AP のローカル Web ページへのアクセス

一般に、Meraki ネットワークは、ローカル インターフェイスではなくダッシュボードを使用して設定されます。ただし、いくつかのタスクにおいては、AP のローカル Web ページ上の情報が役に立ちます。

AP のローカル Web ページにアクセスする手順は次のとおりです。

1. AP を無線でまたは有線クライアントとして関連付けます（AP のイーサネット ポートに接続されているイーサネット ケーブルを使用）。
2. http://my.meraki.com/ にアクセスします。

AP のローカル Web ページは、次を含むさまざまな設定、モニタリング、およびトラブルシューティングの各アクティビティに使用できます。

- AP のステータス（設定、接続、ファームウェアのアップグレードなど）の表示。
- チャネル使用率およびクライアントへの AP の信号強度の表示。
- クライアント/AP 間の速度試験の実行。
- AP のメッシュ ネイバーに関する統計情報の表示。
- AP のスタティック IP アドレスの設定。

新しい AP の追加

[Configure（設定）] > [Add access points（アクセス ポイントの追加）] ページで、新しいアクセス ポイントを簡単に追加できます。

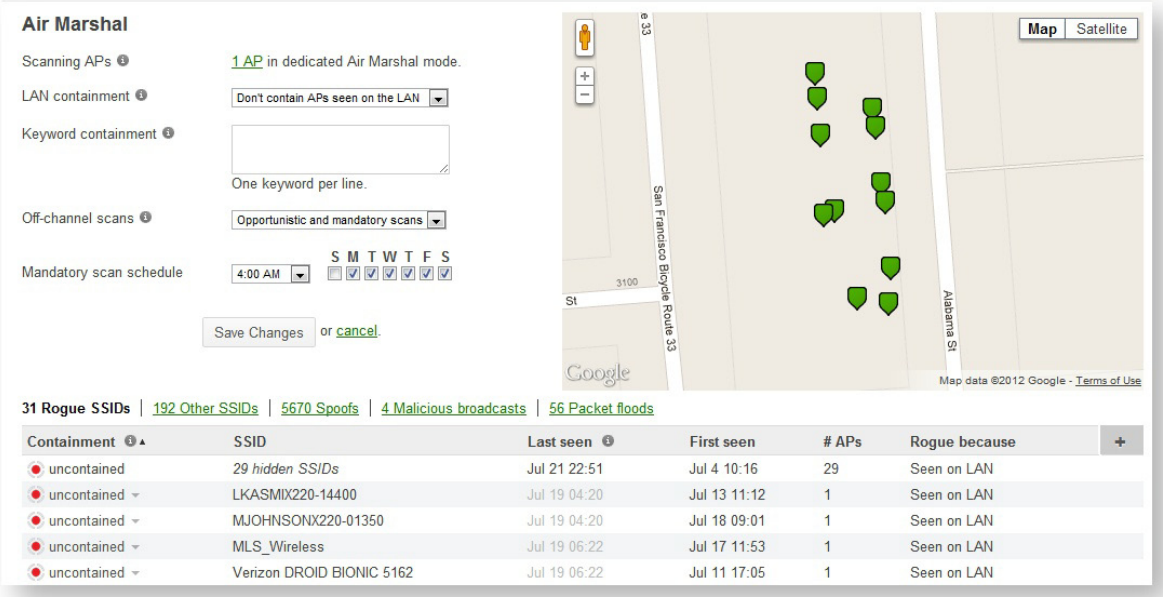
アクセス ポイントの注文番号またはシリアル番号を入力するだけです。新しい住所を入力することで、アクセス ポイントを新たに配置する場所を Google マップ上で指定できます。アクセス ポイントがアクセス ポイント リストに表示されるようになり、既存のネットワーク構成がダウンロードされます。

Meraki

Air Marshal - ワイヤレス侵入防御システム（WIPS）

Meraki の Air Marshal は、フルタイムの堅牢なワイヤレス侵入防御 システム（WIPS）で、ワイヤレス ネットワークに対する潜在的な攻撃を検出、特定、および修復できる強力な機能を実現します。Air Marshal は、ネットワーク事業者が迅速かつ簡単に脅威を特定し、Meraki ワイヤレス ネットワークを健全に保つのに役立ちます。

フルタイムの専用 Air Marshal AP を使用して、有線およびワイヤレス ネットワークが常時モニタされます。特定の条件に一致する不正な AP が出現した際に、指定したユーザに自動でアラートが送信されます。



詳細は、『Meraki Solution Guide for Air Marshal（Air Marshal に関する Meraki ソリューション ガイド）』でも確認できます。

AP ライセンス

Meraki ライセンスの詳細は、「Meraki Licensing FAQ（Meraki ライセンス FAQ）」を参照してください。

組織が Meraki デバイスを管理するには、現行ライセンスを所有している必要があります。各組織には、特定の期間（通常は 3 年または 5 年）、最大数の Meraki デバイス（AP および AP 以外）を使用するライセンスが付与されます。

管理者は、[Configure（設定）] タブの [License Info（ライセンス情報）] ページで組織のライセンスを管理できます。

ライセンスの追加

管理者は、[License Info（ライセンス情報）] ページで AP のライセンス上限を拡張できます。ライセンスが同時に終了するように、Meraki クラウドで組織のライセンス更新日が自動的に延長されます。

ライセンスの更新

管理者は、更新日の 30 日以内であればライセンスを更新できます。更新するには、[License Info（ライセンス情報）] ページで [Renew license（ライセンスの更新）] ボタンをクリックし、ライセンス キーを入力します。

ライセンスの期限切れまたは AP のライセンス制限の超過

組織のライセンスの期限が切れるか、組織の AP の数がライセンス制限を超えた場合、ライセンス付与の状態を有効な状態に戻すための猶予期間が組織の管理者に与えられます。詳細は、「Meraki Licensing FAQ（Meraki ライセンス FAQ）」を参照してください。

AP のソフトウェア アップグレード

Meraki ではそのシステムの管理コスト削減に努めています。この目標を達成するための 1 つの方法として、ソフトウェア アップグレード プロセスの一元管理が挙げられます。ライセンス付与された組織に、管理者およびワイヤレス ユーザの作業中断を最小限に抑える方法で MCC および AP のファームウェアのアップグレードを定期的にリリースしています。

Meraki ネットワークは、インターネットに接続して MCC にアクセス可能でさえあれば、最新ファームウェアにアップグレードされます。アップグレードがある場合、ネットワーク管理者は、アップグレードの約 2 週間前にメール通知を受信します。管理者は Meraki サポートに連絡して、アップグレードを遅らせるか、無期限に延期するかを選択できます。アップグレードは、[Network-wide settings（ネットワーク全体の設定）] の [Firmware upgrades（ファームウェアのアップグレード）] でユーザが指定した日時に実行されます。

AP のローカル Web ページに、アップグレードが進行中であるかどうかが表示されます。アップグレードのダウンロードには、高速インターネット接続を使用した場合、約 30 分かかります。アップグレードが完了すると、ノードが自動的にリブートします。

Meraki AP には、新しいファームウェアをダウンロードするためのメモリ パーティションがあります。そのため AP は、新しいファームウェアのダウンロード中も動作し、クライアントにサービスを提供し続けます。リブート後、AP は新しいファームウェアを試し、ファームウェアに障害が発生した場合は 古いファームウェアに戻します。

Meraki

Meraki AP への IP アドレスの割り当て

すべての Meraki ゲートウェイ AP（イーサネットで LAN に接続する AP）にはルーティング可能な IP アドレスを割り当てる必要があります。これらの IP アドレスは、各 AP で直接設定するか（下記の指示を参照）、アップストリームの DHCP サーバを介して AP に割り当てることができます。

DHCP を介して IP アドレスを取得する場合でも、Meraki AP では、一般に、スタティック IP アドレスの割り当てが推奨されています。この場合、DHCP サーバは、Meraki AP に属する MAC アドレスごとにスタティック IP アドレスを割り当てるように設定する必要があります。802.1x 認証など、ワイヤレス ネットワークのその他の機能は、AP にスタティック IP アドレスが割り当てられていることを想定している場合があります。

Meraki AP でのスタティック IP アドレスの直接設定

所定の AP で直接スタティック IP アドレスを設定するには、次の手順に従います。

1. クライアント マシン（ラップトップなど）を使用して、ワイヤレスで（AP の SSID ブロードキャストに関連付ける）、または有線で AP に接続します（有線の場合、イーサネット ケーブルの一端をクライアント マシンに差し込み、イーサネット ケーブルのもう一端を AP のイーサネット ジャックに差し込みます。クライアント マシンに接続するために、既存のイーサネット接続から AP の接続を外す必要がある場合があります）。
2. クライアント マシンの Web ブラウザで次の URL を開き、AP 内蔵の Web サーバにアクセスします。
   http://my.meraki.com
3. [Static IP Configuration（スタティック IP の設定）] タブをクリックします。ログインするよう求められます。デフォルトのユーザ名は「admin」で、デフォルトのパスワードは AP のシリアル番号（ハイフン含む）です。
4. この AP がインターネットへの有線接続で使用するスタティック IP アドレス、ネット マスク、ゲートウェイ IP アドレス、および DNS サーバを設定します。必要に応じて、この AP を LAN へのイーサネット接続に再接続します。

DHCP 予約による Meraki AP のスタティック IP アドレスの設定

管理者は、各 Meraki AP にスタティック IP アドレスを関連付けて設定するのではなく、アップストリームの DHCP サーバを使用して Meraki AP にスタティック IP アドレスを割り当てるよう設定できます。「DHCP 予約」では、IP アドレスが Meraki AP の MAC アドレス用として「予約」されます。

バンドの選択および帯域のステアリング

バンドの選択

バンドの選択機能を使うことで、管理者は 2.4 GHz 帯域と 5 GHz 帯域の両方（両方とも帯域のステアリングがイネーブル）で、または 5 GHz 帯域のみでブロードキャストするように SSID を設定できます。

帯域のステアリング

帯域のステアリングでは、通常はワイヤレス デバイスによる使用率が非常に高い 2.4 GHz 帯域から、使用率のそれほど高くない 5 GHz 帯域に、5 GHz 対応クライアントをステアリングします。帯域のステアリングによって、クライアントが使用できる総帯域幅およびキャパシティが拡大し、また 5 GHz 帯域によりクライアント パフォーマンスが向上します。

バンドの選択および帯域のステアリングは、[Configure（設定）] タブの [Access Control（アクセス制御）] ページで設定します。

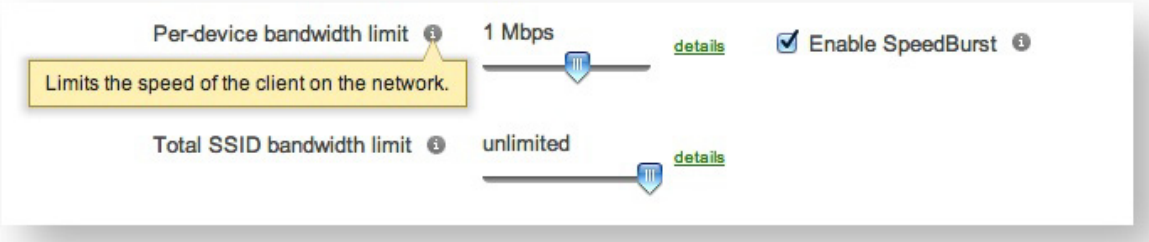
Meraki

帯域幅制御

帯域幅制御によって、許可されている以上の帯域幅をユーザが使用しないようにできます。Meraki クラウドには、アップロード量とダウンロード量の上限値を適用する帯域幅制御モジュールが統合されています。この設定を使用して、たとえば、ある SSID の VOIP ハンドセットへの帯域幅割り当てを増やして、別の SSID のデータのみのユーザへの帯域幅割り当てを減らすことができます。帯域幅の制限は、ワイヤレス クライアントが AP 間でローミングする場合でも一貫してクライアントに適用されるように、Meraki AP が施行しています。

Meraki ダッシュボードでは、アップロード量とダウンロード量に異なる上限値を適用できます。アップロード量とダウンロード量に異なる上限値を設定することは、たとえば、大容量の画像（CAD 図など）を定期的にダウンロードする必要があるが、アップロードすることがないユーザの場合に役立ちます。特定のアプリケーション要件および使用可能な帯域幅を考慮して、最適な帯域幅設定を決定する必要があります。

帯域幅の制限は、SSID ごとまたはユーザごとに適用できます。SSID ごとに帯域幅の制限を設定するには、[Configure（設定）] タブの [Access Control（アクセス制御）] ページに移動します。



管理者は、[Access Control（アクセス制御）] ページの [Bandwidth Limits（帯域幅の制限）] セクションのチェックボックスを使用して、SpeedBurst をイネーブルにすることで帯域制限を使用する際のユーザ エクスペリエンスを向上できます。SpeedBurst によって、各クライアントは割り当てられた上限値を短い時間「一気に」超過できるため、処理が快適になる一方で、特定のユーザが長時間にわたり公正な割り当て分を超えて帯域幅を使用することがなくなります。ユーザは、最長で 5 秒間、割り当てられた帯域幅の制限を 4 倍まで超えることができます。

Meraki ダッシュボードでは、顧客がホストする RADIUS サーバを使用する場合に帯域幅をユーザごとに制限する設定も可能です。

最後に、課金がイネーブルになっている場合、各課金層に適用する帯域幅の制限を設定できます。

ブリッジ モード

ブリッジ モードでは、Meraki AP がブリッジとして機能することにより、ワイヤレス クライアントがアップストリームの DHCP サーバから IP アドレスを取得できます。

次のいずれかに当てはまる場合は、ブリッジ モードをイネーブルにする必要があります。

- ネットワーク内の有線クライアントとワイヤレス クライアントが相互に到達可能である必要がある（たとえば、ワイヤレス ラップトップがネットワーク プリンタの IP アドレスを検出する必要がある、または有線デスクトップがワイヤレス監視カメラに接続する必要がある）。
- レイヤ 2 のマルチキャスト パケットとブロードキャスト パケット（ARP、Bonjour など）が、デバイス検出やネットワーキングなどのために有線クライアントとワイヤレス クライアントの両方に限定的な方法で伝搬される必要がある。
- ワイヤレス ネットワークがレガシー VPN クライアント（つまり、NAT トラバーサル非対応のクライアント）をサポートする必要がある。
- 有線クライアントとワイヤレス クライアントが、モニタリングやアクセス制御（ネットワーク内の Web ゲートウェイがクライアントの IP アドレスに基づいてインターネット アクセスを許可/拒否するなど）のために同じサブネット内の IP アドレスを持つ必要がある。
- Meraki AP とアップストリームの有線インフラストラクチャとの間で、ワイヤレス トラフィックが VLAN タグ付けされる必要がある。

