Mist 検証手引き

PoC テストシナリオ Day2

- 運用 -

ジュニパーネットワークス株式会社

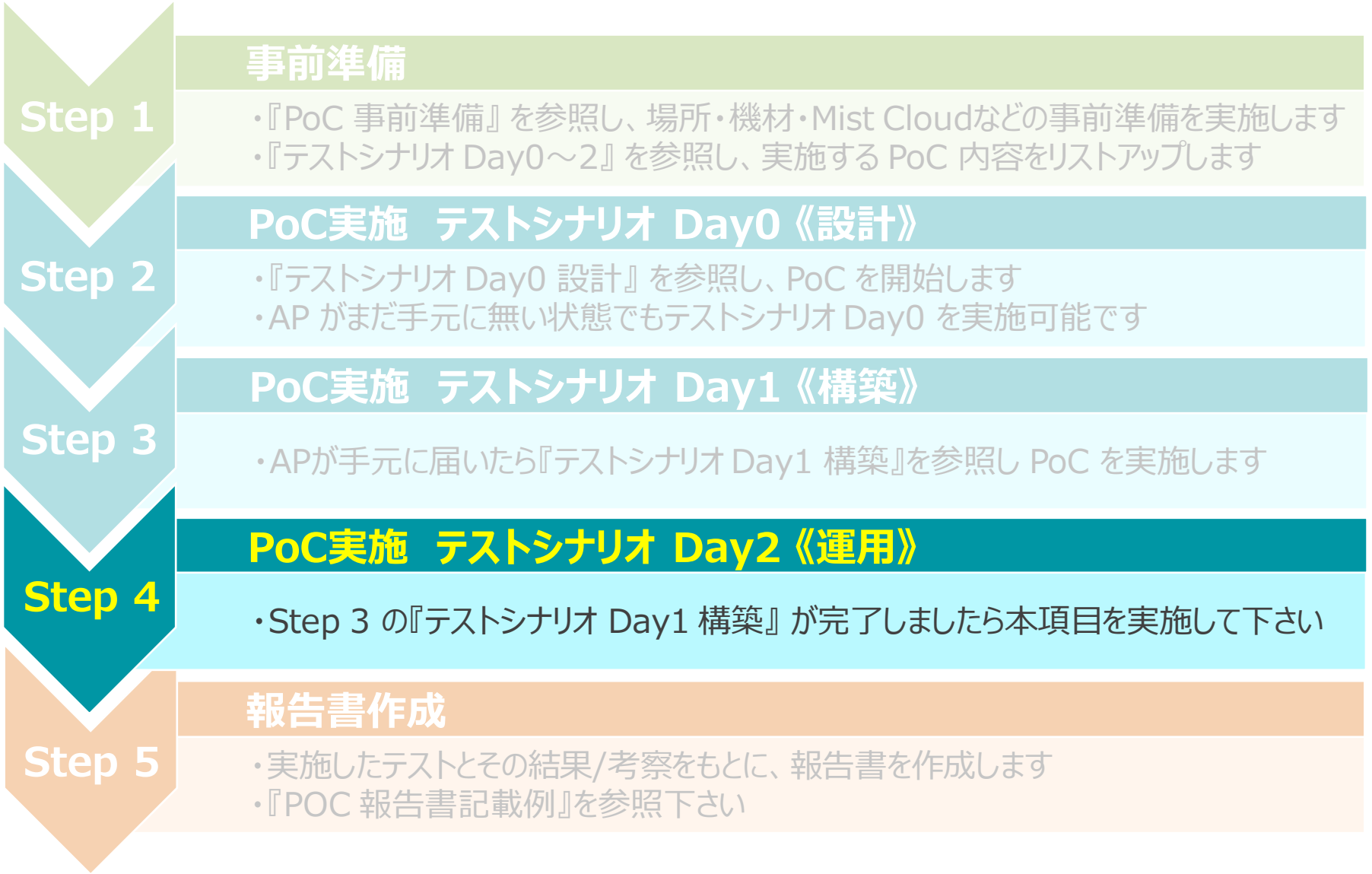
2022年11月 Ver 1.1

JUNIPer driven by Mist AI

はじめに

- 本資料は、 PoC（検証）における Mist 独自の機能を利用した『運用』について記載しています
- PoC を実施する際の設定内容やパラメータは導入する環境や構成によって異なります
  本資料では一例として PoC の準備、実施、報告までのシナリオを記載しております
- 設定内容の詳細は「ソリューション＆テクニカル情報サイト」の Mist 日本語マニュアルをご確認下さい
  https://www.juniper.net/jp/ja/local/solution-technical-information/mist.html

準備から報告書作成までの全体の流れ



テストシナリオ Day2《運用》

APとクライアントの可視化

ユーティリティ（テストツール）

ヒートマップ

SLE・RCA
認証失敗時のトラブルシューティング

RRM
電波干渉時の自動電波調整

Marvis

Marvis Action

ダイナミックパケットキャプチャ

アラート設定/Eメール通知

ネイバーAPと不正APの検出

レポート作成機能

AP ファームウェアの
マニュアルアップグレード

APの設置場所確認

AP 交換時の手順

APとクライアントの可視化

❖ Mist によるワイヤレスネットワークの可視化を確認します。

目的

AP やクライアントがどのように可視化されているのか確認します

手順

AP とクライアントの一覧表示や Insights 画面を確認します

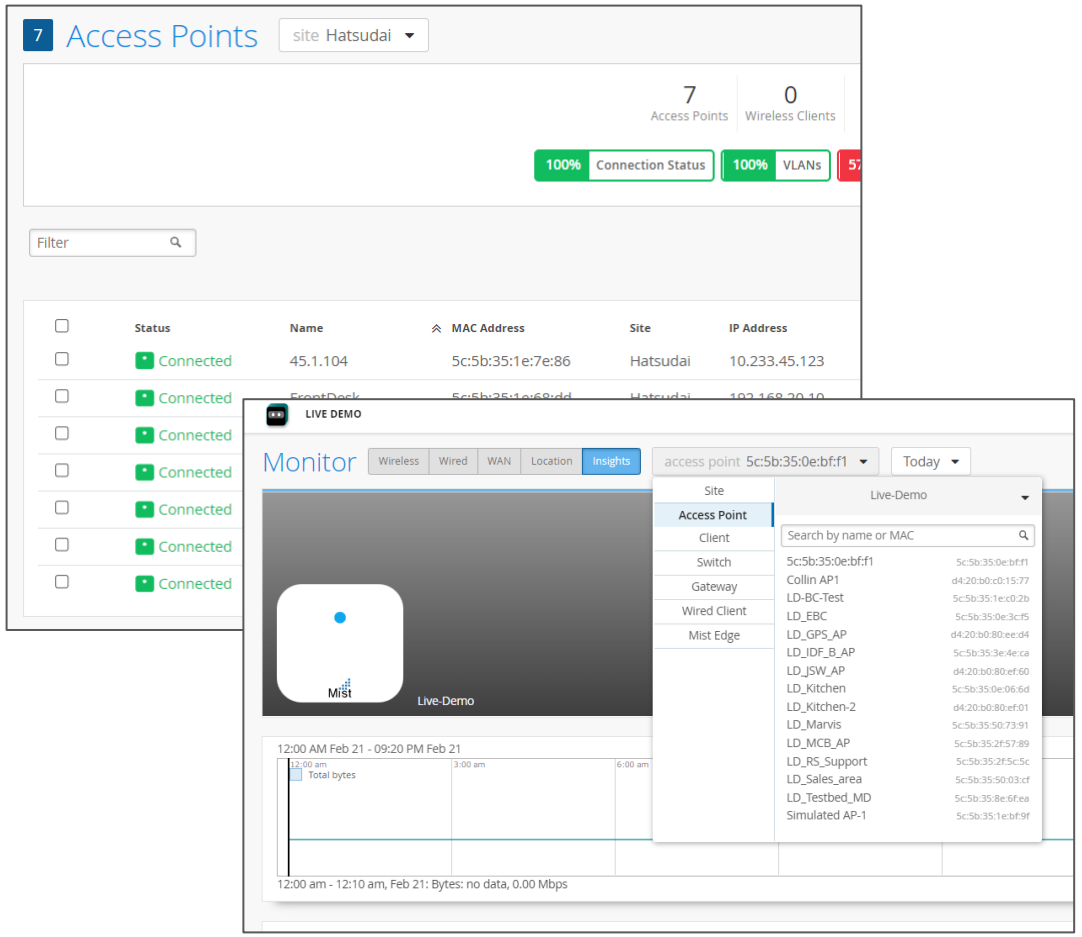
参考マニュアル

アクセスポイント 各種情報確認手順

アクセスポイント ログ確認手順

アクセスポイント アプリケーション通信 確認手順

アクセスポイント 接続クライアント 確認手順

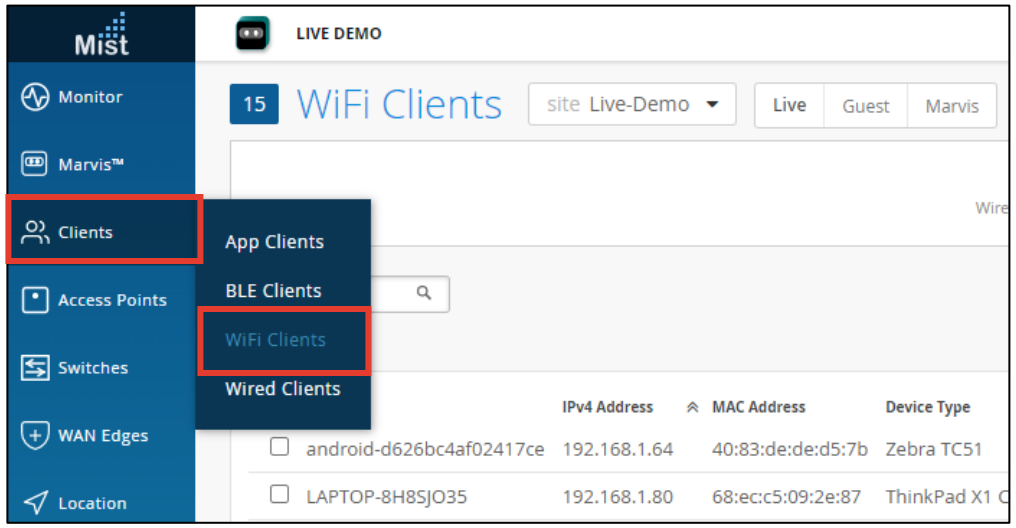


APやクライアントが可視化されることで、運用管理やトラブル対応が効率化されます

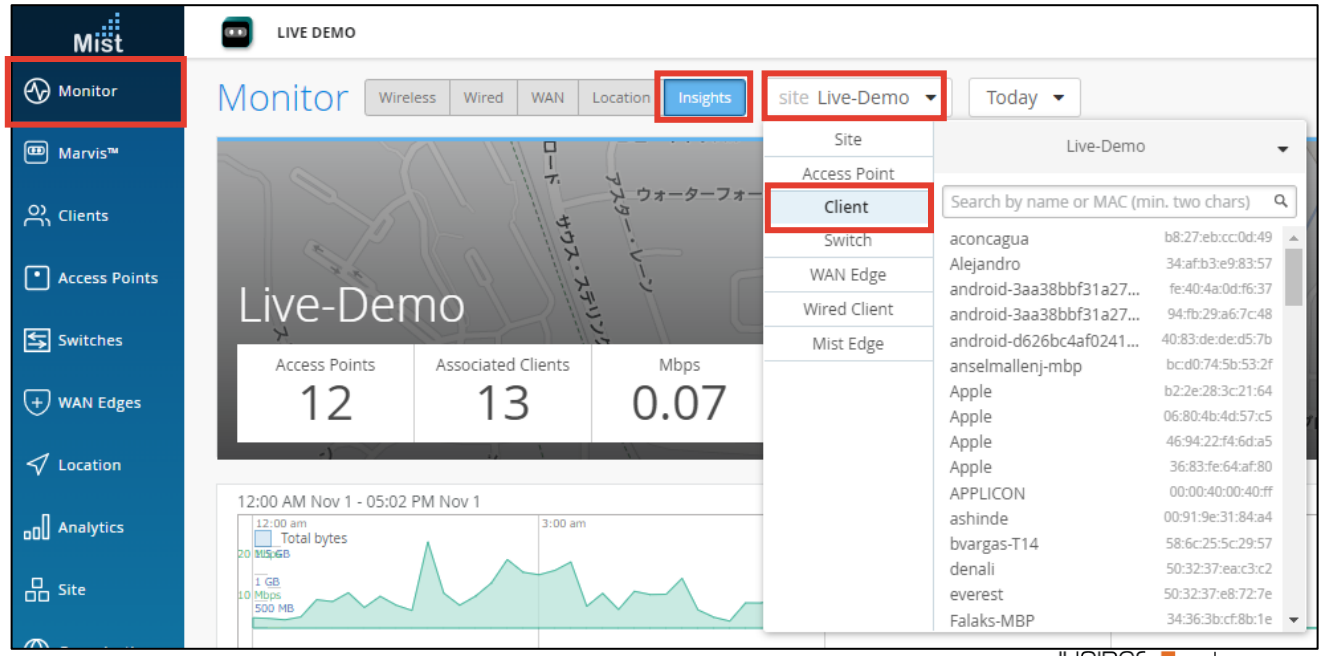
APとクライアントの可視化

AP と同様に、無線クライアントも可視化されます

1. [Clients] から [WiFi Clients] を選択し、
   接続しているクライアントの一覧を確認します



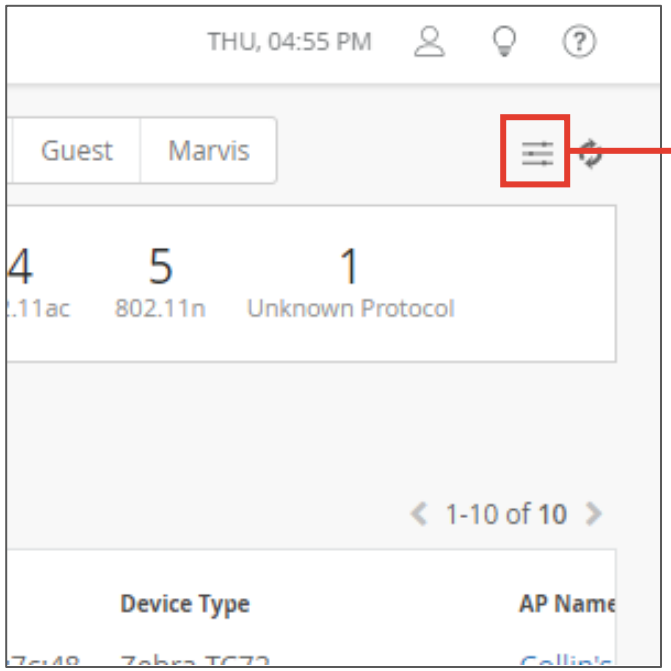
2. [Monitor] から [Insights] を選択し、
   [Client] の項目から、対象のクライアントの選択します
   ログや使用したアプリケーション等の詳細を確認します

