NEC

管理コンソール(Management Console)

ユーザーガイド

エンドユーザー使用許諾契約

Please read the End User License Agreement before installing the Management Device.
Installing Management Console/Management Device constitutes your acceptance of the terms and conditions of the End User License Agreement.
Please read the End User License Agreement before installing Management Console/Management Device. The End User License Agreement is available at the following location
http://www.necat.co.jp/products/na1000w/information/pqFA20k.html
Installing Management Console/Management Device constitutes your acceptance of the terms and conditions of the End User License Agreement.

免責事項

THE INFORMATION IN THIS GUIDE IS SUBJECT TO CHANGE WITHOUT ANY PRIOR NOTICE.
NEC PLATFORMS, LTD.(HEREINAFTER REFERRED TO AS "NECPF") IS NOT LIABLE FOR ANY SPECIAL, INCIDENTAL, INDIRECT, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, OR ANY OTHER PECUNIARY LOSS) ARISING OUT OF THE USE OF OR INABILITY TO USE THIS PRODUCT.
THIS PRODUCT HAS THE CAPABILITY TO BLOCK WIRELESS TRANSMISSIONS FOR THE PURPOSE OF PROTECTING YOUR NETWORK FROM MALICIOUS WIRELESS ACTIVITY. BASED ON THE POLICY SETTINGS, YOU HAVE THE ABILITY TO SELECT WHICH WIRELESS TRANSMISSIONS ARE BLOCKED AND, THEREFORE, THE CAPABILITY TO BLOCK AN EXTERNAL WIRELESS TRANSMISSION. IF
IMPROPERLY USED, YOUR USAGE OF THIS PRODUCT MAY VIOLATE US FCC PART 15 AND OTHER LAWS. BUYER ACKNOWLEDGES THE LEGAL RESTRICTIONS ON USAGE AND UNDERSTANDS AND WILL COMPLY WITH US FCC RESTRICTIONS AS WELL AS OTHER GOVERNMENT REGULATIONS. NECPF IS NOT RESPONSIBLE FOR ANY WIRELESS INTERFERENCE CAUSED BY YOUR USE OF THE PRODUCT. NEC PLATFORMS, LTD. AND ITS AUTHORIZED RESELLERS OR DISTRIBUTORS WILL ASSUME NO LIABILITY FOR ANY DAMAGE OR VIOLATION OF GOVERNMENT REGULATIONS ARISING FROM YOUR USAGE OF THE PRODUCT, EXCEPT AS EXPRESSLY DEFINED IN THE INDEMNITY SECTION OF THIS DOCUMENT.
THE INFORMATION IN THIS GUIDE IS SUBJECT TO CHANGE WITHOUT ANY PRIOR NOTICE.
NEC PLATFORMS, LTD.(hereinafter referred to as “NECPF”) IS NOT LIABLE FOR ANY SPECIAL, INCIDENTAL, INDIRECT, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, OR ANY OTHER PECUNIARY LOSS) ARISING OUT OF THE USE OF OR INABILITY TO USE THIS PRODUCT.
This Product has the capability to block wireless transmissions for the purpose of protecting your network from malicious wireless activity. Based on the policy settings, you have the ability to select which wireless transmissions are blocked and, therefore, the capability to block an external wireless transmission. If Improperly used, your usage of this Product may violate US FCC part 15 and other laws. Buyer acknowledges the legal restrictions on usage and understands and will comply with US FCC restrictions as well as other government regulations. NECPF is not responsible for any wireless interference caused by your use of the Product. NEC PLATFORMS, LTD. and its authorized resellers or distributors will assume no liability for any damage or violation of government regulations arising from your usage of the product, except as expressly defined in the indemnity section of this document.

責任の制限

NECPF will not be liable to customer or any other party for any indirect, incidental, special, consequential, exemplary, or reliance damages arising out of or related to the use of Management Device, Management Console, and NECPF's products under any legal theory, including but not limited to lost profits, lost data, or business interruption, even if NECPF knows of or should have known of the possibility of such damages. Regardless of the cause of action or the form of action, the total cumulative liability of NECPF for actual damages arising out of or related to the use of Management Device, Management Console, and NECPF's products will not exceed the respective price paid for Management Device, Management Console, and NECPF's products.

(C) 2003-2016 Mojo Networks, Inc. All Rights Reserved.
Powered by Marker PacketTM, Active ClassificationTM, Live EventsTM, VLAN Policy MappingTM, Smart ForensicsTM, WEPGuardTM and WPAGuardTM. Mojo Networks and the Mojo Networks logo are trademarks and Mojo is a registered trademark of Mojo Networks, Inc.
This product contains components from Open Source software. These components are governed by the terms and conditions of the GNU Public License. To read these terms and conditions visit http://www.gnu.org/copyleft/gpl.html.
Protected by one or more of U.S. patent Nos. 7,002,943; 7,154,874; 7,216,365; 7,333,800; 7,333,481; 7,339,914; 7,406,320; 7,440,434; 7,447,184; 7,496,094; 7,536,723; 7,558,253; 7,710,933; 7,751,393; 7,764,648; 7,804,808; 7,856,209; 7,856,656; 7,970,894; 7,971,253; 8,032,939; and international patents: AU 200429804; GB 2410154; JP 4639195; DE 60 2004 038 621.9; and GB/NL/FR/SE 1976227. More patents pending. For more information on patents, please visit: www.airtightnetworks.com/patents.

・ Wi-Fi、Wi-Fi Alliance、WPA および WPA2 は、Wi-Fi Alliance の商標または登録商標です。
・ その他、各会社名、各製品名およびサービス名などは各社の商標または登録商標です。

© NEC Platforms, Ltd. 2016-2019
NECプラットフォームズ株式会社の許可なく複製・改版、および複製物を配布することはできません。

目次

本ガイドについて

管理コンソール(Management Console) ユーザーガイドでは、管理コンソール(Management Console)の設定と管理の方法を説明します。
本ガイドでは、以下のとおりの呼びかたで記載します。
アクセスポイント(AP)は、アクセスポイントまたは、AP と呼びます。
管理コンソール(Management Console)は、管理コンソールまたは、Management Console と呼びます。
管理デバイス(Management Device)は、管理デバイスまたは、Management Device と呼びます。
集中管理型 AP モードは、AP モードと呼びます。

※ 本ガイドで掲載している管理コンソールの画面は、ソフトウェアのバージョンにより一部内容が実際の画面と異なる場合があります。また、一部の設定項目の名称および内容についても実際の動作と異なる場合があります。

ご注意：本システムを導入する前に、エンドユーザー使用許諾契約書をよくお読みください。 本システムを導入することにより、エンドユーザー使用許諾契約書の利用条件に同意されたものとみなされます。

製品およびガイドの更新

製品のアップデートに関する重要なお知らせについては購入先へお問い合わせください。

はじめに

管理コンソール(Management Console)は、あなたが本サービスにアクセスするために設定し、そしてモニタすることができる HTML 5 ベースのユーザーインタフェースです。
管理コンソール(Management Console)は直観的で使いやすく、WIPS および（または）Wi-Fi をニーズに合わせて簡単に設定することができます。
コンソールは 7 つのセクションに分かれています（ダッシュボード、ロケーション、デバイス、イベント、フォレンジック、コンフィグレーション、レポート）。
管理コンソール(Management Console)は、コンフィグレーションから設定することができます。コンフィグレーションから、ユーザーの定義と管理、WIPS 構成の設定と管理、 Wi-Fi アクセスの設定、WLAN のインテグレーション設定、企業のセキュリティ管理サーバーのインテグレーション設定などが可能です。
ダッシュボードでは、WIPS および（または）Wi-Fi インプリメンテーションをイメージ図で表示します。それは無線ネットワーク上のアクセスポイント、クライアントの他、WIPS センサーで検出されたネットワークに関連するグラフの中から選択できます。ネットワークに対する無線の脅威の詳細は、WIPS ウィジェットで見ることができます。
管理コンソール(Management Console)は、ロケーションの作成を容易にします。これらのロケーションは、キャンパス内のさまざまな建物やオフィス無線 LAN 内での異なるフロアや階を示すことができます。ロケーションを使用して、小売店やオフィスのロケーションを管理することができます。オフィスの各フロアにレイアウトを設定することが可能です。そのあと、これらのロケーションに固有の WIPS/Wi-Fi ポリシーを定義することができます。
すべての AP、管理デバイス(Management Device)、クライアントはデバイスで表示されます。実際のデバイスに加えて、デバイスには WIPS センサーにより検出されたネットワークのリストが表示されます。
イベントでは、WIPS インプリメンテーションによって検出されたイベントが表示されます。
フォレンジックでは、使い勝手の良い形式で AP 関連の脅威とクライアント関連の脅威を一覧表示しています。フォレンジックを使用して、無線の脅威を集計することができます。
レポートでは、多様なビルトインやカスタムレポートの生成を容易にします。これらのレポートは、さまざまなコンプライアンスレポート、そしてネットワーク内のデバイスおよびネットワークで発生するイベントに関連するレポートを含んでいます。レポートを使用して、レポートをスケジュール管理し、解析データを生成することが可能です。

管理コンソール(Management Console)のコンフィグレーション

管理コンソール(Management Console) は、ネットワークを監視し、防御を開始する前に、使用可能な状態にする必要があります。管理コンソール(Management Console) で、設定する多様なオプションを見るにはコンフィグレーション を クリックします。

コンフィグレーションページでは、さまざまなカテゴリが表示されます（デバイスのコンフィグレーション、WIPS、ユーザーアカウント、イベント、システム設定、ESM インテグレーション）。

デバイスのコンフィグレーション：SSID プロファイルの作成、デバイステンプレートの作成、ネットワークインタフェースの作成を行います。

WIPS：WIPS を使用して無線侵入防御パラメータを設定し管理します。

ユーザーアカウント： ユーザー管理、パスワード管理、LDAP/RADIUS 設定、証明書の設定、アカウント停止管理は**ユーザーアカウント**を使用して行います。

イベント：**イベント**を使用してイベント関連の設定および管理（特定の重要なイベント発生時に電子メールを通知）を行います。

システム設定：本システムの設定と管理を行います。

ESM インテグレーション：ESM インテグレーションを使用してエンタープライズ・セキュリティ管理ソフトウェアとのインテグレーションに関する設定を行います。管理コンソール(Management Console)は、SNMP、Syslog と統合されます。

言語設定

コンフィグレーション>システム設定>言語設定を使用して、システム言語と SSID のエンコーディングを定義します。電子メールの通信や Syslog メッセージなどの言語を設定するために使用されます。
サーバーが同じサーバークラスタの一部である場合は、サーバーから別のサーバーに言語設定をコピーすることができます。

システム言語の設定

システム言語は、システムが電子メール、Syslog メッセージなどを通じて通信するために使用する言語です。**システム言語設定**のデフォルト値は日本語です。

SSID エンコーディングの設定

SSID のようなパラメータが、ページエンコードを用いる（英語以外の言語を使用して）AP で設定されると、そのページのエンコーディングと、ここで選択したエンコーディングとが一致しない場合は文字が正しく表示されません。

システムで正しくローカル言語の SSID を表示するために、あなたの地域で使用される適切な SSID のエンコーディングを選択します。

SSID エンコーディングのデフォルト値は UTF-8 です。 別の SSID エンコーディングを選択するには、次の手順を実行します。
1. **コンフィグレーション>システム設定>言語設定**へ移動します。
2. **SSID エンコーディング**で、必要な SSID エンコーディングを選択します。
3. 新しい SSID エンコーディングを保存するには、**保存**をクリックします。

言語設定を別のサーバーへコピー

両方のサーバーが同じサーバークラスタの一部である場合は、片方のサーバーから別のサーバーへ言語設定をコピーすることができます。 子サーバーから子サーバー、親サーバーから子サーバー、または子サーバーから親サーバーへ言語設定をコピーすることができます。 サーバーから別のサーバーへポリシーをコピーするにはスーパーユーザーまたは管理者である必要があります。
言語設定をコピーするには、次の手順を実行します。
1. 親サーバー上で、**コンフィグレーション>システム設定>言語設定**へ移動します。
2. **ポリシーをコピー**をクリックします。**ポリシーをコピー**が表示されます。
3. 言語設定のコピー元となるサーバーを選択します。
4. 言語設定のコピー先となるサーバーを選択します。
5. 言語設定をコピーするには、**OK** をクリックします。

ロケーションタイムゾーンの設定

コンフィグレーション>システム設定>Location Specific Attributes ページを使用して、 選択したロケーションの適切なタイムゾーンを設定します。 タイムゾーンの設定は個々のロケーションに固有のものであり、親ロケーションから継承することはできません。 ロケーションに対してロケーションタイムゾーンを設定するには管理者権限が必要です。

タイムゾーンの設定は、正確な分析に役立ちます。 選択したロケーションの正確なタイムゾーンを選択してください。
ロケーションフロアは企業の建物内の 1 つのフロアロケーションを表現しますので、 タイムゾーンを 1 つのロケーションフロアに設定することができない点に注意してください。 ロケーションフロアの直接の親ロケーションフォルダーに設定されたタイムゾーンがロケーションフロアに適用されます。
ロケーションフォルダーにタイムゾーンを設定しない場合は、 アナリティクスデータのローカルタイムゾーンが表示されるフィールドにサーバーのタイムゾーンが表示されることになります。

タイムゾーンを設定

タイムゾーンを設定するには、次の手順を実行します。
1. **コンフィグレーション>システム設定>Location Specific Attributes** へ移動します。
2. タイムゾーンを設定したいロケーションを選択します。
3. タイムゾーンを選択します。
4. 新しいタイムゾーンを保存するには、**保存**をクリックします。 操作をキャンセルしたい場合は、**キャンセル**をクリックします。

タイムゾーンを編集

ロケーションのタイムゾーンを編集するには、次の手順を実行します。
1. **コンフィグレーション>システム設定>Location Specific Attributes** へ移動します。
2. タイムゾーンを編集したいロケーションを選択します。
3. 新しいタイムゾーンを選択します。
4. 新しいタイムゾーンを保存するには、**保存**をクリックします。 変更されたタイムゾーンは、再帰的にすべての子ロケーションフォルダーに同様に適用されます。

ロケーションタグの編集

ロケーションタグは、このロケーションで設定された SSID プロファイルで DHCP Option 82 が有効になっているときにサーキット ID に付加することができるロケーション識別子です。

サーキット ID で '%l 'が使用された場合、AP はそれをロケーションタグに置き換えます。

ロケーションにロケーションタグを設定するには、次の手順を実行します。
1. **コンフィグレーション>システム設定>Location Specific Attributes** へ移動します。
2. ロケーションタグを設定したいロケーションを選択します。
3. ロケーションタグを入力します。
4. 変更を保存するには、**保存**をクリックします。

ユーザー管理

管理コンソール(Management Console)のユーザーには 4 つのタイプがあります。スーパーユーザー、管理者、オペレータ、そしてビュアーです。
コンフィグレーション>ユーザーアカウント>ユーザー を介してユーザー関連の操作を管理することができます。 追加、編集、およびユーザーを削除することができます。 ユーザーの検索をすることができ、ロケーションで定義されるユーザーのリストを印刷することができます。

管理コンソール(Management Console)でユーザーを管理するためには管理者権限が必要です。

次の表は、管理コンソール(Management Console)の役割ごとの権限の詳細について説明します。

操作	**ユーザーの役割**			
	スーパーユーザー	管理者	オペレータ	ビュアー
ユーザーアカウントの管理				
ID と認証の設定と変更 （パスワード、証明書、証明書とパスワード、証明書またはパスワード)	Yes	No	No	No
ユーザーの追加と削除	Yes	No	No	No
任意のユーザーのプロパティを閲覧および変更（ユーザー管理画面）	Yes	No	No	No
パスワードの強度、アカウントのロックポリシー、同時セッション最大数を定義	Yes	No	No	No
ユーザー環境設定の表示と変更（電子メール、パスワード、セッションタイムアウト）	Yes (自身のみ)	Yes (自身のみ)	Yes (自身のみ)	Yes (自身のみ)
ユーザーのアクションの監査				
ユーザーのアクションの監査ログのダウンロード	Yes	No	No	No
ユーザーのアクションの監査ライフタイムを変更	Yes	No	No	No
システム設定と運用ポリシー				
システム設定と運用ポリシーを変更（ユーザー管理、ログ、ログイン設定以外の 管理者タブにあるすべての設定)	Yes	Yes	No	No
イベント、デバイス、ロケーション				
生成されたイベントの閲覧	Yes	Yes	Yes	Yes
生成されたイベントの変更と削除	Yes	Yes	Yes	No
デバイスの閲覧	Yes	Yes	Yes	Yes
デバイスの追加、削除、変更（AP、クライアント、センサー)	Yes	Yes	Yes	No
ロケーションの閲覧	Yes	Yes	Yes	Yes
ロケーションの追加、削除、変更	Yes	Yes	Yes	No
ロケーショントラッキングの校正	Yes	Yes	Yes	No
レポート				
共有レポートの追加、削除、変更	Yes (すべて)	Yes (自身作成分だけ)	Yes (自身作成分だけ)	No
共有レポートの生成	Yes	Yes	Yes	Yes
共有レポートのスケジュール	Yes	Yes	Yes	No
マイレポートの追加、削除、変更、生成、スケジュール	Yes (自身作成分のみ)	Yes (自身作成分だけ)	Yes (自身作成分だけ)	No

ユーザーの追加

ユーザーを追加するには、次の手順を実行します。
1. **コンフィグレーション>ユーザーアカウント>ユーザー**へ移動します。
2. ユーザーを追加したいロケーションを選択します。
3. **ユーザーの追加**をクリックします。新規ユーザーの追加・ダイアログボックスが表示されます。

次の表は、**新規ユーザーの追加**ページのフィールドについて説明します。

フィールド	説明
ユーザータイプ	ユーザーのタイプを指定します。
ログイン ID	ユーザーのログイン ID を指定します。
役割	ユーザーに割り当てる役割を指定します。 ビュアー、オペレータ、管理者とスーパーユーザーから選択します。
ファーストネーム	ユーザーの名を指定します。
ラストネーム	ユーザーの姓を指定します。
パスワード	ユーザーのパスワードを指定します。
パスワードの確認	パスワードを確認するために パスワードフィールドに入力したのと同じパスワードを指定します。
電子メール	ユーザーのメールアドレスを指定します。
許可されたロケーション	ユーザーが操作可能なロケーションを指定します。 許可されたロケーションのリストを修正するには、**変更**をクリックします。 ユーザーは 1 つ以上のロケーションで操作することができます。 例えば管理者ユーザーは、複数のロケーションへのアクセス権を持つことが可能です。
パスワード有効期限	パスワードが期限切れになるか、期限切れにならないかを指定します。 デフォルトで、パスワードは無期限です。パスワードの期限を設定するには、 **変更**をクリックします。
パスワード有効期間	パスワードの変更時刻から パスワードが有効期限になる日数を指定します。
パスワード有効期限切れ警告	パスワード満了の前に ユーザーにパスワードを変更することを促す日を指定します。
セッションタイムアウト	ユーザーの現在開いているブラウザ画面とのセッションが、 タイムアウトするまでのアイドル時間間隔を指定します。セッションタイムアウトしたくない場合には**無期限** を選択します。 有効期限を選択してセッションがタイムアウトする時間(10 から 120 分)を指定します。
タイムゾーン	ユーザーが操作するタイムゾーンを指定します。
言語設定	ユーザーが UI のテキストを表示したい言語を指定します。 デフォルト値は日本語です。
多言語	UI が多言語フォントサポートを サポートしているかどうかを指定します。

4. 変更を保存するには、**保存**をクリックします。

ユーザーの編集

ユーザーを編集するには、次の手順を実行します。
1. **コンフィグレーション>ユーザーアカウント>ユーザー**へ移動します。
2. ユーザーを編集したいロケーションを選択します。
3. 編集したいユーザーのログイン ID をクリックします。**ユーザーの詳細を編集**が表示されます。
4. ユーザーの詳細を編集します。
5. 変更を保存するには、**保存**をクリックします。

ロケーションのユーザーリストを印刷

ロケーションに対して定義されたユーザーリストを印刷することができます。

ロケーションのユーザーリストを印刷するには、次の手順を実行します。
1. **コンフィグレーション>ユーザーアカウント>ユーザー**へ移動します。
2. ユーザーリストを印刷したいロケーションを選択します。
3. 印刷されるリストにしたい列を選択します。選択または列の選択を解除するには、任意の列名をクリックします。
4. 印刷アイコンをクリックします。ユーザーリストの印刷プレビューが表示されます。
5. リストを印刷するには、**印刷**をクリックします。

ユーザーの検索

ユーザーのログイン ID または名前を使用してユーザーを検索することができます。

ユーザーを検索するには、次の手順を実行します。
1. **コンフィグレーション>ユーザーアカウント>ユーザー**へ移動します。
2. ユーザーを検索したいロケーションを選択します。
3. クイックサーチボックス内にログイン ID 文字列または名前の文字列を入力してください。
4. Enter キーを押します。
5. 検索文字列に一致するログイン ID または名前を持つユーザーが表示されます。 検索文字列は、ログイン ID またはユーザーの名前の一部にすることも可能です。

ユーザーの削除

ユーザーを削除するには、次の手順を実行します。
1. **コンフィグレーション>ユーザーアカウント>ユーザー**へ移動します。
2. ユーザーを削除したいロケーションを選択します。ユーザーリストが表示されます。
3. 削除するユーザーの**削除**をクリックします。削除を確認するメッセージが表示されます。
4. ユーザーの削除を実行するには、**Yes** をクリックします。

パスワードポリシーの設定

パスワードポリシーは、システムパスワードの最低要件を決定します。 このポリシーは、すべてのユーザーの役割（スーパーユーザー、管理者、オペレータ、およびビュアー）に適用されます。 このポリシーを変更しても以前のパスワードは影響を受けません。 ポリシーの変更後に作成されたパスワードにのみ、新しいポリシーが適用されます。 この設定は、ローカル認証にのみ適用され、LDAP および RADIUS 認証には適用されません。

サーバーが同じサーバークラスタの一部である場合は、サーバーから別のサーバーにパスワードポリシーをコピーすることができます。

パスワードポリシーを設定するには、次の手順を実行します。
1. **コンフィグレーション>ユーザーアカウント>パスワードポリシー**に移動します。
2. パスワードに必要な文字数を指定します。最小文字数は 4、最大文字数は 15 です。
3. パスワードに少なくとも 1 つの数字を含む必要がある場合は、少なくとも 1 つの数字が必要のチェックボックスにチェックを入れます。
4. パスワードに少なくとも 1 つの特殊文字を含む必要がある場合は、少なくとも 1 つの特殊文字が必要のチェックボックスにチェックを入れます。
5. ページに加えた変更を保存するには、**保存**をクリックします。

デフォルトのパスワードポリシーへ戻す

デフォルトのパスワードポリシーは以下のとおりです。
パスワードの長さは 6 文字でパスワードに数値や特殊文字を含む必要はありません。

パスワードポリシーをデフォルトに戻すには、次の手順を実行します。
1. **コンフィグレーション>ユーザーアカウント>パスワードポリシー**に移動します。
2. デフォルトのパスワードポリシーへ戻すには、**デフォルト値に戻す**をクリックします。
3. 変更を保存するには、**保存**をクリックします。

パスワードポリシーを別のサーバーへコピー

両方のサーバーが同じサーバークラスタの一部である場合は、片方のサーバーから別のサーバーへパスワードポリシーをコピーすることができます。 子サーバーから子サーバー、親サーバーから子サーバー、または子サーバーから親サーバーへパスワードポリシーをコピーすることができます。

サーバーから別のサーバーへポリシーをコピーするにはスーパーユーザーまたは管理者である必要があります。

パスワードポリシーをコピーするには、次の手順を実行します。
1. 親サーバー上で、**コンフィグレーション>ユーザーアカウント>パスワードポリシー**に移動します。
2. **ポリシーをコピー**をクリックします。 **ポリシーをコピー**が表示されます。
3. パスワードポリシーのコピー元となるサーバーを選択します。
4. パスワードポリシーのコピー先となるサーバーを選択します。
5. パスワードポリシーをコピーするには、**OK** をクリックします。

アカウント停止設定を構成

アカウントの停止は、辞書攻撃を行った可能性のある偽のログインからシステムを保護します。 **コンフィグレーション>ユーザーアカウント>アカウント停止** を使用して、 アカウントの停止ポリシーを定義します。 システムには利用可能な 4 つの役割（スーパーユーザー、管理者、ビュアーとオペレータ）があります。 これらのユーザーの役割ごとに異なるポリシーを設定できます。 停止時間（分単位）と特定の時間内のログイン失敗回数を設定します。

サーバーが同じサーバークラスタの一部である場合は、サーバーから別のサーバーにアカウント停止設定をコピーできます。

ユーザーの役割に対してアカウント停止設定を構成するには、次の手順を実行します。
1. **コンフィグレーション>ユーザーアカウント>アカウント停止**に移動します。
2. 連続してログイン試行が失敗したときに、5 分から 30 分の停止時間を指定します。
3. 3 から 10 回までのログイン試行の失敗回数を指定します。
   例えば 3 と指定すると、3 回までログイン試行をリトライすることが可能で、4 回目のログイン試行に失敗するとアカウントが停止します。
4. ページに加えた変更を保存するには、**保存**をクリックします。

このポリシーは、ルートロケーションでのみ適用可能です。

アカウント停止設定を別のサーバーへコピー

両方のサーバーが同じサーバークラスタの一部である場合は、片方のサーバーから別のサーバーへアカウント停止設定をコピーすることができます。 子サーバーから子サーバー、親サーバーから子サーバー、または子サーバーから親サーバーへアカウント停止設定をコピーすることができます。 サーバーから別のサーバーへポリシーをコピーするにはスーパーユーザーまたは管理者である必要があります。

アカウント停止設定をコピーするには、次の手順を実行します。
1. 親サーバーの**コンフィグレーション>ユーザーアカウント>アカウント停止**に移動します。
2. **ポリシーをコピー**をクリックします。 **ポリシーをコピー**が表示されます。
3. アカウント停止設定のコピー元となるサーバーを選択します。
4. アカウント停止設定のコピー先となるサーバーを選択します。
5. アカウント停止設定をコピーするには、**OK** をクリックします。

ログインパラメータの設定

管理コンソール(Management Console)にログオンする際にユーザーに表示するウエルカムメッセージとともに、 1 つのユーザーが持つことができる同時コンソール・ログインの数を指定できます。 ユーザーは、最大 5 つの同時コンソール・ログインを持つことができます。
ログインパラメータを設定するには管理者権限が必要です。

サーバーが同じサーバークラスタの一部である場合は、サーバーから別のサーバーにログインパラメータの設定をコピーすることができます。

ログインパラメータを設定するには、次の手順を実行します。
1. **コンフィグレーション>システム設定>ログインコンフィグレーション**に移動します。
2. **ログインメッセージの設定**で、ログイン画面でユーザーに表示するメッセージを入力します。
3. ログイン画面へのメッセージ表示を有効にするには、**ログインメッセージを有効**のチェックボックスにチェックを入れます。
4. ユーザーごとの同時セッション数を指定します。
5. 設定を保存するには、**保存**をクリックします。

ログイン設定をデフォルトに戻す

ログイン設定をデフォルトに戻すには、次の手順を実行します。
1. **コンフィグレーション>システム設定>ログインコンフィグレーション**に移動します。
2. デフォルト値に戻すをクリックします。デフォルト設定が復元されます。
3. 変更を保存するには、**保存**をクリックします。

ログイン設定を別のサーバーへコピー

両方のサーバーが同じサーバークラスタの一部である場合は、片方のサーバーから別のサーバーへログイン設定をコピーすることができます。 子サーバーから子サーバー、親サーバーから子サーバー、または子サーバーから親サーバーへログイン設定をコピーすることができます。 サーバーから別のサーバーへポリシーをコピーするにはスーパーユーザーまたは管理者である必要があります。

ログイン設定をコピーするには、次の手順を実行します。
1. 親サーバー上で、**コンフィグレーション>システム設定>ログインコンフィグレーション**に移動します。
2. **ポリシーをコピー**をクリックします。 **ポリシーをコピー**が表示されます。
3. ログイン設定のコピー元となるサーバーを選択します。
4. ログイン設定のコピー先となるサーバーを選択します。
5. ログイン設定をコピーするには、**OK** をクリックします。

ユーザー認証

LDAP サーバーのパラメータ設定

管理コンソール(Management Console)は、ユーザー認証のために LDAP サーバーを設定することができます。 LDAP サーバー設定後、LDAP サーバーで定義されたユーザーまたはグループは、管理コンソール(Management Console)にログインすることができます。

LDAP コンフィグレーションでは、次の詳細を設定できます。
- LDAP 準拠のディレクトリにアクセスできるようにするための LDAP コンフィグレーションパラメータ
- LDAP サーバー上のレコードを検索するための LDAP 認証情報
- LDAP ユーザーの権限 - ここでは、LDAP サーバーによって役割やロケーション属性が提供されていない場合のために、 新規の LDAP ユーザーがログインするときに割り当てるデフォルトの役割とロケーション属性を指定します。 ここのデフォルト値は、LDAP を介して認証されるすべてのユーザーに適用されることに注意してください。 LDAP サーバーが認証時にユーザーの役割とロケーション属性を提供する場合は、LDAP サーバーで提供される属性はデフォルトの役割とロケーション属性をオーバーライドします。

LDAP サーバーのアクセスパラメータを設定するには、管理者権限を持っている必要があります。

LDAP サーバーのアクセスパラメータを設定するには、次の手順を実行します。
1. **コンフィグレーション>ユーザーアカウント>LDAP コンフィグレーション**に移動します。
2. LDAP 準拠のディレクトリを使用してユーザー認証を有効にするには、**LDAP 認証を有効**を選択します。 LDAP に関連するすべてのフィールドはこのチェックボックスにチェックを入れると有効になります。

3. 以下のテーブルに記載される接続の詳細を入力します。

フィールド	説明
Primary Server IP Address/Hostname	LDAP サーバーのプライマリ・サーバーの IP アドレス/ホスト名です。
(Primary Server) Port	LDAP サーバーのプライマリ・サーバーのポート番号です。(デフォルト：389)
Backup Server IP Address/Hostname	LDAP サーバーのバックアップ・サーバーの IP アドレス/ホスト名です。
(Backup Server) Port	LDAP サーバーのバックアップ・サーバーのポート番号です。
Enforce Use of SSL/TLS	このオプションをオンにすると、LDAP サーバーへは SSL/TLS 接続のみが許可されます。 チェックされていない場合には、LDAP サーバーへは Open または SSL/TLS 接続のいずれかが許可されます。
Verify LDAP Server's Certificate	このオプションを選択すると、証明書のチェックにパスしない限り、LDAP サーバーへの接続が許可されません。 このオプションが選択されていない場合は、LDAP サーバーへの接続は LDAP サーバー証明書を検証することなく許容されます。

4. **Verify LDAP Server's Certificate** を選択した場合は、証明書を追加する必要があります。 LDAP サーバーの信頼されたルート CA 証明書を追加するには**証明書の追加**をクリックし、証明書を選択します。
5. 以下のテーブルに記載される LDAP コンフィグレーションの詳細を入力します。

フィールド	説明
Base Distinguished Name	接続先となるディレクトリのベース識別名です。（例）o=democorp, c=au。 識別名は、ディレクトリ情報ツリー（DIT）内のエントリの一意の識別子です。 名前は、DIT ダウンの先頭から該当のエントリまでの相対識別名（RDN）を連結したものです。
Filter String	これは必須の引数です。 これは、LDAP サーバーがユーザーをフィルターするために使用するための、（既存または新規）属性を指定する文字列です。 例えば、IsUser=A。フィルター文字列を指定することによって、AD 内の特定 OU または利用者定義のグループにログイン・アクセスを許可または禁止することができます。 そのグループのメンバーである人だけにアクセスできるようにするために、任意の特定のグループの DN を（名前を区別）を指定することができます。 （例）memberOf=DC=GroupName,DC=Com。 OR 条件を用いて複数のグループのメンバーを含むことができます。 例えば、Admins OR Reviewer の 2 つのグループの任意のメンバーへ Base DN 下でアクセスをユーザーに許可するには、以下のフィルター文字列を含む必要があります: (|(memberOf=CN=Admins,DC=GroupName,DC=Com)(memberOf=CN=Reviewer,DC=GroupName,DC=Com)) 同様に、 Admins and Reviewer の両方のメンバーへ Base DN 下でアクセスをユーザーに許可するには、以下のフィルター文字列を含む必要があります: (&(memberOf=CN=Admins,DC=GroupName,DC=Com)(memberOf=CN=Reviewer,DC=GroupName,DC=Com)) アクセス権が付与された AD 内のユーザーに新たな属性(ATNWIFI)を追加するなどの AD の代替の構成を持つことが可能です。 （例）フィルター文字列 = ATNWIFI また、付与されたアクセス権を持つ AD のユーザーの新しいグループを作成し、フィルター文字列でグループを含めることができます。 使用できる最も一般的なフィルター文字列は '`objectClass=*`'です。任意の LDAP エントリをフィルターしたくないときは、この文字列を使用することができます。
User ID Attribute	システムがユーザーを識別するために使用する LDAP スキーマーで定義される文字列。(デフォルト: cn)

6. ディレクトリが匿名検索を許可していない場合は、LDAP 準拠のディレクトリを検索するために、ユーザーの資格情報を設定する必要があります。次の表に示すように、ユーザーの資格情報を設定します。

フィールド	説明
Admin User DN	LDAP サーバーへの認証に使用する管理ユーザーの DN。
Append Base DN	LDAP コンフィグレーションの詳細で指定された Base DN を管理ユーザーDN に追加する必要がある場合は、このオプションを選択します。
Password	管理ユーザーのパスワード。

7. 認証オプションをテストするには、**設定のテスト**をクリックします。
8. 新規の LDAP ユーザーのデフォルトの役割とロケーションを設定します。これらを、次の表に示します。

フィールド	説明
User Role Attribute	ユーザーの役割（LDAP スキーマーで定義される）を識別するために、システムが使用するユーザーの役割属性文字列。
User Role	新規の LDAP ユーザーのデフォルトの役割。 次の 4 つのうち 1 つを選択することが可能（スーパーユーザー、管理者、オペレータ、ビュアー）。
User Location Attribute	ユーザーがアクセスを許可されたロケーション（LDAP スキーマーで定義される）を識別するために、システムが使用するユーザーのロケーション属性文字列。
Locations	新規の LDAP ユーザーがアクセス権を持つロケーション。 **変更**をクリックすることで、別のロケーションを選択することが可能。

9. 変更を保存するには、**保存**をクリックします。

LDAP サーバーのアクセスパラメータを編集

LDAP サーバーのアクセスパラメータを編集するには、次の手順を実行します。
1. **コンフィグレーション>ユーザーアカウント>LDAP コンフィグレーション**に移動します。
2. 必要な変更を行います。
3. 接続設定や構成設定を変更した場合は、新しい設定が有効であることを確認するために**設定のテスト**をクリックします。
4. 変更を保存するには、**保存**をクリックします。

LDAP コンフィグレーションを別のサーバーへコピー

両方のサーバーが同じサーバークラスタの一部である場合は、片方のサーバーから別のサーバーへ LDAP コンフィグレーションをコピーできます。 子サーバーから子サーバー、親サーバーから子サーバー、または子サーバーから親サーバーへ LDAP コンフィグレーションをコピーできます。 サーバーから別のサーバーへポリシーをコピーするにはスーパーユーザーまたは管理者である必要があります。

ご注意：LDAP コンフィグレーションが別のサーバーにコピーされると、転送先サーバーで複製されたポリシー内のロケーションフィールドの値は 'root'（ロケーション）に設定されます。

LDAP コンフィグレーションをコピーするには、次の手順を実行します。
1. 親サーバー上で**コンフィグレーション>ユーザーアカウント>LDAP コンフィグレーション**に移動します。
2. **ポリシーをコピー** をクリックします。 **ポリシーをコピー**ダイアログボックスが表示されます。
3. LDAP コンフィグレーションのコピー元となるサーバーを選択します。
4. LDAP コンフィグレーションのコピー先となるサーバーを選択します。
5. LDAP コンフィグレーションをコピーするには、**OK** をクリックします。

RADIUS パラメータの設定

管理コンソール(Management Console)は、ユーザー認証を容易にするために、RADIUS サーバーを使用することができます。 **コンフィグレーション>ユーザーアカウント>RADIUS コンフィグレーション** を使用して、RADIUS サーバーへのアクセスパラメータを設定します。

ユーザーの RADIUS 認証をアクティブにするために、**RADIUS 認証の有効** チェックボックスにチェックを入れます。 このチェックボックスにチェックを入れたあとに、認証、アカウンティング、および詳細設定を行うことができます。 各セクションのフィールドを表示および編集するために、それぞれのオプションをクリックします。

認証パラメータの設定

認証セクションを使用して RADIUS 認証サーバーのアクセスパラメータを設定します。

RADIUS 認証サーバーのアクセスパラメータを設定するには、次の手順を実行します。
1. **コンフィグレーション>ユーザーアカウント>RADIUS コンフィグレーション**に移動します。
2. プライマリおよび(または)セカンダリ RADIUS サーバーの IP アドレス/ホスト名、ポート番号、および共有シークレットを指定します。
3. RADIUS サーバーへの接続をテストするために**テスト**をクリックします。
4. RADIUS を使用して CLI ユーザーを認証するには、CLI ログイン用の RADIUS サーバーインテグレーションを有効を選択します。
5. RADIUS を使用して GUI ユーザーを認証するには、GUI ログイン用の RADIUS サーバーインテグレーションを有効を選択します。
6. 適切なベンダー固有の属性を選択します。ベンダー固有属性が RADIUS サーバー用に定義されていないときに、これらが使用されます。
7. 変更を保存するには、**保存**をクリックします。

アカウンティングパラメータの設定

アカウンティングセクションを使用して RADIUS アカウンティングサーバーのアクセスパラメータを設定します。

RADIUS 認証サーバーのアカウンティングパラメータを設定するには、次の手順を実行します。
1. **コンフィグレーション>ユーザーアカウント>RADIUS コンフィグレーション**に移動します。
2. RADIUS アカウンティングを有効にするには、**RADIUS アカウンティングを有効**を選択します。
3. プライマリおよび(または)セカンダリアカウンティングサーバーの IP アドレス/ホスト名、ポート番号そして共有シークレットを指定します。
4. 変更を保存するには、**保存**をクリックします。

詳細設定

詳細設定セクションを使用して CLI および GUI ユーザーのための領域（ドメイン）を設定します。また、実際の名前がユーザー名（プレフィックス表記または後置記法）に追加する方法を指定することができます。 プレフィックス表記を使用するには、 **プレフィックス表記を使用**のチェックボックスにチェックを入れます。 このチェックボックスが選択されていない場合は、後置記法が使用されます。

詳細設定を行うには、次の手順を実行します。
1. **コンフィグレーション>ユーザーアカウント>RADIUS コンフィグレーション**に移動します。
2. CLI で CLI ユーザーのレルムを入力します。
3. GUI で GUI ユーザーのレルムを入力します。
4. プレフィックス表記を使用するには、**プレフィックス表記を使用**チェックボックスにチェックを入れます。 このチェックボックスが選択されていない場合は後置記法が使用されます。
5. 変更を保存するには、**保存**をクリックします。

デフォルト設定に戻す

デフォルトでは、RADIUS 認証が無効になっています。このデフォルト設定を復元するには、次の手順を実行します。
1. **コンフィグレーション>ユーザーアカウント>RADIUS コンフィグレーション**に移動します。
2. **デフォルト値に戻す**をクリックします。
3. 変更を保存するには、**保存**をクリックします。

RADIUS コンフィグレーションを別のサーバーへコピー

両方のサーバーが同じサーバークラスタの一部である場合は、片方のサーバーから別のサーバーへ RADIUS コンフィグレーションをコピーすることができます。 子サーバーから子サーバー、親サーバーから子サーバー、または子サーバーから親サーバーへ RADIUS コンフィグレーションをコピーできます。 サーバーから別のサーバーへポリシーをコピーするにはスーパーユーザーまたは管理者である必要があります。

ご注意：RADIUS コンフィグレーションが別のサーバーにコピーされると、転送先サーバーで複製されたポリシー内のロケーションフィールドの値は 'root'（ロケーション）に設定されます。

RADIUS コンフィグレーションをコピーするには、次の手順を実行します。
1. 親サーバー上で**コンフィグレーション>ユーザーアカウント>RADIUS コンフィグレーション**に移動します。
2. **ポリシーをコピー**をクリックします。 **ポリシーをコピー**が表示されます。
3. RADIUS コンフィグレーションのコピー元となるサーバーを選択します。
4. RADIUS コンフィグレーションのコピー先となるサーバーを選択します。
5. RADIUS コンフィグレーションをコピーするには、**OK** をクリックします。

証明書ベースの認証パラメータを設定

管理コンソール(Management Console)は、デジタル証明書を使用したユーザー認証をサポートしています。 **コンフィグレーション>ユーザーアカウント>証明書の設定**を使用して、ユーザー認証のための設定を行います。

ユーザーを認証する 4 つの方法があります（パスワードのみ、証明書のみ、証明書とパスワード、証明書またはパスワード）。

パスワードのみ: このオプションでは、ユーザー認証は、パスワードを用いて行われます。 ユーザーは、ログインプロンプトでユーザー名とパスワードを入力する必要があります。 パスワードは、ローカルでシステムによって検証されるか、または必要に応じて外部 LDAP または RADIUS 認証サービスを使用して検証することがでます。

証明書のみ：このオプションでは、ユーザー認証は、クライアント証明書（例えば、スマートカード）を用いて行われます。 ユーザーはコンソールにアクセスする場所でコンピューターに接続されているリーダーにクライアント証明書を含むスマートカードを挿入し、 **ログイン**ボタンを押す必要があります。 次に、システムはクライアント証明書を検証し、証明書からユーザー識別情報（ユーザー名）を取得します。 ユーザーの他の属性は、必要に応じてローカルまたは LDAP や RADIUS などの外部認証サービスから取得されます。

証明書とパスワード: このオプションでは、クライアント証明書とパスワードの両方がユーザー認証のために必要とされます。 ユーザーがコンソールにアクセスすると、そこからコンピューターに接続されたリーダーにクライアント証明書を含むスマートカードを挿入し、 ログインプロンプトでパスワードを入力する必要があります。 システムは、ローカルでまたは必要に応じて外部 LDAP または RADIUS 認証サービスを使用してパスワードを検証します。

証明書またはパスワード： このオプションでは、ユーザー認証は、パスワードまたはクライアント証明書のどちらかを使用して許可されます。 このオプションは、一部でしか認証にスマートカードを使用していない企業に適しています。 ログインプロンプトで、ユーザーは、ログインボックスの証明書の使用をチェックすることで、 証明書認証かもしくはログイン名とパスワードを入力してパスワード認証を継続するかを選択することができます。

要求される認証は、 **証明書ベースの認証を有効**ボックス、 **証明書なしのでアクセスを許可**ボックス、 **ユーザーは、証明書に加えてパスワードを提供が必要**ボックス、 の多様な組み合わせに基づいてアクティベイトされることが可能です。
次の表は、ユーザーが選択したチェックボックスに基づいて認証オプションのアクティベイトを説明しています。

アクティベイトするための認証	**選択されたチェックボックス**		
	証明書ベースの認証を有効	*証明書なしのでアクセスを許可*	*ユーザーは、証明書に加えてパスワードの提供が必要*
パスワードのみ	No	-	-
証明書のみ	Yes	No	No
証明書とパスワード	Yes	No	Yes
証明書またはパスワード	Yes	Yes	No

ご注意： 証明書ベースの認証を使用するためには、GUI ホストが TCP ポート 4433 でサーバーにアクセスできることが必要です。 GUI ホストとサーバー間にファイアウォールが存在する場合は、ホストからサーバーへのポート 4433 を開く必要があります。
証明書のみ、*証明書とパスワード*、*証明書またはパスワード*のいずれかをアクティブにすると、次のような追加の詳細を提供する必要があります。

- ユーザーの識別情報が管理コンソール(Management Console)によって取得することが可能なクライアント証明書内のフィールド。
- クライアント証明書の検証を容易にするためのルート CA 証明書。
- 証明書の失効をチェックする好ましい方法。

証明書設定をデフォルトに戻す

デフォルトでは、証明書ベースの認証が無効になっています。
このデフォルト値を復元するには、次の手順を実行します。
1. **コンフィグレーション>ユーザーアカウント>証明書の設定**に移動します。
2. **デフォルト値に戻す**をクリックします。
3. 変更を保存するには、**保存**をクリックします。

証明書設定を別のサーバーへコピー

両方のサーバーが同じサーバークラスタの一部である場合は、片方のサーバーから別のサーバーへ証明書設定をコピーすることができます。 子サーバーから子サーバー、親サーバーから子サーバー、または子サーバーから親サーバーへ証明書設定をコピーすることができます。 サーバーから別のサーバーへポリシーをコピーするにはスーパーユーザーまたは管理者である必要があります。
証明書設定をコピーするには、次の手順を実行します。
1. 親サーバー上で**コンフィグレーション>ユーザーアカウント>証明書の設定**に移動します。
2. **ポリシーをコピー**をクリックします。 **ポリシーをコピー**が表示されます。
3. 証明書設定のコピー元となるサーバーを選択します。
4. 証明書設定のコピー先となるサーバーを選択します。
5. 証明書設定をコピーするには、**OK** をクリックします。

無線侵入防御システム（WIPS）

Wi-Fi ネットワークは、アクセスポイントを介して簡単にセットアップすることができます。小さなプラグアンドプレイデバイスは、アクセスポイントとして機能することができます。現在では広く使用されているスマートフォンやタブレットにも Wi-Fi が有効になっています。それらは、モバイルホットスポットとして機能することができます。 クライアントは、そのようなアクセスポイントに接続し、容易に企業のネットワークにアクセスすることができます。ネットワークに接続するアクセスポイントの容易さのために、機密データが簡単に危険にさらされることになるため、ネットワークへの許可そして非許可アクセスについて理解し制御することが重要です。

適切な無線侵入防御（WIPS）ポリシーは、ネットワークへの不正アクセスを防止する場所に必要です。 ネットワークへの無線侵入防御のためのルールは、**コンフィグレーション>WIPS** を使用して設定できます。
コンフィグレーション>WIPS にあるオプションを使用して WIPS のルールを設定することができます。

管理コンソール(Management Console)は、組織内のすべてのロケーションに対して一般的な WIPS ポリシー、または個々のロケーションごとの WIPS ポリシーを設定するための柔軟性を提供します。いくつかのロケーションで WIPS をアクティブにし、その他のロケーションでは非アクティブにすることが可能です。

WIPS の設定を行う前に、ロケーションツリーを定義していることを確認してください。
WIPS の設定を行うには管理者権限が必要です。

コンフィグレーション>WIPS>許可された WLAN ポリシー を使用して、許可 AP を識別するために許可された WLAN ポリシーテンプレートを指定します。 これは、親ロケーションからデフォルトで継承されます。 また、ロケーションに合わせて変更することができます。

コンフィグレーション>WIPS>AP の自動分類 を使用して、システムによって検出された AP を自動的に分類するポリシーを設定します。 これは、親ロケーションからデフォルトで継承されます。 また、ロケーションに合わせて変更することができます。

コンフィグレーション>WIPS>クライアントの自動分類 を使用して、システムによって検出されたクライアントを自動的に分類するポリシーを設定します。 これは、親ロケーションからデフォルトで継承されます。 また、ロケーションに合わせて変更することができます。

コンフィグレーション>WIPS>侵入防御 を使用して、侵入防御ポリシーを定義します。 これは、親ロケーションからデフォルトで継承されます。 また、ロケーションに合わせて変更することができます。

コンフィグレーション>WIPS>侵入防御の有効化 を使用して、侵入防止を有効または無効にします。これは、ロケーション固有のものです。 最初にロケーションツリーから目的のロケーションを選択する必要があります。 そのあと、このロケーションに対して侵入防止を有効または無効にする **侵入防御の有効化**を使用します。

コンフィグレーション>WIPS>デバイスのインポート を使用して、AP/クライアント分類について参照可能なデバイスリストをインポートします。 これは、ロケーション固有のものです。 最初にロケーションツリーから目的のロケーションを選択する必要があります。 そのあと、このロケーションに対してデバイスをインポートするために **デバイスのインポート**を使用します。

コンフィグレーション>WIPS>デバイスリストのロックを使用して、ロケーションの許可 AP および(または)クライアントのリストをロックすることができます。
コンフィグレーション>WIPS>禁止されたデバイスリストを指定して禁止されたデバイスリストを管理することができます。

コンフィグレーション>WIPS>詳細設定>スマートデバイスタイプを使用してスマートデバイスの検出に使用されるスマートデバイスの種類を管理できます。

コンフィグレーション>WIPS>詳細設定>ホットスポット SSID を使用してホットスポットの SSID リストを管理することができます。

コンフィグレーション>WIPS>詳細設定>脆弱な SSID を使用して脆弱な SSID リストを管理することができます。

許可された **WLAN** ポリシーの管理

コンフィグレーション>WIPS>許可された WLAN ポリシーで、 ロケーション階層で選択されたロケーションの許可された WLAN ポリシーテンプレートを指定します。

ロケーションに対する認可された WLAN ポリシーは、1 つ以上の許可された無線ネットワークのプロパティを定義する 1 つ以上のポリシーテンプレートのセットが含まれています。 ポリシーテンプレートは、異なるネットワーク関連の設定（例えば、無線ネットワークプロトコル、使用される暗号化プロトコル、許可されたネットワーク SSID、セキュリティ設定、使用される認証タイプ、許可されたネットワークなど）の 1 つの集合です。 また許可された WLAN ポリシーは、ネットワークがそれらの上で Wi-Fi AP を持つことを制限されるかどうかを示しています。 更に、AP を RSSI 信号強度に基づき不正または許可 AP(Authorized AP)に分類するべきかについて指定することも可能です。 これらのすべてのパラメータは、許可された WLAN をポリシーで一緒に構成します。

デバイスの RSSI は、統計的なパラメータです。 したがって、本機能を使うと、自動防御が有効になっている場合は正当な近隣のクライアントが Rogue と分類され閉じ込めを受ける原因になることがありえます。 それらがシステムの適用範囲内にあるとき不正（Rogue）として分類されたクライアントは、他の AP やクライアントに接続することができないので、これは近接する Wi-Fi の混乱を引き起こす原因となります。
たとえ目的が施設内にある AP を識別するために RSSI を使用することであるとしても、それは低出力 AP（例えばソフト AP、スマートフォン上で動作するホットスポット AP、USB AP など）では正しく動作しない、あるいは、RSSI 測定ポイントから離れたところにある AP は RSSI スレッショルドを満たさないため不正 AP(Rogue AP)として分類されません。

ポリシーテンプレートは、AP の分類を支援します。 新規の AP または既存の許可 AP(Authorized AP)は、それが不正または誤設定された AP であるか否かを決定するためにテンプレートと比較されます。 ロケーションのいかなる AP も、そのロケーションに設定した WLAN ポリシーに準拠していない場合は許可 AP(Authorized AP)とはみなされません。

そのロケーションで WLAN ポリシーの使用可能なリストからテンプレートを適用する必要があります。

許可 AP(Authorized AP)を識別し、許可 AP(Authorized AP)上で提供される実際の Wi-Fi アクセスパラメータがセキュリティポリシーを満たすことを常に確認するために、許可されたポリシーテンプレートは使用されます。 複数の WLAN ポリシーテンプレートを定義し、各々のロケーションにそれらを割り当てることができます。 ロケーションに追加されるいかなる新規の AP も、そのロケーションに設定される WLAN ポリシーテンプレートに基づいて検証されます。 いかなるミスマッチも Wi-Fi アクセスネットワークの設定ミスを検出するために使用されます。

システムは、ネットワーク内の設定ミスや不正 AP の存在を検出するために、特定のロケーションで許可された Wi-Fi セットアップに関する詳細情報を使用します。
AP は、以下の場合に許可された WLAN ポリシーに準拠していると考えられます。

- そのロケーションの No Wi-Fi ネットワークに接続されていない
- そのロケーションで設定されるテンプレートの 1 つと SSID が一致している
- そのテンプレートで指定されたネットワークのいずれかに接続されている
- そのテンプレート内の他の設定と一致している（この設定は AP 自体のプロパティではないように、認証フレームワークを除くバックエンド認証システム）

ご注意： テンプレートで特定の許可 AP の機能（例えば Turbo、IEEE802.11n など）を指定した場合は、AP がその機能を持っている必要があります。特定の機能を指定しない場合は、'Any'を選択してください。

ロケーションベースのポリシーを使用すると、異なるロケーションでポリシーテンプレートの異なるセットを適用することができます。 ただし、任意の 1 つのロケーションで同じ SSID を持つ複数のテンプレートを設定することはできません。

ロケーションに適用されるポリシーテンプレートのみが、そのロケーションで AP 分類のために使用されます。 そのロケーションに適用されていない他のテンプレートは、そのロケーションの WLAN ポリシーの要素ではないため AP の分類に使用されることはありません。

他のロケーションで作成された許可されたポリシーテンプレートを選択したロケーションに適用することができますが、編集や削除することはできません。 編集や削除の操作は、テンプレートが作成されたロケーションでのみ可能です。

子ロケーションは自動的にその親から許可された WLAN ポリシーを継承します。 子ロケーションの WLAN ポリシーを変更することができます。 また、変更したポリシーを作成した場合、継承されたポリシーに切り替えることもできます。

許可された WLAN ポリシーを設定

ロケーションの許可された WLAN ポリシーを設定するには、次の手順を実行します。

1. ロケーションツリーからロケーションを選択します。
2. **コンフィグレーション>WIPS>許可された WLAN ポリシー**へ移動します。
3. ロケーションに Wi-Fi がすでに配置されている場合は、**Wi-Fi が、このロケーションで配置されている**チェックボックスを選択します。 このページ上の**ポリシーテンプレート**と**"No Wi-Fi" ネットワークの選択**は、このチェックボックスを選択することで有効になります。
4. 既存のポリシーテンプレートを使用する場合は、既存のポリシーテンプレートをロケーションに適用するために適用アイコンをクリックします。 既存のポリシーテンプレートがなく、新規のポリシーテンプレートを追加する場合は、**新しいポリシーテンプレートを追加**をクリックします。 ポリシーテンプレートの追加や編集方法の詳細については、ポリシーテンプレートの管理セクションを参照してください。
5. ロケーションに接続された AP を持つことが許可されていない任意のネットワークが存在する場合、
   (a) **"No Wi-Fi" ネットワークの選択** セクションまでスクロールダウンします。
   (b) **追加**をクリック。 **No Wi-Fi ネットワークの追加** ダイアログが表示されます。
   (c) 追加するネットワークの SSID や IP アドレスを入力してください。
6. WIPS が近隣のアクティビティを伴わない孤立した環境での使用を意図する場合は、RSSI ベースの分類を定義します。 商業やビジネス街の環境では、このセクションをスキップすることをお勧めします。 次の 2 つのメカニズムのどちらかは、AP を分類するためにオンにする必要があります。
   (a) 不正または未許可の AP として、この値より強い信号強度を持つ AP の事前分類のために使用する RSSI 値のスレッショルド(閾値)を入力。
   (b) モニタされるサブネットに接続される AP を不正または許可 AP として事前分類するために、"モニタされたサブネットに接続した AP を Rogue または許可 AP(Authorized AP)として事前分類"　を選択。
7. 変更を保存するには、**保存** をクリックします。

許可された WLAN ポリシーの編集

ロケーションの許可された WLAN ポリシーを編集するには、次の手順を実行します。

1. ロケーションツリーからロケーションを選択します。
2. **コンフィグレーション>WIPS>許可された WLAN ポリシー**へ移動します。
3. 既存のポリシーを適用する場合は、ポリシーテンプレートリスト内のそのポリシーの適用アイコンをクリックします。
4. ポリシーテンプレートに変更を加えたい場合は、ポリシーテンプレートリスト内のポリシーテンプレートのリンクをクリックしてください。 新規のポリシーテンプレートを追加する場合は、**新しいポリシーテンプレートを追加**をクリックします。 ポリシーテンプレートの追加や編集方法の詳細については、ポリシーテンプレートの管理セクションを参照してください。
5. ロケーションに接続された AP を持つことが許可されていない任意のネットワークが存在する場合、
   (a) **"No Wi-Fi" ネットワークの選択** セクションまでスクロールダウンします。
   (b) **追加**をクリック。 **No Wi-Fi ネットワークの追加** ダイアログが表示されます。
   (c) 追加するネットワークの SSID や IP アドレスを入力してください。
6. WIPS が近隣のアクティビティを伴わない孤立した環境での使用を意図する場合は、RSSI ベースの分類を定義します。 商業やビジネス街の環境では、このセクションをスキップすることをお勧めします。 次の 2 つのメカニズムのどちらかは、AP を分類するためにオンにする必要があります。
   (a) 不正または未許可の AP として、この値より強い信号強度を持つ AP の事前分類のために使用する RSSI 値のスレッショルド(閾値)を入力。
   (b) モニタされるサブネットに接続される AP を不正または許可 AP として事前分類するために、"モニタされたサブネットに接続した AP を Rogue または許可 AP(Authorized AP)として事前分類"　を選択。
7. 変更を保存するには、**保存** をクリックします。

ポリシーテンプレートの管理

ポリシーテンプレートは、ロケーションの許可された WLAN ポリシーの一部を形成します。 ポリシーテンプレートは、許可された SSID またはネットワークのプロパティからなります。 これは、無線ネットワークプロトコル、使用される暗号化プロトコル、許可されたネットワークの SSID、セキュリティ設定、使用される認証タイプや許可されるネットワークなどのように、さまざまなネットワーク関連の設定の集まりです。 組織内の許可されたネットワークの数に基づいて、そのような複数のテンプレートを持つことができます。

ポリシーテンプレートは AP を分類します。 ポリシーテンプレートは、許可 AP(Authorized AP)を識別して許可 AP(Authorized AP)上で提供される実際の Wi-Fi アクセスパラメータが、セキュリティポリシーを満たすことを確認するために使用します。 ロケーションに設定される WLAN ポリシーテンプレートに基づいて、ロケーションに追加される任意の新規 AP を検証します。

複数の WLAN ポリシーテンプレートを定義することができ、各々のロケーションにそれらを割り当てることができます。

ポリシーテンプレートを追加、編集、検索そして削除することができます。 別の名前でポリシーテンプレートを保存して、必要性に応じて変更することができます。 別のロケーションにポリシーテンプレートをコピーすることができます。 次のセクションでは、これらの操作を詳細に説明します。

ポリシーテンプレートの追加

新しいポリシーテンプレートを追加し、ロケーションに適用することができます。

新しいポリシーテンプレートを追加するには、次の手順を実行します。
1. **コンフィグレーション>WIPS>許可された WLAN ポリシー**へ移動します。
2. ロケーションツリーからロケーションを選択します。
3. **Wi-Fi が、このロケーションで配置されている** のチェックボックスにチェックを入れます。 このページの**ポリシーテンプレート**と**"No Wi-Fi" ネットワークの選択**セクションは、このチェックボックスにチェックを入れると有効になります。
4. 新しいポリシーテンプレートを追加するには、**新しいポリシーテンプレートを追加**をクリックします。 **新しいポリシーテンプレートを追加**のダイアログボックスが表示されます。 許可された SSID に関連するポリシーテンプレートのプロパティを定義するには、次の表を参照してください。

フィールド	説明
許可された SSID	既存または新規の許可された SSID の名前またはネットワーク名。 既存の SSID テンプレートリストが、センサーから受信されるデータを使用して構築されます。 新規の名前を入力することも可能です。
テンプレート名	許可されたポリシーテンプレートの名前。
説明	ポリシーテンプレートを識別するための簡単な説明。
これはゲスト SSID です	SSID がゲスト SSID である場合は、このチェックボックスにチェックを入れます。
ネットワークプロトコル	SSID のネットワークプロトコル。 'Any' がデフォルト値です。 'Any' を解除し、IEEE802.11a、IEEE802.11b、IEEE802.11b/g から 1 つ以上プロトコルを選択することができます。
セキュリティ設定	SSID のセキュリティプロトコル。 'Any' がデフォルト値です。 'Any' を解除し、IEEE802.11i、Open、WPA、WEP から 1 つ以上プロトコルを選択することができます。
暗号化プロトコル	SSID の暗号化プロトコル。 SSID のセキュリティプロトコルが WPA または IEEE802.11i の場合にのみ、このフィールドが有効になります。
認証フレームワーク	SSID の認証プロトコル。 SSID のセキュリティプロトコルが WPA または IEEE802.11i の場合にのみ、このフィールドが有効になります。
認証タイプ	SSID への接続にクライアントが使用可能な上位レイヤの認証タイプ。 認証タイプは AP の分類を決定しませんが、クライアントが非許可の認証タイプを使用する場合にイベントを発生させるために使用します。 システムが認証プロトコルのハンドシェイク・フレームを認知する場合だけ、システムはこのイベントを発生します。 'Any' がデフォルト値です。 'Any' を解除し、PEAP、EAP-TLS、LEAP、EAP-TTLS、EAP-FAST と EAP-SIM から 1 つ以上のオプションを選択することができます。
AP ケイパビリティ	AP の追加機能。 これらの高度な機能のいずれかを選択した場合は、分類ロジックはこれらの機能の有無で AP を許可します。 'Any' がデフォルト値です。 'Any' を解除し、特定の機能を選択することができます。
MFP/IEEE802.11w	MFP/IEEE802.11w が SSID 上で有効または無効にされるかを示します。 'Any' がデフォルト値です。 'Any' を解除し、MFP/IEEE802.11 有効または MFP/IEEE802.11 無効を選択することができます。
許可されたネットワーク	SSID 上の無線トラフィックが許可 AP(Authorized AP)を通じてマッピングされるネットワークを選択することができます。 この SSID 上の無線トラフィックが任意のネットワークにマッピングすることを許可するには、'Any'を選択します。 別の方法として、'Any'の選択を解除しシステムによって自動的に検出されたネットワークを選択するか、 もしくはシステムによってまだ検出されていない新しいネットワークを追加から選択することができます。
許可された AP ベンダー	AP が SSID またはネットワークに接続することが可能な許可 AP(Authorized AP)ベンダー。 'Any' がデフォルト値です。 AP ベンダーの定義済みリストから 1 つ以上のベンダーを選択することが可能です。 固有のベンダーを選択するには、'Any' を解除します。
このポリシーテンプレートを現在のロケーションに適用	選択したロケーションにポリシーテンプレートを適用するにはチェックボックスにチェックを入れます。 このチェックボックスが選択されない限り、WLAN はこのポリシーテンプレートによって評価されることはありません。

5. **保存**をクリックします。

ポリシーテンプレートの編集

ポリシーテンプレートが定義されたロケーションでのみ、ポリシーテンプレートを編集することができます。

ポリシーテンプレートを編集するには、次の手順を実行します。
1. **コンフィグレーション>WIPS>許可された WLAN ポリシー**へ移動します。
2. ロケーションツリーからポリシーテンプレートが定義されているロケーションを選択します。
3. ポリシーリスト内のポリシーテンプレートのリンクをクリックします。 **Authorized IEEE802.11 SSID 用のテンプレートを編集** のダイアログボックスが表示されます。 必要に応じて、このダイアログボックスのフィールドを変更します。 許可された SSID に関連するポリシーテンプレートのプロパティを定義するには、次の表を参照してください。

フィールド	説明
許可された SSID	既存または新規の許可された SSID の名前またはネットワーク名。 既存の SSID テンプレートリストが、センサーから受信されるデータを使用して構築されます。
テンプレート名	許可されたポリシーテンプレートの名前。
説明	ポリシーテンプレートを識別するための簡単な説明。
これはゲスト SSID です	SSID がゲスト SSID である場合は、このチェックボックスにチェックを入れます。
ネットワークプロトコル	SSID のネットワークプロトコル。 'Any' がデフォルト値です。 'Any' を解除し、IEEE802.11a、IEEE802.11b、IEEE802.11b/g から 1 つ以上のプロトコルを選択することができます。
セキュリティ設定	SSID のセキュリティプロトコル。 'Any' がデフォルト値です。 'Any' を解除し、IEEE802.11i、Open、WPA、WEP から 1 つ以上のプロトコルを選択することができます。
暗号化プロトコル	SSID の暗号化プロトコル。 SSID のセキュリティプロトコルが WPA または IEEE802.11i の場合にのみ、このフィールドが有効になります。
認証フレームワーク	SSID の認証プロトコル。 SSID のセキュリティプロトコルが WPA または IEEE802.11i の場合にのみ、このフィールドが有効になります。
認証タイプ	SSID への接続にクライアントが使用可能な上位レイヤの認証タイプ。 認証タイプは AP を分類しませんが、クライアントが非許可の認証タイプを使用する場合にイベントを発生させるために使用されます。 システムが認証プロトコルのハンドシェイク・フレームを認知する場合のみ、システムはこのイベントを発生します。 'Any' がデフォルト値です。 'Any' を解除し、PEAP、EAP-TLS、LEAP、EAP-TTLS、EAP-FAST と EAP-SIM から 1 つ以上のオプションを選択することができます。
AP ケイパビリティ	AP の追加機能。 これらの高度な機能のいずれかを選択した場合は、分類ロジックはこれらの機能の有無で AP を許可します。 'Any' がデフォルト値です。 'Any' を解除し、特定の機能を選択することができます。
MFP/IEEE802.11w	MFP/IEEE802.11w が SSID 上で有効または無効にされるかを示します。 'Any' がデフォルト値です。 'Any' を解除し、MFP/IEEE802.11 有効または MFP/IEEE802.11 無効を選択することができます。
許可されたネットワーク	SSID 上の無線トラフィックが、許可 AP(Authorized AP)を通じてマッピングされるネットワークを選択することができます。 この SSID 上の無線トラフィックが任意のネットワークにマッピングすることを許可するには、'Any'を選択します。 別の方法として、'Any'の選択を解除しシステムによって自動的に検出されたネットワークを選択するか、 もしくはシステムによってまだ検出されていない新しいネットワークを追加するか、選択することができます。
許可された AP ベンダー	AP が SSID またはネットワークに接続することが可能な許可 AP(Authorized AP)ベンダー。 'Any' がデフォルト値です。 AP ベンダーの定義済みリストから 1 つ以上のベンダーを選択することが可能です。 固有のベンダーを選択するには、'Any' を解除します。

このポリシーテンプレートを現在のロケーションに適用	選択したロケーションにポリシーテンプレートを適用するにはチェックボックスにチェックを入れます。 このチェックボックスが選択されない限り、WLAN はこのポリシーテンプレートによって評価されることはありません。

4. **保存**をクリックします。

ポリシーテンプレートの検索

名前または SSID に基づいてリストからポリシーテンプレートを検索することができます。 ポリシーテンプレートのリストが検索文字列に基づいてフィルタリングされます。

ポリシーテンプレートを検索するには、次の手順を実行します。
1. ロケーションツリーからロケーションを選択します。
2. **コンフィグレーション>WIPS>許可された WLAN ポリシー**へ移動します。
3. ポリシーテンプレートリストの左上の隅にあるクイック検索ボックスに SSID またはポリシーテンプレート名を入力します。
4. **Enter** キーを押します。
5. SSID またはポリシーテンプレート名の検索文字列を含むポリシーテンプレートがポリシーリスト（テンポラリ）内に表示されます。 検索ユーティリティは、SSID またはポリシーテンプレート名の部分文字列のような検索文字列を持つポリシーテンプレートを検索します。

ポリシーテンプレートを別のロケーションにコピー

ロケーションで作成された許可された WLAN ポリシーを別のロケーションにコピーするには、次の手順を実行します。
1. コピーされるポリシーが存在するロケーションを選択します。
2. **コンフィグレーション>WIPS>許可された WLAN ポリシー**へ移動します。
3. コピーされる WLAN ポリシーのチェックボックスを選択します。
4. ポリシーリストの下にあるコピーアイコンをクリックします。 **ロケーションの選択** ダイアログボックスが表示されます。
5. 選択されたポリシーをコピーするロケーションを選択し、**OK** をクリックします。 WLAN ポリシーは選択したロケーションにコピーされます。

別の名前でポリシーテンプレートを保存

既存のポリシーテンプレートとほぼ同じ設定を持つ新しいポリシーテンプレートを作成したい場合は、既存のポリシーテンプレートのコピーを作成し、編集することができます。
ポリシーテンプレートのコピーを生成するか、異なる名前で既存のポリシーテンプレートを保存するには、次の手順を実行します。
1. **コンフィグレーション>WIPS>許可された WLAN ポリシー**へ移動します。
2. ポリシーテンプレートが作成されているロケーションを選択します。
3. ポリシーテンプレートリスト内のポリシーテンプレートのリンクをクリックします。
   Authorized IEEE802.11 SSID 用のテンプレートを編集 のダイアログボックスが表示されます。
4. テンプレート名を編集し、必要に応じて他のフィールドを変更します。
5. **名前を付けて保存**をクリックします。 ポリシーテンプレートは新しい名前で保存されます。

ポリシーテンプレートのリストを印刷

ロケーションに対して許可された WLAN ポリシーに定義されているポリシーテンプレートのリストを、印刷することができます。
ロケーションに対して許可された WLAN ポリシーのポリシーテンプレートリストを印刷するには、次の手順を実行します。

1. **コンフィグレーション>WIPS>許可された WLAN ポリシー**へ移動します。
2. ポリシーテンプレートリストを印刷したいロケーションを選択します。 選択したロケーションがルートロケーションではない場合、許可された WLAN ポリシーが選択されたロケーションで変更されている場合のみ印刷アイコンは有効になります。
3. 印刷アイコンをクリックすると、ポリシーテンプレートリストの印刷プレビューが表示されます。
4. ロケーションのポリシーテンプレートのリストを印刷するには、**印刷**をクリックします。

ポリシーテンプレートの削除

このオプションは、テンプレートが作成されたロケーション、そして作成されたロケーションの任意の他の子ロケーションでテンプレートが適用されていない場合のみ有効になります。
ポリシーテンプレートを削除するには、次の手順を実行します。

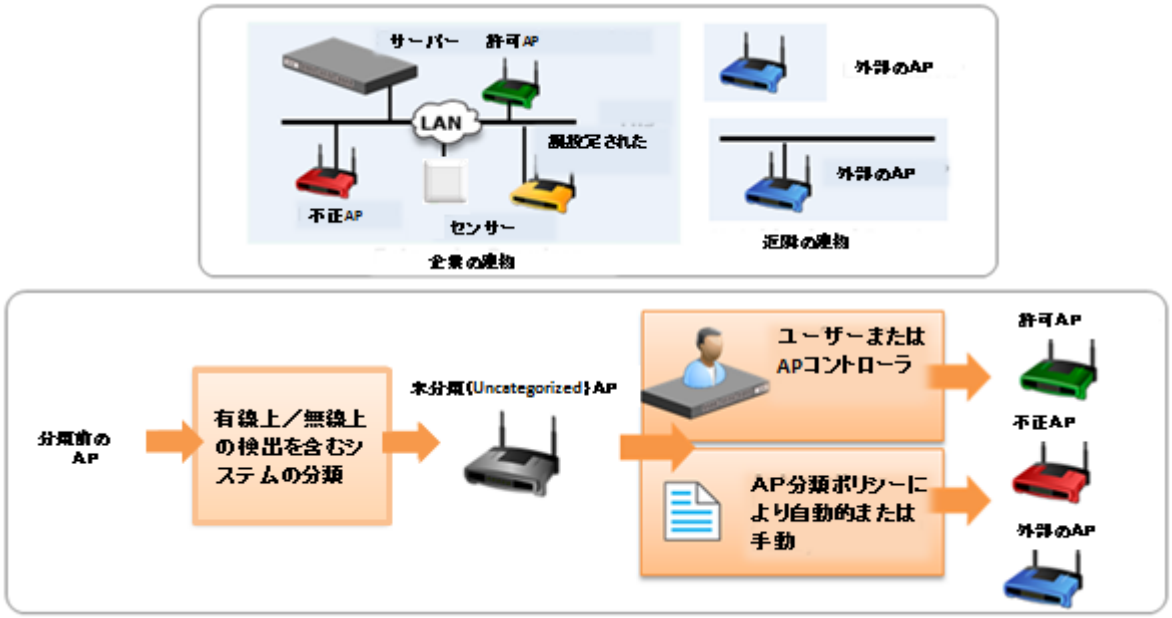
1. **コンフィグレーション>WIPS>許可された WLAN ポリシー**へ移動します。
2. ポリシーテンプレートが作成されているロケーションを選択します。
3. ポリシーテンプレートリストから削除するポリシーテンプレートのチェックボックスにチェックを入れます。
4. ポリシーテンプレートを削除するには、削除アイコンをクリックします。確認メッセージが表示されます。
5. **Yes** をクリックすると、ポリシーテンプレートはポリシーリストから削除されます。