ブリッジ モードをイネーブルにした場合の影響は次のとおりです。

- 管理者は、SSID に基づく成人向けコンテンツ フィルタリングをイネーブルにすることができない。成人向けコンテンツ フィルタリング機能は DNS ベースであるため、ブリッジ モードでは、ネットワークの DHCP サーバによりアドバタイズされる DNS サーバを使用することによって、成人向けコンテンツ フィルタリングがディスエーブルになります。
- 複数の DHCP サーバを使用できるが、これらの DHCP サーバは同じサブネットからの IP アドレスをワイヤレス クライアントに割り当てる必要がある。これにより、これらの IP アドレスを、Meraki AP の接続先の LAN でルーティングできるようになります。

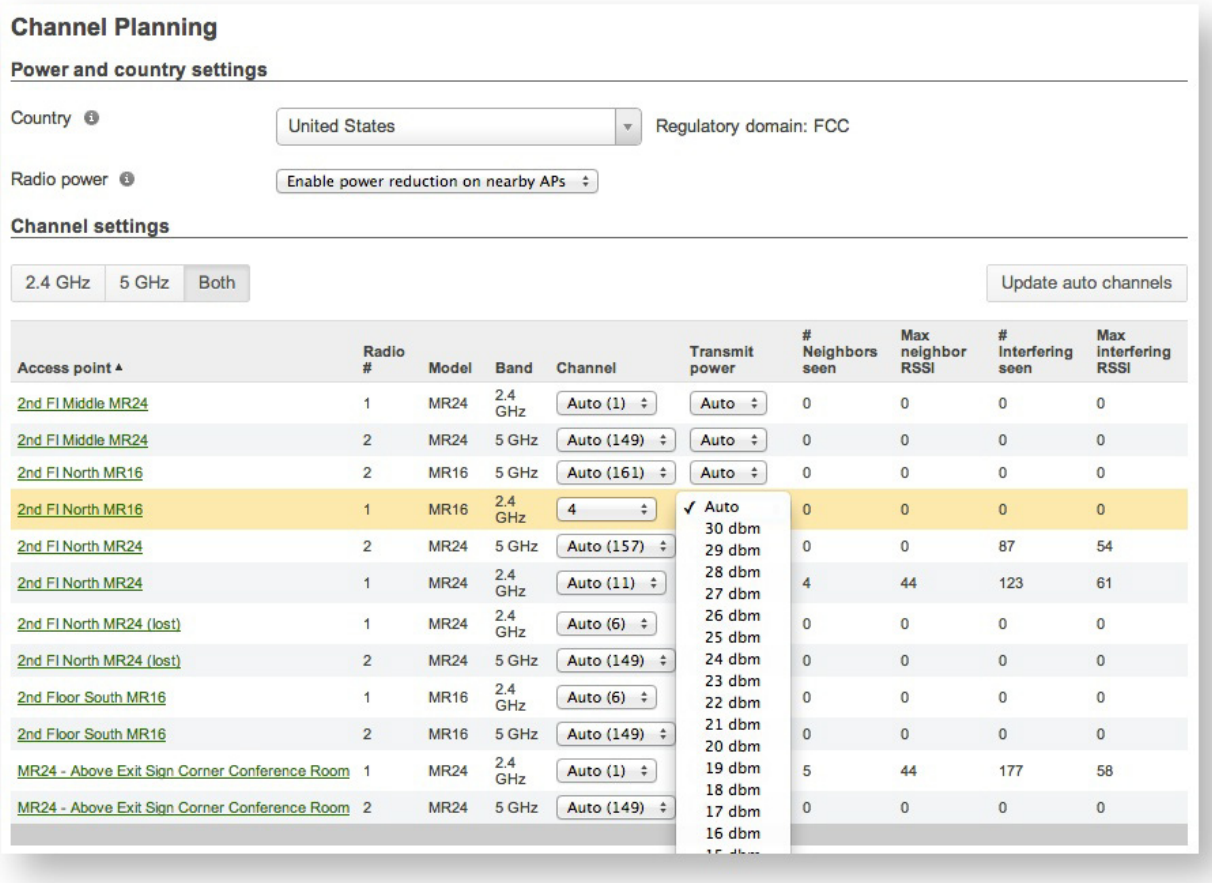
チャネル計画

チャネルの選択

チャネルを選択する際には、Meraki AP の無線に RF チャネルを割り当てます。チャネル割り当てを最適化すると、チャネル干渉やチャネル使用率が低下するため、ネットワークの全体的なパフォーマンスが向上し、ネットワークのクライアント キャパシティが増加します。

チャネルの選択は、[Configure（設定）] タブの [Radio Settings（無線の設定）] ページで設定します。2 つのオプションから選択できます。

1. [Automatic（自動）]：管理者はこのオプションを使用して、Meraki クラウドが AutoRF を使用して最適なチャネルを無線に自動的に割り当てることができるようにします。Meraki クラウドは、全体的なネットワークのパフォーマンスを定期的に測定し、AP に新しいチャネルを割り当てることで、ネットワークの最適なチャネル設定を決定します。
2. [Manual（手動）]：管理者はこのオプションを使用して、Meraki AP が 2.4 GHz 帯域と 5 GHz 帯域で使用するチャネルを手動で設定できます。これらのチャネル割り当ては、ネットワーク内の AP ごとに設定できます。



チャネル割り当てを変更すると、顕著なネットワークのダウンタイムが生じる可能性があります。管理者は、操作が行われない期間（チャネルの再割り当てによる中断が最小限のとき）にワイヤレス ネットワーク内のチャネルを自動的に再割

り当てするように Meraki クラウドを設定できます。または、管理者はクラウドにより算出されたチャネル割り当てを必要に応じて実行できます。

無線に割り当てることができるチャネルのリストは、AP が配置されている国に基づいて自動的に入力されます。そのため、チャネルの管理が地域特有の無線通信規制に準拠するように、[Country（国）] の値を正しく設定する必要があります。[Country（国）] セレクタは、[Channel Selection（チャネル選択）] コントロールの上にあります。

一部の規制機関では、特定のチャネルの屋外 AP での使用が禁止されています。手動によるチャネルの選択を使用して、このようなチャネルを使用しないようにします。たとえば、FCC は、屋外 AP での U-NII-1 チャネル（36、40、44）の使用を禁止しています。

チャネルの拡散

チャネルの選択を自動に設定すると、「チャネルの拡散」が 自動的に設定され、これにより、Meraki AP はさまざまなチャネルで動作できるように なります。チャネルの拡散では、ネットワークでの RF 使用率および RF 干渉を 最小限に抑えるチャネルが選択されるため、全体的なネットワークのパフォーマンスと クライアント キャパシティ（ネットワークに接続できるワイヤレス クライアントの数）が 最大になります。

チャネルの拡散は、単一のチャネルが多数のクライアントで飽和状態になる可能性のある環境に最適です。たとえば、数百のワイヤレス クライアントがある講堂において、複数の AP が同じ空間でブロードキャストしている場合、チャネルの拡散をイネーブルにする必要があります。

送信電力の制御

管理者は、ネットワーク内のすべての AP の送信電力を 100 % に設定するか、最適なパフォーマンスのための最適な電力設定を Meraki クラウドが決定できるようにするかを選択できます。AP が高密度で配置されており、カバレッジが著しく重複している場合、クラウド コントローラは送信電力を下げることで干渉を最小限に抑えられると判断します。この状況では、ある AP が停止してカバレッジにギャップが生じると、それを補うために隣接の AP の電力レベルが自動的に引き上げられます。管理者は、[Radio Settings（無線の設定）] ページで、フル送信電力または送信電力の自動選択を選ぶことができます。

チャネル計画レポート

このレポートを使用すると、管理者は、ネットワークでの現在のチャネル計画の概要と、Meraki AP、Meraki 以外の AP、不正 AP に関係なくすべての AP（実行された直近のネットワーク スキャン時に各チャネルで検出されたもの）を確認できます。管理者はこの表を使用して、現在のチャネル計画、送信電力、および周辺エリアにおける干渉 AP を詳細に把握できます。

クライアント詳細

管理者は、デバイス リスト内の特定のデバイスをクリックして、ワイヤレス クライアントに関する追加情報を取得できます。

次の機能があります。

- [Client configuration details（クライアント設定の詳細）]

  ページの上部で、管理者は特定のクライアントの詳細情報（MAC アドレスと IP アドレス、デバイス タイプとメーカー、オペレーティング システム、Bonjour/DHCP/NetBIOS ホスト名、無線カードの機能、最新の SSID、AP、ネットワーク上の時刻、最新のユーザの Active Directory ユーザ名など）を確認できます。
- [Client location（クライアント ロケーション）]

  ワイヤレス クライアントのおおよそのロケーションが Google マップまたはカスタム フロア プラン上に示されます。
- [Traffic analysis（トラフィック分析）]

  [Client Overview（クライアント概要）] ページと同様の円グラフに、特定のクライアントのネットワーク使用量に関する詳細が表示されます。[Configure（設定）] > [Network Settings（ネットワーク設定）] ページで「カスタム円グラフ」を追加している場合は、追加の円グラフがここに表示され、特定の範囲の HTTP ホスト名、IP、およびポートでのクライアント使用量をカスタムで トラッキングできます。
- [Dynamic access control（ダイナミック アクセス制御）]

  このページを使用して、管理者は、ワイヤレス デバイスをブロックするか、スプラッシュ ページが表示されないようにワイヤレス デバイスをバイパスするダイナミック アクセス制御ポリシーを作成できます。これらの設定を行うには、管理者は [Edit（編集）] ボタンをクリックして、[Network access（ネットワーク アクセス）] フィールドを [normal（標準）]、[blocked（ブロック済み）]、または [whitelisted（ホワイトリスト追加済み）] に変更します。必要に応じて、管理者はブラックリストに追加されたユーザに対してブロック ページで表示するメッセージを設定できます。SSID ごとに設定できるグループ ポリシーをユーザに手動で割り当てることもできます。
- [Event log（イベント ログ）]

  このページには、この特定のクライアントのイベント ログへのリンクもあります。
- [Live tools（ライブ ツール）]

  [AP details（AP 詳細）] ページのライブ ツールと同様、管理者はこのページでクライアントを検索したりクライアントへの ping を実行したり、さらにはユーザのアクティビティを示すリアルタイム パケット カウンタを確認することもできます。

クライアント IP 割り当て

管理者は、次の 2 つのアドレッシング モードのいずれかを使用して IP アドレスをワイヤレス クライアントに割り当てることができます。アドレッシング モードは [Configure（設定）] タブの [Access Control（アクセス制御）] ページで SSID ごとに設定します。

Meraki

クライアント ロケーション サービス

[Client details（クライアント詳細）] ページの右上隅にあるマップには、クライアントのおおよその位置（ロケーション）が青い点で示されます。

クライアント ロケーションは、精度を高めるためにキャリブレーション済み加重平均および AP 選択アルゴリズムを採用した、高度な三角測量技術を使用して特定されます。クライアント ロケーションは、過去 24 時間のデータを使用して算出されます。カスタム フロア プランにクライアント ロケーションを表示するには、ロケーションの算出に使用された、クライアントを「認識できる」すべての AP が同じカスタム フロア プラン上に存在する必要があります。カスタム フロア プランに表示できない場合でも、Google マップにクライアント ロケーションを表示できます。クライアントが現在関連付けられているアクセス ポイントからのクライアント ロケーション データを更新するには、このページの [Live Tools（ライブ ツール）] セクションの [Locate Client（クライアント ロケーションの特定）] ボタンをクリックします。

正確なロケーションを取得するには、少なくとも 3 つのアクセス ポイントが必要です。さらに、すべてのアクセス ポイントが直線に並ぶような配置にすることは避ける必要があります。このような状況では、クライアント ロケーションは、一直線に並んだアクセス ポイントの線上に常に表示されます。 精度を最大にするには、アクセス ポイントを直線上ではなく、分散して配置する必要があります。

Meraki

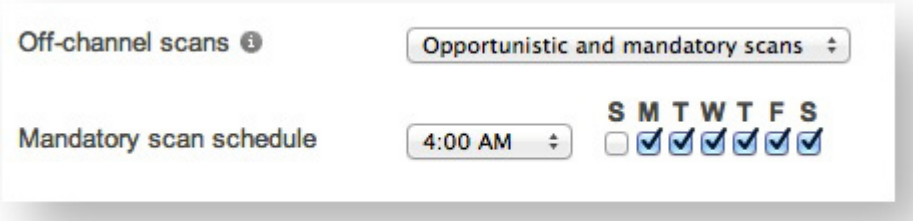
Air Marshal の設定

Air Marshal を使用すると、(a)クライアントにサービスを提供する通常の AP、または(b)スキャン モードのフルタイム専用 Air Marshal AP のいずれかを使用して攻撃を検出できます。

- 定期的な AP スキャンの設定
- Air Marshal AP
- 自動 LAN 封じ込め
- キーワードによる封じ込め
- 手動による封じ込め

定期的な AP スキャンの設定

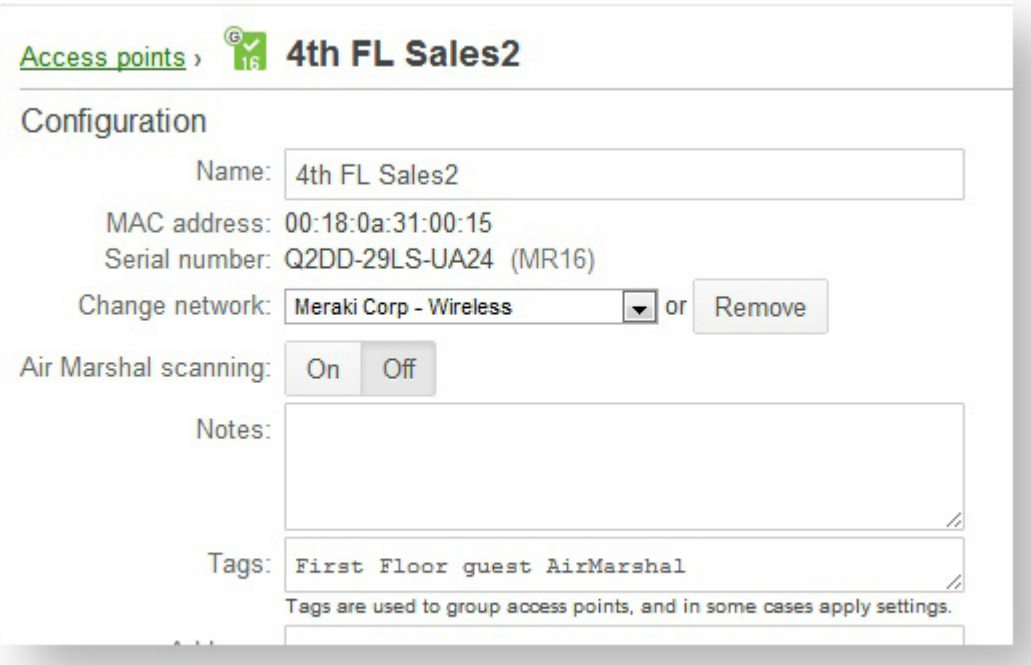
専用スキャン モードでない AP は、現在クライアントにサービスを提供しているチャネルのみをスキャンします。すべてのチャネルのスキャンは、クライアントを切断する可能性があるため、関連付けられているクライアントが存在しない機会を使用して実行します。希望に応じてカスタマイズ可能な時間に必須スキャンをスケジュールすることもできます。