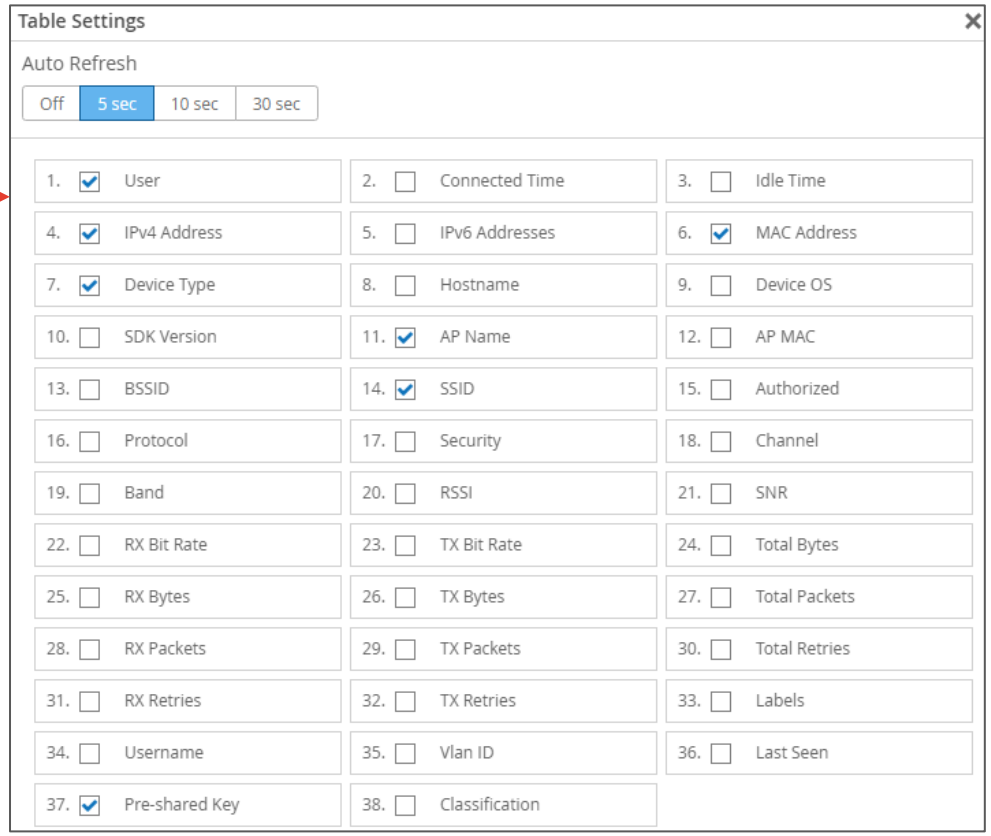


APとクライアントの可視化

AP と無線クライアントの可視化

- AP や無線クライアントの一覧表示では、一覧で表示する内容をカスタマイズ出来ます
  これにより、素早く確認したい情報を、簡単にピックアップする事ができます





ユーティリティ（テストツール）

❖ ユーティリティ（テストツール）を使用し疎通確認を行います。

目的

Utility の [Testing Tools] を使用し、AP からクライアント、
AP からインターネット等のへの疎通確認を実施します

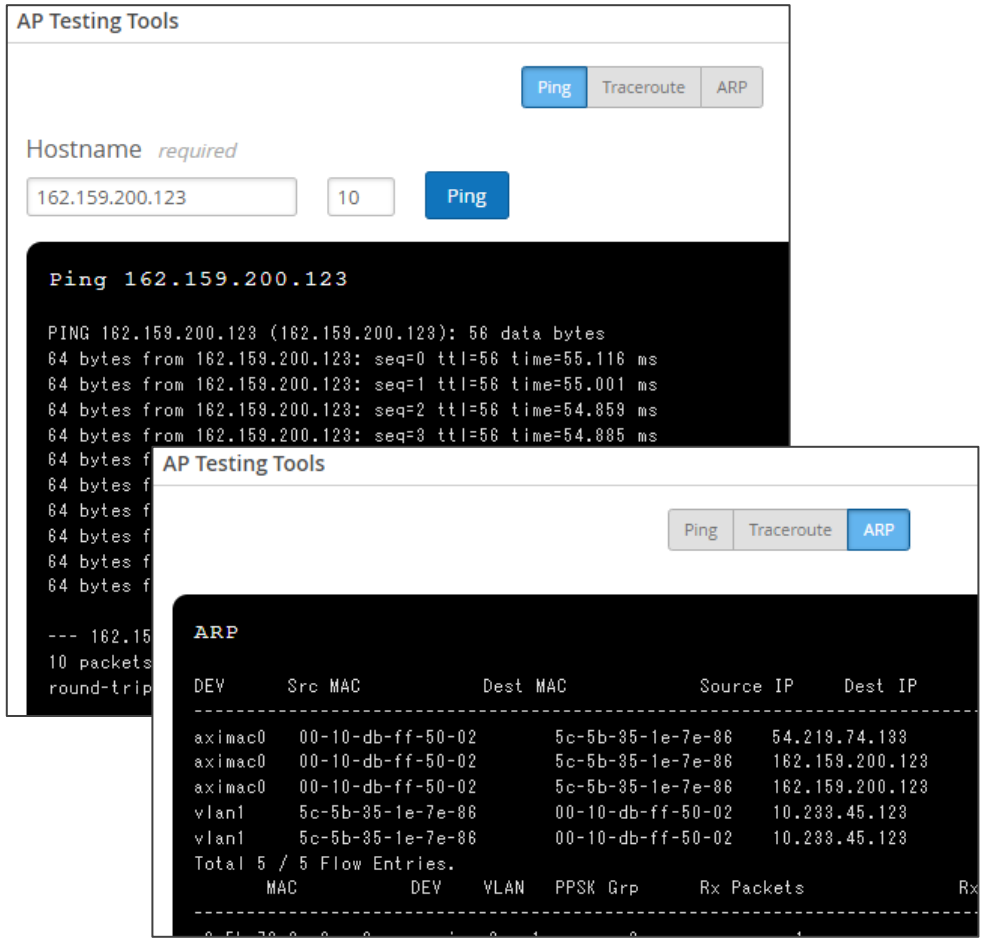
手順

以下のマニュアルを参考に、Testing Tools を使用した試験を行います

アクセスポイント Ping実施手順

アクセスポイント Traceroute実施手順

アクセスポイント ARP 確認手順



ping や traceroute など、GUI上で L3 レベルの疎通確認を簡単に実施できます

ヒートマップ

❖ ヒートマップを確認します。

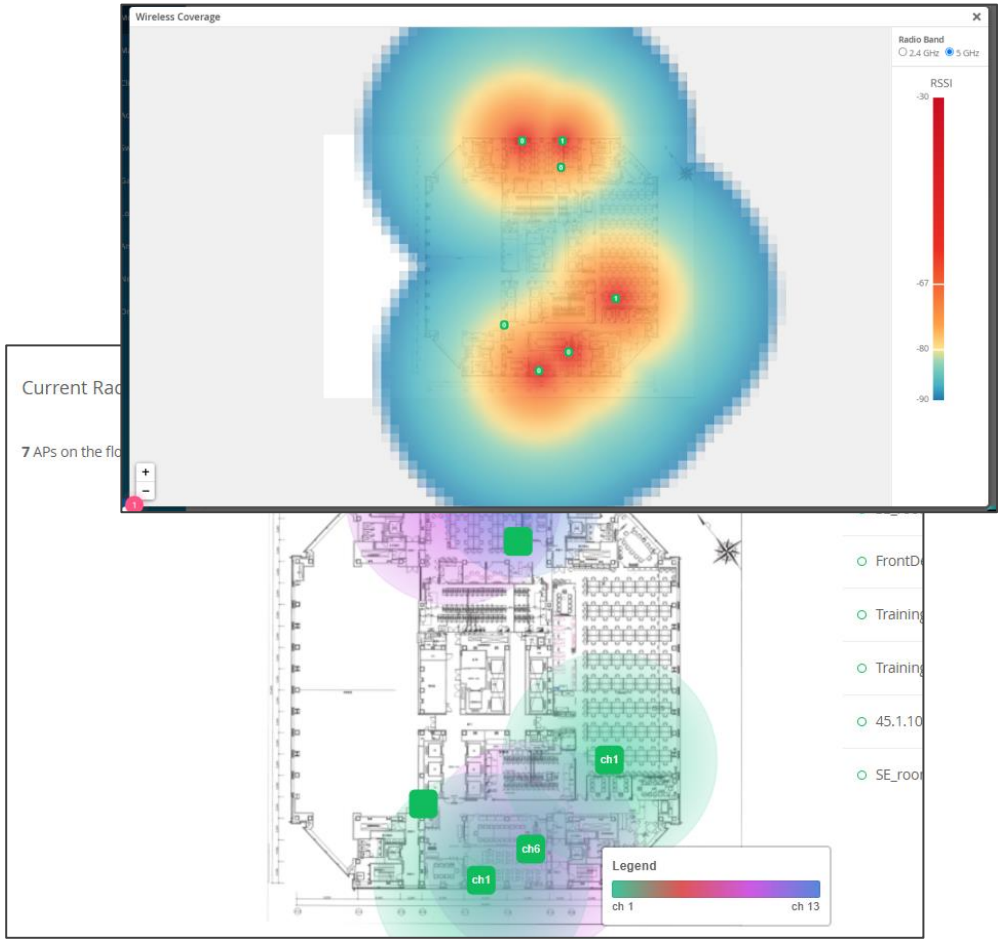
目的

電波の強度、カバレッジ、使用チャネルなどの情報は
ヒートマップにり視覚的に一目で確認することができます

手順

マニュアルを参照し、ヒートマップを確認します

[ヒートマップ 確認手順]



クライアントの電波受信強度では、訪問者が使用するゲストクライアントをリアルタイムに表示し、
訪問者が不満なく通信が行えているのか確認することができます

SLE・Root Cause Analysis

❖ SLE および Root Cause Analysis によってネットワークの品質が可視化されます。

目的

SLE および Root Cause Analysis によって、

どのように無線ネットワークの品質が可視化されるのかを確認します

検証手順

① 正常状態の確認

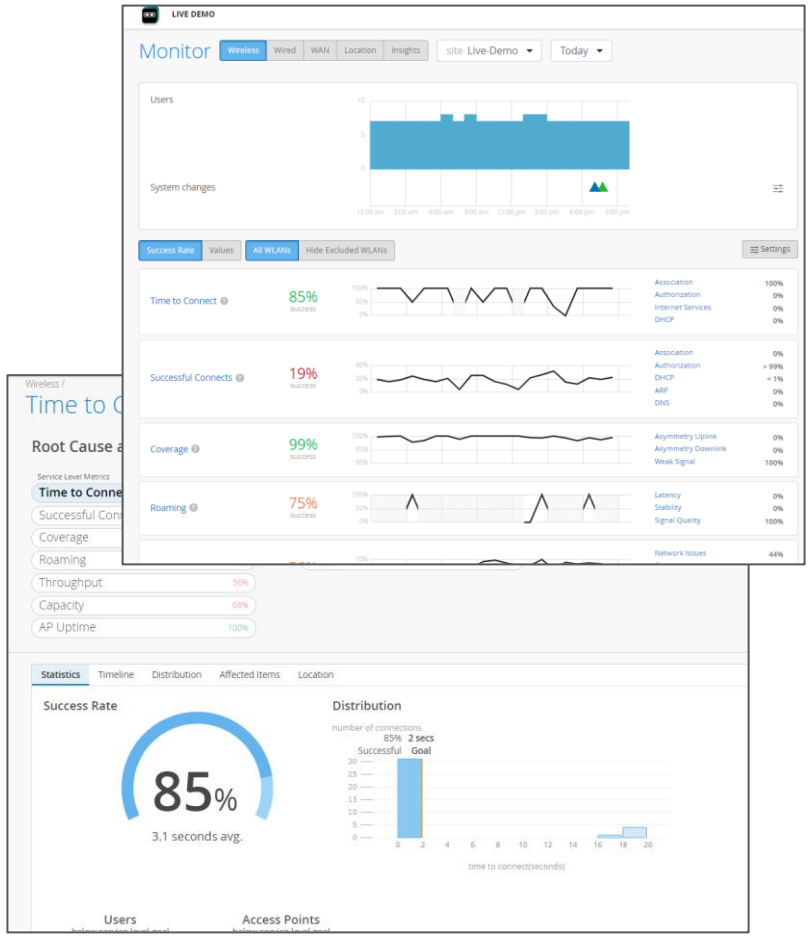
参考マニュアル

Mist Wi-Fi Assurance SLE (Service Levels Expectation)

② トラブルシューティング

PSK 認証または 802.1x 認証失敗時のSLE表示を確認します

Radius サーバを利用している環境のみ802.1x認証が可能です



SLE により、視覚的にも分かりやすく、どこで・どのような問題が発生しているのか確認することができます
また、Root Cause Analysis によりさらにその問題の詳細が確認可能です

