



Tools

[Tools] メニューでは、Cisco Prime Infrastructure の Voice Audit、Location Accuracy Tool、Configuration Audit Summary、および Migration Analysis 機能にアクセスできます。この章の内容は、次のとおりです。

- 「Voice Audit の実行」 (P.17-1)
- 「音声診断の実行」 (P.17-6)
- 「Location Accuracy Tool の設定」 (P.17-10)
- 「監査サマリーの設定」 (P.17-15)
- 「移行分析の設定」 (P.17-15)
- 「TAC ケース添付ファイルの設定」 (P.17-18)

Voice Audit の実行

Prime Infrastructure には、コントローラの設定を確認し、導入ガイドラインからの逸脱を Audit Violation として強調表示するための、音声監査メカニズムが用意されています。

Voice Audit 機能にアクセスするには、[Tools] > [Voice Audit] の順に選択します。[Voice Audit Report] ページが表示されます。

このページには、[Controllers]、[Rules]、[Reports] の 3 つのタブがあります。

- [Controllers] タブでは、音声監査を実行するコントローラを選択できます。
- [Rules] タブでは、この音声監査の該当する VoWLAN SSID と該当するルールを指示できます。
- [Report] タブでは、音声監査の概要とレポート結果が表示されます。

Voice Audit 機能にアクセスするには、[Tools] > [Voice Audit] の順に選択します。

ここでは、次の内容について説明します。

- 「コントローラに対する音声監査の実行」 (P.17-1)
- 「音声監査ルールの選択」 (P.17-2)
- 「音声監査レポートの詳細」 (P.17-6)
- 「音声監査レポートの結果」 (P.17-6)

コントローラに対する音声監査の実行

[Controllers] タブでは、音声監査を実行するコントローラを選択できます。



(注) 1 回の操作で、最大 50 台のコントローラで音声監査を実行できます。

音声監査用のコントローラを選択するには、次の手順を実行します。

- ステップ 1** [Tools] > [Voice Audit] の順に選択します。
- ステップ 2** [Controllers] タブをクリックします。
- ステップ 3** [Run audit on] ドロップダウン リストから、[All Controllers]、[A Floor Area]、または [A Single Controller] を選択します。
- [All Controllers] : 追加のコントローラ情報は不要です。
 - [A Floor Area] : ドロップダウン リストから、該当するキャンパス、ビルディング、フロア、およびコントローラを選択します。
 - [A Single Controller] : 該当するコントローラをドロップダウン リストから選択します。
- ステップ 4** 音声監査のルールを決定するには、[Rules] タブをクリックします。詳細については、「[音声監査ルールの選択](#)」(P.17-2) を参照してください。

音声監査ルールの選択

[Rules] タブでは、この音声監査の該当する VoWLAN SSID と該当するルールを指示できます。

音声監査用のルールを指定するには、次の手順を実行します。

- ステップ 1** [Tools] > [Voice Audit] ページで、[Rules] タブをクリックします。
- ステップ 2** 該当する VoWLAN SSID を [VoWLAN SSID] テキスト ボックスに入力します。
- ステップ 3** [Rules List] から、この音声監査用の該当するルールのチェックボックスをオンにします (表 17-1 を参照)。



(注) 赤い円は無効なルールを示します (データが不十分なため)。緑の円は有効なルールを示します。

表 17-1 音声監査のルール リスト

ルール	ルールの詳細
VoWLAN SSID	説明 : VoWLAN SSID が存在するかどうかを確認します。 ルールの有効性 : ユーザ定義の VoWLAN SSID。
CAC: 7920	説明 : 7920 AP CAC が VoWLAN で有効になっているかどうかを確認します。 ルールの有効性 : ユーザ定義の VoWLAN SSID。
CAC: 7920 Clients	説明 : 7920 クライアント CAC が VoWLAN で無効になっているかどうかを確認します。 ルールの有効性 : ユーザ定義の VoWLAN SSID。

表 17-1 音声監査のルール リスト (続き)

