Cisco Connected Mobile Experiences Configuration Guide, Release 7.6

初版：2013 年 07 月 31 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/

Text Part Number: OL-29330-01-J

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

はじめに

ここでは、『 Configuration Guide』の対象読者、構成、および表記法について説明します。 また、他のマニュアルの入手方法についても説明します。 この章は、次の項で構成されています。

対象読者

このマニュアルの目的は、Context-Aware Service を設定し、管理することです。 作業を開始する前に、ネットワークの構造、用語、および概念を十分に理解しておく必要があります。

関連資料

Mobility Services Engine のインストールおよび設定の詳細については、『Cisco 3355 Mobility Services Engine Getting Started Guide』を参照してください。 これらのマニュアルは、次の URL の Cisco.com で入手できます。

Cisco Unified Wireless Network ソリューションのユーザ向けマニュアルを参照するには、次のリンクをクリックしてください。

http://www.cisco.com/en/US/products/ps9742/tsd_products_support_install_and_upgrade.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/en/US/docs/general/whatsnew/whatsnew.html から入手できます。

『*What's New in Cisco Product Documentation*』に登録します。ここには、すべての新規および改訂済みの Cisco テクニカル マニュアルが RSS フィードとして掲載されており、コンテンツはリーダー アプリケーションを使用してデスクトップに直接配信されます。RSS フィードは無料のサービスです。

第 1 章

概要

この章では、全体的な Cisco Unified Wireless Network（CUWN）内の Cisco Connected Mobile Experience のコンポーネントである、Cisco 3300 シリーズ Mobility Services Engine（MSE）の役割について説明します。

また、Mobility Services Engine でサポートされているサービスおよび CMX のコンポーネントである、Context-Aware Service（CAS）ソフトウェアについても説明します。

この章は、次の内容で構成されています。

Cisco Context-Aware Mobility ソリューションについて

CMX ソリューションの基盤は CUWN のコントローラ ベースのアーキテクチャです。 CUWN には、主要なコンポーネントとしてアクセス ポイント、ワイヤレス LAN コントローラ、Cisco Prime Infrastructure 管理アプリケーション、Cisco 3300 シリーズ Mobility Services Engine が含まれています。

ここでは、次の内容について説明します。

Cisco 3300 シリーズ Mobility Services Engine

Cisco 3300 Mobility Services Engine は、CMX ソリューションのコンポーネントである CAS で動作します。

モビリティ サービス エンジンには 2 種類のモデルがあります。

- Cisco 3355 Mobility Services Engine

- 仮想アプライアンス

CAS

CASにより、シスコアクセスポイントから状況依存情報（ロケーション、温度、可用性など）を取得することで、Mobility Services Engine は数千のモバイル アセットとクライアントを同時に追跡できます。

CAS は、受信したコンテキスト情報を処理するために、*Cisco Context-Aware Engine for Clients and Tags* に依存します。 *Cisco Context-Aware Engine for Clients and Tags* は、Wi-Fi クライアントから受信したデータと Wi-Fi タグから受信したデータを処理します。

[ContextAware] タブ

Prime Infrastructure ホーム ページの [ContextAware] タブにアクセスできます。 このタブには、重要な Context-Aware Service ソフトウェア情報があります。

次の出荷時の初期状態コンポーネントは、[ContextAware] タブに表示されます。

- [MSE Historical Element Count]：指定の期間のタグ、クライアント、不正 AP、不正クライアント、干渉、有線クライアント、およびゲストクライアントの数の履歴トレンドを表示します。

（注） [MSE Historical Element Count] の情報は、時間ベースのグラフで表示されます。時間ベースのグラフでは、グラフ ページの上部に、6 時間、1 日、1 週間、2 週間、4 週間、3 ヵ月、6 ヵ月、1 年、およびカスタムを表示するリンク バーがあります。 選択すると、そのタイム フレームのデータが取得され、対応するグラフが表示されます。

（注） ダッシュレットの [MSE Historical Element Count] は、MSE から 5 分ごとに取得され、Prime Infrastructure データベースに定期的に集約されます。 所定の仮想ドメインでは、その仮想ドメインに割り当てられたフロアに基づいて、要素の数が MSE から取得されます。 これらの数はダッシュレットに集約、表示されます。

- [Rogue Element Detected by CAS]：不正 AP および不正クライアントのインデックスをパーセンテージで示します。 また、1 時間、24 時間、および 24 時間を超える期間以内に各 MSE によって検出された不正 AP と不正クライアントの数も表示します。

  不正 AP のインデックスは、Prime Infrastructure 上のすべての MSE で不正 AP として検出されたアクティブな追跡済み要素の合計に対するパーセンテージとして定義されます。

不正クライアントのインデックスは、Prime Infrastructure 上のすべての MSE で不正クライアントとして検出されたアクティブな追跡済み要素の合計に対するパーセンテージとして定義されます。

- [Location Assisted Client Troubleshooting]：ロケーション アシスタンスとともにこのオプションを使用して、クライアントをトラブルシューティングできます。 トラブルシューティングの基準として MAC アドレス、ユーザ名、または IP アドレスを指定できます。

  ロケーション アシストされるクライアントのトラブルシューティングの詳細については、ContextAware ダッシュボードからの、ロケーション アシストを受けるクライアントに関するトラブルシューティング, （4 ページ）を参照してください。

- [MSE Tracking Counts]：各要素タイプの追跡数と非追跡数を表します。 要素タイプには、タグ、不正 AP、不正クライアント、干渉、有線クライアント、ワイヤレス クライアント、およびゲスト クライアントが含まれます。

  （注） 要素の非追跡数は root ドメインでのみ使用可能です。

- [Top 5 MSEs]：ライセンス使用率のパーセンテージに基づいて上位 5 つの MSE を一覧表示します。 また、MSE ごとに各要素タイプの数を表示します。

詳細なレポートを取得するには、コンポーネントで数リンクをクリックします。 グラフとグリッドビューを切り替えるには、コンポーネント内のアイコンを使用します。 グリッドまたはグラフをページ全体で表示するには、[Enlarge Chart] アイコンを使用します。

クライアントとタグのライセンス情報

アクセス ポイントからタグおよびクライアントに関する状況依存情報を取得するには、シスコからライセンスを購入する必要があります。

- これはタグとクライアント（Base ロケーション ライセンス）に共通のライセンスです。
- タグ、クライアント、不正クライアント、不正アクセス ポイントの詳細については、Context-Aware Service の計画および検証, （89 ページ）を参照してください。
- タグとクライアントのライセンスは 1、10、100 アクセス ポイントの倍数の範囲で、様々な数量が提供されます。 Mobility Services Engine のハードウェアに応じて、最大 25,000 の Wi-Fi クライアントおよび Wi-Fi タグ（合計数）がサポートされます。
- Base ロケーションと拡張ロケーションのサービスで、MSE 3355 は最大 2500 アクセス ポイントを追跡し、VM では最大 5000 アクセス ポイントを追跡できます。 MSE 3355 と VM で追跡できる最大クライアント数は、それぞれ 25,000 台と 50,000 台です。

状況依存情報の表示

収集された状況依存情報は、中央集中型 WLAN 管理プラットフォームで、Prime Infrastructure のグラフィカル ユーザ インターフェイス形式で表示できます。

（注）

ただし、Prime Infrastructure を使用する前に、コマンドライン インターフェイス コンソール セッションを使用して、Mobility Services Engine の初期設定を行う必要があります。 次の URL にある『Cisco 3355 Mobility Services Engine Getting Started Guide』を参照してください:http://www.cisco.com/en/US/products/ps9742/tsd_products_support_series_home.html

Mobility Services Engine のインストールと初期設定が完了したら、Mobility Services Engine は複数の Cisco ワイヤレス LAN コントローラと通信し、オペレータにより定義された状況依存情報を収集できます。 次に、関連付けられている Prime Infrastructure を使用して各 Mobility Services Engine と通信し、選択されたデータを転送および表示できます。

クライアント、不正アクセスポイント、不正クライアント、モバイル ステーション、およびアクティブ RFID アセット タグに関するデータを収集するように Mobility Services Engine を設定できます。

ここでは、次の内容について説明します。

- [ContextAware] タブ，（2 ページ）
- ContextAware ダッシュボードからの、ロケーションアシストを受けるクライアントに関するトラブルシューティング，（4 ページ）

ContextAware ダッシュボードからの、ロケーションアシストを受けるクライアントに関するトラブルシューティング

Prime Infrastructure ホームページの [ContextAware] タブを使用して、クライアントのトラブルシューティングを実行できます。 MAC アドレス、ユーザ名、または IP アドレスを検索条件として指定し、[Troubleshoot] をクリックします。 [Troubleshoot] ページが表示されます。 ダッシュボードを使用して、特定の仮想ドメインに属するワイヤレス クライアントに対して、トラブルシューティング情報が表示されます。 アソシエートされたクライアントの場合、トラブルシューティング情報は、特定の仮想ドメインのフロアに属する場合のみ表示されます。 プローブ クライアントの場合、トラブルシューティング情報は root ドメインで表示されます。

[Context Aware History] タブで Context Aware 履歴レポートを表示できます。 このレポートを MSE 名に基づいてフィルタリングできます。 さらに [Timezone]、[State]、または [All] に基づいて、レポートをフィルタリングできます。 状態は、アソシエート済みまたはディスアソシエート済みのいずれかです。

[Timezone] を選択した場合は、次のいずれかを選択できます。

- 日付と時刻

または

- ドロップダウン リストの次のいずれかの値：
  - **直近の 1 時間**
  - **直近の 6 時間**
  - **直近の 1 日間**
  - **直近の 2 日間**
  - **直近の 3 日間**
  - **直近の 4 日間**
  - **直近の 5 日間**
  - **直近の 6 日間**
  - **直近の 7 日間**
  - **直近の 2 週間**
  - **直近の 4 週間**

別の方法として、[Generate Report] リンクを使用して、クライアント ロケーション履歴レポートを生成できます。 また、レポート ページで使用可能なアイコンを使用して、CSV または PDF 形式にレポートをエクスポートしたり、レポートを電子メールで送信したりもできます。

Prime Infrastructure ホーム ページの [ContextAware] タブの詳細については、[ContextAware] タブ, （2 ページ）を参照してください。

イベント通知

Mobility Services Engine は、次の転送メカニズムを介して、登録されたリスナーにイベント通知を送信します。

- Simple Object Access Protocol（SOAP）
- 簡易メール転送プロトコル（SMTP）メール
- 簡易ネットワーク管理プロトコル（SNMP）
- Syslog

（注） Prime Infrastructure は、SNMP を介してイベント通知を受信するリスナーとして動作できます。イベント通知を使用しない場合、Prime Infrastructure およびサードパーティのアプリケーションは、定期的にロケーションベース サービスからロケーション情報を要求する必要があります。

ただし、プル通信モデルは、ロケーション情報に対するよりリアルタイムの更新を必要とするアプリケーションには適しません。 これらのアプリケーションでは、登録されたリスナーが特定の条件を満たしている場合に、Mobility Services Engine のプッシュ イベント通知を設定できます。

第 2 章

Mobility Services Engine とライセンスの追加および削除

この章では、Cisco 3300 シリーズ Mobility Services Engine を Cisco Prime Infrastructure に対して追加および削除する方法について説明します。

（注）

[Identity Services] タブの [Mobility Services Engines]、[Synchronize Services]、[Synchronization History]、[High Availability]、[Context Aware Notifications]、および [Mobile Concierge] ページは、リリース 7.3.101.0 の root 仮想ドメインでのみ使用できます。

この章の内容は、次のとおりです。

MSE のライセンス要件

MSE には、次のような関連サービス エンジンとアプリケーション プロセスとともに、ネットワーク トポロジ、NMSP（Network Mobility Services Protocol） などの設計、ネットワーク リポジトリに関連する複数の製品機能が付属しています。

次の 3 種類のライセンスを取得できます。

- 基本ロケーション ライセンス：高度なスペクトル性能と、不正デバイス、干渉、Wi-Fi クライアント、RFID タグを追跡する機能が含まれます。 シスコの基本ロケーション ライセンスは、MSE API を使用するサードパーティ ソリューションに対応しています。
- 拡張ロケーション サービス ライセンス：拡張ロケーション ライセンスは、ロケーション分析サービスおよび CMX で利用できます。 アップグレード SKU の購入で、基本ロケーション ライセンスから拡張ロケーション ライセンスにアップグレードが可能です。 このライセンスは、wIPS サービスを除くすべてのサービスに適用されます。
- ワイヤレス侵入防御システム（wIPS）ライセンス：Cisco wIPS には、攻撃や不正アクセス ポイントの検出と緩和を可能にします。ライセンスには 2 種類あります。
  - モニタ モード ライセンス：このライセンスは、ネットワークに導入されている常時モニタリング アクセス ポイントの数に基づいています。
  - 拡張ローカル モード ライセンス：このライセンスは、ネットワークに導入されているローカル モード アクセス ポイントの数に基づいています。

（注） リリース 7.4 からは、ライセンシングは AP 単位となり、エンドポイント単位ではありません。これに対応するため、新しい L-LS ライセンスがリリース 7.4 で導入されました。

（注） CAS ライセンスの有効期間は、標準的な 6 か月の販売終了サポート期間と同じです。 有効期間中は、CAS と LS の両ライセンスが共存します。

- リリース 7.6 からは、Cisco MSE 3355 では、Cisco MSE ロケーション サービスまたは拡張ロケーション サービスにおいて最大 2500 個のアクセス ポイントをサポートします。 Cisco MSE 仮想アプライアンスは、サーバ リソースに応じて、最大 5,000 個のアクセス ポイントをサポートします。
- Cisco MSE 3355 は 25,000 台、ハイエンド仮想アプライアンスは 50,000 台のクライアントをサポートします。 すべてのライセンスは追加できます。
- プラットフォームのエンドポイントの最大数は、インストールされている AP 単位のライセンスに関係なく追跡されます。

ここでは、次の内容について説明します。

- MSE ライセンスの構成マトリクス，（9 ページ）
- MSE ライセンス ファイルのサンプル，（9 ページ）
- MSE ライセンスの取り消しと再使用，（10 ページ）

MSE ライセンスの構成マトリクス

次の表に、MSE、ロケーション サービスまたは Context-Aware Service ソフトウェア、および wIPS について、ハイエンド、ローエンド、および評価ライセンスのライセンス内容を示します。

表 *1* : *MSE* ライセンスの構成マトリクス

	ハイエンド	ローエンド	評価
MSE プラットフォーム	ハイエンドアプライアンスおよびインフラストラクチャプラットフォーム	ローエンドアプライアンスおよびインフラストラクチャプラットフォーム	120 日間
ロケーション サービスまたは Context-Aware Service ソフトウェア	3000、6000、12,000 アクセス ポイント	1000 アクセス ポイント	120 日間、100 タグおよび 100 要素
	3000、6000、12,000 アクセス ポイント	1000 要素	
wIPS	5000 アクセス ポイント	2000 アクセス ポイント	120 日間、20 アクセス ポイント

MSE ライセンス ファイルのサンプル

次に、MSE ライセンス ファイルのサンプルを示します。

```
FEATURE MSE cisco 1.0 permanent uncounted \
VENDOR_STRING=UDI=udi,COUNT=1 \
HOSTID=ANY \
NOTICE="<LicFileID>MSELicense</LicFileID><LicLineID>0</Li cLineID> \
<PAK>dummyPak</PAK>" \
SIGN="0C04 1EBA BE34 F208 404F 98ED 43EC \
45D7 F881 08F6 7FA5 4DED 43BC AF5C C359 0444 36B2 45CF 6EA6 \
1DB1 899F 413F F543 F426 B055 4C7A D95D 2139 191F 04DE"
```

このサンプル ファイルには、ライセンス エントリが 5 つあります。 どのライセンス エントリでも最初の行の先頭の語は、どのタイプのライセンスであるかを示します。 これは、Feature または Increment ライセンスのいずれかになります。 Feature（機能）ライセンスは、単一アイテムの固定ライセンスです。 複数のサービス エンジンを MSE で実行できます。 Increment（増分）ライセンスは、追加型のライセンスです。 MSE では、個々のサービス エンジンが Increment ライセンスとして扱われます。

最初の行の2番めの語は、ライセンス付与する特定のコンポーネントを定義します（MSEなど）。3 番めの語はライセンスのベンダーを示します（Cisco など）。 4 番めの語はライセンスのバージョンを示します（1.0 など）。5番めの語は有効期限を示します。これは、期限のないライセンスの場合は permanent、それ以外の場合は dd-mmm-yyyy の形式の日付になります。 最後の語は、このライセンスをカウントするかどうかを定義します。

MSE ライセンスの取り消しと再使用

MSE アプリケーション ライセンスをあるシステムから取り消し、別のシステムで再使用できます。 ライセンスを取り消すと、ライセンス ファイルはシステムから削除されます。 ライセンスを別のシステムで再使用する場合は、ライセンスをリホストする必要があります。

別のシステムでアップグレード SKU を使用してライセンスを再使用する場合は、対応する Base ライセンス SKU を、アップグレード SKU を再使用するシステムにインストールする必要があります。 対応する Base ライセンス SKU がシステムから削除された場合、そのシステムではアップグレード ライセンス SKU を再使用できません。

ライセンスを取り消すと、ライセンスに対して変更を反映するため、MSE により個別のサービス エンジンが再起動されます。 次に、サービス エンジンは、起動時に MSE から更新された容量を受け取ります。

ライセンスの詳細については、『*Cisco Prime Infrastructure Configuration Guide*, *Release 1.4*』を参照してください。

ガイドラインと制約事項

MSE を Prime Infrastructure に追加し、デバイスおよび wIPS 製品認証キーを登録する場合、次のガイドラインに従います。

- Mobility Services Engine は複数のサービスをサポートできます。
- 新しい Mobility Services Engine を追加すると、ネットワーク設計（キャンパス、ビルディング、および屋外マップ）、コントローラ、スイッチ（Catalyst 3000 シリーズおよび 4000 シリーズのみ）、および Mobility Services Engine のイベント グループと Prime Infrastructure を同期できます。

（注） リリース 7.5 以降は、Cisco Engine for Clients and Tags を使用してタグを追跡します。 リリース 7.2 以降からリリース 7.5 にアップグレードした場合にタグのライセンスが検出されると、AeroScout ライセンスとエンジンの削除に関する警告メッセージが表示されます。 承諾すると、すべてのパートナー エンジンのサブ サービスが削除され、その後 Cisco Tag Engine サブ サービスがデフォルトで有効になります。 パートナー エンジンの削除を承諾しない場合は、インストールを続行します。 アップグレード時にタグのライセンスが検出されない場合、インストールはそのまま進行します。

- 自動インストール スクリプトの実行中にユーザ名とパスワードを変更した場合は、Mobility Services Engine を Prime Infrastructure に追加する際に変更後の値をここで入力します。 デフォルト パスワードを変更しなかった場合は、自動インストール スクリプトを再実行してユーザ名とパスワードを変更することを推奨します。

Prime Infrastructure へのモビリティ サービス エンジンの追加

[Mobility Service] ページの [Add Mobility Services Engine] ダイアログボックスを使用して MSE を追加できます。 このダイアログボックスでは、ライセンス ファイルと追跡パラメータを追加し、マップを MSE に割り当てることができます。 設定のために既存の MSE でウィザードを起動する場合、[Add MSE] オプションの代わりに [Edit MSE Details] として表示されます。

ヒント Cisco Adaptive wIPS 機能の詳細については、http://www.cisco.com/ にアクセスして、マルチメディア プレゼンテーションをご覧ください。 Prime Infrastructure に関するさまざまなトピックについての学習モジュールがあります。 今後のリリースに合わせて、学習を強化する概要プレゼンテーションおよび技術プレゼンテーションが追加されていく予定です。

（注） Prime Infrastructure リリース 1.0 は MSE 3355 を認識し、適切にサポートしています。

（注） [Services] > [Mobility Services Engine] ページは、リリース 7.3.101.0 の仮想ドメインでのみ使用可能です。

Mobility Services Engine を Prime Infrastructure に追加するには、Prime Infrastructure にログインし、次の手順に従います。

ステップ 1 Mobility Services Engine に対して ping を実行できることを確認します。

ステップ 2 [Services] > [Mobility Services] の順に選択し、[Mobility Services] ページを表示します。

ステップ 3 [Select a command] ドロップダウン リストから、[Add Mobility Services Engine] を選択し、[Go] をクリックします。

ステップ 4 [Device Name] テキスト ボックスに、Mobility Services Engine の名前を入力します。

ステップ 5 [IP Address] テキスト ボックスに、Mobility Services Engine の IP アドレスを入力します。

ステップ 6 （任意）[Contact Name] テキスト ボックスに、Mobility Services Engine 管理者の名前を入力します。

ステップ 7 [User Name] および [Password] テキスト ボックスに、Mobility Services Engine のユーザ名とパスワードを入力します。
これは、設定時に作成された Prime Infrastructure 通信ユーザ名とパスワードです。

設定時にユーザ名とパスワードを指定しなかった場合は、デフォルトを使用します。

デフォルトのユーザ名とパスワードはどちらも *admin* です。

（注） 自動インストール スクリプトの実行中にユーザ名とパスワードを変更した場合は、変更後の値をここに入力してください。デフォルト パスワードを変更しなかった場合は、自動インストール スクリプトを再実行してユーザ名とパスワードを変更することを推奨します。

ステップ 8 [HTTPS] チェックボックスをオンにして、Mobility Services Engine とサードパーティ アプリケーションの間の通信を許可します。 デフォルトでは、Prime Infrastructure は MSE との通信に HTTPS を使用します。

ステップ 9 Mobility Services Engine からすべてのサービス割り当てを永久に削除するには、[Delete synchronized service assignments] チェックボックスをオンにします。
このオプションは、ネットワーク設計、有線スイッチ、コントローラ、およびイベント定義に適用されます。 既存のロケーション履歴データは維持されますが、今後ロケーション計算を実行するときには手動サービス割り当てを使用する必要があります。

ステップ 10 [Next] をクリックします。 Prime Infrastructure により、選択されている要素と MSE が自動的に同期されます。
同期完了後、[MSE License Summary] ページが表示されます。 [MSE License Summary] ページから、ライセンスのインストール、ライセンスの追加、ライセンスの削除、アクティベーション ライセンスのインストール、サービス ライセンスのインストールを実行します。 [Select Mobility Service] ページが表示されます。

ステップ 11 Mobility Services Engine 上のサービスを有効にするには、サービスの横にあるチェックボックスをオンにします。 サービスには Context-Aware Service および wIPS が含まれます。
CAS を選択すると、クライアント、不正アクセス ポイント、干渉、有線クライアント、およびタグを追跡できます。

ステップ 12 [Save] をクリックします。

（注） 新しいモビリティ サービス エンジンを追加すると、Prime Infrastructure を使用して、ネットワーク設計（キャンパス、ビルディング、および屋外マップ）、コントローラ、スイッチ（Catalyst シリーズ 3000 のみ）、およびローカル モビリティ サービス エンジンのイベント グループを同期できます。 この同期は、新しい Mobility Services Engine を追加した直後、または後で実行できます。 ローカル データベースと Prime Infrastructure データベースを同期するには、Mobility Services Engine の同期, （19 ページ）を参照してください。

Mobility Services Engine でのサービスの有効化

モビリティ サービス エンジンサービスをイネーブルにするには、次の手順に従います。

ステップ 1 ライセンス ファイルを追加すると、[Select Mobility Service] ページが表示されます。

ステップ 2 Mobility Services Engine 上のサービスを有効にするには、サービスの横にあるチェックボックスをオンにします。 サービスのタイプは次のとおりです。

- [Context Aware Service]：[Context Aware Service] チェックボックスをオンにすると、ロケーション計算を実行するためにロケーション エンジンを選択する必要があります。 CAS を選択すると、クライアント、不正アクセス ポイント、干渉、およびタグを追跡できます。
- [Wireless Intrusion Prevention System]：[Wireless Intrusion Prevention System] チェックボックスをオンにすると、無線およびパフォーマンスの脅威が検出されます。
- [Mobile Concierge Service]：[Mobile Concierge Service] チェックボックスをオンにすると、モバイル デバイスで使用可能なサービスが記述されるサービス アドバタイズメントが提供されます。
- [Location Analytics Service]：[Location Analytics Service] チェックボックスをオンにすると、MSE からの Wi-Fi デバイス位置データを分析するためにパッケージされた各種データ分析ツールを利用できます。

（注） MSE 6.0 以降では、複数のサービス（CAS と wIPS）を同時に有効にできます。 CMX ブラウザ エンジン サービスも利用できます。

ステップ 3 [Next] をクリックして、追跡パラメータを設定します。

ステップ 4 Mobility Services Engine でサービスを有効にすると、[Select Tracking & History Parameters] ページが表示されます。

（注） 追跡パラメータの設定を省略すると、デフォルト値が選択されます。

ステップ 5 追跡するクライアントを選択するには、対応する [Tracking] チェックボックスをオンにします。 追跡パラメータを以下に示します。

- Wired Clients
- Wireless Clients
- Rogue Access Points
  - Exclude Adhoc Rogue APs
- Rogue Clients
- Interferers
- Active RFID Tags

ステップ 6 デバイスの履歴トラッキングを有効にするには、対応するデバイスのチェックボックスをオンにします。 履歴パラメータを以下に示します。

- Wired Stations
- Client Stations
- Rogue Access Points
- Rogue Clients
- Interferers
- Asset Tags

ステップ 7 [Next] をクリックして MSE にマップを割り当てます。

（注） [Assigning Maps] ページは、MSE で有効にするサービスの 1 つとして CAS を選択する場合にだけ使用可能です。

ステップ 8 MSE 追跡パラメータおよび履歴パラメータを設定すると、[Assigning Maps] ページが表示されます。[Assign Maps] ページには以下の情報が表示されます。

- Map Name
- [Type]（ビルディング、フロア、キャンパス）
- Status

ステップ 9 必要なマップ タイプを確認するには、ページで使用可能な [Filter] オプションから [All]、[Campus]、[Building]、[Floor Area]、または [Outdoor Area] を選択します。

ステップ 10 マップを同期するには、[Name] チェックボックスをオンにし、[Synchronize] をクリックします。ネットワーク設計の同期が完了すると、特定のネットワーク設計で AP が割り当てられている適切なコントローラが MSE と自動的に同期されます。 [Done] をクリックして MSE 設定を保存します。

MSE 追跡パラメータおよび履歴パラメータの設定

ステップ 1 Mobility Services Engine でサービスを有効にすると、[Select Tracking & History Parameters] ページが表示されます。

（注） 追跡パラメータの設定を省略すると、デフォルト値が選択されます。

ステップ 2 追跡するクライアントを選択するには、対応する [Tracking] チェックボックスをオンにします。 追跡パラメータを以下に示します。

- Wired Clients
- Wireless Clients
- Rogue Access Points
  - Exclude Adhoc Rogue APs
- Rogue Clients
- Interferers
- Active RFID Tags

ステップ 3 デバイスの履歴トラッキングを有効にするには、対応するデバイスのチェックボックスをオンにします。履歴パラメータを以下に示します。

- Wired Stations
- Client Stations
- Rogue Access Points
- Rogue Clients
- Interferers
- Asset Tags

ステップ 4 [Next] をクリックして MSE にマップを割り当てます。

MSE へのマップの割り当て

（注） [Assigning Maps] ページは、MSE で有効にするサービスの 1 つとして CAS を選択する場合にだけ使用可能です。

MSE にマップを割り当てるには、次の手順に従います。

ステップ 1 MSE 追跡パラメータおよび履歴パラメータを設定すると、[Assigning Maps] ページが表示されます。[Assign Maps] ページには以下の情報が表示されます。

- Map Name
- [Type]（ビルディング、フロア、キャンパス）
- Status

ステップ 2 必要なマップ タイプを確認するには、ページで使用可能な [Filter] オプションから [All]、[Campus]、[Building]、[Floor Area]、または [Outdoor Area] を選択します。

ステップ 3 マップを同期するには、[Name] チェックボックスをオンにし、[Synchronize] をクリックします。ネットワーク設計の同期が完了すると、特定のネットワーク設計で AP が割り当てられている適切なコントローラが MSE と自動的に同期されます。 [Done] をクリックして MSE 設定を保存します。

MSE ライセンス ファイルの削除

MSE ライセンス ファイルを削除するには、次の手順に従います。

ステップ 1 [Services] > [Mobility Service Engine] の順に選択します。
[Mobility Services] ページが表示されます。

ステップ 2 削除する Mobility Services Engine ライセンスを選択するため、対応する [Device Name] チェックボックスをオンにします。

ステップ 3 [Select a command] ドロップダウン リストから [Edit Configuration] を選択します。
[Edit Mobility Services Engine] ダイアログボックスが表示されます。

ステップ 4 [Edit Mobility Services Engine] ダイアログボックスの [Next] をクリックします。
[MSE License Summary] ページが表示されます。

ステップ 5 [MSE License Summary] ページで削除する MSE ライセンス ファイルを選択します。

ステップ 6 [Remove License] をクリックします。

ステップ 7 [OK] をクリックして削除操作を確定するか、または [Cancel] をクリックしてライセンスを削除せずにこのページを閉じます。

ステップ 8 [Next] をクリックして Mobility Services Engine 上でサービスを有効にします。

Prime Infrastructure からのモビリティ サービス エンジンの削除

Prime Infrastructure データベースから 1 つ以上の Mobility Services Engine を削除するには、次の手順に従います。

ステップ 1 [Services] > [Mobility Services] の順に選択します。
[Mobility Services] ページが表示されます。

ステップ 2 削除する Mobility Services Engine を選択するため、対応する [Device Name] チェックボックスをオンにします。

ステップ 3 [Select a command] ドロップダウン リストから [Delete Service(s)] を選択します。 [Go] をクリックします。

ステップ 4 選択したモビリティ サービス エンジンを Prime Infrastructure データベースから削除することを確定するには、[OK] をクリックします。

ステップ 5 削除を中止するには、[Cancel] をクリックします。

デバイスと wIPS 製品認証キーの登録

CAS 要素、wIPS、またはタグのライセンスをシスコに発注すると、製品認証キー（PAK）が配布されます。 Mobility Services Engine 上にインストールするライセンス ファイルを受け取るには、PAK を登録する必要があります。 PAK の登録に成功すると、ライセンス ファイルが電子メールで送信されます。 クライアントおよびワイヤレス IPS の PAK は、シスコに登録します。

インストールするライセンス ファイルを入手するために PAK を登録するには、次の手順に従います。

ステップ 1 Web ブラウザで、http://tools.cisco.com/SWIFT/LicensingUI/Homeに進みます。

ステップ 2 PAK を入力し、[SUBMIT] をクリックします。

ステップ 3 ライセンスの購入内容を確認します。 正しい場合は [Continue] をクリックします。 ライセンス入力ページが表示されます。

（注） ライセンスが正しくない場合は、[TAC Service Request Tool] URL をクリックして問題をレポートしてください。

ステップ 4 [Designate Licensee] ページで、[Host Id] テキスト ボックスに Mobility Services Engine の UDI を入力します。 これは、ライセンスがインストールされている Mobility Services Engine です。

（注） Mobility Services Engine の UDI 情報は、[Services] > [Mobility Services Engine] > [Device Name] > [System] の [General Properties] に表示されます。

ステップ 5 [Agreement] チェックボックスをオンにします。 [Agreement] チェックボックスの下に登録者情報が表示されます。

ステップ 6 登録者とエンド ユーザが異なる場合は、登録者情報の下の [Licensee (End-User)] チェックボックスをオンにしてエンド ユーザ情報を入力します。

ステップ 7 [Continue] をクリックします。 入力したデータの概要が表示されます。

ステップ 8 [Finish and Submit] ページで、登録者データとエンド ユーザ データを確認します。 情報を訂正するには、[Edit Details] をクリックします。 [Submit] をクリックします。` 確認用のページが表示されます。

デバイスおよび wIPS ライセンス ファイルのインストール

Prime Infrastructure からデバイス ライセンスと wIPS ライセンスをインストールできます。 リリース 7.5 以降は、Cisco Engine for Clients and Tags を使用してタグを追跡します。 リリース 7.2 以降からリリース 7.5 にアップグレードした場合にタグのライセンスが検出されると、AeroScout ライセンスとエンジンの削除に関する警告メッセージが表示されます。 承諾すると、すべてのパート

ナー エンジンのサブ サービスが削除され、その後 Cisco Tag Engine サブ サービスがデフォルトで有効になります。パートナーエンジンの排除を承諾しない場合、インストールが続行されます。タグのライセンスが検出されない場合、インストールはそのまま進行します。

[Administration] > [License Center]ページは、リリース 7.3.101.0 以降の仮想ドメインでのみ使用可能です。

PAK の登録後にデバイス ライセンスまたは wIPS ライセンスを Prime Infrastructure に追加するには、次の手順に従います。

ステップ 1 [Administration] > [License Center] を選択します。

ステップ 2 左側のサイドバーのメニューから、[Files] > [MSE Files] を選択します。

ステップ 3 [Add] をクリックします。 [Add a License File] ダイアログボックスが表示されます。

ステップ 4 [MSE Name] ドロップダウン リストから該当する MSE 名を選択します。

（注） 選択されている Mobility Services Engine の UDI が、PAK 登録時に入力したものと一致していることを確認します。

ステップ 5 [Choose File] をクリックし、ライセンス ファイルを参照して選択します。

ステップ 6 [Upload] をクリックします。 新たに追加されたライセンスが MSE ライセンス ファイル リストに表示されます。

第 3 章

Mobility Services Engine の同期

この章では、Cisco ワイヤレス LAN コントローラと Prime Infrastructure を Mobility Services Engine と同期する方法について説明します。

（注） [Services] タブの [Mobility Services Engines]、[Synchronize Services]、[Synchronization History]、[High Availability]、[Context Aware Notifications]、および [MSAP] ページは、リリース 7.3.101.0 で使用できます。

この章の内容は、次のとおりです。

Prime Infrastructure と Mobility Services Engines の同期

ここでは、Prime Infrastructure とモビリティ サービス エンジンを手動および自動的に同期する方法を説明します。

（注） [Services] > [Synchronize Services] ページは、リリース 7.3.101.0 以降の仮想ドメインでのみ使用可能です。

Prime Infrastructure へモビリティ サービス エンジンを追加後、ネットワーク設計（キャンパス、ビルディング、フロア、および屋外マップ）、コントローラ（名前と IP アドレス）、特定の

Catalyst 3000 シリーズおよび 4000 シリーズ スイッチ、およびイベント グループをモビリティ サービス エンジンと同期できます。

- ネットワーク設計：施設全体におけるアクセス ポイントの物理的配置の論理マッピング。 1 つのネットワーク設計は、1 つのキャンパス、そのキャンパスを構成するビルディング、および各ビルディングのフロアという階層構造で構成されています。
- コントローラ：Mobility Services Engine に関連付けられている選択されたコントローラ。 Mobility Services Engine と定期的にロケーション情報を交換します。 定期的な同期により、正確なロケーション情報を維持できます。
- 有線スイッチ：ネットワーク上の有線クライアントへのインターフェイスを提供する有線 Catalyst スイッチ。 定期的な同期により、ネットワーク上の有線クライアントのロケーションが正確に追跡されます。
  - Mobility Services Engine は、Catalyst スタッカブル スイッチ（3750、3750-E、3560、2960、IE-3000 スイッチ）、スイッチ ブレード（3110、3120、3130、3040、3030、3020）、およびスイッチ ポートと同期できます。
  - Mobility Services Engine は、Catalyst 4000 シリーズ スイッチ WS-C4948、WS-C4948-10GE、ME-4924-10GE、WS-4928-10GE、WS-C4900M、WS-X4515、WS-X4516、WS-X4013+、WS-X4013+TS、WS-X4516-10GE、WS-X4013+10GE、WS-X45-SUP6-E、および WS-X45-SUP6-LE とも同期できます。
- イベント グループ：イベントを生成するトリガーを定義する事前定義イベントのグループ。 定期的な同期により、最新の定義イベントが追跡されます。 イベント グループはサードパーティ アプリケーションでも作成できます。 サードパーティ アプリケーションにより作成されたイベント グループの詳細については、データベースの自動同期の設定と Out-of-Sync アラート，（24 ページ）を参照してください。
- サードパーティ要素：要素を MSE と同期する場合、サードパーティ アプリケーションにより MSE にイベント グループが作成されていることがあります。 未使用の要素を削除するか、または未使用の要素をサードパーティ要素としてマークすることができます。
- サービス アドバタイズメント：モバイル コンシェルジュ サービスは、モバイル デバイスにサービス アドバタイズメントを提供します。 これにより、MSE と同期されたサービス アドバタイズメントが示されます。

Mobility Services Engine の同期の前提条件

- 同期を実行する前に、コントローラ、Prime Infrastructure、およびモビリティ サービス エンジン間のソフトウェアの互換性を確認してください。 http://www.cisco.com/en/US/products/ps9742/tsd_products_support_series_home.html で、Mobility Services Engine の最新リリース ノートを参照してください。
- モビリティ サービス エンジン、Prime Infrastructure、およびコントローラ間の通信は、協定世界時（UTC）で実行されます。 各システムで NTP を設定すると、デバイスに UTC 時刻が提供されます。 モビリティ サービス エンジンとその関連コントローラは、同一 NTP サーバ

と同一 Prime Infrastructure サーバにマップする必要があります。 NTP サーバは、コントローラ、Prime Infrastructure、およびモビリティ サービス エンジン間で時刻を自動的に同期する必要があります。 ただし、MSE のタイムゾーンは引き続き UTC に設定する必要があります。 これは、wIPS アラームには MSE 時刻を UTC に設定する必要があるからです。

サードパーティ要素の操作

要素を MSE と同期する場合、MSE にサードパーティ アプリケーションによって作成されたイベント グループがあることがあります。未使用の要素を削除するか、または未使用の要素をサードパーティ要素としてマークすることができます。

要素の削除またはサード パーティ要素としてのマーキング

要素を削除またはサード パーティ要素としてマークするには、次の手順に従います。

ステップ 1 [Services] > [Synchronize Services] の順に選択します。
[Network Designs] ページが表示されます。

ステップ 2 [Network Designs] ページで、左側のサイドバーのメニューから [Third Party Elements] を選択します。
[Third Party Elements] ページが表示されます。

ステップ 3 1 つ以上の要素を選択します。

ステップ 4 次のいずれかのボタンをクリックします。

- [Delete Event Groups]：選択されているイベント グループを削除します。
- [Mark as 3rd Party Event Group(s)]：選択されているイベント グループをサードパーティ イベント グループとしてマークします。

コントローラと Mobility Services Engine の同期

ここでは、コントローラを同期し、MSE を任意のワイヤレス コントローラに割り当て、ネットワーク設計、コントローラ、有線スイッチ、またはイベント グループを Mobility Services Engine から割り当て解除する方法について説明します。

ここでは、次の内容について説明します。

- コントローラ、Catalyst スイッチ、またはイベント グループの同期, （22 ページ）
- コントローラへの MSE の割り当て, （23 ページ）

• ネットワーク設計、有線スイッチ、またはイベント グループの MSE からの割り当て解除, （24 ページ）

コントローラ、Catalyst スイッチ、またはイベント グループの同期

ネットワーク設計、コントローラ、Catalyst スイッチ、またはイベント グループを Mobility Services Engine と同期するには、次の手順に従います。

ステップ 1 [Services] > [Synchronize Services] の順に選択します。
左側のサイドバーのメニューには、[Network Designs]、[Controllers]、[Event Groups]、[Wired Switches]、[Third Party Elements]、および [Service Advertisements] のオプションがあります。

ステップ 2 左側のサイドバーのメニューから、該当するメニュー オプションを選択します。

ステップ 3 Mobility Services Engine にネットワーク設計を割り当てるには、[Synchronize Services] ページの左側のサイドバーのメニューから、[Network Designs] を選択します。
[Network Designs] ページが表示されます。

ステップ 4 対応する [Name] チェックボックスをオンにして、Mobility Services Engine と同期するすべてのマップを選択します。

（注） リリース 6.0 では、Mobility Services Engine に割り当てることができる最も詳細なレベルはキャンパス レベルです。 リリース 7.0 以降では、このオプションはフロア レベルまで拡大されました。 たとえば、floor1 を MSE 1 に、floor2 を MSE 2 に、floor3 を MSE 3 に割り当てることを選択できます。

ステップ 5 [Change MSE Assignment] をクリックします。

ステップ 6 マップと同期する Mobility Services Engine を選択します。

ステップ 7 [MSE Assignment] ダイアログボックスで次のいずれかをクリックします。

- [Save]：Mobility Services Engine 割り当てを保存します。 次のメッセージが [Network Designs] ページの [Messages] 列に黄色の矢印アイコンとともに表示されます。

  To be assigned - Please synchronize.

- [Cancel]：Mobility Services Engine 割り当ての変更内容を取り消し、[Network Designs] ページに戻ります。

  また、[Reset] をクリックすると、Mobility Services Engine の割り当てが取り消されます。

（注） ネットワーク設計には、キャンパス内のフロアや、複数のビルディングが含まれている大規模キャンパス（各ビルディングが異なる Mobility Services Engine によりモニタされる）などがあります。 このため、単一ネットワーク設計を複数の Mobility Services Engine に割り当てる必要がある場合があります。 ネットワーク設計割り当てでは、同期対象のコントローラが自動的に選択されます。

ステップ 8 [Synchronize] をクリックし、Mobility Services Engine データベースを更新します。

項目が同期されると、同期済みエントリの [Sync. Status] 列に緑色の 2 つの矢印のアイコンが表示されます。

有線スイッチまたはイベント グループを Mobility Services Engine に割り当てるときにも同じ手順を使用できます。 Mobility Services Engine にコントローラを割り当てるには、コントローラと Mobility Services Engine の同期を参照してください。

コントローラへの MSE の割り当て

サービス単位（CAS または wIPS）で Mobility Services Engine を任意のワイヤレス コントローラに割り当てるには、次の手順に従います。

ステップ 1 [Services] > [Synchronize Services] の順に選択します。

ステップ 2 [Network Designs] ページで、左側のサイドバーのメニューから [Controller] を選択します。

ステップ 3 対応する [Name] チェックボックスをオンにして、Mobility Services Engine に割り当てるコントローラを選択します。

ステップ 4 [Change MSE Assignment] をクリックします。

ステップ 5 コントローラと同期する必要がある Mobility Services Engine を選択します。

ステップ 6 [Choose MSEs] ダイアログボックスで次のいずれかをクリックします。

- [Save]：Mobility Services Engine 割り当てを保存します。 次のメッセージが [Controllers] ページの [Messages] 列に黄色の矢印アイコンとともに表示されます。

  To be assigned - Please synchronize.

- [Cancel]：Mobility Services Engine 割り当ての変更内容を取り消し、[Controllers] ページに戻ります。

  また、[Reset] をクリックすると、Mobility Services Engine の割り当てが取り消されます。

ステップ 7 [Synchronize] をクリックし、同期プロセスを実行します。

ステップ 8 Mobility Services Engine が、選択されているサービスの各コントローラだけと通信していることを確認します。 これは、ステータス ページの [NMSP status] リンクをクリックして確認できます。

（注） コントローラの同期後、関連付けられているコントローラでタイムゾーンが設定されていることを確認します。

（注） Mobility Services Engine と同期するコントローラの名前は固有でなければなりません。 同じ名前のコントローラが 2 つある場合は 1 つのコントローラだけが同期されます。 Catalyst スイッチまたはイベント グループを Mobility Services Engine に割り当てるときにも同じ手順を使用できます。

（注） スイッチは、1 つの Mobility Services Engine とだけ同期できます。 ただし、Mobility Services Engine には複数のスイッチを接続できます。

ネットワーク設計、有線スイッチ、またはイベント グループの MSE からの割り当て解除

Mobility Services Engine からネットワーク設計、コントローラ、有線スイッチ、またはイベント グループの割り当てを解除するには、次の手順に従います。

ステップ 1 [Services] > [Synchronize Services] の順に選択します。

ステップ 2 左側のサイドバーのメニューから、該当するメニュー オプションを選択します。

ステップ 3 [Name] チェックボックスをオンにして 1 つ以上の要素を選択し、[Change MSE Assignment] をクリックします。
[Choose MSEs] ダイアログボックスが表示されます。

ステップ 4 該当するタブで 1 つ以上の要素をクリックし、[Change MSE Assignment] をクリックします。 [Choose MSEs] ダイアログボックスが表示されます。

ステップ 5 Mobility Services Engine に要素を関連付けない場合は、[CAS] または [wIPS] のいずれかのチェックボックスをオンにして Mobility Services Engine の選択を解除します。

ステップ 6 [Save] をクリックして割り当ての変更を保存します。

ステップ 7 [Synchronize] をクリックします。
[Sync Status] 列がブランクになります。

データベースの自動同期の設定と Out-of-Sync アラート

Prime Infrastructure とモビリティ サービス エンジンのデータベースの手動同期はただちに実行されます。 ただし、将来のデプロイメントの変更（マップやアクセス ポイントの位置の変更など）が原因で、再同期までは、ロケーションの計算やアセットの追跡が正しく行われないことがあります。

同期していない状態が発生しないようにするため、Prime Infrastructure を使用して同期を実行します。 このポリシーにより、Prime Infrastructure と Mobility Services Engine のデータベース間の同期が定期的に実行され、関連アラームがすべてクリアされます。

1 つ以上の同期コンポーネントに対する変更は、Mobility Services Engine と自動的に同期されます。 たとえば、アクセス ポイントが設置されているフロアを特定の Mobility Services Engine と同期し、その後 1 つのアクセス ポイントが同じフロアの新しいロケーション、または別のフロア（Mobility Services Engine と同期されるフロア）に移動すると、アクセス ポイントの変更後のロケーションが自動的に伝達されます。

Prime Infrastructure と MSE が同期されるようにするため、バックグラウンドでスマート同期が実行されます。

ここでは、次の内容について説明します。

データベースの自動同期の設定

スマート同期を設定するには、次の手順に従います。

ステップ 1 [Administration] > [Background Tasks] の順に選択します。

ステップ 2 [Mobility Service Synchronization] チェックボックスをオンにします。
[Mobility Services Synchronization] ページが表示されます。

ステップ 3 Mobility Services Engine が Out-of-Sync アラートを送信するように設定するには、[Out of Sync Alerts] の [Enabled] チェックボックスをオンにします。

ステップ 4 スマート同期を有効にするには、[Smart Synchronization] の [Enabled] チェックボックスをオンにします。

（注） スマート同期は、Mobility Services Engine に割り当てられていない要素（ネットワーク設計、コントローラ、またはイベント グループ）には適用されません。 ただし、これらの未割り当て要素に関する out-of-sync アラームは生成されます。 スマート同期をこれらの要素に適用するには、これらの要素を Mobility Services Engine に手動で割り当てる必要があります。

（注） Prime Infrastructure に Mobility Services Engine が追加されると、Prime Infrastructure のデータは常に、Mobility Services Engine と同期するプライマリ コピーとして扱われます。 モビリティ サービス エンジンに含まれているが、Prime Infrastructure には含まれていない同期対象のネットワーク設計、コントローラ、イベント グループ、および有線スイッチはすべて、モビリティ サービス エンジンから自動的に削除されます。

ステップ 5 スマート同期の実行間隔を分数単位で入力します。
デフォルトでは、スマート同期は有効になっています。

ステップ 6 [Submit] をクリックします。`
スマート コントローラの割り当てと選択のシナリオについては、スマート コントローラの割り当てと選択のシナリオ，（25 ページ）を参照してください。

スマート コントローラの割り当てと選択のシナリオ

シナリオ 1

[Synchronize Services] ページの [Network Designs] メニューで、コントローラからのアクセス ポイントが 1 つ以上存在するフロアを Mobility Services Engine と同期することを選択した場合、アクセス ポイントに接続しているコントローラが、CAS サービスの Mobility Services Engine への割り当て対象として自動的に選択されます。

シナリオ 2

コントローラからの 1 つ以上のアクセス ポイントが、Mobility Services Engine と同期されるフロアに配置されている場合、アクセスポイントに接続しているコントローラは、CASサービスの同じ Mobility Services Engine に自動的に割り当てられます。

シナリオ 3

アクセス ポイントがフロアに追加され、Mobility Services Engine に割り当てられます。 このアクセス ポイントをコントローラ A からコントローラ B に移動すると、コントローラ B が Mobility Services Engine と自動的に同期されます。

シナリオ 4

MSEと同期するフロアに配置されているすべてのアクセスポイントが削除されると、そのコントローラは自動的に Mobility Services Engine 割り当てから削除されるか、または同期されなくなります。

Out-of-Sync アラーム

Out-of-Sync アラームは、重大度が Minor（黄色）のアラームであり、次の条件に対して出されます。

- Prime Infrastructure で要素が変更される（自動同期ポリシーによりこれらの要素がプッシュされます）
- コントローラ以外の要素がモビリティ サービス エンジン データベースに存在するが、Prime Infrastructure に存在しない
- 要素が Mobility Services Engine に割り当てられていない（自動同期ポリシーは適用されません）

Out-of-Sync アラームは、次の条件が発生するとクリアされます。

- Mobility Services Engine が削除される

（注） Mobility Services Engine を削除すると、そのシステムの Out-of-Sync アラームも削除されます。 また、使用可能な最後の Mobility Services Engine を削除すると、「どのサーバにも割り当てられていない要素」のイベントに対するアラームが削除されます。

- 要素が手動または自動で同期される

- ユーザがアラームを手動でクリアする（ただしスケジュールされているタスクが次回実行されるときに、アラームが再び表示される可能性があります）

Mobility Services Engine 同期ステータスの表示

Prime Infrastructure でサービスの同期機能を使用して、ネットワーク設計、コントローラ、スイッチ、およびイベント グループとモビリティ サービス エンジンとの同期のステータスを表示できます。

ここでは、次の内容について説明します。

Mobility Services Engine 同期ステータスの表示

同期ステータスを表示するには、次の手順に従います。

ステップ 1 [Services] > [Synchronize Services] の順に選択します。

ステップ 2 左側のサイドバーのメニューから、[Network Designs]、[Controllers]、[Wired Switches]、[Third Party Elements]、または [Service Advertisements] を選択します。
各要素の [Sync. Status] 列に、 同期ステータスが表示されます。 緑色の 2 つの矢印のアイコンは、対応する要素が指定サーバ（Mobility Services Engine など）と同期されていることを示します。 灰色の 2 つの矢印と赤い円のアイコンは、対応する項目が指定のサーバと同期していないことを示します。

[Message] 列には、要素が同期していない場合の障害の原因が表示されます。

[Monitor] > [Maps] > [System Campus] > [Building] > [Floor] を選択して、同期ステータスを表示することもできます。

このビルディングはキャンパス内のビルディング、フロアはキャンパス ビルディング内の特定のフロアです。

左側のサイドバーのメニューの [MSE Assignment] オプションに、フロアが現在割り当てられている Mobility Services Engine が表示されます。 このページから Mobility Services Engine 割り当てを変更することもできます。

同期履歴の表示

Mobility Services Engine の過去 30 日間の同期履歴を表示できます。 アラームが自動的にクリアされるため、これは特に自動同期が有効な場合に便利です。 同期履歴には、クリアされたアラームの要約が表示されます。

同期履歴を表示するには、[Services] > [Synchronization History] の順に選択します。 [Synchronization History] ページが表示されます。 次の表に、[Synchronization History] ページ のパラメータを示します。

表 *2*：*[Synchronization History]* ページ

テキスト ボックス	説明
Timestamp	同期が実行された日時。
Server	Mobility Services Engine サーバ。
Element Name	同期された要素の名前。
Type	同期された要素のタイプ。
Sync Operation	実行された同期動作。 [Update]、[Add]、または [Delete] です。
Generated By	同期の方法。 [Manual] または [Automatic] です。
Status	同期のステータス。 [Success] または [Failed] のいずれかです。
メッセージ	同期に関するその他のメッセージ。

第 4 章

ハイ アベイラビリティの設定

この章では、MSE 上でハイ アベイラビリティを設定する方法について説明します。 Mobility Services Engine は、複数のモビリティ アプリケーションをホストするプラットフォームです。アクティブな各 MSE は別の非アクティブ インスタンスによりバックアップされます。 アクティブな MSE はプライマリ MSE、非アクティブな MSE はセカンダリ MSE と呼ばれます。

ハイ アベイラビリティ システムの主要なコンポーネントは、ヘルス モニタです。 ヘルス モニタは、ハイ アベイラビリティ セットアップを設定、管理、モニタします。 プライマリ MSE とセカンダリ MSE の間でハートビートが維持されます。 ヘルス モニタは、データベースのセットアップ、ファイルのレプリケーション、アプリケーションのモニタリングを行います。 プライマリ MSE で障害が発生し、セカンダリ MSE に切り替わると、プライマリ MSE の仮想アドレスが透過的に切り替わります。

（注） [Services] タブの [Mobility Services Engines]、[Synchronize Services]、[Synchronization History]、[High Availability]、[Context-Aware Notifications]、および [MSAP] ページは、リリース 7.3 の仮想ドメインでのみ使用できます。

この章の内容は、次のとおりです。

ハイ アベイラビリティ アーキテクチャの概要

ここでは、ハイ アベイラビリティ アーキテクチャの概要について説明します。

- アクティブな各プライマリ MSE は別の非アクティブ インスタンスによりバックアップされます。 セカンダリ MSE の目的は、プライマリ MSE のアベイラビリティと状態をモニタすることです。 セカンダリ MSE は、フェールオーバー手順の開始後にアクティブになります。
- フェールオーバー手順は手動または自動です。
- 1 つのセカンダリ MSE では 2 つのプライマリ MSE をサポートできます。
- 登録されているプライマリ MSE ごとに 1 つのソフトウェアおよびデータベース インスタンスが存在します。

組み合わせ表

次の表 に、サーバ タイプの組み合わせに関する情報を示します。

表 *3*：組み合わせ表

	セカンダリ サーバ タイプ							
プライマリ サーバ タイプ		3310	3350	3355	VA-2	VA-3	VA-4	VA-5
	3310	Y	Y	Y	N	N	N	N
	3350	N	Y	Y	N	N	N	N
	3355	N	Y	Y	N	N	N	N
	VA-2	N	N	N	Y	Y	Y	Y
	VA-3	N	N	N	N	Y	Y	Y
	VA-4	N	N	N	N	N	Y	Y
	VA-5	N	N	N	N	N	N	Y

ハイ アベイラビリティのガイドラインと制約事項

- ヘルス モニタ IP と仮想 IP の両方に Prime Infrastructure からアクセスできるようにする必要があります。

- ヘルス モニタ IP と仮想 IP は常に異なる IP でなければなりません。 ヘルス モニタと仮想インターフェイスは、同じインターフェイス上にあっても別のインターフェイス上にあってもかまいません。
- 手動フェールオーバーと自動フェールオーバーのいずれかを使用できます。 フェールオーバーは、一時的なものであると見なす必要があります。 故障した MSE をできるだけ早く復旧して、フェールバックを再開する必要があります。 故障した MSE の復旧に時間がかかるほど、セカンダリ MSE を共有する他の MSE をフェールオーバー サポートなしで稼働する時間が長くなります。
- 手動フェールバックと自動フェールバックのいずれかを使用できます。
- プライマリ MSE とセカンダリ MSE は、同じソフトウェア バージョンを実行する必要があります。
- WAN 上のハイ アベイラビリティはサポートされません。
- LAN 上のハイ アベイラビリティは、プライマリ MSE とセカンダリ MSE の両方が同じサブネット内にある場合に限りサポートされます。
- プライマリとセカンダリの MSE が通信するポートを開ける（ネットワーク ファイアウォール、アプリケーション ファイアウェイ、ゲートウェイなどでブロックしない）必要があります。

ハイ アベイラビリティのフェールオーバー シナリオ

プライマリ MSE で障害が検出されると、次のイベントが発生します。

（注） 1 つのセカンダリ MSE が複数のプライマリ MSE をバックアップできます。

- セカンダリ MSE のヘルス モニタにより、プライマリ MSE が機能していないこと（ハードウェア障害、ネットワーク障害など）が確認されます。
- 自動フェールオーバーが有効に設定されている場合、セカンダリ MSE がただちに起動し、プライマリ MSE の該当するデータベースを使用します。 自動フェールオーバーが無効にされている場合は、フェールオーバーを手動で開始するかどうかを確認する電子メールが管理者に送信されます。
- 手動フェールオーバーが設定されていると、電子メールが MSE アラーム用に設定されている場合にのみ電子メールが送信されます。 手動フェールオーバーが設定されていて、呼び出されない場合、フェールバックの必要はありません。
- フェールバックが呼び出され、プライマリ MSE がすべての操作を実行するようになります。
- フェールオーバー操作の結果はヘルス モニタ UI でイベントとして示され、クリティカル アラームが管理者に送信されます。

フェールバック

セカンダリ MSE がすでにプライマリ MSE をフェールオーバーしている場合、プライマリ MSE が通常の状態に戻ると、フェールバックを呼び出すことができます。

フェールバックが発生するのは、セカンダリ MSE がプライマリ インスタンスに対して次のいずれかの状態である場合だけです。

- セカンダリ MSE が実際にプライマリ MSE をフェールオーバーしている。
- 手動でのフェールオーバーが設定されているが、管理者が呼び出さなかった。
- プライマリ MSE で障害が発生したが、エラーが検出されたか、またはセカンダリ MSE が別のプライマリ MSE をフェールオーバーしていることが原因で、セカンダリ MSE が引き継ぐことができない。
- フェールバックは、障害が発生したプライマリ MSE を管理者が起動する場合にだけ行われます。

HA ライセンス

ハイ アベイラビリティでは、プライマリおよびセカンダリ仮想アプライアンスでアクティベーション ライセンスが必要です。 セカンダリ MSE では、CAS または wIPS ライセンスは必要ありません。 プライマリ MSE のみで必要です。

MSE でのハイ アベイラビリティの設定

MSE でハイ アベイラビリティを設定するには、次の 操作を行う必要があります。

- MSE ソフトウェアのインストール中に、コマンドライン クライアントを使用して特定の設定を行う必要があります。
- Prime Infrastructure UI からプライマリ MSE とセカンダリ MSE を組み合わせます。

（注） デフォルトでは、すべての MSE がプライマリとして設定されます。 ハイ アベイラビリティ サポートを使用しない場合、および古いリリースからのアップグレードを実行している場合は、引き続き MSE の古い IP アドレスを使用してください。 ハイ アベイラビリティをセットアップするには、ヘルス モニタの IP アドレスを設定する必要があります。 したがって、ヘルス モニタが仮想 IP アドレスになります。

プライマリ MSE でハイ アベイラビリティを設定するには、次の手順に従います。

ステップ 1 プライマリとセカンダリの間のネットワーク接続が機能しており、すべての必要なポートが開いていることを確認します。

ステップ 2 正しいバージョンの MSE をプライマリ MSE 上にインストールします。

ステップ 3 他のプライマリ MSE 上およびセカンダリ MSE 上でロードされているリリース バージョンと同じ MSE リリース バージョンが、新しいプライマリ MSE 上にもロードされていることを確認します。

ステップ 4 プライマリ MSE で次のコマンドを入力します。

```
/opt/mse/setup/setup.sh
----------------------------------------------------------------
Welcome to the appliance setup.
Please enter the requested information.  At any prompt,
enter ^ to go back to the previous prompt. You may exit at
any time by typing <Ctrl+C>.
You will be prompted to choose whether you wish to configure a
parameter, skip it, or reset it to its initial default value.
Skipping a parameter will leave it unchanged from its current
value.
Changes made will only be applied to the system once all the
information is entered and verified.
----------------------------------------------------------------
```

ステップ 5 ホスト名を設定します。

```
Current hostname=[mse]
Configure hostname? (Y)es/(S)kip/(U)se default [Skip]:
```

ホスト名は、ネットワーク上のデバイスを識別できる一意の名前にしてください。ホスト名は、文字で開始し、文字または数字で終了し、文字、数字、およびダッシュだけを含みます。

ステップ 6 ドメイン名を設定します。

デバイスが属するネットワーク ドメインのドメイン名を入力します。ドメイン名は、文字で開始し、*.com* などの有効なドメイン名サフィックスで終了します。ドメイン名には、文字、数字、ダッシュ、ピリオドを使用できます。

```
Current domain=[]
Configure domain name? (Y)es/(S)kip/(U)se default [Skip]:
```

ステップ 7 HA ロールを設定します。

```
Current role=[Primary]
Configure High Availability?  (Y)es/(S)kip/(U)se default [Skip]:
High availability role for this MSE (Primary/Secondary):
Select role [1 for Primary, 2 for Secondary] [1]: 1
Health monitor interface holds physical IP address of this MSE server.
This IP address is used by Secondary, Primary MSE servers and Prime Infrastructure to communicate

among themselves
Select Health Monitor Interface [eth0/eth1] [eth0]:eth0
----------------------------------------------------------------------
```

```
Direct connect configuration facilitates use of a direct cable connection between the primary and
 secondary MSE servers.
This can help reduce latencies in heartbeat response times, data replication and failure detection
 times.
Please choose a network interface that you wish to use for direct connect. You should appropriately
 configure the respective interfaces.
\"none\" implies you do not wish to use direct connect configuration.
------------------------------------------------------------------
```

ステップ 8 イーサネット インターフェイス パラメータを設定します。

```
Select direct connect interface [eth0/eth1/none] [none]: eth0
Enter a Virtual IP address for first this primary MSE server:
Enter Virtual IP address [172.31.255.255]:
Enter the network mask for IP address 172.31.255.255.
Enter network mask [255.255.255.0]:
Current IP address=[172.31.255.255]
Current eth0 netmask=[255.255.255.0]
Current gateway address=[172.31.255.256
Configure eth0 interface parameters? (Y)es/(S)kip/(U)se default [Skip]:
```

ステップ 9 「eth1」インターフェイス パラメータの入力を求められた場合、Skip と入力して次の手順に進みます。 2 つめの NIC は操作に必要ではありません。

```
Configure eth1 interface parameters? (Y)es/(S)kip/(U)se default [Skip]:
```

ステップ 10 セカンダリ MSE のホスト名を設定します。

```
Current hostname=[]
Configure hostname? (Y)es/(S)kip/(U)se default [Skip]:
```

ステップ 11 ドメイン名を設定します。

```
Current domain=
Configure domain name? (Y)es/(S)kip/(U)se default [Skip]:
```

ステップ 12 HA ロールを設定します。

```
Current role=[Primary]
Configure High Availability?  (Y)es/(S)kip/(U)se default [Skip]:
High availability role for this MSE (Primary/Secondary)
Select role [1 for Primary, 2 for Secondary] [1]: 2
Health monitor interface holds physical IP address of this MSE server.
This IP address is used by Secondary, Primary MSE servers and Prime Infrastructure to
communicate among themselves
Select Health Monitor Interface [eth0/eth1] [eth0]: [eth0/eth1]
------------------------------------------------------------------
Direct connect configuration facilitates use of a direct cable connection between the primary and
 secondary MSE servers.
This can help reduce latencies in heartbeat response times, data replication and failure detection
 times.
Please choose a network interface that you wish to use for direct connect. You should appropriately
 configure the respective interfaces.
\"none\" implies you do not wish to use direct connect configuration.
------------------------------------------------------------------
```