AP 自動分類ポリシーの設定

AP の自動分類ポリシー機能を使用すると、異なる AP のカテゴリに対して AP の分類を指定することができます。

未許可の AP は、ネットワークやビジネスに回復不能な損傷を引き起こす可能性があり、ネットワーク内の AP の正当性について知っておくことが重要です。
AP の分類は、WIPS の実装において最も重要です。

AP 分類の概略図を以下に示します。



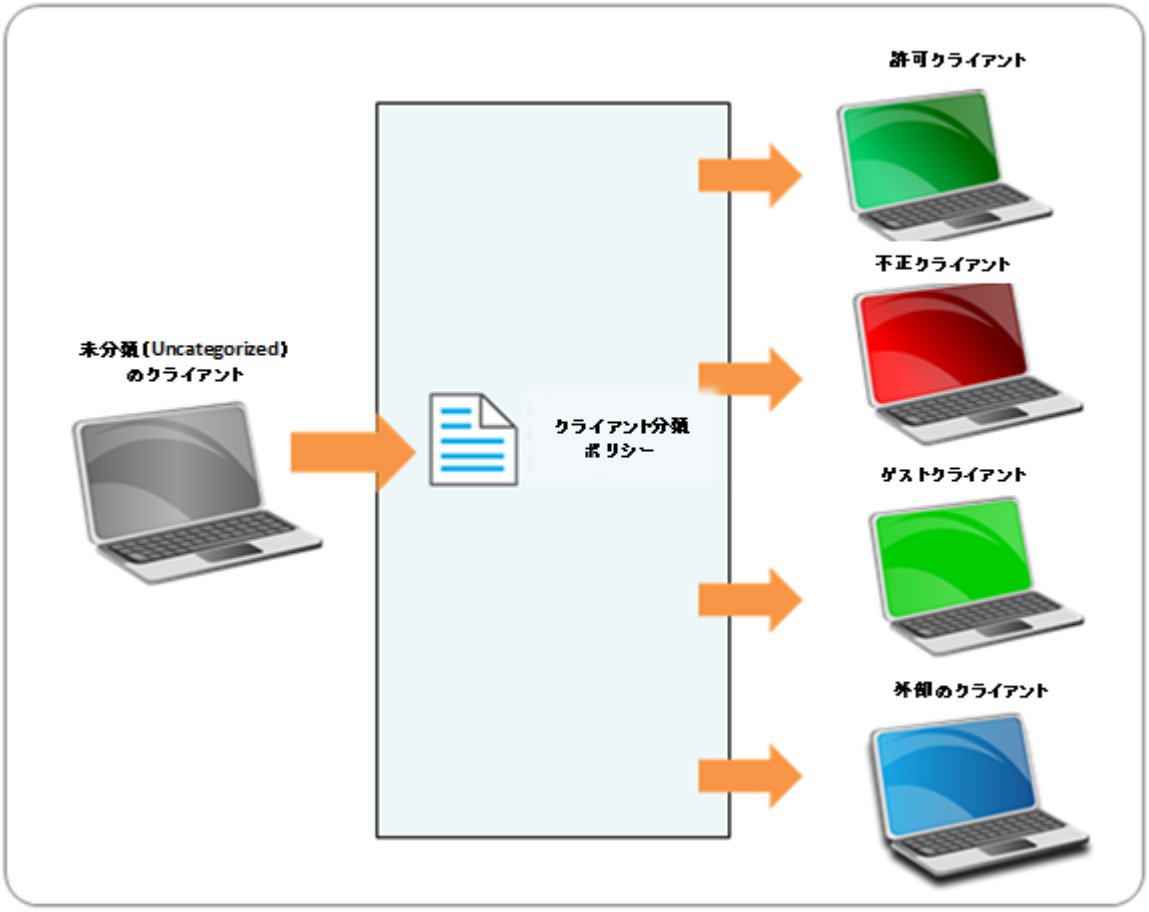
AP 分類

外部 AP(External APs)では、“自動的に External フォルダーへ Uncategorized リスト内の潜在的な External AP を移動”を推奨しています。 あとで AP が企業ネットワークに接続されていることを検出した場合、システムは自動的に外部フォルダーから AP を削除し適切な AP のフォルダーに移動します。

ご注意： いったん AP が Rogue フォルダーへ移動されると、 あとで企業ネットワークに非接続だと検出されたり、 またはセキュリティ設定が変更されたりしても自動的に Rogue フォルダーから取り出されることはありません。

クライアント自動分類ポリシーの設定

クライアントの自動分類ポリシーは、クライアントの最初の発見時とそのあとの AP とのアソシエーションで分類される方法を決定します。



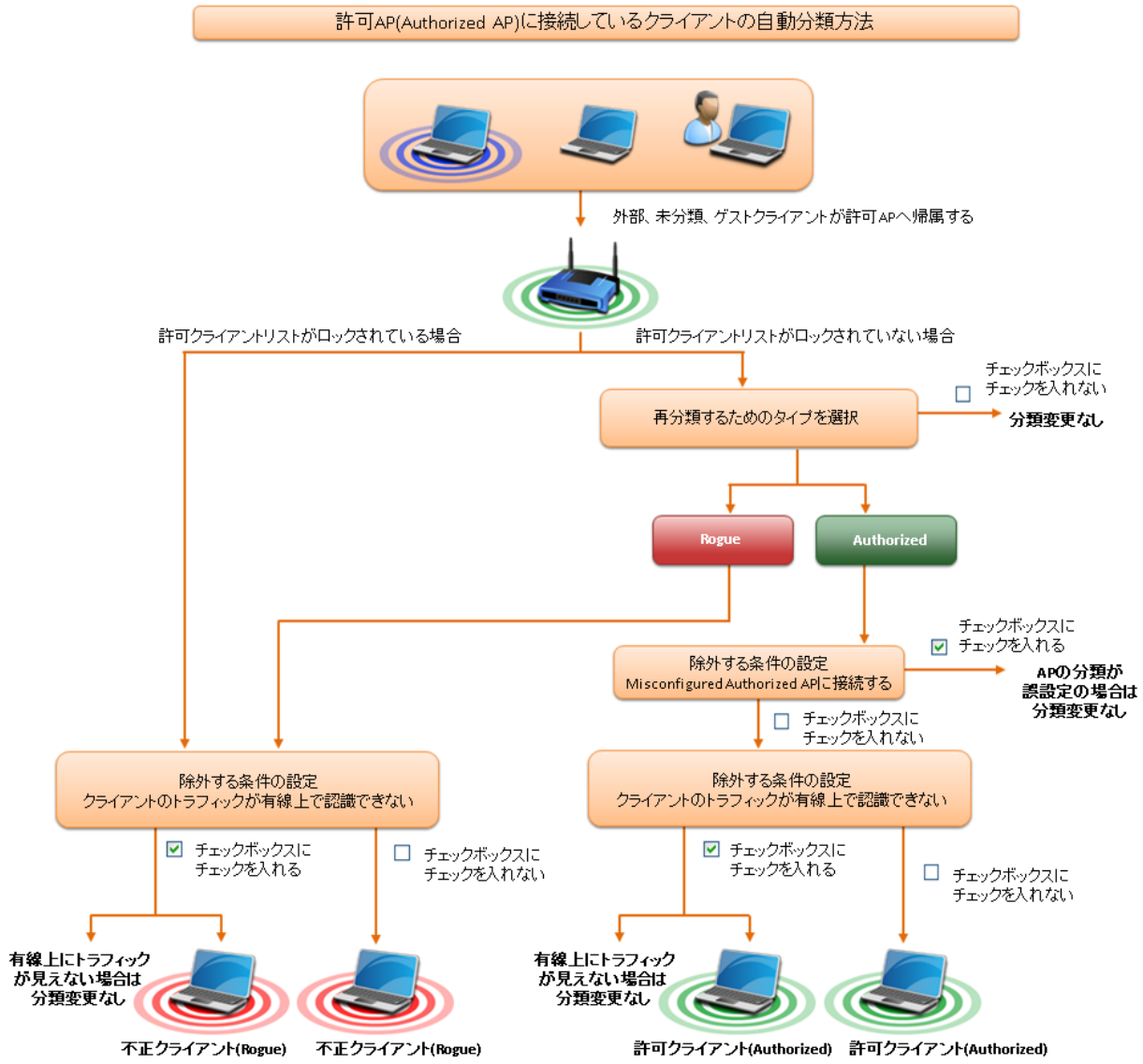
クライアントの自動分類

システムが最初に検出したときとそのあとの AP とのアソシエイトに基づいて、 選択されたロケーションで検出された無線クライアントを分類する方法を定義します。 このポリシーは自動的に選択されたロケーションの子の位置によって継承されます。 無線クライアントに施行される侵入防止アクションは、システムでそれらの分類に基づいて行われます。

クライアントが手動で分類される場合は、それがシステムから削除され再発見されるまで、 システムによって決して自動的に分類されません。

最初のクライアント分類では、 このロケーションで新たに発見されたクライアントを自動分類チェックボックスを選択して、 デフォルトでは未分類とされる特定のロケーションで新たにクライアントが発見された場合に、 外部(External)、許可(Authorized)またはゲスト(Guest)として分類するかを指定します。
クライアントの自動分類 では、 AP とのアソシエイトに基づいて未分類(Uncategorized)と未許可(Unauthorized)クライアントを システムが自動的に再分類することを可能にするために 1 つ以上のオプションを選択します。 次のタイプのクライアントを分類することができます。

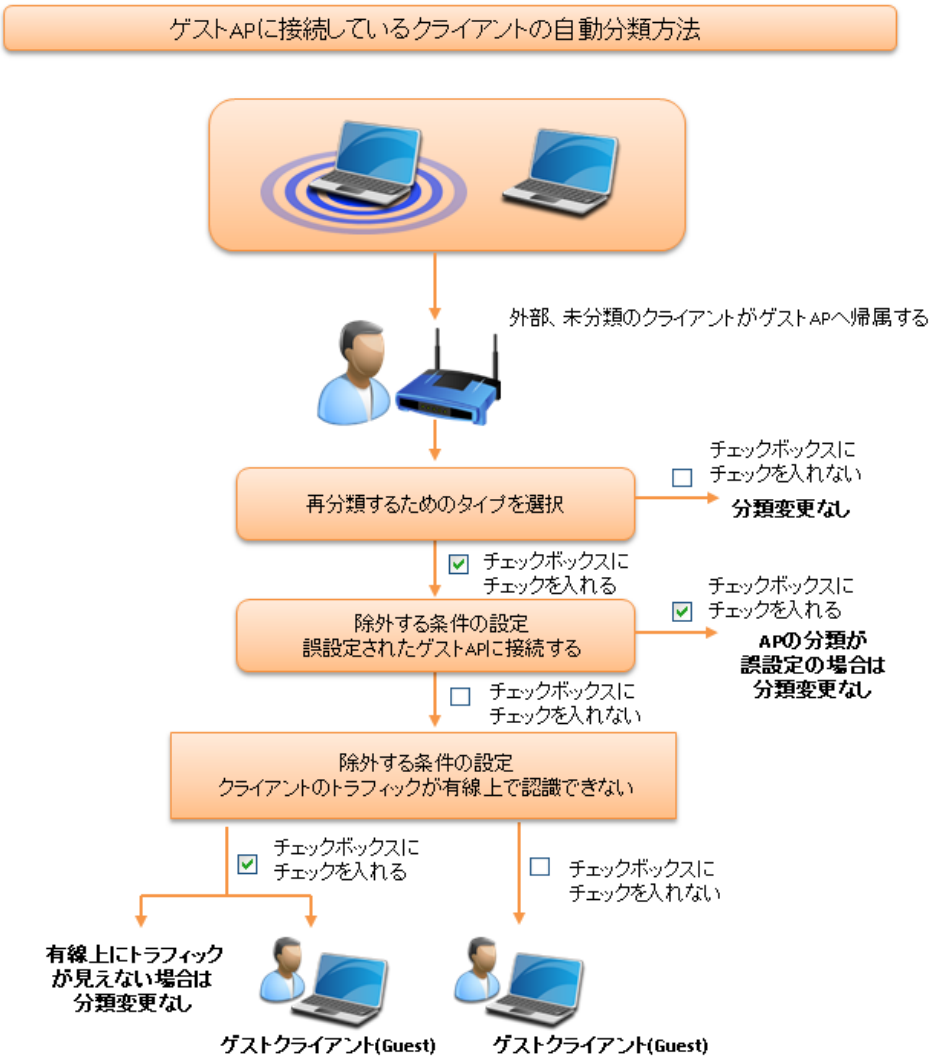
- 許可 AP(Authorized AP)に接続するクライアント
- 許可 AP に接続するすべての外部クライアントを許可(Authorized)として再分類
- 許可 AP に接続するすべての未分類クライアントを許可(Authorized)として再分類
- 許可 AP に接続するすべてのゲストクライアントを許可(Authorized)として再分類
  以下の例外を選択することができます。
- 誤設定された許可 AP(Misconfigured Authorized AP)に接続するクライアントは再分類しない
- 無線データパケットが有線ネットワーク上で検出されない場合はクライアントを再分類しない（接続が WLAN コントローラによって報告されている場合を除く）



許可 AP に接続しているクライアントの分類

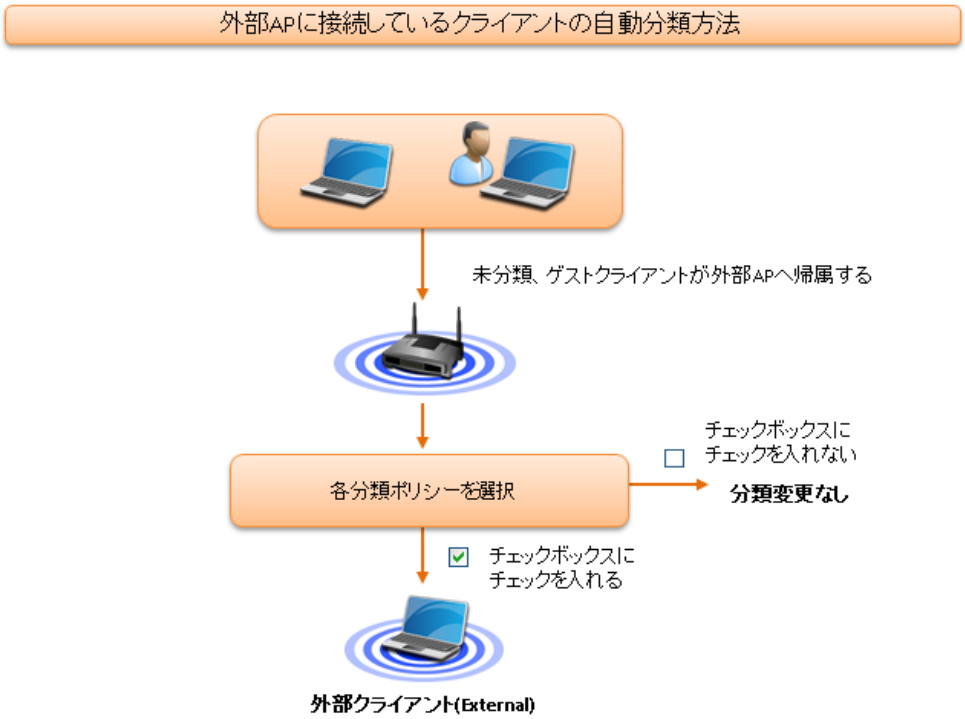
ゲスト AP と外部 AP に接続しているクライアントの自動分類の設定を構成するには、 **詳細設定** をクリックします。

- ゲスト AP に接続しているクライアント
- ゲスト AP に接続するすべての外部クライアントは、ゲストとして再分類
- ゲスト AP に接続するすべての未分類のクライアントは、ゲストとして再分類
  以下の例外を選択することができます
- 誤設定されたゲスト AP に接続しているクライアントは再分類しない
- 無線データパケットが有線上で認識できない場合はゲストとしてクライアントを再分類しない（接続が WLAN コントローラによって報告されている場合を除く）



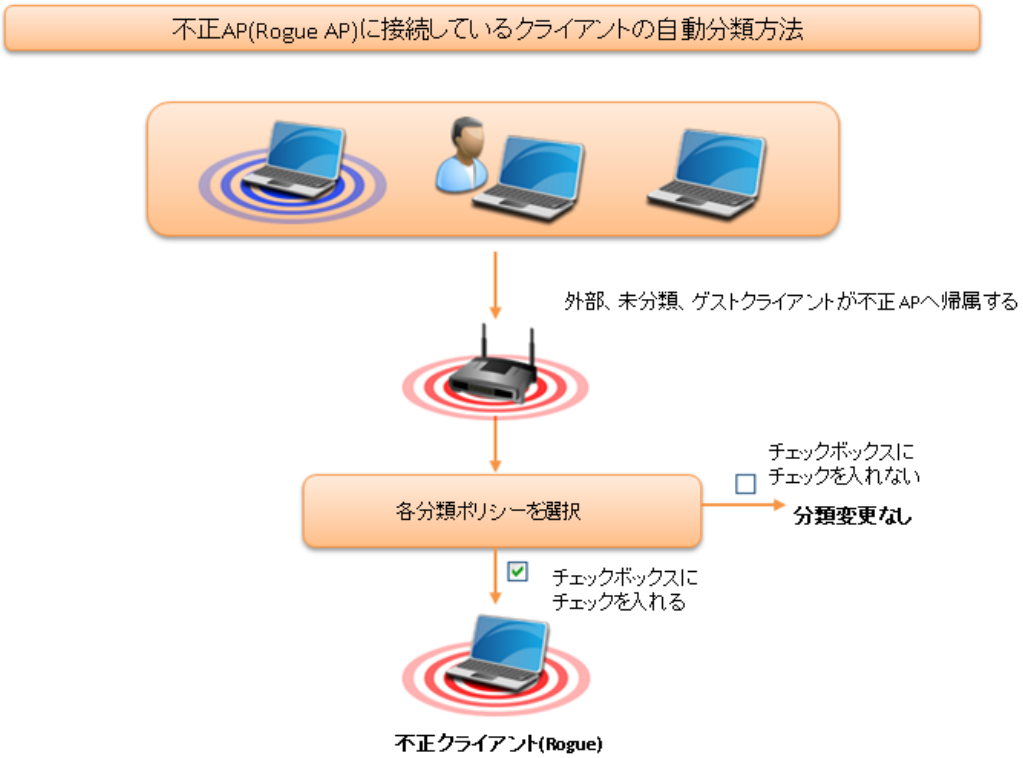
ゲスト AP に接続しているクライアントの分類

- 外部の AP に接続しているクライアント
- 外部 AP に接続するすべての未分類のクライアントは、外部として再分類
- 潜在的な外部 AP に接続するすべての未分類のクライアントは、外部として分類
- 外部 AP に接続するすべてのゲストクライアントは、外部として再分類
- 潜在的な外部 AP に接続するすべてのゲストクライアントは、外部として再分類



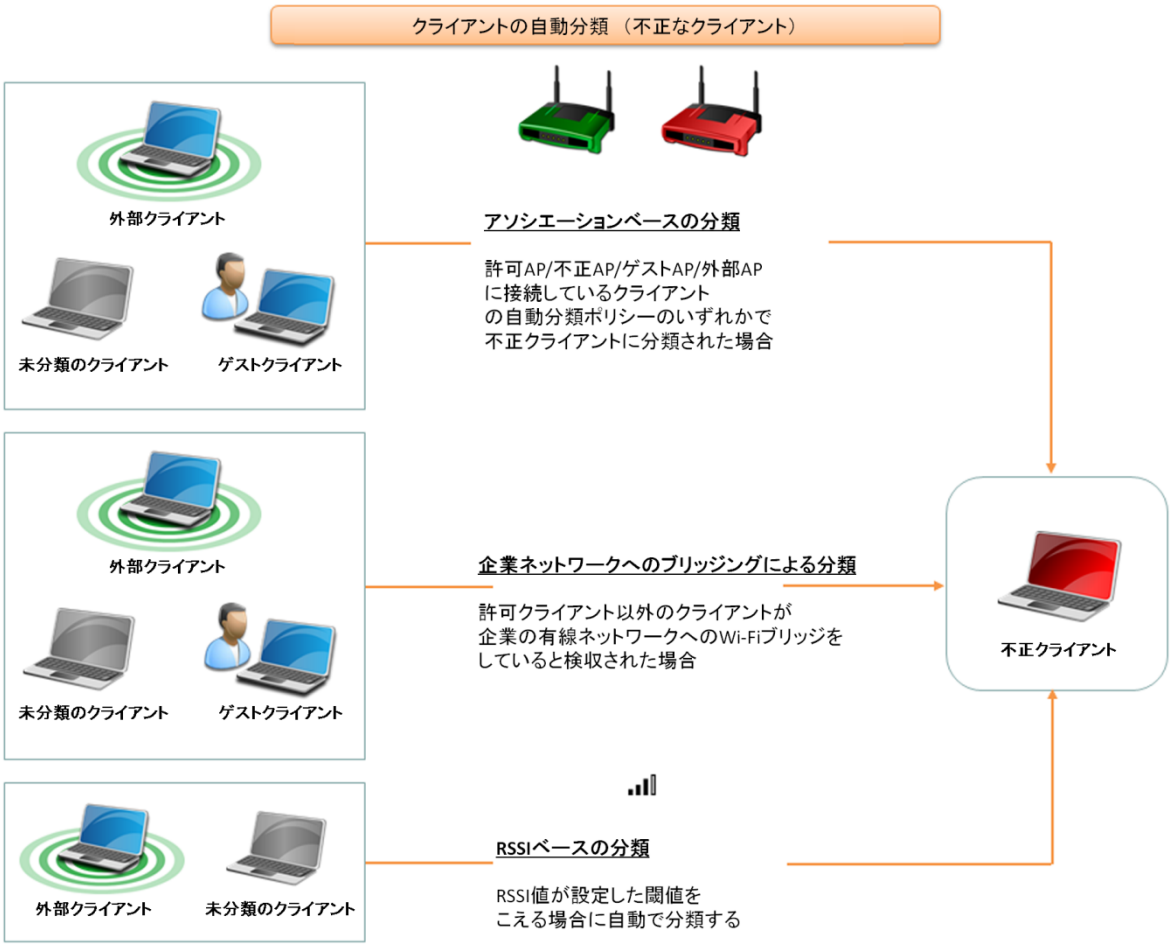
外部の AP に接続しているクライアントの分類

- 不正 AP(Rogue AP)に接続しているクライアント
- Rogue AP に接続する許可クライアント以外のクライアントを不正(Rogue)として再分類
- 潜在的な Rogue AP に接続する許可クライアント以外のクライアントを不正(Rogue)として再分類



不正 AP(Rogue AP)に接続しているクライアントの分類

- 企業ネットワークへのブリッジング
- 企業のネットワークに Wi-Fi をブリッジングしていると検出された場合は、任意の非許可クライアントを不正(Rogue)として分類
- RSSI ベースの分類
  未分類のクライアントおよび（または）外部のクライアントに対して、 RSSI ベースのクライアント分類を可能にし、それらに対して RSSI ベースの分類を設定することができます。 このようなクライアントに対して RSSI スレッショルドとカテゴリを指定します。



企業ネットワークと、RSSI ベースの分類にブリッジングするクライアントの分類

侵入防御

侵入防御ポリシーは、システムが自動的にネットワークを保護し、無線の脅威を判定します。 システムは、このような脅威をもたらしている AP とクライアントを自動的に隔離へ移動させます。 システムは、選択された侵入防御レベルに基づいて、同時に複数の脅威から守ることができます。

サーバーが侵入防止ポリシーに基づいてアクセスポイントまたはクライアントを隔離する場合、 自動隔離を無効とするオプションは、システムが自動的にこの AP またはクライアントを隔離しないことになります（指定された侵入防止ポリシーに関係なく）。

管理コンソール(Management Console)は、IEEE802.11 ネットワーク内の不必要な通信を防ぐことができます。 それは、異なる効果の防御ブロックメカニズムの多様なレベルを提供します。 侵入防御レベルは、望む防御レベルと無線チャネル間の複数の同時防御数の間のトレードオフを指定することができます。
要求される同時防御のチャネル数がより多いほど、不必要な通信を禁止する防御の効果はより小さくなります。 選択される防御レベルに関係なく、新しいデバイスに対してのスキャンは続きます。
以下の侵入防御レベルから選択が可能です。

- Block； 1 台のセンサーは不必要な IEEE802.11b/g 帯域の任意の 1 つのチャネル上と IEEE802.11a 帯域の任意の 1 つのチャネルの通信をブロックすることができます。
- Disrupt： 1 台のセンサーは不必要な IEEE802.11b/g 帯域の任意の 2 つのチャネル上と IEEE802.11a 帯域の任意の 2 つのチャネルの通信を中断することができます。
- Interrupt： 1 台のセンサーは不必要な IEEE802.11b/g 帯域の任意の 3 つのチャネル上と IEEE802.11a 帯域の任意の 3 つのチャネルの通信妨害することができます。
- Degrade： 1 台のセンサーは不必要な IEEE802.11b/g 帯域の任意の 4 つのチャネル上と IEEE802.11a 帯域の任意の 4 つのチャネルの通信を低下することができます。

Block は最も強力な防御レベルで、Ping、SSH、Telnet、FTP、HTTP などを 含むほとんどのポピュラーなインターネット・アプリケーションを厳格にブロックすることができます。このレベルでは 1 台のセンサーは IEEE802.11b/g 帯域の 1 つのチャネルと IEEE802.11a 帯域の 1 つのチャネルでのみ望ましくない通信を同時に防止することができます。 センサーが IEEE802.11b/g や(または) IEEE802.11a 帯域で同時に複数チャネル上で望ましくない通信を防御することを望むならば、 他の防御レベルを選択する必要があります。

ご注意： 防御レベルは、不必要な AP とクライアントからの通信を防御するためのブロック強度を決定します。 システムは、各チャネル上の複数の AP およびクライアントを防ぐことが可能です。 防御レベルは、サービス拒否（DoS）攻撃やアドホックネットワークには適用されません。 より多くのチャネル上のデバイスを防ぐためには、低いブロックレベルを選択する必要があります。 低いブロックレベルを選ぶことは、ブロックされたデバイスからのいくつかのパケットが通過する可能性があることを意味します。

次の脅威に対して侵入防御を有効にすることができます。

- **Rogue APs**: AP はネットワークに接続されているが管理者が許可していません。 攻撃者は不正 AP(Rogue AP)を介してネットワークへのアクセスすることができます。 また、ネットワークに接続される未分類(Uncategorized)、不定(indeterminate)、禁止(Banned)AP を自動的に隔離することができます。
- **Misconfigured APs**: AP は管理者によって承認されますが、セキュリティポリシーに準拠していません。 攻撃者は、誤設定の AP を介してネットワークへのアクセスすることができます。 AP は改ざんによりリセットされたか、セキュリティポリシーを変更された場合に発生する可能性があります。
- **Client Misassociations**: 不正または（隣接する）外部 AP に接続する許可クライアント。 許可クライアント上の企業データは、不正な接続の脅威にさらされています。不正または外部 AP に接続する許可クライアントに対して、自動侵入防御を提供することをお勧めします。

承認されていないスマートデバイス用の特別な侵入防止ポリシーがあります。 現在のクライアントポリシーは、許可クライアントのゲスト AP への接続を制限している場合でも、 未承認のスマートデバイスは許可するようにすることができます。その場合、未承認のスマートデバイスへのゲスト AP の接続を許可または制限する必要があります。

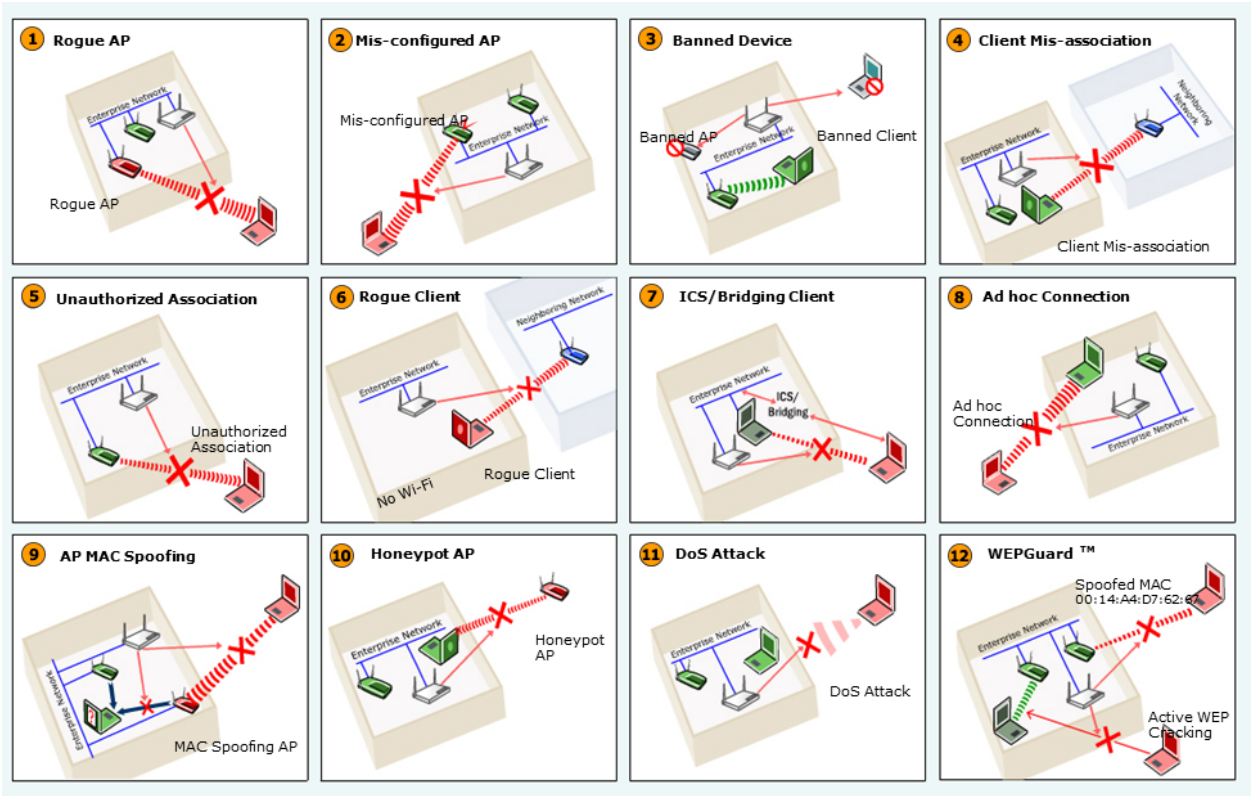
未承認のスマートデバイス用に特別な処理を可能にするため、 **未承認スマートデバイスのための特別な処理を有効** をクリックします。 未承認のスマートデバイスがゲストのみ AP に接続できるようにするには、以下を実行します。

1. **未承認スマートデバイスのための特別な処理を有効**を選択します。
2. **ゲスト AP への接続を許可するが、許可 AP への接続は許可しない**を選択します。

未承認のスマートデバイスによる接続を、ゲスト AP だけでなく許可されたアクセスポイントも許可しないようにするには、 **ゲスト AP と許可 AP への接続を許可しない**を選択します。

無線の脅威

下図は、さまざまな無線の脅威を示しています。



無線の脅威

未許可のアソシエーション； 未許可と禁止されたクライアントの許可 AP への接続は、セキュリティメカニズムが弱い場合に、 攻撃者が許可 AP を介してネットワークへのアクセスを得ることが可能です。 未許可または未分類クライアントのゲスト SSID による許可 AP への接続は、未許可のアソシエーションとみなされません。

- ゲスト AP へのアソシエーション： 外部と未分類クライアントのゲスト AP への接続は、ゲストクライアントとして分類されます。 有線ネットワークまたは誤設定の AP に接続されたクライアントは、このポリシーの例外として指定することができます。
- アドホック接続： クライアント間のピアツーピア接続は、それがアドホック接続に関与している場合は、 許可クライアント上の企業データは脅威にさらされています。
- MAC 偽装： 許可 AP(Authorized AP)の無線 MAC アドレスを偽装する AP により、攻撃者は偽装する AP を介して攻撃を仕掛けることができます。
- ハニーポット/エビルツイン AP： 許可 AP(Authorized AP)と同じ SSID を持つ近隣の AP により、許可クライアントはハニーポット/エビルツイン AP に接続する可能性があります。 これらの許可クライアント上の企業データは、そのような接続により脅威にさらされます。
- サービス妨害(DoS) 攻撃 ： サービス妨害攻撃は、職務上の WLAN のパフォーマンスを低下させます。
- WEPGuard： アクティブな WEP クラッキングツールは、攻撃者が WEP キーを解読し数分あるいは数秒で機密データへのアクセスを得ることができます。 危険にさられた WEP キー鍵は非アクティブの許可クライアントの MAC アドレスを偽装することによって許可された WLAN に侵入するために使用されます。
- クライアント Bridging/ICS： 有線と無線のインタフェース間でパケット転送を有効したクライアント。 企業のサブネットに接続されている許可クライアントのブリッジや不正/未分類クライアントのブリッジは、深刻なセキュリティ上の脅威になります。

ロケーションの侵入防止をアクティベイト

コンフィグレーション>WIPS>侵入防御の有効化を使用してロケーションの侵入防止をアクティブにします。下図は、侵入防御のアクティベーションを説明しています。

侵入防御のアクティベーション

侵入防止ポリシーはロケーション固有のポリシーです。 それは、親ロケーションから継承することはできません。

許可 AP(Authorized AP)は侵入防止をアクティブにする前に、 **Authorized** フォルダーの中に入れる必要があります。 ネットワーク接続のアイコンが有線上、非有線上または不確定の状態を示すことがあります。
あとで新しい許可 AP(Authorized AP)を配置する場合は、侵入防止を無効にする必要はありません。ただし、新しく配置された AP が **Authorized** フォルダーに移動されていることを確認する必要があります。

配置が安定し完全に設定されたあとに、選択したロケーションに対して **侵入防御の有効化** のチェックボックスにチェックを入れることをお勧めします。 配置を変更する場合は、移行の間は偽のアクティビティを避けるために ロケーションに対して **侵入防御の有効化** チェックボックスのチェックを外します。
変更を保存するには、**保存** をクリックします。 変更を取り消すには、**キャンセル** をクリックします。 デフォルト値に戻すには、**デフォルト値に戻す** をクリックします。

デバイスリストのインポート

コンフィグレーション>WIPS>デバイスのインポートを使用して、管理コンソール(Management Console)へ許可 AP(Authorized AP)リスト、許可クライアントリスト、ゲストクライアントリスト、不正 AP リスト、不正クライアントリスト、Management Device リストをインポートすることが可能です。

許可 AP(Authorized AP)リストおよび許可または未許可クライアントのリストをインポートすることは、許可/未許可の箱へこれらのデバイスを手動で移動するのに代わる効率的な手段です。 これらのリストを正常にインポートしたあとで、システムは許可または未許可としてそれぞれのリスト内の AP とクライアントを自動的に分類します。

これはロケーション固有のプロパティで、親ロケーションフォルダーから継承することはできません。デバイスリストをインポートするには、管理者権限が必要です。

デバイスをインポートするには、以下の手順を実行します。

1. 許可 AP(Authorized AP)リスト、許可クライアントリスト、ゲストクライアントリスト、不正クライアントリスト、または Management Device リストをインポートするかどうかに応じて、タグデバイスの上にある**インポート**リストボックスから適切なオプションを選択してください。 選択に基づいてデバイスリストの下のコマンドボタンのテキストが変わります。 例えば、リストボックスから**許可クライアントリスト**のインポートを選択した場合は、 コマンドボタンのテキストは**許可クライアントリストのインポート**に変わります。
2. **自動タグデバイス**エリアで、 選択したロケーションに自動的にデバイスをタグ付けするためには**自動タグデバイス**を選択します。 選択したロケーションに手動でデバイスをタグ付けするには、**手動タグデバイス**を選択します。
3. AP またはクライアントの MAC アドレス、IP アドレスと名前を入力します。 デバイスが Management Device の場合には、MAC アドレスおよび任意の名前を入力します。 また、AP /クライアント/Management Device のデータを含むファイル名を指定することができます。 **ファイルからオートフィル**をクリックし、AP/クライアント/Management Device のデータを含む.txt または.csv ファイルを選択します。
4. 許可 AP(Authorized AP)リストをインポートするには、**許可 AP リストのインポート**をクリックします。 許可クライアントリストをインポートするには、**許可クライアントリストのインポート**をクリックします。 ゲストクライアントリストをインポートするには、**ゲストクライアントリストのインポート**をクリックします。 不正クライアントリストをインポートするには、**不正クライアントリストのインポート**をクリックします。Management Device リストをインポートするには、**Management Device リストのインポート**をクリックします。 ファイルはテキストファイルまたは csv ファイルである必要があります。 AP、クライアント、Management Device リストのテキストおよび csv ファイル形式に関しては、下記を参照してください。

インポートされると、デバイスが**デバイス**ページ上のそれぞれのタブの下に表示されます。 また、**ダッシュボードページ**には新たにインポートした Management Device、AP、クライアントのアクティビティを反映します。

AP/クライアントデータを含む .txt または .csv ファイル形式

各行は、MAC アドレス、IP アドレス、デバイス名のカンマで区切られたリストです。
11:11:11:11:11:11,192.168.8.1,name1
11:11:11:11:11:12,192.168.8.2,name2
11:11:11:11:11:13,192.168.8.3,name3
11:11:11:11:11:14,192.168.8.4,name4
11:11:11:11:11:15,192.168.8.5,name5
11:11:11:11:11:16,192.168.8.6,name6
11:11:11:11:11:17,192.168.8.7,name7

管理デバイス(Management Device)データを含む .txt または .csv ファイル形式

各行は、MAC アドレス、デバイス名のカンマで区切られたリストです。
44:77:11:22:44:77, name1
44:77:11:22:11:12, name2
44:77:11:22:11:13, name3
44:77:11:22:11:14, name4
44:77:11:22:11:15, name5

覚えておくべきポイント

- いったん、AP を **Authorized** フォルダーに移動すると、 たとえ AP が企業のネットワークから取り除かれたとしても、管理コンソール(Management Console)は決して自動的に **Authorized** フォルダーから削除することはありません。
- リストから AP をインポートした場合、セットアップウィザードのポリシー設定は、インポートされた AP には適用されません。
- リストから Management Device をインポートすると、 **デバイス**ページでのみ、インポートされた Management Device を削除できます。
- リストからクライアントをインポートした場合、自動分類のポリシー設定は、これらのクライアントには適用されません。

デバイスリストからデバイスの詳細を削除

デバイスリストからデバイスの詳細を削除するには、次の手順を実行します。
1. AP/クライアント/Management Device の行を選択し、対応する **削除** をクリックします。
2. 削除を確認するメッセージが表示されたら、**Yes** をクリックします。

ロケーションでのデバイスリストのロック

デバイスリストのロックはロケーション固有のプロパティであり、それは親ロケーションから継承することはできません。
コンフィグレーション>WIPS>デバイスリストのロックを使用して選択したロケーションでのデバイスリストをロックします。

ロケーション<選択されたロケーション>に対して AP リストのロックとロケーション<選択されたロケーション>に対してクライアントリストのロックの 2 つのチェックボックスにチェックを入れると、選択されたロケーションで許可 AP(Authorized AP)とクライアントのリストをロックすることができます。特定のデバイスリストをロックすると、そのロケーションでこれ以上そのタイプのデバイスを自動的に Authorized することはできません。 AP が Authorized フォルダーへ自動的に移動しないので、許可 AP(Authorized AP)リストをロックするということは、有線 AP がこのロケーションの潜在的な許可としてタグを付けられないことを意味します。それらは潜在的な Rogue となり、AP 自動分類ポリシーに基づいて Rogue フォルダーへ自動的に移動する可能性があります。すべての許可されたデバイスを識別して分類したあとに、本機能を使用する必要があります。リストがロックされたあとで任意の新しいデバイスを追加する場合は、Authorized カテゴリへ手動で移動しなければなりません。

禁止デバイスリストの管理

コンフィグレーション>WIPS>禁止された（Banned）デバイスリストを使用して、禁止された AP と禁止されたクライアントのリストを作成し管理することができます。 このリストからデバイスが検出された場合は、不正なデバイスとして分類されません。

禁止 AP リストの作成

組織内のブラックリストに載っている AP の無線 MAC アドレスを追加することができます。 これらの MAC アドレスを持つ AP を検知すると管理コンソール(Management Console)はアラートを生成します。

個々の AP の MAC アドレスを入力するか、データベースに禁止された AP のリストをインポートできます。

個々の AP の MAC アドレスを追加するには、次の手順を実行します。
1. **コンフィグレーション>WIPS>禁止された（Banned）デバイスリスト**へ移動します。
2. **禁止された AP リスト**をクリックして展開します。
3. **MAC アドレスの追加**をクリックします。**禁止リストへの追加**が表示されます。
4. 禁止 AP リストで**デバイスの追加**をクリックし、禁止された AP の MAC アドレスを入力します。 この方法で 1 つ以上の禁止 AP の MAC アドレスを追加することができます。

ファイルから AP の MAC アドレスのリストをインポートすることも可能です。AP の MAC アドレスのリストを含むファイルは、csv ファイルである必要があります。

AP の MAC アドレスのリストを含むファイルをインポートするには、次の手順を実行します。
1. **コンフィグレーション>WIPS>禁止された（Banned）デバイスリスト**へ移動します。
2. **禁止された AP リスト**をクリックして展開します。
3. **MAC アドレスの追加**をクリックします。 **禁止リストへの追加** が表示されます。
4. **ファイルのアップロード**をクリックします
5. **ファイルを選択**をクリックし、選択したファイルをアップロードするには**アップロード**をクリックします。
6. 禁止デバイスリストにインポートした AP の MAC アドレスを追加するには、**追加** をクリックします。

禁止クライアントリストの作成

企業内のブラックリストに載っているクライアントの無線 MAC アドレスを追加できます。 例えば、このような MAC アドレスは企業で不要になった従業員のノートパソコンに属している可能性があります。 これらの MAC アドレスを持つクライアントを検知すると管理コンソール(Management Console)はアラートを生成します。

個々のクライアントの MAC アドレスを入力するか、データベースに禁止されたクライアントのリストをインポートすることもできます。

個々のクライアントの MAC アドレスを追加するには、次の手順を実行します。
1. **コンフィグレーション>WIPS>禁止された（Banned）デバイスリスト**へ移動します。
2. **禁止されたクライアントリスト**をクリックして展開します。
3. **MAC アドレスの追加**をクリックします。 **禁止リストへの追加** が表示されます。
4. MAC アドレスを手動で追加するには、**デバイスの追加** のリンクをクリックします。
5. 追加する MAC アドレスを入力します。この方法で 1 つ以上の禁止クライアントの MAC アドレスを追加することができます。
6. 禁止デバイスリストにデバイスを追加するには、**追加** をクリックします。

ファイルからクライアントの MAC アドレスのリストをインポートすることも可能です。クライアントの MAC アドレスのリストを含むファイルは、csv ファイルである必要があります。

クライアントの MAC アドレスのリストを含むファイルをインポートするには、次の手順を実行します。
1. **コンフィグレーション>WIPS>禁止された（Banned）デバイスリスト**へ移動します。
2. **禁止されたクライアントリスト**をクリックして展開します。
3. **MAC アドレスの追加**をクリックします。 **禁止リストへの追加**が表示されます。
4. **ファイルのアップロード**をクリックします。
5. **ファイルを選択**をクリックし、選択したファイルをアップロードするには**アップロード**をクリックします。
6. 禁止デバイスリストにインポートしたクライアントの MAC アドレスを追加するには、追加 をクリックします。

禁止されたデバイスの削除

1. **コンフィグレーション>WIPS>禁止された（Banned）デバイスリスト**へ移動します。
2. デバイスを削除するには、**削除**のリンクをクリックします。削除を確認するために確認メッセージが表示されます。
3. 削除を確認し、**Yes** をクリックします。

禁止デバイスリストを別のサーバーへコピー

両方のサーバーが同じサーバークラスタの一部である場合は、片方のサーバーから別のサーバーへ禁止デバイスリストをコピーすることができます。 子サーバーから子サーバー、親サーバーから子サーバー、または子サーバーから親サーバーへ禁止デバイスリストをコピーすることができます。 サーバーから別のサーバーへポリシーをコピーするにはスーパーユーザーまたは管理者である必要があります。

禁止デバイスリストをコピーするには、次の手順を実行します。
1. 親サーバー上で、**コンフィグレーション>WIPS>禁止された（Banned）デバイスリスト**へ移動します。
2. **ポリシーをコピー**をクリックします。 **ポリシーをコピー**が表示されます。
3. 禁止デバイスリストのコピー元となるサーバーを選択します。
4. 禁止デバイスリストのコピー先となるサーバーを選択します。
5. 禁止デバイスリストをコピーするには、**OK** をクリックします。

スマートデバイスタイプの管理

コンフィグレーション>WIPS> 詳細設定>スマートデバイスタイプ を使用して、スマートデバイスタイプの閲覧、追加、削除が可能です。

スマートデバイスタイプ ページでは、システムで定義されたスマートデバイスタイプと（もしあれば）ユーザーにより定義されたスマートデバイスタイプを表示します。

スマートデバイスタイプの追加

定義済みのスマートデバイスタイプのリストに追加することができます。

新たなスマートデバイスタイプを追加するには、次の手順を実行します。
1. **コンフィグレーション>WIPS> 詳細設定>スマートデバイスタイプ** へ移動します。
2. **新しいスマートデバイスタイプを追加** をクリック。 **新しいスマートデバイスタイプを追加** のダイアログボックスが表示されます。
3. スマートデバイスタイプを入力します。
4. 既存のリストにスマートデバイスタイプを追加するには、**OK** をクリックします。

スマートデバイスタイプの削除

手動で追加されたスマートデバイスタイプのみ削除することができます。 システムで定義されたスマートデバイスタイプを削除することはできません。

ユーザーにより定義されたスマートデバイスタイプを削除するには、次の手順を実行します。
1. **コンフィグレーション>WIPS> 詳細設定>スマートデバイスタイプ** へ移動します。
2. スマートデバイスタイプを選択し、**削除**をクリックします。削除の確認を求めるメッセージが表示されます。
3. 削除を確認し、**Yes** をクリックします。

スマートデバイスタイプのリストを別のサーバーへコピー

両方のサーバーが同じサーバークラスタの一部である場合は、片方のサーバーから別のサーバーへスマートデバイスタイプのリストをコピーすることができます。 子サーバーから子サーバー、親サーバーから子サーバー、または子サーバーから親サーバーへスマートデバイスタイプのリストをコピーすることができます。 サーバーから別のサーバーへポリシーをコピーするにはスーパーユーザーまたは管理者である必要があります。

スマートデバイスタイプのリストをコピーするには、次の手順を実行します。
1. 親サーバー上で、**コンフィグレーション>WIPS> 詳細設定>スマートデバイスタイプ** へ移動します。
2. **ポリシーをコピー**をクリックします。 **ポリシーをコピー**ダイアログボックスが表示されます。
3. スマートデバイスタイプ・リストのコピー元となるサーバーを選択します。
4. スマートデバイスタイプ・リストのコピー先となるサーバーを選択します。
5. スマートデバイスタイプ・リストをコピーするには、**OK** をクリックします。

ホットスポット SSID の管理

コンフィグレーション>WIPS>詳細設定>ホットスポット SSID を使用して、ホットスポット SSID リストを設定し管理します。

ホットスポットの AP が、企業の近隣に存在する可能性は大いにあります。 よく知られているホットスポットの SSID に対して企業のクライアントが接続要求をした場合、故意ではなくユーザーがホットスポットの AP に接続する危険にさらされています。 企業 AP がホットスポットの SSID を使用した場合も、そのような AP はそれに接続する望ましくないクライアントを引き寄せることがあります。
SSID がハッカーに対して脆弱であると考えている場合は、ホットスポットの SSID 画面を開いて、SSID（ASCII 文字列）を入力することが可能です。

ホットスポット SSID の追加

デフォルトで一般的によく知られている SSID が、サーバー内にリスト化されています。

ホットスポットの SSID を追加するには、次の手順を実行します。
1. **コンフィグレーション>WIPS>詳細設定>ホットスポット SSID** へ移動します。
2. **ホットスポット SSID の新規追加**をクリックします。 **ホットスポット SSID の新規追加**が表示されます。
3. 新規のホットスポット SSID を入力し、OK をクリックします。ホットスポット SSID を持つ AP が検出された場合、システムはイベントを生成します。

ホットスポット SSID の検索

ホットスポット SSID を検索するには、次の手順を実行します。
1. **コンフィグレーション>WIPS>詳細設定>ホットスポット SSID** へ移動します。
2. 検索 SSID ボックスに検索文字列を入力し、Enter キーを押します。検索条件に一致するホットスポットの SSID のリストが表示されます。

検索文字列をクリアするには、検索 SSID ボックスの横の X アイコンをクリックします。

ホットスポット SSID の削除

ホットスポット SSID を削除するには、次の手順を実行します。
1. **コンフィグレーション>WIPS>詳細設定>ホットスポット SSID** へ移動します。
2. SSID を削除するには、**削除**のリンクをクリックします。
3. ホットスポット SSID の削除を確認する確認メッセージで **Yes** をクリックします。

デフォルトのホットスポット SSID リストへ戻す

デフォルトのホットスポット SSID リストへ戻すには、次の手順を実行します
1. **コンフィグレーション>WIPS>詳細設定>ホットスポット SSID** へ移動します。
2. **デフォルト値に戻す** をクリック。 操作の確認を求めるメッセージが表示されます。
3. **Yes** をクリックします。デフォルトのホットスポット SSID リストが復元されます。

ホットスポット SSID リストを別のサーバーへコピー

両方のサーバーが同じサーバークラスタの一部である場合は、片方のサーバーから別のサーバーへホットスポット SSID リストをコピーすることができます。 子サーバーから子サーバー、親サーバーから子サーバー、または子サーバーから親サーバーへホットスポット SSID リストをコピーすることができます。 サーバーから別のサーバーへポリシーをコピーするにはスーパーユーザーまたは管理者である必要があります。

ホットスポット SSID リストをコピーするには、次の手順を実行します。
1. 親サーバー上で、**コンフィグレーション>WIPS>詳細設定>ホットスポット SSID** へ移動します。
2. **ポリシーをコピー**をクリックします。 **ポリシーをコピー**が表示されます。
3. ホットスポット SSID リストのコピー元となるサーバーを選択します。
4. ホットスポット SSID リストのコピー先となるサーバーを選択します。
5. ホットスポット SSID リストをコピーするには、**OK** をクリックします。

脆弱な SSID の管理

コンフィグレーション>WIPS> 詳細設定>脆弱な SSID を使用して、脆弱な SSID リストを設定し管理します。

AP はよく知られているデフォルト SSID を持ち、そして多くのユーザーは AP を配置するときにこれらの SSID を変更しない可能性があります。 そのため、デフォルトの SSID を用いた AP が企業の周辺に存在する可能性が大いにあります。 デフォルトの SSID に対して企業のクライアントが接続要求をした場合、必ずしも故意ではなくユーザーが近隣の AP に接続する危険にさらされています。 企業 AP がデフォルトの SSID を使用した場合も、そのような AP はそれに接続する望ましくないクライアントを引き寄せることがあります。
脆弱な SSID の追加 SSID がハッカーに対して脆弱であると考えている場合、脆弱な SSID リストに SSID を追加することが可能です。

脆弱な SSID を追加するには、次の手順を実行します。
1. **コンフィグレーション>WIPS>詳細設定>脆弱な SSID** へ移動します。
2. **脆弱な SSID の新規追加**をクリックします。
3. 新規の脆弱な SSID を入力し、OK をクリック。脆弱な SSID を持つ AP が検出された場合、システムはイベントを生成します。

ご注意： デフォルトで一般的によく知られている SSID が、サーバー内にリスト化されています。

脆弱な SSID の検索

脆弱な SSID を検索するには、次の手順を実行します。
1. **コンフィグレーション>WIPS>詳細設定>脆弱な SSID** へ移動します。
2. 検索 SSID ボックスに検索文字列を入力し、Enter キーを押します。検索条件に一致する脆弱な SSID のリストが表示されます。

検索文字列をクリアするには、検索 SSID ボックスの横の X アイコンをクリックします。

脆弱な SSID の削除

脆弱な SSID を削除するには、次の手順を実行します。
1. **コンフィグレーション>WIPS>詳細設定>脆弱な SSID** へ移動します。
2. SSID を削除するには、**削除**のリンクをクリックします。
3. 脆弱な SSID の削除を確認するメッセージで **Yes** をクリックします。

デフォルトの脆弱な SSID リストへ戻す

デフォルトの脆弱な SSID リストへ戻すには、次の手順を実行します。
1. **コンフィグレーション>WIPS>詳細設定>脆弱な SSID** へ移動します。
2. **デフォルト値に戻す** をクリック。 操作の確認を求める確認メッセージが表示されます。
3. **Yes** をクリックします。デフォルトの脆弱な SSID リストが復元されます。

脆弱な SSID リストを別のサーバーへコピー

両方のサーバーが同じサーバークラスタの一部である場合は、片方のサーバーから別のサーバーへ脆弱な SSID リストをコピーすることができます。 子サーバーから子サーバー、親サーバーから子サーバー、または子サーバーから親サーバーへ脆弱な SSID リストをコピーすることができます。

サーバーから別のサーバーへポリシーをコピーするにはスーパーユーザーまたは管理者である必要があります。

脆弱な SSID リストをコピーするには、次の手順を実行します。
1. 親サーバー上で、**コンフィグレーション>WIPS>詳細設定>脆弱な SSID** へ移動します。
2. **ポリシーをコピー**をクリックします。 **ポリシーをコピー**ダイアログボックスが表示されます。
3. 脆弱な SSID リストのコピー元となるサーバーを選択します。
4. 脆弱な SSID リストのコピー先となるサーバーを選択します。
5. 脆弱な SSID リストをコピーするには、**OK** をクリックします。

Wi-Fi アクセス管理

SSID プロファイルの管理

管理デバイス(Management Device)がアクセスポイント(AP)として構成されるとき、1 つの物理 AP を複数の仮想 AP に分けることができます。 各仮想 AP は、同じ物理 AP 上の他の仮想 AP によって提供されるサービスを妨害することなく、 独立してサービスを提供することができます。
AP として動作する管理デバイス(Management Device)は、有線側で作成される複数の VLAN を サポートしています。

SSID プロファイルは、ネットワークのプロパティのセットです。 1 つ以上の SSID プロファイルを単一の VLAN に割り当てるまたはマッピングすることができます。

例を挙げると、有線側で異なる VLAN 構成を持つことができます。 そのうちの 1 つは企業ネットワークそして他方はゲストネットワークにサービスを提供できます。 AP として機能するように構成されている管理デバイス(Management Device)を使用して、有線側の VLAN のプロパティに 2 つ以上の 仮想 AP のマッピングを定義できます。 企業ネットワークに接続したい無線クライアントは、企業の VLAN に SSID プロファイルマッピングを使用し、 ゲストネットワークに接続したい無線クライアントはゲスト VLAN に SSID プロファイルマッピングを使用します。

仮想 AP には、次の機能があります。

- 各仮想 AP は、Open、WEP、WPA2、WPA/WPA2 (mixed mode)、IEEE802.1x セキュリティをサポートします。個別の仮想 AP は、異なるセキュリティモードを持つことができます。
- 各仮想 AP は、互いに独立している個別のサービスを提供するために使用することができます。
- 1 つの仮想 AP で送受信されるデータが、他の仮想 AP 上のそれと混合されないように、個々の仮想 AP からのデータは VLAN に割り当てることができます。このように、1 つの仮想 AP からのデータは、その仮想 AP 外では認識されません。

コンフィグレーション> デバイスのコンフィグレーション>SSID プロファイルを使用して、SSID プロファイルを設定します。
以前に定義されている SSID のリストが表示されます。
そのロケーションで SSID プロファイルを定義した場合のみ、 選択されたロケーションで SSID プロファイルを編集または削除することができます。

ご注意：同じ SSID プロファイルで BYOD 設定とキャプティブポータルの設定を構成することはできません。 それぞれを独立した SSID プロファイルで設定する必要があります。

SSID プロファイルを追加

無線 SSID プロファイルを追加するには、Wi-Fi プロファイルの新規追加をクリックします。
AP モードで動作する管理デバイス(Management Device)に対して複数の SSID プロファイルを追加することができます。 AP モードでは、単一の物理 AP デバイスは論理的に複数の仮想 AP に分割できます。 各無線プロファイルは、1 つの仮想 AP の構成設定を表現します。 複数の仮想 AP を単一の無線上で設定することができます。 このような仮想 AP は、**Wi-Fi プロファイル追加/編集** ダイアログボックスを使用して設定できます。

SSID プロファイルを追加するには、次の手順で行います。
1. 次の詳細を入力します。

フィールド	説明
プロファイル名	SSID プロファイルの名称。
SSID	SSID または SSID プロファイルのネットワーク名。
SSID ブロードキャスト	無線パケットで SSID のブロードキャストを有効または無効にします。 無線パケットで SSID をブロードキャストするには、チェックボックスにチェックを入れます。 無線パケットで SSID をブロードキャストしたくない場合は、チェックボックスの選択を解除します。
アソシエーション分析	レポートでアソシエーション分析を有効または無効にします。 レポートでアソシエーション分析を有効にするには、チェックボックスにチェックを入れます。 レポートでアソシエーション分析を無効にするには、チェックボックスの選択を解除します。
コンテンツアナリティクス	レポートでコンテンツアナリティクスを有効または無効にします。 このチェックボックスは、アソシエーション分析のチェックボックスを選択した場合のみ表示されます。 コンテンツアナリティクスは、 アクセスポイント(AP)にアソシエイトしているクライアントによってアクセスされるインターネットドメインや IP アドレスについて関連する情報を取得します。 アソシエーション分析の一部として、 インターネットドメインのアクセス情報を収集するには、チェックボックスにチェックを入れます。 この情報は、**レポート>アナリティクス**でダウンロードされる csv ファイルに保存します。 レポートでコンテンツアナリティクスを無効にするには チェックボックスの選択を解除します。

アソシエーション分析は、クライアントと AP 間の通信に関連するデータからなります。 以下のデータが、アソシエーション分析として収集されます。

- クライアントの MAC アドレス
- プロトコル
- クライアントが接続するネットワークの SSID
- クライアントのロケーション
- AP とクライアントのアソシエーションの開始時刻(GMT)
- AP とクライアントのアソシエーションの終了時刻(GMT)
- AP とクライアントのアソシエーション開始時刻（ユーザーのローカル時間）
- AP とクライアントのアソシエーション終了時刻（ユーザーのローカル時間）
- セッション継続時間
- バイト単位のクライアントデバイスからのデータ転送
- バイト単位のクライアントデバイスへのデータ転送
- Kbps のデータレート（Kbps）
- スマートデバイスの種類
- ローカルタイムゾーン
- ロケーション ID
- アクセスされたドメイン

アクセスされたドメインには、コンテンツアナリティクス情報として以下の情報が含まれています。

- ドメイン名
- ドメインへのデータ転送（バイト単位）
- ドメインからのデータ転送（バイト単位）

2. SSID プロファイルを設定する方法に基づいて、他の詳細を入力します。 それぞれの設定を構成するには、SSID プロファイルのネットワーク設定、セキュリティ設定、ファイアウォール設定、トラフィックシェービングと QoS、SSID スケジューリング、キャプティブポータル設定、BYOD - デバイスのオンボーディングの項目を参照してください。
3. 新しい SSID を保存するには、保存をクリックします。

SSID プロファイルを複製

すでに SSID プロファイルを作成している場合は、同様の SSID プロファイルを作成できます。
既存の SSID プロファイルのコピーを作成するには、次の操作を行います。
1. 複製する SSID プロファイルを開きます。
2. SSID プロファイルの新しい名前を入力します。
3. このプロファイルに必要な変更を加えます。
4. **名前を付けて保存**をクリックします。 新しい名前で SSID プロファイルが作成されます。

SSID プロファイルの編集

SSID プロファイルは、それが作成されたロケーションで編集できます。
SSID プロファイルを編集するには、次の操作を行います。
1. SSID プロファイルが作成されているロケーションを選択します。
2. 編集するプロファイル名をクリックします。
3. 必要な変更を加えます。
4. SSID プロファイルへの変更を保存するには、**保存**をクリックします。

他のロケーションへ SSID プロファイルをコピー

他のロケーションに既存の SSID プロファイルのコピーを作成するには、次の操作を行います。
1. SSID プロファイルページで、他のロケーションにコピーする SSID プロファイルのチェックボックスにチェックを入れます。
2. コピー先アイコンをクリックします。
3. SSID プロファイルをコピーするロケーションを選択します。 選択された SSID プロファイルのコピーが選択されたロケーションに作成されます。

SSID プロファイルの削除

デバイステンプレートで使用されている場合は、 SSID プロファイルを削除することはできません。
選択されたロケーション（SSID プロファイルを定義したロケーションでのみ）で SSID プロファイルを削除することができます。
SSID プロファイルを削除するには、次の操作を行います。
1. SSID プロファイルが作成されているロケーションを選択します。
2. SSID プロファイルの削除アイコンをクリックします。削除を確認するメッセージが表示されます。

ロケーションの SSID プロファイルリストを印刷

ロケーションで定義されている SSID プロファイルリストを印刷することができます。
ロケーションの SSID プロファイルリストを印刷するには、次の手順を実行します。

1. SSID プロファイルタブをクリックします。
2. 印刷したいリストの列を選択します。 列を選択または解除するには、任意の列名をクリックします。
3. 印刷アイコンをクリックします。リストの印刷プレビューが表示されます。
4. リストを印刷するには、**印刷**をクリックします。

セキュリティ設定

仮想 AP のセキュリティ設定は、次のいずれかになります。

- **Open**: Open はセキュリティ設定が適用されないことを意味します。 これは、デフォルトのセキュリティ設定です。
- **WEP**: WEP は Wireless Equivalent Privacy の略です。 WEP は IEEE802.11 ネットワークにとって非推奨のセキュリティアルゴリズムです。 これは下位互換性の目的のために提供されています。
- **WPA**: WPA は Wi-Fi Protected Access の略です。 これは、WEP の欠点を解消するセキュリティプロトコルです。WPA を設定する場合は WPA and WPA2 mixed mode を選択してください。
- **WPA2**: WPA2 は、IEEE 802.11i スタンダードに準拠した最新のより堅牢なセキュリティプロトコルです。
- **WPA and WPA2 mixed mode**: これは WPA と WPA2 プロトコルが混在するモードです。

PSK は、 一般的に小規模オフィスのネットワークに使用されます。

大きな企業ネットワークの場合には、RADIUS 認証が使用されます。 複数のポイント間でネットワークポリシーを伝達するために、企業は、ときには RADIUS を使用します。 ユーザーはグループに分割され、ポリシーは効果的にネットワークリソースへのアクセスを制御するために、各グループに適用されます。 各ユーザーグループは、そのユーザーグループに適用されるポリシーに基づいて別の VLAN にリダイレクトされます。 例えば、営業部は人事部がアクセスする VLAN とは異なる VLAN へアクセスします。

アクセスポイント(AP)は、RADIUS サーバーから RADIUS ユーザーと関連する VLAN を取り出すことができます。 このオプションは、SSID プロファイルで IEEE802.1x が有効になっている、WPA2 および WPA and WPA2 mixed mode で使用することが可能です。

RADIUS サーバーにより返される VLAN に基づいて、 アクセスポイント(AP)は、RADIUS 認証されたユーザーのネットワークトラフィックをユーザーが属するグループと関連する VLAN にダイナミックにリダイレクトします。 RADIUS サーバーがユーザーを認証するまで、EAP パケットはデフォルトの VLAN を通過します。
ご注意：SSID プロファイルのネットワーク設定で設定された VLAN ID はデフォルト VLAN として使用されます。

VLAN の RADIUS ベースの割り当てを有効にするには、SSID プロファイル上でダイナミック VLAN を有効にする必要があり、RADIUS ユーザーがリダイレクトされることができるダイナミックな VLAN のリストを指定する必要があります。 ユーザーグループに固有の VLAN が存在しない場合、デフォルトの VLAN が使用されます。

次の RADIUS アトリビュートは、RADIUS サーバーとアクセスポイント(AP)との通信のためにユーザーグループごとに RADIUS 側で設定されている必要があります。

アトリビュート	値
Tunnel Type	VLAN に設定。
Tunnel Medium Type	802 に設定。
Tunnel Private Group ID	ユーザーグループに割り当てられる VLAN ID を入力。

セキュリティ設定

次の表は、**SSID プロファイルの追加/編集**や **セキュリティ設定**のフィールドを説明しています。
セキュリティの設定 でフィールドを表示するには、 **セキュリティ設定**をクリックします。

フィールド	説明	デフォルト値
クライアントアイソレーション	このチェックボックスは、この仮想 AP の 2 台の無線クライアント間の通信が可能かどうかを示します。 選択した場合、仮想 AP で無線クライアント通信が無効になります。	チェックボックスは選択されていない（仮想 AP で無線クライアント間の通信が有効であることを示す）。
セキュリティモード	仮想 AP に適用されるセキュリティモードを指定します。 可能な値は、Open、WEP、WPA2、WPA and WPA2 mixed mode です。	Open
セキュリティモード WEP に関連するフィールド		
認証タイプ	認証タイプがオープンの場合は、 **Open** を選択します。 オープン認証の場合、鍵は暗号化にのみ使用されます。 認証タイプが共有キーの場合は、**Shared** を選択します。 共有キー認証の場合は、同じキーが暗号化と認証の両方で使用されます。	Open
WEP Type	40 ビットの WEP セキュリティを使用する場合は **WEP40** を選択します。 104 ビットの WEP セキュリティを使用する場合は **WEP104** を選択します。	WEP104
Key Type	ASCII 形式に慣れていて、その形式で WEP キーを入力する場合は **ASCII** を選択します。 16 進数形式に慣れていて、その形式で WEP キーを入力する場合は **HEX** を選択します。	ASCII
キー	WEP タイプが WEP40 の場合は、選択されたキーの種類に応じて、5 文字の ASCII 文字キーまたは 10 桁の 16 進キーとしてキーを入力します。 WEP タイプが WEP104 の場合は、選択されたキーの種類に応じて、13 文字の ASCII 文字キーまたは 26 桁の 16 進キーとしてキーを入力します。	空白
キーを表示	画面上に実際のキーを表示するには、このチェックボックスにチェックを入れます。このチェックボックスのチェックを外すと、キーがマスクされます。	クリア
セキュリティモード WPA2/WPA and WPA2 mixed mode に関連するフィールド		
PSK	パーソナルシェアードキーを使用する場合は、**PSK** を選択します。 このオプションを選択すると、 **パスフレーズ** のフィールドが有効になります。	PSK
Pass Phrase	PSK 認証用の長さ 8-63 の ASCII 文字の共有キーを指定します。	空白
キーを表示	画面上に実際のキーを表示するには、このチェックボックスにチェックを入れます。このチェックボックスのチェックを外すと、キーがマスクされます。	クリア

IEEE802.1x	認証に RADIUS サーバーを使用する場合は、**IEEE802.1x** を選択します。 **認証**と**アカウンティング**のタブのフィールドは、このオプションを選択することで有効になります。	クリア
Opportunistic Key Caching	オポーチュニスティック・キー・キャッシュを使用してクライアントの高速ハンドオフを有効にするには、このチェックボックスにチェックを入れます。 キー・キャッシュは同じサブネット内のみ（サブネットを超えない）で機能する点に注意してください。	選択済み
Pre-Authentication	事前認証方式を使用して、クライアントの高速ハンドオフを可能にするには **Pre-Authentication** チェックボックスにチェックを入れます。	クリア
認証 タブフィールド ― プライマリ RADIUS サーバー エリア		
サーバーIP	ここにプライマリ RADIUS サーバーの IP アドレスを入力します。	空白
ポート番号	プライマリ RADIUS サーバーがクライアントのリクエストを受け取るポート番号を入力します。	1812
共有鍵	プライマリ RADIUS サーバーと AP 間の共有鍵を入力します。	空白
RADIUS 認証　セカンダリ認証サーバー エリア		
サーバーIP	ここにセカンダリ RADIUS サーバーの IP アドレスを入力します。	空白
ポート番号	セカンダリ RADIUS サーバーがクライアントのリクエストを受け取るポート番号を入力します。	1812
共有鍵	セカンダリ RADIUS サーバーと AP 間の共有鍵を入力します。	空白
アカウンティングサーバーの詳細 ― プライマリアカウンティングサーバー エリア		
サーバーIP	ここにプライマリアカウンティングサーバーの IP アドレスを入力します。	空白
ポート番号	プライマリアカウンティングサーバーがクライアントのリクエストを受け取るポート番号を入力します。	1813
共有鍵	プライマリアカウンティングサーバーと AP 間の共有鍵を入力します。	空白
アカウンティングサーバーの詳細 ― セカンダリアカウンティングサーバー エリア		
サーバーIP	ここにセカンダリアカウンティングサーバーの IP アドレスを入力します。	空白
ポート番号	セカンダリアカウンティングサーバーがクライアントのリクエストを受け取るポート番号を入力します。	1813
共有鍵	セカンダリアカウンティングサーバーと AP 間の共有鍵を入力します。	空白

SSID プロファイルのネットワーク設定

ネットワークセクションを使用して、NAT デバイスで使用される VLAN と DHCP 設定を構成します。

ネットワーク設定

ゲストクライアントは、特定のサーバーにのみ DNS クエリを行うことが許可されます。 DNS サーバー下でサーバーの IP アドレスまたは Web サイト名をカンマで区切って入力することで、少なくとも 1 つの DNS サーバーを指定します。
最大 3 つの DNS サーバーの IP アドレスを指定できます。 DNS サーバー下で指定されていない DNS サーバーへのリクエストはドロップされます。 ゲストユーザーは、自分で選択した DNS サーバーを構成することはできません。 OpenDNS のような外部のサービスを使用することで、どのようなタイプのサイトが解決されるか管理することができ、ゆえにゲストが許可されます。

NAT のパラメータを設定している場合は、少なくとも 1 つの DNS サーバーを指定する必要があります。 アソシエーションの成功により、無線クライアントは指定された DNS サーバーを取得します。このような DNS サーバーIP アドレスを最大 3 つ指定することができます。

GRE (Generic Routing Encapsulation)は、単一のエンドポイントから、そして、それにネットワークトラフィックのルートを決めて、このエンドポイントでポリシーを適用したい場合に役立ちます。

ご注意： GRE は NAT が有効になっている場合のみ機能します。

ネットワークアドレス変換の設定を構成するには、次の手順を実行します。
1. ブリッジや NAT の設定が適用可能な VLAN ID を指定します。
2. 必要に応じて Enable Proxy ARP setting、Disable DGAF のチェックボックスにチェックを入れます。

フィールド	説明
Enable Proxy ARP setting	"[Enable(チェックを入れている時)] 無線配下の子機から送信された ARP パケット(Broadcast)に対して管理デバイス(Management Device)が代理で ARP Reply を返す機能が有効になります。 Disable の場合、管理デバイス(Management Device)は ARP パケット(Broadcast)に対してすべて有線ネットワークへ転送してしまい、有線側トラフィックに影響がでます。 これを回避するために Enable にすることで、管理デバイス(Management Device)内の ARP テーブルに該当する ARP テーブルがある場合、子機へ代理応答を行います。 [Disable(チェックを外している時)] 上記のとおり、代理応答をしないため、子機から来た ARP パケット(Broadcast)をすべて有線側に転送します。〃
Disable DGAF	"DGAF(Downstream Group Addressed Forwarding)を無効にすることで、hole196 attack という不正攻撃を軽減することができます。 hole196 attack とは AES 暗号の脆弱性を突いた攻撃で、同じ SSID 配下にいる別の子機が不正なトラフィックを行うことで、同一 SSID 上の無線通信を止めてしまう攻撃です。 DGAF を Disable にすることで管理デバイス(Management Device)から子機へのグループアドレスに関する通信をブロックするようになり、hole196 attack から守ることができます。 [Enable(チェックを外している時)] 本件のとおり、マルチキャストストリーミングがそのまま転送されるため、無線上でマルチキャストが流れます。 [Disable(チェックを入れている時)] 管理デバイス(Management Device)からすべての子機に対するマルチキャストストリーミング通信を止めます。これにより、hole196 攻撃からネットワークを守ることができます。同時に、マルチキャストのストリーミングが流れなくなります。通信が停まるものは、DHCP offer 以外のすべてのマルチキャストです。ビデオサーバーからのストリーミングといった映像配信サービスに影響します。"

