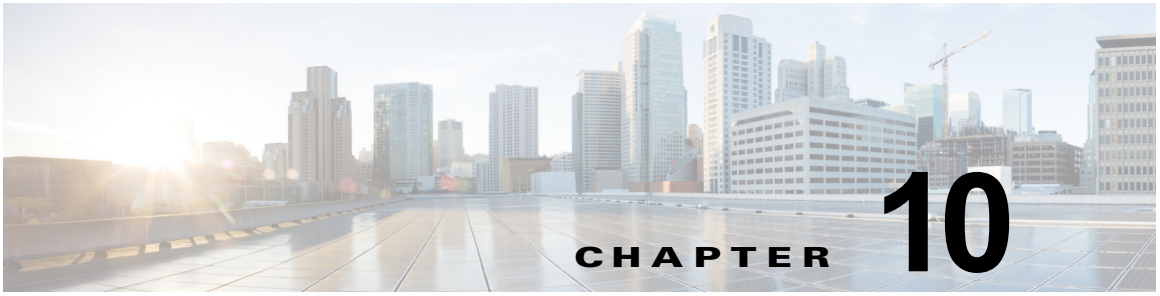

CHAPTER 10

クライアントの管理

クライアントは、アクセス ポイントまたはスイッチに接続されたデバイスです。Prime Infrastructure は、有線クライアントとワイヤレス クライアントの両方をサポートしています。コントローラおよびスイッチを Prime Infrastructure に追加すると、クライアント検出プロセスが開始されます。ワイヤレス クライアントは、管理対象のコントローラまたは Autonomous アクセス ポイントから検出されます。ワイヤレス クライアント数には、Autonomous 型のクライアントも含まれます。Prime Infrastructure では、スイッチの場合に限り、デバイスの追加直後にクライアントをポーリングします。コントローラの場合、デバイスは定期的なクライアント ステータス ポーリング時にポーリングされます。Prime Infrastructure では、スイッチからクライアント情報を取得し、データベースにこの情報を更新します。有線クライアントの場合、クライアント アソシエーションを検出するためのクライアント ステータス ポーリングは、2 時間ごとに行われます（デフォルトの場合）。すべてのスイッチについて、接続されているすべての有線クライアントの完全な情報をポーリングする完全ポーリングが、毎日 2 回実施されます。

Prime Infrastructure では、バックグラウンド タスクを使用して、データ ポーリング操作を実行します。クライアントと関連するタスクは 3 つあります。

1. Autonomous AP Client Status
2. Lighweight Client Status
3. Wired Client Status

（注） [Administration] > [Background Tasks] ページからデータ収集タスクをリフレッシュできます（ポーリング間隔など）。詳細については、「バックグラウンド タスクの実行」（P.15-1）を参照してください。

（注） Prime Infrastructure を使用すると、クライアントを追跡でき、このクライアントがネットワークに接続したときに通知を受けることができます。詳細については、「クライアントの追跡」（P.10-28）を参照してください。

（注） 有線クライアントの検出用にスイッチ上でトラップおよび Syslog を有効にするときの詳細については、「クライアントの追跡」（P.10-28）を参照してください。

802.1x を介して認証されないユーザやデバイス（プリンタなど）もあります。その場合は、ネットワーク管理者がデバイスにユーザ名を割り当てできます。詳細については、「不明デバイスの設定」（P.9-219）を参照してください。

クライアント デバイスが Web 認証を介してネットワークに認証される場合、Prime Infrastructure では、クライアントのユーザ名情報を取得できないことがあります（有線クライアントのみ該当）。

クライアント ステータス（有線クライアントのみ該当）は、接続、切断、または不明で示されます。

- [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 SNMP 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。

（注） クライアントの追跡の詳細については、「不明デバイスの設定」（P.9-219）を参照してください。

Prime Infrastructure は、アイデンティティと非アイデンティティの両方の有線クライアントをサポートしています。有線クライアントのサポートは、アイデンティティ サービスに基づきます。アイデンティティ サービスによって、ユーザおよびデバイスに対するセキュアなネットワーク アクセスが実現される他、ネットワーク管理者は、ユーザの職務権限に基づいて、サービスとリソースをユーザにプロビジョニングできるようになります。

この章の内容は、次のとおりです。

- 「クライアント ロケーション履歴の表示」（P.10-40）
- 「クライアントの音声メトリックの表示」（P.10-40）

[General] ダッシュボード上のクライアント ダッシュレット

（注）　ダッシュボード上のダッシュレットは、インタラクティブ グラフとして表示されます。詳細については、「インタラクティブ グラフ」（P.9-265）を参照してください。

Prime Infrastructure にログインすると、[General] ダッシュボードに、クライアント関連のいくつかのダッシュレットが表示されます。

- [Client Count By Association/Authentication]：選択した期間について、Prime Infrastructure でのアソシエーションおよび認証ごとのクライアントの総数が表示されます。
  - [Associated client]：認証されているかどうかに関係なく接続されているすべてのクライアント。
  - [Authenticated client]：接続されて、認証、許可、およびその他のポリシーをパスし、ネットワークを使用できる状態になったすべてのクライアント。
- [Client Count By Wireless/Wired]：選択した期間について、Prime Infrastructure での有線およびワイヤレスのクライアントの総数が表示されます。

[Client] ダッシュボード

（注）　ダッシュボード上のダッシュレットは、インタラクティブ グラフとして表示されます。詳細については、「インタラクティブ グラフ」（P.9-265）を参照してください。

Prime Infrastructure ホームページの [Client] ダッシュボードには、クライアント関連のダッシュレットが表示されます。これらのダッシュレットにより、ネットワーク上のクライアントをモニタできます。グラフ用のデータも定期的にポーリングおよび更新されて、Prime Infrastructure データベースに保存されます。一方、[Client Details] ページにある情報の大部分は、コントローラまたはスイッチから直接ポーリングされます。

[Edit Content] リンクをクリックして、[Client] ダッシュボードに表示するダッシュレットを選択します。[Available dashlets] リストからダッシュレットを選択してクリックすることにより、左方または右方の列に追加できます。[Edit Content] リンクの使用の詳細については、「ダッシュボード」（P.2-13）を参照してください。たとえば、[General] ダッシュボードと [Client] ダッシュボードの両方でクライアント数を参照する場合は、同じダッシュレットを両方に追加できます。

カスタマイズ前の元の [Client] ダッシュボードに戻すには、[Edit Tabs] をクリックしてから、[Reset to Factory Default] をクリックします。

ここでは、[Client] ダッシュボードのダッシュレットについて説明します。内容は次のとおりです。

- 「[Client Troubleshooting] ダッシュレット」（P.10-4）
- 「Client Distribution ダッシュレット」（P.10-4）
- 「[Client Alarms and Events Summary] ダッシュレット」（P.10-5）
- 「[Client Traffic] ダッシュレット」（P.10-6）

- 「[Wired Client Speed Distribution] ダッシュレット」（P.10-6）
- 「Top 5 SSIDs by Client Count」（P.10-6）
- 「Top 5 Switches by Switch Count」（P.10-7）
- 「[Client Posture Status] ダッシュレット」（P.10-7）
- 「Client Count By IP Address Type」（P.10-7）
- 「IPv6 Assignment Distribution」（P.10-7）
- 「User Auth Failure Count」（P.10-7）
- 「Client Protocol Distribution」（P.10-7）
- 「Client EAP Type Distribution」（P.10-8）
- 「Guest Users Count」（P.10-8）
- 「Client CCX Distribution」（P.10-8）
- 「Top N Client Count」（P.10-8）
- 「Client Mobility Status Distribution」（P.10-8）
- 「Client 11u Distribution」（P.10-8）
- 「11u Client Count」（P.10-8）
- 「11u Client Traffic」（P.10-8）
- 「PMIP Clients Distribution」（P.10-8）
- 「PMIP Client Count」（P.10-9）
- 「Top APs By Client Count」（P.10-9）
- 「Most Recent Client Alarms」（P.10-9）
- 「Recent 5 Guest User Accounts」（P.10-9）
- 「Latest 5 logged in Guest Users」（P.10-9）
- 「Clients Detected by Context Aware Service」（P.10-9）

[Client Troubleshooting] ダッシュレット

クライアントをトラブルシューティングするには、クライアント MAC アドレスを入力し、[Troubleshoot] をクリックします。プロパティ情報が表示されます。

（注）　クライアントが現在アソシエートされていない場合、大部分の情報は表示されません。

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、「クライアントのトラブルシューティング」（P.10-21）を参照してください。

Client Distribution ダッシュレット

このダッシュレットには、現在ネットワーク上にあるクライアントの数が表示されます。クライアントの分散方法をプロトコル、EAP タイプ、および認証タイプ別に参照できます。

- Protocol

  - [802.11] : ワイヤレス クライアント プロトコル
  - [802.3] : 有線クライアント プロトコル

（注）　プロトコルをクリックすると、そのプロトコルに属しているユーザのリストにアクセスできます。たとえば、802.3 プロトコルをクリックすると、[Clients and Users] ページの有線クライアントとユーザのリストに直接アクセスできます。

- [EAP-Type] : EAP-FAST、PEAP などの拡張認証プロトコル（EAP）タイプを表します。
- [Authentication Type] : WPA（TKIP）、WPA2（AES）、オープンなどのタイプを表します。

この情報は、選択により、表形式または円グラフで表示できます。これらの円グラフはクリックできます。円グラフの特定の部分にマウス カーソルを合わせると、見出しと割合が表示されます。円グラフの扇形の 1 つをクリックすると、フィルタされたリストが開きます。[Client Distribution] で示された数（[Client Distribution] ヘッダーの横）をクリックすると、この数によって示されているクライアントのリストが表示されます（[Monitor] > [Clients and Users] を選択した場合と同じページ）。[Dashlet Options] アイコンをクリックし、コントローラ、IP、SSID、またはフロア領域のいずれかを選択することにより、クライアントの分布状況に表示されるデータをフィルタできます。