PSK 認証失敗時のトラブルシューティング

❖ 疑似トラブルを発生させ、PSK 認証失敗時の SLE を確認します

- 検証方法：

  ネットワーク接続時に、わざとパスワードを間違えネットワーク接続を失敗させます

  以下のマニュアル参照し、認証失敗時の SLE を確認します

  ※環境によって SLE への結果の反映は時間がかかることがあります

  認証エラー 確認手順（拠点単位）

  認証エラー 確認手順（クライアント単位）

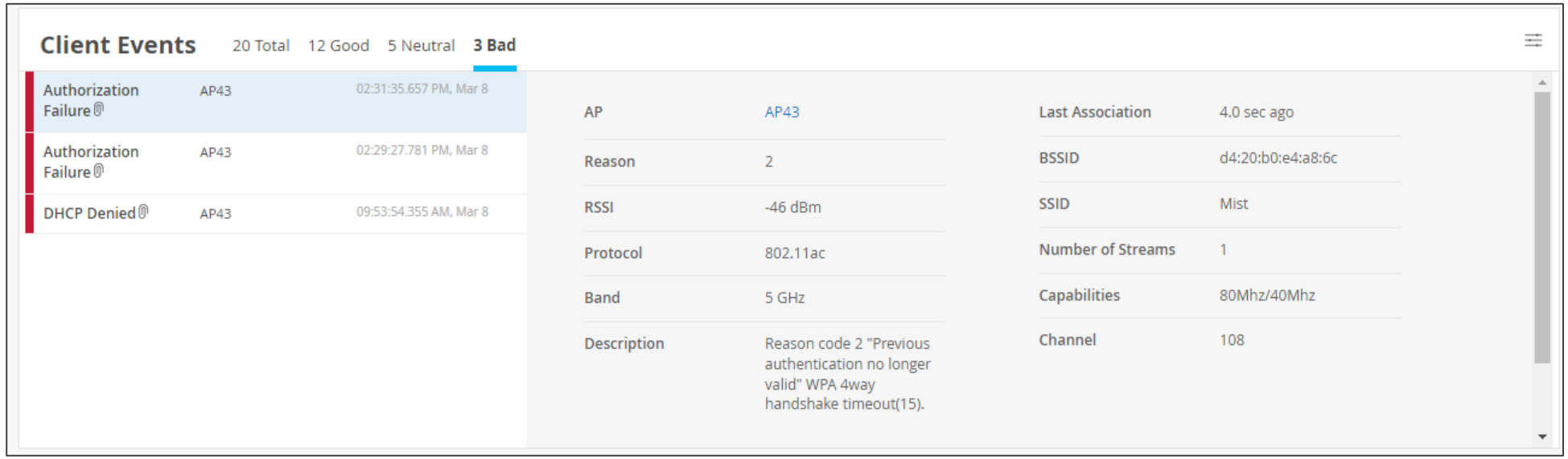
PSK 認証失敗時のトラブルシューティング

❖ 疑似トラブルを発生させ、PSK 認証失敗時の SLE を確認します

- 結果：

  Client Events にて以下のログが出力されます

  Event title： Authorization Failure



802.1x 認証失敗時のトラブルシューティング（Radius サーバ利用）

❖ 疑似トラブルを発生させ、802.1x 認証失敗時の SLE を確認します

- 検証方法：

  ネットワーク接続時に、わざとパスワードを間違えネットワーク接続を失敗させます

  以下のマニュアル参照し、認証失敗時の SLE を確認します

  ※環境によって SLE への結果の反映は時間がかかることがあります

  認証エラー 確認手順（拠点単位）

  認証エラー 確認手順（クライアント単位）

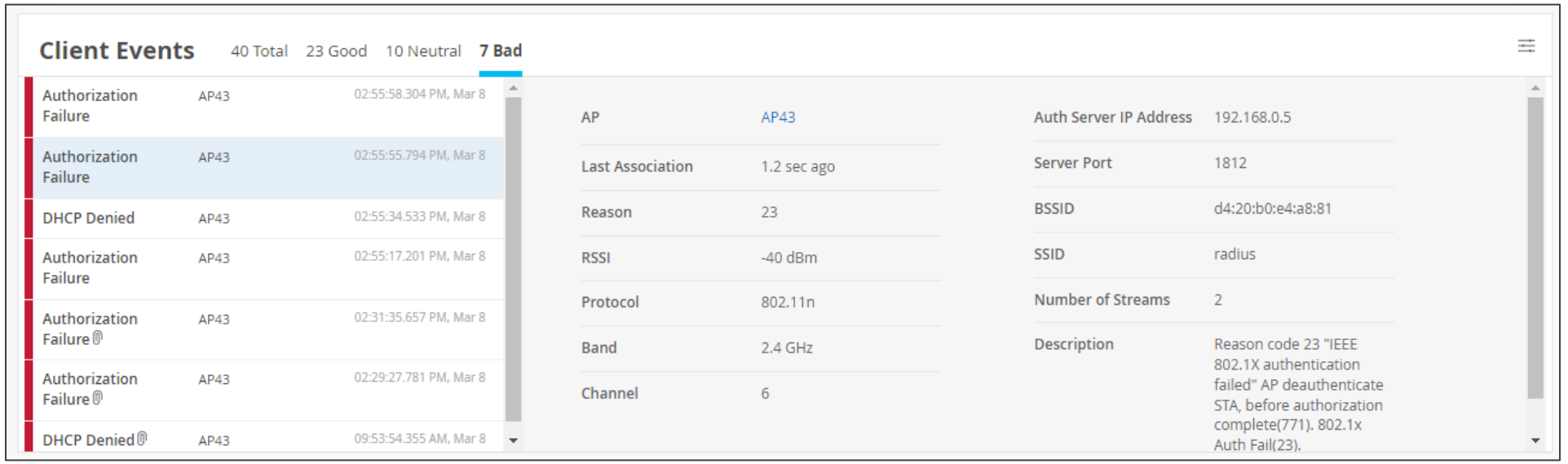
802.1x 認証失敗時のトラブルシューティング（Radius サーバ利用）

❖ 疑似トラブルを発生させ、802.1x 認証失敗時の SLE を確認します

- 結果：

  Client Events にて以下のログが出力されます

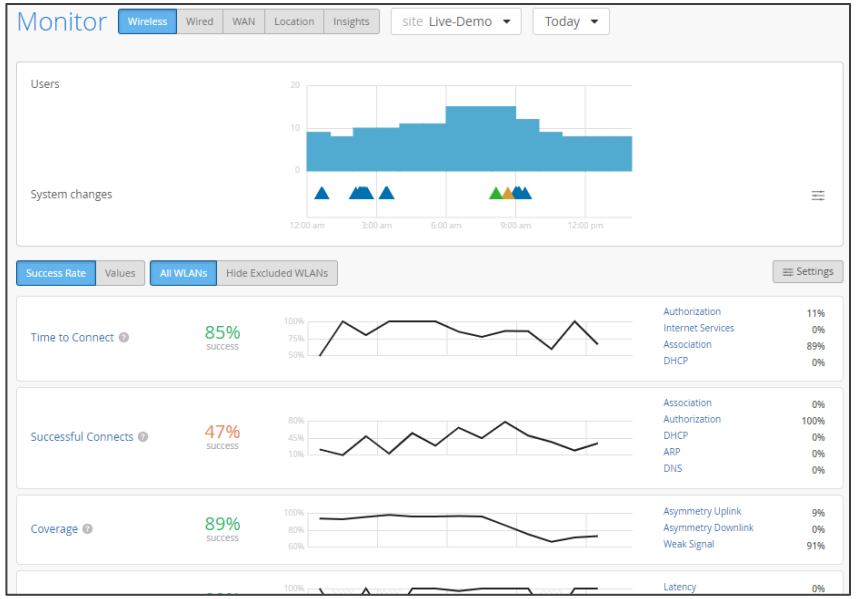
  Event title： Authorization Failure

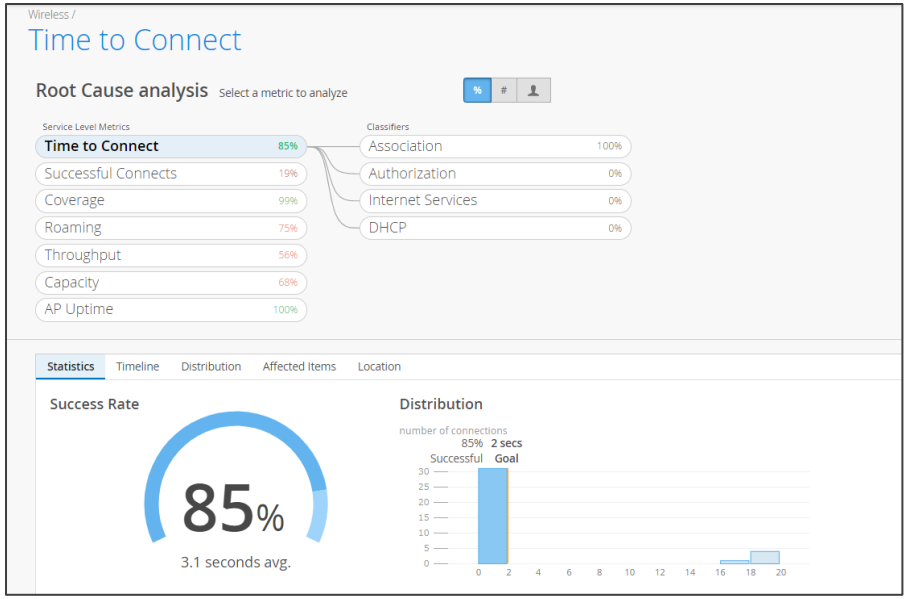


SLE・Root Cause Analysis

❖ SLE および Root Cause Analysis の考察

- SLE により、視覚的にも分かりやすく、どこで・どのような問題が発生しているのか確認することができます
  また、Root Cause Analysis によりさらにその問題の詳細が確認可能です
  これにより、障害解析スキルがなくても、スムーズな障害解析が可能にないります
- 検索機能が優れており、ユーザー・端末から絞り込み、短時間で問題の要因を確認できます





RRM

❖ RRM（無線情報:Radio Resource Management）を確認します。

目的

RRM の表示内容を確認します

手順

以下のマニュアルを参考に、RRM を確認します

無線情報(RRM) 確認手順

電波の統計情報や各 AP の電波状況など詳細に確認できます

RRM　電波干渉時の自動電波調整

❖ 疑似的に電波を干渉させ、Mist が自動的に電波を調整しチャネルが変更されることを確認します。

目的

Mist の電波自動調整機能を確認します

検証手順

電波干渉試験

「AP_01」と同一のチャネルを「AP_02」に手動設定し

「AP_01」が自動的にチャネルを変更する過程を確認します

（※手順の詳細は次項に記載）

結果

チャネルが自動調整され、ログに記載されます

	Band	Channel	Channel Width	Power
z	5 GHz → 5 GHz	108 → 149	20 → 20 MHz	9 → 10 dB
z	5 GHz → 5 GHz	149 → 40	20 → 20 MHz	9 → 9 dBm
z	5 GHz → 5 GHz	48 → 165	20 → 20 MHz	10 → 8 dB
z	5 GHz → 5 GHz	36 → 161	20 → 20 MHz	8 → 8 dBm
z	Disabled → 5 GHz	128 → 128	20 → 20 MHz	8 → 11 dB
z	5 GHz → 5 GHz	56 → 56	20 → 20 MHz	13 → 14 dB

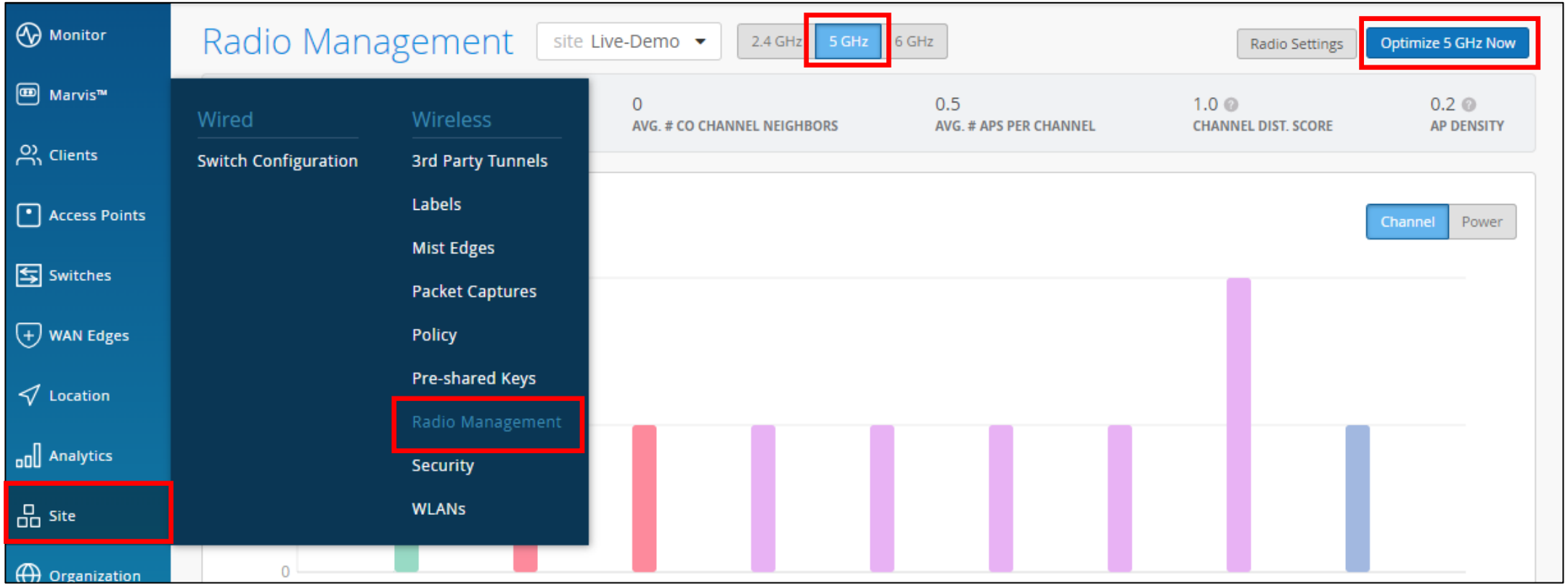
自動的に電波調整され、空いてるチャネルに切り替えることで、効率よく通信を行います

