時に反映され、削除を確認するダイアログボックスは表示されません。

手順

通知を削除するには、[Notifications] ウィンドウで通知の隣にある [Actions] カラムの [Delete] をクリックします。 通知が即時に削除されます。

業種設定機能の管理

Cisco CMX Analytics に含まれているレポート生成機能では、特定の業種において最も重要なメトリックを使用したレポートを自動的に生成できます。 業種を選択することで、事前に定義されているレポートを利用できます。この事前定義レポートにより、ネットワークのセットアップ対象

の業種に基づいて、十分な情報を得たうえでの意思決定が可能になります。 この機能は「業種設定機能」と呼ばれます。

業種をカスタマイズすると、その業種の要件に対応した有用なレポートを迅速に生成できます。カスタマイズされた業種は、各自の業種に適した正しいタグを使用して設定することもできます。CMX Analytics の業種設定機能により、その業種に固有のエンティティ名をカスタマイズできます。 選択する業種によっては、CMX Analytics 業種設定機能でカスタム レポートを生成できます。

Cisco CMX でサポートされている業種の一部と、各業種のレポートを次に示します。

- デフォルト
  - ビジター数（Visitor Count）
  - 接続クライアント数（Connected Clients）
  - 平均滞在時間（Average Response Time）
  - ロケーション相関（Location Correlation）
  - 最も人気のあるゾーン（Most Popular Zones）
  - Path Analysis
- Retail
  - 店舗タイプの人気度（Store Type Popularity）
  - 平均ショッピング時間（Average Shopping Time）
  - 最も人気のある入口（Most Popular Entrance）
  - 最も人気のある部門（Most Popular Department）
  - 部門間の移動（Department Transition）
  - フットボール（Footfall）
- サービス業
  - 最も人気の高いレストラン（Most Popular Restaurant）
  - 接続クライアント数（Connected Clients）
  - 最も多く使用されている施設（Most Used Amenity）
  - ローカル相関（Local Correlation）
  - 使用時間が最も長い施設（Longest Used Amenity）
  - Path Analysis
- Education
  - 廊下と教室（Corridors vs Classroom）
  - 接続クライアント数（Connected Clients）

- ホールあたりの食事客数（Diners per Hall）
- ローカル相関（Local Correlation）
- 図書館滞在時間（Library Time）
- Path Analysis

- 医療
  - ビジター数（Visitor Count）
  - 接続クライアント数（Connected Clients）
  - 最も多忙な部門（Busiest Department）
  - 待ち時間（Wait Times）
  - カフェテリアあたりの食事客数（Diners per Cafeteria）
  - Path Analysis

- モール（Mall）
  - 店舗タイプの人気度（Store Type Popularity）
  - 平均ショッピング時間（Average Shopping Time）
  - 最も人気のある入口（Most Popular Entrance）
  - 最も人気の高いレストラン（Most Popular Restaurant）
  - 部門間の移動（Department Transition）
  - フットボール（Footfall）

業種のカスタマイズ

業種のカスタマイズとは、各自のビジネスに基づいて業種のエンティティの名前を変更することです。業種を最適化するには、固有のニーズに合わせて業種をカスタマイズします。カスタマイズには、業種の階層の名前変更、アイコンの関連付け、タグライブラリの作成、タグロケーションの指定などがあります。

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] > [Verticalization] を選択します。
[Verticalization] ウィンドウに、サポートされている業種のリストが表示されます。

ステップ 3 業種を選択するため、その業種に対応するアイコンをクリックします。

選択した業種で使用可能なカスタム ウィジェットが表示されます。

ステップ 4 [Run Startup Wizard] をクリックします。
セットアップ ウィザードに、業種の最適化とカスタマイズの実行に必要な手順が表示されます。

ステップ 5 [Get Started] をクリックします。

ステップ 6 最初のステップでは、業種の階層を設定できます。 ウィザードの指示に従って、アイコンを選択します。 階層名と関連付けられているアイコンを承認する場合は、[Skip Step] をクリックします。 ウィザードでは、その業種のすべての階層についてこの操作が繰り返されます。

ステップ 7 階層のカスタマイズが完了したら、変更内容を確認し、[Save] をクリックします。

ステップ 8 [Continue] をクリックします。

ステップ 9 タグを使用して、ロケーションとデバイスを分類します。 [Continue] をクリックしてタグを設定します。

ステップ 10 選択した業種に応じて、その業種に固有のタグの一覧が表示されます。 作成するタグを選択するため、そのタグに対応するボタンをクリックします。 セットアップ ウィザードによりタグが作成されます。 [Continue] をクリックします。

ステップ 11 ロケーション タグは、階層に基づいて固有のロケーションに適用されます。 セットアップ ウィザードは、業種の階層でこの操作を繰り返します。 タグ付けする階層を選択するため、対応する名前をクリックします。 右側のペインに、ゾーンアイテム名と、選択できるタグの一覧が表示されます。 ゾーンに適切なタグを選択します。 [Continue] をクリックします。

ステップ 12 [Create a Report] をクリックします。
[Analytics Reports] ウィンドウに、業種のカスタム ウィザードの一覧が表示されます。

GUI の設定

GUI では、マップ、Cisco WLC、およびメール サーバを設定できます。

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 [SYSTEM] をクリックします。
[SETUP ASSISTANT] ウィンドウが表示されます。

ステップ 3 [Next] をクリックし、[New UI Password] を設定します。
[Maps and Controllers] ウィンドウが表示されます。

ステップ 4 [Default] または [Advanced] オプションのいずれかを選択します。

- [Default] ウィンドウでは、Cisco Prime Infrastructure のクレデンシャル（ユーザ名、パスワード、IP アドレスなど）を入力し、[Import Controllers and Maps] をクリックします。 これにより、Cisco Prime Infrastructure からコントローラとマップがインポートされます。
- [Advanced] ウィンドウでは、マップと Cisco WLC の情報を入力し、[Next] をクリックします。

（注） [Override] チェックボックスがオンの場合、インポートによって既存のエントリが上書きされます。

ステップ 5 表示される [Mail Server] ウィンドウに、対応する詳細情報を入力します。

ステップ 6 [Next] をクリックして、設定を完了します。

root ユーザの変更

Cisco CMX 10.2 以前のリリースでは、すべてのプロセスが root ユーザ ロールを使用していました。 これは Cisco CMX 10.2 で変更され、2 つの新しいユーザ ロール（cmx と cmxadmin）が導入されました。 cmx ユーザは、postgres 以外のすべてのプロセスを所有する no-login ユーザです。 cmxadmin は、すべての管理タスクを実行するプライマリ ユーザです。

root ユーザは無効になっていないので、インストールとデバッグに引き続き利用できます。 SSH または コンソールで root に直接ログインすることはできません。 最初に cmxadmin としてログインし、**su** コマンドを発行して root ユーザ レベルに移動します。

注意 Cisco Technical Assistance Center の担当者から指示された場合をのぞき、root ユーザ アカウントは使用しないでください。

第 8 章

Cisco CMX のシステム設定の管理

System サービスの概要

Cisco CMX の System サービスは次のタブで構成されています。これらのタブでは、次に示すタスクをはじめとするさまざまなシステム関連タスクを実行できます。

- [Dashboard]：システムの全体的な情報を把握できます。
- [Alerts]：ライブ アラートを確認できます。
- [Patterns]：さまざまな条件（[Client Count]、[CPU Usage]、[Memory Usage] など）のパターンを検出できます。
- [Metrics]：システム メトリックを確認できます。