（注）　[Client Distribution] の数の横に [Edited] というラベルがあれば、ダッシュレットはカスタマイズされています。デフォルト ページにリセットすると、[Edited] ラベルはクリアされます。

クライアント認証タイプの分布

この [Client Authentication Type] グラフには、認証タイプごとのクライアント数が表示されます。この情報は、選択により、表形式または円グラフで表示できます。[Total Clients] で示された数をクリックすると、この数によって示されているクライアントのリストが表示されます（[Monitor] > [Clients and Users] を選択した場合と同じページ）。[Dashlet Options] アイコンをクリックし、コントローラ、IP、SSID、またはフロア領域のいずれかを選択することにより、クライアントの認証タイプの分布状況に表示されるデータをフィルタできます。

[Client Alarms and Events Summary] ダッシュレット

このダッシュレットには、有線とワイヤレスの両方のクライアントについて、最新のクライアント アラームが表示されます。

- クライアント アソシエーションの失敗
- クライアント認証の失敗
- クライアント WEP キー復号化エラー
- クライアント WPA MIC エラー カウンタのアクティブ化
- クライアントの除外
- Autonomous AP クライアント認証の失敗
- 有線クライアント認証の失敗
- 有線クライアント許可の失敗
- 有線クライアントのクリティカル VLAN 割り当て
- 有線クライアントの認証失敗 VLAN 割り当て

- 有線クライアントのゲスト VLAN 割り当て
- 有線クライアントのセキュリティ違反

（注）　アラームおよびイベントの詳細については、「アラームおよびイベント一覧」（P.13-1）を参照してください。

[Total] 列の数字をクリックすると、[Events] ページ（[Monitor] > [Events] を選択した場合と同じページ）が開きます。

[Client Traffic] ダッシュレット

コントローラでは、クライアントごとの転送および受信バイト数のカウンタを保持しています。Prime Infrastructure では、15 分ごとにこの数を読み取り、直前のポーリングと比較して差異を計算します。このクライアント トラフィック データは、次に 1 時間ごと、1 日ごと、および 1 週ごとに集約されます。ダウンストリームとアップストリームの両方のトラフィックについて、平均値および最大値がメガバイト / 秒単位で表示されます。この情報は、表形式または面グラフで表示できます。フロアをベースとするグラフを生成する場合、Prime Infrastructure では、このフロア上の全クライアント トラフィックを合算します。[Dashlet Options] アイコンをクリックし、コントローラ、IP、SSID、またはフロア領域のいずれかを選択することにより、クライアント トラフィックに表示されるデータをフィルタできます。

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に必要な機能を有効にする必要があります。

[View History] をクリックすると、さまざまなタイム フレームに対する [Client Traffic Historical Charts] ダッシュレットが表示されます。[Client Traffic Historical Charts] ダッシュレットには、過去 6 時間、過去 1 日間、過去 1 週間、過去 1 ヵ月、および過去 1 年間のクライアント トラフィックが表示されます。青色の線は認証されたクライアントの数を示し、オレンジ色の線はアソシエートされたクライアントの数を示します。右上隅には、グラフの最終更新時刻が表示されます。

[Wired Client Speed Distribution] ダッシュレット

このダッシュレットは、有線クライアントの速度と、速度ごとのクライアント数を表示します。クライアントの実行速度は 3 種類あります。

- 10 Mbps
- 100 Mbps
- 1 Gbps

（注）　ポートは、デフォルトでは、自動ネゴシエーション モードです。たとえば、100 Mbps の速度で稼働するクライアントに対しては、100 Mbps の速度になります。

Top 5 SSIDs by Client Count

このダッシュレットには、現在アソシエートされているクライアントおよび認証されているクライアントの数が表示されます。この情報は、選択により、表形式または面グラフで表示できます。

（注）　Prime Infrastructure 1.0 の場合、WGB、有線ゲスト、および OEAP 600（Office Extended Access Point 600）は、ワイヤレス クライアントとして追跡されます。

Top 5 Switches by Switch Count

このダッシュレットは、クライアントの数が最も多い 5 つのスイッチ、およびスイッチにアソシエートされたクライアントの数を表示します。

[Client Posture Status] ダッシュレット

Prime Infrastructure では、アイデンティティ サービス エンジン（ISE）からポスチャ ステータス情報を収集します。許可と認証のために、ISE を追加する必要があります。ISE の追加については、「アイデンティティ サービス エンジンの追加」（P.16-114）を参照してください。ISE で、必要な機能を有効にすると、Prime Infrastructure の [Client Posture Status] ダッシュレットにデータが表示されます。

このダッシュレットは、クライアント ポスチャ ステータスと、次の各ステータス カテゴリのクライアント数を表示します。

- Compliant
- Non-compliant
- Unknown
- Pending
- Not Applicable
- Error

Client Count By IP Address Type

このダッシュレットは、各種 IP アドレス タイプ別にクライアント数のトレンドを時系列で示すグラフを表示します。タイプには、IPv4、IPv6、Dual-Stack、および unknown が含まれます。

IPv6 Assignment Distribution

このダッシュレットは、IPv6 アドレスがどのように割り当てられるかに基づき、すべてのクライアントの分布を示す円グラフを表示します。タイプには、Unknown、DHCPv6、Self-Assigned、および SLACC または Static が含まれます。

User Auth Failure Count

このダッシュレットは、ユーザ認証の失敗数のトレンドを時系列で示すグラフを表示します。

Client Protocol Distribution

このダッシュレットは、現在のクライアント数の分散をプロトコル別に表示します。

Client EAP Type Distribution

このダッシュレットは、EAP タイプに基づいた数を表示します。

Guest Users Count

このダッシュレットは、指定した期間にわたるゲスト クライアント数を表示します。

Client CCX Distribution

このダッシュレットは、各種 CCX バージョン間でのクライアントの分布を示す円グラフを表示します。

Top N Client Count

このダッシュレットは、クライアント数に基づいて、上位 N 個の要素を示す棒グラフを表示します。要素には、SSID、AP、コントローラ、エンドポイント タイプ、ベンダー、スイッチ、アンカー コントローラが含まれます。これは、個々の上位 N グラフを置き換える汎用上位 N グラフです。

Client Mobility Status Distribution

このダッシュレットは、ローカル（非アンカー）とアンカー間でのクライアント分布を示す円グラフを表示します。

Client 11u Distribution

このダッシュレットは、非 11u クライアント上の 11u クライアントを示す円グラフを表示します。

11u Client Count

このダッシュレットは、11u クライアント数のトレンドを時系列で示すグラフを表示します。

11u Client Traffic

このダッシュレットは、11u クライアント トラフィックのトレンドを時系列で示すグラフを表示します。

PMIP Clients Distribution

このダッシュレットは、非 PMIP クライアント上の PMIP クライアントを示す円グラフを表示します。

PMIP Client Count

このダッシュレットは、PMIP クライアント数のトレンドを時系列で示すグラフを表示します。

Top APs By Client Count

このダッシュレットは、上位の AP をクライアント数別に表示します。

Most Recent Client Alarms

このダッシュレットは、最新のクライアント アラームを表示します。

Recent 5 Guest User Accounts

このダッシュレットは、作成または変更された最新のゲスト ユーザ アカウントを表示します。

Latest 5 logged in Guest Users

このダッシュレットは、ログインする最新のゲスト ユーザを表示します。

Clients Detected by Context Aware Service

このダッシュレットは、過去 15 分間以内に Context Aware Service によって検出されたクライアント数を表示します。

クライアントとユーザのモニタリング

クライアントとユーザのモニタ機能を使用すると、ネットワーク内のすべてのクライアント（有線とワイヤレスの両方）を表示できます。クライアント アソシエーション履歴と統計情報を表示することもできます。これらのツールは、ユーザがラップトップ コンピュータを持って建物の中を移動したときに、ネットワークのパフォーマンスについて苦情があった場合に有用です。この情報は、カバレッジが一貫していないエリアや、カバレッジがドロップする可能性があるエリアを評価するために役立ちます。

[Client Detail] ページには、時間ベースのデータを表すためのアソシエーション履歴グラフが表示されます。この情報は、クライアントの問題の特定、診断、および解決に役立ちます。

（注） この章で説明されている機能の一部（無効化、削除など）は、有線クライアントには適用されません。

[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。[Clients and Users] ページが表示されます。[Clients and Users] ページには、クライアントが表形式で表示されており、表の上部にあるさまざまなツールを使用できます。

ここでは、次の内容について説明します。

クライアントとユーザのフィルタリング

デフォルトの [Clients and Users] リスト ページには、アソシエートされているすべてのクライアントが表示されます。プリセットされた 17 個のフィルタがあり、クライアントのサブセットを表示できます（表 10-1 を参照）。

（注） WGB、有線ゲスト、および OEAP 600（Office Extended Access Point 600）は、ワイヤレス クライアントとして追跡されます。

（注） インデックスなしの列でソートを行うと、クライアント一覧ページをロードする際に、重大なパフォーマンスの問題が発生します。Prime Infrastructure では、MAC アドレス、IP アドレス、ユーザ名、AP MAC アドレス、SSID など、インデックス付きの列のソートのみ記憶されます。それでも任意の列でテーブルをソートすることはできます。ただし、列にインデックスが付加されていない場合、このページから移動した後、Prime Infrastructure では、最後に使用した列のソートは記憶されません。