RRM　電波干渉時の自動電波調整

1. AP のチャネルを最適化します

   [Site] の [Radio Management] を開きます

   帯域を [5GHz] に合わせ、[Optimize 5 GHz Now] をクリックするとチャネルが最適化されます

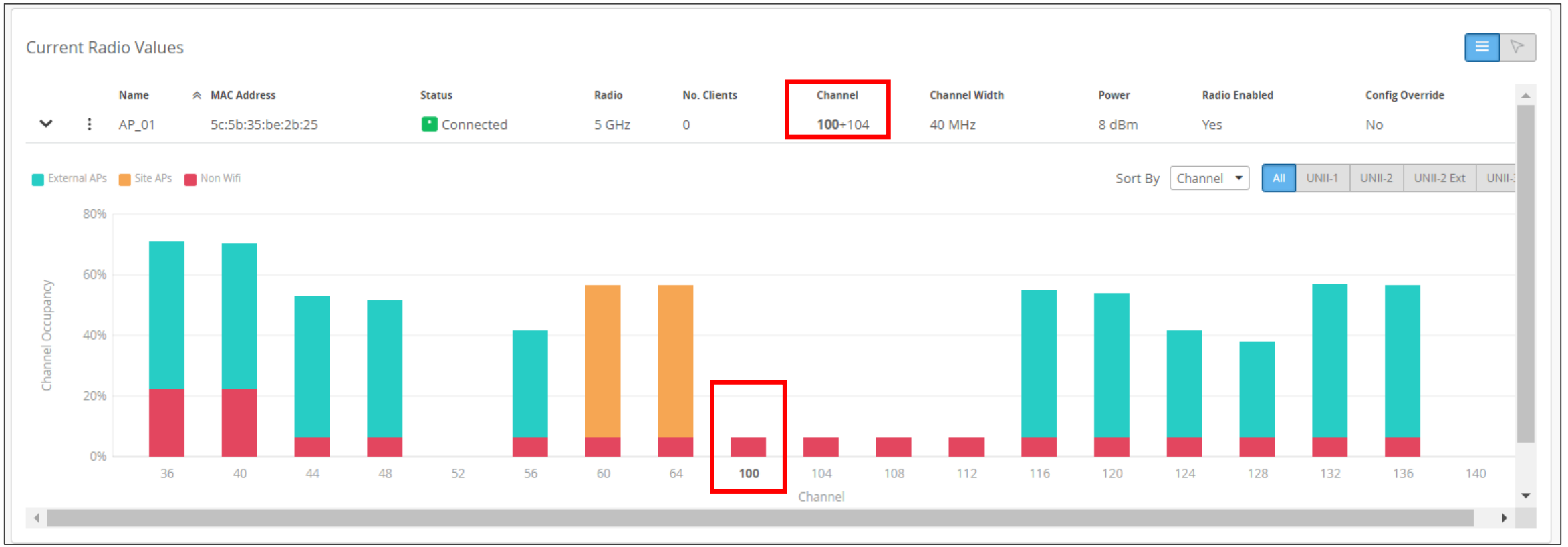


RRM　電波干渉時の自動電波調整

2. AP-01 のチャネルを確認します

   [Radio Management] の「Current Radio Values」の項目で AP_01 の Channel を確認します

   この画像では「100+104」となってます



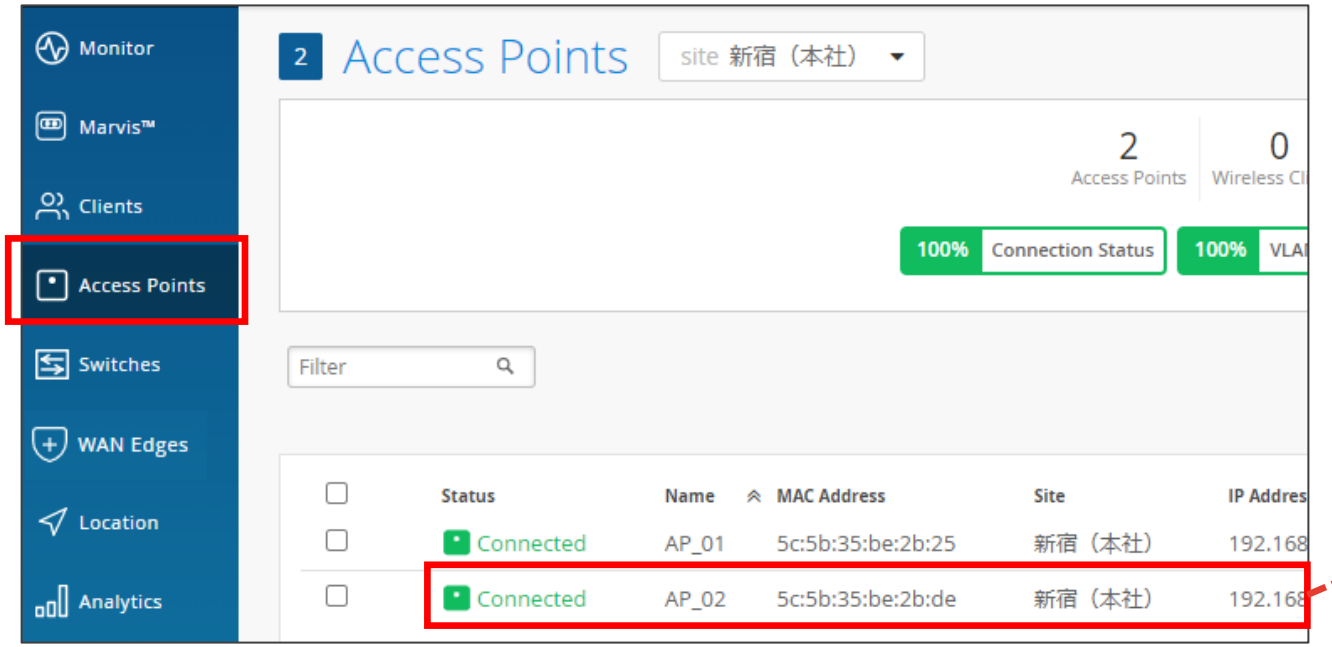
RRM　電波干渉時の自動電波調整

3. AP-02 のチャネルを固定します

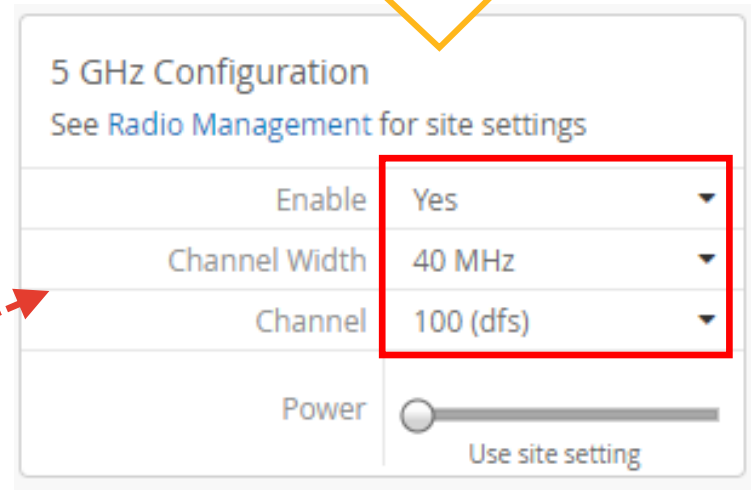
[Access Points] から「AP_02」を選択し AP の設定画面を開きます

「5 GHz Configuration」の項目にて、前項で確認した「AP_01」で使用中の Channel に変更します

（デフォルトの設定では「Use site setting」になっています）



以下の値に変更します
Enable：　Yes
Channel Width：　40 MHz
Channel：　AP_01 の Channel

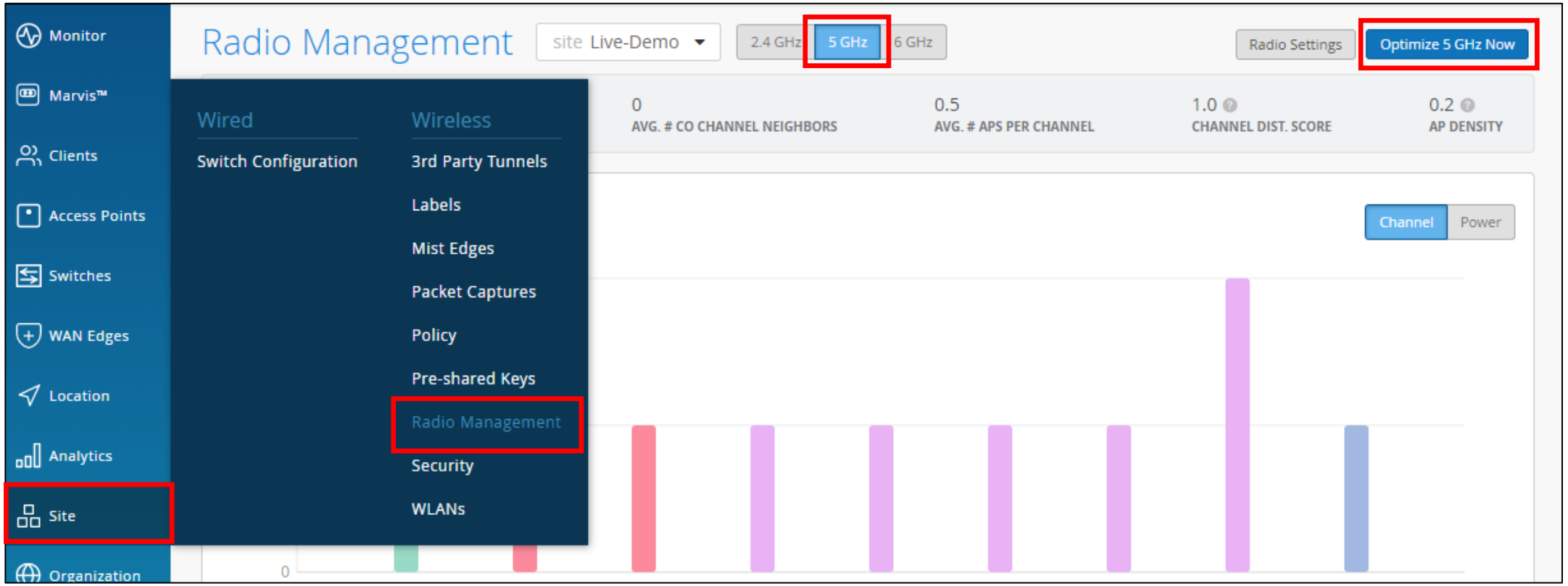


RRM　電波干渉時の自動電波調整

4. 再度 AP のチャネルを最適化します

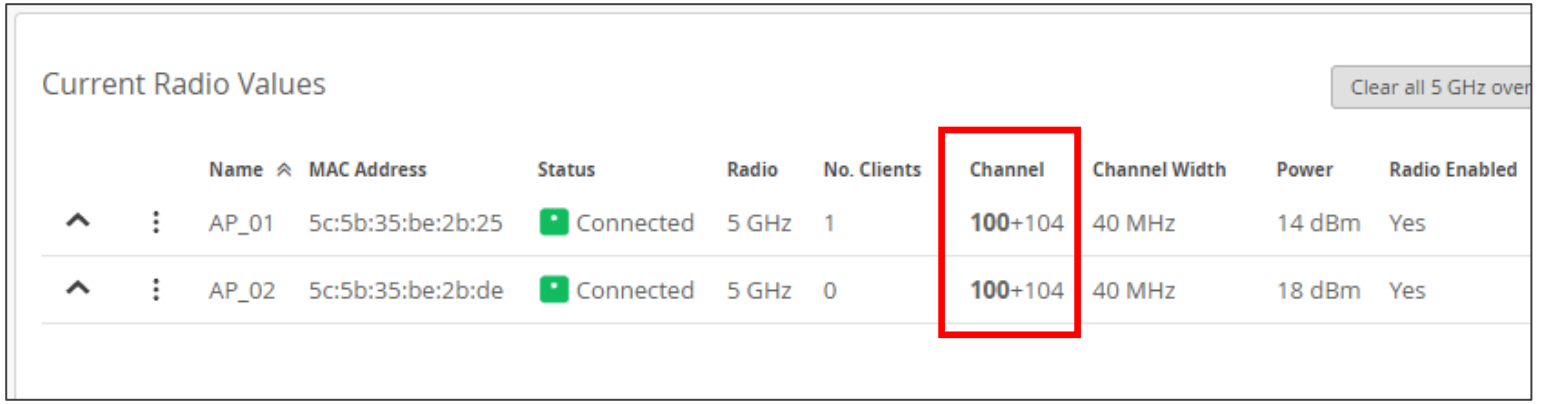
AP_02 の設定変更内容を反映させるため、再度 [Site] の [Radio Management] を開きます

帯域を [5GHz] に合わせ、[Optimize 5 GHz Now] をクリックしチャネルを最適化させます



RRM　電波干渉時の自動電波調整

5. 2台の AP が同じ Channel になっていることを確認します



6. クライアントから通信を行います

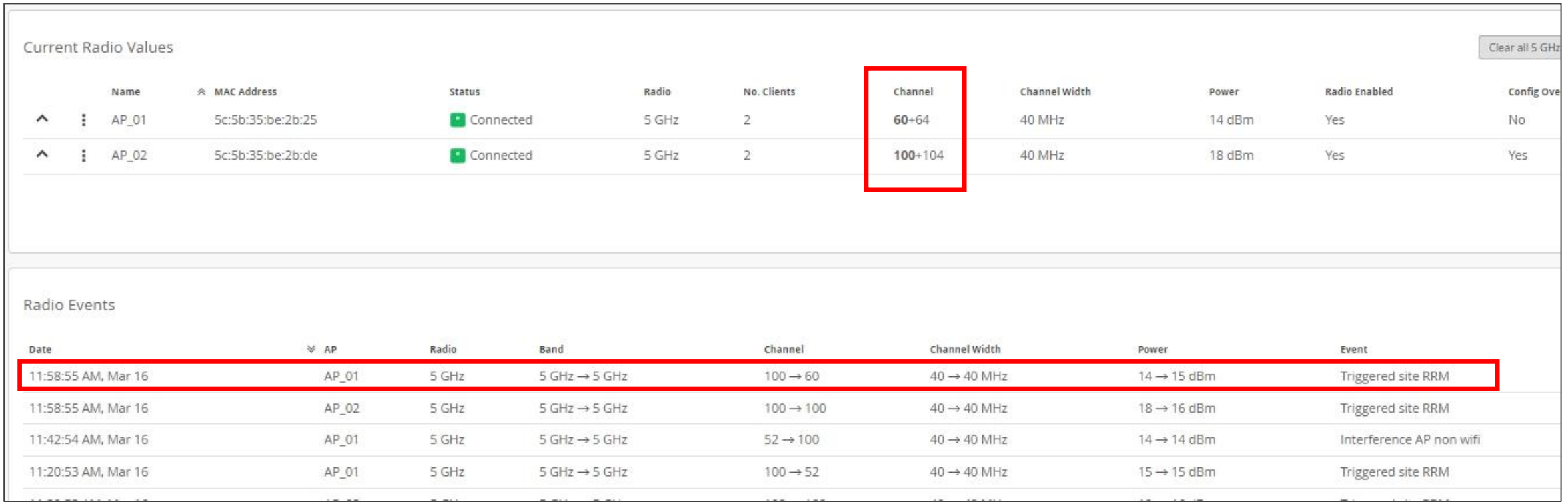
AP_01 もしくは AP_02 にクライアントを Wi-Fi 接続し通信を行います

出来るだけ帯域を使用し、継続的に通信を行うために動画再生等の通信を行ってください

RRM　電波干渉時の自動電波調整

7. Channel が変更されたことを確認します

   [Site] の [Radio Management] を開き、「Current Radio Values」および「Radio Events」の Channel の項目でAP_01 の Channel が変更されていることが確認できます



Current Radio Values

Clear all 5 GHz

Name	MAC Address	Status	Radio	No. Clients	Channel	Channel Width	Power	Radio Enabled	Config Ove
AP_01	5c:5b:35:be:2b:25	Connected	5 GHz	2	**60**+64	40 MHz	14 dBm	Yes	No
AP_02	5c:5b:35:be:2b:de	Connected	5 GHz	2	**100**+104	40 MHz	18 dBm	Yes	Yes