ルール	ルールの詳細
DHCP Assignment	説明：DHCP の割り当てが VoWLAN で無効になっているかどうかを確認します。 ルールの有効性：ユーザ定義の VoWLAN SSID。
MFP Client	説明：VoWLAN で MFP クライアント保護が [Required] に設定されていないかどうかを確認します。 ルールの有効性：ユーザ定義の VoWLAN SSID。
Platinum QoS	説明：VoWLAN で QoS が Platinum (Voice) に設定されているかどうかを確認します。 ルールの有効性：ユーザ定義の VoWLAN SSID。
Non Platinum QoS	説明：非 VoWLAN で QoS が Platinum に設定されていないことを確認します。 ルールの有効性：ユーザ定義の VoWLAN SSID。
WMM	説明：WMM が VoWLAN で有効になっているかどうかを確認します。 ルール データ：ドロップダウン リストから [Allowed] または [Required] を選択します。 ルールの有効性：ユーザ定義の VoWLAN SSID。
CCKM	説明：CCKM が VoWLAN で有効になっているかどうかを確認します。 ルールの有効性：ユーザ定義の VoWLAN SSID。
CCKM With No AES- for 792x phones	説明：VoWLAN 向け Cisco Centralized Key Management (CCKM) を使用して AES 暗号化が有効になっていないことを確認します。このルールは、792x 電話機専用です。 ルールの有効性：ユーザ定義の VoWLAN SSID。
TSM	説明：Traffic Stream Metrics (TSM) が有効になっていることを確認します。 ルール データ：[802.11a/n TSM] と [802.11b/g/n TSM] のいずれかまたは両方のチェックボックスをオンにします。 ルールの有効性：少なくとも 1 つのバンドを選択する必要があります。
DFS	説明：Channel Announcement と Channel Quiet Mode の両方で、動的周波数選択 (DFS) が有効になっているかどうかを確認します。
ACM	説明：アドミSSION制御が有効になっているかどうかを確認します。 ルール データ：[802.11a/n ACM] と [802.11b/g/n ACM] のいずれかまたは両方のチェックボックスをオンにします。 ルールの有効性：少なくとも 1 つのバンドを選択する必要があります。

表 17-1 音声監査のルール リスト (続き)

ルール	ルールの詳細
DTPC	<p>説明：動的送信電力制御が有効になっているかどうかを確認します。</p> <p>ルール データ：[802.11a/n DTPC] と [802.11b/g/n DTPC] のいずれかまたは両方のチェックボックスをオンにします。</p> <p>ルールの有効性：少なくとも 1 つのバンドを選択する必要があります。</p>
Expedited Bandwidth	<p>説明：緊急帯域幅が有効になっているかどうかを確認します。</p> <p>ルール データ：[802.11a/n Expedited Bandwidth] と [802.11b/g/n Expedited Bandwidth] のいずれかまたは両方のチェックボックスをオンにします。</p> <p>ルールの有効性：少なくとも 1 つのバンドを選択する必要があります。</p>
Load Based CAC	<p>説明：負荷ベースのアドミッション制御 (CAC) が有効になっているかどうかを確認します。</p> <p>ルール データ：[802.11a/n Load Based CAC] と [802.11b/g/n Load Based CAC (LBCAC)] のいずれかまたは両方のチェックボックスをオンにします。</p> <p>ルールの有効性：少なくとも 1 つのバンドを選択する必要があります。</p>
CAC: Max Bandwidth	<p>説明：コール アドミッション制御の最大 RF 帯域幅が適切に設定されているかどうかを確認します。</p> <p>ルール データ：テキスト ボックスに、802.11a/n と 802.11b/g/n の最大許容帯域幅のパーセンテージを入力します。</p> <p>ルールの有効性：少なくとも 1 つの帯域のデータを指定する必要があります。有効な範囲は 0 ~ 100 % です。</p>
CAC: Reserved Roaming Bandwidth	<p>説明：コール アドミッション制御の予約済みローミング帯域幅が適切に設定されているかどうかを確認します。</p> <p>ルール データ：テキスト ボックスに、802.11a/n と 802.11b/g/n の最大予約済みローミング帯域幅のパーセンテージを入力します。</p> <p>ルールの有効性：少なくとも 1 つの帯域のデータを指定する必要があります。有効な範囲は 0 ~ 100 % です。</p>
Pico Cell mode	<p>説明：ピコセルモードが無効になっているかどうかを確認します。</p> <p>ルール データ：[802.11a/n Pico Cell mode] と [802.11b/g/n Pico Cell mode] のいずれかまたは両方のチェックボックスをオンにします。</p> <p>ルールの有効性：少なくとも 1 つのバンドを選択する必要があります。</p>

表 17-1 音声監査のルール リスト (続き)

