



CHAPTER 9

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モビリティ サービス エンジンのモニタ方法、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）のカウンタ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、NCS 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。

この章は、次の内容で構成されています。

- 「アラームの処理」 (P.9-1)
- 「イベントの使用」 (P.9-7)
- 「ログの操作」 (P.9-7)
- 「レポートの生成」 (P.9-9)
- 「MSE でのクライアントのサポート」 (P.9-16)

アラームの処理

この項では、NCS を使用したモビリティ サービス エンジンのアラームとイベントの表示、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の詳細についても説明します。

この項では、次のトピックを扱います。

- 「ガイドラインと制限事項」 (P.9-1)
- 「アラームの表示」 (P.9-2)
- 「MSE アラーム詳細の表示」 (P.9-2)
- 「アラームの割り当てと割り当て解除」 (P.9-4)
- 「アラームの削除とクリア」 (P.9-5)
- 「電子メール アラーム通知」 (P.9-5)

ガイドラインと制限事項

重大度が [Clear] になると、アラームは 30 日経過後に NCS から削除されます。

アラームの表示

モビリティ サービス エンジン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、[Severity of Alarms] 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、コンボ ボックスの [Condition] に条件を入力することもできます。
 - 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 [ステップ 2](#) から [ステップ 12](#) を繰り返して、モビリティ サービス エンジンの Context-Aware Service 通知を確認します。 [ステップ 5](#) で、アラーム カテゴリとして「**Context Aware Notifications**」と入力します。
-

MSE アラーム詳細の表示

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。

-
- ステップ 1 [Monitor] > [Alarms] の順に選択します。
 - ステップ 2 [Failure Source] 列にある MSE をクリックして、特定の MSE のアラーム詳細にアクセスします。

または、[Services] > [Services] > [MSE Name] > [System] > [Status] > [NCS Alarms] ページの順に選択し、[Failure Source] 列にある特定の MSE 項目をクリックして、特定の MSE のアラーム詳細にアクセスします (図 9-1 を参照)。

図 9-1 MSE アラーム

表 9-1 に、MSE の [Alarm Detail] ページの各種フィールドを示します。

表 9-1 [General] パラメータ

フィールド	説明
[Failure Source] : アラーム検出デバイス	アラームを生成した MSE。
Owner	このアラームの担当者の名前または空欄。
Acknowledged	担当ユーザがこのアラームを認知しているかどうかを示します。
Category	アラームのカテゴリ。アラーム カテゴリは、MSE のモビリティ サービスです。
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	このフィールドは MSE と表示されます。
Severity	セキュリティのレベル : Critical (重大)、Major (やや重大)、Minor (比較的軽微でない)、Warning (警告)、Clear (クリア)、Info (通知) が色分けして表示されます。
Previous Severity	Critical (重大)、Major (やや重大)、Minor (比較的軽微でない)、Warning (警告)、Clear (クリア)、Info (通知) が色分けして表示されます。



(注)

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、一部のアラーム詳細には、ロケーションおよびスイッチ ポート トレーシング情報が含まれる場合があります。

- [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] 表示ページに表示されます。
- [Messages] : アラームに関する情報が表示されます。
- [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軽微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、ページ上部にページ番号とその両側に他のページへ移動するためのスクロール矢印が表示されます。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。

Select a Command

[Select a command] ドロップダウン リストからは、次の機能にアクセスできます。

- [Assign to me] : 選択したアラームを現在のユーザに割り当てます。
- [Unassign] : 選択したアラームの割り当てを解除します。
- [Delete] : 選択したアラームを削除します。
- [Clear] : 選択したアラームをクリアします。



[注] 重大度が [Clear] になると、アラームは 30 日経過後に NCS から削除されます。

- [Acknowledge] : [Alarm Summary] ページに表示されないように、アラームを承認します。アラームは NCS に保存されるため、アラーム検索機能を使用して、すべての認知しているアラームを検索できます。
- [UnAcknowledge] : すでに認知しているアラームの認知を解除できます。
- [Email Notification] : [All Alarms] > [Email Notification] ページを開き、電子メール通知を表示して設定します。
- [Event History] : [Monitor] > [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。

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 NCS 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、NCS 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。