Radio Events

Date	AP	Radio	Band	Channel	Channel Width	Power	Event
11:58:55 AM, Mar 16	AP_01	5 GHz	5 GHz → 5 GHz	100 → 60	40 → 40 MHz	14 → 15 dBm	Triggered site RRM
11:58:55 AM, Mar 16	AP_02	5 GHz	5 GHz → 5 GHz	100 → 100	40 → 40 MHz	18 → 16 dBm	Triggered site RRM
11:42:54 AM, Mar 16	AP_01	5 GHz	5 GHz → 5 GHz	52 → 100	40 → 40 MHz	14 → 14 dBm	Interference AP non wifi
11:20:53 AM, Mar 16	AP_01	5 GHz	5 GHz → 5 GHz	100 → 52	40 → 40 MHz	15 → 15 dBm	Triggered site RRM

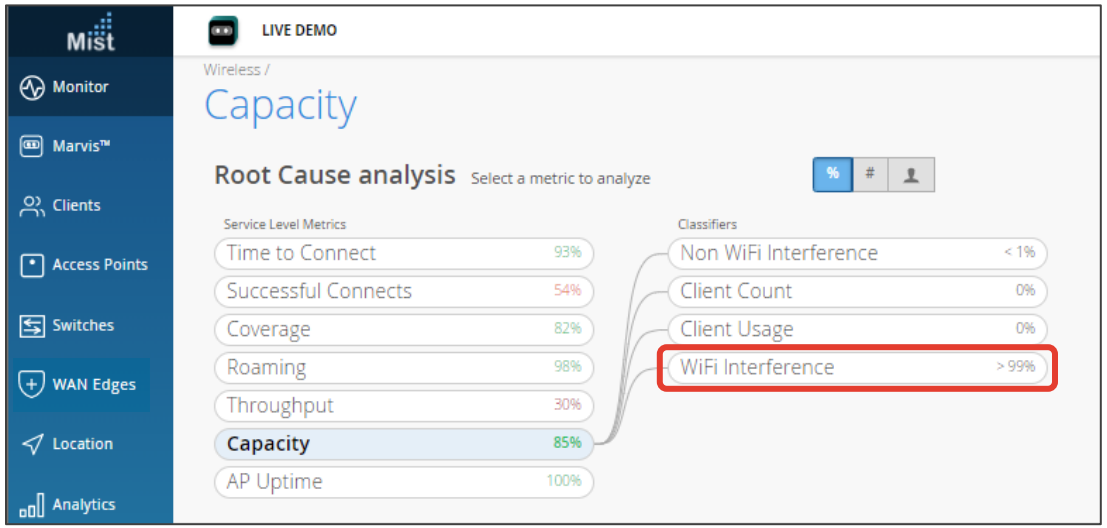
RRM　電波干渉時の自動電波調整

8. 以下のマニュアルを参考に、電波干渉の有無を特定します

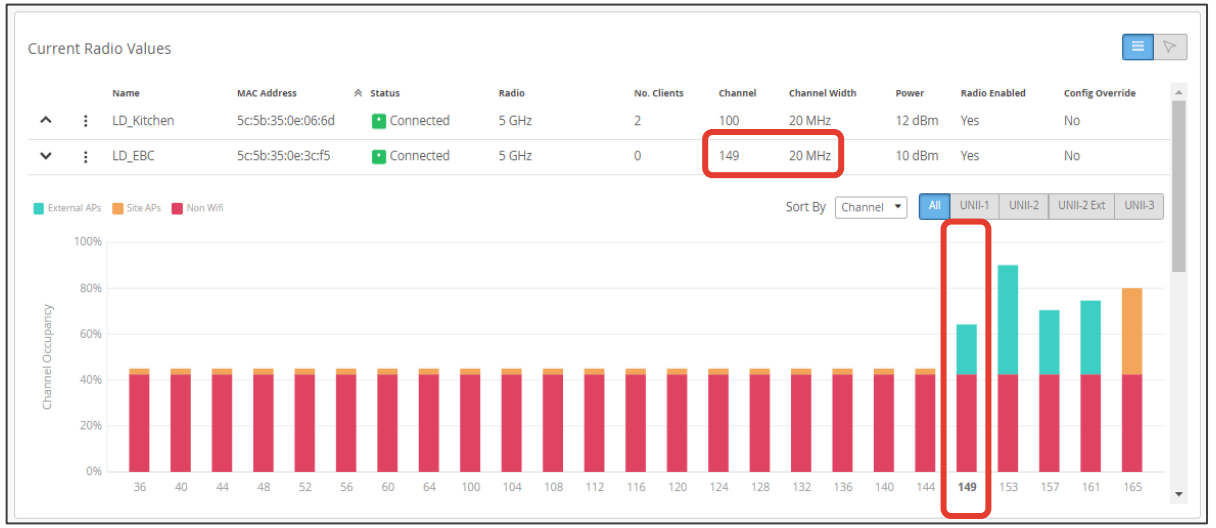
[電波干渉 有無の確認手順（拠点単位）]

[電波干渉 有無の確認手順（クライアント単位）]

❖ SLE の Capacity で Wi-Fi Interference の割合が増加していることを確認



❖ [Site] の [Radio Management] で
自身の利用するチャネルにSite APsの割合が高いことを確認



RRM　電波干渉時の自動電波調整

❖ RRM および自動電波調整についての考察

- 自動的に電波調整され、空いてるチャネルに切り替えることで、効率よく通信を行います
  - カバレッジ、容量、スループット、パフォーマンスなどの RF 情報や問題をユーザーごとに常に収集
  - ディープラーニングにてデータを理解
  - リアルタイムの要件に基づいて自動変更を実施
  - Wi-Fi サービス品質が常に最適化されるように、これらの変更の影響を測定

  このプロセスにより “self-healing (自己修復) WLAN“ を提供します
- これは、世界初の、唯一 Mist のみが実現した、RRM の革新です

- 本シナリオでは Channel の自動調整を確認するために、AP の Channel を固定しましたが、
  通常の運用で特別な理由が無い限り Channel の固定を行う事はありません

Marvis

❖ Marvis は Mist Cloud が提供している AI です。

目的

Marvis に問い合わせを行い、その結果を確認します

検証方法

Marvis への問い合わせ例：

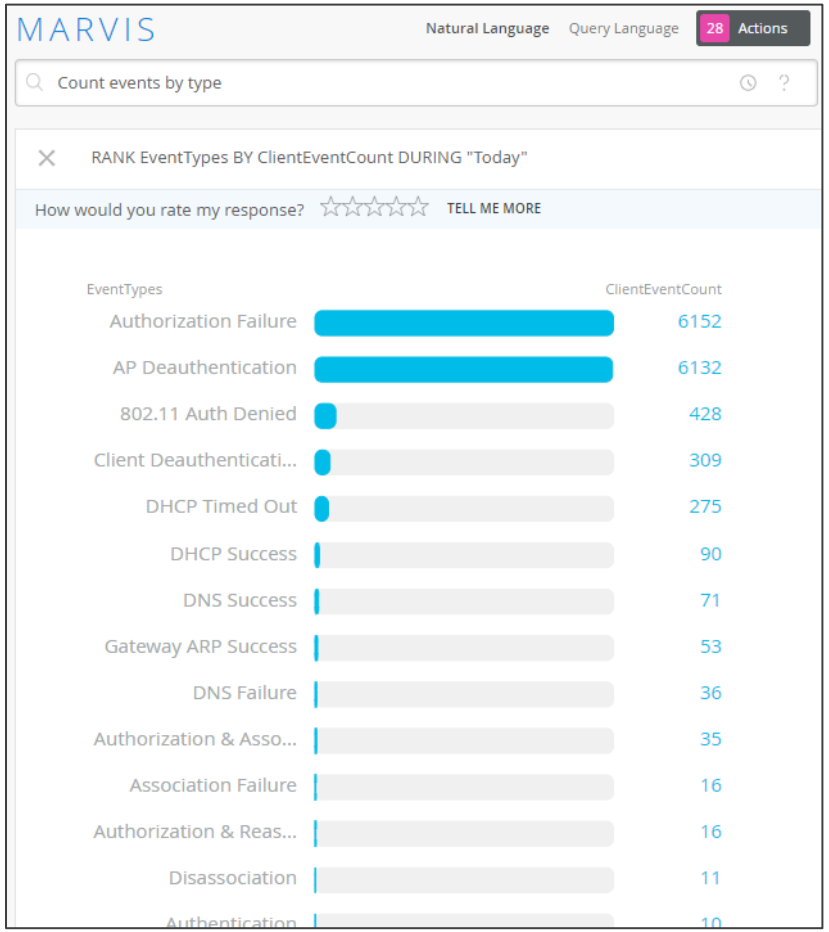
MAC アドレスのリスト化・・・「List MAC addresses」と入力

タイプ別イベントのリスト化・・・「Count events by type」と入力

参考URL：

https://www.mist.com/resources/mist-marvis-overview/

https://manage.mist.com/admin/vnadocs.html



Marvisは、自然言語処理、会話型インターフェイスにより、運用の効率化に役立てることができます

Marvis Action

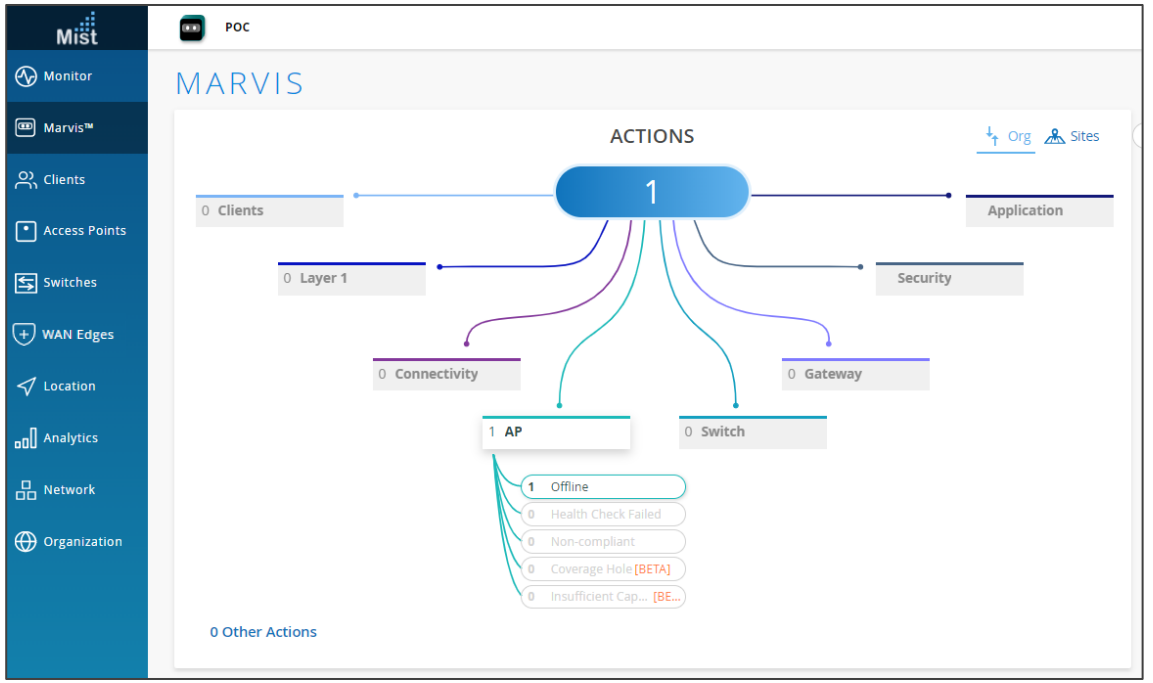
❖ Marvis Action で対処すべき問題を特定し、解決方法を提案します。

目的

Marvis Action で対処すべき問題を特定し、
解決方法を確認します

検証方法

参考URL：
https://www.mist.com/documentation/category/marvis-actions/



Marvis Action は、問題が発生する前に予測したり、トラブル解決に役立ちます

Marvis

❖ Marvis および Marvis Action についての考察

- Marvis は、自然言語処理、会話型インターフェイス、規定のアクション、内蔵されたヘルプデスク機能により、クライアントからクラウドまでの各領域で、洞察力と自動化を提供し、運用を効率化し最適化します
- AIにより、データが取り込まれるにつれて継続的に学習し、増大した知識を活用して問題をリアルタイムで発生前に修正したり、問題が発生する前に予測したり、トラブルチケットを解決します
- クライアントレベルのネットワークビューを表示し、エンドユーザーのデバイスから直接イベントをキャプチャします
- 検証された Mist AI ドリブンサポートにより、ユーザーによって作成されるチケットを最大90%減少させることが可能
- リアルタイムのインサイト、クライアント、デバイス、およびサイトレベルでのトラブルシューティングを簡素化し、サービス品質を向上します

ダイナミック パケットキャプチャー

❖ Mistでは問題発生時に必要になるキャプチャーデータを自動的に取得しています

目的

自動取得されたキャプチャーデータを確認します

検証方法

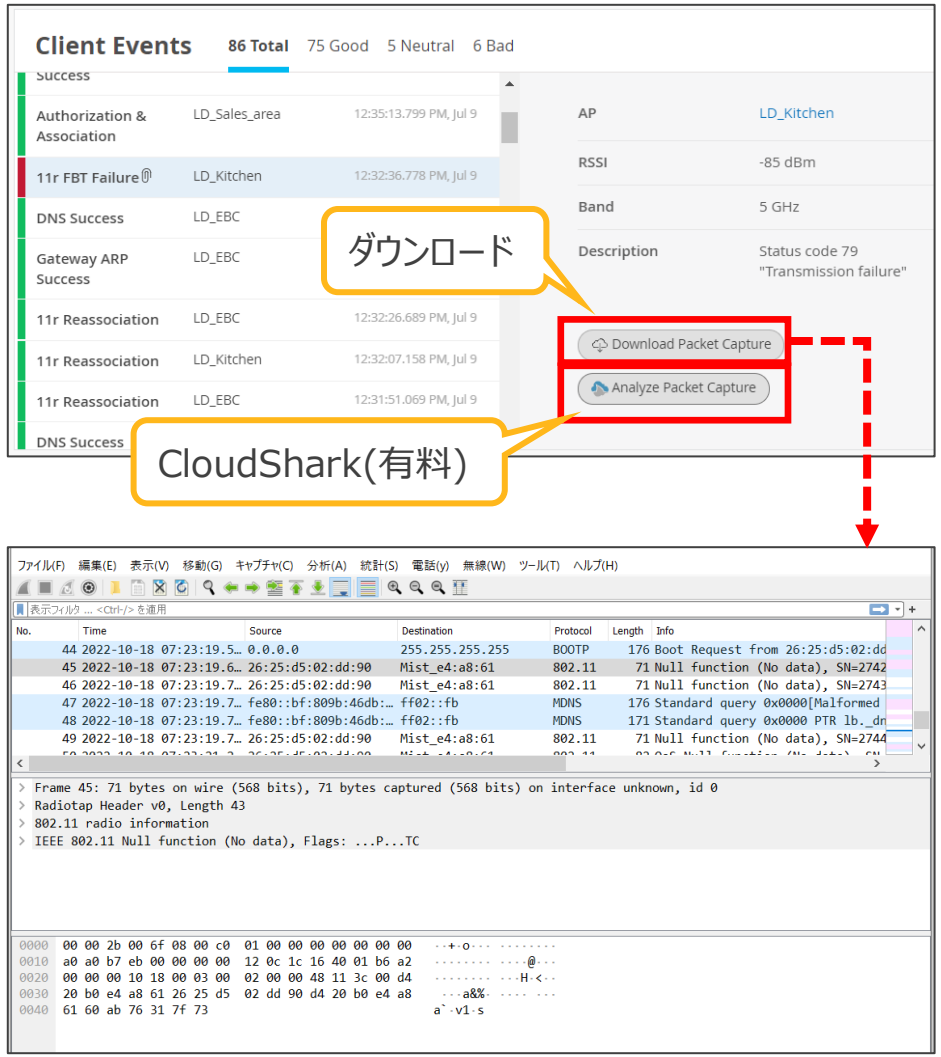
記録されている Bad Event のキャプチャーデータをダウンロードして確認します