3. NAT を有効にする場合は、NAT のチェックボックスにチェックを入れます。
4. NAT 有効にした場合は、以下の NAT 関連の設定を指定します。

フィールド	説明
NAT	NAT（ネットワークアドレス変換）を有効にするには、 このチェックボックスにチェックを入れます。
開始 IP アドレス	選択されたネットワーク ID での DHCP アドレスプールの開始 IP アドレス。
終了 IP アドレス	選択されたネットワーク ID での DHCP アドレスプールの終了 IP アドレス。IP アドレスの払い出し数は終了 IP-開始 IP より 1 つ少ない数になります。例えば開始 IP を 192.168.1.2、終了 IP を 192.168.1.5 とした場合、払い出し数は 3 つです。
ローカル IP アドレス	DHCP アドレスプールの外側に選択されたネットワーク ID 内の IP アドレス。このアドレスは、ゲスト無線ネットワークのゲートウェイアドレスとして使用されます。

サブネットマスク	選択したネットワーク ID のネットマスク。
リース期間	分単位の DHCP リリース期間。 最小値 30 分、最大値 1440 分。
DNS サーバー	無線クライアントが DNS クエリを行うことができる DNS サーバー。

5. GRE (Generic Routing Encapsulation) はトンネルプロトコルの 1 つです。 GRE は、単一のエンドポイントからネットワークトラフィックのルートを決めて、このエンドポイントでポリシーを適用したい場合に役立ちます。

   次の表は、GRE 関連のフィールドについて説明します。

フィールド	説明
GRE	GRE を有効にするには、このページ上の GRE 関連のパラメータを定義することができるように、 チェックボックスにチェックを入れます。
トンネル IP アドレス	アクセスポイント上の GRE トンネルインタフェースの IP アドレス。 この IP アドレスは、アクセスポイント内の他のネットワーク設定と競合しないようにしてください。
リモートエンドポイントの IP アドレス	GRE トンネルのリモートエンドポイントの IP アドレス。
キー	GRE ヘッダー内のキー。 設定されている場合、キーはトンネルの両端で同じである必要があります。 キーは、GRE トンネルで構成することは必須ではありません。
除外ホスト/ネットワーク一覧	GRE トンネルの使用を 除外された、（カンマで区切られた）ネットワークおよび（または）IP アドレスの一覧。

6. ネットワーク設定の変更を保存するには、保存をクリックします。

ネットワーク設定の編集

ネットワークアドレス変換の設定を編集するには、次の手順を実行します。
1. NAT 設定が適用可能な VLAN ID を指定します。
2. NAT を無効にし、ブリッジネットワークにしたい場合は、NAT のチェックボックスのチェックを外します。 NAT の使用を継続したい場合は、必要に応じてそれらを編集します。
3. GRE（Generic Routing Encapsulation）を有効にする場合は、GRE を選択します。
   GRE を使用しない場合は、GRE チェックボックスを無効にします。
4. ネットワーク設定の変更を保存するには、**保存**をクリックします。

キャプティブポータル設定

キャプティブポータルは、クライアントがインターネットにアクセスしようとする際に、 ネットワーク上のクライアントが誘導される Web ページです。
クライアントは、このページで認証され、認証が成功したあとにインターネットにアクセスすることができます。

制限された無線接続（例えば、インターネットのみ）をゲスト無線クライアントへ提供するために、ゲストネットワークとして機能するために無線プロファイルを構成することができます。
Management Device では、そのような複数のゲストネットワークに対応しています。

サポートされているキャプティブポータルの種類

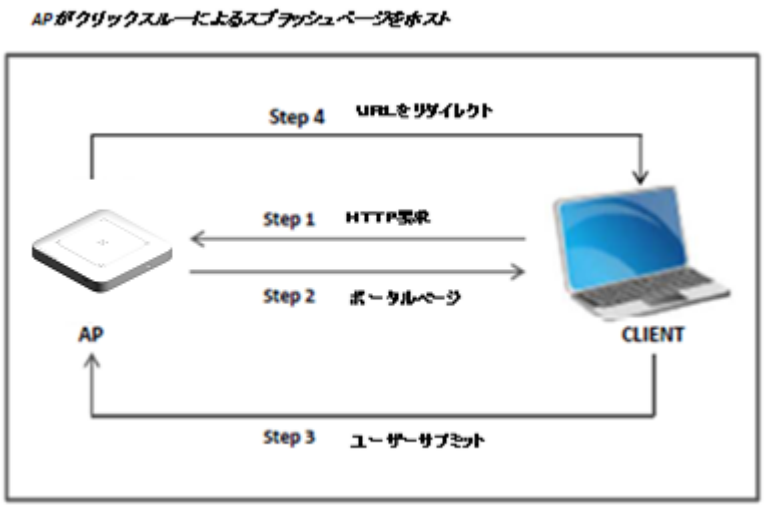
次の 3 種類が Management Device でサポートされています。
1. AP がクリックスルーでスプラッシュページをホスト
2. サインインまたはクリックスルー用の外部スプラッシュページ
3. RADIUS 認証による外部スプラッシュページ

これらは、以下で詳細に説明します。

1. AP がクリックスルーでスプラッシュページをホスト：‘クリックスルー’スプラッシュページは、認証がサポートされていないスプラッシュページです。 ポータルページが AP によってホストされ提供されます。 ポータルページは必要に応じて他の情報と同様に、ゲストネットワークアクセスの利用条件を表示するために 使用できます。

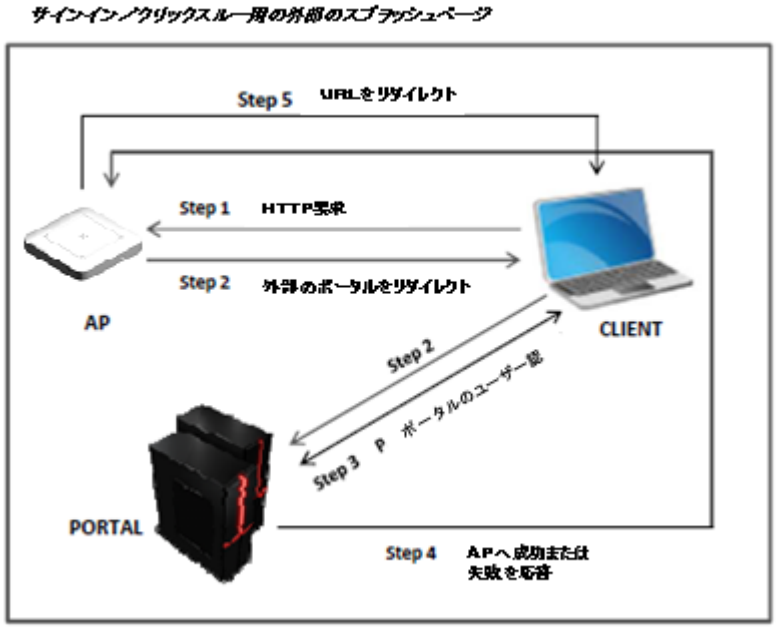
   このタイプのアクセスに必要な手順は、以下のとおりです。
   (a) Wi-Fi ユーザーはゲスト SSID に接続して、 HTTP プロトコルを用いた任意の Web ブラウザから、URL をオープンします。
   (b) アクセスポイント(AP)は、この要求をインターセプトし、 ゲストユーザーへ AP 上でホストされているポータルページをスルーします。
   (c) ゲストユーザーは、利用条件に同意しポータルページに送信します。
   (d) AP はクライアントのためにゲートを開き、クライアントはリダイレクトする URL、または元のリクエストされた URL にリダイレクトされます。

   以下は、 「AP がクリックスルーでスプラッシュページをホスト」の図です。



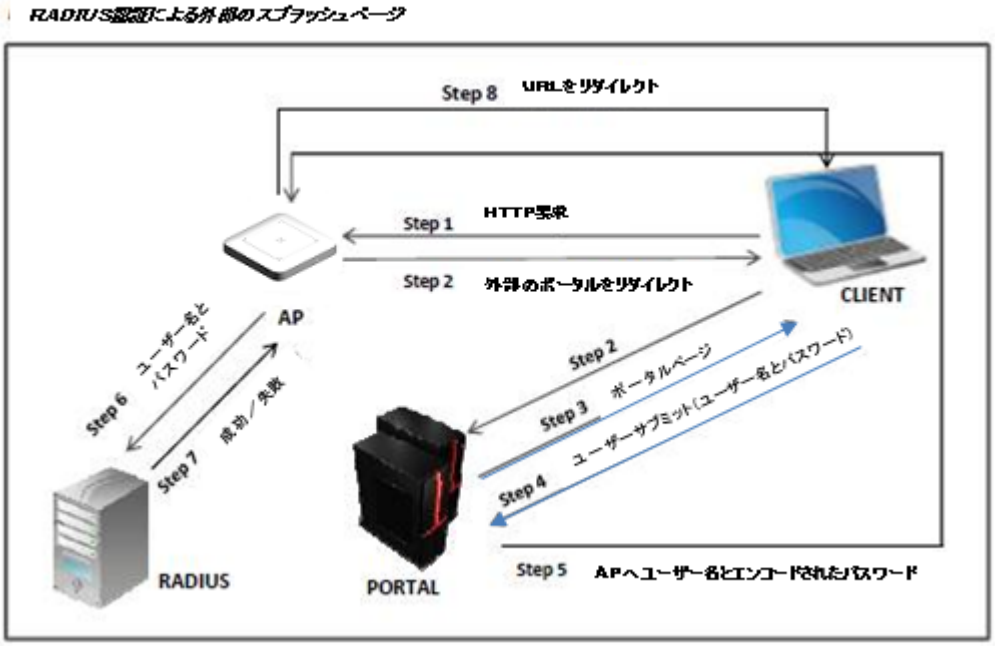
2. サインイン/クリックスルー用の外部スプラッシュページ： 外部サーバーでホストされているポータルです。
ポータルは、 認証なしのクリックスルーまたは適当な独自の認証メカニズムを持っているかのどちらかです。
このタイプのアクセスに必要な手順は、以下のとおりです。
(a) Wi-Fi ユーザーはゲスト SSID に接続して、 HTTP プロトコルを用いた任意の Web ブラウザから、URL をオープンします。
(b) アクセスポイント(AP)は、この要求をインターセプトして、 リダイレクトされた URL の Get パラメータとしてリクエストパラメータと一緒に設定された外部のポータルページにブラウザをリダイレクトします。
(c) ポータルは、無線ユーザーにサインインまたはクリックスルースプラッシュページを促すことにより、 ゲストユーザーを認証します。
(d) 認証後、ポータルは成功または失敗応答でクライアントを AP にリダイレクトします。 AP とポータルが共有鍵で構成されている場合、ポータルは、AP がポータルから応答を確認する検証コードを送ります。 AP とポータルの間で共有鍵を使うことは、なりすまし攻撃を使ってアクセスを得る偽のユーザーを回避することになります。
(e) 検証の成功後に、 AP はクライアントに対してゲートを開き、クライアントはリダイレクトする URL、 または元のリクエストされた URL にリダイレクトされます。

以下は、 「 サインイン/クリックスルー用の外部スプラッシュページ」の図です。



3. **RADIUS 認証による外部スプラッシュページ：** ゲストユーザーは外部サーバーでホストされているポータルにリダイレクトされます。 外部のポータルにログインしたときにゲストユーザーは、RADIUS サーバーによって認証されます。
   このタイプのアクセスに必要な手順は、以下のとおりです。
   (a) Wi-Fi ユーザーはゲスト SSID に接続して、 HTTP プロトコルを用いた任意の Web ブラウザから、URL をオープンします。
   (b) アクセスポイント(AP)は、この要求をインターセプトして、 リダイレクトされた URL の Get パラメータとしてリクエストパラメータと一緒に設定された外部のポータルページにブラウザをリダイレクトします。
   (c) ポータルは、 ユーザー名とパスワードを入力するようにスプラッシュページをユーザーに促します。
   (d) ユーザーは、ユーザー名とパスワードを送信します。
   (e) ポータルはユーザー名と共有鍵を用いてエンコードされたパスワードで、 ゲストユーザーを AP にリダイレクトします。
   (f) アクセスポイント(AP)は、 ユーザー名とデコードされたパスワードを使用して RADIUS サーバーによってゲストユーザーを認証します。
   (g) RADIUS サーバーは、ゲストユーザーへアクセスの受け入れまたは拒否メッセージを返信します。
   (h) AP は、クライアントのためにゲートを開き、 クライアントはリダイレクトする URL、または元のリクエストされた URL にリダイレクトされます。

   以下は、「 RADIUS 認証による外部スプラッシュページ」の図です。



ウォールドガーデンをセットアップ

ウォールドガーデンは、インターネットへの制限付きアクセスを提供する方法です。 ウォールドガーデンの宛先は、スプラッシュページを表示せずに、指定したポート番号でアクセスすることができます。 また Domain (例 domain.com) は、そのサブドメイン (例 subdomain.domain.com) をカバーします。

除外されるドメイン、サブドメイン、IP アドレス範囲、およびポート番号のリストを設定します(例 192.168.1.0/24)。 これらの IP アドレス上のサービスは、ポータルページへのリダイレクトなしでアクセスできます。 ポータルページの一部分（例えば画像ファイルなど）が Web サーバーに配置されているならば、 Web サーバーの IP アドレスは内容が正常に示されるためにこのリストに含まれる必要があります。

ウォールドガーデンを設定するには、次の操作を行います。
1. **追加** をクリックします。**宛先追加** ダイアログがオープンします。
2. 詳細を入力します。

フィールド	説明
デスティネーション	ルールが適用される、 ドメイン名、サブドメイン名、ホスト名、サブネットまたは IP アドレス。 ここで複数のホスト名のリストを提供することができます。 例： 192.168.8.173 www.facebook.com 192.168.121.0/24
デフォルトポート	ポート番号。 ここに ポート番号またはポート範囲のカンマ区切りのリストを提供することができます。 例： 20-22,80,443.

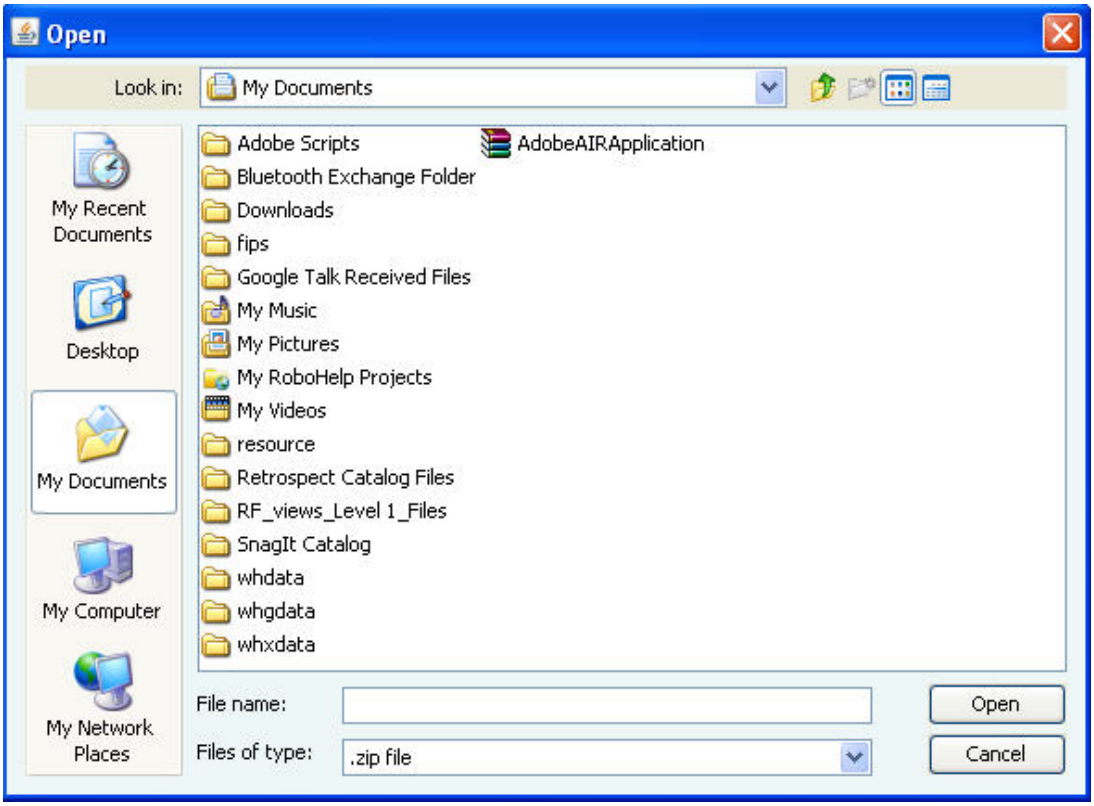
3. 除外される宛先を削除するには、エントリを選択し、**削除**をクリックします。

キャプティブポータル設定を構成

キャプティブポータル設定を行うには、次の操作を行います。

1. ゲストネットワークを用いるクライアントへ提示されるポータルページを表示するために、 キャプティブポータルを有効 チェックボックスにチェックを入れます。
2. キャプティブポータルを介すインターネットへのアクセスモードを選択します。 以下のいずれかを行います。
   (a) オプションをクリックして、 AP がクリックスルー用のスプラッシュページをホスティングを選択します。 イメージ、スタイルシートなどのような任意の他のファイルとともにポータルページの.zip ファイルを作成し、 このファイルをアップロードする必要があります。 zip ファイルが 正常に動作するようにポータルの次の要件を満たす必要があります。
      i. zip ファイルには、ルート層に名前が index.html のファイルを持つ必要があります（すなわち、任意の他のフォルダーの外側）。 これは、ポータルページのメインです。 それは、index.html ファイルで参照されるルート層で、 他のファイルとフォルダー（とフォルダー内のフォルダー）を持つことができます。
      ii. バンドル内の解凍されたファイルの合計サイズは、100 KB 未満である必要があります。 大きな画像やその他のコンテンツがページ上に表示される場合は、このコンテンツは、 index.html ファイルからの参照で外部 Web サーバー上に配置することができます。 この場合、外部 Web サーバーの IP アドレスは除外されるホストのリストに含まれなければなりません。
      iii. index.html ファイルは、ポータルが正しく動作するために、以下の HTML タグが含まれている必要があります：
         - 正確な開始タグを持つフォームエレメント ：<form method="POST" action="$action">
         - “mode_login”の名前を持つ上記のフォームエレメント内のサブミットボタン。 例： <input type=”image” name=”mode_login” src=”images/login.gif”> 上記フォームエレメント内の正確なタグ： <input type="hidden" name="redirect" value="$redirect"> 。

   工場出荷時のデフォルトのポータルバンドルファイルをダウンロードし、 カスタムポータルバンドルを作成するためのテンプレートとして使用できます。 工場出荷時のデフォルトのポータルバンドルファイルをダウンロードするには、 **サンプルダウンロード** をクリックします。
   ポータルバンドル（デフォルトまたはカスタム）をアップロードします。 バンドルをアップロードするには**バンドルをアップロード** のあとに続く **ファイルの選択** をクリックします。



ポータルバンドルをアップロードするには、開くをクリックします。

ポータルバンドルを工場出荷時のデフォルトのファイルへ戻すには、 **デフォルトに戻す** をクリックします。

(b) **サインイン/クリックスルー用の外部スプラッシュページ** を選択します。 無線ユーザーが外部のポータルにリダイレクトされる **スプラッシュページ URL** を指定します。 このポータルは、無線ユーザーにユーザー名とパスワードの入力を促します。 必要に応じて、共有鍵のチェックボックスを選択し、SSID（外部ポータル通信用の）共有鍵を指定する必要があります。

(c) **RADIUS 認証による外部スプラッシュページ** を選択します。
この場合、次のフィールドを指定する必要があります
無線ユーザーが外部のポータルにリダイレクトされる **スプラッシュページ URL** を指定します。 SSID（外部ポータル通信用の）共有鍵を指定する必要があります。 AP が無線ユーザーを実際に認証する RADIUS サーバー設定を構成するために、RADIUS 設定をクリックします。プライマリおよび必要に応じて、セカンダリ認証サーバーの詳細を指定します。

フィールド	説明
Called Station ID	AP が認証プロセス中に、標準の RADIUS パラメータ（'Called-Station-ID '）で RADIUS サーバーに渡す自由形式のテキストパラメータ。 特別な書式指定子 '%m'は、AP のイーサネット MAC アドレスに拡張され 指定することができます。
プライマリ認証サーバーの詳細	
サーバーIP	プライマリ認証サーバーの IP アドレス。
ポート番号	クライアントの要求を受け取るプライマリ認証サーバーのポート番号。
共有鍵	AP とプライマリ認証サーバー間の共有鍵。
セカンダリ認証サーバーの詳細	
サーバーIP	セカンダリ認証サーバーの IP アドレス。
ポート番号	クライアントの要求を受け取るセカンダリ認証サーバーのポート番号。
共有鍵	AP とセカンダリ認証サーバー間の共有鍵。

RADIUS アカウンティングを有効にしたい場合は、アカウンティングのチェックボックスにチェックを入れて、 AP が無線ユーザーを実際に認証するアカウンティングの詳細を指定します。 RADIUS サーバーの設定で、 RADIUS サーバーが稼働している**サーバーの IP** と**ポート**を指定します。

フィールド	説明
インターバル	アカウンティング・インターバル（分単位）。 最小間隔は 1 分で、最大の間隔は 60 分とすることが可能。
プライマリアカウンティングサーバーの詳細	
サーバーIP	プライマリアカウンティングサーバーの IP アドレス。
ポート番号	クライアントの要求を受け取るプライマリアカウンティングサーバーのポート番号。
共有鍵	AP とプライマリアカウンティングサーバー間の共有鍵。
セカンダリアカウンティングサーバーの詳細	
サーバーIP	セカンダリアカウンティングサーバーの IP アドレス。
ポート番号	クライアントの要求を受け取るセカンダリアカウンティングサーバーのポート番号。
共有鍵	AP とセカンダリアカウンティングサーバー間の共有鍵。

3. 外部ポータルパラメータを設定します。詳細については、下記の外部ポータルパラメータの設定 を参照してください。
4. 無線クライアントがある AP から他へローミングした際にスプラッシュページを表示したくない場合は、 **ローミング** チェックボックスにチェックを入れます。

5. インターネットに接続後、インターネット接続を失った場合にポータルエラーページを表示したい場合は、**インターネット接続の検出を有効** チェックボックスにチェックを入れます。
   インターネットがゲスト SSID 上で一時的に利用できないとき、'インターネット接続の検出を有効'機能はゲストにフィードバックを提供するために用いることが可能です。 アクセスポイント(AP)は、インターネット接続がゲスト VLAN から利用可能でないことを検出すると、 自動的にインターネットが一時的に使用できないメッセージと共にスプラッシュページへのゲストユーザーのすべての HTTP 要求をリダイレクトします。 **AP がクリックスルーでスプラッシュページをホスト** を使用している場合は、 “NoInternet.html”という名前でバンドルに含まれているカスタマイズされたスプラッシュページが インターネットがダウンした際に表示されます。 このページがバンドルに含まれていない場合、または外部スプラッシュページが設定されている場合、 インターネットがダウンすると AP は工場出荷時のスプラッシュページを表示します。
   インターネットがダウンしているとき、**インターネット接続の検出を有効**にする機能が有効になっている場合だけでなく、 ゲストユーザーはローカルの HTTP サービスにアクセスすることができなくなることに注意してください。
   インターネット接続の検出を有効 にする機能は、 GRE を設定した SSID プロファイルでは動作しません。
6. ポータルページを設定したあとに無線ユーザーがゲストネットワークにアクセスすることができるための、 **ログインタイムアウト**（分単位）を指定します。
   タイムアウト後に、ゲストネットワークへのアクセスを停止しポータルページが再び表示されます。 ユーザーは、ゲストネットワークへのアクセスを回復するために、ポータルページを設定しなければなりません。 ユーザーがセッションタイムアウト前にゲストネットワークに対して切断し、そして再接続した場合は スプラッシュページで資格情報を入力する必要はありません。
7. 分単位で、**ブラックアウト時間**を指定します。 これは、ユーザーが前の成功したセッションをタイムアウトしたあとに、ログインが許可されない時間です。
   例えば、 セッションタイムアウトが 1 時間で、ブラックアウト時間が 30 分である場合、ユーザーは成功したログインの 1 時間後にタイムアウトします。 このポイントのあと、ユーザーは 30 分間再度ログインすることができません。 30 分経過すると、ユーザーは再度ログインすることができます。
8. **リダイレクト URL** を指定します。 ユーザーがポータルページで送信ボタンをクリックしたあと、ブラウザにはこの URL がリダイレクトされます。
   空白のままにすると、ブラウザはポータルページが表示されていたブラウザから本来のアクセスする URL にリダイレクトされます。
9. **外部ポータルパラメータ**で定義した**サービス識別子**の値を指定します。 これは、外部ポータルに渡すことができる自由形式のパラメータです。
   このパラメータは、 SSID プロファイルに特定の機能を実装するために、外部ポータルによって使用することができます。 例えば、それぞれの SSID は別々のポータルページを持つことができます。
10. 設定を保存するには、**保存**をクリックします。

外部ポータルパラメータの設定

外部サーバーでホストされるポータルページにユーザーをリダイレクトする場合は、外部のポータルパラメータを設定する必要があります。

アスタリスクでマークされているすべてのリクエストとレスポンスの属性が必須です。 リクエストパラメータ/属性は外部のポータルに、AP から送信されます。 レスポンスパラメータは、AP に外部のポータルから送信されます。 次の表は、詳細なリクエストとレスポンスの属性を説明しています。

リクエスト属性	**説明**
リクエストタイプ	要求タイプフィールドのフィールド名。
Challenge*	認証に使用されるランダムテキストのフィールド名。
Client MAC アドレス	クライアントの MAC アドレス用のフィールド名。
AP IP アドレス*	外部ポータルと通信しているアクセスポイント(AP)の MAC アドレスのフィールド名。
AP IP アドレス	外部ポータルと通信しているアクセスポイント(AP)の IP アドレスのフィールド名。 これは、外部のポータルで使用されるフィールド名と一致する必要があります。
AP ポート番号*	AP と外部サーバーが通信する AP のポート番号のフィールド名。
失敗回数	ログイン試行の失敗数のカウントのフィールド名。
リクエスト URL	要求された URL のフィールド名。 AP を介してクライアントから要求された（外部サーバーへの）URL。
ログイン URL*	ログイン URL のフィールド名。
ログオフ URL	ログオフ URL のフィールド名。
残りのブラックアウト時間	残りブラックアウト時間のフィールド名。
サービス識別子	外部ポータルへサービス識別子の値を渡すために使用されるポータルパラメータの名前。 サービス識別子の値は、SSID プロファイルのキャプティブポータルセクションで指定されている。 異なる SSID などのために異なるポータルのような SSID プロファイル特定機能を実装するために、外部ポータルによって使用することが可能。
レスポンス属性	**説明**
Challenge*	Challenge のフィールド名。
レスポンスタイプ*	レスポンスタイプのフィールド名。
Challenge レスポンス*	Challenge レスポンスタイプのフィールド名。
リダイレクト URL	リダイレクト URL のフィールド名。
ログインタイムアウト	ログインタイムアウトのフィールド名。
ユーザー名*	ユーザー名のフィールド名。
パスワード*	パスワードのフィールド名。
ご注意： AP によって使用される個々のフィールド名は、ポータルをホストしている外部サーバーによって使用される対応するフィールド名と一致する必要があります。 同じパラメータの名前がいずれかの側で異なる場合、AP と外部サーバーは通信することができない可能性があります。 **外部**	

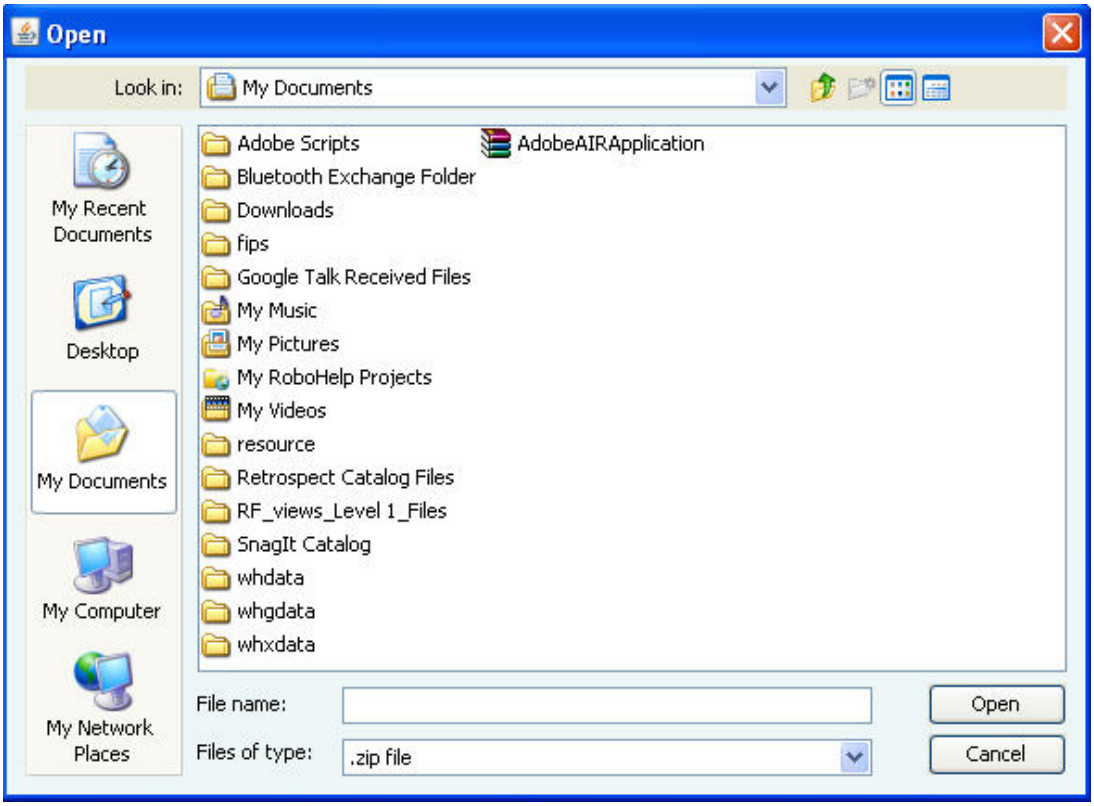
ポータルパラメータ のフィールドは、管理デバイス(Management Device)のフィールド名の変更を容易にします。

キャプティブポータル設定の編集

キャプティブポータルの設定を編集するには、次の操作を行います。

1. ゲストネットワークを用いるクライアントへ提示されるポータルページを表示するために、 **キャプティブポータルを有効**チェックボックスにチェックを入れます。
2. キャプティブポータルを介すインターネットへのアクセスモードを選択します。 以下のいずれかを行います。
   (a) オプションをクリックして、 AP がクリックスルー用のスプラッシュページをホスティングを選択します。 イメージ、スタイルシートなどのような任意の他のファイルとともにポータルページの.zip ファイルを作成し、 このファイルをアップロードする必要があります。 zip ファイルが 正常に動作するようにポータルの次の要件を満たす必要があります。
      i. zip ファイルには、ルート層に名前が index.html のファイルを持つ必要があります（すなわち、任意の他のフォルダーの外側）。 これは、ポータルページのメインです。 それは、index.html ファイルで参照されるルート層で、 他のファイルとフォルダー（とフォルダー内のフォルダー）を持つことができます。
      ii. バンドル内の解凍されたファイルの合計サイズは、100KB 未満である必要があります。 大きな画像やその他のコンテンツがページ上に表示される場合は、このコンテンツは、 index.html ファイルからの参照で外部 Web サーバー上に配置することができます。 この場合、外部 Web サーバーの IP アドレスは除外されるホストのリストに含まれなければなりません。
      iii. index.html ファイルは、ポータルが正しく動作するために、以下の HTML タグが含まれている必要があります。
         - 正確な開始タグを持つフォームエレメント ： <form method="POST" action="$action">
         - “mode_login”の名前を持つ上記のフォームエレメント内のサブミットボタン。 例： <input type=”image” name=”mode_login” src=”images/login.gif”>上記フォームエレメント内の正確なタグ： <input type="hidden" name="redirect" value="$redirect"> 。

   工場出荷時のデフォルトのポータルバンドルファイルをダウンロードし、 カスタムポータルバンドルを作成するためのテンプレートとして使用することができます。 工場出荷時のデフォルトのポータルバンドルファイルをダウンロードするには、 **サンプルダウンロード**をクリックします。
   ポータルバンドル（デフォルトまたはカスタム）をアップロードします。 バンドルをアップロードするには**バンドルをアップロード** のあとに続く **ファイルの選択** をクリックします。



ポータルバンドルをアップロードするには、開くをクリックします。
ポータルバンドルを工場出荷時のデフォルトのファイルへ戻すには、 **デフォルトに戻す**をクリックします。

(b) **サインイン/クリックスルー用の外部スプラッシュページ** を選択します。 無線ユーザーが、外部のポータルにリダイレクトされる **スプラッシュページ URL** を指定します。 このポータルは、無線ユーザーにユーザー名とパスワードの入力を促します。 必要に応じて、共有鍵のチェックボックスを選択し、SSID（外部ポータル通信用の）共有鍵を指定する必要があります。

(c) **RADIUS 認証による外部スプラッシュページ** を選択します。
この場合、次のフィールドを指定する必要があります
無線ユーザーが外部のポータルにリダイレクトされる **スプラッシュページ URL** を指定します。 SSID（外部ポータル通信用の）共有鍵を指定する必要があります。 AP が無線ユーザーを実際に認証する RADIUS サーバー設定を構成するために、RADIUS 設定をクリックします。

フィールド	説明
Called Station ID	AP が認証プロセス中に、標準の RADIUS パラメータ（'Called-Station-ID'）で RADIUS サーバーに渡す自由形式のテキストパラメータ。 特別な書式指定子 '%m'は、AP のイーサネット MAC アドレスに拡張され 指定することができます。
プライマリ認証サーバーの詳細	
サーバーIP	プライマリ認証サーバーの IP アドレス。
ポート番号	クライアントの要求を受け取るプライマリ認証サーバーのポート番号。
共有鍵	AP とプライマリ認証サーバー間の共有鍵。
セカンダリ認証サーバーの詳細	
サーバーIP	セカンダリ認証サーバーの IP アドレス。
ポート番号	クライアントの要求を受け取るセカンダリ認証サーバーのポート番号。

共有鍵	AP とセカンダリ認証サーバー間の共有鍵。

RADIUS アカウンティングを有効にしたい場合は、アカウンティングのチェックボックスにチェックを入れて、 AP が無線ユーザーを実際に認証するアカウンティングの詳細を指定します。
RADIUS サーバーの設定で、 RADIUS サーバーが稼働している**サーバーの IP** と**ポート番号**を指定します。

フィールド	**説明**
インターバル	アカウンティング・インターバル（分単位）。 最小間隔は 1 分で、最大の間隔は 60 分とすることが可能。
プライマリアカウンティングサーバーの詳細	
サーバーIP	プライマリアカウンティングサーバーの IP アドレス。
ポート番号	クライアントの要求を受け取るプライマリアカウンティングサーバーのポート番号。
共有鍵	AP とプライマリアカウンティングサーバー間の共有鍵。
セカンダリアカウンティングサーバーの詳細	
サーバーIP	セカンダリアカウンティングサーバーの IP アドレス。
ポート番号	クライアントの要求を受け取るセカンダリアカウンティングサーバーのポート番号。
共有鍵	AP とセカンダリアカウンティングサーバー間の共有鍵。

3. 外部ポータルパラメータを設定します。詳細については、 外部ポータルパラメータの設定 を参照してください。
4. 無線クライアントがある AP から他へローミングした際にスプラッシュページを表示したくない場合は、 **ローミング** チェックボックスにチェックを入れます。
5. インターネットに接続後、インターネット接続を失った場合にポータルエラーページを表示したい場合は、 **インターネット接続の検出を有効** チェックボックスにチェックを入れます。
   インターネットがゲスト SSID 上で一時的に利用できないとき、 'インターネット接続の検出を有効'機能はゲストにフィードバックを提供するために用いることが可能です。 アクセスポイント (AP)は、インターネット接続がゲスト VLAN から利用可能でないことを検出すると、 自動的にインターネットが一時的に使用できないメッセージと共にスプラッシュページへのゲストユーザーのすべての HTTP 要求をリダイレクトします。 **AP がクリックスルーでスプラッシュページをホスト** を使用している場合は、 “NoInternet.html”という名前でバンドルに含まれているカスタマイズされたスプラッシュページが インターネットがダウンした際に表示されます。 このページがバンドルに含まれていない場合、または外部スプラッシュページが設定されている場合、 インターネットがダウンすると AP は工場出荷時のスプラッシュページを表示します。
   インターネットがダウンしているとき、 **インターネット接続の検出を有効**にする機能が有効になっている場合だけでなく、 ゲストユーザーはローカルの HTTP サービスにアクセスすることができなくなることに注意してください。
   インターネット接続の検出を有効 にする機能は、 GRE を設定した SSID プロファイルでは動作しません。
6. ポータルページを提出したあとに無線ユーザーがゲストネットワークにアクセスすることができるための、 **ログインタイムアウト**（分単位）を指定します。
   タイムアウト後に、ゲストネットワークへのアクセスを停止しポータルページが再び表示されます。 ユーザーは、ゲストネットワークへのアクセスを回復するために、ポータルページを設定しなければなりません。 ユーザーがセッションタイムアウト前にゲストネットワークに対して切断し、そして再接続した場合は スプラッシュページで資格情報を入力する必要はありません。

7. 分単位で、**ブラックアウト時間**を指定します。 これは、ユーザーが前の成功したセッションをタイムアウトしたあとに、ログインが許可されない時間です。
   例えば、 セッションタイムアウトが 1 時間で、ブラックアウト時間が 30 分である場合、ユーザーは成功したログインの 1 時間後にタイムアウトします。 このポイントのあと、ユーザーは 30 分間再度ログインすることができません。 30 分経過すると、ユーザーは再度ログインすることができます。
8. **リダイレクト URL** を指定します。 ユーザーがポータルページで送信ボタンをクリックしたあと、ブラウザにはこの URL がリダイレクトされます。
   空白のままにすると、ブラウザはポータルページが表示されていたブラウザから本来のアクセスする URL にリダイレクトされます。
9. **外部ポータルパラメータ**で定義した**サービス識別子**の値を指定します。 これは、外部ポータルに渡すことができる自由形式のパラメータです。
   このパラメータは、 SSID プロファイルに特定の機能を実装するために、外部ポータルによって使用することができます。 例えば、それぞれの SSID は別々のポータルページを持つことができます。
10. 設定を保存するには、**保存**をクリックします。

キャプティブポータルを無効にする

キャプティブポータルの設定を無効にするには、 **キャプティブポータルを有効** チェックボックスのチェックを外します。

ファイアウォール設定

ファイアウォールは、定義された一連のルールに基づいて、ネットワークトラフィックの受信（Incoming）および送信（Outgoing）を制御します。 SSID プロファイルでファイアウォールの設定を構成するには、**SSID プロファイル追加**ページで**ファイアウォール**をクリックします。 あなたは、追加、変更、並べ替え、および**ファイアウォール**セクションからファイアウォールのルールを削除することができます。

SSID プロファイルで定義されたファイアウォールルールは、トップダウン方式で評価されます。 すなわち、それぞれのホスト名と方向の一致するものが見つかるまで、最初のルールが評価され、その次のルールがあとに続きます。

SSID プロファイルを作成するときに、デフォルトのルールでは任意のホストまたはドメインからのすべての受信および送信要求をブロックするように設定されています。特定のファイアウォールルールが定義されていないため、IP アドレス、ホスト名、サブドメイン名またはドメイン名から、 いずれかのタイプの要求を許可またはブロックするために、 **Allow** または **Block** を選択することでデフォルトのルールを定義します。

SSID プロファイルのファイアウォールを有効にするには、 **ファイアウォール有効**のチェックボックスにチェックを入れます。 それが、以前に選択されていて、SSID プロファイルのファイアウォールを無効にしたい場合は、 **ファイアウォール有効**のチェックボックスのチェックを外します。

ご注意： SSID プロファイルが NAT を有効にしている場合、DHCP アドレスプールの中の IP アドレスを指定して Allow または Block することはできません。

新しいファイアウォールルールの追加

ファイアウォールルールを追加するには、次の手順で行います。

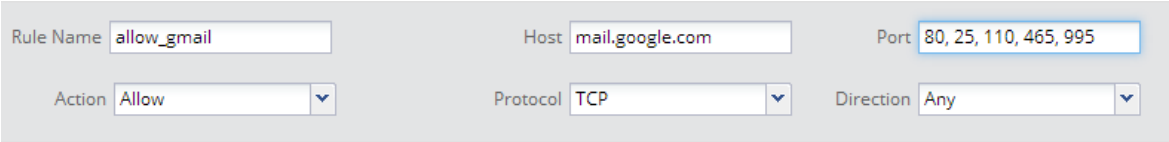
1. **新ルールの追加**をクリックします。
2. 1 つ以上のルールがすでに定義されている場合は、ルールの優先順位を決定する方法に応じて、選択したルールの上または下に新しいルールを挿入するために、 **選択したルールの上に** または **選択したルールの下に** を選択します。
3. 次の表に示すように、ルールの詳細を入力します。

フィールド	説明
Rule Name	ルールの名前。
Host	ルールが適用される、 ドメイン名、サブドメイン名、ホスト名、サブネットまたは IP アドレス。 ここに カンマで区切った複数のホスト名のリストを提供することができます。 例： 192.168.8.173, www.facebook.com, 192.168.121.0/24
Port	ポート番号。 ここに ポート番号またはポート範囲のカンマ区切りのリストを提供することができます。 例： 20-22, 80, 443
Action	Host から（または、Host への）トラフィックを ブロックしたい場合は、**Block** を選択します。Host から（または、Host への）トラフィックを 許可したい場合は、**allow** を選択します。

フィールド	説明
Protocol	ネットワークプロトコル。次のオプションが使用可能です。 **TCP**: ルールが TCP ベースの通信用の場合は、 **TCP** を選択します。 **UDP**: ルールが UDP ベースの通信用の場合は、 **UDP** を選択します。 **Other**: ルールが TCP と UDP ベース以外の通信の場合は、 **Other** を選択します。 この場合は、プロトコル番号を指定する必要があります。 **Any**: ルールが固有のプロトコルのものでない場合は、 **'Any'** を選択します。
Protocol No.	プロトコル番号。このフィールドはプロトコルに **Other** を選択した場合にのみ表示されます。
Direction	ネットワークトラフィックの方向。次のオプションが利用可能です。 **Outgoing**: ルールがネットワークから出て行く（無線から有線へ）データに適用される場合、**Outgoing** を選択します。 **Incoming**: ルールがネットワークに入ってくる（有線から無線へ）データに適用される場合、**Incoming** を選択します。 **Any**: ルールが送信と受信の両方のトラフィックに適用する場合は、**'Any'**を選択します。 例えば、 無線ネットワークのユーザーが特定の Web サイトまたはドメインにアクセスするのを許可するか、またはブロックしたいならば、 方向を **Outgoing** としてそれぞれのルールを定義することができます。同様に、 特定のホストから無線ネットワークへの アクセスをブロックしたいならば、方向を **Incoming** としてこのホスト名またはドメイン名に固有のルールを定義することが できます。

例えば、 ホスト 'mail.google.com'、ポート 80, 25, 110, 465, 995 からのすべての受信と送信の TCP リクエストを 許可したい場合は、以下のとおりルールの詳細を指定します。
ルールを追加するには、 **新ルールの追加** をクリックします。
Rule Name でルールに適切な名前を指定します。
Host Name を 'mail.google.com、**Port** を 80, 25,110, 465, 995 **Action** を **Allow、Protocol** を **TCP、Direction** を **Any** として指定します。 ルールについては下の画像を参照。

ファイアウォールルール



4. ルールを保存するには、**保存** をクリックします。

ファイアウォールルールの並べ替え(Reorder)

1 つ以上の定義したファイアウォールルールがある場合は、 それらを並べ替えることができます。
ルールを並べ替えるには次の手順を実行します。

1. 移動するためにルールをクリックします。
2. マウスボタンを押したまま、目的の位置にルールをドラッグします（例えば他のルールとルールの間へ）。
3. マウスを放します。ルールは、新しい位置に配置されます。
4. ルールの並べ替えを保存するには、**保存** をクリックします。

ファイアウォールルールの編集

ファイアウォールルールを編集するには、次の手順で行います。

1. 編集するルールのラジオボタンをクリックします。
2. 次の表に示すようにルールの詳細を編集します。

フィールド	説明
Rule Name	ルールの名前。
Host	ルールが適用される、 ドメイン名、サブドメイン名、ホスト名、サブネットまたは IP アドレス。 ここに カンマで区切った複数のホスト名のリストを提供することができます。 例： 192.168.8.173, www.facebook.com, 192.168.121.0/24
Port	ポート番号。 ここに ポート番号またはポート範囲のカンマ区切りのリストを提供することができます。 例： 20-22, 80, 443
Action	Host から（または、Host への）トラフィックを ブロックしたい場合は、**Block** を選択します。Host から（または、Host への）トラフィックを 許可したい場合は、**allow** を選択します。
Protocol	ネットワークプロトコル。次のオプションが使用可能です。 **TCP**: ルールが TCP ベースの通信用の場合は、 **TCP** を選択します。 **UDP**: ルールが UDP ベースの通信用の場合は、 **UDP** を選択します。 **Other**: ルールが TCP と UDP ベース以外の通信の場合は、 **Other** を選択します。 この場合は、プロトコル番号を指定する必要があります。 **Any**: ルールが固有のプロトコルのものでない場合は、 **'Any'** を選択します。
Protocol No.	プロトコル番号。このフィールドはプロトコルに **Other** を選択した場合にのみ表示されます。
Direction	ネットワークトラフィックの方向。次のオプションが利用可能です。 **Outgoing**: ルールがネットワークから出て行く（無線から有線へ）データに適用される場合、**Outgoing** を選択します。 **Incoming**: ルールがネットワークに入ってくる（有線から無線へ）データに適用される場合、**Incoming** を選択します。 **Any**: ルールが送信と受信の両方のトラフィックに適用する場合は、**'Any'**を選択します。 例えば、 無線ネットワークのユーザーが特定の Web サイトまたはドメインにアクセスするのを許可するか、またはブロックしたいならば、 方向を **Outgoing** としてそれぞれのルールを定義することができます。同様に、 特定のホストから無線ネットワークへの アクセスをブロックしたいならば、方向を **Incoming** としてこのホスト名またはドメイン名に固有のルールを定義することが できます。

ファイアウォールルールの削除

ルールを削除するには、次の手順で行います。
1. 削除するルールの**削除**をクリックします。
2. 削除操作を確認するために表示されるメッセージで **Yes** をクリックします。 削除操作をキャンセルするには **No** をクリックします。
3. ファイアウォールルールへの変更を保存するには、**保存**をクリックします。

トラフィックシェーピングと QoS

ネットワーク帯域幅の有効活用は、さまざまな方法で実現することができます。
ネットワークのアップロードおよびダウンロードの制限、クライアントのアソシエーション数を制限、QoS パラメータを定義する方法があります。 ネットワークトラフィック、SSID 上で使用されるアプリケーションそして使用中の管理デバイス(Management Device)モデルによって、これらの方法を選ぶことができます。

トラフィックシェーピング

SSID 上のアップロードと(または)ダウンロード帯域幅を制限することが可能です。

SSID 上のアップロード帯域幅を制限するには、次の手順を実行します。
1. ここで指定した値に SSID のアップロード帯域幅を制限するには、**SSID 上のアップロード帯域幅を制限**のチェックボックスにチェックを入れて、データレートを入力します。
2. 変更を保存するには**保存**をクリックします。

SSID 上のダウンロード帯域幅を制限するには、次の手順を実行します。
1. ここで指定した値に SSID のダウンロード帯域幅を制限するには、**SSID 上のダウンロード帯域幅を制限**のチェックボックスにチェックを入れて、0～1024Kbps の範囲でデータレートを入力します。
2. 変更を保存するには**保存**をクリックします。

企業では、ときとしてアクセスする複数のポイント間でネットワークポリシーを伝達するために RADIUS アトリビュートを使用しています。 ユーザーはグループに分割され、ネットワークリソースへのアクセスを効果的にコントロールするためにポリシーが各々のグループに適用されます。 各ユーザーグループは、そのユーザーグループの必要性に基づいて、アップロード帯域幅およびダウンロードの帯域幅が割り当てられます。

RADIUS サーバーを使用してクライアントを認証するような場合、RADIUS サーバーで定義された帯域幅の制御設定を取得して使用するようにアクセスポイント(AP)を設定することができます。

RADIUS サーバーによって返される値に基づいて、アクセスポイント(AP)は RADIUS 認証されたユーザーに対してアップロードとダウンロード帯域幅をダイナミックに設定します。RADIUS サーバーが帯域幅の値を返さない場合は、トラフィックシェーピングと QoS 設定で定義されたデフォルトのアップロードとダウンロード帯域幅が使用されます。 ユーザーが複数のデバイスを有する場合、帯域幅の制限はこれらのデバイスのそれぞれに個別に適用されます。 これは、ユーザーが 2 つのデバイスを使用しユーザーまたはユーザーグループの帯域幅が 4Mbps の場合、これらのデバイスのそれぞれに適用される帯域幅の制限が 4Mbps であることを意味します。

ユーザー固有の帯域幅の値は、以下の 1 つ以上から取得できます。

- 外部の RADIUS 認証サーバーを持つポータルから。
- RADIUS サーバーから（SSID に IEEE802.1x セキュリティが設定されている場合）。
- 管理コンソールサーバーから（上記のいずれかで値が返されない場合は、管理コンソールサーバーで定義されたデフォルト値が使用されます）。

帯域幅の値が上記の複数のソースによって返された場合、適用する帯域幅の制限を識別するための優先順位は上記と同じになります。 つまり、外部の RADIUS 認証サーバーが最優先となり、続いて GAMS ポータル、そして最後が IEEE802.1x 認証に使用される RADIUS サーバーになります。

他のソースのいずれも帯域幅の値を返さない場合にのみ、デフォルトの管理コンソールサーバーの帯域幅の値が使用されます。

RADIUS ユーザーのユーザーグループに基づいて、帯域幅の RADIUS ベースの割り当てを有効にする手順は、以下のとおりです。

1. **コンフィグレーション>デバイスのコンフィグレーション>SSID プロファイル**に移動します。
2. SSID プロファイルタブで、SSID プロファイルの追加または編集を行います。
3. **トラフィックシェーピングと QoS** をクリックします。セクションが展開されます。
4. **ユーザー単位の帯域幅制御を有効**のチェックボックスを選択します。 **ユーザーのアップロード帯域幅を制限** と **ユーザーのダウンロード帯域幅を制限**のフィールドが表示されます。
5. アップロード帯域幅のデフォルトの帯域幅の値を指定するには、**ユーザーのアップロード帯域幅を制限**のチェックボックスを選択して、値を指定します。 これは、RADIUS サーバーから RADIUS ユーザーに対してアップロード帯域幅が返されない場合に使用されます。
6. ダウンロード帯域幅のデフォルトの帯域幅の値を指定するには、**ユーザーのダウンロード帯域幅を制限**のチェックボックスを選択して、0～1024 Kbps の間で値を指定します。 これは、RADIUS サーバーから RADIUS ユーザーに対してダウンロード帯域幅が返されない場合に使用されます。

ユーザーの帯域幅ごとのセットに使用される RADIUS ユーザーアトリビュートは、ベンダー固有のアトリビュート- IETF ID：26 に分類されます。 NEC のベンダーID は 119 です。

以下のテーブルは、RADIUS アトリビュートによる NEC アトリビュートのマッピングを示しています。

NEC アトリビュート	**RADIUS アトリビュート ID**
Download Limit	154
Upload Limit	155

AP とアソシエイトするクライアントを制限

ネットワークの帯域幅を制限するために AP とアソシエイトするクライアントの数を制限することができます。
AP とアソシエイトするクライアントの数を制限するには、次の手順を実行します。

1. AP とアソシエイトすることができるクライアントの最大数を指定したい場合は、**アソシエーションの制限数**のチェックボックスにチェックを入れます。
2. **アソシエーションの制限数**チェックボックスの隣のフィールドに、クライアントの最大数を指定します。
3. 変更を保存するには**保存**をクリックします。

ご注意：AP に同時にアソシエイトされる無線クライアント数が多すぎる場合、満足な無線通信性能が出ない場合があります。10 台以下での運用を推奨します。

最小データ転送速度を定義

AP とクライアントの通信の最小データ転送速度を指定することができます。指定されたデータ転送速度よりも高いデータレートが、クライアントとの通信に使用されます。
最小データ転送速度を指定するには、次の手順を実行します。

1. **最小データ転送速度**のチェックボックスにチェックを入れます。
2. **最小データ転送速度**の隣のフィールドに通信を行うための最小データ転送速度を指定します。
3. 変更を保存するには**保存**をクリックします。

Enable BSS Load

BSS Load の情報はビーコンやプローブ応答に含めることができます。
BSS Load は接続された子機の数やアクセスポイントに対するトラフィック量を示します。
トラフィック量はチャネル使用率 および 使用可能なアドミッションキャパシティ によって判別されます。

BSS Load を有効にすると、子機はローミングする際に BSS Load の情報を確認して接続できそうな AP を選択することができます。
ただし、有効にした場合でも AP が子機の接続要求を受け入れないことがあります。

チャネル幅が 40/80MHz 幅で利用されている場合でも、チャネル使用率はプライマリチャネルでのみ算出されます。

BSS Load を有効にするには、下記手順を実施します。
1. Enable BSS Load のチェックボックスにチェックを入れる。
2. **保存**をクリックする。

QoS (Quality of Service)

多様なタイプのトラフィックのプライオリティが、QoS で定義されています。 QoS はサービス品質を表します。 サービス保証は、ストリーミング・マルチメディア・アプリケーション （例えば、VoIP、ビデオ、オンラインゲームなど）では不可欠です。 ネットワーク帯域幅がこのようなアプリケーションに対して共有される場合は、 プライオリティを定義することが必要です。 このようなアプリケーションに対して SSID を使用しているならば、 QoS パラメータを定義する必要があります。 より高いプライオリティを必要としているアプリケーションまたはトラフィックが、 必要とされるプライオリティを得ることを QoS は保証します。 QoS プライオリティに基づく十分な帯域幅を割り当てることによって、 提供されるサービスは保証されます。
IEEE802.11n/11ac モードで無線 LAN を構成する場合は、WMM が IEEE802.11n/11ac モードでは必須であるため、 WMM（Wi-Fi マルチメディア）は常に有効になります。
IEEE802.11n/11ac モードで **QoS** のチェックボックスが選択されていない場合は、 システムはデフォルトの QoS パラメータを使用しています。
デフォルトの QoS 設定は次のようになっています。

- SSID プライオリティは音声。
- プライオリティタイプは上限。
- ダウンストリームマッピングは DSCP。
- アップストリームマーキング有効で、値は IEEE802.1p マーキング。

QoS のチェックボックスにチェックが入っている場合は、システムはユーザーが設定した QoS 設定を使用します。

QoS の設定を構成するには、次の手順を実行します。

1. **QoS** のチェックボックスにチェックを入れて、SSID プロファイルの Wi-Fi マルチメディア用に独自の QoS 設定を定義します。
2. 必要条件に応じて、**SSID のプライオリティ** として音声、ビデオ、ベストエフォートまたはバックグラウンドを指定してください。
3. IEEE802.1p または IP ヘッダーで示されるプライオリティにかかわりなくこの SSID のすべてのトラフィックが、 選択されたプライオリティで送られなければならないならば、**プライオリティタイプ**を **固定**として選択します。 この SSID のトラフィックが選択されたプライオリティと同等か低い場合は、 **上限**として **プライオリティタイプ**を選択します。
4. **プライオリティタイプ**を **上限**として選択した場合は **ダウンストリームマッピング**を選択します。 プライオリティは選択されたフィールド（IEEE802.1p、DSCP または TOS）から抽出され、 選択された SSID のプライオリティの最大値を前提として、ダウンストリーム・トラフィックのために無線アクセスカテゴリにマッピングされます。 ダウンストリームマッピングに対して、マッピングは DSCP 値、TOS 値または IEEE802.1p アクセスカテゴリの 最初の 3 ビット（クラス・セレクタ）によって決まります。 唯一の例外は、WMM アクセスカテゴリの 'Voice'にマッピングされる DSCP 値 46 になります。
5. 必要条件にしたがって**アップストリームマーキング**を選択します。 インカミング無線アクセスカテゴリは選択された SSID のプライオリティの最大値を前提としてマッピングされ、 選択された IEEE802.1p ヘッダーと IP ヘッダーに設定されます。
6. 変更を保存するには**保存**をクリックします。

ダウンストリームマッピングについては、以下の表を参照してください。

IEEE802.1p Class of Service	IEEE802.11e 規格/WMM access category
0 (Background)	1 (Background)
1 (Best Effort)	0 (Best Effort)
2 (Excellent Effort)	3 (Best Effort)
3 (Critical Apps)	4 (Video)
4 (Video)	5 (Video)
5 (Voice)	6 (Voice)
6 (Internetwork Ctrl)	7 (Voice)
7 (Network Ctrl)	7 (Voice)

IEEE802.11e 規格/WMM アクセスカテゴリと対応する IEEE802.1p サービスクラスと DSCP 値（アップストリームマーキングで使用される）に関しては以下の表を参照してください。
IEEE802.1p マークを有効にした場合、IEEE802.11e 規格/WMM アクセスカテゴリは対応する IEEE802.1p サービスクラスにマッピングされます。 DSCP/ TOS マーキングが有効になっている場合は、IEEE802.11e 規格アクセスカテゴリは、対応する DSCP 値にマッピングされます。

IEEE802.11e 規格/WMM access category	IEEE802.1p Class of Service	DSCP
0	1	0
1	0	10
2	0	18
3	2	0
4	3	26
5	4	34
6	5	46
7	6	48

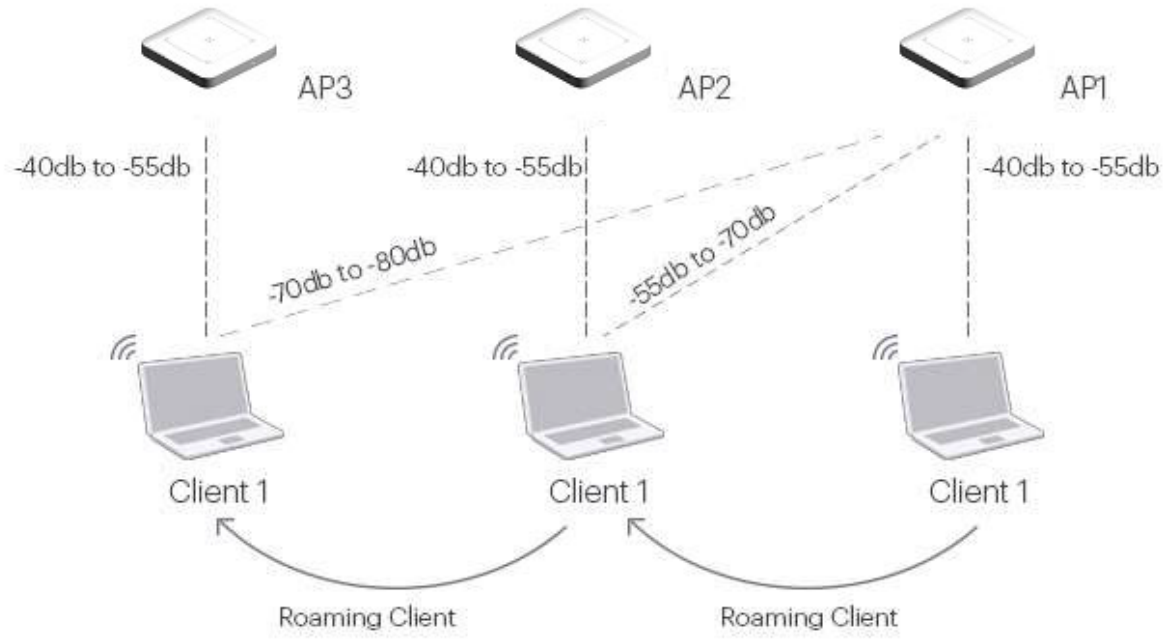
RF Optimizations（無線ネットワークの最適化）

BYODやゲストWi-Fiの急速な増加により、異なるメーカーの機器やオペレーティングシステムからの多種多様なデバイスが無線ネットワークに接続しています。ローミングやネットワークを切り替えることになると、クライアントはいつローミングし、そしてどのアクセスポイントにローミングするかを常に決定します。このローミング動作は、各クライアント装置で独自です。また、各デバイスは異なる送信電力、アンテナの向き、パワーセーブモードの決定を有しており、ローミングプロセスがより予測不可能になることがあります。

ワイヤレス業界では“スティッキークライアント”の問題が話題になります。クライアントは、通常最初の試みで最も良い信号強度を提供するアクセスポイントに接続します。スティッキークライアントは、周辺のより良い信号強度を提供する他のアクセスポイントにローミングせずに、（たとえ弱い信号強度でも）現在のアクセスポイントとの接続を継続する傾向にあるデバイスです。これは、クライアントへWi-Fiカバレッジを提供するために、複数のアクセスポイントを使用する大規模なネットワークで発生します。

例えば、オフィス環境では特定の時間にアクセスポイントに接続される複数のノートパソコンまたはタブレットが存在し得ます。以下の図に示すように、ノートパソコンのいずれかがアクセスポイントから離れて移動する場合、その範囲内にあるアクセスポイントを検出し、より良好な信号強度を提供するアクセスポイントに接続することが予想されます。“スティッキークライアント”の場合、クライアントはローミングまたは別のアクセスポイントへスイッチを行いません。その代わりに、遠くのアクセスポイントへの接続を維持します。下図は、ノートパソコンが別の場所に移動し、弱い信号強度だとしても、遠くのアクセスポイントとの関連付けを継続することを示しています。

これは、スティッキークライアントに対してだけでなく、同じアクセスポイントに接続する他のクライアントに対してもネットワーク速度の低下を引き起こします。たとえ、より良好な接続性を提供している隣接するアクセスポイントがあったとしても、ほとんどのクライアントは今後も現在のアクセスポイントとの接続を継続します。



弱い信号強度とスティッキークライアント

このシナリオでは、クライアントが最良の信号強度を提供するアクセスポイントに接続することを選択しない限り、スティッキークライアントは良好な接続速度を得ることができません。

ローミング機能の最適化設定

ローミング機能の最適化設定は、クライアントをより良好なアクセスポイントへ積極的に誘導することによってスティッキークライアントの問題を解決しようとします。アクセスポイント(AP)は、クライアントのRSSI信号強度を継続的に監視します。信号強度が小さな周期または事前定義された連続的な読み取りの間で、特定のあらかじめ設定された閾値を下回ると、アクセスポイントが認証解除を送信することでローミングを開始します。次に、クライアントは、プロービングを開始し、良好な信号強度を提供するアクセスポイントに接続します。

ローミング機能の最適化設定を有効にするには

管理コンソール(Management Console) は、スティッキークライアントの問題を解決するために、ローミング機能の最適化設定を有効にすることができます。

ローミング機能の最適化設定を有効にするには、次の手順を実行します。

1. **コンフィグレーション>デバイスのコンフィグレーション>SSIDプロファイル**へ移動します。
2. Wi-Fiプロファイルを新規追加するか、または編集する既存のWi-Fiプロファイルを選択します。
3. Wi-Fiプロファイルのダイアログボックス内の **RF Optimizations（無線ネットワークの最適化）**へ移動します。
4. **Smart Steering（スマートステアリング）**と **Min Association RSSI** のチェックボックスにチェックを入れます。

ご注意：ローミング機能の最適化設定を有効にすると、アクセスポイントから弱い信号強度を持つクライアントを積極的に切断します。もし、あなたのクライアントがこれに起因する接続の問題に直面する場合は、本機能を無効にします。また、音声トラフィックがある場合や、施設内に高いRSSIカバレッジが計画されていない場合は、ローミング機能の最適化設定を無効にすることをお勧めします。

ご注意：Min Association RSSIを有効にすると、アクセスポイントは指定された信号強度以下のクライアントからのアソシエーション要求を拒否します。
ただし、有効にしている場合でも、アクセスポイントは設定されているディスペレット・クライアント時間内に、クライアントから最大アソシエーションリトライ数を超えた回数のアソシエーション要求があった場合は、その要求を許可します。

ローミング機能の最適化設定ローミング機能の最適化設定を構成するには、次の手順を実行します。

1. **コンフィグレーション>デバイスのコンフィグレーション>デバイステンプレート**へ移動します。
2. 新しいデバイステンプレートを追加する場合は、**デバイステンプレートの追加 > ラジオ設定**へ移動します。もしくは、編集するデバイステンプレートを開いて、**ラジオ設定**をクリックします。
3. **モデル設定の定義**をクリックします。
4. 利用可能なモデルのリストからデバイスを選択します。
5. **ラジオ詳細設定**をクリックし、**Smart Steering（スマートステアリング）**を選択します。
6. 以下の値を設定します。

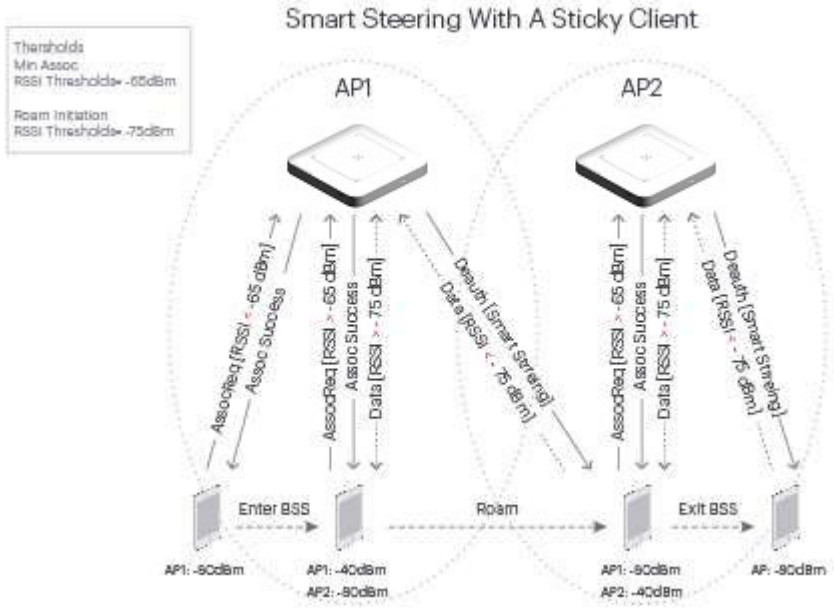
値	説明
ローミング開始の RSSI 閾値	APがスマートステアリング・ロジックを開始するRSSIの閾値です。クライアントの信号強度がこの閾値よりも小さく、**ローミング開始閾値時間**ならびに**ローミング開始閾値パケット**の条件を満たした場合、APは、クライアントに認証解除を送信します。
ローミング開始閾値時間	秒単位の時間間隔です。APがローミングを開始する前にこの期間待ちます。言い換えると、低い信号強度が指定された期間続くとAPは、ローミングを開始します。
ローミング開始閾値パケット	低いRSSI値を持つクライアントを切断するための、パケット数の条件に関する閾値です。簡潔に言うと、APがローミングを開始するために、「ローミング開始閾値時間」内に、クライアントが送信する必要があるパケットの最小数です。

7. 以下の Min Association RSSI 値を設定します。

値	説明
RSSI スレッショルド（閾値）	クライアントの信号強度がこの閾値以下である場合、APはアソシエーション失敗を使って、クライアントのアソシエーション要求に応答します。
ディスペレット・クライアント時間	この期間内にクライアントからのアソシエーション要求数が**最大アソシエーションリトライ**を超えた場合、クライアントはAPにアソシエーションすることが許可されます。
ディスペレット・クライアントタイムアウト	いったん、**ディスペレット・クライアント時間**がトリガーされると、クライアントは**ディスペレット・クライアントタイムアウト**期間の間、その状態で保持されます。
最大アソシエーションリトライ	**ディスペレット・クライアント時間**内に、クライアントからのアソシエーション要求数が**最大アソシエーションリトライ**を超えた場合、クライアントはAPにアソシエーションすることが許可されます。

ローミング機能の最適化設定の使いかた

ローミング機能の最適化設定がスティッキークライアントに対してどのように機能するかを次の図に示します。下図は、クライアントのRSSIが所定の閾値に達したときに、APが認証解除フレームを送信することを示しています。これには、クライアントがベストなRSSIを提供する最も近いアクセスポイントに接続するために、クライアントデバイスが周囲で利用可能なアクセスポイントに対してプロービングを開始するトリガーになります。



ローミング機能の最適化設定はバンドステアリングとどのように違うか

バンドステアリングの場合には、クライアントは IEEE802.11b/g/n と IEEE802.11a/n の両帯域の機能を持ちます。バンドステアリング機能は、2.4GHz 帯と 5GHz 帯両方で動作可能なデュアルバンドクライアントが 2.4GHz 帯でアクセスポイント(AP)へ接続しようとしている場合に、無線干渉を防止するために、2.4GHz 帯から 5GHz 帯へ Wi-Fi クライアントを誘導できます。
バンドステアリングは、5GHz帯のクライアントの信号強度が指定された閾値よりも高い場合に、5GHz帯の無線へデュアルバンドクライアントを誘導しようと試みます。

しかし、ローミング機能の最適化設定は、帯域の誘導ではありません。スマートステアリングは（無線の帯域に関係なく）ベストなRSSIと接続速度を提供する最も近いアクセスポイントに接続するようにクライアントを促します。

ローミング機能の最適化設定を設定するベストプラクティス

- ローミング機能の最適化設定を設定するにはネットワーク内に複数のアクセスポイントが必要です。
- ローミング機能の最適化設定が効果的に機能するためには、アクセスポイントは常にクライアントに可視される必要があり、また、Wi-Fiのカバレッジ範囲内に"良好"な RSSIを提供する必要があります。
- VoIPまたはビデオタイプのトラフィックを通信する環境下では、ローミング機能の最適化設定を有効にしないことをお勧めします。

バンドステアリング

バンドステアリング機能を有効にすることで、指定した SSID が 2.4GHz 帯と 5GHz 帯両方に設定されている場合、両方の帯域で動作可能なクライアントをアクセスポイント(AP)の 5GHz 帯に誘導して接続させることが可能です。
一般的に 2.4GHz 帯は Wi-Fi 以外にもさまざまな機器で利用されており混雑していることから無線干渉が多く、クライアントを 5GHz 帯に誘導することで無線干渉による通信品質の低下を解消することに役立ちます。
バンドステアリングは 2.4GHz 帯に帰属しようとしたクライアントを 5GHz 帯に帰属させるために動作します。

以下のすべての条件を満たす場合に、指定した SSID に接続しようとするクライアントは 5GHz 帯へ誘導されます。

- SSID プロファイル上でバンドステアリングが有効になっている。
- クライアントの RSSI が、SSID プロファイルの **RF Optimizations（無線ネットワークの最適化）**設定で掲げられた RSSI スレッショルド以上である。
- 5GHz 帯に接続しているクライアント数が、2.4GHz 帯に接続しているクライアント数と比べてデバイステンプレートの **2.4GHz 帯のラジオ詳細設定**にて設定する**バンドステアリングロードバランシングスレッショルド**の値より少ない場合。