システム全体の状態の表示

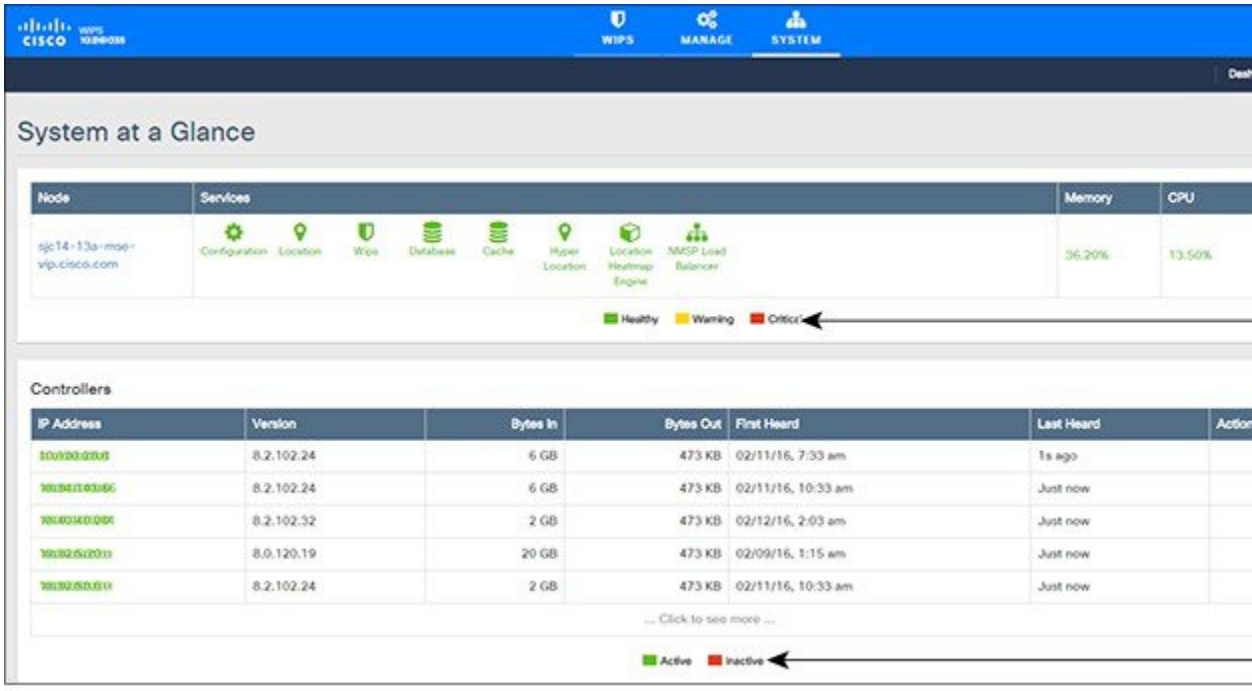
手順

Cisco Connected Mobile Experiences（Cisco CMX）にログインします。
[System at a Glance] ウィンドウが表示されます。このウィンドウは次のセクションで構成されています。

- [System at a Glance] 詳細については、[System at a Glance] テーブルの使用，（107 ページ）を参照してください。
- [Controllers] テーブル 詳細については、[Controllers] テーブルについて，（108 ページ）を参照してください。

[Cluster] テーブルと [Controllers] テーブルを次の図に示します。

図 *3*：*[System at a Glance]*



[System at a Glance] ウィンドウの各部分を次に説明します。

- 1：クラスタ サービスおよびメトリックを設定するための [Gear] アイコン
- 2：[System at a Glance] テーブル
- 3：クラスタ テーブル サービスのステータス インジケータの凡例
- 4：[Controllers] テーブル
- 5：[Controllers] テーブルのシスコ ワイヤレス コントローラ（Cisco WLC）のステータス インジケータの凡例アクティブなコントローラの IP アドレスは緑色で表示されます。非アクティブなコントローラの IP アドレスは赤色で表示されます。

[System at a Glance] テーブルの使用

[System at a Glance] ウィンドウには次の情報が表示されます。

- [Node]：関連付けられているすべての Cisco CMX ノードを示します。
  - ノード名をクリックすると、メトリックが表示されます。CMX ノード メトリックの表示, （117 ページ）を参照してください。

- [Services]：各 Cisco CMX ノードのすべてのサービスを示します。
  - これらのサービスに関連するアイコンの色は、サービスのステータスを示します。サービスが緑色であることを確認してください。緑色は、正常な状態を示します。
  - サービスのアイコンをクリックすると、対応するサービス メトリックまたはシステム メトリックが表示されます。
- [Memory]：メモリの負荷をパーセンテージで表示します。
  - これをクリックすると、[Live Alerts] ウィンドウが表示されます。ライブ システム アラートの表示, （123 ページ）を参照してください。
- [CPU]：CPU の負荷をパーセンテージで表示します。
  - これをクリックすると、[Live Alerts] ウィンドウが表示されます。ライブ システム アラートの表示, （123 ページ）を参照してください。
- [Actions]：ノードのすべてのサービスを再起動できます。

[Controllers] テーブルについて

[System at a Glance] ウィンドウの [Controllers] テーブルには、Network Mobility Services Protocol（NMSP）データを Cisco CMX に送信する Cisco WLC が示されます。このテーブルには、各 Cisco WLC に関する次の詳細情報が表示されます。

- [IP Address]：各 IP アドレスの左側のテーブル枠の色は、Cisco WLC がアクティブであるかどうかを示します。
- [Version]：Cisco WLC ソフトウェアのバージョンです。
- [Bytes In and Bytes Out]：Cisco WLC から受信したバイト数とこの WLC へ送信したバイト数。
- [First Heard]：Cisco WLC から最初の通信を受信した時点からの経過秒数。
- [Last Heard]：Cisco WLC から通信を受信した時点からの経過秒数。
- [Action]：既存のコントローラの詳細を変更するか、または既存のコントローラを削除することができます。

Cisco CMX の一般設定の表示

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 [System] > [Dashboard] を選択します。

[System at a Glance] ウィンドウが表示されます。

ステップ 3 ウィンドウの右上隅にある [Gear] アイコンをクリックします。
[Settings] ウィンドウが表示されます。このウィンドウでは、[General] タブがすでに選択されています。 ノードに関する次の詳細情報が表示されます。

- [Name]：Cisco CMX ノード名。
- [Associated Nodes]：このノードに関連付けられている Cisco CMX ノード。

Cisco CMX ノードの詳細情報の表示

手順

ステップ 1 Cisco CMX にログインします。

ステップ 2 [System] > [Dashboard] を選択します。
[System at a Glance] ウィンドウが表示されます。

ステップ 3 ページの右上隅にある [Gear] アイコンをクリックします。
[Settings] ウィンドウが表示されます。

ステップ 4 [Node Details] タブをクリックします。

ステップ 5 ノード名をクリックします。ノードの詳細情報（[Node ID]、[Name]、[Hostname]、および [Type] など）が表示されます。

デバイス追跡パラメータの設定

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 [System] > [Dashboard] を選択します。
[System at a Glance] ウィンドウが表示されます。

ステップ 3 ウィンドウの右上隅にある [Gear] アイコンをクリックします。
[Default Cluster Settings] ダイアログボックスが表示されます。

ステップ 4 [Tracking] タブをクリックします。

[Tracking Parameters] テーブルが表示されます。

ステップ 5 [Elements] カラムで、追跡対象として選択する各デバイスのチェックボックスをオンにします。ここで選択された要素だけが、ネットワーク ロケーション サービスにより追跡され、[Activity Map] ウィンドウに表示されます。

（注） Bluetooth Low Energy（BLE）ビーコン タグを追跡するには、[Interferers] をオンにします。 BLE ビーコン対応デバイスを追跡するには、ソフトウェア リリース 8.0.115.0 以降の Cisco WLC が必要です。

ステップ 6 [Save] をクリックします。

フィルタ パラメータの設定

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 [System] > [Dashboard] を選択します。
[System at a Glance] ウィンドウが表示されます。