通常の AP でもワイヤレス攻撃を検出できますが、攻撃の検出とアラートがリアルタイムで行われない可能性があります。真にリアルタイムでの可視化を実現するには、AP を Air Marshal モードに設定する必要があります。

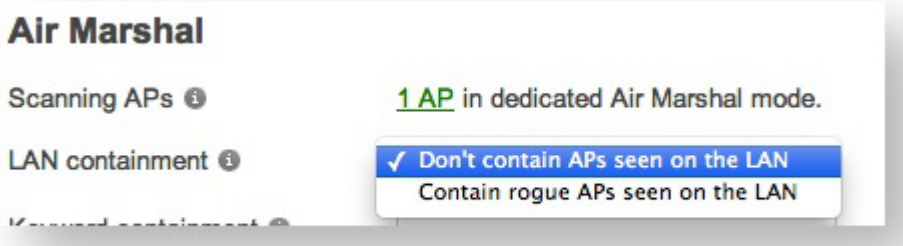
Air Marshal AP

専用のフルタイム スキャンをイネーブルにするには、AP が専用フルタイム Air Marshal モードになっている必要があります。この Air Marshal AP は、有線ネットワークとワイヤレス ネットワークを継続的にスキャンして侵入を検知します。Meraki の Air Marshal の予防的保護では、有線ネットワーク上の不正 AP を自動的に封じ込めたり、ユーザ指定キーワードが含まれる不正 SSID を封じ込めたりすることができます。AP をフルタイムの専用侵入スキャナとして設定するには、AP タグ「AirMarshal」を特定の AP に追加するか、または [AP details(AP 詳細)] ページで Air Marshal をオンにします。



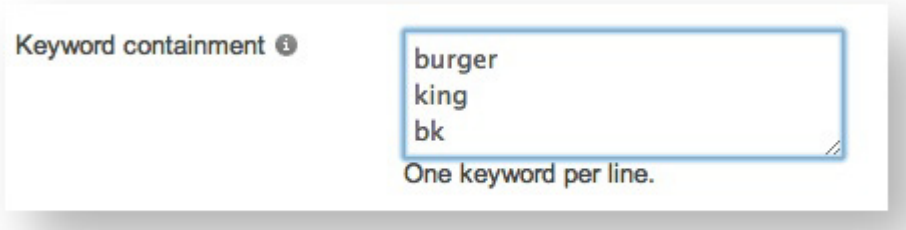
自動 LAN 封じ込め

有線ネットワーク上の不正アクセス ポイントを自動的に封じ込めるために、自動 LAN 封じ込みを設定できます。これを設定するには、[Monitor（モニタ）] > [Air Marshal] ページで、[LAN containment（LAN 封じ込め）] セクションの [Contain rogue APs seen on the LAN（LAN で検出された不正 AP を封じ込める）] を選択します。



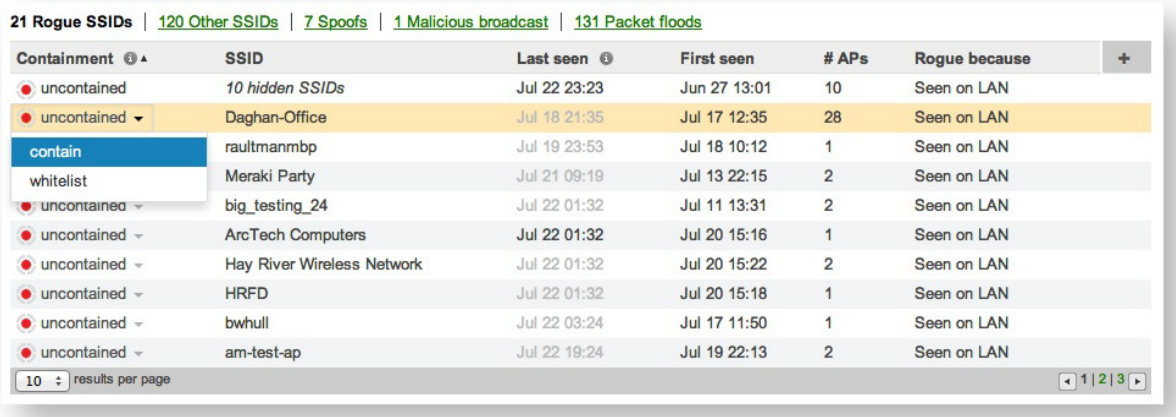
キーワードによる封じ込め

特定の指定キーワードに一致する不正 AP を自動的に封じ込めるように Air Marshal AP を設定できます。特定のキーワードを含む SSID を自動的に封じ込めるように Meraki AP を設定するには、[Keyword containment（キーワードによる封じ込み）] フィールドで、1 行に 1 つずつキーワードを入力します。



手動による封じ込め

[Air Marshal] ページでは、潜在的な脅威のリストを表示して、手動で措置を講じることができます。デバイスが不正である根拠を示す情報と、そのデバイスが確認された最初と最後の時間、デバイスのメーカー、デバイスがどの VLAN に存在したかなどのパラメータを確認し、列を追加してカスタマイズすることができます。追加の措置を講じることもでき、デバイスをホワイトリストに加えるか、封じ込めることができます。

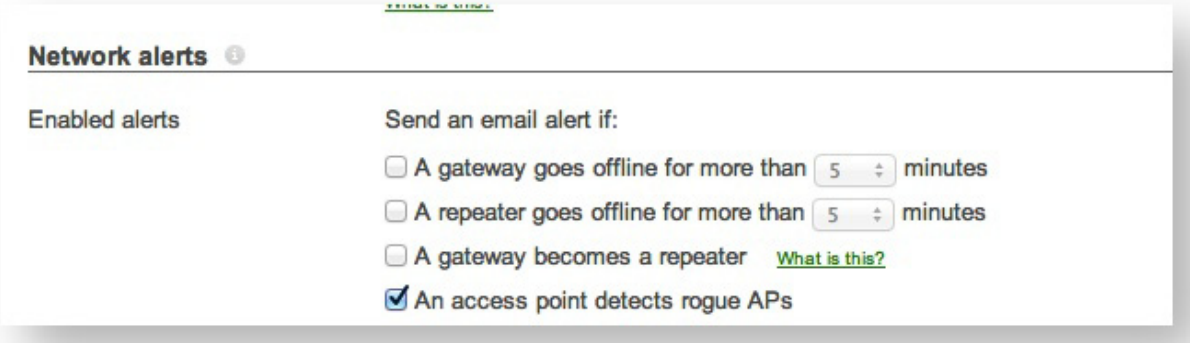


アラームの設定

Meraki AP は、ネットワーク上に不正 AP が出現した場合にネットワーク管理者に自動的に 連絡して、管理者が潜在的な脅威に関する最新情報を把握できるように します。

不正アラームをイネーブルにするには、次の手順に従います。

1. [Configure（設定）] > [Network-wide settings（ネットワーク全体の設定）] にアクセスします。
2. 「アクセス ポイントが不正 AP を検出」した場合に電子メールのアラートを送信するためのチェックボックスを選択します。



次のいずれかの条件に一致する不正 AP がネットワークに侵入すると常にアラームが送信されます。

- 有線 LAN 上の不正 AP
- SSID キーワードに一致する不正 AP

認証サーバの設定

Meraki クラウドでは、次の 5 つの異なる用途の認証サーバがサポートされています。

1. Meraki-Hosted 認証サーバ
2. MAC ベースのアクセス制御や WPA2-Enterprise 802.1x 認証用の、外部でホストされている RADIUS サーバ
3. サインオン スプラッシュ ページ認証用の、外部でホストされている RADIUS サーバ
4. サインオン スプラッシュ ページ認証用の、外部でホストされている Active Directory サーバ
5. サインオン スプラッシュ ページ認証用の、外部でホストされている LDAP サーバ

認証サーバのタイプは [Configure（設定）] タブの [Access Control（アクセス制御）] ページで SSID ごとに設定します。たとえば、管理者は、Meraki-Hosted 認証サーバを使用してゲスト SSID のゲスト ユーザ アカウントを管理する一方で、顧客がホストする RADIUS サーバまたは Active Directory サーバを使用して従業員 SSID の従業員を認証します。

LAN の設定

Meraki ワイヤレス ネットワークに必要な有線 LAN インフラストラクチャの要件は最小限ですが、若干の変更が必要になることがあります。

Meraki AP のファイアウォール設定

ファイアウォールが設置されている場合は、特定のポートと IP アドレスの組み合わせで送信接続を許可する必要があります。最も基本的な設定の場合は、ポート 80（Web トラフィック）を開くだけで十分です。送信ポートと IP アドレスの最新のリストは次のサイトにあります。

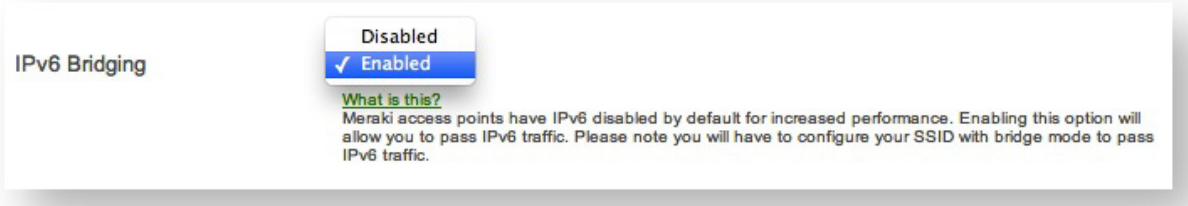
http://tinyurl.com/y79une3

IPv6 サポートのイネーブル化

[Addressing（アドレッシング）] の下にある SSID 固有の設定を使用しており、トラフィックが [Bridge mode（ブリッジ モード）] に設定されている場合、Meraki アクセス ポイントは IPv6 トラフィックを渡すことができます。IPv6 は Meraki NAT モードと互換性がないため、IPv6 の使用時にはトラフィックの分析や操作を行えません。また、IPv6 のファイアウォール機能、VPN 機能、およびルーティングもまだサポートされていません。クラウド コントローラとの通信には IPv4 が必須であることにも注意してください。

IPv6 サポートのイネーブル化

すべての新しい Meraki ワイヤレス ネットワークでは、デフォルトで IPv6 がイネーブルになっています。既存の Meraki ワイヤレス ネットワークの場合、[Configure（設定）] > [Network Settings（ネットワーク設定）] ページに移動して、[IPv6 Bridging（IPv6 ブリッジング）] で [enabled（イネーブル化）] を選択して、IPv6 をパススルー モードでイネーブルにすることができます。



すべての Meraki ハードウェアは、ネイティブで IPv6 をサポートする能力を備えており（トラフィック分析、VPN、およびファイアウォールのすべての機能が IPv6 で動作可能です）、このサポートは後でファームウェアのアップグレードを介して追加されます。

外部でホストされている Active Directory サーバ

サインオン スプラッシュ ページが使用されている場合、RADIUS を必要とせずに Meraki ワイヤレス ネットワークを Active Directory とネイティブに統合することができます。RADIUS 統合により提供される追加の設定オプションが不要なネットワークの場合は、仲介として機能する RADIUS サーバなしで AP が Active Directory と直接通信できると一定の利点があります。AD とネイティブに統合することにより、Microsoft NPS（またはその他の RADIUS サーバ）の設定が不要になります。また、マルチドメイン フォレストで RADIUS 統合を使用している場合（たとえば、学校で、サインオン スプラッシュ認証を使用するドメインが職員用に 1 つと学生用に 1 つある場合など）、ユーザはユーザ名に忘れずにドメインを含める必要があります（忘れるケースが多くあります）。あるいは、ユーザのログイン プロセスを簡単にするために、複雑な階層の RADIUS プロキシ サーバやカスタム スクリプトが必要になる場合があります。

Active Directory とのネイティブ統合を設定するには、サインオン スプラッシュが設定され、[Configure（設定）] > [Access Control（アクセス制御）] の [Authentication Server（認証サーバ）] ドロップダウン メニューで [Use My Active Directory Server（Active Directory サーバを使用）] が選択されている必要があります。

Active Directory サーバ オプションを選択したら、認証に使用されるすべてのドメイン コントローラの内部 IP アドレスと、使用されるすべてのドメイン コントローラに対する読み取り権限を持つ Active Directory 管理者のクレデンシャルを入力する必要があります。

Active Directory 認証を提供するための別個のアカウントを作成することをお勧めします。ユーザは、このアカウントを保護するために次の手順を実行する必要があります。

1. ドメイン（またはフォレスト）にグローバル セキュリティ グループを作成します。
2. ユーザ アカウントを作成し、新しいグループに追加します。
3. 新しいセキュリティ グループがユーザのプライマリ グループになるようにこのユーザ アカウントを更新します。
4. ドメイン ユーザ グループをこのアカウントから削除します。