バンドステアリングを有効にする場合、クライアントの RSSI スレッショルドを指定する必要があります。 弱い信号強度を有するクライアントは 5GHz 帯で効率的に動作できないため、5GHz 帯で動作することが可能であっても誘導されるべきではないためです。

バンドステアリングを設定するには、次の手順を実行します。

1. **コンフィグレーション>デバイスのコンフィグレーション>SSIDプロファイル**へ移動します。
2. バンドステアリングを設定するSSIDのWi-Fiプロファイルを選択するため、Wi-Fiプロファイルを新規追加するか、編集する既存のWi-Fiプロファイルを選択します。
3. Wi-Fiプロファイルのダイアログボックス内の **RF Optimizations（無線ネットワークへの最適化）** へ移動します。
4. **Band steering（バンドステアリング）**のチェックボックスにチェックを入れます。
5. **RSSIスレッショルド**を指定します。
6. 変更を保存するには**保存**をクリックします。
7. **コンフィグレーション>デバイスのコンフィグレーション>デバイス**のテンプレートへ移動します。
8. バンドステアリングを設定するデバイスを選択するため、デバイステンプレートの追加を選択するか、編集する既存のWi-Fiプロファイルを選択します。
9. **デバイステンプレート**の**ラジオ設定**で、バンドステアリングを設定するモデルを選択し、2.4GHz帯のラジオ詳細設定を開きます。
10. **バンドステアリングロードバランシングスレッショルド**を指定します。
11. 変更を保存するには**保存**をクリックします。

無線クライアントによっては、5GHz帯へ積極的に接続要求を行うため、設定したバンドステアリングロードバランシングスレッショルドの値を超えて5GHz帯のSSIDに帰属する場合があります。

BYOD - デバイスのオンボーディング

デバイスのオンボーディングは、システムによって隔離されている未承認のクライアントが、 他のすべての通信をブロックされている間に、任意の Web アクセスを行うと同時に構成されたスプラッシュページの URL に リダイレクトされる技術です。この技術は、すべてのクライアントまたは特定のスマートクライアント（スマートフォン とタブレットのみ）に対して有効にすることが可能です。

BYOD - デバイスのオンボーディング

BYOD のデバイスオンボーディングを設定するには、次の手順を実行します。

1. BYOD のデバイスオンボーディングを有効にするには、 BYOD 有効 チェックボックスにチェックを入れます。
2. この技術を未承認のスマートクライアントに対してのみ（他のラップトップのような無線クライアントではなく）有効にするには、 スマートフォン/タブレット を選択します。 あるいは、すべてのタイプの未承認の無線クライアントに対してこの技術を有効にしたい場合は、 すべてのクライアント を選択します。
3. URL にリダイレクトでスプラッシュページの URL を指定します。 無線クライアントが任意の Web 要求を行う際に、この URL にリダイレクトされます。 スプラッシュページのホストの IP アドレスまたはホスト名は、 リダイレクトが機能するためにはウォールドガーデンの設定に追加する必要があります。
4. ウォールドガーデンの設定を行います。 ウォールドガーデンに IP アドレスまたはホスト名を追加するには、追加をクリックします。 ウォールドガーデンから IP アドレスまたはホスト名を削除するには、削除をクリックします。 またリダイレクションから除外する必要がある他のホスト名または IP アドレスを、ここで追加することができます。
5. 変更を保存するには、保存 をクリックします。

Hotspot 2.0 Settings

HotSpot 2.0 は少ないユーザー設定にて容易にネットワークの発見と選択を可能にします。それは Wi-Fi の手動設定や帰属といったオーバーヘッドを必要とせず、自動ローミングが可能です。
Passpoint で認証されたモバイル端末はシームレスに Hotspot2.0 が設定された AP に帰属することができます。
Hotspot AP とモバイル端末間の通信は Access Network Query Protocol (ANQP)が使用されます。
ご注意：Hotspot2.0 を使用するには AP のセキュリティモードは WPA2 の IEEE802.1x を設定してください。
Hotspot 2.0 の設定は以下のとおりです。

1. Enable Hotspot 2.0 のチェックボックスにチェックを入れます。
2. 以下の設定をしてください。

フィールド	説明
Network Type	適切なネットワークタイプを選んでください。
Network Auth Type	適切なネットワーク認証タイプを選んでください。
IPv4 Address	適切な IPv4 アドレスを選んでください。 Address type not available(アドレスタイプなし) Public IPv4 address available(グローバルな IP アドレス) Port-restricted IPv4 address available(ポート制限ありの IP アドレス) Single NATed private IPv4 address available (NAT が 1 段あるプライベート IP アドレス) Double NATed private IPv4 address available (NAT が 2 段あるプライベート IP アドレス) Port-restricted IPv4 address and single NATed private IPv4 address available(ポート制限ありで NAT が 1 段あるプライベート IP アドレス) Port-restricted IPv4 address and double NATed private IPv4 address available(ポート制限ありで NAT が 2 段あるプライベート IP アドレス) NAT に関するオプションを使用する際は、SSID プロファイルで NAT を有効にしてください。
Internet Access	クライアントのインターネットアクセスを許可する場合はチェックボックスにチェックを入れてください。
HESSID	相同の拡張されたサービスセット識別子です。Hotspot AP を識別に使います。同じ HESSID との AP は同じ Hotspot 2.0 コンフィグレーションを持っています。
Redirect URL	Hotspot AP と接続後にリダイレクトされる URL。このフィールドはネットワーク認証タイプと連携して使われます。
IPv6 Address	適切な IPv6 アドレスを選んでください。

3. Roaming consortium list を設定してください。最大 32 個まで設定できます。
4. Roaming consortium を記入して Add を押してください。

フィールド	説明
Venue Group	Hotspot AP を設置する場所のグループを選択してください。
Venue Type	詳細な場所を選択してください。
Venue Name	場所名を入力してください。最大文字数は 252 バイトで最大 32 個の場所名を指定できます。
Language Code	言語コードを設定してください。言語コードについては ISO 639.2 を参照してください。

5. Domain name list を設定してください。Domain name は最大 32 個を設定できます。Domain name のサイズは 255 バイトを超えてはいけません。
6. 3 桁のモバイル国コードと 2～3 桁のモバイルネットワークコードを指定してください。
7. NAI Realm を指定してください。最大 255 バイトで 32 個まで設定できます。
8. EAP method を指定してください。1 つの Realm に最大 4 つの EAP method を追加できます。
9. 下の表にしたがって WAN metrics を設定してください。

フィールド	説明
Link Status	設定可能な Link Status を選択してください。 Link up- Link up している場合はこちらを選択してください。 Link Down- Link Down している場合はこちらを選択してください。 Link in test- Link テスト中の場合はこちらを選択してください。 Not Configured- Link Status を設定しない場合はこちらを選択してください。
Symmetric Link Status	アップリンクとダウンリンクのスピードが同じ場合は Same を選択してください。 アップリンクとダウンリンクのスピードが異なる場合は Different を選択してください。
Downlink Speed	ダウンリンクのスピードを設定してください。
Uplink Speed	アップリンクのスピードを設定してください。

10. Operator friendly name list を設定してください。最大 32 個まで設定できます。

フィールド	説明
Name	文字数は 252 バイトを超えてはいけません。
Language Code	言語コードを設定してください。言語コードについては ISO 639.2 を参照してください。

11. Connection capability を設定してください。ネットワーク接続でサポートされているプロトコル、対応するポート番号、そしてポートが開いているか閉じているかを指定することができます。これらの設定は、Hotspot AP が接続されている有線ネットワークの機能を示します。
12. Save を押すと設定が保存されます。

メッシュプロファイルの管理

無線メッシュネットワークは、有線接続の大部分を置き換えるために無線リンクを介して、複数のアクセスポイント(AP)が相互接続し互いに通信するネットワークです。 AP およびネットワークデータのルーティング間の通信は、AP の無線 LAN を介して行われます。 無線メッシュネットワークを形成する AP は、メッシュ AP です。
有線ネットワークの敷設が費用対効果の低い場所において、無線メッシュネットワークは屋内または屋外で使用されます。 特定のエリアの周辺を移動しながらネットワークに接続する必要がある場合、それらは特定の領域で使用することができます。 それらは、スタジアム、学校などです。

ソースのメッシュ AP は、同じメッシュ内の宛先メッシュ AP と直接または宛先のメッシュ AP に到達するまで別のメッシュ AP をホップすることにより通信を行います。 無線クライアントと AP 間の通信、 そして AP 間の通信は無線または有線ネットワークを介して行われます。

AP 機能を持つ管理デバイス(Management Device)は、無線メッシュネットワークの生成をサポートします。管理デバイス(Management Device)を使用して作成した無線メッシュネットワークは、ルートおよび非ルート AP で構成されます。

ルート AP は、有線ネットワークに直接接続されている AP です。 非ルート AP は有線ネットワークに直接接続されていない AP です。 それは、ルート AP を通じて有線ネットワークに接続します。
非ルート AP は、直接ルート AP と通信するか別の非ルート AP を経由することができます。 無線メッシュネットワーク内に、1 つまたは複数のルート AP と複数の非ルート AP が存在する可能性があります。

ルート AP は、有線ネットワークを介して Management Console サーバーに接続します。 すべてのクライアントと他の非ルート・メッシュ AP は、ルート AP を介して Management Console サーバーと通信します。

管理デバイス(Management Device)を使用して作成されるメッシュネットワークは、論理的ツリー型トポロジとして実現されます。
ツリー型トポロジでは、親ノードと複数の子ノードが存在します。 子ノードはメッシュプロファイル構成においてダウンリンクと呼ばれています。親ノードは、アップリンクと呼ばれます。

メッシュネットワークのセットアップ

無線メッシュネットワークをセットアップするには、まずメッシュ AP として機能する AP を特定する必要があります。

無線メッシュネットワークをセットアップしたい場合は、メッシュのプロファイルを定義する必要があります。 メッシュプロファイルは、メッシュネットワークのパラメータを表します。 メッシュプロファイルを追加、編集、削除することが可能です。
無線メッシュネットワーク用に定義されたメッシュプロファイルは、メッシュ AP の無線 LAN のいずれかに適用する必要があります。 この無線 LAN は、メッシュネットワーク上の他の AP と通信するため専用の無線 LAN として機能します。
コンフィグレーションが有効になっているデバイスごと（すべてのメッシュ AP に対して）に、デバイステンプレートを適用する必要があります。 すべてのメッシュ AP に対して、有効にされる装置構成ごとに、1 つのデバイステンプレートを適用する必要があります。 その次に、メッシュ AP のうちどれがルート AP であるかを指定します。 デフォルトでは、メッシュ内の他の AP は非ルート AP として扱われます。
メッシュパラメータを定義しメッシュ AP にデバイステンプレートの設定を上書きしたあとは、管理コンソール(Management Console)上のロケーションセクションで、メッシュネットワーク・トポロジの図式表現を見ることができます。 メッシュネットワーク・トポロジの表示方法の詳細については、ロケーションとロケーションレイアウトの管理 の「メッシュ・トポロジの表示」を参照してください。

ご注意： Management Device の AP と Management Device 以外の AP との組み合わせで無線メッシュネットワークを作成することはできません。 メッシュネットワークは、Management Device の AP のみで構成する必要があります。

ロケーションの無線メッシュネットワークをセットアップするには、次の手順を実行します。

1. ロケーションツリーからロケーションを選択します。
2. **コンフィグレーション>デバイスのコンフィグレーション>SSID プロファイル>メッシュプロファイル** へ移動します。
3. メッシュプロファイルを設定します。メッシュプロファイルを追加するには、下記のメッシュプロファイルの追加 を参照してください。
4. **コンフィグレーション>デバイスのコンフィグレーション>デバイステンプレート**へ移動します。
5. メッシュ AP として機能する管理デバイス(Management Device)モデルのデバイステンプレートを定義します。 詳細については、デバイステンプレートの管理を参照してください。 このデバイステンプレートのデバイス固有の設定を有効にすることを忘れないでください。 メッシュ AP が相互に通信するチャネルが、無線メッシュネットワークを構成するすべての管理デバイス(Management Device)モデルで同じであることを確認してください。 チャネルは手動で選択する必要があります。
6. **デバイステンプレート**の**ラジオ設定**に移動します。 前のステップで説明したいずれかの設定されたメッシュプロファイルを選択します。
7. デバイステンプレートの他の詳細を設定し、デバイステンプレートを保存するために**保存**をクリックします。
8. 有線ネットワークへメッシュ AP として機能するすべての管理デバイス(Management Device)を接続します。 それらがルートか非ルート AP であるかどうかにかかわりなく、すべての管理デバイス(Management Device)を接続する必要があります。
9. メッシュ AP として機能するすべてのデバイスにデバイステンプレートを適用します。
10. 有線ネットワークから非ルート AP を外します。有線ネットワークに接続されたルート AP はそのままにしてください。
11. **デバイス>Management Devices** に移動します。 無線メッシュネットワーク内のルート AP または AP を指定してください。 ルートおよび非ルート AP を指定する詳細については、デバイステンプレート設定の上書きを参照してください。メッシュネットワークの設定は以上です。

メッシュプロファイルの追加

ご注意：2.4GHz 帯と 5GHz 帯両方の無線 LAN でメッシュプロファイルを構成することはサポートされていません。IEEE802.11a の帯域でメッシュプロファイルを設定する場合は、W52 チャネルのみ利用可能です。同じ周波数帯域で、複数のメッシュプロファイルを設定することはできません。

メッシュプロファイルを追加するには、次の手順を実行します。

1. **コンフィグレーション>デバイスのコンフィグレーション>SSID プロファイル>メッシュプロファイル** へ移動します。
2. ロケーションツリーからロケーションを選択します。 **メッシュプロファイル**内にロケーションで利用可能なメッシュプロファイルのリストが(もしあれば)見ることができます。
3. **メッシュプロファイルの新規追加**をクリックします。
4. メッシュプロファイルのパラメータを指定します。

フィールド	説明
プロファイル名	メッシュプロファイルの名前。
SSID	メッシュプロファイルの SSID。これは、メッシュネットワークのネットワーク名です。
最大ホップカウント	有線ネットワークに到達することが可能な最大ホップ数。 例えば、直接有線ネットワークに接続されているようなルート AP の場合はホップ数が 0 になります。 同様に、直接ルート AP と通信する非ルート AP のホップは 1 になります。
最大ダウンリンク	メッシュネットワーク内の非ルート AP またはルート AP と直接接続可能なメッシュ AP の最大数。 これは、親ノードがメッシュツリートポロジ内で持つことができる子ノードの最大数を示します。 0 から 5 の間の値を入力することができます。
最小 RSSI 値	メッシュで別の AP に接続する AP のための最小 RSSI 値。 別の AP に接続することを要求する AP が、他の AP に接続することができるためには指定された RSSI を持つ必要があります。 -100 から 0 dBm の間の値を入力することができます。

5. 新しく追加されたメッシュプロファイルを保存するには、**保存**をクリックします。

メッシュプロファイルの編集

メッシュプロファイルを編集するには、次の手順を実行します。

1. **コンフィグレーション>デバイスのコンフィグレーション>SSID プロファイル>メッシュプロファイル** へ移動します。
2. ロケーションツリーから、編集するメッシュプロファイルのロケーションを選択します。 **メッシュプロファイル**内にロケーションで利用可能なメッシュプロファイルのリストを見ることができます。
3. 編集するメッシュプロファイルの名前をクリックします。
4. メッシュプロファイルのパラメータを編集します。

フィールド	説明
プロファイル名	メッシュプロファイルの名前。
SSID	メッシュプロファイルの SSID。これは、メッシュネットワークのネットワーク名です。
最大ホップカウント	有線ネットワークに到達することが可能な最大ホップ数。 例えば、直接有線ネットワークに接続されているようなルート AP の場合はホップ数が 0 になります。 同様に、直接ルート AP と通信する非ルート AP のホップは 1 になります。
最大ダウンリンク	メッシュネットワーク内の非ルート AP またはルート AP と直接接続可能なメッシュ AP の最大数。 これは、親ノードがメッシュツリートポロジ内で持つことができる子ノードの最大数を示します。 0 から 5 の間の値を入力することができます。
最小 RSSI 値	メッシュで別の AP に接続する AP のための最小 RSSI 値。 別の AP に接続することを要求する AP が、他の AP に接続することができるためには指定された RSSI を持つ必要があります。 -100 から 0 dBm の間の値を入力することができます。

5. メッシュプロファイルへの変更を保存するには、**保存**をクリックします。

メッシュプロファイルのコピーを作成

メッシュプロファイルのコピーを作成し、それを修正することによって別のメッシュプロファイルとして使用することができます。
メッシュプロファイルのコピーを作成するには、次の手順を実行します。

1. **コンフィグレーション>デバイスのコンフィグレーション>SSID プロファイル>メッシュプロファイル** へ移動します。
2. ロケーションツリーから、メッシュプロファイルのロケーションを選択します。 **メッシュプロファイル**内にロケーションで利用可能なメッシュプロファイルのリストを見ることができます。
3. 別の名前で保存するには、メッシュプロファイルの名前をクリックします。
4. メッシュプロファイルの名前を変更します。必要に応じて他のパラメータを変更します。

フィールド	説明
SSID	メッシュプロファイルの SSID。これは、メッシュネットワークのネットワーク名です。
最大ホップカウント	有線ネットワークに到達することが可能な最大ホップ数。 例えば、直接有線ネットワークに接続されているようなルート AP の場合はホップ数が 0 になります。 同様に、直接ルート AP と通信する非ルート AP のホップは 1 になります。
最大ダウンリンク	メッシュネットワーク内の非ルート AP またはルート AP と直接接続可能なメッシュ AP の最大数。 これは、親ノードがメッシュツリートポロジ内で持つことができる子ノードの最大数を示します。 0 から 5 の間の値を入力することができます。
最小 RSSI 値	メッシュで別の AP に接続する AP のための最小 RSSI 値。 別の AP に接続することを要求する AP が、他の AP に接続することができるためには指定された RSSI を持つ必要があります。 -100 から 0 dBm の間の値を入力することができます。

5. メッシュプロファイルへの変更を保存するには、**保存**をクリックします。

別のロケーションへメッシュプロファイルをコピー

あるロケーションから別のロケーションにメッシュプロファイルをコピーするには、次の手順を実行します。

1. **コンフィグレーション>デバイスのコンフィグレーション>SSID プロファイル>メッシュプロファイル** へ移動します。
2. コピーするメッシュファイルが作成されているロケーションを選択します。そのロケーションのメッシュプロファイルのリストが表示されます。
3. 別のロケーションにコピーするメッシュプロファイルを選択します。
4. コピー先アイコンをクリック。ロケーションを選択するダイアログボックスが表示されます。
5. メッシュプロファイルをコピーしたいロケーションを選択します。
6. OK をクリックします。選択したメッシュプロファイルのコピーが選択したロケーションに作成されます。

ロケーションのメッシュプロファイルのリストを印刷

ロケーションに対して定義されたメッシュプロファイルのリストを印刷することができます。

ロケーションのメッシュプロファイルのリストを印刷するには、次の手順を実行します。

1. **コンフィグレーション>デバイスのコンフィグレーション>SSID プロファイル>メッシュプロファイル** へ移動します。
2. リストの中から印刷を希望する列を選択します。 列の選択または選択解除するには、任意の列名をクリックします。
3. 印刷アイコンをクリックします。リストの印刷プレビューが表示されます。
4. リストを印刷するには、**印刷**をクリックします。

メッシュプロファイルの削除

使用中のメッシュプロファイルを削除することはできません。

メッシュプロファイルを削除するには、次の手順を実行します。

1. **コンフィグレーション>デバイスのコンフィグレーション>SSID プロファイル>メッシュプロファイル** へ移動します。
2. 削除するメッシュファイルが作成されているロケーションを選択します。そのロケーションのメッシュプロファイルのリストが表示されます。
3. 削除するメッシュプロファイルを選択します。
4. 削除アイコンをクリックします。メッシュプロファイルの削除を確認するメッセージが表示されます。
5. 削除を確認して、メッシュプロファイルを削除するために、**Yes** を選択してください。

デバイステンプレートの管理

デバイステンプレートは、例えば、無線に関する設定、モニタするチャネル、モニタする VLAN、オフラインセンサー設定、アンテナ選択そしてポート割り当てなどの設定パラメータの集まりです。このテンプレートは、複数の Management Device に適用することができます。あなたの組織内に複数のデバイスがある場合には、個々のデバイスを設定することは単調で退屈で時間のかかる可能性があります。デバイステンプレートは、同時に複数の Management Device で Wi-Fi、および（または）WIPS 設定の標準セットを適用することにより、時間と労力を節約し、一貫性を保証する便利な方法です。 デフォルトのデバイステンプレートとしてテンプレートを構成することで、ロケーションに展開されているすべてのデバイスに対して共通のデバイステンプレートを持つことができます。

コンフィグレーション>デバイスのコンフィグレーション>デバイステンプレート を使用して、デバイステンプレートを管理します。 デバイステンプレートを管理するには管理者権限が必要です。

サーバーは、**System Template** と呼ばれるあらかじめ定義されたテンプレートで、 デフォルトのデバイス設定を保存しています。**System Template** は変更することが可能です。 デバイスが追加や発見されるたびに、サーバーがデバイスに自動的にこの テンプレートの構成設定を割り当てます。あなたのニーズに合わせて、**System Template** のデフォルトの 構成設定を編集することができます。あなたは、ロケーションのデフォルト テンプレート としてテンプレートを設定することができます。 このテンプレートは、そのロケーションにタグ付けされた新しいデバイスに適用されます。

ユーザー定義のデバイステンプレートを削除すると、 **System Template** は、そのテンプレートに関連付けられているすべてのデバイスに適用されます。 **デバイス> Management Devices** タブから、手動で Management Device に適用されたテンプレートを上書きすることができます。 テンプレートの設定をカスタマイズすると、新しい設定はこのテンプレートが適用されている Management Device に適用されます。 カスタマイズした設定を適用するには、Management Device に新しい設定をプッシュする必要があります。

ロケーションのポリシー/デバイステンプレートをカスタマイズ

ポリシーは、ロケーションに適用されるルールのセットです。このルールのセットは、デバイステンプレートによって表現されます。

新しいロケーションフォルダーを作成すると、親のロケーションフォルダーからデフォルトのポリシーまたはデバイステンプレートを継承します。 ロケーションのフロアは、その直接の親ロケーションフォルダーからデフォルトのデバイステンプレートを継承します。 これは、このロケーションに接続するすべての管理デバイス(Management Device)がこのデフォルトのテンプレートを使用することを意味します。

独自のデバイステンプレートを定義し、そのロケーションフォルダーのデフォルトのテンプレートにすることができます。 これを、選択されたロケーションでポリシーまたはデバイステンプレートをカスタマイズすると呼びます。

あなたは、ロケーションフォルダー・レベルでポリシーまたはデバイステンプレートをカスタマイズすることができます。 このカスタマイズは、ロケーションフロア・レベルでは利用できません。

ロケーションでデバイステンプレートを変更すると、変更後にロケーションに接続するすべての管理デバイス(Management Device) は新しく適用されたデバイステンプレートを使用します。 そのロケーションに存在するデバイスで、変更されたデバイステンプレートを使用するか、 以前のデフォルトのデバイステンプレートを引き続き使用するどうかを選択することができます。 これは、そのロケーションでデフォルトのデバイステンプレートの変更をしたときに行うことができます。

選択したロケーションでポリシーをカスタマイズするには、次の手順を実行します。

1. デバイステンプレートのページにある、 **編集を有効にしてポリシーをカスタマイズするにはここをクリックしてください。** のリンクをクリックします。 **コンフィグレーション> デバイスのコンフィグレーション> デバイステンプレート** のデバイステンプレートリストで、ユーザー定義のデバイステンプレートで**デフォルトにする** リンクが有効になります。
2. ロケーションのデフォルトテンプレートを変更するには、デフォルトテンプレートとして設定したいデバイステンプレートの **デフォルトにする** のリンクをクリックします。確認のメッセージが表示されます。
3. そのロケーションで既存のデバイスに新しいデバイステンプレートを適用する場合は、 **Yes** をクリックします。 既存のデバイスは、古いデフォルトのデバイステンプレートを引き続き使用したい場合は、 **No** をクリックします。

継承されたデバイステンプレートに戻す

ロケーションでカスタマイズしたデバイステンプレートを定義したあと、親のデバイステンプレートを継承したい場合は、次の手順を実行します。

1. **デバイステンプレート** ページの下にある **親ロケーションから継承しますか？** のリンクをクリックします。
2. 親ロケーションから継承するかどうかの確認を求めるメッセージで **Yes** をクリックします。 別の確認メッセージが表示されます。
3. そのロケーションで既存のデバイスに継承されたデバイステンプレートを適用する場合は、**Yes** をクリックします。 既存のデバイスでカスタマイズしたデフォルトのデバイステンプレートを引き続き使用したい場合は、**No** をクリックします。

デバイステンプレートの追加

デバイステンプレートを追加する際に、デバイステンプレートの名前と説明を指定し、テンプレートを保存することができます。 テンプレートが、このようにデバイス設定やラジオ設定なしで定義されデバイスに適用されると、そのデバイスは WIPS センサーとして機能します。

新しいデバイステンプレートを追加するには、次の手順を行います。

1. 新しいデバイステンプレートを追加するには、**コンフィグレーション>デバイスのコンフィグレーション> デバイステンプレート** で **デバイステンプレートの追加** をクリックします。
2. 次の値を指定します。

フィールド	説明
テンプレート名	デバイステンプレートの名前。
説明	デバイステンプレートの簡単な説明。
デバイス固有のカスタマイズを許可	デバイステンプレートを 介して行われた設定を上書きする場合は、このチェックボックスにチェックを入れます。 詳しくは デバイステンプレート設定の上書き を参照。
運用地域	管理デバイス(Management Device)の 運用地域または国。

3. **デバイステンプレートの追加** ダイアログボックス上の**デバイス設定 > デバイスのパスワード** で、デバイスのパスワードを指定します。
4. デバイステンプレートの設定を保存するには、**保存** をクリックします。

デバイステンプレートのデバイス設定を構成するには、**デバイステンプレートの追加** 画面上の**デバイス設定** をクリックします。

デバイス設定

デバイス設定は、VLAN の監視、デバイスのパスワード、デバイスアクセスログ、オフライン設定、サードパーティ解析のインテグレーション、およびチャネル設定に、更に細かく分かれます。
これらの各々は、以下で説明されます。

VLAN モニタリング

VLAN モニタリングは、有線側接続ステータスの検出、ホスト名検出、スマートデバイス検出、 不正 AP(Rogue AP)の検出、その他のために不可欠です。デバイスが追加の VLAN をモニタするのを可能にするために、 **追加の VLAN をモニタ** のチェックボックスを選択してください。 カンマ区切りのリストとして、監視対象のすべての追加の VLAN を含めます。 サーバーと通信するデバイスによって用いられる VLAN は、常に監視されているのでここで指定する必要はありません。 監視対象の追加の VLAN は、デバイスが接続されるスイッチポートの上で構成され、 DHCP が有効にされている必要があります。 スイッチの実際の VLAN 番号にかかわりなく、VLAN ID '0'は、デバイスが接続されるスイッチポート上でタグがない VLAN を示します。

ご注意： VLAN が静的 IP アドレスで設定されている場合は、CLI より VLAN を設定します。

デバイステンプレートが適用される 1 つまたは複数の特定のデバイスを監視するために VLAN をカスタマイズしたい場合は、**デバイス > デバイスのプロパティ**を使用してそれを行うことができます。 更に監視対象の VLAN をオーバーライドするためには、**デバイス固有のカスタマイズを許可** チェックボックスを選択する必要があります。

デバイスのパスワード

デバイステンプレートで管理デバイス(Management Device)のコマンドラインインタフェース（CLI）のユーザー'config' 用のパスワードを管理することができます。 デバイステンプレートでパスワードを定義することで、個別に各デバイス上でそれを変更することなく、 デバイスグループのパスワードを管理することができます。 パスワードは、少なくとも 6 文字以上でスペースを含めることはできません。

'config' ユーザーの新しいパスワードを指定する必要があります。保存する前に新しいパスワードを確認します。 新しいパスワードは、デバイステンプレートに関連付けられているすべてのデバイスに適用されます。

デバイスアクセスログ

管理コンソール(Management Console)は、Syslog サーバーへセンサーのアクセスログを送信するための機能を提供します。 本機能は、監査の目的に有用であり、デバイステンプレートで有効または無効にすることができます。 有効にした場合は、アクセスログが送信される **Syslog サーバーの IP/ホスト名**を指定します。

オフライン設定

本機能は、管理デバイス(Management Device)とサーバーとの間で接続がない場合でも、いくつかのセキュリティ上の保証を提供します。それは、サーバーから切断されたときにセンサーがいくつかのデバイス分類と防御機能を提供します。 センサーは、イベントを発生させ、それらを格納し、 再接続時にサーバーにそれらをプッシュします。 本機能を有効にするには、 **オフラインモードを有効** を選択します。
センサーがサーバーから何の通信も受信せずに、 かつオフラインセンサーモードが有効にされている場合は、一定の時間経過後にセンサーはオフラインモードに自動的に移行します。
（最小：5 分、最大：60 分、デフォルト：15 分）

オフライン設定には 3 つのサブセクションがあります。

1. **Management Device パラメータ**：Management Device パラメータのセクションでは、以下を指定することができます。
   AP の数：デバイスがオフラインモードで保存する AP 識別の最大数 （デフォルト：128）。
   クライアント数： デバイスがオフラインモードで保存するクライアント識別の最大数 （デフォルト：256）。
   イベント数： デバイスがオフラインモードでバッファリングする発生したイベントの最大数（デフォルト：256）。これは、リングバッファとして保持されます。 つまり、発生したイベントがこの制限を超えると、最も古いイベントが上書きされます。 デバイスがサーバーに再接続したときにバッファリングされたイベントはサーバーに転送されます。
   侵入防御レコード数： センサーがオフラインモードでバッファリングする防御レコードの最大数（デフォルト：256）。これは、リングバッファとして保持されます。 つまり、発生したイベントがこの制限を超えると、最も古いイベントが上書きされます。 デバイスがサーバーに再接続したときにバッファリングされたイベントはサーバーに転送されます。

2. **デバイス分類ポリシー** ： サーバーに接続されていない場合に、センサーが AP とクライアントデバイスを分類する方法を指定します。
   AP およびクライアントの分類ポリシーを以下の方法で設定します。
   - 不正 AP としてネットワーク上の AP を分類したい場合は、**ネットワーク接続された AP を移動** チェックボックスを選択し、 このチェックボックスの次に、ドロップダウンリストから **Rogue** を選択します。
   - 許可 AP(Authorized AP)としてネットワーク上の AP を分類したい場合は、**ネットワーク接続された AP を移動** チェックボックスを選択し、 このチェックボックスの次に、ドロップダウンリストから **Authorized** を選択します。
   - 外部 AP として非ネットワーク上の AP を分類したい場合は、 **非ネットワーク AP を外部フォルダーへ移動** チェックボックスを選択します。
   - クライアント分類ポリシーも同様に設定します。

3. **侵入防御ポリシー**： サーバーに接続されていない場合に、センサーで有効にする侵入防御の脅威を指定します。
   オフラインモード時に、センサーが防御することを望む脅威に対して、1 つ以上のチェックボックスを選択します。
   センサーは、以下の脅威に対して侵入防止を行うことができます： 不正 AP(Rogue AP),ネットワークに接続されている未分類 AP、 AP は許可として分類されているがセキュリティ対策を行っていない、 AP は許可として分類されているが弱いセキュリティ対策を行っている、 許可クライアントの外部 AP への接続、 未許可クライアントの許可 AP(Authorized AP)への接続、 未分類クライアントの許可 AP(Authorized AP)への接続、 許可クライアントのアドホックネットワークへの参加、 ハニーポット/エビルツイン AP。

サードパーティ解析のインテグレーション

本機能は、サードパーティ製の外部サーバーと管理デバイス(Management Device)の統合を可能にし、サードパーティ製の外部サーバーに可視性の分析データを送信します。

サードパーティ製の外部サーバーとの統合を有効にするには、次の手順を実行します。

1. **有効** チェックボックスを選択します。
2. **サーバーURL** にサードパーティ製の外部サーバーの URL または IP アドレスを入力します。
3. **認証キー**にサードパーティ製の外部サーバーと認証するための管理デバイス(Management Device)のキーを入力します。
4. **送信間隔**は、管理デバイス(Management Device)がサードパーティ製の外部サーバーへクライアントの RSSI 値を送信すべき時間間隔を指定します。

チャネル設定

センサーが利用可能なチャネルのリストからモニタするためのチャネルを選択します。 これらのチャネルは、運用する国によって異なります。

ラジオ設定

AP モードでは、1 つの物理的な AP デバイスは複数の仮想 AP に論理的に分割されることができます。 AP として機能するために管理デバイス(Management Device)を構成する場合は、ラジオ設定を構成し、1 つ以上の SSID プロファイルを指定することができます。 各 SSID プロファイルは、1 つの仮想 AP の構成設定に対応します。

アクセスポイントモードでラジオ設定を行うには、次の手順を実行します。

1. **コンフィグレーション>デバイスのコンフィグレーション>デバイステンプレート**へ移動します。
2. **デバイステンプレートの追加** ダイアログボックスまたは適用可能な**デバイステンプレートの編集**ダイアログボックスで、**ラジオ設定**をクリックします。
3. **モデルの設定を定義** リンクをクリックします。利用可能な管理デバイス(Management Device)モデルのドロップダウンリストが表示されます。
4. 適切なモデルを選択します。モデルの詳細が表示されます。
5. **アクセスポイント**として希望する無線に対して**動作モード**を選択します。
6. ラジオ設定を構成します。

フィールド	説明
周波数帯	無線の周波数帯。 可能な値は、2.4GHz 帯と 5GHz 帯です。
チャネル幅	無線のチャネル幅。
動作チャネル	無線の動作チャネル。 デフォルトで AP は自動的に動作チャネルを選択します (**自動**)。 ユーザーは、必要に応じて手動でチャネルを設定することができます。 動作チャネルを設定するには、 **手動** を選択します。 左側のボックスで選択されるロケーションに基づいて、チャネル番号のリストが手動のチャネル選択のために現れ提示されます。
選択間隔	このフィールドは 動作チャネルが**自動**に設定されている場合にのみ表示されます。 このフィールドには、チャネル選択が発生する時間の時間間隔を指定します。1 から 48 の任意の値を入力することができます。
チャネル番号	このフィールドは 動作チャネルが**手動**に設定されている場合にのみ表示されます。 メッシュネットワーク内の AP にチャネル番号を定義している場合は、メッシュ AP として機能するすべての管理デバイス(Management Device)モデルで チャネル番号が同じであることを確認してください。
バックグラウンドスキャン	AP による バックグラウンドスキャンを有効にするには、このチェックボックスにチェックを入れます。 **ご注意：** 無線が VoIP（Voice over IP）で使用されている場合は、バックグラウンドスキャンを有効にしないでください。
ラジオ詳細設定	
送信出力	このフィールドは、 AP の送信出力の制御が可能となります。 送信出力チェックボックスをオンにして、dBm 単位で AP の送信出力を指定します。 送信パワーをカスタムするチェックボックスの選択が解除されている場合は、使用する国で許可されている最大の許可送信出力が AP に設定されます。
フラグメンテーション スレッショルド(閾値)	バイト単位での フラグメンテーションの閾値です。このフィールドの許容値は 256 から 2346 バイトです。 このフィールドは、5GHz 帯および 2.4GHz 帯のモードで適用可能です。

RTS スレッショルド(閾値)	バイト単位での 送信要求（RTS）閾値です。 AP が送信のために送信要求(RTS)/受信準備完了(CTS)ハンドシェイクを使用しなければならいない フレームサイズの上限に対する閾値を指定します。 このフィールドは、5GHz 帯および 2.4GHz 帯のモードで適用可能です。 **ご注意：** 閾値が非常に小さな値に設定されている場合、無線チャネルが効率的に利用されません。 この閾値は、 大きなフレームが衝突によりそれらを失って、チャネルリソースの浪費を引き起こすことを避けるために使われます。
Beacon 間隔	AP のビーコン送信間隔を ミリ秒単位で指定します。値は 100 ミリ秒に設定されます。これを変更することはできません
DTIM 間隔	DTIM (Delivery Traffic Indication Message) 間隔は、AP に接続されるクライアントが AP 上にバッファリングされている データをチェックしなければならない間隔です。
IEEE802.11n/ac ガードインターバル	次の信号を 送信する前に、信号が消散することを可能にするための各 OFDM シンボルの終わりの時間間隔です。 これは、連続する 2 つのシンボル間の重複を防止します。 レガシーの IEEE802.11a/b/g デバイスは 800ns の GI を使用しています。400ns の GI は、IEEE802.11n および ac 用のオプションです。 このフィールドは IEEE802.11n および ac 固有のものです。
フレームアグリゲーション有効	このフィールドは MPDU（MAC Protocol Data Unit）の有効/無効化を指定します。このフィールドは IEEE802.11n 固有のものです。
バンドステアリングロードバランシングスレッショルド	5GHz 帯に接続しているクライアント数が、2.4GHz 帯に接続しているクライアント数と比べてここで指定したスレッショルドより少ない場合は、新規のクライアントは 5GHz 帯に誘導されます。バンドステアリングが有効になっている場合のみ誘導されます。 **ご注意：** 無線 LAN クライアントによっては、5GHz 帯へ積極的に接続要求を行う機種があるため、設定したスレッショルドの値を超えて 5GHz 帯の SSID に帰属する場合があります。
Spatial Streams	このフィールドは AP の無線通信における送受信の空間ストリーム数を設定します。3x3、2x2、1x1 より選択してください（ファームウェアバージョン 1.3〈1.3.02〉以降に対応）。 **ご注意：**本設定を変更して AP にデバイステンプレートを適用する場合は、必ず AP を再起動してください。

7. **SSID プロファイルの追加**をクリックし、利用可能なリストから AP に関連する SSID プロファイルを選択します。 AP に複数の SSID プロファイルを追加したい場合は、この手順を繰り返します。 同様に、メッシュ AP として機能する管理デバイス(Management Device)にテンプレートを適用する場合は、デバイステンプレートにメッシュプロファイルを追加することが可能です。

センサーモードでラジオ設定を構成するには、次の手順を実行します。
モデルの設定を定義 リンクをクリックします。 利用可能な管理デバイス(Management Device)モデルのドロップダウンリストが表示されます。
1. 適切なモデルを選択します。 モデルの詳細が表示されます。デフォルトでは、すべての利用可能な無線はセンサーモードで構成されています。

デバイステンプレートから デバイスモデルの設定を削除するには、次の手順を実行します。
1. テンプレートの詳細を表示するには、 それぞれのデバイステンプレートのリンクをクリックしてください。
2. **ラジオ設定**をクリックします。
3. モデル名をクリックします。モデル構成が表示されます。
4. モデル構成の右上にある**モデルの削除** のリンクをクリックしてください。
5. 変更を保存するために、**保存** をクリックします。

モデルを削除し、再度それを追加したいような場合は、次の手順を実行します。
1. **モデルの追加** をクリックして、 構成設定を定義するモデルを選択します。
2. デバイスモデルの構成設定を定義します。

3. 変更を保存するために、**保存** をクリックします。

デバイステンプレート設定の上書き

デバイステンプレートは、複数の管理デバイス(Management Device)へ適用することができます。いくつかの固有の理由で、デバイステンプレートが適用される少数の AP に対して送信出力、チャネルまたはモニタする VLAN の追加を変更したい場合は、デバイス固有のカスタマイズを許可してください。
送信出力、チャネル、またはモニタする VLAN 追加は、カスタマイズして上書きすることができるフィールドです。

次のタスクを実行して、デバイスレベルでのデバイステンプレートの設定を上書きすることができます。
1. **コンフィグレーション>デバイスのコンフィグレーション>デバイステンプレート**へ移動します。
2. デバイステンプレートを編集します。
3. 管理デバイス(Management Device)に適用されているデバイステンプレートで **デバイス固有のカスタマイズを許可** チェックボックスを選択します。ラジオ設定パラメータのチャネル、送信出力、モニタする VLAN 追加を上書きできます。
4. **デバイス**ページに移動し、設定を上書きしたい管理デバイス(Management Device)を選択します。
5. 必要な設定を変更し、変更を保存します。 これらの設定のカスタマイズの詳細については、デバイステンプレートの設定をカスタマイズ を参照してください。

ご注意： たとえデバイステンプレートでデバイス構成ごとに有効にするとしても、あとの時点でカスタマイズされた設定を指定することができます。

デバイステンプレートの編集

デバイステンプレートを編集するには、次の手順を実行します。
1. **コンフィグレーション>デバイスのコンフィグレーション>デバイステンプレート**へ移動します。
2. デバイステンプレート名のリンクをクリックしてください。
3. 次の値の 1 つ以上を変更します。

フィールド	説明
テンプレート名	デバイステンプレート固有の名前。
説明	デバイステンプレートの簡単な説明。
デバイス固有 のカスタマイズを許可	デバイステンプレートで 行われる設定を上書きするには、このチェックボックスを選択します。 詳細については、デバイステンプレート設定の上書きを参照。
運用地域	管理デバイス(Management Device)の運用域または国。

4. デバイス設定を変更するためには、**デバイス設定**をクリックしてください。 詳細については、デバイス設定 を参照。
5. ラジオ設定を変更するためには、**ラジオ設定**をクリックしてください。 詳細については、 ラジオ設定 を参照。
6. デバイステンプレートの設定を保存するには、 **保存** をクリックします。

ご注意： そのロケーションでデバイステンプレートを定義した場合のみ、 選択されたロケーションでデバイステンプレートを編集することができます。

デバイステンプレートの検索

テンプレート名に基づいてデバイステンプレートを検索することができます。

デバイステンプレートを検索するには、次の手順を実行します。
1. **コンフィグレーション>デバイスのコンフィグレーション>デバイステンプレート**へ移動します。
2. デバイステンプレートページで、右上隅のテンプレート名の**クイックサーチ** ボックスにキーワードまたは検索文字列を入力します。
3. キーワードまたは検索文字列に基づくテンプレートのリストをフィルターするために **Enter** を押します。 検索条件に一致するデバイステンプレートが、デバイステンプレートのリストに表示されます。

デバイステンプレートのコピー

別のロケーションにデバイステンプレートをコピーすることができます。 コピーされたデバイステンプレートは、新しいロケーションで編集可能です。

あるロケーションから別のロケーションにデバイステンプレートをコピーするには、 次の手順を実行します。
1. **コンフィグレーション>デバイスのコンフィグレーション>デバイステンプレート**へ移動します。
2. デバイステンプレートを選択します。
3. コピー先アイコンをクリックします。ロケーションの選択 ダイアログボックスが表示されます。
4. デバイステンプレートをコピーしたいロケーションを選択します。
5. OK をクリックします。

ロケーションのデバイステンプレートリストを印刷

ロケーションに対して定義されたデバイステンプレートのリストを印刷することができます。

ロケーションのデバイステンプレートのリストを印刷するには、次の手順を実行します。
1. **コンフィグレーション>デバイスのコンフィグレーション>デバイステンプレート**へ移動します。
2. デバイステンプレートのリストを印刷したいロケーションを選択します。
3. リストの中から印刷を希望する列を選択します。 列の選択または選択解除するには、任意の列名をクリックします。
4. 印刷アイコンをクリックします。リストの印刷プレビューが表示されます。
5. リストを印刷するには、**印刷**をクリックします。

デバイステンプレートの削除

そのロケーションでデバイステンプレートが定義されている場合だけ、選択されたロケーションでデバイステンプレートを削除することが可能です。
テンプレートの削除は、結果としてデフォルトのデバイステンプレートをこのテンプレートと関連する管理デバイス(Management Device)に割り当てることになります。
System Template を削除することはできません。

デバイステンプレートを削除するには、次の手順を実行します。
1. **コンフィグレーション>デバイスのコンフィグレーション>デバイステンプレート**へ移動します。
2. デバイステンプレートを削除したいロケーションを選択します。

3. 削除したいデバイステンプレートのチェックボックスを選択します。
4. 削除アイコンをクリックします。削除を確認するメッセージが表示されます。
5. デバイステンプレートの削除を実行するために、**Yes** をクリックしてください。

ネットワークインタフェースプロファイルの管理

ネットワークインタフェースプロファイルは、設定された SSID とリモートのエンドポイントとを結ぶための設定情報を表示しています。ネットワークインタフェースプロファイルは、GRE(EoGRE) 設定でイーサネットを設定するために使われます。一般的なルーティングカプセル化(GRE)は、ネットワークの上のバーチャルなポイントツーポイントリンクの中でさまざまなネットワーク層プロトコルをカプセル化することができるトンネルプロトコルです。 1 以上がアクセスポイントから集合機器にトンネルを掘るセットアップに、EoGRE は能力を提供します。複数の SSID からの通信はそのようなトンネルを通して行うことができます。

ネットワークインタフェースプロファイルを設定する場合、プライマリエンドポイントとセカンダリエンドポイントを指定することができます。プライマリエンドポイントとの接続が失敗するならば、セカンダリエンドポイントとの接続を行います。セカンダリエンドポイントの設定はオプションです。

ネットワークインタフェースプロファイルの設定は SSID プロファイルの設定の際にリモートブリッジングをあらかじめ設定しておく必要があります。

ネットワークインタフェースプロファイルの追加

ネットワークインタフェースを作成するには以下の手順を行います。

1. **コンフィグレーション>デバイスのコンフィグレーション>ネットワークインタフェース**を選択します。
2. 以下の設定値を入力します。

フィールド	説明
Profile Name	プロファイル名を設定してください。260 バイトまで入力可能です。
Tunnel Type	Ethernet over GRE を選択してください。
ベーシックパラメータ（またはプライマリエンドポイントパラメータ）	
Remote Endpoint(IP Address)	プライマリエンドポイントの IP アドレスを設定してください。DHCP オプション 42 を使って NTP サーバーの IP アドレスを使用する場合は空白でも設定可能です。
Local Endpoint VLAN	VLAN ID を設定してください。
セカンダリエンドポイント関連パラメータ	
Enable Secondary Endpoint	セカンダリエンドポイントを使用する場合はチェックボックスにチェックを入れてください。
Remote Endpoint(IP Address)	セカンダリエンドポイントの IP アドレスを設定してください。DHCP オプション 42 を使って NTP サーバーの IP アドレスを使用する場合は空白でも設定可能です。
Local Endpoint VLAN	VLAN ID を設定してください。
Network Probe Interval	エンドポイントとの疎通確認のための Ping パケットのインターバルを設定してください。10 の倍数で設定してください。
Network Ping Retry Count	Ping パケットの送信回数を設定してください。
Network Ping Timeout	Ping 応答のタイムアウト時間を設定してください。
Prefer Primary Tunnel over Secondary Tunnel	セカンダリエンドポイントよりもプライマリエンドポイントとの接続を優先する場合はチェックボックスにチェックを入れてください。
Ethernet over GRE	
GRE Primary Key	GRE ヘッダーで使用するプライマリキーを設定してください。キーの入力は必須ではありません。
GRE Secondary Key	GRE ヘッダーで使用するプライマリキーを設定してください。キーの入力は必須ではありません。

3. Save を押して保存してください。

イベント管理

イベントの表示と管理

イベントページは、システムによって生成されたイベントに関する情報を提供します。 このページでは、フィルター、ロケーション、承認、既読または未読としてマークを表示することができ、脆弱性評価へのイベントの関与の状態を切り替えることができます。 また、ロケーションで表示されるイベントのリストを印刷することができます。

WIPS センサーは次のタイプにイベントを分類します（セキュリティ、システム、およびパフォーマンス）。
セキュリティイベントは、無線セキュリティの脅威に関連しています。 例えば、不正 AP(Rogue AP) がネットワークにアクセスしようと試みると、セキュリティイベントが生成されます。
セキュリティイベントは、更に無線セキュリティの脅威に基づいて分類されます。次のようなセキュリティイベントのカテゴリがあります。
・不正 AP(Rogue AP)によって生成されるイベント。
・誤設定された AP(Misconfigured AP)によって生成されるイベント。
・不正なクライアント(misbehaving Client)によって生成されるイベント。
・アドホックネットワークによって生成されるイベント。
・中間者攻撃(man-in-the-middle attacks)によって生成されるイベント。
・DoS 攻撃（サービス拒否）に起因して生成されるイベント。
・MAC なりすましに起因して生成されるイベント。
・防御に起因して生成されるイベント。
・無線の収集活動に起因して生成されるイベント。
・無線ネットワークのクラッキングに起因して生成されるイベント。

システムイベントは、システムの正常性を示します。 センサー、管理コンソールサーバーそしてトラブルシューティング・イベントによって生成されるイベントに基づいて更に分類されます。

パフォーマンスイベントは、無線ネットワークのパフォーマンスの問題を示しています。 帯域幅、設定、カバレッジ、および干渉に基づいて更に分類されます。 これらは、無線ネットワークのパフォーマンスに関連する問題を理解するために使用することができます。

イベントページは 2 つのパネルに分かれています。 上のパネルには選択したロケーションのイベントリストが表示されます。 下のパネルのサブイベントの詳細では、**イベント**ページの上のパネルで選択したイベントに関与するイベントとサブイベント内のデバイスの詳細を表示します。

上下のパネルの間にはツールバーがあります。 これには、イベントのロケーション変更やイベントの脆弱性ステータスの変更、イベントの削除、イベントの印刷などの多様なイベント関連の操作を実行するためのアイコンが含まれています。

次の表では、**イベント**ページの上部パネルに表示されるイベント関連のフィールドについて説明します。

フィールド	説明
ID	システムがイベントに対して生成したイベント ID。
イベント深刻度	イベントの深刻度は、アイコンによって示されます。 深刻度は高、中、低のいずれかになります。
イベントのアクティビティ・ステータス	イベントステータスはアイコンで示されます。 取りうる値は、ライブ、瞬間的(instantaneous)、更新済み、期限切れのいずれかになります。
詳細	イベントの説明。
カテゴリ	イベントのカテゴリ。
ロケーション	イベントが発生したロケーション。
開始時間	イベントが開始した時間。
イベントのリード・ステータス	イベントが既読、未読、承認または未承認かどうかを示します。
イベントの脆弱性ステータス	イベントの脆弱性を示します。
イベントタイプ	イベントのタイプ。 タイプはアイコンで示されます。 取りうる値は、セキュリティ、システム、パフォーマンスです。
停止時間	イベントが停止した時刻。

ロケーションのイベントを表示

イベントカテゴリに基づいて選択したロケーション（および、その子ロケーション）でのイベントを表示することができます。 それらのカテゴリとサブカテゴリに基づいてイベントをフィルタリングすることができます。
ロケーションに関するイベントを表示するには、次の手順を実行します。

1. **イベント**へ移動します。
2. イベントを表示したいロケーションを選択します。
3. ネットワーク内のセキュリティの脆弱性や違反を示すイベントを表示するには、**セキュリティ** のチェックボックスにチェックを入れます。 各セキュリティイベントのチェックボックスを選択または解除することで、セキュリティイベントを表示することや、フィルタリングすることができます。 セキュリティイベントのリストを表示するには、「セキュリティ」の文字の横にある下矢印をクリックします。
4. システムの正常性を示すイベントを表示するには、**システム** のチェックボックスにチェックを入れます。 各システムイベントのチェックボックスを選択または解除することで、タイプに基づいてシステムイベントを表示することや、フィルタリングすることができます。 システムイベントのリストを表示するには、「システム」の文字の横にある下矢印をクリックします。
5. 無線ネットワークのパフォーマンス問題を示すイベントを表示するには、**パフォーマンス** のチェックボックスにチェックを入れます。 各パフォーマンスイベントのチェックボックスを選択または解除することで、タイプに基づいてパフォーマンスイベントを表示することや、フィルタリングすることができます。 パフォーマンスイベントのリストを表示するには、「パフォーマンス」の文字の横にある下矢印をクリックします。

ご注意： サーバークラスタ内の親サーバー上のルートロケーションを表示している場合は、子サーバーと親サーバー上のすべてのイベントが集約されています。 現在、親サーバーのみに属するイベントを表示する適切なメカニズムはありません。

ロケーションの削除されたイベントを表示

削除としてマークしたイベントを表示するには、次の手順を実行します。
1. **イベント**へ移動します。
2. 削除されたイベントを表示したいロケーションを選択します。
3. ツールバーの**更に**をクリックし、**削除されたイベントを表示**を選択します。 イベントは削除としてマークされます。

イベントロケーションの変更

イベントのロケーションを変更するには、次の手順を実行します。
1. **イベント**へ移動します。
2. イベントが発生したロケーションを選択します。
3. ロケーションを変更したいイベントのチェックボックスにチェックを入れます。
4. 「ロケーションの変更」アイコンをクリックします。 ロケーションを選択するダイアログボックスが表示されます。
5. 新しいロケーションを選択し、[OK]をクリックします。イベントは、新しいロケーションに移動されます。

イベントを承認

イベントを承認するには、次の手順を実行します。
1. **イベント**へ移動します。
2. イベントを承認したいロケーションを選択します。
3. 承認したいイベントのチェックボックスを選択し、ツールバーの「承認」アイコンをクリックします。
4. 「承認」ダイアログボックスが表示されます。ノートを入力し、[OK]をクリックします。

イベントの脆弱性ステータスをオン

イベントの脆弱性ステータスをオンにするには、次の手順を実行します。
1. **イベント**へ移動します。
2. イベントの脆弱性ステータスを変更したいロケーションを選択します。
3. 脆弱性ステータスをオンにするイベントのチェックボックスを選択します。
4. イベントの脆弱性をオンにするには、「脆弱性のステータスをオン」アイコンをクリックします。

イベントの脆弱性ステータスをオフ

イベントの脆弱性ステータスをオフにするには、次の手順を実行します。
1. **イベント**へ移動します。
2. イベントの脆弱性ステータスを変更したいロケーションを選択します。
3. 脆弱性ステータスをオフにするイベントのチェックボックスを選択します。
4. イベントの脆弱性をオフにするには、「脆弱性のステータスをオフ」アイコンをクリックします。

既読としてイベントをマーク

既読としてイベントをマークするには、次の手順を実行します。
1. **イベント**へ移動します。
2. 既読としてマークしたいイベントのロケーションを選択します。
3. 既読としてマークしたいイベントのチェックボックスにチェックを入れます。
4. ツールバーの**更に**をクリックし、**既読としてマーク**を選択します。 イベントは既読としてマークされます。

削除としてイベントをマーク

削除済みとしてイベントをマークするには、次の手順を実行します。
1. **イベント**へ移動します。
2. イベントを削除したいロケーションを選択します。
3. 削除としてマークしたいイベントのチェックボックスにチェックを入れます。
4. ツールバーの**更に**をクリックし、**削除済みとしてマーク**を選択します。 イベントは削除済みとしてマークされます。

カスタムフィルターを追加

カスタムフィルターを作成し、任意の名前で保存することができます。 管理コンソール(Management Console)上にある列内のデータにフィルター条件を設定することができます。 名前を付けてこのフィルターを保存することができ、同様に複数のフィルターを作成することが可能です。

カスタムフィルターを使用する際は、次の点に注意してください。
- 列の可視性と列データのソート設定は、カスタムフィルターには保存されません。 フィルター基準のみが保存されます。
- カスタムフィルターは、ユーザー固有です。カスタムフィルターを定義したユーザー用に保存され、他のユーザーからは見えません。
- 保存されていないフィルターは、ツールバーの**フィルター**の横にあるフィルター名にアスタリスクで表示されます。
- ユーザーがフィルターを保存せずにログアウトした場合、未保存のフィルターは保存されません。

カスタムフィルターを作成するには、次の手順を実行します。
1. **イベント**へ移動します。
2. 列のヘッダーの横にあるアイコンをクリックすると、オプションのリストが表示されます。
3. **フィルター**にマウスをポイントして、カラムのフィルターテキストを入力し、**Enter** キーを押します。
4. ツールバーの**フィルター**の横にあるアイコンをクリックして、 **名前を付けて保存**をクリックします。 **名前を付けて保存**のダイアログボックスが表示されます。
5. カスタムフィルターの名前を入力し、**OK** をクリックします。 カスタムフィルターが保存されます。

カスタムフィルターの編集

カスタムフィルターを編集するには、次の手順を実行します。
1. **イベント**へ移動します。
2. **フィルター**の横にあるアイコンをクリックして、必要なフィルターを選択します。
3. 列のヘッダーの横にあるアイコンをクリックすると、オプションのリストが表示されます。
4. **フィルター**にマウスをポイントして、列のフィルターテキストを入力するか、必要に応じてのフィルター条件を変更します。
5. ツールバーの**フィルター**の横にあるアイコンをクリックして、 **保存**をクリックします。 変更されたカスタムフィルターが保存されます。

カスタムフィルターの削除

カスタムフィルターを削除するには、次の手順を実行します。
1. **イベント**へ移動します。
2. ツールバーの**フィルター**の横にあるアイコンをクリックして、アイコンをクリックします。 削除を確認するよう問いかけるメッセージが表示されます。
3. カスタムフィルターの削除を確定するために、**Yes** をクリックします。

ロケーションのイベントリストを印刷

ロケーションで生成されるイベントのリストを印刷することができます。
ロケーションでイベントのリストを印刷するには、次の手順を実行します。
1. イベントへ移動します。
2. リストに印刷する列を選択します。 列を選択または解除するには、上のパネルで任意のカラム名をクリックします。
3. 印刷アイコンをクリックします。 ロケーションのすべてのイベントリストの印刷プレビューが表示されます。
4. リストを印刷するには、印刷をクリックします。

イベント通知の設定

特定のイベントの発生は、Syslog、SNMP などの外部エージェントに通知する必要があります。この設定は、**コンフィグレーション>イベント>コンフィグレーション** を使用して行います。

WLAN が機能しているときにさまざまな種類のイベントが発生します。これらは管理コンソール(Management Console)によって、セキュリティ、パフォーマンス、およびシステムイベントとして分類されます。
これらの各タイプは、**コンフィグレーション** ページでそれぞれのタブに表示されています。

セキュリティイベントは、ネットワーク内のセキュリティの脆弱性や違反を示しています。セキュリティイベントは、以下のとおり更に分類されます。

- Misconfigured AP イベント
- DoS イベント
- Reconnaissance イベント
- Rogue AP イベント
- Man-in-the-middle イベント
- Ad hoc イベント
- Cracking イベント
- MAC spoofing イベント
- Misbehaving clients イベント
- Prevention イベント

パフォーマンスイベントは、無線ネットワークの問題を示しています。パフォーマンスイベントは、以下のとおり更に分類されます。

- Coverage イベント
- Configuration イベント
- Bandwidth イベント
- Interference イベント

システムイベントは、システムの状態を示しています。システムイベントは、以下のとおり更に分類されます。

- Troubleshooting イベント
- Sensor イベント
- Server イベント

セキュリティ、パフォーマンス、およびシステムイベントのサブカテゴリのそれぞれで複数のイベントがあります。

一部のイベントは、発生時にコンソールに表示されます。ユーザーや管理者は、特定のイベントが発生した際に電子メールで通知を受け取ることができます。**コンフィグレーション** ページを使用して管理コンソール(Management Console)で発生するイベントに対しての設定を行います。

セキュリティ、**パフォーマンス**、**システム** タブのいずれかで、個々のイベントに対して設定を構成するために、以下のすべてもしくはいずれかを行います。

- **イベント** ページに表示したいイベントに対応する**表示** のチェックボックスを選択します。
- **コンフィグレーション>イベント>電子メール受信者**で構成されたユーザーに電子メール通知を送信するには、対象のイベントの **Email** のチェックボックスを選択します。
- SNMP、Syslog などの外部エージェントに通知を送信するには、対象のイベントに対応する **通知** のチェックボックスを選択します。
- WLAN が脆弱になるイベントに対応する **脆弱性** のチェックボックスを選択します。これらのイベントのいずれかが発生した場合、**ダッシュボード** の**セキュリティステータス** ウィジェットには**脆弱** としてステータスが表示されます。
- 各イベントの深刻度に基づいて、**高**, **中**、 または **低** を選択します。

ロケーションのイベント生成をアクティベイト

コンフィグレーション>イベント>有効化 を使用して、選択したロケーションのイベント生成をアクティベイトします。
有効化スイッチ は、選択されたロケーションに対してハイレベルな管理の設定を定義します。これは、任意の競合するポリシーよりも優先されます。

<選択したロケーション> の**ロケーションのイベント生成を有効化** チェックボックスを選択しない限り、イベントは生成されません。

下図は、イベント生成のアクティベーションを表しています。

イベント生成をアクティベイト

ご注意： このポリシーは親から継承できませんー ロケーションに固有のものです。

<選択したロケーション> の**ロケーションのイベント生成を有効化** チェックボックスを選択する前に、運用が安定し完全に設定が完了していることをお勧めします。

ページに加えた変更を保存するには**保存** をクリックします。 ページ上で保存されていない変更を取り消すには、**キャンセル** をクリックします。 ページの各項目をデフォルト値に戻すには、**デフォルト値に戻す**をクリックします。

電子メール受信者の設定

選択されたロケーションで特定のイベントの発生時に通知する必要があるユーザーのメールアドレスを指定します。**コンフィグレーション>イベント>電子メール受信者** で、イベントが送信される e-mail を設定します。

システムで利用可能な電子メールアドレスを使用するか、もしくは新たに電子メールアドレスを追加することができます。カンマまたはスペースを使用して、すべての電子メールアドレスを区切るか、**Tab** または **Enter** を押してください。 ページに加えた変更を保存するには、**保存**をクリックします。ページ上で保存されていない変更を取り消すには、**キャンセル** をクリックします。ページの各項目のデフォルト値を復元するには **デフォルト値に戻す**をクリックします。

デバイスとサーバー間の通信設定

管理デバイス(Management Device)と管理コンソール(Management Console)サーバー間の通信に使用する通信キーを設定またはリセットするには、 **コンフィグレーション>システム設定>高度な設定>デバイスコミュニケーションキー** で行います。 また、コミュニケーションキーは管理デバイス(Management Device)とサーバー間の通信を暗号化するために使用されます。 キーまたはパスフレーズを使用して通信を行うことができます。

デバイスとサーバー間通信にキーを使用

管理デバイス(Management Device)と管理コンソールサーバーの間の通信のキーを 16 進数で直接設定することができます。 16 進数での作業に慣れている場合は、このオプションを選択します。

デバイスとサーバー間の通信のキーを 16 進数で設定するには、次の手順を実行します。
1. **コンフィグレーション>システム設定>高度な設定>デバイスコミュニケーションキー** に移動します。
2. 通信にキーを使用するには **キー** を選択します。
3. **キーを入力** に 32 桁の 16 進数を入力します。
4. **キーを確認** に再度同じキーを入力します。
5. 変更を保存するには、**設定** をクリックします。

デバイスとサーバー間通信にパスフレーズを使用

管理デバイス(Management Device)と管理コンソールサーバーの間の通信に英数字のパスフレーズを設定することができます。 16 進数での作業に慣れていない場合は、このオプションを選択します。

デバイスとサーバー間の通信の英数字のパスフレーズを設定するには、次の手順を実行します。
1. **コンフィグレーション>システム設定>高度な設定>デバイスコミュニケーションキー** に移動します。
2. 通信にパスフレーズを使用するには **パスフレーズ** を選択します。
3. **パスフレーズを入力** に英数字のパスフレーズを入力します。
4. **パスフレーズを確認** に再度同じパスフレーズを入力します。
5. 変更を保存するには、**設定** をクリックします。

コミュニケーションキーをリセット

コミュニケーションキーをリセットするには、**デフォルト値に戻す** をクリックします。

ライセンスの詳細表示/アップグレード

※ソフトウェアバージョン 1.3.07 以降には、本ライセンスに関するページはありません。

コンフィグレーション>システム設定>ライセンス ページでは、ライセンスに関しての情報（サーバー上で有効なライセンス機能の一覧）を表示します。

新しいライセンスを使用して機能を有効または無効にするには現在のバージョンをアップグレードすることができます。

ライセンスをアップグレードするには、次の手順を実行します。
1. **コンフィグレーション>システム設定>ライセンス**へ移動します。
2. **ライセンスの変更**下で、**ファイルを選択** をクリックして新しいライセンスファイルのパスを選択します。
3. 新しいライセンスを適用するには、**ライセンスの適用**をクリックします。 ライセンスを適用するには、ログアウトしてコンソールにログオンします。

現在のライセンス情報 には、現在適用されているライセンスにて 管理コンソール(Management Console)で利用可能な機能が表示されます。 次の表は、**現在のライセンス情報**でライセンスページに表示されるフィールドを説明しています。

フィールド	説明
有効期限	管理コンソール(Management Console)のライセンス有効期限。
管理デバイス (Management Device) 最大許容数	現在のライセンスで許可される管理デバイス(Management Device)の最大数。
AP への 許容コンバージョン	現在のライセンスでアクセスポイントとしての機能に変換することが許可されている管理デバイス(Management Device)の最大数。
レポート	ライセンスでレポート機能が使用できるかどうか。
パフォーマンス監視	ライセンスでパフォーマンス監視機能が利用できるかどうか。
防御	ライセンスで防御機能が利用できるかどうか。
アナリティクス	ライセンスでアナリティクス機能が利用できるかどうか。
フォレンジック	ライセンスでフォレンジック機能が利用できるかどうか。

レポートのルック＆フィールの管理

コンフィグレーション>システム設定>高度な設定>レポートのルック＆フィール を使用して、 レポートの外観と雰囲気を変更することができます。

レポートは、さまざまなセクション（ヘッダーテキスト、レポートの概要と詳細セクションなど）に分かれています。

これらのコンポーネントを変更することができます。

レポート内の各セクションで表示されるテキストを変更することができます。

送信元と送信先のサーバーが同じサーバークラスタに属している場合、あるサーバーから別のサーバーに「レポートのルック＆フィール」の設定をコピーすることが可能です。

レポートヘッダーテキストを変更

レポートのヘッダーテキストの外観、タイトルテキスト、レポート生成情報、説明テキストを変更することができます。

レポートヘッダーテキストの外観を変更するには、次の手順を実行します。

1. **コンフィグレーション>システム設定>高度な設定>レポートのルック＆フィール**へ移動します。
2. レポートのルック＆フィールの変更をする場合は、**カスタムのルック＆フィールを使用** のチェックボックスにチェックを入れます。
3. 左詰めのヘッダーテキストを変更するには、フィールドに新しい値を入力します。
4. 右詰めのヘッダーテキストを変更するには、フィールドに新しい値を入力します。
5. タイトルテキストを変更するには、フィールドに新しい値を入力します。
6. レポート内にレポート生成情報を表示するには、**レポート生成の情報を表示** のチェックボックスにチェックを入れます。
7. レポート内にレポートの説明を表示するには、**レポートの説明テキストを表示** のチェックボックスにチェックを入れます。
8. 変更を保存するには、**保存** をクリックします。

概要テーブルを変更

概要テーブルのテキストの外観を変更するには、次の手順を実行します。

1. **コンフィグレーション>システム設定>高度な設定>レポートのルック＆フィール**へ移動します。
2. レポートのルック＆フィールの変更をする場合は、**カスタムのルック＆フィールを使用** のチェックボックスにチェックを入れます。
3. レポートに概要情報を表示するには、**レポートの概要を表示** のチェックボックスにチェックを入れます。
4. レポート内の **レポート概要テキスト** を変更するには、フィールドに新しい値を入力します。
5. レポートに結果なしのセクションを含めるには、**概要テーブル** で **0 の結果でセクションを含む** のチェックボックスにチェックを入れます。
6. レポートにレポート概要テーブルを表示するには、**概要テーブルの列ヘッダーの定義** にある**レポート概要テーブルを表示**のチェックボックスにチェックを入れます。
7. レポートにセクション名を表示するには、**概要テーブルの列ヘッダーの定義** にある**セクション名を表示**のチェックボックスにチェックを入れます。 レポートのセクション名のテキストの代わりに異なるテキストを表示するには、**セクション名** に変更されるテキストを入力します。
8. レポートにセクションの説明を表示するには、**概要テーブルの列ヘッダーの定義** にある**セクションの説明を表示**のチェックボックスにチェックを入れます。 レポートのセクション説明のテキストの代わりに異なるテキストを表示するには、**セクション説明** に変更されるテキストを入力します。
9. レポートにセクションクエリタイプを表示するには、**概要テーブルの列ヘッダーの定義** にある**クエリタイプ**のチェックボックスにチェックを入れます。 レポートのクエリタイプのテキストの代わりに異なるテキストを表示するには、**セクションクエリの種類** に変更されるテキストを入力します。
10. 概要テーブルの列ヘッダーの定義 にある**結果カウント**のチェックボックスにチェックを入れます。 レポートの結果カウントのテキストの代わりに異なるテキストを表示するには、**発生数** に変更されるテキストを入力します。
11. レポートにハイパーリンクへのジャンプを表示するには、 **概要テーブルの列ヘッダーの定義** にある **Jump to** のチェックボックスにチェックを入れます。 レポートの Jump to のテキストの代わりに異なるテキストを表示するには、**ジャンプする** に変更されるテキストを入力します。
12. レポートに円グラフや棒グラフの形式でレポートデータを表示するには、**概要チャート** の適切なオプションを選択します。 レポートに任意のグラフを表示したくない場合は、**概要チャート**の**グラフを表示しない**を選択します。
13. 変更を保存するには、**保存** をクリックします。

セクション結果を変更

セクション結果テキストの外観を変更するには、次の手順を実行します。

1. **コンフィグレーション>システム設定>高度な設定>レポートのルック＆フィール**へ移動します。
2. レポートのルック＆フィールの変更をする場合は、**カスタムのルック＆フィールを使用** のチェックボックスにチェックを入れます。
3. レポート内のセクション名タイトルのテキストを変更するには、フィールドに新しい値を入力します。
4. レポートにセクションの説明テキストを表示するには、セクションの説明テキストを表示のチェックボックスにチェックを入れます。
5. レポートにセクションクエリを表示するには、セクションクエリを表示のチェックボックスにチェックを入れます。
6. 変更を保存するには、**保存** をクリックします。

レポートのルック＆フィールの設定をデフォルト値に戻す

ルック＆フィールの設定をデフォルト値に戻すことで、変更は無効になります。

レポートのルック＆フィールの設定をデフォルトに戻すには、次の手順を実行します。
1. **コンフィグレーション>システム設定>高度な設定>レポートのルック＆フィール**へ移動します。
2. **デフォルト値に戻す**をクリックします。
3. 変更を保存するには、**保存** をクリックします。

レポートのルック＆フィールの設定を他のサーバーへコピー

両方のサーバーが同じサーバークラスタの一部である場合は、片方のサーバーから別のサーバーへレポートのルック＆フィールの設定をコピーすることができます。 子サーバーから子サーバー、親サーバーから子サーバー、または子サーバーから親サーバーへルック＆フィールの設定をコピーすることができます。 サーバーから別のサーバーへポリシーをコピーするにはスーパーユーザーまたは管理者である必要があります。

レポートのルック＆フィールの設定をコピーするには、次の手順を実行します。
1. 親サーバー上で、**コンフィグレーション>システム設定>高度な設定>レポートのルック＆フィール**へ移動します。
2. **ポリシーをコピー**をクリックします。 **ポリシーをコピー**ダイアログボックスが表示されます。
3. ルック＆フィール設定のコピー元となるサーバーを選択します。
4. ルック＆フィール設定のコピー先となるサーバーを選択します。
5. ルック＆フィール設定をコピーするには、**OK** をクリックします。

RF プロパゲーション設定を構成

コンフィグレーション>システム設定>高度な設定>RF プロパゲーション を使用して、 ロケーショントラッキングのために用いられる、AP、クライアント、センサーのデフォルトのアンテナゲイン値を設定します。

デフォルトの RF プロパゲーション設定には、次のオプションがあります。

- デフォルトのアンテナゲイン値： デフォルトのセンサー、AP そしてクライアントのアンテナのゲイン値を指定します。 アンテナの出力、（アンテナを用いて信号を受信（または送信）するために電力の利得として定義された） 信号を送信または受信するために使用されるアンテナの特性です。
- Sensor Antenna Gain (dB)： センサーに取り付けたアンテナのゲインを設定します。(デフォルト： 2.3 dB)
- AP Antenna Gain (dB): AP に取り付けたアンテナのゲインを設定します。(デフォルト： 2.3 dB)
- Client Antenna Gain (dB): クライアントに取り付けたアンテナのゲインを設定します。(デフォルト： 0 dB)