ルール	ルールの詳細
Beacon Period	<p>説明：ビーコン周期が適切に設定されているかどうかを確認します。</p> <p>ルール データ：テキスト ボックスに、11a/n および 11b/g/n のビーコン周期 (ミリ秒単位) を入力します。</p> <p>ルールの有効性：少なくとも 1 つの帯域のデータを指定する必要があります。有効な範囲は 20 ~ 1000 です。帯域を検査しない場合は、0 を入力するか、空のままにします。</p>
Short Preamble	<p>説明：短いプリアンプルが 11b/g で有効かどうかを確認します。</p>
Fragmentation Threshold	<p>説明：フラグメンテーションしきい値が適切に設定されているかどうかを確認します。</p> <p>ルール データ：テキスト ボックスに、11a/n と 11b/g/n のフラグメンテーションしきい値 (バイト単位) を入力します。</p> <p>ルールの有効性：少なくとも 1 つの帯域のデータを指定する必要があります。有効な範囲は 256 ~ 2346 です。帯域を検査しない場合は、0 を入力するか、空のままにします。</p>
Data Rate	<p>説明：データ レートが適切に設定されているかどうかを確認します。</p> <p>11b/g のデータ レート設定：各 Mbps カテゴリで、[Disabled]、[Supported]、または [Mandatory] を選択します。</p> <p>11a のデータ レート設定：各 Mbps カテゴリで、[Disabled]、[Supported]、または [Mandatory] を選択します。</p>
Aggressive Load Balancing	<p>説明：アグレッシブ ロード バランシングが無効になっているかどうかを確認します。</p>
QoS Profile	<p>説明：QoS プロファイルがデフォルト値から変更されていないかどうかを確認します。</p>
EAP Request Timeout	<p>説明：EAP 要求タイムアウトが適切に設定されているかどうかを確認します。</p> <p>ルール データ：EAP 要求タイムアウトの時間制限 (秒単位) を入力します。</p> <p>ルールの有効性：データを空白のままにしたりゼロを設定したりできません。有効な範囲は 1 ~ 120 です。</p>
ARP Unicast	<p>説明：ARP ユニキャストが無効になっているかどうかを確認します。</p>



(注) 値をデフォルト設定にリセットするには [Reset] をクリックします。

ステップ 4 この音声監査でルールが設定されている場合、[Save] をクリックして現在の設定を保存するか、[Save and Run] をクリックし設定を保存してレポートを実行します。

ステップ 5 レポート結果を表示するには [Report] タブをクリックします。詳細については、「[音声監査レポートの詳細](#)」(P.17-6) を参照してください。

音声監査レポートの詳細

音声監査の詳細では、次の情報が表示されます。

- [Audit Status] : 監査が完了しているかどうかを示します。
- [Start Time and End Times] : 音声監査が開始および終了した時刻を示します。
- [# Total Devices] : 音声監査に関係するデバイスの数を示します。
- [# Completed Devices] : ツールが監査を試みたデバイスの数を示します。



(注) コントローラが到達不能な場合、そのコントローラの監査がスキップされます。そのコントローラに対してはルール チェックが実行されません。

- [# Rules] : 音声監査で選択されたルールの数を示します。

音声監査レポートの結果

音声監査レポートの結果には、次の情報が含まれています。

- [IP Address] : 音声監査に関係するコントローラの IP アドレスを示します。
- [Rule] : このコントローラに適用されたルールを示します。
- [Result] : 適用されたルールの結果 ([Skipped]、[Violation]、[Unreachable]) を示します。



(注) 現在の設定とルール値に不一致が存在しない場合、そのルールの結果は表示されません。

- [Details] : ルールの結果の説明を定義します。



(注) 適用されたルールの結果が [Violation] である場合、[Details] リンクをクリックすると、名前、デバイス値、ルール値などの詳細が表示されます。リンクにマウス カーソルを合わせると詳細が表示されます。

- [Time] : 音声監査のタイムスタンプが表示されます。

音声診断の実行

音声診断ツールでは、リアルタイムでボイスコールを診断するインタラクティブ ツールです。このツールは、クライアントのコール制御関連のエラー、ローミング履歴、および関連 AP で許可および拒否されたアクティブ コールの合計数をレポートします。このツールを使用して、音声診断を開始または停止できます。

音声診断テストは複数のコントローラに対してプロビジョニングされます。つまり、ローミング時に AP が複数のコントローラにアソシエートされた場合、音声診断テストにより、アソシエートされたすべてのコントローラがテストされます。Prime Infrastructure は、AP が上下 3 フロアに配置されたコントローラのテストをサポートしています。たとえば、Prime Infrastructure マップにフロア 1 ~ 4 があり、すべての AP がコントローラ (wlc1、wlc2、wlc3、wlc4) にアソシエートされており、Prime

Infrastructure マップに配置されているとします。ここで、クライアントが 1 階にある wlc1 の AP にアソシエートされ、音声診断テストがこのクライアントに対して開始された場合、テストは wlc2 から wlc3 にもプロビジョニングされます。これは、ローミングのために実行されます。

[Voice diagnostic] ページには、以前に実行されたテストがリストされます（ある場合）。[Voice diagnostic] ページには、次の詳細情報が表示されます。