モビリティ サービス エンジン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

NCS では、特定の電子メール アドレスに電子メール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。

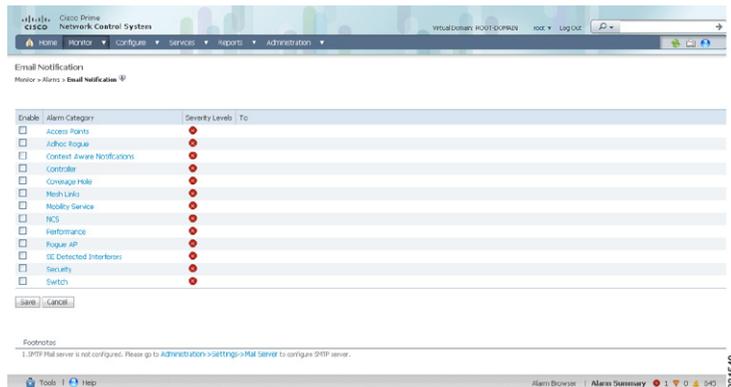
自分に電子メールで送信されるアラーム重大度のタイプ (Critical、Major、Minor、および Warning) を選択できます。

アラーム通知を送信するには、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 [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 (図 9-2 を参照)。

図 9-2 [All Alarms > Email Notification] ページ



(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、モビリティ サービス エンジンとロケーション 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。モビリティ サービス エンジン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

NCS を使用して、モビリティ サービス エンジンおよびロケーション通知イベントを確認できます。イベントは、それぞれの重大度（Critical、Major、Minor、Warning、Clear、Info）およびイベント カテゴリに基づき検索して表示できます。

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は、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 検索条件に一致するイベントが見つかったら、それらのイベントが一覧表示されます。



(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。

この項では、次のトピックを扱います。

- 「ガイドラインと制限事項」(P.9-7)
- 「ロギング オプションの設定」(P.9-8)
- 「MAC アドレスに基づくロギング」(P.9-9)
- 「ログ ファイルのダウンロード」(P.9-9)

ガイドラインと制限事項

- 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

NCS 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 Engines] の順に選択します。
- ステップ 2** 設定するモビリティ サービス エンジン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。選択されているモビリティ サービス エンジンのロギング 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

[Error] と [Trace] は、Cisco Technical Assistance Center (TAC) 担当者の指示がある場合にだけ使用してください。

- 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](#)」(P.9-9) 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。
- モビリティ サービス エンジンで維持するログ ファイルの数。モビリティ サービス エンジンで維持できるログ 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 アドレスに基づく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](#)」(P.9-9) 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 アドレスのエントリ固有のログ 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

モビリティ サービス エンジン ログ ファイルを解析する必要がある場合は、NCS 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。NCS はログ ファイルが含まれている `.zip` ファイルをダウンロードします。

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 Engines] の順に選択します。
- ステップ 2** ステータスを表示するモビリティ サービス エンジン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。

レポートの生成

NCS 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、NCS 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 NCS 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 つまたは複数のモビリティ サービス エンジン
- 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

この項では、次のトピックを扱います。

- 「デバイス使用率レポートの作成」(P.9-10)
- 「保存した使用率レポートの表示」(P.9-12)
- 「スケジュールされた使用率の実行の表示」(P.9-12)

デバイス使用率レポートの作成

モビリティ サービス エンジン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 リストボックス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。次の値が可能です。

- 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 からステップ 10 まで完了したら、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 [NCS] 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。



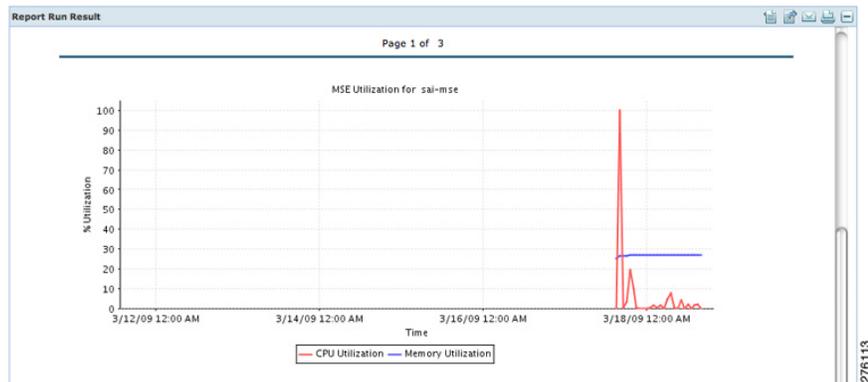
(注) [Run Now] をクリックして、保存する前に定義済みのレポート条件を確認したり、必要に応じてレポートを実行したりすることもできます。