これにより、このアカウントは、通常のドメイン ユーザのようには動作しなくなります。

さらに、グローバル カタログ（ポート 3268）を各ドメイン コントローラに対してイネーブルにする必要があります。

外部でホストされている LDAP サーバ

Active Directory と同様、サインオン スプラッシュ ページが使用されている場合、Meraki ワイヤレス ネットワークを LDAP 認証サーバとネイティブに統合できます。この認証を設定する方法は、「外部でホストされている Active Directory サーバ」で説明している方法とよく似ています。LDAP とのネイティブ統合を設定するには、サインオン スプラッシュが設定され、[Configure（設定）] > [Access Control（アクセス制御）] の [Authentication Server（認証サーバ）] ドロップダウン メニューで [Use My LDAP Server（LDAP サーバを使用）] が選択されている必要があります。

LDAP サーバ オプションを選択したら、認証に使用されるすべての LDAP サーバの内部 IP アドレス、適切なポート番号、および使用されるすべてのドメインに対する管理権限を持つ管理者のクレデンシャルを入力する必要があります。共通名（cn）およびドメイン コンポーネント（dc）は、次の図に示されている形式で入力する必要があります。

Meraki

外部でホストされている RADIUS サーバ

多くの組織が、既存のユーザ認証サーバまたはディレクトリ サーバを使って、無線 LAN へのアクセスを制御したいと考えています。一般的なサーバ タイプには、LDAP や Active Directory があります。RADIUS インターフェイスを備えていれば、どのタイプの認証サーバも Meraki ワイヤレス ネットワークと統合できます。管理者は、Meraki クラウドを使用して、複数の RADIUS サーバをフェールオーバー用に設定できます。

外部でホストされている RADIUS サーバを MAC ベースのアクセス制御または WPA2-Enterprise 802.1x 認証のどちらかとともに使用する場合、Meraki AP が RADIUS サーバにアクセス可能である必要があります。Meraki クラウドには、すべての Meraki AP が RADIUS サーバに接続できることを検証したり、RADIUS サーバに対する特定のユーザ クレデンシャルのセットをチェックしたりするための管理者向けのテスト ツールが用意されています。このテスト ツールは、[Configure（設定）] タブの [Access Control（アクセス制御）] ページに表示されます。

外部でホストされている RADIUS サーバをサインオン スプラッシュ ページで使用する場合、管理者は、外部でホストされている RADIUS サーバをユーザ認証に使用するように Meraki ワイヤレス ネットワークを設定できます。Meraki クラウドは、この設定における仲介として機能し、（1）一貫したエンド ユーザ エクスペリエンス（たとえば、ワイヤレス ユーザが別の AP に再関連付けされるときにスプラッシュ ページが再度表示されないようにする）を実現し、（2）RADIUS アカウンティング機能を提供します。

サインオン スプラッシュ ページが Meraki クラウドでホストされている場合、対話は Meraki クラウドと外部 RADIUS サーバとの間の直接的な RADIUS 交換になります。

サインオン スプラッシュ ページ自体が外部でホストされている場合、対話はスプラッシュ ページ サーバ、Meraki クラウド、および RADIUS サーバの間での交換になります。具体的には次のとおりです。

1. ワイヤレス クライアントが Meraki ワイヤレス ネットワークに関連付けられます。
2. ユーザが、Web ブラウザで最初の URL 要求を行います。
3. Meraki AP により、ユーザはスプラッシュ ページ サーバ上の URL にリダイレクトされます（管理者は、Meraki クラウドのこの URL を [Configure（設定）] タブの [Splash Page（スプラッシュ ページ）] ページで設定します）。ユーザをスプラッシュ ページ サーバにリダイレクトする際に、HTTP リダイレクトに Meraki AP によって次の HTTP パラメータが組み込まれます。
    a. continue_url：ユーザが要求した元の URL。スプラッシュ ページ サーバでは、このパラメータを解釈し、認証に成功した場合のユーザのリダイレクト先を決定できます。
    b. login_url：スプラッシュ ページ サーバが、HTTP POST ならびに収集されたユーザ クレデンシャルを送信する、Meraki クラウドでの URL（ステップ 4 を参照）。このパラメータはエスケープされ、中に continue_url が埋め込まれます。このパラメータがスプラッシュ ページ サーバによって解釈されることはありません。
    c. ap_mac：ユーザが関連付けられる Meraki AP の MAC アドレス。
    d. ap_name：ユーザが関連付けられる Meraki AP の名前（設定されている場合）。
    e. ap_tags：ユーザが関連付けられる Meraki AP に適用されるタグ（設定されている場合）。
    f. mauth：認証およびセキュリティ用に Meraki クラウドで使用される不透明型（opaque）の文字列。

4. 外部スプラッシュ ページ サーバは、ユーザのクレデンシャルをキャプチャし、login_url に指定された URL を使用して HTTP POST を Meraki クラウドに送信するための Web フォームをユーザに対して提示します（ステップ 3 を参照）。サーバにより、この HTTP POST に次のパラメータが組み込まれます。
    a. username：ワイヤレス ユーザがスプラッシュ ページ サーバで指定したユーザ名。
    b. password：ワイヤレス ユーザがスプラッシュ ページ サーバで指定したパスワード。
    c. success_url（オプション）：認証に成功した場合にワイヤレス ユーザがリダイレクトされる URL。スプラッシュ ページ サーバは、このパラメータを使用してユーザが要求した元の continue_url を上書きできます。
5. Meraki クラウドは、スプラッシュ ページ サーバから HTTP POST を受信すると、ユーザ名とパスワードを使用して外部 RADIUS サーバに RADIUS Access-Request を送信します。
6. RADIUS サーバは Meraki クラウドからの RADIUS Access-Request を処理し、Meraki クラウドに RADIUS Access-Accept または Access-Reject で応答します。RADIUS サーバは必要に応じて Meraki クラウドに RADIUS 属性を送信し、ワイヤレス ユーザ指定の情報より RADIUS 属性が優先されるようにできます。
7. Meraki クラウドは RADIUS サーバからの応答を処理し、それに従ってワイヤレス ユーザをリダイレクトします。
    a. Meraki クラウドが Access-Accept メッセージを RADIUS サーバから受信した場合は、ユーザの認証に成功しています。Meraki クラウドは、ユーザが要求した元の URL（continue_url）か、スプラッシュ ページ サーバにより オプションの success_url に指定された URL（ステップ 4 を参照）にユーザをリダイレクトします。
    b. Meraki クラウドが RADIUS サーバから Access-Reject メッセージを受信した場合は、ユーザの認証に失敗しています。この場合、スプラッシュ ページ サーバの URL（ステップ 3）にリダイレクトされます。

外部 RADIUS サーバへの接続が必要なため、Meraki クラウドが RADIUS サーバにアクセス可能である必要があります。この要件のために、RADIUS サーバへのインバウンド接続を許可するようにファイアウォールを変更することが必要となる場合があります。RADIUS サーバが一時的に利用不可になると、すでに認証されているワイヤレス クライアントは接続されたままになりますが、新たにネットワークにアクセスするワイヤレス クライアントの認証は行えなくなります。

Meraki

ファイアウォール規則

カスタム ファイアウォール規則により、管理者は、LAN 分離機能で行うよりも詳細にアクセスを制御できます。管理者は、SSID に関連付けられたワイヤレス ユーザから送信されるすべての要求を評価するための、一連のファイアウォール規則を定義できます。ファイアウォール規則は上から下に評価されます。一致した最初の規則が適用されると、それより後の規則は評価されません。一致する規則がない場合は、デフォルトの規則（すべてのトラフィックを許可）が適用されます。

レイヤ 3 ファイアウォール規則

次の図に、レイヤ 3 で適用される一連のカスタム ファイアウォール規則の例を示します。

#	Policy	Protocol	Destination	Port	Comment	Actions
1	Deny	TCP	Any	25	Block SMTP	
2	Deny	TCP	Any	6881	Block BitTorrent	
3	Allow	TCP	192.168.1.37/32	Any	Access to student printer	
	Deny	Any	Local LAN	Any	Wireless clients accessing LAN	
	Allow	Any	Any	Any	Default rule	

次の表に示すように、各種要求がさまざまな規則に一致します。CNN に対する Web 要求の場合、規則 1 ～ 4 が一致しないため規則 5（デフォルトの規則）が適用され、要求が許可されます。一方、TCP ポート 6881 経由の BitTorrent 要求の場合、規則 1 は一致しませんが、規則 2 は一致します。要求は拒否され、それより後の規則は評価されません。

Rule #	Attempted Action			
	Example #1: Web request to www.cnn.com.	Example #2: Print to 192.168.1.37.	Example #3: Send BitTorrent traffic.	Example #4: Access file server on LAN.
1	(no match)	(no match)	(no match)	(no match)
2	(no match)	(no match)	MATCH (deny)	(no match)
3	(no match)	MATCH (allow)		(no match)
4	(no match)			MATCH (deny)
5	MATCH (allow)			

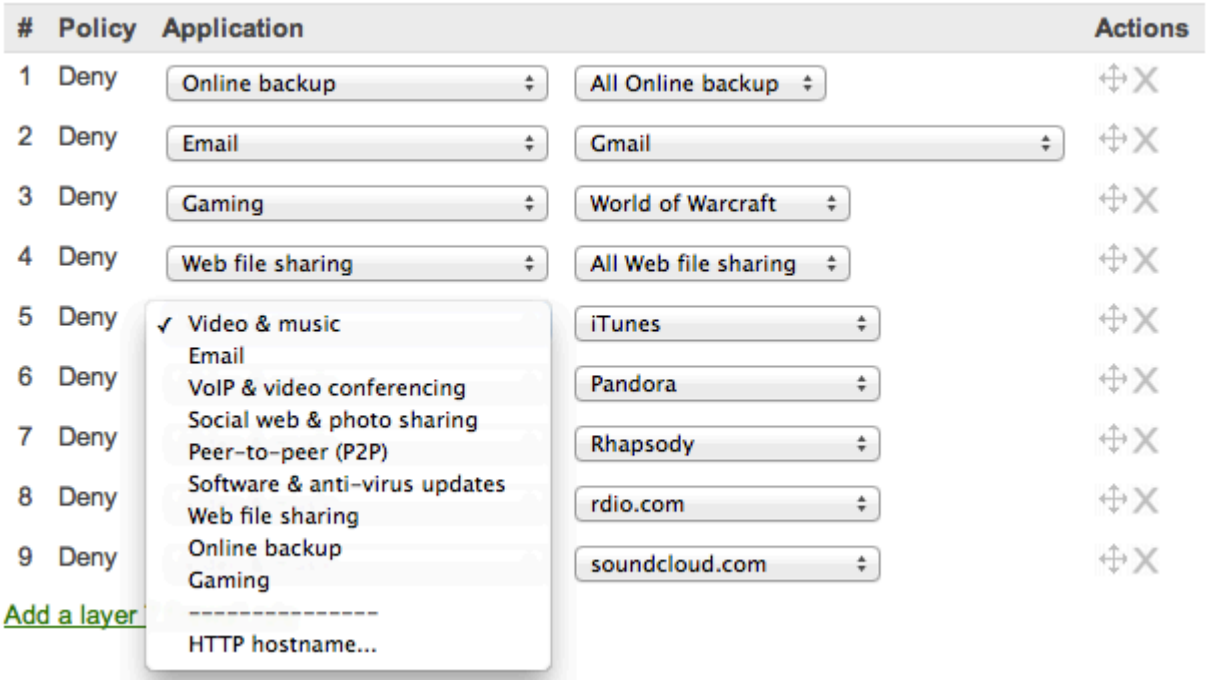
ファイアウォール規則は特定の SSID に適用することも、グループ ポリシーの一部として適用することもできます。

「ローカル LAN を拒否」というファイアウォール規則を作成すると、セキュアなゲスト SSID を簡単に作成できます。

レイヤ 7 ファイアウォール規則

Meraki 独自のレイヤ 7 トラフィック分析テクノロジーを使用すると、レイヤ 7 ファイアウォール規則を作成し、Meraki のヒューリスティック アプリケーション フィンガープリントを使用して特定の IP アドレスやポート範囲を指定しなくても、特定のアプリケーションを完全にブロックできます。これは、アプリケーションが使用する IP アドレスやポート範囲が 複数であったり、一定でなかったりする場合に役立ちます。

アプリケーションを [All video & music sites（すべてのビデオ/音楽サイト）] などのカテゴリでブロックしたり、カテゴリ内の特定のタイプのアプリケーション（たとえば、[Video & music（ビデオ/音楽）] カテゴリ内の [iTunes] のみ）をブロックしたりすることができます。次の図は一連のレイヤ 7 ファイアウォール規則を示しており、カテゴリ全体でアプリケーションがブロックされるものと、1 つのカテゴリ内で特定のアプリケーションがブロックされるものがあります。



www.cnn.com などの HTTP ホスト名でブロックすることも可能です。

ライブ アップデート

[Monitor（モニタ）] タブの [Maps（マップ）]、[Access Points（アクセス ポイント）]、および [Clients（クライアント）] の各ページではライブ アップデートがサポートされており、ネットワーク ステータスやクライアント使用状況などの情報がリアルタイムで表示されます。管理者は、この機能に対応しているページで [Live updates（ライブ アップデート）] リンクをクリックできます。ライブ アップデートがイネーブルになっている場合、Meraki クラウドでは、管理者がページを閲覧している間は約 30 秒ごとに、そのページの最新情報がワイヤレス ネットワークから取得されます。ライブ アップデートは、管理者が別のページを閲覧するとすぐに無効になります。ライブ アップデートは、トラブルシューティングを行い、AP のステータス（AP がネットワークから切断された場合など）とクライアント使用状況（現在どのクライアントがワイヤレス ネットワークに関連付けられ、どの程度の帯域幅を使用しているかなど）を詳細にモニタするための効果的な方法です。

MAC ベースの認証

MAC ベースのアクセス制御では、接続デバイスの MAC アドレスに基づいてワイヤレスの関連付けを許可または拒否します。ワイヤレス デバイスが関連付けを試みると、Meraki AP は Access-Request メッセージを使用して顧客構内 RADIUS サーバに問い合わせます。RADIUS サーバは、MAC アドレスに基づいて Access-Accept メッセージまたは Access-Reject メッセージで Meraki AP に応答し、デバイスをそれぞれ許可または拒否します。

この認証方式では、クライアント側の設定は必要ありません。ただし、ユーザ エクスペリエンスは低下します。ワイヤレスの関連付けを拒否されたワイヤレス クライアントは SSID に接続できないだけで、なぜ接続できないのかに関する明確な通知を受け取りません。

この認証方式を選択する場合は、[Access Control（アクセス制御）] ページの [RADIUS for MAC-based access control（MAC ベースのアクセス制御用 RADIUS）] セクションで、1 つ以上の RADIUS サーバを設定しておく必要があります。このセクションには、ネットワーク内のすべての Meraki AP に対するワイヤレス デバイス接続をシミュレートするテスト ツールがあります。