ステップ 3 ウィンドウの右上隅にある [Gear] アイコンをクリックします。

ステップ 4 [Filtering] タブをクリックします。
次のフィルタリング パラメータを設定できます。

- [Duty Cycle Cutoff]：これはパーセント値です。 デューティ サイクルが、指定されたカットオフよりも小さい干渉源は、追跡されません。
- [RSSI Cutoff]：フィルタリングのための無線信号強度カットオフ値です。 デフォルトは -85 dBm です。
- [Exclude probing clients]：プローブのみのクライアントをフィルタで除外する場合は、このチェックボックスをオンにします。 これにより、接続クライアントだけを追跡できます。
- [Enable Locally Administered MAC filtering]：自己割り当て MAC アドレスをフィルタで除外するには、このチェックボックスをオンにします。 このパラメータは、デフォルトでオンになっています。 これにより、Apple iOS8 のランダム MAC アドレスが無視されます。
- [Enable Location MAC filtering]：特定の MAC アドレスをフィルタで除外するには、このチェックボックスをオンにします。 たとえば、従業員のデバイスの MAC アドレスを除外する場合に使用できます。 これをオンにした後で、許可または拒否する MAC アドレスを指定するか、または以前に入力した MAC アドレスを削除することができます。

ステップ 5 [Save] をクリックします。

ロケーション計算パラメータの設定

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 [System] > [Dashboard] を選択します。
[System at a Glance] ウィンドウが表示されます。

ステップ 3 ウィンドウの右上隅にある [Gear] アイコンをクリックします。
[Settings] ダイアログボックスが表示されます。

ステップ 4 [Location Setup] タブをクリックします。
次のロケーション計算パラメータを設定できます。

- [Enable OW Location]：ロケーション計算に外部ウオール（障害物）を使用できるようにするには、このチェックボックスをオンにします。
- [Enable Location Filtering]：現在ロケーションの推定時に以前のロケーション推定を使用するには、このチェックボックスをオンにします。 このパラメータは、クライアント ロケーションの計算だけに適用されます。 このパラメータを有効にすると、ステーショナリ クライアントのロケーション ジッタが低下し、モバイル クライアントのロケーション追跡が向上します。 このパラメータは、デフォルトで有効になっています。
- [Use new location algorithm]：新しい集計アルゴリズムにより、ロケーション計算前の RSSI の集計方法が変更されます。 シスコのテクニカル サポートからの指示がない限り、このパラメータを変更しないことをお勧めします。
- [User Default Heatmaps for Non Cisco Antennas]：ロケーション計算中に、シスコ以外のアンテナにデフォルトのヒートマップを使用できるようにするには、このチェックボックスをオンにします。
- [Chokepoint Usage]：チョークポイント プロキシミティを使用してデバイスのロケーションを判別できるようにするには、このチェックボックスをオンにします。 これは、チョークポイント プロキシミティを報告可能なシスコ互換タグだけに適用されます。 このパラメータは、デフォルトで有効になっています。
- [Enable Hyperlocation]：Cisco CMX で Hyperlocation を有効にするには、このチェックボックスをオンにします。 このパラメータはデフォルトではディセーブルになっています。
- [Use Chokepoints for Interfloor conflicts]：フロア間の競合発生時に正しいフロアを判別するための周波数を指定するには、このドロップダウン リストを使用します。
- [Chokepoint Out of Range Timeout]：シスコ互換タグがチョークポイント プロキシミティ範囲を離れた時点から、このタイムアウト値に指定された期間の経過後に、ロケーションの判別に RSSI 情報が再び使用されます。 タイムアウト値は秒単位で指定します。

- [Relative discard RSSI time]：ここに指定する期間（分単位）の経過後に、RSSI 測定が古いものと見なされ、ロケーション計算に使用されなくなります。 この時間は、最新の RSSI サンプルからの時間であり、絶対時間ではありません。 たとえばこの値を 3 分に設定し、2 つのサンプルが 10 分と 12 分で受信される場合、両方のサンプルが保持されます。 15 分に受信された追加サンプルは無視されます。 シスコのテクニカルサポートからの指示がない限り、このパラメータを変更しないことをお勧めします。
- [Absolute discard RSSI time]：最新サンプルに関係なく、ここに指定する時間（分単位）の経過後に、RSSI 測定が古いものと見なされ、ロケーション計算に使用されなくなります。 シスコのテクニカルサポートからの指示がない限り、このパラメータを変更しないことをお勧めします。
- [RSSI cutoff]：サーバが AP 測定を無視する RSSI カットオフ値を dBm 単位で入力します。 シスコのテクニカルサポートからの指示がない限り、このパラメータを変更しないことをお勧めします。

また、次の移動検出パラメータも設定できます。

- [Individual]：個別 RSSI 移動再計算をトリガーするしきい値を dBm 単位で入力します。 シスコのテクニカルサポートからの指示がない限り、このパラメータを変更しないことをお勧めします。
- [Aggregated RSSI change threshold]：集計 RSSI 移動再計算のトリガーしきい値を指定します。 シスコのテクニカルサポートからの指示がない限り、このパラメータを変更しないことをお勧めします。
- [Many new RSSI change percentage threshold]：多数の新規 RSSI 変更の再計算のトリガーしきい値（パーセント値）を指定します。 シスコのテクニカルサポートからの指示がない限り、このパラメータを変更しないことをお勧めします。
- [Many missing RSSI percentage threshold]：多数の欠落 RSSI 変更の再計算のトリガーしきい値（パーセント値）を指定します。 シスコのテクニカル サポートからの指示がない限り、このパラメータを変更しないことをお勧めします。

次の履歴保存パラメータを設定できます。

- [History Pruning Interval]：ロケーション マップでクライアント ロケーション履歴が保存される日数を指定します。

ステップ 5 [Save] をクリックします。

通知のためのメール サーバの設定

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 [System] > [Dashboard] を選択します。
[System at a Glance] ウィンドウが表示されます。

ステップ 3 ウィンドウの右上隅にある [Gear] アイコンをクリックします。
[Default Cluster Settings] ダイアログボックスが表示されます。

ステップ 4 [Mail Server] タブをクリックします。
次の項目を設定できます。

- [From Email Address]：メール サーバ ホストの電子メール アドレス。
- [To Email Address]：通知送信先の電子メール アドレスを入力します。
- [Server]：メール サーバの URL。
- [Port]：メールに使用されるポート番号。 デフォルトは、ポート 25 です。
- [Authentication]：メール認証を有効または無効にするためのオプション。
- [SSL]：第三者が電子メール メッセージを表示できないようにするための Secure Sockets Layer（SSL）による電子メールの保護を有効または無効にするためのオプション。
- [TLS]：Transport Layer Security（TLS）による電子メールの保護を有効または無効にするためのオプション。

ステップ 5 設定をテストするには、[Test Settings] をクリックし、次に [Send e-mail] をクリックします。

ステップ 6 テストが正常に完了したら、[Save] をクリックして設定を保存します。

Cisco CMX へのマップとコントローラのインポート

Cisco Prime Infrastructure からマップとコントローラを直接インポートするには、次の手順を実行します。

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 [System] > [Dashboard] を選択します。

[System at a Glance] ウィンドウが表示されます。

ステップ 3 ウィンドウの右上隅にある [Gear] アイコンをクリックします。

ステップ 4 [Controllers and Maps Setup] > [Import] タブを選択し、次のパラメータを入力します。

a) [Username]：Cisco Prime Infrastructure サーバのユーザ名。

b) [Password]：Cisco Prime Infrastructure サーバのパスワード。

c) [IP Address]：Cisco Prime Infrastructure サーバの IP アドレス。 Cisco Prime Infrastructure で SNMP コミュニティ文字列が適切に設定されていることを確認します。

Cisco Prime Infrastructure のクレデンシャルを保存するには、[Save Cisco Prime Credentials] チェックボックスをオンにします。

インポート時に、現在 Cisco CMX に存在する既存のマップを上書きするには、[Override Maps] チェックボックスをオンにします。

デフォルトでは、同期と同様に上書きのチェックボックスはオンになっています。 Cisco CMX は既存のマップを削除し、インポートするファイルに含まれているマップに置き換えます。 このチェックボックスがオフの場合、Cisco CMX はファイルにマップを追加します。