- [Test Name] : テストの名前。
- [First Client] : テスト対象の 1 番目の電話機の Mac アドレス。
- [Second Client] : テスト対象の 2 番目の電話機の Mac アドレス。
- [Start Time] : テストが開始された時刻。
- [Remaining Time] : テストの残り時間。
- [State] : テストの状態。これは、4 つの状態 ([Running]、[Completed]、[Stopped]、または [Aborted]) のいずれかです。
- Problem : テストのステータス。赤はテストで問題が検出されたことを示します。緑は通話中に問題が検出されなかった音声診断テストを示します。

ドロップダウン リストの [Select a command] から、新しいテストを開始すること、既存のテスト結果を表示することや、テストを削除することができます。

テストの詳細を表示するには、[Test Name] リンクをクリックします。[test detail] ページには、次の詳細情報が表示されます。

- [Test Name] : テストの名前。
- [State] : テストの状態。これは、4 つの状態 ([Running]、[Completed]、[Stopped]、または [Aborted]) のいずれかです。
- Problem : テストのステータス。赤はテストで問題が検出されたことを示します。緑は音声診断テストが問題なく成功したことを示します。
- [Duration] : テストが実行された期間。期間は、10、20、30、40、50、または 60 分です。デフォルトの選択は 10 分です。
- [Starting Time] : テストが開始された時刻。
- [Remaining/Stopped Time] : テストの残り時間。
- [First Client Details] : クライアントの MAC アドレス、クライアントに対してプロビジョニングされたすべてのコントローラなど、1 番目のクライアントの詳細が表示されます。コントローラが到達不能の場合は、プロビジョニングが失敗したコントローラもリストされます。
- [Second Client Details] : クライアントの MAC アドレス、クライアントに対してプロビジョニングされたすべてのコントローラなど、2 番目のクライアント（ある場合）の詳細が表示されます。コントローラが到達不能の場合は、プロビジョニングが失敗したコントローラもリストされます。



(注)

このツールは、ローミングをサポートするために、同じビルディング内のコントローラを、クライアントのアソシエート AP ビルディングのコントローラとして認識し、すべてのコントローラの監視リストに追加します。このツールは、コントローラを設定するために、クライアントの現在のアソシエーション AP の場所から上下 5 階のコントローラを検索します。コントローラの監視リストには、エントリーは 10 分間設定されます。10 分後に、コントローラは監視リストからエントリーを削除します。

音声診断テストの開始

音声診断テストを開始するには、次の手順に従います。

-
- ステップ 1** [Tools] > [Voice Diagnostics] の順にクリックします。
- ステップ 2** [Select a command] ドロップダウン リストから、[New test] を選択し、[Go] をクリックします。設定ページが表示されます。
- このページで、ボイスコール診断の目的で最大 2 つのクライアントを設定できます。両方のクライアントを同じコールで診断すること、または別のコールで診断することができます。
- ステップ 3** テスト名およびボイスコールを監視する期間を入力します。音声診断テストは 10、20、30、40、50、または 60 分間実行できます。Prime Infrastructure では 10 分間がデフォルトで選択されます。
- ステップ 4** 音声診断テストの対象デバイスの MAC アドレスを入力します。
- ステップ 5** デバイス タイプを選択します。これは、Cisco ベースの電話機かカスタム電話機です。カスタム電話機の場合、そのカスタム電話機の RSSI 範囲を入力する必要があります。Cisco 電話機の場合、RSSI 範囲は事前に選択されています。
- ステップ 6** [StartTest] をクリックしてテストを開始します。テストが完了した場合、テストを再び開始できます。



(注) テストが完了していない場合、状態は [Running] で、テストが完了すると状態は [Completed] になります。テストを途中で停止するために、[Stop] ボタンを使用できます。停止すると状態は [Stopped] になります。

音声診断テスト レポートの表示

テスト レポートは表形式のデータを使用して表示されます。4 つの主要タブがあります。ここでは、次の内容について説明します。

- 「[Summary] タブ」 (P.17-8)
- 「[Charts] タブ」 (P.17-9)
- 「[Roam History] タブ」 (P.17-9)
- 「[Events] タブ」 (P.17-10)

[Summary] タブ

このタブは 3 つの領域に分割されており、上部の領域にはテストとクライアントの詳細が表示され、中間の領域には問題が表示され、下部の領域には対応するログ メッセージが表示されます。

Test and Client Details

[Test Status] に、テストの名前、1 番目のクライアントの MAC アドレス、2 番目のクライアントの MAC アドレス、デバイス タイプ、テスト ステータス、開始時刻、残り時間、テスト期間などのテスト詳細が表示されます。テストが停止または完了した場合、テストを再開します。実行中のテストを停止するために、[Stop] ボタンが用意されています。ステータスおよびクライアントの詳細を更新するには、[Refresh Status Tab] ボタンおよび [Refresh Client Tab] ボタンを使用します。クライアント ユーザー名、IP アドレス、MAC アドレス、ベンダー、CCX バージョンは、802.11 ステート、プロトコル、SSID、プロファイル名、AP 詳細などのクライアント詳細が表示されます。クライアントの MAC アドレスをクリックすると、クライアントの詳細を表示できます。