管理ロールの管理

組織管理者

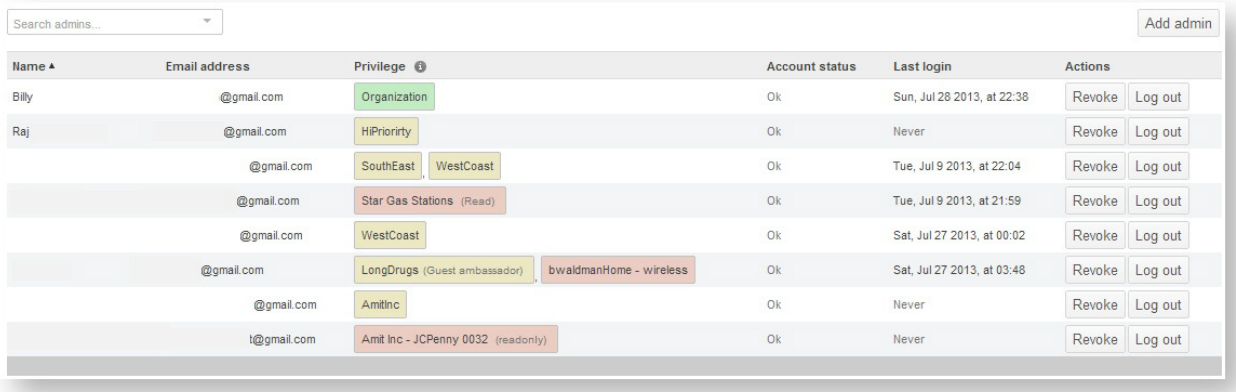
組織管理者は、組織内のすべてのネットワークを表示できます。組織管理者の種類には、(1)フルと(2)読み取り専用の 2 つがあります。組織管理アカウントは、[Organization(組織)] タブの [Configure(設定)] ページで管理されます。

フル組織管理者は、自分が属する組織内で次の操作を実行できます。

- 組織のフルまたは読み取り専用組織管理者アカウント、または組織のネットワーク管理者アカウントを作成および編集します。
    - 管理者が管理アカウントのパスワードをリセットすると、電子メールで管理者に新規パスワードが送信されます。管理者は、MCC で、任意のページの上部にある [my profile(マイ プロファイル)] リンクをクリックして自分のパスワードをリセットできます。
- ネットワークを作成、編集、および削除します。
- Cisco Meraki デバイスのライセンスを追加または更新します。

新規組織の最初のネットワークを作成した管理者は、自動的に組織管理者に指定されます。

組織管理者は、[Organization(組織)] > [Administrators(管理者)] ページ(次の図を参照)でネットワーク管理者を表示、追加、および削除します。このページでは、他の組織管理者を表示、追加、および削除することもできます。



ネットワーク管理者

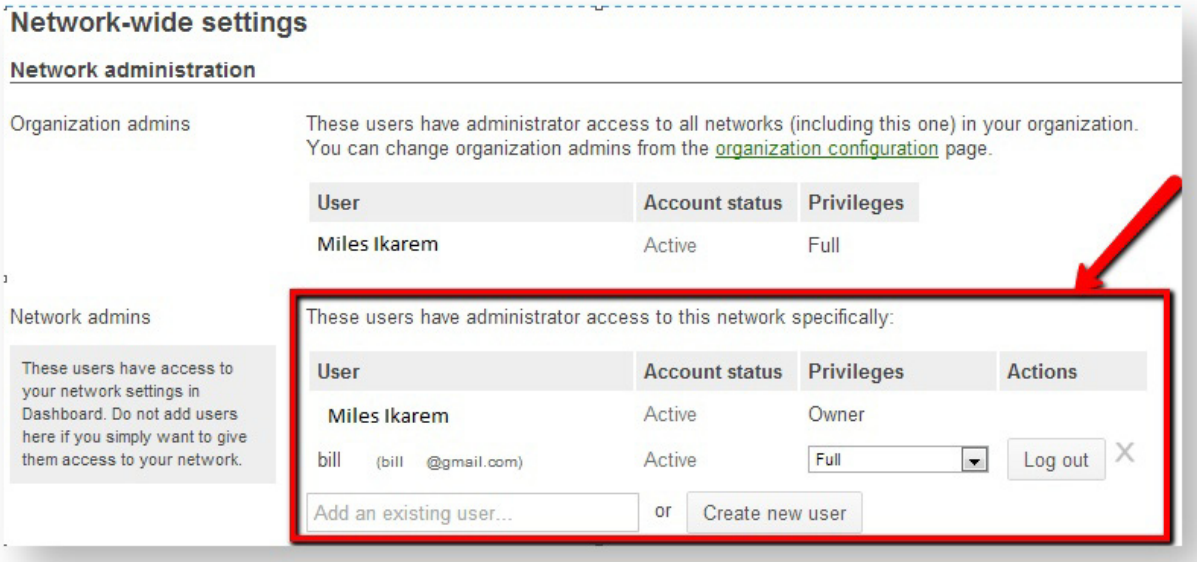
組織のネットワーク管理者として指定されている場合、その組織内のすべてのネットワークを表示できます。ネットワーク管理者の種類には、フル(読み取り/書き込み)と読み取り専用の 2 つがあります。管理アカウントは、[Configure(設定)] タブの [Network Wide Settings(ネットワーク全体の設定)] ページで管理されます。

ネットワーク管理者は、自分が属する組織内で次の操作を実行できます。

- 組織の管理者アカウントを作成、編集、および削除します。
    - 管理者が管理アカウントのパスワードをリセットすると、電子メールで管理者に新規パスワードが送信されます。管理者は、ダッシュボードで、任意のページの上部にある [my profile(マイ プロファイル)] リンクをクリックして自分のパスワードをリセットできます。
- 管理権限を付与されているネットワークを作成、編集、および削除します。

- 定義上、管理者は自分が作成するすべてのネットワークに対する管理権限を持っています。しかし、そのネットワークの作成者以外の管理者は、(ネットワークに対する管理アクセスを持つ別の管理者によって)ネットワークに対する管理アクセスが付与された後でないと、ネットワークにアクセスできません。

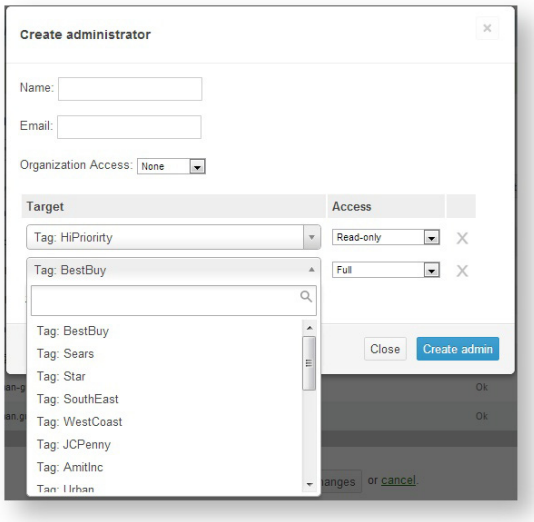
フル アクセス(読み取り/書き込み)を持つネットワーク管理者は、[Network Wide(ネットワーク全体)] > [Alerts & Administration(アラートと管理)] ページで他のネットワーク管理者を表示、追加、および削除できます。



タグベースの管理者割り当て

ここで説明しているように、組織内のネットワークにタグを付けて、グループや階層、あるいはその両方を作成できます。[Organization(組織)] > [Administrators(管理者)] ページを使用して、ネットワーク管理者を、ネットワーク タグにより割り当てられる権限とともに追加できます。上記の例では、ネットワーク管理者に SouthEast、WestCoast、および AmitInc の各ネットワーク タグに対するフル権限が付与されています。その他の管理者には、ネットワーク固有のアクセスが付与されています(たとえば、AmitInc - JCPenny 0032)。

[Add Admin(管理者の追加)] またはリストされている既存の管理者権限をクリックすると、組織内の個々のネットワークまたはネットワーク タグ、またはその組織自体にロールを追加するためのウィンドウが表示されます。



権限の優先順位

管理者に権限が重複して割り当てられている場合は、最も許可範囲の広い権限が使用されます。たとえば、A、B、および C の 3 つのネットワークを持つ組織で、ネットワーク B および C に「HighPriority」というタグが付けられているとします。組織管理者が John Doe にネットワーク C に対する読み取り専用アクセスを割り当て、一方で HighPriority タグへのフル アクセスを割り当てている場合、John Doe はネットワーク B および C に対するフル アクセス権を持つことになります。

管理ロールの管理の詳細については、ナレッジ ベースを参照してください。

Meraki-Hosted 認証サーバ

Meraki-Hosted 認証のイネーブル化

Meraki-Hosted 認証サーバを選択するためのオプションは、[Configure（設定）] > [Access control（アクセス制御）] ページで次のいずれかを設定すると表示されます。

- サインオン スプラッシュ ページ
- WPA2-Enterprise 802.1X 認証

ユーザの設定

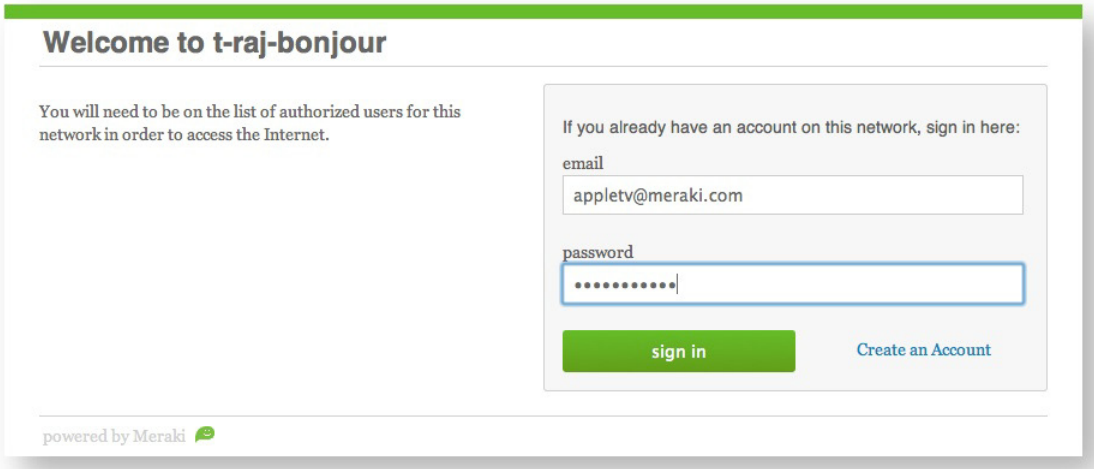
Meraki-Hosted 認証サーバは、Meraki クラウドを使用して設定します。管理者は [Configure（設定）] > [Users（ユーザ）] ページで、ユーザ アカウントを作成、編集、および削除できます。各ユーザ アカウントについて、管理者はそのユーザがログインに使用する名前、電子メール アドレス、およびパスワードを設定できます。また、有効期限をオプションで設定できます（一定期間の経過後に自動的に期限が切れるユーザ アカウントを作成する場合）。

ユーザ アカウントに有効期限を設定することにより、一定期間が経過した後にそのアカウントを無効にすることができます。この機能はゲスト アカウントの場合に役立ちます。最後に、[Access Control（アクセス制御）] ページには、ユーザが自分でアカウントを作成できる [self-registration（自己登録）] オプションがあります。ただし、作成されたアカウントは、このネットワークで許可されるユーザのリストに管理者が手動で追加するまでは、ネットワークにアクセスできません。管理者には、アカウントを承認するこのメニューにアクセスするための「ゲスト代表」権限を持つ特別なアクセスを付与できます。設定方法の詳細は、「Guest Management（ゲスト管理）」ページを参照してください。

ユーザ サインオン

エンドユーザは、Meraki-Hosted サーバで作成されたクレデンシャルを使用して、スプラッシュまたは WPA2 を介してサインオンできます。いずれの場合も、サインオン用のユーザ名は電子メール アドレスであり、パスワードはエンドユーザが Meraki スプラッシュから自分のアカウントを作成するときに選択するか、管理者がエンドユーザのアカウントを手動で作成するときに設定したものです。

MacBook での WPA2 を使用したサインオン ウィンドウ。



スプラッシュ ページを使用したサインオン ウィンドウ。

Meraki-Hosted 認証サーバで設定したユーザ アカウントは、組織内のネットワークで共通で使用されるアカウントになります。そのため、あるネットワークでユーザ アカウントに加えたパスワードの変更は、そのユーザ アカウントを使用できるその他のネットワークに適用されます。

Meraki AP は、Meraki-Hosted 認証サーバを使用するために、Meraki クラウドにアクセス可能である必要があります。Meraki クラウドが一時的に利用不可になると、すでに認証されているワイヤレス クライアントは接続されたままになりますが、新たにワイヤレス ネットワークにアクセスするワイヤレス クライアントの認証は行えなくなります。管理者は、Meraki クラウドが使用できない場合に新しいワイヤレス クライアントがネットワーク アクセスを取得できるかどうかを、[Configure（設定）] タブの [Access Control（アクセス制御）] ページにある [Disconnection behavior（切断時の動作）] セクションで設定できます。

Meraki

メッシュ ネットワーキング

ワイヤレス メッシュ ネットワークでは、（有線イーサネットへの接続の有無にかかわらず）複数の AP がワイヤレス インターフェイス経由で通信し、1 つのネットワークを形成します。各 AP が隣接デバイスのリストを作成し、ネットワーク内の他の AP と情報を交換してそのネットワーク全体でのルートを形成します。Meraki AP が有線イーサネットに接続し、（スタティック IP の設定または DHCP のいずれかによって）IP アドレスを取得すると、AP は「メッシュ ゲートウェイ」のアイデンティティを取得します。AP が有線イーサネットに接続されていないか、その接続から IP アドレスを取得しない場合、AP は「メッシュ リピータ」として動作します。メッシュ リピータは、メッシュ ネットワークを通過するワイヤレス トラフィックをゲートウェイまたは他のリピータに渡します。