ステップ 5 設定をテストするには、[Test Settings] をクリックし、次に [Send e-mail] をクリックします。

ステップ 6 テストが正常に完了したら、[Save] をクリックして設定を保存します。

マップのインポートとコントローラの追加

Web インターフェイスを使用してマップを手動でインポートし、Cisco WLC を Cisco CMX に追加できます。

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 [System] > [Dashboard] を選択します。
[System at a Glance] ウィンドウが表示されます。

ステップ 3 ウィンドウの右上隅にある [Gear] アイコンをクリックします。

ステップ 4 [Controllers and Maps Setup] > [Advanced] タブを選択します。

ステップ 5 マップを手動でインポートするには、次の手順を実行します。

a) [Maps] エリアの下にある [Browse] をクリックします。
[File Upload] ダイアログボックスが表示されます。

（注） [Override Maps] チェックボックスをオンにすると、Cisco CMX の既存のマップが、Cisco Prime Infrastructure からインポートするマップに置き換えられます。

b) マップ ファイルの場所に移動し、マップ ファイルを選択し、[Open] をクリックします。

c) [Upload] をクリックします。

d) [Save] をクリックします。

ステップ 6 Cisco WLC をインポートするには、[Controllers] エリアで次のパラメータを設定します。

a) [Controller type]：[Cisco WLC] または [NGWC] を選択します。
b) [IP address / Hostname]：Cisco WLC の IP アドレスまたはホスト名。
c) [Applicable Services]：Context Aware Service（CAS）が適用可能な場合は、[CAS] チェックボックスをオンにします。
d) [Controller SNMP version]：[v1]、[v2c]、[v3] のいずれかを選択します。
e) [Controller SNMP Write Community]：コントローラ SNMP write コミュニティ ストリングを入力します。 デフォルトは *private* です。
f) [Add Controller] をクリックします。

ステップ 7 [Save] をクリックします。

Cisco CMX のアップグレード

Cisco CMX 10.2 のインストール後にアップグレードを実行するには、cmxadmin としてログインし、Cisco CMX GUI を使用するか、または **cmxos upgrade** CLI コマンドと .cmx ファイルを使用します（例：cmxos upgrade <**CISCO_CMX$$$.cmx**>）。

GUI を使用して Cisco CMX を今後のリリースにアップグレードするには、次の作業を行います。

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 [System] > [Dashboard] を選択します。
[System at a Glance] ウィンドウが表示されます。

ステップ 3 ウィンドウの右上隅にある [Gear] アイコンをクリックします。

ステップ 4 [Settings] ダイアログボックスで [Upgrade] タブをクリックし、[Upgrade] をクリックします。

ステップ 5 ローカル .cmx ファイルを選択するか、または .cmx ファイルの URL をポイントします。
ローカル ファイル オプションを選択する前に、Web GUI へのアクセスが確立されるマシンで .cmx ファイルが使用可能であることを確認します。

アップグレード プロセスでは次の処理が行われます。

1. .cmx ファイルが /opt/image/newimage にコピーされます。
2. cmxos upgrade コマンドがバックグラウンドで実行されます。
   - サービスが停止します。
   - 新しいファイルがコピーされ、設定されます。

• サービスが再起動されます。

システム サマリ メトリックの表示

[System Summary Metrics] ウィンドウには、次の情報が表示されます。

- [Number of Active Clients]
- [Number of NMSP messages processed by the system per second, in the last one minute]
- [Overall CPU usage metics]
- [Overall memory usage metics]
- [Overalldisk usage metics]

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 [SYSTEM] > [Metrics] を選択します。
左側のペインの [System Summary] タブがデフォルトで選択されており、該当する詳細情報が表示されます。

システム サマリ メトリックの表示

システムサマリ メトリックをダッシュボードから表示することもできます。このためには、次の手順を実行します。

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 [SYSTEM] > [Dashboard] を選択します。
[System at a Glance] ウィンドウが表示されます。

ステップ 3 [Services] カラムで [Configuration]、[Location Heatmap Engine]、[NMSP Load Balancer]、または [Proxy] アイコンをクリックし、対応するシステム サマリ メトリックを表示します。

（注） 説明と詳細情報を参照するには、メトリックとグラフにカーソルを合わせます。

CMX ノード メトリックの表示

Cisco CMX ノードの [CMX Node Metrics] ウィンドウに、次の情報が表示されます。

- [Number of active clients]
- [Location latency time]
- [Number of incoming and outgoing NMSP messages]
- [Number of Controllers]
- [Number of location servers]
- [CPU usage metrics for each service]
- [Memory usage metrics for each service]
- [Disk IO metrics]
- [Disk usage metrics]

Cisco CMX ノードのノード メトリックを表示するには、次の手順を実行します。

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 [SYSTEM] > [Metrics] を選択します。
ステップ 3 左側のペインで、メトリックを表示する Cisco CMX ノードの名前をクリックします。

CMX ノード メトリックの表示

ノード メトリックをダッシュボードから表示することもできます。このためには、次の手順を実行します。

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 [SYSTEM] > [Dashboard] を選択します。
[System at a Glance] ウィンドウが表示されます。
ステップ 3 [Node] カラムで、メトリックの詳細情報を表示する Cisco CMX ノードの名前をクリックします。

（注） 説明と詳細情報を参照するには、メトリックとグラフにカーソルを合わせます。

データベース メトリックの表示

[Database Metrics] ウィンドウには、次のメトリックが表示されます。

- **[Database size]**
- **[Number of open connections]**
- **[Number of queries]**

データベース メトリックを表示するには、次の手順を実行します。

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 [SYSTEM] > [Metrics] を選択します。
ステップ 3 左側のペインで、[Database Metrics] をクリックします。

データベース メトリックの表示

データベース メトリックをダッシュボードから表示することもできます。このためには、次の手順を実行します。

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 [SYSTEM] > [Dashboard] を選択します。
[System at a Glance] ウィンドウが表示されます。
ステップ 3 [Services] カラムで [Database] アイコンをクリックします。
（注） 説明と詳細情報を参照するには、メトリックとグラフにカーソルを合わせます。

キャッシュ メトリックの表示

[Cache Metrics] ウィンドウには、次のメトリックが表示されます。

- [Blocked connections]
- [Connected clients]
- [Used memory]
- [Evicted keys]

キャッシュ メトリックを表示するには、次の手順を実行します。

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 [SYSTEM] > [Metrics] を選択します。
ステップ 3 左側のメニューで、[Cache Metrics] をクリックします。

キャッシュ メトリックの表示

キャッシュ メトリックをダッシュボードから表示することもできます。このためには、次の手順を実行します。

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 [SYSTEM] > [Dashboard] を選択します。
[System at a Glance] ウィンドウが表示されます。
ステップ 3 [Services] カラムで [Cache] アイコンをクリックします。
（注） 説明と詳細情報を参照するには、メトリックとグラフにカーソルを合わせます。

ロケーション メトリックの表示

[Location Metrics] ウィンドウには、各 Cisco CMX ノードの次のメトリックが表示されます。

- [Location counts]

- [Location times]：ロケーションの計算時間には、ロケーション計算の算術部分が含まれます。ほとんどの場合この時間は 10 ～ 20 ミリ秒です。 ロケーションの遅延時間は、メッセージが NMSPLB からロケーションに到着した時点の遅延計算、集計、キャッシュの作成、および計算にかかった時間の合計です。
- [Location and Nmsplb rates]：NMSPLB に着信する Network Mobility Services Protocol（NMSP）メッセージの着信率。
- [Hyperlocation Rates]：Hyperlocation メッセージの着信率。

ロケーション メトリックを表示するには、次の手順を実行します。

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 [SYSTEM] > [Metrics] を選択します。
ステップ 3 左側のペインで、[Location Metrics] をクリックします。

ロケーション メトリックの表示

ロケーション メトリックをダッシュボードから表示することもできます。このためには、次の手順を実行します。

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 [SYSTEM] > [Dashboard] を選択します。
[System at a Glance] ウィンドウが表示されます。
ステップ 3 [Services] カラムで [Location] アイコンをクリックします。
（注） 説明と詳細情報を参照するには、メトリックとグラフにカーソルを合わせます。