ステップ 13 イーサネット インターフェイス パラメータを設定します。

```
Select direct connect interface [eth0/eth1/none] [none]: eth1
Enter a Virtual IP address for first this primary MSE server
Enter Virtual IP address [172.19.35.61]:
Enter the network mask for IP address 172.19.35.61:
Enter network mask [255.255.254.0]:
Current IP address=[172.19.35.127]
Current eth0 netmask=[255.255.254.0]
Current gateway address=[172.19.34.1]
Configure eth0 interface parameters? (Y)es/(S)kip/(U)se default [Skip]:
```

ステップ 14 プライマリ MSE とセカンダリ MSE の両方を設定したら、Prime Infrastructure UI を使用してプライマリ MSE とセカンダリ MSE の組み合わせを設定する必要があります。

ステップ 15 プライマリ MSE を適切に追加したら、[Services] > [High Availability] の順に選択するか、または [Services] > [Mobility Services Engine] ページを選択してこのページでプライマリ MSE デバイスをクリックし、左側のサイドバーのメニューから [HA Configuration] > [Service High Availability] の順に選択します。
[HA Configuration] ページが表示されます。

ステップ 16 プライマリ MSE とペアにするセカンダリ デバイスの名前を入力します。

ステップ 17 セカンダリ IP アドレス（セカンダリ MSE のヘルス モニタ IP アドレス）を入力します。

ステップ 18 セカンダリのパスワードを入力します。 これは、MSE 上で設定されている Prime Infrastructure 通信パスワードです。

ステップ 19 フェールオーバー タイプを指定します。 [Failover Type] ドロップダウン リストから [Manual] または [Automatic] を選択できます。 10 秒後にシステムがフェールオーバーします。 セカンダリ サーバは、プライマリ サーバからの次のハートビートを最大 10 秒間待機します。 10 秒以内にハートビートを受信しないと、失敗が宣言されます。

ステップ 20 [Failback Type] ドロップダウン リストから [Manual] または [Automatic] を選択して、フェールバック タイプを指定します。

ステップ 21 [Long Failover Wait] に秒単位で値を指定します。
10 秒後にシステムがフェールオーバーします。 最大フェールオーバー待機時間は 2 秒です。

ステップ 22 [Save] をクリックします。
ペアリングと同期が自動的に行われます。

ステップ 23 プライマリ MSE からハートビートを受信しているかどうかを確認するには、[Services] > [Mobility Services Engine] の順に選択するか、[Device Name] をクリックして設定されているパラメータを表示します。

ステップ 24 左側のサイドバーのメニューから [HA Configuration] > [Service High Availability] の順に選択します。
プライマリ MSE からハートビートを受信しているかを確認します。

ハイアベイラビリティについて設定されているパラメータの表示

ハイ アベイラビリティについて設定されているパラメータを表示するには、次の手順に従います。

ステップ 1 [Services] > [High Availability] の順に選択します。

ステップ 2 [Device Name] をクリックして、設定されているフィールドを表示します。
[HA Configuration] ページが表示されます。

ステップ 3 左側のサイドバー メニューから [Services High Availability] > [HA Configuration] の順に選択します。 [HA Configuration] ページには次の情報が表示されます。

- Primary Health Monitor IP
- Secondary Device Name
- Secondary IP Address
- Secondary Password
- Failover Type
- Failback Type
- Long Failover Wait

ハイ アベイラビリティ ステータスの表示

ハイ アベイラビリティ ステータスを表示するには、次の手順に従います。

ステップ 1 [Services] > [High Availability] の順に選択します。

ステップ 2 [Device Name] をクリックして、該当するステータスを表示します。
[HA Configuration] ページが表示されます。

ステップ 3 左側のサイドバーのメニューから [HA Status] を選択します。 [HA Configuration] ページには次の情報が表示されます。

- Current high Availability Status
  - [Status]：プライマリ MSE インスタンスとセカンダリ MSE インスタンスが正しく同期されているかどうかを示します。

- [Heartbeats]：プライマリ MSE からハートビートを受信しているかどうかを示します。
- [Data Replication]：プライマリ データベースとセカンダリ データベース間でデータ レプリケーションが実行されているかどうかを示します。
- [Mean Heartbeat Response Time]：プライマリ MSE インスタンスとセカンダリ MSE インスタンス間での平均ハートビート応答時間を示します。

- [Event Log]：MSE により生成されるすべてのイベントを表示します。 最新 20 イベントを表示できます。

第 5 章

MSE 配信モード

Cisco MSE は、さまざまなパフォーマンス特性を持つ物理アプライアンスにプリインストールされます。 MSE は、物理アプライアンスと仮想アプライアンスの 2 つのモードで提供されます。

この章の内容は、次のとおりです。

物理アプライアンス

物理アプライアンスに MSE を配置する場合、標準の License Center UI を使用して新規ライセンスを追加できます。 物理アプライアンスに MSE を配置する場合、ライセンス インストール プロセスは Cisco UDI（Unique Device Identifier）に基づきます。 Cisco Prime Infrastructure UI で [**Administration**] > [**License Center**] の順に選択して、ライセンスを追加します。

（注） 仮想アプライアンス ライセンスは物理アプライアンスでは使用できません。

仮想アプライアンス

MSE は、下位レベル、ハイ エンド、および超ハイ エンドの展開をサポートするために、仮想アプライアンスとしても提供されます。 仮想アプライアンスに MSE を配置する場合、ライセンスは、UDI ではなく、VUDI（Virtual Unique Device Identifier）に対して検証されます。

（注） MSE は、リリース 7.2 以降の仮想アプライアンスとして使用できます。 仮想アプライアンスは、他のサービスのライセンスをインストールする前に、最初にアクティブにする必要があります。

MSE 仮想アプライアンス ソフトウェアは、Open Virtualization Archive（OVA）ファイルとして配布されます。 MSE 仮想アプライアンスは、VMware 環境でサポートされる OVF を展開するための方法のいずれかを使用してインストールできます。 開始する前に、MSE 仮想アプライアンスの配布アーカイブが、vSphere Client を実行しているコンピュータからアクセス可能な場所にあることを確認します。

仮想アプライアンスの場合は、アクティベーション ライセンスが必要です。 アクティベーション ライセンスがない場合、MSE は評価モードで開始されます。 サービス ライセンスがホスト上に存在する場合でも、アクティベーション ライセンスがインストールされていないとサービス ライセンスは拒否されます。

（注） VMware 環境の設定の詳細については、VMware vSphere 4.0 のマニュアルを参照してください。

MSE を初めてインストールしている場合は [**Services**] > [**Mobility Services Engine**] > [**Add Mobility Services Engine**] ページを使用して、仮想アプライアンス ライセンスを追加および削除できます。または、[**Administration**] > [**License Center**] ページを使用してライセンスを追加または削除できます。

Mobility Services Engine ウィザードを使用したライセンスの追加およびライセンスの削除については、Mobility Services Engine とライセンスの追加および削除およびMSE ライセンス ファイルの削除, （16 ページ）を参照してください。

ここでは、次の内容について説明します。

オペレーティング システムの要件

次のオペレーティング システムがサポートされています。

- Red Hat Linux Enterprise Server 5.4 64 ビット オペレーティング システム インストールがサポートされています。
- Red Hat Linux バージョンでは、ローカル ストレージまたはファイバ チャネル経由の SAN のいずれかを備えた VMware ESX/ESXi バージョン 4.1 以降がサポートされています。

（注） 仮想アプライアンスには、UCA および ESX/ESXi の導入を推奨します。

クライアントの要件

MSE ユーザ インターフェイスには、Google Chrome プラグインまたは Mozilla Firefox 3.6 以降のリリースとともに Microsoft Internet Explorer 7.0 以降が必要です。

（注） サードパーティのブラウザ拡張は有効にしないことを強く推奨します。 Internet Explorer では、[Tools] > [Internet Options] を選択して、[Advanced] タブで [Enable third-party browser extensions] チェックボックスを選択解除することで、サードパーティのブラウザ拡張を無効にできます。

ブラウザを実行するクライアントには、最小で 1 GB のメモリと 2 GHz のプロセッサが必要です。クライアント デバイスでは、CPU やメモリを大量に使用するアプリケーションを実行しないでください。

仮想アプライアンスのサイジング

次の表に、仮想アプライアンスのサイジング情報を示します。

表 *4*：仮想アプライアンスのサイジング

サポートされるライセンス（個別）				
プライマリ ESM				
仮想アプライアンスレベル	仮想アプライアンス合計（ライセンス）	仮想 wIPS ライセンス		
2 GHz エンドポイント	2000	非サポート		
6000				
5 GHz エンドポイント	10000			
6000				

物理アプライアンスでの MSE の再インストール

物理アプライアンスにMSEをインストールするには、root権限が必要です。 物理アプライアンスに MSE を再インストールするには、次の手順を実行します。

ステップ 1 提供される MSE ソフトウェア イメージ DVD を挿入します。 システムがブートし、コンソールが表示されます。

ステップ 2 MSE ソフトウェア イメージを再インストールするには、オプション 1 を選択します。 システムがリブートし、[configure appliance] 画面が表示されます。

ステップ 3 初期設定パラメータを入力すると、システムが再度リブートします。 DVD を取り出し、手順に従って MSE サーバを起動します。

MSE 仮想アプライアンスの配置

ここでは、[Deploy OVF] ウィザードまたはコマンド ラインから vSphere Client を使用して ESXi ホストに MSE 仮想アプライアンスを展開する方法について説明します。 ここでは、次の内容について説明します。

- VMware vSphere Client からの MSE 仮想アプライアンスの展開, （43 ページ）
- MSE 仮想アプライアンス VM を起動するための基本設定, （46 ページ）
- コマンドライン クライアントを使用した MSE 仮想アプライアンスの展開, （47 ページ）

VMware vSphere Client からの MSE 仮想アプライアンスの展開

MSE 仮想アプライアンスは、vSphere Client を使用して ESXi に展開できる OVA ファイルとして配布されます。 OVA は、項目の集合を単一のアーカイブにしたものです。 vSphere Client では、この項で説明されているように、[Deploy OVA] ウィザードを使用して MSE 仮想アプライアンス アプリケーションを実行する仮想マシンを作成できます。

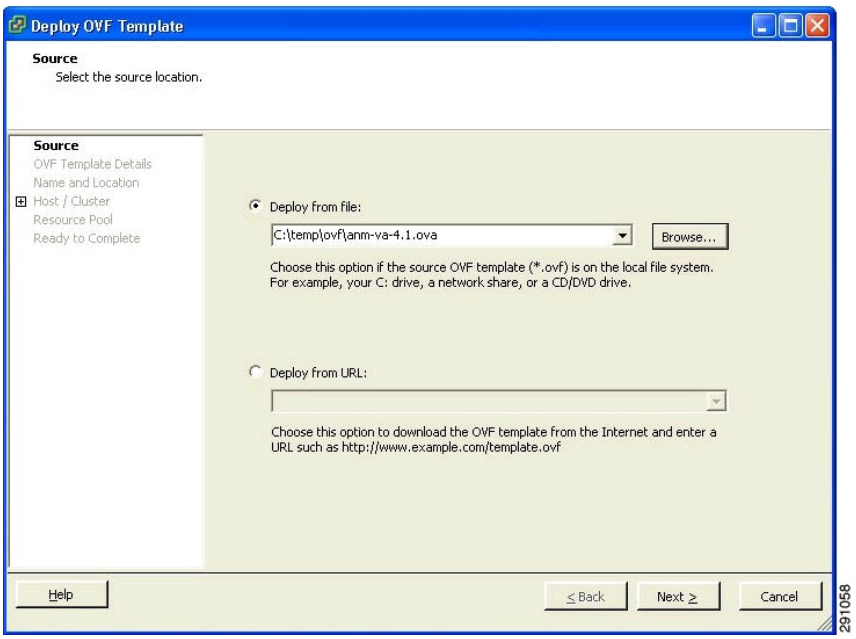
（注） 次の手順には、MSE 仮想アプライアンスの展開に関する一般的なガイドラインが記載されていますが、実行する必要がある正確な手順は、ご使用のVMware環境と設定の特性によって異なる可能性があります。

（注） 仮想アプライアンスを展開するには、ESXi ホスト データベース上に使用可能なディスク領域が 500 GB 以上必要です。 ESXi 4.1 以前には、ホスト上のデータストアのブロック サイズに 4 MB 以上を推奨します。そうでない場合、展開に失敗することがあります。 ESXi 5.0 以降のデータストアにはこの制限はありません。

MSE 仮想アプライアンスを展開するには、次の手順を実行します。

ステップ 1 VMware vSphere Client のメイン メニューで、[File] > [Deploy OVF Template] を選択します。 [Deploy OVF Template] ウィンドウが表示されます。

図 *1*：*[Deploy OVF Template]* ウィンドウ

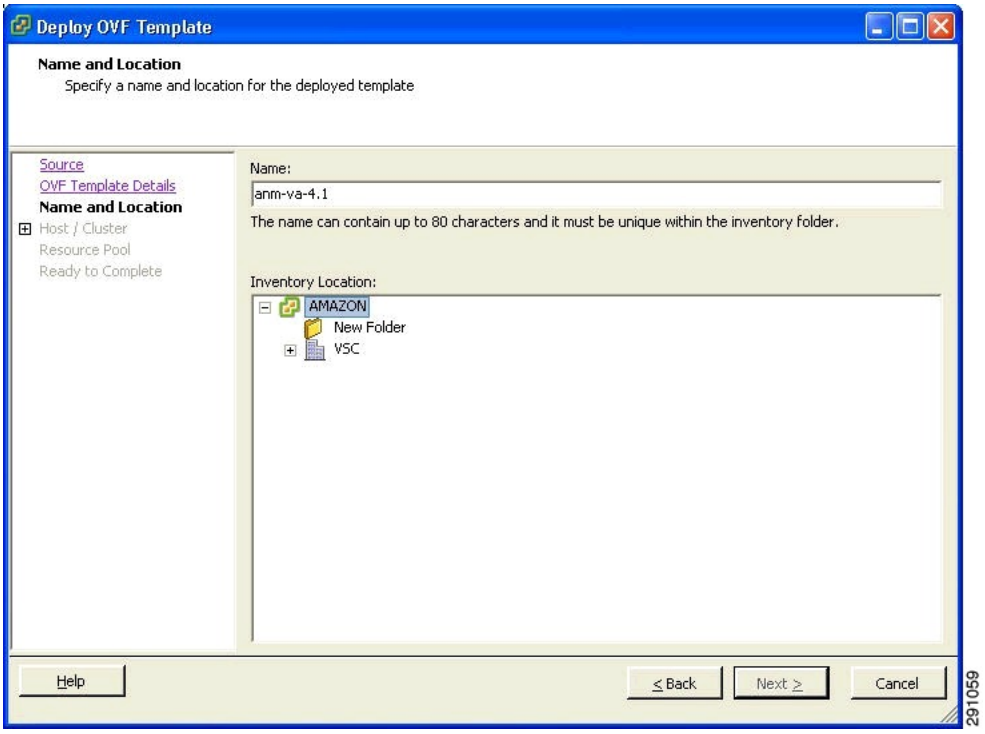


ステップ 2 [Deploy From File] オプション ボタンを選択して、ドロップダウン リストから MSE 仮想アプライアンス配布が含まれている OVA ファイルを選択します。

ステップ 3 [Next] をクリックします。 [OVF Template Details] ウィンドウが表示されます。 VMware ESX/ESXi が OVA 属性を読み取ります。 詳細には、インストールする製品、OVA ファイルのサイズ（ダウンロード サイズ）、および仮想マシンに使用できる必要があるディスク領域の量が含まれます。

ステップ 4 OVF テンプレートの詳細を確認して、[Next] をクリックします。 [Name and Location] ウィンドウが表示されます。

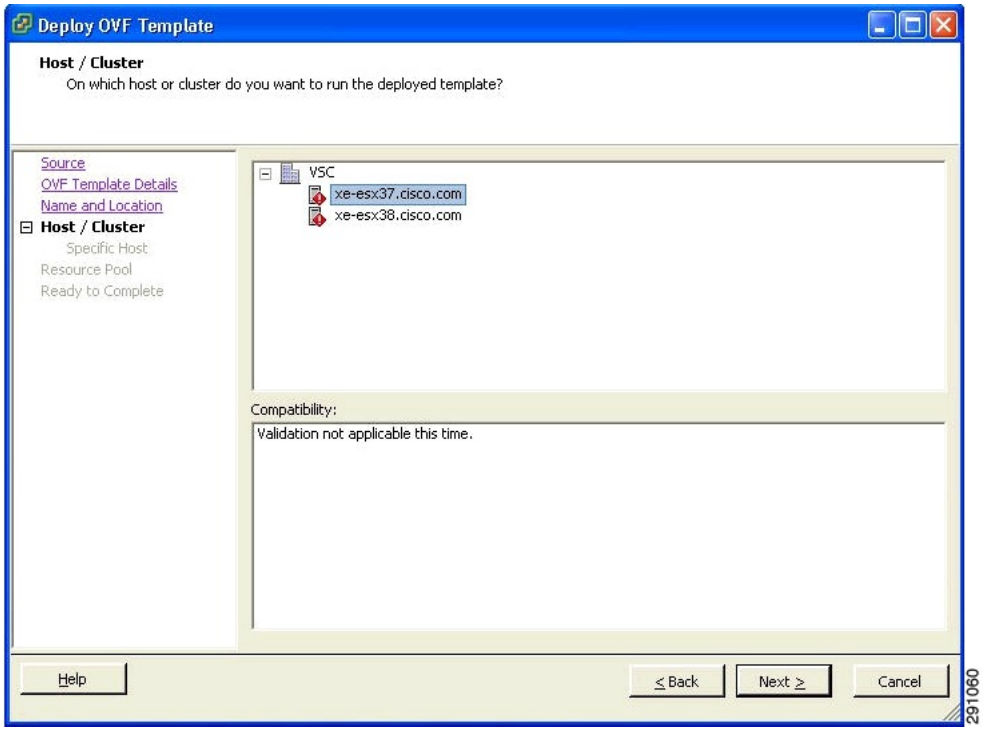
図 *2*：*[Name and Location]* ウィンドウ



ステップ 5 [Name] テキスト ボックスで展開対象の VM のデフォルトの名前を維持するか、新しい名前を指定して、[Next] をクリックします。 この名前値は、VMware インフラストラクチャで新しい仮想マシンを識別する

ために使用されます。この特定のVMをご使用の環境で区別する任意の名前を指定する必要があります。[Host/Cluster] ウィンドウが表示されます。

図 *3*：*[Host/Cluster]* ウィンドウ



ステップ 6 MSE VM を展開する宛先ホストまたはHA クラスタを選択して、[Next] をクリックします。 [Resource Pool] ウィンドウが表示されます。

ステップ 7 宛先ホスト環境に複数のリソース プールがある場合は、展開に使用するリソース プールを選択して、[Next] をクリックします。 [Ready to Complete] ウィンドウが表示されます。

ステップ 8 展開のために表示される設定を確認して、必要に応じて [Back] をクリックして示される設定を変更します。

ステップ 9 [Finish] をクリックして、展開を完了します。 インストールが完了するとメッセージで通知され、インベントリで MSE 仮想アプライアンスを確認できます。

ステップ 10 [Close] をクリックして、[Deployment Completed Successfully] ダイアログボックスを閉じます。

MSE 仮想アプライアンス VM を起動するための基本設定

新規仮想マシンへの MSE 仮想アプライアンスの展開（インストール）が完了しました。 仮想マシンのノードが、VMware vSphere Client ウィンドウのリソース ツリーに表示されるようになります。 OVF テンプレートを展開すると、MSE 仮想アプライアンス アプリケーションと関連するリ

ソースがすでにインストールされた新規仮想マシンが vCenter に作成されます。 展開後に、MSE 仮想アプライアンスの基本設定を行う必要があります。

MSE の設定を開始するには、次の手順を実行します。

ステップ 1 vSphere Client で、リソース ツリーの [MSE virtual appliance] ノードをクリックします。 仮想マシン ノードが、MSE 仮想アプライアンスを展開したホスト、クラスタ、またはリソース プールの下の Hosts and Clusters ツリーに表示されます。

ステップ 2 [Getting Started] タブで、[Basic Tasks] にある [Power on the virtual machine] というリンクをクリックします。 [vSphere Client] ペインの下部にある [Recent Tasks] ウィンドウは、仮想マシンの起動に関連するタスクのステータスを示しています。 仮想マシンを正常に起動した後で、タスクのステータス列に [Completed] と表示されます。

ステップ 3 キーボード入力でコンソール プロンプトをアクティブにするには、コンソール ペイン内で [Console] タブをクリックします。

ステップ 4 MSE セットアップ ウィザードを使用して設定を完了します。

コマンドライン クライアントを使用した MSE 仮想アプライアンスの展開

ここでは、コマンド ラインから MSE 仮想アプライアンスを展開する方法について説明します。 vSphere Client を使用して MSE OVA 配布を展開する代わりに、コマンドライン クライアントである VMware OVF ツールを使用できます。

VMware OVF ツールを使用して OVA を展開するには、**ovftool** コマンドを使用します。このコマンドは、次の例に示すように、展開する OVA ファイルの名前と宛先ロケーションを引数として使用します。

```
ovftool MSE-VA-X.X.X-large.ova vi://my.vmware-host.example.com
```

この場合、展開する OVA ファイルは MSE-VA-X.X.X-large.ova で、宛先 ESX ホストは my.vmware-host.example.com です。 VMware OVF ツールの詳細については、VMware vSphere 4.0 のマニュアルを参照してください。

仮想アプライアンス ライセンスの Prime Infrastructure への追加

次の 2 つのオプションを使用して、仮想アプライアンス ライセンスを Prime Infrastructure に追加できます。

- MSE を初めてインストールする場合、[Add Mobility Service Engine] ページを使用する。 詳細については、Prime Infrastructure へのモビリティ サービス エンジンの追加, （11 ページ）を参照してください。
- [License Center] ページを使用する。 詳細については、License Center を使用したライセンス ファイルの MSE への追加, （48 ページ）を参照してください。

License Center を使用したライセンス ファイルの MSE への追加

ライセンスを追加するには、次の手順を実行します。

ステップ 1 MSE 仮想アプライアンスをインストールします。

ステップ 2 Prime Infrastructure に MSE を追加します。

ステップ 3 Prime Infrastructure UI で **Administration** > **License Center**の順に選択して、[License Center] ページにアクセスします。

ステップ 4 左側のサイドバーのメニューから、**Files** > **MSE Files** を選択します。

ステップ 5 Click **Add**をクリックして、ライセンスを追加します。
[Add A License File] メニューが表示されます。

ステップ 6 MSE を選択し、アクティベーション ライセンス ファイルを参照します。

ステップ 7 をクリックします。`**Submit**.
送信したら、ライセンスがアクティブになり、[License Center] ページにライセンス情報が表示されます。

License Center を使用した MSE ライセンス情報の表示

License Center では、Prime Infrastructure、ワイヤレス LAN コントローラ、および MSE のライセンスを管理できます。 ライセンス情報を表示するには、次の手順を実行します。

ステップ 1 [Administration] > [License Center] を選択して、[License Center] ページにアクセスします。

ステップ 2 左側のサイドバーのメニューから、[Summary] > [MSE] を選択して、[MSE Summary] ページを表示します。
次の表に、[MSE Summary] ページのフィールドを示します。

表 *5* : *[MSE Summary]* ページ

フィールド	説明
MSE Name	MSE ライセンス ファイルのリスト ページへのリンクを提供します。

フィールド	説明
サービス	サービス タイプには、CAS、wIPS、Mobile Concierge サービス、Location Analytics サービス、Billboard サービス、Proxy サービスを使用できます。
Platform Limit	プラットフォームの制限。
Type	MSE のタイプを指定します。
Installed Limit	MSE 上でライセンス付与されたクライアント アクセス ポイントの合計数を表示します。
License Type	永久、評価、および拡張の3つの異なるタイプのライセンス。
Count	MSE 上で現在ライセンス付与されている CAS または wIPS の要素数。

License Center を使用したライセンス ファイルの削除

ライセンスを削除するには、次の手順を実行します。

ステップ 1 MSE 仮想アプライアンスをインストールします。

ステップ 2 ウィザードを使用して Prime Infrastructure に MSE を追加します。

ステップ 3 [Administration] > [License Center] を選択して、[License Center] ページにアクセスします。

ステップ 4 左側のサイドバーのメニューから、[Files] > [MSE Files] を選択します。

ステップ 5 [MSE License File] オプション ボタンを選択して、削除する MSE ライセンス ファイルを選択し、[Remove] をクリックします。

ステップ 6 [OK] をクリックして、削除を実行します。

第 6 章

システム プロパティの設定および表示

この章では、Mobility Services Engine でシステム プロパティを設定および表示する方法を説明します。

この章の内容は、次のとおりです。

ライセンス要件

Mobility Services Engine には CAS および wIPS の評価ライセンスが付属しています。 評価版は 60 日間（480 時間）有効で、各サービスに対してデバイスの制限が事前設定されています。 これらは、120 日ライセンスとともに提供されます（残り日数は経過日数ではなく、実際に使用した日数によって減少します）。

ライセンスの購入およびインストールの詳細については、次の URL を参照してください。

http://www.cisco.com/en/US/prod/collateral/wireless/ps9733/ps9742/data_sheet_c07-473865.html

一般プロパティの編集およびパフォーマンスの表示

[General Properties]：Cisco Prime Infrastructure を使用して Mobility Services Engine の一般プロパティを編集できます。一般プロパティには、連絡先名、ユーザ名、パスワード、システム上で有効な

サービス、サービスの有効化または無効化、同期のための Mobility Services Engine の有効化などがあります。 詳細については、一般プロパティの編集, （52 ページ）を参照してください。

（注） Mobility Services Engine の初期設定時に定義したユーザ名とパスワードを変更するには、一般プロパティを使用します。

[Performance]：Prime Infrastructure を使用して特定の Mobility Services Engine の CPU およびメモリの使用率を表示できます。 詳細については、パフォーマンス情報の表示, （55 ページ）を参照してください。

ここでは、次の内容について説明します。

一般プロパティの編集

Mobility Services Engine の一般プロパティを編集するには、次の手順に従います。

ステップ 1 [Services] > [Mobility Services] の順に選択し、[Mobility Services] ページを表示します。

ステップ 2 編集する Mobility Services Engine の名前をクリックします。 [General] と [Performance] の 2 つのタブが表示されます。

（注） デフォルトで [General Properties] ページが表示されない場合、左側のサイドバーのメニューから [Systems] > [General Properties] の順に選択します。

ステップ 3 [General] タブで、必要に応じてフィールドを変更します。 この表に、[General Properties] ページのフィールドを示します。

表 *6*：*[General]* タブ

フィールド	設定オプション
デバイス名（Device Name）	Mobility Services Engine のユーザ割り当て名。
Device Type	Mobility Services Engine のタイプを示します（例：Cisco 3310 Mobility Services Engine）。 デバイスが仮想アプライアンスであるかどうかを示します。
Device UDI	デバイス UDI（Unique Device Identifier）ストリングは二重引用符で囲まれています（ストリングの末尾にスペースがある場合はスペースも含まれます）。
Version	製品 ID のバージョン

フィールド	設定オプション
Start Time	サーバが起動された起動時刻を示します。
IP Address	Mobility Services Engine の IP アドレスを示します。
連絡先名	Mobility Services Engine の連絡先名を入力します。
ユーザ名	Mobility Services Engine を管理する Prime Infrastructure サーバのログイン ユーザ名を入力します。 これにより、初期設定時に設定されたユーザ名を含む、以前に定義されたユーザ名が置き換えられます。
パスワード	Mobility Services Engine を管理する Prime Infrastructure サーバのログイン パスワードを入力します。 これにより、初期設定時に設定されたパスワード名を含む、以前に定義されたパスワードが置き換えられます。
Legacy Port	HTTPS 通信をサポートするモビリティ サービスのポート番号を入力します。 [Legacy HTTPS] オプションも有効にする必要があります。
Legacy HTTPS	これは Mobility Services Engine には適用されません。 ロケーション アプライアンスにのみ適用されます。
Delete synchronized service assignments and enable synchronization	Mobility Services Engine からすべてのサービス割り当てを永久に削除するには、このチェックボックスをオンにします。 このオプションが表示されるのは、モビリティ サービス エンジンを追加するときに [Delete synchronized service assignments] チェックボックスをオフにした場合のみです。

フィールド	設定オプション
Mobility Services	Mobility Services Engine 上のサービスを有効にするには、サービスの横にあるチェックボックスをオンにします。 サービスには、Context Aware、wIPS、Mobile Concierge、CMX Analytics、CMX Browser Engage、Proxy サービスが含まれます。 CAS を選択すると、クライアント、不正アクセス ポイント、干渉、有線クライアント、およびタグを追跡できます。 タグを追跡するには、次のいずれかのエンジンを選択します。 • Cisco Tag Engine または • Partner Tag Engine （注） Partner Tag Engine は、タグ追跡にのみ使用します。 クライアントは、引き続き Cisco Context-Aware Engine によって追跡されます。 （注） 選択すると、サービスは [Up]（アクティブ）として表示されます。 アクティブでないサービスはすべて、選択された（現行）システム上およびネットワーク上で [Down]（非アクティブ）として表示されます。 （注） CAS および wIPS は Mobility Services Engine 上で同時に稼働できます。 現在のシステムで割り当て可能なデバイスの数を確認するには、[here] リンクをクリックします。 ネットワーク上のすべての Mobility Services Engine のライセンスの詳細を表示するには、[License Center] ページで、左側のサイドバーのメニュー オプションから [MSE] を選択します。 （注） ライセンスの購入およびインストールの詳細については、次の URL を参照してください。 http://www.cisco.com/en/US/prod/collateral/wireless/ps9733/ps9742/data_sheet_c07-473865.html

（注） 次の tcp ポートはリリース 6.0 の MSE で使用中です。tcp：22 MSE SSH ポート、tcp 80：MSE HTTPポート、tcp 443：MSE HTTPS ポート、tcp 1411：、tcp 8001：レガシー・ポート。 ロケーション API に使用されます。

（注） 次の udp ポートはリリース 6.0 の MSE で使用中です。udp：123 NTPD ポート（NTP 設定後にオープン）、udp 32768：ロケーション内部ポート。

（注） MSE で **enable http** コマンドを入力した場合、MSE でポート 80 が有効になります。 CA が発行する証明書が MSE にインストールされている場合、MSE でポート 8880 および 8843 は閉じられます。

ステップ 4 [Save] をクリックして、Prime Infrastructure データベースと Mobility Services Engine データベースを更新します。

パフォーマンス情報の表示

パフォーマンスの詳細を表示するには、次の手順に従います。

ステップ 1 [Services] > [Mobility Services] の順に選択し、[Mobility Services] ページを表示します。

ステップ 2 表示する Mobility Services Engine の名前をクリックします。 [General] と [Performance] の 2 つのタブが表示されます。

ステップ 3 [Performance] タブをクリックします。
1 日を超える期間のパフォーマンスの数値を表示するには、y 軸上の期間（[1w] など）をクリックします。

パフォーマンスの概要をテキストで表示するには、CPU の下の 2 つ目のアイコンをクリックします。

ページを拡大するには、右下にあるアイコンをクリックします。

NMSP パラメータの変更

ネットワーク モビリティ サービス プロトコル（NMSP）は、モビリティ サービスとコントローラ間の通信を管理するプロトコルです。 Mobility Services Engine とコントローラ間のテレメトリ、緊急、およびチョークポイントの情報の転送は、このプロトコルによって管理されます。

このメニュー オプションは、MSE Release 7.0.105.0 以前のみで使用できます。

- ネットワークの応答が遅くなっている場合や大幅な遅延が発生している場合を除き、デフォルトのパラメータ値を変更しないでおくことを推奨します。
- テレメトリ、緊急、およびチョークポイント情報は、コントローラおよびソフトウェア リリース 4.1 以降でインストールされた Prime Infrastructure でのみ表示されます。
- コントローラと Mobility Services Engine との通信には、TCP ポート 16113 が使用されます。コントローラと Mobility Services Engine の間にファイアウォールがある場合は、NMSP を機能させるにはこのポートが開いている（ブロックされていない）ことが必要です。

NMSP パラメータを設定するには、次の手順に従います。

ステップ 1 [Services] > [Mobility Services] の順に選択します。

ステップ 2 プロパティを編集する Mobility Services Engine の名前をクリックします。

ステップ 3 [System] > [NMSP Parameters] の順に選択します。 設定オプションが表示されます。

ステップ 4 必要に応じて、NMSP パラメータを変更します。 次の表に、NMSP パラメータを示します。

表 *7*：*NMSP* パラメータ

フィールド	説明
エコー間隔	Mobility Services Engine からコントローラにエコー要求を送信する頻度 デフォルト値は 15 秒です。 有効値の範囲は 1 ～ 120 秒です。 （注） ネットワークの応答が遅くなっている場合は、[Echo Interval]、[Neighbor Dead Interval]、[Response Timeout] の値を大きくし、エコー確認の失敗回数を制限できます。
Neighbor Dead Interval	neighbor deadの宣言までに、Mobility Services Engine がコントローラからの正常なエコー応答を待機する秒数。 この時間は、エコー要求が送信された時点から始まります。 デフォルト値は 30 秒です。 有効値の範囲は 1 ～ 240 秒です。 （注） この値はエコー間隔値の 2 倍以上でなければなりません。
応答タイムアウト	Mobility Services Engine が、保留要求をタイムアウトと見なすまでに待機する時間 デフォルト値は 1 秒です。 最小値は 1 です。 最大値はありません。
Retransmit Interval	Mobility Services Engine が、応答タイムアウトの通知を受け取ってから要求再送信を開始するまで待機する時間 デフォルト設定は 3 秒です。 有効値の範囲は 1 ～ 120 秒です。
最大再送信回数	どの要求にも応答がない場合に送信される再送信の最大回数。デフォルト設定は 5 です。 許容最小値は 0 です。 最大値はありません。

ステップ 5 [Save] をクリックして、Prime Infrastructure データベースと Mobility Services Engine データベースを更新します。

システムのアクティブ セッションの表示

Mobility Services Engine のアクティブなユーザ セッションを表示できます。

アクティブなユーザ セッションを表示するには、次の手順に従います。

ステップ 1 [Services] > [Mobility Services] の順に選択します。

ステップ 2 アクティブ セッションを表示する Mobility Services Engine の名前をクリックします。

ステップ 3 [System] > [Active Sessions] の順に選択します。
Prime Infrastructure は各セッションに関する次の情報を表示します。

- セッション ID
- Mobility Services Engine のアクセス元の IP アドレス
- 接続ユーザのユーザ名
- セッションが開始された日時
- Mobility Services Engine が最後にアクセスされた日時
- 最終アクセス以降セッションがアイドルになっていた期間

トラップ宛先の追加および削除

Mobility Services Engine により生成される SNMP トラップを受信する Prime Infrastructure または Cisco Security Monitoring, Analysis, and Response System（CS-MARS）ネットワーク管理プラットフォームを指定できます。

ユーザが Prime Infrastructure を使用して Mobility Services Engine を追加すると、その Prime Infrastructure プラットフォームはデフォルトのトラップ宛先として自動的に確立されます。 Prime Infrastructure に冗長設定がある場合、プライマリの Prime Infrastructure に障害が発生しバックアップ システムが引き継ぐまでは、バックアップ用の Prime Infrastructure はデフォルトのトラップの宛先としてリストされません。 アクティブな Prime Infrastructure だけがトラップ宛先としてリストされます。

ここでは、次の内容について説明します。

- トラップ宛先の追加, （58 ページ）
- トラップ宛先の削除, （59 ページ）

トラップ宛先の追加

トラップ宛先を追加するには、次の手順に従います。

ステップ 1 [Services] > [Mobility Services Engines] の順に選択します。

ステップ 2 新しい SNMP トラップ宛先サーバを定義する Mobility Services Engine の名前をクリックします。

ステップ 3 [System] > [Trap Destinations] の順に選択します。

ステップ 4 [Select a command] ドロップダウン リストから、[Add Trap Destination] を選択します。 [Go] をクリックします。
[New Trap Destination] ページが表示されます。

以下の表は、[Add Trap Destination] ページのフィールドを示します。

表 *8*：*[Add Trap Destination]* ページのフィールド

フィールド	説明
IP Address	トラップ宛先の IP アドレス。
Port Number	トラップ宛先のポート番号。 デフォルト ポート番号は、162 です。
Destination Type	このフィールドは編集できず、値 [Other] が表示されます。
SNMP Version	[SNMP Version] ドロップダウン リストから [v2c] または [v3] を選択します。
SNMP バージョンとして v3 を選択した場合にだけ表示されるフィールドを以下に示します。	
ユーザ名	SNMP バージョン 3 のユーザ名。
Security Name	SNMP バージョン 3 のセキュリティ名。
Authentication Type	ドロップダウン リストから、次のいずれかのオプションを選択します。 **HMAC-MD5** **HMAC-SHA**
Authentication Password	SNMP バージョン 3 の認証パスワード。

フィールド	説明
Privacy Type	ドロップダウン リストから、次のいずれかのオプションを選択します。 **CBC-DES** **CFB-AES-128** **CFB-AES-192** **CFB-AES-256**
Privacy Password	SNMP バージョン 3 のプライバシー パスワード。

（注） 自動的に作成されるデフォルトのトラップ宛先を除き、すべてのトラップ宛先はその他として識別されます。

ステップ 5 [Save] をクリックします。
[Trap Destination Summary] ページが表示され、新たに定義されたトラップがリストされます。

トラップ宛先の削除

トラップ宛先を削除するには、次の手順に従います。

ステップ 1 [Services] > [Mobility Services Engines] の順に選択します。
ステップ 2 SNMP トラップ宛先サーバを削除する Mobility Services Engine の名前をクリックします。
ステップ 3 [System] > [Trap Destinations] の順に選択します。
ステップ 4 削除するトラップ宛先エントリの横にあるチェックボックスをオンにします。
ステップ 5 [Select a command] ドロップダウン リストから、[Add Trap Destination] を選択します。 [Go] をクリックします。
ステップ 6 表示されるダイアログボックスで、[OK] をクリックして削除を実行します。

詳細パラメータの表示および設定

[Prime Infrastructure Advanced Parameters] ページで、Mobility Services Engine の一般的なシステム レベル設定を表示し、モニタリング パラメータを設定することができます。

- 現在のシステム レベルの詳細パラメータを表示するには、詳細パラメータ設定の表示を参照してください。
- 現在のシステム レベルの詳細パラメータを変更するか、またはシステムの再起動やシャットダウンなどの拡張コマンドを実行するか、またはコンフィギュレーション ファイルをクリアするには、詳細コマンドの開始を参照してください。

詳細パラメータ設定の表示

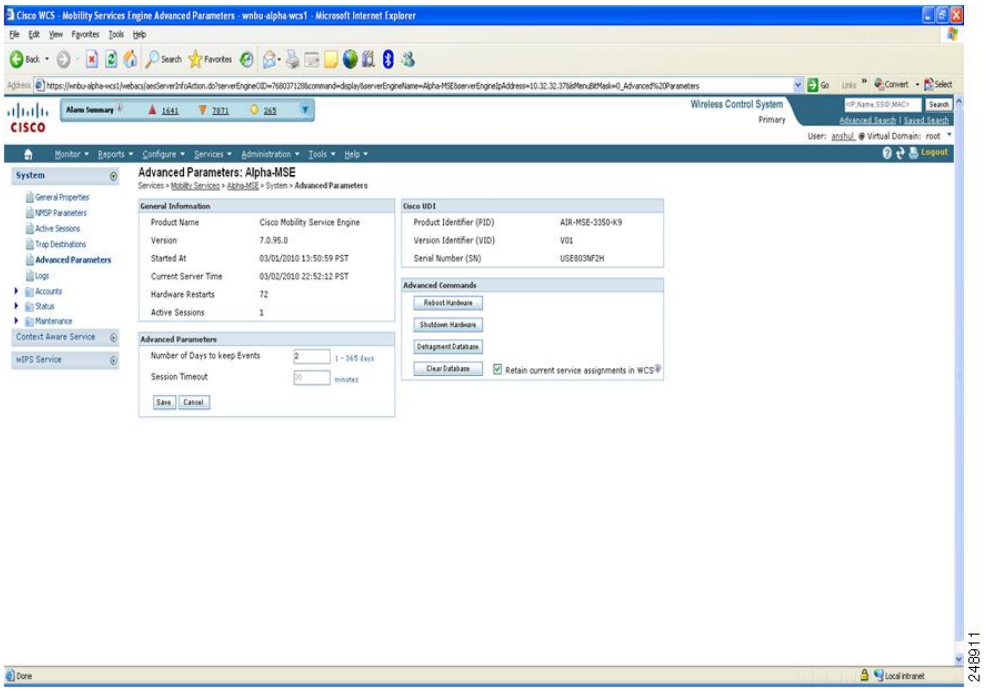
Mobility Services Engine の詳細パラメータ設定を表示するには、次の手順に従います。

ステップ 1 [Services] > [Mobility Services Engines] の順に選択します。

ステップ 2 ステータスを表示する Mobility Services Engine の名前をクリックします。

ステップ 3 [System] > [Advanced Parameters] の順に選択します。 [Advanced Parameters] ページが表示されます。

図 *4*：*[Advanced Parameters]* ページ



詳細パラメータの開始

Prime Infrastructure の [Advanced Parameters] ページでは、イベントを維持する日数およびセッション タイムアウト値を設定できます。 また、システムの再起動またはシャットダウンを実行したり、システム データベースを消去したりできます。

（注） Prime Infrastructure を使用して、Mobility Services Engine またはロケーション アプライアンスのトラブルシューティング パラメータを変更できます。

[Advanced Parameters] ページでは、次の目的で Prime Infrastructure を使用できます。

- イベントを維持する期間およびセッション タイムアウトまでの期間の設定

  詳細については、詳細パラメータの設定を参照してください。

- システムの再起動またはシャットダウンの実行、システム データベースの消去

  詳細については、詳細コマンドの開始を参照してください。

詳細パラメータの設定

詳細パラメータを設定するには、次の手順に従います。

ステップ 1 [Services] > [Mobility Services Engines] の順に選択します。

ステップ 2 プロパティを編集するモビリティ サービスの名前をクリックします。

ステップ 3 左側のサイドバーのメニューから、[System] > [Advanced Parameters] の順に選択します。

ステップ 4 必要に応じて詳細パラメータを確認または変更します。

- 一般情報
  - Product Name
  - Version
  - Started At
  - Current Server Time
  - Hardware Resets
  - Active Sessions
- Advanced Parameters

  注意 詳細デバッグは、モビリティ サービスの処理速度を低下させるため、Cisco TAC 担当者の指示の下でのみ有効にしてください。

- [Number of Days to keep Events]：ログを維持する日数を入力します。 モニタリングとトラブルシューティングで変更する必要がある場合に、この値を変更します。
- [Session Timeout]：セッションがタイムアウトになるまでの分数を入力します。 モニタリングとトラブルシューティングで変更する必要がある場合に、この値を変更します。 現時点では、このオプションは淡色表示されます。

• Cisco UDI

- [Product Identifier (PID)]：Mobility Services Engine の製品 ID。
- [Version Identifier (VID)]：Mobility Services Engine のバージョン番号。
- [Serial Number (SN)]：Mobility Services Engine のシリアル番号。

• Advanced Commands

- [Reboot Hardware]：モビリティ サービス ハードウェアを再起動する場合にクリックします。 詳細については、システムの再起動またはシャットダウン，（63 ページ）を参照してください。
- [Shutdown Hardware]：モビリティ サービス ハードウェアをオフにする場合にクリックします。 詳細については、システムの再起動またはシャットダウン，（63ページ）を参照してください。
- [Clear Database]：モビリティ サービス データベースをクリアする場合にクリックします。 詳細については、システム データベースの消去，（63 ページ）を参照してください。 Prime Infrastructure と MSE から既存のサービス割り当てをすべて削除するには、[Retain current service assignments in the Prime Infrastructure] チェックボックスをオフにします。 [Services] > [Synchronize Services] ページでリソースを再割り当てする必要があります。 デフォルトでは、このオプションが選択されています。

ステップ 5 [Save] をクリックして、Prime Infrastructure データベースと Mobility Services Engine データベースを更新します。

詳細コマンドの開始

システムの再起動やシャットダウン、システム データベースの消去には、[Advanced Parameters] ページで該当するボタンをクリックします。

ここでは、次の内容について説明します。

- システムの再起動またはシャットダウン
- システム データベースの消去

システムの再起動またはシャットダウン

Mobility Services Engine を再起動またはシャットダウンするには、次の手順に従います。

ステップ 1 [Services] > [Mobility Services Engines] の順に選択します。

ステップ 2 再起動またはシャットダウンする Mobility Services Engine の名前をクリックします。

ステップ 3 [System] > [Advanced Parameters] の順に選択します。

ステップ 4 [Advanced Commands] グループ ボックスで、該当するボタン（[Reboot Hardware] または [Shutdown Hardware]）をクリックします。
確認のダイアログボックスで [OK] をクリックして、再起動またはシャットダウン プロセスを開始します。 プロセスを中止するには、[Cancel] をクリックします。

システム データベースの消去

Mobility Services Engine 設定をクリアし、出荷時の初期状態に戻すには、次の手順に従います。

ステップ 1 [Services] > [Mobility Services Engines] の順に選択します。

ステップ 2 設定する Mobility Services Engine の名前をクリックします。

ステップ 3 [System] > [Advanced Parameters] の順に選択します。

ステップ 4 [Advanced Commands] グループ ボックスの [Retain current service assignments in Prime Infrastructure] チェックボックスをオフにして、Prime Infrastructure と MSE から既存のサービス割り当てをすべて削除します。 [Services] > [Synchronize Services] ページでリソースを再割り当てする必要があります。 デフォルトでは、このオプションが選択されています。

ステップ 5 [Advanced Commands] グループ ボックスで [Clear Database] をクリックします。

ステップ 6 [OK] をクリックし、Mobility Services Engine データベースをクリアします。

第 7 章

モバイル コンシェルジュ サービス

Cisco Mobile Concierge サービスは、モバイル クライアントとサーバに必要な要素を満たすサービスで、これら相互のメッセージ交換方法を規定します。 モバイル コンシェルジュ ソリューションは、スマート フォンを使用する顧客に固有のストア内エクスペリエンスを提供します。

モバイル コンシェルジュ サービスは、ネットワーク接続を確立するための各種ポリシーが設定されたモバイル デバイスで使用されます。 モバイル コンシェルジュ サービス により、モバイル デバイスは、ローカル ネットワークで使用可能なネットワークベース サービスまたはサービス プロバイダーを介して有効にされたサービスを検出しやすくなります。 ストアの Wi-Fi ネットワークに接続すると、電子クーポン、提供プロモーション、顧客ロイヤルティのデータ、製品の推奨など、各種サービスを受け取ります。

この章の内容は、次のとおりです。

モバイル コンシェルジュのライセンス

有効な拡張ロケーション サービス ライセンスがある場合に限り、モバイル コンシェルジュ サービスを有効にできます。 Base ロケーション ライセンスがある場合、アップグレード SKU を購入することで拡張ロケーション サービスにアップグレードできます。 SKU の詳細については、*Cisco 3300 Series Mobility Services Engine, Release 7.5* のリリース ノートを参照してください。

場所の定義

場所を定義するには、次の手順に従います。

ステップ 1 [Services] > [Mobile Concierge] の順に選択します。

ステップ 2 左側のサイドバーのメニューから [Mobile Concierge Services] > [Venues] の順に選択します。[Venue] ページが表示されます。

ステップ 3 [Select a command]ドロップダウン リストから、[Define New Venue] を選択し、[Go] をクリックします。[Venue Wizard] ページが表示されます。

ステップ 4 [Venue Name] テキスト ボックスに場所の名前を入力し、[Next] をクリックします。

ステップ 5 [Floor/Outdoor Association グループ ボックスで、次を実行します。

- [Area Type] ドロップダウン リストから、サービス アドバタイズメントを表示するエリア タイプを選択します。 指定できる値は、[Floor Area] および [Outdoor Area] です。

  （注） エリア タイプとして [Floor Area] を選択した場合に限り、[Building, Floor Area, and Coverage Area] ドロップダウン リストが表示されます。

- [Campus] ドロップダウン リストから、サービス アドバタイズメントを表示させるキャンパス名を選択します。
- [Building] ドロップダウン リストから、アドバタイズメントを表示させるビルディング名を選択します。
- [Floor] ドロップダウン リストから、フロア タイプを選択します。
- [Coverage Area] ドロップダウン リストから、フロア内のカバレッジ領域を選択します。
- [Outdoor Area] ドロップダウン リストから、サービス アドバタイズメントを表示する屋外領域を選択します。 このフィールドは、エリア タイプとして [Outdoor Area] を選択した場合にのみ表示されます。

ステップ 6 [Next] をクリックします。 [Audio] グループ ボックスが表示されます。

ステップ 7 [Audio] グループ ボックスで [Choose File] をクリックして、モバイル デバイスでオーディオ通知を再生するためのオーディオ ファイルを参照して選択します。

ステップ 8 [Next] をクリックします。 [Icons] グループ ボックスが表示されます。

ステップ 9 [Icons] グループ ボックスで、[Choose File] をクリックし、アイコンを参照して選択します。

ステップ 10 [Next] をクリックします。 [Venue Apps] グループ ボックスが表示されます。

ステップ 11 [Venue Apps] グループ ボックスで、サービス アドバタイズメントをブロードキャストする場所を選択します。

ステップ 12 [Next] をクリックします。 [Additional Venue Information] グループ ボックスが表示されます。

ステップ 13 [Additional Information] グループ ボックスで、次の手順を実行します。

- [Location Detail] テキスト ボックスに場所の詳細情報を入力します。 ここでは、場所のストア アドレス、郵便番号、住所などロケーションの詳細を指定します。
- [Latitude and Longitude] テキスト ボックスに、場所の GPS 緯度および経度を入力します。 これにより、アプリケーションが場所を正確に特定しやすくなります。
- その他の詳細情報を、[Additional Information]テキスト ボックスに入力ます。

ステップ 14 [Save] をクリックします。 この情報は MSE に適用され、自動的に同期されます。

場所の削除

場所を削除するには、次の手順に従います。

ステップ 1 [Services] > [Mobile Concierge] の順に選択します。
[Venues] ページが表示されます。

ステップ 2 削除する場所のチェックボックスをオンにします。

ステップ 3 [Select a command] ドロップダウン リストから、[Delete Venue] を選択し、[Go] をクリックします。

ステップ 4 [OK] をクリックして、削除を実行します。

ポリシーを使用した新しいサービスプロバイダーの追加

ポリシーを使用してサービス プロバイダーを追加するには、次の手順に従います。

ステップ 1 [Service] > [Mobile Concierge] の順に選択します。

ステップ 2 左側のサイドバーのメニューから [Mobile Concierge Services] > [Providers] の順に選択します。
[Providers] ページが表示されます。

ステップ 3 [Select a command] ドロップダウン リストから、[Define New Provider] を選択し、[Go] をクリックします。
[Provider Wizard] ページが表示されます。

ステップ 4 [Provider Name] テキスト ボックスにサービス プロバイダーの名前を入力します。

ステップ 5 [Next] をクリックします。 [Icons] グループ ボックスが表示されます。

ステップ 6 [Choose File] をクリックして、サービス プロバイダーに関連付けるアイコンを選択します。 これは、クライアント ハンドセットに表示されるアイコンです。

ステップ 7 [Next] をクリックします。 [Local Services] グループ ボックスが表示されます。

ステップ 8 [Local Services] グループ ボックスで、次の手順を実行します。

- [Local Service # name] の左側にある青色の逆三角形アイコンをクリックして [Local Service] を展開し、以下を設定します。
  - [Service Type] ドロップダウン リストからサービス タイプを選択します。 選択可能なオプションは、[Directory Info]、[Sign Up]、[Discount Coupon]、[Network Help]、および [Other] です。
  - [Display Name] テキスト ボックスに、クライアント ハンドセットに表示する名前を入力します。
  - [Description] テキスト ボックスにサービスの説明を入力します。
  - [Service URI] ドロップダウン リストからサービス URI を選択します。

ステップ 9 [Save] をクリックします。 この情報は MSE に適用され、自動的に同期されます。

ポリシーを使用した新しいサービスプロバイダーの追加

ポリシーを使用してサービス プロバイダーを追加するには、次の手順に従います。

ステップ 1 [Service] > [Mobile Concierge] の順に選択します。

ステップ 2 左側のサイドバーのメニューから [Mobile Concierge Services] > [Providers] の順に選択します。 [Providers] ページが表示されます。

ステップ 3 [Select a command] ドロップダウン リストから、[Define New Provider] を選択し、[Go] をクリックします。 [Provider Wizard] ページが表示されます。

ステップ 4 [Provider Name] テキスト ボックスにサービス プロバイダーの名前を入力します。

ステップ 5 [Next] をクリックします。 [Icons] グループ ボックスが表示されます。

ステップ 6 [Choose File] をクリックして、サービス プロバイダーに関連付けるアイコンを選択します。 これは、クライアント ハンドセットに表示されるアイコンです。

ステップ 7 [Next] をクリックします。 [Local Services] グループ ボックスが表示されます。

ステップ 8 [Local Services] グループ ボックスで、次の手順を実行します。

- [Local Service # name] の左側にある青色の逆三角形アイコンをクリックして [Local Service] を展開し、以下を設定します。

- [Service Type] ドロップダウン リストからサービス タイプを選択します。 選択可能なオプションは、[Directory Info]、[Sign Up]、[Discount Coupon]、[Network Help]、および [Other] です。
- [Display Name] テキスト ボックスに、クライアント ハンドセットに表示する名前を入力します。
- [Description] テキスト ボックスにサービスの説明を入力します。
- [Service URI] ドロップダウン リストからサービス URI を選択します。

ステップ 9 [Save] をクリックします。 この情報は MSE に適用され、自動的に同期されます。

サービス プロバイダーの削除

サービス プロバイダーを削除するには、次の手順を実行します。

ステップ 1 [Services] > [Mobile Concierge] の順に選択します。
[Venue] ページが表示されます。

ステップ 2 左側のサイドバーのメニューから [Mobile Concierge Services] > [Providers] の順に選択します。
[Providers] ページが表示されます。

ステップ 3 削除するサービス プロバイダーのチェックボックスをオンにします。

ステップ 4 [Select a command] ドロップダウン リストから、[Delete Provider] を選択し、[Go] をクリックします。
[OK] をクリックして、削除を実行します。

新しいポリシーの定義

新しいポリシーを定義するには、次の手順に従います。

ステップ 1 [Services] > [Mobile Concierge] の順に選択します。

ステップ 2 左側のサイドバーのメニューから [Mobile Concierge Services] > [Policies] の順に選択します。
[Policies] ページが表示されます。

ステップ 3 [Select a command] ドロップダウン リストから [Define New Policy] を選択し、[Go] をクリックします。
[Policy Wizard] ページが表示されます。

ステップ 4 [Venue] ドロップダウン リストから、ポリシーを適用する場所を選択します。

ステップ 5 [Next] をクリックします。 [Provider] グループ ボックスが表示されます。

ステップ 6 [Provider] ドロップダウン リストからサービス プロバイダーを選択します。

ステップ 7 [Next] をクリックします。

ステップ 8 [SSID] ドロップダウン リストから、サービス アドバタイズメントをブロードキャストする SSID を選択し、[OK] をクリックします。 複数の SSID を選択できます。

ステップ 9 [Next] をクリックします。 [Display Rule] グループ ボックスが表示されます。

ステップ 10 [Display Rule] グループ ボックスで、次の手順を実行します。
[Display Rule] オプション ボタンを選択します。 [Display everywhere] または [Display near selected APs] オプション ボタンのいずれかを選択できます。 デフォルトでは、[Display everywhere] が選択されています。

[Display everywhere] を選択した場合、これらの SSID を提供するすべてのモバイル コンシェルジュ対応コントローラが検索され、それらのコントローラが MSE に割り当てられます。

[Display near selected APs] を選択した場合、次のパラメータを設定できます。

- [AP]：アドバタイズメントをブロードキャストする AP を選択します。
- [Radio]：アドバタイズメントをブロードキャストする無線周波数を選択します。 選択した無線帯域の近くにモバイルデバイスがある場合、サービス アドバタイズメントが表示されます。 指定できる値は 2.4 GHz または 5 GHz です。
- [min RSSI]：ユーザ インターフェイスにサービス アドバタイズメントを表示する RSSI の値を入力します。

ステップ 11 [Finish] をクリックします。

ポリシーの削除

ポリシーを削除するには、次の手順に従います。

ステップ 1 [Services] > [Mobile Concierge] の順に選択します。

ステップ 2 左側のサイドバーのメニューから [Mobile Concierge Services] > [Policies] の順に選択します。
[Policies] ページが表示されます。

ステップ 3 削除するポリシーのチェックボックスをオンにします。

ステップ 4 [Select a command] ドロップダウン リストから、[Delete Policy] を選択し、[Go] をクリックします。

ステップ 5 [OK] をクリックして、削除を確認します。

第 8 章

ユーザとグループの管理

この章では、ユーザ、グループ、および Mobility Services Engine へのホスト アクセスを管理する方法について説明します。

この章の内容は、次のとおりです。

前提条件

Cisco Prime Infrastructure が Mobility Services Engine にアクセスするには、フル アクセス権限が必要です。

注意事項と制約事項

グループ権限は個々のユーザの権限を上書きします。たとえば、ユーザにフルアクセス権限を付与し、読み取り専用アクセス権限が付与されているグループにそのユーザを追加すると、ユーザは Mobility Services Engine の設定を設定できなくなります。

ユーザ グループの管理

この項では、ユーザ グループの追加、削除、および編集の方法について説明します。

ユーザ グループを使用すると、ユーザに異なるアクセス権限を割り当てることができます。

ここでは、次の内容について説明します。

ユーザ グループの追加

Mobility Services Engine にユーザ グループを追加するには、次の手順を実行します。

（注） [Services] > [Mobility Services Engine] ページは、root 仮想ドメインでのみ使用可能です。

ステップ 1 [Services] > [Mobility Services] の順に選択します。
ステップ 2 ユーザ グループを追加する Mobility Services Engine の名前をクリックします。
ステップ 3 [System] > [Accounts] > [Groups] の順に選択します。
ステップ 4 [Select a command] ドロップダウン リストから [Add Group] を選択します。 [Go] をクリックします。
ステップ 5 [Group Name] テキストボックスにグループ名を入力します。
ステップ 6 [Permission] ドロップダウン リストから権限レベル（[read]、[write]、または [full]）を選択します。
（注） Prime Infrastructure が Mobility Services Engine にアクセスするには、フル アクセス権限が必要です。
ステップ 7 [Save] をクリックします。

ユーザ グループの削除

Mobility Services Engine からユーザ グループを削除するには、次の手順を実行します。

ステップ 1 [Services] > [Mobility Services] の順に選択します。
ステップ 2 ユーザ グループを削除する Mobility Services Engine の名前をクリックします。
ステップ 3 [System] > [Accounts] > [Groups] の順に選択します。
ステップ 4 削除するグループのチェックボックスをオンにします。
ステップ 5 [Select a command] ドロップダウン リストから、[Delete Group] を選択し、[Go] をクリックします。
ステップ 6 [OK] をクリックします。

ユーザ グループの権限の変更

注意 グループ権限は個々のユーザの権限を上書きします。 たとえば、ユーザにフル アクセス権限を付与し、読み取りアクセス権限のみ付与されているグループにそのユーザを追加すると、ユーザはモビリティ サービス エンジンの設定を設定できなくなります。

ユーザ グループの権限を変更するには、次の手順を実行します。

ステップ 1 [Services] > [Mobility Services] の順に選択します。
ステップ 2 編集する Mobility Services Engine の名前をクリックします。
ステップ 3 [System] > [Accounts] > [Groups] の順に選択します。
ステップ 4 編集するグループの名前をクリックします。
ステップ 5 [Permission] ドロップダウン リストから権限レベル（[read]、[write]、または [full]）を選択します。
ステップ 6 [Save] をクリックします。

ユーザの管理

このセクションでは、Mobility Services Engine のユーザの追加、削除、および編集の方法について説明します。 アクティブなユーザ セッションの表示方法についても説明します。

ここでは、次の内容について説明します。

- ユーザの追加
- ユーザの削除
- ユーザ プロパティの変更

ユーザの追加

注意 グループ権限は個々のユーザの権限を上書きします。 たとえば、ユーザにフル アクセス権限を付与し、読み取りアクセス権限のみ付与されているグループにそのユーザを追加すると、ユーザはモビリティ サービス エンジンの設定を設定できなくなります。

Mobility Services Engine にユーザを追加するには、次の手順を実行します。

ステップ 1 [Services] > [Mobility Services] の順に選択します。
ステップ 2 ユーザを追加する Mobility Services Engine の名前をクリックします。
ステップ 3 [System] > [Accounts] > [Users] の順に選択します。
ステップ 4 [Select a command] ドロップダウン リストから、[Add User] を選択します。 [Go] をクリックします。
ステップ 5 [Username] テキストボックスにユーザ名を入力します。
ステップ 6 [Password] テキストボックスにパスワードを入力します。
ステップ 7 [Group Name] テキストボックスにユーザが属するグループの名前を入力します。
ステップ 8 [Permission] ドロップダウン リストから権限レベル（[read]、[write]、または [full]）を選択します。
（注） Prime Infrastructure が Mobility Services Engine にアクセスするには、フル アクセス権限が必要です。
ステップ 9 [Save] をクリックします。

ユーザの削除

Mobility Services Engine からユーザを削除するには、次の手順を実行します。

ステップ 1 [Services] > [Mobility Services] の順に選択します。
ステップ 2 ユーザを削除する Mobility Services Engine の名前をクリックします。
ステップ 3 [System] > [Accounts] > [Groups] の順に選択します。
ステップ 4 削除するユーザのチェックボックスをオンにします。
ステップ 5 [Select a command] ドロップダウン リストから [Delete User] を選択します。 [Go] をクリックします。
ステップ 6 [OK] をクリックします。

ユーザ プロパティの変更

ユーザ プロパティを変更するには、次の手順に従います。

ステップ 1 [Services] > [Mobility Services Engines] の順に選択します。
ステップ 2 編集する Mobility Services Engine の名前をクリックします。
ステップ 3 [System] > [Accounts] > [Users] の順に選択します。
ステップ 4 編集するグループの名前をクリックします。
ステップ 5 [Password] および [Group Name] テキスト ボックスで必要な変更を行います。
ステップ 6 [Save] をクリックします。

第 9 章

イベント通知の設定

Cisco Prime Infrastructure では、Mobility Services Engine に通知を特定のリスナーに送信させる条件を定義できます。 この章では、イベントおよびイベント グループの定義方法とイベント通知の概要の表示方法について説明します。

（注） [Services] タブの [Mobility Services Engines]、[Synchronize Services]、[Synchronization History]、[High Availability]、[Context Aware Notifications]、および [MSAP] ページは、リリース 7.3.101.0 の仮想ドメインでのみ使用できます。

この章の内容は、次のとおりです。

イベント通知について

- イベント グループ：イベント通知を編成しやすくなります。
- イベント定義：イベント定義には、イベントを発生させた条件、イベントが適用されるアセット、イベント通知の宛先が含まれます。
- イベント通知：Mobility Services Engine は、次の転送メカニズムを介して、登録されたリスナーにイベント通知を送信します。
  - Simple Object Access Protocol（SOAP）
  - 簡易メール転送プロトコル（SMTP）メール
  - 簡易ネットワーク管理プロトコル（SNMP）

- Syslog

ここでは、次の内容について説明します。

イベント通知の概要の表示

Mobility Services Engine は、イベント通知を送信しますが、イベントを保存しません。 ただし、通知イベントの宛先が Prime Infrastructure の場合、Prime Infrastructure は受信した通知を保存し、次に示す 7 つのカテゴリに分類します。

- [Absence (Missing)]：Mobility Services Engine は、アセットが不明になった場合に Absence イベントを生成します。 つまり、Mobility Services Engine は、指定された時間で WLAN のアセットを検出できません。
- [In/Out Area (Containment)]：Mobility Services Engine は、アセットが指定エリアに移動するかエリアから出ると Containment イベントを生成します。

（注） Containment エリア（キャンパス、ビルディング、またはフロア）は、[Monitor] > [Maps] で定義します。 カバレッジ エリアを定義するには、Map Editor を使用します。

- [Movement from Marker (Movement/Distance)]：Mobility Services Engine は、マップで定義した指定マーカーから指定された距離を超えてアセットが移動された場合、Movement イベントを生成します。
- [Location Changes]：Mobility Services Engine は、クライアント ステーション、アセット タグ、不正クライアント、または不正アクセス ポイントのロケーションが変更されると Location Changes イベントを生成します。
- [Battery Level]：Mobility Services Engine は、追跡されるすべてのアセット タグについて Battery Level イベントを生成します。
- [Emergency]：Mobility Services Engine は、タグのパニック ボタンがトリガーされるか、タグが削除されるか、改ざんされるか、非アクティブになるか、不明な状態を報告すると、Cisco CX v.1 準拠のアセット タグの Emergency イベントを生成します。 この情報は、Cisco CX v.1 準拠のタグについてのみ、報告および表示されます。
- [Chokepoint Notifications]：Mobility Services Engine は、タグがチョークポイントによって誘導されたときにイベントを生成します。 この情報は、Cisco CX v.1 準拠のタグについてのみ、報告および表示されます。

（注） すべての要素のイベントは時間単位と日単位で要約されます。

（注） トラック グループとイベントは、Mobility Services Engine と同期する必要があります。

通知のクリア

- [Missing (Absence)]：要素（クライアント、タグ、不正アクセス ポイント、または不正クライアント）が再表示される。
- [In/Out Area (Containment)]：要素が Containment エリア内に戻るか、このエリアから外に出る。
- [Distance]：要素がマーカーから指定された距離以内に戻る。
- [Location Changes]：クリア状態はこの条件には適用されません。
- [Battery Level]：タグが検出され、普通の電池残量で動作している。

（注） Prime Infrastructure の [Notifications Summary] ページには、クリアされたイベント条件の通知を受信したかどうかが反映されます。

通知メッセージ形式

- XML の通知形式, （80 ページ）
- テキストの通知形式, （79 ページ）

テキストの通知形式

通知をテキスト形式で送信するように指定すると、Mobility Services Engine は、状態を示すためにプレーン テキストの文字列を使用します。

Tag 00:02:02:03:03:04 is in Floor <floorName> Tag 00:02:02:03:03:04 is outside Floor <floorName> Client 00:02:02:03:09:09 is in Area <areaName> RogueClient 00:02:02:08:08:08 is outside Building <buildingName> Tag 00:02:02:03:03:06 has moved 105 feet where the trigger distance was 90 feet. Tag 00:02:02:03:03:20 missing for 14 mins, last seen <timestamp>.