CloudShark (有料)を契約している場合は、WEB でも確認できます

参考マニュアル：

CloudSharkの利用

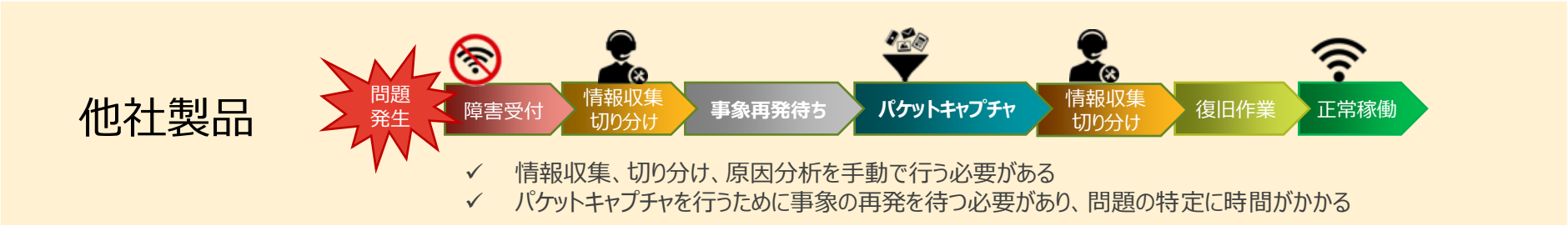
事象再発を待つ必要がなく、迅速な問題解決を可能にします



ダイナミック パケットキャプチャー

❖ ダイナミックパケットキャプチャーの考察

- すべてのパケットのヘッダ情報のみが Mist Cloud に送信されています (ペイロード部はセキュリティ上の理由のため収集されません)
- SLE を下回るなど必要と判断された場合、パケットが保存され Mist Cloud で確認できます
- 同一または類似事象の重複したパケットは破棄される場合があります
- 必要な情報が収集されているため、事象の再現待ちは不要です



アラート設定/Eメール通知

❖ 検知したいアラートを設定し、必要に応じてメール通知を設定することができます

目的

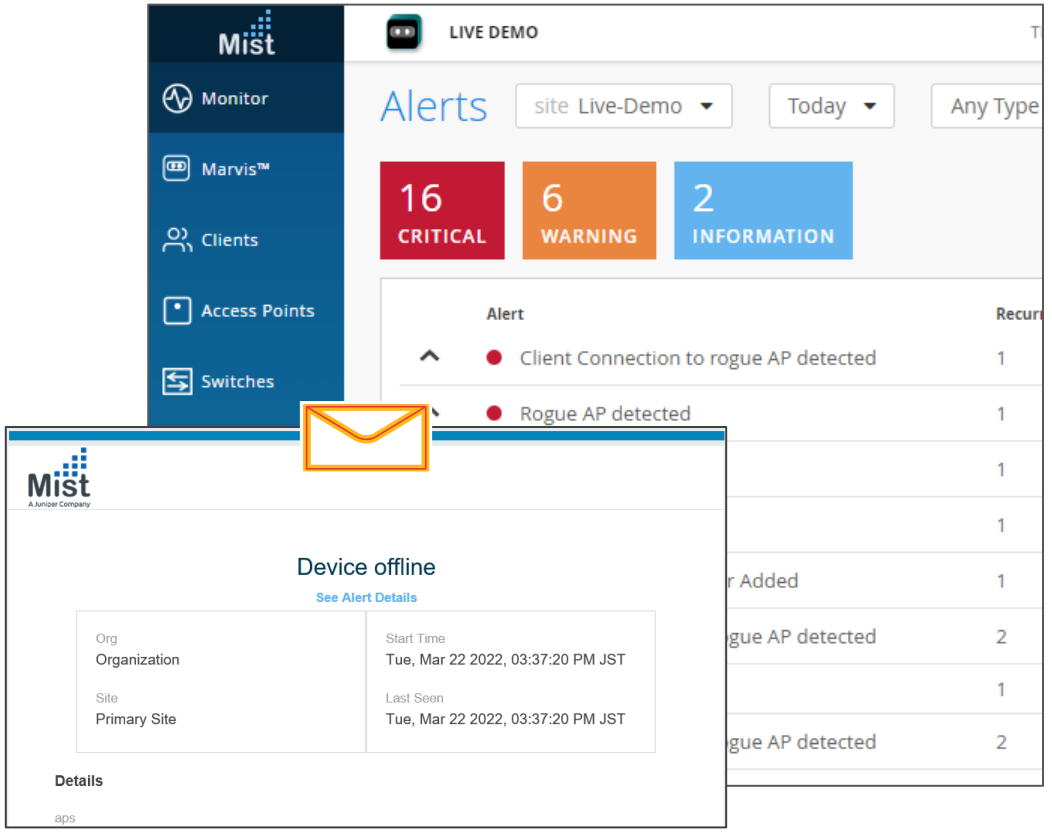
アラートの設定とアラート通知メールを確認します

検証手順

1. アラート通知メールの対象範囲と通知先を設定します
2. Device offline のしきい値を5分に設定します
3. AP からケーブルを抜線します

結果

アラート内容がメール通知されます

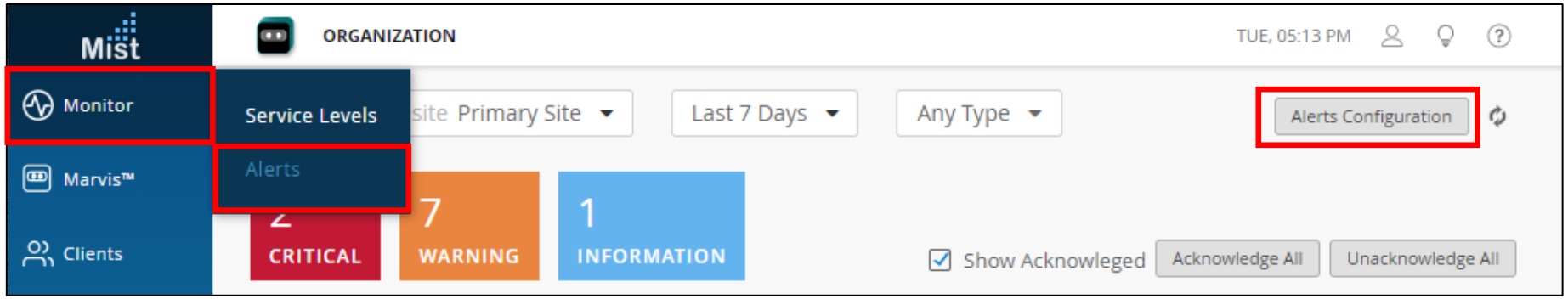


50種以上のアラートが設定できます
テンプレート機能を使うことで、管理者やSite別に検知項目をカスタマイズできます

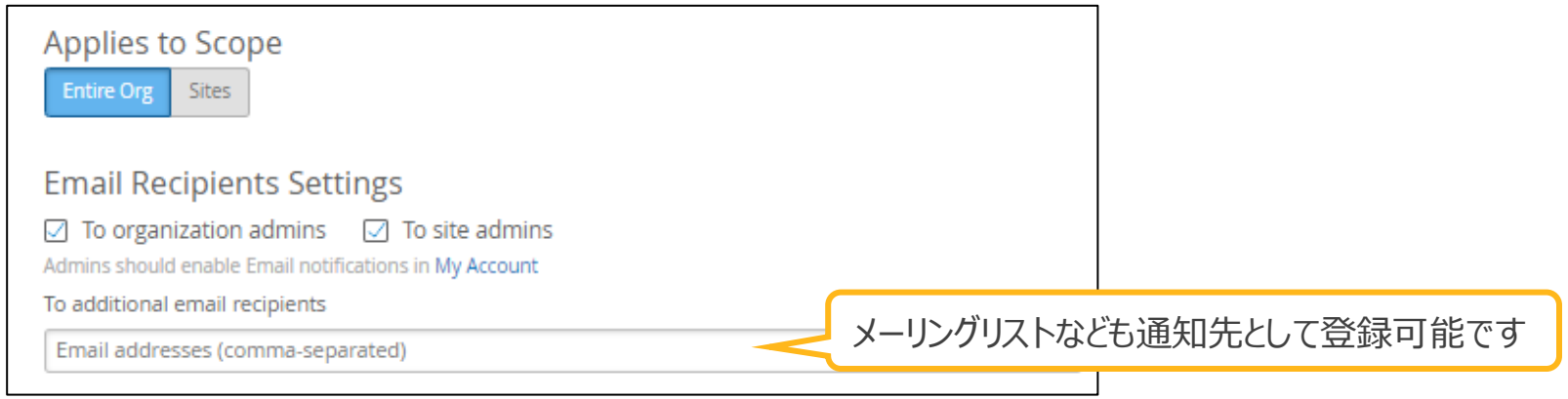
アラート設定/Eメール通知

❖ アラート通知メールの対象範囲と通知先を設定します

1. [Monitor] から [Alerts] を選択し、[Alerts Configuration] をクリックします



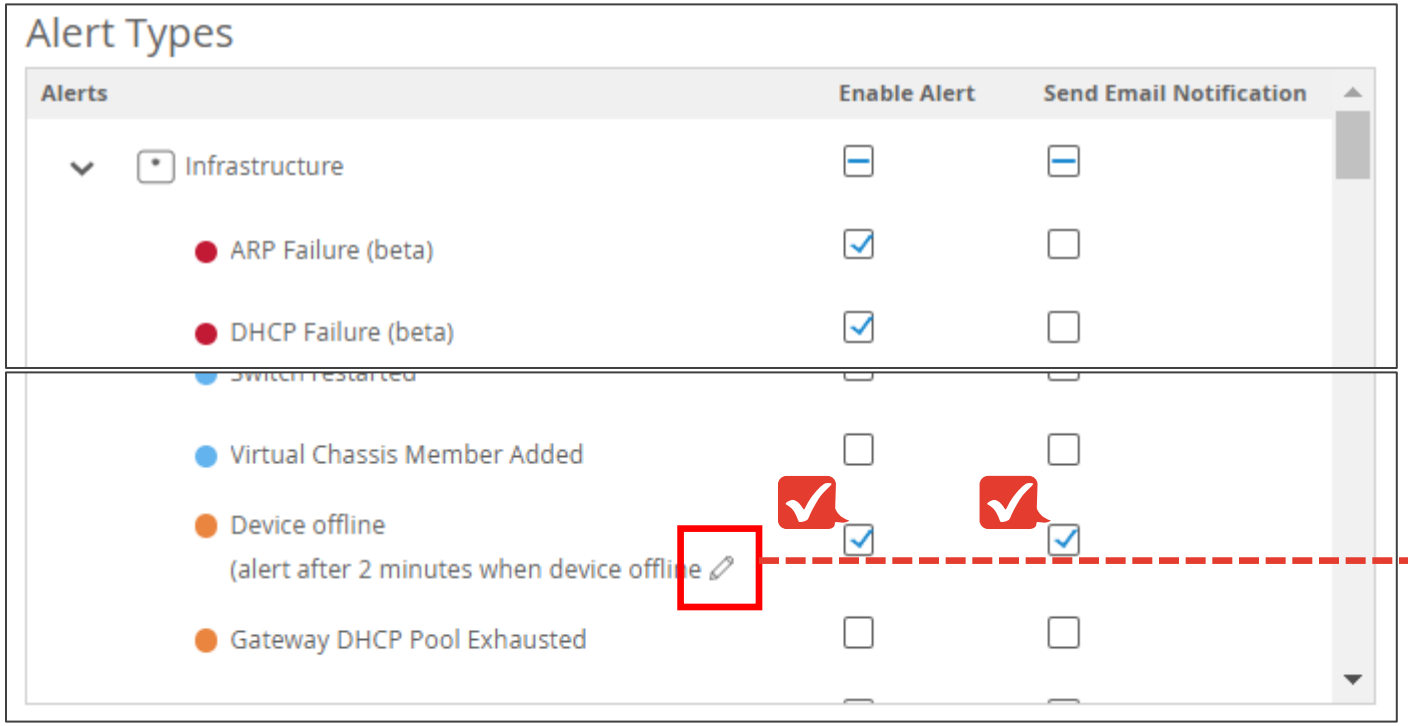
2. メール通知対象範囲 (Organization全体、各サイト) と通知先を設定します