Analytics 通知メトリックの表示

[Analytics Notification Metrics] ウィンドウには、Analytics サービスに関連する最も重要なパフォーマンス指標が表示されます。 デバイスから重大な移動が検出されると、Location サービスから Analytics サービスに通知が送信されます。 各通知には、1 つのデバイスのロケーションに関する最新情報が含まれています。

[Analytics Notification Metrics] ウィンドウには、各 Cisco CMX ノードの次のメトリックが表示されます。

- [Notification processing time]：着信通知の平均処理時間。 この時間はさまざまな要因に基づきますが、最も代表的なものとしてネットワークのサイズ、つまり建物、フロア、ゾーン、タグなどの数があります。 このメトリックは、システム起動時にピークとなることが予期されますが、比較的安定しています。
- [Notification queue size]：着信通知のキューのサイズ。着信通知は処理前にキューに入れられます。 システムの負荷に応じて、Location サービスが通知を一括で送信します。 そのため、キューのサイズは常に 0 よりも大きいことを予期できます。 またこのメカニズムにより、一部のズーム レベルでは、上下の変動が多い非常に不規則なグラフとなることがあります。これは予期されている動作です。
  着信率の増加に伴い、キュー サイズが増加することが予測されます。 増加し続けると、[Notification dropped rate] メトリックでドロップされる通知が確認されるようになります。
- [Notification dropped rate]：着信通知のキューのサイズは制限されています。 そのため、キューが大きくなりすぎると通知が拒否されます。 [Notification dropped rate] グラフに、1 秒あたりの拒否された通知の数が表示されます。 このグラフの線が 0 のままで平坦であることが理想的です。 0 ではない場合は、Analytics サービスを実行するために別のサーバをクラスタに追加することを検討する必要があります。 これにより、負荷が 2 台のサーバに分散されます。
- [Notification incoming rate]：1 秒あたりに Analytics サービスから受信した通知の数です。 このトレンドは、クライアント数とほぼ等しくなるはずです。つまり、Location サービスで検出されるクライアントが増えると、通知の数も増加することが予期されます。ただし、この通知はデバイスのロケーションが変わったときにのみ送信されるので、このトレンドにはクライアントの移動率も影響します。

Analytics 通知メトリックを表示するには、次の手順を実行します。

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 [SYSTEM] > [Metrics] を選択します。
ステップ 3 左側のペインで、[Analytics Notification Metrics] をクリックします。

ダッシュボードを使用したAnalytics通知メトリックの表示

Analytics 通知メトリックをダッシュボードから表示することもできます。このためには、次の手順を実行します。

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 [SYSTEM] > [Dashboard] を選択します。
[System at a Glance] ウィンドウが表示されます。

ステップ 3 [Services] カラムで [Analytics] アイコンをクリックします。
（注） 説明と詳細情報を参照するには、メトリックとグラフにカーソルを合わせます。

Presence メトリックの表示

[Presence Metrics] ウィンドウには、次のメトリックが表示されます。

- [Presence Counts]
- [Presence Rates]

プレゼンス メトリックを表示するには、次の手順を実行します。

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 [SYSTEM] > [Metrics] を選択します。

ステップ 3 左側のペインで、[Presence Metrics] をクリックします。

パターンの表示

[Patterns] ウィンドウには、選択された期間の 1 週間における特定機能のパターン（クライアント数、固有デバイスなど）が表示されます。 たとえば、過去 1 ヵ月のクライアント数を選択した場合、過去 1 ヵ月でクライアント数が最も多かった 1 週間のうちの日または時間が示されます。

- [Client Count]：特定の時点で検出されるデバイスの合計数を表示します。
- [Location Calculation Time]：ロケーション アルゴリズムによるクライアント ロケーションの計算の平均時間（ミリ秒単位）を表示します。
- [Incoming Rate]：NMSP ロード バランサから受信する Network Mobility Services Protocol（NMSP）メッセージの数を表示します。
- [CPU Usage]：ノード単位での CPU 使用率を表示します。

- [Memory Usage]：ノード単位でのメモリ使用率を表示します。
- [Dropped]：Cisco CMX により Analytics サービスに送信されたが、何らかの理由（Analytics のキューがいっぱいだった場合など）によってドロップされた通知を表示します。
- [NMSP LB Read Operations]：ソケットから受信したバイト数を表示します。
- [Redis Connections Received]：キャッシュ サービスが受信した接続の合計数を表示します。

パターンを表示するには、以下の手順を実行します。

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 [SYSTEM] > [Patterns] を選択します。
[Patterns] ウィンドウが表示されます。

ステップ 3 [Select Criteria] ドロップダウン リストから、パターン データの表示条件を選択します。

ステップ 4 [Select Date Range] ドロップダウン リストから、条件パターンの時間枠を選択します。

ステップ 5 オプションで、[Select Server] ドロップダウン リストから、パターンデータを表示する Cisco CMX ノードを選択します。デフォルトでは、クラスタ内のすべての Cisco CMX ノードのパターンデータが表示されます。

ライブ システム アラートの表示

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 [System] > [Alerts] を選択します。

ステップ 3 表示される [Live Alerts] ウィンドウで、右上隅のドロップダウン リストを使用して、アラートを [By Severity]、[By Node]、または [By Service] にソートします。
アラートを消去するには、対応するノード名の隣にある [Actions] カラムで、[Dismiss] アイコンをクリックします。

第 9 章

管理タスクの実行

この章では、Cisco CMX を使用して管理タスクを実行する方法について説明します。 管理権限が割り当てられているユーザが管理タスクを実行できます。

Cisco CMX のユーザ アカウント

Cisco CMX 10.2 より前のリリースでは、Cisco CMX プロセスはすべて Linux の root ユーザ アカウントで実行されていました。 発生する可能性のあるリスクを防ぎ、システムを保護する目的で、Cisco CMX 10.2 では 2 種類の新しいユーザ アカウント（cmx と cmxadmin）が導入されました。

- root：root ユーザ アカウント。 ユーザはこのアカウントを使用できません。

（注） rootアカウントのパスワードはシステム所有者により設定、保守されます。デフォルトのパスワードは設定されません。 これにより、このアカウントを引き続き特殊なケースのインストールや問題のデバッグ処理に使用できます。また、root ユーザはエンドユーザにより所有されます。 パスワード回復は、シングルユーザ ログイン プロセスを使用して行われます。 詳細については、パスワードの復旧，（130 ページ）を参照してください。

- cmx：postgress を除くすべての CMX プロセスを所有する no login アカウント。
- cmxadmin：CLI を使用してすべての管理タスクを実行するためのプライマリ アカウント。root レベル アクセスを必要とするタスクを実行するには、ユーザはこのアカウントから *sudo*

を実行します。 このアカウントは、GUI を使用して Cisco CMX 10.2 を将来のリリースにアップグレードするときに使用します。

- admin：Cisco CMX Web UI を使用してマップと Cisco WLC を設定し、サービスを再起動するための管理ユーザ アカウント。
- 通常のユーザ アカウント：ユーザ定義のアカウント。

データのバックアップ

Cisco CMX を正常にインストールして実行したら、データの損失を防ぐためバックアップを作成できます。

次の状況では CMX サーバのデータが失われる可能性があります。

- CMX サーバのハード ディスクで障害が発生する
- CMX サーバのデータがアップグレード中に破損する

したがってデータのバックアップをとることで、データを元の状態に復元できるようになります。

Cisco CMX に大量のデータが保存されている場合、バックアップ操作に必要なディスク領域が増えます。 この場合、次のように対処することを検討できます。

- Cisco CMX サーバに十分な領域がない場合は、外部ドライブにバックアップします。 この操作を実行するには、リムーバブル ハードディスクまたはマウント ハードディスクを装着します。
- バックアップ操作を実行した後で、（ftp または scp を使用して）バックアップ ファイルを別のサーバに移動し、Cisco CMX サーバからバックアップ ファイルを削除します。