Problems

[Problems] ペインは [test and client status details] ペインの下に表示されます。このペインには、現在の診断に関連するすべての問題が表示されます。このペインは 5 秒ごとに個別に更新されます。ページ全体を更新する必要はありません。ペインのいずれかの列をクリックすることで、このペインの情報をソートできます。[Problems] ペインのいずれかの行をクリックすると、ポップアップ ダイアログボックスが表示され、そこに問題の詳しい説明と推奨措置が表示されます。



(注)

コントローラ間ローミング障害の一部のケースでは、[From AP] 情報の MAC アドレスが不正確で、「00:00:00:00:00:00」と表示される場合があります。

Logs

[Logs] ペインは、[Problems] ペインの下に表示されます。このペインには、この診断時にコントローラと WCS 間で交換されたすべてのメッセージが表示されます。ペインのいずれかの列をクリックすることで、このペインの情報をソートできます。このペインは、ページ全体を更新しなくても、5 秒ごとに個別に更新されます。

[Charts] タブ

このタブには、各クライアントのアップリンクおよびダウンリンク トラフィックのグラフが表示されます。グラフは 10 秒ごとに更新されます。

[Client Uplink and DownLink TSM] グラフとローミング

[Client Uplink Traffic Stream Metric (TSM)] グラフには、CCX V4 以上をサポートするクライアントが表示されます。TSM のデータは 10 秒ごとにプロットされます。TSM グラフには、一連のメトリックが表示されます。これらのメトリックは、グラフの [Select Series] ボタンを使用して有効または無効にできます。

[Client Uplink and DownLink QoS] グラフ

各インターバルで、QoS が計算され、グラフに表示されます。[Client Uplink QoS] グラフが表示されます。この円グラフでは、QoS グラフの合計数と 3 つのカテゴリにおけるその分布が示されます。これらのカテゴリは、通常、ボイスコールの品質を示します。

Average Uplink and Downlink AC Queue

[AC Queue] には、パケットのタイプおよび 1 つのシリーズのパケットの数が表示されます。[Select Series] ボタンを使用して、シリーズを有効または無効にできます。

[Roam History] タブ

このタブでは、[Roaming] テーブルにローミング履歴情報が表示されます。この [Roaming] テーブルには、成功および失敗したローミングの履歴が表示されます。[Roaming] テーブルは次の情報を提供します。

- クライアントのローミングが実行された時刻
- クライアントの移動元の AP の名前
- クライアントの移動元の無線のタイプ

- クライアントの移動元のコントローラの IP アドレス
- クライアントの移動先の AP の名前
- クライアントの移動先のコントローラの IP アドレス
- クライアントの移動先の無線のタイプ
- ローミングの結果（成功または失敗）
- ローミングが失敗した場合は、失敗した原因

[Events] タブ

[Event] タブには、ボイスコール中のクライアントと AP に関連するイベント履歴がリスト形式で表示されます。直近 10 のイベントが表示されます。2 つのイベント テーブル ([Client Events] および [AP Events]) を使用できます。[Client Events] テーブルには、ボイスコール中のクライアント固有イベントが表示され、[AP Event] テーブルには、AP 固有イベントが表示されます。

イベントの詳細については、「イベントのモニタリング」セクションを参照してください。

Location Accuracy Tool の設定

Location Accuracy Tool を使用すると、不正でないクライアント、不正クライアント、干渉源、およびアセット タグの位置精度を分析できます。

位置精度を確認することによって、既存のアクセス ポイントの導入が、少なくとも 90 % の確率で、10 m 以内にある要素の真の位置を推定できることを確認できます。

Location Accuracy Tool では、次のいずれかのテストを実行できます。

位置精度をテストするには、次の 2 つの方法があります。

- **スケジュール設定された精度テスト**：クライアント、タグ、干渉源がすでに展開されており、無線 LAN インフラストラクチャにすでにアソシエートされている場合に使用します。クライアント、タグ、干渉源がすでに事前に配置されている場合は、テストが定期的なスケジュールに基づいて実行できるように、スケジュール設定された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、干渉源の位置精度をテストするために使用します。

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。

- 「[Location Accuracy Tool の有効化](#)」 (P.17-11)
- 「[現在スケジュール設定されている精度テストの表示](#)」 (P.17-11)
- 「[精度テストの詳細の表示](#)」 (P.17-12)
- 「[スケジュール設定された精度テストを使用した現在の位置の検証](#)」 (P.17-12)
- 「[オンデマンド精度テストを使用した位置精度のテスト](#)」 (P.17-14)