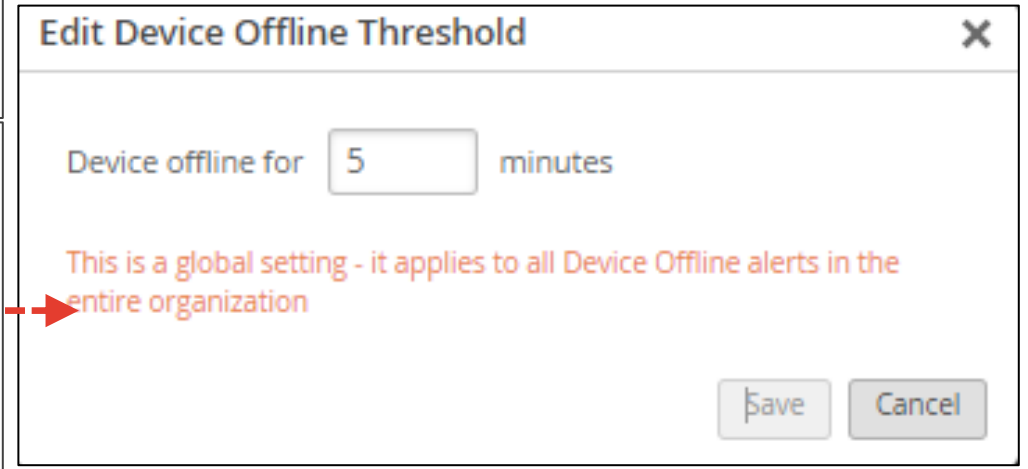


アラート設定/Eメール通知

- アラート通知メールの対象範囲と通知先を設定します

3. Alert Types の項目から “Device offline” のアラートとメール通知にチェックを入れ、しきい値を「5分」で設定します



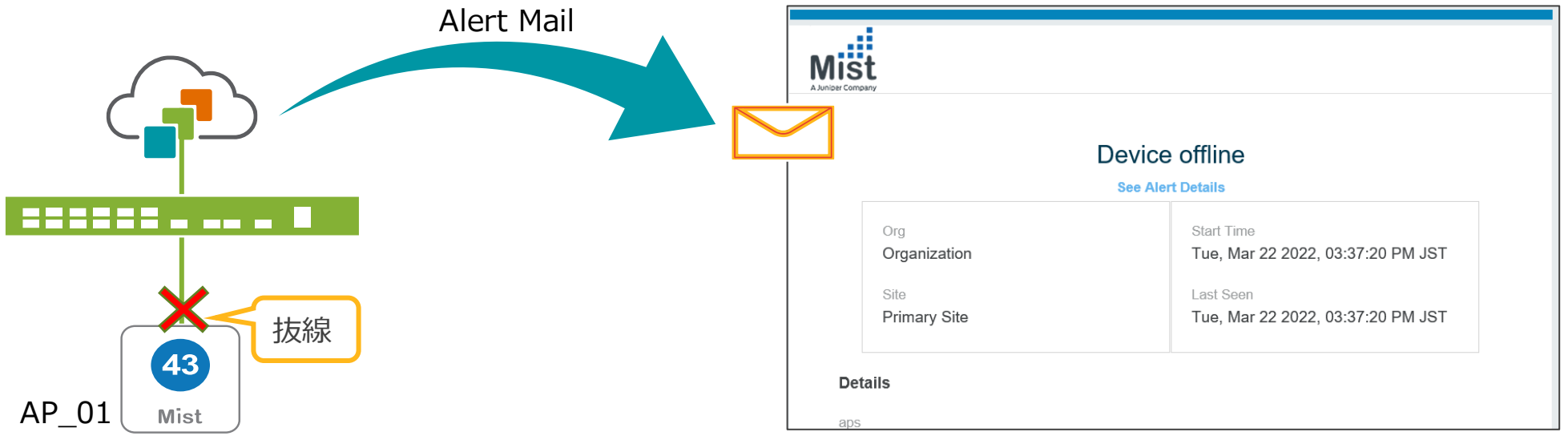


アラート設定/Eメール通知

- APを切り離しアラート通知メールを確認します

4. AP からケーブルを抜線します

   登録したメールアドレスに送付されたアラート通知メールを確認します



From : no-reply@mist.com

Subject : [Mist.com] Alert Device offline in サイト名

ネイバーAPと不正APの検出

❖ ネイバーAPと不正APを検出します。

目的

ネイバーAPと不正APを検出し、Mist AP 以外も可視化します

不正APが検出された場合はクライアントの接続をブロックします

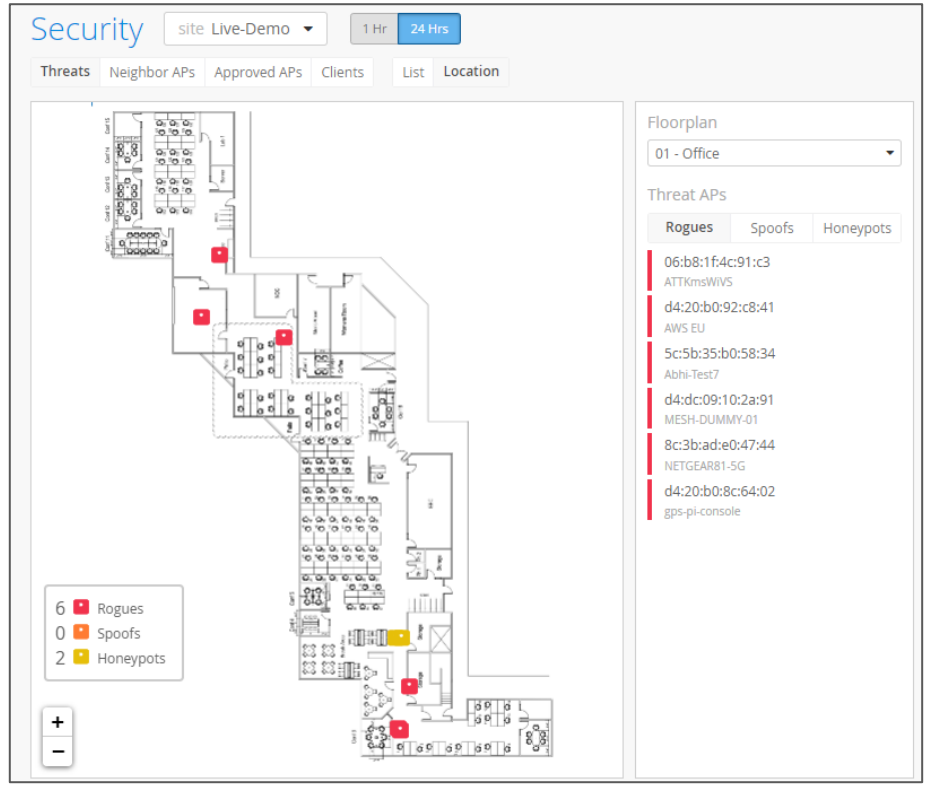
検証方法

マニュアルを参照し、ネイバーAPと不正APを確認します

周囲のAP, SSID情報 確認手順

サイトの設定 不正APの検出

（※詳細な手順は次項に記載）

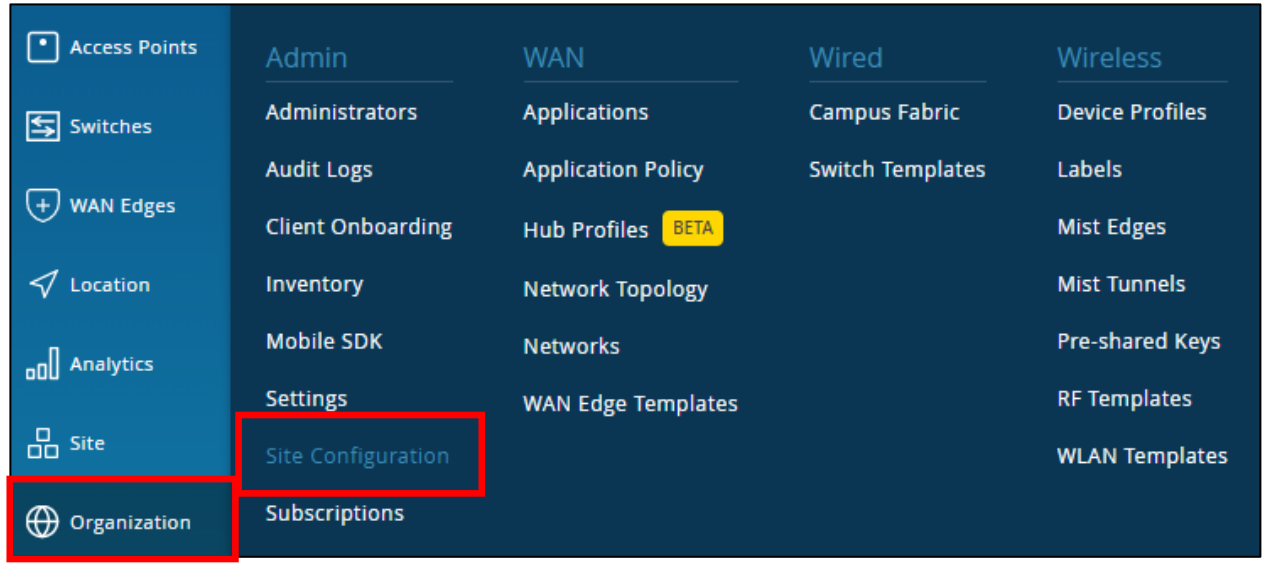


悪意ある Honeypot AP の検出をはじめ、近隣のAP、正規に使用が認められていないシャドーIT機器や今後増加が予想されるIoT機器の可視化ができます

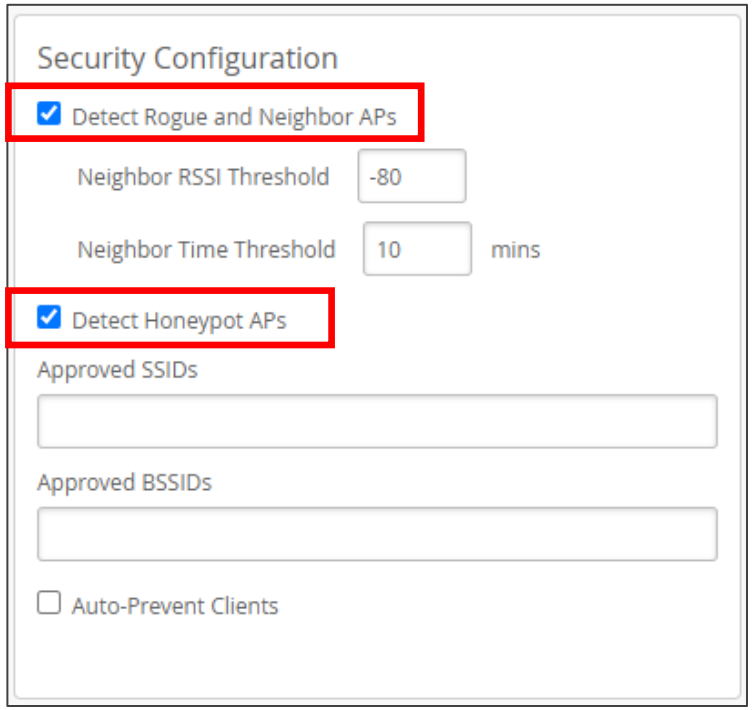
ネイバーAPと不正APの検出

❖ ネイバーAPと不正APの確認方法

1. ネイバーAPと不正APの検知を有効化
   [Organization] から [Site Configuration] を選択し
   PoC で使用している Site を選択します