バックアップに含まれるコンポーネントは次のとおりです。

- データベース
- Cache
- Cassandra
- Influxdb
- Consul
- フロア マップ
- ライセンス
- セットアップ
- Conf

手順

バックアップ操作を実行するには、cmxadmin（非rootユーザ）アカウントを使用して**cmxos backup**コマンドを実行します。
バックアップでは -i パラメータを使用して、バックアップに含めるコンポーネントを選択できます（例：cmxos backup -i database）。

cmxos backup コマンドのサンプル出力を次に示します。

```
[cmxadmin@test ~]$ cmxos backup
Please enter the path for backup file [/tmp]: /tmp
[17:01:30] Preparing for backup...
Data size 287388806
Available disk space 139165282304
Pre-backup took: 0.0118758678436 seconds
['database', 'cache', 'cassandra', 'influxdb', 'consul', 'floormaps', 'licenses' , 'setup',
 'conf']
[17:01:30] Backup Database...
Backup database took: 1.15777993202 seconds
[17:01:32] Backup Cache...
Backup cache took: 0.383176088333 seconds
[17:01:32] Backup Cassandra...
Backup Cassandra DB took: 2.99715185165 seconds
[17:01:35] Backup InfluxDb...
Backup Influx DB took: 0.0846002101898 seconds
[17:01:35] Backup Consul...
Backup Consul took: 0.0185141563416 seconds
[17:01:35] Backup Floormaps...
Backup floor maps took: 0.000938892364502 seconds
[17:01:35] Backup licenses...
Backup licenses took: 0.000122785568237 seconds
[17:01:35] Backup setup...
Backup setup took: 0.000464200973511 seconds
[17:01:35] Backup node configuration...
Backup configuration took: 0.476609945297 seconds
[17:01:35] Creating tar file..
Post backup took: 16.3115179539 seconds
[17:01:52] Done Backup. Created backup file
/tmp/cmx_backup_test.cisco.com_2015_07_28_17_01.tar.gz
[cmxadmin@test ~]$
```

ハードディスク領域の増加

Cisco CMX が稼働する仮想マシンでバックアップ用のディスク領域が不足している場合は、ハードディスク領域を増やすことができます。

手順

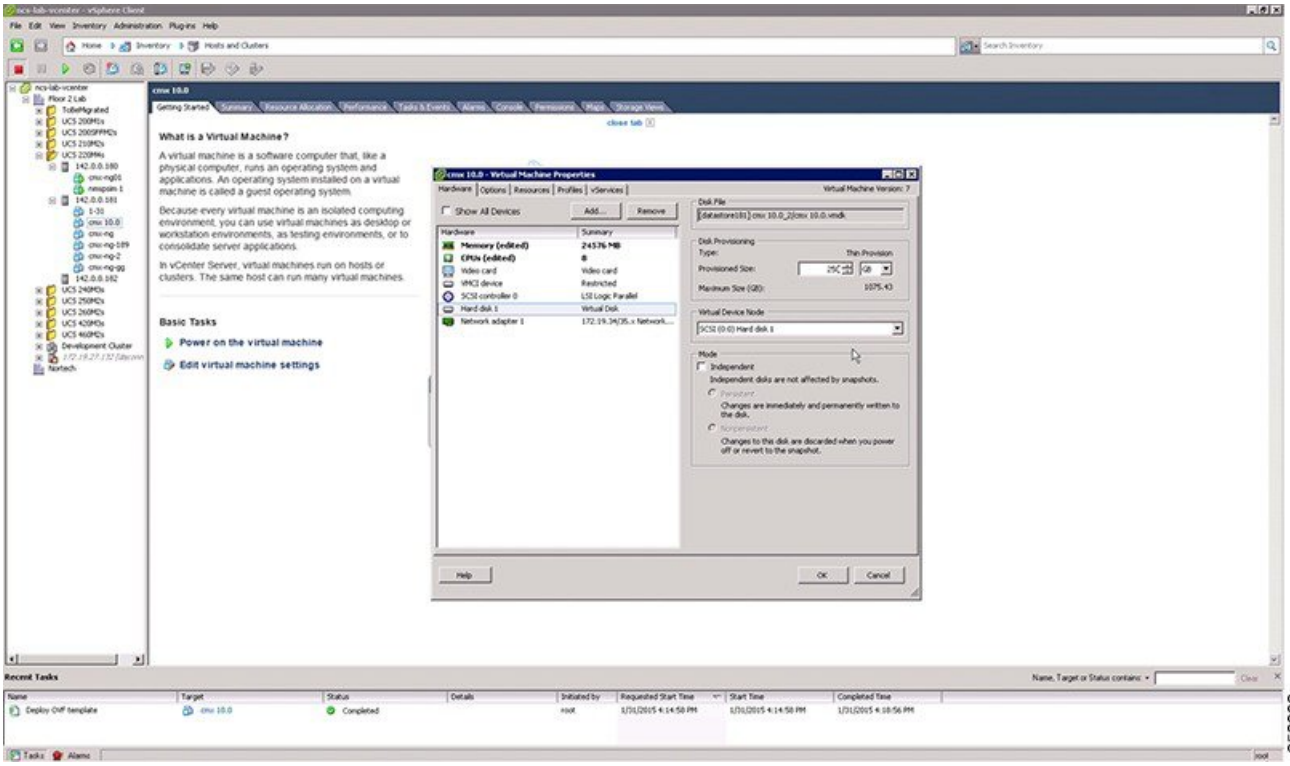
ステップ 1 次のコマンドを入力して、すべての Cisco CMX サービスを停止します。
cmxctl stop

cmxctl stop -a

ステップ 2 次のコマンドを入力して、仮想マシンをシャットダウンします。
Shutdown –h now

ステップ 3 仮想マシン設定を編集し、ハードディスク領域を増やします。

（注） 仮想マシンをスナップショットから復元した場合は、ハードディスク領域を増やすことはできません。



ステップ 4 仮想マシンを再起動します。
上記の手順の実行後に、Cisco CMX をバックアップできます。

CMX サービスのステータスを確認するには、**cmxctl status** コマンドを入力します。 どのサービスも実行されていない場合は、**cmxctl restart <サービス名>** コマンドを入力してサービスを再起動する必要がある場合があります。

データの復元

バックアップ完了後に、バックアップファイルを安全な場所に保管できます。 必要に応じて、その場所から復元できます。

Cisco CMX サーバに十分なディスク スペースがない場合にデータを復元するには、外部ドライブからファイルの解凍を試行します。 解凍されるファイルはバイナリ形式であり、データベースサーバが読み取ることができます。

手順

データを復元するには、cmxadmin（非 root ユーザ）アカウントを使用して **cmxos restore** コマンドを入力します。

restore コマンドに-iパラメータを指定することで、復元するコンポーネントを選択できます（例：cmxos restore -i database）。

cmxos restore コマンドのサンプル出力を次に示します。

```
[cmxadmin@test~]$ cmxos restore
Please enter the backup file path: /tmp/cmx_backup_test.cisco.com_2015_07_28_17_01.tar.gz
Please enter the path for untar backup file [/tmp]: /tmp
[17:08:54] Preparing for restore...
Restore size 27866720
Available disk space in /tmp is 139137040384
Available disk space is 139424529077
[17:08:54] Untarring backup file...
[17:08:55] Stopping all services...
Pre restore took: 26.4669179916 seconds
[17:09:21] Restoring Database...
Created database mse
Running command /usr/bin/sudo -u postgres  pg_restore -d mse -Fc
/tmp/cmx_backup_test.cisco.com_2015_07_28_17_01/postgres/mse.dump
Restored database mse
Restarting database...
Restore database took: 18.3071520329 seconds
[17:09:39] Restoring Cache...
Stopping cache_6383...
Restarting cache_6383...
Stopping cache_6380...
Restarting cache_6380...
..............
Stopping cache_6382...
Restarting cache_6382...
Stopping cache_6379...
Restarting cache_6379...
Stopping cache_6381...
Restarting cache_6381...
Stopping cache_6378...
Restarting cache_6378...
Restore Cache took: 46.7663149834 seconds
[17:10:26] Restoring Cassandra...
Stopping Cassandra...
Starting casandra
Creating cassandra scehma
..............
Restore Cassandra took: 29.5983269215 seconds
[17:10:56] Restoring Influxdb...
Stopping Influxdb...
Restarting Influxdb...
Restore Influx DB took: 13.9934449196 seconds
[17:11:10] Restoring consul...
Restore Consul took: 0.761927843094 seconds
[17:11:10] Restoring floormaps...
Restore floor maps took: 0.0269021987915 seconds
[17:11:10] Restoring licenses...
Restore licenses took: 0.00019907951355 seconds
[17:11:10] Restoring setup...
Restore setup took: 0.000532150268555 seconds
[17:11:10] Running Post Restore Tasks...
[17:11:10] Migrating Schemas...
[17:11:11] Migrating Cassandra schemas...
[17:11:12] Restarting all services...
stopping cassandra
Post restore took: 6.64956212044 seconds
[17:11:17] Starting all services...
..............
[17:12:45] Done
$
```