Location Accuracy Tool の有効化



(注)

スケジュール設定済みおよびオンデマンドの位置精度ツールのテスト機能を使用するには、Prime Infrastructure で [Advanced Debug] オプションを有効にする必要があります。[Advanced Debug] オプションが有効になっていない場合、Location Accuracy Tool は [Tools] メニューに選択肢として表示されません。

Prime Infrastructure で詳細デバッグ オプションを有効にするには、次の手順に従います。

- ステップ 1 Prime Infrastructure で、[Monitor] > [Maps] をクリックします。
- ステップ 2 [Select a command] ドロップダウンリストから [Properties] を選択し、[Go] をクリックします。
- ステップ 3 表示されるページで [Enabled] チェックボックスをオンにし、Advanced Debug モードを有効にします。[OK] をクリックします。



(注) Advanced Debug がすでに有効になっている場合は、さらに操作を行う必要はありません。[Cancel] をクリックします。

これで、Location Accuracy Tool を使用して、モビリティ サービス エンジンに対して位置精度テストを実行できるようになります。

「スケジュール設定された精度テストを使用した現在の位置の検証」(P.17-12) または「オンデマンド精度テストを使用した位置精度のテスト」(P.17-14) に進みます。

現在スケジュール設定されている精度テストの表示

現在スケジュール設定されている位置精度テストを表示するには、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 [Accuracy Tests] ページに、現在スケジュール設定されているすべての精度テストが表示されます。このページには、次の情報が表示されます。
 - テスト名：名前をクリックすると、この精度テストに関する詳細が表示されます。
 - テストの種類
 - フロア領域または屋外領域：このテストの位置が表示されます。
 - ステータス
 - 精度 %
 - 平均エラー数 (m)

新しいスケジュール設定された精度テストまたはオンデマンドの精度テストの作成、最後の実行のログのダウンロード、すべてのログのダウンロード、現在の精度テストの削除を行うには、[Select a command] ドロップダウン リストを使用します。



(注)

- [Accuracy Tests] 概要ページから精度テストのログをダウンロードできます。これを行うには、精度テストを選択し、[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。

精度テストの詳細の表示

現在の精度テストに関する詳細を表示するには、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** 詳細にアクセスする精度テストの名前をクリックします。
[Accuracy Test Details] ページで、テスト ポイントの配置や精度テストの削除を行うことができます。
- ステップ 3** [Accuracy Test] 概要ページに戻るには、[Cancel] をクリックします。
-

スケジュール設定された精度テストを使用した現在の位置の検証

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。
- 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 [Area Type] を選択します。
- ステップ 5** キャンパスは、デフォルトでルート領域として設定されています。この設定を変更する必要はありません。
- ステップ 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 時間表記で入力します。



(注)

テスト開始時間を入力する場合には、マップ上にテストポイントを配置するためにテスト開始前に十分な時間があることを確認します。

-
- ステップ 9** テスト結果は [Accuracy Tests] > [Results] ページに表示されます。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] 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。フロア上のすべてのクライアント、タグ、および干渉源が、MAC アドレスとともにフロア マップに表示されます。

ステップ 11 位置精度を確認する各クライアント、タグ、および干渉源の隣のチェックボックスをオンにします。

[MAC Address] チェックボックスをオンにすると、2 つのアイコンが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、タグ、または干渉源の 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別のフロアのロケーション サーバ上にある場合は、左端の隅 (0, 0 の位置) にアイコンが表示されます。

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。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。精度テストが成功したことを確認するダイアログ ボックスが表示されます。

ステップ 14 [OK] をクリックして、確認ダイアログボックスを閉じます。[Accuracy Tests] 概要ページに戻ります。



(注) テストの実行直前は、精度テスト ステータスは [Scheduled] と表示されます。テストが処理中の場合は [Running] ステータスが表示され、テストが完了した場合は [Idle] ステータスが表示されます。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 位置精度テストの結果を表示するには、テスト名をクリックして表示されるページの [Results] タブをクリックします。

ステップ 16 [Results] ページで、[Saved Report] 見出しの下の [Download] リンクをクリックしてレポートを表示します。

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位置精度レポート。
- エラー距離ヒストグラム。
- 累積エラー分布グラフ。
- エラー距離経時グラフ。
- 位置精度がテストされた MAC アドレスごとのサマリー。このサマリーでは、実際の位置、エラー距離、空間精度を示すマップ (実際の位置と計算された位置)、および MAC ごとの時系列でのエラー距離が示されます。