メッシュ ネットワーク構成内の Meraki デバイスは、Meraki が設計した独自のルーティング プロトコルを使用して通信します。このプロトコルはワイヤレス メッシュ ネットワーキングに特化した設計になっており、ワイヤレス ネットワーク固有のいくつかの特徴はこのプロトコルによるものです。これらの特徴には、ノイズやマルチパス干渉が原因のリンク品質のばらつきや、複数のホップを通過するルーティング トラフィックがパフォーマンスに与える影響などがあります。また、このプロトコルは、チャネルのオーバーヘッドを低く抑えながら、配置が容易で、短時間でのコンバージェンスを実現できるような設計になっています。

ネットワーク内のメッシュ リピータが、切断や環境における変化が原因で利用不可になる場合があります。Meraki メッシュ ネットワーク内の各 AP は、そのルーティング テーブルを定期的に更新し、ネットワーク ゲートウェイへの最適パスを取得します。ノード障害やルート メトリックが原因で最適パスが変更されると、トラフィックは既知の最適パスを通るようになります。

メッシュ ゲートウェイの障害やより適したルーティング メトリックを持つ新しいメッシュ ゲートウェイが現れると、すべての新しいトラフィック フローがその新しいメッシュ ゲートウェイに転送されます。特定のメッシュ ゲートウェイが他とは異なる IP サブネット上に存在する可能性があるため、TCP フローをそれぞれ特定のメッシュ ゲートウェイにマップすることにより、確立済みの接続が切断されないようにします。ネットワークを通過して特定のメッシュ ゲートウェイに至るルートは、ネットワークの状況に適応するために時間の経過に伴い変わることがあります。

アクセス ポイントのモニタリング

[Access Points（アクセス ポイント）] ページでは、ネットワーク上の AP を識別し、そのステータス、アクティビティ、および使用状況を表示します。最上位のページには、ネットワーク内の AP のリストが示されます。[Access Points（アクセス ポイント）] ページには次の機能があります。

- 列のヘッダーをクリックして並べ替えできます。
- [Display Options（表示オプション）] をクリックして、リスト内の列を追加、削除、または順序変更できます。
- AP 名、シリアル番号、または MAC アドレスで検索します。

[Access Points Detail（アクセス ポイント詳細）] ページ

管理者はリスト内の AP をクリックして、各 AP の詳細情報を表示するページを開くことができます。表示される情報は次のとおりです。

- 識別情報（MAC アドレス、シリアル番号、ステータスなど）。
- パフォーマンス データ（接続、スループット、遅延、メッシュ ネイバーなど）。さまざまな期間にわたるズームおよびパン機能付き。
- リモートでのトラブルシューティング用のライブ ツール。

ping テスト、スループット テスト、ライブ干渉グラフ、および現行クライアント リストなど、ワイヤレスの問題をリモートでトラブルシューティングおよびデバッグするために使用できるさまざまなリアルタイム ツールがあります。

ライブ干渉スキャンでは、その時点で関連付けられているクライアントが切断されます。

AP タギング

何百または何千もの AP が存在する大規模ネットワークで、AP をより簡単に検索、並べ替え、およびフィルタするための便利な方法として、AP タギングを使用することができます。アクセス ポイントに英数字のタグを割り当てて、場所別（たとえば、Building_1、Floor_4、West_Campus）またはその他の基準別に AP のグループを作成できます。[Access Points（アクセス ポイント）] ページでタグによる検索を行い、AP の特定のグループをすばやく簡単にフィルタできます。

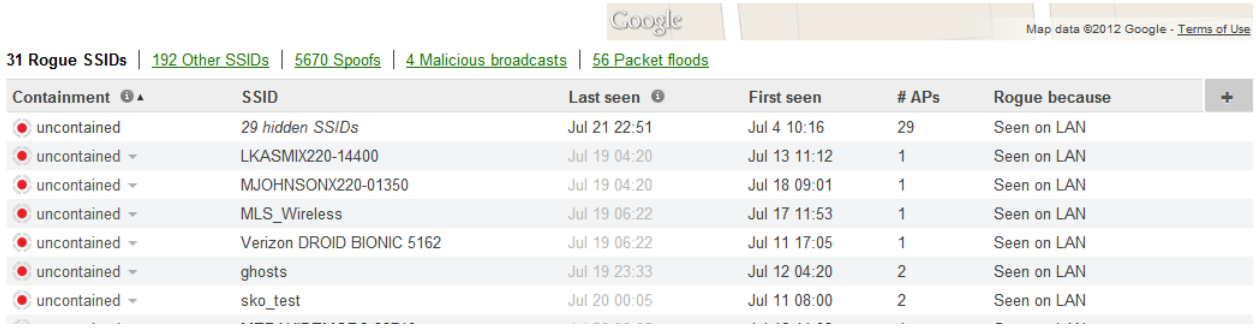
[AP details（AP 詳細）] ページで個別の AP にタグ付けすることも、[AP] ページで [Action（アクション）] > [Add Tags（タグの追加）] を選択して複数の AP を選択してタグ付けすることもできます。

アクセス ポイント データのエクスポート

[Access Points（アクセス ポイント）] ページのリスト データは、さらに処理および分析するために XML 形式でエクスポートできます。管理者は [Download as XML（XML としてダウンロード）] リンクをクリックしてデータを取得できます。Microsoft Excel などのほとんどのスプレッドシート プログラムで、XML ファイルを開くことができます。

ワイヤレスの脅威のモニタリング

正常に機能する有用なワイヤレス ネットワークを維持するためには、ワイヤレスの脅威および干渉を視認できることが重要です。[Monitor（モニタ）] > [Air Marshal] に移動することによって、専用 Air Marshal AP により検出された脅威がリストされた表を確認できます。ビューは、ブロードキャスト MAC、チャネル、メーカー、VLAN、および SSID のタイプ（暗号化または 非暗号化）といった、不正 AP に関する情報が表示されるようにカスタマイズできます。



ワイヤレスの脅威は、（1）不正 SSID、（2）他の SSID、（3）AP スプーフィング、（4）悪意のあるブロードキャスト、（5）パケット フラッドの 5 つのセクションに分類されます。各基準のより詳しい定義は、「ワイヤレス攻撃の定義」セクションを参照してください。

Meraki

ワイヤレス ネットワークのモニタリング

Meraki の組み込みダッシュボード ツールの使用

Meraki ダッシュボードは、ワイヤレス ネットワークを管理するための直観的で使いやすいインターフェイスを備えています。アクセス ポイントおよびクライアントを Google マップおよびフロア プラン上で簡単に見つけることができ、リストはインライン テキストで検索 できます。クライアント リストで「iPad」を検索するだけで、すべての iPad のリストが表示されます。または、「user:richard」を検索すると、「richard」というユーザ ID がログインに使用したすべてのデバイスが表示されます。

レイヤ 7 アプリケーションの優れた可視性により、ネットワークの使用状況を簡単に確認できます。電子メール、WebEx、および Skype などのビジネス アプリケーションが、YouTube や Netflix などの娯楽アプリケーションによって流量制限されている 場合は、トラフィック シェーピング規則で娯楽関連トラフィックの流量を制限します。

SNMP を使用したモニタリング

SNMP を使用して、Solarwinds などのサードパーティ モニタリング システムによりネットワークで特定のパラメータをモニタすることもできます。Meraki では、Meraki クラウドの SNMP ポーリングおよび Meraki AP の直接 SNMP ポーリングの両方をサポートしています。この 2 つのポーリング方法の設定情報は次のとおりです。

(1)Meraki クラウドの SNMP ポーリング:[Organization(組織)] > [Settings(設定)] ページでイネーブルにできます。詳細な設定手順は、ここを参照してください。ポーリング可能なすべてのパラメータのリストは、ここを参照してください。最後に、使用可能なパラメータのリストを含む MIB ファイルはここで入手できます。

(2)Meraki AP の直接 SNMP ポーリング:[Configuration(設定)] > [Network-wide settings(ネットワーク全体の設定)] ページでイネーブルにできます。ポーリング可能な OID パラメータのリストを含む詳細な設定手順は、ここを参照してください。

MR モニタリング クライアント

[Clients（クライアント）] ページには、ネットワークの使用状況およびネットワークを使用しているクライアント デバイスが表示されます。

[Clients（クライアント）] ページには次のような特徴があります。

- ワイヤレス ネットワークによってアドバタイズされたすべての SSID で関連付けられているクライアント、または特定の SSID で関連付けられているクライアントのみを表示します。これは、画面上部の [SSID] ドロップダウン メニューを使用して選択できます。
- MAC、OS、デバイス タイプ、または NetBIOS/Bonjour 名でクライアントを検索します。
- ズーム コントロール。管理者はこれを使用して、指定の期間内に関連付けられたクライアントのみを表示できます。
- 管理者は、[blocked list（ブロック済みリスト）] をクリックして、MAC ブラックリストに記載されているクライアントのみを表示することもできます。
- [Access Points（アクセス ポイント）] ページと同様、[Clients（クライアント）] ページには、カスタマイズ（列の追加、削除、および順序変更）および並べ替え（列のヘッダーをクリック）が可能なリストがあります。
- [Description（説明）] 列には、（NetBIOS から）判別可能な場合はデバイス名が表示されます。判別できない場合は単にデバイスの MAC アドレスが表示されます。
- [Operating system（オペレーティング システム）] 列には、OS のフィンガープリント（特定のオペレーティング システムが DHCP 経由で IP アドレスを要求する際に使用する一意のパターン）から判別される、デバイスのオペレーティング システムが表示されます。
- 管理者がデバイス リスト内の行にカーソルを移動すると、使用量グラフに新しい折れ線グラフが表示されます。これは、総帯域幅のうち、強調表示されているデバイスが使用した割合を示します。

クライアント データのエクスポート

[Clients（クライアント）] ページのリスト データは、さらに処理および分析するために XML 形式でエクスポートできます。管理者は [Download as XML（XML としてダウンロード）] リンクをクリックしてデータを取得できます。Microsoft Excel などのほとんどのスプレッドシート プログラムで、XML ファイルを開くことができます。

NAT モード

NAT モードでは、Meraki AP は、NAT 後のプライベート IP アドレス プール 10.x.x.x からの IP アドレスをワイヤレス クライアントに割り当てる DHCP サーバとして実行されます。

次のいずれかに当てはまる場合は、NAT モードをイネーブルにする必要があります。

- SSID に関連付けられたワイヤレス クライアントにインターネット専用アクセスが必要である。
- ワイヤレス クライアントに IP アドレスを割り当てることができる DHCP サーバが LAN に存在しない。
- LAN に DHCP サーバが存在するが、ワイヤレス クライアントに割り当てる IP アドレスが不足している。
- 異なるサブネットから IP アドレスを割り当てる複数の DHCP サーバがネットワークに存在する。これは、異種バックホール接続がある場合に一般的です（ネットワーク内の一部の AP が T1 でインターネットに接続し、同じネットワーク内の他の AP がビジネスクラス DSL でインターネットに接続する場合など）。
- 成人向けコンテンツ フィルタリング機能をイネーブルにしたい場合。

NAT モードをイネーブルにした場合の影響は次のとおりです。

- ワイヤレス ネットワーク外のデバイスは、ワイヤレス クライアントへの接続を開始できない。
- ワイヤレス クライアントは、レイヤ 2 検出プロトコルを使用して有線ネットワークまたはワイヤレス ネットワーク上の他のデバイスを検出できない。
- レガシー VPN クライアント（つまり、NAT トラバーサル非対応のクライアント）は、ワイヤレス ネットワーク上で IPSec トンネルを確立できない場合がある（回避策の 1 つとして、VPN クライアントをアップグレードするか、SSL など、TCP 経由の IPSec トンネルを確立するように VPN クライアントを設定する方法があります）。
- VLAN タギング ワイヤレス トラフィックは NAT モードではサポートされない。

ネットワーク概要

すべてのネットワークの概要

すべてのネットワークの概要のページには、特定の組織のすべてのネットワークの概要が表示されます。このページを表示するには [Organization（組織）] > [Network map（ネットワーク マップ）] を選択します。上部にある使用量グラフにはすべてのネットワークでの使用量の累積が示され、マップにはネットワーク ロケーションがマーカー付きで示されます。マーカーの色は、使用量グラフの左側にあるネットワーク リストに示されたネットワークに対応しています。ユーザがリストのネットワーク上にカーソルを移動すると、マップ上のネットワーク マーカーと、使用量グラフでのその特定のネットワークの使用量が強調表示されます。マップ上の特定のネットワーク マーカーまたはリスト内のネットワーク名をクリックすると、その特定のネットワークの [Overview（概要）] ページにドリルダウンできます。

個々のネットワークの概要

[Overview（概要）] ページには、ネットワーク使用量およびネットワーク ステータスの概要が表示されます。管理者は、前日または先週ネットワークに関連付けられたユーザの数、それらのユーザがその期間内に転送したデータ量、および先週の使用帯域幅の変動を確認できます（ネットワーク使用量グラフ）。このページを表示するには、[Monitor（モニタ）] > [Overview（概要）] に移動するか、または [All Network Overview（すべてのネットワークの概要）] ページから特定のネットワークにドリルダウンします。

航空マップにはネットワーク内の AP に関する最新情報が表示されます。管理者は、右上隅にあるオプションを使用して、グラフィカル マップ、衛星画像、またはハイブリッド ビュー上に AP を表示できます。左上隅にある矢印コントロールを使用するとパンできます。パンニングは、マップをクリックしてドラッグすることによっても行えます。矢印コントロールの下にあるスケール コントロールを使用して、ズーム レベルを調整できます。ズーム レベルは、矢印コントロールの横にある虫眼鏡を使用するか、または拡大する特定の地域をダブルクリックして制御できます。

マップ上の色付きの点は AP を表しています。AP のステータスは色によって示されます。

- 緑色：AP は何の問題も報告していません。
- 黄色：AP は稼働中ですが、最近問題が発生しました。場合によっては、管理者が [Access Points（アクセス ポイント）] ページでこのアラートを消去できることがあります。
- 赤色：AP は現在ダウンしています。
- グレー：AP は 7 日以上ダウンしています。

管理者は AP をクリックして、その名前、メッシュ モード（メッシュ ゲートウェイまたはメッシュ リピータ）、過去 24 時間以内に関連付けられたユーザの数（AP 上の数字でも示されます）、および過去 24 時間以内に転送されたデータ量を確認できます。AP 間のグレーの線はメッシュ リンクを表します。メッシュ リピータにカーソルを移動すると、AP がメッシュ ゲートウェイ（および LAN）にアクセスする際にメッシュ ネットワーク内で通過するパスを示す線が強調表示されます。