パスワードの復旧

Cisco CMX リリース 10.2 は、シングル ユーザ モードで root ユーザと cmxadmin ユーザのパスワードをリセットします。

シングル ユーザ モードを開始するための要件を次に示します。

- Cisco Mobility Services Engine（Cisco MSE）への（非 SSH）コンソール接続。
- Cisco MSE アプライアンスの電源投入。

GUI 管理ユーザ パスワードをデフォルトの admin にリセットするには、Cisco MSE CLI から次のコマンドを使用します。

cmxctl reset ui-password

cmxadmin ユーザの CLI にアクセスするためのパスワードがわかっている必要があります。

root または cmxadmin のパスワードをリセットするには、次の手順を実行します。

手順

ステップ 1 コンソール アクセスを確立します。

ステップ 2 Cisco MSE の電源を投入します。

ステップ 3 画面に最初のテキストが表示されてから 6 秒以内に上矢印キーを押します。

ステップ 4 GRUB メニューが表示されたら、次の手順を実行します。

a) 最初のエントリが強調表示されているかどうかを確認します。
b) 編集するため **e** キーを押します。

ステップ 5 下矢印キーを使用して最初のエントリを強調表示します。

a) エントリを編集するため **e** キーを押します。
b) Space バーを押して **single** と入力し、Enter キーを押します。
c) 選択したエントリを起動するため **b** キーを押します。

ステップ 6 システムが起動し、# プロンプトが表示されたら、次の操作を行います。

a) **passwd** <ユーザ名> と入力し、Enter キーを押します。
b) プロンプトが表示さたら、ユーザ（root/cmxadmin）の新しいパスワードを入力して Enter キーを押します。
c) 確認のためにパスワードを再入力します。

ステップ 7 **reload** と入力して Enter キーを押します。システムが再起動し、Cisco CMX サービスがロードされます。

Cisco CMX サーバのシャットダウンの問題のトラブルシューティング

Cisco CMX サーバは、ディスク領域の使用率が 85□ に達すると、すべてのサービスをシャットダウンします。 この問題が発生した場合は、サーバから不要なファイル（存在する場合）を削除して、Cisco CMX サーバでディスク領域を確保します。 十分な領域ができたら、**cmxctl start –a** コマンドを実行して Cisco CMX サーバを再起動します。

付 録 A

ソーシャルネットワークアカウントを使用した認証

Facebook での OAuth の設定

（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。

手順

ステップ 1 カスタム ポータルの [Social Login] 画面で、Facebook の右側にあるリンク（）アイコンをクリックし、関連付けられているデベロッパー Web サイトに移動します。

ステップ 2 ユーザ名とパスワードを使用して Facebook にログインします。

ステップ 3 [+Add a New App] ボタンをクリックします。

ステップ 4 [Website] ボタンをクリックします。

ステップ 5 アプリケーションの名前を入力し、[Create New Facebook App ID] をクリックします。

ステップ 6 [Choose a Category] ドロップダウン リストから、新しいアプリケーションのカテゴリを選択し、[Create App ID] ボタンをクリックします。

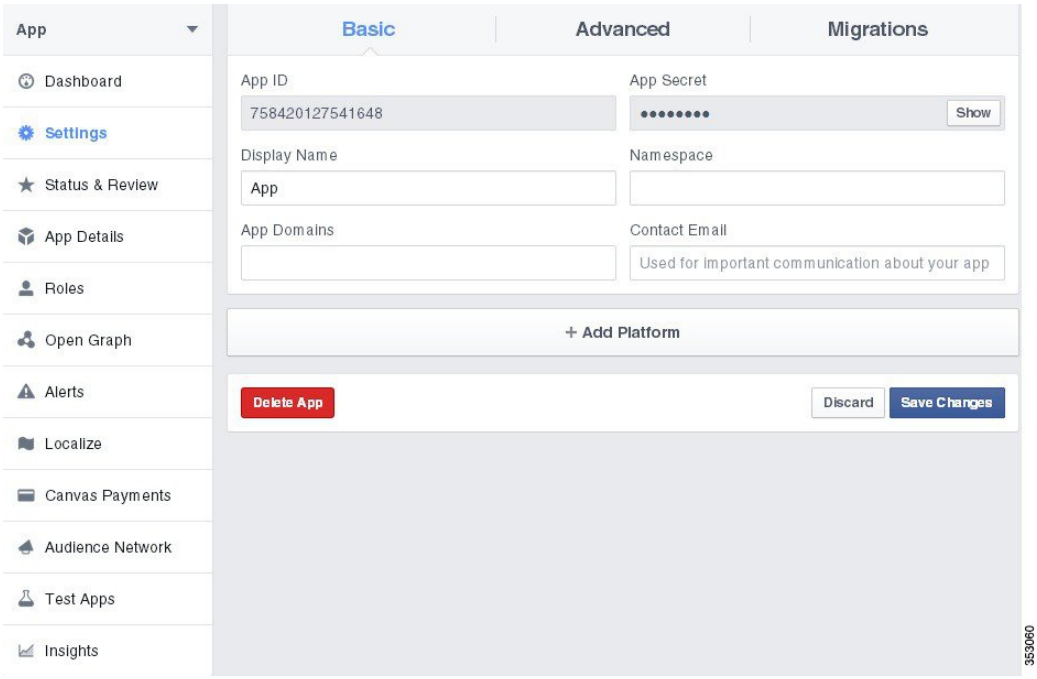
ステップ 7 [Tell us about your website] エリアまで下へスクロールし、[Site URL] フィールドにワイヤレス LAN コントローラ（WLC）リダイレクト URL（http://<CMX>/visitor/login）と同じ URL を入力し、[Next] ボタンをクリックします。

（注） Cisco CMX の IP アドレスが 172.x.x.x の範囲内のアドレスである場合、これが Facebook URL として表示されるため、この設定は失敗します。

ステップ 8 [Skip to Developer Dashboard] リンクをクリックします。

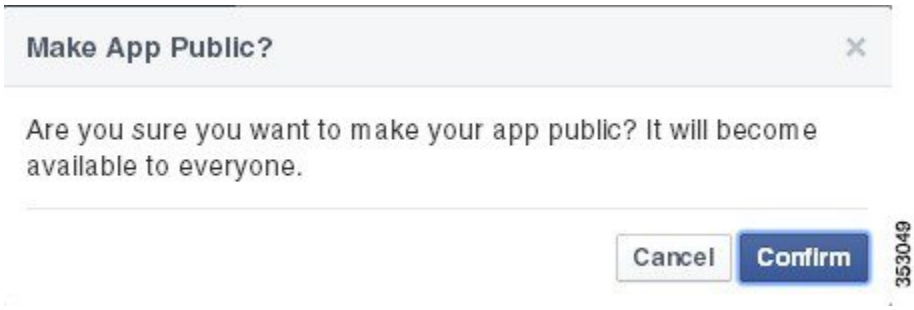
ステップ 9 後のステップで使用するため、アプリ ID を選択してコピーします。