オンデマンド精度テストを使用した位置精度のテスト

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、干渉源の位置精度をテストするために使用します。

オンデマンド精度テストを実行するには、次の手順に従います。

-
- 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 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 [Area Type] を選択します。
- ステップ 5** キャンパスは、デフォルトでルート領域として設定されています。この設定を変更する必要はありません。
- ステップ 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** テスト結果の宛先を選択します。テスト結果は [Accuracy Tests] > [Results] ページに表示されます。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** 特定の位置の位置精度と RSSI をテストするには、左側のドロップダウン リストからクライアント、タグ、または干渉源を選択します。選択したオプション (クライアント、タグ、干渉源のいずれか) のすべての MAC アドレスのリストが、オプションの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位置に移動して、マウスをクリックして配置します。
- ステップ 12** [Zoom percentage] ドロップダウン リストから、マップのズーム パーセンテージを選択します。
[X] および [Y] テキスト ボックスには、マップ内の赤色の十字線の位置に基づいて座標が入力されません。
- ステップ 13** [Start] をクリックして、精度データの収集を開始します。
- ステップ 14** [Stop] をクリックして収集を終了します。[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 15** 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 11** ~ **ステップ 14** を繰り返します。
- ステップ 16** テストポイントのマッピングが終了したら、[Analyze Results] をクリックします。
- ステップ 17** 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位置精度レポート。
 - エラー距離ヒストグラム
 - 累積エラー分散グラフ
-

監査サマリーの設定

[Tools] > [Config Audit] の順に選択して、[Config Audit Summary] ページを表示します。

このページには、次の概要が表示されます。

- [Total Enforced Config Groups] : バックグラウンド監査用に設定され適用が有効になっている、設定グループのテンプレートの数を示します。

リンクを起動すると、[Enforce Configuration] が有効な設定グループを示す [Config Group] ページが表示されます。

- [Total Mismatched Controllers] : 一致しないコントローラの数を表示します。一致しないコントローラは、最近の監査時に Prime Infrastructure とコントローラに間に設定の相違が見つかったことを示します。

リンクをクリックすると、[Mismatched audit status] 列でソートされたコントローラ リストが表示されます。[Audit Status] 列の項目をクリックすると、このコントローラの監査レポートが表示されます。

- [Total Config Audit Alarms] : 設定グループに監査の矛盾が施行された場合に生成されたアラーム数を示します。

リンクをクリックすると、すべての設定監査アラームの詳細が表示されます。



(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。

- [Most recent 5 config audit alarms] : 監査アラームのオブジェクト名、イベントのタイプ、日付と時刻など、最近の設定監査のアラームを示します。

[View All] をクリックすると該当する [Alarm] ページが開き、すべての設定監査アラームが表示されます。

移行分析の設定

[Migration Analysis Summary] ページを表示するには、[Tools] > [Migration Analysis] の順に選択します。



(注) また、[Configure] > [Autonomous AP] > [Migration Templates] の順に選択し、[Select a command] ドロップダウンリストから [View Migration Analysis Summary] を選択することでも、移行分析の概要にアクセスできます。

Autonomous アクセス ポイントは、すべての基準のステータスが合格の場合のみ移行対象になります。赤い X は適格でないことを示し、緑のチェック マークは適格であることを示します。これらの列は次のものを表しています。

- [Privilege 15 Criteria] : Autonomous アクセス ポイントの検出の一部として指定された Telnet クレデンシャルは、特権 15 であることが必要です。
- [Software Version] : 12.3(7)JA リリースからの変換のみがサポートされています。ただし、12.3(11)JA、12.3(11)JA1、12.3(11)JA2、および 12.3(11)JA3 を除きます。

- [Role Criteria] : アソシエーション要求を送信するには、アクセス ポイントとコントローラの有線接続が必要です。そのため、次の Autonomous アクセス ポイント ロールが必要です。
 - root
 - ルート アクセス ポイント
 - root fallback repeater
 - root fallback shutdown
 - root access point only

[Radio Criteria] : デュアル無線アクセス ポイントの場合、1 つの無線の種類のみがサポートされている場合でも変換を実行できます。

ここでは、次の内容について説明します。

- 「Autonomous アクセス ポイントのアップグレード」 (P.17-16)
- 「ファームウェア アップグレード レポートの表示」 (P.17-17)
- 「ロール変更レポートの表示」 (P.17-17)

Autonomous アクセス ポイントのアップグレード

Autonomous アクセス ポイントは、手動または自動でアップグレードできます。[Migration Analysis] ページで、ソフトウェア バージョンが [failed] と表示されたアクセス ポイントを選択し、[Select a command] ドロップダウン リストから [Upgrade Firmware (Manual or Automatic)] を選択します。このプロセスにより、Cisco IOS アクセス ポイントの自律ファームウェア イメージがサポートされているバージョンにアップグレードされます。