表 10-1 に、[Clients and Users] ページで使用可能なプリセット フィルタを示します。[Show] ドロップダウン リストから、表示するフィルタを選択します。

表 10-1　クライアント リスト フィルタ

フィルタ	結果
All	非アクティブなクライアントを含むすべてのクライアント。 **（注）** 通常、「All」フィルタは、フィルタなしを意味します。すべての SSID で、PMIP、WGB、有線ゲスト クライアントなど、すべてのコントローラに接続されているすべてのクライアントが返されます。
2.4 GHz Clients	2.4 GHz 無線帯域を使用しているすべてのクライアント。
5 GHz Clients	5.0 GHz 無線帯域を使用しているすべてのクライアント。
All Lightweight Clients	Lightweight AP に接続されたすべてのクライアント。
All Autonomous Clients	Autonomous AP に接続されたすべてのクライアント。
All Wired Clients	Prime Infrastructure によって管理されているスイッチに直接接続されたすべてのクライアント。

表 10-1　クライアント リスト フィルタ （続き）

フィルタ	結果
Associated Clients	認証されているかどうかにかかわらず、ネットワークに接続されているすべてのクライアントが表示されます。
Clients detected by MSE	有線クライアントおよびワイヤレス クライアントを含め、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 in last 24 hours	過去 24 時間に検出されたすべてのクライアント。
Clients Known by ISE	ISE で認証されたすべてのクライアントが表示されます。
Clients with Problems	アソシエートされている一方で、ポリシーが完了していないクライアント。
Excluded Clients	コントローラによって除外された、すべての Lightweight ワイヤレス クライアント。
FlexConnect Locally Authenticated	FlexConnect AP に接続され、ローカルで認証されたクライアント。
New Clients detected in last 24 hours	過去 24 時間に検出された新規クライアント。
On Network Clients	認証および許可を完了しており、データを送受信できるクライアント。つまり、設定されたすべてのポリシーを完了しており、ネットワーク上にあるクライアントです。クライアントはアイデンティティ クライアントではなく、常に「On Network」と表示されます。
WGB Clients	すべての WGB クライアント。 **（注）** ブリッジ機能を持つアクセス ポイントの AP モードに [Bridge] を設定すると、クライアントを WGB として識別して表示できます。WGB クライアントは、無線を有線にブリッジします。Cisco IOS アクセス ポイントはすべて、有線クライアントが接続された無線クライアントとして、WGB のロールを果たすことができます。この WGB についての情報はコントローラに伝えられ、Prime Infrastructure と WLC の両方でクライアントとして表示されます。

フィルタ アイコン（）を使用して、フィルタのルールと一致するレコードをフィルタすることもできます。フィルタのルールを指定するには、[Show] ドロップダウン リストから [All] を選択してから をクリックします。

（注） プリセット フィルタを選択してフィルタ アイコンをクリックすると、フィルタ条件は無効になります。そのフィルタ基準は参照可能ですが変更できません。[All] オプションを選択してすべてのエントリを表示し、フィルタ アイコンをクリックすると、クイック フィルタのオプションが表示されます。ここで、フィールドを使用してデータをフィルタできます。自由形式のテキスト ボックスに、表のフィルタリング用のテキストを入力することもできます。

（注） IPv6 アドレスに対する詳細クライアント フィルタリングを実行する場合、指定する各オクテットは、完全なオクテットである必要があります。オクテットの一部を指定した場合は、フィルタリングで正しい結果が表示されないことがあります。次に、IPv6 アドレスに対する詳細クライアント フィルタリングの動作の例を示します。
この例は、システムに次の IP アドレスがあることを前提としています。

```
10.10.40.1
10.10.40.2
10.10.40.3
10.10.240.1
Fec0::40:20
Fe80::240:20
```

40 を含むすべての IP アドレスを検索すると、次の結果が得られます。

```
10.10.40.1
10.10.40.2
10.10.40.3
Fec0::40:20
```

このフィルタリング機能では、完全なオクテットを入力することを前提としているため、240 を含む IP アドレスはフィルタ基準と一致しません。

クライアントとユーザの表示

（注） 詳細検索機能を使用して、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、「検索機能の使用方法」（P.2-37）または「Advanced Search」（P.2-38）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、「クライアントとユーザのフィルタリング」（P.10-10）を参照してください。

（注） 他の使用可能なクライアント パラメータについては、「検索結果表示の設定」（P.10-30）を参照してください。このクライアント リストのフィルタリングについては、「クライアントとユーザのフィルタリング」（P.10-10）を参照してください。

（注） [Monitor] > [Clients and Users] ページで完全な詳細を表示したり、無線測定などの操作を実行したりするには、ユーザ定義グループのユーザは、[Monitor Clients]、[View Alerts & Events]、[Configure Controllers]、および [Client Location] のページにアクセスする前に権限を必要とします。

クライアントおよびユーザを表示するには、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。[Clients and Users] ページが表示されます。

[Clients and Users] テーブルにはデフォルトでいくつかの列が表示されます。使用可能な追加の列を表示するには、 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。

[Clients and Users] テーブルには、次の列があります。

- [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] フィールドに表示されます。

  - IPv4 アドレス。
  - IPv6 固有グローバル 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、いずれ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 固有ローカル アドレス。IPv6 固有ローカル アドレスが複数存在する場合は、最新のアドレスが使用されます。
  - IPv6 リンクローカル アドレス。IPv6 クライアントは、常にリンクローカル アドレスを少なくとも 1 つ持ちます。

  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。
  - グローバル ユニキャスト：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識別します。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。

  （注） 同じタイプの IP アドレスが複数ある場合は、そのタイプで最新の IP アドレスのみが表示され、それ以外のアドレスは、[QuickView (+)] アイコンにマウス カーソルを合わせたときに [QuickView] ページに表示されます。

- [IP Address Type]：IPv4、IPv6 などの IP アドレス タイプ。
- [Global Unique]：IPv6 アドレスの集約グローバル ユニキャスト アドレス。このフィールドには、クライアントにグローバル固有 IPv6 アドレスが割り当てられている場合のみ値が入力されます。
- [Unique Local]：IPv6 アドレスのローカル ユニキャスト アドレス。このフィールドには、クライアントにローカル固有 IPv6 アドレスが割り当てられている場合のみ値が入力されます。
- [Link Local]：IPv6 アドレスのリンクローカル ユニキャスト アドレス。このフィールドには、クライアントにリンクローカル IPv6 アドレスが割り当てられている場合のみ値が入力されます。
- [User Name]：802.1x 認証または Web 認証に基づくユーザ名。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。
- [AP Name]：ワイヤレスのみ
- [Device Name]：WLC、スイッチなどのネットワーク認証デバイス名。
- [Location]：接続しているデバイスのマップ位置。
- [ISE]：[Yes] または [No]。この列は、Prime Infrastructure に追加されている ISE を使用してクライアントが認証されているかどうかを示します。
- [Endpoint Type]：ISE が追加されている場合に限り適用される、ISE によって報告されるエンドポイント タイプ（iPhone、iPad、Windows ワークステーションなど）。
- [Posture]：最新のクライアント ポスチャ ステータス
- [SSID]：ワイヤレスのみ
- [Profile Name]：ワイヤレスのみ
- [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 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 認証完了。
  - [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。
  - [Power Save]：クライアントを省電力モードで実行しています。
  - [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削除されるクライアント。
  - [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
- [Speed]：イーサネット ポートの速度（有線のみ）。ワイヤレスの場合は「N/A」が表示されます。
- [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、この列は空になります。
- [Session Length]：セッションの長さ。
- [First Seen]：クライアントが最初に検出された日時が表示されます。
- [Authentication Type]：WPA、WPA2、802.1x、MAC 認証バイパス、または Web 認証。
- [Authorization Profile Names]：ISE によってこのクライアントに適用された許可プロファイル。ISE が追加されており、クライアントが ISE によって認証されている場合に限り、データを含みます。
- [Traffic (MB)]：このセッションの MB 単位のトラフィック（送信または受信）
- [Average Session Throughput (kbps)]：kbps 単位の平均セッション スループット。

- [Automated Test Run]：クライアントが自動テスト モードかどうかを示します。ワイヤレス クライアントのみに適用されます。
- [AP MAC Address]：ワイヤレスのみ。
- [AP IP Address]：ワイヤレスのみ。
- [Anchor Controller]：Lightweight ワイヤレスのみ。
- [On Network]：関連付けられており、必要に応じて認証が正常に完了しているクライアントに対して [Yes] が表示されます。
- [CCX]：Lightweight ワイヤレスのみ。
- [Client Host Name]：有線およびワイヤレス。DNS 逆引きの結果です。
- [Device IP Address]：接続されたデバイスの IP アドレス（WLC、スイッチ、または Autonomous AP）。
- [Port]：WLC 上のスイッチ ポート。
- [E2E]：Lightweight ワイヤレスのみ。
- [Encryption Cipher]：ワイヤレスのみ。
- [MSE]：このクライアントを管理している MSE サーバ。
- [RSSI]：ワイヤレスのみ。
- [SNR]：ワイヤレスのみ。
- [Router Advertisements Dropped]：特定のセッションを対象とする、クライアントごとのドロップされたルータ アドバタイズメントの数。
- [Session ID]：ISE およびスイッチで使用される監査セッション ID。
- [FlexConnect Local Authentication]：このクライアントに対して FlexConnect ローカル認証が有効かどうかを示します。
- [WGB Status]：Work Group Bridge（WGB）モードのステータスを示します。
- [Mobility Status]：ワイヤレス クライアントのモビリティ ステータスを示します。
- [SNMP NAC State]：アウトオブバンド モードの NAC アプライアンスのステータスを示します。