ステップ 10 左側のナビゲーション ウィンドウの [Settings] をクリックし、連絡先メールを追加し、[Save Changes] ボタンをクリックします。



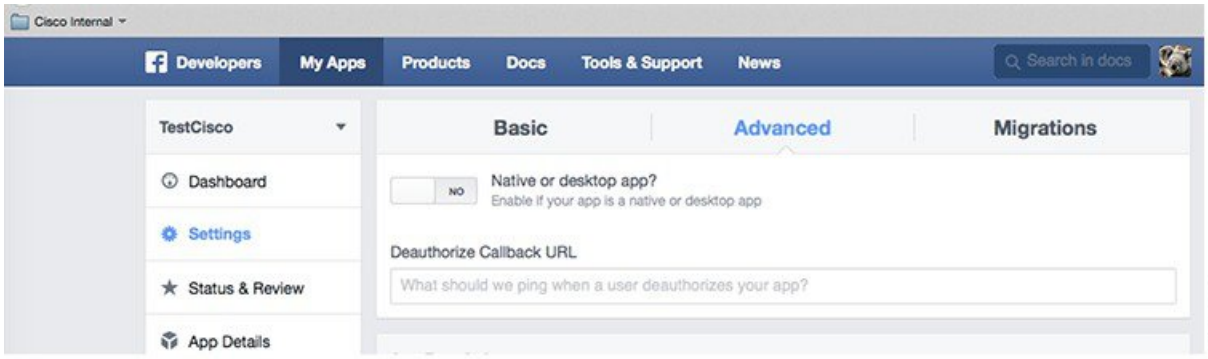
ステップ 11 左側のナビゲーション ウィンドウの [Status & Review] をクリックし、[Yes/No] スライダをクリックして、アプリを一般公開します。

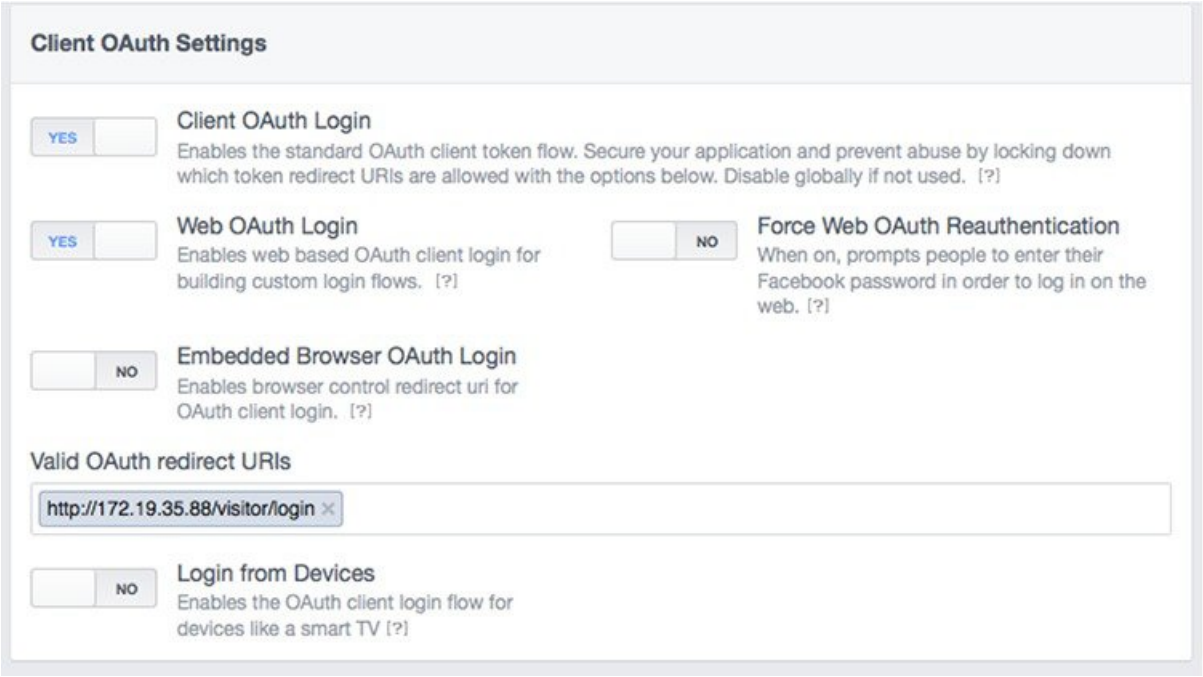
ステップ 12 [Confirm] ボタンをクリックします。



ステップ 13 名、姓、友達リストなどの情報を収集する場合は、Facebook による承認のためこれらのアイテムを送信します。

ステップ 14 Facebook Oauth 設定のためにプライベート IP アドレスを設定するには、[Advanced] タブを選択し、[Valid OAuth redirect URIs] フィールドに **http://cmxIP/visitor/login** と入力します。 デフォルトでは、[Valid OAuth redirect URIs] フィールドは空白です。





ステップ 15 カスタム ポータルに移動して [Create New] をクリックし、アプリ名を追加し、前の手順で生成したアプリ ID 情報を貼り付けます。

ステップ 16 [Scope] ドロップダウン リストから、ソーシャル ネットワーク データの収集範囲を選択し、[Facebook] チェックボックスをオンにします。

Facebook のデータの収集

Cisco CMX は Facebook の友達に関する情報を収集しますが、Facebook API は同じアプリを使用している友達に関する情報だけを返します。

Instagram での OAuth の設定

手順

ステップ 1 カスタム ポータルの [Social Login] 画面で、Instagram の右側にあるリンク（  ）アイコンをクリックし、関連付けられているデベロッパー Web サイトに移動します。

ステップ 2 Instagram にログインするには、右上にある [Log In] をクリックしてから、ユーザ名とパスワードを入力して、[Log In] ボタンをクリックします。

ステップ 3 [Manage Clients] タブで [Register a New Client] ボタンをクリックします。

ステップ 4 アプリケーション名とその説明を入力します。

ステップ 5 [Website] フィールドと [OAuth redirect_url] フィールドにワイヤレス LAN コントローラ（WLC）リダイレクト URL（http://<CMX>/visitor/login）と同じ URL を入力します。 [Disable Implicit OAuth] チェックボックスをオンにします。

ステップ 6 Captcha と入力し、[Register] ボタンをクリックします。

ステップ 7 次のステップで使用するクライアント ID を選択し、コピーします。

ステップ 8 カスタム ポータルに移動し、[Create New] をクリックして、アプリ名を追加し、前の手順で生成したクライアント ID を貼り付けます。

Foursquare での OAuth の設定

手順

ステップ 1 カスタム ポータルの [Social Login] 要素で、Foursquare の右側にあるリンク（  ）アイコンをクリックし、関連付けられているデベロッパー Web サイトに移動します。

ステップ 2 右上にある [My Apps] タブをクリックして、Foursquare にログインします。

ステップ 3 電子メールアドレスとパスワードを入力し、[Log In] ボタンをクリックします。

ステップ 4 [CREATE A NEW APP] ボタンをクリックします。

ステップ 5 [Download/welcome page url] フィールド、[Your privacy policy url] フィールド、および [Redirect URI(s)] フィールドに、ワイヤレス LAN コントローラ（WLC）リダイレクト URL（http://<CMX>/visitor/login）と同じ URL を入力します。

ステップ 6 [SAVE CHANGES] ボタンをクリックします。

ステップ 7 次のステップで使用するクライアント ID を選択し、コピーします。

ステップ 8 カスタム ポータルに移動し、[Create New] をクリックし、アプリ名を追加して、前の手順でコピーしたクライアント ID を貼り付けます。

ステップ 9 [Scope] ドロップダウンリストから、ソーシャル ネットワーク データの収集範囲を選択し、チェックボックスをオンにします。