マップの右上にある [Options（オプション）] ボックスで、ユーザは AP 上の数字で何を表すか（接続されているクライアント、ゲートウェイまでのメッシュ ホップ数など）、およびメッシュ リンクの表示設定を選択できます。

左上隅のネットワーク名の下にある [Current clients（現在のクライアント）] リンクをクリックすると、クライアントが現時点でネットワーク内の SSID とチャネル全体にどのように分散されているかを示す表が開きます。

左上隅のネットワーク名の真上にあるリンクをクリックするか、または画面上部にある [Network（ネットワーク）] ドロップダウン セレクタで [All-network Overview（すべてのネットワークの概要）] オプションを選択すると、[All Network Overview（すべてのネットワークの概要）] ページが表示されます。

[Maps（マップ）] ページ

管理者は、[Maps（マップ）] ページを使用してカスタム マップおよびフロア プランをアップロードし、ネットワークの可視性を高めることができます。たとえば、複数の画像をアップロードして、オフィス ビルの複数のフロアや組織のさまざまなブランチ オフィスでの AP の配置を可視化できます。

オープン認証

オープン モードでは、あらゆるデバイスがワイヤレス ネットワークに接続できます。オープン モードの主な利点はそのシンプルさにあります。あらゆるクライアントが、複雑な設定をしなくても簡単に接続できます。オープン モードが推奨されるのは、ネットワークの利用を必要とするゲストが存在する場合や、より一般的には、簡単に接続できることが最優先されるためアクセス制御を不要とする場合です。

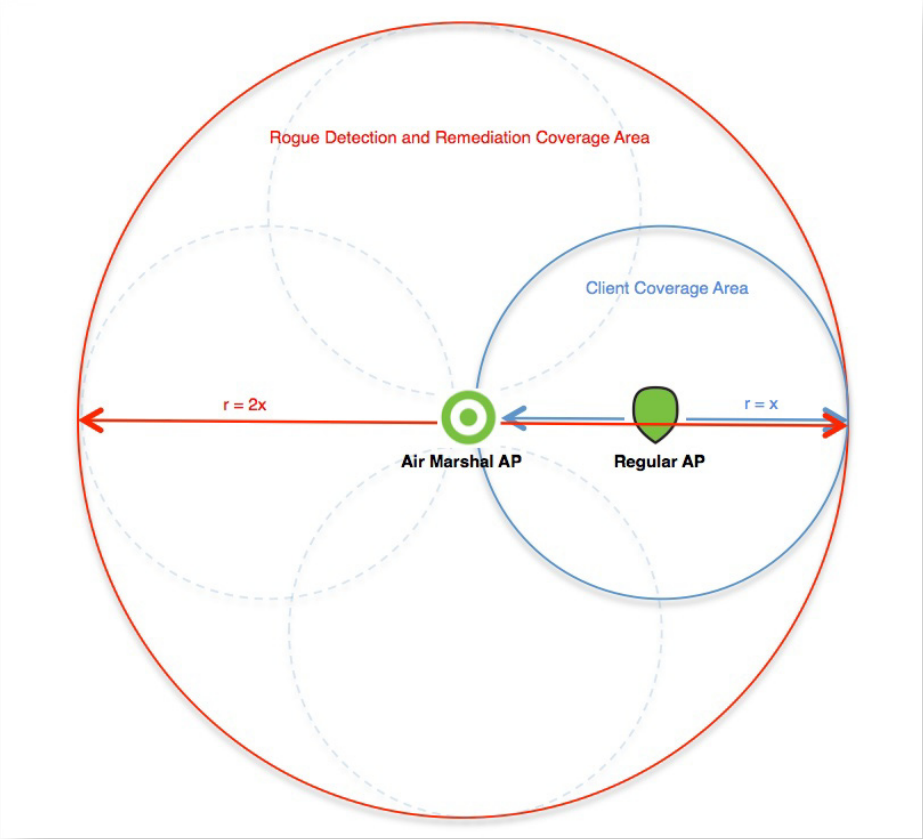
ほとんどの環境で、管理者は、オープン ネットワーク上で関連付けられたワイヤレス クライアントがファイル共有などの LAN リソースにアクセスできないようにする必要があります。管理者は VLAN タギングまたはファイアウォール規則を使用してアクセスを制御できます。

Meraki

Air Marshal AP の物理的な配置

WIPS スキャン用のフルタイム Air Marshal として使用する AP は、壁に取り付ける、PoE を使用するなど、クライアントにサービスを提供する通常の AP とまったく同じ方法で配置できます。

Air Marshal AP は、不正 AP を検出し、クライアント接続を維持するために必要なビットレートより低いビット レートにその不正 AP を封じ込めることができるため、その有効半径は通常の AP よりも広くなります。Air Marshal AP が不正アクセス ポイントを検知して修復するカバレッジ半径は、クライアントにサービスを提供するためのカバレッジ エリアの約 2 倍であるため、WIPS スキャンのための合計カバレッジ エリアは、クライアントにサービスを提供するためのエリアの約 4 倍になります。WIPS 全体のカバレッジを計画している場合、Air Marshal AP と、クライアントにサービスを提供する AP との比率は約 1 対 4 になりますが、配置のパラメータや必要な WIPS カバレッジ密度に応じて 1 対 3 ～ 1 対 5 になることがあります。



事前共有キー（WEP、WPA/WPA2-Personal）

事前共有キー（PSK）では、キーを持っていれば誰でもワイヤレス ネットワークを使用できます。

WEP は、RC4 暗号化を使用する、オリジナルの 802.11 標準の事前共有キー メカニズムです。WEP はハッキングに対して脆弱であり、十分なトラフィックを見ることができる傍受者は暗号キーを導き出すことができます。WEP は、たとえば、ネットワークに WPA/WPA2 非対応のレガシー クライアント デバイスが存在する場合など、より高度なセキュリティを利用できない場合にだけ使用してください。

WPA-Personal および WPA2-Personal（Wi-Fi Protected Access）では、WEP よりも高度な暗号化が使用されます（WPA-Personal では RC4 暗号化による TKIP が使用され、WPA2- Personal では AES 暗号化が使用されます）。WPA2-Personal が推奨されます。

PSK は、クライアント側でのいくつかの設定を必要としますが、比較的簡単に設定できます。ユーザが少数の場合や、クライアントが WPA2-Enterprise などの高度な認証メカニズムに対応していない場合には PSK が適しています。ただし、PSK に基づいた配置の場合はあまり拡張性がありません。PSK は、望ましくないユーザに共有されないように定期的に変更する必要がありますが、多数のユーザが存在する場合は PSK を変更することが難しくなります。

Meraki

Quality of Service

Meraki MR は、トラフィックの優先順位付けに関する Wireless Multimedia Extensions（WMM）標準に対応しています。WMM は IEEE 802.11e 仕様に基づく Wi-Fi アライアンス標準で、ワイヤレス VOIP フォンなどのデバイスが Meraki ワイヤレス ネットワークに接続したときに正しく動作するように、EDCA コンポーネントに重点を置いています。WMM には、音声、ビデオ、ベスト エフォート、およびバックグラウンドという 4 つの異なるトラフィック クラスがあります。WMM に対応し、より高いサービス レベルを要求するデバイス（Wi-Fi ハンドセットなど）には、Meraki ワイヤレス ネットワーク上でより高い優先順位が付けられます。

QoS により、選択したトラフィック タイプの遅延、ジッター、および損失が、妥当な範囲内に維持されます。ダウンストリーム トラフィック（AP からクライアント）に対して QoS を提供する場合は、アップストリーム トラフィック（クライアントから AP）がベスト エフォートとして処理されます。ネットワークにかかる負荷が軽い場合、QoS 機能の適用が顕著にはわからない可能性があります。メディアにかかる負荷が軽いのに遅延、ジッター、および損失が顕著な場合は、システム障害、ネットワーク設計の問題が生じているか、またはアプリケーションと、アプリケーションが実行されているネットワークとの間で遅延、ジッター、損失の要件が一致していないことを示しています。ネットワークの負荷が増えると、アプリケーションのパフォーマンスへの QoS 機能の適用が始まります。

Meraki

無線の設定

Meraki クラウドには、Meraki の統合された RF インテリジェンスである AutoRF 機能があります。AutoRF はローカルの RF 環境を定期的にスキャンし、システム ネットワーク全体での AP チャネル選択および送信電力を最適化することにより、ネットワークのパフォーマンスと信頼性を最大限に高めます。多くの設定は手動で行うこともできます。

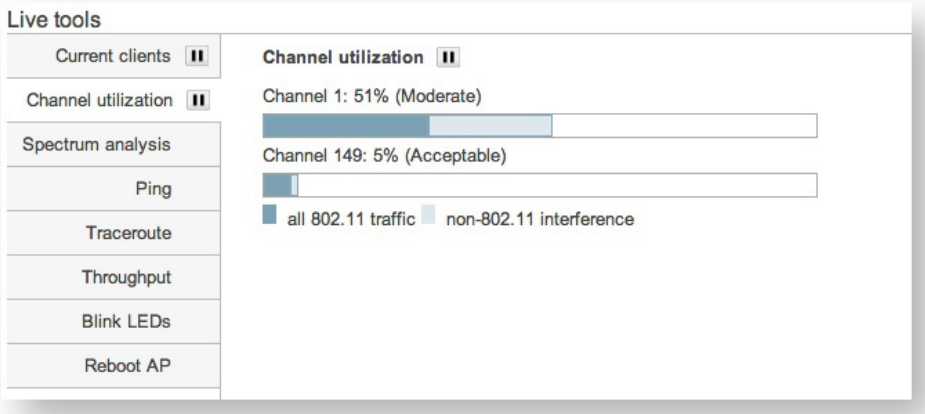
修復ポリシーの設定

ワイヤレス環境を健全に保つためには、Meraki Air Marshal によって検出された脅威に対して適切な措置を講じることが重要です。このような措置として、有線 LAN 上で、または指定したキーワードにより検出された脅威を自動的に封じ込めることができます。他の方法として、Air Marshal によって検出された不正およびその他の SSID を手動で封じ込めることもできます。不正およびその他の SSID への関連付けを試みるクライアントには、Air Marshal AP から認証解除メッセージが定期的に送信されます。

スペクトラム解析

Meraki AP にはスペクトラム解析機能が内蔵されています。AP は、RF 干渉の 802.11（他の AP）と非 802.11 の両方のソース をスキャンします（Bluetooth ヘッドセット、コードレス電話、電子レンジなど）。スキャンしたデータは、Meraki Auto RF 計画アルゴリズムに送られ、最適なチャネル計画（自動チャネル選択がイネーブルになっている場合）および送信電力設定が決定されます。自動チャネル選択はデフォルトでイネーブルになっており、[Configure（設定）] タブの [Radio settings（無線の設定）] ページで変更できます。 AP はクライアントへのサービス提供とネットワーク スキャンの両方を実行するため、別個のセンサー AP を配置する必要がありません。

[Access Point Details（アクセス ポイント詳細）] ページの [Live Tools（ライブ ツール）] セクションからチャネル使用率およびスペクトラム解析スキャンをリアルタイムで実行できるため、管理者は特定の AP エリアにおける干渉ソースに関する即時データと履歴データの両方を取得できます。[Live Tools（ライブ ツール）] の [channel utilization（チャネル使用率）] には、AP がブロードキャストしている 2.4 GHz チャネルと 5 GHz チャネルの干渉情報が表示されます。

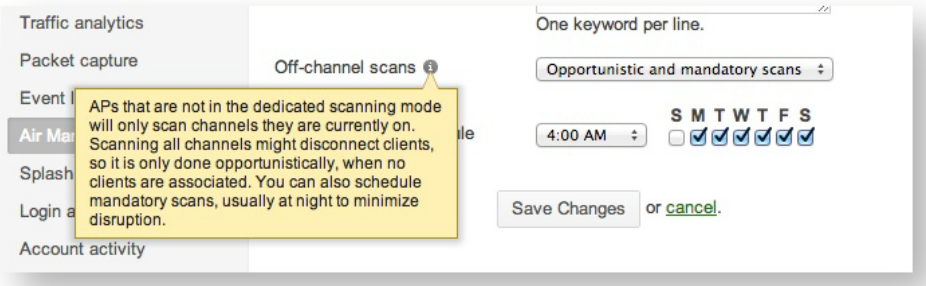


サポートされている AP では、スペクトラム解析スキャンを実行し、スペクトラム情報をダッシュボードに表示することもできます。

自動ネットワーク スキャン

Meraki AP は自動ネットワーク スキャンを実行し、RF 環境に関する情報（チャネル使用率、チャネル干渉など）を収集して、不正 AP を検出します。次の 2 種類のネットワーク スキャンがあります。

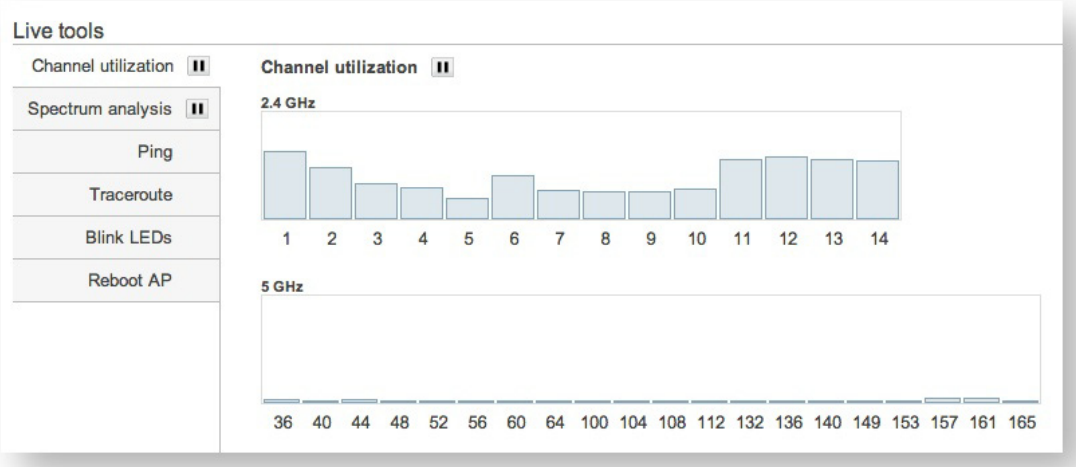
- 状況対応型スキャン：各 AP に関連付けられているクライアントがない場合に実行されます。
- 必須スキャン：ユーザ定義の時刻（特定の曜日）にネットワーク内のすべての AP によって実行されます。必須スキャンでは、Meraki AP に関連付けられている可能性のあるすべてのクライアントがスキャンの開始時に切断されることに注意してください。