ステップ 2　クライアントまたはユーザを選択します。次の情報が表示されます。

- 「クライアント属性」（P.10-16）
- 「クライアント統計情報」（P.10-17）

（注）　[Client Statistics] には、クライアント詳細の表示に続いて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」（P.10-17）
- 「クライアント イベント情報」（P.10-18）
- 「クライアント ロケーション情報」（P.10-19）
- 「有線ロケーション履歴」（P.10-19）
- 「クライアント CCXv5 情報」（P.10-20）

次の属性は、ISE が Prime Infrastructure に追加された場合にのみ設定されます。

- ISE

- エンドポイント タイプ
- ポスチャ
- 許可プロファイル名

（注） Prime Infrastructure は、このデータを設定するために、最近 24 時間のクライアント認証レコードを ISE に問い合わせます。Prime Infrastructure での検出の 24 時間前にクライアントがネットワークに接続されていた場合、ISE 関連データはこのテーブルには表示されない場合があります。このデータは、クライアント詳細ページに表示される可能性があります。これを回避するには、クライアントをネットワークに接続し直します。次回のクライアント バックグランド タスクの実行後に、ISE 情報がテーブルに表示されます。

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、[Clients and Users] リストにクライアント属性が表示されます。クライアントは、MAC アドレスを使用して特定されます。

（注） [Client Attributes] グループ ボックスに表示される詳細情報はデバイスから取得される一方で、[Clients and Users] リストに表示される詳細情報はデータベースから取得されます。したがって、[Clients and Users] リストと [Client Attributes] グループ ボックスでは、表示される詳細情報が食い違うこと場合があります。

（注） 有線クライアントの場合、この情報はスイッチから取得されます。また、詳細ページに表示されるデータは、コントローラ/スイッチ/ISE からオンデマンドで収集されたライブ データです。

これらの詳細には、次のクライアント詳細が含まれます。

- [General]：ユーザ名、MAC アドレスなどの生成情報をリストします。

  （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。

- [Session]：クライアント セッション情報をリストします。
- [Security]（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）：セキュリティ ポリシー、認証情報、および EAP タイプをリストします。

  （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） [Client Attributes] グループ ボックスに表示されるデータは、クライアントのタイプ、つまりアイデンティティ クライアントなのか非アイデンティティ クライアントなのかに応じて異なります。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。

（注）　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。

クライアント IPv6 アドレス

[Clients and Users] リストから IPv6 クライアントを選択すると、クライアント IPv6 アドレスの詳細が表示されます。この詳細情報は、コントローラから直接取得されています。

IPv6 アドレスを持つ有線クライアントの場合、Prime Infrastructure では、スイッチ上の IPv6 ネイバーテーブルからクライアント アドレスを検出します。

この詳細には、次の情報が含まれます。

- IP アドレス：クライアントの IPv6 アドレス。
- スコープ
- アドレス タイプ
- 検出時間

クライアント統計情報

クライアント統計情報には、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。
- 経時データ レート

（注）　グラフ上にマウス カーソルを合わせると、その他の統計情報が表示されます。

（注）　この情報は、インタラクティブ グラフで表示されます。詳細については、「インタラクティブ グラフ」（P.9-265）を参照してください。

クライアント 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に役立つことがあります。

- クライアント アソシエーション履歴（ワイヤレス クライアントの場合）には、次の情報が含まれます。
  - アソシエーションの日付と時刻
  - アソシエーションの期間
  - ユーザ名
  - IP アドレス
  - アクセス ポイント名
  - コントローラ名
  - SSID
  - プロトコル
  - トラフィックの量（MB）
  - ホスト名
  - ローミング理由（*コントローラから認識されなくなった、新規アソシエーションを検出したなど*）
- クライアント アソシエーション履歴（有線クライアントの場合）には、次の情報が含まれます。
  - アソシエーションの日付と時刻
  - アソシエーションの期間
  - ユーザ名
  - IP アドレス
  - アクセス ポイントおよびコントローラ名
  - マップ ロケーション
  - SSID
  - プロトコル
  - トラフィックの量（MB）
  - ホスト名
  - ローミング理由（*コントローラから認識されなくなった、新規アソシエーションを検出したなど*）

（注） [Current Associated Clients] テーブルの列を追加、削除、順序変更するには、[Edit View] リンクをクリックします。[Edit View] から追加できる以外の新規パラメータの追加については、「アクセス ポイント リストの表示の設定」（P.5-46）を参照してください。

クライアント イベント情報

[Client Details] ページの [Client Event] ダッシュレットには、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 タイプの詳細を表示するには、イベント タイプをクリックします。詳細については、「障害のあるオブジェクトのモニタリング」（P.5-146）を参照してください。

クライアント ロケーション情報

選択したクライアントの次のロケーション パラメータが表示されます（該当する場合）。

- [Map Area]：クライアントが最後に検出されたマップ領域。
- [ELIN]：緊急ロケーション識別番号。MSE によって検出される有線クライアントのみに適用されます。
- [Civic Address]：[Civic Address] タブにあるフィールドは、クライアントの Civic アドレスがインポートされている場合のみ入力されます。MSE によって検出される有線クライアントのみに適用されます。
- [Advanced]：クライアントの詳細情報。このタブにあるフィールドは、クライアントの Civic アドレスがインポートされている場合のみ入力されます。

クライアントの Civic 情報をインポートするときに詳細については、「スイッチ ロケーションの設定」（P.9-216）を参照してください。

有線ロケーション履歴

有線クライアントのロケーション履歴を表示できます。

（注）　有線クライアントは MSE によって検出されている必要があり、有線クライアントの履歴が MSE で有効化されている必要があります。

クライアントに関する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
- ステート
- 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 ロケーション
- 都市ロケーション

ワイヤレス ロケーション履歴

ワイヤレス クライアントのロケーション履歴を表示できます。

（注）　ワイヤレス クライアントは MSE によって検出されている必要があり、有線クライアントの履歴が MSE で有効化されている必要があります。

クライアント CCXv5 情報

CCXv5 クライアントは、Cisco Compatible Extensions バージョン 5（CCXv5）をサポートするクライアント デバイスです。CCXv5 クライアントに固有のレポートにより、クライアントの診断およびトラブルシューティングを強化するクライアントの詳細が提供されます。

（注）　CCXv5 製造元情報は、CCXv5 クライアントの場合のみ表示されます。

特定のクライアント詳細を表示するには、該当する検索パラメータを使用して、クライアント検索を実行します。クライアント検索の実行の詳細については、「クライアント CCXv5 情報」（P.10-20）または 「Advanced Search」（P.2-38）を参照してください。

CCXv5 情報は、[Monitor Clients] > [Client Details] ページに表示されます。CCXv5 情報には次のような内容が含まれます。

CCXv5 製造元情報：

- [Organizationally Unique Identifier]：IEEE によって割り当てられた組織固有識別子。無線ネットワーク接続デバイスの MAC アドレスの最初の 3 バイトなど。
- [ID]：無線ネットワーク アダプタの製造業者 ID。
- [Model]：無線ネットワーク アダプタのモデル。
- [Serial Number]：無線ネットワーク アダプタのシリアル番号。
- [Radio]：クライアントの無線の種類。
- [MAC Address]：クライアントに割り当てられた MAC アドレス。
- [Antenna Type]：無線ネットワーク アダプタに接続されるアンテナの種類。
- [Antenna Gain]：無線ネットワーク アダプタに接続される指向性アンテナのピーク ゲイン（dBi）、および全方向性アンテナの平均ゲイン（dBi）。ゲインは 0.5dBi の倍数で表します。整数値 4 は、4 X 0.5 = 2dBi のゲインであることを意味します。

（注）　次の付加的な CCXv5 パラメータを表示するには、[More] をクリックします。

[Automated Troubleshooting Report]：自動テストが実行された場合、このレポートには、自動トラブルシューティングのログである AUTO_TS_LOG<ClientMac>.txt の場所が表示されます。自動テストが実行されていない場合は [Not Exists] が表示されます。

- [Export] をクリックして .zip ファイルを保存します。ファイルには、自動トラブルシューティング レポート、フレーム ログ、およびウォッチ リスト ログの 3 つのログが含まれます。

（注）　[Settings] > [Client] ページでは、診断チャネル上で自動クライアント トラブルシューティングを有効にできます。これらの機能は、Cisco Compatible Extensions クライアント バージョン 5 だけでサポートされています。詳細については、「診断トラップの処理」（P.15-59）を参照してください。

[Radio Receiver Sensitivity]：次の情報を含む、ワイヤレス ネットワーク アダプタの受信装置の感度が表示されます。

- 無線
- データ レート
- 最小および最大 RSSI

[CCXV5 Capability Information]：CCXv5 クライアントに限り、Capability Information パラメータが表示されます。

- Radio
- [Client Status]：成功または失敗。
- [Service Capability]：音声、ストリーミング（一方向）ビデオ、インタラクティブ（双方向）ビデオなどのサービス機能。