Prime Infrastructure は Telnet ベースの接続を使用してアクセス ポイントのファームウェアをアップグレードします。自動オプションを選択した場合、Prime Infrastructure にあるデフォルト イメージとともに内部 TFTP サーバが使用されます。デバイスの種類ごとのデフォルト イメージは次のとおりです。

- ap801-k9w7-tar.124-10b.JA3.tar
- ap802-k9w7-tar
- c1100-k9w7-tar.123-7.JA5.tar
- c1130-k9w7-tar.123-7.JA5.tar
- c1200-k9w7-tar.123-7.JA5.tar
- c1240-k9w7-tar.12307.JA5.tar
- c1250-k9w7-tar.124-10b.JA3.tar
- c1310-k9w7-tar.123-7.JA5.tar

手動オプションを選択した場合、TFTP サーバ IP、ファイル パス、ファイル パス名を含む追加のページが表示されます。最終的なページは [Report] ページです。

ルート モードへのステーション ロールの変更

アソシエーション要求を送信するには、アクセス ポイントとコントローラの有線接続が必要であるため、Autonomous アクセス ポイントに適切なロールを割り当てる必要があります。ロールが不適格として表示される場合は、[Select a command] ドロップダウン リストから [Change Station Role to Root Mode] を選択してモードを変更します。

移行分析の実行

[Migration Analysis Summary] ページの [Select a command] ドロップダウン リストから [Run Migration Analysis] を選択します。得られた移行分析の概要には、さまざまな条件の現在のステータスが表示されます。アクセス ポイントが検出されると、最初に移行分析が自動的に実行されます。

移行分析レポートの表示

[Migration Analysis Summary] ページの [Select a command] ドロップダウン リストから [View Migration Analysis Report] を選択してレポートを生成できます。レポートには次の情報が含まれます。

- アクセス ポイントのアドレス
- ステータス
- タイムスタンプ
- アクセス ポイントのログ

ファームウェア アップグレード レポートの表示

選択したアクセス ポイントのアップグレード ステータスの現在のレポートを表示するには、[Select a command] ドロップダウン リストから [View Firmware Upgrade Report] を選択します。

次の情報が表示されます。

- [AP Address] : アクセス ポイントの IP アドレス。
- [Status] : ファームウェア アップグレードの現在のステータス。
- [TimeStamp] : アップグレードの日時。
- AP Logs

[Migration Analysis Summary] ページに戻るには [OK] をクリックします。

詳細については、「[Autonomous アクセス ポイントのアップグレード](#)」(P.17-16) を参照してください。

ロール変更レポートの表示

アソシエーション要求を送信するには、アクセス ポイントとコントローラとの有線接続が必要であるため、Autonomous アクセス ポイントに適切なロールを割り当てる必要があります。

これらのロール変更のレポートを表示するには、[Select a command] ドロップダウン リストから [View Role Change Report] を選択します。次の情報が表示されます。

- [AP Address] : アクセス ポイントの IP アドレス。
- [Status] : ロール変更の現在のステータス。
- [TimeStamp] : アップグレードの日時。
- AP Logs

[Migration Analysis Summary] ページに戻るには [OK] をクリックします。

TAC ケース添付ファイルの設定



(注) TAC ケース添付ファイルを設定する前に、有効なメール サーバを設定する必要があります。

TAC Case Attachment ツールを使用すると、該当するすべてのコントローラ TAC ケース情報を一度に簡単に添付できます。このツールには次の 2 つのオプションがあります。

- [Send] : attach@cisco.com に電子メールを送信します。
- [Download] : ローカル コンピュータに情報をダウンロードします。データを attach@cisco.com に電子メールで手動送信する必要があります。このオプションは、Prime Infrastructure サーバと Cisco の間に電子メール接続がない場合、または情報が大きすぎて電子メールに添付できない場合に便利です。

このツールでは、次の情報が送信されます。

- [Network Information] : デバイス インベントリの詳細とクライアントの種類が送信されます。
- [Controller Information] : 実行コンフィギュレーションの詳細、テクニカル サポート、メッセージ ログ、トラップ ログ、コントローラ クラッシュ ファイルが送信されます。
- [Access Point Information] : クラッシュ ファイルと無線コアダンプが送信されます。

情報を [Send] または [Download] するには、次の内容を入力する必要があります。

- 有効な TAC ケース番号を入力します。
- コントローラまたは AP 情報を送信する場合は、コントローラを選択します。



(注) [additional comments] テキスト ボックスを使用して追加情報を送信することもできます。情報を送信した後、Case ツールの [attachment] セクションを参照することで、データが Cisco に到着したかどうかを確認できます。



(注) このツールでは、コントローラまたはアクセス ポイントの情報を収集およびアップロードするために、コントローラに対する読み書きアクセス権が必要です。