結果はページの一番下に表示されます (図 9-3 を参照)。



(注) 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 9-3 を参照)。

図 9-3 [Devise] > [MSE Utilization] > [Results]



ステップ 12 [Save] または [Save and Run] オプションを選択した場合は、[Reports] > [Saved Reports] の順に選択します（または、レポートが未実行で、実行がスケジュールされている場合は、[Reports] > [Scheduled Runs] の順に選択します）。[Utilization Reports Summary] ページが表示されます。

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 13 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。

wIPS のセキュリティ レポートとアラーム

wIPS のセキュリティ レポートとアラームを確認、変更、または作成できます。



(注) セキュリティ レポートには、Autonomous アクセス ポイントのステータスは表示されません。

次の選択肢があります。

- [Adaptive wIPS Alarms] : モニタ モードのアクセス ポイントで wIPS に報告されるアラームです。
- [Adaptive wIPS Top 10 AP] : モニタ アクセス ポイントで報告された最新の 10 イベントが一覧表示されます。
- [Adhoc Rogue Event] : 選択した時間帯に NCS が受信したアドホック イベントがすべて表示されます。
- [Adhoc Rogues] : 選択した時間帯に更新されたアドホックがすべて表示されます。
- [New Rogue APs] : 選択した時間帯に検出された不正アクセス ポイントが表形式ですべて表示されます。選択した時間内に検出された新しい不正アクセス ポイントを示します。作成時刻は、不正アクセス ポイントが最初に検出された時刻です。
- [New Rogue AP Count] : 選択した時間帯に検出された不正アクセス ポイントがグラフ形式ですべて表示されます。
- [Rogue APs] : ネットワーク内のアクティブな不正アクセス ポイントと選択した時間帯に更新された不正アクセス ポイントがすべて表示されます。NCS は、検出された不正アクセス ポイントの更新イベントを受信します。
- [Rogue APs Event] : NCS が受信したすべてのイベントが表示されます。属性が変更されるか、または新しい不正アクセス ポイントが検出されると、最新の不正アクセス ポイント検出情報がコントローラから送信されます。



(注) このレポートは、正式には Rogue Detected by AP と呼ばれます。

- [Security Summary] : アソシエーション失敗回数、不正なアクセス ポイント数、不正なアドホック数、不正なアクセス ポイント接続数、または 1 か月以上にわたる切断が表示されます。
- [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、そのレポートにアソシエートされているスケジュール時間に関係なく実行され、[Results] タブで確認することができます。また、レポートは指定した時刻に実行され、[Schedule] タブでの定義に従い、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、レポートのキャンセルや削除ができます。

この項では、次のトピックを扱います。

- 「wIPS のセキュリティまたはアラームのレポートの新規作成」 (P.9-14)
- 「保存した wIPS レポートの表示」 (P.9-15)
- 「wIPS レポートの実行スケジュールの表示」 (P.9-15)

wIPS のセキュリティまたはアラームのレポートの新規作成

セキュリティ レポートには、wIPS のアクセス ポイントと不正アクセス ポイントに関する多くの詳細が表示されます。

新しいセキュリティ レポートを作成するには、次の手順を実行します。



(注) この手順またはオプションの中には、レポートによっては必要ないものもあります。

- ステップ 1 [Reports] > [Report Launch Pad] の順に選択します。[Report Launch Pad] ページが表示されます。
- ステップ 2 [Security] を選択し、左側のペインでいずれかのレポート タイプ ([Adaptive wIPS Top 10 Report Details] など) をクリックします。
- ステップ 3 [New] をクリックします。[New report] ページが表示されます。
- ステップ 4 [Settings] ペインで、レポートのタイトルを入力します。
- ステップ 5 [Report By] は、デフォルトでは [MSE with Adaptive wIPS Service] です。
- ステップ 6 [Report Criteria] は常に、特定のモビリティ サービス エンジンか、[All MSEs with Adaptive wIPS Service] です。
- ステップ 7 [Edit] をクリックして、[Report Criteria] を追加または変更します。[Filter Criteria] ダイアログボックスが表示されます。
- ステップ 8 レポート期間を入力します。時間単位、週単位、または特定の日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 9 [Schedule] ペインで、[Enable Schedule] チェックボックスをオンにします。
- ステップ 10 [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 11 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 12 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 13 [hour] と [minute] のドロップダウン リストを使用して開始時刻を選択します。
- ステップ 14 [Recurrence] オプションのいずれかを選択して、レポートの実行頻度を決定します。