[Radio Channels]：該当する各無線のチャネルを識別します。

[Transmit Data Rates]：各無線の伝送データ レート（Mbps）を識別します。

[Transmit Power Values]：次の情報を含む送信電力を示します。

- 電源モード
- 無線
- 電力（dBm）

クライアントとユーザのエクスポート

クライアントとユーザのリストを CSV ファイル（カンマ区切りの値を含むスプレッドシート形式）に簡単にエクスポートできます。

（注） [Clients and Users] テーブルに表示される列は、CSV ファイルのみにエクスポートされます。

クライアントとユーザのリストをエクスポートするには、次の手順を実行します。

ステップ 1　[Monitor] > [Clients and Users] を選択します。

ステップ 2　ツールバーで アイコンをクリックします。ダイアログボックスが表示されます。

ステップ 3　[File Download] ダイアログボックスで、[Save] をクリックします。

クライアントのトラブルシューティング

トラブルシューティングは、[Client] ダッシュボードで MAC アドレスを入力する、検索機能を使用する、または [Monitor] > [Clients and Users] ページで行を選択するという、複数の方法で開始できます。これらの方法のいずれかにより、クライアントの履歴問題をトラブルシューティングするために必要なすべての情報が提供されます。接続のステータスのモニタ、ユーザの現在および過去のロケーションの確認、クライアントの接続に関する問題のトラブルシューティングができます。クライアント トラブルシューティング オプションは、ユーザが接続の問題を繰り返し経験する場合などに必要になります。[Client Details] ページには、SNR の経時変化、RSSI の経時変化、クライアントの再アソシエーション、クライアントの再認証、およびすべての RRM イベントが表示されます。管理者は、再アソシエーションと再認証を関連付け、問題がネットワークにあるか、クライアントにあるかを判別できます。

（注） トラブルシューティングできるのは、現在のクライアントの問題のみです。クライアントの履歴上の問題は、トラブルシューティングできません。ただし、ロケーション アシストされるクライアントの場合、ロケーション履歴を確認できます。

（注）　クライアントのトラブルシューティング機能は、アイデンティティ有線クライアントに対してのみ使用できます。この機能は、非アイデンティティ有線クライアントに対しては使用できません。

Prime Infrastructure では、有線およびワイヤレスのデバイスまたはクライアントを統合管理できます。有線クライアントとワイヤレス クライアントの両方をモニタおよびトラブルシューティングできます。SNMP は、クライアントの検出とクライアント データの収集に使用されます。クライアント統計情報およびその他の属性を収集して、関連するダッシュボードのダッシュレットおよびレポートにデータを入力するために、ISE は定期的にポーリングされます。ISE がシステムに追加されており、デバイスを ISE で認証している場合は、[Client Details] ページにセキュリティ情報が表示されます。

[Client Troubleshooting] ツールを起動するには、クライアントを選択してから、トラブルシューティングする IP アドレスの上に表示されている  アイコンをクリックします。[Troubleshooting Client] ページが表示されます。

トラブルシューティング ページには、有線クライアントの次の状態が表示されます。

- リンク接続
- 802.1X 認証
- MAC 認証
- Web 認証
- IP 接続
- 許可
- 正常接続

（注）　表示される正確な状態は、そのクライアントで使用しているセキュリティのレベルによって異なります。

クライアントでは、次のセキュリティ メカニズムが使用されます。

- 802.1X
- MAC 認証
- Web 認証

表 10-2 に、セキュリティ タイプに対して有効な状態をまとめてあります。状態は、クライアントのたどる順に並べてあります。

表 10-2　セキュリティ メカニズム

セキュリティ / クライアント状態	リンク接続	802.1X 認証	MAC 認証	Web 認証	IP 接続	許可
802.1X	X	X	–	–	X	X
MAC 認証	X	–	X	–	X	X
Web 認証	X	–	–	X	X	X

表 10-3 に、クライアントが失敗したときの状態に応じた問題と推奨措置をリストします。

表 10-3　クライアントの状態、問題、および推奨措置

クライアントの状態	問題	推奨措置
Link Connectivity	ネットワークでクライアントが見つからない	• クライアントのケーブルがネットワークに接続されているかどうかを確認します。 • クライアントで適切なケーブルを使用してネットワークに接続しているかどうかを確認します。 • クライアントの接続先のポートが管理目的で無効になっていないことを確認します。 • クライアントの接続先のポートがエラーによって無効になっていないことを確認します。 • クライアントの接続先のポートで、速度およびデュプレックスが自動に設定されているかどうかを確認します。
	認証の進行中	• クライアントが長時間この状態の場合は、次の点を確認します。 – クライアント上のサプリカントが必要に応じて適切に設定されているかどうかを確認します。 – 認証方式に関連するタイマーを変更し、再試行します。 – そのクライアントで機能する認証方式が不明な場合は、フォールバック認証機能を使用します。 – 切断と再接続を試行します。
802.1X Authentication	802.1X 認証の失敗	• スイッチから RADIUS サーバに到達可能かどうかを確認します。 • クライアントで選択されている EAP が RADIUS サーバでサポートされているかどうかを確認します。 • クライアントのユーザ名、パスワード、証明書が有効かどうかを確認します。 • RADIUS サーバで使用している証明書をクライアントで受け入れているかどうかを確認します。
MAC Authentication	MAC 認証の失敗	• スイッチから RADIUS サーバに到達可能かどうかを確認します。 • クライアントの MAC アドレスが RADIUS サーバにある既知クライアントのリストにあるかどうかを確認します。 • クライアントの MAC アドレスが除外されたクライアントのリストにないことを確認します。

表 10-3　クライアントの状態、問題、および推奨措置 （続き）

クライアントの状態	問題	推奨措置
Web Authentication	Web/ゲスト インターフェイスを介してクライアントを認証できない	• ゲスト クレデンシャルが有効であり、期限が切れていないことを確認します。 • クライアントをログイン ページにリダイレクトできるかどうかを確認します。 • RADIUS サーバに到達可能かどうかを確認します。 • ポップアップがブロックされていないことを確認します。 • クライアント上の DNS 解決が機能することを確認します。 • クライアントでいずれのプロキシ設定も使用していないことを確認します。 • クライアントで https://<virtual-ip>/login.html にアクセスできるかどうかを確認します。 • クライアントのブラウザで、コントローラの提供する自己署名証明書を受け入れるかどうかを確認します。
IP Connectivity	クライアントで DHCP インタラクションを完了できない	• DHCP サーバに到達可能かどうかを確認します。 • その WLAN で使用できるように DHCP サーバが設定されているかどうかを確認します。 • DHCP スコープをすべて使用したかどうかを確認します。 • 複数の DHCP サーバでオーバーラップするスコープが設定されているかどうかを確認します。 • DHCP ブリッジ モードが有効にされている（このサーバをセカンドに移動）場合に、ローカル DHCP サーバがあることを確認します。DHCP サーバからアドレスを取得するようにクライアントが設定されていることを確認します。 • クライアントに静的 IP が設定されており、クライアントで IP トラフィックを生成しているかどうかを確認します。
Authorization	許可の失敗	• 許可用に定義されている VLAN がスイッチで使用可能であることを確認します。 • デフォルト ポート ACL が ACL 許可用に設定されていることを確認します。
Successful Connection	なし	なし。

検索機能を使用したクライアントのトラブルシューティング

クライアント検索の主目的はクライアントの場所を見つけることです。検索機能の詳細説明については、「検索機能の使用方法」（P.2-37）を参照してください。

検索機能を使用してクライアントをトラブルシューティングするには、次の手順に従います。

ステップ 1　[Monitor] > [Clients and Users] を選択します。

ステップ 2　[Advanced Search] テキスト ボックスにクライアント MAC アドレスの全体または一部を入力して、[Search] をクリックします。[Search Results] ページが表示されます。

ステップ 3　[View List] をクリックすると、検索基準と一致するクライアントが [Clients] ページに表示されます。[Monitor] > [Clients and Users] ページが表示されます。

（注）　[Reset] リンクをクリックすると、テーブルをデフォルト表示に設定して、検索基準の適用をやめることができます。

ステップ 4　クライアントを選択してから、トラブルシューティングする IP アドレスの上に表示されている  アイコンをクリックします。[Troubleshooting Client] ページが表示されます。Cisco Compatible Extension v5 クライアント（ワイヤレス）をトラブルシューティングする場合は、[Troubleshooting Client] ページに追加のタブが表示されます。

（注）　クライアントがいずれのアクセス ポイントにも接続されていないというメッセージを受け取る場合は、クライアントを接続し直して [Refresh] をクリックします。

（注）　ページの右上隅にある [detach]/[clone] アイコンを使用すると、現在のページを新しいウィンドウまたはタブとして切り離すことができます。

（注）　クライアント トラブルシューティングを起動したページに戻るには、[Go back] をクリックします。たとえば、リスト ページからクライアントのトラブルシューティングを起動した場合、そのリスト ページに戻ることができます。

要約ページでは、問題が簡単に説明され、一連の操作を行うよう推奨されます。

（注）　Windows ワークステーションで Mozilla Firefox 11.0 以降または Internet Explorer 8 以降以外の Web ブラウザを使用している場合、一部の Cisco Compatible Extension 機能は正しく動作しません。

ステップ 5　クライアントに対して記録されたログ メッセージを表示するには、[Log Analysis] タブをクリックします。

ステップ 6　クライアントに関するログ メッセージをコントローラから取得するには、[Start] をクリックします。ログ メッセージの取得を停止するには、[Stop] をクリックします。すべてのログ メッセージをクリアするには、[Clear] をクリックします。

（注）　ログ メッセージは 10 分間取得され、自動的に停止されます。続行するには、[Start] をクリックする必要があります。

ステップ 7　表示するログ メッセージを選択するには、[Select Log Messages] の下にあるいずれかのリンクをクリックします（カッコ内の数字はメッセージの数を示します）。メッセージはグループ ボックス内に表示されます。メッセージに含まれる情報は、次のとおりです。

- ステータス メッセージ
- コントローラの時刻
- 情報またはエラーの重大度レベル（エラーの表示は赤）
- クライアントに接続されているコントローラ

ステップ 8　クライアントのイベント履歴を表示するには、[Event History] タブをクリックします。

[Event History] には、このクライアントの接続イベントに関連するメッセージが表示されます。この例では、クライアントは正常に認証できませんでした。日時情報は、ネットワーク管理者によるこのクライアントのトラブルシューティング用です。