- トランスミッタロス： ご使用の環境に適したトランスミッタ信号損失値を選択します。
- ご使用の環境が、金属やコンクリートの壁がある場合は、より高い信号値を選択します。
- ご使用の環境が、信号がそれほど障害物なく広がることができる大きな無線 LAN の場合は、より低い信号値を選択します。

  デバイスが送信した場合、一部の電力の損失はアンテナコネクタ、電磁気、および環境要因で発生します。 この損失は違う周波数帯域で異なる場合があります。また各帯域内のおおよその損失を指定することができます。
  ・IEEE802.11a トランスミッタのソースでのロス (dB): (デフォルト： 10 dB)
  ・IEEE802.11b/g トランスミッタのソースでのロス (dB): (デフォルト： 10 dB)

- 信号減衰値： 信号伝搬は環境に大きく依存します。障害物は、その範囲を制限し、信号伝搬妨げる可能性があります。正確に環境のすべての種類の信号伝搬をモデル化することは非常に困難ですが、次の 4 つを調整することにより、多少、環境ごとの信号伝搬を特徴づけることが可能です。

- 信号減衰値： 信号伝搬は環境に大きく依存します。障害物は、その範囲を制限し、信号伝搬を妨げる可能性があります。正確に環境のすべての種類の信号伝搬をモデル化することは非常に困難ですが、次の 4 つを調整することにより、多少、環境ごとの信号伝搬を特徴づけることが可能です。

- Minimum/Maximum Signal Decay Constants は減衰指数の範囲を指定します（つまり、信号の距離による減衰指数）。 Signal Decay Slope (Beta) と Signal Decay Inflection (Alpha) は、 最小値と最大値からどのように減衰指数を変更するかを制御します。

RF プロパゲーションを構成するには、次の手順を実行します。
1. **コンフィグレーション>システム設定>高度な設定>RF プロパゲーション**へ移動します。
2. デフォルトのセンサー、AP、およびクライアントのアンテナゲイン値を指定します。

フィールド	説明
Sensor Antenna Gain (dB)	センサーに割り当てるアンテナのゲイン
AP Antenna Gain (dB)	AP に割り当てるアンテナのゲイン
Client Antenna Gain (dB)	クライアントに割り当てるアンテナのゲイン

3. ご使用の環境でのトランスミッタ信号ロスの値を選択します。
4. IEEE802.11a トランスミッタのソースでのロス(dB)を指定します。
5. IEEE802.11b/g トランスミッタのソースでのロス(dB)を指定します。
6. GIF、JPEG、空白レイアウトのノードの場合には、次を指定します（Minimum Signal Decay Constant, Maximum Signal Decay Constant, Signal Decay Slope(Beta), Signal Decay Slope(Alpha)）。
7. 変更を保存するには、**保存**をクリックします。

RF プロパゲーションをデフォルト値に戻す

RF プロパゲーションの設定を復元するには、次の手順を実行します。
1. **コンフィグレーション>システム設定>高度な設定>RF プロパゲーション**へ移動します。
2. **デフォルト値に戻す**をクリックします。 フィールドには、各デフォルト値が入ります。
3. 変更を保存するには、**保存**をクリックします。

RF プロパゲーション設定を他のサーバーへコピー

両方のサーバーが同じサーバークラスタの一部である場合は、片方のサーバーから別のサーバーへ RF プロパゲーション設定をコピーすることができます。 子サーバーから子サーバー、親サーバーから子サーバー、または子サーバーから親サーバーへ RF プロパゲーション設定をコピーすることができます。 サーバーから別のサーバーへポリシーをコピーするにはスーパーユーザーまたは管理者である必要があります。

RF プロパゲーション設定をコピーするには、次の手順を実行します。
1. 親サーバー上で、**コンフィグレーション>システム設定>高度な設定>RF プロパゲーション**へ移動します。
2. **ポリシーをコピー**をクリックします。 ポリシーをコピーダイアログボックスが表示されます。
3. RF プロパゲーション設定のコピー元となるサーバーを選択します。
4. RF プロパゲーション設定のコピー先となるサーバーを選択します。
5. RF プロパゲーション設定をコピーするには、**OK** をクリックします。

ライブ RF ビュー設定の構成

コンフィグレーション>システム設定>高度な設定>ライブ RF ビュー設定 で、ライブ RF ビューで使用されるパラメータを定義します。 これらのパラメータは、各環境において固有のものです。 パラメータを調整することで、より正確なビューを見ることができます。

侵入検知と防御領域では、システムがセンサーのカバレッジ表示で侵入検出と防御領域を示す dBm 値を指定します。

検出の範囲は、センサーが確実に無線アクティビティを検出することができる領域です。 **侵入検知の表示スレッショルド(閾値)**は、この範囲のスレッショルド(閾値)を決定します。

防御の範囲は、センサーが未許可の無線アクティビティを防御することができる領域です。 **侵入防御の表示スレッショルド(閾値)**は、この範囲のスレッショルド(閾値)を決定します。

検知と防御範囲の両方は、RF プロパゲーションセクションのパラメータの影響を受けます。

ご注意： 防御の信頼性は、**コンフィグレーション>WIPS>侵入防御** ページで選択される侵入防御レベルにも依存します。

ライブ RF ビュー設定のを構成するには、次の手順を実行します。
1. **コンフィグレーション>システム設定>高度な設定>ライブ RF ビュー設定**へ移動します。
2. **侵入検知の表示スレッショルド(閾値)**を指定します。
3. **侵入防御の表示スレッショルド(閾値)**を指定します。
4. 変更を保存するには、**保存**をクリックします。

ライブ RF ビュー設定をデフォルト値に戻す

侵入検知の表示スレッショルド(閾値)のデフォルト値は-85dBm です。 侵入防御の表示スレッショルド(閾値)のデフォルト値は-75 dBm です。

ライブ RF ビューの設定をデフォルトに戻すには、次の手順を実行します。
1. **コンフィグレーション>システム設定>高度な設定>ライブ RF ビュー設定**へ移動します。
2. **デフォルト値に戻す**をクリックします。
3. 変更を保存するには、**保存** をクリックします。

ライブ RF ビューの設定を他のサーバーへコピー

両方のサーバーが同じサーバークラスタの一部である場合は、片方のサーバーから別のサーバーへライブ RF ビューの設定をコピーすることができます。 子サーバーから子サーバー、親サーバーから子サーバー、または子サーバーから親サーバーへライブ RF ビューの設定をコピーすることができます。 サーバーから別のサーバーへポリシーをコピーするにはスーパーユーザーまたは管理者である必要があります。

ライブ RF ビューの設定をコピーするには、次の手順を実行します。
1. 親サーバー上で、**コンフィグレーション>システム設定>高度な設定>ライブ RF ビュー設定**へ移動します。
2. **ポリシーをコピー**をクリックします。 **ポリシーをコピー**ダイアログボックスが表示されます。
3. ライブ RF ビュー設定のコピー元となるサーバーを選択します。
4. ライブ RF ビュー設定のコピー先となるサーバーを選択します。
5. ライブ RF ビュー設定をコピーするには、**OK** をクリックします。

ロケーショントラッキングを設定

コンフィグレーション>システム設定>高度な設定>ロケーショントラッキング コンフィグレーション を使用して、 特定のデバイスのロケーションを追跡することが可能です。 システムは、ロケーショントラッキングを行うためには、少なくとも 3 つのセンサーを必要とします。 ロケーショントラッキング画面では、ロケーショントラッキングを制御するパラメータを定義できます。

デフォルトのロケーショントラッキングパラメータには、次のオプションがあります。

- **ロケーショントラッキングに使用する監視デバイスの最大数:** ロケーショントラッキングのために使用されるセンサーの最大数を選択します。 センサーはデバイスのロケーションを追跡し、システムは最大値のセンサーを使用します。 より高い値は、より良好な結果を得る可能性があります。
  (最小： 3; 最大： 10; デフォルト： 4)

- **AP のデフォルト送信出力** (mW)： ロケーショントラッキングは、 検出されている AP の送信出力を入力として必要とします。送信出力が不明の場合、ここで設定したデフォルト値が使用されます。
  (最小： 1 mW〈=0dBm〉; 最大： 100 mW〈=20dBm〉; デフォルト： 10 mW〈=10 dBm〉)

- **クライアントのデフォルト送信出力** (mW)： ロケーショントラッキングは、 検出されているクライアントの送信出力を入力として必要とします。 送信出力が不明な場合は、ここで設定したデフォルト値が使用されます。
  (最小： 1 mW〈=0dBm〉; 最大： 100 mW〈=20dBm〉; デフォルト： 10 mW〈=10 dBm〉)

- **信号強度モニタリングデバイス**：ロケーショントラッキングは、モニタリングデバイスの信号強度に基づいています。 この値は、RF 環境での微妙な変化により実際の値からずれる可能性があります。 AP（管理デバイス(Management Device)）と管理デバイス(Management Device)やロケーショントラッキングをコントロールために使用される AP を指定することができます。 システムのアプリケーション・プログラミング・インタフェース（API）を使用して、AP は信号強度のソースとしてレポートされることができます。 これらの AP からの情報は、ロケーショントラッキングのために使用することが可能です。

ロケーショントラッキングの設定をデフォルト値に戻す

ロケーショントラッキング設定のデフォルト値は、以下のとおりです。

ロケーショントラッキングに使用する監視デバイスの最大数	4
AP のデフォルト送信出力	30
クライアントのデフォルト送信出力	10
信号強度モニタリングデバイス	管理デバイス(Management Device)と(または)AP

ロケーショントラッキングの設定をデフォルトに復元するには、次の手順を実行します。

1. **コンフィグレーション>システム設定>高度な設定>ロケーショントラッキング コンフィグレーション**へ移動します。
2. ページ上のロケーショントラッキングの設定フィールドをデフォルト値に復元するためには、**デフォルト値に戻す**をクリックします。
3. 変更を保存するには、**保存** をクリックします。

ロケーショントラッキングの設定を他のサーバーへコピー

両方のサーバーが同じサーバークラスタの一部である場合は、片方のサーバーから別のサーバーへロケーショントラッキングの設定をコピーすることができます。 子サーバーから子サーバー、親サーバーから子サーバー、または子サーバーから親サーバーへロケーショントラッキングの設定をコピーすることができます。 サーバーから別のサーバーへポリシーをコピーするにはスーパーユーザーまたは管理者である必要があります。

ロケーショントラッキングの設定をコピーするには、次の手順を実行します。

1. 親サーバー上で、**コンフィグレーション>システム設定>高度な設定>ロケーショントラッキングコンフィグレーション**へ移動します。
2. **ポリシーをコピー**をクリックします。 **ポリシーをコピー**ダイアログボックスが表示されます。
3. ロケーショントラッキング設定のコピー元となるサーバーを選択します。
4. ロケーショントラッキング設定のコピー先となるサーバーを選択します。
5. ロケーショントラッキング設定をコピーするには、**OK** をクリックします。

自動ロケーションタギングの管理

コンフィグレーション>システム>高度な設定>自動ロケーションタギング ページでは、 管理コンソール(Management Console)によって発見されるデバイスと管理コンソール(Management Console)によって生成されるイベントの自動タグ付けに関する設定を構成することが可能です。

デバイスまたはイベントに設定されているロケーションタグは、そのイベントまたはデバイスのロケーションを識別するのに役立ちます。 管理コンソール(Management Console)は自動的にそれらが検出されたロケーションにデバイスおよびイベントをタグ付けします。

自動ロケーションタグ付けの設定には、次のオプションが含まれています。

- **デバイス**： デバイスの最初のロケーションに基づいて、 AP とクライアントは、発見のあと直ちに自動タグ付けされます。 システムがアクセスポイントまたはクライアントの最初のロケーションタグを計算する方法を選択することができます。 手動でタグ付けされている場合、システムは AP またはクライアントの自動タグ付けをすることはありません。 デバイスの自動ロケーションタグ付けを有効にするには、 デバイスを削除しシステムがそれを再発見する必要があります。 手動でセンサーをタグ付けする必要があります。次のいずれかを行うことができます。
  - ○ デバイスの RSSI 値の最も高い値を認知するセンサーのロケーションタグを選択します。
  - ○ デバイスの RSSI 値の最も高い値を認知する選択されたセンサーの数のロケーションタグを選択します。
    (最小： 2; 最大： 10; デフォルト： 2)

より高い RSSI をレポートするセンサーと値を比較したあとに、より低い RSSI を認知するセンサーを破棄することもできます。
(最小： 20 dB; 最大： 40 dB; ：デフォルト: 30 dB)

- **イベント**:システムは、イベントに関与するデバイスのロケーションに基づくイベントをタグ付けします。 システムは、プライマリデバイス（各イベントの AP、クライアント、センサー）をはじめに識別します。 システムは、イベントと関連したプライマリデバイスのためにタグに基づいてイベントのロケーションをタグ付けします。

ご注意： システムは、イベントに 2 回以上タグを付けません。 ロケーションの変更アイコンをクリックして、イベントページで手動にてイベントのロケーションにタグ付けすることができます。

自動ロケーションタギングの設定をデフォルト値に戻す

自動ロケーションタギング設定のデフォルト値は、以下のとおりです。

・　デバイスに対して最も大きい RSSI 値を見ているトップ 2 の管理デバイス(Management Device)を含むロケーションタグを選択する。
・　デバイスに対して最も大きい RSSI 値を見ている管理デバイス(Management Device)より 30dB より低い RSSI 値を見ている管理デバイス(Management Device)を破棄する。

自動ロケーションタギングの設定をデフォルトに復元するには、次の手順を実行します。

1. **コンフィグレーション>システム>高度な設定>自動ロケーションタギング**へ移動します。
2. ページ上の自動ロケーションタギングの設定フィールドをデフォルト値に復元するためには、**デフォルト値に戻す**をクリックします。
3. 変更を保存するには、**保存** をクリックします。

自動ロケーションタギングの設定を他のサーバーへコピー

両方のサーバーが同じサーバークラスタの一部である場合は、片方のサーバーから別のサーバーへ自動ロケーションタギングの設定をコピーすることができます。 子サーバーから子サーバー、親サーバーから子サーバー、または子サーバーから親サーバーへ自動ロケーションタギングの設定をコピーすることができます。 サーバーから別のサーバーへポリシーをコピーするにはスーパーユーザーまたは管理者である必要があります。

自動ロケーションタギングの設定をコピーするには、次の手順を実行します。

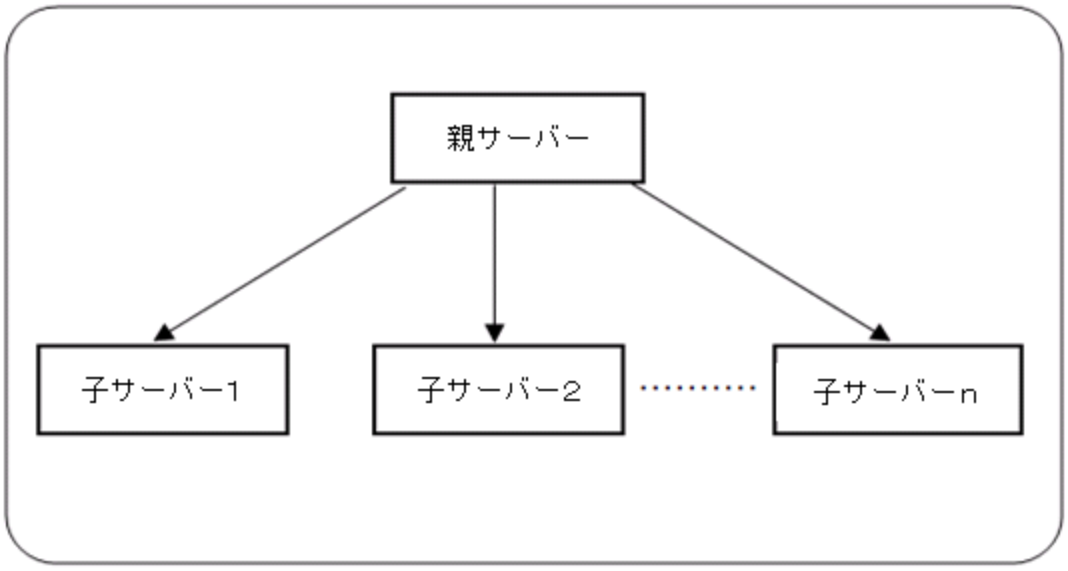
1. 親サーバー上で、**コンフィグレーション>システム>高度な設定>自動ロケーションタギング**へ移動します。
2. **ポリシーをコピー**をクリックします。 **ポリシーをコピー**ダイアログボックスが表示されます。
3. 自動ロケーションタギング設定のコピー元となるサーバーを選択します。
4. 自動ロケーションタギング設定のコピー先となるサーバーを選択します。
5. 自動ロケーションタギング設定をコピーするには、**OK** をクリックします。

サーバークラスタ

サーバークラスタの設定と管理

サーバークラスタは、グループ化された 2 つ以上の管理コンソールサーバーから構成されます。 これらのサーバーのいずれかが管理サーバーになり、1 つ以上の管理コンソールサーバーを管理します。 このように、複数のサーバーを 1 つのサーバークラスタで単一のサーバーコンソールにより管理することが可能です。

管理するサーバーは**親サーバー**と呼ばれ、親サーバーから管理されるサーバーは**子サーバー**と呼ばれます。 親サーバーはクラスタ内の複数の子サーバーから収集したデータを取り出して、親サーバーのデータとともに管理コンソール(Management Console)上に表示します。



サーバークラスタ

サーバークラスタの利点

以下は、サーバークラスタの利点です。
- **複数のサーバーを管理するための別の製品が不要：**サーバークラスタは、管理コンソール(Management Console)を介してアクセスできます。 各種のテンプレートやポリシーは、親サーバーのロケーションツリーから子サーバーにプッシュすることができます。
- **管理デバイス(Management Device)と接続 ：**管理デバイス(Management Device)は、サーバークラスタ内の親サーバーとして機能する管理デバイス(Management Device)サーバーに接続することができます。
- **すべての管理デバイス(Management Device)機能が利用可能：** サーバーがサーバークラスタの一部であっても、すべての管理デバイス(Management Device)の機能が利用できます。
- **ポリシーの自動同期：** ポリシーが親サーバーから同期される場合、子サーバーが利用できない場合でも手動で子サーバー上のポリシーを同期する必要はありません。 子サーバーが次回起動したときに自動的に行われます。
- **サーバークラスタ内のあるサーバーから別のサーバーにポリシーを複製：** サーバークラスタ内のあるサーバーから別のサーバーにほとんどのポリシーを複製することが可能です。 これはポリシーが親サーバーから子サーバーまたは子サーバーから親サーバーへコピーされるかどうかに関係しません。
- **ダッシュボードウィジェット内のデータの集約：**サーバークラスタ内のすべてのアクティブなサーバーから集約されたデータは、管理コンソール(Management Console)上のダッシュボードウィジェットで大部分が見ることができます。

サーバークラスタの生成と管理

サーバークラスタの生成とサーバークラスタ内のサーバーの管理は、サーバーのコマンドラインインタフェース（CLI）を使用して行われます。 集約されたサーバークラスタデータの表示および親サーバーから子サーバー上のポリシー管理は、親サーバーの管理コンソール(Management Console)を介して行われます。

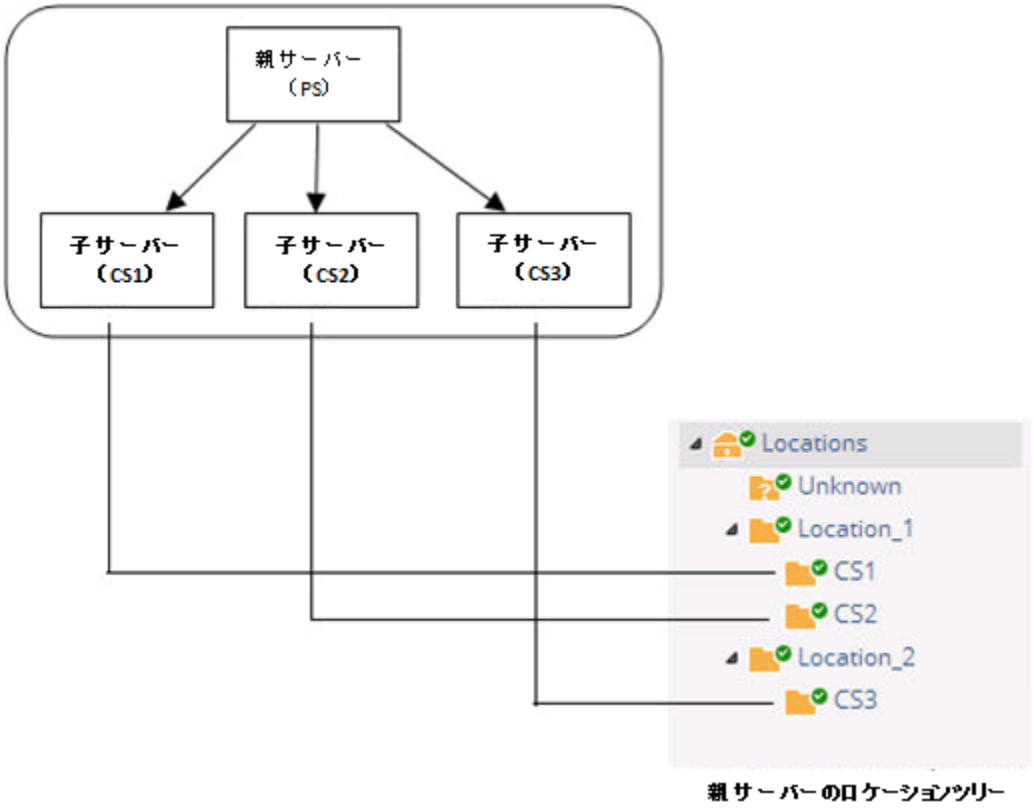
以下は、サーバークラスタを作成するための必要条件です。
- クラスタを形成する管理デバイス(Management Device)サーバーは、同じバージョンおよびビルドのソフトウェアがインストールされている必要があります。
- サーバークラスタに追加するすべての子サーバーに有効なライセンスが適用されている必要があります。
  （ソフトウェアバージョン 1.3.07 以降を使用の場合、ライセンスを使用しません。）
- 子サーバーは他のサーバークラスタの一部であってはなりません。
- ファイアウォールがネットワーク上でアクティブになっている場合、TCP ポート 22 と UDP ポート 1194 はクラスタ形成と親-子のコミュニケーションのためにファイアウォール上で開いている必要があります。 TCP ポート 22 は子サーバーへの接続用で、UDP ポート 1194 は親サーバーへの接続用です。

サーバーのコマンドラインインタフェースから 5 つのクラスタ関連の操作を行うことができます。それらは以下のとおりです。
1. サーバークラスタをセットアップし、サーバークラスタへ親サーバーを割り当てます。
2. サーバークラスタに子サーバーを追加します。
3. サーバークラスタから子サーバーを削除、または取り除きます。
4. すべてのサーバークラスタを削除します。
5. クラスタ内のサーバーの状態を確認、またはサーバーがクラスタの一部であるかどうかを確認します。

サーバークラスタ内のサーバーは、サーバークラスタのメンバーとなるときに ID が割り当てられます。 親サーバーは、クラスタ内の ID として 1 が割り当てられます。 子サーバーが追加されると、それらは順次インクリメントした ID が割り当てられます。 最初に追加された子サーバーに ID2 が割り当てられ、次は ID3 が割り当てられます。

クラスタを作成したら、UI 上で集約されたサーバーのデータを表示することや、子サーバーに親サーバーからポリシーをプッシュすることができるように、親サーバーのロケーションツリー上に子サーバーをマウントする必要があります。

下図は、サーバークラスタ内の子サーバーを持つロケーションツリーのマッピングを示します。



親サーバーのロケーションツリー

サーバークラスタの制限

以下は、サーバークラスタの制限です。

- サーバー（親サーバーまたは子サーバー）は、任意の時点で 1 つだけのクラスタのメンバーになることができます。
- 子サーバーは、クラスタ内の他のサーバーの親になることはできません。

サーバークラスタ関連コマンド

サーバーのコマンドラインインタフェースを介して 1 つの親と複数の子サーバーからなるクラスタを設定することができます。
以下はサーバークラスタの作成と管理の固有のサーバー設定ファイルシェルコマンドのサブセットです。

コマンド	説明
`cluster set`	サーバークラスタ内の親サーバーとしてサーバーを設定します。 このコマンドは、親サーバーとして設定されるサーバー上で実行する必要があります。
`cluster reset`	サーバークラスタまたはクラスタから子サーバーを削除します。 このコマンドは、親サーバーまたは子サーバー上で実行することができます。 親サーバー上で実行すると、クラスタ全体が無効になり、クラスタ内のすべてのサーバーはスタンドアロンのサーバーとして動作します。 子サーバー上で実行すると、子サーバーと親サーバーとの間の関係を無効にします。 クラスタの残りの部分はそのまま残ります。 **ご注意：** 親サーバー上でのみこのコマンドを実行することを推奨します。 サーバークラスタから子を削除する他の方法がない場合のみ、子サーバー上で実行することができます。
`cluster add child`	サーバークラスタに子を追加します。 このコマンドは、サーバークラスタ内の親サーバー上で実行する必要があります。
`cluster delete child`	サーバークラスタから子を削除また取り除きます。 このコマンドは、サーバークラスタ内の親サーバー上で実行する必要があります。
`cluster show status`	サーバークラスタの状態を表示します。 このコマンドを使用して、クラスタ内のサーバーおよび(または)クラスタ内のサーバーの状態を確認することができます。 このコマンドは、サーバークラスタにあるか否かに関係なく任意のサーバー上で実行することができます。

サーバークラスタのセットアップ

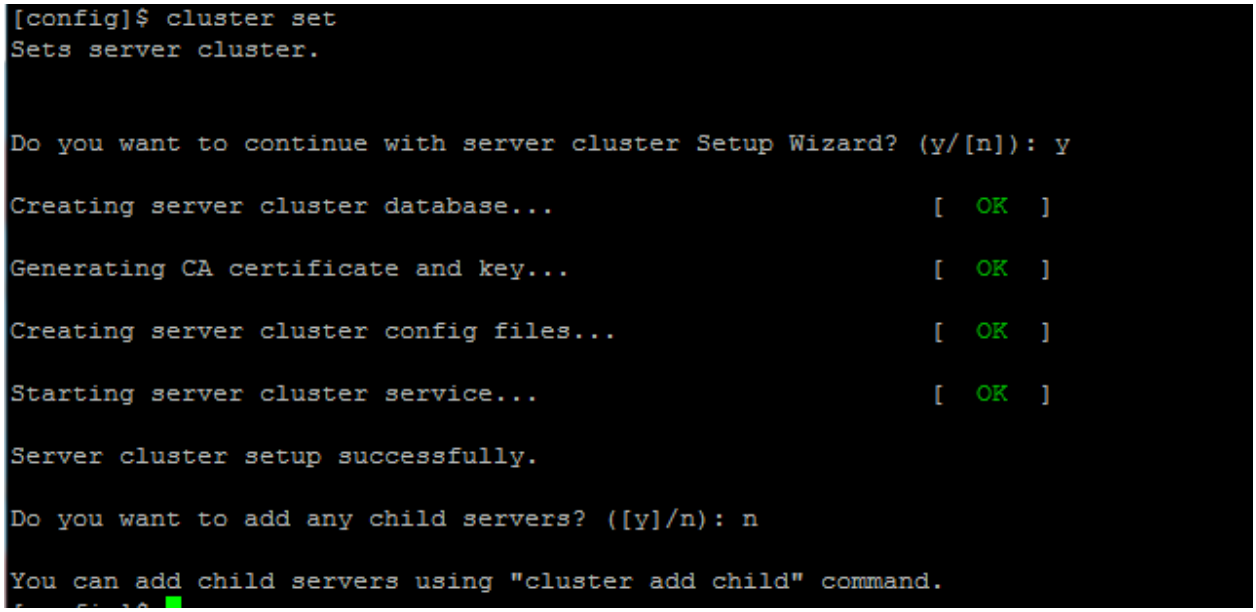
`cluster set` コマンドは、クラスタを設定するために使用されます。 このコマンドは、サーバークラスタ内の親サーバーとして割り当てられるサーバーのコマンドラインインタフェース上で実行する必要があります。

必要に応じて、サーバークラスタに子サーバーを追加するためにサーバークラスタのセットアップウィザードを実行するかを選択できます。
`cluster show status` コマンドを実行することでサーバーの状態を確認できます。

クラスタをセットアップするには、次の手順を実行します。

1. サーバークラスタ内の親サーバーとして設定するサーバーのコマンドラインインタフェースにログインします。 'config' ユーザーでサーバーにログインします。
2. コマンドラインで `cluster set` コマンドを実行します。 サーバーは、サーバークラスタ内の親サーバーとして設定されます。
3. すぐに子サーバーを追加する場合は、子サーバーを追加するプロンプトが表示されたら'y'を入力します。 子サーバーを追加するために、子サーバーの名前、IP アドレス、そして子サーバーの config ユーザー用のパスワードを入力します。 更に子サーバーを追加するには、この手順を繰り返します。

`cluster set` コマンドに関しては次のスクリーンショットを参照してください。



サーバークラスタに子サーバーを追加

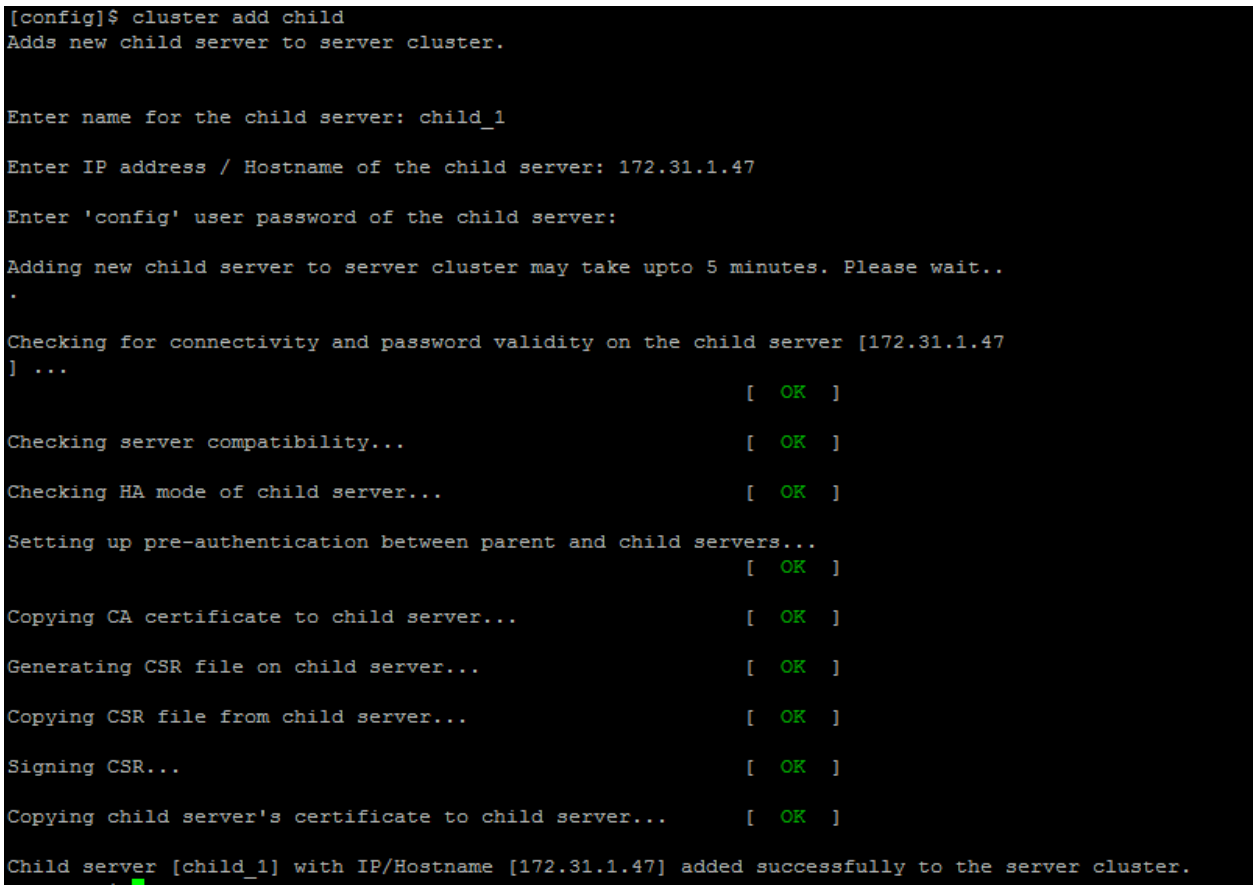
サーバークラスタに子サーバーを追加するには、2 つの方法があります。

1. `cluster set` コマンドを実行したあとに利用可能なサーバークラスタのセットアップウィザードを使用します。 これは、'サーバークラスタのセットアップ'のセクションで説明されています。
2. `cluster add child` コマンドを追加実行します。 このコマンドは、親サーバーのコマンドラインで実行する必要があります。 これは、以下で説明されます。

`cluster add child` コマンドを使用してサーバークラスタに子サーバーを追加するには、次の手順を実行します。

1. "config" ユーザーで親サーバーのコマンドラインインタフェースにログインします。
2. コマンドラインで `cluster add child` コマンドを実行します。 サーバークラスタに追加する子サーバーの名前を入力するように求められます。
3. 子サーバーの適切な名前を入力します。 子サーバーのホスト名または IP アドレスを入力するように求められます。
4. 子サーバーのホスト名または IP アドレスを入力します。 子サーバー用の"config"ユーザーのパスワードを入力するように求められます。
5. "config" ユーザーのパスワードを入力します。 入力されたすべてのデータが正しければ、指定されたホスト名/ IP アドレスを持つサーバーは、サーバークラスタ内の子サーバーとして追加されます。

`cluster add child` コマンドに関しては次のスクリーンショットを参照してください。



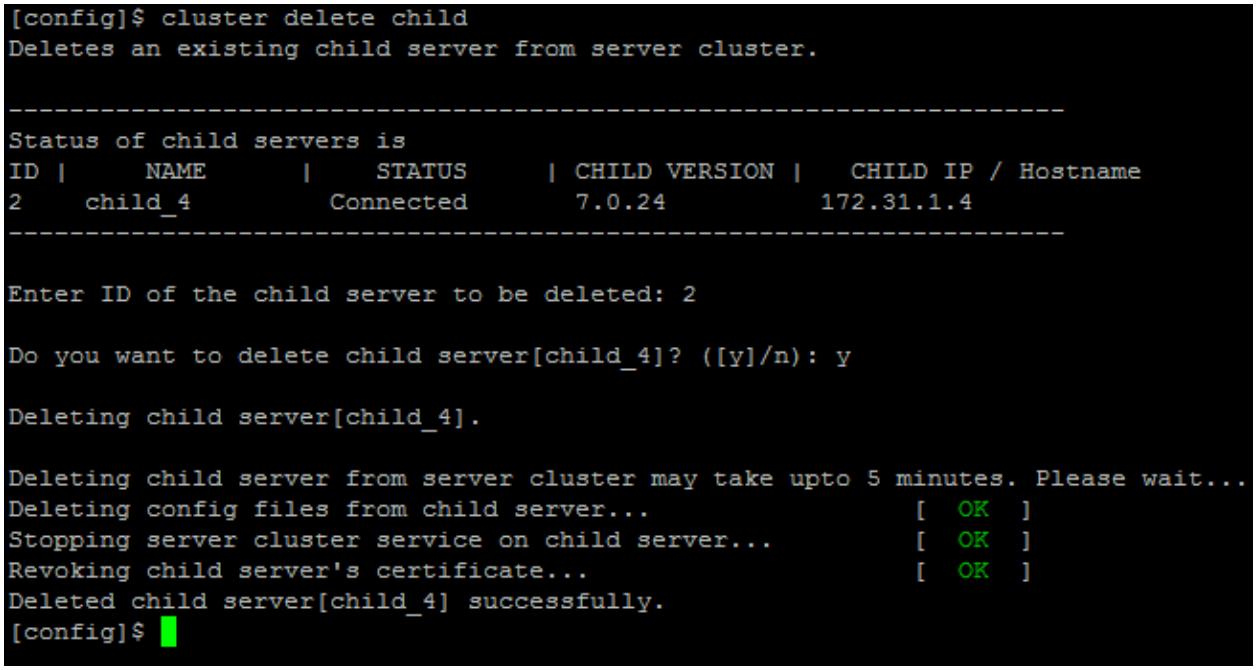
サーバークラスタから子サーバーを削除

子サーバーは、`cluster delete child` コマンドを使用して、サーバークラスタから削除することができます。 サーバークラスタから子サーバーを削除すると、親サーバーと子サーバー間のリンクが破棄されます。 サーバークラスタの残りの部分はクラスタとして機能し続けます。

サーバークラスタから子サーバーを削除するには、次の手順を実行します。

1. "config" ユーザーで親サーバーのコマンドラインインタフェースにログインします。
2. コマンドラインで `cluster delete child` コマンドを実行します。 サーバークラスタから削除する子サーバーの ID を入力するよう求められます。
3. 削除する子サーバーの ID を入力します。 サーバークラスタから子サーバーの削除を確認するメッセージが表示されます。
4. サーバークラスタから子サーバーを削除するには、y を入力します。 子サーバーはサーバークラスタから削除されます。

`cluster delete child` コマンドに関しては次のスクリーンショットを参照してください。



サーバークラスタの削除

サーバークラスタは、`cluster reset` コマンドを使用して削除することができます。 このコマンドはクラスタ全体を削除するため、親サーバーのコマンドラインで実行する必要があります。

ご注意： `cluster reset` コマンドを子サーバーのコマンドラインで実行すると、クラスタから子を削除します。 クラスタから子サーバーを削除する方法が他にない限り、このアクションは推奨されません。

サーバークラスタから子サーバーを削除するには、`cluster delete child` コマンドを使用します。

サーバークラスタを削除するには、次の手順を実行します。
1. "config" ユーザーで親サーバーのコマンドラインインタフェースにログインします。
2. コマンドラインで `cluster reset` コマンドを実行します。 クラスタのリセットを確認するメッセージが表示されます。
3. クラスタリセットまたはサーバークラスタの削除を実行するには、y を入力します。 クラスタが削除されます。

`cluster reset` コマンドに関しては次のスクリーンショットを参照してください。

```
[config]$ cluster reset
Resets server cluster.


Do you want to reset server cluster? (y/[n]):y


Server cluster reset successfully.
```

サーバークラスタに関するサーバーの状態を確認

`cluster show status` コマンドを使用して、サーバークラスタの一部であるかどうかを確認できます。 サーバーがサーバークラスタの一部である場合は、`cluster show status` コマンドを使用して、サーバーが親サーバーまたは子サーバーであるかどうかを調べることができます。
サーバークラスタ内のサーバーでなくてもこのコマンドを実行することが可能です。 つまり任意のアクティブなサーバーでこのコマンドを実行することができます。

サーバーの状態を確認するには、次の手順を実行します。
1. "config" ユーザーで親サーバーのコマンドラインインタフェースにログインします。
2. コマンドラインで `cluster show status` コマンドを実行します。 サーバーのステータスがコマンドによって返されます。

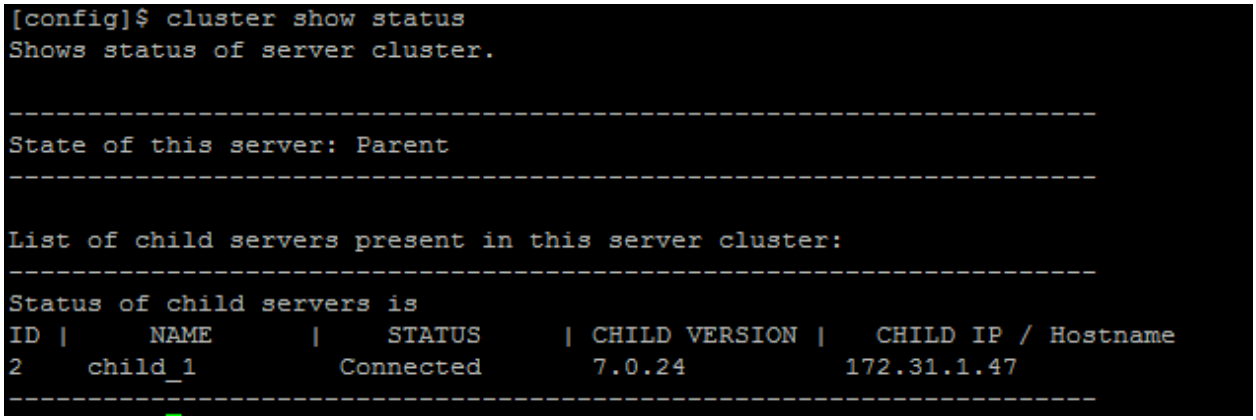
別のサーバーの状態については、以下のスクリーンショットを参照してください。

以下は、子サーバー上で実行したコマンドのスクリーンショットです。

```
[config]$ cluster show status
Shows status of server cluster.

------------------------------------------------------------------------
State of this server: Child
Parent server's IP/Hostname: 172.31.1.5
```

以下は、親サーバー上で実行したコマンドのスクリーンショットです。



子サーバーをマウントし、親サーバーの管理コンソール(Management Console)からそれらを管理する方法については、 サーバークラスタ内の親サーバーから子サーバーを管理を参照してください。

親サーバーからポリシーを継承

サーバークラスタが作成され、子サーバーがマウントポイントにマウントされるとき、子サーバーは以前にそれに適用されたポリシーを保持します。 デフォルトでは、親サーバーのポリシーを継承しません。 子サーバーに親サーバーポリシーを適用する場合は、個別のポリシーに移動し親サーバーからポリシーを継承する必要があります。

以下のポリシーは、ロケーション固有であり継承することはできません。
- 侵入防御のアクティベーション
- ロケーションのタイムゾーン
- イベントのアクティベーション
- デバイスリストのロック

しかし、子サーバーのマウントポイントでのこれらのポリシーを変更し、再帰的に適用されるこれらの変更を保存する場合は、変更内容はマウントポイントの下に存在するすべてのロケーションにプッシュされます。

親サーバーからポリシーを継承するには、次の手順を実行します。
1. 親サーバーからポリシーを継承したい子サーバー上のロケーションを選択します。
2. 継承するポリシーにナビゲートします。
3. **ポリシーの継承** のリンクをクリックします。 ポリシーを継承する確認を求めるメッセージが表示されます。
4. 確認メッセージで **Yes** をクリックします。 親サーバーのポリシーが子サーバー上の選択されたロケーションに適用されます。

サーバークラスタ内の親サーバーから子サーバーを管理

サーバークラスタはサーバーのグループです。 サーバークラスタは、親サーバーと 1 つまたは複数の子サーバーで構成されます。
サーバークラスタは、単一のサーバーを使用して複数のサーバーを管理するために作成されます。 この管理するサーバーは親サーバーと呼ばれ、親サーバーから管理されるサーバーは子サーバーと呼ばれます。 親サーバーはクラスタ内の複数の子サーバーから集約されたデータを取得し、親サーバーのデータとともに管理コンソール(Management Console)上に表示します。 親サーバーから複数の子サーバーに共通のポリシーをプッシュすることも可能です。
サーバー（親サーバーまたは子サーバー）は、任意の時点で 1 つのクラスタのみの一部にすることができます。 子サーバーは、クラスタの他のサーバーの親にすることはできません。

サーバークラスタの生成およびサーバークラスタ内のサーバーの管理は、サーバーのコマンドラインコンソールを使用して行われます。

集約されたサーバークラスタのデータ表示およびクラスタ内の親サーバーから子サーバー上のポリシー管理は管理コンソール(Management Console)を介して行われます。 管理コンソール(Management Console)を介してサーバークラスタに関連するオプションの表示そしてサーバークラスタのデータとポリシーを管理するには、スーパーユーザーである必要があります。

サーバークラスタに親サーバーを割り当てサーバークラスタに子サーバーを追加すると、親サーバーの管理コンソール(Management Console)にログインし、**コンフィグレーション>システム設定>サーバークラスタ**に移動することができます。 （それらが存在していない場合は）1 つまたは複数のロケーションを作成し、親サーバーのロケーションツリー上に子サーバーをマウントします。 ロケーションがすでに追加されている場合は、これらのロケーション上に子サーバーをマウントします。

子サーバーをマウントし同じサーバークラスタ内のあるサーバーから別のサーバーにポリシーをコピーすることができます。
サーバークラスタ内の子サーバーのリストを印刷することができます。 リスト内のサーバーを検索することができます。

親サーバーのロケーションツリー上に子サーバーをマウント

親サーバーを介して子サーバー上のポリシーを管理することや、すべてのサーバークラスタの集約されたサーバーデータを表示することができるようにするためには、親サーバーのロケーションツリー上で個々の子サーバーをマウントする必要があります。 親サーバーのロケーションツリーにマウントする前に、有効なライセンスを子サーバーに適用する必要があります。

次のような状況では、親サーバーのロケーションツリー上に子サーバーをマウントすることはできません。

- サーバークラスタ内の親サーバーがアップグレードされ、親サーバーと子サーバーのバージョンが一致しません。 バージョンの不一致を修正するには、親サーバーと子サーバー間のバージョン不一致を修正セクションを参照してください。
- 有効なライセンスが子サーバーに適用されていない、または子サーバー上のライセンスの有効期限が切れています。 ライセンスエラー状態を修正するためには、子サーバーの無効なライセンス状態を修正セクションを参照してください。

子サーバーがマウントされると、親サーバーのポリシーは自動的に子サーバーに継承されません。 子サーバーはサーバークラスタに追加される前に適用されたポリシーを使用し続けます。 子サーバー上の個々のポリシーは親サーバーから継承することができます。 詳細については、親サーバーからポリシーを継承を参照してください。

親サーバーで子サーバーをマウントするには、次の手順を実行します。

1. **コンフィグレーション>システム設定>サーバークラスタ**へ移動します。
2. 親サーバーのルートロケーションを選択します。子サーバーが表示されます。
3. 子サーバーをマウントするためには、**Not Mounted** リンクをクリックします。 **ロケーションの選択**のダイアログボックスが表示されます。
4. 子サーバーをマウントするために適切なロケーションを選択します。 ロケーションが作成されていない場合は、最初にロケーションを作成します。
5. 選択したロケーションに子サーバーをマウントするには、**保存** をクリックします。

子サーバーのマウントポイントを変更

いつでも子サーバーのマウントポイントを変更することができます。 ライセンスが子サーバーに適用されていないか、子サーバーのライセンスの有効期限が切れている場合は、子サーバーのマウントポイントを変更することはできません。

親サーバーのロケーションツリー上で子サーバーのマウントポイントを変更するには、次の手順を実行します。

1. **コンフィグレーション>システム設定>サーバークラスタ**へ移動します。
2. 親サーバーのルートロケーションを選択します。子サーバーが表示されます。
3. 子サーバーをマウントするためのマウントポイントのリンクをクリックします。
4. **マウントポイントの変更**をクリックします。
5. 子サーバーをマウントするために適切なロケーションを選択します。 ロケーションが作成されていない場合は、最初にロケーションを作成します。
6. 選択したロケーションに子サーバーをマウントするには、**保存** をクリックします。

親のロケーションツリーからサーバーをアンマウント

親のロケーションツリーから子サーバーをアンマウントすることができます。

親サーバーのロケーションツリーから子サーバーをアンマウントするには、次の手順を実行します。
1. **コンフィグレーション>システム設定>サーバークラスタ**へ移動します。
2. 親サーバーのルートロケーションを選択します。子サーバーが表示されます。
3. 子サーバーをアンマウントするマウントポイントリンクをクリックします。
4. **アンマウント**をクリックします。
5. 親のロケーションツリーから子サーバーをアンマウントするには、**保存** をクリックします。

親サーバーと子サーバー間のバージョン不一致を修正

親サーバーとサーバークラスタ内の子サーバーが互いに通信する際に正しく機能するためには、それらにインストールされるソフトウェアが同じバージョン番号である必要があります。 親サーバーをアップグレードし、親サーバーとマウントする子サーバー間のバージョンの不一致がある場合、親サーバーのロケーションツリーから子サーバーのロケーションにアクセスすることは許可されていません。 親サーバーのロケーションツリーから子サーバーロケーションにアクセスできるようにするには、バージョンの不一致を修正する必要があります。
バージョンの不一致がある場合は、**バージョンの不一致を修正**リンクが有効になります。 子サーバーのバージョンの不一致を修正するために、このリンクをクリックすることができます。 子サーバーは、アップグレードを適用したあとに再起動します。

バージョンの不一致の修正に進む前に、最新のアップグレードバンドルを入手する必要があります。

親サーバーと子サーバー間のバージョン不一致を修正するには、次の操作を行います。
1. 親サーバーのルートロケーションを選択します。子サーバーが表示されます。
2. **コンフィグレーション>システム設定>サーバークラスタ**へ移動します。 親サーバーとバージョンの不一致を持つ子サーバーで修正リンクが有効になっています。
3. 修正のリンクをクリックします。 **修正バージョンの不一致** のダイアログボックスが表示されます。
4. ファイルの選択のリンクをクリックして、ダウンロードされている場所からアップグレードバンドル・ファイルを選択します。
5. アップグレードバンドルをアップロードするために、**アップロードとアップグレード**をクリックし、バージョンの不一致がある子サーバーをアップグレードします。

子サーバーの無効なライセンス状態を修正

サーバークラスタがコマンドラインを使用して作成されたあと、有効なライセンスを下位サーバーに適用する必要があります。 これは、クラスタ内の親サーバーから行うことができます。

有効なライセンスが子サーバーにまだ適用されていないとき、またはライセンスの有効期限が切れているにときに、子サーバーは無効なライセンス状態となります。

子サーバーの無効なライセンス状態を修正するには、次の手順を実行します。
1. 親サーバーのルートロケーションを選択します。子サーバーが表示されます。
2. **コンフィグレーション>システム設定>サーバークラスタ**へ移動します。 無効なライセンスを持つ子サーバーには、**ライセンス修正** リンクが有効になっています。
3. **ファイルの選択**のリンクをクリックして、ダウンロードされている場所からライセンスファイルを選択します。
4. 子サーバーにライセンスを適用するには、**ライセンス適用**をクリックします。 ライセンスの適用が成功すると子サーバーは再起動します。

ポリシー設定をコピー

サーバークラスタ内のサーバーから別のサーバーにポリシー設定をコピーすることができます。 子サーバーから子サーバー、親サーバーから子サーバー、子サーバーから親サーバーへポリシー設定をコピーすることができます。 あるサーバーから別のサーバーにポリシーをコピーするには、スーパーユーザーである必要があります。 下記に関連するポリシー設定は、コピーすることが可能です。

- アカウントの停止(Account Suspension)
- パスワードポリシー(Password Policy)
- ログインコンフィグレーション(Login Configuration)
- 言語設定(Language Setting)
- 監査ログ(Audit Logs)
- RF プロパゲーション(RF Propagation)
- 自動ロケーションタギング(Auto Location Tagging)
- 自動削除(Auto Deletion)
- SMTP コンフィグレーション(SMTP Configuration)
- RADIUS コンフィグレーション(RADIUS Configuration)
- スマートデバイスタイプ(Smart Device Type)
- 証明書の設定(Certificate Configuration)
- LDAP Configuration
- ロケーショントラッキング コンフィグレーション(Location Tracking Configuration)
- 禁止されたデバイスリスト(Banned Device List) - AP
- 禁止されたデバイスリスト(Banned Device List) - Client
- ライブ RF ビュー設定(Live RF View Settings)
- レポートのルック&フィール(Reports Look and Feel)
- ホットスポット SSID(Hotspot SSIDs)
- 脆弱な SSID(Vulnerable SSIDs)
- Syslog インテグレーション(Syslog Integration)
- SNMP

あるサーバーから別のサーバーに 1 つ以上のポリシーをコピーするには、次の手順を実行します。

1. **コンフィグレーション>システム設定>サーバークラスタ**へ移動します。
2. **コピー**をクリック。ポリシーコピーのダイアログボックスが表示されます。
3. ポリシー設定のコピー元のサーバーを選択します。
4. ポリシー設定のコピー先のサーバーを選択します。
5. コピーするポリシー設定を選択します。 **>** をクリックします。 使用可能なすべてのポリシー設定をコピーするには、**>>**をクリックします。 コピーするポリシー設定の一覧から任意のポリシーを削除したい場合は、右側のボックスでポリシーを選択し、**削除**をクリックします。
6. ポリシー設定をコピーするには、**OK** をクリックします。

子サーバーの検索

サーバー名またはサーバーの IP アドレスで子サーバーを検索することができます。

子サーバーを検索するには、次の手順を実行します。

1. ルートロケーションを選択します。
2. **コンフィグレーション>システム設定>サーバークラスタ**へ移動します。
3. クイック検索ボックスに、サーバー名またはサーバーの IP アドレスを入力します。
4. Enter キーを押します。
5. 検索文字列に一致する名前または IP アドレスを持つサーバーが表示されます。 検索文字列は、名前または IP アドレスの部分文字列である可能性があります。

子サーバー一覧の印刷

サーバークラスタ内の子サーバーのリストを印刷することができます。

親サーバーのルートロケーションで子サーバーリストを印刷するには、次の手順を実行します。
1. **コンフィグレーション>システム設定>サーバークラスタ**へ移動します。
2. 親サーバーのルートロケーションを選択します。
3. リストに印刷したい列を選択します。列の選択または解除するには、任意の列名をクリックします。
4. 印刷アイコンをクリックします。子サーバーの一覧の印刷プレビューが表示されます。
5. 子サーバーのリストを印刷するには、**印刷**をクリックします。

ベンダーOUI の管理

コンフィグレーション>システム>ベンダーOUI を使用して、個々の MAC プレフィックスとともにポピュラーなベンダーの一覧を表示し管理することが可能です。3 バイトの MAC プレフィックスは、任意の IEEE802.11 デバイスベンダーを識別します。

ベンダー/MAC プレフィックスの追加

新しいベンダー/MAC プレフィックスのペアまたは既存のベンダー名に新しいプレフィックスを追加するには **ベンダー/MAC プレフィックスの追加** をクリックします。 既存のベンダーを選択して、ベンダーに対して新しい MAC アドレスを追加します。 同様に、そのベンダーに対応した新しいベンダーと 1 つまたは複数の MAC アドレスを追加することができます。

ベンダー/MAC プレフィックスの削除

削除するには MAC プレフィックスに対応対するそれぞれの **削除** をクリックします。

SMTP 設定を構成

コンフィグレーション>システム設定>SMTP コンフィグレーション を使用して、 イベント発生時に電子メールを送信するために簡易メール転送プロトコル（SMTP）の設定を行います。 SMTP 設定を構成するには、管理者権限を持っている必要があります。

以下は、SMTP の設定ページのフィールドとその説明です。

SMTP 設定を構成するには、次の手順を実行します。
1. **コンフィグレーション>システム設定>SMTP コンフィグレーション** へ移動します。
2. 詳細情報を入力します。次の表は、SMTP に関連するフィールドについて説明します。

フィールド	説明
SMTP Server IP Address/Hostname	電子メールでアラートを送信するためにシステムが使用する SMTP サーバーの IP アドレスまたはホスト名を指定します。 デフォルト値は 127.0.0.1 です。 SMTP サーバーの認証プロトコルは、次のとおりです。 • PLAIN • LOGIN • NTLM
Port	電子メールでアラートを送信するためにシステムが使用する SMTP サーバーのポート番号。
Email Address in From field	電子メールアラートが送信される送信元アドレス。
StartTLS の使用を強制(TLSv1)	StartTLS は、暗号化された通信のために別々のポートを利用する代わりに、暗号化された（TLS または SSL）接続にプレーンテキスト接続をグレードアップする方法を提供する SMTP のようなプレーンテキスト通信プロトコルの拡張です。 暗号化されたフォーマットで電子メールを送信するために StartTLS の使用を強制する場合は、このチェックボックスにチェックを入れます。
SMTP サーバーの証明書を確認	ビルトインされた周知の CA 証明書 または更新された CA 証明書に対して SMTP サーバーの証明書を確認するためには、このチェックボックスを選択します。 このチェックボックスをオンにすると証明書の照合に失敗した場合には、電子メールは送信されません。
証明書のセット	SMTP サーバーの CA 証明書がアプライアンスにパッケージされた CA 証明書に存在しない場合は、SMTP テストの操作は失敗します。 そのような場合は、SMTP サーバーのプライベート CA 証明書をアップロードすることができます。 このボタンをクリックし、SMTP サーバーの認証に使用されるプライベート CA 証明書ファイルを選択します。 プライベート証明書がアップロードされている場合は、この証明書だけが認証に使用されます。ビルトインされた証明書は使用されません。 アップロードされたファイルが複数エントリを含んでいる場合は、最初のエントリが検証のために利用されます。 証明書を削除するには、証明書の削除をクリックし削除を実行します。 プライベート証明書のアップロードまたは削除の操作を行ったあとに、サーバーアプリケーションが再起動されることに注意してください。
Authentication Required	SMTP 認証を有効にするには、このチェックボックスにチェックを入れます。
ユーザー名	SMTP サーバー認証有効時の SMTP サーバーの認証用のユーザー名。
パスワード	SMTP サーバー認証有効時の SMTP サーバーの認証用のパスワード。

3. 必要に応じて、サーバーのアクセス URL を変更します。
4. 変更を保存するには、**保存** をクリックします。

SMTP 設定をデフォルトに戻す

SMTP 設定のデフォルト値は、以下のとおりです。

SMTP Server IP Address/Hostname	127.0.0.1
Port	25
Email Address in From field	server@localhost.localdomain
Authentication Required	not selected
Server Access URL	https://wifi-security-server

SMTP 設定のデフォルト値を復元するには、次の手順を実行します。
1. **コンフィグレーション>システム設定>SMTP コンフィグレーション** へ移動します。
2. SMTP コンフィグレーションフィールドのデフォルト値を復元するには、**デフォルト値に戻す** をクリックします。
3. 変更を保存するには、**保存** をクリックします。

SMTP 設定のテスト

SMTP 設定をテストするには、テストメールを送信することができます。 SMTP 構成の設定がこのメールに使用されます。

このメールに使用される設定は、あなた設定した SMTP 設定になります。 設定をテストする前に、SMTP が正しく設定されいることを確認してください。

SMTP 設定をテストするには、次の手順を実行します。
1. **コンフィグレーション>システム設定>SMTP コンフィグレーション** へ移動します。
2. テストメールを送信するには、**SMTP 設定をテスト**をクリックします。 設定が正しければ、メールが送信されます。

SMTP 設定を別のサーバーへコピー

両方のサーバーが同じサーバークラスタの一部である場合は、片方のサーバーから別のサーバーへ SMTP 設定をコピーすることができます。 子サーバーから子サーバー、親サーバーから子サーバー、または子サーバーから親サーバーへ SMTP 設定をコピーすることができます。 サーバーから別のサーバーへポリシーをコピーするにはスーパーユーザーまたは管理者である必要があります。

SMTP 設定をコピーするには、次の手順を実行します。
1. 親サーバー上で、**コンフィグレーション>システム設定>SMTP コンフィグレーション** へ移動します。
2. **ポリシーをコピー**をクリックします。 **ポリシーをコピー**のダイアログボックスが表示されます。
3. SMTP 設定のコピー元となるサーバーを選択します。
4. SMTP 設定のコピー先となるサーバーを選択します。
5. SMTP 設定をコピーするには、**OK** をクリックします。

システムステータスの表示

コンフィグレーション>システム設定>システムステータス ページでは、管理デバイス(Management Device)サーバーに関する情報を表示します。
すべてのスタティックなサーバー情報が **システム情報**で利用可能です。

サーバーの現在のステータスが、**サーバー情報**の下に表示されます。

サーバーに保存されているバックアップファイルに関する情報が、**サーバー上に保存されたバックアップファイル**の下に表示されます。
次の表は、**システムステータスページ**に表示されるスタティックな情報を示しています。

フィールド	説明
サーバーID	サーバーの一意の ID を明示。 1 台のサーバーをインストールしている場合は、デフォルトのサーバーID(1)を保持します。
管理デバイス (Management Device) コミュニケーションポート	管理コンソール(Management Console)サーバーがデバイスと通信するための管理デバイス(Management Device)のポート番号。
シリアル番号	管理コンソール(Management Console)サーバーのハードウェアシリアル番号。
管理デバイス (Management Device) 最大許容数	ライセンスで許可されている管理デバイス(Management Device)の最大数。 ※ソフトウェアバージョン 1.3.07 以降は、本項目はありません。
AP への 許容コンバージョン	現在のライセンスでアクセスポイントとしての機能に変換することが許可されている管理デバイス(Management Device)の最大数。 ※ソフトウェアバージョン 1.3.07 以降は、本項目はありません。
ソフトウェアバージョン	管理コンソール(Management Console)・ソフトウェアのバージョン番号。
ソフトウェアビルド	管理コンソール(Management Console)・ソフトウェアのビルド番号。
オペレーティングシステム	管理コンソール(Management Console)オペレーティングシステムを表示します。
アライアンスモデル	管理コンソール(Management Console)の構成を表示します。
ライセンスの有効期限	ライセンスの有効期限。 ※ソフトウェアバージョン 1.3.07 以降は、本項目はありません。
IPv6 ステータス	サーバー上で IPv6 プロトコルが有効か無効になっているかどうかを明示。

サーバー起動/停止

システムのステータスに関するライブ情報は、**サーバー情報**の下で見ることができます。 サーバーが動作、停止、またはエラー状態になっていることを見ることができます。
このページからサーバーを停止することができます。 サーバーが停止している場合は、サーバーを起動することができます。

サーバーを停止するには、**サーバー情報**で、**サーバーを停止**をクリックします。 サーバーを起動するには、**サーバー情報**で、**サーバーを起動**をクリックします。 **サーバーステータスの変更** ボタンのテキストは、サーバーが起動中か停止中であるかに基づいて、 **サーバーを停止** と **サーバーを起動** に交互に変わります。

サーバーを停止するには、次の手順を実行します。
1. **コンフィグレーション>システム設定>システムステータス**へ移動します。
2. サーバーを停止するには、**サーバーを停止**をクリックします。

サーバーを起動するには、次の手順を実行します。
1. **コンフィグレーション>システム設定>システムステータス**へ移動します。
2. サーバーを起動するには、**サーバーを起動**をクリックします。

サーバーのアップグレード

コンフィグレーション>システム設定>サーバーのアップグレード を使用して、 管理コンソール(Management Console)の最新バージョンにアップグレードすることができます。 'スーパーユーザー'の権限を持つユーザーだけが、サーバーのアップグレードを行うことができます。

アップグレードのための前提条件

管理コンソール(Management Console)の新しいバージョンにグレードアップする前に以下のことに注意する必要があります。

- コンソールにアクセスするコンピューター上のポップアップブロッカーで、 サーバーからのポップアップウィンドウを許可する必要があります。
- コンソールにアクセスするコンピューターと サーバーの間にファイアウォールがある場合は、サーバーの TCP ポート 8080 はそのコンピューターから アクセス可能にする必要があります。

推奨：サーバーを新しいバージョンにアップグレードするには、 IP アドレスのネットワークアドレス変換（NAT）によって変更されていないコンピューターを使用して コンソールにアクセスしていることを確認します。 NAT IP を使用して、コンソールにアクセスすると、アップグレードはバックグラウンドで継続されますが、 アップグレードの進捗メッセージを表示することができません。

アップグレードプロセス

1. アップグレードバンドルを選択するには、 **ファイル選択** をクリックします。
2. サーバーへアップグレードバンドルを転送するために、 **アップロードとアップグレード** をクリックします。
3. アップグレードの確認ダイアログボックスで、 **Yes** をクリックします。
4. プログレスバーにアップロードバンドルをアップロード中のメッセージが現れます。
5. アップグレードバンドルのアップロード中は、いつでも **キャンセル** をクリックしてアップグレードをキャンセルすることができます。
6. サーバーアップグレードバンドルのアップロードが完了すると、サーバーのアップグレードが自動的に起動します。
7. アップグレードがはじまったらそのままお待ちください。 サーバーアップグレードプロセスのステータスを表示する新しいウィンドウが起動されます。 サーバーアップグレードプロセス・ウィンドウに表示される指示にしたがっています。
8. サーバーのアップグレードに成功すると、サーバーは自動的に再起動します。
9. サーバーアップグレードプロセス・ウィンドウ上のすべての指示を読んだあと、 サーバーアップグレードプロセス・ウィンドウを含むすべての Web ブラウザのウィンドウを閉じます。
10. サーバーが再起動するために 5 分間待ちます。 そのあと、再びサーバーにアクセスすることができます。

ご注意：いったん、サーバーアップグレードプロセス・ウィンドウが起動されると、 サーバーアップグレードプロセスを中断またはキャンセルすることはできません。 またサーバーアップグレードプロセス・ウィンドウが閉じられたとしても、 サーバーアップグレードプロセスは継続されます。

自動削除の設定を構成

管理コンソール(Management Console)は、認識できるデバイスやそれらのデバイスに関連するイベントの履歴情報を格納します。 この情報の増加率は、配置される運用場所の無線環境の変動性に依存します。 それは時間の経過とともに役に立たなくなるので、定期的にこの情報を削除する必要があります。 これは、**コンフィグレーション>システム設定>自動削除** を使用して行われます。

イベント関連の設定に基づいて、システムはイベント数を発生し格納します。 かなりの数のイベントを生成し格納されるように設定を構成した場合、保存されるイベントデータのサイズは 急速に増えていきます。このイベントデータは、定期的なクリーンアップが必要です。
自動削除 では、情報の削除の頻度を制御するさまざまな自動削除パラメータの値を指定することができます。 システムは、自動削除のアクションを追跡するイベントを生成します。 このイベントは、デバイスの削除についての情報を提供します。 イベントの削除を示すための個別に生成されるイベントはありません。

自動削除パラメータは、アクセスポイント、クライアント、ネットワーク、イベントに関連しています。これらを、以下に詳細に説明します。

アクセスポイント削除パラメータ ： 削除可能な AP のカテゴリは、 **Rogue** です。 **許可 AP(Authorized AP)** は、 システムから自動的に削除されません。非アクティブな許可 AP(Authorized AP)を削除したい場合は、手動で削除する必要があります。
自動削除期間を設定したい AP のカテゴリを選択します。 AP 関連の情報がそれぞれのカテゴリで自動的に削除対象となるまでの非アクティブな日数を指定します。 非アクティブの最小日数は 1 で、最大日数は 30 です。

クライアント削除パラメータ： 削除可能なクライアントのカテゴリは、**Authorized 、Rogue** です。
自動削除期間を設定したいクライアントのカテゴリを選択します。 適切なチェックボックスをオンにして、クライアント関連の情報が自動的にそれぞれのカテゴリで削除対象となるまでの非アクティブな日数を指定します。 非アクティブの最小日数は 1 で、最大日数は 30 です。

ネットワーク削除パラメータ： **隔離したネットワークを保持する日数** のチェックボックスにチェックを入れ、 隔離したネットワークがサーバーで保持される日数を指定します。 このフィールドのデフォルト値は 30 日です。システム内に保持される最小値は 1 日で最大値は 90 日です。

イベント削除パラメータ: サーバー上に保持されるセキュリティ、パフォーマンス、およびシステムイベントの最大数を指定します。

イベントをデータベースに保持する期間を指定： イベントを保持する最小日数は 1 日で、最大日数は 180 日です。 指定された期間よりも古いイベントがデータベースから削除されます。

システムによって生成される特別なイベントをモニタリングすることにより、非アクティブな AP、クライアント、およびイベントの自動削除を追跡することができます。 システムは、情報の任意の物理的な削除が実際に行われた場合に限り、自動削除の動作中に実行されるアクションの概要を含むイベントを生成します。

自動削除の設定を別のサーバーへコピー

両方のサーバーが同じサーバークラスタの一部である場合は、片方のサーバーから別のサーバーへ自動削除設定をコピーすることができます。 子サーバーから子サーバー、親サーバーから子サーバー、または子サーバーから親サーバーへ自動削除設定をコピーすることができます。 サーバーから別のサーバーへポリシーをコピーするにはスーパーユーザーまたは管理者である必要があります。

自動削除設定をコピーするには、次の手順を実行します。
1. 親サーバー上で、**コンフィグレーション>システム設定>自動削除** へ移動します。
2. **ポリシーをコピー**をクリックします。 **ポリシーをコピー**のダイアログボックスが表示されます。
3. 自動削除設定のコピー元となるサーバーを選択します。
4. 自動削除設定のコピー先となるサーバーを選択します。
5. 動削除設定をコピーするには、**OK** をクリックします。

監査ログ設定の管理

管理コンソール(Management Console)は、ユーザーのアクティビティを追跡します。 ユーザーアクションのログを表示する目的でサーバーからダウンロードすることができます。 これは、**コンフィグレーション>システム設定>監査ログ** を使用して行います。 スーパーユーザーだけがユーザーアクションログをダウンロードする権限を持っています。
監査ログは、ユーザーアクションログとも呼ばれます。

監査ログのダウンロード期間を設定

何日から何日迄のユーザーアクションログをダウンロードしたいかを、 **From** と **To** フィールドを使用して、時間間隔を指定することができます。 あるいは、ユーザーアクションログをダウンロードしたい経過時間の数を示すことで時間間隔を指定することができます。 ダウンロードできるログエントリの種類を選択することができます。 これを指定するには**タイプ**フィールドを使用します。 デフォルトでは、すべてのタイプのレコードがダウンロードされたログファイルに含まれています。
ログイン試行の日付時間、モジュール、ホスト・アドレス、ユーザー役割、ログイン名、タイプとステータスに関してログをソートすることができます。 ソートフィールドを選択するために、**順序**フィールドを使用します。 ログエントリのデフォルトのソートは、日付と時刻に基づいて行われます。

ダウンロードするユーザーアクションログの設定を構成するには、次の手順を実行します。
1. **コンフィグレーション>システム設定>監査ログ**へ移動します。
2. ダウンロードするユーザーアクションログのタイプを選択します。
3. ユーザーアクションログがダウンロードされる **From** と **To** の日付を選択します。 別の方法として、**ラスト**を選択してユーザーアクションログをダウンロードしたい経過時間、日数または月数を指定することができます。
4. 変更を保存するには、**保存**をクリックします。

監査ログのダウンロード

ダウンロードするユーザーアクションログの期間や種類を設定したあとに。ユーザーアクションログをダウンロードすることができます。

ダウンロードするには、次の手順を実行します。
1. **コンフィグレーション>システム設定>監査ログ**へ移動します。
2. **ダウンロード**をクリック。 ユーザーアクションログは csv ファイルとしてダウンロードされます。 ログの内容は、ダウンロードされたアクションログの種類によって異なります。

ご注意： サーバーがサーバークラスタの親サーバーである場合、ダウンロードされたログは親サーバーと子サーバーのログデータの集約されたものになります。 これは、子サーバーのログが親サーバーのログに含まれることを意味します。 この場合、監査ログには、'Cluster Server'の列が追加され含まれています。 親サーバーのログエントリは、 'Cluster Server'列の値になります。子サーバーのログエントリは、子サーバー自身の名前を持つ列の値です。

ユーザーアクションログのダウンロード設定をデフォルト値に復元

1. **コンフィグレーション>システム設定>監査ログ**へ移動します。
2. デフォルト値に戻すには、**デフォルト値に戻す**をクリックします。
3. 変更を保存するには、**保存**をクリックします。

監査ログの設定を別のサーバーへコピー

両方のサーバーが同じサーバークラスタの一部である場合は、片方のサーバーから別のサーバーへ監査ログの設定をコピーすることができます。 子サーバーから子サーバー、親サーバーから子サーバー、または子サーバーから親サーバーへ監査ログの設定をコピーすることができます。 サーバーから別のサーバーへポリシーをコピーするにはスーパーユーザーまたは管理者である必要があります。

監査ログの設定をコピーするには、次の手順を実行します。
1. 親サーバー上で、**コンフィグレーション>システム設定>監査ログ**へ移動します。
2. **ポリシーをコピー**をクリックします。 **ポリシーをコピー**のダイアログボックスが表示されます。
3. 監査ログの設定のコピー元となるサーバーを選択します。
4. 監査ログの設定のコピー先となるサーバーを選択します。
5. 監査ログの設定をコピーするには、**OK** をクリックします。

エンタープライズセキュリティ管理サーバーとの統合を構成

ESM インテグレーション

コンフィグレーション>ESM インテグレーション ページを使用して、さまざまな企業のセキュリティ管理（ESM）サーバーに統合するために、管理コンソール(Management Console)を構成することが可能です。

管理コンソール(Management Console)は、ESM サーバーと統合します（収集・解析・イベントを表示）。管理コンソール(Management Console)は、これらのサーバーにセキュリティイベントに関連する情報を送信します。

管理コンソール(Management Console)は、SNMP、Syslog サーバーと統合します。

Syslog インテグレーション

管理コンソール(Management Console)が Syslog サーバーと通信しログメッセージを送信するためのインテグレーション設定を構成することができます。

Syslog インテグレーションが有効になっている場合、システムは設定された Syslog サーバーにメッセージを送信します。 それ以外の場合は、Syslog インテグレーションサービスは遮断されています。 管理コンソール(Management Console)が Syslog サーバーにメッセージを送信するには、Syslog とのインテグレーションを有効にする必要があります。 Syslog サーバーとの管理コンソール(Management Console)のインテグレーションを可能にするために、**Syslog インテグレーション有効** のチェックボックスを選択します。

現在のステータス には、Syslog サーバーのステータスが表示されます。これは Syslog サーバーのステータスに応じて、**Running** または **Stopped** または **Error** の場合があります。 システムが停止した場合、有効な Syslog サーバーのホスト名を解決できない場合、または内部エラーが発生した場合は、**Error** ステータスが表示されます。内部エラーが発生した場合には、購入先へお問い合わせください。

Syslog サーバーの追加

Syslog サーバーを追加するには、次の手順を実行します。
1. **コンフィグレーション>ESM インテグレーション>Syslog インテグレーション**へ移動します。
2. **Syslog サーバーの管理**で、Syslog サーバーの詳細設定を追加するために **Syslog サーバーの追加**をクリックします。
3. イベントの送信先となる Syslog サーバーの IP アドレスまたはホスト名を指定します。
4. システムがイベントを送信する Syslog サーバーのポート番号を指定します。デフォルトのポート番号は 514 です。
5. 侵入検知メッセージ交換形式（IDMEF）またはテキスト形式で、イベントが送信される形式を指定します。
6. イベントをこの Syslog サーバーに送信する場合は、"有効"チェックボックスにチェックを入れます。これは、デフォルトで"有効"になっています。
7. Syslog サーバーのエントリにバイトオーダー・マークを付加したい場合は、"BOM ヘッダを付加"チェックボックスを選択します。
8. Syslog サーバーにイベントを送信するには Forward Events チェックボックスにチェックを入れます。
9. Syslog サーバーに監査 log を送信するには Forward Audit Logs チェックボックスにチェックを入れます。これはプレーンテキストフォーマットのときにのみ実施できます。
10. 新しい Syslog サーバーに関する詳細を追加するには、**OK** をクリックします。

Syslog サーバーの編集

Syslog サーバーに対する Syslog サーバー設定を編集するには、次の手順を実行します。
1. **コンフィグレーション>ESM インテグレーション>Syslog インテグレーション**へ移動します。
2. Syslog サーバーリスト内の Syslog サーバーの IP アドレスとポートのをクリックします。
3. 必要な変更を加えます。
4. 変更を保存するには、**OK** をクリックします。

Syslog サーバーの削除

Syslog サーバーのリストから Syslog サーバーを削除することが可能です。リストから削除すると、エントリはこのサーバーに送信されません。

Syslog サーバーを削除するには、次の手順を実行します。
1. **コンフィグレーション>ESM インテグレーション>Syslog インテグレーション**へ移動します。
2. Syslog サーバーを削除するには、Syslog サーバーの **削除** をクリックします。

Syslog サーバーの設定を別のサーバーへコピー

両方のサーバーが同じサーバークラスタの一部である場合は、片方のサーバーから別のサーバーへ Syslog サーバーの設定をコピーすることができます。 子サーバーから子サーバー、親サーバーから子サーバー、または子サーバーから親サーバーへ Syslog サーバーの設定をコピーすることができます。 サーバーから別のサーバーへポリシーをコピーするにはスーパーユーザーまたは管理者である必要があります。

Syslog サーバーの設定をコピーするには、次の手順を実行します。
1. 親サーバー上で、**コンフィグレーション>ESM インテグレーション>Syslog インテグレーション**へ移動します。
2. **ポリシーをコピー**をクリックします。 **ポリシーをコピー**のダイアログボックスが表示されます。
3. Syslog サーバー設定のコピー元となるサーバーを選択します。
4. Syslog サーバー設定のコピー先となるサーバーを選択します。
5. Syslog サーバー設定をコピーするには、**OK** をクリックします。

SNMP インテグレーション

SNMP サーバーとの通信に関するインテグレーション設定を構成するには **コンフィグレーション >ESM インテグレーション>SNMP** に移動します。
SNMP ページでは、指定された SNMP トラップレシーバに SNMP トラップとして、管理コンソール (Management Console)からイベントの送信を可能にします。また、 IF-MIB、MIB-II そして Host Resources MIB を使用して、SNMP マネージャーがサーバーの動作パラメータを照会することを可能にします。

SNMP サーバーとのインテグレーションを可能にするために **SNMP インテグレーションを有効** チェックボックスを選択します。 SNMP インテグレーションを有効にすると、システムは設定されている SNMP サーバーに SNMP トラップを送信します。 他のシステムは、SNMP サーバーからネットワーク・エンティティに関する情報を要求することができます。それ以外の場合は、SNMP インテグレーションサービスが遮断されます。

現在のステータス には、SNMP サーバーの現在のステータスが表示されます。これは SNMP サーバーのステータスに応じて、**Running** または **Stopped** または **Error** の場合があります。システムのサーバーが停止した場合、または、内部エラーが発生した場合に **Error** ステータスが表示されます。内部エラーが発生した場合には、購入先へお問い合わせください。

SNMP 設定 では、SNMP Get または Trap を設定します。

SNMP Get と SNMP Trap を設定

IF-MIB、MIB-II そして Host Resources MIB に参加しサーバーの動作パラメータを照会することを SNMP マネージャーに許可するには、**SNMP Get を有効** チェックボックスを選択します。すべての MIB に関連する問い合わせをブロックするためには、このチェックボックスをオフにします。

あるいは、SNMP v3 Get パラメータ（ユーザー名、認証パスワード、プライバシーパスワード、認証プロトコル、プライバシープロトコル）を設定するために、**SNMP v3 Get パラメータ** チェックボックスを選択します。（デフォルトのユーザー名は admin。デフォルトの認証パスワードは password。デフォルトのプライバシーパスワードは password。デフォルトの認証プロトコルは MD5。デフォルトのプライバシープロトコルは DES です。） マスクなしでパスワードを表示するには、**キーを表示** チェックボックスを選択します。

SNMP トラップを設定された SNMP サーバーに送信するには、**SNMP Trap を有効** チェックボックスを選択します。
また、有効にする SNMP のバージョンを選択して、関連する設定を構成します。サーバー上に存在する SNMP エージェントは、SNMP Trap レシーバにトラップを配信するために SNMP のバージョンパラメータを使用します。

SNMP v1、v2 プロトコルを使用してトラップを受け入れるすべてのトラップレシーバにトラップを送信するためには、**SNMP v1,v2** Get パラメータ チェックボックスを選択します。あなたは、SNMP エージェントの**コミュニティストリング**を変更することができます。 すべての SNMP v1, v2 レシーバは、Trap を受信するために、このコミュニティストリングを使用するよう設定される必要があります。（デフォルト：public）

SNMP v3 プロトコルを使用してトラップを受け入れるすべてのトラップレシーバにトラップを送信するためには、 **SNMP v3** Get パラメータ チェックボックスを選択します。Trap レシーバを追加/宛先を追加する際に、個々のパラメータ（**ユーザー名、認証パスワード、プライバシーパスワード、認証プロトコル、プライバシープロトコル**） を設定することが可能です。 すべての SNMP v3 Trap レシーバは、Trap を受信するために、これらのパラメータを使用するよう設定される必要があります。

エンジン ID は編集できません。

デフォルトのユーザー名は admin。デフォルトの認証パスワードは password。デフォルトのプライバシーパスワードは password。デフォルトの認証プロトコルは MD5。デフォルトのプライバシープロトコルは DES です。

SNMP MIBs では、以下の SNMP MIB を個々に有効または無効にすることでクエリを選択することが可能です。

- IF MIB
- Host Resources MIB
- NEC-MIB: 選択した場合、システムは Trap を受信するために、外部の SNMP Trap レシーバを有効にします。
- MIB-II: 選択した場合、System Contact、System Name、System Location を設定します。(デフォルトの System Name は、na100mc です。).