（注） シスコは、テキストの通知形式を予告なしに変更する権利を保持します。

（注） XML は、通知の内容を解析または分析する必要があるシステムの推奨形式です。

XML の通知形式

- Missing (Absence) 条件, （80 ページ）
- In/Out (Containment) 条件, （81 ページ）
- Distance 条件, （81 ページ）
- Battery Level, （81 ページ）
- Location Change, （82 ページ）
- Chokepoint 条件, （82 ページ）
- Emergency 条件, （82 ページ）

（注） XML 形式はサポート対象 API の一部です。シスコは、API が今後更新されるたびに、Mobility Services Engine API プログラムの一環として変更を通知します。

Missing (Absence) 条件

Absence 要素のメッセージ形式：

```
<AbsenceTrackEvent
missingFor="<time in secs entity has been missing>"
lastSeen="time last seen"
trackDefn="<name of track definition>"
entityType="Mobile Station | Tag | Rogue AP | Rogue Client"
entityID="<mac address"/>
```

クリア状態のメッセージ形式：

```
<AbsenceTrackEvent
state="clear"
trackDefn="<name of track definition>"
entityType="Mobile Station | Tag | Rogue AP | Rogue Client"
entityID="<mac address"/>
```

次に例を示します。

```
<AbsenceTrackEvent state="set" missingFor="34" lastSeen="15:00:20 08
Jun 2009" trackDefn="absenceDef1" entityType="Mobile Station"
entityID="00:0c:f1:53:9e:c0"/>

<AbsenceTrackEvent state="clear" entityType="Tag"
trackDefn="absenceDef1" entityID="00:0c:cc:5b:fc:da"/>
```

In/Out (Containment) 条件

Containment 要素のメッセージ形式：

<ContainmentTrackEvent in="true | false" trackDefn="<name of track definition>" containerType="Floor | Area | Network Design | Building" containerID="<fully quality name of container>" entityType="Mobile Station | Tag | Rogue AP | Rogue Client" entityID="<mac address"/>
クリア状態のメッセージ形式：

<ContainmentTrackEvent state="clear" trackDefn="<name of track definition>" entityType="Mobile Station | Tag | Rogue AP | Rogue Client" entityID="<mac address"/>
次に例を示します。

<ContainmentTrackEvent in="true" trackDefn="myContainerRule1" containerType="Area" containerID="nycTestArea,5th Floor,Bldg-A,Rochester_Group,Rochester,"

（注） containerID ストリングは、キャンパス Rochester の Bldg-A の 5 階にある nycTestArea というカバレッジ エリアを表します。

entityType="Tag" entityID="00:0c:cc:5b:fa:44"/> <ContainmentTrackEvent state="clear" entityType="Tag" trackDefn="myContainerRule1" entityID="00:0c:cc:5b:f8:ab"/>

Distance 条件

同じフロアにある要素のメッセージ形式：

<MovementTrackEvent distance="<distance in feet at which the element was located>" triggerDistance="<the distance specified on the condition" reference="<name of the marker specified on the condition>" trackDefn="<name of event definition>" entityType="Mobile Station | Tag | Rogue AP | Rogue Client" entityID="<mac address"/>
別のフロアにある要素のメッセージ形式：

<MovementTrackEvent optionMsg="has moved beyond original floor" reference="<name of the marker specified on the condition>" trackDefn="<name of event definition>" entityType="Mobile Station | Tag | Rogue AP | Rogue Client" entityID="<mac address"/>
クリア状態のメッセージ形式：

<MovementTrackEvent state="clear" trackDefn="<name of event definition>" entityType="Mobile Station | Tag | Rogue AP | Rogue Client" entityID="<mac address"/>
次に例を示します。

<MovementTrackEvent distance="115.73819627990147" triggerDistance="60.0" reference="marker2" trackDefn="distance2" entityType="Mobile Station" entityID="00:0c:41:15:99:92"/>
<MovementTrackEvent optionMsg="has moved beyond original floor" reference="marker2" entityType="Tag" trackDefn="distance2" entityID="00:0c:cc:5b:fa:4c"/>
<MovementTrackEvent state="clear" entityType="Tag"

Battery Level

例：

<BatteryLifeTrackEvent lastSeen="10:28:52 08 Jun 2009" batteryStatus="medium" trackDefn="defn1" entityType="Tag" entityID="00:01:02:03:04:06"/>

Location Change

例：

<MovementTrackEvent distance="158.11388300841898" triggerDistance="5.0" reference="marker1" referenceObjectID="1" trackDefn="defn1" entityType="Mobile Station" entityID="00:01:02:03:04:05"/>

Chokepoint 条件

例：

<ChokepointTrackEvent lastSeen="11:10:08 PST 08 Jun 2009" chokepointMac="00:0c:cc:60:13:a3" chokepointName= "chokeA3" trackDefn="choke" entityType="Tag" entityID="00:12:b8:00:20:4f"/>
クリア状態の例を次に示します。

<ChokepointTrackEvent state="clear" entityType="Tag" trackDefn="choke" entityID="00:12:b8:00:20:4f"/>

Emergency 条件

要素のロケーションの例を次に示します。

<ChokepointTrackEvent lastSeen="11:36:46 PST June 08 2009" emergencyReason= "detached" trackDefn="emer" entityType="Tag" entityID="00:12:b8:00:20:50"/>

（注） [Emergency] イベントがクリアされることはありません。

イベント グループの追加および削除

（注） [**Services**] > [**Context Aware Notifications**] ページは、ルート仮想ドメインでのみ使用可能です。

ここでは、次の内容について説明します。

- イベント グループの追加, （83 ページ）
- イベント グループの削除, （83 ページ）

イベント グループの追加

イベント グループを追加するには、次の手順を実行します。

ステップ 1 [Services] > [Context Aware Notifications] を選択します。
ステップ 2 [Notification Definitions] を選択します。
ステップ 3 [Select a command] ドロップダウン リストから、[Add Event Group] を選択します。 [Go] をクリックします。
ステップ 4 [Group Name] テキストボックスにグループ名を入力します。
ステップ 5 [Save] をクリックします。
[Event Settings] ページに新しいイベント グループが表示されます。

イベント グループの削除

イベント グループを削除するには、次の手順を実行します。

ステップ 1 [Services] > [Context Aware Notifications] を選択します。
ステップ 2 [Notification Definitions] を選択します。
ステップ 3 対応するチェックボックスをオンにして、削除するイベント グループを選択します。
ステップ 4 [Select a command] ドロップダウン リストから、[Delete Event Group(s)] を選択します。 [Go] をクリックします。
ステップ 5 [OK] をクリックして、削除を確認します。
ステップ 6 [Save] をクリックします。

イベント定義の追加、削除、およびテスト

ここでは、イベント定義の追加、削除、およびテスト方法について説明します。内容は次のとおりです。

イベント定義の追加

イベント定義を追加するには、次の手順を実行します。

ステップ 1 [Services] > [Context Aware Notifications] を選択します。

ステップ 2 左側のサイドバーのメニューから、[Notification Definitions] を選択します。

ステップ 3 イベント定義を追加するグループの名前をクリックします。 イベント グループの既存のイベント定義が示された [Event Settings] ページが表示されます。

ステップ 4 [Select a command] ドロップダウン リストから、[Add Event Definition] を選択します。 [Go] をクリックします。

ステップ 5 [Conditions] タブで、1 つ以上の条件を追加します。 追加する条件ごとに、イベント通知を生成するためのルールを指定します。

ヒント たとえば、病院で心臓モニタによる経過観察を行う場合、（1）心臓モニタを見失ってから 1 時間経過したとき、（2）心臓モニタがその割り当てられたフロアから移動したとき、（3）心臓モニタがフロア内の特定のカバレッジ エリアに入ったときに通知を生成するルールを追加します。 この例では、これらの発生に対応する 3 つの異なるルールを追加します。

条件を追加するには、次の手順を実行します。

1. [Add] をクリックして、通知を生成する条件を追加します。
2. [Add/Edit Condition] ダイアログ ボックスで、次の手順を実行します。
   a. [Condition Type] ドロップダウン リストから条件タイプを選択します。
      - [Condition Type] ドロップダウン リストから [Missing] を選択した場合は、不明なアセットによって通知が生成されてから経過した分数を入力します。 たとえば、このテキスト ボックスに 10 を入力すると、デバイスが非アクティブになるかシステムに存在しなくなった後で 10 分経過してもアセットが見つからない場合に、Mobility Services Engine は不明なアセット通知を生成します。 この状態は、コントローラが不在を検出して Mobility Services Engine に通知したとき、または Mobility Services Engine が 60 分間（デフォルト）コントローラからこのデバイスについて何も受信しない場合に発生します。 この値は、クライアントの場合は **config mobile-node-inactive-in-minutes** コマンド、タグの場合は **config tag-inactive-time-in-minutes** コマンドを使用して、（コンソールで cmdshell を使用してアクセス可能な）MSE コマンドライン インターフェイスから設定可能です。 手順 イベント定義の追加 に進みます。
      - [Condition Type] ドロップダウン リストから [In/Out] を選択した場合、[Inside of] または [Outside of] を選択して、[Select Area] をクリックします。 選択したエリアからのアセットの出入りがモニタされます。 [Select] ダイアログボックスで、モニタするエリアを選択し [Select] をクリックします。 モニタするエリアは、キャンパス全体、キャンパス内のビルディング、ビルディング内のフロア、またはカバレッジ エリアになります（Map Editor を使用してカバレッジ エリアを定義できます）。 たとえば、ビルディング内のフロア部分をモニタするには、[Campus] ドロップダウン リストからキャンパスを、[Building] ドロップダウン リストからビルディングを、[Floor Area] ドロップダウン リストからモニタするエリアを選択します。 次に、[Select] をクリックします。 手順 イベント定義の追加 に進みます。

- [Condition Type] ドロップダウン リストから [Distance] を選択した場合、アセットがこれを超えるとイベント通知を生成する指定マーカーからの間隔（フィート単位）を入力します。 [Select Marker] をクリックします。 [Select] ダイアログボックスで、キャンパス、ビルディング、フロア、およびマーカーを、対応するドロップダウン リストから選択し、[Select] をクリックします。 たとえば、マーカーをフロア図面に追加して、[Trigger If] テキスト ボックスの距離を 60 フィートに設定すると、モニタ対象のアセットがマーカーから 60 フィートを超えて離れた場合にイベント通知が生成されます。 手順 イベント定義の追加 に進みます。

  （注） Map Editor を使用して、マーカーおよびカバレッジ エリアを作成できます。 マーカー名を作成する場合は、システム全体で一意になるようにします。

- [Condition Type] ドロップダウン リストから [Battery Level] を選択した場合は、通知を生成する該当の電池残量（**低**、**中**、**普通**）の横にあるチェックボックスをオンにします。 手順 イベント定義の追加 に進みます。

- [Condition Type] ドロップダウン リストから [Location Change] を選択した場合は、手順 イベント定義の追加 に進みます。

- [Condition Type] ドロップダウン リストから [Emergency] を選択した場合は、通知を生成する該当の緊急事態（すべて、パニック ボタン、改ざん、削除）の横にあるボタンをクリックします。 手順 イベント定義の追加 に進みます。

- [Condition Type] ドロップダウン リストから [Chokepoint] を選択した場合は、手順 イベント定義の追加 に進みます。 生成条件は 1 つのみあり、デフォルトで表示されます。 設定は必要ありません。

3. [Trigger If] テキスト ボックスで、通知を生成する時間を分単位で指定します。 デフォルトは 60 分です。

4. [Notification Frequency] オプション ボタンから [Recurring] または [Non-recurring] のいずれかを選択します。 頻度が非繰り返しの場合は、MSE は一度のみ不在通知を送信します。 繰り返しの頻度の場合は、MSE は、デバイスが再度存在するようになるまで不在通知を定期的に送信します。 ここでの期間は、不在定義の設定値を示します。

5. [Apply To] ドロップダウン リストから、生成条件を満たした場合に通知を生成するアセットのタイプ（[Any]、 [Clients]、[Tags]、[Rogue APs]、[Rogue Clients]、または [Interferers]）を選択します。

   （注） [Apply to] ドロップダウン リストから [Any] を選択した場合は、タグ、クライアント、不正アクセス ポイント、および不正クライアントのすべてに電池の条件が適用されます。

   （注） Emergency 通知および Chokepoint 通知は、Cisco Compatible Extensions（CX）のタグのバージョン 1 以降のみに適用されます。

6. [Match By] ドロップダウン リストには、次の選択が左から右に含まれています。

   - 最初のドロップダウン リストから一致基準（[MAC Address]、[Asset Name]、[Asset Group]、または [Asset Category]）を選択します。
   - 2 番目のドロップダウン リストから演算子（[Equals] または [Like]）を選択します。
   - ユーザが選択した [Match By] 基準に基づいてテキスト ボックスに関連するテキストを入力します。

次の例では、指定可能なアセットの一致基準について説明します。

- 最初のドロップダウン リストから [MAC Address]を選択し、2 番目のドロップダウン リストから [Equals] を選択して、テキスト ボックスに MAC アドレス（たとえば、12:12:12:12:12:12）を入力した場合、MAC アドレスが 12:12:12:12:12:12（完全一致）の要素にイベント条件が適用されます。
- 最初のドロップダウン リストから [MAC Address] を選択して、2 番目のドロップダウン リストから [Like] を選択して、テキスト ボックスに 12:12 と入力すると、イベント条件は、MAC アドレスが 12:12 で始まる要素に適用されます。

（注） MAC アドレスが部分的な MAC アドレスの場合、Prime Infrastructure でパフォーマンスの問題が生じることがあります。

7 [Add] をクリックして、定義済みの条件を追加します。

（注） チョークポイントを定義している場合は、条件を追加した後にチョークポイントを選択する必要があります。

イベント定義の削除

Prime Infrastructure から 1 つ以上のイベント定義を削除するには、次の手順に従います。

ステップ 1 [Services] > [Context Aware Notifications] を選択します。

ステップ 2 [Notification Definitions] を選択します。

ステップ 3 イベント定義を削除するグループの名前をクリックします。

ステップ 4 削除するイベント定義を、対応するチェックボックスをオンにして選択します。

ステップ 5 [Select a command] ドロップダウン リストから、[Delete Event Definition(s)] を選択します。 [Go] をクリックします。

ステップ 6 [OK] をクリックして、選択したイベント定義を削除することを確認します。

イベント定義のテスト

イベント定義の 1 つ以上のイベント通知をテストするには、次の手順に従ってください。

ステップ 1 [Services] > [Context Aware Notifications] を選択します。

ステップ 2 [Notification Settings] を選択します。

ステップ 3 テストするイベント定義を含むグループの名前をクリックします。

ステップ 4 対応するチェックボックスをオンにして、テストするイベント定義を選択します。

ステップ 5 [Select a command] ドロップダウン リストから、[Test-Fire Event Definition(s)] を選択します。 [Go] をクリックします。

ステップ 6 イベント通知をテストすることを確認するには、[OK] をクリックします。

ステップ 7 指定した受信者に通知が送信されたことを確認します。

通知リスナーとしての Prime Infrastructure

Prime Infrastructureは、通知リスナーとして動作します。 Prime Infrastructure はトラップをユーザ インターフェイス アラートに変換し、次の形式で表示します。

- 不明 (不在)

  ```
  Absence of Tag with MAC 00:0c:cc:5b:e4:1b, last seen at 16:19:45 08
  June 2009.
  ```

- In/Out (特定のエリア)

  ```
  Tag with MAC 00:0c:cc:5b:fa:44 is In the Area 'Rochester > Rochester
  > 5th Floor > nycTestArea'
  ```

- 距離

  Tag with MAC 00:0c:cc:5b:fa:47 has moved beyond the distance configured for the marker 'marker2'.
  Tag with MAC 00:0c:cc:5b:f9:b9 has moved beyond 46.0 ft. of marker 'marker2', located at a range of 136.74526528595058 ft.

- バッテリー レベル

  Tag 00:01:02:03:04:06 has medium battery, last seen 11:06:01 08 June 2009

- 位置変更

  Tag 00:01:02:03:04:06 has medium battery, last seen 11:06:01 08 June 2009

- 位置変更

  Mobile Station 00:01:02:03:04:05 has moved
  158.11388300841898ft, where the trigger distance was 5.0

第 10 章

Context-Aware Service の計画および検証

この章の内容は、次のとおりです。

ライセンス要件

アクセス ポイントからタグとクライアントに関する状況依存情報を取得するには、ライセンスが必要です。クライアントのライセンスには、不正クライアントおよび不正アクセスポイントの追跡も含まれます。 タグとクライアントのライセンスは個別に提供され、3,000 ～ 12,000 単位の数量の範囲で提供されます。 詳細については、次のURLで『Cisco 3300 Series Mobility Services Engine Licensing and Ordering Guide』を参照してください。http://www.cisco.com/en/US/products/ps9742/products_data_sheets_list.html

データ、音声、およびロケーションの展開についての計画

ここでは、次の内容について説明します。

注意事項と制約事項

- マップに表示するには、アクセス ポイント、クライアント、およびタグを [Monitor] > [Site Maps] ページの [Floor Settings] メニューで選択する必要があります。
- 推奨される計算では、常に強い信号が必要であると見なされます。 場合によっては、推奨未満のアクセス ポイントが必要になることがあります。
- 推奨されるアクセス ポイントにおいて、少なくとも 90 % の確率で、7 m 以内にある要素の真のロケーションが提供されるようにするには、[Location Services] を選択する必要があります。

アクセス ポイントの配置の計算

フロア上のアクセス ポイントの推奨される数および配置を計算する手順は、次のとおりです。

ステップ 1 [Monitor] > [Maps] を選択します。
[Site Map] ページが表示されます。

ステップ 2 表示される概要リストの適切なマップ名のリンクをクリックします。
ビルディングのマップを選択した場合は、[Building View] ページでフロア マップを選択します。

インストールされているすべての要素（アクセス ポイント、クライアント、タグ）の配置および相対的な信号強度を示した、色分けされたマップが表示されます。

（注） マップに表示するには、[Access Points]、[Clients]、および [802.11 Tags] チェックボックスを [Monitor] > [Site Maps] ページの [Floor Settings] ダイアログボックスで選択する必要があります。

ステップ 3 [Select a command] ドロップダウン リスト（右上）から、[Planning Mode] を選択し、[Go] をクリックします。
マップがページ上部に [Planning Mode] オプションとともに示されます。

ステップ 4 [Add APs] をクリックします。
表示されるページで、破線の四角形を、推奨されるアクセス ポイントを計算するマップ ロケーションにドラッグします。

（注） 四角形の端を選択し、Shift キーを押したままにして、四角形のサイズまたは配置を調整します。必要に応じてマウスを動かし、目的の位置の輪郭を描きます。

ステップ 5 フロアで使用されるサービスの隣の [Select] チェックボックスをオンにします。 オプションには、[Data/Coverage (default)]、[Voice]、[Location]、および [Location with Monitor Mode APs] があります。[Calculate] をクリックします。
推奨される数のアクセス ポイントが表示されます。

（注） 各サービス オプションには、そのオプションの上に示されているすべてのサービスが含まれます。 たとえば、[Location] チェックボックスをオンにした場合、計算では、必要なアクセス ポイント数を決定する際に、データ/カバレッジ、音声、およびロケーションが考慮されます。

ステップ 6 [Apply] をクリックして、選択した領域のアクセス ポイントの推奨数および提案された配置に基づいてマップを生成します。

キャリブレーション モデル

指定した RF モデルがフロアのレイアウトを十分に表していない場合、減衰特性をより正確に表すキャリブレーション モデルを作成し、フロアに適用できます。一般的な減衰特性を多くのフロアで共有している環境（図書館など）では、キャリブレーション モデルを 1 つ作成して、同一の物理レイアウトおよび同一の展開を持つフロアに適用できます。

2 つの方法のいずれかを使用してキャリブレーションのデータを収集できます。

- データ ポイント収集：キャリブレーション ポイントを選択し、カバレッジ領域のロケーションを一度に 1 つ計算します。
- リニア ポイント収集：一連のリニア パスを選択して、パスを経由する際にカバレッジ領域を計算します。 通常、このアプローチはデータ ポイント収集よりも速く計算できます。 また、データ ポイント収集を使用すると、リニア パスで見つからないロケーション データを増やすことができます。

ここでは、次の内容について説明します。

- キャリブレーション モデルのガイドラインと制約事項, （91 ページ）
- データ ポイントおよびキャリブレーション モデルの作成および適用, （92 ページ）

キャリブレーション モデルのガイドラインと制約事項

- キャリブレーション モデルは、クライアント、不正なクライアント、および不正なアクセス ポイントのみに適用できます。 タグのキャリブレーションには、AeroScout システム マネージャを使用します。 タグのキャリブレーションの詳細については、URL http://support.aeroscout.com にあるマニュアルを参照してください。

- 802.11a/n 無線と 802.11b/g/n 無線の両方をサポートするクライアント デバイスを使用して、両方の周波数帯のキャリブレーションを迅速に処理することを推奨します。
- ラップトップやその他のワイヤレス デバイスを使用して、Prime Infrastructure サーバへのブラウザを開き、キャリブレーション プロセスを実行します。
- キャリブレーション データの収集には関連付けられたクライアントのみを使用します。
- 近辺にあるすべてのアクセス ポイントでクライアントが均等に検出されるように、データ収集中のキャリブレーション クライアント ラップトップを回転させます。
- データ収集バーが完了を示したとしても、終了ポイントに到達するまでデータ収集を中止しないでください。
- 通常、ポイント キャリブレーションでは、リニア キャリブレーションよりも正確なキャリブレーションが行われることが明らかになっています。

データ ポイントおよびキャリブレーション モデルの作成および適用

データ ポイントとリニア キャリブレーション モデルを作成して適用するには、次の手順に従ってください。

ステップ 1 [Monitor] > [Site Maps] を選択します。

ステップ 2 [Select a command] ドロップダウン リストから、[RF Calibration Models] を選択します。 [Go] をクリックします。
[RF Calibration Models]ページには、キャリブレーション モデルのリストが表示されます。 デフォルトのキャリブレーション モデルは、すべての仮想ドメインで使用できます。

ステップ 3 [Select a command] ドロップダウン リストから、[Create New Model] を選択します。 [Go] をクリックします。

ステップ 4 [Model Name] テキスト ボックスでモデルに名前を割り当てます。 [OK] をクリックします。
新しいモデルは、他の RF キャリブレーション モデルとともに表示されますが、そのステータスは [Not yet calibrated] として表示されます。

ステップ 5 キャリブレーション プロセスを開始するには、[Model Name] リンクをクリックします。 新しいモデルの詳細が示された新しいページが表示されます。

（注） このページでは、[Select a command list] ドロップダウン リストから適切なオプションを選択して、キャリブレーション モデルの名前変更と削除を行うことができます。 モデルの名前を変更する場合は、[Rename Model] を選択する前に新しい名前を入力します。

ステップ 6 [Select a command] ドロップダウン リストから、[Add Data Points] を選択し、[Go] をクリックします。
このページに表示されるキャンパス、ビルディング、フロアは、仮想ドメインに基づいてフィルタリングされます。

ステップ 7 Cisco Centralized アーキテクチャを介して Prime Infrastructure に接続されたモバイル デバイスからこのプロセスを実行すると、[MAC address] テキスト ボックスに自動的にデバイスのアドレスが読み込まれます。

キャリブレーションの実行に使用しているデバイスの MAC アドレスを手動で入力することもできます。手動で入力する MAC アドレスはコロンで区切る必要があります（例：FF:FF:FF:FF:FF:FF）。

（注） このプロセスが Cisco Centralized アーキテクチャを介して Prime Infrastructure に接続されたモバイル デバイスから実行されている場合は、MAC アドレス テキスト ボックスに自動的にデバイスのアドレスが読み込まれます。

ステップ 8 キャリブレーションを実行する適切なキャンパス、ビルディング、フロア、または屋外領域を選択します。 [Next] をクリックします。

（注） 屋外領域のキャリブレーションはリリース 7.0.200.x 以降でサポートされています。 このオプションを使用して、キャリブレーションデータ ポイントを屋外領域に追加できます。 キャリブレーションと同様の手順を使用して、データ ポイントを屋外領域に追加できます。

ステップ 9 選択したフロア マップおよびアクセス ポイントのロケーションが表示されるときには、キャリブレーションのためにデータが収集されたロケーションがプラス マーク（+）のグリッドで表されます。
これらのロケーションをガイドラインとして使用して、[Calibration Point] ポップアップ（ポイント収集の場合）または [Start]/[Finish] ポップアップ（リニア収集の場合）のいずれかを適切に配置することにより、データのポイント収集またはリニア収集のいずれかを実行できます。これらのポップアップは、それぞれのオプションが表示されるとマップ上に表示されます。

1 ポイント収集を実行するには、次の手順を実行します。

a [Collection Method] ドロップダウン リストから **[Point]** を選択し、**[Show Data Points]** チェックボックスがまだオンになっていない場合にはオンにします。 マップ上に [Calibration Point] ポップアップ メニューが表示されます。

b データ ポイント（+）に [Calibration Point] ポップアップの先端を配置し、[Go] をクリックします。データ収集の進捗を示すページが表示されます。

c 選択したデータ ポイントでデータ収集が完了し、カバレッジ領域がマップ上に表示されたら、[Calibration Point] ポップアップを別のデータ ポイントに移動して [Go] をクリックします。

（注） マップ上に表示されたカバレッジ領域は色分けされ、そのデータを収集するために使用した特定の無線 LAN 規格に対応します。 色分けに関する情報は、左側のサイドバー メニューの凡例内に表示されます。 また、キャリブレーション処理の進捗は、凡例の上の 2 つのステータス バーに示されます。1 つは 802.11a/n 用、もう 1 つは 802.11b/g/n 用です。

（注） データ ポイントを削除するには、[Delete] をクリックして適切なデータ ポイント上に表示される黒の四角形を移動します。 必要に応じて、**Ctrl** キーを押しながらマウスを移動し、四角形のサイズを変更します。

d 関連する周波数帯（802.11a/n、802.11b/g/n）のキャリブレーション ステータス バーに [done] と表示されるまで、ポイント収集のステップ a1 ～ a3 を繰り返します。

（注） キャリブレーション ステータス バーは、少なくとも 50 か所の異なるロケーションと 150 個の測定結果を収集すると、キャリブレーションのデータ収集の完了を表示します。キャリブレーション プロセスで保存されたそれぞれの位置で、複数のデータ ポイントが収集されます。 キャリブレーション処理の進捗は、凡例の上の 2 つのステータス バーに示されます。1 つは 802.11b/g/n 用、もう 1 つは 802.11a/n 用です。

2 リニア収集を実行するには、次の手順を実行します。

a [Collection Method] ドロップダウン リストから [Linear] を選択し、[Show Data points] チェックボックスがまだオンになっていない場合にはオンにします。 [Start] ポップアップと [Finish] ポップアップの両方と共に、マップ上に線が表示されます。

b 開始データ ポイントに [Start] ポップアップの先端を配置します。

c 終了データ ポイントに [Finish] ポップアップを配置します。

d 開始データ ポイントにラップトップを持って立ち、[Go] をクリックします。 定義されたパスに沿って終了ポイントに向かって一定のペースで歩きます。 データ収集が処理中であることを示すダイアログボックスが表示されます。

（注） データ収集バーが完了を示したとしても、終了ポイントに到達するまでデータ収集を中止しないでください。

e 終了ポイントに到達したら、スペース バー（またはデータ収集ページ上の **[Done]**）を押します。 収集ダイアログボックスには、収集したサンプル数が表示されます。収集ダイアログボックスが閉じると、マップが表示されます。 マップには、データが収集されたすべてのカバレッジ領域が表示されます。

（注） 誤って選択したデータ ポイントを削除するには、[Delete] をクリックして適切なデータ ポイント上に表示される黒の四角形を移動します。 必要に応じて、**Ctrl** キーを押しながらマウスを移動し、四角形のサイズを変更します。

（注） カバレッジ領域は色分けされ、そのデータの収集に使用される特定のワイヤレス LAN の規格（802.11a/n、802.11b/g/n、802.11a/b/g/n）に対応します（左ペインの凡例を参照してください）。

f 各周波数帯のステータス バーが [complete] になるまで、ステップ b2 ～ b5 を繰り返します。

（注） リニア収集に加えてデータ ポイント収集を実行すると、見つからないカバレッジ領域に対応できます。

ステップ 10 データ ポイントのキャリブレーションを行うには、ページ上部のキャリブレーション モデル名をクリックします。 このモデルのメイン ページが表示されます。

ステップ 11 [Select a command] ドロップダウン リストから、[Calibrate] を選択し、[Go] をクリックします。

ステップ 12 キャリブレーションが完了したら、[Inspect Location Quality] をクリックします。 RSSI 測定値を示すマップが表示されます。

ステップ 13 新しく作成されたキャリブレーション モデルを使用するには、それが作成されたフロアにそのモデル適用する必要があります（また、類似する減衰特性を持つその他のフロアについても同様）。 **[Monitor] > [Site Maps]** を選択して、フロアを見つけます。 フロア マップのインターフェイスで、ドロップダウン リストから [Edit Floor Area] を選択し、[Go] をクリックします。

ステップ 14 [Floor Type (RF Model)] ドロップダウン リストから、新たに作成したキャリブレーション モデルを選択します。 [OK] をクリックして、フロアにモデルを適用します。

（注） このプロセスを、必要なモデルとフロアの数に応じて繰り返します。 モデルをフロアに適用すると、すべてのロケーションは、キャリブレーション モデルからの収集された減衰データを使用して決定されます。

ロケーションの準備状態と品質の調査

ここでは、次の内容について説明します。

注意事項と制約事項

物理的な検査およびキャリブレーション中に収集されるデータ ポイントを使用して、ロケーションがロケーション仕様（7 m、90 %）を満たしていることを確認できます。

アクセス ポイント データを使用したロケーションの準備状態の確認

アクセス ポイント データを使用してロケーションの準備状態を調べるには、次の手順に従います。

ステップ 1 [Monitor] > [Site Maps] を選択します。

ステップ 2 リストから該当するフロア ロケーション リンクを選択します。
インストールされているすべてのアクセス ポイント、クライアント、およびタグの配置およびその相対的な信号強度を示すマップが表示されます。

（注） RSSI が表示されない場合、[Floor Settings] で [AP Heatmaps] を有効にできます。

（注） クライアント、802.11 タグ、アクセス ポイント、および干渉が表示されない場合は、[Floor Settings] メニューでそれぞれのチェックボックスがオンになっていることを確認します。また、クライアントとタグをそれぞれ追跡するには、クライアントとタグの両方のライセンスを購入済みである必要があります。

（注） クライアントとタグのライセンスのインストールの詳細については、Mobility Services Engine とライセンスの追加および削除, （7 ページ）を参照してください。

ステップ 3 [Select a command] ドロップダウン リストから、[Inspect Location Readiness] を選択し、[Go] をクリックします。
10 m、90 % の位置仕様を満たす領域（[Yes] で示される）と満たさない領域（[No] で示される）を示す、色分けされたマップが表示されます。

キャリブレーション データを使用した位置の品質の調査

領域を実際に調査する際に生成されたデータ ポイントに基づくキャリブレーション モデルが完了すると、アクセス ポイントの位置品質を調査できます。 キャリブレーション データに基づき位置品質を調査するには、次の手順を実行します。

ステップ 1 [Monitor] > [Site Maps] を選択します。

ステップ 2 [Select a command] ドロップダウン リストから、[RF Calibration Model] を選択します。 [Go] をクリックします。
定義されたキャリブレーション モデルの一覧が表示されます。

ステップ 3 適切なキャリブレーション モデルをクリックします。
最後のキャリブレーションの日付、キャリブレーションに使用される信号タイプ別（802.11a、802.11 b/g）のデータ ポイントの数、位置、およびカバレッジを含むキャリブレーションの詳細が表示されます。

ステップ 4 [Inspect Location Quality] リンクをクリックします。
ロケーション エラーの割合を示す、色分けされたマップが表示されます。

（注） 選択されている距離を変更して、位置エラーへの影響を確認できます。

ロケーション精度の確認

ロケーション精度を確認することによって、既存のアクセス ポイントの配置が配置のロケーション精度を予測できることを確認します。

Location Accuracy Tool を使用すると、不正ではないクライアントと不正クライアント、アセット タグ、および干渉のロケーション精度を分析できます。

Location Accuracy Tool では、スケジュール設定済みまたはオンデマンドのいずれかのロケーション精度テストを実行できます。 両方とも、シングル ウィンドウで設定および実行されます。

Location Accuracy Tool を使用してロケーション精度をテストするには 2 種類の方法があります。

- Scheduled Accuracy Testing：クライアントとタグが既に展開されており、無線 LAN にアソシエートされている場合に使用します。 テストが定期的なスケジュール設定済みベースで実行できるようにクライアントとタグが既に事前に配置されている場合は、定期テストを設定して保存できます。
- オンデマンド精度テスト：要素はアソシエートされているが、事前に配置されていない場合に使用します。 オンデマンドテストを使用すると、多数のさまざまな位置のクライアント、タグ、および干渉源の位置精度をテストできます。 通常は、少数のクライアント、タグ、干渉源のロケーション精度をテストするために使用します。

（注） Accuracy Tool では、スケジュール設定済みまたはオンデマンドのいずれかのロケーション精度テストを実行できます。 両方のテストとも、1 つのページで設定および実行されます。

ここでは、次の内容について説明します。

スケジュール設定された精度テストを使用した現在のロケーション精度の検証

スケジュール設定された精度テストを設定するには、次の手順を実行します。

ステップ 1 [Tools] > [Location Accuracy Tool] の順に選択します。

ステップ 2 [Select a command] ドロップダウン リストから、[New Scheduled Accuracy Test] を選択します。

（注） このページに表示されるキャンパス、ビルディング、フロアは、仮想ドメインに基づいてフィルタリングされます。

ステップ 3 テスト名を入力します。

ステップ 4 ドロップダウン リストから領域タイプを選択します。

ステップ 5 [Campus] はデフォルトでシステムのキャンパスとして設定されます。 この設定を変更する必要はありません。

ステップ 6 ドロップダウン リストからビルディングを選択します。

ステップ 7 ドロップダウン リストからフロアを選択します。

ステップ 8 日、時、分を入力して、テストの開始時間および終了時間を選択します。 時間は、24 時間表記です。

（注） テストの開始時間を入力する場合は、テストの開始前にマップ上にテストポイントを配置するのに十分な時間を確保します。

ステップ 9 テスト結果の宛先を選択します。 ユーザに電子メールで送信するレポートを使用することも、[Accuracy Tests] > [Results] ページからテスト結果をダウンロードすることもできます。 レポートは PDF 形式で示されます。

（注） [Email] オプションを選択する場合は、目的の電子メール アドレスに対して SMTP メール サーバを定義しておく必要があります。 [Administrator] > [Settings] > [Mail Server Configuration] の順に選択して、適切な情報を入力します。

ステップ 10 [Position Testpoints] をクリックします。 MAC アドレスを持つフロア上のクライアントおよびタグすべてのリストと共にフロア マップが表示されます。

ステップ 11 ロケーション精度を確認する各クライアントおよびタグの隣のチェックボックスをオンにします。 クライアントまたはタグの MAC アドレスのチェックボックスを選択すると、2 つの重複したアイコンがその要素のマップに表示されます。

一方のアイコンは実際の位置を表し、もう一方のアイコンは報告された位置を表しています。

（注） 一覧表示されないクライアントまたはタグの MAC アドレスを入力するには、[Add New MAC] チェックボックスをオンにして MAC アドレスを入力し、[GO] をクリックします。 その要素のアイコンがマップに表示されます。 新しく追加された要素が Mobility Services Engine の別のフロアにある場合は、アイコンの左隅（0,0）位置に表示されます。

ステップ 12 要素の実際の位置が報告された位置と同じではない場合、その要素の実際の位置アイコンをマップ上の正しい位置にドラッグします。

（注） 実際の位置のアイコンだけをドラッグできます。

ステップ 13 すべての要素が配置されたら [Save] をクリックします。 正常な精度テストを確認するページが表示されます。

ステップ 14 [OK] をクリックして、確認ページを閉じます。 [Accuracy Tests] 概要ページに戻ります。

（注） テストの実行直前には、精度テスト ステータスは [Scheduled] と表示されます。 テストが実行中であると、ステータスに [In Progress] が表示され、テストが終了すると [Idle] が表示されます。 テストが正常に終了しないと [Failure] ステータスが表示されます。

ステップ 15 ロケーション精度テストの結果を表示するには、[Test name] をクリックして表示されるページの [Download] をクリックします。

Scheduled Location Accuracy Report に表示される情報は、次のとおりです。

- さまざまなエラー範囲内の要素の割合を説明する概要のロケーション精度レポート
- エラー距離ヒストグラム
- 累積エラー分散グラフ
- エラー距離経時グラフ
- ロケーション精度テストを実施した MAC アドレスごとの概要。実際の位置、エラー距離、および空間精度（実際の位置と計算上の位置の比較）と時系列でのエラー距離を示すマップが各 MAC について報告されます。

オンデマンドのロケーション精度テストの使用

オンデマンド精度テストは、要素がアソシエートされているが、事前に配置されていない場合に実行します。 オンデマンド精度テストを使用すると、多数のさまざまな位置のクライアントとタ

グの位置精度をテストできます。 通常は、少数のクライアントとタグのロケーション精度をテストするのに使用します。 オンデマンド精度テストを実行するには、次の手順に従ってください。

ステップ 1 [Tools] > [Location Accuracy Tool] の順に選択します。

ステップ 2 [Select a command] ドロップダウン リストから、[New On demand Accuracy Test] を選択します。

ステップ 3 テスト名を入力します。

ステップ 4 ドロップダウン リストから領域タイプを選択します。

ステップ 5 [Campus] はデフォルトでシステムのキャンパスとして設定されます。 この設定を変更する必要はありません。

ステップ 6 ドロップダウン リストからビルディングを選択します。

ステップ 7 ドロップダウン リストからフロアを選択します。

ステップ 8 [Accuracy Tests] > [Results] ページのテスト結果を参照します。 レポートは PDF 形式で示されます。

ステップ 9 [Position Testpoints] をクリックします。 座標（0,0）に赤色の十字線が付いたフロア マップが表示されます。

ステップ 10 ロケーション精度とロケーションの RSSI をテストするには、左側のドロップダウン リストから [client] または [tag] のいずれかを選択します。 選択したオプション（[client] または [tag]）のすべての MAC アドレスのリストが、右側のドロップダウン リストに表示されます。

ステップ 11 ドロップダウン リストから MAC アドレスを選択し、赤色の十字線をマップ ロケーションに移動して、マウスをクリックして配置します。

ステップ 12 精度データの収集を開始するには、[Start] をクリックします。

ステップ 13 データの収集を終了するには、[Stop] をクリックします。 [Stop] をクリックする前に少なくとも 2 分間テストを実行してください。

ステップ 14 マップ上にプロットする各テスト ポイントについてステップ 10 ～ステップ 13 を繰り返します。

ステップ 15 テストポイントのマッピングが終了したら、[Analyze] をクリックします。

ステップ 16 表示されるページで [Results] タブをクリックします。
[On-demand Accuracy Report] に表示される概要は、次のとおりです。

- さまざまなエラー範囲内の要素の割合を説明する概要のロケーション精度レポート
- エラー距離ヒストグラム
- 累積エラー分散グラフ

ステップ 17 [Accuracy Tests] 概要ページから精度テスト ログをダウンロードするには、次の手順を実行します。

- [listed test] チェックボックスをオンにし、[Select a command] ドロップダウン リストから [Download Logs] または [Download Logs for Last Run] を選択します。
- [Go] をクリックします。

  [Download Logs] オプションは、選択したテストのすべての精度テストのログをダウンロードします。 [Download Logs for Last Run] オプションは、選択したテストの最新のテスト実行のログのみをダウンロードします。

最適化モニタモードを使用したタグロケーションレポートの強化

タグのモニタリングとロケーション計算を最適化するには、アクセス ポイントの 2.4GHz 帯（802.11b/g 無線）内で、最高 4 つのチャネルに対して TOMM（追跡最適化モニタ モード）を有効にできます。 これによって、タグが機能するようにプログラミングされているチャネルだけを対象にチャネル スキャンを実行できます（チャネル 1、チャネル 6、チャネル 11 など）。

TOMM を有効にして、アクセス ポイントの 802.11 b/g 無線にモニタリング チャネルを割り当てる前に、アクセス ポイント レベルでモニタ モードを有効にする必要があります。

ここでは、次の内容について説明します。

注意事項と制約事項

モニタ対象として 4 つすべてのチャネルを選択する必要はありません。

タグのモニタリングとロケーション計算の最適化

タグのモニタリングとロケーション計算を最適化するには、次の手順に従ってください。

ステップ 1 次の手順に従って、アクセス ポイントでモニタ モードを有効にします。

a) [Configure] > [Access Point] > [AP Name] を選択します。
b) AP モードとして [Monitor] を選択します。

ステップ 2 次の手順を実行して、アクセス ポイント無線で TOMM を有効にして、モニタリング チャネルを割り当てます。

a) アクセス ポイント レベルでモニタ モードを有効にした後、[Configure] > [Access Points] の順に選択します。
b) [Access Points] 概要ページで、モニタ モードが有効になっているアクセス ポイントの [802.11 b/g Radio] リンクをクリックします。
c) [Radio details] ページで、チェックボックスを選択解除して [Admin Status] を無効にします。 無線が無効になります。
d) [Enable TOMM] チェックボックスをオンにします。

e) アクセス ポイントでタグをモニタする最大 4 つのチャネル（[Channel 1]、[Channel 2]、[Channel 3]、[Channel 4]）を選択します。
（注） モニタ チャネルを削除するには、チャネルのドロップダウン リストから [None] を選択します。
f) [Save] をクリックします。
g) [Radio] パラメータ ページで、[Admin Status] チェックボックスを選択して無線を再度有効にします。
h) [Save] をクリックします。 これで、アクセス ポイントが TOMM アクセス ポイントとして設定されました。
[Monitor] > [Access Points] ページに、AP モードが [Monitor] と表示されます。

干渉の通知の設定

この機能は、[Campus, Building, and Floor View] ページからのみ設定できます。 干渉の通知を設定するには、次の手順に従います。

ステップ 1 [Design] > [Site Maps] を選択します。
ステップ 2 適切なフロア、建物、またはキャンパス領域の名前をクリックします。
ステップ 3 [Select a command]ドロップダウン リストから [Configure Interferer Notifications] を選択して、[Go] をクリックします。
[Interferer CAS notification Configuration]ページが表示されます。 次のデバイスが表示されます。

- Bluetooth リンク
- 電子レンジ
- 802.11FH
- Bluetooth 検出
- TDD トランスミッタ
- Jammer
- 連続トランスミッタ
- DECT like Phone
- Video Camera
- 80.15.4
- WiFi Inverted
- WifI Invalid チャネル
- Super AG

- レーダー
- Canopy
- XBox
- WiMax Mobile
- WiMax Fixed

ステップ 4 通知を生成するデバイスのチェックボックスをオンにします。

ステップ 5 [Save] をクリックします。

Context-Aware Service パラメータの変更

クライアントとタグのロケーション計算（Receiver Signal Strength Indicator（RSSI）測定など）に影響するパラメータの変更も可能です。アドホックの不正クライアントと不正アクセスポイントの追跡解除とレポート解除。

ここでは、次の内容について説明します。

- ライセンス要件, （89 ページ）
- 注意事項と制約事項, （103 ページ）
- 追跡パラメータの変更, （103 ページ）
- フィルタリング パラメータの変更, （108 ページ）
- 履歴パラメータの変更, （110 ページ）
- ロケーション プレゼンスの有効化, （112 ページ）
- アセット情報のインポートとエクスポート, （114 ページ）
- ロケーション パラメータの変更, （115 ページ）

ライセンス要件

アクセス ポイントからタグとクライアントに関する状況依存情報を取得するには、ライセンスが必要です。クライアントのライセンスには、不正クライアントおよび不正アクセスポイントの追跡も含まれます。タグとクライアントのライセンスは個別に提供され、3,000 ～ 12,000 単位の数量の範囲で提供されます。詳細については、次のURLで『Cisco 3300 Series Mobility Services Engine Licensing and Ordering Guide』を参照してください。http://www.cisco.com/en/US/products/ps9742/products_data_sheets_list.html

注意事項と制約事項

Cisco 3315 Mobility Services Engine は、最大 2,000 個のクライアントとタグをサポートし、Cisco 3350 Mobility Services Engine は最大 18,000 個のクライアントとタグをサポートします。

追跡パラメータの変更

Mobility Services Engine は、正規ライセンスの購入と Mobility Services Engine によって、Cisco 3355 Mobility Service Engine では最大 25,000 のクライアント、仮想アプライアンスでは最大 50,000 のクライアント（不正クライアント、不正アクセス ポイント、有線クライアント、干渉を含む）およびタグ（合計数）を追跡できます。 追跡中のタグ、クライアント、および干渉のロケーションに関する更新情報は、コントローラから Mobility Services Engine に送信されます。

コントローラが追跡しているタグ、クライアント、および干渉のみが、Prime Infrastructure マップ、クエリー、およびレポートに表示されます。 追跡対象外の要素のイベントとアラームは一切収集されず、クライアントまたはタグの 18,000 個の要素上限にはカウントされません。

Prime Infrastructure を使用して次の追跡パラメータを変更できます。

- ロケーションをアクティブに追跡する有線クライアント ステーションとワイヤレス クライアント ステーション、アクティブなアセット タグ、不正クライアント、干渉、およびアクセス ポイントを有効および無効にします。
- 有線クライアント ロケーションの追跡により、データセンターのサーバはネットワーク上の有線クライアントを容易に検出できるようになります。 サーバにはネットワーク上の有線スイッチ ポートが関連付けられています。
- 追跡対象とする特定要素の上限を設定します。

  たとえば、25,000 の追跡対象ユニットのクライアント ライセンスで、追跡できるクライアント ステーションの数の制限を 10,000 として設定できます（この場合残りの 15,000 ユニット分は、不正クライアントと不正アクセス ポイント間の追跡に使用できます）。 特定の要素の追跡上限に達すると、追跡されていない要素の合計数が [Tracking Parameters] ページに表示されます。

この項では、次のトピックについて取り上げます。

- 注意事項と制約事項, （103 ページ）
- Mobility Services Engine の追跡パラメータの設定, （104 ページ）

注意事項と制約事項

- Mobility Services Engine をリリース 6.0 から 7.0 にアップグレードすると、ワイヤレス クライアントまたは不正の制限が設定されている場合、この制限はリセットされます。これは、リリース 7.0 では有線クライアントの制限が変更されているためです。

- 追跡対象クライアントの実際の数は、購入ライセンスによって決まります。
- 追跡対象のアクティブ RFID タグの実際の数は、購入ライセンスによって決まります。
- より適切な遅延と正確性を確保するために、リリース 4.2 以降のコントローラを使用することを推奨します。

Mobility Services Engine の追跡パラメータの設定

Mobility Services Engine の追跡パラメータを設定するには、次の手順に従います。

ステップ 1 [Services] > [Mobility Services] の順に選択します。 [Mobility Services] ページが表示されます。

ステップ 2 プロパティを編集する Mobility Services Engine の名前をクリックします。 [General Properties] ページが表示されます。

ステップ 3 設定オプションを表示するには、[Context Aware Service] > [Administration] > [Tracking Parameters] を選択します。

ステップ 4 必要に応じて、追跡パラメータを変更します。 次の表に、追跡パラメータを示します。

表 *9* : *Tracking Parameters*

フィールド	設定オプション
Tracking Parameters	
Wired Clients	**1** Mobility Services Engine によるクライアント ステーションの追跡を有効にするには、[Enable] チェックボックスをオンにします。 リリース 7.0 では、クライアント ライセンスはすべてのネットワーク ロケーション サービス要素を対象としており、有線クライアント、ワイヤレス クライアント、不正クライアント、不正アクセス ポイント、および干渉の間で共有されます。 有線クライアント数の制限は、Mobility Services Engine 7.0 および Prime Infrastructure Release 7.0 以降でサポートされています。 つまり、有線クライアントの数を一定数（例：500）に制限できます。 この制限を設定することで、ライセンスで許可されているデバイスの数が有線クライアントによって使い切ることがなく、一部のライセンスがワイヤレス クライアントに対して使用可能になります。 **注意** Mobility Services Engine をリリース 6.0 からアップグレードすると、ワイヤレス クライアントまたは不正クライアント/アクセス ポイントの制限が設定されている場合、この制限はリセットされます。これは、リリース 7.0 では有線クライアントの制限が変更されているためです。 （注） [Active Value]（表示のみ）：現在追跡されている有線クライアント ステーションの数を示します。 （注） [Not Tracked]（表示のみ）：上限を超えている有線クライアント ステーションの数を示します。

フィールド	設定オプション
Wireless Clients	1 Mobility Services Engine によるクライアント ステーションの追跡を有効にするには、[Enable] チェックボックスをオンにします。 2 追跡対象クライアント ステーションの数の上限を設定するには、[Enable Limiting] チェックボックスをオンにします。 3 上限が有効になっている場合は、上限値を入力します。 入力できる上限値は、18,000（Mobility Services Engine で追跡できるクライアントの最大数）までの正の値です。 （注） [Active Value]（表示のみ）：現在追跡されているクライアント ステーションの数を示します。 （注） [Not Tracked]（表示のみ）：上限を超えているクライアント ステーションの数を示します。
Rogue Access Points	1 Mobility Services Engine による不正アクセス ポイントの追跡を有効にするには、[Enable] チェックボックスをオンにします。 2 追跡対象不正アクセス ポイントの数の制限を設定するには、[Enable Limiting] チェックボックスをオンにします。 3 上限が有効になっている場合は、上限値を入力します。入力できる制限は、18,000（Mobility Services Engine で追跡できる不正アクセス ポイントの最大数）までの正の値です。 （注） [Active Value]（表示のみ）：現在追跡している不正アクセス ポイントの数を示します。 （注） [Not Tracked]（表示のみ）：制限を超えた不正アクセス ポイントの数を示します。
Exclude Ad-Hoc Rogues	ネットワーク内のアドホックの不正クライアント/アクセス ポイントの追跡と報告を無効にするには、このチェックボックスをオンにします。 このように設定すると、Prime Infrastructure マップにアドホック不正クライアント/アクセス ポイントが表示されず、イベントとアラームが報告されません。

フィールド	設定オプション
Rogue Clients	1 Mobility Services Engine による不正クライアントの追跡を有効にするには、[Enable] チェックボックスをオンにします。 2 追跡対象不正クライアントの数の上限を設定するには、[Enable Limiting] チェックボックスをオンにします。 3 上限が有効になっている場合は、上限値を入力します。入力できる上限値は、任意の正の値です。この上限値は、プラットフォームによって異なります。上限値は、Mobility Services Engine で追跡できる不正クライアントの最大数です。 （注） [Active Value]（表示のみ）：追跡されている不正クライアントの数を示します。 （注） [Not Tracked]（表示のみ）：上限を超えている不正クライアントの数を示します。
Interferers	1 Mobility Services Engine による干渉の追跡を有効にするには、[Enable] チェックボックスをオンにします。 2 追跡対象干渉の数の制限を設定するには、[Enable Limiting] チェックボックスをオンにします。 3 上限が有効になっている場合は、上限値を入力します。 リリース 7.0 では、クライアント ライセンスはすべてのネットワーク ロケーション サービス要素を対象としており、有線クライアント、ワイヤレス クライアント、不正クライアント、不正アクセス ポイント、および干渉の間で共有されます。 リリース 7.0.200.x では、クライアント ライセンスはすべてのネットワーク ロケーション サービス要素を対象としており、有線クライアント、ワイヤレス クライアント、不正クライアント、不正アクセス ポイント、干渉、およびゲストの間で共有されます。 （注） [Active Value]（表示のみ）：現在追跡されている干渉の数を示します。 （注） [Not Tracked]（表示のみ）：上限を超えている干渉の数を示します。
Asset Tracking Elements	

フィールド	設定オプション
Active RFID Tags	Mobility Services Engine によるアクティブ RFID タグの追跡を有効にするには、[Enable] チェックボックスをオンにします。 （注） 追跡対象のアクティブ RFID タグの実際の数は、購入ライセンスによって決まります。 （注） [Active Value]（表示のみ）：現在追跡されているアクティブ RFID タグの数を示します。 （注） [Not Tracked]（表示のみ）：上限を超えているアクティブ RFID タグの数を示します。
SNMP Retry Count	ポーリング サイクルの再試行回数を入力します。 デフォルト値は 3 です。 有効値は 1 ～ 99999 です。 （コントローラ リリース 4.1 以前とロケーション サーバ リリース 3.0 以前のみで設定可能）。
SNMP Timeout	ポーリングサイクルがタイムアウトになるまでの秒数を入力します。デフォルト値は 5 です。 有効値は 1 ～ 99999 です。 （コントローラ リリース 4.1 以前とロケーション サーバ リリース 3.0 以前のみで設定可能）。
Client Stations	クライアント ステーションのポーリングを有効にし、ポーリング間隔（秒数）を入力するには、[Enable] チェックボックスをオンにします。 デフォルト値は 300 です。 有効値は 1 ～ 99999 です。 （コントローラ リリース 4.1 以前とロケーション サーバ リリース 3.0 以前のみで設定可能）。
Active RFID Tags	アクティブ RFID タグのポーリングを有効にし、ポーリング間隔（秒数）を入力するには、[Enable] チェックボックスをオンにします。 有効値は 1 ～ 99999 です。 （注） モビリティ サービスがコントローラからアセット タグ データを収集する前に、コントローラで **config rfid status enable** コマンドを使用して、アクティブ RFID タグの検出を有効にする必要があります。
Rogue Clients and Access Points	不正アクセス ポイントのポーリングを有効にし、ポーリング間隔（秒数）を入力するには、[Enable] チェックボックスをオンにします。 デフォルト値は 600 です。 指定できる値は 1 ～ 99999 です（コントローラ リリース 4.1 以前とロケーション サーバ リリース 3.0 以前のみで設定可能）。
統計情報	モビリティ サービスの統計ポーリングを有効にし、ポーリング間隔（秒数）を入力するには、[Enable] チェックボックスをオンにします。 デフォルト値は 900 です。 指定できる値は 1 ～ 99999 です（コントローラ リリース 4.1 以前とロケーション サーバ リリース 3.0 以前のみで設定可能）。

ステップ 5 [Save] をクリックし、Mobility Services Engine データベースに新しい設定を保存します。

フィルタリング パラメータの変更

- MAC アドレス

  特定の MAC アドレスを入力し、ロケーション追跡の許可または不許可を設定できます。 許可または不許可にするMACアドレスを記述したファイルをインポートするか、またはPrime Infrastructure に個々の MAC アドレスを入力することができます。

  MAC アドレスの入力形式は xx:xx:xx:xx:xx:xx です。 MAC アドレスのファイルをインポートする場合、ファイルは次の特定の形式に従っている必要があります。

  - 各 MAC アドレスを 1 行ずつ記述する必要があります。
  - 最初に許可 MAC アドレスを最初にリストする必要があります。この際、許可 MAC アドレスの前に [Allowed] 行項目を記述します。 [Disallowed] の後に不許可 MAC アドレスをリストする必要があります。
  - ワイルドカードを使用して MAC アドレスの範囲を指定できます。 たとえば、次の [Allowed] リストの 1 番目のエントリ「00:11:22:33:*」はワイルドカードです。

  （注） 許可 MAC アドレスの形式は、[Filtering Parameters] 設定ページに表示されます。

  ファイルの記述例：

  [Allowed] 00:11:22:33:* 22:cd:34:ae:56:45 02:23:23:34:* [Disallowed] 00:10:* ae:bc:de:ea:45:23

- プローブ クライアント

  プローブ クライアントは、あるコントローラに関連付けられているが、プロービング アクティビティによって別のコントローラから認識され、そのプライマリ コントローラとともにプローブ済みコントローラの要素としてカウントされるクライアントです。

  ここでは、次の内容について説明します。

- 注意事項と制約事項, （108 ページ）
- Mobility Services Engine のフィルタリング パラメータの設定, （109 ページ）

注意事項と制約事項

プローブ クライアントを除外すると、関連付けられたクライアントのライセンスを解放できます。

Mobility Services Engine のフィルタリング パラメータの設定

Mobility Services Engine のフィルタリング パラメータを設定するには、次の手順に従います。

ステップ 1 [Services] > [Mobility Services Engines] の順に選択します。 [Mobility Services] ページが表示されます。

ステップ 2 プロパティを編集する Mobility Services Engine の名前をクリックします。 [General Properties] ページが表示されます。

ステップ 3 設定オプションを表示するには、[Context Aware Service] > [Administration] > [Filtering Parameters] を選択します。

ステップ 4 必要に応じて、フィルタリング パラメータを変更します。 次の表に、フィルタリング パラメータを示します。

表 *10* : ***Filtering Parameters***

フィールド	設定オプション
Advanced Filtering Params	
Duty Cycle Cutoff Interferers	指定した制限を満たすデューティ サイクルのある干渉のみ追跡され、CASに対してカウントされるように、干渉のデューティ サイクルのカットオフ値を入力します。 [Duty Cycle Cutoff Interferers] のデフォルト値は 0% で、設定可能な範囲は 0% ～ 100% です。 ロケーション ライセンスをより適切に使用するために、干渉のデューティ サイクルに基づいて干渉のフィルタを指定することもできます。
プローブ クライアントの RSSI Cutoff	RSSI 値が cutoff 値を下回るクライアントをレポートするように、プローブ クライアントの RSSI Cutoff の値を入力します。プローブ クライアントのRSSI Cutoffのデフォルト値は、1-128dBです。
MAC Filtering Params	
Exclude Probing Clients	プローブ クライアントのロケーション計算を実行しないようにするには、このチェックボックスをオンにします。

フィールド	設定オプション
Enable Location MAC Filtering	1 MAC アドレスによる特定要素のフィルタリングを有効にするには、このチェックボックスをオンにします。 2 MAC アドレスのファイルをインポートするには（[Upload a file for Location MAC Filtering]テキスト ボックス）、ファイル名を検索して選択し、[Save] をクリックしてファイルをロードします。 リストのMACアドレスが、ファイルの指定に基づいて [Allowed List] と [Disallowed List] に自動的に読み込まれます。 （注） 許可MACアドレスの形式を表示するには、[Upload a file for Location MAC Filtering] テキスト ボックスの横にある赤色の疑問符をクリックします。 3 個々の MAC アドレスを追加するには、MAC アドレス（形式：xx:xx:xx:xx:xx:xx）を入力して [Allow] または [Disallow] をクリックします。 該当する列にアドレスが表示されます。 （注） [Allow] 列と [Disallow] 列の間でアドレスを移動するには、MACアドレス項目を選択し、該当する列の下にあるボタンをクリックします。 （注） 複数のアドレスを移動するには、最初の MAC アドレスをクリックし、Ctrl キーを押しながら他の MAC アドレスを選択します。 その列にアドレスを入れるには、[Allow] または [Disallow] をクリックします。 （注） MAC アドレスが [Allow] 列と [Disallow] 列のいずれにもリストされていない場合、デフォルトでは [Blocked MACs] 列に表示されます。 [Unblock] ボタンをクリックすると、MACアドレスは自動的に [Allow] 列に移動します。 [Disallow] 列に移動するには、[Allow] 列の下にある [Disallow] ボタンをクリックします。