ステップ 9　イベント ログを表示するには、[Event Log] タブをクリックします。クライアントからのログ メッセージの取得を開始するには、[Start] をクリックします。十分な数のメッセージが収集されたら、[Stop] をクリックします。

（注）　クライアント トラブルシューティング イベント ログおよびメッセージング機能は、Management Service のバージョンが 2 以降の場合のみ CCX バージョン 6 クライアントに対して使用できます。

ステップ 10　[ACS View Server] タブをクリックすると、Cisco Access Control System（ACS）View Server と対話できます。このタブには、ACS View サーバまたはアイデンティティ サービス エンジン（ISE）のいずれか（Prime Infrastructure に設定されている方）から受信した最新の認証レコードが表示されます。このタブにアクセスする前に、View Server クレデンシャルを確立する必要があります。（View Server が設定されていない場合、このタブには空白のサーバ リストが表示されます）。クレデンシャル確立の手順は、「ACS View Server クレデンシャルの設定」（P.9-264）を参照してください。

ACS View サーバがすでに設定されている場合は、期間を選択し、[Submit] をクリックして、ACS View サーバから認証レコードを取得できます。Prime Infrastructure では、記録の取得に ACS View NS API が使用されます。

ステップ 11　[Identity Services Engine] タブをクリックすると、ISE 認証に関する情報を表示できます。過去の認証および許可に関する情報を取得する日付と時刻の範囲を入力し、[Submit] をクリックします。照会の結果は、ページの [Authentication Records] 部分に表示されます。

ステップ 12　[CleanAir] タブをクリックすると、電波品質パラメータおよび CleanAir 対応のアクセス ポイントに対するアクティブな干渉に関する情報を表示できます。このタブには、CleanAir 対応のアクセス ポイントによって検出された電波品質に関する次の情報があります。

- [AP Name]：アクセス ポイントの詳細を表示する場合にクリックします。詳細については、「アクセス ポイントの詳細のモニタリング」（P.5-57）を参照してください。
- AP MAC Address
- Radio
- [CleanAir Capable]：アクセス ポイントが CleanAir 対応かどうかを示します。
- [CleanAir Enabled]：アクセス ポイントで CleanAir が有効になっているかどうかを示します。
- [Admin Status]：有効または無効。

- [Operational Status]：Cisco Radio の動作ステータス（[Up] または [Down]）を表示します。
- [Channel]：Cisco Radio がブロードキャストしているチャネル。
- [Extension Channel]：Cisco Radio がブロードキャストしているセカンダリ チャネルを示します。
- [Channel Width]：この無線インターフェイスのチャネル帯域幅を示します。チャネル帯域幅の設定の詳細については、「802.11a/n RRM 動的チャネル割り当ての設定」（P.9-134）を参照してください。
- [Power Level]：アクセス ポイントの送信電力レベル：1 = 国コード設定で許可される最大電力、2 = 50 % の電力、3 = 25 % の電力、4 = 6.25 ～ 12.5 % の電力、5 = 0.195 ～ 6.25 % の電力。
- 電力レベルおよび使用可能なチャネルは国コード設定によって定義されており、国別に規制されています。
- [Average AQ Index]：Air Quality インデックスの平均値。
- [Minimum AQ Index]：Air Quality インデックスの最小値。

アクティブな干渉に関する次の情報が表示されます。

- [Interferer Name]：干渉デバイスの名前。
- [Affected Channels]：干渉デバイスが影響を与えているチャネル。
- [Detected Time]：干渉源が検出された時刻。
- [Severity]：干渉デバイスの重大度インデックス。
- [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）。
- [RSSI(dBm)]：干渉しているデバイスの受信信号強度。
- Air Quality インデックスの詳細を参照するには、[CleanAir Details] をクリックします。

ステップ 13　（任意）Cisco Compatible Extension バージョン 5 またはバージョン 6 クライアントが使用可能な場合、[Test Analysis] タブをクリックできます。

（注）　クライアント トラブルシューティング テスト解析機能は、Management Service のバージョンが 2 以降の場合のみ CCX バージョン 6 クライアントに対して使用できます。

[Test Analysis] タブにより、クライアントでさまざまな診断テストを実行することができます。適用可能な診断テストのチェックボックスをオンにし、該当するすべての入力情報を入力して、[Start] をクリックします。次のような診断テストが用意されています。

- [DHCP]：完全な DHCP の Discover/Offer/Request/ACK 交換を実行し、コントローラとクライアント間で DHCP が正常に動作しているかどうかを判別します。
- [IP Connectivity]：クライアントに DHCP テストで取得したデフォルト ゲートウェイの ping テストを実行させ、ローカル サブネットに IP 接続が存在しているかどうかを確認します。
- [DNS Ping]：クライアントに DHCP テストで取得した DNS サーバの ping テストを実行させ、DNS サーバとの IP 接続が存在しているかどうかを確認します。
- [DNS Resolution]：DNS クライアントに解決可能であることがわかっているネットワーク名の解決を試行させ、名前解決が正常に機能しているかどうかを確認します。
- [802.11 Association]：特定のアクセス ポイントとのアソシエーションを完了させ、クライアントが指定した WLAN と適切にアソシエートできるかどうかを確認します。
- [802.1X Authentication]：特定のアクセス ポイントとのアソシエーションおよび 802.1X 認証を完了させ、クライアントが適切に 802.1X 認証を完了できるかどうかを確認します。

- [Profile Redirect]：診断システムは、いつでもクライアントに対して、設定済み WLAN プロファイルのいずれかをアクティブにし、そのプロファイルにより動作を継続するよう指示できます。

（注）　プロファイルの診断テストを実行する場合、クライアントは診断チャネル上になければなりません。このテストでは、プロファイル番号を入力として使用します。ワイルドカード リダイレクトを指定するには、0 を入力します。このリダイレクトによって、クライアントは診断チャネルとのアソシエーションを解除し、任意のプロファイルとアソシエートすることを求められます。また、有効なプロファイル ID を入力することもできます。テストが実行されているときにクライアントが診断チャネル上にあるため、プロファイル リストで返されるプロファイルは 1 つだけです。プロファイル リダイレクト テストでは、このプロファイル ID を使用する必要があります（ワイルドカード リダイレクトが必要でない場合）。

ステップ 14　（任意）Cisco Compatible Extension バージョン 5 またはバージョン 6 クライアントが使用可能な場合は、[Messaging] タブが表示されます。このタブを使用して、即時にテキスト メッセージをこのクライアントのユーザに送信できます。[Message Category] ドロップダウン リストからメッセージを選択し、[Send] をクリックします。

（注）　クライアント トラブルシューティング イベント ログおよびメッセージング機能は、Management Service のバージョンが 2 以降の場合のみ CCX バージョン 6 クライアントに対して使用できます。

ステップ 15　[Identity Services Engine] タブをクリックすると、アイデンティティ サービス パラメータに関する情報を表示できます。このタブにアクセスするには、まずアイデンティティ サービス エンジン（ISE）を設定する必要があります。（ISE が設定されていない場合、このタブのサーバ リストは空になります）。

（注）　ISE が設定されていない場合は、ISE を Prime Infrastructure に追加するためのリンクが表示されます。

ISE では、REST API を介して Prime Infrastructure に認証レコードを渡します。ネットワーク管理者は ISE から認証レコードを取得するための期間を選択できます。

ステップ 16　クライアント ロケーション履歴を表示するには、[Context Aware History] タブをクリックします。

ステップ 17　[Troubleshooting Client] ページを閉じます。

クライアントの追跡

この機能を使用すると、クライアントを追跡でき、このクライアントがネットワークに接続したときに通知を受けることができます。

クライアントを追跡するには、次の手順を実行します。

ステップ 1　[Monitor] > [Clients and Users] を選択します。

ステップ 2　[Track Clients] をクリックします。現在追跡されているクライアントをリストした [Track Clients] ダイアログボックスが表示されます。

ヒント このテーブルは、最大 2000 行に対応しています。新規の行を追加またはインポートするには、古いエントリをいくつか削除する必要があります。

ステップ 3　単一のクライアントを追跡するには、[Add] をクリックしてから、次のパラメータを入力します。

- Client MAC address
- [Expiration]：[Never] を選択するか、日付を入力します。

ステップ 4　複数のクライアントを追跡するには、[Import] をクリックします。これにより、CSV ファイルからクライアント リストをインポートできます。MAC アドレスおよびユーザ名を入力します。

データ形式を規定した、サンプル CSV ファイルをダウンロードできます。

```
# MACAddress, Expiration: Never/Date in MM/DD/YYYY format
00:40:96:b6:02:cc,10/07/2010
00:02:8a:a2:2e:60,Never
```

通知設定

クライアント追跡用の通知設定を指定するには、次の手順を実行します。

ステップ 1　[Monitor] > [Clients and Users] を選択します。

ステップ 2　[Track Clients] をクリックします。現在追跡されているクライアントをリストした [Track Clients] ダイアログボックスが表示されます。

ステップ 3　通知設定を指定する、追跡されるクライアントを選択します。

ステップ 4　通知設定を指定します。通知のオプションは 3 つあります。

a. [Purged Expired Entries]：追跡対象クライアントを Prime Infrastructure データベースに保持する期間を設定できます。クライアントは、次の期間で削除できます。

- 1 週間後
- 2 週間後
- 1 ヵ月後
- 2 ヵ月後
- 6 ヵ月後
- 無期限で保持

b. [Notification Frequency] : Prime Infrastructure で追跡対象クライアントの通知をいつ送信するかを指定できます。