IF MIB、Host Resources MIB、MIB II は、インターネットからダウンロードすることができる標準的な MIB です。NEC-MIB に関しては、購入先へお問い合わせください。

SNMP トラップ宛先サーバーの追加

SNMP トラップ宛先サーバーでは、SNMP 設定ダイアログを開くために追加をクリックし SNMP サーバーの詳細を追加することが可能です。

宛先サーバー（IP アドレス/ホスト名）： イベントが送信される SNMP サーバーの IP アドレスとホスト名を指定します。
SNMP Protocol Version： SNMP エージェントの SNMP プロトコルバージョンを指定します。(デフォルト： SNMP v3)
ポート番号： SNMP トラップの送信先となる受信側システムのポート番号を指定します。 (デフォルト： 162)
有効： SNMP サーバーが SNMP トラップを受信することができるかどうかを指定します。 (デフォルト：有効)
ユーザー名： SNMP v3 のユーザー名を指定します。 (デフォルト： 空欄)
認証パスワード： SNMP v3 認証パスワードを指定します。 (デフォルト： 空欄)
プライバシーパスワード：SNMP v3 プライバシーパスワードを指定します。 (デフォルト： 空欄)
認証プロトコル： SNMP v3 認証プロトコルを指定します。 (デフォルト： MD5)
プライバシープロトコル： SNMP v3 プライバシープロトコルを指定します。 (デフォルト： DES)
ご注意： 別のアプリケーションがデフォルトのポートを使用している場合は、別のポート番号を指定する必要があります。 認証とプライバシープロトコルのすべての組み合わせについては、v3 Get/Trap パラメータに別のユーザー名を指定する必要があります。
新しい SNMP サーバーの詳細を追加するには、追加をクリックします。

SNMP トラップ宛先サーバーの編集

SNMP トラップ宛先サーバーの一覧で SNMP トラップ宛先サーバーの IP アドレスとポートをクリックします。必要な変更を行います。 変更を保存するには **OK** をクリックします。

SNMP トラップ宛先サーバーの削除

サーバーを削除するには、SNMP トラップ宛先サーバーの**削除**をクリックします。いったんリストから削除すると、イベントはこのサーバーに送信されることはありません。

SNMP 設定を別のサーバーへコピー

両方のサーバーが同じサーバークラスタの一部である場合は、片方のサーバーから別のサーバーへ SNMP 設定をコピーすることができます。 子サーバーから子サーバー、親サーバーから子サーバー、または子サーバーから親サーバーへ SNMP 設定をコピーすることができます。 サーバーから別のサーバーへポリシーをコピーするにはスーパーユーザーまたは管理者である必要があります。

SNMP 設定をコピーするには、次の手順を実行します。
1. 親サーバー上で、**コンフィグレーション>ESM インテグレーション>SNMP** へ移動します。
2. **ポリシーをコピー**をクリックします。 **ポリシーをコピー**のダイアログボックスが表示されます。
3. SNMP 設定のコピー元となるサーバーを選択します。
4. SNMP 設定のコピー先となるサーバーを選択します。
5. SNMP 設定をコピーするには、**OK** をクリックします。

ダッシュボード

ダッシュボードは、無線 LAN パフォーマンスの状態表示です。 管理コンソール(Management Console)は、ユーザーによって構成することができる使いやすいダッシュボードを提供します。 ユーザーは、事前に定義されたウィジェットのコレクションから選択して、ダッシュボードに追加できます。 ダッシュボードウィジェットは、アクセスポイント・ウィジェット、クライアント・ウィジェット、ネットワーク・ウィジェットと WIPS ウィジェットに分類されます。 ウィジェットは、さまざまな AP、クライアント、ネットワークおよび管理コンソール(Management Console)によって管理される WLAN での WIPS 関連のアクティビティを視覚的に表示します。
サーバークラスタ内の親サーバーのロケーションでトレンドチャートを表示している場合は、トレンドチャートには集約データが表示されます。

ダッシュボード を表示するにはダッシュボードをクリックします。

ダッシュボードの 各ページでは、利用可能なウィジェット・カテゴリ（アクセスポイント・ウィジェット、クライアント・ウィジェット、ネットワーク・ウィジェットと WIPS ウィジェット）から、複数のウィジェットを持つことが可能です。

これらのウィジェットのカテゴリやウィジェットを表示するには、  をクリックします。

アクセスポイントのウィジェットを表示するには、 **アクセスポイント** をクリックします。 クライアントのウィジェットを表示するには、 **クライアント** をクリックします。 ネットワークのウィジェットを表示するには、 **ネットワーク** をクリックします。 WIPS（無線侵入防御システム）のウィジェットを表示するには、 **WIPS** をクリックします。  と  を使用してウィジェットをスクロールします。

それぞれのダッシュボードページを表示するには、ページ番号をクリックしてください。 各ページには、'ダッシュボード' とページ番号の組み合わせでデフォルトの名前を持っています。 例えば、ダッシュボードのページ 1 は、デフォルト名が 'ダッシュボード 1' になります。 これは、ページ番号の左側に表示されています。 ダッシュボードの各ページ名を変更することも可能です。名前を変更するには、名前を変更したいページに移動します。 [名前]ボックスの内側をクリックして名前を変更し、変更を保存するために[名前]ボックスの外側をクリックします。

ダッシュボードにページを追加

ダッシュボードは、最大 10 ページまで作成できます。 各ページには、その上に最大 9 つのウィジェットを持つことができます。 必要に応じてダッシュボードにページを追加できます。 また、各ページに持つことができるウィジェットの数を定義できます。 同じページ上に異なるウィジェットのカテゴリからウィジェットを持つことができます。 同じページに複数回、同じウィジェットを追加することができます。 ページにウィジェットを追加するには、目的のウィジェットにスクロールして、それをクリックします。

ダッシュボードに新しいページを追加するには、 をクリックします。 新しいページがダッシュボード上の既存のページのあとに追加されます。 新しいページを追加するために をクリックしたあと、 マウスをドラッグして、ウィジェットの数やページ上に表示するレイアウトを選択します。 選択されたウィジェットの数は、このページに追加できるウィジェットの最大数を示しています。

以下の選択は、新しいページに 4 つのウィジェットの追加を可能にします。 これらのウィジェットはページの上部に 2 つ配置され、そして残りの 2 つは最初の 2 つのウィジェットの下に配置されます。

新しいページ上のウィジェット数とレイアウト

ダッシュボードからページを削除

ダッシュボードから現在のページを削除するには をクリックします。

特定のページを削除するには、ページ番号をクリックしてそのページに移動し、 をクリックします。

ダッシュボードページの印刷

ダッシュボードページを印刷できます。ページを印刷するときダッシュボードページ上に表示されるすべてのウィジェットが出力されます。

ダッシュボードページを印刷するには、それぞれのダッシュボードページに移動し、 アイコンをクリックします。

WIPS ウィジェット

ダッシュボード上で **WIPS** をクリックすることによって無線侵入防御に関係するウィジェットが見ることができます。 WIPS のウィジェットは以下のとおりです。

- **セキュリティステータス （Security Status）**
  このウィジェットは、ネットワークのセキュリティステータスが表示されます。 セキュリティステータスの一因となるイベントがウィジェットをクリックすると表示されます。 下図は、'安全' と'脆弱' な状態を説明しています。

セキュリティステータス

- **Management Devices**
  このチャートは、管理デバイス(Management Device)とその動作モードを示します。 すべて、アクティブまたは非アクティブなデバイスを表示するには、ステータスフィルターを使用します。

- **AP 分類 （AP Classification）**
  このチャートは、カテゴリに基づくアクセスポイントを提示します。 すべて、アクティブまたは非アクティブなデバイスを表示するには、ステータスフィルターを使用します。

- **クライアント分類 （Client Classification）**
  このチャートは、カテゴリに基づくクライアントを提示します。 すべて、アクティブまたは非アクティブなクライアントを表示するには、ステータスフィルターを使用します。

- **最新のセキュリティイベント （Latest Security Events）**
  このテーブルには、このロケーションで認められた最新のイベントを一覧表示します。 特定の期間に発生したイベント、目的の深刻度そしてイベント数を表示するには、時間、深刻度と数のフィルターを使用します。

- **隔離内のデバイス （Devices in Quarantine）**
  このチャートは、隔離内のいろいろな状態のアクセスポイントとクライアントを示します。

- **セキュリティ・イベント・カテゴリのトップ （Top Security Event Categories）**
  このチャートは、カテゴリ別のイベント数を示します。 特定の期間中に発生したイベントをフィルタリングするには時間フィルターを使用します。

- **イベントによるロケーション**
  このウィジェットでは各ロケーションごとに発生したイベント数をトップ形式、もしくはボトム形式で表示します。

- **有効化スイッチ**
  有効化スイッチウィジェットは、イベントの有効化と侵入防御ポリシーのステータスを表示します。 このウィジェットから、これらのポリシーに変更を加えることが可能です。 それぞれのページにナビゲートするには、ウィジェット上のイベント有効化または侵入防御スイッチをクリックして、イベント有効化または侵入防御を有効/無効にします。

ウィジェット上のデータを更新するには、利用可能な場所の  をクリックします。 ウィジェットをクローズするには、  をクリック後、クローズしたいウィジェットの  をクリックします。

ネットワーク・ウィジェット

ダッシュボード上で**ネットワーク**をクリックすることによってネットワークに関係するウィジェットが見ることができます。 ネットワークのウィジェットは以下のとおりです。

- **ロケーションマップ （Location Map）**
  このウィジェットは、このウィジェットを使用するには、事前にロケーションおよびレイアウトが作成されている必要があります。ロケーションおよびレイアウトの作成方法の詳細はロケーションとロケーションレイアウトの管理を参照してください。

- **AP 別のロケーション （Locations by APs）**
  このウィジェットは、AP 数が多いロケーションを最大 5 つまで表示します。 ウィジェットの上部にある適切なオプションを選択して、選択したロケーションのアクティブまたは非アクティブの AP を表示することができます。 また、**すべて**を選択することで、選択したロケーションのアクティブおよび非アクティブの両方の AP を表示することができます。 ウィジェットで利用可能な SSID を選択して、コンテンツをフィルタリングすることが可能です。

- **アクティブ AP トレンド （Active APs Trend）**
  このウィジェットは、時間の経過に伴うアクティブな AP の数の傾向を示します。 特定の Wi-Fi ネットワークと特定の期間中のそれぞれの統計情報を表示するには、SSID と時間フィルターを使用します。

- **アソシエーション・トレンド （Associations Trend）**
  このウィジェットは、時間の経過に伴うアソシエーションするクライアントの数の傾向を示します。 特定の Wi-Fi ネットワークと特定の期間中のそれぞれの統計情報を表示するには、SSID と時間フィルターを使用します。

- **AP データ転送トレンド （AP Data Transfer Trend）**
  このチャートの傾向は、時間の経過に伴う選択したロケーションでのすべての管理対象 AP の全体の平均データレートを示します。 特定の Wi-Fi ネットワークと特定の期間中の統計情報を表示するには、SSID と時間フィルターを使用します。

- **SSID 別のスマートデバイスのアソシエーション （Smart Device Associations by SSID）**
  このウィジェットは、選択したロケーションで SSID 別にアソシエイトしたスマートフォンやタブレットの現在アクティブな数が表示されます。

- **SSID 別のデータ転送 （Data Transfer by SSID）**
  このチャートは、データ転送によるトップの SSID が表示されます。 SSID は、管理された AP 上で設定される必要があります。 指定された期間中のそれぞれのトップの SSID 数を表示するには、数と時間フィルターを使用します。

- **SSID 別の平均アソシエーション （Average Association by SSID）**
  このチャートは、時間の経過に伴う SSID 別のアソシエーションの平均数が表示されます。

- **アソシエーション別のロケーション （Locations by Associations）**
  このチャートは、アソシエーション数に基づくロケーションが表示されます。 特定の Wi-Fi ネットワークと特定の期間、トップとボトム、ロケーション数の統計情報を表示するには、SSID と時間、トップ/ボトムと数のフィルターを使用します。

- **最新のパフォーマンスイベント （Latest Performance Events）**
  このチャートは、ロケーションの最新のパフォーマンスイベントが表示されます。 特定の期間に発生したイベント、目的の深刻度そしてイベント数を表示するには、時間、深刻度、数のフィルターを使用します。

- **平均のデータ転送 （Average Data Transfer）**
  このチャートは、平均データ転送に基づくロケーションが表示されます。 データ転送は、アップリンクとダウンリンクの両方を含みます。 これは 管理コンソール(Management Console)を介して管理されるアクセスポイント(AP)のみになります。 特定の Wi-Fi ネットワークと特定の期間、トップとボトム、ロケーション数のそれぞれの統計情報を表示するには、SSID と時間、トップ/ボトムと数のフィルターを使用します。

一般的には、ウィジェット上のデータを更新するには、利用可能な場所の  をクリックします。

ウィジェットの機能の詳細については、  をクリックします。 ウィジェットを閉じるには、  をクリック後、クローズしたいウィジェットの  をクリックします。

クライアント・ウィジェット

ダッシュボード上で**クライアント** をクリックすることによってクライアントに関係するウィジェットが見ることができます。 クライアントのウィジェットは以下のとおりです。

- **スマートデバイスの分布 （Smart Devices Distribution）**
  このチャートは、お使いの Wi-Fi ネットワーク上のスマートフォンやタブレットの数が表示されます。 特定の Wi-Fi ネットワークと特定の期間中のそれぞれの統計情報を表示するには、SSID と時間フィルターを使用します。

- **クライアントプロトコルの分布 （Client Protocol Distribution）**
  このチャートは、使用している Wi-Fi プロトコルによって、接続されたクライアントの数を表示します。 特定の Wi-Fi ネットワークの統計情報を表示するには、SSID フィルターを使用します。

- **トラフィック別のクライアント （Clients by Traffic）**
  このチャートは、生成されるトラフィック量に基づくクライアントを表示します。 トラフィックは、アップリンクおよびダウンリンクのデータ転送の両方を含みます。 特定期間の統計情報を表示するために時間フィルターとトップ/ボトムを使用します。

- **データレート別のクライアント （Clients by Data Rate）**
  このチャートは、平均データレートに基づいてクライアントを表示します。自社の Wi-Fi ネットワークの周辺に低速なクライアントがいる場合、Wi-Fi ネットワークの通信能力に影響を与える可能性があります。 特定期間中の統計情報を表示するために時間フィルターとトップ/ボトムを使用します。

一般的には、ウィジェット上のデータを更新するには、利用可能な場所の  をクリックします。

ウィジェットの機能の詳細については、  をクリックします。 ウィジェットを閉じるには、  をクリック後、クローズしたいウィジェットの  をクリックします。

アクセスポイント・ウィジェット

ダッシュボード上で**アクセスポイント** をクリックすることによってアクセスポイント(AP)に関係するウィジェットが見ることができます。 AP のウィジェットは以下のとおりです。

- **アソシエーション別の AP（APs by Association）**
  このチャートは、アソシエイトしたクライアントの数が最も多いまたは最も少ない AP を最大 10 台まで表示します。
   をクリックして **トップ**（接続されたクライアントの数が最も多い AP を表示）または **ボトム**（接続されたクライアントの数が最も少ない AP を表示）の **チャートタイプ** を選択します。 ウィジェットで表示する AP の最大数を入力し、**保存**をクリックします。
  特定の Wi-Fi ネットワークと特定の期間中のそれぞれの統計情報を表示するには、SSID フィルター、時間フィルターを使用します。

- **トラフィック別の AP （APs by Traffic）**
  このチャートは、トラフィック（ダウンリンクとアップリンクを含む）が最も多いまたは少ない AP を最大 10 台まで表示します。  をクリックして **トップ**（トラフィックが最も多い AP を表示）または **ボトム**（トラフィックが最も少ない AP を表示）の **チャートタイプ** を選択します。 ウィジェットで表示する AP の最大数を入力し、**保存**をクリックします。
  特定の Wi-Fi ネットワークと特定の期間中のそれぞれの統計情報を表示するには、SSID と時間フィルターを使用します。

- **利用率別の AP（APs by Utilization）**
  このチャートは、チャネルを最大に利用する AP が表示されます。 AP のチャネル利用率は、任意のフレームの送信または受信している AP の動作として定義されています。 データと管理フレームはこの計算に考慮されます。
   をクリックして **トップ**（利用率が最も多い AP を表示）または **ボトム**（利用率が最も少ない AP を表示）の **チャートタイプ** を選択します。 ウィジェットで表示する AP の最大数を入力し、**保存**をクリックします。

- **データレート別の AP （APs by Data Rate）**
  このチャートは、平均データレートに基づいて AP を表示します。 データレートは、ダウンリンクとアップリンクの両方を含みます。 AP の非常に低いデータレートは、ネットワーク内のカバレッジの問題や低速レガシーデバイスが存在する（例：IEEE802.11b）可能性を示し、AP の本来の能力に影響を与える恐れがあります。
   をクリックして **トップ**（トラフィックの多い AP を表示）または **ボトム**（トラフィックの少ない AP を表示）の **チャートタイプ** を選択します。 ウィジェットで表示する AP の最大数を入力し、**保存**をクリックします。
  特定の Wi-Fi ネットワークと特定の期間中のそれぞれの統計情報を表示するには、SSID フィルター、時間フィルターそしてトップ/ボトムを使用します。

- **AP セキュリティ分布 （AP Security Distribution）**
  このチャートは、セキュリティの設定別のアクティブな AP の数を表示します。 特定の Wi-Fi ネットワークの統計情報を表示するには、SSID フィルターを使用します。

- **AP プロトコル分布 （AP Protocol Distribution）**
  このチャートは、Wi-Fi プロトコル設定別のアクティブな AP の数を表示します。 特定の Wi-Fi ネットワークの統計情報を表示するには、SSID フィルターを使用します。

一般的には、ウィジェット上のデータを更新するには、利用可能な場所の  をクリックします。

ウィジェットの機能の詳細については、  をクリックします。 ウィジェットを閉じるには、 
をクリック後、クローズしたいウィジェットの  をクリックします。

デバイスの監視

デバイス ページでは、システムで認識できる AP、クライアント、管理デバイス(Management Device)、ネットワークについての情報を提供します。 デバイスプロパティを表示し、そのプロパティに基づいて表示を並べ替え、使用するデバイステンプレートを変更することができます。 デバイスに関連する AP、クライアント、ネットワークを表示することができます。

ロケーションでデバイスを表示するロケーションを選択します。

Management Devices タブは、選択されたロケーションに関連付けられた管理デバイス(Management Device)の一覧を表示します。
APs タブは、選択されたロケーションに関連付けられたアクセスポイントの一覧を表示します。
Clients タブは、選択されたロケーションに関連付けられたクライアントの一覧を表示します。
Networks タブは、選択されたロケーションに関連付けられたネットワークの一覧を表示します。

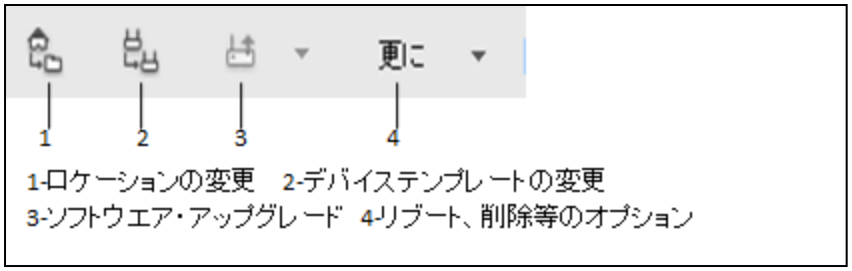
管理デバイス(Management Device)

デバイス> Management Devices タブには、選択したロケーションに関連付けられているすべての Management Device が表示されます。Management Device は管理デバイス(Management Device)上で 設定可能なアクセスポイント／センサーデバイスです。

Management Device が認識する AP、クライアントおよび VLAN のリストを表示するには、Management Device を選択します。

Management Devices タブは、水平に 2 つのペインに分割されています。 上部のペインには、選択したロケーションの Management Device のリストが表示されます。 下部のペインには、タブの上部ペインで選択したデバイスに関連したデバイスのプロパティが表示されます。 下部のペインには、選択されたデバイスが認識できる VLAN、アクセスポイント、およびクライアントのリストを表示することができます。 また、下部ペインに、選択されたデバイスから認識できるアクティブな AP のリスト、アクティブなクライアント、および過去 12 時間の間にデバイスが受ける干渉を表示することができます。

下図のようなツールバーが 2 つのペインの間に表示されます。 ツールバー上にあるオプションを使用して、 Management Device に関連するさまざまな操作を実行することができます。
ツールバーによって任意の操作を実行するには、上のペインで Management Device 列を選択する必要があります。



ご注意： 各種の操作を行うために使用可能なオプションは、ログインしたユーザーの役割によって異なります。

特定のデバイスに対してデバイステンプレートの設定を変更する場合は、デバイスのプロパティで行います。

次の表は、 Management Devices タブの上部ペインに表示されるフィールドの説明を示します。

フィールド	説明
名前	Management Device のユーザー定義名。
MAC アドレス	デバイスが使用する IEEE802.11 PHY モードの固有の 48 ビットアドレス。
IP アドレス	デバイスの IP アドレス。
ケイパビリティ	使用される IEEE802.11 のプロトコル（IEEE802.11a、IEEE802.11b のみ、IEEE802.11b/g または IEEE802.11a/b/g（IEEE802.11n 機能有無））。
モデル	Management Device のモデル番号。
ロケーション	Management Device のロケーション。
ビルド	ファームウェアのビルド番号。
アップ/ダウン	Management Device がアップ/ダウンしてからの日付と時刻。
監視対象の VLAN	現在の監視対象の VLAN の総数。
デバイステンプレート	Management Device に適用されたデバイステンプレート。
コンフィグレーションステータス	デバイス固有のカスタマイズを許可されたデバイスにアイコンが表示されます。
動作モード	現在の動作モードが表示されます。
AP モード	AP モードの場合は有効と表示されます。
メッシュモード	メッシュモードが設定されている場合は有効と表示されます。
Device Tag	デバイスのプロパティにあるデバイスタグに記載した内容が表示されます。

デバイスプロパティ

次の表は、デバイスのプロパティについて説明します。

フィールド	説明
現在のアクティブ状態	Management Device の状態。 **Yes** はデバイスがアクティブで、**No** はデバイスが非アクティブであることを指しています。
名前	Management Device の名前。
MAC アドレス	Management Device が使用する IEEE802.11 PHY モードの固有の 48 ビットアドレス。
デバイスタグ	Management Device に関する追加情報を提供するテキスト。
運用する国	Management Device を運用する国。
モデル	Management Device のモデル番号。
IP アドレス	Management Device の IP アドレス。
デバイステンプレート	Management Device に適用したデバイステンプレート。
ロケーション	Management Device のロケーション。
フロアマップ上に配置？	Management Device がロケーションのレイアウトに配置されているかどうかを示す。
アップ/ダウン	Management Device がアップ/ダウンしてからの日付と時刻。
チャネルスキャン機能 (a)	Management Device がスキャンするように設定されている IEEE802.11a チャネル。このフィールドは、Management Device を運用する国に基づいて設定されます。
チャネル防御機能 (a)	Management Device が防御するように設定されている IEEE802.11a チャネル。 このフィールドは、Management Device を運用する国に基づいて設定されます。
チャネルスキャン機能 (b/g)	Management Device がスキャンするように設定されている IEEE802.11 b/g チャネル。 このフィールドは、Management Device を運用する国に基づいて設定されます。
チャネル防御機能 (b/g)	Management Device が防御するように設定されている IEEE802.11 b/g チャネル。このフィールドは、Management Device を運用する国に基づいて設定されます。

チャネルスキャン機能 (Turbo a)	Management Device がスキャンするように設定されている Turbo IEEE802.11a チャネル。 このフィールドは、Management Device を運用する国に基づいて設定されます。Turbo モードとは特定のアクセスポイントでサポートしている機能です。
チャネルスキャン機能 (Turbo b/g)	Management Device がスキャンするように設定されている Turbo IEEE802.11 b/g チャネル。 このフィールドは、Management Device を運用する国に基づいて設定されます。Turbo モードとは特定のアクセスポイントでサポートしている機能です。
ソフトウェアのビルド	デバイス上のソフトウェアのビルド番号。
最初に検出された日時	サーバーによって Management Device が最初に検出された日付と時刻。
動作モード	デバイスが現在動作しているモード。 Management Device は、それに適用されるデバイステンプレートに応じて、AP またはセンサーのいずれかとして動作することが可能です。
ケイパビリティ	Management Device が使用する IEEE802.11 プロトコル。
設定された SSID	Management Device の無線に設定された SSID。
デバイス固有のカスタマイズ	動作チャネルとカスタム送信出力のカスタマイズをします。この設定はデバイステンプレートでデバイス固有のカスタマイズを許可チェックボックスにチェックを入れている場合のみ表示されます。詳細については、デバイステンプレートの設定をカスタマイズ を参照してください。
追加の VLAN モニタリング	追加の VLAN の監視設定をカスタマイズする。 監視する追加の VLAN をカスタマイズすることができ、デバイスごとにモニタされる追加の VLAN をオーバーライドし、設定することができます。 監視対象の VLAN をカスタマイズするには、ここでダブルクリックします。 詳細については、デバイステンプレートの設定をカスタマイズ を参照してください。

デバイスのプロパティの編集

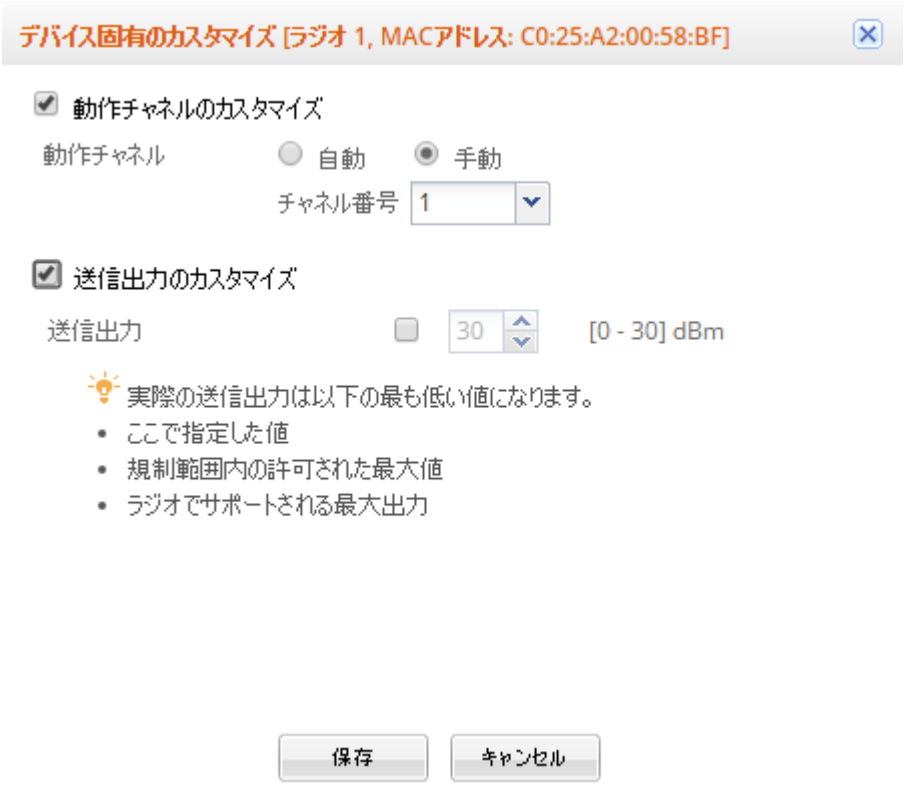
いくつかのデバイスのプロパティは編集可能です。 デバイスのプロパティを編集するには、それをダブルクリックして編集し、新しい値を保存します。

デバイステンプレートの設定をカスタマイズ

デバイステンプレートを定義する際に、**デバイス固有のカスタマイズを許可**のチェックボックスにチェックを入れている場合は、 デバイステンプレートを介してデバイスに適用したいくつかの設定をカスタマイズしオーバーライドすることができます。 デバイスのデバイスプロパティ内にあるラジオ設定と追加の VLAN モニタリングをカスタマイズすることが可能です。
デバイスプロパティのラジオ設定を変更することで、AP モードで動作している Management Device のラジオ設定をカスタマイズすることができます。

これらの設定は、Management Device に適用デバイステンプレートを使用して実行する設定をオーバーライドします。

ラジオ設定をカスタマイズするには、次の手順を実行します。
1. **デバイス**をクリックします。
2. **Management Devices** タブを選択します。
3. **デバイスのプロパティ**へ移動します。
4. **デバイスのプロパティ**内の**ラジオ設定デバイス固有のカスタマイズ** を選択します。 無線の動作チャネルおよび(または)送信出力を変更することができます。



Management Device のラジオ設定をカスタマイズ

動作チャネルを設定するには、次の手順を実行します。
1. **動作チャネルのカスタマイズ** のチェックボックスを選択します。
2. チャネルの自動選択をしたい場合は **自動**を選択し、 **選択間隔**で時間単位のチャネルの選択間隔を指定します。
3. チャネル設定を手動で行いたい場合は**手動**を選択し、**チャネル番号**を選びます。

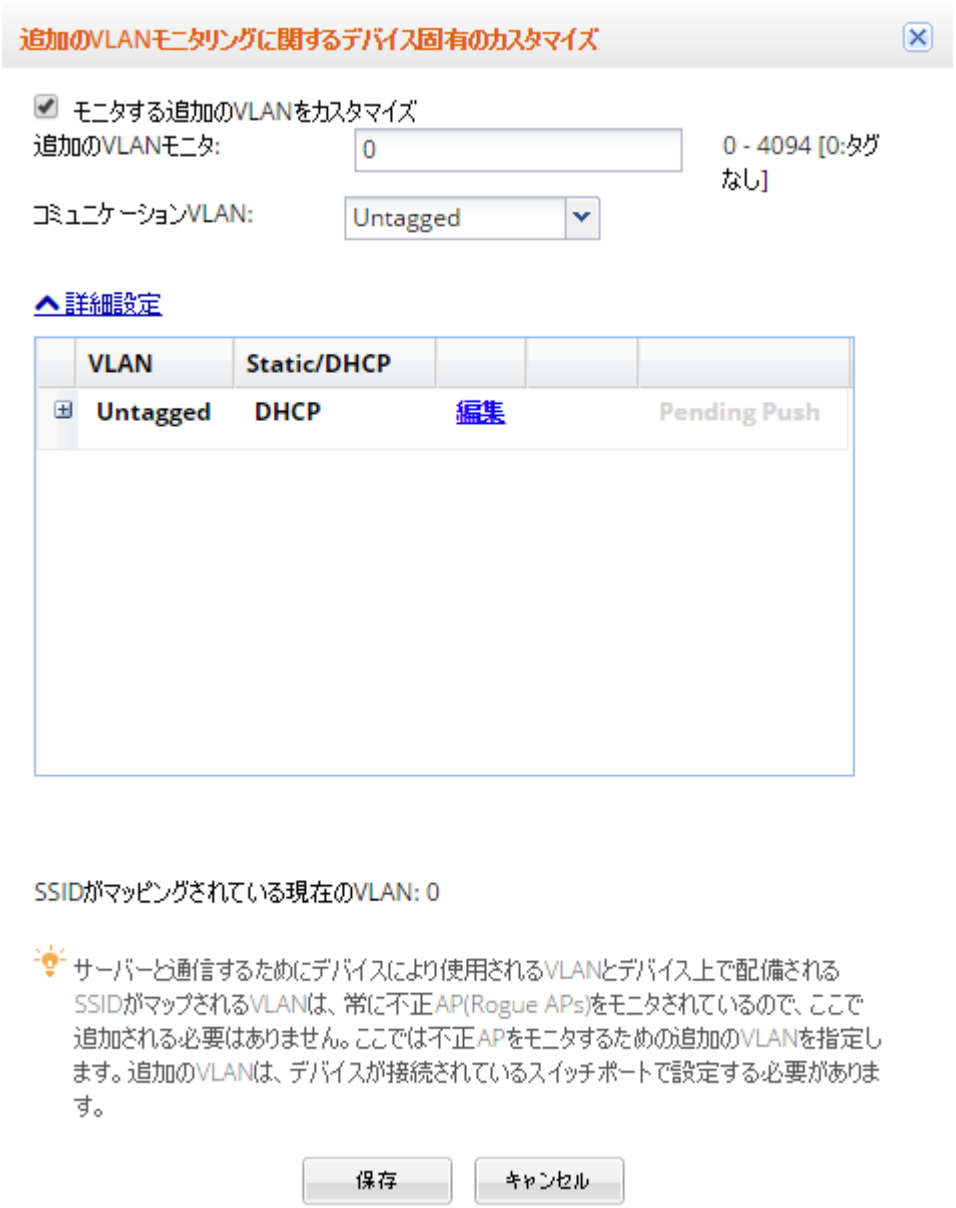
ご注意： メッシュ用の無線の動作チャネルを変更することはできません。

送信出力を変更するには、次の手順を実行します。

1. **送信出力のカスタマイズ**のチェックボックスを選択します。
2. **送信出力**の横にあるチェックボックスを選択し、値を入力します。 **送信出力** の横にあるチェックボックスを選択しない場合、その値は AP の動作する国の許可される最大送信出力に設定されています。

モニタする追加の VLAN を設定するには、次の手順を実行します。

1. 追加の VLAN モニタリングを設定したいデバイスを選択します。
2. **デバイスプロパティ** の追加の VLAN モニタリングをクリックします。 **追加の VLAN モニタリングに関するデバイス固有のカスタマイズ** が表示されます。



3. **モニタする追加の VLAN をカスタマイズ** チェックボックスをクリックします。
4. カンマ区切りのリストとして、監視対象の追加の VLAN を指定します。
5. 必要に応じて、コミュニケーション VLAN を変更します。 0 がコミュニケーション VLAN です。ただし、コミュニケーション VLAN として別の番号を指定することができます。
   ご注意： コミュニケーション VLAN は UI から設定されたあとは、CLI から変更することはできません。UI から誤ったコミュニケーション VLAN を設定し、それを変更したい場合は、まず管理デバイス(Management Device)を工場出荷時の状態にリセットして、 正しいコミュニケーション VLAN を設定する必要があります。
6. 追加の VLAN モニタリングのプロパティを編集することや、AP または WIPS センサーにこれらの VLAN の IP 設定を再設定するには、**詳細設定**をクリックします。
   a) VLAN の VLAN プロパティを編集するには、**編集**をクリックします。必要に応じて、静的または DHCP にアドレス指定メカニズムを変更し、変更を保存します。そのあと、追加の VLAN モニタリングに関するデバイス固有のカスタマイズのウィンドウを閉じます。
   b) Management Device に追加の VLAN モニタリングの修正された IP 設定を再プッシュするには、デバイスのプロパティー追加の VLAN モニタリングをクリックして、**Repush** をクリックし、**保存**をクリックします。 再プッシュをキャンセルしたい場合は、**保存**をクリックする前に**キャンセル**をクリックします。 リンク上のテキストは、Management Device から応答を受信するまで再プッシュの保留に変化します。
   c) **詳細設定**に**削除**リンクを持ついくつかの VLAN が表示される場合があります。 これらは以前の追加の VLAN モニタリングです。 監視対象リストからこれらを削除する必要があります。
7. デバイスへの追加の VLAN モニタリングの設定を保存するためには、 **デバイスのプロパティ**上の**追加の VLAN モニタリング**下の **Save** をクリックします。

可視 LAN の閲覧

可視の VLAN セクションでは、選択された Management Device が WIPS センサーとして動作している場合に、 認識できる LAN の一覧を閲覧することができます。 VLAN ID、IP アドレス、ネットマスク、およびステータスなどの VLAN の詳細が表示されます。 センサーがサーバーとの通信に使用する VLAN には、アスタリスク（*）を付けています。

可視 AP の閲覧

可視の AP セクションを表示するには、デバイスリストの下にある  をクリックします。 **可視の AP** セクションでは、選択された Management Device が WIPS センサーとして動作している場合に、 認識できる AP の一覧を閲覧することができます。 名前、センサーで受信された RSSI 値のような AP の詳細が表示されます。

可視クライアントの閲覧

可視のクライアントセクションを表示するには、デバイスリストの下にある  をクリックします。 **可視のクライアント**セクションでは、関連付けされているか、 または選択された Management Device によって認識できるクライアントの一覧を閲覧することができます。 名前、センサーで受信された RSSI 値のようなクライアントの詳細が表示されます。

アクティブな AP の閲覧

アクティブな AP セクションでは、チャネル上で過去 12 時間にわたってアクティブな AP のグラフを表示するために、 チャネル番号を選択することができます。 上部のペインで選択される Management Device で認識できる AP がここで表示されます。

アクティブなクライアントの閲覧

アクティブなクライアントセクションでは、チャネル上で過去 12 時間にわたってアクティブなクライアントのグラフを表示するために、 チャネル番号を選択することができます。 上部のペインで選択される Management Device で認識できるクライアントがここで表示されます。

Management Device イベントの閲覧

イベントセクション下では、Management Device に関連するイベントを見ることができます。

チャネル占有率を閲覧

チャネル占有セクション下では、選択された時間に基づいてさまざまなチャネル上のアクティブな AP およびアクティブなクライアントのグラフィック表示を閲覧することができます。 チャネル占有率を表示したい時間数を選択するためには時間間隔をクリックします。
選択された帯域と時間に基づいてチャネルマップを棒グラフの形式で表示するにはチャネルマップをクリックします。

干渉の閲覧

干渉セクションでは、チャネル上で過去 12 時間にわたって受けた干渉のグラフを表示するために、チャネル番号を選択することができます。 ここで表示される干渉は、上部のペインで選択される Management Device で認識できるものになります。

メッシュネットワークリンクの閲覧

これは、選択された Management Device がメッシュ無線ネットワークの要素の場合だけ関連します。

1. **デバイス**をクリックします。
2. **Management Devices** タブを選択します。
3. 選択された管理デバイス(Management Device)に関するメッシュネットワークのリンクを表示するには、デバイスリストの下にある  をクリックします。
4. メッシュネットワークトポロジ内の選択された Management Device の AP の直接の親のアクセスポイント(AP)が **Up Link** に表示されます。 選択したデバイスの親のデバイス名と RSSI が **Up Link** に表示されます。 メッシュネットワークトポロジ内の子ノードとして、選択されたアクセスポイント(AP)に接続されているアクセスポイント(AP)が **Down Links** に表示されます。 選択したデバイスの子ノードのデバイス名と RSSI が **Down Links** に表示されます。

Management Device の検索

検索文字列に名前または MAC アドレスを使用して Management Device を検索することができます。 それらの名前または MAC アドレスで検索文字列または部分文字列を持っているすべての Management Device が表示されます。

1 つまたは複数の Management Device を検索するには、次の手順を実行します。
1. **デバイス**をクリックします。
2. **Management Devices** タブを選択します。
3. 右上の隅にある **クイックサーチ**ボックスに名前または MAC アドレスを入力します。
4. 検索文字列が表示され、一致する Management Device の検索結果が表示されます。

Management Device の並べ替え

昇順または降順にタブの列を並べ替えることができ、表示される列を選択することができます。 デバイスリストの列をポイントし、並べ替えるために列の上で をクリックするか、表示する列を選択します。

ロケーションの変更

デバイスのロケーションを変更するには、次の手順を実行します。
1. **デバイス**をクリックします。
2. **Management Device** タブを選択します。
3. デバイスリストから、Management Device を選択します。
4. ロケーション変更アイコンをクリックします。 ロケーションの選択ダイアログボックスが表示されます。
5. Management Device の新しいロケーションを選択します。
6. OK をクリックします。 デバイスは、新しいロケーションに移動されます。

ロケーションの **Management Device** 情報を印刷

上部ペイン内のすべての Management Device で表示されるすべての情報を印刷することができます。 それらを選択することで UI 上に表示される列を選択することが可能です。 上部ペインに表示される情報は、プリントアウトで見ることができる情報です。

paginated view が有効になっている場合は、現在のページの Management Device のリストが印刷されます。ロケーションのすべての Management Device のリストを印刷するには、各ページに移動し個々のページを印刷する必要があります。

paginated view が無効になっている場合は、UI 上に見える Management Device のリストのみが印刷されます。これは 25 レコードが存在し、UI 上に最初の 5 つが示されている場合、これらの 5 つのレコードが印刷されることを意味します。

印刷する前に paginated view を有効または無効にする必要があります。

ロケーションの Management Device リストを印刷するには、次の手順を実行します。
1. **デバイス**をクリックして、**Management Devices** タブをクリックします。
2. ロケーションを選択します。
3. 印刷される列を選択します。 列の選択または解除するには、任意の列名をクリックします。
4. 印刷アイコンをクリック。 Management Device リストの印刷プレビューが表示されます。
5. リストを印刷するには、**印刷** をクリックします。

デバイステンプレートの変更

Management Device のデバイステンプレートを変更するには、次の手順を実行します。
1. **デバイス**をクリックします。
2. **Management Device** タブを選択します。
3. デバイスリストから、Management Device を選択します。
4. ツールバー上にあるデバイステンプレートの変更アイコンをクリックします。**デバイステンプレートの変更** が表示されます。
5. デバイステンプレートの利用可能なリストからデバイステンプレートを選択します。
6. 変更を保存するために、**保存** をクリックします。

デバイスの再起動

Management Device を再起動するには、次の手順を実行します。
1. **デバイス**をクリックします。
2. **Management Device** タブを選択します。
3. デバイスリストから Management Device を選択します。
4. ツールバー上にある 更に>リブートアイコンをクリックします。 再起動の確認メッセージが表示されます。
5. デバイスを再起動するには、**Yes** をクリックします。 デバイスを再起動したくない場合は、**No** をクリックします。

デバイスのトラブルシューティング

アクティブな Management Device は自身をトラブルシューティングすることができます。 アクティブな Management Device に対して、パケットレベルモードでトラブルシューティングを行うことができます。
トラブルシューティングをはじめるには、管理コンソール(Management Console)を起動するために使用されるコンピューターから、Management Device が到達可能であることを確認する必要があります。

Wireshark（または使用可能な他のツール）のようなパケットキャプチャツールを使用してトラブルシューティングを行うことができます。

別の方法として、管理コンソールサーバーにパケットトレースの履歴を保存することができ、あとの参考のために履歴ファイルをダウンロードすることができます。 パケットトレースの履歴は .pcap ファイルとして保存されます。 これは Wireshark などを使用して表示することが可能です。

トラブルシューティングセッションは自動的にタイムアウトするか、アクティビティにかかわりなく指定されたタイムアウト後に停止します。 手動でトラブルシューティングセッションを終了するには、このセクション内の'トラブルシューティングの停止'サブセクションを参照してください。

ローカルマシン上の **Wireshark** などを使用して **Management Device** をトラブルシューティング

Management Device のトラブルシューティングを行うには、次の手順を実行します。
1. **デバイス**をクリックします。
2. **Management Devices** タブを選択します。
3. トラブルシューティングを行う Management Device のチェックボックスにチェックを入れます。
4. ツールバー上にある**更に>パケットキャプチャ** をクリックします。
5. **トラブルシューティングモード**の下にある**ライブパケットキャプチャ**を選択します。
6. **ストリーミングオプション**で**ローカルマシン上の Wireshark/ Other** を選択します。
7. **タイムアウト**にタイムアウト間隔を指定します。 パケットレベルのトラブルシューティングモードのデフォルトのタイムアウトは 5 分です。 タイムアウトの最小値は 1 分で、最大値は 720 分です。
8. パケットタイプを選択します。 特定のパケットタイプをキャプチャしたい場合は、フィルターを選択してトラブルシューティング時にキャプチャが必要なデータフレームおよび(または)管理フレームを選択します。
9. **プロトコルとチャネル選択** セクションでは、トラブルシューティングの対象となるプロトコルおよびチャネルを選択します。 単一のチャネルを選択したい場合は、**チャネルを選択**で、チャネル番号と **Width**（チャネルオフセット）を指定します。 デフォルトでは、プロトコルおよびチャネルはトラブルシューティングのセンサーに適用されるデバイステンプレートに基づいて表示されます。 必要に応じて、異なるプロトコルおよび(または)チャネルを選択することができます。 また、すべての有効なチャネルをトラブルシューティングするには、**全チャネル**を選択することが可能です。
10. トラブルシューティングを開始するには、**トラブルシューティング開始** をクリックします。 センサーは、ライブパケットをキャプチャすることが可能となります。
11. ライブパケットキャプチャのために適切なツールを選択します。 ツールがインストールされていない場合は、Wireshark か他のツールをダウンロードすることができます。

12. パケットキャプチャを表示するには、使用するツールに応じて Wireshark 下に示したコマンドを、お使いのコンピューターにインストールされているオペレーティングシステムのコマンドラインインタフェースを開いて実行します。 **パケットレベルモードのトラブルシューティング**では、Wireshark に対して実行するコマンドのガイドラインを提供します。 下記の図では、Wireshark では、rpcap はプロトコル、192.168.1.102 はトラブルシュートする Management Device の IP アドレス、そして atn0 はインタフェースになります。 コマンドライン上で実際に Wireshark コマンドを実行する際は、適切な Management Device の IP アドレスを入力します。

パケット履歴を管理コンソールサーバーにアップロードする **Management Device** のトラブルシューティング

Management Device のトラブルシューティングを行うには、次の手順を実行します。
1. **デバイス**をクリックします。
2. **Management Devices** タブを選択します。
3. トラブルシューティングを行う Management Device のチェックボックスにチェックを入れます。
4. ツールバー上にある**更に>パケットキャプチャ** をクリックします。
5. **トラブルシューティングモード**の下にある**ライブパケットキャプチャ**を選択します。
6. **ストリーミングオプション**で **サーバーにアップロード** を選択します。
7. **ファイル名のプレフィックス**にファイル名に適したプレフィックスを入力します。 これはパケット履歴をダウンロードすると際に、トラブルシューティングのファイルを識別するのに役立ちます。
8. **タイムアウト**にタイムアウト間隔を指定します。 パケットレベルのトラブルシューティングモードのデフォルトのタイムアウトは 5 分です。 タイムアウトの最小値は 1 分で、最大値は 720 分です。
9. パケットタイプを選択します。 特定のパケットタイプをキャプチャしたい場合は、フィルターを選択してトラブルシューティング時にキャプチャが必要なデータフレームおよび(または)管理フレームを選択します。
10. **プロトコルとチャネル選択** セクションで、トラブルシューティングの対象となるプロトコルおよびチャネルを選択します。 単一のチャネルを選択したい場合は、**チャネルを選択**で、チャネル番号と **Width**（チャネルオフセット）を指定します。 デフォルトでは、プロトコルおよびチャネルはトラブルシューティングのセンサーに適用されるデバイステンプレートに基づいて表示されます。 必要に応じて、異なるプロトコルおよび(または)チャネルを選択することができます。 また、すべての有効なチャネルをトラブルシューティングするには、**全チャネル**を選択することが可能です。
11. トラブルシューティングを開始するには、**トラブルシューティング開始** をクリックします。 センサーは、ライブパケットをキャプチャすることが可能となります。

トラブルシューティングの停止

トラブルシューティングセッションは自動的にタイムアウトするか、アクティビティにかかわりなく指定されたタイムアウト後に停止します。 手動でトラブルシューティングセッションを終了することができます。

手動でアクティブなトラブルシューティングセッションを停止するには、次の手順を実行します。
1. 右上の隅にある通知アイコンをクリックします。アクティブなトラブルシューティングセッションが存在する場合は、他の通知と一緒に表示されます。
2. アクティブなトラブルシューティングセッションの通知をクリックします。 センサーのトラブルシューティングセッションのリストが表示されます。
3. 終了するトラブルシューティングセッションのチェックボックスを選択します。
4. **停止**をクリック。 トラブルシューティングセッションが終了し、トラブルシューティングセッションの終了を示すメッセージが表示されます。 **トラブルシューティングモード**で**ストリーミング**として**サーバーにアップロード**が選択されている場合、パケットトレース履歴は管理コンソールサーバーにアップロードされています。

パケットキャプチャのダウンロード

トラブルシューティング停止後、管理コンソールサーバーは 30 分間トラブルシューティング・インスタンスのパケットキャプチャ履歴を保持します。

この履歴は、ダウンロードして、今後の参考のために保存することができます。 パケットトレースの履歴は .pcap ファイルとして保存されます。

パケットトレースファイルをダウンロードするには、次の手順を実行します。
1. ロケーションツリーから要求するロケーションを選択します。
2. **デバイス**をクリックします。
3. **Management Devices** タブを選択します。
4. ツールバー上にある**更に>Packet Capture and Connections History** をクリックします。 **過去のパケットキャプチャー覧** が表示されます。 ファイル名、ファイルサイズ(KB)、トラブルシューティング開始時間および停止時間を持つリストが表示されます。
5. ダウンロードするパケットトレースの**ダウンロード**リンクをクリックして、パケットトレースを保存するパスを選択してください。 パケットトレースファイルは指定された場所に保存されます。

パケットキャプチャファイルの削除

トラブルシューティング停止後、管理コンソールサーバーは 30 分間トラブルシューティング・インスタンスのパケットキャプチャ履歴を保持します。
サーバーからこのパケットキャプチャの履歴を削除することができます。パケットキャプチャファイルは.pcap フォーマットで提供されています。

パケットキャプチャファイルを削除するには、次の手順を実行します。
1. ロケーションツリーから要求するロケーションを選択します。
2. **デバイス**をクリックします。
3. **Management Devices** タブを選択します。
4. ツールバー上にある**更に>Packet Capture and Connections History** をクリックします。 **過去のパケットキャプチャー覧** が表示されます。 ファイル名、ファイルサイズ(KB)、トラブルシューティング開始時間および停止時間を持つリストが表示されます。
5. 削除するログファイルのチェックボックスにチェックを入れます。 削除する複数のファイルを一度に選択することができます。
6. アイコンをクリックします。削除を確認するメッセージが表示されます。
7. 選択したファイルの削除を実行するには、**Yes** をクリックします。

デバイスのアップグレード

デバイスをアップグレードまたは修復するには、次の手順を実行します。
アップグレードはデバイスのソフトウェアバージョンが古い場合など、アップグレードが必要な場合にのみ実行できます。
1. **デバイス**をクリックします。
2. **Management Devices** タブを選択します。
3. 同じモードで動作する 1 つ以上のデバイスを選択します。
4. ツールバー上にあるソフトウェアのアップグレードアイコンをクリックします。
5. **アップグレード**を選択します。

オプション	説明
アップグレード	デバイスを新しいソフトウェアバージョンにアップグレード。

カスタムフィルターの追加

カスタムフィルターを作成し、任意の名前で保存することができます。 管理コンソール(Management Console)上に表示される任意の列を選択することができ、列内のデータ上でフィルターをセットすることが可能です。 名前を付けてこのフィルターを保存することができます。このようにして複数のフィルターを作成することができます。

カスタムフィルターを使用する際は、次の点に注意してください。

- 列の可視性と列のデータのソートの初期設定は、カスタムフィルターには保存されません。フィルター基準のみが保存されます。
- カスタムフィルターは、ユーザー固有のものです。これらは、カスタムフィルターを定義したユーザー用に保存され、他のユーザーには見えません。
- 保存されていないフィルターは、ツールバーの**フィルター**の隣にあるフィルター名の横にアスタリスクで示されます。
- ユーザーがフィルターを保存せずにログアウトした場合、保存されていないフィルターは保存されません。

カスタムフィルターを作成するには、次の手順を実行します。
1. **デバイス> Management Devices** へ移動します。
2. 列のヘッダーの横にある アイコンをクリックします。オプションのリストが表示されます。
3. **Filters** にマウスのポインタを合わせて、列のフィルターテキストを入力します。
4. ツールバー上の **フィルター**の隣にある アイコンをクリックして、**名前を付けて保存**をクリックします。 **名前を付けて保存**ダイアログボックスが表示されます。
5. フィルターの名前を入力し、**OK** をクリックします。カスタムフィルターが保存されます。

カスタムフィルターの編集

カスタムフィルターを編集するには、次の手順を実行します。
1. **デバイス> Management Devices** へ移動します。
2. ツールバー上の **フィルター**の隣にある アイコンをクリックして、要求するフィルターを選択します。
3. 列のヘッダーの横にある アイコンをクリックします。オプションのリストが表示されます。
4. **Filters** にマウスのポインタを合わせて、列にフィルターテキストを入力するか、必要に応じてフィルター条件を変更します。
5. ツールバー上の **フィルター**の隣にある アイコンをクリックして、**保存**をクリックします。 変更されたカスタムフィルターが保存されます。

カスタムフィルターの削除

カスタムフィルターを削除するには、次の手順を実行します。
1. **デバイス> Management Devices** へ移動します。
2. ツールバー上の **フィルター**の隣にある アイコンをクリックして、フィルターを削除するために アイコンをクリックします。 削除を確認するメッセージが表示されます。
3. カスタムフィルターの削除を実行するには、**Yes** をクリックします。

デバイスの削除

Management Device を削除するには、次の手順を実行します。

1. **デバイス**をクリックします。
2. **Management Devices** タブを選択します。
3. 削除する Management Device を選択します。
4. ツールバー上にある**更に>削除** をクリックします。
5. 削除を実行するには、**Yes** をクリックします。

クライアントの監視

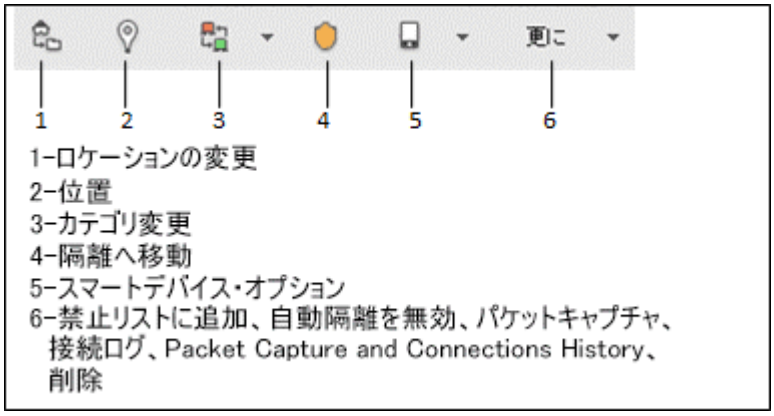
デバイス>Clients タブには、選択したロケーションに関連付けられているすべてのクライアントが表示されます。

選択されたロケーションで許可、ゲスト、不正、外部、未分類の AP リストを表示するには、**Authorized**、 **Guest**、 **Rogue**、 **External**、 **Uncategorized** のカテゴリから選択します。 一度に複数のカテゴリを選択することが可能です。 すべてのカテゴリよりクライアントを表示するには、**All** を選択します。

Clients タブは、水平に 2 つのペインに分割されています。 上部のペインには、選択したロケーションのクライアントリストが表示されます。 下部のペインには、**Clients** タブの上部ペインで選択したクライアントに関連したクライアントのプロパティが表示されます。 許可、不正、外部および未分類のクライアントの場合は、選択されたクライアントに関連付けられている最近のアソシエイトした AP またはアドホックネットワークのリストを閲覧することができます。

許可クライアントの場合は、下のペインに、クライアントのトラフィック、クライアントの平均データレートを閲覧することができます。

下のイメージに示すように、ツールバー上にあるオプションを使用してクライアントに関連するさまざまな操作を行うことができます。



ツールバーによって任意の操作を実行するには、上部ペインのクライアント行を選択する必要があります。 いくつかの操作では複数のクライアントを選択することができます。

ご注意： 各種の操作を実行するために使用可能なオプションは、ログインしたユーザーの役割によって異なります。

無線メッシュネットワーク内でメッシュ AP をアップリンクに接続されている非ルートメッシュ AP の無線ステーション仮想 AP はクライアントとして表示されます。 これらはデフォルトで、許可（Authorized）に分類されます。 これらのクライアントのカテゴリを変更することはできません。 隔離または自動的にこのようなクライアントを禁止することはできません。 したがって、ツールバーの **'更に'** の下にあるオプションは、そのようなクライアントでは無効になっています。

Clients タブの上部ペインの列を昇順または降順に並べ替えることができ、表示される列を選択することができます。 列をポイントし並べ替えるために をクリックします（表示する列を選択する）。 あるいは、選択された列のテキストと一致するフィルターテキストに基づいて表示されるデータをフィルターします。

右上の**クイックサーチ** ボックスに名前、MAC アドレスを入力しクライアントを検索することが可能です。

ページサイズを設定するには ページサイズのセットをクリックします。
次の表は、**Clients** タブの上部ペインに表示されるフィールドの説明を示します。

フィールド	説明
RSSI	クライアントの観測された RSSI（Received Signal Strength Indicator）の値を表示します。
スマートデバイスタイプ	スマートデバイスタイプを示します。
名前	クライアントのユーザー定義名を示します。
MAC アドレス	クライアントの MAC 固有アドレスを示します。
ベンダー	クライアントのメーカーを示します。 ベンダー名は、MAC アドレスの最初の 3 バイトから推測されます。
ロケーション	クライアントのロケーションを示します。
アソシエイトした AP	クライアントがアソシエイトしている AP を示します。 この AP を介して、クライアントは他のクライアントや他のネットワークと通信します。
プロトコル	クライアントがアソシエイトしている AP によって使用される IEEE802.11 プロトコル（IEEE802.11n 機能の有無で）を示します。
SSID	クライアントがアソシエイトしている AP の SSID を示します。
アップ/ダウン	クライアントがアップ/ダウンしてからの日付と時刻を示します。
セル ID	アドホックモードのクライアントの ID を示します。 セル ID は、単一のアドホック接続を形成するすべてのクライアントで共通です。
IP アドレス	クライアントの IP アドレスを示します。
ユーザー名	クライアントにログオンしたユーザーID を示します。

クライアントのプロパティを表示

いくつかのクライアントのプロパティは編集可能です。 クライアントプロパティの値の右側に表示される鉛筆のアイコンは、プロパティが編集可能であることを示します。 クライアントのプロパティを編集するには、それをダブルクリックして編集し、新しい値を保存します。

次の表では、クライアントプロパティのフィールドごとの説明を示します。

フィールド	説明
現在のアクティブ状態	クライアントが現在アクティブかどうか示します。 Yes はクライアントがアクティブで、No はクライアントが非アクティブであることを指しています。
クライアント名	クライアントのホスト名を示します。
ユーザー名	クライアントにログオンしたユーザーID を示します。
分類	クライアントが 許可（Authorized）、ゲスト（Guest）、 不正（Rogue） 外部（External）として分類されているかどうかを示します。 Uncategorized は、クライアントが分類されていないことを示します。
デバイスタグ	クライアントに関する追加情報を提供します。
ロケーション	クライアントのロケーションを示します。
アップ/ダウン	クライアントがアクティブ/非アクティブになった時間を示します。
スマートデバイス	クライアントがスマートデバイスであるかどうかを示します。*Yes* は、クライアントがスマートデバイスであることを示し、*No* は、クライアントがスマートデバイスでないことを示しています。
動作モード	クライアントが AP（インフラストラクチャモード）またはピアツーピアネットワーク（アドホックモード）に接続されているかどうかを示します。
アドホック セル ID	選択したクライアントがメンバーとなっているアドホックネットワーク接続の一意の ID を示します。
IP アドレス	クライアントの IP アドレスを示します。
ベンダー	クライアントのメーカーを示します。 ベンダー名は、MAC アドレスの最初の 3 バイトから推測されます。
プロトコル	クライアントが現在動作している IEEE802.11 プロトコルを示します。
チャネル	クライアントが動作するチャネル番号を示します。
セキュリティ	AP に適用されるセキュリティ規格を示します。 これは、AP に適用されたテンプレートより取り出されます。
ネットワーク	クライアントが配置されているネットワークを識別する IP アドレスとサブネットの追加情報を表示します。
アソシエイトした AP	クライアントが関連付けられている AP の BSSID を指定します。このフィールドは、マージされた AP のみ表示されます
最初に検出された日時	システムによってクライアントが最初に検出された日付と時刻を示します。

最近の AP/アドホックネットワークへのアソシエイト

最近の AP/アドホックネットワークへのアソシエイト では、クライアントがアソシエイトした AP/アドホックネットワークのリストを閲覧することができます。 AP/アドホックネットワークのアクティブ/非アクティブアイコン、AP 名/アドホック ID、SSID、最後の検出などの詳細は、同じ行に表示されます。

クライアントに関連するイベント

イベント下では、クライアントに関連するすべてのイベントを見ることができます。 イベント ID、イベントの説明、イベントの開始時間、イベント停止時間が表示されます。

クライアント再送レート・トレンド

このウィジェットは、許可クライアントでのみ表示されます。 時間間隔を選択し、選択された時間間隔にわたるクライアントの再送率の傾向をグラフィカルに表示することができます。

クライアントを認識しているデバイス

クライアントを認識しているデバイスでは、 選択したクライアントを検出したアクティブなデバイスを閲覧できます。 デバイス名とデバイスの RSSI 値をこのセクションで見ることができます。 このセクションは、すべてのタイプのクライアントが取り込まれます。

クライアント・平均データレート

クライアントの平均データレートは許可クライアントに対してのみ見ることができます。 クライアントを認識している管理デバイス(Management Device)は、AP の BSS 内のデータフレームにある送信レートの追跡を続け、 15 分おきに加重した平均送信レートをレポートします。

クライアント・トラフィック

クライアントのトラフィックは許可クライアントに対してのみ見ることができます。 クライアントを認識している管理デバイス(Management Device)は、15 分おきにクライアントにより送受信されるデータトラフィックをレポートします。 チャネルを順に確認している管理デバイス(Management Device)は、任意のチャネル上で合計時間の数パーセントを費やします。 そのため、デバイスの無線でスキャンされるチャネルの合計数と等しい要因により、このパラメータは実際のトラフィックを通常は過小評価します。 例えば、管理デバイス(Management Device)が全部で 30 のチャネルをスキャンする場合、測定したトラフィックは実際のトラフィックの 1/30 になります。 トラフィックの性質がバースト状態である場合は、そのような単純なスケーリングは適用することはできません。

クライアントのロケーションを変更

選択したクライアントのクライアントロケーションを変更することができます。

クライアントロケーションを変更するには、次の手順を実行します。
1. **デバイス**へ移動します。
2. **Clients** タブを選択します。
3. ロケーションを変更するクライアントを選択します。
4. 'ロケーションの変更' アイコンをクリックします。 '新しいロケーションの選択'が表示されます。
5. クライアントの新しいロケーションを選択します。
6. OK をクリックします。クライアントは新たに選択されたロケーションに移動されます。

クライアントの隔離

クライアントを隔離するには、次の手順を実行します。
1. **デバイス**へ移動します。
2. **Clients** タブを選択します。
3. 隔離するクライアントを選択します。
4. '隔離へ移動' アイコンをクリックします。 隔離を確認するメッセージが表示されます。
5. 選択したクライアントを隔離するには、Yes をクリックします。

自動隔離の無効／侵入防御ポリシーからデバイスを除外

デバイスの自動隔離を無効にすることで、侵入防御ポリシーからデバイスを除外することができます。

自動隔離を無効にするには、次の手順を実行します。
1. **デバイス**へ移動します。
2. **Clients** タブを選択します。
3. 自動隔離を無効にするクライアントを選択します。
4. ツールバー上にある '更に' をクリックします。
5. 自動隔離を無効にするには、'更に'下の自動隔離の無効アイコンをクリックします。 自動隔離を無効にする確認メッセージが表示されます。
6. デバイスの自動隔離を無効にするには、Yes をクリックします。