2. Security Configuration の項目で
   Detect Rogue and Neighbor APs (デフォルト無効) と
   Detect Honeypot APs にチェックを入れます



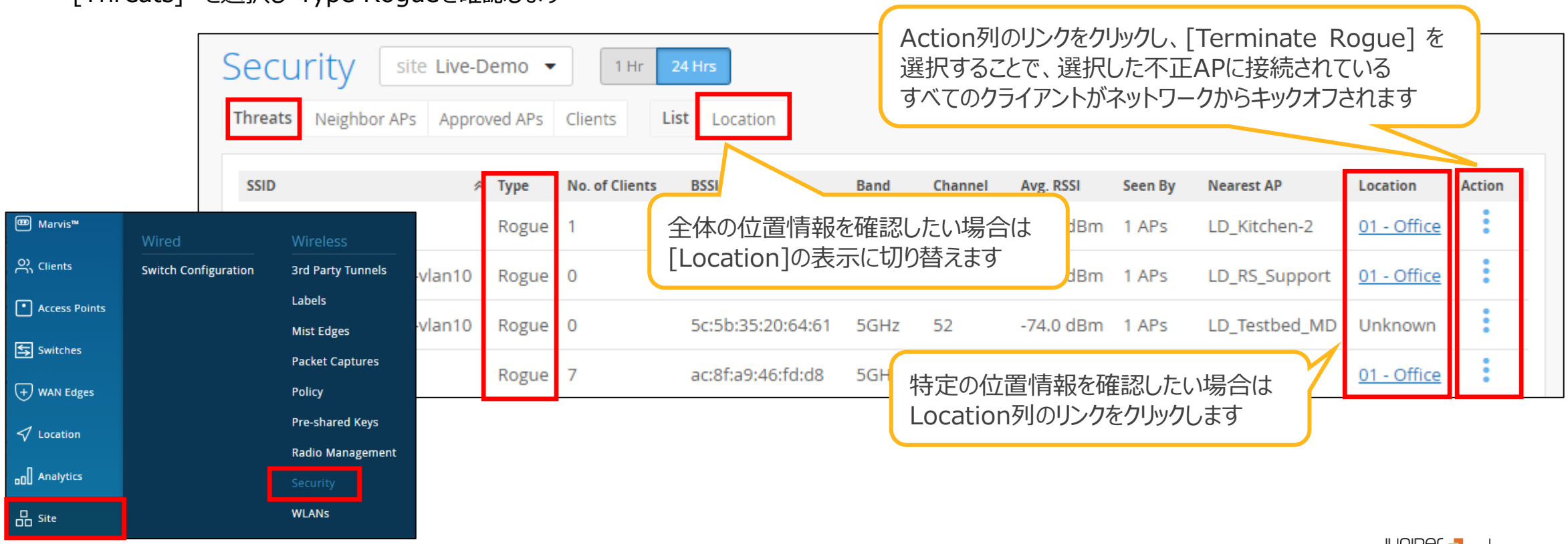
ネイバーAPと不正APの検出

❖ ネイバーAPと不正APの確認方法

3. 不正APの確認

[Site] から [Security] を選択し、PoCで使用している Site を選択します

[Threats] を選択し Type Rogueを確認します



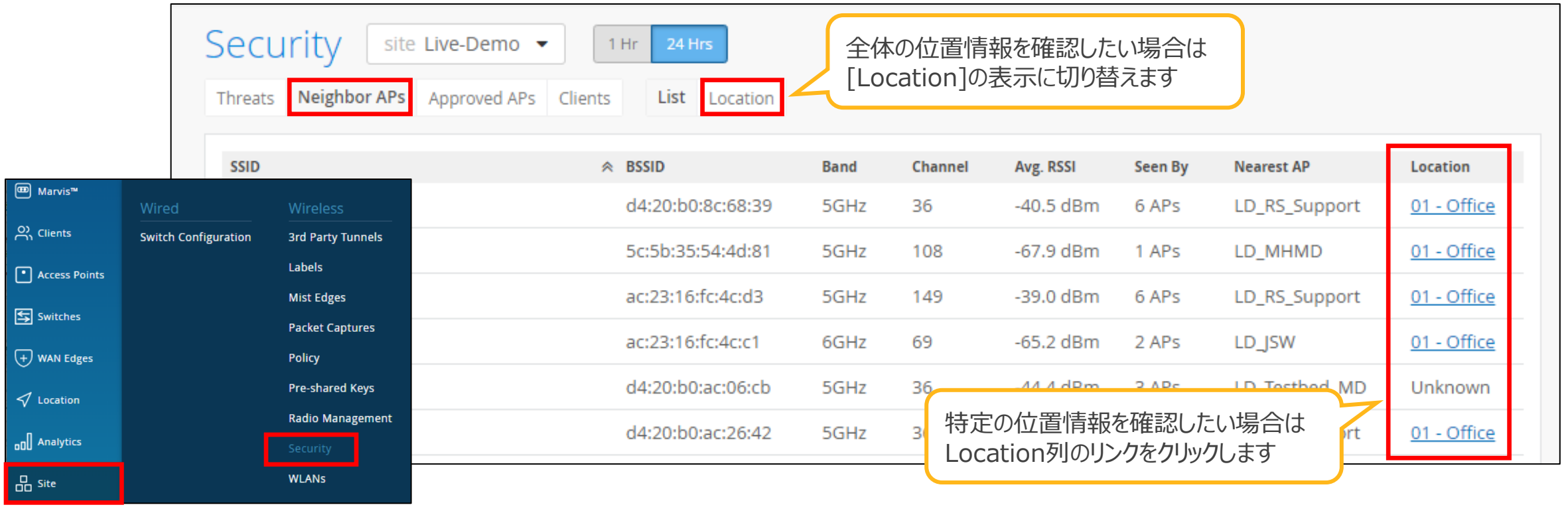
ネイバーAPと不正APの検出

❖ ネイバーAPと不正APの確認方法

4. ネイバーAPの確認

[Site] から [Security] を選択し、PoCで使用している Site を選択します

[Neighbors Aps] を選択し Mistの管理下にない周囲のアクセスポイント，SSID, Channelを確認します



レポート作成機能

❖ レポート作成機能を使用しレポート作成します。

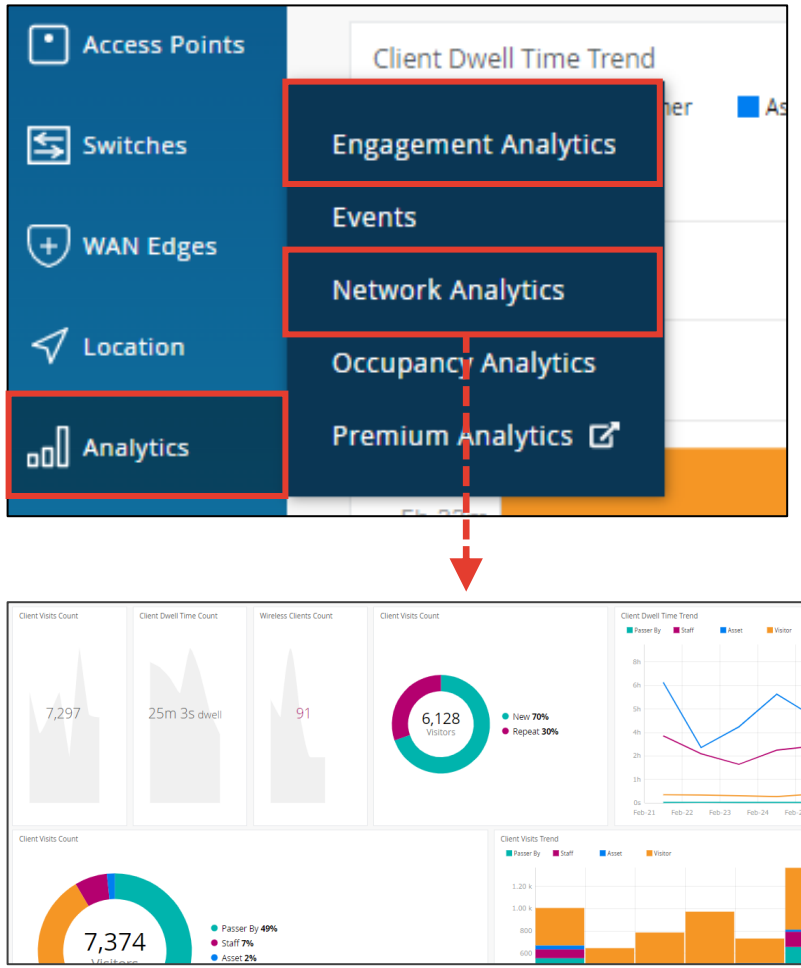
目的

Engagement Analytics または Network Analytics を使用し、
TOPクライアント、TOP WLAN、接続の問題の割合、接続数の多いAP、
TOPアプリケーションなどの必要な情報を登録しレポートを作成します

検証方法

マニュアルを参照し、レポートを作成します
エンゲージメントアナリティクスの設定

参考 URL：
https://www.mist.com/documentation/network-and-engagement-analytics/



レポートは複数登録可能ですので、報告先に合わせて何度もレポートを作成する必要はありません

APファームウェアのマニュアルアップグレード

❖ AP のファームウェアを手動でアップグレードします。

目的

production から rc1 へ、GUI 上から AP の手動アップグレードを実行し、
断時間や影響範囲を確認します

検証方法

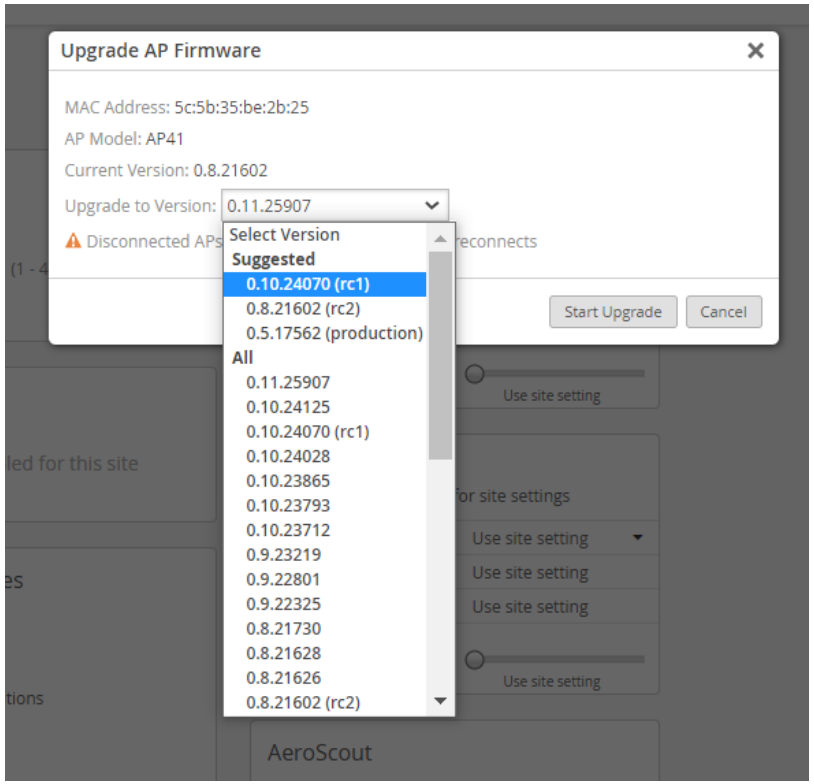
マニュアルを参照し、AP ファームウェアを手動でアップグレードします

ファームウェア 手動アップグレード手順

以下のバージョンへアップグレードします

現在のバージョン　：production firmware の最新バージョン

ターゲットバージョン　：rc1 firmware の最新バージョン



このシナリオでは手動でバージョンを変更しましたが、通常は指定したタイミングに
自動でアップグレードされるため運用コストを抑えることが可能です

APの設置場所確認

❖ Locating 機能を使いAPの設置場所を特定します。

目的

[Locating] ボタンをクリックし、AP の LED 点灯パターンを確認します

Locating 機能は、AP の場所を特定する際に役立ちます

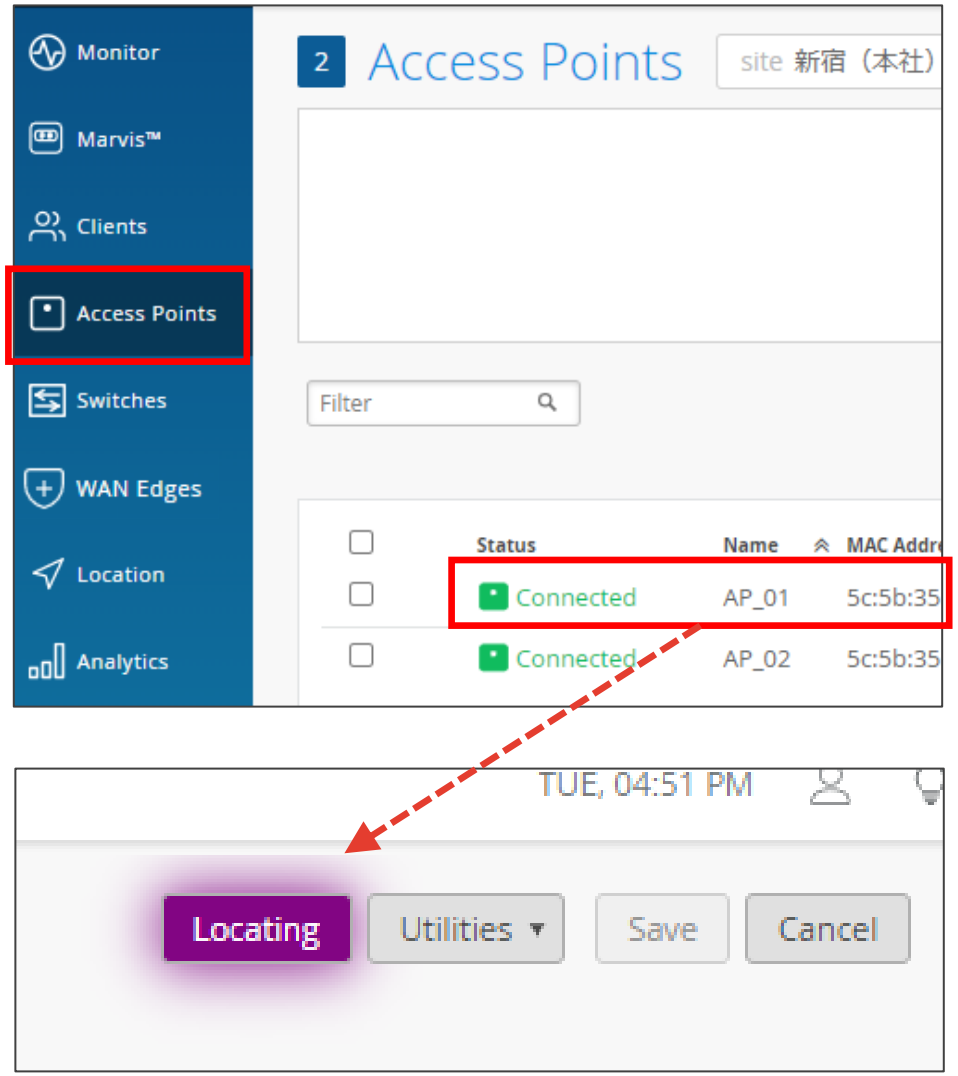
手順

[Access Points] から 任意のAPを選択します

AP 設定画面右上にある [Locating] ボタンをクリックします

AP の LED がカラフルに点灯します

再度 [Locating] ボタンをクリックすると、通常のLED表示に戻ります



例えば、APリプレース作業時に、現地の作業員が、
素早く、間違いなく作業対象のAPを特定することが可能です

AP 交換時の手順

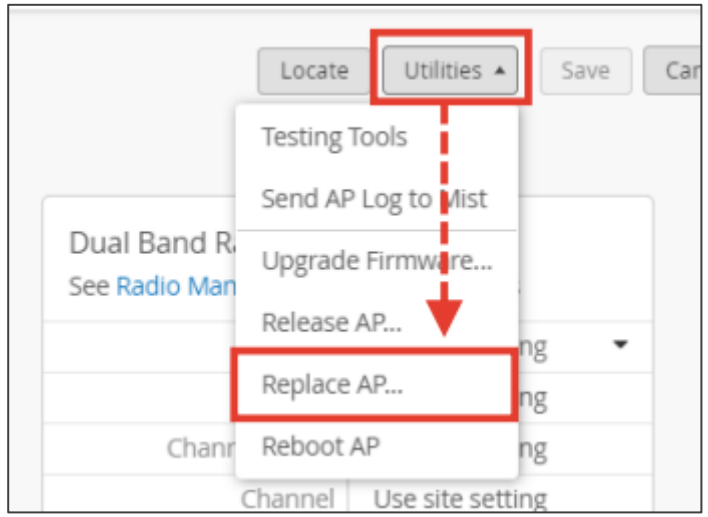
❖ AP の交換を実施します。

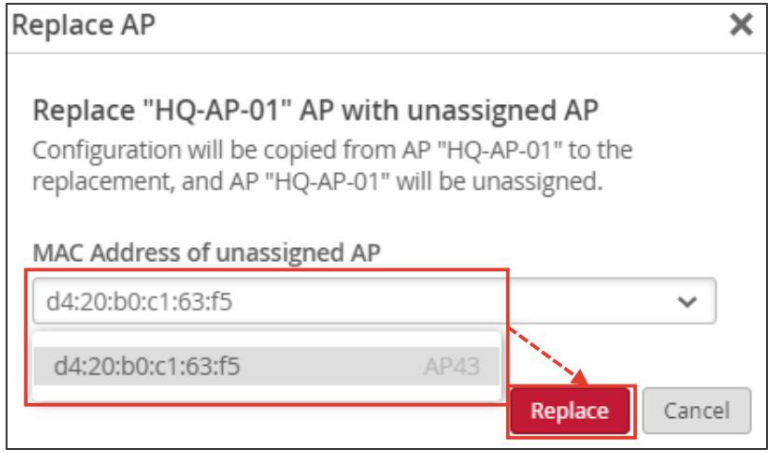
目的

遠隔の拠点の AP をリプレースすると仮定し、AP のリプレースを実施します
- 遠隔の拠点で AP をリプレースすると仮定したとき
  拠点へ代替 AP と取付を行う作業員を手配し、物理的な取付作業と
  AP のクレームを行います
  同時に本社のシステム担当者は、マニュアルにある登録変更を行います

検証方法

AP を1台登録解除し、代替 AP として扱い、AP のリプレースを実施します
以下のマニュアルを参照し、AP のリプレースを実施します
アクセスポイント 交換手順





リプレースが必要になったとしても、システム担当者が拠点に向かう必要はなく、
登録変更も簡単に行うことができます

Thank you