- 最初の検出時
- 検出ごと

c. [Notification Method]：追跡対象クライアント イベントによりアラームを生成するか、電子メールを送信するか指定できます。

ステップ 5　[Save] をクリックします。

不明ユーザの識別

802.1x を介して認証されないユーザやデバイス（プリンタなど）もあります。その場合は、ネットワーク管理者がデバイスにユーザ名を割り当てできます。

クライアント デバイスが Web 認証を介してネットワークに認証される場合、Prime Infrastructure では、クライアントのユーザ名情報を取得できないことがあります（有線クライアントのみ該当）。

クライアントは、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ます。クライアント ステータス（有線クライアントのみ該当）は、接続、切断、または不明で示されます。

- [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。

不明なデバイスを表示するには、次の手順を実行します。

ステップ 1　[Monitor] > [Clients and Users] を選択します。

ステップ 2　[Identify Unknown Users] をクリックします。

ステップ 3　クライアント MAC アドレスをユーザ名に割り当てるには、[Add] をクリックします。

ステップ 4　MAC アドレスおよびユーザ名を入力します。

（注）　クライアントおよび MAC アドレスが追加されると、Prime Infrastructure では、MAC アドレスの照合に基づくクライアントの検索に、このデータが使用されます。

ステップ 5　[Add] をクリックします。

ステップ 6　ステップ 3 からステップ 5 を繰り返して、各クライアントの MAC アドレスおよび対応するユーザ名を入力します。

ステップ 7　[Save] をクリックします。

（注）　このテーブルは、最大 10,000 行に対応しています。新規の行を追加またはインポートするには、古いエントリをいくつか削除する必要があります。

検索結果表示の設定

[Edit View] ページでは、[Clients] テーブルの列を追加、削除、または並べ替えができます。

[Clients] テーブルの使用可能な列を編集するには、次の手順を実行します。

ステップ 1　[Monitor] > [Clients and Users] を選択します。

ステップ 2　[Edit View] リンクをクリックします。

ステップ 3　[Clients] テーブルに新しい列を追加するには、左側の領域で、追加する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 [Clients] テーブルに表示されます。

ステップ 4　[Clients] テーブル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 [Clients] テーブルに表示されません。

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。

（注）　付加的なクライアント パラメータには、AP MAC Address、Anchor Controller、Authenticated、CCX、Client Host Name、Controller IP Address、Controller Port、E2E、Encryption Cipher、MSE、RSSI、SNR、および FlexConnect Local Authentication があります。

自動クライアント トラブルシューティングの有効化

[Settings] > [Client] ページでは、診断チャネルでの自動クライアント トラブルシューティングを有効にできます。これらの機能は、Cisco Compatible Extensions クライアント バージョン 5 だけでサポートされています。

自動クライアント トラブルシューティングを有効にするには、次の手順を実行します。

ステップ 1　[Administration] > [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、[Client] を選択します。

ステップ 3　[Automatically troubleshoot client on diagnostic channel] チェックボックスをオンにします。

（注）　このチェックボックスがオンの場合、Prime Infrastructure は診断アソシエーション トラップを処理します。このチェックボックスがオフの場合、Prime Infrastructure はトラップを発生させますが、自動トラブルシューティングは開始されません。

ステップ 4　[Save] をクリックします。

アクセス ポイント ページでのクライアント詳細の表示

アクセス ポイント ページからクライアント情報を表示することもできます。[Monitor] > [Access Points] の順に選択します。アクセス ポイントの詳細を参照するには、その列のアクセス ポイント URL をクリックします。[Current Associated Clients] タブをクリックします。

現在アソシエートされているクライアントの表示

スイッチ詳細ページから現在アソシエートされているクライアント（有線）を表示することもできます。[Monitor] > [Controllers] の順に選択し、IP アドレスを選択し、左側のサイドバーのメニューから [Clients] > [Current Associated Clients] を選択します。

クライアント レポートの実行

Busiest Clients、Client Count、Client Sessions、Client Summary、Throughput、Unique Clients と v5 クライアントの統計などクライアント レポートをレポート ラウンチ パッドから実行できます。「新しいレポートの作成、スケジューリング、および実行」（P.14-2）を参照してください。

ISE レポートの実行

レポート ラウンチ パッドから ISE レポートを起動することもできます。「新しいレポートの作成、スケジューリング、および実行」（P.14-2）を参照してください。ISE レポートの実行の詳細については、ISE オンライン ヘルプを参照してください。

クライアント設定の指定

[Administration] > [Settings] > [Client] ページでは、さまざまなクライアント設定を指定できます。詳細については、「クライアントの設定」（P.15-59）を参照してください。

クライアントの無線測定の受信

クライアント ページで、無線測定を受信できるのは、クライアントが Cisco Compatible Extensions v2（以上）であり、Associated 状態（有効な IP アドレスを持つ）である場合だけです。測定が問い合わせられたときクライアントがビジー状態の場合、測定を引き受けるかどうかが検討されます。クライアントが測定の実行を拒否する場合、クライアントからのデータは表示されません。

（注） この機能は、Foundation サービスのバージョンが 1 以降の場合のみ、CCX バージョン 6 クライアントで使用できます。

無線測定を受信するには、次の手順を実行します。

ステップ 1　[Monitor] > [Clients and Users] を選択します。

ステップ 2　[Client Username] 列からクライアントを選択します。

（注） Prime Infrastructure 検索機能を使用して特定のクライアントの検索を実行することもできます。詳細については、「検索機能の使用方法」（P.2-37）または「Advanced Search」（P.2-38）を参照してください。

ステップ 3　[Test] ドロップダウン リストから [Radio Measurement] を選択します。

（注）　[Radio Measurement] オプションは、クライアントが Cisco Compatible Extensions v2（以上）であり、Associated 状態（有効な IP アドレスを持つ）である場合に限り表示されます。

ステップ 4　このチェックボックスをオンにして、ビーコンの測定、フレームの測定、チャネルの負荷、またはノイズ ヒストグラムを指定するかどうかを示します。

ステップ 5　[Initiate] をクリックします。測定が異なると、生成される結果も異なります。詳細については、「クライアントの無線測定の結果」（P.10-33）を参照してください。

（注）　測定には、約 5 ミリ秒かかります。Prime Infrastructure からのメッセージにより、進捗状況が示されます。クライアントが測定を実行しないと選択した場合は、そのことが通知されます。

クライアントの無線測定の結果

要求した測定のタイプに応じて、次のような情報が表示されます。

- Beacon Response
  - [Channel]：この測定に対するチャネル数
  - [BSSID]：ビーコンまたはプローブの応答を送信したステーションの 6 バイトの BSSID
  - [PHY]：物理メディアの種類（FH、DSS、OFDM、高いデータレートの DSS または ERP）
  - [Received Signal Power]：ビーコンまたはプローブの応答フレームの dBm 単位の強度
  - [Parent TSF]：サービス中のアクセス ポイントの TSF 値の下位 4 バイト
  - [Target TSF]：ビーコンまたはプローブの応答に含まれている 8 バイトの TSF 値
  - [Beacon Interval]：受信したビーコンまたはプローブの応答に含まれる 2 バイトのビーコン間隔
  - [Capability information]：ビーコンまたはプローブの応答に含まれている情報
- Frame Measurement
  - [Channel]：この測定に対するチャネル番号
  - [BSSID]：受信したデータ フレームの MAC ヘッダーに含まれる BSSID
  - [Number of frames]：送信アドレスから受信したフレームの数
  - [Received Signal Power]：802.11 フレームの dBm での信号強度
- Channel Load
  - [Channel]：この測定に対するチャネル数
  - [CCA busy fraction]：上限と定義された測定時間のうち、チャネルがビジーであると CCA が示した時間の長さの割合（チャネルがビジーであると CCA が示した時間の長さに 255 を乗算して測定時間で除算した数値）
- Noise Histogram
  - [Channel]：この測定に対するチャネル数
  - 8 つの各電力範囲における RPI 密度

クライアント V5 統計の表示

[Statistics request] ページにアクセスするには、次の手順を実行します。

ステップ 1　[Monitor] > [Clients and Users] を選択します。

ステップ 2　[Client Username] 列からクライアントを選択します。

ステップ 3　[Test] ドロップダウン リストから [V5 Statistics] を選択します。

（注）　このメニューは、CCX v5 以降のクライアントだけに表示されます。

ステップ 4　[Go] をクリックします。

ステップ 5　必要な統計のタイプ（[Dot11 Measurement] または [Security Measurement]）を選択します。

ステップ 6　[Initiate] をクリックして測定を開始します。

（注）　測定期間は 5 秒間です。

ステップ 7　要求した V5 統計のタイプに応じて、次のカウンタが結果ページに表示されます。

- Dot11 測定
  - 送信フラグメント数
  - マルチキャスト送信フレーム数
  - 失敗数
  - 再試行数
  - 複数再試行数
  - フレーム重複数
  - Rts 成功数
  - Rts 失敗数
  - Ack 失敗数
  - 受信フラグメント数
  - マルチキャスト受信フレーム数
  - FCS エラー数 : このカウンタは、受信した MPDU で FCS エラーが検出されたときに増分されます。
  - 送信フレーム数
- セキュリティ
  - ペアワイズ暗号
  - Tkip ICV エラー数
  - Tkip ローカル MIC 失敗数
  - Tkip 再試行数
  - Ccmp 再試行数
  - Ccmp 復号化エラー数
  - 管理統計 Tkip ICV エラー数

- 管理統計 Tkip ローカル MIC 失敗数
- 管理統計 Tkip 再試行数
- 管理統計 Ccmp 再試行数
- 管理統計 Ccmp 復号化エラー数
- 管理統計 Tkip MHDR エラー数
- 管理統計 Ccmp MHDR エラー数
- 管理統計ブロードキャスト アソシエーション解除数
- 管理統計ブロードキャスト認証解除数
- 管理統計ブロードキャスト アクション フレーム数