禁止リストに追加

禁止クライアントリストにクライアントを追加するには、次の手順を実行します。
1. **デバイス**へ移動します。
2. **Clients** タブを選択します。
3. クライアントを選択します。
4. ツールバーにある '禁止リストに追加' アイコンをクリックします。 クライアントは禁止リストに追加されます。

スマートデバイスの分類／解除

スマートデバイスとしてクライアントを分類するには、次の手順を実行します。
1. **デバイス**へ移動します。
2. **Clients** タブを選択します。
3. クライアントを選択します。
4. クライアントをスマートデバイスとして分類／解除するには、ツールバー上にある 'スマートデバイス' アイコンをクリックします。 クライアントがすでにスマートデバイスとしてマークされている場合は、それが承認済みまたは未承認かどうかを指定することができます。
5. スマートデバイスとしてクライアントを分類するには、**スマートデバイスである** 選択します。スマートデバイスの分類を解除するには、**スマートデバイスでない** 選択します。

クライアントのカテゴリを変更

クライアントのカテゴリを変更するには、次の手順を実行します。
1. **デバイス**へ移動します。
2. **Clients** タブを選択します。
3. クライアントを選択します。
4. 既存のクライアントのカテゴリを変更するには、ツールバー上の 'カテゴリを変更' アイコンをクリックします。
5. 状況に応じて、 **Authorized**、 **External**、 **Rogue**、 **Guest** から目的のカテゴリを選択します。

クライアントの検出

フロアマップ上のクライアントを見つけるには、次の手順を実行します。
1. **デバイス>Clients** タブへ移動します。
2. フロアマップ上のクライアントを見つけるには 'Locate' アイコンをクリックします。

最近プローブされた **SSID** を表示

最近プローブされた SSID を表示するには、次の手順を実行します。
1. **デバイス>Clients** タブへ移動します。
2. クライアントを選択。
3. 選択したクライアントの最近プローブされた SSID とその詳細を表示するには、下部のペインで '最近プローブされた SSID' ウィジェットに移動します。

クライアントのトラブルシューティング

センサーモードで動作している管理デバイス(Management Device)を使用して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。

トラブルシューティングをはじめるには、管理コンソール(Management Console)を起動するために使用されるコンピューターから、管理デバイス(Management Device)(センサー)が到達可能であることを確認する必要があります。管理デバイス(Management Device)が隔離でビジーまたはトラブルシューティングで使用中の場合、選択したクライアントをトラブルシューティングすることができません。

管理デバイス(Management Device)（センサー）をパケットレベルモードまたはイベントレベルモードでクライアントのトラブルシューティングに用いることが可能です。 このセンサーは Wireshark（または使用できる他のツール）のようなパケットキャプチャツールを使用して、トラブルシューティングを行うことができます。

トラブルシューティングセッションは自動的にタイムアウトするか、アクティビティにかかわりなく指定されたタイムアウト後に停止します。

ご注意： トラブルシューティングセッションが進行中である場合、アクティブなトラブルシューティングセッションに関する通知は、管理コンソール(Management Console)の右上隅にある **通知** で見ることができます。

ご注意： コンソールからパケットキャプチャベースのトラブルシューティングセッションがはじまり、パケットキャプチャツールが中断または（正常または突然に）終了のいずれかになった場合、別のパケットキャプチャセッションを開始する前に、まずはじめに（まだ進行中であれば）手動でコンソールから進行中のトラブルシューティングセッションを停止するか、セッションが本当に終わったことを確認する必要があります。 手動でトラブルシューティングセッションを終了するには、このセクション内の'トラブルシューティングの停止'サブセクションを参照してください。

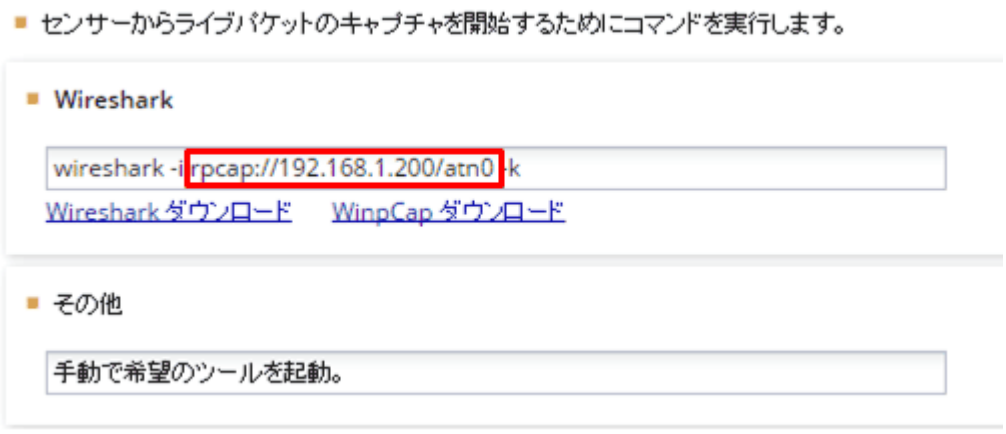
そのあと、コンソールからの新たなトラブルシューティングセッションを再起動することができます。

選択されたツール (Wireshark など)で進行中のトラブルシューティングセッションがある場合、同じまたは他のコンピューターからコマンドプロンプトでユーザー指定のパラメータ（すなわち rpcap://sensor-ip/iface）を使用して他のキャプチャを行っても正常に動作しません。

パケットレベルモードでのクライアントのトラブルシューティング

パケットレベルモードでのクライアントのトラブルシューティングを行うには、次の手順を実行します。

1. **デバイス**へ移動します。
2. **Clients** タブを選択します。
3. トラブルシューティングを行うクライアントのチェックボックスにチェックを入れます。
4. ツールバー上にある**更に>パケットキャプチャ** をクリックします。 クライアントデバイスのトラブルシューティングを行うが表示されます。
5. **ライブパケットキャプチャ**を選択します。
6. **タイムアウト**にタイムアウト間隔を指定します。 パケットレベルのトラブルシューティングモードのデフォルトのタイムアウトは 5 分です。 タイムアウトの最小値は 1 分で、最大値は 720 分です。
7. **トラフィックの選択**でトラブルシューティング中に参照するパケットタイプを選択します。 トラブルシューティングを行うセンサーで認識できるすべてのパケットを表示する場合は、**チャネル上のすべてのパケット**を選択します。 トラブルシューティングを行うセンサーでクライアントからのパケットだけを表示したい場合は、**選択したクライアント <クライアント MAC> のみ** を選択します。
8. センサーとして動作する管理デバイス(Management Device)のリストから、トラブルシューティングを行うために使用するセンサーのチェックボックスを選択します。 デバイスを認知しているセンサーは、それらの可用性と信号強度に基づいてソートされます。
9. **プロトコルとチャネル選択** では、トラブルシューティングの対象となるプロトコルおよびチャネルを選択します。 単一のチャネルを選択したい場合は、**チャネルを選択**で、チャネル番号と **Width**（チャネルオフセット）を指定します。 デフォルトでは、プロトコルおよびチャネルはトラブルシューティングのセンサーに適用されるデバイステンプレートに基づいて表示されます。必要に応じて、異なるプロトコルおよび(または)チャネルを選択することができます。 また、すべての有効なチャネルをトラブルシューティングするには、**全チャネル**を選択することが可能です。
10. トラブルシューティングを開始するには、**トラブルシューティング開始** をクリックします。 センサーは、ライブパケットをキャプチャすることが可能となります。
11. ライブパケットキャプチャのために適切なツールを選択します。 ツールがインストールされていない場合は、Wireshark か他のツールをダウンロードすることができます。
12. パケットキャプチャを表示するには、使用するツールに応じて Wireshark 下に示したコマンドを、お使いのコンピューターにインストールされているオペレーティングシステムのコマンドラインインタフェースを開いて実行します。 **パケットレベルモードのトラブルシューティング**では、Wireshark に対して実行するコマンドのガイドラインを提供します。下記の図では、Wireshark では、rpcap はプロトコル、192.168.1.102 はトラブルシュートするセンサーの IP アドレス、そして atn0 はインタフェースになります。 コマンドライン上で実際に Wireshark コマンドを実行する際は、適切なセンサーの IP アドレスを入力します。



イベントレベルモードでのクライアントのトラブルシューティング

イベントレベルモードでクライアントのトラブルシューティングを行うには、次の手順を実行します。

1. **デバイス**へ移動します。
2. **Clients** タブを選択します。
3. トラブルシューティングを行うクライアントのチェックボックスにチェックを入れます。
4. ツールバー上にある**更に>パケットキャプチャ** をクリックします。 クライアントデバイスのトラブルシューティングを行うダイアログボックスが表示されます。
5. **デバイスに対して新たなイベントを生成**を選択します。
6. **タイムアウト**にタイムアウト間隔を指定します。 イベントレベルのトラブルシューティングモードのデフォルトのタイムアウトは 2 分です。 タイムアウトの最小値は 1 分で、最大値は 5 分です。
7. センサーとして動作する管理デバイス(Management Device)のリストから、トラブルシューティングを行うために使用するセンサーのチェックボックスを選択します。
8. **プロトコルとチャネル選択** セクションでは、トラブルシューティングの対象となるプロトコルおよびチャネルを選択します。 単一のチャネルを選択したい場合は、**チャネルを選択**で、チャネル番号と **Width**（チャネルオフセット）を指定します。 デフォルトでは、プロトコルおよびチャネルはトラブルシューティングのセンサーに適用されるデバイステンプレートに基づいて表示されます。 必要に応じて、異なるプロトコルおよび(または)チャネルを選択することができます。 また、すべての有効なチャネルをトラブルシューティングするには、**全チャネル**を選択することが可能です。
9. トラブルシューティングを開始するには、**トラブルシューティング開始** をクリックします。 トラブルシューティング中にセンサーがイベントを生成します。これらはセンサーの最新のイベントとしてデバイスリストで見ることができます。

トラブルシューティングの停止

トラブルシューティングセッションは自動的にタイムアウトするか、アクティビティにかかわりなく指定されたタイムアウト後に停止します。 手動でトラブルシューティングセッションを終了することができます。

手動でアクティブなトラブルシューティングセッションを停止するには、次の手順を実行します。
1. 右上の隅にある通知アイコンをクリックします。アクティブなトラブルシューティングセッションが存在する場合は、他の通知と一緒に表示されます。
2. アクティブなトラブルシューティングセッションの通知をクリックします。 センサーのトラブルシューティングセッションのリストが表示されます。
3. 終了するトラブルシューティングセッションのチェックボックスを選択します。
4. **停止**をクリック。 トラブルシューティングセッションが終了し、トラブルシューティングセッションの終了を示すメッセージが表示されます。

パケットキャプチャのダウンロード

トラブルシューティング停止後、管理コンソールサーバーは 30 分間トラブルシューティング・インスタンスのパケットキャプチャ履歴を保持します。

この履歴をダウンロードして、今後の参考のためにそれらを保存することができます。 パケットトレースの履歴は .pcap ファイルとして保存されます。

パケットトレースファイルをダウンロードするには、次の手順を実行します。
1. ロケーションツリーから要求するロケーションを選択します。
2. **デバイス**をクリックします。
3. **Clients** タブを選択します。
4. ツールバー上にある**更に>過去のパケットキャプチャ** をクリックします。 **パケットキャプチャ** ダイアログボックスが表示されます。 ファイル名、ファイルサイズ(KB)、トラブルシューティング開始時間および停止時間を持つリストが表示されます。
5. ダウンロードするパケットトレースの**ダウンロード**リンクをクリックして、パケットトレースを保存するパスを選択してください。 パケットトレースファイルは指定された場所に保存されます。

パケットキャプチャファイルの削除

トラブルシューティング停止後、管理コンソールサーバーは 30 分間トラブルシューティング・インスタンスのパケットキャプチャ履歴を保持します。

サーバーからこのパケットキャプチャの履歴を削除することができます。パケットキャプチャファイルは.pcap フォーマットで提供されています。

パケットキャプチャファイルを削除するには、次の手順を実行します。
1. ロケーションツリーから要求するロケーションを選択します。
2. **デバイス**をクリックします。
3. **Clients** タブを選択します。
4. ツールバー上にある**更に>過去のパケットキャプチャ** をクリックします。 **過去のパケットキャプチャ** ダイアログボックスが表示されます。 ファイル名、ファイルサイズ(KB)、トラブルシューティング開始時間および停止時間を持つリストが表示されます。
5. 削除するログファイルのチェックボックスにチェックを入れます。 削除する複数のファイルを一度に選択することができます。
6.  アイコンをクリックします。削除を確認するメッセージが表示されます。

7. 選択したファイルの削除を実行するには、**Yes** をクリックします。

クライアント接続に関する問題をデバッグ

アクセスポイント(AP)への接続に問題がある場合、問題の根本的な原因を見つけるためにクライアント接続のトラブルシューティングを行うことが可能です。 ツールバーにある接続のトラブルシューティングは、無線クライアントが直面する接続の問題をデバッグすることができます。

1 つ以上の管理デバイス(Management Device)またはクライアントの近くにある他の類似デバイスが、バックグラウンドスキャンモードまたはセンサーモードで動作する場合、管理コンソール(Management Console)の**デバイス>Clients** 下でクライアントを検知し認識することができます。
クライアントの近くで動作している管理デバイス(Management Device)または他の類似デバイスでバックグラウンドスキャンが無効にされている、あるいはセンサーがクライアントの近くにない場合、管理コンソール(Management Console)でクライアントを認識できません。
いずれの場合でも、**Devices>Clients** 下のクライアントリストで認識できるかどうかにかかわりなく、クライアントをデバッグすることが可能です。

クライアントが管理コンソール(Management Console)のクライアントリスト下で認識できる場合は、このクライアントを選択して接続の問題をデバッグすることができます。 そうでない場合は、手動でクライアントの MAC アドレスを入力して、このクライアントの接続の問題をデバッグすることができます。

一度に複数のクライアントをトラブルシュートすることが可能です。つまり、あるクライアントで接続のトラブルシューティングが進行中の間、別のクライアントに対してトラブルシューティングセッションを開始することができます。 同時クライアントのトラブルシューティングセッション数に制限はありません。

トラブルシューティングが進行中であるとき、接続ログは管理コンソール(Management Console)上に表示されます。 これは、すぐに問題の正確な原因を見つけることの助けになります。 それは、Wireshark のようなパケットキャプチャツールを補完します。
トラブルシューティングを停止すると、（今後の参考のために）接続ログの履歴をダウンロードすることができます。 これは、テキストファイル（.txt）として保存されます。 接続ログの履歴をダウンロードする方法の詳細については、接続ログのダウンロードを参照してください。

Devices>Clients 下で認識できるデバイスのトラブルシューティングを行うには、次の手順を実行します。
1. ロケーションツリー上の必要なロケーションを選択します。
2. **デバイス**をクリックします。
3. **Clients** タブを選択します。
4. トラブルシューティングするクライアントのチェックボックスにチェックを入れます。
5. ツールバー上の **更に>接続ログ** をクリックします。 **接続ログ** が表示されます。
6. 必要に応じてタイムアウト値を変更します。デフォルトは 5 分です。
7. SSID リストに SSID を入力します。カンマ区切りのリストとして複数の SSID を入力することができます。
8. **AP を表示** をクリックします。AP のリストが表示されます。
9. クライアントが接続を試みる AP を選択します。
10. **トラブルシューティングの開始** をクリックします。 接続ログが表示されます。
11. トラブルシューティングを終了するときは、**トラブルシューティングの停止** をクリックします。トラブルシューティングを停止後に、接続ログ履歴から接続ログファイルをダウンロードすることができます。

Devices>Clients 下で認識できないデバイスのトラブルシューティングを行うには、次の手順を実行します。

1. ロケーションツリー上の必要なロケーションを選択します。
2. **デバイス**をクリックします。
3. **Clients** タブを選択します。
4. ツールバー上の **更に>接続ログ** をクリックします。 **接続ログ** のダイアログボックスが表示されます。
5. **Client MAC** にクライアントの MAC アドレスを入力してください。
6. 必要に応じてタイムアウト値を変更します。デフォルトは 5 分です。
7. SSID リストに SSID を入力します。カンマ区切りのリストとして複数の SSID を入力することができます。
8. **AP を表示** をクリックします。AP のリストが表示されます。
9. クライアントが接続を試みる AP を選択します。
10. **トラブルシューティング開始** をクリック。 接続ログが表示されます。
11. トラブルシューティングを終了するときは、**トラブルシューティング停止** をクリックします。トラブルシューティングを停止後に、接続ログ履歴から接続ログファイルをダウンロードすることができます。

接続ログのダウンロード

管理コンソールサーバーはトラブルシューティングを停止後、すべてのクライアント接続のトラブルシューティングのインスタンスのログ履歴を 30 分間保持します。

このデバッグログの履歴をダウンロードして、今後の参考のためにそれらを保存することができます。接続ログは .txt 形式で提供されます。

デバイス>Clients 下で認識できるクライアントの接続ログをダウンロードするには、次の手順を実行します。

1. ロケーションツリー上の必要なロケーションを選択します。
2. **デバイス**をクリックします。
3. **Clients** タブを選択します。
4. 接続ログの履歴をダウンロードしたいクライアントのチェックボックスを選択します。
5. ツールバー上の **更に>Packet Capture and Connections History** をクリックします。 **Packet Capture and Connections History** が表示されます。
6. 管理コンソールサーバーに保存されているこのクライアントの接続ログの一覧が表示されます。ファイル名は、トラブルシューティング開始時間とトラブルシューティング停止時間で表示されます。
7. ダウンロードする接続ログのダウンロードリンクをクリックし、接続ログを保存するパスを選択してください。 接続ログは、指定した場所に保存されます。

デバイス>Clients 下で認識できないクライアントの接続ログをダウンロードするには、次の手順を実行します。

1. ロケーションツリー上の必要なロケーションを選択します。
2. **デバイス**をクリックします。
3. **Clients** タブを選択します。
4. ツールバー上の **更に>Packet Capture and Connections History** をクリックします。 **Packet Capture and Connections History** のダイアログボックスが表示されます。
5. **MAC Address** にクライアントの MAC アドレスを入力します。
6. **履歴を取得**をクリック。 管理コンソールサーバーに保存されているこのクライアントの接続ログの一覧が表示されます。 ファイル名は、トラブルシューティング開始時間とトラブルシューティング停止時間で表示されます。
7. ダウンロードする接続ログのダウンロードリンクをクリックし、接続ログを保存するパスを選択してください。 接続ログは、指定した場所に保存されます。

接続ログ履歴の削除

管理コンソールサーバーはトラブルシューティングを停止後、すべてのクライアント接続のトラブルシューティングのインスタンスのログ履歴を 30 分間保持します。

この接続のログ履歴をサーバーから削除することができます。接続ログは .txt 形式で提供されています。

デバイス>Clients 下で認識できるクライアントの接続ログを削除するには、次の手順を実行します。

1. ロケーションツリー上の必要なロケーションを選択します。
2. **デバイス**をクリックします。
3. **Clients** タブを選択します。
4. 接続ログの履歴を削除したいクライアントのチェックボックスを選択します。
5. ツールバー上の **更に>Packet Capture and Connections History** をクリックします。 **Packet Capture and Connections History** のダイアログボックスが表示されます。
6. 管理コンソールサーバーに保存されているこのクライアントの接続ログの一覧が表示されます。ファイル名は、トラブルシューティング開始時間とトラブルシューティング停止時間で表示されます。
7. 削除するログファイルのチェックボックスにチェックを入れます。 削除する複数のログファイルを選択することができます。
8. アイコンをクリックします。 削除を確認するメッセージが表示されます。
9. 選択したログファイルの削除を実行するには、**Yes** をクリックします。

デバイス>Clients 下で認識できないクライアントの接続ログを削除するには、次の手順を実行します。

1. ロケーションツリー上の必要なロケーションを選択します。
2. **デバイス**をクリックします。
3. **Clients** タブを選択します。
4. ツールバー上の **更に>Packet Capture and Connections History** をクリックします。 **Packet Capture and Connections History** が表示されます。
5. **MAC Address** にクライアントの MAC アドレスを入力します。
6. **履歴を取得**をクリック。 管理コンソールサーバーに保存されているこのクライアントの接続ログの一覧が表示されます。 ファイル名は、トラブルシューティング開始時間とトラブルシューティング停止時間で表示されます。
7. 削除するログファイルのチェックボックスにチェックを入れます。 削除する複数のログファイルを選択することができます。
8. アイコンをクリックします。 削除を確認するメッセージが表示されます。
9. 選択したログファイルの削除を実行するには、**Yes** をクリックします。

カスタムフィルターの追加

カスタムフィルターを作成し、任意の名前で保存することができます。 表示されるカラムを選択することが可能です。必要に応じて管理コンソール(Management Console)上で表示される列内のデータにフィルターを設定することができます。 任意の名前でこのフィルターを保存することができ、同様に複数のフィルターを作成することができます。

カスタムフィルターを使用する際は、次の点に注意してください。

- 列の可視性と列のデータのソートの初期設定は、カスタムフィルターには保存されません。フィルター基準のみが保存されます。
- カスタムフィルターは、ユーザー固有のものです。これらは、カスタムフィルターを定義したユーザー用に保存され、他のユーザーには見えません。
- 保存されていないフィルターは、ツールバーの**フィルター**の隣にあるフィルター名の横にアスタリスクで示されます。
- ユーザーがフィルターを保存せずにログアウトした場合、保存されていないフィルターは保存されません。

カスタムフィルターを作成するには、次の手順を実行します。
1. **デバイス>Clients** へ移動します。
2. 列のヘッダーの横にある アイコンをクリックします。オプションのリストが表示されます。
3. **Filters** にマウスのポインタを合わせて、列のフィルターテキストを入力します。
4. ツールバー上の **フィルター**の隣にある アイコンをクリックして、**名前を付けて保存**をクリックします。 **名前を付けて保存**ダイアログボックスが表示されます。
5. フィルターの名前を入力し、**OK** をクリックします。カスタムフィルターが保存されます。

カスタムフィルターの編集

カスタムフィルターを編集するには、次の手順を実行します。
1. **デバイス>Clients** へ移動します。
2. ツールバー上の **フィルター**の隣にある アイコンをクリックして、要求するフィルターを選択します。
3. 列のヘッダーの横にある アイコンをクリックします。オプションのリストが表示されます。
4. **Filters** にマウスのポインタを合わせて、列にフィルターテキストを入力するか、必要に応じてフィルター条件を変更します。
5. ツールバー上の **フィルター**の隣にある アイコンをクリックして、**保存**をクリックします。 変更されたカスタムフィルターが保存されます。

カスタムフィルターの削除

カスタムフィルターを削除するには、次の手順を実行します。
1. **デバイス>Clients** へ移動します。
2. ツールバー上の **フィルター**の隣にある アイコンをクリックして、フィルターを削除するために アイコンをクリックします。 削除を確認するメッセージが表示されます。
3. カスタムフィルターの削除を実行するには、**Yes** をクリックします。

ロケーションのクライアント一覧を印刷

上部ペイン内のすべてのクライアントのすべての情報を印刷することができます。 それらを選択することで UI 上に表示されるカラムを選ぶことが可能です。 上部ペインに表示される情報がプリントアウトで表示される情報です。

ロケーションのクライアントリストを印刷するには、次の手順を実行します。
1. **デバイス>Clients** タブへ移動します。
2. クライアントのリストを印刷したいロケーションを選択します。
3. リストを印刷したいクライアントのタイプを選択します。
4. 印刷されるリストで希望する列を選択します。 カラムを選択または解除するには、任意のカラム名をクリックします。
5. 印刷アイコンをクリックします。 クライアントリストの印刷プレビューが表示されます。
6. リストを印刷するには、**印刷**をクリックします。

クライアントの削除

クライアントを削除するには、次の手順を実行します。
1. **デバイス**へ移動します。
2. **Clients** タブを選択します。
3. クライアントを選択します。
4. クライアントの削除操作を開始するには、ツールバー上の削除アイコンをクリックします。
5. 削除するには、確認画面で **Yes** をクリックします。 削除されたアクティブなクライアントは、センサーによって再発見されクライアントリストに再び表示される可能性があります。 非アクティブなクライアントは削除によってクライアントリストから消えます。

スペクトログラム

デバイス> Management Devices タブで、選択した管理デバイス(Management Device)のスペクトログラムを表示します。**干渉** ウィジェット上にある **スペクトログラム** をクリックします。

スペクトログラムは、管理デバイス(Management Device)の選択された無線と時間枠に対しての干渉を表すグラフです。

アクセスポイント(AP)の監視

デバイス>APs タブには、選択したロケーションに関連付けられているすべての AP が表示されます。 これには、Management Device の AP も含まれています。

アクセスポイント(AP)は、無線ネットワークで無線信号を送受信するハードウェアデバイスです。 ノートパソコンやスマートフォンなどのクライアントは、アクセスポイントに接続するか接続されているネットワーク上のデータにアクセスするためにアクセスポイントに接続します。 アクセスポイントは、有線ネットワークを拡張するために使用されます。

管理コンソール(Management Console)は、4 つのタイプに AP を分類します。

未分類の AP（Uncategorized AP） - AP が最初に WIPS センサーによって検出されると、未分類の AP として扱われます。

許可 AP(Authorized AP)- この AP は、ネットワークおよびネットワークリソースにアクセスするためにネットワーク管理者によって許可されています。

不正 AP(Rogue AP)-ネットワークまたはネットワークリソースにアクセスする権限がない AP です。 ネットワーク管理者から許可されていないまたは認識なしに、認可されていない方法でインストールされる AP です。 ネットワークに障害を引き起こすことや、ネットワークリソースから機密データを盗むような悪意のある接続がされる恐れがあります。 不正 AP(Rogue AP)とそれに接続するクライアントからネットワークを保護する必要があります。

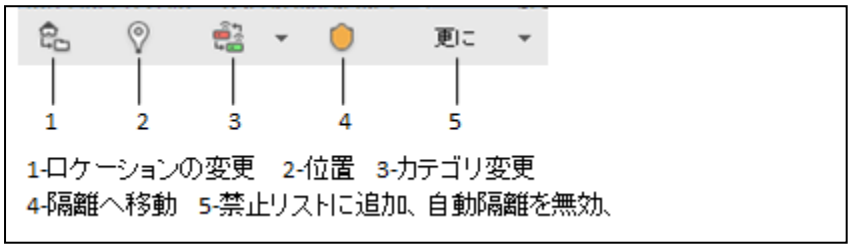
外部の AP（External AP） - この AP はネットワークに接続されていませんが、AP が出力する無線信号により WIPS センサーにより検出されます。

AP の各タイプは異なる色で表されます。

選択されたロケーションの許可、不正、外部、未分類の AP リストを表示するには、 **Authorized**、**Rogue**、**External**、**Uncategorized** のカテゴリから選択します。 一度に複数のカテゴリを選択することが可能です。 すべてのカテゴリより AP を表示するには、 **All** を選択します。
無線メッシュネットワークを形成するアクセスポイント(AP)は常に許可 AP(Authorized AP)として分類されます。 このようなアクセスポイント(AP)のカテゴリを変更することはできません。
Management Device 以外のベンダーの AP がメッシュネットワークの一部である場合、許可から任意の他のカテゴリにこれらの AP のカテゴリを変更することが可能です。

APs タブは、水平に 2 つのペインに分割されています。 上部のペインには、選択したロケーションの AP リストが表示されます。 下部のペインには、**APs** タブの上部ペインで選択した AP に関連した AP のプロパティが表示されます。 許可、不正、外部および未分類のアクセスポイントの場合は、選択された AP に関連付けられている最近のアソシエイトしたクライアントのリストを閲覧することができます。
許可 AP(Authorized AP)の場合は、下のペインに、AP の使用率、AP が接続されたクライアント、AP トラフィック、AP の平均データレートを確認することができます。

下図に示すように、ツールバーは 2 つのペインの間に表示されます。 ツールバー上に存在するオプションを使用して、AP に関連するさまざまな操作を行うことができます。
ツールバーによって任意の操作を実行するには、上部ペインの AP の行を選択する必要があります。



ご注意： 各種の操作を実行するために使用可能なオプションは、ログインしたユーザーの役割によって異なります。

メッシュ AP は、デフォルトで Authorized(許可)に分類されます。 それらが Management Device の AP である場合は、メッシュ AP のカテゴリを変更することはできません。 これらの AP を隔離、自動的に禁止することはできません。 したがって、ツールバーの '更に'下にあるオプションは、メッシュ AP では無効になっています。
AP が Management Device 以外のベンダーから提供されている場合は、メッシュ AP のカテゴリを変更することが可能です。

次の表は、**APs** タブの上部ペインに表示されるフィールドの説明を示します。

フィールド	説明
RSSI	AP の観測された RSSI（Received Signal Strength Indicator）の値を表示します。
名前	AP のユーザー定義名を示します。
MAC アドレス	AP の MAC アドレスを示します。
チャネル	AP が動作するチャネル番号を示します。
プロトコル	使用される IEEE802.11 のプロトコルを示します（IEEE802.11a、IEEE802.11b のみ、IEEE802.11b/g または IEEE802.11a/b/g（IEEE802.11n/ac 機能の有無で））。
クライアント	AP にアソシエイトするアクティブなクライアント数を示します。
SSID	クライアントがネットワークを認識するために使用する、AP の SSID を示します。
セキュリティ	AP に適用されるセキュリティ標準（Open、WEP、WPA、IEEE802.11i、または Unknown）を示します。 これは、AP に適用されたテンプレートより取り出されます。
ロケーション	AP のロケーションを示します。
アップ/ダウン	AP がアップ/ダウンしてからの日付と時刻。

AP のプロパティを表示

AP を選択しそのプロパティを表示します。 いくつかの AP プロパティは編集可能です。 AP プロパティを編集するには、それをダブルクリックして編集し、新しい値を保存します。

次の表は、AP プロパティのフィールドごとの説明を示します。

フィールド	説明
現在のアクティブ状態	AP が現在アクティブかどうか示します。Yes は AP がアクティブで、No は AP が非アクティブであることを指しています。
名前	AP の名前です。
分類	AP が許可（Authorized）、外部（External）、または不正（Rogue）として分類されているかどうかを示します。 Uncategorized は、AP が分類されていないことを示します。
ロケーション	AP のロケーションを示します。
フロアプラン上の配置	AP がロケーションのレイアウトに配置されているかどうかを示します。
MAC アドレス	AP の MAC アドレスを示します。
プロトコル	ワイヤレス接続を提供するために、AP によって使用される無線プロトコルを示します。
ケイパビリティ	IEEE802.11n、IEEE802.11ac、Super AG、Turbo のようなデバイスの動作モード機能を示します。
SSID	AP が接続されている WLAN の SSID を示します。
ゲスト	AP がゲスト AP であるかどうかを示します。
デバイスタグ	AP に関する追加情報を提供するテキストを示します。
IP アドレス	AP が許可されている場合は、IP アドレスを示します。 AP が不正（Rogue）か、外部（External）である場合、このフィールドは空白になっています。
ネットワーク	AP が接続されているネットワークのネットワークタグを示します。 AP がネットワークに接続されていない場合、この値は空白になっています。
ベンダー名	AP ベンダーの名前を示します。
最初に検出された日時	システムによって AP が最初に検出された日付と時刻を示します。
ダウン	AP がダウンした以降の日付と時刻を示します。
チャネル	AP が動作するチャネル番号を示します。
ベーシックリンクレート(Mbps)	AP でサポートされているリンク速度をカンマ区切りのリストで示します。
セキュリティ	AP に適用されるセキュリティ標準を示します。 これは、AP に適用されたテンプレートより取り出されます。
認証	クライアントの識別情報を検証するために AP によって使用される一連の処理を示します。
ペアワイズ暗号化方式	AP とクライアント間のユニキャスト通信に使用する暗号を示します。 すべての BSSID の MAC/プロトコル フィールドで選択された場合には、MULTIPLE が表示されます。
グループワイズ暗号化方式	AP からのブロードキャストやマルチキャスト通信のために使用される暗号を示します。 すべての BSSID の MAC/プロトコル フィールドで選択された場合には、MULTIPLE が表示されます。
ビーコン間隔(ms)	AP の連続するビーコン間の間隔をミリ秒単位で示します。
IEEE802.11n ケイパビリティ	AP の IEEE802.11n の機能を示します。 このフィールドは、AP が IEEE802.11n 規格の初期または標準実装に準拠しているかどうかについての情報を提供します。

チャネル幅	AP が 20MHz、40MHz または 80MHz のチャネル幅で動作していることを示しています。 IEEE802.11n では、20MHz の標準的なチャネル幅または 40MHz の 2 倍のチャネル幅の使用を可能にします。 40MHz のチャネル幅は、同時にデータを送信するために 2 つの隣接チャネルを使用することによって達成されます。 IEEE802.11ac は、20MHz の標準的なチャネル幅または 80MHz のチャネル幅の使用を可能にします。 80MHz のチャネル幅は同時にデータを送信するために 4 つの隣接するチャネルを使用することによって達成されます。
チャネルオフセット	AP が 40 MHz のチャネル幅で動作する場合、チャネルオフセットが 40MHz 動作で使用される隣接するチャネルがプライマリチャネルの上または下にあるかどうかを示します。
データ転送速度	クライアントと通信する AP の最大のリンク速度を示します。
GI (20MHz)	AP が 20MHz のショートガードインターバルを使用できるかどうかを示します。
GI (40MHz)	AP が 40MHz のショートガードインターバルを使用できるかどうかを示します。
MCS サポート	IEEE802.11n/ac のためにサポートされるさまざまな変調および符号化スキーム（MCS）を示します。
グリーンフィールドモード	AP がグリーンフィールドモードで動作することが可能であるかどうかを示します。グリーンフィールドモードは IEEE802.11n 規格のオプションの高いスループットモードです。それはレガシー（IEEE802.11a/b/g）プロトコルと下位互換性を持たず、IEEE802.11n の最大性能利点を提供します。
ビームフォーミングケイパビリティ	AP がビームフォーミングが可能であるかどうかを示します。ビームフォーミングは、受信側クライアントで直接放射された RF エネルギーを集束するのに役立つ RF 送信方法です。これにより、クライアントでの信号の受信、結果的にスループットが向上します。

最近のアソシエイトしたクライアント

最近のアソシエイトしたクライアント では、選択された AP に最近接続されたクライアントのリストが表示されます。クライアントのアクティブ/非アクティブ・アイコン、クライアント名、SSID、最後の検出のような詳細が同じ行に表示されます。

AP 利用率

AP 利用率 セクションでは、 最後の 12 時間にわたる AP の利用率をグラフ表示で見ることができます。 **AP 利用率** セクションは、許可 AP(Authorized AP)のみ表示されます。 Management Device は、チャネルの合計スキャンタイムの割合として累積時間占有率の軌跡を 15 分おきに保ちます。

AP がアソシエイトしたクライアント

AP がアソシエイトしたクライアント セクションでは、 過去 12 時間で AP に接続されたクライアントのグラフ表示を見ることができます。Management Device は、AP とクライアントのアソシエーション数を 15 分おきに取得します。

AP のトラフィック

AP トラフィックセクションでは、過去 12 時間の AP トラフィックのグラフ表示を見ることができます。 AP トラフィックセクションは許可クライアントに対してのみ見ることができます。 AP を認識している Management Device は、AP によって送受信されるデータトラフィックを 15 分おきにレポートします。 チャネルを順に確認している Management Device は、任意のチャネル上で合計時間の数パーセントを費やします。 そのため、デバイスの無線でスキャンされるチャネルの合計数と等しい要因により、このパラメータは実際のトラフィックを通常は過小評価します。 例えば、Management Device が全部で 30 のチャネルをスキャンする場合、測定したトラフィックは実際のトラフィックの 1/30 になります。 トラフィックの性質がバースト状態である場合は、そのような単純なスケーリングは適用することはできません。

AP の平均データレート

AP の平均データレート セクションでは、 過去 12 時間で AP の平均データレート（Mbps）のグラフ表示を見ることができます。 **AP の平均データレート**は許可 AP(Authorized AP)に対してのみ見ることができます。

AP を認識しているデバイスの表示

AP を認識しているデバイス・ウィジェットは、上部ペインで選択された AP を検出したセンサーモードの Management Device を表示します。
AP を認識している Management Device を表示するには、次の手順を実行します。

1. **デバイス>APs** タブへ移動します。
2. ロケーションを選択します。
3. AP を選択します。
4. 下部ペインに選択された AP を認識している Management Device のリストを表示するには、**AP を認識しているデバイス・ウィジェット**のページに移動します。

AP イベントの表示

上部ペインで選択された AP の現在のイベントを表示するには、次の手順を実行します。

1. **デバイス>APs** タブへ移動します。
2. ロケーションを選択します。
3. AP を選択します。
4. 下部ペインに選択された AP のアクティブなイベントリストを表示するには、**イベント・ウィジェット**のページに移動します。

AP のロケーションを変更

フロアマップ上の AP のロケーションを変更するには、次の手順を実行します。

1. **デバイス>APs** タブへ移動します。
2. ロケーションを選択します。
3. ロケーションを変更したい AP を選択します。
4. 'ロケーションの変更' アイコンをクリックします。 '新しいロケーションの選択' ダイアログボックスが表示されます。
5. AP の新しいロケーションを選択します。
6. OK をクリックします。

AP の位置を検出

フロアマップ上の AP の位置を検出するには、次の手順を実行します。
1. **デバイス>APs** タブへ移動します。
2. AP が配置されているロケーションを選択します。
3. AP を選択します。
4. ロケーション・フロアマップ上の AP の位置を検出するには、Locate アイコンをクリックします。

AP の隔離

AP を隔離するには、次の手順を実行します。
1. **デバイス>APs** タブへ移動します。
2. 隔離する AP があるロケーションを選択します。
3. 隔離する AP を選択します。
4. 隔離へ移動のアイコンをクリックして、AP を隔離するために確認メッセージで Yes をクリックします。

AP のカテゴリを変更

AP のカテゴリを変更するには、次の手順を実行します。
1. **デバイス>APs** タブへ移動します。
2. AP のカテゴリを変更したいロケーションを選択します。
3. カテゴリを変更したい AP のチェックボックスにチェックを入れます。
4. ツールバー上にあるカテゴリ変更のアイコンをクリックします。
5. 必要に応じて **Authorized**、 **External**、**Rogue** から目的のカテゴリを選択します。

自動隔離を無効にする

1. **デバイス>APs** タブへ移動します。
2. AP が配置されているロケーションを選択します。
3. AP を選択して、ツールバー上の **更に** をクリックします。
4. AP の自動隔離を無効にするには、自動隔離を無効をクリックします。

禁止リストに追加

AP を禁止リストへ追加するには、次の手順を実行します。
1. **デバイス>APs** タブへ移動します。
2. AP が配置されているロケーションを選択します。
3. AP を選択して、ツールバー上の **更に** をクリックします。
4. AP を禁止リストへ追加するには、禁止リストに追加をクリックします。

AP をソート

APs タブの上部ペインで、列上の AP の詳細をソートすることができます。 順または降順で AP を並べ替えることが可能です。

1. **デバイス>APs** タブへ移動します。
2. ロケーションを選択します。
3. ソートした上部ペインの列を指して、 をクリックします。
4. 矢印を再度クリックすると、ソート順を逆順にすることができます。 アイコンは、現在のソート順により上矢印または下矢印になる可能性があります。

AP の詳細をフィルター

選択した列のテキストと一致するフィルターテキストに基づいて、UI に表示される AP 情報をフィルタリングすることができます。

例えば、WPA セキュリティを持つ AP のみを表示するには、次の操作を行います。
1. **デバイス>APs** タブへ移動します。
2. ロケーションを選択します。
3. 上部ペインで **セキュリティ** をポイントして、 をクリックし、フィルターテキストに'WPA'を入力します。
4. WPA セキュリティを持つ AP を表示するには、**Enter** キーを押します。

表示される列を選ぶには、以下を実行します。
1. **デバイス>APs** タブへ移動します。
2. ロケーションを選択します。
3. 上部ペインで任意のカラム名をポイントして、 をクリックします。 メニューが表示されます。
4. メニューの **Columns** をポイントして、UI 上に列を表示するためにチェックボックスにチェックを入れます。 すでに選択済みで UI 上に表示したくない列に対しては、チェックボックスのチェックを外します。

AP の検索

AP の名前、AP の MAC アドレスまたは AP の SSID を使用して、AP を検索することができます。

AP（または複数の AP）を検索するには、次の手順を実行します。
1. **デバイス>APs** タブへ移動します。
2. AP を検索したいロケーションを選択します。
3. 右上の隅にある **クイックサーチボックス**に AP の名前、MAC アドレスまたは SSID を入力します。
4. Enter キーを押します。検索条件に一致する AP が上部ペインに表示されます。

ページサイズのセット

上部ペインのページごとに見ることができる AP の数を設定することができます。

ページサイズを設定するには、次の手順を実行します。
1. **デバイス>APs** タブへ移動します。
2. ロケーションを選択します。
3. ページサイズをセットするには、**ページサイズのセット**をクリックします。
4. 適切なサイズを設定します。

カスタムフィルターの追加

カスタムフィルターを作成し、任意の名前で保存することができます。 表示されるカラムを選択することが可能です。 必要に応じて管理コンソール(Management Console)上で表示される列内のデータにフィルターを設定することができます。 任意の名前でこのフィルターを保存することができ、同様に複数のフィルターを作成することができます。

カスタムフィルターを使用する際は、次の点に注意してください。
- 列の可視性と列のデータのソートの初期設定は、カスタムフィルターには保存されません。フィルター基準のみが保存されます。
- カスタムフィルターは、ユーザー固有のものです。これらは、カスタムフィルターを定義したユーザー用に保存され、他のユーザーには見えません。
- 保存されていないフィルターは、ツールバーの**フィルター**の隣にあるフィルター名の横にアスタリスクで示されます。
- ユーザーがフィルターを保存せずにログアウトした場合、保存されていないフィルターは保存されません。

カスタムフィルターを作成するには、次の手順を実行します。
1. **デバイス>APs** タブへ移動します。
2. 列のヘッダーの横にある アイコンをクリックします。オプションのリストが表示されます。
3. **Filters** にマウスのポインタを合わせて、列のフィルターテキストを入力します。
4. ツールバー上の **フィルター**の隣にある アイコンをクリックして、**名前を付けて保存**をクリックします。 **名前を付けて保存**ダイアログボックスが表示されます。
5. フィルターの名前を入力し、**OK** をクリックします。カスタムフィルターが保存されます。

カスタムフィルターの編集

カスタムフィルターを編集するには、次の手順を実行します。
1. **デバイス>APs** タブへ移動します。
2. ツールバー上の **フィルター**の隣にある アイコンをクリックして、要求するフィルターを選択します。
3. 列のヘッダーの横にある アイコンをクリックします。オプションのリストが表示されます。
4. **Filters** にマウスのポインタを合わせて、列にフィルターテキストを入力するか、必要に応じてフィルター条件を変更します。
5. ツールバー上の **フィルター**の隣にある アイコンをクリックして、**保存**をクリックします。 変更されたカスタムフィルターが保存されます。

カスタムフィルターの削除

カスタムフィルターを削除するには、次の手順を実行します。
1. **デバイス>APs** タブへ移動します。
2. ツールバー上の **フィルター**の隣にある アイコンをクリックして、フィルターを削除するために アイコンをクリックします。 削除を確認するメッセージが表示されます。
3. カスタムフィルターの削除を実行するには、**Yes** をクリックします。

ロケーションの AP 一覧を印刷

上部ペイン内のすべての AP のすべての情報を印刷することができます。 それらを選択することで UI 上に表示されるカラムを選ぶことが可能です。 上部ペインに表示される情報がプリントアウトで見られる情報です。

paginated view が有効になっている場合は、現在のページの AP のリストが印刷されます。ロケーションのすべての AP のリストを印刷するには、各ページに移動し個々のページを印刷する必要があります。

paginated view が無効になっている場合は、UI 上に見える AP のリストのみが印刷されます。これは 25 レコードが存在し、UI 上に最初の 5 つが示されている場合、これらの 5 つのレコードが印刷されることを意味します。

印刷する前に paginated view を有効または無効にする必要があります。

ロケーションの AP リストを印刷するには、次の手順を実行します。
1. **デバイス>APs** タブへ移動します。
2. AP のリストを印刷したいロケーションを選択します。
3. リストを印刷したい AP のタイプを選択します。
4. 印刷されるリストで希望する列を選択します。カラムを選択または解除するには、任意のカラム名をクリックします。
5. 印刷アイコンをクリックします。クライアントリストの印刷プレビューが表示されます。
6. リストを印刷するには、**印刷**をクリックします。

AP をマージ

APs タブに表示される AP は、仮想 AP または物理 AP のどちらかである可能性があります。 1 つまたは複数の仮想 AP は、実際には、単一の物理的実体である可能性があります。 より良い管理のために APs タブを介してこのような仮想 AP を単一の AP にマージすることができます。 許可 AP(Authorized AP)のみマージすることが可能です。

許可 AP(Authorized AP)をマージするには、次の手順を実行します。
1. **デバイス>APs** タブへ移動します。
2. AP をマージしたいロケーションを選択します。
3. マージする 2 つ以上の許可 AP(Authorized AP)を選択して、ツールバー上の **更に** アイコンをクリックします。
4. AP をマージするには、**マージ**を選択します。

AP の分割

単一の AP を形成するためにマージされた 1 つまたは複数の仮想 AP を、元の AP の数に分割することができます。 マージされた AP を選択する場合だけ分割が利用できます。 マージが許可 AP(Authorized AP)でのみ利用可能なように、AP 分割も許可 AP(Authorized AP)でのみ使用できます。

許可 AP(Authorized AP)を分割するには、次の手順を実行します。
1. **デバイス>APs** タブへ移動します。
2. マージされた AP を分割したいロケーションを選択します。
3. 分割するマージされた AP を選択して、ツールバー上の **更に** アイコンをクリックします。
4. AP を分割するには、**分割**をクリックします。

AP のトラブルシューティング

センサーモードで動作している Management Device を使用して AP のトラブルシューティングを行うことができます。
トラブルシューティングをはじめるには、管理コンソール(Management Console)を起動するために使用されるコンピューターから、Management Device(センサー)が到達可能であることを確認する必要があります。 Management Device が隔離でビジーまたはトラブルシューティングで使用中の場合、選択した AP をトラブルシューティングすることができません。

Management Device（センサー）をパケットレベルモードまたはイベントレベルモードで AP のトラブルシューティングに用いることが可能です。 このセンサーは Wireshark（または使用できる他のツール）のようなパケットキャプチャツールを使用して、トラブルシューティングを行うことができます。

別の方法として、管理コンソールサーバーにパケットトレースの履歴を保存することができ、あとの参考のために履歴ファイルをダウンロードすることができます。 パケットトレースの履歴は .pcap ファイルとして保存されます。 これは Wireshark や OmniPeek などを使用して表示することが可能です。

複数の BSSID を持つマージされた AP をトラブルシュートすることはできません。 マージされた AP の単一の BSSID のトラブルシューティングを行うことができます。

トラブルシューティングセッションが進行中である場合、アクティブなトラブルシューティングセッションに関する通知は、管理コンソール(Management Console)の右上隅にある **通知** で見ることができます。

トラブルシューティングセッションは自動的にタイムアウトするか、アクティビティにかかわりなく指定されたタイムアウト後に停止します。

ご注意： コンソールからパケットキャプチャベースのトラブルシューティングセッションがはじまり、パケットキャプチャツールが中断または（正常または突然に）終了のいずれかになった場合、別のパケットキャプチャセッションを開始する前に、まずはじめに（まだ進行中であれば）手動でコンソールから進行中のトラブルシューティングセッションを停止するか、セッションが本当に終わったことを確認する必要があります。 手動でトラブルシューティングセッションを終了するには、このセクション内の'トラブルシューティングの停止'サブセクションを参照してください。
そのあと、コンソールからの新たなトラブルシューティングセッションを再起動することができます。
選択されたツール (Wireshark など)で進行中のトラブルシューティングセッションがある場合、同じまたは他のコンピューターからコマンドプロンプトでユーザー指定のパラメータ（すなわち rpcap://sensor-ip/iface）を使用して他のキャプチャを行っても正常に動作しません。

ローカルマシン上の Wireshark を使用してパケットレベルモードで AP をトラブルシューティング

パケットレベルモードでの AP のトラブルシューティングを行うには、次の手順を実行します。

1. **デバイス**をクリックします。
2. **APs** タブを選択します。
3. トラブルシューティングを行う AP のチェックボックスにチェックを入れます。
4. ツールバー上にある**更に>パケットキャプチャ** をクリックします。 AP のトラブルシューティングを行うダイアログボックスが表示されます。
5. センサーとして動作する Management Device のリストから、トラブルシューティングを行うために使用するセンサーのチェックボックスを選択します。 デバイスを認知しているセンサーは、それらの可用性と信号強度に基づいてソートされます。
6. **トラブルシューティングモード**の下にある**ライブパケットキャプチャ**を選択します。
7. **ストリーミング**で**ローカルマシン上の Wireshark** を選択します。
8. **タイムアウト**にタイムアウト間隔を指定します。 パケットレベルのトラブルシューティングモードのデフォルトのタイムアウトは 5 分です。 タイムアウトの最小値は 1 分で、最大値は 720 分です。
9. **トラフィックの選択**でトラブルシューティング中に参照するパケットタイプを選択します。 トラブルシューティングを行うセンサーで認識できるすべてのパケットを表示する場合は、**チャネル上のすべてのパケット**を選択します。 トラブルシューティングを行うセンサーで AP からのパケットだけを表示したい場合は、**選択された BSSID <BSSID 値> のみ** を選択します。
10. **プロトコルとチャネル選択** セクションでは、トラブルシューティングの対象となるプロトコルおよびチャネルを選択します。 単一のチャネルを選択したい場合は、**チャネルを選択**で、チャネル番号と **Width**（チャネルオフセット）を指定します。 デフォルトでは、プロトコルおよびチャネルはトラブルシューティングのセンサーに適用されるデバイステンプレートに基づいて表示されます。 必要に応じて、異なるプロトコルおよびチャネルを選択することができます。 また、すべての有効なチャネルをトラブルシューティングするには、**全チャネル**を選択することが可能です。
11. トラブルシューティングを開始するには、**トラブルシューティング開始** をクリックします。 センサーは、ライブパケットをキャプチャすることが可能となります。
12. ライブパケットキャプチャのために適切なツールを選択します。 ツールがインストールされていない場合は、Wireshark か他のツールをダウンロードすることができます。
13. パケットキャプチャを表示するには、使用するツールに応じて Wireshark 下に示したコマンドを、お使いのコンピューターにインストールされているオペレーティングシステムのコマンドラインインタフェースを開いて実行します。 **パケットレベルモードのトラブルシューティング**ダイアログボックスでは、Wireshark に対して実行するコマンドのガイドラインを提供します。下記の図では、Wireshark では、rpcap はプロトコル、192.168.1.102 はトラブルシュートするセンサーの IP アドレス、そして atn0 はインタフェースになります。 コマンドライン上で実際に Wireshark コマンドを実行する際は、適切なセンサーの IP アドレスを入力します。

パケット履歴を管理コンソールサーバーにアップロードする AP のトラブルシューティング

パケットレベルモードで AP のトラブルシューティングを行うには、次の手順を実行します。

1. **デバイス**をクリックします。
2. **APs** タブを選択します。
3. トラブルシューティングを行う AP のチェックボックスにチェックを入れます。
4. ツールバー上にある**更に>パケットキャプチャ** をクリックします。 AP のトラブルシューティングを行うダイアログボックスが表示されます。
5. センサーとして動作する Management Device のリストから、トラブルシューティングを行うために使用するセンサーのチェックボックスを選択します。 デバイスを認知しているセンサーは、それらの可用性と信号強度に基づいてソートされます。
6. **トラブルシューティングモード**の下にある**ライブパケットキャプチャ**を選択します。
7. **ストリーミングオプション**で**サーバーにアップロード** を選択します。
8. **ファイル名のプレフィックス**にファイル名に適したプレフィックスを入力します。 これはパケット履歴をダウンロードすると際に、トラブルシューティングのファイルを識別するのに役立ちます。
9. **タイムアウト**にタイムアウト間隔を指定します。 パケットレベルのトラブルシューティングモードのデフォルトのタイムアウトは 5 分です。 タイムアウトの最小値は 1 分で、最大値は 720 分です。
10. **トラフィックの選択**でトラブルシューティング中に参照するパケットタイプを選択します。 トラブルシューティングする Management Device から見えるアクセスポイント(AP)のすべての BSSID のパケットをキャプチャする場合は、**このアクセスポイント(AP)上のすべての BSSID のパケット** を選択します。 トラブルシューティングを行うセンサーで AP からのパケットだけを表示したい場合は、**選択された BSSID <AP MAC アドレス> のみ** を選択します。
11. パケットタイプを選択します。 すべてのパケットをキャプチャしたい場合は、**All** を選択します。 特定のパケットタイプをキャプチャしたい場合は、フィルターを選択して、トラブルシューティング間にキャプチャするために必要なデータフレームおよび管理フレームを選択します。
12. **プロトコルとチャネル選択** セクションでは、トラブルシューティングの対象となるプロトコルおよびチャネルを選択します。 単一のチャネルを選択したい場合は、**チャネルを選択**で、チャネル番号と **Width**（チャネルオフセット）を指定します。 デフォルトでは、プロトコルおよびチャネルはトラブルシューティングのセンサーに適用されるデバイステンプレートに基づいて表示されます。 必要に応じて、異なるプロトコルおよびチャネルを選択することができます。 また、すべての有効なチャネルをトラブルシューティングするには、**全チャネル**を選択することが可能です。
13. トラブルシューティングを開始するには、**トラブルシューティング開始** をクリックします。 センサーは、ライブパケットをキャプチャすることが可能となります。

イベントレベルモードでの AP のトラブルシューティング

イベントレベルモードで AP のトラブルシューティングを行うには、次の手順を実行します。
1. **デバイス**をクリックします。
2. **APs** タブを選択します。
3. トラブルシューティングを行う AP のチェックボックスにチェックを入れます。
4. ツールバー上にある**更に>パケットキャプチャ** をクリックします。 AP のトラブルシューティングを行うダイアログボックスが表示されます。
5. センサーとして動作する Management Device のリストから、トラブルシューティングを行うために使用するセンサーのチェックボックスを選択します。 デバイスを認知しているセンサーは、それらの可用性と信号強度に基づいてソートされます。
6. **トラブルシューティングモード** の下にある、**デバイスに対して新たなイベントを生成** を選択します。
7. **タイムアウト**にタイムアウト間隔を指定します。 イベントレベルのトラブルシューティングモードのデフォルトのタイムアウトは 2 分です。 タイムアウトの最小値は 1 分で、最大値は 5 分です。
8. **トラフィックの選択**でトラブルシューティング中に参照するパケットタイプを選択します。 トラブルシューティングする Management Device から見えるアクセスポイント(AP)のすべての BSSID のパケットをキャプチャする場合は、**このアクセスポイント(AP)上のすべての BSSID のパケット** を選択します。 トラブルシューティングを行うセンサーで AP からのパケットだけを表示したい場合は、**選択された BSSID <AP MAC アドレス> のみ** を選択します。
9. **プロトコルとチャネル選択** セクションでは、トラブルシューティングの対象となるプロトコルおよびチャネルを選択します。 単一のチャネルを選択したい場合は、**チャネルを選択**で、チャネル番号と **Width**（チャネルオフセット）を指定します。 デフォルトでは、プロトコルおよびチャネルはトラブルシューティングのセンサーに適用されるデバイステンプレートに基づいて表示されます。 必要に応じて、異なるプロトコルおよびチャネルを選択することができます。 また、すべての有効なチャネルをトラブルシューティングするには、**全チャネル**を選択することが可能です。
10. トラブルシューティングを開始するには、**トラブルシューティング開始** をクリックします。 トラブルシューティング中にセンサーがイベントを生成します。これらはセンサーの最新のイベントとしてデバイスリストで見ることができます。

トラブルシューティングの停止

トラブルシューティングセッションは自動的にタイムアウトするか、アクティビティにかかわりなく指定されたタイムアウト後に停止します。 手動でトラブルシューティングセッションを終了することができます。

手動でアクティブなトラブルシューティングセッションを停止するには、次の手順を実行します。
1. 右上の隅にある通知アイコンをクリックします。 （存在する場合は）アクティブなトラブルシューティングセッションは、他の通知と一緒に表示されます。
2. アクティブなトラブルシューティングセッションの通知をクリックします。 センサーのトラブルシューティングセッションのリストが表示されます。
3. 終了するトラブルシューティングセッションのチェックボックスを選択します。
4. **停止**をクリック。 トラブルシューティングセッションが終了し、トラブルシューティングセッションの終了を示すメッセージが表示されます。 **トラブルシューティングモード**で**ストリーミングオプション**として**サーバーにアップロード**が選択されている場合、パケットトレース履歴は管理コンソールサーバーにアップロードされています。

パケットキャプチャのダウンロード

トラブルシューティング停止後、管理コンソールサーバーは 30 分間トラブルシューティング・インスタンスのパケットキャプチャ履歴を保持します。

この履歴をダウンロードして、今後の参考のためにそれらを保存することができます。 パケットトレースの履歴は .pcap ファイルとして保存されます。

パケットキャプチャファイルをダウンロードするには、次の手順を実行します。
1. ロケーションツリーから要求するロケーションを選択します。
2. **デバイス**をクリックします。
3. **APs** タブを選択します。
4. ツールバー上にある**更に>Packet Capture History** をクリックします。 **Packet Capture History** ダイアログボックスが表示されます。 ファイル名、ファイルサイズ(KB)、トラブルシューティング開始時間および停止時間を持つリストが表示されます。
5. ダウンロードするパケットトレースの**ダウンロード**リンクをクリックして、パケットトレースを保存するパスを選択してください。 パケットトレースファイルは指定された場所に保存されます。

パケットキャプチャの削除

トラブルシューティング停止後、管理コンソールサーバーは 30 分間トラブルシューティング・インスタンスのパケットキャプチャ履歴を保持します。

サーバーからこのパケットキャプチャの履歴を削除することができます。パケットキャプチャファイルは.pcap フォーマットで提供されています。

パケットキャプチャファイルを削除するには、次の手順を実行します。
1. ロケーションツリーから要求するロケーションを選択します。
2. **デバイス**をクリックします。
3. **APs** タブを選択します。
4. ツールバー上にある**更に>Packet Capture and Connections History** をクリックします。 **過去のパケットキャプチャ** ダイアログボックスが表示されます。 ファイル名、ファイルサイズ(KB)、トラブルシューティング開始時間および停止時間を持つリストが表示されます。
5. 削除するログファイルのチェックボックスにチェックを入れます。 削除する複数のファイルを一度に選択することができます。
6. アイコンをクリックします。削除を確認するメッセージが表示されます。
7. 選択したファイルの削除を実行するには、**Yes** をクリックします。

AP の削除

一度に同じロケーションで 1 つ以上の AP を削除することができます。アクティブな AP はセンサーとして設定された管理デバイス(Management Device)により再発見される可能性があり、AP の分類ポリシーに基づいて、関連するカテゴリで AP タブに再表示する可能性があります。
非アクティブな AP が削除されると、アクティブになるまで表示されないことがあります。

AP を削除するには、次の手順を実行します。
1. **デバイス>AP** タブへ移動します。
2. AP を削除したいロケーションを選択します。
3. 削除する 1 つ以上の AP を選択して、ツールバーの**更に**をクリックします。
4. AP の削除操作を開始するには、ツールバー上の削除アイコンをクリックします。 AP の削除を確認するメッセージが表示されます。
5. 削除を実行するには、**Yes** をクリックします。

ネットワークの監視

Networks タブは、ネットワークリストとネットワークに関連付けられた AP とセンサーを表示します。

Networks タブは、水平に 2 つのペインに分割されています。
ツールバーは、上部と下部ペインの間にあります。 このツールバーには、上部ペインで選択したネットワーク上の各種の操作を実行するためのアイコンがあります。
上部ペインには選択したロケーションで検出されたネットワークのリストが表示されます。 下部ペインには、**Networks** タブの上部ペインで選択したネットワーク内の AP とセンサーに関連するネットワークのプロパティが表示されます。

Network プロパティ：アクセスポイント は、**Networks** タブの下部ペインの 1 ページ目に表示されます。

Network プロパティ：アクセスポイント には、そのネットワークとそのロケーション（サブロケーションも含む）に関連付けられたすべての AP が表示されます。

アクセスポイントタブ内のフィールドは、**デバイス>AP** タブで表示されるものと同じです。 AP のカテゴリ（Authorized、Rogue、External、Uncategorized）に基づいて、表示する AP をフィルターすることが可能です。 すべてのタイプの AP を表示するには、All のチェックボックスを選択します。
AP のリストの下にツールバーがあります。 このツールバーを使用すると、**デバイス>AP** タブで実行できる操作と同様に、これらの AP に関連するすべての操作を実行することができます。 選択したネットワーク内の AP 上で任意の操作を実行するには、操作を実行したい AP を選択しそれぞれのアイコンをクリックします。

Network プロパティ：センサーは、**Networks** タブの下部ペインの 2 ページ目に表示されます。
センサータブ内のフィールドは、**デバイス> Management Device** タブで表示されるものと同じです。
センサータブには、ネットワーク内で現在アクティブなセンサーのみが表示されます。

次の表は、**Networks** タブで表示される各フィールドの説明です。

フィールド	説明
名前	ネットワーク名
ネットワークアドレス	ネットワークの IP アドレス
ロケーション	ネットワークのロケーション
監視中のセンサー	ネットワークを監視しているセンサー
Gateway MAC	Gateway MAC アドレス
エクスポーズ	ネットワークが発見されてからの日付と時刻

ネットワークのロケーションを変更

ネットワークのロケーションは、最初にネットワークをレポートしたセンサーのロケーションと同じです。 ネットワークに接続された複数のセンサーが存在する場合、そのようなネットワークのロケーションは、すべてのレポートのセンサーの最も近い共通のロケーションです。

ネットワークの場所を変更するには、次の手順を実行します。
1. **デバイス**へ移動します。
2. **Networks** タブを選択します。
3. ネットワークが検出されたネットワークを選択します。
4. ロケーションを変更するネットワークのチェックボックスを選択します。
5. ロケーションの変更のアイコンをクリックします。
6. 表示される新しいロケーションの選択ダイアログボックスで新しいロケーションを選択します。
7. 新しいロケーションにネットワークを移動するには、OK をクリックします。

選択する新しいロケーション上で、ネットワークは新しいロケーションの下で認識されます。

ネットワークの名前を変更

ネットワークの名前を変更するには、次の手順を実行します。
1. **デバイス**へ移動します。
2. **Networks** タブを選択します。
3. 名前を変更するネットワークのチェックボックスを選択します。
4. ネットワーク名の変更アイコンをクリックします。
5. 表示される名前変更ダイアログボックスに新しい名前を入力します。
6. 選択したネットワークの名前を変更するには、OK をクリックします。

カスタムフィルターを追加

カスタムフィルターを作成し、任意の名前で保存することができます。 表示されるカラムを選択することが可能です。 必要に応じて管理コンソール(Management Console)上で表示される列内のデータにフィルターを設定することができます。 任意の名前でこのフィルターを保存することができ、同様に複数のフィルターを作成することができます。

カスタムフィルターを作成するには、次の手順を実行します。
1. **デバイス>Networks** へ移動します。
2. カスタムフィルターを作成したいロケーションを選択します。
3. アイコンをクリックします。オプションのリストが表示されます。
4. **Columns** にマウスのポインタを合わせて、表示する列のチェックボックスを選択します。
5. 列のデータをソートしたい場合は、列名をクリックし **Sort Ascending** または **Sort Descending** を選択します。
6. 列に表示されるデータをフィルターしたい場合は、列名の横の アイコンをクリックし、**Filters** のチェックボックスを選択します。
7. ツールバー上の**フィルター**の横にある をクリックして、**名前を付けて保存**をクリックします。 **名前を付けて保存**のダイアログボックスが表示されます。
8. フィルターの名前を入力し、**OK** をクリックします。カスタムフィルターが保存されます。

カスタムフィルターの編集

カスタムフィルターを編集するには、次の手順を実行します。
1. **デバイス>Networks** へ移動します。
2. カスタムフィルターを編集したいロケーションを選択します。
3. ツールバー上の**フィルター**の隣にある アイコンをクリックして、要求するフィルターを選択します。
4. 必要に応じてフィルターを変更します。
5. **フィルター**の横にある アイコンをクリックして、**保存**をクリックします。 変更されたカスタムフィルターが保存されます。

カスタムフィルターの削除

カスタムフィルターを削除するには、次の手順を実行します。
1. **デバイス>Networks** へ移動します。
2. カスタムフィルターを削除したいロケーションを選択します。
3. フィルターを削除するには、 ツールバー上の**フィルター**の隣にあるアイコンをクリックして、 アイコンをクリックします。 削除を確認するメッセージが表示されます。
4. カスタムフィルターの削除を実行するには、**Yes** をクリックします。

ロケーションのネットワーク一覧を印刷

上部ペイン内のすべてのネットワークのすべての情報を印刷することができます。 それらを選択することで UI 上に表示されるカラムを選ぶことが可能です。 上部ペインに表示される情報がプリントアウトできる情報です。

paginated view が有効になっている場合は、現在のページのネットワークのリストが印刷されます。ロケーションのすべてのネットワークのリストを印刷するには、各ページに移動し個々のページを印刷する必要があります。

paginated view が無効になっている場合は、UI 上に見えるネットワークのリストのみが印刷されます。例えば、25 レコードが存在し、UI 上に最初の 5 つが表示されている場合、表示されている 5 つのレコードのみが印刷されます。

印刷する前に paginated view を有効または無効にする必要があります。

ロケーションのネットワークリストを印刷するには、次の手順を実行します。
1. **デバイス>Networks** へ移動します。
2. ネットワークリストを印刷したいロケーションを選択します。
3. 印刷されるリストで希望する列を選択します。カラムを選択または解除するには、任意のカラム名をクリックします。
4. 印刷アイコンをクリックします。ネットワークリストの印刷プレビューが表示されます。
5. ネットワークリストを印刷するには、**印刷** をクリックします。

ネットワークタイプの変更

管理コンソール(Management Console)をリリース 7.1 Update 3 にアップグレードすると、デフォルトですべてのネットワークはカード会員データ環境（CDE：Cardholder Data Environment）ネットワークとしてマークされます。Networks タブに表示されるネットワークがクレジットカード・データを備えていないか、または送信しないならば、非 CDE タイプのネットワークに変更することができます。

同様に、非 CDE ネットワークを CDE ネットワークに変更することができます。

一度に同じタイプの複数のネットワークを選択し、必要に応じて非 CDE または CDE としてそれらをマークすることができます。

ネットワークのネットワークタイプを変更するには、次の手順を実行します。
1. **デバイス**へ移動します。
2. **Networks** タブを選択します。
3. CDE または非 CDE としてマークするネットワークのチェックボックスを選択します。
4. ツールバーの  アイコンの横にある下矢印をクリックします。必要に応じて CDE または非 CDE を選択します。確認メッセージが表示されます。
5. ネットワークタイプを変更するには、確認メッセージで **Yes** をクリックします。
6. ネットワークタイプが変更され、新たなネットワークタイプが Network type カラムの下に表示されます。

Networks ページからのネットワークの削除

Networks タブからネットワークを削除するには、次の手順を実行します。

1. **デバイス**へ移動します。
2. **Networks** タブを選択します。
3. 削除するネットワークのチェックボックスを選択します。
4. ネットワークの削除アイコンをクリックします。
5. ネットワークの削除アイコンをクリックして表示される確認ダイアログで、**Yes** をクリックします。

ロケーションとロケーションレイアウトの管理

管理コンソール(Management Console)では、特定のロケーションに対してロケーションおよびデバイスの配置に関するグラフィカルな表現を持つことができます。 これをロケーションレイアウトと呼びます。 ロケーションフロアのレイアウトは、フロアプランを表します。 同様に、ロケーションフォルダーのレイアウトは、サブロケーションの地理的な配置を表すことができます。
また、ロケーションのレイアウトを見ることで、フロアプラン上の各デバイスの配置と互いに関連するロケーションの配置を把握することができます。

選択したロケーションのレイアウトを管理するために ロケーションページに移動します。 各ロケーションフォルダーとロケーションフロア用に定義されたレイアウトを持つことができます。 そのあと、サブロケーションに配置することができます。 同様に、ロケーションフロアのレイアウト上にデバイスを配置することができます。

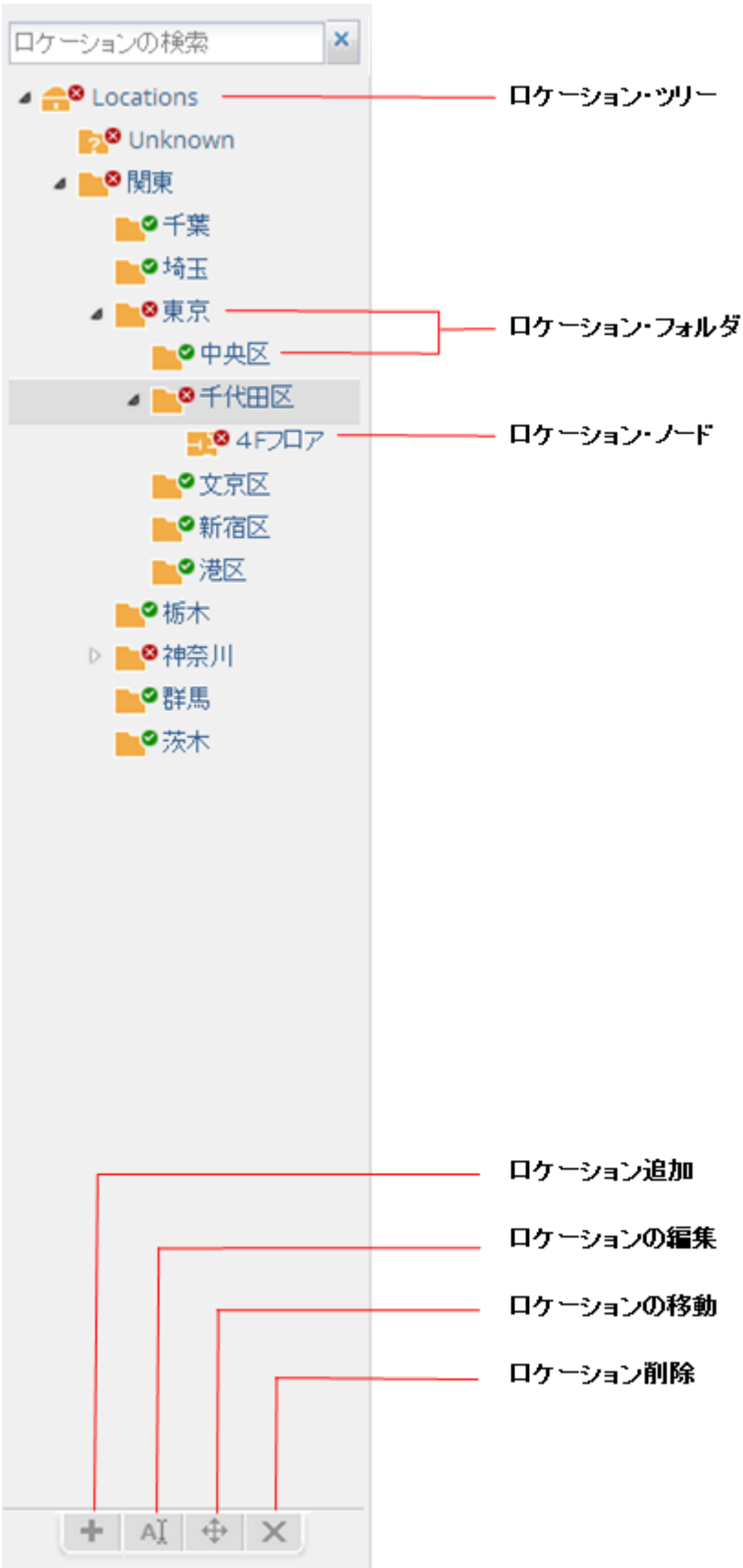
ロケーションツリーの定義

ロケーションページを表示するには、**ロケーション** をクリックします。
ロケーションツリーがページの左側に表示されます。 レイアウトはページの右側に構成されています。