ステップ 5 [Save] をクリックし、Mobility Services Engine データベースに新しい設定を保存します。

履歴パラメータの変更

この項では、Mobility Services Engine 履歴パラメータの設定, （111 ページ）について説明します。

注意事項と制約事項

ロケーション プレゼンスを有効にする前に、Mobility Services Engine を同期してください。

Mobility Services Engine 履歴パラメータの設定

Mobility Services Engine の履歴を設定するには、次の手順に従ってください。

ステップ 1 [Services] > [Mobility Services Engines] の順に選択します。

ステップ 2 プロパティを編集する Mobility Services Engine の名前をクリックします。

ステップ 3 [Context Aware Service] > [Administration] > [History Parameters] を選択します。

ステップ 4 次に示す履歴パラメータを必要に応じて変更します。 次の表に、履歴パラメータを示します。

表 *11* : ***History Parameters***

フィールド	説明
Archive for	ロケーション サーバで有効な各カテゴリの履歴を維持する日数を入力します。 デフォルト値は 30 です。 有効値は 1 ～ 365 です。
Prune data starting at	ロケーション サーバがデータ プルーニングを開始する時刻（時間と分）を入力します（時間は 0 ～ 23、分は 1 ～ 59）。 データ プルーニングを再び開始するまでの間隔（分）を入力します（1 ～ 99900000）。 デフォルトの開始時刻は 23 時間 50 分、デフォルトの間隔は 1440 分です。 （注） パフォーマンスを高めるには、デフォルトの制限を入力します。
Client Stations	クライアント ステーションの履歴データの収集をオンにするには、[Enable] チェックボックスをオンにします。
Wired Stations	有線ステーションの履歴データの収集をオンにするには、[Enable] チェックボックスをオンにします。
Asset Tags	履歴データの収集をオンにするには、[Enable] チェックボックスをオンにします。 （注） モビリティ サービスがコントローラからアセット タグ データを収集する前に、**config rfid status enable** コマンドを使用して、RFID タグの検出を有効にする必要があります。
Rogue Clients and Access Points	履歴データの収集をオンにするには、[Enable] チェックボックスをオンにします。
Interferers	履歴データの収集をオンにするには、[Enable] チェックボックスをオンにします。

ステップ 5 Mobility Services Engine データベースに選択を保存するには、[Save] をクリックします。

ロケーション プレゼンスの有効化

Mobility Services Engine でロケーション プレゼンスを有効にすると、シスコのデフォルト設定（キャンパス、ビルディング、フロア、XY 座標）以外の都市ロケーション情報（市町村、州、郵便番号、国）および地理的なロケーション情報（経度、緯度）を拡張できます。 ロケーションベースのサービスおよびアプリケーションで使用するために、ワイヤレス クライアントと有線クライアントに関するにこの情報をオンデマンドで要求できます。

また、拡張ロケーション情報（有線クライアントの MAC アドレス、有線クライアントが接続している有線スイッチのスロットおよびポートなど）をインポートできます。

新しいキャンパス、ビルディング、フロア、または屋外領域を後で追加または設定するときに、ロケーション プレゼンスを設定できます。

有効にすると、Mobility Services Engine は要求 Cisco CX v5 クライアントに対しそのクライアントのロケーションを示すことができます。

（注） この機能を有効にする前に、Mobility Services Engine を同期する必要があります。

ここでは、次の内容について説明します。

- 注意事項と制約事項, （111 ページ）
- Mobility Services Engine でのロケーション プレゼンスの有効化と設定, （113 ページ）

注意事項と制約事項

ロケーション プレゼンスを有効にする前に、Mobility Services Engine を同期してください。

Mobility Services Engine でのロケーション プレゼンスの有効化と設定

Mobility Services Engine でロケーション表示を有効化および設定するには、次の手順に従います。

ステップ 1 [Services] > [Mobility Services Engines] の順に選択します。 キャンパス、ビルディング、またはフロアが割り当てられている Mobility Services Engine を選択します。

ステップ 2 [Context Aware Service] > [Administration] > [Presence Parameters] を選択します。 [Presence] ページが表示されます。

ステップ 3 [Service Type On Demand] チェックボックスをオンにし、Cisco CX クライアント v5 のロケーション表示を有効にします。

ステップ 4 次のロケーション解決オプションのいずれかを選択します。

a) [Building] が選択されている場合、Mobility Services Engine は要求クライアントに対し、そのクライアントのロケーションをビルディングで示します。

- たとえば、Building A に配置されているクライアントがそのロケーションを要求している場合、Mobility Services Engine はクライアント アドレスとして *Building A* を返します。

b) [AP] が選択されている場合、Mobility Services Engine は要求クライアントに対し、そのクライアントのロケーションを、関連付けられているアクセス ポイントで示します。 アクセス ポイントの MAC アドレスが表示されます。

- たとえば、MAC アドレス 3034:00hh:0adg のアクセス ポイントに関連付けられているクライアントがそのロケーションを要求している場合、Mobility Services Engine はクライアントにアドレス *3034:00hh:0adg* を返します。

c) [X,Y] が選択されている場合、Mobility Services Engine は要求クライアントに対し、そのクライアントのロケーションを XY 座標で示します。

- たとえば、（50, 200）に位置しているクライアントがそのロケーションを要求している場合、Mobility Services Engine はクライアントにアドレス *50, 200* を返します。

ステップ 5 必要なロケーション形式のチェックボックスをオンにします。

a) [Cisco] チェックボックスをオンにすると、ロケーションがキャンパス、ビルディング、フロア、および XY 座標で示されます。 これがデフォルト設定です。

b) [Civic] チェックボックスをオンにすると、キャンパス、ビルディング、フロア、または屋外領域の名前とアドレス（通り、市、州、郵便番号、国）が示されます。

c）[GEO] チェックボックスをオンにすると、緯度と経度による座標が示されます。

ステップ 6 デフォルトでは、[Location Response Encoding] の [Text] チェックボックスがオンになっています。 これは、クライアントが受信する情報の形式を示しています。 この設定を変更する必要はありません。

ステップ 7 受信側クライアントが受信した情報を別の相手へ再送信できるようにするには、[Retransmission Rule] の [Enable] チェックボックスをオンにします。

ステップ 8 [Retention Expiration] 値を分単位で入力します。 これにより、クライアントで格納される受信情報が上書きされるまでの時間を決定します。 デフォルト値は 24 時間（1440 分）です。

ステップ 9 [Save] をクリックします。

アセット情報のインポートとエクスポート

ここでは、次の内容について説明します。

アセット情報のインポート

Prime Infrastructure を使用して Mobility Services Engine のアセット、チェックポイント、および TDOA レシーバ情報をインポートするには、次の手順に従います。

ステップ 1 [Services] > [Mobility Services Engines] の順に選択します。

ステップ 2 アセット情報のインポート先 Mobility Services Engine の名前をクリックします。

ステップ 3 [Context Aware Service] > [Administration] > [Import Asset Information] の順に選択します。

ステップ 4 テキスト ファイル名を入力するか、ファイル名を参照して選択します。
インポート ファイルの情報を次の形式で指定します。

- タグ形式：# タグ、00:00:00:00:00:00、カテゴリ名、グループ名、アセット名
- ステーション形式：# ステーション、00:00:00:00:00:00、カテゴリ名、グループ名、アセット名

ステップ 5 [Import] をクリックします。

アセット情報のエクスポート

Prime Infrastructure を使用してアセット、チェックポイント、および TDOA レシーバ情報を Mobility Services Engines からファイルにエクスポートするには、次の手順に従います。

ステップ 1 [Services] > [Mobility Services Engines] の順に選択します。

ステップ 2 情報のエクスポート元 Mobility Services Engine の名前をクリックします。

ステップ 3 [Context Aware Service] > [Administration] > [Export Asset Information] の順に選択します。
エクスポート ファイルの情報を次の形式で指定します。

- タグ形式 : # タグ、00:00:00:00:00:00、カテゴリ名、グループ名、アセット名
- ステーション形式 : # ステーション、00:00:00:00:00:00、カテゴリ名、グループ名、アセット名

ステップ 4 [Export] をクリックします。

ステップ 5 [Open]（ページに表示）、[Save]（外部 PC またはサーバに表示）、または [Cancel] をクリックします。
（注） [Save] をクリックすると、アセット ファイルの宛先と名前を選択するよう求められます。 デフォルトのファイル名は assets.out です。 ダウンロードが完了したら、ダイアログボックスから [Close] をクリックします。

ロケーション パラメータの変更

ここでは、次の内容について説明します。

- ロケーション パラメータの設定, （115 ページ）

ロケーション パラメータの設定

ロケーション パラメータを設定するには、次の手順に従います。

ステップ 1 [Services] > [Mobility Services Engines] の順に選択します。

ステップ 2 プロパティを変更する Mobility Services Engine の名前をクリックします。

ステップ 3 [Context Aware Service] > [Advanced] > [Location Parameters] を選択します。 設定オプションが表示されます。

ステップ 4 必要に応じて、ロケーションパラメータを変更します。次の表に、ロケーションパラメータを示します。

表 *12* : ***Location Parameters***

フィールド	設定オプション
Enable Calculation time	ロケーション計算に要する時間の計算を開始するには、[Enable] チェックボックスをオンにします。 （注） このパラメータは、クライアント、不正アクセス ポイント、不正クライアント、および干渉のみに適用されます。 **注意** 全体的なロケーション計算が遅くなるため、Cisco TAC 担当者の指導の下でのみこのパラメータを有効にしてください。
有効外壁（OW）位置	ロケーション計算の一部として外壁（OW）計算を含めるには、[Enable] チェックボックスをオンにします。 （注） このパラメータは、Mobility Services Engine によって無視されます。
Relative discard RSSI time	最新の RSSI サンプルから、RSSI 測定が廃棄されるまでの経過時間を分単位で入力します。たとえば、このパラメータを3分に設定し、Mobility Services Engine は、10 ～ 12 分で 2 つのサンプルを受信する場合、両方のサンプルが保持されます。 15 分で受信されたその他のサンプルは廃棄されます。デフォルト値は3です。有効値の範囲は 0 ～ 99999 です。 3 未満の値を指定することは推奨されません。 （注） このパラメータは、クライアント、不正アクセス ポイント、不正クライアント、および干渉のみに適用されます。
Absolute discard RSSI time	最新のサンプルに関係なく、RSSI 測定が古いものと見なされ廃棄されるまでの経過時間を分単位で入力します。デフォルト値は 60 です。 有効値の範囲は 0 ～ 99999 です。 60 未満の値を指定することは推奨されません。 （注） このパラメータは、クライアントだけに適用されます。

フィールド	設定オプション
RSSI Cutoff	1 mW（dBm）に基づく RSSI の遮断の値をデシベル（dBs）単位で入力します。この値を超えると、Mobility Services Engine は常にアクセス ポイント測定を使用します。 デフォルト値は -75 です。 （注） RSSI の遮断値を上回る 3 つ以上の測定が使用可能な場合、Mobility Services Engine では計算には最も強力な 3 つ（またはこれ以上）の測定が使用され、それ以外の弱い値（RSSI の遮断値を下回る値）はすべて廃棄されます。ただし、RSSI の遮断値を下回る弱い測定のみが使用可能な場合は、これらの値が計算に使用されます。 （注） このパラメータは、クライアントだけに適用されます。 注意 変更は、シスコ TAC 担当者の指示がある場合にだけ行ってください。 この値を変更すると、ロケーション計算の精度が低下する可能性があります。
Enable Location Filtering	計算されるロケーションのジッターを抑えるために、ロケーションのフィルタリングが使用されます。 これは、配置されたデバイスがフロアマップ上の2つの異なるポイント間で割り込みを行うことを防ぎます。
Chokepoint Usage	チョークポイントがシスコ互換のタグを追跡できるようにするには、[Enable] チェックボックスをオンにします。
Use Chokepoints for Interfloor conflicts	境界チョークポイントまたは重み付けロケーションの測定値を使用して、シスコ互換のタグを見つけることができます。 オプション： • [Never]：選択すると、シスコ互換のタグを見つけるために、境界チョークポイントは使用されません。 • [Always]：選択すると、シスコ互換のタグを見つけるために、境界ポイントが使用されます。 • [Floor Ambiguity]：選択すると、シスコ互換のタグを見つけるために、重み付けされロケーションの測定値と境界チョークポイントの両方が使用されます。 類似するロケーションが2つの方法で計算される場合、境界チョークポイント値がデフォルトで使用されます。
Chokepoint Out of Range timeout	シスコ互換のタグがチョークポイントの範囲外になる場合、入力したタイムアウト期間は、ロケーションの決定に RSSI 値が再度使用されるまでに経過した期間です。

フィールド	設定オプション
Absent Data cleanup interval	不在のモバイルステーションに関するデータを保持する分数を入力します。 不在のモバイル ステーションは、検出されたがネットワークに表示されないステーションです。デフォルト値は1440です。
Use 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可能にするには、このチェックボックスをオンにします。 このオプションは、デフォルトで無効です。
Movement Detection	
Individual RSSI change threshold	このパラメータには、個別 RSSI 移動再計算トリガーしきい値を指定します。 0 ～ 127 dBm の範囲内のしきい値を入力します 変更は、シスコ TAC 担当者の指示がある場合にだけ行ってください。
Aggregated RSSI change threshold	このパラメータには、集約 RSSI 移動再計算しきい値を指定します。 0 ～ 127 dBm の範囲内のしきい値を入力します 変更は、シスコ TAC 担当者の指示がある場合にだけ行ってください。
Many new RSSI change percentage threshold	このパラメータには、多数の新規 RSSI 移動再計算トリガーしきい値（パーセンテージ）を指定します。 変更は、シスコ TAC 担当者の指示がある場合にだけ行ってください。

ステップ 5　[Save] をクリックします。

通知の有効化および通知パラメータの設定

ここでは、次の内容について説明します。

• 通知統計情報の表示，（121 ページ）

通知の有効化

ユーザ設定の条件付き通知によって、Prime Infrastructure、または Mobility Services Engine の通知との互換性があるサードパーティの宛先に Mobility Services Engine が送信する通知が管理されます。

ノースバウンド通知により、モビリティ サービス エンジンがサードパーティ アプリケーションに送信するタグ通知が定義されます。クライアントの通知は転送されません。 Prime Infrastructure でノースバウンド通知を有効にすると、チョークポイント、テレメトリ、緊急、電池、ベンダー データの 5 つのイベント通知が送信されます。 タグのロケーションを送信するには、その通知を別に有効にする必要があります。

Mobility Services Engine は、決まった形式ですべてのノースバウンド通知を送信します。 詳細については、次の URL のシスコ開発者向けサポート ポータルを参照してください。http://developer.cisco.com/web/cdc

通知パラメータの設定

Mobility Services Engine が通知を生成し、通知の最大キュー サイズを設定し、特定の期間の通知の再試行制限を設定するレートを制限できます。

通知パラメータ設定は、通知パラメータの設定，（119 ページ） に記載されている場合を除き、ユーザが設定可能な条件付き通知およびノースバウンド通知に適用されます。

（注） 通知パラメータを変更するのは、Mobility Services Engine が大量の通知を送信する場合、または通知を受信しない場合だけにしてください。

ノースバウンド通知を有効にし、通知パラメータを設定するには、次の手順に従ってください。

ステップ 1 [Services] > [Mobility Services] の順に選択します。

ステップ 2 設定する Mobility Services Engine の名前をクリックします。

ステップ 3 [Context Aware Service] > [Advanced] > [Notification Parameters] の順に選択して設定オプションを表示します。

ステップ 4 [Enable Northbound Notifications] チェックボックスをオンにし、この機能を有効にします。

ステップ 5 通知をサードパーティアプリケーションに送信するため（ノースバウンド）、[Notification Contents] チェックボックスをオンにします。

ステップ 6 次の [Notification Contents] チェックボックスを 1 つ以上オンにします。

- **チョークポイント**
- **Telemetry**

- **Emergency**
- **Battery Level**
- **[Vendor Data]**
- **Location**

ステップ 7 [Notification Triggers] チェックボックスをオンにします。

ステップ 8 次の [Notification Triggers] チェックボックスを 1 つ以上オンにします。

- **チョークポイント**
- **Telemetry**
- **Emergency**
- **Battery Level**
- **[Vendor Data]**
- **[Location Recalculation]**

ステップ 9 ノースバウンド通知を受信するシステムの IP アドレスまたはホスト名およびポートを入力します。

ステップ 10 ドロップダウン リストからトランスポート タイプを選択します。

ステップ 11 宛先システムに安全にアクセスするために HTTPS プロトコルを使用する場合は、[HTTPS] チェックボックスをオンにします。

ステップ 12 通知パラメータ設定を変更するには、[Advanced] ページで該当するテキスト ボックスに新しい値を入力します。 次の表に、ユーザが設定可能な条件付き通知とノースバウンド通知のフィールドを示します。

表 *13*：ユーザが設定可能な条件付き通知とノースバウンド通知のフィールド

フィールド	設定オプション
Rate Limit	モビリティ サービス エンジンが通知を生成するレートをミリ秒単位で入力します。値 0（デフォルト）を指定すると、Mobility Services Engine は可能な限り迅速に通知を生成します（ノースバウンド通知のみ）。
Queue Limit	通知送信のイベント キュー制限を入力します。 モビリティ サービス エンジンは、この制限を超過するイベントをすべてドロップします。 デフォルト値：Cisco 3350（30000）、Cisco 3310（5,000）、および Cisco 2710（10,000）。
再試行数	リフレッシュ時間の終わりまでにイベント通知を生成する回数を入力します。 このパラメータは非同期トランスポート タイプの場合にだけ使用されます。非同期トランスポート タイプでは通知受信が確認されないため、通知が送信中に失われる可能性があります。 デフォルト値は 1 です。 （注） Mobility Services Engine データベースにイベントが保存されません。

フィールド	設定オプション
Refresh Time	通知を再送信するまで待機する必要がある時間を分単位で入力します。 たとえば、In Coverage Area 通知の対象としてデバイスが設定されており、このデバイスがカバレッジエリア内で頻繁に検出されるとします。 この通知は、リフレッシュ時間ごとに 1 回送信されます。 デフォルト値は 0 分です。
Drop Oldest Entry on Queue Overflow	（読み取り専用）。 起動時以降にキューからドロップされたイベント通知の数。
Serialize Events per Mac address per Destination	同じMACアドレスの連続するイベントを、連続して1つの宛先に送信するには、このオプションを選択します。

ステップ 13 [Save] をクリックします。

通知統計情報の表示

特定のモビリティ エンジンの通知統計情報を表示できます。 固有の Mobility Services Engine の通知の統計情報を表示するには、次の手順に従ってください。

ステップ 1 [Services] > [Mobility Services] の順に選択します。

ステップ 2 設定する Mobility Services Engine の名前をクリックします。

ステップ 3 [Context Aware Service] > [Advanced] > [Notification Parameters] の順に選択して設定オプションを表示します。

特定の Mobility Services Engine の通知統計情報を表示できます。 通知を表示するには、[Services] > [Mobility Services] > [MSE-name] > [Context Aware Service] > [Notification Statistics] を選択します。

MSE-name は、Mobility Services Engine の名前です。

次の表に、[Notification Statistics] ページのフィールドを示します。

表 *14*：*[Notification Statistics]*ページ

フィールド	説明
概要	
Destinations	
Total	Destinations の合計数。

フィールド	説明
概要	
Unreachable	到達不能宛先の数。
Notification Statistics Summary	
Track Definition Status	トラック定義のステータス。 トラック通知ステータスは [Enabled] または [Disabled] のいずれかです。
Track Definition	トラック定義は、[Northbound] または [CAS event notification] です。
Destination IP Address	通知送信先の宛先 IP アドレス。
宛先ポート	通知送信先の宛先ポート。
Destination Type	宛先のタイプ。 例：SOAP_XML。
Destination Status	宛先デバイスのステータス。 ステータスは [Up] または [Down] です。
Last Sent	最終通知が宛先デバイスに送信された日時。
Last Failed	通知に失敗した日時。
Total Count	宛先に送信された通知の合計数。 宛先デバイスの通知統計詳細情報を表示するには、カウント リンクをクリックします。

コントローラのロケーション テンプレート

ロケーション テンプレートでは、次の一般パラメータと詳細パラメータを設定できます。

- [General] パラメータ：RFID タグの収集の有効化、調整クライアントまたは通常の（非調整）クライアントのロケーション パス損失の設定、クライアント、タグ、および不正アクセス ポイントの測定通知の設定、クライアント、タグ、および不正アクセス ポイントの RSSI 有効期限タイムアウト値の設定を行います。
- [Advanced] パラメータ：RFID タグ データ タイムアウト値の設定、調整クライアントのマルチバンドのロケーション パス損失設定の有効化を行います。

ここでは、コントローラの新しいロケーションテンプレートの設定,（123ページ）について説明します。

コントローラの新しいロケーション テンプレートの設定

ステップ 1 [Configure] > [Controller Template Launch Pad] を選択します。

ステップ 2 新しいロケーションテンプレートを作成するには、[Location] 見出しの下にある [New (Location Configuration)] リンクを選択します。

ステップ 3 [New Controller Template] ページで、[General] タブにロケーション テンプレートの名前を入力します。

ステップ 4 [General] タブで、必要に応じてパラメータを変更します。 以下のに、[General]タブのフィールドを示します。

表 *15*：*[General]* タブのフィールド

パラメータ	設定オプション
RFID タグの計算	タグのデータを収集するには、[Enabled] チェックボックスをオンにします。
Calibrating Client	調整クライアントを使用するには、[Enabled] チェックボックスをオンにします。コントローラは、アクセスポイントから校正クライアントに通常の S36 または S60 要求を送信します（クライアント機能に異なります）。パケットは、すべてのチャネルで送信されます。 チャネルに関係なくすべてのアクセス ポイント（チャネル変更なし）が、RSSI データを各位置のクライアントから収集します。 これらの追加送信およびチャネル変更は、同時に発生する音声またはビデオ トラフィックの質が低下する場合があります。 使用可能なすべての無線（802.11a/b/g/n）を使用するには、[Advanced] タブでマルチバンドを有効にする必要があります。
Normal Client	非調整クライアントを使用するには、[Enabled]チェックボックスをオンにします。S36 または S60 要求はクライアントに送信されません。
Measurement Notification Interval	クライアント、タグ、および不正アクセス ポイントとクライアントの Network Mobility Services Protocol（NMSP） 測定通知間隔を設定するには、値を入力します。 この値は、テンプレートによって選択したコントローラに適用できます。 コントローラでこの値を設定すると、[Services] > [Synchronize Services] ページで表示できる同期外れ通知が生成されます。 コントローラと Mobility Services Engine に 2 個の異なる測定間隔がある場合、これら 2 つのうち最大の間隔設定が Mobility Services Engine によって採用されます。 このコントローラが Mobility Services Engine と同期されると、Mobility Services Engine で新しい値が設定されます。

パラメータ	設定オプション
RSSI Expiry Timeout for Clients	通常の（非調整）クライアントの RSSI タイムアウト値を設定するには、値を入力します。
RSSI Expiry Timeout for Calibrating Clients	調整クライアントの RSSI タイムアウト値を設定するには、値を入力します。
RSSI Expiry Timeout for Tags	タグの RSSI タイムアウト値を設定するには、値を入力します。
RSSI Expiry Timeout for Rogue APs	不正アクセスポイントの RSSI タイムアウト値を設定するには、値を入力します。

ステップ 5 [Advanced] タブで、必要に応じてパラメータを変更します。
次の表は、□Advanced□ タブの各フィールドについて説明します。

表 *16*：*[Advanced Location]* フィールド

フィールド	設定オプション
RFID Tag Data Timeout	RFID タグのデータ タイムアウト値を入力します。
Calibrating Client Multiband	すべてのチャネルで S36 および S60 パケット（該当する場合）を送信するには、[Enabled] チェックボックスをオンにします。 調整クライアントは、[General] タブで有効にする必要があります。

ステップ 6 [Save] をクリックします。

有線スイッチおよび有線クライアントでのロケーション サービス

有線スイッチを定義し、Mobility Services Engine と同期すると、有線スイッチに接続された有線クライアントの詳細が、NMSP 接続経由で Mobility Services Engine にダウンロードされます。 その後、Prime Infrastructure を使用して、有線スイッチおよび有線クライアントを表示できます。

都市および緊急ロケーション識別番号（ELIN）のインポートと表示は、次の URL に概要が示されている、RFC 4776 の仕様を満たしています。http://tools.ietf.org/html/rfc4776#section-3.4

ここでは、次の内容について説明します。

有線クライアントのロケーションサービスをサポートするための前提条件

- Catalyst スイッチを設定します。
- Prime Infrastructure に Catalyst スイッチを追加します。
- Catalyst スタッカブル スイッチとスイッチ ブレードは、Cisco IOS Release 12.2(52) SG 以降を実行している必要があります。
- Catalyst スイッチを Mobility Services Engine に割り当てて、同期化します。

注意事項と制約事項

- WS-C4948、WS-C4948-10GE、ME-4924-10GE、WS-4928-10GE、WS-C4900M、WS-X4515、WS-X4516、WS-X4013+、WS-X4013+TS、WS-X4516-10GE、WS-X4013+10GE、WS-X45-SUP6-E、および WS-X45-SUP6-LE
- スイッチは、1 つの Mobility Services Engine とだけ同期できます。 ただし、Mobility Services Engine には複数のスイッチを接続できます。

CLI を使用した Catalyst スイッチの設定

（注） すべてのコマンドは、コマンドラインインターフェイスの特権EXECモードで実行されます。

有線スイッチまたは有線クライアントのロケーション サービスを設定し、インターフェイスに適用するには、次の手順を実行します。

ステップ 1 スイッチのコマンドライン インターフェイスにログインします。

```
Switch > enable
```

```
Switch#
Switch# configure terminal
```

ステップ 2 NMSP を有効にします。

```
Switch(Config)# nmsp
Switch(config-nmsp)# enable
```

ステップ 3 SNMP コミュニティを設定します。

```
Switch(config)# snmp-server community wired-location
```

ステップ 4 スイッチでの IP デバイスのトラッキングを有効にします。

```
Switch(config)# ip device tracking
```

ステップ 5 （任意）スイッチの都市ロケーションを設定します。

（注） 特定のロケーションの都市および緊急ロケーション識別番号（ELIN）を定義できます。 この ID は、スイッチまたはスイッチ上の複数のポートに割り当てて、そのロケーションを表すことができます。 このロケーション ID は、6 などの単一の番号（1 ～ 4095）で表されます。 これによって、同じ場所にある複数のスイッチまたはポートを設定する際にタイマーが保存されます。

Enter configuration commands, one per line. Ctrl-Z を押して、終了します。

次に、都市ロケーションの設定例を示します。

```
Switch(config)# location civic-location identifier 6
Switch(config-civic)# name "switch-loc4"
Switch(config-civic)# seat "ws-3"
Switch(config-civic)# additional code "1e3f0034c092"
Switch(config-civic)# building "SJ-14"
Switch(config-civic)# floor "4"
Switch(config-civic)# street-group "Cisco Way"
Switch(config-civic)# number "3625"
Switch(config-civic)# type-of-place "Lab"
Switch(config-civic)# postal-community-name "Cisco Systems, Inc."
Switch(config-civic)# postal-code "95134"
Switch(config-civic)# city "San Jose"
Switch(config-civic)# state "CA"
Switch(config-civic)# country "US"
Switch(config-civic)# end
```

ステップ 6 スイッチの ELIN ロケーションを設定します。

（注） ELIN ロケーションの長さは、10 ～ 25 文字にする必要があります。 次の例では、4084084000 がその仕様を満たしています。 この数は、408-408-4000 として入力することもできます。 また、800-CISCO-WAY や 800CISCOWAY など、数字とテキストを組み合わせた値を入力することもできます。 ただし、ハイフンなしで数字またはテキストの間にスペースを入れる場合は、"800 CISCO WAY" のように引用符を使用する必要があります。

```
Switch(config)# location elin-location "4084084000" identifier 6
Switch(config)# end
```

ステップ 7 スイッチ上のポートのロケーションを設定します。

スイッチには、指定された数のスイッチポートがあり、クライアントおよびホストはこれらのポートで接続されます。 特定のスイッチ ポートのロケーションを設定した場合、そのポートに接続されているクライアントのロケーションは、そのポート ロケーションであると見なされます。

スイッチ（switch2）が別のスイッチ（switch1）のポート（port1 など）に接続されている場合は、port1 に設定されているロケーションが、switch2 に接続されているすべてクライアントに割り当てられます。

ポートを定義するための構文は、**interface** {**GigabitEthernet** | **FastEthernet**} ***slot***/***module***/***port*** です。

1 行に 1 つのロケーション定義だけを入力し、Ctrl-Z を押して行を終了します。

```
Switch(config)# interface GigabitEthernet 1/0/10
Switch(config-if)# location civic-location-id 6
Switch(config-if)# location elin-location-id 6
Switch(config-if)# end
```

ステップ 8 スイッチ自体にロケーションを割り当てます。
次のポート ロケーションが、スイッチの FastEthernet ネットワーク管理ポートで設定されます。

Enter configuration commands, one per line. Ctrl-Z を押して、終了します。

```
Switch(config)# interface FastEthernet 0
Switch(config-if)# location civic-location-id 6
Switch(config-if)# location elin-location-id 6
Switch(config-if)# end
```

Prime Infrastructure への Catalyst スイッチの追加

すべての Catalyst スイッチは、Prime Infrastructure に追加する前にロケーション サービスで設定する必要があります。 有線ロケーション サービスに対して設定された Catalyst スイッチを Prime Infrastructure に追加するには、次の手順に従ってください。

ステップ 1 [Configure] > [Ethernet Switches] を選択します。

ステップ 2 [Select a command] ドロップダウン リストから [Add Ethernet Switches] を選択します。 [Add Ethernet Switches] ページが表示されます。

ステップ 3 [Add Format Type] ドロップダウン リストから [Device Info] または [File] を選択します。

（注） 手動で 1 つ以上のスイッチ IP アドレスを入力するには、[Device Info] を選択します。 複数の Catalyst スイッチ IP アドレスが定義されたファイルをインポートするには、[File] を選択します。 ファイルを選択すると、インポートされたファイルの許容される形式を定義するダイアログボックスが表示されます。

ステップ 4 1 つ以上の IP アドレスを入力します。

ステップ 5 [Location Capable] チェックボックスをオンにします。

ステップ 6 ドロップダウン リストから、デフォルトと異なる場合は SNMP のバージョンを選択します。

ステップ 7 [Retries] テキスト ボックスと [Timeout] テキスト ボックスを変更する必要はありません。

ステップ 8 [Community] テキスト ボックスに SNMP コミュニティ ストリングとして **wired-location** を入力します。

ステップ 9 [Prime Infrastructure] をクリックします。 Prime Infrastructure への正常な追加を確認するページが表示されます。

ステップ 10 [Add Switches Result] ページで [OK] をクリックします。 新しく追加されたスイッチが [Ethernet Switches] ページに表示されます。

Mobility Services Engine への Catalyst スイッチの割り当ておよび同期

Prime Infrastructure に Catalyst スイッチを追加した後で、Mobility Services Engine に割り当てて、2 台のシステムを同期する必要があります。 これらを同期すると、コントローラと Mobility Services Engine 間の NMSP 接続が確立されます。 有線スイッチ、およびこれらのスイッチに接続されている有線クライアントに関するすべての情報が、Mobility Services Engine にダウンロードされます。

（注） スイッチは、1 つの Mobility Services Engine とだけ同期できます。 ただし、Mobility Services Engine には複数のスイッチを接続できます。

Mobility Services Engine に Catalyst スイッチを割り当てて同期するには、次の手順に従ってください。

ステップ 1 [Services] > [Synchronize Services] の順に選択します。

ステップ 2 Mobility Services Engine にスイッチを割り当てるには、[Wired Switches] タブをクリックします。

ステップ 3 Mobility Services Engine と同期する 1 つ以上のスイッチを選択します。

ステップ 4 [Change MSE Assignment] をクリックします。

ステップ 5 スイッチと同期化する Mobility Services Engine を選択します。

ステップ 6 [Synchronize] をクリックし、Mobility Services Engine データベースを更新します。
項目が同期されると、同期済みエントリの [Sync. Status] 列に緑色の 2 つの矢印のアイコンが表示されます。

ステップ 7 スイッチと Mobility Services Engine 間の NMSP 接続を確認するには、Mobility Services Engine への NMSP 接続の確認, （129 ページ）を参照してください。

Mobility Services Engine への NMSP 接続の確認

NMSP は、Mobility Services Engine とコントローラまたはロケーション対応 Catalyst スイッチ間の通信を管理します。 Mobility Services Engine とコントローラまたはロケーション対応 Catalyst スイッチ間のテレメトリ、緊急、およびチョークポイント情報の転送は、このプロトコルによって管理されます。

Mobility Services Engine とコントローラまたはロケーション対応 Catalyst スイッチ間の NMSP 接続を確認するには、次の手順に従ってください。

ステップ 1 [Services] > [Mobility Services Engines] の順に選択します。

ステップ 2 [Mobility Services] ページで、該当する Catalyst スイッチまたはコントローラのデバイス名リンクをクリックします。

ステップ 3 [System] > [Status] > [NMSP Connection Status] を選択します。

ステップ 4 [NMSP Status] が [ACTIVE] であることを確認します。
アクティブではない場合、Catalyst スイッチまたはコントローラと Mobility Services Engine を再同期します。

（注） Catalyst 有線スイッチで、**show nmsp status** コマンドを入力して NMSP 接続を確認します。

第 11 章

マップの使用

マップでは、キャンパス、ビルディング、屋外領域、およびフロア上にあるすべての管理対象システムの概要を表示できます。

この章の内容は、次のとおりです。

マップについて

次世代マップ機能は、デフォルトで有効になっています。

次世代マップ機能には、次のような利点があります。

- マップ上に大量の情報を表示します。 さまざまなクライアント、干渉、アクセス ポイントがある場合、Prime Infrastructure マップ ページでの表示を乱し、ページのロードに時間がかかる場合があります。 リリース 7.3 は情報のクラスタリングおよび階層化を導入しています。 情報のクラスタにより、高レベルでノイズを軽減し、オブジェクトをクリックすると、より多くの情報を表します。 詳細については、フロア領域のモニタリング，（163 ページ）を参照してください。

- AP をマップに追加するプロセスを効率化し、迅速化します。 従来のマップでは、マップへのアクセス ポイントの追加プロセスは手作業で手間がかかりました。 リリース 7.3 では、自動階層作成を使用して、アクセス ポイントを追加し命名できます。 詳細については、マップ作成のための自動階層の使用方法, （167 ページ）を参照してください。
- 容易なナビゲーションとズーム/パン コントロールによる高品質なマップ イメージを提供します。 従来のマップでは、マップ イメージの品質が低く、ナビゲーション、ズーム、パンが低速でした。 リリース 7.3 では、次世代のタイル対応マップ エンジンを使用して、マップを高速にロードしズーム/パンを容易に操作できます。 次世代マップでは、高解像度のマップをより高速にロードし、マップ内を容易に移動できます。 詳細については、次世代マップを使用したパンおよびズーム, （163 ページ）を参照してください。

ここでは、次の内容について説明します。

- フロア領域の追加, （133 ページ）
- Map Editor の使用, （171 ページ）

キャンパス マップへのビルディングの追加

Prime Infrastructure データベース内のキャンパス マップにビルディングを追加するには、次の手順を実行します。

ステップ 1 [Design] > [Site Maps] を選択して、[Maps] ページを表示します。

ステップ 2 目的のキャンパスをクリックします。 [Site Maps] > [Campus Name] ページが表示されます。

ステップ 3 [Select a command] ドロップダウン リストから、[New Building] を選択し、[Go] をクリックします。

ステップ 4 [Campus Name] > [New Building] ページで、関連するフロア図面マップを整理するために架空のビルディングを作成するには、次の手順を実行します。

1. ビルディング名を入力します。
2. ビルディング問い合わせ先の名前を入力します。
3. 地上のフロア数と地下のフロア数を入力します。
4. 水平位置（ビルディングの四角形の隅からキャンパス マップの左端までの距離）と垂直位置（ビルディングの四角形の隅からキャンパス マップの上端までの距離）をフィート単位で入力します。

   （注） 測定単位（フィートまたはメートル）を変更するには、[Design] > [Site Maps] を選択して、[Select a command] ドロップダウン リストから [Properties] を選択します。
5. ビルディングのおおまかな水平方向スパンと垂直方向スパン（マップ上の幅と奥行き）をフィート単位で入力します。

   （注） 水平方向スパンと垂直方向スパンは、後から追加するフロアのサイズと等しいかそれより大きくする必要があります。

ヒント　キャンパス マップの左上にある境界領域のサイズを変更するには、Ctrl キーを押した状態でクリックします。境界領域のサイズを変更すると、ビルディングの水平方向スパンおよび垂直方向スパンのパラメータも操作に応じて変わります。

6 [Place] をクリックして、ビルディングをキャンパス マップ上に配置します。 Prime Infrastructure では、キャンパス マップのサイズに合わせてサイズ変更されたビルディングの四角形が作成されます。

7 ビルディングの四角形をクリックして、キャンパス マップ上の目的の位置までドラッグします。

（注）　新しいビルディングを追加した後で、このビルディングをあるキャンパスから別のキャンパスに移動するときも、ビルディングを再作成する必要はありません。

8 [Save] をクリックして、このビルディングとキャンパス上の位置をデータベースに保存します。 Prime Infrastructure では、キャンパス マップ上の四角形の中にビルディング名が保存されます。

（注）　ビルディングには、該当する [Map] ページに移動するためのハイパーリンクが関連付けられます。

ステップ 5　（任意）新しい屋外領域に位置プレゼンス情報を割り当てる手順は、次のとおりです。

1 [Select a command] ドロップダウン リストから、[Edit Location Presence Info] を選択します。 [Go] をクリックします。 [Location Presence] ページが表示されます。

2 [Civic Address] タブ、または [Advanced] タブをクリックします。

- [Civic Address] では、名前、通り、住所番地、住居番地詳細、市（address line2）、州、郵便番号、そして国によってキャンパスを特定します。
- [Advanced] では、近隣、区、国、郵便のコミュニティ名など、Civic の拡張情報でキャンパスを特定します。

（注）　選択した各フィールドには、上記のすべてが含まれています。 たとえば、[Advanced] を選択した場合、クライアントからの要求により Civic 位置情報も提供できます。 選択した設定は、ロケーション サーバ レベルでの設定（[Services] > [Mobility Services]）と一致する必要があります。

3 デフォルトでは、[Override Child's Presence Information] チェックボックスはオンになっています。 独立したビルディングについては、この設定を変更する必要はありません。

ステップ 6　[Save] をクリックします。

フロア領域の追加

ここでは、Prime Infrastructure データベース内のキャンパスのビルディングまたは独立したビルディングにフロア図面を追加する方法を説明します。

ここでは、次の内容について説明します。

- キャンパスのビルディングへのフロア領域の追加, （134 ページ）

• 独立したビルディングへのフロア図面の追加, （136 ページ）

キャンパスのビルディングへのフロア領域の追加

（注） マップ ビューのサイズの拡大または縮小、およびマップ グリッド（マップ サイズをフィートまたはメートル単位で表示したもの）の表示または非表示を行うには、キャンパス イメージ上部にあるズーム コントロールを使用します。

キャンパスのビルディングにフロア領域を追加するには、次の手順を実行します。

ステップ 1 図面マップを .PNG、.JPG、.JPEG または .GIF 形式で保存します。

（注） マップは任意のサイズにできます。これは、Prime Infrastructure がワークスペースに適合するようマップを自動的にサイズ変更するためです。

（注） auto-cad ファイルの変換に問題がある場合は、エラー メッセージが表示されます。 Prime Infrastructure は、ネイティブのイメージ変換ライブラリを使用して、auto-cad ファイルを .png などのラスタ形式に変換します。 ネイティブ ライブラリをロードできなかった場合、Prime Infrastructure は「unable to convert the auto-cad file」メッセージを表示します。 このエラーが表示された場合は、ネイティブ ライブラリに必要な依存関係がすべて満たされていることを確認してください。 依存関係の問題を見つけるには、Linux プラットフォーム上で ldd を使用します。 Prime Infrastructure のインストール ディレクトリ（/webnms/rfdlls）に、次の DLL が存在する必要があります。LIBGFL254.DLL、MFC71.DLL、MSVCR71.DLL、MSVCP71.DLL。 依存関係の問題が発生した場合は、必要なライブラリをインストールし、Prime Infrastructure を再起動する必要があります。

（注） フロア マップ イメージが拡張され、ズームおよびパンニングできるようになります。 フロア イメージは、この操作が完了しないと全体は表示されません。マップ イメージを拡大縮小して全体を表示できます。 たとえば、サイズが約 60 MB である高解像度のイメージ（181 メガピクセル程度）がある場合は、マップに表示されるまでに 2 分かかる場合があります。

ステップ 2 **[Design]** > **[Site Maps]** を選択します。

ステップ 3 [Maps Tree View] または [Design] > [Site Maps] リストから、該当するキャンパスのビルディングを選択し、[Building View] ページを開きます。

ステップ 4 マウス カーソルを既存のビルディングの四角形の中にある名前に移動して、強調表示します。

（注） [Campus View] ページからビルディングにアクセスすることもできます。 [Campus View] ページで、ビルディング名をクリックし、[Building View] ページを開きます。

ステップ 5 [Select a command] ドロップダウン リストから、[New Floor Area] を選択します。

ステップ 6 [Go] をクリックします。 [New Floor Area] ページが表示されます。

ステップ 7 [New Floor Area] ページで、関連するフロア図面マップを整理するためにフロアをビルディングに追加するには、次の手順を実行します。

1. フロア領域と連絡先の名前を入力します。
2. [Floor] ドロップダウン リストから、フロアまたは地下の数を選択します。

3 フロアまたは地下のタイプ（RF Model）を選択します。

4 フロア間の高さをフィート単位で入力します。

（注） 測定単位（フィートまたはメートル）を変更するには、[Design] > [Site Maps] を選択して、[Select a command] ドロップダウン リストから [Properties] を選択します。

5 [Image or CAD File] チェックボックスをオンにします。

6 目的のフロアまたは地下のイメージまたは CAD ファイル名を参照および選択してから、[Open] をクリックします。

（注） CAD ファイルをインポートする場合は、[Convert CAD File] ドロップダウン リストを使用し、変換するイメージ ファイルを決定します。

ヒント auto-cad 変換に .JPEG（.JPG）形式を使用することは推奨しません。 JPEG が特別に必要でない限り、高品質な画像には .PNG 形式または .GIF 形式を使用します。

7 [Next] をクリックします。 CAF ファイルが指定されている場合、この時点でデフォルトのイメージ プレビューが生成されて読み込まれます。

（注） Prime Infrastructure は、ネイティブのイメージ変換ライブラリを使用して、auto-cad ファイルを .PNG などのラスタ形式に変換します。 ネイティブ ライブラリのロードに問題があるとき、Prime Infrastructure は次のエラーを表示します。「Unable to convert the auto-cad file. Reason: Error while loading the auto-cad image conversion library.」詳細については、Prime Infrastructure のオンライン ヘルプ、または Prime Infrastructure のマニュアルを参照してください。

CAD ファイル レイヤの名前が一覧表示されます。有効になっているレイヤには、イメージの右側にあるチェックボックスがオンになっています。

（注） フロアまたは地下のイメージ ファイル名を選択すると、Prime Infrastructure はビルディングのサイズに合わせたグリッド内にイメージを表示します。

（注） マップは任意のサイズにできます。これは、Prime Infrastructure がワークスペースに適合するようマップを自動的にサイズ変更するためです。

（注） マップは .PNG、.JPG、.JPEG、または .GIF 形式で保存する必要があります。

8 CAD ファイル レイヤがある場合、いくつでも選択または選択解除し、[Preview] をクリックして更新したイメージを表示できます。 選択したレイヤで次に進む準備ができたら、[Next] をクリックします。

フロア領域に関する残りのパラメータを入力します。

9 元のイメージの縦横比を維持するには、[Maintain Aspect Ratio] チェックボックスをオンのままにし、イメージの縦横比を変更するにはチェックボックスをオフにします。

10 フロアまたは地下のおおまかな水平方向スパンと垂直方向スパン（マップ上の幅と奥行き）をフィート単位で入力します。

（注） 水平方向スパンと垂直方向スパンは、Prime Infrastructure データベース内のビルディングの水平方向スパンおよび垂直方向スパン以下にする必要があります。

11 必要に応じて、水平位置（屋外領域の四角形の隅からキャンパス マップの左端までの距離）と垂直位置（屋外領域の四角形の隅からキャンパス マップの上端までの距離）をフィートまたはメートル単位で入力します。

ヒント ビルディングのサイズに合わせてグリッド内のイメージのサイズを変更するには、Ctrl キーを押した状態でクリックします。

12 必要に応じて [Launch Map Editor after floor creation] チェックボックスをオンにして、フロアの縮尺を変更し、壁を描画します。

13 [OK] をクリックして、このフロア図面をデータベースに保存します。 フロアは [Maps Tree View] と [Design] > [Site Maps] リストに追加されます。

（注） ビルディングごとに異なるフロア名を使用します。 キャンパス マップに複数のビルディングを追加する場合、別のビルディングに存在するフロア名を使用しないでください。 フロア名が重複すると、フロアとビルディング間のマッピング情報が不正確になります。

14 フロア図面または地下のマップを表示するには、フロアまたは地下のイメージをクリックします。

（注） マップを拡大または縮小してさまざまなサイズで表示したり、アクセス ポイントを追加したりできます。

独立したビルディングへのフロア図面の追加

独立したビルディングにフロア図面を追加するには、次の手順を実行します。

ステップ 1 フロア図面マップを .PNG、.JPG、または .GIF 形式で保存します。

（注） マップは任意のサイズにできます。これは、Prime Infrastructure がワークスペースに適合するようマップを自動的にサイズ変更するためです。

ステップ 2 ファイル システムの任意の場所にあるフロア図面マップを参照して、インポートします。 DXF または DWG 形式の CAD ファイル、またはステップ 1 で作成した形式のうちどの CAD ファイルでもインポートできます。

（注） auto-cad ファイルの変換に問題がある場合は、エラー メッセージが表示されます。 Prime Infrastructure は、ネイティブのイメージ変換ライブラリを使用して、auto-cad ファイルを .PNG などのラスタ形式に変換します。 ネイティブ ライブラリをロードできなかった場合、Prime Infrastructure は「unable to convert the auto-cad file」メッセージを表示します。 このエラーが表示された場合は、ネイティブ ライブラリに必要な依存関係がすべて満たされていることを確認してください。 依存関係の問題を見つけるには、Linux プラットフォーム上で ldd を使用します。 Prime Infrastructure のインストール ディレクトリ（/webnms/rfdlls）に、次の DLL が存在する必要があります。LIBGFL254.DLL、MFC71.DLL、MSVCR71.DLL、MSVCP71.DLL。 依存関係の問題が発生した場合は、必要なライブラリをインストールし、Prime Infrastructure を再起動する必要があります。

ステップ 3 [Design] > [Site Maps] を選択します。

ステップ 4 [Maps Tree View] または左側のサイドバー メニューの [Design] > [Site Maps] から、目的のビルディングを選択し、[Building View] ページを表示します。

ステップ 5 [Select a command] ドロップダウン リストから、[New Floor Area] を選択します。

ステップ 6 [Go] をクリックします。

ステップ 7 [New Floor Area] ページで、次の情報を追加します。

- フロア領域と連絡先の名前を入力します。
- [Floor] ドロップダウン リストから、フロアまたは地下の数を選択します。
- フロアまたは地下のタイプ（RF Model）を選択します。
- フロア間の高さをフィート単位で入力します。
- [Image or CAD File] チェックボックスをオンにします。
- 目的のフロアまたは地下のイメージまたは CAD ファイルを参照および選択してから、[Open] をクリックします。

（注） CAD ファイルをインポートする場合は、[Convert CAD File] ドロップダウン リストを使用し、変換するイメージ ファイルを決定します。

ヒント auto-cad 変換に .JPEG（.JPG）形式を使用することは推奨しません。 .JPEG が特別に必要でない限り、高品質な画像には .PNG 形式または .GIF 形式を使用します。

ステップ 8 [Next] をクリックします。 CAD ファイルが指定されている場合、この時点でデフォルトのイメージ プレビューが生成されて読み込まれます。

（注） Prime Infrastructure は、ネイティブのイメージ変換ライブラリを使用して、auto-cad ファイルを .PNG などのラスタ形式に変換します。 ネイティブ ライブラリのロードに問題があるとき、Prime Infrastructure は次のエラーを表示します。「Unable to convert the auto-cad file. Reason: Error while loading the auto-cad image conversion library. For more information, see the Prime Infrastructure online help or the Prime Infrastructure documentation.」

CAD ファイル レイヤの名前が一覧表示されます。有効になっているレイヤには、イメージの右側にあるチェックボックスがオンになっています。

（注） フロアまたは地下のイメージ ファイル名を選択すると、Prime Infrastructure はビルディングのサイズに合わせたグリッド内にイメージを表示します。

（注） マップは任意のサイズにできます。これは、Prime Infrastructure がワークスペースに適合するようマップを自動的にサイズ変更するためです。

（注） マップは .PNG、.JPG、.JPEG、または .GIF 形式で保存する必要があります。

CAD ファイル レイヤがある場合、いくつでも選択または選択解除し、[Preview] をクリックして更新したイメージを表示できます。 選択したレイヤで次に進む準備ができたら、[Next] をクリックします。

ステップ 9 フロア領域に関する残りのパラメータを入力します。

- 元のイメージの縦横比を維持するには、[Maintain Aspect Ratio] チェックボックスをオンのままにし、イメージの縦横比を変更するにはチェックボックスをオフにします。

- フロアまたは地下のおおまかな水平方向スパンと垂直方向スパン（マップ上の幅と奥行き）をフィート単位で入力します。

  （注） 水平方向スパンと垂直方向スパンは、Prime Infrastructure データベース内のビルディングの水平方向スパンおよび垂直方向スパン以下にする必要があります。

- 必要に応じて、水平位置（屋外領域の四角形の隅からキャンパス マップの左端までの距離）と垂直位置（屋外領域の四角形の隅からキャンパス マップの上端までの距離）をフィートまたはメートル単位で入力します。

  （注） ビルディングのサイズに合わせてグリッド内のイメージのサイズを変更するには、Ctrl キーを押した状態でクリックします。

- [Launch Map Editor] の隣のチェックボックスを選択することで、Prime Infrastructure の Map Editor でフロアの特性を調整します。 Map Editor 機能の詳細については、「Map Editor の使用」（10-17ページ）を参照してください。

ステップ 10 [OK] をクリックして、このフロア図面をデータベースに保存します。 フロアは [Maps Tree View] と [Design] > [Site Maps] リストに追加されます。

ステップ 11 フロア図面または地下のマップを表示するには、フロアまたは地下のイメージをクリックします。

（注） マップを拡大または縮小してさまざまなサイズで表示したり、アクセス ポイントを追加したりできます。

キャンパス マップの追加

単一のキャンパス マップを Prime Infrastructure データベースに追加するには、次の手順を実行します。

ステップ 1 マップを .PNG、.JPG、.JPEG、または .GIF 形式で保存します。

（注） マップは任意のサイズにできます。これは、Prime Infrastructure が作業領域に適合するようマップを自動的にサイズ変更するためです。

ステップ 2 ファイル システムの任意の場所にあるマップを参照して、インポートします。

ステップ 3 [Design] > [Site Maps] を選択して、[Maps] ページを表示します。

ステップ 4 [Select a command] ドロップダウン リストから [New Campus] を選択し、[Go] をクリックします。

ステップ 5 [Maps] > [New Campus] ページで、キャンパス名とキャンパスの連絡先の名前を入力します。

ステップ 6 キャンパス マップが含まれているイメージ ファイル名を参照および選択してから、[Open] をクリックします。

ステップ 7 [Maintain Aspect Ratio] チェックボックスをオンにして、Prime Infrastructure でマップのサイズが変更されたときに、縦横比が変わらないようにします。

ステップ 8 マップの水平方向スパンと垂直方向スパンをフィート単位で入力します。

（注） 測定単位（フィートまたはメートル）を変更するには、[Design] > [Site Maps] を選択して、[Select a command] ドロップダウン リストから [Properties] を選択します。 水平方向スパンと垂直方向スパンは、キャンパスに追加するビルディングやフロア図面よりも大きい値にする必要があります。

ステップ 9 [OK] をクリックして、このキャンパス マップを Prime Infrastructure データベースに追加します。 Prime Infrastructure に、データベース内のマップ、マップの種類、およびキャンパスのステータスの一覧を含む [Maps] ページが表示されます。

ステップ 10 （任意）位置プレゼンス情報を割り当てるには、[Design] > [Site Maps] ページで新たに作成したキャンパスのリンクをクリックします。

キャンパス マップへのビルディングの追加

NCS データベース内のキャンパス マップにビルディングを追加するには、次の手順を実行します。

ステップ 1 [Monitor] > [Site Maps] を選択して、[Maps] ページを表示します。

ステップ 2 目的のキャンパスをクリックします。 [Site Maps] > [Campus Name] ページが表示されます。

ステップ 3 [Select a command] ドロップダウン リストから、[New Building] を選択し、[Go] をクリックします。

ステップ 4 [Campus Name] > [New Building] ページで、関連するフロア図面マップを整理するために架空のビルディングを作成するには、次の手順を実行します。

a) ビルディング名を入力します。

b) ビルディング問い合わせ先の名前を入力します。

c) 地上のフロア数と地下のフロア数を入力します。

d) 水平位置（ビルディングの四角形の隅からキャンパス マップの左端までの距離）と垂直位置（ビルディングの四角形の隅からキャンパス マップの上端までの距離）をフィート単位で入力します。

（注） 測定単位（フィートまたはメートル）を変更するには、[Monitor] > [Site Maps] を選択して、[Select a command] ドロップダウン リストから [Properties] を選択します。

e) ビルディングのおおまかな水平方向スパンと垂直方向スパン（マップ上の幅と奥行き）をフィート単位で入力します。

（注） 水平方向スパンと垂直方向スパンは、後から追加するフロアのサイズと等しいかそれより大きくする必要があります。

ヒント Ctrl キーを押した状態でクリックすることで、キャンパス マップの左上隅にある境界領域のサイズを変更できます。 境界領域のサイズを変更すると、ビルディングの水平方向スパンおよび垂直方向スパンのパラメータも操作に応じて変わります。

f) [Place] をクリックして、ビルディングをキャンパス マップ上に配置します。 Cisco NCS では、キャンパス マップのサイズに合せてサイズ変更されたビルディングの四角形が作成されます。

g) ビルディングの四角形をクリックして、キャンパス マップ上の目的の位置までドラッグします。

（注） 新しいビルディングを追加した後で、このビルディングをあるキャンパスから別のキャンパスに移動するときも、ビルディングを再作成する必要はありません。

h) [Save] をクリックして、このビルディングとキャンパス上の位置をデータベースに保存します。 NCS では、キャンパス マップ上にあるビルディングの四角形の中にビルディング名が保存されます。

（注） ビルディングには、該当する [Map] ページに移動するためのハイパーリンクが関連付けられます。

ステップ 5 （任意）新しい屋外領域に位置プレゼンス情報を割り当てる手順は、次のとおりです。

a) [Select a command] ドロップダウン リストから、[Edit Location Presence Info] を選択します。 [Go] をクリックします。 [Location Presence] ページが表示されます。

（注） デフォルトでは、[Override Child Element] の [Presence Info] チェックボックスがオンになっています。キャンパスのロケーションをそのキャンパス上のすべてのビルディングおよびフロアに伝播する場合は、このオプションをオンのままにしておいてください。キャンパス マップにビルディングを追加する際は、キャンパスのロケーション情報をインポートできます。チェックボックスがオフの場合は、キャンパスの住所をビルディングにインポートできません。 ?1 つのキャンパスの住所をすべてのビルディングに割り当てるのではなく、ビルディング固有の住所をそのキャンパス上のビルディングに割り当てる場合は、このオプションをオフのままにしておいてください。

b) **[Civic Address]** タブ、**[GPS Markers]** タブ、または **[Advanced]** タブをクリックします。

- [Civic Address] では、名前、通り、住所番地、住居番地詳細、市（address line2）、州、郵便番号、そして国によってキャンパスを特定します。
- [GPS Markers] では、経度と緯度でキャンパスを特定します。
- [Advanced] では、近隣、区、国、郵便のコミュニティ名など、Civic の拡張情報でキャンパスを特定します。

（注） 選択した各フィールドには、上記のすべてが含まれています。 たとえば、[Advanced] を選択した場合、クライアントからの要求により GPS および Civic 位置情報も提供されます。 選択した設定は、ロケーション サーバ レベルでの設定（[Services] > [Mobility Services]）と一致する必要があります。

（注） クライアントが、キャンパスに対して GPS Markers フィールドで設定されていないビルディング、フロア、または屋外領域などのロケーション情報を要求した場合、エラーメッセージが返されます。

c) デフォルトでは、[Override Child's Presence Information] チェックボックスはオンになっています。 独立したビルディングについては、この設定を変更する必要はありません。

ステップ 6 [Save] をクリックします。

独立したビルディングの追加

Prime Infrastructure データベースに独立したビルディングを追加するには、次の手順を実行します。

ステップ 1 [Monitor] > [Site Maps] を選択して、[Maps] ページを表示します。

ステップ 2 [Select a command] ドロップダウン リストから、[New Building] を選択し、[Go] をクリックします。

ステップ 3 [Maps] > [New Building] ページで、関連するフロア図面マップを整理するために架空のビルディングを作成するには、次の手順を実行します。

a) ビルディング名を入力します。

b) ビルディング問い合わせ先の名前を入力します。

（注） 新しいビルディングを追加した後で、このビルディングをあるキャンパスから別のキャンパスに移動するときも、ビルディングを再作成する必要はありません。

c) 地上のフロア数と地下のフロア数を入力します。

d) ビルディングのおおまかな水平方向スパンと垂直方向スパン（マップ上の幅と奥行き）をフィート単位で入力します。

（注） 測定単位（フィートまたはメートル）を変更するには、[Monitor] > [Site Maps] を選択して、[Select a command] ドロップダウン リストから [Properties] を選択します。

（注） 水平方向スパンと垂直方向スパンは、後から追加するフロアのサイズと等しいかそれより大きくする必要があります。

e) [OK] をクリックして、このビルディングをデータベースに保存します。

ステップ 4 （任意）新しいビルディングに位置プレゼンス情報を割り当てる手順は、次のとおりです。

a) [Select a command] ドロップダウン リストから、[Location Presence] を選択します。 [Go] をクリックします。 [Location Presence] ページが表示されます。

b) [Civic] タブ、[GPS Markers] タブ、または [Advanced] タブをクリックします。

- [Civic Address] では、名前、通り、住所番地、住居番地詳細、市（address line2）、州、郵便番号、そして国によってキャンパスを特定します。
- [GPS Markers] では、経度と緯度でキャンパスを特定します。
- [Advanced] では、近隣、区、国、郵便のコミュニティ名など、Civic の拡張情報でキャンパスを特定します。

（注） 選択した各フィールドには、上記のすべてが含まれています。 たとえば、[Advanced] を選択した場合、ユーザからの要求により GPS および Civic 位置情報も提供されます。選択した設定は、ロケーション サーバ レベルでの設定（[Services] > [Mobility Services]）と一致する必要があります。

（注） クライアントが、キャンパスに対して GPS Markers フィールドで設定されていないビルディング、フロア、または屋外領域などのロケーション情報を要求した場合、エラーメッセージが返されます。

c) デフォルトでは、[Override Child Element] の [Presence Info] チェックボックスがオンになっています。キャンパスのロケーションをそのキャンパス上のすべてのビルディングおよびフロアに伝播する場合は、このオプションをオンのままにしておいてください。 キャンパス マップにビルディングを追加する際は、ロケーション情報をインポートできます。 チェックボックスがオフの場合は、キャンパスの住所をビルディングにインポートできません。 1 つのキャンパスの住所をすべてのビルディングに割り当てるのではなく、ビルディング固有の住所をそのキャンパス上のビルディングに割り当てる場合は、このオプションをオフのままにしておいてください。

ステップ 5 [Save] をクリックします。

（注） 独立したビルディングは、システム キャンパス内に自動的に配置されます。

フロア領域の追加

ここでは、Prime Infrastructure データベース内のキャンパスのビルディングまたは独立したビルディングにフロア図面を追加する方法を説明します。

ここでは、次の内容について説明します。

- キャンパスのビルディングへのフロア領域の追加, （134 ページ）
- 独立したビルディングへのフロア図面の追加, （136 ページ）

キャンパスのビルディングへのフロア領域の追加

（注） マップ ビューのサイズの拡大または縮小、およびマップ グリッド（マップ サイズをフィートまたはメートル単位で表示したもの）の表示または非表示を行うには、キャンパス イメージ上部にあるズーム コントロールを使用します。

キャンパスのビルディングにフロア領域を追加するには、次の手順を実行します。

ステップ 1 図面マップを .PNG、.JPG、.JPEG または .GIF 形式で保存します。

（注） マップは任意のサイズにできます。これは、Prime Infrastructure がワークスペースに適合するようマップを自動的にサイズ変更するためです。

（注） auto-cad ファイルの変換に問題がある場合は、エラー メッセージが表示されます。 Prime Infrastructure は、ネイティブのイメージ変換ライブラリを使用して、auto-cad ファイルを .png などのラスタ形式に変換します。 ネイティブ ライブラリをロードできなかった場合、Prime Infrastructure は「unable to convert the auto-cad file」メッセージを表示します。 このエラーが表示された場合は、ネイティブ ライブラリに必要な依存関係がすべて満たされていることを確認してください。 依存関係の問題を見つけるには、Linux プラットフォーム上で ldd を使用します。 Prime Infrastructure のインストール ディレクトリ（/webnms/rfdlls）に、次の DLL が存在する必要があります。LIBGFL254.DLL、MFC71.DLL、MSVCR71.DLL、MSVCP71.DLL。 依存関係の問題が発生した場合は、必要なライブラリをインストールし、Prime Infrastructure を再起動する必要があります。