(注) [Days of the week] チェックボックスは [Weekly] オプション ボタンを選択した場合のみ表示されます。

[Customize Report] オプションを使用して、レポートをカスタマイズすることもできます。[Customize] をクリックして、レポートを生成するのに必要な情報を入力します。

ステップ 15 ステップ 1 からステップ 14 まで完了したら、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] ペインでの定義に従い、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] ペインでの定義に従い、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 [NCS] 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できます。

結果はページの一番下に表示されます。

ステップ 16 作成する wIPS レポートごとに、ステップ 2 からステップ 15 までを繰り返します。

保存した wIPS 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** [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** 必要なレポートの [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。

wIPS レポートの実行スケジュールの表示

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。



(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。

MSE でのクライアントのサポート

NCS 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。詳細については、「[Using the Search Feature](#)」(P.2-34) を参照してください。[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。詳細については、「[Filtering Client and Users](#)」(P.10-11) を参照してください。

この項では、次のトピックを扱います。

- 「[IPv6 アドレスによる MSE 上の NCS のワイヤレスクライアントの検索](#)」(P.9-16)
- 「[MSE で検出されたクライアントの表示](#)」(P.9-17)

IPv6 アドレスによる MSE 上の NCS のワイヤレスクライアントの検索



(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。

NCS 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、次の手順を実行します。

- ステップ 1** NCS UI の右上隅にある [Advanced Search] をクリックします。
- ステップ 2** [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 NCS 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、NCS 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 で検出されたクライアントをすべて選択します。

有線とワイヤレスを含む、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 つ持っていたとしても、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。
 -  Lightweight クライアントを示します
 -  有線クライアントを示します
 -  Autonomous クライアントを示します
- [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)。
- Protocol
 - [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。

ステップ 3

[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。次のようなさまざまなクライアント 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せん。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 アドレス
 - MAC アドレス

- バンダー
- 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
- ホスト名
- E2E
- 電力節約
- CCX
- 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



(注) ユーザ名の横にある  アイコンをクリックすると、ユーザの関連するユーザにアクセスします。

- セッション：次のクライアント セッション情報をリストします。
 - 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
 - プロファイル名
 - 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。

Statistics

[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cope：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 scope 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] ダッシュレットには、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。

[Association History] ダッシュレットには、次の情報が含まれます。

- アソシエーション時間
- 持続時間
- ユーザ名
- IP アドレス
- IP アドレス タイプ
- AP 名
- コントローラ名
- SSID

イベント

[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。

- タイムスタンプ
- 状態
- ポート タイプ
- スロット
- モジュール
- ポート
- ユーザ名

- IP アドレス
- 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 NCS 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 NCS データベースに追加する方法を説明します。

この項では、次のトピックを扱います。

- 「キャンパス マップへのビルディングの追加」(P.9-23)
- 「ビルディングの表示」(P.9-26)
- 「ビルディングの編集」(P.9-27)
- 「ビルディングの削除」(P.9-27)
- 「ビルディングの移動」(P.9-27)

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。NCS 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。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せん。

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

NCS 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。
- 連絡先
- 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。詳細については、「[Monitoring Clients and Users](#)」(P.10-10) 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](#)」(P.9-23) 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](#)」(P.9-27) 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](#)」(P.9-27) 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 リストから対象のキャンパスを選択します。
 - 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。

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、この機能はデバイスのジオメトリックロケーション座標を Geo-Location 座標（経度と緯度）に変換し、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します。



(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。

この項では、次のトピックを扱います。

- 「フロア マップへの GPS マーカーの追加」 (P.9-28)
- 「GPS マーカーの編集」 (P.9-29)
- 「フロアにある GPS マーカーの削除」 (P.9-29)

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 オプションをクリックして、[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** 左上のメニューの [Add/Edit GPS Markers Information] メニュー オプションをクリックして、[Add/Edit GPS] ページを表示します。
- ステップ 4** 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。
-

フロアにある GPS マーカーの削除

フロアにある GPS マーカーを削除するには、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 オプションをクリックして、[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) 複数の [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。
-