クライアント動作パラメータの表示

特定のクライアント動作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　[Monitor] > [Clients and Users] を選択します。

ステップ 2　[Client Username] 列からクライアントを選択します。

ステップ 3　[Test] ドロップダウン リストから [Operational Parameters] を選択します。

次の情報が表示されます。

動作パラメータ：

- [Device Name]：デバイスのユーザ定義の名前。
- [Client Type]：クライアントの種類は次のいずれかになります。
  - laptop(0)
  - pc(1)
  - pda(2)
  - dot11mobilephone(3)
  - dualmodephone(4)
  - wgb(5)
  - scanner(6)
  - tabletpc(7)
  - printer(8)
  - projector(9)
  - videoconfsystem(10)
  - camera(11)
  - gamingsystem(12)
  - dot11deskphone(13)
  - cashregister(14)
  - radiotag(15)
  - rfidsensor(16)

  - server(17)
- [SSID]：クライアントで使用している SSID。
- [IP Address Mode]：静的設定、DHCP などの IP アドレス モード。
- [IPv4 Address]：クライアントに割り当てられた IPv4 アドレス。
- [IPv4 Subnet Address]：クライアントに割り当てられた IPv4 サブネット アドレス。
- [IPv6 Address]：クライアントに割り当てられた IPv6 アドレス。
- [IPv6 Subnet Address]：クライアントに割り当てられた IPv6 サブネット アドレス。
- [Default Gateway]：このクライアントで選択されているデフォルト ゲートウェイ。
- [Operating System]：ワイヤレス ネットワーク アダプタを使用しているオペレーティング システムを識別します。
- [Operating System Version]：ワイヤレス ネットワーク アダプタを使用しているオペレーティング システムのバージョンを識別します。
- [WNA Firmware Version]：クライアントに現在インストールされているファームウェアのバージョン。
- [Driver Version]：
- [Enterprise Phone Number]：クライアントの企業電話番号。
- [Cell Phone Number]：クライアントの携帯電話番号。
- [Power Save Mode]：省電力モードとして awake、normal、または maxPower のいずれかが表示されます。
- [System Name]：
- [Localization]：

無線情報：

- [Radio Type]：次の無線の種類が使用可能です。
  - unused(0)
  - fhss(1)
  - dsss(2)
  - irbaseband(3)
  - ofdm(4)
  - hrdss(5)
  - erp(6)
- [Radio Channel]：使用中の無線チャネル。

DNS/WNS 情報：

- [DNS Servers]：DNS サーバの IP アドレス。
- [WNS Servers]：WNS サーバの IP アドレス。

セキュリティ情報：

- [Credential Type]：クライアントに設定されているクレデンシャルの方法を示します。
- [Authentication Method]：クライアントで使用する認証方式。
- [EAP Method]：クライアントで使用する拡張認証プロトコル（EAP）の方式。
- [Encryption Method]：クライアントで使用する暗号化方式。

- [Key Management Method]：クライアントで使用するキー管理方式。

クライアント プロファイルの表示

特定のクライアント プロファイル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 and Users] を選択します。

ステップ 2　[Client Username] 列からクライアントを選択します。

ステップ 3　[More] ドロップダウン リストから [Profiles] を選択します。

次の情報が表示されます。

- [Profile Name]：ハイパーリンクになったプロファイル名のリスト。クリックすると、プロファイルの詳細が表示されます。
- [SSID]：このクライアントをアソシエートする WLAN の SSID。

現在のクライアントの無効化

現在のクライアントを無効にするには、次の手順を実行します。

ステップ 1　[Monitor] > [Clients and Users] を選択します。

ステップ 2　無効にするクライアントを選択します。

ステップ 3　[Disable] をクリックします。[Disable Client] ページが表示されます。

ステップ 4　[Description] テキスト ボックスに説明を入力します。

ステップ 5　[OK] をクリックします。

（注）　無効にしたクライアントは、コントローラ上のいずれのネットワークおよび SSID にも接続できません。クライアントを再度有効にするには、[Configure] > [Controllers] > [IP Address] > [Security] > [Manually Disabled Clients] の順に選択し、クライアントのエントリを削除します。

現在のクライアントの削除

現在のクライアントを削除するには、次の手順を実行します。

ステップ 1　[Monitor] > [Clients and Users] を選択します。

ステップ 2　削除するクライアントを選択します。

ステップ 3　[Remove] を選択します。

ステップ 4　[Remove] をクリックして、削除を実行します。

ミラー モードの有効化

ミラー モードを有効にすると、単一のクライアント デバイスまたはアクセス ポイントが起点または終点であるすべてのトラフィックを（別のポートに）複製できます。

（注）　ミラー モードは特定のネットワーク問題を診断する際には役立ちますが、このポートへの接続には反応しなくなるため、使用されていないポートだけで有効にする必要があります。

ミラー モードを有効にするには、次の手順を実行します。

ステップ 1　[Monitor] > [Clients and Users] を選択します。

ステップ 2　[Client Username] 列からクライアントを選択します。

ステップ 3　[More] ドロップダウン リストから [Enable Mirror Mode] を選択します。

ステップ 4　[Go] をクリックします。

クライアントの最近のロケーションを示す高レゾリューション マップの表示

クライアントの最近のロケーションを示す高レゾリューション 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] > [Clients and Users] を選択します。

ステップ 2　[Client Username] 列からクライアントを選択します。

ステップ 3　[More] ドロップダウン リストから [Recent Map (High Resolution)] を選択します。

ステップ 4　[Go] をクリックします。

クライアントの現在のロケーションを示す高レゾリューション マップの表示

クライアントの現在のロケーションを示す高レゾリューション 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] > [Clients and Users] を選択します。

ステップ 2　[Client Username] 列からクライアントを選択します。

ステップ 3　[More] ドロップダウン リストから [Present Map (High Resolution)] を選択します。

ステップ 4　[Go] をクリックします。

クライアントのクライアント セッション レポートの実行

このクライアントの最新のクライアント セッション レポートを表示するには、次の手順を実行します。

ステップ 1　[Monitor] > [Clients and Users] を選択します。

ステップ 2　[Client Username] 列からクライアントを選択します。

ステップ 3　[More] ドロップダウン リストから [Client Sessions Report] を選択します。

ステップ 4　[Go] をクリックします。Client Session レポートの詳細が表示されます。詳細については、「クライアント レポート」（P.14-7）を参照してください。

クライアントのローミング理由レポートの表示

このクライアントの最新のローミング レポートを表示するには、次の手順を実行します。

ステップ 1　[Monitor] > [Clients and Users] を選択します。

ステップ 2　[Client Username] 列からクライアントを選択します。

ステップ 3　[More] ドロップダウン リストから [Roam Reason] を選択します。

ステップ 4　[Go] をクリックします。

このページには、クライアントの最新のローミング レポートが表示されます。各ローミング レポートには、次の情報が含まれます。

- 新規 AP MAC アドレス
- 旧（前）AP MAC アドレス
- 前の AP SSID
- 前の AP チャネル
- 遷移時間：クライアントを新しいアクセス ポイントにアソシエートするためにかかった時間。
- ローミング理由：クライアントのローミング理由。

検出アクセス ポイントの詳細の表示

信号強度、SNR など、クライアントと通信できるアクセス ポイント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] > [Clients and Users] を選択します。

ステップ 2　[Client Username] 列からクライアントを選択します。

ステップ 3　[More] ドロップダウン リストから [Detecting APs] を選択します。

ステップ 4　[Go] をクリックします。

クライアント ロケーション履歴の表示

RF フィンガープリントに基づくクライアント ロケーションの履歴を表示するには、次の手順を実行します。

ステップ 1　[Monitor] > [Clients and Users] を選択します。

ステップ 2　[Client Username] 列からクライアントを選択します。

ステップ 3　[More] ドロップダウン リストから [Location History] を選択します。

ステップ 4　[Go] をクリックします。

クライアントの音声メトリックの表示

このクライアントのトラフィック ストリーム メトリックを表示するには、次の手順を実行します。

ステップ 1　[Monitor] > [Clients and Users] を選択します。

ステップ 2　[Client Username] 列からクライアントを選択します。

ステップ 3　[More] ドロップダウン リストから [Voice Metrics] を選択します。

ステップ 4　[Go] をクリックします。

次の情報が表示されます。

- [Time]：アクセス ポイントから統計情報が収集された時刻。
- QoS
- AP Ethernet MAC
- Radio
- [% PLR (Downlink)]：90 秒の間隔中にダウンリンク（アクセス ポイントからクライアント）で失われたパケットの割合。
- [% PLR (Uplink)]：90 秒の間隔中にアップリンク（クライアントからアクセス ポイント）で失われたパケットの割合。
- [Avg Queuing Delay (ms) (Uplink)]：アップリンクの平均キューイング遅延（ミリ秒）。パケット キューイング遅延の平均は、音声キューを横断する音声パケットの平均遅延です。パケット キュー遅延は、パケットが送信のためにキューに入れられた時点から、パケットが正常に送信される時点まで測定されます。これには、必要に応じて再試行時間が含まれます。
- [% Packets > 40 ms Queuing Delay (Downlink)]：40 ms を超えるキューイング遅延パケットの割合。

- [% Packets 20ms-40ms Queuing Delay (Downlink)] : 20 ms を超えるキューイング遅延パケットの割合。
- [Roaming Delay] : ローミング遅延（ミリ秒）。クライアントによって測定されるローミング遅延は、古いアクセス ポイントから最後のパケットを受信した時点から、ローミングが正常に行われた後で新しいアクセス ポイントから最初のパケットを受信した時点まで測定されます。