（注） フロア マップ イメージが拡張され、ズームおよびパンニングできるようになります。 フロア イメージは、この操作が完了しないと全体は表示されません。 マップ イメージを拡大縮小して全体を表示できます。 たとえば、サイズが約 60 MB である高解像度のイメージ（181 メガピクセル程度）がある場合は、マップに表示されるまでに 2 分かかる場合があります。

ステップ 2 **[Design]** > **[Site Maps]** を選択します。

ステップ 3 [Maps Tree View] または [Design] > [Site Maps] リストから、該当するキャンパスのビルディングを選択し、[Building View] ページを開きます。

ステップ 4 マウス カーソルを既存のビルディングの四角形の中にある名前に移動して、強調表示します。

（注） [Campus View] ページからビルディングにアクセスすることもできます。 [Campus View] ページで、ビルディング名をクリックし、[Building View] ページを開きます。

ステップ 5 [Select a command] ドロップダウン リストから、[New Floor Area] を選択します。

ステップ 6 [Go] をクリックします。 [New Floor Area] ページが表示されます。

ステップ 7 [New Floor Area] ページで、関連するフロア図面マップを整理するためにフロアをビルディングに追加するには、次の手順を実行します。

1. フロア領域と連絡先の名前を入力します。
2. [Floor] ドロップダウン リストから、フロアまたは地下の数を選択します。
3. フロアまたは地下のタイプ（RF Model）を選択します。
4. フロア間の高さをフィート単位で入力します。

   （注） 測定単位（フィートまたはメートル）を変更するには、[Design] > [Site Maps] を選択して、[Select a command] ドロップダウン リストから [Properties] を選択します。
5. [Image or CAD File] チェックボックスをオンにします。
6. 目的のフロアまたは地下のイメージまたは CAD ファイル名を参照および選択してから、[Open] をクリックします。

   （注） CAD ファイルをインポートする場合は、[Convert CAD File] ドロップダウン リストを使用し、変換するイメージ ファイルを決定します。

   ヒント auto-cad 変換に .JPEG（.JPG）形式を使用することは推奨しません。 JPEG が特別に必要でない限り、高品質な画像には .PNG 形式または .GIF 形式を使用します。
7. [Next] をクリックします。 CAF ファイルが指定されている場合、この時点でデフォルトのイメージ プレビューが生成されて読み込まれます。

（注） Prime Infrastructure は、ネイティブのイメージ変換ライブラリを使用して、auto-cad ファイルを .PNG などのラスタ形式に変換します。 ネイティブ ライブラリのロードに問題があるとき、Prime Infrastructure は次のエラーを表示します。「Unable to convert the auto-cad file. Reason: Error while loading the auto-cad image conversion library.」詳細については、Prime Infrastructure のオンライン ヘルプ、または Prime Infrastructure のマニュアルを参照してください。

CAD ファイル レイヤの名前が一覧表示されます。有効になっているレイヤには、イメージの右側にあるチェックボックスがオンになっています。

（注） フロアまたは地下のイメージ ファイル名を選択すると、Prime Infrastructure はビルディングのサイズに合わせたグリッド内にイメージを表示します。

（注） マップは任意のサイズにできます。これは、Prime Infrastructure がワークスペースに適合するようマップを自動的にサイズ変更するためです。

（注） マップは .PNG、.JPG、.JPEG、または .GIF 形式で保存する必要があります。

8 CADファイル レイヤがある場合、いくつでも選択または選択解除し、[Preview]をクリックして更新したイメージを表示できます。 選択したレイヤで次に進む準備ができたら、[Next] をクリックします。

フロア領域に関する残りのパラメータを入力します。

9 元のイメージの縦横比を維持するには、[Maintain Aspect Ratio] チェックボックスをオンのままにし、イメージの縦横比を変更するにはチェックボックスをオフにします。

10 フロアまたは地下のおおまかな水平方向スパンと垂直方向スパン（マップ上の幅と奥行き）をフィート単位で入力します。

（注） 水平方向スパンと垂直方向スパンは、Prime Infrastructure データベース内のビルディングの水平方向スパンおよび垂直方向スパン以下にする必要があります。

11 必要に応じて、水平位置（屋外領域の四角形の隅からキャンパス マップの左端までの距離）と垂直位置（屋外領域の四角形の隅からキャンパス マップの上端までの距離）をフィートまたはメートル単位で入力します。

ヒント ビルディングのサイズに合わせてグリッド内のイメージのサイズを変更するには、Ctrl キーを押した状態でクリックします。

12 必要に応じて [Launch Map Editor after floor creation] チェックボックスをオンにして、フロアの縮尺を変更し、壁を描画します。

13 [OK] をクリックして、このフロア図面をデータベースに保存します。 フロアは [Maps Tree View] と [Design] > [Site Maps] リストに追加されます。

（注） ビルディングごとに異なるフロア名を使用します。 キャンパス マップに複数のビルディングを追加する場合、別のビルディングに存在するフロア名を使用しないでください。 フロア名が重複すると、フロアとビルディング間のマッピング情報が不正確になります。

14 フロア図面または地下のマップを表示するには、フロアまたは地下のイメージをクリックします。

（注） マップを拡大または縮小してさまざまなサイズで表示したり、アクセス ポイントを追加したりできます。

独立したビルディングへのフロア図面の追加

独立したビルディングにフロア図面を追加するには、次の手順を実行します。

ステップ 1 フロア図面マップを .PNG、.JPG、または .GIF 形式で保存します。

（注） マップは任意のサイズにできます。これは、Prime Infrastructure がワークスペースに適合するようマップを自動的にサイズ変更するためです。

ステップ 2 ファイル システムの任意の場所にあるフロア図面マップを参照して、インポートします。 DXF または DWG 形式の CAD ファイル、またはステップ 1 で作成した形式のうちどの CAD ファイルでもインポートできます。

（注） auto-cad ファイルの変換に問題がある場合は、エラー メッセージが表示されます。 Prime Infrastructure は、ネイティブのイメージ変換ライブラリを使用して、auto-cad ファイルを .PNG などのラスタ形式に変換します。 ネイティブ ライブラリをロードできなかった場合、Prime Infrastructure は「unable to convert the auto-cad file」メッセージを表示します。 このエラーが表示された場合は、ネイティブ ライブラリに必要な依存関係がすべて満たされていることを確認してください。 依存関係の問題を見つけるには、Linux プラットフォーム上で ldd を使用します。 Prime Infrastructure のインストール ディレクトリ（/webnms/rfdlls）に、次の DLL が存在する必要があります。LIBGFL254.DLL、MFC71.DLL、MSVCR71.DLL、MSVCP71.DLL。 依存関係の問題が発生した場合は、必要なライブラリをインストールし、Prime Infrastructure を再起動する必要があります。

ステップ 3 [Design] > [Site Maps] を選択します。

ステップ 4 [Maps Tree View] または左側のサイドバー メニューの [Design] > [Site Maps] から、目的のビルディングを選択し、[Building View] ページを表示します。

ステップ 5 [Select a command] ドロップダウン リストから、[New Floor Area] を選択します。

ステップ 6 [Go] をクリックします。

ステップ 7 [New Floor Area] ページで、次の情報を追加します。

- フロア領域と連絡先の名前を入力します。
- [Floor] ドロップダウン リストから、フロアまたは地下の数を選択します。
- フロアまたは地下のタイプ（RF Model）を選択します。
- フロア間の高さをフィート単位で入力します。
- [Image or CAD File] チェックボックスをオンにします。
- 目的のフロアまたは地下のイメージまたは CAD ファイルを参照および選択してから、[Open] をクリックします。

（注） CAD ファイルをインポートする場合は、[Convert CAD File] ドロップダウン リストを使用し、変換するイメージ ファイルを決定します。

ヒント auto-cad 変換に .JPEG（.JPG）形式を使用することは推奨しません。 .JPEG が特別に必要でない限り、高品質な画像には .PNG 形式または .GIF 形式を使用します。

ステップ 8 [Next] をクリックします。 CAD ファイルが指定されている場合、この時点でデフォルトのイメージ プレビューが生成されて読み込まれます。

（注） Prime Infrastructure は、ネイティブのイメージ変換ライブラリを使用して、auto-cad ファイルを .PNG などのラスタ形式に変換します。 ネイティブ ライブラリのロードに問題があるとき、Prime Infrastructure は次のエラーを表示します。「Unable to convert the auto-cad file. Reason: Error while loading the auto-cad image conversion library. For more information, see the Prime Infrastructure online help or the Prime Infrastructure documentation.」

CAD ファイル レイヤの名前が一覧表示されます。有効になっているレイヤには、イメージの右側にあるチェックボックスがオンになっています。

（注） フロアまたは地下のイメージ ファイル名を選択すると、Prime Infrastructure はビルディングのサイズに合わせたグリッド内にイメージを表示します。

（注） マップは任意のサイズにできます。これは、Prime Infrastructure がワークスペースに適合するようマップを自動的にサイズ変更するためです。

（注） マップは .PNG、.JPG、.JPEG、または .GIF 形式で保存する必要があります。

CAD ファイル レイヤがある場合、いくつでも選択または選択解除し、[Preview] をクリックして更新したイメージを表示できます。 選択したレイヤで次に進む準備ができたら、[Next] をクリックします。

ステップ 9 フロア領域に関する残りのパラメータを入力します。

- 元のイメージの縦横比を維持するには、[Maintain Aspect Ratio] チェックボックスをオンのままにし、イメージの縦横比を変更するにはチェックボックスをオフにします。
- フロアまたは地下のおおまかな水平方向スパンと垂直方向スパン（マップ上の幅と奥行き）をフィート単位で入力します。

  （注） 水平方向スパンと垂直方向スパンは、Prime Infrastructure データベース内のビルディングの水平方向スパンおよび垂直方向スパン以下にする必要があります。

- 必要に応じて、水平位置（屋外領域の四角形の隅からキャンパス マップの左端までの距離）と垂直位置（屋外領域の四角形の隅からキャンパス マップの上端までの距離）をフィートまたはメートル単位で入力します。

  （注） ビルディングのサイズに合わせてグリッド内のイメージのサイズを変更するには、Ctrl キーを押した状態でクリックします。

- [Launch Map Editor] の隣のチェックボックスを選択することで、Prime Infrastructure の Map Editor でフロアの特性を調整します。 Map Editor 機能の詳細については、「Map Editor の使用」（10-17ページ）を参照してください。

ステップ 10 [OK] をクリックして、このフロア図面をデータベースに保存します。 フロアは [Maps Tree View] と [Design] > [Site Maps] リストに追加されます。

ステップ 11 フロア図面または地下のマップを表示するには、フロアまたは地下のイメージをクリックします。

（注） マップを拡大または縮小してさまざまなサイズで表示したり、アクセス ポイントを追加したりできます。

フロア設定の構成

さまざまなフロア設定のチェックボックスをオンまたはオフにすることにより、フロア マップの外観を変更できます。 オンにしたフロア設定はマップ イメージに表示されます。

（注） Prime Infrastructure に、Mobility Services Engineがあるかどうかに応じて、フロア設定の一部が表示されないことがあります。 [Clients]、[802.11 Tags]、[Rogue APs]、[Adhoc Rogues]、[Rouge Clients]、および [Interferers] は、MSE が Prime Infrastructure に存在する場合のみ表示されます。

[Floor Settings] オプションには次の項目が含まれます。

- [Access Points]：詳細については、アクセス ポイントのフロア設定のフィルタリングを参照してください。
- [AP Heatmaps]：詳細については、アクセス ポイント ヒートマップのフロア設定のフィルタリングを参照してください。
- [AP Mesh Info]：詳細については、[AP Mesh Info] のフロア設定のフィルタリングを参照してください。
- [Clients]：詳細については、クライアントのフロア設定のフィルタリングを参照してください。
- [802.11 Tags]：詳細については、802.11 タグのフロア設定のフィルタリングを参照してください。
- [Rogue APs]：詳細については、不正 AP のフロア設定のフィルタリングを参照してください。
- [Rogue Adhocs]：詳細については、不正アドホックのフロア設定のフィルタリングを参照してください。
- [Rogue Clients]：詳細については、不正クライアントのフロア設定のフィルタリングを参照してください。
- Coverage Areas
- Location Regions
- Rails
- Markers
- チョークポイント
- Wi-Fi TDOA Receivers
- [Interferers]：詳細については、干渉設定のフィルタリングを参照してください。
- [wIPS Attackers]：詳細については、wIPS Attacker フロア設定のフィルタリング，（160 ページ）を参照してください。

青色の矢印を使用して、アクセス ポイント、アクセス ポイント ヒートマップ、クライアント、802.11 タグ、不正アクセス ポイント、不正アドホック、および不正クライアントに関するフロア設定フィルタにアクセスします。 フィルタリング オプションを選択したら、[OK] をクリックします。

最後のドロップダウン リスト内の [Show MSE data] を使用して、Mobility Services Engine のデータの期間を選択します。 過去 2 分間から最大 24 時間の範囲で、Mobility Services Engine のデータを表示できます。 このオプションは、Mobility Services Engine が Prime Infrastructure に存在する場合のみ表示されます。

[Save Settings] をクリックすると、現在のビューとフィルタ設定がすべてのマップに対する新しいデフォルトになります。

フロア上の包含リージョンと除外リージョンの定義

フロア上のロケーション計算の精度をさらに高めるために、計算に含める領域（包含領域）と計算に含めない領域（除外領域）を定義できます。

たとえば、ビルディング内のアトリウムや階段の吹き抜けなどの領域を除外して、作業領域（小個室、研究室、製造現場など）を含めることができます。

Cisco 1000 シリーズ Lightweight アクセス ポイントのアイコン

アイコンは、アクセスポイントの現在のステータスを示します。アイコンの円部分は水平方向に半分に分割できます。 2 つの Cisco Radio の色のうちより重大な方が、大きい三角形ポインタの色を決定します。

（注） アイコンが 802.11a/n と 802.11b/n を表している場合は、上半分が 802.11a/n ステータスを示し、下半分が 802.11b/g/n ステータスを示します。 アイコンが 802.11b/g/n のみを表している場合は、アイコン全体が 802.11b/g/n ステータスを示します。 三角形はより重大な色を示します。

次の表に、Prime Infrastructure ユーザインターフェイスのマップ表示で使用されるアイコンを示します。

表 *17*：アクセス ポイント アイコンの説明

アイコン	説明
	緑色のアイコンは、障害のないアクセス ポイント（AP）を示します。 円の上半分は、オプションの 802.11a Cisco Radio を表します。 円の下半分は、802.11b/g Cisco Radio のステートを示します。

アイコン	説明
	黄色のアイコンは、比較的重大でない障害があるアクセス ポイントを示します。円の上半分は、オプションの 802.11a Cisco Radio を表します。 円の下半分は、802.11b/g Cisco Radio のステートを示します。 （注） 黄色の点滅するアイコンは、802.11a または 802.11b/g の干渉、ノイズ、カバレッジ、または負荷プロファイル違反があることを示します。 黄色の点滅するアイコンは、802.11a および 802.11b/g のプロファイル違反があることを示します。
	赤色のアイコンは、やや重大な障害または重大な障害があるアクセス ポイント（AP）を示します。 円の上半分は、オプションの 802.11a Cisco Radio を表します。円の下半分は、802.11b/g Cisco Radio のステートを示します。
	中央に疑問符が付いている灰色のアイコンは、到達不能なアクセス ポイントを表します。 ステータスが判断できないため、灰色になっています。
	中央に疑問符が付いていない灰色のアイコンは、アソシエートされていないアクセス ポイントを表します。
	円の中央に赤い「x」が付いているアイコンは、管理目的で無効にされているアクセス ポイントを表します。
	上半分が緑色で下半分が黄色のアイコンは、障害のないオプションの 802.11a Cisco Radio（上）と、比較的重大でない障害がある 802.11b/g Cisco Radio（下）を示します。 2 つの Cisco Radio の色のうちより重大な方が、大きい三角形ポインタの色を決定します。
	上半分が緑色で下半分が赤色のアイコンは、障害がなく正常に動作しているオプションの 802.11a Cisco Radio（上）と、やや重大な障害または重大な障害がある 802.11b/g Cisco Radio（下）を示します。 2 つの Cisco Radio の色のうちより重大な方が、大きい三角形ポインタの色を決定します。
	上半分が黄色で下半分が赤色のアイコンは、比較的重大でない障害がある、オプションの 802.11a Cisco Radio（上）と、やや重大な障害または重大な障害がある 802.11b/g Cisco Radio（下）を示します。 2 つの Cisco Radio の色のうちより重大な方が、大きい三角形ポインタの色を決定します。

アイコン	説明
	上半分が黄色で下半分が緑色のアイコンは、比較的重大でない障害がある、オプションの 802.11a Cisco Radio（上）と、障害がなく正常に動作している 802.11b/g Cisco Radio（下）を示します。 2 つの Cisco Radio の色のうちより重大な方が、大きい三角形ポインタの色を決定します。
	上半分が赤色で下半分が緑色のアイコンは、やや重大な障害または重大な障害がある、オプションの 802.11a Cisco Radio（上）と、障害がなく正常に動作している 802.11b/g Cisco Radio（下）を示します。 2 つの Cisco Radio の色のうちより重大な方が、大きい三角形ポインタの色を決定します。
	上半分が赤色で下半分が黄色のアイコンは、やや重大な障害または重大な障害がある、オプションの 802.11a Cisco Radio（上）と、比較的重大でない障害がある 802.11b/g Cisco Radio（下）を示します。 2 つの Cisco Radio の色のうちより重大な方が、大きい三角形ポインタの色を決定します。
     	上半分（オプションの 802.11a）に赤い「x」が付いているアイコンは、示されている Cisco Radio が管理目的で無効にされていることを表します。 記載されている 6 つのカラー コーディングが存在します。

各アクセス ポイント アイコンには、内部の Side A アンテナの方向を示す、小さい黒矢印があります。

下の表に、Prime Infrastructureユーザインターフェイスのマップ画面で使用される矢印の例を示します。

表 *18*：矢印

矢印の例	方向
	0 度、またはマップ上の右方向。
	45 度、またはマップ上の右下方向。
	90 度、またはマップ上の下方向。
これらは、矢印の角度を 45 度ずつ増加させた例の最初の 3 つ分を示しています。45 度ずつ増加させた例はあと 5 つあります。	

アクセス ポイントのフロア設定のフィルタリング

アクセス ポイントのフロア設定を有効にし、[Floor Settings] の右側の青い矢印をクリックすると、フィルタリング オプションを含む [Access Point Filter] ダイアログボックスが表示されます。

アクセス ポイントのフィルタリング オプションには、次の項目が含まれます。

- [Show]：このオプション ボタンを選択すると、無線ステータスまたはアクセス ポイントのステータスが表示されます。

（注） アクセス ポイント アイコンの色はアクセス ポイントのステータスに基づいており、選択されているステータスによってアイコンの色は異なります。 フロア マップのデフォルトは無線ステータスです。

- [Protocol]：ドロップダウン リストから、表示する無線タイプを選択します（802.11a/n、802.11b/g/n、または両方）。

（注） 表示されるヒートマップは、選択した無線タイプに対応します。

- [Display]：ドロップダウン リストから、マップ イメージ上に表示されるアクセス ポイントの識別情報を選択します。
  - [Channels]：Cisco Radio のチャネル番号を表示するか、「Unavailable」（アクセス ポイントが接続されていない場合）を表示します。

（注） 使用可能なチャネルは、国コードの設定によって定義され、各国で規制されています。 詳細については、次の URL を参照してください。?http://www.cisco.com/en/US/prod/collateral/wireless/ps5679/ps5861/product_data_sheet0900aecd80537b6a_ps430_Products_Data_Sheet.html

  - [TX Power Level]：現在の Cisco Radio の送信電力レベル（1 が高い）または「Unavailable」（アクセス ポイントが接続されていない場合）を表示します。

（注） 電力レベルはアクセス ポイントのタイプによって異なります。 1000 シリーズのアクセス ポイントでは 1 ～ 5 の値、1230 アクセス ポイントでは 1 ～ 7 の値、1240 および 1100 シリーズのアクセス ポイントでは 1 ～ 8 の値をとります。

次の表には、送信電力レベルの数値と対応する電力設定を示します。

表 *19*：送信電力レベル値

送信電力?レベルの数値	電力設定
1	国コード設定で許可される最大の電力
2	50% の電力
3	25% の電力
4	12.5 ～ 6.25 % の電力
5	6.25 ～ 0.195% の電力

（注） 電力レベルは、国コードの設定によって定義され、各国で規制されています。 詳細については、次の URL を参照してください。?http://www.cisco.com/en/US/prod/collateral/wireless/ps5679/ps5861/product_data_sheet0900aecd80537b6a_ps430_Products_Data_Sheet.html

- [Channel and Tx Power]：チャネルと送信電力レベルの両方（またはアクセス ポイントが接続されていない場合は「Unavailable」）を表示します。
- [Coverage Holes]：接続が切断されるまでに信号が弱くなったクライアントの割合を表示します。接続されていないアクセス ポイントに対しては「Unavailable」を表示し、監視専用モードのアクセス ポイントに対しては「MonitorOnly」を表示します。

（注） カバレッジ ホールとは、クライアントがワイヤレス ネットワークから信号を受信できない領域のことです。 無線ネットワークを展開する場合、初期ネットワーク展開のコストとカバレッジ ホール領域の割合を考慮する必要があります。 展開するにあたってのカバレッジ ホールの妥当な条件とは、2 ～ 10% です。 これは、100 か所のランダムに選択したテスト ロケーションのうち、2 ～ 10 か所でサービスが制限される可能性があることを意味します。 展開後、Cisco Unified Wireless Network Solution の Radio Resource Management（RRM; 無線リソース管理）によってこれらのカバレッジ ホール領域が特定され、IT マネージャに報告されます。IT マネージャはユーザからの要求に基づいてカバレッジ ホールに対応します。

- [MAC Addresses]：アクセス ポイントがコントローラにアソシエートされているかどうかに関係なく、アクセス ポイントの MAC アドレスを表示します。
- [Names]：アクセス ポイント名を表示します。 これはデフォルト値です。
- [Controller IP]：アクセス ポイントがアソシエートされているコントローラの IP アドレスを表示します。アソシエーションを解除されたアクセス ポイントでは、「Not Associated」を表示します。
- [Utilization]：アソシエートされたクライアント デバイスで使用されている帯域幅の割合（受信、送信、およびチャネル使用率を含む）を表示します。アソシエーションを解除されたアクセス ポイントでは [Unavailable]、monitor-only モードのアクセス ポイントでは [MonitorOnly] が表示されます。
- [Profiles]：対応するオペレータ定義の閾値の負荷、ノイズ、干渉、およびカバレッジ コンポーネントを表示します。 超えていないしきい値には「Okay」、超えているしきい値には「Issue」、接続されていないアクセス ポイントには「Unavailable」を表示します。

（注） [Profile Type] ドロップダウン リストを使用して、[Load]、[Noise]、[Interference]、または [Coverage] を選択します。

- [CleanAir Status]：アクセス ポイントの CleanAir ステータスと、アクセス ポイントで CleanAir が有効かどうかを表示します。
- [Average Air Quality]：このアクセス ポイントの平均電波品質を表示します。 詳細には、帯域と平均電波品質が含まれます。

- [Minimum Air Quality]：このアクセス ポイントの最小電波品質を表示します。 詳細には、帯域と最小電波品質が含まれます。
- [Average and Minimum Air Quality]：このアクセス ポイントの平均電波品質と最小電波品質を表示します。 詳細には、帯域、平均電波品質、および最小電波品質が含まれます。
- [Associated Clients]：アソシエートされているクライアントの数を表示します。接続されていないアクセス ポイントに対しては「Unavailable」を表示し、monitor-only モードのアクセス ポイントに対しては「MonitorOnly」を表示します。

（注）

- Bridge Group Names
- [RSSI Cutoff]：ドロップダウン リストから、RSSI Cutoff レベルを選択します。 RSSI Cutoff の範囲は -60 dBm ～ -90 dBm です。
- [Show Detected Interferers]：チェックボックスをオンにすると、アクセス ポイントで検出されるすべての干渉を表示します。
- Max. [Interferers/label]：ドロップダウン リストから、ラベルごとに表示される干渉の最大数を選択します。

該当するすべてのフィルタリング基準を選択したら、[OK] をクリックします。

アクセス ポイント ヒートマップのフロア設定のフィルタリング

RF ヒートマップは、変数から取得した値をマップに色として表した、RF ワイヤレス データのグラフィック表示です。 現在のヒートマップは、RSSI 予測モデル、アンテナの方向、および AP 送信電力に基づいて計算されます。

[Access Point Heatmap] フロア設定を有効にし、[Floor Settings] の右側の青い矢印をクリックすると、ヒートマップのフィルタリング オプションを含む [Contributing APs] ダイアログが表示されます。 詳細については、RF ヒートマップの計算についてを参照してください。

Prime Infrastructure ではダイナミック ヒートマップが導入されました。 ダイナミック ヒートマップを有効にすると、Prime Infrastructure は変更された RSSI 値を表すためにヒートマップを再計算します。 ダイナミック ヒートマップを設定する手順の詳細については、マップ プロパティの編集を参照してください。

アクセス ポイント ヒートマップのフィルタリング オプションには、次の項目が含まれます。

- [Heatmap Type]：[Coverage] または [Air Quality] を選択します。 [Air Quality] を選択した場合は、アクセス ポイントのヒート マップ タイプを平均電波品質または最小電波品質でさらにフィルタリングできます。 該当するオプション ボタンを選択します。

（注） フロア計画にモニタ モード アクセス ポイントがある場合、IDS ヒートマップ タイプまたはカバレッジ ヒートマップ タイプのいずれかを選択できます。 カバレッジ ヒートマップでは、モニタ モード アクセス ポイントは除外されます。

（注） カバレッジ ヒートマップおよび電波品質ヒートマップには、ローカル モード、FlexConnect モード、またはブリッジ モードの AP のみが関係します。

- [Total APs]：マップに配置されているアクセス ポイントの数を表示します。
- アクセス ポイントのチェックボックスをオンにして、イメージ マップ上に表示するヒートマップを決定します。

該当するすべてのフィルタリング基準を選択したら、[OK] をクリックします。

[AP Mesh Info] のフロア設定のフィルタリング

（注） [AP Mesh Info] チェックボックスは、ブリッジ アクセス ポイントがフロアに追加されているときのみ表示されます。

このチェックボックスをオンにすると、Prime Infrastructure はコントローラとの通信を開始し、ブリッジ アクセス ポイントの情報を表示します。 次の情報が表示されます。

- 子アクセス ポイントと親アクセス ポイントとの間のリンク。
- 子アクセス ポイントから親アクセス ポイントへの方向を示す矢印。
- 信号対雑音比（SNR）を示す、色分けされたリンク。 緑色のリンクは高い SNR（25 dB 超）を表し、オレンジ色のリンクは許容範囲内の SNR（20 ～ 25 dB）を表し、赤色のリンクは非常に低い SNR（20 dB 未満）を表します。

[AP Mesh Info] フロア設定を有効にし、[Floor Settings] の右側の青い矢印をクリックすると、メッシュのフィルタリング オプションを含む [Mesh Parent-Child Hierarchical View] ページが表示されます。

マップ上に表示するアクセス ポイントを選択することにより、マップ ビューを更新できます。 [Quick Selections] ドロップダウン リストから、ルート アクセス ポイントのみを選択するか、1 番めのホップから 4 番めのホップの間のさまざまなホップを選択するか、またはすべてのアクセス ポイントを選択します。

（注） 子アクセス ポイントを表示するには、その親が選択されている必要があります。

該当するすべてのフィルタリング基準を選択したら、[OK] をクリックします。

クライアントのフロア設定のフィルタリング

（注） [Clients] オプションは、モビリティ サーバが Prime Infrastructure に追加されている場合のみ表示されます。

[Clients] フロア設定を有効にし、右側の青い矢印をクリックすると、[Client Filter] ダイアログボックスが表示されます。

クライアントのフィルタリング オプションには、次の項目が含まれます。

- [Show All Clients]：チェックボックスをオンにすると、マップ上のすべてのクライアントが表示されます。
- [Small Icons]：チェックボックスをオンにすると、マップ上の各クライアントのアイコンが表示されます。

（注） [Show All Clients] チェックボックスと [Small Icons] チェックボックスをオンにすると、その他のすべてのドロップダウン リスト オプションが灰色になります。 ??[Small Icons] チェックボックスをオフにすると、ラベルにMAC アドレス、 IP アドレス、ユーザ名、アセット名、アセット グループまたはアセット カテゴリを表示するかどうかを選択できます。??[Show All Clients] チェックボックスをオフにすると、クライアントをフィルタリングする方法を指定し、特定の SSID を入力できます。

- [Display]：マップ上に表示するクライアントの識別子（IP アドレス、ユーザ名、MAC アドレス、アセット名、アセット グループ、またはアセット カテゴリ）を選択します。
- [Filter By]：クライアントをフィルタリングするパラメータを選択します（IP アドレス、ユーザ名、MAC アドレス、アセット名、アセット グループ、アセット カテゴリ、またはコントローラ）。 選択したら、特定のデバイスをテキスト ボックスに入力します。
- [SSID]：入力可能なテキスト ボックスにクライアントの SSID を入力します。
- [Protocol]：ドロップダウン リストから [All]、[802.11a/n]、または [802.11b/g/n] を選択します。
  - [All]：領域内のすべてのアクセス ポイントを表示します。
  - [802.11a/n]：802.11a/n 無線通信機を使用するクライアントに対するカバレッジパターンを示す色付きのオーバーレイを表示します。 色は、赤（-35dBm）～濃い青（-85dBm）までの受信信号強度を表します。

- [802.11b/g/n]：802.11b/g/n 無線通信機を使用するクライアントに対するカバレッジ パターンを示す色付きのオーバーレイを表示します。 色は、赤（-35dBm）～濃い青（-85dBm）までの受信信号強度を表します。 これはデフォルト値です。

- [State]：ドロップダウン リストから [All]、[Idle]、[Authenticated]、[Probing]、または [Associated] を選択します。

該当するすべてのフィルタリング基準を選択したら、[OK] をクリックします。

802.11 タグのフロア設定のフィルタリング

[802.11 Tags] フロア設定を有効にし、右側の青い矢印をクリックすると、[Tag Filter] ダイアログが表示されます。

タグのフィルタリング オプションには、次の項目が含まれます。

- [Show All Tags]：チェックボックスをオンにすると、マップ上のすべてのタグが表示されます。
- [Small Icons]：チェックボックスをオンにすると、マップ上の各タグのアイコンが表示されます。

（注） [Show All Tags] チェックボックスと [Small Icons] チェックボックスをオンにすると、その他のすべてのドロップダウン リスト オプションが灰色になります。 [Small Icons] チェックボックスをオフにすると、ラベルに MAC アドレス、アセット名、アセット グループまたはアセット カテゴリを表示するかどうか選択できます。 [Show All Tags] チェックボックスをオフにすると、タグをフィルタリングする方法を指定できます。

- [Display]：マップ上に表示するタグの識別子（MACアドレス、アセット名、アセット グループ、またはアセット カテゴリ）を選択します。
- [Filter By]：クライアントをフィルタリングするパラメータを選択します（MAC アドレス、アセット名、アセットグループ、アセットカテゴリ、またはコントローラ）。 選択したら、特定のデバイスをテキスト ボックスに入力します。

該当するすべてのフィルタリング基準を選択したら、[OK] をクリックします。

不正 AP のフロア設定のフィルタリング

[Rogue APs] フロア設定を有効にし、右側の青い矢印をクリックすると、[Rogue AP filter] ダイアログボックスが表示されます。

不正 AP のフィルタリング オプションには、次の項目が含まれます。

- [Show All Rogue APs]：チェックボックスをオンにすると、マップ上のすべての不正アクセス ポイントが表示されます。

- [Small Icons]：チェックボックスをオンにすると、マップ上の各不正アクセス ポイントのアイコンが表示されます。

（注） [Show All Rogue APs] チェックボックスと [Small Icons] チェックボックスをオンにすると、その他のすべてのドロップダウン リスト オプションが灰色になります。 [Show All Rogue APs] チェックボックスをオフにすると、不正アクセス ポイントをフィルタリングする方法を指定できます。

- [Show Rogue AP Zone of Impact]：不正アクセスによる影響のゾーンを表示する場合に、このチェックボックスをオンにします。 不正アクセスによる影響ゾーンは、不正アクセス ポイントの送信電力と不正アクセス ポイントに関連するクライアント数によって決まります。
  - 不正 AP に関連するクライアント数によって、マップ上でゾーンの色の濃さが決まります。
  - 影響ゾーンの半径は、次の不正 AP の送信電力に基づいて決まります。

表 *20*：送信電力

帯域	送信電力	Tx Power 前提
2.5 GHz	20 dBm	18 dBm
5 GHz	17 dBm	15 dBm

- [MAC Address]：特定のMACアドレスを表示する場合は、そのMACアドレスを [MAC Address] テキスト ボックスに入力します。
- [State]：ドロップダウン リストを使用して、[Alert]、[Known]、[Acknowledged]、[Contained]、[Threat]、または [Unknown] から封じ込めステートを選択します。
- [On Network]：ドロップダウン リストを使用して、ネットワーク上の不正アクセス ポイントを表示するかどうか指定します。

該当するすべてのフィルタリング基準を選択したら、[OK] をクリックします。

不正アドホックのフロア設定のフィルタリング

[Rogue Adhocs] フロア設定を有効にし、右側の青い矢印をクリックすると、[Rogue Adhoc filter] ダイアログが表示されます。

不正アドホックのフィルタリング オプションには、次の項目が含まれます。

- [Show All Rogue Adhocs]：チェックボックスをオンにすると、マップ上のすべての不正アドホックが表示されます。

- [Small Icons]：チェックボックスをオンにすると、マップ上の各不正アドホックのアイコンが表示されます。

（注） [Show All Rogue Adhocs] チェックボックスと [Small Icons] チェックボックスをオンにすると、その他のすべてのドロップダウン リスト オプションが灰色になります。 [Show All Rogue Adhocs] チェックボックスをオフにすると、不正アドホックをフィルタリングする方法を指定できます。

- [MAC Address]：特定の MAC アドレスを表示する場合は、その MAC アドレスを [MAC Address] テキスト ボックスに入力します。
- [State]：ドロップダウン リストを使用して、[Alert]、[Known]、[Acknowledged]、[Contained]、[Threat]、または [Unknown] から封じ込めステートを選択します。
- [On Network]：ドロップダウン リストを使用して、ネットワーク上の不正アドホックを表示するかどうか指定します。

該当するすべてのフィルタリング基準を選択したら、[OK] をクリックします。

不正クライアントのフロア設定のフィルタリング

[Rogue Clients] フロア設定を有効にし、右側の青い矢印をクリックすると、[Rogue Clients filter] ダイアログが表示されます。

不正クライアントのフィルタリング オプションには、次の項目が含まれます。

- [Show All Rogue Clients]：チェックボックスをオンにすると、マップ上のすべての不正クライアントが表示されます。
- [Small Icons]：チェックボックスをオンにすると、マップ上の各不正クライアントのアイコンが表示されます。

（注） [Show All Rogue Clients] チェックボックスと [Small Icons] チェックボックスをオンにすると、その他のすべてのドロップダウン リスト オプションが灰色になります。 [Show All Rogue Clients] チェックボックスをオフにすると、不正クライアントをフィルタリングする方法を指定できます。

- [Assoc. Rogue AP MAC Address]：特定の MAC アドレスを表示する場合は、その MAC アドレスを [MAC Address] テキスト ボックスに入力します。
- [State]：ドロップダウン リストを使用して、[Alert]、[Contained]、[Threat]、または [Unknown] から封じ込めステートを選択します。

該当するすべてのフィルタリング基準を選択したら、[OK] をクリックします。

干渉設定のフィルタリング

[Interferer] フロア設定を有効にし、右側の青い矢印をクリックすると、[Interferers filter] ダイアログボックスが表示されます。

干渉のフィルタリング オプションには、次の項目が含まれます。

- [Show active interferers only]：チェックボックスをオンにすると、すべてのアクティブな干渉が表示されます。
- [Small Icons]：チェックボックスをオンにすると、マップ上の各干渉のアイコンが表示されます。
- [Show Zone of Impact]：おおまかな干渉の影響領域を表示します。 円の不透明度はその重大度を示します。 赤一色の円は Wi-Fi 通信を妨害する可能性がある非常に強い干渉を表し、薄いピンク色の円は弱い干渉を表します。
- 該当するすべてのフィルタリング基準を選択したら、[OK] をクリックします。

wIPS Attacker フロア設定のフィルタリング

[wIPS Attacker] フロア設定を有効にし、右側の青い矢印をクリックすると、[wIPS Attack Filter] ダイアログボックスが表示されます。

（図をここに追加します）

wIPS Attack フィルタリングのオプションには次が含まれます。

- [Show All wIPS Attacks]：チェックボックスをオンにすると、マップ上のすべての wIPS 攻撃が表示されます。
- [Small Icons]：チェックボックスをオンにすると、マップ上の各 wIPS 攻撃のアイコンが表示されます。

（注） [Show All wIPS Attacks] チェックボックスと [Small Icons] チェックボックスをオンにすると、その他のすべてのドロップダウン リスト オプションが灰色になります。 [Small Icons] チェックボックスをオフにすると、ラベルに MAC アドレス、アラーム カテゴリ、アラーム名を表示するかどうかを選択できます。 [Show All wIPS Attacks] チェックボックスをオフにすると、wIPS 攻撃をフィルタリングする方法を指定できます。

- [Filter By]：wIPS 攻撃のフィルタリングの基準にするパラメータを選択します。
  - [MAC Address]：特定の MAC アドレスを表示する場合は、その MAC アドレスを [MAC Address] テキスト ボックスに入力します。

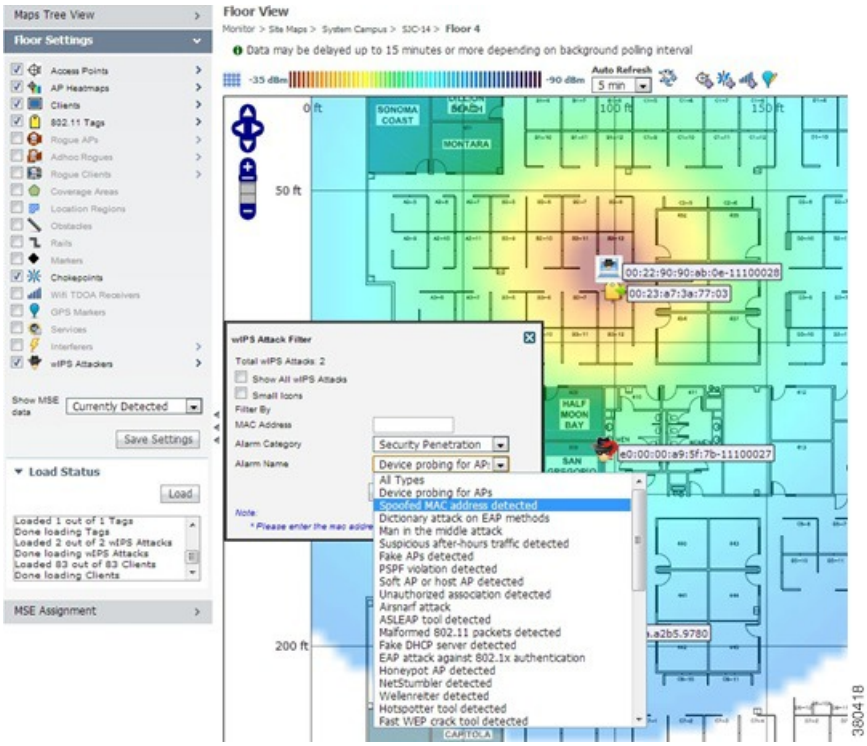
- [Alarm Category]：[Alarm Category] ドロップダウン リストからアラームのカテゴリを選択します。 選択可能なカテゴリには、[All Types]、[Security Penetration]、[DoS] があります。

（注） アラーム名は、選択したアラーム カテゴリに基づいて入力されます。

- [Alarm Name]：[Alarm Name] ドロップダウン リストからアラーム名を選択します。

該当するすべてのフィルタリング基準を選択したら、[OK] をクリックします。

図 *5*：*wIPS* 攻撃名のフィルタリング



マップに表示される各デバイスを区別するために、次のアイコンが使用されます。

図 *6*：アイコン

マップおよび AP ロケーション データのインポート

Autonomous から Lightweight アクセス ポイントに、および WLSE から Prime Infrastructure に変換する場合、変換手順の 1 つとして、アクセス ポイント関連情報を手動で Prime Infrastructure に再入力する方法があります。 この処理を高速化するために、WLSE からアクセス ポイントに関する情報をエクスポートして、Prime Infrastructure にインポートすることができます。

（注） Prime Infrastructure は、.tar ファイルを想定しているため、ファイルをインポートする前に .tar 拡張子かどうかをチェックします。 インポートしようとしているファイルが .tar ファイルでない場合は、Prime Infrastructure にエラー メッセージが表示され、別のファイルをインポートするためのプロンプトが表示されます。

（注） WLSE データ エクスポート機能（WLSE バージョン 2.15）の詳細については、次の URL を参照してください。 http://<WLSE_IP_ADDRESS>:1741/debug/export/exportSite.jsp

Prime Infrastructure Web インターフェイスを使用して、プロパティをマップし、WLSE データを含む tar ファイルをインポートするには、次の手順を実行します。

ステップ 1 [Monitor] > [Site Maps] を選択します。

ステップ 2 [Select a command] ドロップダウン リストから、[Import Maps] を選択し、[Go] をクリックします。

ステップ 3 [WLSE Map and AP Location Data] オプションを選択して、[Next] をクリックします。

ステップ 4 [Import WLSE Map and AP Location Data] ページで、[Browse] をクリックしてインポートするファイルを選択します。

ステップ 5 インポートする .tar ファイルを見つけて選択し、[Open] をクリックします。
Prime Infrastructure では、[Import From] テキスト ボックスにファイルの名前が表示されます。

ステップ 6 [Import] をクリックします。
CS によってファイルがアップロードされ、ファイルが処理されている間は一時的にファイルはローカル ディレクトリに保存されます。 処理できないデータがファイルに含まれている場合、Prime Infrastructure は問題を修正して再試行するようユーザに促します。 ファイルのロードが完了すると、Prime Infrastructure に追加された内容を示すレポートが Prime Infrastructure に表示されます。 レポートには、追加できない内容とその理由も記載されます。

インポートするデータの一部がすでに存在している場合、Prime Infrastructure では、キャンパスの場合は既存のデータを使用し、ビルディングとフロアの場合はインポートされたデータで既存のデータを上書きします。

（注） WLSE サイトとビルディングの組み合わせ、および Prime Infrastructure キャンパス（または最上位レベルのビルディング）とビルディングの組み合わせの間に重複する名前がある場合、Prime Infrastructure の実行前インポート レポートに、既存のビルディングを削除することを示すメッセージが表示されます。

ステップ 7 [Import] をクリックして、WLSE データをインポートします。
Prime Infrastructure に、インポートされた内容を示すレポートが表示されます。

ステップ 8 インポートされたデータを表示するには、[Monitor] > [Site Maps] を選択します。

フロア領域のモニタリング

フロア領域は、ビルディングの各フロアの領域で、外壁の外面に対して測定されます。 この領域には、ロビー、地下室、エレベータ シャフトが含まれ、集合住宅ビルディングではすべての共有面積が含まれます。

ここでは、次の内容について説明します。

- 次世代マップを使用したパンおよびズーム, （163 ページ）
- アクセス ポイントのフロア領域への追加, （164 ページ）
- アクセス ポイントの配置, （166 ページ）

次世代マップを使用したパンおよびズーム

計画

マップを移動するには、左マウス ボタンをクリックしたまま、新しい場所にマッピングをドラッグします。 また、パン矢印を使用して、マップを東西南北に移動することもできます。 これはマップの左上隅にあります。

（注） キーボードの矢印キーを使用してパン操作を実行することもできます。

ズームインとズームアウト：スケールの変更

ズーム レベルは画像の解像度によって異なります。 高解像度のイメージの場合、ズーム レベルが高くなります。 さまざまなスケールでマップの表示状態を変えるたびにズーム レベルが変わり、表示が詳細になったり、広範になったりします。 マップの中にはスケールを小さくしても大きくしても、同じ状態のマップもあります。

マップをさらに詳細に表示するには、ズームインする必要があります。 マップの左側のズーム バーを使用してこれを行うことができます。 ズーム バーの上部にある [+] 記号をクリックします。 ある場所を中心にズームインするには、その場所をダブルクリックします。マップを広い範囲で表示するには、ズームアウトする必要があります。 これを行うには、ズームバーの下部にある [-] 記号をクリックします。

（注） マウスまたはキーボードを使用してズーム操作を実行できます。 キーボードでは、[+] または [-] の記号をクリックし、ズームインまたはズームアウトします。 マウスの場合は、マウスのスクロール ホイールを使用してズームインまたはズームアウトします。あるいは、ダブルクリックしてズームインします。

アクセス ポイントのフロア領域への追加

.PNG、.JPG、.JPEG、または .GIF 形式のフロア図面と屋外領域のマップを Prime Infrastructure データベースに追加した後に、Lightweight アクセス ポイント アイコンをマップ上に配置して、ビルディング内の設定位置を示すことができます。 アクセス ポイントをフロア領域と屋外領域に追加するには、次の手順を実行します。

ステップ 1 [Design] > [Site Maps] を選択します。

ステップ 2 [Maps Tree View] または左側のサイドバー メニューの [Design] > [Site Maps] から、該当するフロアを選択し、[Floor View] ページを開きます。

ステップ 3 [Select a Command] ドロップダウン リストから、[Add Access Points] を選択し、[GO] をクリックします。

ステップ 4 [Add Access Points] ページで、フロア領域に追加するアクセス ポイントのチェックボックスをオンにします。

（注） アクセス ポイントを検索する場合は、AP 名または MAC アドレス（イーサネット/無線）/IP を [Search AP] の [Name/MacAddress (Ethernet/Radio)/IP] テキスト ボックスに入力して、[Search] をクリックします。 検索では大文字と小文字は区別されません。

（注） フロアおよび屋外領域にまだ割り当てられていないアクセス ポイントのみがリストに表示されます。

（注） リストの上部にあるチェックボックスをオンにして、すべてのアクセス ポイントを選択します。

ステップ 5 該当するすべてのアクセス ポイントが選択されたら、アクセス ポイント リストの下部にある [OK] をクリックします。 [Position Access Points] ページが表示されます。
フロア マップに追加するために選択した各アクセス ポイントは、灰色の円で表され（アクセス ポイント名や MAC アドレスにより区別）、フロア マップの左上部分に並べられます。

ステップ 6 各アクセス ポイントをクリックし、適切な位置にドラッグします。 アクセス ポイントは選択されると青色に変わります。

（注） マップ上にアクセス ポイントをドラッグすると、[Horizontal] テキスト ボックスと [Vertical] テキスト ボックスにアクセス ポイントの水平位置と垂直位置が表示されます。

（注） 各アクセス ポイントの横の小さい黒矢印は各アクセス ポイントの Side A を表し、各アクセス ポイントの矢印は、アクセス ポイントが設置された方向と一致する必要があります。 Side A はそれぞれの 1000 シリーズ アクセス ポイント上で明確に記されており、802.11a/n 無線とは関係ありません。 方向の矢印を調整するには、[Antenna Angle] ドロップダウン リストから適切な方向を選択します。

アクセス ポイントを選択すると、そのアクセス ポイントの詳細がページの左側に表示されます。 アクセス ポイントの詳細には、次の情報が含まれます。

- [AP Model]：選択したアクセス ポイントのモデル タイプを示します。
- [Protocol]：ドロップダウン リストから、このアクセス ポイントのプロトコルを選択します。
- [Antenna]：ドロップダウン リストから、このアクセス ポイントの適切なアンテナ タイプを選択します。
- [Antenna/AP Image]：[Antenna] ドロップダウン リストから選択したアンテナがアンテナ イメージに反映されます。 アンテナイメージの右上の矢印をクリックすると、画像のサイズが拡大します。
- [Antenna Orientation]：アンテナ タイプに応じて、[Azimuth] と [Elevation] の方向を度数で入力します。

（注） [Omnidirectional] アンテナのパターンでは方位角が存在しなくなるため、[Azimuth] オプションは表示されません。

（注） 内部アンテナでは、同じ垂直方向の角度が両方の無線に適用されます。

アンテナの角度は、マップの X 軸に対して相対的です。 X（水平）座標および Y（垂直）座標の原点はマップの左上の角であるため、0 度はアクセス ポイントの Side A を右に、90 度は Side A を下に、180 度は Side A を左に向けることになります。

アンテナの Elevation（垂直面）は、最大 90 度までアンテナを垂直（上下）に移動するために使用されます。

（注） 各アクセス ポイントがマップ上の正しい位置に設置されていること、またアンテナの方向が正しいことを確認します。マップを使って、カバレッジ ホールや不正アクセス ポイントを発見するときは、正確なアクセス ポイントの位置決めが重要です。

アンテナの垂直方向の角度および方位角のパターンの詳細については、次の URL を参照してください。
http://www.cisco.com/en/US/products/hw/wireless/ps469/tsd_products_support_series_home.html

ステップ 7 各アクセス ポイントの配置と調整が完了したら、[Save] をクリックします。

（注） [Save] をクリックすると、アクセス ポイントのアンテナ ゲインが選択したアンテナに一致します。 これにより、無線がリセットされる可能性があります。

Prime Infrastructure によって、カバレッジ領域の RF 予測が計算されます。 この RF 予測は、カバレッジ領域マップ上の RF 信号の相対強度を示しているため、一般的には「ヒート マップ」として知られています。

（注）　（注）

ここでは、石壁や金属の物体など、ビルディングのさまざまな素材の減衰は考慮されておらず、RF 信号が障害物に跳ね返る影響も表示されないため、実際の RF 信号強度の近似値だけが表示されています。

（注）　マップへのアクセス ポイント配置の詳細については、「アクセス ポイントの配置」（10-14 ページ）を参照してください。

（注）　ファイルをインポートまたはエクスポートすることにより、アクセス ポイントの位置を変更できます。 詳細については、「Wi-Fi TDOA レシーバの配置」（10-30 ページ）を参照してください。

アクセス ポイントの配置

無線 LAN のカバレッジ領域での全デバイスの最適な位置を判断するには、アクセス ポイントの密度と位置を考慮する必要があります。

少なくとも 3 個、可能な場合は 4 個か 5 個のアクセス ポイントが、デバイス位置を必要とする各領域にカバレッジを提供していることを確認します。 デバイスを検出するアクセスポイントは多いほど効果が増します。 この高水準のガイドラインが生み出す最良の実施例は次のとおりです。優先度順に並べられています。

1. 最も重要なのは、アクセス ポイントが目的の位置を囲むことです。
2. アクセス ポイントは約 17 ～ 20m（50 ～ 70 リニア フィート）間隔で配置される必要があります。 これは、230 ～ 450 平方メートル（2,500 ～ 5,000 平方フィート）ごとに 1 つのアクセス ポイントということです。

（注）　アクセス ポイントは、約 6m（20 フィート）未満の高さで設置する必要があります。 性能を最大限に引き出すためには、約 3m（10 フィート）での設置が理想的です。

これらのガイドラインに従うと、アクセス ポイントが追跡したデバイスをより検出しやすくなります。 2 つの物理環境が同じ RF 特性を持つことはほとんどありません。 ユーザは特定の環境や要件に合わせてこれらのパラメータを変更しなければならない場合があります。

（注）　コントローラが情報を Location Appliance に転送するために、-75dBm を超える信号でデバイスを検出する必要があります。 3 つ以上のアクセス ポイントが、-75dBm 以下の信号でデバイスを検出できなければなりません。

（注） 全方向性アンテナを内蔵した天井マウント型APがある場合は、Prime Infrastructureでアンテナの方向を必ずしも設定する必要はありません。ただし、同じAPを壁にマウントする場合は、アンテナの方向を90度に設定する必要があります。 アクセス ポイントの方向については、アクセス ポイントの配置, （166 ページ）を参照してください。

表 *21*：アクセス ポイントのアンテナ方向

アクセス ポイント	アンテナの方向
1140（天井に取り付けた場合）	Cisco ロゴは床面に向けてください。 垂直方向：0 度。
1240（天井に取り付けた場合）	アンテナはアクセス ポイントと垂直にする必要があります。 垂直方向：0 度。
1240（壁面に取り付けた場合）	アンテナはアクセス ポイントと平行にする必要があります。 垂直方向：0 度。 アンテナが AP と垂直な場合、角度は 90 度になります（ダイポール アンテナは全方向性のため、方向の上下は関係ありません）。

マップ作成のための自動階層の使用方法

自動階層作成はすばやくマップを作成し、Prime Infrastructureのマップにアクセス ポイントを割り当てる方法です。 ワイヤレス LAN コントローラを Prime Infrastructure に追加し、アクセス ポイントに名前を付けたら、自動階層作成を使用してマップを作成できます。 また、ネットワークにアクセス ポイントを追加した後、自動階層作成を使用して、Prime Infrastructureのマップにアクセス ポイントを割り当てることができます。

（注） 自動階層作成機能を使用するには、マップのキャンパス、ビルディング、フロア、または屋外領域名を指定する、ワイヤレス アクセス ポイントに対して確立された命名パターンを必要とします。 たとえば、San Jose-01-GroundFloor-AP3500i1 などです。

自動階層を使用してマップを作成するには、次の手順に従います。

ステップ 1 [Design] > [Automatic Hierarchy Creation] を選択して、[Automatic Hierarchy Creation] ページを表示します。

ステップ 2 テキスト ボックスに、システムのアクセス ポイントの名前を入力します。 または、リストから名前を 1 つ選択できます。
この名前は、マップを作成する正規表現を作成するために使用されます。

（注） 以前に作成した正規表現を更新するには、式の横の [Load and Continue] をクリックし、式を適宜更新します。

正規表現を削除するには、式の横にある [Delete] をクリックします。

ステップ 3 [Next] をクリックします。

ステップ 4 アクセス ポイントの名前にデリミタがある場合は、それをテキスト ボックスに入力し、[Generate] をクリックします。 システムではデリミタに基づいてアクセス ポイントの名前と一致する正規表現が作成されます。
たとえば、ダッシュ（-）のデリミタをアクセス ポイント名、San Jose-01-GroundFloor-AP3500i1 で使用すると、正規表現 /(.*)-(.*)-(.*)-(.*)/ が作成されます。

より複雑なアクセス ポイント名がある場合は、手動で正規表現を入力できます。

（注） 先頭と末尾のスラッシュを入力する必要はありません。

ステップ 5 [Test] をクリックします。 システムは、アクセス ポイント名に対して作成されたマップと、入力された正規表現を表示します。

ステップ 6 [Group] フィールドを使用して、階層型に一致するグループを割り当てます。
たとえば、アクセス ポイントに SJC14-4-AP-BREAK-ROOM の名前が付けられた場合

この例では、キャンパス名が SJC、ビルディング名が 14、フロア名が 4、AP 名が AP-BREAK-ROOM です。

正規表現 /([A-Z]+)(\d+)-(\d+)-(.*)/ を使用します。

AP 名から、次のグループが抽出されます。

1 SJC

2 14

3 4

4 AP-BREAK-ROOM

一致するグループは、1 から始めて、左から右へ割り当てられます。 一致するグループを階層要素と一致させるには、各グループ番号のドロップダウン リストを使用して、適切な階層要素を選択します。

これにより、アクセス ポイント名内の位置は、ほとんどどのような順番でも可能になります。

たとえば、アクセス ポイントに EastLab-Atrium2-3-SanFrancisco の名前が付けられた場合

正規表現 /(.*)-(.*)-(.*)-(.*)/ を次のグループと使用する場合：

1 ビルディング

2 デバイス名（Device Name）

3 Floor

4 Campus

自動階層作成では、SanFrancisco というキャンパス、EastLab というビルディング、EastLab の 3 というフロアを作成します。

（注） デバイス名がない、またはデバイスが影響を与えない 2 つの階層タイプでは、他の目的で一致するグループを使用する必要がある場合は、グループを省略できます。

自動階層作成は、アクセス ポイントを配置するマップを計算するためにマップする次のグループが必要です。

表 *22*：グループ

キャンパス グループは一致しているか?	ビルディング グループは一致しているか?	フロア グループは一致しているか?	結果の位置
Yes	Yes	Yes	キャンパス > ビルディング > フロア
Yes	Yes	No	不一致
Yes	No	Yes	キャンパス > フロア（フロアが屋外領域の場合）
Yes	No	No	不一致
No	Yes	Yes	システム キャンパス > ビルディング > フロア
no	yes	no	不一致
no	yes	no	不一致
no	no	yes	不一致
no	no	no	不一致

自動階層作成では、フロア名からフロア インデックスを推測しようとします。 フロア名が数値の場合、AHC はフロアを正数のフロア インデックスに割り当てます。 フロア名が負の数値または文字 B で始まる場合（b1、-4、または B2 など）、AHC はフロアを負数のフロア インデックスに割り当てます。 これは、フロアが地下であることを示します。

アクセス ポイントを配置する既存のマップを検索する場合、AHC は、アクセス ポイントの名前と同じフロア インデックスを持つアクセス ポイントのビルディング内のフロアを考慮します。

たとえば、SF > MarketStreet > Sublevel1 というマップがあり、フロア インデックスが -1 の場合、そのフロアにはアクセス ポイント SF-MarketStreet-b1-MON1 が割り当てられます。

ステップ 7 [Next] をクリックします。 アクセス ポイントの対象を増やしてテストできます。 [Add more device names to test against] フィールドにアクセス ポイントを入力して [Add] をクリックすると、より多くのアクセス ポイントに対する正規表現と一致グループのマッピングをテストできます。
次に、[Test] ボタンをクリックして、テーブル内の各アクセス ポイント名をテストします。 各テストの結果がテーブルに表示されます。

必要に応じて、現在の正規表現の正規表現またはグループ マッピングを編集するには、前のステップに戻ります。

ステップ 8 [Next] をクリックしてから、[Save and Apply] をクリックします。 これでシステムに正規表現が適用されます。 システムはマップに割り当てられていないすべてのアクセス ポイントを処理します。

（注） フロア イメージ、正しい寸法などを含めるようにマップを編集できます。 自動階層作成でマップを作成する場合は、20 フィート X 20 フィートのデフォルト寸法が使用されます。 正しい寸法などの属性を指定するには、作成されたマップを編集する必要があります。 自動階層作成を使用して作成されるマップは、不完全なアイコンがマップ リストに表示されます。 マップの編集を完了すると、不完全なアイコンが消えます。 [Edit View] リンクをクリックして、不完全なマップの列を非表示にできます。

Map Editor の使用

Map Editor を使って、フロア図面情報を定義、描画、および拡張します。 また、Map Editor では、アクセスポイントに対する RF 予測ヒートマップを計算するときに反映できるように、障害物を作成できます。 その特定の領域にあるクライアントとタグを特定する、Location Appliances のカバレッジ領域を追加することもできます。

ここでは、次の内容について説明します。

Map Editor の使用に関するガイドライン

Map Editor を使用してビルディングまたはフロア マップを変更する際には、次の内容を考慮してください。

（注） 以前の Floor Plan Editor から .FPE ファイルをインポートするのではなく、Map Editor を使用して壁やその他の障害物を描画することを推奨します。 必要に応じて .FPE ファイルを引き続きインポートできます。 そのためには、目的のフロア領域に移動します。[Select a command] ドロップダウン リストから、[**Edit Floor Area**] を選択し、[**Go**] をクリックします。[**FPE File**] チェックボックスをオンにしてから、.FPE ファイルを参照して選択します。

- Map Editor でフロア図面に追加できる壁の数に制限はありません。ただし、クライアント ワークステーションの処理能力およびメモリによって、Prime Infrastructure でのリフレッシュやレンダリングが制限されることがあります。

  （注） RAM が 1 GB 以下のコンピュータでは、実用的な制限として、フロアごとの壁数を 400 個までにすることを推奨します。

- すべての壁は、Prime Infrastructure が RF カバレッジ ヒートマップを生成する際に使用されます。

フロア上の包含領域と除外領域に関するガイドライン

包含領域と除外領域は、最低 3 点を持つ多角形で表すことができます。

フロア上の包含リージョンを 1 つだけ定義できます。 デフォルトでは、各フロアの包含リージョンは、そのリージョンが Prime Infrastructure に追加されるときに定義されます。 包含リージョンは水色の実線で示され、通常はリージョンの輪郭を描きます。

フロア上の除外リージョンを複数定義できます。

新たに定義された包含リージョンと除外リージョンは、Mobility Services Engine によってロケーションがフロアで再計算された後にヒートマップ上に表示されます。

Map Editor の表示

Map Editor を開くには、次の手順に従います。

ステップ 1 [Design] > [Site Map Design] の順に選択します。

ステップ 2 目的のキャンパスをクリックします。 [Site Maps] > [Campus Name] ページが表示されます。

ステップ 3 キャンパスをクリックし、次にビルディングをクリックします。

ステップ 4 目的のフロア領域をクリックします。 [Site Maps] > [Campus Name] > [Building Name] > [Floor Area Name] ページが表示されます。

ステップ 5 [Select a command] ドロップダウン リストから、[Map Editor] を選択し、[Go] をクリックします。 [Map Editor] ページが表示されます。

Map Editor を使用したカバレッジ領域の描画

長方形以外のビルディングがある場合、またはフロア内に長方形以外の領域をマークする場合には、Map Editor を使用してカバレッジ領域を描画できます。

Map Editor を使用してカバレッジ領域を描画するには、次の手順に従います。

ステップ 1 フロア図面が Prime Infrastructure にまだ表示されていない場合は、フロア図面を追加します。

ステップ 2 [Monitor] > [Site Maps] を選択します。

ステップ 3 編集する屋外領域、キャンパス、ビルディングまたはフロアに対応する [Map Name] をクリックします。

ステップ 4 [Select a command] ドロップダウン リストから、[Map Editor] を選択し、[Go] をクリックします。

ステップ 5 [Map Editor] ページで、ツールバーの [Draw Coverage Area] アイコンをクリックします。
ポップアップ メニューが表示されます。

ステップ 6 定義する領域の名前を入力します。 [OK] をクリックします。
描画ツールが表示されます。

ステップ 7 輪郭を描く領域に描画ツールを移動します。

- 左マウス ボタンをクリックして、線の描画を開始および終了します。
- 領域の輪郭を完全に描いたら、左マウス ボタンをダブルクリックすると、ページ内で領域が強調表示されます。