ネットワークで状況対応型スキャンのみを実行するか、状況対応型スキャンと必須スキャンの両方を実行するかは、[Monitor（モニタ）] タブの [Air Marshal] ページで設定します。必須スキャンのスケジュールもこのセクションで設定します。

Air Marshal を使用したきめ細かい RF 分析

無線チャネル計画をよりきめ細かく制御したい場合は、Air Marshal で実行される AP を使用して、チャネル全体での干渉をリアルタイムでトラッキングできます。Air Marshal モードで実行される AP により、2.4 GHz 帯域と 5 GHz 帯域のすべてのチャネルでの干渉情報が、[Live tools（ライブ ツール）] セクションにリアルタイムで表示されます。



この情報を手動によるチャネル計画制御とともに使用すると、管理者は AP の RF 設定をきめ細かく制御できるようになります。

SSID のアベイラビリティ

[SSID Availability（SSID のアベイラビリティ）] ページで、管理者は時間とロケーションに基づいた SSID の可視性とアベイラビリティを管理できます。

SSID の可視性

管理者は SSID のアドバタイズメントを次のフレームでディスエーブルにすることによって、SSID を「非表示」にできます。

- AP が定期的にブロードキャストするビーコン フレーム。
- AP がワイヤレス クライアントからのプローブ要求フレームに応答して送信するプローブ応答フレーム。

手動で非表示 SSID が設定されたワイヤレス クライアントのみが非表示 SSID に接続できます。非表示 SSID への接続が設定されていないその他のクライアントは、非表示 SSID を利用可能なワイヤレス ネットワークとして検出できません。

この機能を使用して、ワイヤレス ユーザが特定の SSID に接続するのを防止できます。たとえば、学校で「VOIP」SSID を非表示にして、学生がこの SSID に接続する可能性を低くします。ただし、電話は SSID に接続するように設定できます。

SSID を非表示にするこの機能はセキュリティのための機能ではないことに注意する必要があります。基本的なワイヤレス スヌーピングや傍受の手法を使用すれば、非表示 SSID を検出できます。非表示 SSID を使用する際には、ワイヤレス暗号化および認証などの適切なワイヤレス セキュリティ方式の併用が必要です。

SSID を非表示にするオプションは、[Configure（設定）] タブの [Access Control（アクセス制御）] ページにあります。

AP 別の SSID ブロードキャスト コントロール

AP タギングを使用することで、管理者は特定の AP だけが SSID をブロードキャストできるように選択できます。

例として、オフィス ビルのロビーだけでブロードキャストされるゲスト SSID が挙げられます。ロビー エリア内に配置された AP には「Lobby」というタグが付けられます。タグ付けされた AP だけがゲスト SSID をブロードキャストするためには、[SSID availability（SSID のアベイラビリティ）] セクションで AP 選択ドロップダウン メニューを使用して、[This SSID is enabled on some APs...（この SSID を一部の AP でイネーブル...）] を選択します。

時間制限が設定された SSID ブロードキャスト

無料の公衆ワイヤレス アクセスを提供する小売店などの特定の導入タイプでは、管理者は一定の営業時間だけネットワーク アクセスを提供することがあります。時間制限が設定された SSID ブロードキャストの場合、SSID がブロードキャストされる時間をダッシュボードで設定でき、管理者が 1 日の終わりに SSID を手動でディスエーブルにする必要はありません。この機能は SSID を非表示にするのではなく、SSID を実際にディスエーブルにします。

SSID のブロードキャスト時間を設定するオプションは、[Configure（設定）] タブの [Access Control（アクセス制御）] ページにあります。

トラフィック シェーピング

管理者は、ユーザ別の制御をアプリケーションごとに適用するシェーピング ポリシーを作成できます。これにより、娯楽用アプリケーション（ピアツーピアのファイル共有プログラムなど）の流量制限と、企業アプリケーション（Salesforce.com など）の優先順位付けが可能になり、ビジネスクリティカルなアプリケーション パフォーマンスが損なわれないようにできます。

シェーピング規則の作成

トラフィック シェーピング ポリシーは、ポリシーに示されている順序で評価される、カスタム ファイアウォール規則に似た一連の規則で構成されています。各規則には、規則定義と規則アクションという 2 つの主要な構成要素があります。

- 規則定義

  規則は 2 つの方法で定義できます。管理者は、[Video & music（ビデオ/音楽）]、[Peer-to-Peer（ピアツーピア）]、[Email（電子メール）] などのさまざまな定義済みアプリケーション カテゴリから選択できます。規則定義の 2 つ目の方法では、カスタム規則定義を使用します。管理者は、HTTP ホスト名（salesforce.com など）、ポート番号（80 など）、IP 範囲（192.168.0.0/16 など）、または IP 範囲とポートの組み合わせ（192.168.0.0/16:80 など）を指定して規則を作成できます。

- 規則アクション

  指定した規則セットに一致するトラフィックに対してシェーピングまたは優先順位付けを行うか、この両方を行うことができます。 帯域幅制限を次のいずれかに指定できます。

  a. [Access Control（アクセス制御）] ページで特定の SSID に対して指定されているすべての制限を無視する（無制限の使用帯域幅を許可）
  b. 指定されている SSID 制限に従う
  c. SSID 制限よりも制約の多い制限を適用する アップロードとダウンロードに異なる上限値を指定するには、帯域幅スライダ コントロールの横にある [Details（詳細）] リンクをクリックします。

Quality of Service（QoS）の優先順位付けをレイヤ 2 と 3 のトラフィックに適用できます。レイヤ 2 の優先順位付けは、アクセス ポイントからの発信トラフィックの 802.1q ヘッダー内の PCP タグの値を指定することによって行います。この機能は、VLAN タギングがイネーブルになっている SSID にのみ使用可能です。レイヤ 3 のトラフィックに優先順位を付けるには、すべての着信 IP パケットと発信 IP パケットの IP ヘッダー内の DSCP タグの値を選択します。これは、トラフィックの WMM 優先順位にも影響します。この機能の利点を十分に活用するには、アップストリームの有線スイッチとルータも QoS 優先順位付け用に設定する必要があります。

ワイヤレス攻撃の定義

ワイヤレス攻撃は、特定のポリシー一致に基づいてヒューリスティックに定義された多数のさまざまな基準に従って分類されます。次にリストの定義を示します。

- 不正 SSID：LAN 上で確認されるか、キーワードに一致する SSID。
  - 有線 LAN 上の不正 AP：ユーザのネットワーク上のいずれかの AP と同じ有線 LAN 上にある不正 AP。これは、攻撃者が有線ネットワークに物理的にアクセスし、そのネットワークを使用してワイヤレス信号をブロードキャストしていることを示しています。
  - キーワードに一致する不正 AP：[Air Marshal] ページで指定したトークン キーワードを含むか、または正確に一致する SSID をブロードキャストしていることが確認された AP。その他の SSID：スキャン中に確認されたものの、脅威とは見なされない SSID。
- AP スプーフィング：ユーザの MAC アドレスおよび SSID をコピーしている AP。AP スプーフィングは、攻撃者が意図的にユーザのネットワークを偽装していることを意味し、最高レベルの重大度で扱う必要があります。
- 悪意のあるブロードキャスト：一定の許容可能なしきい値を超えてクライアントに継続的に送信されるサービス拒否（DoS）攻撃メッセージ。DoS 攻撃は、過剰な数のブロードキャスト再承認メッセージをクライアントに送信することによって、クライアントが AP に関連付けできないようにするものです。
- パケット フラッド：パケット フラッドは、AP に過剰な数のパケットを送信する、ワイヤレス クライアントまたは AP のフラッディングです。パケットは、ビーコン、認証、および関連付けの各フレームを含む複数のカテゴリに基づいてモニタおよび分類されます。いずれかのカテゴリの過剰な数のパケットが短時間に確認されるとパケット フラッドが引き起こされます。

Meraki

ワイヤレスの暗号化および認証

MR は、単純なオープン アクセスから WPA2-Enterprise 802.1x 認証まで、多様な暗号化方式および認証方式をサポートしています。暗号化および認証は、[Configure（設定）] タブの [Access Control（アクセス制御）] ページにある [MCC] で設定します。一般的に、暗号化方式は [Association requirements（関連付け要件）] で設定し、認証方式は [Network sign-on method（ネットワーク サインオン方式）] で設定します。

クライアントがワイヤレス ネットワークに関連付けられるには、正しい暗号キーが必要です（関連付け要件）。関連付けられた後、ワイヤレス クライアントはワイヤレス ネットワーク上のリソースにアクセスする前に情報の入力が必要になる場合があります（ネットワーク サインオン方式）。

サポートされている暗号化方式と認証方式の組み合わせは次のとおりです。

	Network sign-on method			
Association requirements	Direct access	Click-through splash page	Sign-on splash page	Billing (paid access)
Open (no encryption)	✓	✓	✓	✓
MAC-based access control (no encryption)	✓	✓		
WEP (shared network key)	✓	✓	✓	
WPA2-PSK (shared network key)	✓	✓	✓	
WPA2-Enterprise with 802.1x authentication	✓	✓		

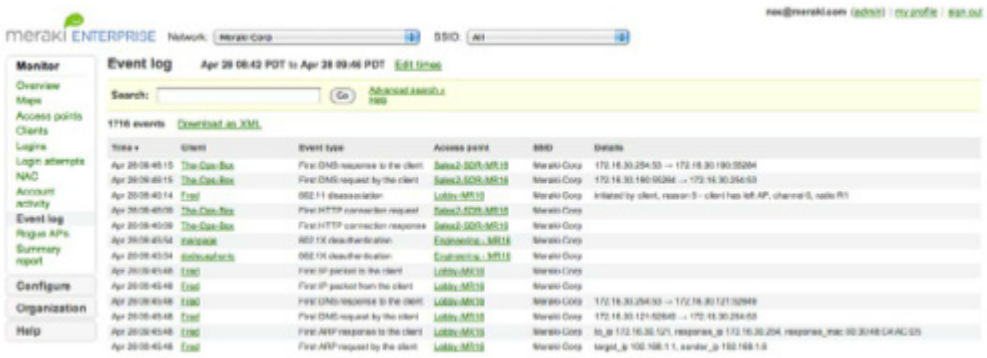
Meraki

ワイヤレス イベント ログ

[Event Log（イベント ログ）] ページには、次のようなさまざまなクライアント アクティビティに関する詳細なログが表示されます。

- 関連付け/関連付け解除
- 認証の試行とその結果
- DHCP アクティビティ
- 初期トラフィック
- デバイス パケット フラッド

管理者は、これらのログを使用して、ワイヤレス ネットワーク上で問題が発生している可能性があるクライアントのトラブルシューティングを行うことができます。



[Event Log（イベント ログ）] ページでは、管理者はイベント ログがレポートされる時間間隔を調整できます。また、[Event Log（イベント ログ）] ページには検索ツールが用意されています。これにより管理者は、指定した AP または指定したクライアントのイベント ログを表示できます。これらのフィルタは両方とも、検索ツールを使用しても、[Access Points（アクセス ポイント）] ページや [Clients（クライアント）] ページからイベント ログ リンクにアクセスすることによっても適用することができます。

ワイヤレス PCI レポート

管理者は、[Monitor（モニタ）] タブの [PCI Report（PCI レポート）] ページを使用して、PCI DSS v2.0 WLAN 要件に照らしてネットワーク設定をチェックできます。結果には、各 WLAN PCI 要件についての合格または不合格と、その理由の詳細が示されます。不合格の場合は、準拠のために変更が必要なネットワーク設定に関するガイダンスが提供されます。レポートは印刷してファイルしたり、セキュリティ監査員に提出したりできます。

ワイヤレス サマリー レポート

ネットワーク管理者は、[Monitor（モニタ）] タブの [Summary Report（サマリー レポート）] ページで各種のネットワーク分析情報を取得できます。このレポートでは、ネットワークの開始からの Meraki ワイヤレス ネットワークの使用状況と稼働時間に関する情報が提供され、次の統計情報の一部が含まれます。

- データ消費およびクライアント ログイン数上位 10 台の AP
- データ消費上位 10 台のクライアント
- SSID および AP モデル別の使用量内訳
- クライアント ログイン数およびデータ消費で上位のクライアント デバイスのメーカーおよび OS タイプ

ある特定の期間の統計情報を示すようにレポートをカスタマイズおよび表示して、特定の日、週、または月の統計分析情報を得ることができます。

レポートは、定期的に確認できるように、設定可能なスケジュールに従って電子メールで送信できます。サマリー レポートを複数のユーザに送信する場合、管理者は、[Schedule monthly e-mails（月次電子メールのスケジュール）] タブで 1 つ以上の電子メール アドレスを設定できます。レポートに組織のロゴを追加することもできます。

Meraki

WPA2-Enterprise 802.1x 認証

802.1X は、有線ネットワークまたはワイヤレス ネットワークへの関連付けを試みるユーザを暗号化および認証するための IEEE 標準フレームワークです。WPA-Enterprise では RC4 暗号化による TKIP が使用されますが、WPA2-Enterprise では AES 暗号化が追加されます。

802.1X はワイヤレス ユーザに対して透過的にできます。たとえば、ユーザがマシンへのログインで入力するクレデンシャルと同じものが、ワイヤレス認証のために認証サーバに自動的に渡されるように Windows マシンでシングル サインオンを設定できます。ユーザがクレデンシャルの再入力を求められることはありません。

802.1X では、拡張認証プロトコル（EAP）を使用して、認証の交換に関連する参加者間にセキュアなトンネルが確立されます。MR では、ネットワークで Meraki-Hosted 認証サーバが使用されているか、顧客がホストする認証サーバが使用されているかに応じて、複数の EAP タイプをサポートしています。次の表に、MR によってサポートされる EAP タイプを示します。

EAP Mode	Customer RADIUS	Meraki RADIUS
PEAPv0/EAP-MSCHAPv2	✓	✓
EAP-TTLS/MSCHAPv2	✓	✓
EAP-TLS	✓	
PEAPv1/EAP-GTC	✓	

WPA2-Enterprise 802.1X 認証は、一般的には顧客構内 RADIUS サーバとともに使用されます。RADIUS サーバは、Meraki AP の IP アドレスからの認証要求を許可するように設定する必要があります。

802.1X は、通常、マシンでユーザのクレデンシャルが入力されたときに 1 回だけ実行されます。