  マップ上で輪郭を描いた領域を強調表示するには、閉じたオブジェクトである必要があります。

ステップ 8 ツールバーの [ディスク] アイコンをクリックして、新たに描画した領域を保存します。

フロア上の包含リージョンの定義

包含領域を定義するには、次の手順を実行します。

ステップ 1 [Design] > [Site Maps] を選択します。

ステップ 2 該当するフロア領域の名前をクリックします。

ステップ 3 [Select a command] ドロップダウン リストから [Map Editor] を選択します。

ステップ 4 [Go] をクリックします。

ステップ 5 マップで、ツールバーの水色のボックスをクリックします。

（注） 一度に 1 つの包含領域のみ定義できることを示すメッセージ ボックスが表示されます。 新しい包含リージョンを定義すると、以前に定義されていた包含リージョンは自動的に削除されます。デフォルトでは、各フロアの包含リージョンは、そのリージョンが Prime Infrastructure に追加されるときに定義されます。 包含リージョンは水色の実線で示され、通常はリージョンの輪郭を描きます。

ステップ 6 表示されるメッセージ ボックスで [OK] をクリックします。 包含領域の輪郭を描画するための描画アイコンが表示されます。

ステップ 7 包含領域の定義を開始するには、描画アイコンをマップ上の開始ポイントに移動して、1 回クリックします。

ステップ 8 含める領域の境界に沿ってカーソルを移動させ、クリックして境界線を終了します。 再びクリックすると、次の境界線を定義できます。

ステップ 9 領域の輪郭が描画されるまでフロア上の包含リージョンの定義を繰り返したら、描画アイコンをダブルクリックします。 水色の実線によって包含領域が定義されます。

ステップ 10 [Command] メニューから [Save] を選択するか、ツールバーの**ディスク** アイコンをクリックして、包含リージョンを保存します。

（注） 包含領域を誤って定義した場合は、領域をクリックします。 選択された領域の輪郭が水色の破線で描かれます。 次に、ツールバーの [X] アイコンをクリックします。 領域がフロア マップから削除されます。

ステップ 11 [Location Regions] チェックボックスがまだオンになっていない場合にはオンにします。 これをすべてのフロア マップに適用する場合は、[Save settings] をクリックします。 [Layers configuration] ページを閉じます。

ステップ 12 Prime Infrastructure データベースと MSE データベースを再同期するには、[Services] > [Synchronize Services] を選択します。

（注） 2 つの DB がすでに同期されている場合は、変更があるたびに自動的に再同期が実行されます。明示的に再同期する必要はありません。

ステップ 13 [Synchronize] ページで、[Synchronize] ドロップダウン リストから [Network Designs] を選択して、[Synchronize] をクリックします。

[Sync. Status] 列で 2 つの緑色の矢印を調べることで、同期が正常に行われたことを 確認できます。

（注） 新たに定義された包含リージョンと除外リージョンは、Mobility Services Engine が既存デバイスのロケーションを再計算した後のみ、ロケーションの計算に含まれます。

フロア上の除外リージョンの定義

フロア上のロケーション計算の精度をさらに高めるために、計算に含めない除外領域を定義できます。たとえば、ビルディング内のアトリウムや階段の吹き抜けなどの領域を除外できます。通常、除外領域は包含領域の境界内に定義されます。

除外領域を定義するには、次の手順を実行します。

ステップ 1 [Design] > [Site Maps] を選択します。

ステップ 2 該当するフロア領域の名前をクリックします。

ステップ 3 [Select a command] ドロップダウン リストから [Map Editor] を選択します。

ステップ 4 [Go] をクリックします。

ステップ 5 マップで、ツールバーの紫色のボックスをクリックします。

ステップ 6 表示されるメッセージ ボックスで [OK] をクリックします。 除外領域の輪郭を描画するための描画アイコンが表示されます。

ステップ 7 包含領域の定義を開始するには、描画アイコンをマップ上の開始ポイントに移動して、1 回クリックします。

ステップ 8 除外する領域の境界に沿って描画アイコンを移動させます。 1 回クリックして境界線を開始し、再びクリックして境界線を終了します。

ステップ 9 領域の輪郭が描画されるまでフロア上の除外リージョンの定義を繰り返したら、描画アイコンをダブルクリックします。 定義された除外領域は、領域が完全に定義されると紫色で網掛けされます。 除外された領域は紫色で網掛けされます。

ステップ 10 すべての除外領域を定義したら、[Command] メニューから [Save] を選択するか、ツールバーの**ディスク**アイコンをクリックして、除外リージョンを保存します。

（注） 除外領域を削除するには、削除する領域をクリックします。 選択された領域の輪郭が紫色の破線で描かれます。 次に、ツールバーの [X] アイコンをクリックします。 領域がフロア マップから削除されます。

ステップ 11 [Location Regions] チェックボックスがまだオンになっていない場合にはオンにします。 これをすべてのフロア マップに適用する場合は、[Save settings] をクリックします。 完了したら [Layers configuration] ページを閉じます。

ステップ 12 Prime Infrastructure データベースと MSE データベースを再同期するには、[Services] > [Synchronize Services] を選択します。

（注） 2 つの DB がすでに同期されている場合は、変更があるたびに自動的に再同期が実行されます。明示的に再同期する必要はありません。

ステップ 13 [Synchronize]ページで、[Synchronize] ドロップダウン リストから [Network Designs] を選択して、[Synchronize] をクリックします。
[Sync. Status] 列で 2 つの緑色の矢印を調べることで、同期が正常に行われたことを 確認できます。

フロアでのレール ラインの定義

フロア上にコンベヤ ベルトを表すレール ラインを定義できます。 また、レール領域の周囲にスナップ幅とも呼ばれる、ロケーション計算を一層サポートする領域を定義できます。 この領域は、クライアントが表示されると予測される領域を表します。 スナップ幅の領域内に配置されたクライアントは、レール ライン上に表示されるか（多数）、スナップ幅領域の外側に表示されます（少数）。

（注） レール ラインの設定はタグには適用されません。

スナップ幅領域は、フィートまたはメートル（ユーザ定義）単位で定義され、レールの片側（東および西、または北および南）からモニタされる距離を表します。

レールをフロアに定義するには、次の手順を実行します。

ステップ 1 [Design] > [Site Maps] を選択します。
ステップ 2 該当するフロア領域の名前をクリックします。
ステップ 3 [Select a command] ドロップダウン リストから、[Map Editor] を選択します。
ステップ 4 [Go] をクリックします。
ステップ 5 マップで、ツールバーの**レール** アイコン（紫色の除外アイコンの右側）をクリックします。
ステップ 6 表示されるメッセージ ダイアログボックスで、レールのスナップ幅（フィートまたはメートル）を入力し、[OK] をクリックします。 描画アイコンが表示されます。
ステップ 7 レール ラインの開始ポイントで**描画**アイコンをクリックします。 ラインの描画を停止するときやラインの方向を変えるときは、再びクリックします。
ステップ 8 フロア マップ上にレール ラインを完全に描画したら、**描画**アイコンを 2 回クリックします。 レール ラインはマップ上に表示され、片側は定義されたスナップ幅リージョンに接します。
（注） レール ラインを削除するには、削除する領域をクリックします。 選択された領域の輪郭が紫色の破線で描かれます。 次に、ツールバーの [X] アイコンをクリックします。 領域がフロア マップから削除されます。

ステップ 9 フロア マップで、[Layers] ドロップダウン リストを選択します。

ステップ 10 完了したら、[Rails] チェックボックスがまだオンになっていない場合にはオンにし、[Save settings] をクリックし、[Layers configuration] パネルを閉じます。

ステップ 11 Prime Infrastructure と Mobility Services Engine を再同期するには、[Services] > [Synchronize Services] を選択します。

ステップ 12 [Synchronize] ページで、[Synchronize] ドロップダウン リストから [Network Designs] を選択して、[Synchronize] をクリックします。
[Sync. Status] 列で 2 つの緑色の矢印を調べることで、同期が正常に行われたことを 確認できます。

屋外領域の追加

（注） 屋外領域マップをデータベースに追加したことがあるかどうかに関係なく、屋外領域を Prime Infrastructure データベース内のキャンパス マップに追加することができます。

屋外領域をキャンパス マップに追加するには、次の手順を実行します。

ステップ 1 屋外領域のマップをデータベースに追加する場合は、マップを .PNG、.JPG、.JPEG、または .GIF 形式で保存します。 ファイル システムの特定の場所にあるマップを参照して、インポートします。
（注） 屋外領域を追加するのにマップは必要ありません。 屋外領域をデータベースに追加するため、領域の寸法を定義する必要があるだけです。 Prime Infrastructure では、作業領域に合わせてマップのサイズが自動的に調整されるため、マップは任意のサイズにすることができます。

ステップ 2 [Design] > [Site Maps] を選択します。

ステップ 3 目的のキャンパスをクリックすると、[Design] > [Site Maps] > [Campus View] ページが表示されます。

ステップ 4 [Select a command]ドロップダウン リストから、[New Outdoor Area] を選択します。

ステップ 5 [Go] をクリックします。 [Create New Area] ページが表示されます。

ステップ 6 [New Outdoor Area] ページで、次の情報を入力します。

- [Name]：新しい屋外領域のユーザ定義の名前。
- [Contact]：ユーザ定義の連絡先の名前。
- [Area Type (RF Model)]：[Cubes And Walled Offices]、[Drywall Office Only]、[Outdoor Open Space]（デフォルト）。
- [AP Height (feet)]：アクセス ポイントの高さを入力します。
- [Image File]：屋外領域マップを含むファイルの名前。 [Browse] をクリックしてファイルを検索します。

ステップ 7 [Next] をクリックします。

ステップ 8 [Place] をクリックして、屋外領域をキャンパス マップ上に配置します。 Prime Infrastructure では、キャンパス マップのサイズに合わせてサイズ変更された屋外領域の四角形が作成されます。

ステップ 9 屋外領域の四角形をクリックし、キャンパス マップ上の目的の位置までドラッグします。

ステップ 10 [Save] をクリックして、この屋外領域とキャンパス上の位置をデータベースに保存します。

（注） 屋外領域には、該当する [Maps] ページに移動するためのハイパーリンクが関連付けられます。

ステップ 11 （任意）新しい屋外領域に位置プレゼンス情報を割り当てるには、[Edit Location Presence Info] を選択し、[Go] をクリックします。

（注） デフォルトでは、[Override Child Element Presence Info] チェックボックスがオンになっています。屋外領域については、この設定を変更する必要はありません。

プランニング モードの使用

プランニング モードでは、プランニング ツールが起動されるブラウザ ウィンドウで Map Editor を開きます。 元のブラウザ ウィンドウがフロアのページから移動している場合は、フロアのページに戻って、Map Editor を起動する必要があります。

データ トラフィック、音声トラフィック、および位置がそれぞれアクティブかどうかに基づいて、アクセス ポイントの推奨される数および位置を計算できます。

（注） プランニング モードでは、各プロトコル（802.11a または 802.11 b/g）に指定されるスループットに基づいて、ネットワーク内で最適カバレッジを提供するために必要な合計アクセス ポイント数が計算されます。

プランニング モードのオプション：

- [Add APs]：マップへのアクセス ポイントの追加を可能にします。 詳細については、「アクセス ポイントのフロア領域への追加」（10-11 ページ）を参照してください。
- [Delete APs]：選択したアクセス ポイントを削除します。
- [Map Editor]：[Map Editor] ウィンドウを開きます。
- [Synchronize with Deployment]：プランニング モードのアクセス ポイントを現在の導入シナリオと同期します。
- [Generate Proposal]：現在のアクセス ポイント導入のプランニング概要を表示します。
- [Planned AP Association Tool]：Excel または CSV ファイルから AP アソシエーションの追加、削除、またはインポートを実行できます。 アクセス ポイントを定義したら、[Planned AP Association Tool] を使用して、そのアクセス ポイントをベース無線の MAC アドレスにアソシエートできます。 AP が検出されない場合、 AP はスタンバイ バケットに送られ、AP が検出されたときにアソシエートされます。

（注） AP アソシエーションには、AP はフロアまたは屋外領域に属さないという制限があります。 APがすでにフロアまたは屋外領域に割り当てられている場合は、スタンバイ バケットが AP を保持し、フロアまたは屋外領域から AP が削除されたときに、指定されたフロアに配置されます。 1 つの MAC アドレスを複数のフロアまたは屋外領域のバケットに入力することはできません。

（注） マップの同期は、AP がベース無線の MAC アドレスにアソシエートされている場合のみ動作し、イーサネットMACアドレスにアソシエートされている場合は動作しません。

チョークポイントを使用したタグの位置報告の精度の向上

チョークポイントは、チョークポイントのベンダーによって推奨されるとおりに設置および設定されます。 チョークポイントのインストールが完了して動作可能になったら、チョークポイントをロケーション データベースに入力して、Prime Infrastructure マップ上に表示できます。

アクティブな Cisco CX 準拠のタグと一緒にチョークポイントを使用すると、タグとそのアセットに関するロケーション情報が即座に提供されます。 Cisco CX タグがチョークポイントの範囲外に出ると、後続のビーコンフレームには、チョークポイントの識別情報が何も含まれません。タグのロケーションは、デフォルトで、タグに関連付けられたアクセス ポイントにより報告される RSSI に基づいた標準の計算方法で決定されます。

ここでは、次の内容について説明します。

Prime Infrastructure へのチョークポイントの追加

Prime Infrastructure データベースにチョークポイントを追加するには、次の手順を実行します。

ステップ 1 [Configure] > [Chokepoints] を選択します。

ステップ 2 [Select a command] ドロップダウン リストから、[Add Chokepoints] を選択します。

ステップ 3 [Go] をクリックします。

ステップ 4 チョークポイントの MAC アドレスと名前を入力します。

ステップ 5 [Entry/Exit Chokepoint] チェックボックスをオンにします。

ステップ 6 チョークポイントのカバレッジ範囲を入力します。

（注） チョークポイントの範囲は視覚的に表示されるだけです。 これは製品固有です。 実際の範囲は、該当するチョークポイント ベンダー ソフトウェアを使用して別個に設定する必要があります。

ステップ 7 [OK] をクリックします。

（注） データベースにチョークポイントを追加したら、適切な Prime Infrastructure フロア マップに配置できます。

Prime Infrastructure マップへのチョークポイントの追加

チョークポイントをマップに追加するには、次の手順を実行します。

ステップ 1 [Design] > [Site Maps] を選択します。

ステップ 2 [Maps] ページで、チョークポイントのフロアの位置に対応するリンクを選択します。

ステップ 3 [Select a command] ドロップダウン リストから、[Add Chokepoints] を選択します。

ステップ 4 [Go] をクリックします。

（注） [Add Chokepoints] 概要ページには、データベースには存在しているが、まだマップされていない、最近追加されたチョークポイントがすべて一覧表示されます。

ステップ 5 マップ上に配置するチョークポイントの横にあるチェックボックスを選択します。

ステップ 6 [OK] をクリックします。
チョークポイント アイコンが左上隅に配置されたマップが表示されます。 これで、マップ上にチョークポイントを配置する準備ができました。

ステップ 7 チョークポイント アイコンを左クリックし、適切な位置までドラッグします。

（注） チョークポイント アイコンを配置するためにクリックすると、左側のダイアログボックスにチョークポイントの MAC アドレス、名前、およびカバレッジ範囲が表示されます。

ステップ 8 [Save] をクリックします。
フロア マップ ページが再度表示され、追加されたチョークポイントがマップに示されます。

（注） 新たに作成されたチョークポイント アイコンは、そのフロアの表示設定に応じて、マップに表示される場合と表示されない場合があります。

（注） チョークポイントの周囲の輪は、カバレッジ領域を示しています。 CCX タグとそのアセットがカバレッジ領域内を通過すると、位置の詳細がブロードキャストされ、タグはチョークポイント カバレッジ円上に自動的にマップされます。 タグがチョークポイントの範囲外に出ると、その位置は以前と同様に計算されるので、チョークポイントの輪の上にはマップされなくなります。

（注） チョークポイントのマップ アイコンの上にマウス カーソルを移動すると、チョークポイントの MAC アドレス、名前、Entry/Exit チョークポイント、スタティック IP アドレス、および範囲が表示されます。

ステップ 9 チョークポイントがマップ上に表示されない場合は、[Floor Settings] メニューにある [Chokepoints] チェックボックスを選択します。

（注） すべてのマップに対してこの表示条件を保存しない場合には、[Save Settings] をクリックしないでください。

（注） チョークポイント情報を適用するには、ネットワーク設計を Mobility Services Engine またはロケーション サーバと同期する必要があります。

Prime Infrastructure からのチョークポイントの削除

一度に 1 つ以上のチョークポイントを削除できます。 チョークポイントを削除するには、次の手順を実行します。

ステップ 1 [Configure] > [Chokepoints] を選択します。 [Chokepoints] ページが表示されます。

ステップ 2 削除するチョークポイントの隣のチェックボックスをオンにします。

ステップ 3 [Select a command] ドロップダウン リストから、[Add Chokepoints] を選択し、[Go] をクリックします。

ステップ 4 チョークポイントの削除を確認するには、表示されるダイアログボックスで [OK] をクリックします。 [Chokepoints] ページが再度表示され、チョークポイントの削除を確認します。 削除されたチョークポイントはページには表示されなくなります。

第 12 章

システムとサービスのモニタリング

この章では、アラーム、イベント、およびログの設定と表示による Mobility Services Engine のモニタ方法、システムの使用率および要素（タグ、クライアント、不正クライアント、干渉、およびアクセス ポイント）のカウントについてのレポートの生成方法について説明します。 また、Prime Infrastructure を使用して、クライアント（有線と無線）、タグ、チェックポイント、および Wi-Fi TDOA 受信機をモニタする方法についても説明します。

この章の内容は、次のとおりです。

- 有線スイッチのモニタリング，254 ページ
- 干渉のモニタリング，256 ページ
- MSE を使用したモニタ モード AP のクラスタリング，258 ページ

アラームの処理

この項では、Prime Infrastructure を使用した Mobility Services Engine のアラームの表示、割り当て、およびクリア方法について説明します。 また、アラーム通知（All、Critical、Major、Minor、Warning）の定義方法、およびそれらのアラーム通知を電子メール送信する方法についても説明します。

ここでは、次の内容について説明します。

- 注意事項と制約事項，（184 ページ）
- アラームの表示，（185 ページ）
- Cisco Adaptive wIPS アラームの詳細のモニタリング，（186 ページ）
- アラームの割り当てと割り当て解除，（188 ページ）
- アラームの削除とクリア，（188 ページ）
- 電子メール アラーム通知，（189 ページ）

注意事項と制約事項

重大度が [Clear] になると、アラームは 30 日経過後に Prime Infrastructure から削除されます。

アラームの表示

Mobility Services Engine のアラームを表示するには、次の手順を実行します。

ステップ 1 [Monitor] > [Alarms] の順に選択します。

ステップ 2 ナビゲーション バーにある [Advanced Search] リンクをクリックします。 アラーム用の設定可能な検索ダイアログボックスが表示されます。

ステップ 3 [Search Category] ドロップダウン リストから [Alarms] を選択します。

ステップ 4 [Severity] ドロップダウン リストから、アラームの重大度を選択します。 オプションは、[All Severities]、[Critical]、[Major]、[Minor]、[Warning]、または [Clear] です。

ステップ 5 [Alarm Category] ドロップダウン リストから、[Mobility Service] を選択します。

ステップ 6 [Condition] コンボ ボックスから [Condition] を選択します。 または、[Condition] テキスト ボックスに条件を入力できます。

ステップ 7 [Time Period] ドロップダウン リストから、アラームを確認するタイム フレームを選択します。
オプションの範囲は、分単位（5、15、および 30）から、時間単位（1 ～ 8）、日数単位（1 ～ 7）までです。 すべてを表示するには、[Any time] を選択します。

ステップ 8 [Alarm Summary] ページの認知しているアラームとそれぞれのカウントを除外するには、[Acknowledged State] チェックボックスをオンにします。

ステップ 9 [Alarm Summary] ページの割り当て済みのアラームとそれぞれのカウントを除外するには、[Assigned State] チェックボックスをオンにします。

ステップ 10 [Items per page] ドロップダウン リストから、各ページに表示するアラーム数を選択します。

ステップ 11 後で使用するために検索条件を保存するには、[Save Search] チェックボックスをオンにして、検索の名前を入力します。

（注） その後は、[Saved Search] リンクをクリックすることで、その検索を開始できます。

ステップ 12 [Go] をクリックします。 [alarms summary] ダイアログボックスが表示され、検索結果が表示されます。

（注） アラームをソートするには、列見出し（[Severity]、[Failure Source]、[Owner]、[Date/Time]、[Message]、および [Acknowledged]）をクリックします。

ステップ 13 Mobility Services Engine の Context-Aware Service Notification を表示するには、ステップ 2 から ステップ 12 を繰り返します。 Step 5 で、アラーム カテゴリとして「Context Aware Notifications」と入力します。

Cisco Adaptive wIPS アラームの詳細のモニタリング

MSE アラームの詳細を表示するには、次の手順を実行します。

選択した Cisco wIPS アラームの詳細を表示するには、[Monitor] > [Alarms] > [failure object] の順に選択します。 Cisco Adaptive wIPS アラームについて、次のアラームの詳細が表示されます。

- [General Properties]：全般情報は、アラームのタイプによって異なる場合があります。 たとえば、アラーム詳細の中に、ロケーションおよびスイッチ ポート トレーシング情報を含む場合もあります。 次の表に、MSE アラームと wIPS トラップの条件に関連付けられている一般パラメータの説明を示します。
  - [Detected By wIPS AP]：アラームを検出したアクセス ポイント。
  - [wIPS AP IP Address]：wIPS アクセス ポイントの IP アドレス。
  - [Owner]：このアラームに割り当てられている個人の名前またはブランク。
  - [Acknowledged]：アラームがユーザによって承認されているかどうかを表示します。
  - [Category]：wIPS の場合、アラーム カテゴリは [Security] です。
  - [Created]：アラームが作成された日時（月、日、年、時、分、秒、AM/PM）。
  - [Modified]：アラームが最後に変更された日時（月、日、年、時、分、秒、AM/PM）。
  - [Generated By]：アラーム イベントの生成方法（NMS またはトラップから）を示します。

    [NMS (Network Management System - Prime Infrastructure)]：ポーリングによって生成されます。 Prime Infrastructure は、コントローラを定期的にポーリングして、イベントを生成します。 Prime Infrastructure がイベントを生成するのは、トラップを無効にしたときか、これらのイベントのトラップが失われたときです。 この場合、NMS 「によって生成されます」。

    [Trap]：コントローラによって生成されます。 Prime Infrastructure は、これらのトラップを処理して、対応するイベントを発生させます。 この場合、コントローラ「によって生成されます」。
  - [Severity]：重大度（重大、やや重大、比較的重大でない、警告、およびクリア）。
  - [Last Disappeared]：潜在的な攻撃が最後になくなった日時。
  - [Channel]：潜在的な攻撃が発生したチャネル。
  - [Attacker Client/AP MAC]：攻撃を開始したクライアントまたはアクセス ポイントの MAC アドレス。

- [Attacker Client/AP IP Address]：攻撃を開始したクライアントまたはアクセス ポイントの IP アドレス。
- [Target Client/AP IP Address]：攻撃者により攻撃対象となったクライアントまたはアクセス ポイントの IP アドレス。
- [Controller IP Address]：アクセス ポイントがアソシエートされているコントローラの IP アドレス。
- [MSE]：関連付けられている Mobility Services Engine の IP アドレス。
- [Controller MAC Address]：アクセス ポイントがアソシエートされているコントローラの MAC アドレス。
- wIPS access point MAC address
- Forensic File
- [Event History]：[Monitoring Alarms] ページに移動し、このアラームのすべてのイベントを表示します。

- [Annotations]：このテキスト ボックスに新しい注釈を入力して [Add] をクリックすると、該当するアラームが更新されます。 注釈は [Annotations] 表示領域に表示されます。
- [Messages]：アラーム名を表示します。
- [Description]：アラームに関する統合された情報を表示します。
- [Mitigation Status]：どの緩和アクションが攻撃に対して開始されたかを表示します。
- [Audit Report]：クリックして、設定監査アラームの詳細を表示します。 このレポートは、設定監査アラームにだけ使用できます。

  監査の矛盾が設定グループに施行されると、設定監査アラームが生成されます。

（注） 施行が失敗すると、設定グループに重大なアラームが生成されます。 施行が成功すると、設定グループに比較的重大でないアラームが生成されます。 アラームには監査レポートへのリンクがあり、各コントローラの矛盾のリストを表示できます。

- [Event History]：[MSE Alarm Events] ページを開き、このアラームのイベントを表示します。アラーム ページが複数ある場合は、ページ番号および他のページへ移動するためのスクロール矢印がページ上部に表示されます。 これらのスクロール矢印を使用して、その他のアラームを表示します。
- [Rogue Clients]：障害が発生したオブジェクトが不正なアクセス ポイントの場合、不正なクライアントに関する情報が表示されます。
- [Map Location]：アラームのマップの位置を表示します。
  - [Floor]：この攻撃が検出された場所。

- [Last Located At]：攻撃が最後に検出された時刻。
- [On MSE]：この攻撃が検出されたモビリティ サーバ エンジン。
- [Location History]：[Location History] をクリックすると、現在の攻撃者と被害者の場所の詳細を表示します。

• [Related Alarm List]：特定の攻撃に関連するすべてのアラームを示します。 これは、アラームを統合する際にどの統合ルールが使用されたかを示します。

- [Alarm Name]：アラームの名前。
- [First Heard]：攻撃が最初に確認された日時を示します。
- [Last Heard]：攻撃が最後に確認された日時を示します。
- [Status]：攻撃のステータス。

アラームの割り当てと割り当て解除

アラームの割り当ておよび割り当て解除を行うには、次の手順を実行します。

ステップ 1 [Monitor] > [Alarms] の順に選択して、[Alarms] ページを開きます。

ステップ 2 対応するチェックボックスをオンにすることで、自分に割り当てるアラームを選択します。

（注） 自分に割り当てられているアラームを割り当て解除するには、該当アラームの隣にあるボックスをオフにします。 他の人に割り当てられているアラームの割り当ては解除できません。

ステップ 3 [Select a command] ドロップダウン リストから、[Assign to Me]（または [Unassign]）を選択します。 [Go] をクリックします。

[Assign to Me] を選択した場合、自分のユーザ名が [Owner] 欄に表示されます。 [Unassign] を選択した場合、ユーザ名の欄は空白になります。

アラームの削除とクリア

アラームを削除すると、アラームはPrime Infrastructureによってデータベースから削除されます。アラームをクリアすると、Prime Infrastructureデータベースには残りますが、[Clear] 状態になります。 アラームは、その原因となった状況が存在しなくなったときにクリアする必要があります。

Mobility Services Engine からアラームを削除またはクリアするには、次の手順を実行します。

ステップ 1 [Monitor] > [Alarms] の順に選択して、[Alarms] ページを開きます。

ステップ 2 対応するチェックボックスをオンにして、削除またはクリアするアラームを選択します。

ステップ 3 [Select a command] ドロップダウン リストから [Delete] または [Clear] を選択します。 [Go] をクリックします。

電子メール アラーム通知

Prime Infrastructure では、特定の電子メール アドレスにアラーム通知を送信できます。 電子メール経由で通知を送信することで、必要な場合に迅速なアクションをとることができます。

自分に電子メールで送信されるアラーム重大度のタイプ（Critical、Major、Minor、および Warning）を選択できます。

メールにアラーム通知を送信するには、次の手順に従います。

ステップ 1 [Monitor] > [Alarms] の順に選択します。

ステップ 2 [Select a command] ドロップダウン リストから、[Email Notification] を選択します。 [Go] をクリックします。 [Email Notification] ページが表示されます。

（注） SMTP メール サーバは、電子メール通知の対象となる電子メール アドレスを入力する前に定義しておく必要があります。 [Administrator] > [Settings] > [Mail Server Configuration] の順に選択して、適切な情報を入力します。

ステップ 3 [Mobility Service] の隣にある [Enabled] チェックボックスをオンにします。

（注） [Mobility Service] アラーム カテゴリを有効にすると、Mobility Services Engine とロケーション アプライアンスに関連するすべてのアラームが定義済みの電子メール アドレスに送信されます。

ステップ 4 [Mobility Service] リンクをクリックします。 Mobility Services Engine に報告されるアラーム重大度のタイプを設定するページが表示されます。

ステップ 5 電子メール通知を送信するすべてのアラーム重大度のタイプの隣にあるチェックボックスをオンにします。

ステップ 6 [To] テキスト ボックスに、電子メール通知を送信する 1 つまたは複数の電子メール アドレスを入力します。 電子メール アドレスはカンマで区切ります。

ステップ 7 [OK] をクリックします。

[Alarms > Notification] ページに戻ります。 報告されたアラーム重大度のレベルに対する変更と電子メール通知の受信者の電子メール アドレスが表示されます。

イベントの使用

Prime Infrastructure を使用して、Mobility Services Engine とロケーション通知のイベントを表示できます。イベントは、それぞれの重大度（Critical、Major、Minor、Warning、Clear、Info）およびそれらのカテゴリに基づき検索して表示できます。

ここでは、ロケーション通知イベントの表示の手順ついて説明します。

ロケーション通知イベントの表示

ロケーション通知イベントを表示するには、次の手順を実行します。

ステップ 1 [Monitor] > [Events] を選択します。

ステップ 2 [Events] ページでは、次の操作を実行できます。

- 特定の要素のイベントを表示する場合に、その IP アドレス、名前、WLAN SSID、または MAC アドレスがわかっている場合は、ナビゲーション バーの [Search] テキスト ボックスにその値を入力します。 [Search] をクリックします。
- 重大度やカテゴリでイベントを表示するには、ナビゲーション バーで [Advanced Search] をクリックして、[Severity] および [Event Category] ドロップダウン リスト ボックスから適切なオプションを選択します。 [Go] をクリックします。

ステップ 3 Prime Infrastructure は検索条件に一致するイベントを見つけると、それらのイベントを一覧表示します。

（注） イベントの詳細を表示するには、イベントに関連付けられている [Failure Source] をクリックします。 また、イベントの概要を各列見出しで並べ替えることができます。

ログの操作

この項では、ロギング オプションの設定方法と、ログ ファイルのダウンロード方法について説明します。

ここでは、次の内容について説明します。

注意事項と制約事項

- ログ レベルから適切なオプションを選択する際には、Cisco TAC 担当者から [Error] と [Trace] のみ使用するように指示があった場合は、指示に従ってください。
- 詳細デバッグは、モビリティ サービスの処理速度を低下させるため、Cisco TAC 担当者の指示の下でのみ有効にしてください。

ロギング オプションの設定

Prime Infrastructure を使用して、ログに記録するメッセージのタイプとログ レベルを指定できます。

ロギング オプションを設定するには、次の手順を実行します。

ステップ 1 [Services] > [Mobility Services] の順に選択します。

ステップ 2 設定する Mobility Services Engine の名前をクリックします。

ステップ 3 [System] メニューから [Logs] を選択します。 選択されている Mobility Services Engine のロギング オプションが表示されます。

ステップ 4 [Logging Level] ドロップダウン リストから適切なオプションを選択します。
ロギング オプションは、[Off]、[Error]、[Information]、および [Trace] の 4 つです。

ログ レベルが [Error] またはこれよりも上のレベルに設定されているログ レコードはすべて、新しいエラー ログ ファイル locserver-error-%u-%g.log に記録されます。 これは、ロケーション サーバの locserver-%u-%g.log ログ ファイルとともに維持される追加のログ ファイルです。 このエラー ログ ファイルには、[Error] レベルのログとそのコンテキスト情報が記録されます。 コンテキスト情報には、当該エラーよりも前の 25 ログ レコードが含まれています。 最大 10 のエラー ログ ファイルを維持できます。 各ログ ファイルの最大許容サイズは 10 MB です。

注意 Cisco Technical Assistance Center（TAC）の担当者から指示された場合のみ、[Error] と [Trace] を使用できます。

ステップ 5 イベントのロギングを開始する各要素の隣にある [Enabled] チェックボックスをオンにします。

ステップ 6 [Advanced Parameters] の [Enable] チェックボックスをオンにして、詳細デバッグを有効にします。 デフォルトでは、このオプションは無効になっています。

注意 詳細デバッグは、モビリティ サービスの処理速度を低下させるため、Cisco TAC 担当者の指示の下でのみ有効にしてください。

ステップ 7 サーバからログ ファイルをダウンロードするには、[Download Logs] をクリックします。 詳細については、 ログ ファイルのダウンロード を参照してください。

ステップ 8 [Log File] グループ ボックスに、以下の情報を入力します。

- Mobility Services Engine で維持するログ ファイルの数。 Mobility Services Engine で維持できるログ ファイルの数は 5 ～ 20 です。

- 最大ログ ファイル サイズ（MB 単位）。 ログ ファイルのサイズは 10 ～ 50 MB です。

ステップ 9 [MAC Address Based Logging] ページで、次の手順を実行します。

- [Enable] チェックボックスをオンにし、MAC アドレス ロギングを有効にします。 デフォルトでは、このオプションは無効になっています。
- ロギングを有効にする 1 つ以上の MAC アドレスを追加します。 また、以前に追加した MAC アドレスを削除できます。削除するには、リストから MAC アドレスを選択して [Remove] をクリックします。

  MAC アドレス ベースのロギングの詳細については、MAC アドレスに基づくロギングを参照してください。

ステップ 10 [Save] をクリックして変更を適用します。

MAC アドレスに基づくロギング

この機能では、指定されている MAC アドレスのエンティティ固有のログ ファイルを作成できます。 ログ ファイルは次に示すパスの locserver ディレクトリ内に作成されます。

```
/opt/mse/logs/locserver
```

一度に最大で 5 つの MAC アドレスをログに記録できます。 MAC アドレス aa:bb:cc:dd:ee:ff のログ ファイルの形式は次のとおりです。

macaddress-debug-aa-bb-cc-dd-ee-ff.log

1 つの MAC アドレスに対して最大 2 つのログ ファイルを作成できます。 2 つのログ ファイルは、1 つのメインと 1 つのバックアップまたはロールオーバー ログ ファイルで構成できます。

MAC ログ ファイルの最小サイズは 10 MB です。 最大許容サイズは、MAC アドレスあたり 20 MB です。 24 時間以上更新されていない MAC ログ ファイルはプルーニングされます。

ログ ファイルのダウンロード

Mobility Services Engine ログ ファイルを解析する必要がある場合は、Prime Infrastructure を使用してログ ファイルをシステムにダウンロードできます。 Prime Infrastructure ではログ ファイルを含む .zip ファイルがダウンロードされます。

ログ ファイルが含まれている .zip ファイルをダウンロードするには、次の手順を実行します。

ステップ 1 [Services] > [Mobility Services] の順に選択します。
ステップ 2 ステータスを表示する Mobility Services Engine の名前をクリックします。
ステップ 3 左側のサイドバーのメニューから、[Logs] を選択します。
ステップ 4 [Download Logs] をクリックします。
ステップ 5 [File Download] ダイアログボックスの指示に従い、ファイルを表示するか、または .zip ファイルをシステムに保存します。

「Generating Reports」

Prime Infrastructure では、さまざまな種類のレポートを生成できます。 この項では、Prime Infrastructure Report Launch Pad を使用して、Context Aware レポートを生成する方法について説明します。 デフォルトでは、レポートは Prime Infrastructure サーバに保存されます。

レポート基準を定義したら、今後の診断で使用するためにレポートを保存し、臨時的に、またはスケジュール ベースでレポートを実行できます。

レポートの次の基準を定義できます。

- モニタする 1 つまたは複数の Mobility Services Engine
- レポートの生成頻度
- グラフ上でのデータの表示方法
- レポートを電子メールで送信するか、ファイルにエクスポートするか

レポート ラウンチ パッド

レポート ラウンチ パッドでは、1 つのページからすべての Prime Infrastructure レポートにアクセスできます。 このページでは、現在のレポートを表示し、特定のタイプのレポートを開き、新しいレポートを作成して保存し、スケジュール設定された実行を管理できます。 レポート ラウンチ パッドの [ContextAware reports] セクションにアクセスすると、ContextAware レポートを生成できます。

ヒント レポート タイプの横のツール チップ上にマウス カーソルを合わせると、レポートの詳細が表示されます。

ここでは、次の内容について説明します。

- 新規レポートの作成と実行, （194 ページ）

• 現在のレポートの管理, （200 ページ）
• スケジュールされた実行結果の管理, （201 ページ）
• 保存したレポートの管理, （202 ページ）

新規レポートの作成と実行

レポートを新規作成して実行するには、次の手順を実行します。

ステップ 1 [Reports] > [Report Launch Pad] の順に選択します。
レポートは、ページのメインセクションおよび左側のサイドバーのメニューに、カテゴリ別にリストされます。

ステップ 2 レポート ラウンチ パッドのメイン セクションで該当するレポートを見つけてください。
（注） レポート ラウンチ パッドでレポート名をクリックするか、[Report Launch Pad] ページの左側にあるナビゲーションを使用して、該当するレポートタイプに対する、現在保存されているレポートを表示します。

ステップ 3 [New] をクリックします。 [Report Details] ページが表示されます。

ステップ 4 [Report Details] ページで、次の [Settings] パラメータを入力します。

（注） 一部のパラメータは、レポート タイプによっては表示されることも、表示されないこともあります。

- [Report Title]：保存したレポートとしてこれを使用する場合は、レポート名を入力します。
- [Report By]：ドロップダウン リストから該当する [Report By]（レポート単位）のカテゴリを選択します。
- [Report Criteria]：事前に選択した [Report By] に応じて、結果をソートできます。 [Edit] をクリックして、[Filter Criteria] ページを開きます。

  （注） [Select] をクリックしてフィルタ条件を確認するか、[Close] をクリックして前のページに戻ります。

- [Connection Protocol]：[All Clients]、[All Wired (802.3)]、[All Wireless (802.11)]、[All 11u Capable Clients]、[802.11a/n]、[802.11b/g/n]、[802.11a]、[802.11b]、[802.11g]、[802.11n (5 GHz)]、[802.11n (2.4 GHz)]
- Reporting Period
  - [Select a time period…]ドロップダウン リストからレポート期間を選択します。 指定できる値は、[Today]、[Last 1 Hour]、[Last 6 Hours]、[Last 12 hours]、[Last 1 Day]、[Last 2 Days]、[Last 3 days]、[Last 4 Days]、[Last 5 Days]、[last 6 Days]、[Last 7 Days]、[Last 2 Weeks]、[Last 4 weeks]、[Previous Calendar Month]、[Last 8 Weeks]、[Last 12 Weeks]、[Last 6 Months]、[Last 1 Year] です。
  - [From]：[From]オプション ボタンを選択して、開始日時と終了日時を入力します。 テキスト ボックスに日付を入力するか、カレンダー アイコンをクリックして日付を選択できます。 ドロップダウン リストから時間と分を選択します。
  - [Show]：各ページに表示するレコード数を入力します。

    （注） すべてのレコードを表示するには、テキスト ボックスをブランクのままにします。

ステップ 5 このレポートを後で実行するか、繰り返しのレポートとして実行する場合は、[Schedule] パラメータを入力します。 [Schedule] パラメータを使用すると、レポートの実行時と実行頻度を管理できます。

- [Scheduling]：設定したスケジュールに従ってレポートを実行するには、[Enable] チェックボックスをオンにします。
- [Export Format]：エクスポートするファイルの形式（CSV または PDF）を選択します。
- [Destination]：宛先タイプ（[File] または [E-mail]）を選択します。 該当するファイルの場所または電子メール アドレスを入力します。

  （注） CSV ファイルおよび PDF ファイルのデフォルトの場所は、次のとおりです。

  /localdisk/ftp/reports/Inventory/<ReportTitleName>_<yyyymmdd>_<HHMMSS>.csv

  /localdisk/ftp/reports/Inventory/,ReportTitleName>_<yyyymmdd>_<HHMMSS>.pdf

（注） 電子メール用のメール サーバ セットアップを設定するには、[Administration] > [Settings] を選択し、左側のサイドバーのメニューの [Mail Server] を選択して [Mail Server Configuration] ページを開きます。 SMTP およびその他の必要な情報を入力します。

- [Start Date/Time]：表示されるテキスト ボックスに日付を入力するか、カレンダー アイコンをクリックして、日付を選択できるカレンダーを開きます。 時間と分のドロップダウン リストから時刻を選択します。 このデータに対するレポートの実行が、この日時に開始されます。
- [Recurrence]：このレポートの頻度を入力します。
  - [No Recurrence]：レポートは 1 度だけ実行されます（[Start Date/Time] で示した時間に実行）。
  - [Hourly]：レポートは、[Entry] テキスト ボックスに入力する時間数で示す間隔で実行されます。
  - [Daily]：レポートは、[Every] テキスト ボックスに入力する日数で示す間隔で実行されます。
  - [Weekly]：レポートは、[Every] テキスト ボックスに入力する週数およびチェックボックスをオンにした曜日に実行されます。
  - [Monthly]：レポートは、[Every] テキスト ボックスに入力する月数で示す間隔で実行されます。

[Create Custom Report] ページでは、レポート結果をカスタマイズできます。 次の表に、カスタマイズ可能なレポート、複数のサブレポートのあるレポート、および使用可能なレポート ビューを示します。 今後のリリースでは、すべてのレポートをカスタマイズできます。

表 *23*：レポートのカスタマイズ

レポート	カスタマイズの可否	複数サブレポート	レポート ビュー	データ フィールドのソート
Air Quality vs Time	Yes	No	表形式	No
Security Risk Interferers	Yes	No	表形式	No
Worst Air Quality APs	Yes	No	表形式	No
Worst Interferers	Yes	No	表形式	No
Busiest Clients	Yes	No	表形式	No
クライアント数	Yes	No	グラフ式	No
Client Session	Yes	No	表形式	No
Client Summary	Yes	Yes	各種	Yes
Client Traffic	Yes	No	グラフ式	No
Client Traffic Stream Metrics	Yes	No	表形式	No

レポート	カスタマイズの可否	複数サブレポート	レポート ビュー	データ フィールドのソート
Throughput	No	No	表形式	No
Unique Clients	Yes	No	表形式	No
v5 Client Statistics	No	No	表形式	No
Configuration Audit	Yes	No	表形式	No
PCI DSS Detailed	Yes	No	表形式	No
PCI DSS Summary	Yes	No	グラフ式	No
AP Profile Status	Yes	No	表形式	No
Device Summary	Yes	No	表形式	No
Busiest APs	Yes	No	表形式	No
Inventory - Combined Inventory	Yes	Yes	各種	Yes
Inventory - APs	Yes	Yes	各種	Yes
Inventory - Controllers	Yes	Yes	各種	Yes
Inventory - MSEs	Yes	Yes	各種	Yes
Up Time	Yes	No	表形式	No
Utilization - Controllers	No	No	グラフ式	No
Utilization - MSEs	No	No	グラフ式	No
Utilization - Radios	No	No	グラフ式	No
Guest Account Status	Yes	No	表形式	No
Guest Association	Yes	No	表形式	No
Guest Count	No	No	表形式	No
Guest User Sessions	Yes	No	表形式	No

レポート	カスタマイズの可否	複数サブレポート	レポート ビュー	データ フィールドのソート
Prime Infrastructure Guest Operations	Yes	No	表形式	No
Alternate Parent	Yes	No	表形式	No
Link Stats - Link Stats	Yes	No	表形式	No
Link Stats - Node Hops	Yes	No	グラフ式	No
ノード	Yes	No	表形式	No
Packet Stats - Packet Stats	No	No	グラフ式	No
Packet Stats - Packet Error Stats	No	No	グラフ式	No
Packet Stats - Packet Queue Stats	No	No	グラフ式	No
Stranded APs	No	No	表形式	No
Worst Node Hops - Worst Node Hop	Yes	Yes	各種	No
Worst Node Hops - Worst SNR Link	Yes	Yes	各種	No
802.11n Summary	No	Yes	グラフ式	No
Executive Summary	No	Yes	各種	No
802.11 Counters	Yes	No	両方	Yes
Coverage Holes	Yes	No	表形式	No
Network Utilization	Yes	Yes	両方	Yes
Traffic Stream Metrics	Yes	Yes	両方	Yes
Tx Power and Channel	No	No	グラフ式	No
VoIP Calls Graph	No	No	グラフ式	No
VoIP Calls Table	No	No	表形式	No

レポート	カスタマイズの可否	複数サブレポート	レポート ビュー	データ フィールドのソート
Voice Statistics	No	No	グラフ式	No
wIPS アラーム	Yes	No	表形式	No
wIPS Alarm Summary	Yes	No	両方	No
wIPS Top 10 APs	Yes	No	表形式	No
Adhoc Rogue Count Summary	Yes	No	両方	No
Adhoc Rogues	Yes	No	表形式	No
New Rogue AP Count Summary	Yes	No	両方	No
New Rogue APs	No	No	グラフ式	No
Rogue AP Count Summary	Yes	No	両方	No
Rogue APs	Yes	No	表形式	No
Security Alarm Trending Summary	Yes	No	グラフ式	No

ステップ 6 別の [Create Custom Report] ページを開くには、[Customize] をクリックします。

a) □Custom Report Name□ドロップダウン リストから、実行するレポートを選択します。 [Available and Selected] 列見出しの選択肢は、選択したレポートに応じて異なる場合があります。

b) [Report View] ドロップダウン リストから、レポートを表形式、グラフ形式、または両方を組み合わせた形式のいずれで表示するかを指定します。 このオプションは、一部のレポートでは使用できません。

c) 2 つのグループ ボックス（[Available data fields] と [Data fields to include]）間で強調表示された列見出しを移動するには、[Add >] ボタンと [< Remove] ボタンを使用します。

（注）

青の列見出しは、現在のサブレポートでは必須です。 これらは、[Selected Column] グループ ボックスから削除できません。

d) 結果テーブルの列の順序を決定するには、順序変更ボタン（[Move Up] または [Move Down]）を使用します。 [Selected Columns] リストで上方の列見出しが、結果表の左方に表示されます。

e) [Data field sorting] グループ ボックスで、ソート設定（[Ascending] または [Descending]）を指定します。 レポート データのソート方法を指定します。

- ソート順序を指定できる 4 つのデータ フィールドを選択できます。 [Sort by] および [Then by] ドロップダウン リストを使用して、ソートする各データ フィールドを選択します。
- ソートされたデータ フィールドごとに、[Ascending] でソートするか [Descending] でソートするかを選択します。

（注） 表形式のレポートのみソートできます（グラフおよび複合形式は不可）。 ソートできるフィールドのみが [Data field sorting] ドロップダウン リストに表示されます。

f) 変更内容を確定するには [Apply] を、列をデフォルトに戻すには [Reset] を、変更せずにこのページを閉じるには [Cancel] をクリックします。

（注） [Create Custom Report] ページで行った変更は、[Report Details] ページで [Save] をクリックしないうちは保存されません。

ステップ 7 すべてのレポート パラメータを設定したら、次のいずれかを選択します。

- [Save]：レポートをすぐに実行せずにこのレポート設定を保存するには、[Save] をクリックします。スケジュールしておいた時間になるとレポートは自動的に実行されます。
- [Save and Run]：このレポート設定を保存して、すぐにレポートを実行するには、[Save and Run] をクリックします。
- [Run Now]：レポート設定を保存せずにレポートを実行するには、[Run Now] をクリックします。
- [Cancel]：このレポートを実行も保存もせずに前のページに戻るには、[Cancel] をクリックします。

現在のレポートの管理

特定のレポート タイプに対するレポートが保存されている場合は、レポート ラウンチ パッドから現在のレポートにアクセスできます。

新しいチョークポイントが作成されると、すべての仮想ドメインで使用できます。 フロアに配置したあと、フロアと同じ仮想ドメインで使用できるように更新されます。 チョークポイントをフロアから削除すると、すべての仮想ドメインで再び利用可能になります。

[Report Launch Pad] から現在または保存されたレポートにアクセスするには、次の手順に従います。

ステップ 1 [Reports] > [Report Launch Pad] の順に選択します。

ステップ 2 左側のサイドバーのメニューまたはレポート ラウンチ パッドのメイン セクションから、特定のレポートを選択します。 [Report Launch Pad] ページには、このレポート タイプの現在のレポートのリストが表示されます。
保存されたレポートのリストを表示するには、[Reports] > [Saved Reports] を選択します。

スケジュールされた実行結果の管理

（注） スケジュールされた実行のリストは、レポート カテゴリ、レポート タイプ、およびタイム フレームでソートできます。

スケジュールされた実行結果のソート

[Show] ドロップダウン リストを使用すると、[Scheduled Run Results] をカテゴリ、タイプ、およびタイム フレームでソートできます。

- [Report Category]：ドロップダウン リストから該当するレポート カテゴリを選択するか [All] を選択します。
- [Report Type]：ドロップダウン リストから該当するレポート タイプを選択するか [All] を選択します。 レポート タイプの選択項目は、選択したレポート カテゴリに応じて変わります。
- [From]/[To]：レポートの開始日（[From]）と終了日（[To]）をテキスト ボックスに入力するか、カレンダー アイコンをクリックして開始日と終了日を選択します。
- レポート生成方式：ドロップダウン リストから適切なレポート生成方法を選択します。 考えられる方法は、[Scheduled]、[On-demand Export]、[On-demand Email] です。

このリストをソートするには、[Go] をクリックします。 条件に一致するレポートのみが表示されます。

スケジュールされた実行の詳細の表示または編集

保存したレポートを表示または編集するには、次の手順を実行します。

ステップ 1 [Report] > [Scheduled Run Results] の順に選択します。
ステップ 2 該当するレポートの [Report Title] リンクをクリックして、[Report Details] ページを開きます。
ステップ 3 スケジュールされた実行の詳細をこのページで表示または編集できます。
ステップ 4 スケジュールされた実行のすべてのパラメータを必要に応じて編集したら、次から選択します。

- [Save]：レポートをすぐに実行しないでこのスケジュール実行を保存するには、[Save] をクリックします。 スケジュールしておいた時間になるとレポートは自動的に実行されます。

- [Save and Run]：このスケジュールされた実行を保存して、レポートをすぐに実行するには、[Save and Run] をクリックします。
- [Cancel]：このレポートを実行も保存もせずに前のページに戻るには、[Cancel] をクリックします。
- [Delete]：現在保存されているレポートを削除するには、[Delete] をクリックします。

保存したレポートの管理

[Saved Reports] ページでは、保存したレポートを作成および管理できます。 Prime Infrastructure でこのページを開くには、[Reports] > [Saved Reports] の順に選択します。

（注） 保存したレポートのリストは、レポート カテゴリ、レポート タイプ、およびスケジュールされたステータス（有効、無効、または期限切れ）でソートできます。

[Saved Reports] ページには、次の情報が表示されます。

- [Report Title]：ユーザが割り当てたレポート名を示します。 このレポートの詳細を表示するには、レポート タイトルをクリックします。
- [Report Type]：特定のレポート タイプを示します。
- [Scheduled]：このレポートが有効か無効かを示します。
- [Next Schedule On]：このレポートの次回の実行の日時が示されます。
- [Last Run]：このレポートが最後に実行された日時が示されます。
- [Download]：レポートの結果の .csv ファイルを開くか保存するには、[Download] アイコンをクリックします。
- [Run Now]：現在のレポートをすぐに実行するには、[Run Now] アイコンをクリックします。

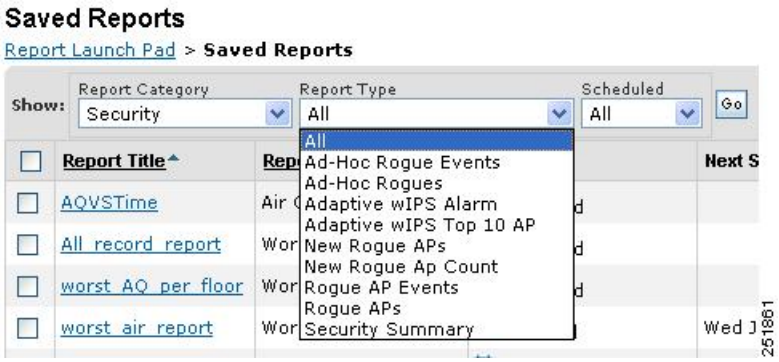
保存したレポートのソート

[Show] ドロップダウン リストを使用すると、[Saved Reports] リストをカテゴリ、タイプ、およびスケジュールされたステータスによってソートできます。

- [Report Category]：ドロップダウン リストから該当するレポート カテゴリを選択するか [All] を選択します。
- [Report Type]：ドロップダウン リストから該当するレポート タイプを選択するか [All] を選択します。 レポート タイプの選択項目は、選択したレポート カテゴリに応じて変わります。

- [Scheduled]：[All]、[Enabled]、[Disabled]、または [Expired] を選択して、スケジュールされたステータスによって [Saved Reports] リストをソートします。

図 7：保存したレポートのソート



このリストをソートするには、[Go] をクリックします。 条件に一致するレポートのみが表示されます。

保存したレポートの詳細の表示または編集

保存したレポートを表示または編集するには、次の手順を実行します。

ステップ 1 [Report] > [Saved Reports] を選択します。

ステップ 2 該当するレポートの [Report Title] リンクをクリックして、[Report Details] ページを開きます。

ステップ 3 [Report Details] ページで、保存したレポートの詳細を表示または編集できます。

ステップ 4 すべてのレポート パラメータを編集したら、次のいずれかを選択します。

- [Save]：レポートをすぐに実行せずにこのレポート設定を保存するには、[Save] をクリックします。スケジュールしておいた時間になるとレポートは自動的に実行されます。
- [Save and Run]：このレポート設定を保存して、すぐにレポートを実行するには、[Save and Run] をクリックします。
- [Run Now]：レポート設定を保存せずにレポートを実行するには、[Run Now] をクリックします。
- [Cancel]：このレポートを実行も保存もせずに前のページに戻るには、[Cancel] をクリックします。
- [Delete]：現在保存されているレポートを削除するには、[Delete] をクリックします。

MSE 分析レポートの生成

MSE 分析レポートはロケーション履歴データに基づいて生成されます。 この項では、Prime Infrastructure レポート ラウンチ パッドを介して生成できるさまざまな MSE 分析レポートを示しながら説明します。

MSE 分析レポートを生成するには、タイプ横の [New] をクリックします。

現在保存されているレポートを表示するには、レポート タイプをクリックします。 このページで、現在保存されているレポートを有効化、無効化、削除、または実行できます。

ここでは、作成可能な MSE 分析レポートについて説明します。内容は次のとおりです。

選択したゾーンでの関連付けられたクライアントと プローブ クライアント

このレポートは、関連づけられたクライアントとプローブ クライアントの、選択したゾーンにおける指定期間での数の比較を示します。 レポートの最初の部分は時系列グラフに数を示し、以降の部分ではフロアでのクライアントの分布を示します。

ここでは、次の内容について説明します。

- 選択したゾーンでの関連付けられたクライアントと プローブ クライアントの設定
- 関連付けられたクライアントと プローブ クライアントのレポート結果

クライアント ロケーション

このレポートには、MSEによって検出されたワイヤレス クライアントのロケーションの履歴が表示されます。

（注） クライアント ロケーション レポートは root 以外の仮想ドメインではフィルタリングされません。

ここでは、次の内容について説明します。

- Client Location History レポートの設定, （204 ページ）
- クライアント ロケーションの結果, （205 ページ）

Client Location History レポートの設定

Client Location History レポートの結果は root ドメインでのみ使用可能です。 Client Location History レポートを設定するには、次の手順に従います。

Settings

- [Report Title]：このレポートを保存する場合は、レポート名を入力します。
- [Report By]：デフォルトでは、[Client MAC Address] が選択されます。
- [Report Criteria]：[Edit] をクリックし、フィルタ基準として有効な MAC アドレスを入力します。

（注） [Report Criteria] ページで、[Select] をクリックしてフィルタ基準を確認するか、[Close] をクリックして前のページに戻ります。

Reporting Period

- オプション ボタンを選択して、ドロップダウン リストから期間を選択します。

  または

- [From] オプション ボタンを選択して、開始日時と終了日時を入力します。 テキスト ボックスに日付を入力するか、**カレンダー** アイコンをクリックして日付を選択できます。 ドロップダウン リストから時間と分を選択します。

（注） レポート期間は、アラームの最終検出時刻に基づいています。 時間はUTC タイム ゾーンです。

スケジュール

このレポートを後で実行するか、繰り返しのレポートとして実行する場合は、スケジューリング パラメータを入力します。 レポートのスケジュールの詳細については、保存したレポートの管理, （202 ページ）を参照してください。

レポートのカスタマイズ フォーム

[Customize Report form] では、レポート結果をカスタマイズできます。 レポート結果のカスタマイズの詳細については、保存したレポートの管理, （202 ページ）を参照してください。

（注） 固定された列は青色のフォントで表示され、使用可能な列には移動できません。

クライアント ロケーションの結果

Client Location History レポートの結果には、次の情報が含まれます。

- [Last Located]：クライアントが検出された時間。
- [Client Location]：検出された時間のクライアントの位置。

- [MSE]：このクライアントを検出した MSE の名前。
- [User]：クライアントのユーザ名。
- [Detecting Controllers]：検出中のコントローラの IP アドレス。
- [802.11 State]：802.11 の状態。 [Probing] または [Associated] のいずれかになります。
- [IP Address]：クライアントの IP アドレス。
- [AP MAC Address]：アソシエートされたアクセス ポイントの MAC アドレス。
- [Authenticated]：認証済みかどうか。 [Yes] または [No] のいずれかになります。
- [SSID]：クライアントで使用する SSID。
- [Protocol]：クライアントから情報を取得するために使用されるプロトコル。

（注） このレポートのロケーション フィールドはハイパーリンクであり、そのハイパーリンクをクリックすると、検出された時間のフロア マップでのクライアントの位置が表示されます。

Client Location Density

このレポートには、フィルタリング基準に基づいて、MSE によって検出されたワイヤレス クライアントと、このクライアントのロケーションが表示されます。

ここでは、次の内容について説明します。

- Client Location Density レポートの設定, （206 ページ）
- Client Location Density の結果, （208 ページ）

Client Location Density レポートの設定

Client Location History レポートの結果は root ドメインでのみ使用可能です。 Client Location History レポートを設定するには、次の手順に従います。

Settings

- [Report Title]：このレポートを保存する場合は、レポート名を入力します。
- Report By
  - MSE By Floor Area
  - MSE By Outdoor Area
  - MSE
- [Report Criteria]：レポート基準は、選択した [Report By] オプションによって異なります。 [Edit] をクリックして、必要なフィルタ基準を選択します。

（注） [Report Criteria] ページで、[Select] をクリックしてフィルタ基準を確認するか、[Close] をクリックして前のページに戻ります。

- Reporting Period
  - オプション ボタンを選択して、ドロップダウン リストから期間を選択します。

    または

  - [From] オプション ボタンを選択して、開始日時と終了日時を入力します。 テキスト ボックスに日付を入力するか、**カレンダー** アイコンをクリックして日付を選択できます。 ドロップダウン リストから時間と分を選択します。

（注） レポート期間は、アラームの最終検出時刻に基づいています。 時間はUTC タイム ゾーンです。

Reporting Period

- オプション ボタンを選択して、ドロップダウン リストから期間を選択します。

  または

- [From] オプション ボタンを選択して、開始日時と終了日時を入力します。 テキスト ボックスに日付を入力するか、**カレンダー** アイコンをクリックして日付を選択できます。 ドロップダウン リストから時間と分を選択します。

（注） レポート期間は、アラームの最終検出時刻に基づいています。 時間はUTC タイム ゾーンです。

スケジュール

このレポートを後で実行するか、繰り返しのレポートとして実行する場合は、スケジューリング パラメータを入力します。

レポートのカスタマイズ フォーム

[Customize Report form] では、レポート結果をカスタマイズできます。

（注） 固定された列は青色のフォントで表示され、使用可能な列には移動できません。

Client Location Density の結果

Client Location Density レポートの結果には、次の情報が含まれます。

- [Last Located]：選択した [Report Time] 基準内にクライアントが最後に検出された時間。
- [MAC Address]：クライアントの MAC アドレス
- [Client Location]：検出された時間のクライアントの位置。
- [MSE]：クライアントを検出した MSE の名前。
- [User]：クライアントのユーザ名。
- [Detecting Controllers]：検出中のコントローラの IP アドレス。
- [802.11 State]：802.11 の状態。 [Probing] または [Associated] のいずれかです。
- [IP Address]：クライアントの IP アドレス。
- [SSID]：クライアントで使用する SSID。
- [Protocol]：クライアントから情報を取得するために使用されるプロトコル。

（注） このレポートのロケーション フィールドはハイパーリンクであり、そのハイパーリンクをクリックすると、検出された時間のフロア マップでのクライアントの位置が表示されます。

Device Count by Zone

このレポートでは、選択したゾーン内の MSE によって検出されたデバイスの数が示されます。

ここでは、次の内容について説明します。

- Device Dwell by Zone レポートの設定, （208 ページ）
- Device Count by Zone の結果, （210 ページ）

Device Dwell by Zone レポートの設定

ここでは、Device Dwell Count Time by Zone レポートの設定方法について説明します。内容は次のとおりです。

Settings

- [Report Title]：このレポートを保存する場合は、レポート名を入力します。
- Report By
  - 屋内領域

- 屋外領域

- [Report Criteria]：レポート基準は、選択した [Report By] オプションによって異なります。[Edit] をクリックして、必要なフィルタ基準を選択します。

（注） [Report Criteria] ページで、**[Select]** をクリックしてフィルタ基準を確認するか、**[Close]** をクリックして前のページに戻ります。

- Device Type
  - すべて（All）
  - クライアント
  - タグ
  - Rogue Clients
  - Rogue APs
  - Interferers

- Reporting Period
  - オプション ボタンを選択して、ドロップダウン リストから期間を選択します。

    または

  - [From] オプション ボタンを選択して、開始日時と終了日時を入力します。 テキスト ボックスに日付を入力するか、**カレンダー** アイコンをクリックして日付を選択できます。 ドロップダウン リストから時間と分を選択します。

（注） レポート期間は、最後に検出されたアラームに基づいています。 時間は UTC タイム ゾーンです。

スケジュール

このレポートを後で実行するか、繰り返しのレポートとして実行する場合は、スケジューリング パラメータを入力します。

レポートのカスタマイズ フォーム

[Customize Report form] では、レポート結果をカスタマイズできます。

（注） 固定された列は青色のフォントで表示され、使用可能な列には移動できません。

Device Count by Zone の結果

Device Count by Zone レポートの結果には、次の情報が含まれます。

- [MSE]：このクライアントを検出した MSE の名前。
- [Zone]：Device Count by Zone の結果。
- [Device Type]：デバイスのタイプ。
- [MSE Analytics Report Link]：MSE 分析レポートを取得するためにリンクします。

Device Dwell Time by Zone

このレポートは、MSE で検出されたデバイスのドウェル時間レポートを提供します。 ここでは、次の内容について説明します。

ここでは、次の内容について説明します。

Device Dwell by Zone レポートの設定

ここでは、Device Dwell Count Time by Zone レポートの設定方法について説明します。内容は次のとおりです。

Settings

- [Report Title]：このレポートを保存する場合は、レポート名を入力します。
- Report By
  - 屋内領域
  - 屋外領域
- [Report Criteria]：レポート基準は、選択した [Report By] オプションによって異なります。[Edit] をクリックして、必要なフィルタ基準を選択します。

（注） [Report Criteria] ページで、**[Select]** をクリックしてフィルタ基準を確認するか、**[Close]** をクリックして前のページに戻ります。

- Device Type
  - すべて（All）
  - クライアント
  - タグ
  - Rogue Clients

- Rogue APs
- Interferers

- Reporting Period
  - オプション ボタンを選択して、ドロップダウン リストから期間を選択します。

    または

  - [From] オプション ボタンを選択して、開始日時と終了日時を入力します。 テキスト ボックスに日付を入力するか、**カレンダー** アイコンをクリックして日付を選択できます。 ドロップダウン リストから時間と分を選択します。

（注） レポート期間は、最後に検出されたアラームに基づいています。 時間は UTC タイム ゾーンです。

スケジュール

このレポートを後で実行するか、繰り返しのレポートとして実行する場合は、スケジューリング パラメータを入力します。

レポートのカスタマイズ フォーム

[Customize Report form] では、レポート結果をカスタマイズできます。

（注） 固定された列は青色のフォントで表示され、使用可能な列には移動できません。

Device Count by Zone の結果

Device Count by Zone レポートの結果には、次の情報が含まれます。

- [MSE]：このクライアントを検出した MSE の名前。
- [Zone]：Device Count by Zone の結果。
- [Device Type]：デバイスのタイプ。
- [MSE Analytics Report Link]：MSE 分析レポートを取得するためにリンクします。

Guest Location Density

このレポートには、フィルタリング基準に基づいて、MSEによって検出されたゲストクライアントと、このクライアントのロケーションが表示されます。

ここでは、次の内容について説明します。

Guest Location Density の設定

ここでは、次の内容について説明します。

Settings

- [Report Title]：このレポートを保存する場合は、レポート名を入力します。
- Report by
  - MSE By Floor Area
  - MSE By Outdoor Area
  - MSE
- [Report Criteria]：レポート基準は、選択した [Report By] オプションによって異なります。[Edit] をクリックして、必要なフィルタ基準を選択します。

（注） [Report Criteria] ページで、[Select] をクリックしてフィルタ基準を確認するか、[Close] をクリックして前のページに戻ります。

- Reporting Period
  - オプション ボタンを選択して、ドロップダウン リストから期間を選択します。

    または

  - [From] オプション ボタンを選択して、開始日時と終了日時を入力します。 テキスト ボックスに日付を入力するか、**カレンダー** アイコンをクリックして日付を選択できます。 ドロップダウン リストから時間と分を選択します。

（注） レポート期間は、最後に検出されたアラームに基づいています。 時間は UTC タイム ゾーンです。

- **スケジュール**

  このレポートを後で実行するか、繰り返しのレポートとして実行する場合は、スケジューリング パラメータを入力します。 詳細については、保存したレポートの管理, （202 ページ）を参照してください。

- **レポートのカスタマイズ フォーム**

  [Customize Report form] では、レポート結果をカスタマイズできます。 レポートのスケジュールの詳細については、保存したレポートの管理, （202 ページ）を参照してください。

Guest Location Density の結果

Guest Location Tracking レポートの結果には、次の情報が含まれます。

- [Last Located]：選択した [Report Time] 基準内にゲスト クライアントが最後に検出された時間。
- [Guest Username]：ゲスト クライアント ユーザのログイン名。
- [MAC Address]：ゲスト クライアントの MAC アドレス。
- [Guest Location]：検出された時間のゲスト クライアントの位置。
- [MSE]：このゲスト クライアントを検出した MSE の名前。
- [Detecting Controllers]：検出中のコントローラの IP アドレス。
- [IP Address]：ゲスト クライアントの IP アドレス。
- [AP MAC Address]：ゲスト クライアントがアソシエートされているアクセス ポイントの MAC アドレス。
- [SSID]：ゲスト クライアントで使用する SSID。
- [Protocol]：ゲスト クライアントから情報を取得するために使用されるプロトコル。

（注） このレポートのロケーション フィールドはハイパーリンクであり、そのハイパーリンクをクリックすると、検出された時間のフロア マップでのゲスト クライアントのロケーションが表示されます。

Location Notifications by Zone

このレポートには、MSE によって生成された Context-Aware 通知が表示されます。

ここでは、次の内容について説明します。

- Location Notification レポートの設定, （213 ページ）
- Location Notification の結果, （214 ページ）

Location Notification レポートの設定

ここでは、Rogue Client Location Tracking レポートの設定方法について説明します。

Settings

- [Report Title]：このレポートを保存する場合は、レポート名を入力します。
- Report by

- MSE By Floor Area
- MSE By Outdoor Area
- MSE

- [Report Criteria]：レポート基準は、選択した [Report By] オプションによって異なります。[Edit] をクリックして、必要なフィルタ基準を選択します。

（注） [Report Criteria] ページで、[Select] をクリックしてフィルタ基準を確認するか、[Close] をクリックして前のページに戻ります。

- Reporting Period
  - オプション ボタンを選択して、ドロップダウン リストから期間を選択します。

    または

  - [From] オプション ボタンを選択して、開始日時と終了日時を入力します。 テキスト ボックスに日付を入力するか、**カレンダー** アイコンをクリックして日付を選択できます。 ドロップダウン リストから時間と分を選択します。

（注） レポート期間は、アラームの最終検出時刻に基づいています。 時間はUTC タイム ゾーンです。

スケジュール

このレポートを後で実行するか、繰り返しのレポートとして実行する場合は、スケジューリング パラメータを入力します。 レポートのスケジュールの詳細については、保存したレポートの管理, （202 ページ）を参照してください。

レポートのカスタマイズ フォーム

[Customize Report form] では、レポート結果をカスタマイズできます。 レポート結果のカスタマイズの詳細については、保存したレポートの管理, （202 ページ）を参照してください。

（注） 固定された列は青色のフォントで表示され、使用可能な列には移動できません。

Location Notification の結果

Location Notification レポートの結果には、次の情報が含まれます。

- [Last Seen]：デバイスが最後に検出された日時。
- [MAC Address]：デバイスの MAC アドレス。

- [Device Type]：デバイス タイプ。
- [Asset Name]：アセットの名前。
- [Asset Group]：アセット グループの名前。
- [Asset Category]：アセット カテゴリの名前。
- [Map Location]：デバイスが検出されたマップ ロケーション。
- [serverName]：ContextAware 通知を送信するサーバの名前。

Mobile MAC Statistics

このレポートは、MSAPサーバまたは場所によるクリック数に基づいて、最もアクティブなMobile MAC Statistics を表示します。

ここでは、次の内容について説明します。

Mobile MAC Statistics の設定

ここでは、Mobile MAC Statistics レポートの設定方法について説明します。内容は次のとおりです。

Settings

- [Report Title]：このレポートを保存する場合は、レポート名を入力します。
- Report By
  - MSE By Floor Area
  - MSE By Outdoor Area
  - MSE
- [Report Criteria]：レポート基準は、選択した [Report By] オプションによって異なります。[Edit] をクリックして、必要なフィルタ基準を選択します。

（注） [Report Criteria] ページで、[Select] をクリックしてフィルタ基準を確認するか、[Close] をクリックして前のページに戻ります。

- Reporting Period
  - オプション ボタンを選択して、ドロップダウン リストから期間を選択します。

    または

  - [From] オプション ボタンを選択して、開始日時と終了日時を入力します。 テキスト ボックスに日付を入力するか、カレンダー アイコンをクリックして日付を選択できます。 ドロップダウン リストから時間と分を選択します。

（注） レポート期間は、アラームの最終検出時刻に基づいています。 時間はUTC タイム ゾーンです。

スケジュール

このレポートを後で実行するか、繰り返しのレポートとして実行する場合は、スケジューリング パラメータを入力します。 レポートのスケジュールの詳細については、保存したレポートの管理, （202 ページ）を参照してください。

レポートのカスタマイズ フォーム

[Customize Report form] では、レポート結果をカスタマイズできます。 レポート結果のカスタマイズの詳細については、保存したレポートの管理, （202 ページ）を参照してください。

（注） 固定された列は青色のフォントで表示され、使用可能な列には移動できません。

Mobile MAC Tracking の結果

Mobile MAC Statistics レポートの結果には次の情報が含まれます。

- 場所
- クリック数
- Mobile MAC Address

（注） このレポートのロケーション フィールドはハイパーリンクであり、そのハイパーリンクをクリックすると、検出された時間のフロア マップでの不正 AP のロケーションが表示されます。

Rogue AP Location Density

このレポートには、フィルタリング基準に基づいて、MSE によって検出された不正 AP と、この AP のロケーションが表示されます。

ここでは、次の内容について説明します。

Rogue AP Location Density の設定

ここでは、AP Location Density レポートの設定方法について説明します。内容は次のとおりです。

Settings

- [Report Title]：このレポートを保存する場合は、レポート名を入力します。
- Report By
  - MSE By Floor Area
  - MSE By Outdoor Area
- [Report Criteria]：レポート基準は、選択した [Report By] オプションによって異なります。[Edit] をクリックして、必要なフィルタ基準を選択します。

（注） [Report Criteria] ページで、[Select] をクリックしてフィルタ基準を確認するか、[Close] をクリックして前のページに戻ります。

- Device Type
  - すべて（All）
  - クライアント
  - タグ
  - Rogue Clients
  - Rogue APs
  - Interferers
- Reporting Period
  - オプション ボタンを選択して、ドロップダウン リストから期間を選択します。

    または
  - [From] オプション ボタンを選択して、開始日時と終了日時を入力します。 テキスト ボックスに日付を入力するか、**カレンダー** アイコンをクリックして日付を選択できます。 ドロップダウン リストから時間と分を選択します。

（注） レポート期間は、アラームの最終検出時刻に基づいています。 時間はUTC タイム ゾーンです。

スケジュール

このレポートを後で実行するか、繰り返しのレポートとして実行する場合は、スケジューリング パラメータを入力します。 レポートのスケジュールの詳細については、保存したレポートの管理, （202 ページ）を参照してください。

レポートのカスタマイズ フォーム

[Customize Report form] では、レポート結果をカスタマイズできます。 レポート結果のカスタマイズの詳細については、保存したレポートの管理, （202 ページ）を参照してください。

（注） 固定された列は青色のフォントで表示され、使用可能な列には移動できません。

Rogue AP Location Density

このレポートには、フィルタリング基準に基づいて、MSE によって検出された不正 AP と、この AP のロケーションが表示されます。

ここでは、次の内容について説明します。

Rogue Client Location Density

このレポートには、フィルタリング基準に基づいて MSE で検出された Rogue Client Location Density が示されます。

ここでは、次の内容について説明します。

Rogue Client Location Density の設定

ここでは、Rogue Client Location Density の設定方法について説明します。内容は次のとおりです。

Settings

- [Report Title]：このレポートを保存する場合は、レポート名を入力します。
- Report by
  - MSE By Floor Area
  - MSE By Outdoor Area
  - MSE
- [Report Criteria]：レポート基準は、選択した [Report By] オプションによって異なります。[Edit] をクリックして、必要なフィルタ基準を選択します。

（注） [Report Criteria] ページで、[Select] をクリックしてフィルタ基準を確認するか、[Close] をクリックして前のページに戻ります。

- Reporting Period
  - オプション ボタンを選択して、ドロップダウン リストから期間を選択します。

    または

- [From] オプション ボタンを選択して、開始日時と終了日時を入力します。 テキスト ボックスに日付を入力するか、**カレンダー** アイコンをクリックして日付を選択できます。 ドロップダウン リストから時間と分を選択します。

（注） レポート期間は、アラームの最終検出時刻に基づいています。 時間はUTC タイム ゾーンです。

Reporting Period

- オプション ボタンを選択して、ドロップダウン リストから期間を選択します。

  または

- [From] オプション ボタンを選択して、開始日時と終了日時を入力します。 テキスト ボックスに日付を入力するか、**カレンダー** アイコンをクリックして日付を選択できます。 ドロップダウン リストから時間と分を選択します。

（注） レポート期間は、アラームの最終検出時刻に基づいています。 時間はUTC タイム ゾーンです。

スケジュール

このレポートを後で実行するか、繰り返しのレポートとして実行する場合は、スケジューリング パラメータを入力します。 レポートのスケジュールの詳細については、保存したレポートの管理, （202 ページ）を参照してください。

レポートのカスタマイズ フォーム

[Customize Report form] では、レポート結果をカスタマイズできます。 レポート結果のカスタマイズの詳細については、保存したレポートの管理, （202 ページ）を参照してください。

（注） 固定された列は青色のフォントで表示され、使用可能な列には移動できません。

Rogue Client Location Density

このレポートには、フィルタリング基準に基づいてMSE で検出されたRogue Client Location Density が示されます。

ここでは、次の内容について説明します。

Tag Location Tracking

このレポートには、MSE によって検出されたタグの Tag Location Tracking が表示されます。

ここでは、次の内容について説明します。

Tag Location Tracking の設定

ここでは、Tag Location Tracking レポートの設定方法について説明します。内容は次のとおりです。

Settings

- [Report Title]：このレポートを保存する場合は、レポート名を入力します。
- Report by
  - MSE By Floor Area
  - MSE By Outdoor Area
  - MSE
- [Report Criteria]：レポート基準は、選択した [Report By] オプションによって異なります。[Edit] をクリックして、必要なフィルタ基準を選択します。

（注） [Report Criteria] ページで、[Select] をクリックしてフィルタ基準を確認するか、[Close] をクリックして前のページに戻ります。

- Reporting Period
  - オプション ボタンを選択して、ドロップダウン リストから期間を選択します。

    または
  - [From] オプション ボタンを選択して、開始日時と終了日時を入力します。 テキスト ボックスに日付を入力するか、**カレンダー** アイコンをクリックして日付を選択できます。 ドロップダウン リストから時間と分を選択します。

（注） レポート期間は、アラームの最終検出時刻に基づいています。 時間は UTC タイム ゾーンです。

スケジュール

このレポートを後で実行するか、繰り返しのレポートとして実行する場合は、スケジューリング パラメータを入力します。 レポートのスケジュールの詳細については、保存したレポートの管理, （202 ページ）を参照してください。

レポートのカスタマイズ フォーム

[Customize Report form] では、レポート結果をカスタマイズできます。 レポート結果のカスタマイズの詳細については、保存したレポートの管理, （202 ページ）を参照してください。

（注） 固定された列は青色のフォントで表示され、使用可能な列には移動できません。

Tag Location Tracking の結果

Tag Location Tracking レポートの結果には、次の情報が含まれます。

- [Last Located]：選択した [Report Time] 基準内にタグが最後に検出された時間。
- [Tag Location]：検出された時間のタグの位置。
- [MSE]：このタグを検出した MSE の名前。
- [Detecting Controller]：検出中のコントローラの IP アドレス。
- [Vendor]：タグ ベンダーの名前。
- [Battery Status]：このタグのバッテリ ステータス。

（注） このレポートのロケーション フィールドはハイパーリンクであり、そのハイパーリンクをクリックすると、検出された時間のフロア マップでのタグのロケーションが表示されます。

デバイス使用率レポートの作成

Mobility Services Engine のデバイス使用率レポートを作成するには、次の手順を実行します。

ステップ 1 [Reports] > [Report Launch Pad] の順に選択します。
ステップ 2 [Device] > [Utilization] の順に選択します。
ステップ 3 [New] をクリックします。 [Utilization Report Details] ページが表示されます。
ステップ 4 [Report Details] ページで、次の [Settings] パラメータを入力します。

（注）　一部のパラメータは、レポートタイプによっては機能することも、機能しないこともあります。

- [Report Title]：このレポートを保存する場合は、レポート名を入力します。
- [Report Type]：デフォルトでは、レポート タイプは MSE が選択されます。
- [Report By]：ドロップダウン リストから該当する [Report By]（レポート単位）のカテゴリを選択します。 カテゴリはレポートごとに異なります。 各レポートの [Report By] カテゴリについては、特定のレポートの項を参照してください。
- [Report Criteria]：このパラメータを指定すると、事前に選択した [Report By] に応じて、結果をソートできます。 [Edit] をクリックして、[Filter Criteria] ページを開きます。
- [Connection Protocol]：[All Clients]、[All Wired (802.3)]、[All Wireless (802.11)]、[802.11a/n]、[802.11b/g/n]、[802.11a]、[802.11b]、[802.11g]、[802.11n (5-GHz)]、または [802.11n (2.4-GHz)] からいずれかのプロトコルを選択します。
- [SSID]：[All SSIDs] がデフォルト値です。
- [Reporting Period]：時間単位、週単位、または特定の日時にデータを収集するようにレポートを定義できます。 選択したレポート期間のタイプは、x 軸に表示されます。

（注）　レポート期間には、12 時間表記ではなく 24 時間表記が使用されます。 たとえば、午後 1 時の場合は、**13 時**を選択します。

ステップ 5　[Schedule] グループ ボックスで、[Enable Schedule] チェックボックスをオンにします。

ステップ 6　[Export Report] ドロップダウン リストから、レポート形式（[CSV] または [PDF]）を選択します。

ステップ 7　レポートの保存先として、[File] または [Email] を選択します。

- [File] オプションを選択する場合は、先に [Administration] > [Settings] > [Report] ページで保存先パスを定義しておく必要があります。 [Repository Path] テキスト ボックスに、ファイルの保存先パスを入力します。
- [Email] オプションを選択する場合は、目的の電子メール アドレスを入力する前に、SMTP メール サーバを定義しておく必要があります。 [Administrator] > [Settings] > [*Mail Server Configuration*] の順に選択して、適切な情報を入力します。

ステップ 8　開始日（MM:DD:YYYY）を入力するか、[Calendar] アイコンをクリックして日付を選択します。

ステップ 9　[hour] と [minute] のドロップダウン リストを使用して開始時刻を指定します。

ステップ 10　[Recurrence] オプション ボタンを選択して、レポートの実行頻度を決定します。 指定できる値には次があります。

- No Recurrence
- Hourly
- Daily
- Weekly
- Monthly

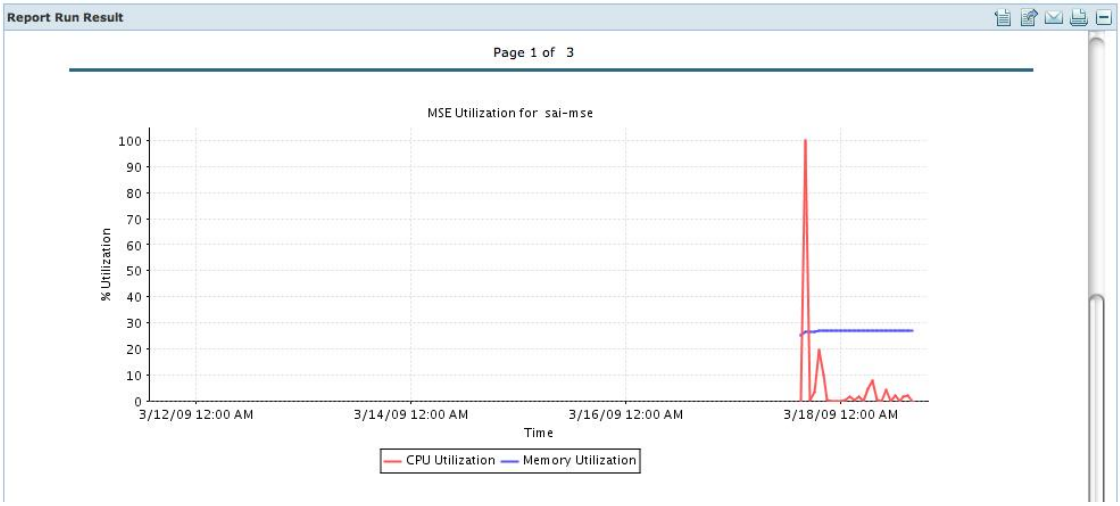
（注） 曜日は [Weekly] オプションを選択した場合のみページ上に表示されます。

ステップ 11 ステップ 1 から デバイス使用率レポートの作成 を終了したら、次のいずれかを実行します。

- [Save] をクリックして編集を保存します。 指定した時刻にレポートが実行され、[Schedule] グループ ボックスでの定義に従い、結果が電子メールで送信されるか、保存先ファイルに保存されます。
- [Save and Run] をクリックして、変更内容を保存し、レポートをすぐに実行します。 レポートは、そのレポートのスケジュールされた実行が保留中であっても実行されます。 結果はページの一番下に表示されます。 レポートは指定した時刻にも実行され、[Schedule] グループ ボックスでの定義に従い、結果が電子メールで送信されるか、保存先ファイルに保存されます。
  - 結果のページで、[Cancel] をクリックして、定義済みのレポートをキャンセルします。
- レポートをすぐに実行して結果を [Prime Infrastructure] ページで確認するには、[Run Now] をクリックします。 レポートは、そのレポートのスケジュールされた実行が保留中であっても実行されます。 結果はページの一番下に表示されます。 入力したレポート条件を保存する場合は [Save] をクリックします。

（注） [Run Now] をクリックして、保存する前に定義済みのレポート条件を確認したり、必要に応じてレポートを実行したりすることもできます。 次の例には、CPU とメモリの使用率レポートのみ表示されています。

図 8：***[Devise] > [MSE Utilization] > [Results]***



スケジュールされているレポートは、「enabled」として表示され、次の実行スケジュール日が表示されます。

実行済みで次の実行がスケジュールされていないレポートは、「expired」として表示されます。

実行済みで再度実行するようにスケジュールされているレポートは、「disabled」として表示されます。

ステップ 12 レポートを有効化、無効化、または削除するには、そのレポートタイトルの隣にあるチェックボックスをオンにして、適切なオプションをクリックします。

保存した使用率レポートの表示

保存したレポートをダウンロードするには、次の手順を実行します。

ステップ 1 [Reports] > [Saved Reports] の順に選択します。

ステップ 2 レポートの [Download] アイコンをクリックします。 レポートがダウンロードされ、定義済みのディレクトリに保存されるか、電子メールで送信されます。

スケジュールされた使用率の実行の表示

スケジュールされたレポートのステータスを確認するには、次の手順を実行します。

ステップ 1 [Reports] > [Scheduled Runs] の順に選択します。

ステップ 2 [History] アイコンをクリックして、レポートの最終実行日を確認します。

ステップ 3 レポートの [Download] アイコンをクリックします。 レポートがダウンロードされ、定義済みのディレクトリに保存されるか、電子メールで送信されます。

OUI の管理

Prime Infrastructure では、IEEE 組織固有識別子（OUI）データベースを使用してクライアント ベンダー名マッピングが識別されます。 Prime Infrastructure では、ベンダー OUI マッピングは、vendorMacs.xml という名前の XML ファイルに保存されます。 OUI の更新により、以下を実行できます。

- 既存の OUI のベンダー表示名の変更。
- Prime Infrastructure への新しい OUI の追加。
- 新しいベンダー OUI マッピングによる vendorMacs.xml ファイルの更新、および Prime Infrastructure へのそのファイルのアップロード。

ここでは、次の内容について説明します。

新しいベンダー OUI マッピングの追加

[User Defined OUI List] ページに、作成したベンダー OUI マッピングのリストが表示されます。 このページで、新しいベンダー OUI マッピングの追加、OUI エントリの削除、および vendorMacs.xml ファイルに存在する OUI のベンダー名の更新を実行できます。

OUI を追加すると、Prime Infrastructure は vendorMacs.xml ファイルを調べて OUI があるかどうかを確認します。 OUI がある場合、Prime Infrastructure は OUI のベンダー名を更新します。 OUI がない場合、Prime Infrastructure はベンダー OUI マッピングに新しい OUI エントリを追加します。

新しいベンダー OUI マッピングを追加するには、次の手順に従います。

ステップ 1 [Administration] > [System Settings] の順に選択します。

ステップ 2 左側のサイドバーのメニューから、[User Defined OUI] を選択します。 [User Defined OUI] ページが表示されます。

ステップ 3 [Select a command] ドロップダウン リストから、[Add OUI Entries] を選択し、[Go] をクリックします。

ステップ 4 [OUI] フィールドに有効な OUI を入力します。 形式は aa:bb:cc です。

ステップ 5 [Check] をクリックして、OUI がベンダー OUI マッピングに存在するかどうかを確認します。

ステップ 6 [Name] フィールドに、OUI のベンダーの表示名を入力します。

ステップ 7 [Change Vendor Name] チェックボックスをオンにして、OUI がベンダー OUI マッピングに存在する場合に、ベンダーの表示名を更新します。

ステップ 8 [OK] をクリックします。

ステップ 9 新しい OUI を追加した後、変更を有効にするには Prime Infrastructure サーバを再起動する必要があります。 Prime Infrastructure サーバをシャット ダウンして再起動するには、次のコマンドを使用できます。

- サービスを停止するには、ncs stop コマンドを使用します。
- サービスを再起動するには、ncs start コマンドを使用します。

更新されたベンダー OUI マッピング ファイルのアップロード

cisco.com に掲載されている vendorMacs.xml ファイルをダウンロードして、同じファイル名（vendorMacs.xml）でローカル ディレクトリに保存できます。 その後、このファイルを Prime Infrastructure にアップロードできます。 Prime Infrastructure は、既存の vendorMacs.xml ファイルを

アップロードされたファイルに置き換えて、ベンダー OUI マッピングを更新します。ただし、新しいベンダー OUI マッピングまたはユーザが行ったベンダー名の更新は上書きされません。

更新されたベンダー OUI マッピング ファイルをアップロードするには、次の手順に従います。

ステップ 1 [Administration] > [System Settings] の順に選択します。

ステップ 2 左側のサイドバーのメニューから、[Upload OUI] を選択します。[Upload OUI From File] ページが表示されます。

ステップ 3 Cisco.com からダウンロードした vendorMacs.xml ファイルを参照し、選択します。

ステップ 4 [OK] をクリックします。

ワイヤレス クライアントのモニタリング

ここでは、ワイヤレス クライアントのモニタリングについて説明します。内容は次のとおりです。

マップを使用したワイヤレス クライアントのモニタリング

Prime Infrastructure マップでは、クライアントが関連付けられたアクセス ポイントの名前、IP アドレス、アセット情報、認証、SSID、802.11 プロトコル、およびクライアントのロケーション情報が最後に更新された時間を表示できます。この情報を表示するには、マップのクライアント アイコンの上にマウス カーソルを置きます。

また、そのクライアントの統計情報（クライアント関連付け、クライアント RSSI、およびクライアント SNR など）、送信したパケットの値および受信したパケットの値、イベント、およびセキュリティ情報を提供する、クライアントの詳細ページを表示することもできます。

マップでクライアントのロケーション ステータスを判別し、マップを使用してクライアントの詳細ページを表示するには、次の手順に従ってください。

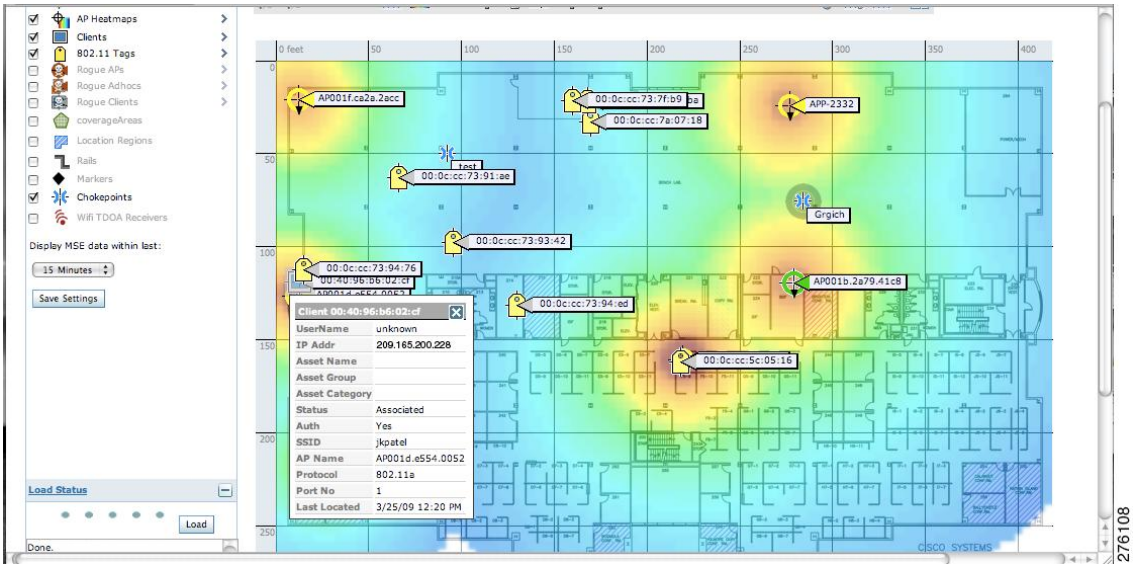
ステップ 1 [Monitor] > [Site Maps] を選択します。

ステップ 2 Mobility Services Engine およびクライアントが検出されたビルディングとフロアを選択します。

ステップ 3 まだ選択していない場合は、[Floor Settings] の左側のサイド バーのメニューで [Clients] チェックボックスをオンにします。

すべてのマップに対してフロア設定に加えた変更を保存しない場合には、[Save Settings] をクリックしないでください。

図 *9*：*[Monitor] > [Maps] > [Building] > [Floor Page]*



（注） マップには、関連付けられたクライアントだけがデフォルトで表示されます。 すべての状態のクライアントを表示するには、[show all clients] オプションを選択します。

（注） マップには、直前の 15 分間に表示されたクライアントが表示されます。 この値は、[Maps] ページの左側のサイド バーのメニューのドロップダウン リストを使用して変更できます。

ステップ 4 クライアント アイコン（青色の四角形）の上にマウス カーソルを移動すると、設定の概要がポップアップ ダイアログボックスで表示されます。

（注） 概要ダイアログボックスでクライアントのカスタム メモを入力できます。 [Client Details] ページでは編集が可能です。

ステップ 5　クライアントの詳細を表示するには、[Client] アイコンをクリックします。

図 *10*：*[Client Details]* ページ（*1/2*）

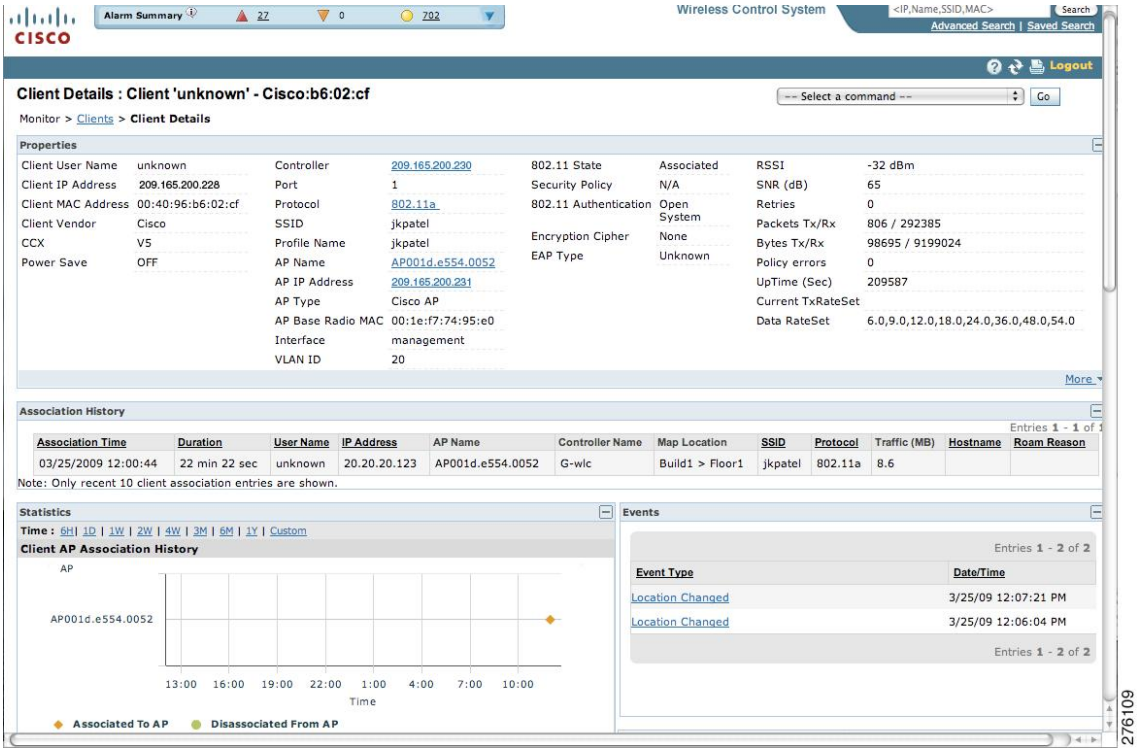
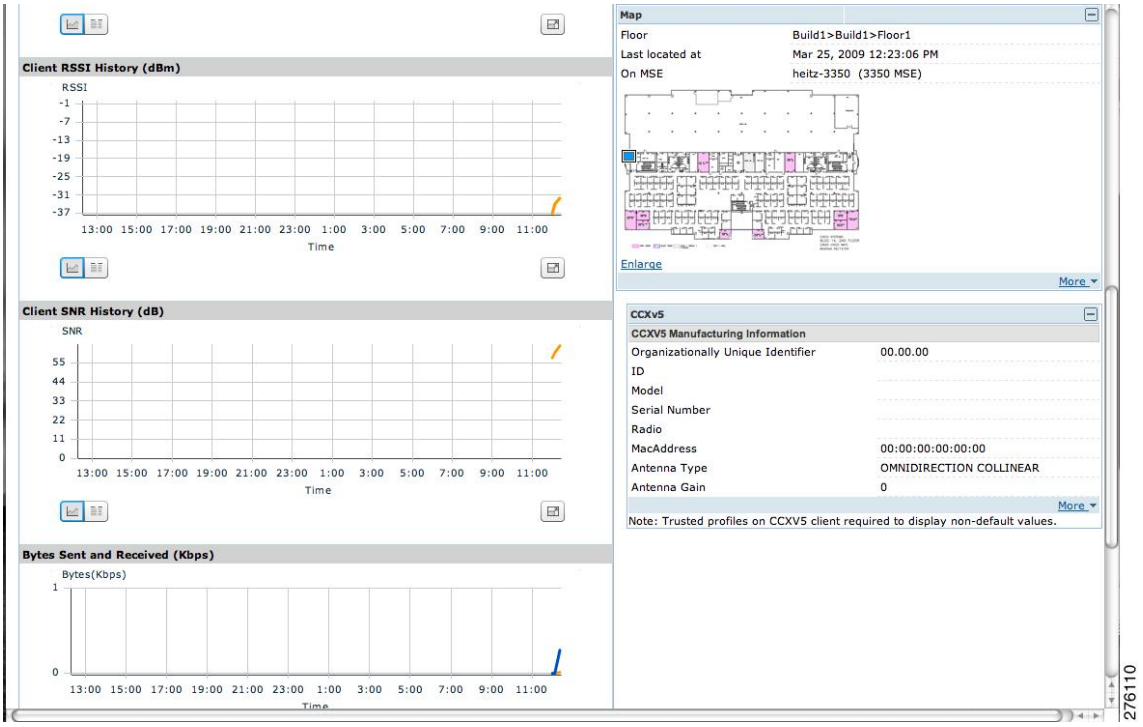


図 *11*：*[Client Details]* ページ（*2/2*）



ステップ 6　クライアントのアセット情報を設定するには、[More] リンクをクリックします。

検索を使用したワイヤレス クライアントのモニタリング

はじめる前に

[Monitor] > [Clients] ページと [Maps] ページ（[Monitor] > [Maps]）内で、クライアント情報の概要と詳細を表示できます。
クライアント情報を表示するには、次の手順を実行します。

ステップ 1　[Monitor] > [Clients] を選択します。
[Clients] 要約ページが表示されます。

ステップ 2　[Show] ドロップダウン リストから、[Clients Detected by MSEs] を選択します。 [Go] をクリックします。
Mobility Services Engines が検出した全クライアントおよび Prime Infrastructure が管理するロケーション アプライアンスの概要が表示されます。（図 11-6 を参照）。 MSE が検出するクライアントは、有線クライアントと無線クライアントを合わせたものです。

ロケーション情報は、無線クライアントのみ MSE に保存され、有線クライアントでは保存されません。このため、仮想ドメインによってクライアントをフィルタリングするには、有線クライアントを表示する

ために所定の仮想ドメインでスイッチをフロアに割り当てる必要があります。割り当てないと無線クライアントのみがここにリストされます。

（注） クライアントに複数の IP アドレスがアソシエートされている場合でも、情報を確認するためにそのクライアントの上にカーソルを移動した場合、1 つの IP アドレスのみ表示されます。 詳細ページには、すべての IP アドレスが表示されます。 表示されるクライアントは、クライアントに設定できる複数の IP アドレス（全体または一部）のいずれかを使用してフィルタリングすることもできます。 表示される IP アドレスは、検索文字列と最も一致しているものです。

a) IP アドレス、名前、SSID、または MAC アドレスで特定のクライアントを見つけるには、ナビゲーション バーの [Search] テキスト ボックスにその値を入力します（すべてのクライアントにすべての検索値が適用されるわけではありません）。
たとえば、[Search] テキスト ボックスに MAC アドレスを入力すると、次のページが表示されます。

b) クライアントに関するその他の設定の詳細を表示するには、クライアント項目タイプの [View List] をクリックします。 表示される詳細には、関連付けられたデバイス（アクセス ポイント、コントローラ）、マップのロケーション、VLAN、プロトコル、および認証タイプが含まれます。

c) クライアントのアラームを表示するには、アラーム項目タイプの [View List] をクリックします。 重大度、障害の発生元（アラームの説明）、アラームの所有者（割り当てられている場合）、アラームの日時、アラームが認知されているかどうかを示す、そのクライアントのアクティブなすべてのアラームのリスト。

（注） [Select a command] ドロップダウン リストから該当するオプションを選択することで、このページでアラームの割り当てまたは割り当て解除、電子メール送信、削除またはクリア、認知と認知の解除を行うこともできます。

d) デバイス、ネットワーク、マップのロケーション、およびクライアントのタイプ（通常、不正、または回避）別にクライアントまたは複数のクライアントを検索するには、[Advanced Search] リンクをクリックします。
[Search By] ドロップダウン リストを使用して、すべてのクライアント、すべての除外クライアント、すべての有線ゲスト クライアント、ログインしているすべてのクライアントによって、クライアント カテゴリをさらに定義できます。

適切なクライアントをクリックします。

MSE でのクライアントのサポート

Prime Infrastructure の Advanced Search 機能を使用して、特定のカテゴリおよびフィルタに基づいて、クライアント リストを絞り込むことができます。[Show] ドロップダウン リストを使用して、現在のリストをフィルタリングすることもできます。

ここでは、次の内容について説明します。

- IPv6 アドレスによる MSE 上の Prime Infrastructure のワイヤレス クライアントの検索
- MSE で検出されたクライアントの表示

IPv6 アドレスによる MSE 上の Prime Infrastructure のワイヤレス クライアントの検索

Prime Infrastructure の Advanced Search 機能を使用して、MSE の配置されたクライアントを検索するには、次の手順に従います。

ステップ 1 Prime Infrastructure UI の右上隅にある [Advanced Search] をクリックします。

ステップ 2 [New Search] ダイアログで、[Search Category] ドロップダウン リストから検索カテゴリとして [Clients] を選択します。

ステップ 3 [Media Type] ドロップダウン リストから、[Wireless Clients] を選択します。

（注） メディア タイプとして [Wireless Clients] を選択した場合だけ、[Wireless Type] ドロップダウン リストが表示されます。

ステップ 4 [Wireless Type] ドロップダウン リストから、[All]、[Lightweight]、または [Autonomous Clients] のうちいずれかのタイプを選択します。

ステップ 5 [Search By] ドロップダウン リストから、[IP Address] を選択します。

（注） IP アドレスによるクライアントの検索は、IP アドレス全体または一部を対象にできます。 各クライアントは、最大 16 個の IPv6 アドレスと 4 個の IPv4 アドレスを持つことができます。

ステップ 6 [Clients Detected By] ドロップダウン リストから、[clients detected by MSE] を選択します。
コントローラと直接通信することで、MSE の Context-Aware Service で検索されるクライアントが表示されます。

ステップ 7 [Last detected within] ドロップダウン リストから、クライアントが検出された時間帯を選択します。

ステップ 8 [Client IP Address] テキスト ボックスにクライアント IP アドレスを入力します。 IPv6 アドレスの一部または全体を入力できます。

（注） IPv4 アドレスを使用して、MSE 上で Prime Infrastructure のクライアントを検索している場合は、[Client IP Address] テキスト ボックスに IPv4 アドレスを入力します。

ステップ 9 [Client States] ドロップダウン リストから、クライアントの状態を選択します。 ワイヤレス クライアントに指定できる値は、[All States]、[Idle]、[Authenticated]、[Associated]、[Probing]、または [Excused] です。 有線クライアントに指定できる値は、[All States]、[Authenticated]、および [Associated] です。

ステップ 10 [Posture Status] ドロップダウン リストからポスチャ ステータスを選択すると、デバイスがクリーンであるかどうかを判別します。 指定できる値は、[All]、[unknown]、[Passed]、および [Failed] です。

ステップ 11 [CCX Compatible] チェックボックスをオンにすると、Cisco Client Extensions と互換性のあるクライアントを検索します。 指定できる値は、[All Versions]、[V1]、[V2]、[V3]、[V4]、[V5]、および [V6] です。

ステップ 12 [E2E Compatible] チェックボックスをオンにすると、エンドツーエンドの互換性のあるクライアントを検索します。 指定できる値は、[All Versions]、[V1]、および [V2] です。

ステップ 13 [NAC State] チェックボックスをオンにすると、特定のネットワーク アドミッション コントロール（NAC）の状態で特定されるクライアントを検索します。 指定可能な値は、[Quarantine]、[Access]、[Invalid]、および [Not Applicable] です。

ステップ 14 [Include Disassociated] チェックボックスをオンにすると、ネットワーク上には存在しなくなったが、Prime Infrastructure には履歴レコードが残っているクライアントが含まれます。

ステップ 15 [Items per page] ドロップダウン リストから、検索結果ページに表示するレコードの数を選択します。

ステップ 16 [Save Search] チェックボックスをオンにして、選択した検索オプションを保存します。

ステップ 17 [Go] をクリックします。
[Clients and Users] ページに、MSE で検出されたすべてのクライアントが表示されます。

MSE で検出されたクライアントの表示

MSE で検出されたすべてのクライアントを表示するには、次の手順を実行します。

ステップ 1 [Monitor] > [Clients and Users] を選択して、有線クライアントとワイヤレス クライアントの両方の情報を表示します。
[Client and Users] ページが表示されます。

[Clients and Users] 表にはデフォルトでいくつかの列が表示されます。 使用可能な列を追加して表示する場合は、 をクリックし、[Columns] をクリックします。 使用可能な列が表示されます。 [Clients and Users] 表に表示する列を選択します。 列内の任意の場所をクリックすると、その列が選択され、クライアントの詳細が表示されます。

ステップ 2 [Show] ドロップダウン リストから [Clients detected by MSE] を選択して、現在のリストをフィルタリングし、MSE で検出されるクライアントをすべて選択します。
有線およびワイヤレスを含め、MSE で検出されたすべてのクライアントが表示されます。 有線およびワイヤレスを含め、MSE で検出されたすべてのクライアントが表示されます。

[Clients Detected by MSE] 表では、次のさまざまなパラメータを使用できます。

- [MAC Address]：クライアント MAC アドレス。

- [IP Address]：クライアント IP アドレス。

  [IP Address] 列に表示される IP アドレスは、定義済みの優先順位によって決まります。 使用可能な最初の IP アドレスが次の順番で [IP address] テキスト ボックスに表示されます。

  - IPv4 アドレス

    （注） このリリースでは、ワイヤレス クライアントだけが IPv6 アドレスを使用します。各クライアントは、最大 16 個の IPv6 アドレスと 4 個の IPv4 アドレスを持つことができます。

  - IPv6 グローバル固有アドレス。 このタイプのアドレスが複数ある場合は、クライアントが受信した最新の IPv6 アドレスが表示されます。ユーザがグローバル IPv6 アドレスを 2 つ持っていても、どちらかが期限切れになっている古いルータ アドバタイズメントによって取得したアドレスである場合があるためです。

  - IPv6 ローカル固有アドレス。複数ある場合は、最新の IPv6 ローカル固有アドレスがクライアントによって使用されます。

  - IPv6 リンク ローカル アドレス。 他の IPv6 アドレスが割り当てられる前に、セルフアサインされ、通信に使用されるクライアントの IPv6 アドレス。

    次のようなさまざまな IPv6 アドレス タイプがあります。

  - リンクローカルユニキャスト：リンクローカルアドレスは、自動アドレス設定、ネイバー探索、ルータが存在しないときなどのために、単一リンクでのアドレス指定に使用するように設計されています。

  - サイトローカル ユニキャスト：サイトローカル アドレスは、グローバル プレフィックスには必要のない、サイト内部でのアドレス指定に使用するように設計されています。

  - 集約可能グローバルユニキャスト：集約可能グローバルユニキャストアドレスは、グローバル ネットワーク内でクライアントを一意に特定します。パブリック IPv4 アドレスと同等です。 クライアントは複数の集約可能グローバル ユニキャスト アドレスを持つことができます。

- [IP Type]：クライアントの IP アドレス タイプ。 指定できるのは、IPv4、IPv6、またはデュアル スタック（IPv4 アドレスと IPv6 アドレスの両方があるクライアントを表す）です。

  - グローバル固有

  - 固有ローカル

  - リンク ローカル

- [User Name]：802.1x 認証に基づいたユーザ名。 ユーザ名を使用しないで接続されたクライアントの場合は [Unknown] と表示されます。

- [Type]：クライアント タイプを示します。

- [Vendor]：OUI から導き出されたデバイス ベンダー。

- [Device Name]：ネットワーク認証デバイス名。 たとえば、WLC、スイッチなどです。
- [Location]：接続しているデバイスのマップ位置。
- [VLAN]：このクライアントのアクセス VLAN ID を示します。
- [Status]：現在のクライアントのステータス。
  - [Idle]：正常の動作。クライアントのアソシエーション要求は拒否されていません。
  - [Auth Pending]：AAA トランザクションを実行しています。
  - [Authenticated]：802.11 認証が完了しています。
  - [Associated]：802.11 アソシエーションが完了しています。 これは、現在クライアントがネットワークに接続されていることを示すために有線クライアントでも使用されます。
  - [Disassociated]：802.11 ディスアソシエーションが完了しています。 これは、現在クライアントがネットワーク上に存在しないことを示すために有線クライアントでも使用されます。
  - [To Be Deleted]：ディスアソシエーション後にクライアントが削除されます。
  - [Excluded]：セキュリティの脅威と見なされたため、システムによって自動的に無効化されています。
- [Interface]：クライアントが接続するコントローラ インターフェイス（ワイヤレス）またはスイッチ インターフェイス（有線）。
- プロトコル
  - [802.11]：ワイヤレス
  - [802.3]：有線
- [Association Time]：最後のアソシエーションの開始時間（ワイヤレス クライアントの場合）。 有線クライアントの場合、これは、クライアントがスイッチ ポートに接続した時間です。 クライアントがアソシエートされているが、ネットワーク上で問題がある場合は空欄になります。
- [CCX]：Lightweight ワイヤレスのみ。
  - [Client and User] ページの MAC アドレスの横にあるオプション ボタンを選択して、アソシエートされたクライアント情報を表示します。 次の各クライアント パラメータが表示されます。
- クライアント属性
- クライアント IPV6 アドレス
- クライアント統計情報

（注） クライアントの統計には、クライアント詳細情報の後に統計情報が表示されます。

- クライアント アソシエーション履歴

- クライアント イベント情報
- クライアント ロケーション情報
- 有線ロケーション履歴
- クライアント CCX 情報
- クライアント属性

[Clients and Users] リストからクライアントを選択すると、次のクライアント詳細情報が表示されます。 クライアントは、MAC アドレスを使用して特定されます。

- 全般：次の情報がリストされます。
  - ユーザ名
  - IP Address
  - MAC アドレス
  - ベンダー
  - エンドポイント タイプ
  - クライアント タイプ
  - メディア タイプ
  - モビリティ ロール
  - Hostname
  - E2E
  - ファンデーション サービス
  - 管理サービス
  - 音声サービス
  - ロケーション サービス

- [Session]：次の情報が表示されます。
  - コントローラ名
  - AP 名
  - AP IP アドレス
  - AP タイプ
  - AP ベース無線 MAC
  - アンカー アドレス
  - 802.11 ステート

- アソシエーション ID
- ポート
- インターフェイス
- SSID
- Profile Name
- プロトコル
- VLAN ID
- AP モード

- セキュリティ（ワイヤレス クライアントおよびアイデンティティ有線クライアントのみ）：次のセキュリティ情報をリストします。
  - セキュリティ ポリシー タイプ
  - EAP タイプ
  - ネットワーク上
  - 802.11 認証
  - 暗号化方式
  - SNMP NAC の状態
  - RADIUS NAC の状態
  - AAA Override ACL 名
  - AAA Override ACL の適用された状態
  - リダイレクト URL
  - ACL 名
  - ACL の適用された状態
  - FlexConnect ローカル認証
  - Policy Manager ステート
  - 認証 ISE
  - 認可プロファイル名
  - ポスチャ ステータス
  - TrustSec セキュリティ グループ
  - Windows AD ドメイン

（注） アイデンティティ クライアントは、認証タイプが 802.1x、MAC 認証バイパス、または Web 認証のクライアントです。 アイデンティティ クライアント以外の認証タイプは N/A です。

（注） クライアント属性の下に表示されるデータは、アイデンティティ クライアントかそうでないかによって異なります。アイデンティティ クライアントの場合は、認証ステータス、監査セッション ID などのセキュリティ情報を確認できます。

- [Statistics]（ワイヤレスのみ）
- [Traffic]：クライアントのトラフィック情報を表示します。
- ワイヤレス クライアントの場合、クライアントのトラフィック情報はコントローラから取得します。有線クライアントの場合、クライアントのトラフィック情報はISEから取得するため、スイッチ上でアカウンティング情報およびその他の必要な機能を有効にする必要があります。

統計情報

[Statistics] グループ ボックスには、選択したクライアントの次の情報が含まれます。

- クライアント AP アソシエーション履歴。
- クライアント RSSI 履歴（dBm）：クライアントがアソシエートされたアクセス ポイントで検出された RSSI（受信信号強度インジケータ）の履歴。
- クライアント SNR 履歴：クライアントがアソシエートされたアクセス ポイントで検出された SNR（クライアント RF セッションの信号対雑音比）の履歴。
- 送受信バイト（Kbps）：アソシエートされたアクセス ポイントで送受信したバイト数。
- 送受信パケット（毎秒）：アソシエートされたアクセス ポイントで送受信したパケット数。
- クライアントのデータ レート

この情報は、インタラクティブ グラフで表示されます。

クライアント IPV6 アドレス

[Client IPv6 Address] グループ ボックスには、選択したクライアントの次の情報が含まれます。

- IP アドレス：クライアント IPv6 アドレスを表示します。
- スコープ：グローバル固有、ローカル固有、およびリンク ローカルの 3 つのスコープ タイムがあります。
- アドレス タイプ：アドレス タイプを表示します。
- 検出時間：IP が検出された時間です。

アソシエーション履歴

[Association History] グループ ボックスには、選択したクライアントの過去 10 件のアソシエーション時間に関する情報が表示されます。 この情報は、クライアントのトラブルシューティングの際に役立ちます。

- アソシエーション時間
- 持続時間
- ユーザ名
- IP Address
- IP アドレス タイプ
- AP 名
- コントローラ名
- SSID

Event

[Client Details] ページの [Event] グループ ボックスには、イベント タイプやイベントの日時など、このクライアントのすべてのイベントが表示されます。

- イベント タイプ
- イベント時間
- 説明

マップ

[View Location History] をクリックすると、有線クライアントおよびワイヤレス クライアントのロケーション履歴の詳細が表示されます。

有線クライアントまたはワイヤレス クライアントの次のロケーション履歴情報が表示されます。

- Timestamp
- 状態
- ポート タイプ
- スロット
- Module
- ポート
- ユーザ名
- IP Address
- スイッチ IP
- サーバ名
- マップ位置の都市ロケーション

ビルディングの設定

キャンパス マップをデータベースに追加したことがあるかどうかに関係なく、ビルディングを Prime Infrastructure データベースに追加できます。 ここでは、ビルディングをキャンパス マップに追加する方法、または独立したビルディング（キャンパスの一部ではないビルディング）を Prime Infrastructure データベースに追加する方法を説明します。

ここでは、次の内容について説明します。

キャンパス マップへのビルディングの追加

Prime Infrastructure データベース内のキャンパス マップにビルディングを追加するには、次の手順を実行します。

ステップ 1 [Monitor] > [Site Maps] を選択して、[Maps] ページを表示します。

ステップ 2 目的のキャンパスをクリックします。 [Site Maps] > [Campus Name] ページが表示されます。

ステップ 3 [Select a command] ドロップダウン リストから、[New Building] を選択し、[Go] をクリックします。

ステップ 4 [Campus Name] > [New Building] ページで、関連するフロア図面マップを整理するために架空のビルディングを作成するには、次の手順を実行します。

a) ビルディング名を入力します。

b) ビルディング問い合わせ先の名前を入力します。

c) 地上のフロア数と地下のフロア数を入力します。

d) 水平位置（ビルディングの四角形の隅からキャンパス マップの左端までの距離）と垂直位置（ビルディングの四角形の隅からキャンパス マップの上端までの距離）をフィート単位で入力します。

（注） 測定単位（フィートまたはメートル）を変更するには、[Monitor] > [Site Maps] を選択して、[Select a command] ドロップダウン リストから [Properties] を選択します。

e) ビルディングのおおまかな水平方向スパンと垂直方向スパン（マップ上の幅と奥行き）をフィート単位で入力します。

（注）

水平方向スパンと垂直方向スパンは、後から追加するフロアのサイズと等しいかそれより大きくする必要があります。

ヒント　キャンパス マップの左上にある境界領域のサイズを変更するには、Ctrl キーを押した状態でクリックします。境界領域のサイズを変更すると、ビルディングの水平方向スパンおよび垂直方向スパンのパラメータも操作に応じて変わります。

f) [Place] をクリックして、ビルディングをキャンパス マップ上に配置します。 Prime Infrastructure では、キャンパス マップのサイズに合わせてサイズ変更されたビルディングの四角形が作成されます。

g) ビルディングの四角形をクリックして、キャンパス マップ上の目的の位置までドラッグします。

（注）　新しいビルディングを追加した後で、このビルディングをあるキャンパスから別のキャンパスに移動するときも、ビルディングを再作成する必要はありません。

h) [Save] をクリックして、このビルディングとキャンパス上の位置をデータベースに保存します。 Prime Infrastructure では、キャンパス マップ上のビルディングの四角形の中にビルディング名が保存されます。

（注）　ビルディングには、該当する [Map] ページに移動するためのハイパーリンクが関連付けられます。

ステップ 5　（任意）新しい屋外領域に位置プレゼンス情報を割り当てる手順は、次のとおりです。

a) [Select a command] ドロップダウン リストから、[Edit Location Presence Info] を選択します。 [Go] をクリックします。 [Location Presence] ページが表示されます。

（注）　デフォルトでは、[Override Child Element] の [Presence Info] チェックボックスがオンになっています。キャンパスのロケーションをそのキャンパス上のすべてのビルディングおよびフロアに伝播する場合は、このオプションをオンのままにしておいてください。キャンパス マップにビルディングを追加する際は、キャンパスのロケーション情報をインポートできます。チェックボックスがオフの場合は、キャンパスの住所をビルディングにインポートできません。 1 つのキャンパスの住所をすべてのビルディングに割り当てるのではなく、ビルディング固有の住所をそのキャンパス上のビルディングに割り当てる場合は、このオプションをオフのままにしておいてください。

b) [Civic Address] タブ、または [Advanced] タブをクリックします。

- [Civic Address] では、名前、通り、住所番地、住居番地詳細、市（address line2）、州、郵便番号、そして国によってキャンパスを特定します。
- [Advanced] では、近隣、区、国、郵便のコミュニティ名など、Civic の拡張情報でキャンパスを特定します。

c) デフォルトでは、[Override Child's Presence Information] チェックボックスはオンになっています。 独立したビルディングについては、この設定を変更する必要はありません。

ステップ 6　[Save] をクリックします。

独立したビルディングの追加

Prime Infrastructure データベースに独立したビルディングを追加するには、次の手順を実行します。

ステップ 1 [Monitor] > [Site Maps] を選択して、[Maps] ページを表示します。

ステップ 2 [Select a command] ドロップダウン リストから、[New Building] を選択し、[Go] をクリックします。

ステップ 3 [Maps] > [New Building] ページで、関連するフロア図面マップを整理するために架空のビルディングを作成するには、次の手順を実行します。

a) ビルディング名を入力します。

b) ビルディング問い合わせ先の名前を入力します。

（注） 新しいビルディングを追加した後で、このビルディングをあるキャンパスから別のキャンパスに移動するときも、ビルディングを再作成する必要はありません。

c) 地上のフロア数と地下のフロア数を入力します。

d) ビルディングのおおまかな水平方向スパンと垂直方向スパン（マップ上の幅と奥行き）をフィート単位で入力します。

（注） 測定単位（フィートまたはメートル）を変更するには、[Monitor] > [Site Maps] を選択して、[Select a command] ドロップダウン リストから [Properties] を選択します。

（注） 水平方向スパンと垂直方向スパンは、後から追加するフロアのサイズと等しいかそれより大きくする必要があります。

e) [OK] をクリックして、このビルディングをデータベースに保存します。

ステップ 4 （任意）新しいビルディングに位置プレゼンス情報を割り当てる手順は、次のとおりです。

a) [Select a command] ドロップダウン リストから、[Location Presence] を選択します。 [Go] をクリックします。 [Location Presence] ページが表示されます。

b) [Civic] タブ、[GPS Markers] タブ、または [Advanced] タブをクリックします。

- [Civic Address] では、名前、通り、住所番地、住居番地詳細、市（address line2）、州、郵便番号、そして国によってキャンパスを特定します。
- [GPS Markers] では、経度と緯度でキャンパスを特定します。
- [Advanced] では、近隣、区、国、郵便のコミュニティ名など、Civic の拡張情報でキャンパスを特定します。

（注） 選択した各パラメータには、上記のすべてが含まれています。 たとえば、[Advanced] を選択した場合、ユーザからの要求により GPS および Civic 位置情報も提供されます。選択した設定は、ロケーション サーバ レベルでの設定（[Services] > [Mobility Services]）と一致する必要があります。

（注） クライアントが、キャンパスに対して GPS Markers パラメータで設定されていないビルディング、フロア、または屋外領域などの位置情報を要求した場合、エラー メッセージが返されます。

c) デフォルトでは、[Override Child Element] の [Presence Info] チェックボックスがオンになっています。キャンパスのロケーションをそのキャンパス上のすべてのビルディングおよびフロアに伝播する場合は、このオプションをオンのままにしておいてください。 キャンパス マップにビルディングを追加する際は、ロケーション情報をインポートできます。 チェックボックスがオフの場合は、キャンパスの住所をビルディングにインポートできません。 1 つのキャンパスの住所をすべてのビルディングに割り当てるのではなく、ビルディング固有の住所をそのキャンパス上のビルディングに割り当てる場合は、このオプションをオフのままにしておいてください。

ステップ 5 [Save] をクリックします。

（注） 独立したビルディングは、システム キャンパス内に自動的に配置されます。

ビルディングの表示

現在のビルディング マップを表示するには、次の手順を実行します。

ステップ 1 **Monitor** > **[Site Maps]** を選択します。.

ステップ 2 ビルディング マップの名前をクリックして、詳細ページを開きます。 [Building View] ページには、各フロアのフロア マップの一覧とマップの詳細が表示されます。

（注） [Building View] ページの [Floor] 列見出しをクリックして、一覧をフロアの昇順または降順にソートできます。

マップの詳細には、次の情報が含まれます。

- フロア領域
- フロア インデックス：フロア レベルを示します。 マイナスの数は地下のフロア レベルを示します。
- Contact
- ステータス：このマップ上に配置されているアクセス ポイントまたは子のアクセス ポイントで、重大度の最も高いアラームを示します。
- マップに配置されているアクセス ポイントの総数。
- マップに配置されている 802.11a/n 無線および 802.11b/g/n 無線の数。
- 停止している（OOS）無線の数。
- クライアント数：数字のリンクをクリックすると、[Monitor] > [Clients] ページが表示されます。

ステップ 3 [Select a command] ドロップダウン リストには、次のオプションが表示されます。

- [New Floor Area]：詳細については、キャンパス マップへのビルディングの追加, （239 ページ）を参照してください。

- [Edit Building]：詳細については、ビルディングの編集, （243 ページ） を参照してください。
- [Delete Building]：詳細については、ビルディングの削除, （243 ページ） を参照してください。

ビルディングの編集

現在のビルディング マップを編集するには、次の手順を実行します。

ステップ 1 [Monitor] > [Site Maps] を選択します。

ステップ 2 ビルディング マップの名前をクリックして、詳細ページを開きます。

ステップ 3 [Select a command] ドロップダウン リストから [Edit Building] を選択します。

ステップ 4 [Building Name]、[Contact]、[Number of Floors]、[Number of Basements]、および [Dimensions (feet)] に必要な変更を加えます。

（注） 測定単位（フィートまたはメートル）を変更するには、[Monitor] > [Site Maps] を選択して、[Select a command] ドロップダウン リストから [Properties] を選択します。

ステップ 5 [OK] をクリックします。

ビルディングの削除

現在のビルディング マップを削除するには、次の手順を実行します。

ステップ 1 [Monitor] > [Site Maps] を選択します。

ステップ 2 削除するビルディングのチェックボックスをオンにします。

ステップ 3 マップ リスト下部の [Delete] をクリックします（または、[Select a command] ドロップダウン リストから [Delete Maps] を選択して、[Go] をクリックします）。

ステップ 4 [OK] をクリックして、削除を実行します。

（注） ビルディングを削除すると、そのコンテナ マップもすべて削除されます。 削除されるすべてのマップのアクセス ポイントが、未割り当てステートに移行されます。

ビルディングの移動

別のキャンパスにビルディングを移動するには、次の手順を実行します。

ステップ 1 [Monitor] > [Site Maps] を選択します。
ステップ 2 該当するビルディングのチェックボックスをオンにします。
ステップ 3 [Select a command] ドロップダウン リストから [Move Buildings] を選択します。
ステップ 4 [Go] をクリックします。
ステップ 5 ドロップダウン リストから [Target Campus] を選択します。
ステップ 6 移動するビルディングを選択します。 現在のロケーションを維持するビルディングをオフにします。
ステップ 7 [OK] をクリックします。

タグのモニタリング

[Monitor] > [Tags] ページでは、Prime Infrastructure マップでタグ ステータスとロケーションのモニタリングやタグの詳細の確認などができます。 [Advanced Search] を使用してタグをモニタリングすることもできます。

ここでは、次の内容について説明します。

- マップを使用したタグのモニタリング, （244 ページ）
- 検索を使用したタグのモニタリング, （245 ページ）
- 重複タグ, （248 ページ）

マップを使用したタグのモニタリング

Prime Infrastructure マップでは、タグ付きのアセットの信号を生成したアクセス ポイントの名前、その信号の強度、およびアセットのロケーション情報が最後に更新された日時を確認できます。この情報を表示するには、マップのタグ アイコンの上にマウス カーソルを置きます。

マップ上でタグの位置ステータスを有効にするには、次の手順を実行します。

ステップ 1 [Monitor] > [Maps] を選択します。
ステップ 2 Mobility Services Engine およびタグが検出されたビルディングとフロアを選択します。
ステップ 3 まだ選択していない場合は、[Floor Settings] メニューで [802.11 Tags] チェックボックスをオンにします。

（注） すべてのマップに対してフロア設定に加えた変更を保存しない場合には、[Save Settings] をクリックしないでください。

ステップ 4 タグ アイコン（黄色のタグ）の上にマウス カーソルを移動すると、そのタグの設定概要が [Tag] ダイアログボックスに表示されます。

ステップ 5 タグの詳細を表示するには、**タグ** アイコンをクリックします。
また、[Asset Info] グループ ボックスに必要な情報を入力して、アセット情報を設定することもできます。

ステップ 6 タグのロケーション履歴を表示するには、[Select a command] ドロップダウン リストから [Location History] を選択します。 [Go] をクリックします。

検索を使用したタグのモニタリング

アセット タイプ（名前、カテゴリ、およびグループ）、MAC アドレス、システム（コントローラまたは MSE）、および領域（フロア領域および屋外領域）によってタグを検索できます。

[Advanced Search] パラメータを使用して、さらに検索を微調整し、将来使用するために検索条件を保存できます。 保存した検索を取得するには、[Saved Searches] をクリックします。

検索結果ページでタグの場所の MAC アドレスをクリックすると、タグの次の詳細が表示されます。

- タグ ベンダー
- タグが関連付けられているコントローラ
- テレメトリ データ（CCX v1 準拠のタグのみ）
  - 表示されるテレメトリ データはベンダー固有ですが、GPS の場所、バッテリー拡張情報、圧力、温度、湿度、動作、ステータス、および緊急コードなど、いくつかの内容が共通して報告されます。
- 資産情報（名前、カテゴリ、グループ）
- 統計情報（受信したバイトとパケット）
- 場所（フロア、最終場所、MSE、マップ）
- 場所の通知（不在、封じ込め、距離、すべて）
- 緊急データ（CCX v1 準拠のタグのみ）

タグを検索するには、次の手順に従います。

ステップ 1 [Monitor] > [Tags] の順に選択します。 [Tag Summary] ページが表示されます。

ステップ 2 特定の Mobility Services Engine と関連付けられたタグの概要を表示するには、[Total Tags] リンクをクリックします。

（注） Mobility Services Engine またはタグのリストが長い場合は、[Search] または [Advanced Search] を使用して、特定のタグを分離させることができます。

ステップ 3 特定のタグを検索するには、その MAC アドレスとアセット名（すべてのタグにすべての検索値が適用されるわけではありません）がわかっている場合は、[Search] リンクをクリックします。

ステップ 4 デバイス（MSE またはコントローラ）、マップのロケーション（フロアまたは屋外領域）、アセット名またはカテゴリ、またはタグベンダーなどのより広範囲の検索基準を使用して特定のタグまたは複数のタグを検索するには、[Advanced Search] リンクをクリックします。

a) [Advanced Search] ペインで、検索カテゴリとして [Tags] を選択します。

b) 追加のタグの検索基準を選択します。

c) すべての詳細検索パラメータを選択したら、[Go] をクリックします。

（注） 選択した検索条件に基づいてタグが見つからない場合、見つからなかったということ、検索が失敗した理由、および可能なアクションを示すメッセージが表示されます。

表 *24*：タグの検索基準と値

検索基準	可変の検索基準	有効な値
Search for tags by (Tier 1 search criteria)	—	[All Tags]、[Asset Name]、[Asset Category]、[Asset Group]、[MAC Address]、[Controller]、[MSEs]、[Floor Area]、または [Outdoor Area]。 （注） MSE の検索には、ロケーションサーバおよび Mobility Services Engine の両方が含まれます。
Search in (Tier 2 search criteria)	—	MSEs または Prime Infrastructure またはコントローラ。 （注） Prime Infrastructure コントローラオプションは、Prime Infrastructure でコントローラの検索が行われたことを示します。 （注） MSE の検索には、ロケーションサーバおよび Mobility Services Engine の両方が含まれます。
Last detected within	—	オプションは 5 分～ 24 時間です。

検索基準	可変の検索基準	有効な値
Variable search criteria (Tier 3 search criteria) （注） [Search for tabs by (Tier 1 search)] 値によって決定できる検索条件。	[Search for tags by] 値が次の場合： [Asset Name]、次にタグのアセット名を入力します。 [Asset Category]、次にタグのアセット カテゴリを入力します。 [Asset Group]、次にタグのアセット グループを入力します。 [MAC Address]、次にタグの MAC アドレスを入力します。 [Controller]、次にコントローラの IP アドレスを選択します。 [MSEs]、次にドロップダウン リストから MSE の IP アドレスを選択します。 [Floor Area]、次にキャンパス、ビルディング、およびフロア領域を選択します。 [Outdoor Area]、次にキャンパスおよび屋外領域を選択します。	
Telemetry tags only	—	テレメトリ タグを表示するためのチェックボックス。 オプションをオフのままにすると、すべてのタグが表示されます。 （注） [Search In] オプションが [MSE] の場合のみ表示されるオプション。 （注） テレメトリをサポートしているベンダー タグのみが表示されます。
タグ ベンダー	—	ドロップダウン リストからタグ ベンダーを選択するためのチェックボックス。 （注） [Search In] オプションが [MSE] の場合のみ表示されるオプション。
Items per page	—	検索要求ごとに表示するタグの数を選択します。 値の範囲は 10 ～ 500 です。
Save search	—	検索条件に名前を付けて保存するためのチェックボックス。保存したエントリは、[Saved Searches] 見出しの下に表示されます。

重複タグ

複数のタグが相互に隣接する場合、Prime Infrastructure マップ（[Monitor] > [Maps]）でロケーションを表すために、概要タグが使用されます。 概要タグには、そのロケーションにあるタグの数のラベルが付けられます。

マップで重複タグの上にマウス カーソルを移動すると、重複タグの要約情報が示されたダッシュレットが表示されます。

個々のタグ概要のダッシュレット間を移動するには、[Prev] および [Next] リンクを選択します。タグの概要情報を表示しながら特定のタグの詳細情報を表示するには、[Detail] リンクを選択します。

タグの概要情報には、[Tag MAC address]、[Asset Name]、[Asset Group]、[Asset Category]、[Vendor (Type)]、[Battery Life]、および [Last Located data (date and time)] が含まれます。 タグが Cisco CX v.1 準拠の場合、テレメトリ情報も表示されます。

- タグの詳細情報には、関連付けられたコントローラの IP アドレス、統計情報、ロケーション通知、ロケーション履歴、およびロケーションデバッグ機能が有効かどうかが含まれます。
  - タグのロケーション履歴を表示するには、そのオプションを [Select a command] ドロップダウン リストから選択し、[Go] をクリックします。
  - 詳細ページに戻るには、[Select a Command] ドロップダウン リストから [Location History] ページを選択し、[Go] をクリックします。

Geo-Location のモニタリング

MSE は、有線クライアント、有線エンドポイント、スイッチ、コントローラ、ワイヤレス ネットワーク構成内にあるアクセス ポイントの物理ロケーションを提供します。 現在、MSE はノースバウンド エンティティからサウスバウンド エンティティまでの外部エンティティに Geo-Location 形式でロケーション情報を提供しています。

MSE によって提供される Geo-Location 情報の精度を向上するために、この機能によりデバイス位置の座標は Geo-Location 座標（経度と緯度）に変換され、ノースバウンド インターフェイスとサウスバウンド インターフェイスを介して外部エンティティに提供されます。

（注） Geo-Location の計算には、少なくとも 3 つの GPS マーカーが必要です。 追加できる GPS マーカーの最大数は 20 です。

ここでは、次の内容について説明します。

- フロア マップへの GPS マーカーの追加, （249 ページ）
- GPS マーカーの編集, （249 ページ）
- フロアからの GPS マーカーの削除, （250 ページ）

フロア マップへの GPS マーカーの追加

GPS マーカーをフロア マップに追加するには、次の手順を実行します。

ステップ 1 [Monitor] > [Site Maps] を選択して、[Maps] ページを表示します。

ステップ 2 [Campus Name] > [Building Name] > [Floor Name] の順に選択します。

ステップ 3 左上のメニューの [Add/Edit GPS Markers Information] メニュー オプションを選択して、[Add/Edit GPS] ページを表示します。
マップの左上隅（X = 0、Y = 0）に [GPS Marker] アイコンが表示されます.

ステップ 4 [GPS Marker] アイコンをドラッグして、マップ上の希望する場所に配置することができます。また、左側のサイドバー メニューにある [GPS Marker Details] テーブルに X と Y の位置の値を入力して、マーカーを希望する位置に移動することができます。
（注） 追加したマーカーの位置が近すぎると、Geo-Location 情報の精度は低下します。

ステップ 5 左側のサイドバー メニューで選択した [GPS Marker] アイコンの経度と緯度を入力します。

ステップ 6 [Save] をクリックします。
[GPS Marker] の情報がデータベースに保存されます。

ステップ 7 [Apply to other Floors of Building] をクリックして、ビルディングの 1 フロアの GPS マーカーをそのビルディングの残りのすべてのフロアにコピーします。

GPS マーカーの編集

フロアにある GPS マーカーを編集するには、次の手順を実行します。

ステップ 1 [Monitor] > [Site Maps] を選択して、[Maps] ページを表示します。

ステップ 2 [Campus Name] > [Building Name] > [Floor Name] の順に選択します。

ステップ 3 [Add/Edit GPS Markers Information] メニュー オプションを選択して、[Add/Edit GPS] ページを表示します。

ステップ 4 左側のサイドバー メニューから、フロアにある既存の GPS マーカーを選択します。

ステップ 5 左側のサイドバー メニューから、その GPS マーカーにアソシエートされている [Latitude]、[Longitude]、[X Position]、および [Y Position] を変更できます。

ステップ 6 [Save] をクリックします。
これで、変更した GPS マーカーの情報がデータベースに保存されます。

フロアからの GPS マーカーの削除

フロアから GPS マーカーを削除するには、次の手順に従います。

ステップ 1 [Monitor] > [Site Maps] を選択して、[Maps] ページを表示します。

ステップ 2 [Campus Name] > [Building Name] > [Floor Name] の順に選択します。

ステップ 3 [Add/Edit GPS Markers Information] メニュー オプションを選択して、[Add/Edit GPS] ページを表示します。

ステップ 4 左側のサイドバー メニューから、フロアにある既存の GPS マーカーを選択します。

（注） [Multiple GPS Markers] チェックボックスをオンにすることで、フロアにある複数の GPS マーカーを削除できます。

ステップ 5 [Delete GPS Marker] をクリックします。
選択した GPS マーカーがデータベースから削除されます。

チョークポイントのモニタリング

チョークポイントは、モニタするロケーションのマップに割り当てられている必要があります。マップに TDOA レシーバを追加したら、マップに表示するために、ネットワーク設計（[Services] > [Synchronize Services]）を Mobility Services Engine と再同期する必要があります。

新しいチョークポイントが作成されると、すべての仮想ドメインで使用できます。 フロアに配置したあと、フロアと同じ仮想ドメインで使用できるように更新されます。 チョークポイントをフロアから削除すると、すべての仮想ドメインで再び利用可能になります。

既存のチョークポイントがフロアにある場合、すべてフロアと同じ仮想ドメインに属します。チョークポイントがフロアに配置されていない場合、すべての仮想ドメインで使用できます。

チョークポイントがマップに割り当てられていない場合、[Search] または [Advanced Search] を使用してそのチョークポイントを見つけることができません。 すべてのチョークポイント設定は、AeroScout システム マネージャを使用して実行されます。

（注） 設定の詳細については、次の URL にある『AeroScout Context-Aware Engine for Tags, for Cisco Mobility Services Engine Users Guide』を参照してください。http://support.aeroscout.com

チョークポイントをモニタするには、次の手順に従ってください。

ステップ 1 [Monitor] > [Chokepoints] の順に選択します。 すべてのマップされたチョークポイントが示された [Chokepoint] ページが表示されます。

ステップ 2 広範な一覧が表示されたときに検索基準を微調整するには、MAC アドレスまたはチョークポイント名で検索します。

a) MAC アドレスまたはチョークポイント名でチョークポイントの検索を開始するには、[Search] テキスト ボックスにその値を入力します。 [Search] をクリックします。 次に、MAC アドレスによる検索例を示します。 一致が存在しない場合、[Search Results] ページにメッセージが表示されます。

b) MAC アドレスまたは名前でチョークポイントの詳細検索を開始するには、[Advanced Search] リンクをクリックします。

- 検索カテゴリとして [Chokepoint] を選択します。
- [Search for Chokepoint by] ドロップダウン リストから、[Chokepoint Name] または [MAC Address] のいずれかを選択します。
  このリストには、現在の仮想ドメインに属するチョークポイントが表示されます。 フロアに配置されないチョークポイントは、すべての仮想ドメインに属します。 チョークポイントがフロアに配置されている場合、チョークポイントが配置されるフロアと同じ仮想ドメインに表示されます。
- チョークポイント名または MAC アドレスのいずれかを入力します。
- [Search] をクリックします。
  次に、チョークポイント名を使用した詳細検索の例を示します。 一致が存在しない場合、ページにメッセージが表示されます。 存在する場合は、[Search Results] ページが表示されます。

Wi-Fi TDOA レシーバのモニタリング

Wi-Fi TDOA レシーバは、モニタするロケーションのマップに割り当てられている必要があります。 マップに TDOA レシーバを追加したら、マップに表示するために、ネットワーク設計（[Services] > [Synchronize Services]）を Mobility Services Engine と再同期する必要があります。

TDOA レシーバがマップに割り当てられていない場合、[Search] または [Advanced Search] を使用して検索できません。

すべての TDOA レシーバ設定は、AeroScout システム マネージャを使用して実行されます。

新しい TDOA レシーバを作成すると、すべての仮想ドメインで使用できます。 フロアに配置したあと、フロアと同じ仮想ドメインで使用できるように更新されます。 TDOA レシーバをフロアから削除すると、すべての仮想ドメインで再び利用可能になります。

既存の TDOA レシーバがフロアにある場合、すべてフロアと同じ仮想ドメインに属します。チョークポイントがフロアに配置されていない場合、すべての仮想ドメインで使用できます。

（注） 設定の詳細については、次の URL にある『AeroScout Context-Aware Engine for Tags, for Cisco Mobility Services Engine Users Guide』を参照してください。http://support.aeroscout.com

TDOA レシーバをモニタするには、次の手順に従ってください。

ステップ 1 [Monitor] > [WiFi TDOA Receivers] の順に選択します。 [WiFi TDOA Receivers] 概要ページに、マッピングされているすべての TDOA レシーバが表示されます。

ステップ 2 広範な一覧が表示されたときに検索基準を微調整するには、MAC アドレスまたは TDOA レシーバ名で検索します。

a) MAC アドレスまたは名前で TDOA レシーバの検索を開始するには、[Search] テキスト ボックスにその値を入力します。 [Search] をクリックします。

b) すべてのアラームの一覧を表示するには、[View List] をクリックします。
一致が存在しない場合、[Search Results] ページにメッセージが表示されます。

c) MAC アドレスまたは名前で TDOA レシーバの詳細検索を開始するには、[Advanced Search] リンクをクリックします。

1. [Search Criteria] ドロップダウン リストから検索カテゴリとして [WiFi TDOA Receiver] を選択します。
2. [Search for WiFi TDOA Receiver by] ドロップダウン リストから、[WiFi TDOA Receivers Name] または [MAC Address] を選択します。

   このリストには、現在の仮想ドメインに属する Wi-Fi TDoA レシーバが表示されます。 フロアに配置されない Wi-Fi TDoA レシーバは、すべての仮想ドメインに所属します。 Wi-Fi TDoA レシーバがフロアに配置されている場合、レシーバが配置されているフロアと同じ仮想ドメインに表示されます。
3. TDOA レシーバ名または MAC アドレスのいずれかを入力します。
4. [Search] をクリックします。

一致が存在しない場合、[Search Results] ページにメッセージが表示されます。

Ekahau Site Survey の統合

Ekahau Site Survey（ESS）ツールは、高機能 Wi-Fi ネットワークの設計、導入、維持、およびトラブルシューティングに使用します。 ESS はあらゆる 802.11 ネットワーク上で機能し、集中管理型の 802.11n Wi-Fi ネットワーク用に最適化されています。

ESS ツールを使用して、Prime Infrastructure から既存のフロア マップをインポートし、プロジェクトを Prime Infrastructure にエクスポートできます。 詳細については、ESS オンライン ヘルプの「Cisco Prime Infrastructure Integration」を参照してください。

（注） Prime Infrastructure サイト調査のキャリブレーションでは、150 以上の調査データ ポイントが 50 の異なる場所で収集されている必要があります。 十分な調査データ ポイントがない場合は、調査データをエクスポートしようとすると警告が表示されます。

（注） サイト調査時に Prime Infrastructure にアクセス ポイントがない場合、サイト調査は実施されません。

（注） Prime Infrastructure でフロア マップのスケールが正しくない場合、ESS の視覚的な表示が乱れます。

AirMagnet Survey と AirMagnet Planner の統合

AirMagnet Survey と AirMagnet Planner は、Cisco Prime Infrastructure に統合されます。 この統合により、一般的にワイヤレス LAN ネットワークの導入と管理に付随するワイヤレス計画と実地調査の作業を何度も行う必要がなくなり、運用効率性を高めることができます。

AirMagnet Survey ツールにより、現実世界の調査データを Prime Infrastructure にエクスポートして、Planner モデリングのキャリブレーションに利用できます。 AirMagnet Planner では、Planner プロジェクトを作成し、直接 Prime Infrastructure にエクスポートできます。 これにより Prime Infrastructure で、インポートした AirMagnet Planner ツールから独自のプロジェクトを作成できます。 詳細については、Fluke Networks の Web サイトで提供されている『AirMagnet Survey and Planning』マニュアルを参照してください。

有線クライアントのモニタリング

有線クライアントの詳細情報（MAC アドレス、IP アドレス、ユーザ名、シリアル番号、UDI、モデル番号、ソフトウェア バージョン、および VLAN ID）、ポート、都市情報を表示できます。

スイッチと Mobility Services Engine が同期されると（[Services] > [Synchronize Services] > [Switches]）、Prime Infrastructure を介して有線クライアント データが Mobility Services Engine にダウンロードされます。

有線クライアントの詳細は、[Wired Switches] ページ（[Context Aware Service] > [Wired] > [Wired Switches]）または [Wired Clients] ページ（[Context Aware Service] > [Wired] > [Wired Clients]）に表示されます。

- IP アドレス、MAC アドレス、VLAN ID、シリアル番号、またはユーザ名が判明している場合は、[Wired Clients] ページの [Search] テキスト ボックスを使用できます。
- 特定のスイッチに関連する有線クライアントを調べるには、[Wired Switches] ページでその情報を確認できます。

有線クライアントの詳細を表示するには、次の手順に従います。

ステップ 1 [Services] > [Mobility Services Engines] の順に選択します。 [Mobility Services] ページが表示されます。

ステップ 2 該当する有線ロケーション スイッチのデバイス名リンクをクリックします。

ステップ 3 [Context Aware Service] > [Wired] > [Wired Clients] の順に選択します。
[Wired Clients] 要約ページでは、クライアントがスイッチ別にグループ化されています。 クライアントのステータスは、接続、切断、または不明です。 定義は、次のように要約されます。

- [Connected clients]：有線スイッチに接続しているアクティブなクライアント。
- [Disconnected clients]：有線スイッチから接続が解除されたクライアント。
- [Unknown clients]：有線スイッチとの NMSP 接続が失われた時点で、不明としてマークされたクライアント。
- 有線クライアントの MAC アドレスが判明している場合は、そのリンクをクリックしてクライアントの詳細ページを表示するか、または [Search] テキスト ボックスを使用することができます。
  - 有線クライアントを IP アドレス、ユーザ名、または VLAN ID で検索することもできます。
- スイッチの IP アドレスをクリックすると、スイッチの詳細ページが表示されます。

ステップ 4 有線クライアントが終端するスイッチ ポート、スロット、またはモジュールの物理ロケーション、クライアントのステータス（接続、切断、または不明）、およびスイッチの IP アドレスを参照するには、[Port Association] タブをクリックします。

ステップ 5 都市アドレス情報を表示するには、[Civic Address] タブをクリックします。

ステップ 6 有線クライアントの拡張物理アドレスの詳細（存在する場合）を表示するには、[Advanced] タブをクリックします。

（注） クライアントは、クライアントが終端するポートに対して設定されている都市アドレス情報と拡張ロケーション情報を使用します。 ポート（ポート、スロット、モジュール）に対して都市情報と拡張情報が定義されていない場合、ロケーション データは表示されません。

有線スイッチのモニタリング

有線スイッチの詳細情報（IP アドレス、シリアル番号、ソフトウェア バージョン、ELIN）と、ポート、有線クライアント（カウントとステータス）、および都市情報の詳細を確認できます。

イーサネット スイッチとモビリティ サービス エンジンが同期されると（[Services] > [Synchronize Services] > [Switches]）、Prime Infrastructure を介して有線スイッチ データが Mobility Services Engine にダウンロードされます。 ロケーション対応スイッチと Mobility Services Engine は、NMSP 経由で通信します。 Prime Infrastructure と Mobility Services Engine は XML 経由で通信します。

有線スイッチの詳細を表示するには、次の手順に従います。

ステップ 1 [Services] > [Mobility Services Engines] の順に選択します。

ステップ 2 [Mobility Services] ページで、該当する有線ロケーション スイッチのデバイス名リンクをクリックします。

ステップ 3 [Context Aware Service] > [Wired] > [Wired Switches] の順に選択します。 Mobility Services Engine と同期された有線スイッチの概要が表示されます。

ステップ 4 スイッチ、ポート、有線クライアント（カウントおよびステータス）、および都市情報の詳細については、[IP address] リンクをクリックしてください。

（注） スイッチから都市情報をエクスポートするには、[Select a command] ドロップダウン リストからそのオプションを選択します。 このオプションは、[Wired Switches] ページの 4 つのタブすべてで使用可能です。

- [Switch Information] タブでは、スイッチに接続されている有線クライアントの合計数が、その状態（接続、切断、および不明）とともに要約されています。
- [Connected clients]：有線スイッチに接続しているクライアント。
- [Disconnected clients]：有線スイッチから接続が解除されたクライアント。
- [Unknown clients]：有線スイッチとの NMSP 接続が失われた時点で、クライアントは不明としてマークされます。

有線クライアントの詳細情報を表示するには、クライアント カウント リンク（合計クライアント数、接続、切断、不明）のいずれかをクリックします。

ステップ 5 スイッチ上のポートの詳細リストを表示するには、[Switch Ports] タブをクリックします。
ポート IP アドレス、スロット番号、モジュール番号、ポート番号のリストの順序（昇順、降順）を変更できます。変更するには、該当する列見出しをクリックします。

ステップ 6 有線スイッチの都市情報の詳細リストを表示するには、[Civic] タブをクリックします。

ステップ 7 有線スイッチの追加の都市情報の詳細リストを表示するには、[Advanced] タブをクリックします。

干渉のモニタリング

[Monitor] > [Interferers] > [AP Detected Interferers]

ワイヤレス ネットワーク上の CleanAir 対応アクセス ポイントにより検出されたすべての干渉デバイスを表示するには、[Monitor] > [Interferers] の順に選択します。 このページには干渉デバイスの概要が表示されます。表示される概要には、次のデフォルト情報が含まれています。

- [Interferer ID]：干渉の固有識別子。 干渉源の詳細を参照するには、このリンクをクリックします。
- [Type]：干渉源のカテゴリを示します。 デバイスのタイプの詳細を参照するには、ここをクリックします。 詳細が示されたポップアップ ダイアログが表示されます。 次のカテゴリがあります。
  - [Bluetooth link]：Bluetooth リンク（802.11b/g/n のみ）
  - [Microwave Owen]：**電子レンジ**（802.11b/g/n のみ）
  - [802.11 FH]：802.11 周波数ホッピング デバイス（802.11b/g/n のみ）
  - [Bluetooth Discovery]：Bluetooth 検出（802.11b/g/n のみ）
  - [TDD Transmitter]：時分割複信（TDD）トランスミッタ
  - [Jammer]：電波妨害デバイス
  - [Continuous Transmitter]：連続トランスミッタ
  - [DECT-like Phone]：Digital Enhanced Cordless Communication（DECT）対応電話
  - [Video]：ビデオ カメラ
  - 802.15.4：802.15.4 デバイス（802.11b/g/n のみ）
  - [WiFi Inverted]：スペクトル反転 Wi-Fi 信号を使用するデバイス
  - [WiFi Invalid]：非標準の Wi-Fi チャネルを使用するデバイス
  - [SuperAG]：802.11 SuperAG デバイス
  - [Canopy]：Motorola Canopy デバイス
  - [Radar]：レーダー デバイス（802.11a/n のみ）
  - [XBox]：Microsoft Xbox（802.11b/g/n のみ）
  - [WiMAX Mobile]：WiMAX モバイル デバイス（802.11a/n のみ）
  - [WiMAX Fixed]：WiMAX 固定デバイス（802.11a/n のみ）
- [Status]：干渉デバイスのステータスを示します。

- [Active]：干渉が現在 CleanAir 対応アクセス ポイントにより検出されていることを示します。
- [Inactive]：干渉が CleanAir 対応アクセス ポイントにより検出されないか、または干渉が Prime Infrastructure から到達可能ではないと CleanAir 対応アクセス ポイントが見なしたことを示します。

- [Severity]：干渉デバイスの重大度ランクを示します。
- [Affected Band]：このデバイスが干渉している帯域を表示します。
- [Affected Channels]：影響を受けるチャネルを表示します。
- [Duty Cycle (%)]：干渉デバイスのデューティ サイクル（パーセンテージ）。
- [Discovered]：検出された時刻を表示します。
- [Last Updated]：干渉源が最後に検出された時刻。
- [Floor]：干渉デバイスが存在していたロケーション。

（注） 干渉デバイスは、[Tracking Parameters] ページで干渉デバイスを追跡するオプションが有効な場合にだけ表示されます。 このオプションは、デフォルトで無効です。 追跡パラメータの詳細については、追跡パラメータの変更，（103 ページ）を参照してください。

[Monitor] > [Interferers] > [Edit View]

[Edit View] ページでは、[AP Detected Interferers Summary] ページの列を追加、削除、並び替えできます。 また、干渉を検索できます。 デフォルトでは、アクティブな状態でありシビリティが 5 以上の干渉のみが [AP Detected Interferers] ページに表示されます。

[AP Detected Interferers] ページの列を編集するには、次の手順に従います。

ステップ 1 [Monitor] > [Interferers] の順に選択します。 [AP Detected Interferers] ページが表示されます。このページには、CleanAir 対応アクセス ポイントにより検出された干渉源の詳細が表示されます。

ステップ 2 [AP Detected Interferers] ページの [Edit View] リンクをクリックします。

ステップ 3 アクセス ポイント表に新しい列を追加するには、左側の領域で、列見出しをクリックして選択します。 [Show] をクリックして、選択した列見出しを右側の領域へ移動します。 右側の領域にあるすべての項目が表に表示されます。

ステップ 4 アクセス ポイント表から列を削除するには、右側の領域で、削除する列見出しをクリックして選択します。 [Hide] をクリックして、選択した列見出しを左側の領域へ移動します。 左側の領域にある項目はすべて、表に表示されません。

ステップ 5 [Up] ボタンと [Down] ボタンを使用して、表内での情報の並び順を指定します。 目的の列見出しを選択し、[Up] または [Down] をクリックして、現在のリスト内での位置を変更します。

ステップ 6 デフォルト表示に戻すには、[Reset] をクリックします。

ステップ 7 [Submit] をクリックして、変更内容を確定します。

MSE を使用したモニタ モード AP のクラスタリング

ここで、*value* は、クラスタリングの距離（フィート）です。 デフォルト値は 150 です。

第 13 章

メンテナンス操作の実行

この章では、Mobility Services Engine データのバックアップおよび復元方法と Mobility Services Engine ソフトウェアの更新方法について説明します。 また、その他のメンテナンス操作についても説明します。

この章の内容は、次のとおりです。

注意事項と制約事項

- パスワードを忘れないようにしてください。パスワードの変更は絶対に必要な場合にだけ行ってください。
- 失われたルート パスワードの回復中に、シングル ユーザ モード パスワードをセットアップすると、シェル プロンプトは表示されません。

失われたパスワードの復旧

Mobility Services Engine のパスワードを紛失または忘れた場合に回復するには、次の手順に従います。

ステップ 1 [GRUB] ページが表示されたら、Esc を押してブート メニューに入ります。

ステップ 2 e を押して編集します。

ステップ 3 *kernel* から始まる行に移動し、**e** を押します。
行の最後に、スペースに続けて数字の **1** を入力します。 Enter を押してこの変更を保存します。

ステップ 4 b を押してブートを開始します。
ブート シーケンスの最後にシェル プロンプトが表示されます。

ステップ 5 **passwd** コマンドを入力すると、ルート パスワードを変更できます。

ステップ 6 新しいパスワードを入力して確定します。

ステップ 7 マシンをリブートします。

失われたルート パスワードの回復

Mobility Services Engine のルート パスワードを紛失または忘れた場合に回復するには、次の手順に従います。

ステップ 1 [GRUB] ページが表示されたら、Esc を押してブート メニューに入ります。

ステップ 2 e を押して編集します。

ステップ 3 *kernel* から始まる行に移動し、**e** を押します。
行の最後に、スペースに続けて数字の **1** を入力します。 Enter を押してこの変更を保存します。

ステップ 4 b を押してブート シーケンスを開始します。
ブート シーケンスの最後にシェル プロンプトが表示されます。

（注） 単一ユーザ モードパスワードを設定する場合は、シェル プロンプトは表示されません。

ステップ 5 **passwd** コマンドを入力すると、ルート パスワードを変更できます。

ステップ 6 新しいパスワードを入力して確定します。

ステップ 7 マシンを再起動します。

（注） ルート パスワードを忘れないようにしてください。パスワードの変更は絶対に必要な場合にだけ行ってください。

Mobility Services Engine データのバックアップおよび復元

ここでは、Mobility Services Engine データのバックアップおよび復元方法について説明します。また、自動バックアップを有効にする方法についても説明します。

ここでは、次の内容について説明します。

Mobility Services Engine の履歴データのバックアップ

Prime Infrastructure には、Mobility Services Engine のデータをバックアップするための機能があります。

Mobility Services Engine データをバックアップするには、次の手順に従います。

ステップ 1 [Services] > [Mobility Services] の順に選択します。

ステップ 2 バックアップする Mobility Services Engine の名前をクリックします。

ステップ 3 [System] > [Maintenance] の順に選択します。

ステップ 4 [Backup] をクリックします。

ステップ 5 バックアップの名前を入力します。

ステップ 6 [Submit] をクリックし、Prime Infrastructure が実行されているサーバのハード ドライブに履歴データをバックアップします。
バックアップの処理中に、バックアップのステータスをこのページに表示できます。 バックアップ プロセス中に、このページには 3 つの項目が表示されます。（1）[Last Status] テキスト ボックスには、バックアップのステータスを示すメッセージが表示され、（2）[Progress] テキスト ボックスには、バックアップの完了率が表示され、（3）[Started at] テキスト ボックスには、バックアップの開始日時が表示されます。

（注） 他の Prime Infrastructure ページで他の Mobility Services Engine 操作を実行しながら、バックアップ プロセスをバックグラウンドで実行できます。 バックアップは、Prime Infrastructure インストール時に指定した FTP ディレクトリに保管されます。

Mobility Services Engine の履歴データの復元

Prime Infrastructure を使用して、バックアップされた履歴データを復元できます。

Mobility Services Engine データを復元するには、次の手順に従います。

ステップ 1 [Services] > [Mobility Services] の順に選択します。

ステップ 2 復元する Mobility Services Engine の名前をクリックします。

ステップ 3 [System] > [Maintenance] の順に選択します。

ステップ 4 [Restore] をクリックします。

ステップ 5 ドロップダウン リストから、復元するファイルを選択します。

ステップ 6 Mobility Services Engine からすべてのサービス割り当てを永久に削除するには、[Delete synchronized service assignments] チェックボックスをオンにします。
このオプションは、ネットワーク設計、有線スイッチ、コントローラ、およびイベント定義に適用されます。 既存のロケーション履歴データは維持されますが、今後ロケーション計算を実行するときには手動サービス割り当てを使用する必要があります。

ステップ 7 [Submit] をクリックして復元プロセスを開始します。

ステップ 8 [OK] をクリックし、Prime Infrastructure サーバのハード ドライブからデータを復元することを確定します。
復元が完了すると、Prime Infrastructure にそのことを示すメッセージが表示されます。

（注） 復元プロセスの実行中に、他の Mobility Services Engine 操作を実行しないでください。

ロケーション データの自動バックアップの有効化

ロケーション データの自動バックアップを定期的に実行するように Prime Infrastructure を設定できます。

Mobility Services Engine のロケーション データの自動バックアップを有効にするには、次の手順に従います。

ステップ 1 [Administration] > [Background Tasks] の順に選択します。

ステップ 2 [Mobility Service Backup] **チェックボックス**をオンにします。

ステップ 3 [Select a command] ドロップダウン リストから、[Enable Task] を選択し、[Go] をクリックします。
バックアップは、Prime Infrastructure インストール時に指定した FTP ディレクトリに保管されます。

Mobility Services Engine へのソフトウェアのダウンロード

ソフトウェアを Mobility Services Engine にダウンロードするには、次の手順に従います。

ステップ 1 アプリケーション コードのダウンロードに使用する Prime Infrastructure サーバまたは外部 FTP サーバから、Mobility Services Engine に対して ping を実行できることを確認します。

ステップ 2 [Services] > [Mobility Services Engine] の順に選択します。

ステップ 3 ソフトウェアをダウンロードする Mobility Services Engine の名前をクリックします。

ステップ 4 左側のサイドバーのメニューから、[System] > [Maintenance] > [Download Software] の順に選択します。

ステップ 5 ソフトウェアをダウンロードするには、次のいずれかを実行します。

- Prime Infrastructure ディレクトリにリストされているソフトウェアをダウンロードするには、[Select from uploaded images to transfer into the Server] オプション ボタンを選択します。 ドロップダウン リストからバイナリ イメージを選択します。

  Prime Infrastructure のインストール時に指定した FTP サーバ ディレクトリにバイナリ イメージがダウンロードされます。

- ローカルまたはネットワーク経由で使用可能なダウンロード済みソフトウェアを使用するには、[Browse a new software image to transfer into the Server] オプション ボタンを選択し、[Choose File] をクリックします。 ファイルを探し、[Open] をクリックします。

ステップ 6 [Download] をクリックし、ソフトウェアをモビリティ サービス エンジンの /opt/installers ディレクトリにダウンロードします。

ステップ 7 イメージが Mobility Services Engine に転送されたら、Mobility Services Engine のコマンドライン インターフェイスにログインします。

ステップ 8 **./.bin mse image** コマンドを入力して、/opt/installers ディレクトリからインストーラ イメージを実行します。 これによりソフトウェアがインストールされます。

ステップ 9 ソフトウェアを実行するには、/etc/init.d/msed start コマンドを入力します。

（注） ソフトウェアを停止するには、**/etc/init.d/msed stop** コマンドを入力し、ステータスをチェックするには、**/etc/init.d/msed status** コマンドを入力します。

ソフトウェアの手動ダウンロード

Prime Infrastructure を使用して Mobility Services Engine ソフトウェアを自動的に更新しない場合、次の手順に従い、ローカル（コンソール）またはリモート（SSH）接続を使用してソフトウェアを手動でアップグレードします。

ステップ 1 新しい Mobility Services Engine イメージをハード ドライブに転送します。

a) root としてログインし、バイナリ設定を使用して外部 FTP サーバのルート ディレクトリからイメージを送信します。 リリース ノート形式は CISCO-MSE-L-K9-x-x-x-x-64bit.bin.gz のようになり、リリースごとに変更されます。

（注） この時点では、Mobility Services Engine イメージは圧縮されています。

（注） FTP サーバのデフォルト ログイン名は ftp-user です。

たとえば、次のようなエントリになります。

```
#cd/opt/installers
ftp <FTP Server IP address>
Name:<login>
Password: <password>
binary
get Cisco-MSE-L-K9-x-x-x-x-64bit.bin.gz
<CTRL-Z)
#
```

b) イメージ（CISCO-MSE-L-K9-x-x-x-x-64bit.bin.gz）が Mobility Services Engine の /opt/installers ディレクトリにあることを確認します。

c) イメージ ファイルを圧縮解除（解凍）するには、次のコマンドを入力します。

```
gunzip CISCO-MSE-L-K9-x-x-x-x-64bit.bin.gz
```

圧縮解除すると、bin ファイルが生成されます。

d) CISCO-MSE-L-K9-x-x-x-x-64bit.bin.gz ファイルにルート ユーザの実行権限があることを確認します。ない場合は、次のコマンドを入力します。

```
chmod 755 CISCO-MSE-L-K9-x-x-x-x.bin
```

ステップ 2 Mobility Services Engine を手動で停止します。

ステップ 3 root としてログインし、次のコマンドを入力します。

```
/etc/init.d/msed stop
```

ステップ 4 新しい Mobility Services Engine イメージをインストールするには、次のコマンドを入力します。

```
/opt/installers/CISCO-MSE-L-K9-x-x-x-x.bin
```

ステップ 5 次のコマンドを入力して、新しい Mobility Services Engine ソフトウェアを開始します。

```
/etc/init.d/msed start
```

注意 スクリプト ファイルをアンインストールする次の手順を実行するように指示された場合に限り、この手順を実行します。 ファイルを削除すると、履歴データが不必要に消去されます。

ステップ 6 次のコマンドを入力して、Mobility Services Engine のスクリプト ファイルをアンインストールします。

```
/opt/mse/uninstall
```

NTP サーバの設定

NTP サーバを設定して、Mobility Services Engine の時刻と日付を設定できます。

（注） Mobility Services Engine の自動インストール スクリプトの一環として、NTP をイネーブルにし、NTP サーバ IP アドレスを入力するように求めるプロンプトが自動的に表示されます。 自動インストール スクリプトの詳細については、次の URL にある『Cisco 3350 Mobility Services Engine Getting Started Guide』または『Cisco 3310 Mobility Services Engine Getting Started Guide』を参照してください。http://www.cisco.com/en/US/products/ps9742/prod_installation_guides_list.html

（注） Mobility Services Engine のインストール後に NTP サーバのインストールを追加または変更する必要がある場合、自動インストール スクリプトを再実行します。 スクリプトをタブで指定して他の値を調整せずに NTP サーバを設定できます。

（注） NTP サーバの設定の詳細については、Linux の設定ガイドを参照してください。

システムのリセット

Mobility Services Engine ハードウェアの再起動またはシャットダウンについては、システムの再起動またはシャットダウン，（63 ページ）を参照してください。

コンフィギュレーション ファイルの消去

コンフィギュレーション ファイルの消去については、システム データベースの消去，（63 ページ）を参照してください。

付 録 A

MSE システムとアプライアンスの強化のガイドライン

この付録では、公開するべきサービスおよびプロセスが適切に動作するために必要な MSE の強化について説明します。 これは、MSE アプライアンスのベスト プラクティスと呼ばれます。MSE の強化には、不要なサービスの無効化、最新のサーババージョンへのアップグレード、ファイル、サービス、エンド ポイントへの適切な制限付き権限の適用が含まれます。

この章の内容は、次のとおりです。

セットアップ ウィザードの更新

ここでは、Setup.sh スクリプトに含まれる設定オプションについて説明します。内容は次のとおりです。

- 将来の再起動日時の設定
- MSE ログをパブリッシュするためのリモート Syslog サーバの設定
- ホストのアクセス コントロールの設定

将来の再起動日時の設定

MSE を再起動する日時を指定する場合は、このオプションを使用します。何も指定しない場合、土曜日の午前 1 時がデフォルトとして使用されます。（この後のセクション全体で config コマンド オプションを書き換えます）

例：

```
Configure future restart day and time ? (Y)es/(S)kip [Skip]:
```

MSE ログをパブリッシュするためのリモート Syslog サーバの設定

IP アドレス、プライオリティ パラメータ、プライオリティ レベル、および機能を指定して、リモート Syslog サーバを設定するには、このオプションを使用します。

例：

```
A Remote Syslog Server has not been configured for this machine.
Configure Remote Syslog Server Configuration parameters? (Y)es/(S)kip/(U)se default [Skip]:
 y
Configure Remote Syslog Server IP address: 283.12.13.4

Configure Remote Syslog Server Priority parameter.
select a priority level
1)ERROR (ERR)
2)WARNING
3)INFO
Enter a priority level (1-3) :2
Configure Remote Syslog Server's Facility parameter.
Select a logging facility
    KERN(0), // Kernel messages
    USER(1), // user-level messages
    MAIL(2), // mail system
    DAEMON(3), // system daemons
    AUTH(4), // security/authorization messages (note 1)
    SYSLOG(5), // messages generated internally by syslogd
    LPR(6), // line printer subsystem
    NEWS(7), // network news subsystem
    UUCP(8), // UUCP subsystem
    CRON(9), // clock daemon (note 2)
    SECURITY(10), // security/authorization messages (note 1)
    FTP(11), // FTP daemon
    NTP(12), // NTP subsystem
    LOGAUDIT(13), // log audit (note 1)
    LOGALERT(14), // log alert (note 1)
    CLOCK(15), // clock daemon (note 2)
    LOCAL0(16), // local use 0  (local0)
    LOCAL1(17), // local use 1  (local1)
    LOCAL2(18), // local use 2  (local2)
    LOCAL3(19), // local use 3  (local3)
    LOCAL4(20), // local use 4  (local4)
    LOCAL5(21), // local use 5  (local5)
    LOCAL6(22), // local use 6  (local6)
    LOCAL7(23); // local use 7  (local7)

Enter a facility(0-23) :4
```

ホストのアクセス コントロールの設定

このオプションを使用して、MSEにアクセスするためのホストを追加、削除、またはクリアできます。

例：

```
Enter whether or not you would like to change the iptables for this machine (giving access
 to certain host).
Configure Host access control settings ? (Y)es/(S)kip [Skip]: y
Choose to add/delete/clear host for access control(add/delete/clear): add
Enter IP address of the host / subnet for access to MSE : 258.19.35.0/24 (Rewrite the IP)
```

Setup.sh スクリプトの詳細については、『*Cisco 3350 Mobility Services Engine Getting Started Guide*』を参照してください。

Certificate Management

現在、MSEは自己生成の証明書とともに出荷されます。SSL接続の確立時に信頼を確立するために、MSEは、有効なシスコの認証局（CA）発行の証明書を使用するか、有効なCA発行のサーバ証明書のインポートを許可します。これを実行するには、コマンドラインインターフェイスベースのCertMgmt.shを使用して、サーバとCA証明書をインポートします。

CertMgmt.sh スクリプト ファイルにアクセスするには、次のフォルダに移動します。

/opt/mse/framework/bin/

ここでは、CertMgmt.shスクリプトを使用して実行できるタスクについて説明します。内容は次のとおりです。

- CSR の作成
- CA 証明書のインポート
- サーバ証明書のインポート
- クライアント証明書検証の有効化または無効化
- OCSP の設定
- CRL のインポート
- 証明書設定のクリア
- 証明書設定の表示

CSR の作成

証明書署名要求を作成するには、このオプションを使用します。この要求の出力は、サーバの証明書署名要求およびキーです。サーバCSRをコピーし、それを認証局Webサイトに貼り付けて、CA 証明書を生成する必要があります。

例：

```
Certificate Management Options
                1: Import CA Certificate
                2: Import Server Certificate
                3: Enable Client Certificate Validation
                4. Disable Client Certificate Validation
                5: OCSP Settings
                6: Import a CRL
                7: Create a CSR (Certificate Signing request)
                8: Clear Certificate Configuration
                9: Show Certificate Configuration
                10: Exit
Please enter your choice (1-10)
7
Enter the directory in which the CSR needs to be stored:/root/TestFolder
Enter the Keysize: 2048
Generating a 2048 bit RSA private key
.....................................................+++
.........+++
writing new private key to '/root/TestFolder/mseserverkey.pem'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
Verify failure
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [GB]:IN
State or Province Name (full name) [Berkshire]:State
Locality Name (eg, city) [Newbury]:City
Organization Name (eg, company) [My Company Ltd]:xyz
Organizational Unit Name (eg, section) []:ABCD
Common Name (eg, your name or your server's hostname) []:example-mse
Email Address []:user@example.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:password123
An optional company name []:abc
The CSR is in: /root/TestFolder/mseservercsr.pem
The Private key is in: /root/TestFolder/mseserverkey.pem
```

CA 証明書のインポート

認証局は、送信したサーバ CSR と秘密キーに基づいて CA 証明書を送信します。

CA 証明書をインポートするには、[Import CA Certificate] オプションを使用します。

例：

```
Certificate Management Options
                1: Import CA Certificate
                2: Import Server Certificate
                3: Enable Client Certificate Validation
                4. Disable Client Certificate Validation
                5: OCSP Settings
                6: Import a CRL
                7: Create a CSR (Certificate Signing request)
                8: Clear Certificate Configuration
                9: Show Certificate Configuration
```

```
                10: Exit
Please enter your choice (1-10)
1
Do you want to file(0) or scp(1) transfer (0/1) 0
Enter the full path of the CA certificate file /root/TestFolder/CACert.cer
Successfully transferred the file
Import CA Certificate successful
```

サーバ証明書のインポート

CA 証明書を取得した後、サーバ証明書を取得する必要があります。 次に、サーバ証明書の最後の方に秘密キー情報を付ける必要があります。

サーバ証明書をインポートするには、[Import Server Certificate] オプションを使用します。

例：

```
Certificate Management Options
                1: Import CA Certificate
                2: Import Server Certificate
                3: Enable Client Certificate Validation
                4. Disable Client Certificate Validation
                5: OCSP Settings
                6: Import a CRL
                7: Create a CSR (Certificate Signing request)
                8: Clear Certificate Configuration
                9: Show Certificate Configuration
                10: Exit
Please enter your choice (1-10)
2
Do you want to file(0) or scp(1) transfer (0/1) 0
Enter the full path of the server certificate file /root/TestFolder/ServerCertUpdated.cer
Successfully transferred the file
Enter pass phrase for /var/mse/certs/exportCert.cer:
Enter Export Password:
Verifying - Enter Export Password:
Enter password for PKCS12 file:
pk12util: PKCS12 IMPORT SUCCESSFUL
Validation is Successful
Import Server Certificate successful
```

クライアント証明書検証の有効化または無効化

認証局から取得する CA 証明書は、関連付けられたクライアントにもコピーされます。

このオプションを使用して、クライアント証明書検証を有効化または無効化します。

例：

```
Certificate Management Options
                1: Import CA Certificate
                2: Import Server Certificate
                3: Enable Client Certificate Validation
                4. Disable Client Certificate Validation
                5: OCSP Settings
                6: Import a CRL
                7: Create a CSR (Certificate Signing request)
                8: Clear Certificate Configuration
                9: Show Certificate Configuration
                10: Exit
Please enter your choice (1-10)
3
Enabling client certificate validation done
```

```
Certificate Management Options
                1: Import CA Certificate
                2: Import Server Certificate
                3: Enable Client Certificate Validation
                4. Disable Client Certificate Validation
                5: OCSP Settings
                6: Import a CRL
                7: Create a CSR (Certificate Signing request)
                8: Clear Certificate Configuration
                9: Show Certificate Configuration
                10: Exit
Please enter your choice (1-10)
3
Enabling client certificate validation done
```

OCSP の設定

Online Certificate Status Protocol（OCSP）設定を行うには、このオプションを使用します。 OCSP URL およびデフォルト名を入力するように促されます。 つまり、認証局の URL およびデフォルト名を指定するよう求められます。

例：

```
Certificate Management Options
                1: Import CA Certificate
                2: Import Server Certificate
                3: Enable Client Certificate Validation
                4. Disable Client Certificate Validation
                5: OCSP Settings
                6: Import a CRL
                7: Create a CSR (Certificate Signing request)
                8: Clear Certificate Configuration
                9: Show Certificate Configuration
                10: Exit
Please enter your choice (1-10)
5
Enter the OCSP URL :
http://ocsp.227.104.178.224
Enter the default ocsp name :ExampleServer
```

CRL のインポート

認証局の Web サイトから取得した証明書失効リスト（CRL）をインポートするには、このオプションを使用します。

例：

```
Certificate Management Options
                1: Import CA Certificate
                2: Import Server Certificate
                3: Enable Client Certificate Validation
                4. Disable Client Certificate Validation
                5: OCSP Settings
                6: Import a CRL
                7: Create a CSR (Certificate Signing request)
                8: Clear Certificate Configuration
                9: Show Certificate Configuration
                10: Exit
Please enter your choice (1-10)
6
Do you want to file(0) or scp(1) transfer (0/1) 0
```

```
Enter the full path of the CRL file /root/TestFolder/Sample.crl
Successfully transferred the file
Import CRL successful
```

証明書設定のクリア

証明書設定をクリアするには、このオプションを使用します。

例：

```
Certificate Management Options
                1: Import CA Certificate
                2: Import Server Certificate
                3: Enable Client Certificate Validation
                4. Disable Client Certificate Validation
                5: OCSP Settings
                6: Import a CRL
                7: Create a CSR (Certificate Signing request)
                8: Clear Certificate Configuration
                9: Show Certificate Configuration
                10: Exit
Please enter your choice (1-10)
8
httpd (no pid file) not running
Flushing firewall rules: [  OK  ]
Setting chains to policy ACCEPT: filter [  OK  ]
Unloading iptables modules: [  OK  ]
```

証明書設定の表示

証明書設定の詳細を表示するには、このオプションを使用します。

例：

```
Certificate Management Options
                1: Import CA Certificate
                2: Import Server Certificate
                3: Enable Client Certificate Validation
                4. Disable Client Certificate Validation
                5: OCSP Settings
                6: Import a CRL
                7: Create a CSR (Certificate Signing request)
                8: Clear Certificate Configuration
                9: Show Certificate Configuration
                10: Exit
Please enter your choice (1-10)
9

Certificate Nickname                                         Trust Attributes
                                                             SSL,S/MIME,JAR/XPI

CA-Cert1296638915                                            CT,,
Server-Cert                                                  u,u,u
============================================================
************************  Certificates in the database  *******************
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            74:a1:38:25:75:94:a5:9a:43:2d:4a:23:bd:82:bc:e5
        Signature Algorithm: PKCS #1 SHA-1 With RSA Encryption
        Issuer: "CN=ROOTCA1"
        Validity:
            Not Before: Tue Nov 16 18:49:25 2010
```

```
            Not After : Mon Nov 16 18:59:25 2015
        Subject: "CN=ROOTCA1"
        Subject Public Key Info:
            Public Key Algorithm: PKCS #1 RSA Encryption
            RSA Public Key:
                Modulus:
                    da:06:43:70:56:d8:41:ec:69:e6:65:ad:c5:3b:04:0b:
                    cb:cd:83:7c:5f:6e:8f:aa:17:50:6b:6a:3a:48:35:a6:
                    65:8a:47:91:48:2f:93:2b:d8:53:6b:33:5c:a9:c2:b2:
                    33:c2:fc:9c:55:25:19:d0:79:23:3f:66:60:24:04:ce:
                    a3:08:c7:60:f0:b0:8d:b1:31:71:f5:b9:3f:17:46:1a:
                    fd:3d:c9:3b:9f:bf:fe:a3:8d:13:52:aa:6b:59:80:43:
                    f8:24:e7:49:10:ca:54:6c:f7:aa:77:04:4b:c2:3f:96:
                    8d:a1:46:e8:16:1e:a8:e6:86:f4:5c:a0:e5:15:eb:f8:
                    5a:72:97:f9:09:65:84:f6:a5:0b:a3:c6:ab:a9:9e:61:
                    07:5a:8d:b1:af:93:3b:68:53:8a:5d:f0:14:6e:02:e4:
                    38:d2:31:29:5e:a2:1a:93:de:a0:bd:44:9b:05:fd:7b:
                    5f:59:23:a1:47:97:87:84:dd:0e:9f:0a:09:cd:df:34:
                    b9:6f:9c:b5:4d:07:23:8b:a5:27:16:cd:75:5a:6e:f1:
                    c1:5b:6b:21:3a:fd:d9:4d:72:b4:d6:dc:37:86:c2:e3:
                    60:56:69:3c:52:27:19:bf:4c:0c:ea:6e:34:29:8c:cf:
                    17:50:b3:31:cc:86:1e:32:dc:40:58:92:26:88:58:63
                Exponent: 65537 (0x10001)
        Signed Extensions:
            Name: Certificate Key Usage
            Usages: Digital Signature
                    Certificate Signing
                    CRL Signing

            Name: Certificate Basic Constraints
            Critical: True
            Data: Is a CA with no maximum path length.

            Name: Certificate Subject Key ID
            Data:
                30:89:49:06:62:fe:6c:29:75:bc:90:8b:a5:6a:87:f8:
                8e:61:49:eb

            Name: Microsoft CertServ CA version
            Data: 0 (0x0)

    Signature Algorithm: PKCS #1 SHA-1 With RSA Encryption
    Signature:
        d6:35:b9:27:1f:5b:1a:12:9d:41:a3:16:3a:3a:08:ba:
        91:f4:a9:4b:1b:ff:71:7c:4e:74:16:36:05:04:37:27:
        d0:73:66:a2:47:50:0d:b3:fa:b1:34:dc:36:b8:a9:0a:
        2d:5c:84:35:30:51:4f:7b:55:47:00:53:73:40:c8:95:
        a9:82:83:32:06:ed:0c:95:6d:b1:13:08:3a:e3:cc:88:
        40:9f:e6:43:8c:36:88:e4:a1:91:3e:20:74:29:bf:91:
        25:c1:ef:bc:10:bb:cb:be:08:2c:64:2d:41:a1:3f:81:
        48:ed:80:ed:97:68:6d:83:30:e2:c8:90:ce:45:3a:45:
        cc:78:3c:c4:af:62:73:6a:29:60:c7:70:b1:4c:84:43:
        77:2d:9c:b9:13:dc:9c:b5:8c:74:62:7b:8e:41:ed:37:
        b8:2c:c0:3b:0c:49:cf:61:40:cc:2c:22:74:b2:6b:50:
        e8:31:c9:5f:b8:04:dd:39:7a:9a:46:5e:ee:5a:e8:6a:
        4b:75:97:69:7e:fc:7f:9d:9f:df:f0:3f:06:62:79:77:
        d9:a8:49:a6:00:bf:93:61:00:aa:55:11:26:92:f4:c2:
        8a:61:21:80:af:ef:ab:22:11:ee:10:79:15:4b:1a:8f:
        ae:55:c5:61:03:8e:db:1a:3e:5a:6f:a6:6d:3e:5b:a4
    Fingerprint (MD5):
        31:54:A0:D3:A7:40:1A:1E:95:8E:8A:D9:EC:70:47:35
    Fingerprint (SHA1):
        F5:72:62:5C:46:AB:2A:5D:7A:75:DA:CB:44:E6:38:76:E0:9E:17:C3

    Certificate Trust Flags:
        SSL Flags:
            Valid CA
            Trusted CA
            Trusted Client CA
        Email Flags:
        Object Signing Flags:

Certificate:
```

```
Data:
    Version: 3 (0x2)
    Serial Number:
        4d:a9:34:de:00:00:00:00:00:0b
    Signature Algorithm: PKCS #1 SHA-1 With RSA Encryption
    Issuer: "CN=ROOTCA1"
    Validity:
        Not Before: Wed Feb 02 22:40:44 2011
        Not After : Thu Feb 02 22:50:44 2012
    Subject: "E=abc@example.com,CN=abc-mse,OU=XYZ,O=Companyo,L=City,S
        T=State,C=IN"
    Subject Public Key Info:
        Public Key Algorithm: PKCS #1 RSA Encryption
        RSA Public Key:
            Modulus:
                a8:7b:2f:57:94:53:fc:90:c9:37:cb:9a:b3:f6:f4:b8:
                02:04:f3:f8:d8:e1:d1:23:d4:62:7b:30:05:d2:b0:da:
                17:88:b0:22:d5:a6:04:c6:66:fc:64:54:ff:78:5b:f9:
                ef:05:3a:3e:ec:b8:01:7c:3c:9b:78:ac:1d:7f:fb:3b:
                39:f5:31:d2:a2:27:d8:d1:ee:2e:77:98:04:bb:7c:f6:
                0b:9c:ea:15:12:cf:3d:1c:b8:57:63:df:2b:00:48:25:
                32:e4:58:9a:e1:ff:80:5d:2c:24:75:e2:06:de:e6:ae:
                03:7e:c5:f6:e7:97:4d:c1:ad:19:4f:47:20:6c:8d:7a:
                60:75:85:34:3e:ed:f3:1a:77:65:e2:7a:18:e1:17:3d:
                bd:62:1a:1c:4a:d9:49:c3:93:2e:6a:69:fc:e8:87:1e:
                dc:69:11:63:f1:17:63:41:e4:8d:1e:19:3c:e8:80:a9:
                6b:04:c8:18:fb:c9:fe:9d:77:71:30:d2:87:46:82:49:
                0a:1d:ed:4d:ad:66:ad:65:6f:fb:b2:6a:31:45:33:59:
                a7:04:3a:2d:72:f7:55:02:fa:99:02:d9:dd:5e:21:4b:
                2c:c9:3e:cc:a4:a0:dd:4c:4f:7f:be:45:a7:dd:a9:c4:
                ad:bc:a9:25:a6:1f:53:b8:d0:98:4a:b7:c3:41:a3:d7
            Exponent: 65537 (0x10001)
    Signed Extensions:
        Name: Certificate Subject Key ID
        Data:
            bc:a3:66:c6:19:07:56:0a:90:7a:b1:1a:ea:37:17:20:
            74:b8:f1:f5

        Name: Certificate Authority Key Identifier
        Key ID:
            30:89:49:06:62:fe:6c:29:75:bc:90:8b:a5:6a:87:f8:
            8e:61:49:eb

        Name: CRL Distribution Points
        URI: "http://win-bncnizib5e2/CertEnroll/ROOTCA1.crl"
        URI: "file://WIN-BNCNIZIB5E2/CertEnroll/ROOTCA1.crl"

        Name: Authority Information Access
        Method: PKIX CA issuers access method
        Location:
            URI: "http://win-bncnizib5e2/CertEnroll/WIN-BNCNIZIB5E2_ROOTC
                A1.crt"
        Method: PKIX CA issuers access method
        Location:
            URI: "file://WIN-BNCNIZIB5E2/CertEnroll/WIN-BNCNIZIB5E2_ROOTC
                A1.crt"

Signature Algorithm: PKCS #1 SHA-1 With RSA Encryption
Signature:
    aa:13:74:0d:d1:8c:85:cc:3d:8f:35:c7:e5:9b:a6:4c:
    f8:8b:12:a0:12:9f:dc:0a:0a:b5:40:12:eb:05:a9:2b:
    65:c5:a3:22:62:1f:47:cd:dd:0f:b8:03:11:a5:63:23:
    64:a7:f8:8b:ec:d4:21:dc:d8:22:de:52:75:d9:fb:23:
    d4:14:35:d8:78:b7:e2:23:75:05:b4:d0:09:e0:55:ec:
    96:8c:22:23:fb:86:74:71:69:ac:03:57:b6:ec:14:a9:
    f9:99:b3:98:4c:00:69:e2:26:f8:7b:e9:a0:2a:c2:f4:
    6a:75:fc:d1:08:d6:5b:76:93:7a:2c:21:8b:83:ab:52:
    a0:85:16:f1:38:35:01:8d:21:34:60:b7:82:39:a7:42:
    e7:5f:1a:b7:9d:bf:54:ee:27:97:ba:f8:ca:31:d4:35:
    67:55:36:02:b4:48:ab:16:ee:0f:65:56:48:51:de:aa:
    9f:7d:35:9b:eb:58:3a:0c:4a:8a:ae:3a:18:47:e3:11:
    7b:82:b3:fb:88:94:df:85:82:23:0b:07:46:12:2c:d0:
    dd:a7:91:c0:e1:4c:e7:38:9e:34:30:9b:b6:db:c6:8d:
```

```
        03:df:6e:6b:27:76:da:31:50:44:cd:c8:21:30:42:3c:
        75:dc:99:d2:6b:91:9e:bd:b0:5c:8a:52:6b:92:41:0f
    Fingerprint (MD5):
        77:73:3C:D6:B9:2E:F2:AA:C4:A6:7E:9F:60:D7:55:F7
    Fingerprint (SHA1):
        60:F8:DC:D2:75:BA:D9:35:4D:21:60:CA:90:EF:09:67:FF:D0:DC:CF

    Certificate Trust Flags:
        SSL Flags:
            User
        Email Flags:
            User
        Object Signing Flags:
            User

****************************  CRLs in the database  ***********************
None
******************  Client Certification Settings  ****************************
Client Certificate Validation is disabled
****************************  OCSP Setting  ********************************
OCSP URL :
http://ocsp.227.104.178.224
OCSP nick name :ExampleServer
============================================================
```

更新されたオープン ポートのリスト

非ユーザ要件の一部として、MSE は HTTP（8880）および HTTP（8843）ポートでリッスンします。

次に、MSE のオープン ポートを示します。

TCP	80、443、22、8001
	4096、1411、4000X（x=1、5）
UDP	162、12091、12092

syslog サポート

DoD 要件に確実に準拠するために、wIPS では syslog メッセージングがサポートされます。

MSE および RHEL 5

MSE OS は、RHEL（Red Hat Enterprise Linux）5 に基づいており、MSE OS でサポートされる最新バージョンの RHEL は 5.4 です。 RHEL 5.3 以前を使用している場合は、openssl パッチをダウンロードして更新します。 RHEL5.4 へのアップグレードでは、（4.3p2-26.el5_2.1 の脆弱性に対応する）OpenSSH バージョン 4.3p2-36.el5 がサポートされます。

索 引

た

つ

と

ね

は

ひ

ふ

へ

ほ

り

ろ

わ