ロケーションツリーは、ロケーションフォルダーやロケーションフロアから構成されます。
ロケーションフォルダーは、建物、都市、または国などの組織的なコンポーネントを表します。
ロケーションフロアは、建物のフロアなどのコンポーネントの詳細を表しています。

ルートロケーションのデフォルトのロケーションフォルダーは **Unknown** フォルダーです。 **Unknown** フォルダーの名前を変更することはできますが、 **Unknown** フォルダーを作成、削除、移動、またはロケーションを追加することはできません。 ロケーション認識デバイスのロケーションタグが不明であるか、判断できない場合は **Unknown** フォルダーにタグ付けされます。 デフォルトで、**Unknown** フォルダーはルートロケーションからデバイス分類と防御ポリシーを除くすべてのポリシーを継承します。 これらのポリシーを変更することが可能です。

下図は、ロケーションツリーを示しています。 下の図の「ロケーションの管理」で示すように、ロケーション追加、ロケーションの編集、ロケーションの移動、ロケーション削除のボタンをクリックします。


ロケーションの検索
Locations
Unknown
関東
千葉
埼玉
東京
中央区
千代田区
4Fフロア
文京区
新宿区
港区
栃木
神奈川
群馬
茨木
ロケーション・ツリー
ロケーション・フォルダ
ロケーション・ノード
ロケーション追加
ロケーションの編集
ロケーションの移動
ロケーション削除

ロケーションの管理

ロケーションフォルダーまたはロケーションフロアを選択して、そのレイアウトを追加します。 ロケーションフォルダーのレイアウトが地理的なマップであり、一方、ロケーションフロアのレイアウトはフロアマップになります。ロケーションフォルダーのレイアウトにロケーションフォルダーやロケーションフロアを追加することができます。ロケーションフロアのレイアウトに、管理コンソール(Management Console)で動作するように構成されたデバイスを追加することができます。 ロケーションやデバイスの配置またはロケーションレイアウトに関連するその他の事項を説明するために、レイアウトにロケーションおよびデバイスのノートを追加することができます。

ロケーションレイアウト内のメッシュネットワーク・トポロジーを図的表現で表示することができます。
ロケーションフォルダーまたはロケーションノードのロケーションレイアウトに追加や変更を加えるには、管理者としてログインする必要があります。

スーパーユーザーとしてサーバークラスタの親サーバーにログインしている場合、サーバークラスタ内の任意のロケーションまたはサーバーのレイアウトを変更することができます。

ロケーションの追加

ロケーションフォルダーを使用して、建物、地理的位置を表すことができます。 ロケーションフロアを使用して、建物内のフロアまたは階層を表すことができます。 ルートロケーションの下または他のロケーションフォルダーの下に 1 つ以上のロケーションフォルダーを追加することができます。ロケーションフォルダーの下に 1 つ以上のロケーションフロアを追加することができます。 **Unknown** フォルダーにロケーションフォルダーまたはロケーションフロアを追加することはできません。 ロケーションフロアの下にロケーションフロアを追加することはできません。

ロケーションフォルダーを追加するには、次の手順を実行します。
1. **ロケーション**に移動します。 ロケーションツリーには、サブフォルダー**Unknown** を持つルートロケーションと作成したロケーションが表示されます。
2. ロケーションフォルダーを追加したいロケーションを選択します。
3. ロケーションツリーの下にある追加アイコン（＋記号）をクリックします。 **ロケーションの新規追加** ダイアログボックスが表示されます。
4. **ロケーションタイプ**を**フォルダー** として選択します。
5. **ロケーション名**にロケーションの名前を入力します。
6. **タイムゾーン**からロケーションの適切なタイムゾーンを選択します。 正しいタイムゾーンを選択することは、正確な分析の生成に不可欠です。
7. **OK** をクリックします。ロケーションフォルダーが、選択したロケーションの下に追加されます。

ロケーションフロアを追加するには、次の手順を実行します。
1. **ロケーション**に移動します。 ロケーションツリーには、サブフォルダー**Unknown** を持つルートロケーションと作成したロケーションが表示されます。
2. ロケーションフロアを追加したいロケーションを選択します。
3. ロケーションツリーの下にある追加アイコン（＋記号）をクリックします。 **ロケーションの新規追加** ダイアログボックスが表示されます。
4. **ロケーションタイプ**を**フロア** として選択します。
5. **ロケーション名**にロケーションの名前を入力します。
6. **OK** をクリックします。ロケーションフロアが、選択したロケーションの下に追加されます。

ロケーションの編集

ロケーションフォルダーまたはロケーションフロアを編集するには、次の手順を実行します。
1. **ロケーション**に移動します。
2. 編集するロケーションフォルダーまたはロケーションフロアを選択します。
3. ロケーションツリーの下にある編集アイコン（文字 'A'）をクリックします。 **ロケーションの編集** ダイアログボックスが表示されます。
4. 必要な変更を行います。
5. **OK** をクリックします。

ロケーションの移動

あるロケーションから別のロケーションにロケーションフォルダーやロケーションフロアを移動するには、次の手順を実行します。
1. **ロケーション**に移動します。
2. 移動するロケーションフォルダーまたはロケーションフロアを選択します。
3. ロケーションツリーの下にある移動アイコン（矢十字）をクリックします。 **宛先のロケーション選択** ダイアログボックスが表示されます。
4. 移動先のロケーションを選択します。
5. **OK** をクリックします。ロケーションフォルダーやロケーションフロアは新しい宛先に移動されます。

ロケーションの削除

ロケーションツリーからロケーションフォルダーまたはロケーションフロアを削除するには、次の手順を実行します。
1. **ロケーション**に移動します。
2. 削除するロケーションフォルダーまたはロケーションフロアを選択します。
3. ロケーションツリーの下にある削除アイコン（×記号）をクリックします。 削除を確認するメッセージが表示されます。
4. 削除を実行するには、**Yes** をクリックします。

ロケーションの検索

ロケーションを検索するには、次の手順を実行します。
1. **ロケーション**に移動します。
2. （ロケーションツリーの上にある）**ロケーションの検索**にロケーションフォルダーまたはロケーションフロアの名前と一致するテキストの部分文字列を入力します。
3. この検索条件が含まれるすべてのロケーションフォルダーとロケーションフロアを表示するには、Enter キーを押します。 テキスト文字列または部分文字列を使用して検索されたあとに、一致するロケーションがロケーションツリーのロケーション階層に表示されます。

ロケーションの検索をクリアするには、**ロケーションの検索**の横にある[X]をクリックします。

レイアウトの追加

選択されたロケーションに定義されたレイアウトがない場合は、**ロケーション**タブ上にロケーションに対してレイアウトが存在しないことを通知する**レイアウトの追加**が表示されます。 レイアウトイメージが追加されると、ロケーションフォルダーのレイアウトイメージにロケーションのメモを追加することができます。 同様に、ロケーションフロアのレイアウトイメージにデバイスやメモを追加することができます。
ロケーションリストを表示 と **ロケーションリストを隠す** をクリックすることで、ロケーションリストを表示/非表示することが可能です。
ロケーションリストからロケーションを選択し、レイアウト上の望ましい位置に配置するためにドラッグすることができます。 同様に、レイアウト上のロケーションを選択し、レイアウトからロケーションを削除するためにロケーションリストに戻すようドラッグすることができます。

ご注意： ロケーションのレイアウトを追加する前に、ロケーションツリーの定義を確認してください。 ロケーションツリーが定義されていないと、ロケーションフォルダーのレイアウト上で配置するいかなるロケーションも持てません。

ロケーションフォルダーにレイアウトを追加するには、次の手順を実行します。
1. **ロケーション**に移動します。
2. ロケーションツリーから、レイアウトを追加したいロケーションフォルダーを選択します。 レイアウトがロケーションに設定されていない場合、**レイアウトの追加**のリンクを伴うメッセージが表示されます。
3. **レイアウトの追加**のリンクをクリックします。
4. **ファイルを選択** をクリックします。 ファイルを開くダイアログボックスが表示されます。
5. 追加する任意のレイアウトイメージのパスを参照し、**開く**をクリックします。 イメージがロケーションに適用されます。 ロケーションのリストを見ることができるようになります。
6. レイアウト上の適切な位置に、ロケーションリストからロケーションをドラッグ＆ドロップします。 ロケーションリストが表示されていない場合、利用可能なロケーションのリストを表示するには、**ロケーションリストを表示** をクリックします。
7. レイアウトを保存する場合は、**保存** をクリックします。

ロケーションフロアにレイアウトイメージを使用してレイアウトを追加するには、次の手順を実行します。
1. **ロケーション**に移動します。
2. ロケーションツリーから、レイアウトを追加したいロケーションフロアを選択します。 レイアウトがロケーションに設定されていない場合、**レイアウトの追加**のリンクを伴うメッセージが表示されます。
3. **レイアウトの追加**のリンクをクリックします。**レイアウトの追加**のダイアログボックスが表示されます。
4. **レイアウトイメージ**の横にある**ファイルを選択**をクリックします。 ファイルを開くダイアログボックスが表示されます。
5. 追加するレイアウトイメージのパスを参照し、**開く**をクリックします。 イメージがロケーションに適用されます。
6. **単位**に寸法の測定単位を選択します。
7. **Length（Horizontal）**にレイアウトイメージの長さ（横方向）を指定します。
8. **Width（Vertical）**にレイアウトイメージの幅（縦方向）を指定します。
9. レイアウト上の適切な位置にデバイスリストからデバイスをドラッグ＆ドロップします。 デバイスリストが表示されていない場合、利用可能なデバイスのリストを表示するには、**デバイスリストを表示** をクリックします。
10. レイアウトを保存する場合は、**保存** をクリックします。

レイアウトの編集

ロケーションフォルダーやロケーションフロアのレイアウトイメージを置き換えることができます。 そのあと、新規のレイアウトイメージ上に再びロケーションまたはデバイスを配置する必要があります。 また、ロケーションフォルダーまたはロケーションフロアに取り付けたレイアウトイメージまたは.spm ファイルを変更することなく、ロケーションレイアウト上のロケーションやデバイスを再配置することが可能です。

レイアウトを編集するには、次の手順を実行します。
1. **ロケーション**に移動します。
2. ロケーションツリーから、レイアウトを編集したいロケーションフロアを選択します。
3. **レイアウトの編集** のリンクをクリックします。
4. 必要な変更を加えます。
5. レイアウトの変更を保存するには、**保存**をクリックします。

レイアウトの削除

ロケーションフォルダーやロケーションフロアに適用したロケーションのレイアウトを削除することができます。 レイアウトを削除すると、すべてのデバイスの配置は取り消されます。

ロケーションフォルダーまたはロケーションフロアに取り付けられたロケーションのレイアウトを削除するには、次の手順を実行します。
1. **ロケーション**に移動します。
2. ロケーションツリーから、レイアウトを削除したいロケーションのフォルダーまたはフロアを選択します。
3. **レイアウトの削除** のリンクをクリックします。 レイアウトの削除を確認するように求められます。
4. レイアウトの削除を実行するには、**Yes** をクリックします。レイアウトが削除されデバイスが見えなくなります。

ロケーションリストの表示/非表示

ハイパーリンクのラベルは、ロケーションリストがレイアウト上に表示されているかどうかに応じて、 **ロケーションリストを隠す** と **ロケーションリストを表示** で切り替わります。

ロケーションリストを表示/非表示するには、次の手順を実行します。
1. **ロケーション**に移動します。
2. ロケーションツリーからロケーションフォルダーまたはロケーションフロアを選択します。
3. レイアウト上にロケーションリストを表示するには、**ロケーションリストを表示** のリンクをクリックします。 ロケーションリストを非表示にするには、**ロケーションリストを隠す** のリンクをクリックします。

ロケーション上のデバイスの表示/非表示

パーリンクのラベルは、レイアウト上にデバイスリストが表示されているかどうかに応じて、**デバイスリストを隠す** と **デバイスリストを表示** で切り替わります。

ロケーションのデバイスリストを表示/非表示するには、次の手順を実行します。
1. **ロケーション**に移動します。
2. ロケーションツリーから、ロケーションフォルダーまたはロケーションフロアを選択します。
3. デバイスリストを表示するには、**デバイスリストを表示** のリンクをクリックします。 デバイスリストを非表示にするには、**デバイスリストを隠す** のリンクをクリックします。

レイアウト上にデバイス/ロケーションを配置

ロケーションは、ロケーションフォルダーのレイアウト上に配置することができます。 デバイスは、ロケーションフロアのレイアウト上に配置することができます。
ロケーションフォルダーのレイアウト上にロケーションを配置するには、ロケーションフォルダーにレイアウトを追加する必要があります。 同様に、ロケーションフロアのレイアウト上にデバイスを配置するには、ロケーションフロアにレイアウトを追加する必要があります。
サーバークラスタ内の親サーバーにログインして作業している場合は、ロケーションレイアウト上でサーバーを配置することはできません。

ロケーションフォルダーのレイアウト上にロケーションを配置するには、次の手順を実行します。
1. **ロケーション**に移動します。
2. ロケーションツリーから、ロケーションフォルダーを選択します。
3. ロケーションリストからロケーションを選択し、ロケーションレイアウト上の希望の位置にロケーションをドラッグ＆ドロップします。
4. ロケーションレイアウト上のロケーションの配置を保存するには、**保存**をクリックします。

ロケーションフロアのレイアウト上にデバイスを配置するには、次の手順を実行します。
1. **ロケーション**に移動します。
2. ロケーションツリーから、ロケーションフロアを選択します。
3. デバイスリストからデバイスを選択し、ロケーションレイアウト上の希望の位置にドラッグ＆ドロップします。
4. ロケーションレイアウト上のデバイスの配置を保存するには、**保存**をクリックします。

ロケーションレイアウトからデバイス/ロケーションを削除

ロケーションフォルダーのレイアウト上に配置されたロケーションを削除することができます。 同様に、ロケーションフロアのレイアウト上に配置されたデバイスを削除することができます。

ロケーションフォルダーのレイアウトからロケーションを削除するには、次の手順を実行します。
1. **ロケーション**に移動します。
2. ロケーションツリーから、ロケーションフォルダーを選択します。 ロケーションレイアウト上に、配置されているロケーションが表示されます。
3. ロケーションレイアウトから削除するロケーションにマウスを移動します。 ロケーションの右側にゴミ箱のアイコンが表示されます。
4. ロケーションレイアウトからロケーションを削除するには、ゴミ箱のアイコンをクリックします。
5. 変更を保存するには、**保存** をクリックします。

ロケーションフロアのレイアウトからデバイスを削除するには、次の手順を実行します。
1. **ロケーション**に移動します。
2. ロケーションツリーから、ロケーションフロアを選択します。 ロケーションレイアウト上に、配置されているデバイスが表示されます。
3. ロケーションレイアウトから削除するデバイスにマウスを移動します。 デバイスの右側にゴミ箱のアイコンが表示されます。
4. ロケーションレイアウトからデバイスを削除するには、ゴミ箱のアイコンをクリックします。
5. 変更を保存するには、**保存** をクリックします。

RF カバレッジ/ヒートマップビュー

ヒートマップビューでは、利用可能な AP カバレッジ、センサーカバレッジを選択することで、 ロケーションフロアのヒートマップや RF カバレッジを表示することが可能です。

- AP カバレッジ
- センサーカバレッジ
- AP リンクスピード
- AP チャネルカバレッジ

AP カバレッジビューは、レイアウト上の各ポイントで dBm に基づいて IEEE802.11 RF カバレッジマップの表示を有効にします。 この情報は、各ポイントで利用可能な信号強度を知ることに有用です。 使用される色分けは、マップの読みやすさを向上させます。

センサーカバレッジビューは、選択されたセンサーの可視性の検知と防御のゾーンを表示することができます。 検出範囲は、センサーが送信出力スライダーで設定された値を超える電力レベルで動作する無線アクティビティを確実に検出することができるエリアです。 侵入検知表示の閾値は、この範囲の閾値を決定します。
防御範囲は、センサーが許可されていない無線アクティビティを防ぐことができるエリアです。

AP チャネルビューでは、フロア上の各ポイントで接続に使用できる、すべての IEEE802.11 チャネルを表示することができます。 それは、潜在的なチャネル干渉のシナリオを防止するのに役立ちます。

AP リンクスピードビューでは、特定のポイントでクライアントがフロア上で AP に接続することができる最大のダウンリンク速度を表示できます。

使用される色分けスキームはマップの読みやすさを向上させます。

ロケーションフロアでライブ RF カバレッジマップを表示するには、許可 AP(Authorized AP)とセンサーをロケーションフロアのロケーションレイアウト上に配置する必要があります。

AP カバレッジ表示

AP カバレッジを表示するには、次の手順を実行します。
1. **ロケーション**に移動します。
2. ロケーションツリーから、AP カバレッジを表示したいロケーションフロアを選択します。
3. デバイスが配置されていない場合は、ロケーションのレイアウト上にデバイスを配置します。
4. **ヒートマップ表示** の下したにある **AP カバレッジ**の リンクをクリックします。
5. IEEE802.11a モードで動作する AP を表示する場合は IEEE802.11a を選択します。
6. IEEE802.11b/g モードで動作する AP を表示する場合は IEEE802.11b/g を選択します。
7. 解像度で適切な解像度を選択します。

RSSI 値による AP カバレッジ表示

ロケーションマップ上に配置されるすべての許可 AP(Authorized AP)が提供する AP カバレッジを表示するために RSSI 値を選択することができます。 それは、異なるスレッショルド(閾値)値で RSSI カバレッジの境界線を理解するのに役立ちます。

RSSI 値による AP カバレッジを表示するには、次の手順を実行します。
1. **ロケーション**に移動します。
2. ロケーションツリーから、AP カバレッジを表示したいロケーションフロアを選択します。
3. デバイスが配置されていない場合は、ロケーションのレイアウト上にデバイスを配置します。
4. **ヒートマップ表示**の下したにある **AP カバレッジ** のリンクをクリックします。
5. IEEE802.11a モードで動作する AP を表示する場合は IEEE802.11a を選択します。
6. IEEE802.11b/g モードで動作する AP を表示する場合は IEEE802.11b/g を選択します。
7. RSSI 値のチェックボックスを選択し、要求する RSSI 値にスライダーを移動します。 選択された RSSI で AP がカバーするエリアがロケーションマップ上に表示されます。

センサーカバレッジ表示

センサーカバレッジを表示するには、次の手順を実行します。
1. **ロケーション**に移動します。
2. ロケーションツリーから、センサーカバレッジを表示したいロケーションフロアを選択します。
3. デバイスが配置されていない場合は、ロケーションのレイアウト上にデバイスを配置します。
4. **ヒートマップ表示** の下したにある **センサーカバレッジ** のリンクをクリックします。
5. IEEE802.11a モードで動作する AP を表示する場合は IEEE802.11a を選択します。
6. IEEE802.11b/g モードで動作する AP を表示する場合は IEEE802.11b/g を選択します。
7. 解像度で適切な解像度を選択します。
8. センサーとして機能する管理デバイス(Management Device)の視認性の検出ゾーンを表示する場合は**検出**を選択します。
9. センサーとして機能する管理デバイス(Management Device)の視認性の防御ゾーンを表示する場合は**防御**を選択します。
10. 送信出力を選択します。センサーカバレッジを見ることができます。

AP リンクスピード表示

AP リンクスピードを表示するには、次の手順を実行します。
1. **ロケーション**に移動します。
2. ロケーションツリーから、AP リンクスピードを表示したいロケーションフロアを選択します。
3. デバイスが配置されていない場合は、ロケーションのレイアウト上にデバイスを配置します。
4. **ヒートマップ表示** の下したにある **AP リンクスピード** のリンクをクリックします。
5. IEEE802.11a モードで動作する AP を表示する場合は IEEE802.11a を選択します。
6. IEEE802.11b/g モードで動作する AP を表示する場合は IEEE802.11b/g を選択します。
7. 解像度で適切な解像度を選択します。

AP チャネルカバレッジ表示

AP チャネルカバレッジを表示するには、次の手順を実行します。
1. **ロケーション**に移動します。
2. ロケーションツリーから、AP チャネルカバレッジを表示したいロケーションフロアを選択します。
3. デバイスが配置されていない場合は、ロケーションのレイアウト上にデバイスを配置します。
4. **ヒートマップ表示** の下したにある **AP チャネルカバレッジ** のリンクをクリックします。
5. IEEE802.11a モードで動作する AP を表示する場合は IEEE802.11a を選択します。
6. IEEE802.11b/g モードで動作する AP を表示する場合は IEEE802.11b/g を選択します。
7. 解像度で適切な解像度を選択します。

RF ビューのキャリブレーション

キャリブレーションは、実際の観測と AP およびセンサーの予測を比較するために WIPS センサーが使用する RF パラメータのチューニングに役立ちます。 RF ビューを校正する際に、予測対観測の信号強度のグラフを表示することができます。
WIPS センサーはまた不一致の場合には手動の介入を可能にする強固なキャリブレーション技術を持っています。 予測を改善するために、最小信号減衰指数と最大信号減衰指数を微調整することができます。

最小信号減衰指数は、送信機（センサー）に近い領域で許容可能な信号損失の量を指定します。 最大信号減衰指数は、送信機から離れた領域で許容可能な信号損失の量を指定します。 信号損失は信号減衰指数に正比例します。

ご注意： 予測値の曲線は、できるだけ多く観測値の曲線に重なる必要があります。

最小信号減衰指数、最大信号減衰指数、信号減衰スロープ（Beta）、信号減衰のインフレクション（Alpha）を変更すると、RF ビューと遮るもののない領域のロケーショントラッキングが影響を受けます。 閉塞した領域では、ロケーショントラッキングは影響を受けますが RF ビューは影響を受けません。 手動でキャリブレーションを行うとグラフが自動的に更新されます。

自動的に RF ビューをキャリブレーションするには、次の手順を実行します。

1. **ロケーション**に移動します。
2. ロケーションツリーから、RF ビューをキャリブレーションしたいロケーションを選択します。
3. RF カバレッジ/ヒートマップビューセクションで説明されるステップで、RF カバレッジ/ヒートマップビューを生成します。
4. **キャリブレーション** のリンクをクリックすると、キャリブレーションのダイアログボックスが表示されます。
5. 自動的にキャリブレーションを行うには、**自動キャリブレーション** の下にある **キャリブレート** をクリックします。
6. 手動でキャリブレーションを行うには、手動キャリブレーションを選択後、信号減衰指数の最小値、信号減衰指数の最大値、信号減衰スロープ（Beta）、信号減衰のインフレクション（Alpha）の値を変更します。 システムは RF を計算する際に、これらのパラメータを使用して障害物がない送信機周辺の領域を規定します。
7. 確実に調整します。
8. 2 つの曲線が平行（ただし一致しない）になるように手動でパラメータを調整した場合は、**OK** または **適用** をクリックします。

ご注意： コンフィグレーション>システム設定>高度な設定>ライブ RF ビュー設定 で、 侵入検知の表示スレッショルド(閾値)と侵入防御の表示スレッショルド(閾値)を変更することが可能です。

レイアウトの縮小/拡大

ズーム スライダーは **ロケーション** ページの左側にあります。 レイアウトを拡大するには**ズーム**スライダーを上に移動させます。 レイアウトを縮小するには**ズーム**スライダーを下に移動させます。

ヒートマップのレンダリングに適切な解像度を選択します。 低解像度では、高画素化の効果はないが高速なレンダリングを意味します。 高解像度では、値を計算するピクセルの数が大きくなるため、レンダリングが遅くなります。 実際のサイズの 400%まで拡大することができ、25%まで縮小することができます。

レイアウトの不透明度を調整

レイアウトの不透明度を調整するために、**不透明度** スライダーを左右に移動します。 このスライダーは、**ロケーション**ページの右上にあります。

- より良い方法で RF カバレッジを把握するためにはイメージの不透明度を下げます。
- 正確なデバイス配置情報を正確に特定するにはイメージの不透明度を上げます。

ノートの追加

ロケーションのレイアウトにメモを追加することができます。 これらは、デバイスやレイアウトに関連する追加の説明文またはコメントなどに使用することができます。

ロケーションのレイアウトにノートを追加するには、次の手順を実行します。
1. **ロケーション**に移動します。
2. 目的のロケーションを選択します。 レイアウトが追加されていることを確認してください。 レイアウトが追加されていない場合、はじめにレイアウトを追加します。
3. **ノートの追加** のリンクをクリックします。
4. ノートの名前を入力します。
5. ノートの説明を入力します。
6. **OK** をクリックします。マウスを使ってノートを移動します。
7. レイアウト上の目的の位置にマウスをポイントします。
8. ポイントした位置にノートを配置するには、マウスをクリックしてください。

ノートの編集

ロケーションのレイアウトに配置されたノートを編集するには、次の手順を実行します。
1. **ロケーション**に移動します。
2. 編集するノートが存在するロケーションを選択します。
3. 編集するノートの上にマウスをおききます。鉛筆のアイコンが表示されます。
4. ノートを編集するには、鉛筆のアイコンをクリックします。
5. 名前や説明に必要な変更を行います。
6. 変更内容を保存するには、**OK** をクリックします。

ノートの移動

ロケーションのレイアウト上の別の位置に既存のノートを移動することができます。

レイアウト上のある位置から同じレイアウト上の別の位置にノートを移動するには、次の手順を実行します。
1. **ロケーション**に移動します。
2. 移動するノートがおきかれているロケーションを選択します。
3. ロケーションのレイアウト上の希望する位置に、マウスでノートをドラッグ＆ドロップします。ノートが新しい位置に移動されます。

ノートを非表示

ロケーションのレイアウト上におきかれている既存のノートを非表示にすることができます。

既存のノートを非表示にするには、次の手順を実行します。
1. **ロケーション**に移動します。
2. ノートがおきかれている目的のロケーションを選択します。
3. ノートを非表示にするには、**ノートを非表示** のリンクをクリックします。

ノートを表示

ロケーションのレイアウト上で隠れたノートを表示することができます。

既存のノートを表示するには、次の手順を実行します。
1. **ロケーション**に移動します。
2. ノートがおきかれている目的のロケーションを選択します。
3. ノートを表示にするには、**ノートを表示** のリンクをクリックします。

メッシュ・トポロジの表示

ロケーションページ上で、メッシュ AP として機能するアクティブな管理デバイス(Management Device)の図的表現を確認することができます。 無線メッシュネットワークを形成するために互いに接続されたルートおよび非ルートメッシュ AP の配置を見ることができます。

メッシュ・トポロジを表示するには、次の手順を実行します。
1. **ロケーション**に移動します。
2. **メッシュ・トポロジを表示** のリンクをクリックします。AP のメッシュネットワークが表示されます。

ご注意：メッシュ AP が適切に構成されていることを確認するのは、システム/ネットワーク管理者の責任です。 **ロケーション**ページでは、単にメッシュ AP として管理デバイス(Management Device)の設定に基づくメッシュ・トポロジを表示します。

メッシュ・トポロジを非表示

ロケーションのレイアウト上で、メッシュ・トポロジを非表示にすることができます。

メッシュ・トポロジを非表示するには、次の手順を実行します。
1. **ロケーション**に移動します。
2. **メッシュ・トポロジを隠す** のリンクをクリックします。 AP のメッシュネットワークのグラフィック表示が隠されます。

イベントの表示と管理

イベントページは、システムによって生成されたイベントに関する情報を提供します。 このページでは、イベントの閲覧、フィルター、ロケーションの変更、未読または既読としてマーク、脆弱性の評価でイベントの状態を切り替えることが可能です。 また、ロケーションで表示されるイベントのリストを印刷することができます。

WIPS センサーは次のタイプにイベントを分類します。

- セキュリティ
- システム
- パフォーマンス

セキュリティイベントは、無線セキュリティの脅威に関連しています。 例えば、不正 AP(Rogue AP) がネットワークにアクセスしようと試みると、セキュリティイベントが生成されます。

セキュリティイベントは、更に無線セキュリティの脅威に基づいて分類されます。次のようなセキュリティイベントのカテゴリがあります。

- 不正 AP(Rogue AP)によって生成されるイベント
- 誤設定された AP(Misconfigured AP)によって生成されるイベント
- 不正なクライアント (misbehaving client)によって生成されるイベント
- アドホックネットワークによって生成されるイベント
- 中間者攻撃(man-in-the-middle attacks)によって生成されるイベント
- DoS 攻撃（サービス拒否）に起因して生成されるイベント
- MAC なりすましに起因して生成されるイベント
- 防御に起因して生成されるイベント
- 無線の収集活動に起因して生成されるイベント
- 無線ネットワークのクラッキングに起因して生成されるイベント

システムイベントは、システムの正常性を示します。 センサー、管理コンソールサーバーそしてトラブルシューティングによって生成されるイベントに基づいて、更に分類されます。

パフォーマンスイベントは、無線ネットワークのパフォーマンスの問題を示しています。 帯域幅、設定、カバレッジ、および干渉に基づいて、更に分類されます。 これらは、無線ネットワークのパフォーマンスに関連する問題を理解するために使用することができます。

イベントページは 2 つのパネルに分かれています。 上のパネルには選択したロケーションのイベントリストが表示されます。 下のパネルのサブイベントの詳細では、**イベント**ページの上のパネルで選択したイベントに関与するイベントとサブイベント内のデバイスの詳細を表示します。

上下のパネルの間にはツールバーがあります。 これには、イベントのロケーション変更やイベントの脆弱性ステータスの変更、イベントの削除、イベントの印刷など、多様なイベント関連の操作を実行するためのアイコンが含まれています。

次の表は、上部パネルのイベント関連のフィールドについて説明します。

フィールド	説明
ID	システムがイベントに対して生成したイベント ID です。
イベント深刻度	イベントの深刻度がアイコンによって示されます。 深刻度は高、中、低のいずれかです。
イベントのアクティビティ・ステータス	イベントのステータスがアイコンで示されます。ステータスは、ライブ、瞬間的(instantaneous)、更新済み、期限切れのいずれかです。
詳細	イベントの説明です。
カテゴリ	イベントのカテゴリです。
ロケーション	イベントが発生したロケーションです。
開始時間	イベントが開始した時間です。
イベントのリード・ステータス	イベントが既読、未読、承認または未承認かどうかを示します。
イベントの脆弱性ステータス	イベントの脆弱性を示します。
イベントタイプ	イベントのタイプがアイコンで示されます。 イベントタイプは、セキュリティ、システム、パフォーマンスのいずれかです。
停止時間	イベントが停止した時刻です。

ロケーションのイベントを表示

イベントカテゴリに基づいて選択したロケーション（とその子ロケーション）でのイベントを表示することができます。 それらのカテゴリとサブカテゴリに基づいて、イベントをフィルタリングすることができます。

ロケーションに関するイベントを表示するには、次の手順を実行します。

1. **イベント**へ移動します。
2. イベントを表示したいロケーションを選択します。
3. ネットワーク内のセキュリティの脆弱性や違反を示すイベントを表示するには、**セキュリティ** のチェックボックスにチェックを入れます。それぞれのセキュリティイベントでチェックボックスを選択または解除することで、セキュリティイベントを表示または非表示にすることができます。 セキュリティイベントのリストを表示するには、「セキュリティ」文字の隣の三角形をクリックします。
4. システムの健全性を示すイベントを表示するには、**システム** のチェックボックスにチェックを入れます。 それぞれのシステムイベントでチェックボックスを選択または解除することで、タイプに基づいてシステムイベントを表示または非表示にすることができます。 システムイベントのリストを表示するには、「システム」文字の隣の三角形をクリックします。
5. 無線ネットワークのパフォーマンス問題を示すイベントを表示するには、**パフォーマンス** のチェックボックスにチェックを入れます。 それぞれのパフォーマンスイベントでチェックボックスを選択または解除することで、タイプに基づいてパフォーマンスイベントを表示または非表示にすることができます。 パフォーマンスイベントのリストを表示するには、「パフォーマンス」文字の隣の三角形をクリックします。

ご注意： サーバークラスタ内の親サーバー上のルートロケーションを表示している場合は、子サーバーと親サーバー上のすべてのイベントが集約されています。 現在、親サーバーのみに属するイベントを表示する適切なメカニズムはありません。

ロケーションで削除されたイベントを表示

削除としてマークしたイベントを表示するには、次の手順を実行します。
1. **イベント**へ移動します。
2. 削除されたイベントを表示したいロケーションを選択します。
3. ツールバーの**更に**をクリックし、**削除されたイベントを表示**を選択します。 イベントは削除としてマークされます。

イベントロケーションの変更

イベントのロケーションを変更するには、次の手順を実行します。
1. **イベント**へ移動します。
2. イベントが発生したロケーションを選択します。
3. ロケーションを変更したいイベントのチェックボックスにチェックを入れます。
4. 「ロケーションの変更」アイコンをクリックします。 ロケーションを選択するダイアログボックスが表示されます。
5. 新しいロケーションを選択し、[OK]をクリックします。イベントは、新しいロケーションに移動されます。

イベントを承認

イベントを承認するには、次の手順を実行します。
1. **イベント**へ移動します。
2. イベントを承認したいロケーションを選択します。
3. 承認したいイベントのチェックボックスを選択し、ツールバーの「承認」アイコンをクリックします。
4. 「承認」ダイアログボックスが表示されます。ノートを入力し、[OK]をクリックします。

イベントの脆弱性ステータスをオン

イベントの脆弱性ステータスをオンにするには、次の手順を実行します。
1. **イベント**へ移動します。
2. イベントの脆弱性ステータスを変更したいロケーションを選択します。
3. 脆弱性ステータスをオンにするイベントのチェックボックスを選択します。
4. イベントの脆弱性をオンにするには、「脆弱性のステータスをオン」アイコンをクリックします。

イベントの脆弱性ステータスをオフ

イベントの脆弱性ステータスをオフにするには、次の手順を実行します。
1. **イベント**へ移動します。
2. イベントの脆弱性ステータスを変更したいロケーションを選択します。
3. 脆弱性ステータスをオフにするイベントのチェックボックスを選択します。
4. イベントの脆弱性をオフにするには、「脆弱性のステータスをオフ」アイコンをクリックします。

既読としてイベントをマーク

既読としてイベントをマークするには、次の手順を実行します。
1. **イベント**へ移動します。
2. 既読としてマークしたいイベントのロケーションを選択します。
3. 既読としてマークしたいイベントのチェックボックスにチェックを入れます。
4. ツールバーの**更に**をクリックし、**既読としてマーク**を選択します。 イベントは既読としてマークされます。

削除としてイベントをマーク

削除済みとしてイベントをマークするには、次の手順を実行します。
1. **イベント**へ移動します。
2. イベントを削除したいロケーションを選択します。
3. 削除としてマークしたいイベントのチェックボックスにチェックを入れます。
4. ツールバーの**更に**をクリックし、**削除済みとしてマーク**を選択します。 イベントは削除済みとしてマークされます。

カスタムフィルターを追加

カスタムフィルターを作成し、任意の名前で保存することができます。 管理コンソール (Management Console)上に表示される列内のデータのフィルター条件を設定することができます。 名前を付けてこのフィルターを保存することができ、同様に複数のフィルターを作成することが可能です。

カスタムフィルターを使用する際は、次の点に注意してください。
- 列の可視性と列データのソート設定は、カスタムフィルターには保存されません。 フィルター基準のみが保存されます。
- カスタムフィルターは、ユーザー固有です。 これはカスタムフィルターを定義したユーザー用に保存され、他のユーザーには見えません。
- 保存されていないフィルターは、ツールバーの**フィルター**の横にあるフィルター名にアスタリスクで示されます。
- ユーザーがフィルターを保存せずにログアウトした場合、未保存のフィルターは保存されません。

カスタムフィルターを作成するには、次の手順を実行します。
1. **イベント**へ移動します。
2. 列のヘッダーの横にあるアイコンをクリックします。オプションのリストが表示されます。
3. **フィルター**にマウスをポイントして、カラムのフィルターテキストを入力し、**Enter** キーを押します。
4. ツールバーの**フィルター**の横にあるアイコンをクリックして、 **名前を付けて保存**をクリックします。 **名前を付けて保存**のダイアログボックスが表示されます。
5. カスタムフィルターの名前を入力し、**OK** をクリックします。 カスタムフィルターが保存されます。

カスタムフィルターの編集

カスタムフィルターを編集するには、次の手順を実行します。
1. **イベント**へ移動します。
2. **フィルター**の横にある アイコンをクリックして、必要なフィルターを選択します。
3. 列のヘッダーの横にあるアイコンをクリックします。オプションのリストが表示されます。
4. **フィルター**にマウスをポイントして、列のフィルターテキストを入力するか、必要に応じてのフィルター条件を変更します。
5. ツールバーの**フィルター**の横にあるアイコンをクリックして、 **保存**をクリックします。 変更されたカスタムフィルターが保存されます。

カスタムフィルターの削除

カスタムフィルターを削除するには、次の手順を実行します。
1. **イベント**へ移動します。
2. ツールバーの**フィルター**の横にあるアイコンをクリックして、 アイコンをクリックします。 削除を確認するよう問いかけるメッセージが表示されます。
3. カスタムフィルターの削除を確定するために、**Yes** をクリックします。

ロケーションのイベントリストを印刷

ロケーションで生成されるイベントのリストを印刷することができます。paginated view が有効になっている場合は、選択したロケーションのすべてのイベントの一覧が印刷されます。paginated view が無効になっている場合は、現在表示中のページに表示されているイベント一覧だけが印刷されます。印刷する前に paginated view を有効または無効にする必要があります。

ロケーションでイベントのリストを印刷するには、次の手順を実行します。
1. **イベント**へ移動します。
2. ベントリストを印刷したいロケーションを選択します。
3. リストに印刷する列を選択します。 列を選択または解除するには、上のパネルで任意のカラム名をクリックします。
4. 印刷アイコンをクリックします。 ロケーションのすべてのイベントリストの印刷プレビューが表示されます。
5. リストを印刷するには、**印刷**をクリックします。

フォレンジック

フォレンジックページを利用して、ネットワーク内で検出された無線 の脅威に関するフォレンジックデータを集計することができます。 **管理コンソール**は、検出された脅威に関する重要な詳細をキャプチャし、**フォレンジック**ページの分かりやすい形式でそれらを提示します。 このページでは、そのようなデバイスの ID や構成、接続記録、デバイスのロケーション、 システム応答、および検出されたワイヤレス脅威に関する管理者のアクションなど の詳細を確認することができます。

フォレンジック ページは、選択したロケーションで発生した AP 関連 の脅威とクライアント関連の脅威を提示します。選択したロケーションに関するこれらの脅威はリストとして、そして円グラフとして表示されます。 リストと円グラフは並べて表示されます。AP 関連の脅威のリストとその円グラフが上部に表示されます。 クライアント関連の脅威のリストとその円グラフは下部に表示されます。
円グラフは、脅威に関する概要情報を表示します。

AP 関連の脅威： これらは、主に関与する/影響するデバイスが AP である脅威です。
以下のとおり、AP 関連の脅威は更に分類されます。

- Rogue AP
- Mis-configured AP
- Honeypot AP
- Banned AP
- DoS

クライアント関連の脅威: これらは、主に関与する/影響するデバイスがクライアントである脅威です。
以下のとおり、クライアント関連の脅威は更に分類されます。

- Unauthorized Association
- Mis-association
- Bridging Client
- Banned Client
- Ad hoc Networks

円グラフ形式の表示**デバイス**（円グラフ上の）をクリックすると、AP タイプまたはクライアントタイプに基づく円グラフ表示を見ることができます。 'デバイス'は、脅威のタイプに関与した一意のプライマリデバイスの数を明示します。
インスタンス（円グラフ上の）をクリックすると、イベントタイプに基づく円グラフ表示を見ることができます。 'インスタンス'は、与えられた時間枠内のそれぞれのタイプの脅威の数を明示します。

経過時間に基づいて脅威をフィルタリングすることができます。これを行うには、 **期間選択**のドロップダウンリストから、過去 4 時間、過去 12 時間、過去 24 時間、 もしくは過去 48 時間を選択します。カスタムの期間に基づいて脅威を表示するには、 **期間選択**から**カスタム**を選択し、開始日と終了日を選択して、 **適用**をクリックします。

AP 関連/クライアント関連の脅威の詳細を表示

AP/クライアント関連の脅威のリストで、脅威のタイプをクリックすると、 この脅威のタイプに該当するすべてのイベントと、それぞれのイベントに関与するデバイスリストが表示されます。これは、その脅威の種類を詳細に集計し、 AP 関連/クライアント関連の脅威が検出されたときに実行されるアクションを決定するための参考となります。

ページ前半に脅威の詳細やイベントが表示されます。 ページ後半は、関与しているデバイスの詳細と管理者の操作ログが表示されます。 ページ中央には、ページ前半に表示されるイベントに関連するさまざまな操作ができるツールバーがあります。

ロケーションに対する脅威を表示させるには、次の手順を実行します。

1. **フォレンジック**へ移動します。
2. 脅威を表示するロケーションを選択すると、 選択したロケーションの AP とクライアント関連の脅威が表示されます。
3. 脅威を表示する時間間隔を決めるには、**期間を選択**の隣にある時間をクリックします。 この期間の AP に関連する脅威と、クライアントに関連する脅威が、表示されます。
4. AP 関連の脅威またはクライアント関連の脅威で、脅威のタイプをクリックします。 選択された期間中に発生したこの脅威のカテゴリに該当する、すべてのイベントが表示されます。 次の表は、脅威の詳細に表示されるフィールドを説明します。

フィールド	説明
ID	イベント ID
イベントの深刻度	イベントの深刻度を示します。 アイコンで表示され、高、中、低に分類されます。
詳細	イベントの説明
開始時間	イベントの開始時間
停止時間	イベントの停止時間
イベントのリード・ステータス	イベントが読み込まれたかどうかを示し、 アイコンで表示されます。
イベントの 脆弱性ステータス	イベントがロケーションの脆弱性の要因となるかどうかを示し、アイコンで表示されます。
ロケーション	イベントのロケーション
カテゴリ	イベントのカテゴリ
イベントタイプ	イベントの種類がアイコンで表示され、セキュリティとパフォーマンスに分類されます。

デバイスベースでイベントをフィルター

デバイスに関する脅威の詳細に表示されるイベントを、フィルターすることができます。 このデバイスのイベントを表示させるには、適切なデバイスを選択します。
すべてのデバイスのイベントを表示させるには、**すべてのデバイス** を選択してください。

イベント概要の表示

ロケーションに対する脅威を表示させるには、次の手順を実行します。
1. **フォレンジック**へ移動します。
2. 脅威を表示するロケーションを選択すると、 選択したロケーションの AP とクライアント関連の脅威が表示されます。
3. 脅威を表示する時間間隔を決めるには、**期間を選択**の隣にある時間をクリックします。 この期間の AP に関連する脅威と、クライアントに関連する脅威が、表示されます。
4. AP またはクライアントの詳細を表示させるためには、イベント行の ID をクリックします。 推奨アクションとアクノレッジ・トレイルが表示されます。 推奨アクションは、脅威の性質、脅威の影響、そして影響を緩和するために推奨されるアクションを説明します。 イベントが承認されている、または脆弱性がオン/オフされた場合には、このアクティビティに対するコメントのトレイルが表示されます。

関与するデバイスと隔離ステータスの表示

AP 関連の脅威では、AP はプライマリデバイスです。 クライアント関連の脅威の場合には、AP はプライマリデバイス（クライアント）に 関連付けられたデバイスです。
AP 関連の脅威の場合には、 クライアントはプライマリデバイス（AP）に関連付けられたデバイスです。 クライアント関連の脅威の場合には、クライアントはプライマリデバイスです。

フォレンジックに表示されるイベントを選択すると、イベントに関与しているデバイスの詳細を表示することができます。 また、これらのデバイスの隔離ステータスを表示することができます。

関与しているデバイスの詳細、および隔離ステータスを表示するには、次の手順を実行します。
1. **フォレンジック**へ移動します。
2. 脅威を表示するロケーションを選択すると、 選択したロケーションの AP とクライアント関連の脅威が表示されます。
3. 脅威を表示する時間間隔を決めるには、**期間を選択**の隣にある時間をクリックします。 この期間の AP に関連する脅威とクライアントに関連する脅威が表示されます。
4. AP 関連の脅威またはクライアント関連の脅威で、脅威のタイプをクリックします。 選択された期間中に発生したこの脅威のカテゴリに該当するすべてのイベントが表示されます。
5. イベント行を選択すると、イベントリストの下にある関与するデバイスセクション内に、関与するデバイスが表示されます。 以下のフィールドが関与するデバイスで表示されます。

フィールド	説明
AP	AP の名前
クライアント	クライアントの名前
アソシエーション開始時間	プライマリデバイスとそのデバイスとのアソシエイト開始時刻
アソシエーション終了時間	プライマリデバイスとそのデバイスとのアソシエイト終了時刻

関与するデバイスの位置

AP 関連またはクライアント関連の脅威が発生させた関与するデバイスの位置を、確認することができます。

1. **フォレンジック**へ移動します。
2. 脅威を表示するロケーションを選択すると、 選択したロケーションの AP とクライアント関連の脅威が表示されます。
3. 脅威を表示する時間間隔を決めるには、**期間を選択**の隣にある時間をクリックします。 この期間の AP に関連する脅威と、クライアントに関連する脅威が、表示されます。
4. AP 関連の脅威またはクライアント関連の脅威で、脅威のタイプをクリックします。 選択された期間中に発生したこの脅威のカテゴリに該当する、すべてのイベントが表示されます。
5. イベント行を選択すると、イベントリストにある関与するデバイスセクション内に関与するデバイスが表示されます。
6. **関与するデバイス**で、デバイスを確認するために**ロケート**をクリックしてください。 選択した時点のデバイスの位置がマップ上に表示されます。 脅威が検出されたロケーションに設定されているフロアマップ上に、デバイスが表示されます。 検出しているデバイスから検出されたデバイスの距離を確認するには、**近接表示に切り替え**をクリックします。 現在認識できる表示に応じて、**マップ表示に切り替え**と**近接表示に切り替え**を切り替えます。

管理アクションログを表示

管理者のアクションログは、イベントの開始時間と終了時間の間に AP で行われたすべての管理者のアクションを 示しています。

イベントの管理アクションログを表示するには、次の手順を実行します。

1. **フォレンジック**へ移動します。
2. 脅威を表示するロケーションを選択すると、 選択したロケーションの AP とクライアント関連の脅威が表示されます。
3. 脅威を表示する時間間隔を決めるには、**期間を選択**の隣にある時間をクリックします。 この期間の AP に関連する脅威と、クライアントに関連する脅威が、表示されます。
4. AP 関連の脅威またはクライアント関連の脅威で、脅威のタイプをクリックします。 選択された期間中に発生したこの脅威のカテゴリに該当するすべてのイベントが表示されます。
5. イベントの管理者アクションログを表示するには、ページの後半で 2 をクリックしてください。 次の表は、管理者アクションログに表示されるフィールドを説明します。

フィールド	説明
ユーザー	脅威に対してアクションを実行したユーザーの名前
アクション	脅威に対してユーザーが実行した対応措置の内容
時間	脅威に対してユーザーがアクションを実行した時刻

イベントの承認

イベントを承認するには、次の手順を実行します。
1. **フォレンジック**へ移動します。
2. 脅威を表示するロケーションを選択すると、 選択したロケーションの AP とクライアント関連の脅威が表示されます。
3. 脅威を表示する時間間隔を決めるには、**期間を選択**の隣にある時間をクリックします。 この期間の AP に関連する脅威と、クライアントに関連する脅威が、表示されます。
4. AP 関連の脅威またはクライアント関連の脅威で、脅威のタイプをクリックします。 選択された期間中に発生したこの脅威のカテゴリに該当するすべてのイベントが表示されます。 次の表は、脅威の詳細に表示されるフィールドを説明します。
5. 承認したいイベントのチェックボックスにチェックを入れます。
6. 承認アイコンをクリックします。
7. ノートを入力し OK をクリックします。

イベントのロケーションを変更

イベントのロケーションを変更するには、次の手順を実行します。
1. **フォレンジック**へ移動します。
2. 脅威を表示するロケーションを選択すると、 選択したロケーションの AP とクライアント関連の脅威が表示されます。
3. 脅威を表示する時間間隔を決めるには、**期間を選択**の隣にある時間をクリックします。 この期間の AP に関連する脅威と、クライアントに関連する脅威が、表示されます。
4. AP 関連の脅威またはクライアント関連の脅威で、脅威のタイプをクリックします。 選択された期間中に発生したこの脅威のカテゴリに該当するすべてのイベントが表示されます。 次の表は、脅威の詳細に表示されるフィールドを説明します。
5. 別のロケーションに移動したいイベントのチェックボックスにチェックを入れます。
6. ロケーションの変更アイコンをクリックすると、 新しいロケーションの選択ダイアログボックスが表示されます。
7. 新しいロケーションにイベントを移動するには、新しいロケーションを選択し、OK をクリックします。

脆弱性ステータスのオン/オフ

イベントの脆弱性ステータスをオン/オフするには、次の手順を実行します。
1. **フォレンジック**へ移動します。
2. 脅威を表示するロケーションを選択すると、 選択したロケーションの AP とクライアント関連の脅威が表示されます。
3. 脅威を表示する時間間隔を決めるには、**期間を選択**の隣にある時間をクリックします。 この期間の AP に関連する脅威と、クライアントに関連する脅威が、表示されます。
4. AP 関連の脅威またはクライアント関連の脅威で、脅威のタイプをクリックします。 選択された期間中に発生したこの脅威のカテゴリに該当するすべてのイベントが表示されます。
5. 脆弱性ステータスをオンまたはオフにしたいイベントのチェックボックスにチェックを入れます。
6. イベントの脆弱性をオンにする場合は、脆弱性ステータスのオン・アイコンをクリックします。 イベントの脆弱性をオフにする場合は、脆弱性ステータスのオフ・アイコンをクリックします。 脆弱性をオンにすると、イベント概要の**脆弱性ステータス**は Yes として表示されます。 脆弱性をオフにすると、イベント概要の**脆弱性ステータス**は No として表示されます。

ロケーションのイベントリストを印刷

ロケーションに対する脅威の中で、特定のタイプのイベントリストを印刷することが可能です。
イベントリストを印刷するときは、次の手順を実行します。

1. **フォレンジック**へ移動します。
2. 脅威を表示するロケーションを選択すると、 選択したロケーションの AP とクライアント関連の脅威が表示されます。
3. 脅威を表示する時間間隔を決めるには、**期間を選択**の隣にある時間をクリックします。 この期間の AP に関連する脅威と、クライアントに関連する脅威が、表示されます。
4. AP 関連の脅威またはクライアント関連の脅威で、脅威のタイプをクリックします。 選択された期間中に発生したこの脅威のカテゴリに該当するすべてのイベントが表示されます。
5. 表示されているイベントのリストを印刷するには、印刷アイコンをクリックします。 イベントリストの印刷プレビューが表示されます。
6. リストを印刷するときは、**印刷**をクリックします。

削除済みとしてイベントをマーク

削除済みとしてイベントをマークすることができます。 これらが削除済みとしてマークされている場合でも、データベースには保持されます。

削除済みとしてイベントをマークするには、次の手順を実行します。

1. **フォレンジック**へ移動します。
2. 脅威を表示するロケーションを選択すると、 選択したロケーションの AP とクライアント関連の脅威が表示されます。
3. 脅威を表示する時間間隔を決めるには、**期間を選択**の隣にある時間をクリックします。 この期間の AP に関連する脅威と、クライアントに関連する脅威が、表示されます。
4. AP 関連の脅威またはクライアント関連の脅威で、脅威のタイプをクリックします。 選択された期間中に発生したこの脅威のカテゴリに該当するすべてのイベントが表示されます。
5. 削除済みとしたいイベントのチェックボックスにチェックを入れます。
6. **更に**をクリックし、削除済みとしてマークのオプションを選択します。

既読としてイベントをマーク

既読としてイベントをマークするには、次の手順を実行します。

1. **フォレンジック**へ移動します。
2. 脅威を表示するロケーションを選択すると、 選択したロケーションの AP とクライアント関連の脅威が表示されます。
3. 脅威を表示する時間間隔を決めるには、**期間を選択**の隣にある時間をクリックします。 この期間の AP に関連する脅威と、クライアントに関連する脅威が、表示されます。
4. AP 関連の脅威またはクライアント関連の脅威で、脅威のタイプをクリックします。 選択された期間中に発生したこの脅威のカテゴリに該当するすべてのイベントが表示されます。
5. 既読としてマークしたいイベントのチェックボックスにチェックを入れます。
6. **更に**をクリックし、既読としてマークのオプションを選択します。

削除済みイベントの表示/非表示

デバイス上の脅威の詳細で、削除済みとしてマークされたイベントを、表示または非表示にすることができます。

1. **フォレンジック**へ移動します。
2. 脅威を表示するロケーションを選択すると、 選択したロケーションの AP とクライアント関連の脅威が表示されます。
3. 脅威を表示する時間間隔を決めるには、**期間を選択**の隣にある時間をクリックします。 この期間の AP に関連する脅威と、クライアントに関連する脅威が、表示されます。
4. AP 関連の脅威またはクライアント関連の脅威で、脅威のタイプをクリックします。 選択された期間中に発生したこの脅威のカテゴリに該当するすべてのイベントが表示されます。 次の表は、脅威の詳細に表示されるフィールドを説明します。
5. 削除されたイベントを表示または非表示にするには、状況に応じて、削除されたイベントを表示アイコン、または削除されたイベントを隠すアイコンをクリックします。

レポート

レポートページでは、通信が停まる前に定義された、または、変更したレポートを生成できます。
このシステムは、事前定義されたコンプライアンスレポートを提供します。：ヘルス・インシュランス・ポータビリティー・アンド・アカウンタビリティー法（HIPAA）、サーベンズ・オックスリー法（SOX）、グラム・リーチ・ブライリー法（GLBA）、ペイメントカード業界（PCI）スタンダードなど。 また、デバイスやイベントに関する情報は、既製レポートの形式でもご覧になれます。
あなたは、レポートを PDF、HTML および XML フォーマットで生成することができます。 一度に、これらのいずれかの形式でレポートを生成することができます。 あなたは、将来の参照用にレポートを暗号化することができます。 また、レポートは指定した電子メールアドレスに電子メールで送信することができます。
以下のとおり事前に定義されたレポートが分類されています。

- コンプライアンスレポート
- インシデントレポート
- デバイスインベントリ レポート
- パフォーマンスレポート

これらのレポートは共有レポートです、そして、すべてのユーザーによって閲覧することが可能です。

管理コンソール(Management Console)でレポートを定義することができます。

同様に、レポートを表示し**マイレポート**にレポートを分類することができます。

ニーズに基づいてレポートをデザインすることができます。これらのレポートは **カスタム** レポートです。
カスタムレポートは管理コンソール(Management Console)で作成することができます。 レポートをインポートするには、**レポートのインポート** リンクをクリックします。 目的のパスを参照し、管理コンソール(Management Console)にレポートをインポートします。
.zip ファイル形式で管理コンソール(Management Console)からこれらのレポートをエクスポートすることもできます。 .zip ファイルは、**カスタム** タブと **マイレポート** タブで管理コンソール(Management Console)にインポートすることができます。

マイレポート は、それを定義したユーザーだけが利用できるレポートを含みます。

スケジュールレポートは、 **自分用にスケジュールされたレポート** と **自分によってスケジュールされたレポート**で構成されています。

自分によるスケジュール は、現在のユーザーによってスケジュールされた共有レポートです。これらのレポートは、他のユーザーのためにスケジュールすることが可能です。

自分用のスケジュールは、 現在のユーザーのためにスケジュールされた共有レポートです。これらのレポートは、別のユーザーが現在のユーザーのためにスケジュールすることが可能です。

レポートは、以下のカテゴリに分類されます。

- コンプライアンス
- インシデント
- デバイスインベントリ
- パフォーマンス
- カスタム
- マイレポート

コンプライアンスレポート

管理コンソール(Management Console)は、無線セキュリティの脆弱性に関する連邦政府機関およびその他の規制当局で要求されるさまざまなコンプライアンスレポートを提供します。 管理コンソール(Management Console)の **レポート** を使用して、以下のレポートを生成することができます。なお、各レポートの詳細内容については、規定している各団体にお問い合わせください。

- **国防総省命令 8100.2 コンプライアンスレポート** - このレポートのセクションでは、 ネットワークとこれらの脆弱性に起因するセキュリティのリスクの重要度で 検出された無線の脆弱性を示します。

- **GLBA 無線コンプライアンスレポート** - 1999 年制定のグラム・リーチ・ブライリー法(GLBA)は、 金融機関が顧客の個人を特定できる金融情報のセキュリティと 機密性を保護することを義務付けています。
  GLBA のセクション 501（タイトル v、サブタイトル A）は、 権限のないユーザーへの顧客の財務データの漏洩を制御することを求めています。 連邦取引委員会（FTC）防衛ルール 16 CFR 項目 314.4 は、 すべての金融機関がそれぞれの情報セキュリティプログラムを 組み込まなければならないという要項を明確に記述しています。 このレポートは、企業の無線セキュリティ状況を査定し、 あなたの企業を顧客金融データ漏洩の危機にさらす可能性のある、無線脆弱性を指摘します。
  1. 項目 314.4(a): このセクションは、機関が、情報セキュリティプログラムをコーディネートするために、社員にその使命を負わせることを要求しています。 このレポートは、社員が、無線を通しての顧客の金融データの漏洩を防止するよう使命を負っていることを証明します。
  2. 項目 314.4(b): このセクションは、機関が、不許可露見になる可能性のある顧客情報の、機密性・無欠性に対するリスクを発見することを要求しています。 この GLBA レポートを定期的に生成し、記録を保管することは、 あなたの企業が無線を通しての顧客の金融データの漏洩を防止するための 保護を常に行っていることを証明します。
  3. 項目 314.4(c): このセクションは、機関が情報の保護設定を行い、 日常的にこの保護設定の有効性をモニタリングすることを要求しています。 この GLBA レポートを定期的に生成し、記録を保管することは、 あなたの企業が無線を通しての顧客の金融データの漏洩を防止するための保護を常に行っていることを証明します。

- **HIPAA 無線コンプライアンスレポート** - 米国保健福祉局（DHHS）による、 ヘルス・インシュランス・ポータビリティー・アンド・アカウンタビリティー法（HIPAA） 1996 年 は、医療機関が、電子送信された患者の健康情報の、 プライバシーと安全性を保護しなければならないことを義務付けています。
  HIPAA セキュリティ ルール 45 DFR は、未承認のユーザーへの、 患者の健康データの漏洩をコントロールすることを追求しています。 このレポートは、企業の無線安全状況を査定し、 あなたの企業を患者の健康データ漏洩の危機にさらす可能性のある無線の脆弱性を特定します。
  1. セクション 164.308(a)(1): このレポートは、危機査定と管理のために設定される安全管理プロセスを要求しています。 この HIPAA レポートは、無線を通して 患者の健康データが漏洩する危機を査定・管理するための、 安全管理プロセスを確立する最初のステップです。
  2. セクション 164.308(a)(6): このレポートは、無線セキュリティ事象に迅速に対応するための、 正式書類と対応手順の設定を要求しています。 この HIPAA レポートを定期的に生成し、記録を保管することは、 あなたの企業には、無線を通しての患者の健康データの漏洩に関する事象を、 対処するための正式書類と迅速な対応プログラムがあることを証明します。

3. セクション 164.312(e)(1): このセクションは、無線ネットワークを介して送られた患者の健康データが、 未承認のアクセスから守られていることを要求しています。 この HIPAA レポートを定期的に生成し、記録を保管することは、あなたの企業が、 無線を通しての患者の健康データの漏洩を、モニタリング、検知、および保護を行う能力があることを証明します。

無線環境は絶えず変化するので、 少なくとも 15 日ごとに 1 回、HIPAA 無線脆弱性査定を行うことが推奨されます。 SOX 無線コンプライアンスレポートを記録保管してください。
1 番の脆弱性を修正し、あなた無線セキュリティの露見を最小限に留めるために、 進行して行う無線安全対策を確立させます。
このレポートのセクションでは、 あなたのネットワークで検知された無線の脆弱性と、それらの脆弱性によって生じた安全危機の深刻度を一覧にします。

- **MITS 無線 コンプライアンスレポート -** マネージメント・オブ インフォメーション・テクノロジー・セキュリティ(MITS)は、 カナダの大蔵委員会によって確立された実践のセキュリティ基準です。 2004 年に確立されたこの基準は、カナダの連邦局が、 情報の安全性と情報テクノロジー（IT）資産が彼らの管理下にあることを 保証するために遂行しなければならない、 標準的な安全性の必要条件を定義しています。
  MITS は、情報の機密性、完全無欠性、有効性を守ること、 更に IT 資産を守ることを追求しています。 このレポートは、企業の無線安全状況を査定し、 情報の機密性や IT 資産を危うくする可能性のある無線の脆弱性を特定します。
  MITS の以下のセクションは、 無線の再配備に関するものです。
  パート I, セクション 4: このセクションは、 各部署の会社上層部の人員を、内部コントロールを、 ハイレベルの IT セキュリティに確立し、維持する責任者としています。 この MITS レポートは、無線の漏洩から機密情報と IT 資産を守るために、 内部コントロールを確立する最初のステップです。
  パート II, セクション 10: このセクションは、 各部署が IT セキュリティ ポリシーを確立することを要求しています。 この MITS レポートは、無線セキュリティポリシーの存在を確立します。
  パート II, セクション 12.11.2: このセクションは、 すべてのセキュリティ リスクのために実行される内部監査を要求しています。 この MITS レポートは、無線セキュリティのリスクを記述する、監査書類として使用できます。
  パート III, セクション 16: このセクションは、 情報の機密性、完全無欠性、有効性を守るため、 更に IT 資産を守るための保護手段を確立することを要求しています。 この MITS レポートを定期的に生成し記録を保管することは、あなたの企業には、無線の漏洩から、 機密情報と IT 資産を守るための保護手段があることを 確立します。
  パート III, セクション 17: このセクションは、 セキュリティ事象のモニタリングと検知を要求しています。 この MITS レポートを定期的に生成し記録を保管することは、あなたの企業には、無線の漏洩から、 機密情報と IT 資産を守るための保護手段があることを確立します。
  無線環境は絶えず変化するので、少なくとも 15 日ごとに 1 回、 MITS 無線脆弱性査定を行うことが推奨されます。 MITS 無線コンプライアンスレポートを記録保管してください。 1 番の脆弱性を修正し、あなた無線セキュリティの露見を最小限に留めるために、 進行して行う無線安全対策を確立させます。
  このレポートのセクションでは、 あなたのネットワークで検知された無線の脆弱性と、 それらの脆弱性によって生じた安全危機の深刻度を一覧にします。

- **PCI DSS 3.0 無線コンプライアンスレポート** - 2013 年 11 月に発表した Payment Card Industry データセキュリティ基準 (PCI DSS) Version 3.0 は、カード会員データを保護するために推奨されたセキュリティコントロールを定めています。PCI DSS はクレジットカード会社（VISA とマスターカードを含む）のコンソーシアムによって定義されました。PCI スタンダードの要件は、カード会員データを保存、処理または伝送するすべてのメンバー、加盟店とサービスプロバイダに適用されます。 PCI DSS Version3.0 の以下のセクションでは、未許可の無線アクセスからカード会員データを保護する観点で関連しています。このレポートは WLAN 配備の PCI DSS 3.0 コンプライアンスを見直す手助けを目的とします。それは自動的に WLAN ネットワークに関連する PCI DSS 3.0 要件を満たすことを意味するものではありません。コンプライアンス認定を取得するためには PCI 認定セキュリティ監査機関（QSA）に相談してください。
  1. 要件 1.2: カード会員データ環境に必要なプロトコルを除いて、「信頼できない」ネットワークとホストからのトラフィックを拒否します。このレポートは、レポート期間中に検出された不正または誤って構成された無線アクセスポイントのリストを提供しています。不正なカード会員データへのアクセスは、これらのアクセスポイントを通じて可能です。
  2. 要件 2.1.1: 無線機器のベンダーにより提供されたデフォルト値を変更します。無線機器の場合は、デフォルトのパスワード、SSID、WEP キーとセキュリティの設定を変更する必要があります。可能な限り、WPA または WPA2 を使用する必要があります。このレポートでは、デフォルトの SSID やセキュリティ設定を使用している無線アクセスポイントのリストを提供しています。
  3. 要件 4.1.1: カード会員データを伝送する無線ネットワーク通信に適切な暗号化方式を使用していることを確認します。カード会員データの保護のため、WEP（Wired Equivalent Privacy）に対する依存を回避する必要があります。このレポートでは、オープンまたは安全でない暗号化方式を使用して通信する無線アクセスポイントとクライアントのリストを提供します。
  4. 要件 6.2: 新たに発見された脆弱性を識別するためのプロセスを確立し、新たな脆弱性の問題に対処するために構成基準を更新する。Generate and review contents of this report periodically so that newly discovered vulnerabilities can be identified and acted upon.新たに発見された脆弱性を識別し対処するために、定期的にこのレポートを生成し内容を検討します。
  5. 要件 10.5.4: 集中管理した内部ログサーバーまたは変更が困難な媒体に無線ネットワークのログをコピーします。レポート生成エンジンは、保存目的のためにすべての無線アクティビティのログを保持しています。
  6. 要件 11.1: 使用中のすべての無線デバイスを識別するために、少なくとも年 4 回無線アナライザを使用してください。このレポートは、使用中のすべての無線デバイスのリストを提供します。また、スキャナーが継続的に使用されているすべての無線デバイスを監視し、自動的に管理コンソールサーバーによって維持される無線デバイスのリストを更新します。
  7. 要件 11.2: 四半期に一度、そしてネットワークでの大幅な変更後にネットワークの脆弱性スキャンを実行します。このレポートは、レポート生成間隔の間に発見された無線脆弱性のリストを提供しています。このレポートは必要に応じて、またはスケジュールされた間隔で生成することができます。
  8. 要件 11.4: ネットワークの侵入検知システムや侵入防御システムを使用して、ネットワークトラフィックを監視し、侵害の疑いがある場合は担当者に警告します。侵入は、無線を通じて発生する可能性があります。無線スキャナーは継続的に監視し、ログと（オプションの）アラートおよび無線侵入の試みをブロックします。

9. 要件 12.10: インシデント対応計画を実施する。セキュリティ違反（無線バックドア介して起こったものを含む）に直ちに対応できるよう準備する。無線スキャナーは、24 時間 365 日モニタしてどんな不正な無線活動も瞬時に検出します。インシデント対応は、無線スキャナーを用いて手動または自動で行うことができます。 無線環境はダイナミックに変化するので、少なくとも 15 日おきに 1 回は PCI 無線脆弱性評価を実施するよう推奨する。PCI コンプライアンス評価レポートを保管してください。重要な脆弱性を解決して、無線セキュリティリスクを最小限にするために継続的な無線セキュリティ計画を確立してください。 このレポートのセクションでは、ネットワークとこれらの脆弱性に起因するセキュリティ上のリスクの深刻度で検出された無線の脆弱性を示します。

- **PCI DSS 2.0 無線コンプライアンスレポート** - 2010 年 10 月に発表した ペイメントカード業界セキュリティ基準 (PCI DSS) Version 2.0 では、 カード会員データを保護するために推奨されたセキュリティコントロールを定めています。 PCI DSS はクレジットカード会社（VISA とマスターカードを含む）の コンソーシアムによって定義されました。 PCI スタンダードの要件は、カード会員データを保存、 処理または伝送するすべてのメンバー、加盟店とサービスプロバイダに適用されます。
  PCI DSS Version 2.0 の以下のセクションでは、 カード会員データを不正な無線アクセスから保護する観点から関連しています。 このレポートは WLAN 配備の PCI DSS 2.0 コンプライアンスを見直す手助けを目的とします。 それは自動的に WLAN ネットワークに関連する PCI DSS 2.0 要件を満たすことを意味するものではありません。 コンプライアンス認定を取得するための PCI 認定セキュリティ監査機関（QSA）に相談してください。
  1. 要件 1.2: カード会員データ環境に必要なプロトコルを除いて、「信頼できない」ネットワークと ホストからのトラフィックを拒否します。 このレポートは、レポート期間中に検出された不正な、 または誤って構成された無線アクセスポイントのリストを提供しています。 不正なカード会員データへのアクセスは、これらのアクセスポイントを通じて可能です。
  2. 要件 2.1.1: 無線機器のベンダー提供のデフォルト値を変更します。 無線機器の場合は、デフォルトのパスワード、SSID、WEP キーとセキュリティの設定を変更する必要があります。 可能な限り、WPA または WPA2 を使用する必要があります。 このレポートでは、デフォルトの SSID やセキュリティ設定を使用している無線アクセスポイントのリストを提供しています。
  3. 要件 4.1.1: カード会員データの無線ネットワーク通信に適切な暗号化方式を使用していることを確認します。 カード会員データの保護のため、WEP（Wired Equivalent Privacy）に対する依存は、回避しなければなりません。 このレポートでは、オープンまたは、安全でない暗号化方式を使用して通信する 無線アクセスポイントとクライアントのリストを提供します。
  4. 要件 6.2: 新たに発見されたセキュリティ上の脆弱性を特定し、それに応じて構成基準を更新するプロセスを確立します。 定期的にこのレポートを生成し、内容を検討することは、 新たに発見された脆弱性を識別し対処することができます。
  5. 要件 10.5.4: 変更が困難な集中管理した内部ログサーバーまたは媒体に無線ネットワークのログをコピーします。 レポート生成エンジンは、保存目的のために、すべての無線活動のログを保持しています。
  6. 要件 11.1: 使用中のすべての無線デバイスを識別するために、少なくとも年 4 回無線アナライザを使用してください。 このレポートでは、使用中のすべての無線デバイスのリストを提供します。
  7. 要件 11.2: ネットワークの脆弱性スキャンを四半期に 1 度およびネットワークでの大幅な変更後に実行します。 このレポートは、レポート生成間隔の間に発見された無線脆弱性のリストを提供しています。 このレポートは必要に応じて、またはスケジュールされた間隔で生成することができます。
  8. 要件 11.4: ネットワークの侵入検知システムや侵入防御システムを使用して、 ネットワークトラフィックを監視し、侵害の疑いがある場合は担当者に警告します。 侵入は、無線を通じて発生する可能性があります。 無線スキャナーは継続的に監視し、ログと（オプションで）アラートおよび無線侵入の試みをブロックします。

9. 要件 12.9: インシデントレスポンス計画を実施します。 セキュリティ違反に直ちに対応できるよう準備します。 （無線バックドアを通って起こっているものを含む） 無線スキャナーは、24 時間 365 日モニタして、どんな不正な無線活動も瞬時に検出します。 インシデントレスポンスは、無線スキャナーを用いて手動または自動で行うことができます。無線環境はダイナミックに変化するので、 少なくとも 15 日おきに 1 回は PCI 無線コンプライアンス評価を実施することをお勧めします。 PCI コンプライアンス評価レポートを保管してください。 重要な脆弱性を解決して、無線セキュリティリスクを最小限にするために 継続的な無線セキュリティ計画を確立してください。このレポートのセクションでは、 ネットワークと、これらの脆弱性に起因するセキュリティ上の リスクの深刻度で検出された無線の脆弱性を示します。

- **PCI DSS 1.2 無線コンプライアンスレポート** - 2008 年 10 月に発行された、 ペイメント カード インダストリー データ セキュリティ スタンダード(PCI DSS) バージョン 1.2 は、 カード保有者のデータを保護するための、推奨されるセキュリティ コントロールを定義します。 PCI DSS は、VISA やマスターカードを含む、クレジットカード会社の組合によって定義されました。 PCI スタンダードの要件は、すべての会員、およびカード保有者のデータを保持、 プロセス、送信するすべての業者とサービス提供者に適用されます。
  PCI DSS バージョン 1.2 の以下のセクションは、 不許可の無線アクセスからカード保有者データを守るという観点に関連しています。 このレポートは、単に、無線 LAN 配備の PCI DSS 1.2 準拠を見直す助けになるよう意図されたものであり、 あなたの無線 LAN ネットワークに関連する PCI DSS 1.2 の要件を自動的に満たすものではありません。 準拠証明の取得に関しては、PCI 有資格セキュリティ監査官（QSA）に相談してください。
  1. 要件 1.2: 信用できない" ネットワークやホストからの通信は、カード保有者のデータ環境のために必要なプロトコルを除いて拒否します。 信用できないネットワークやホストからの通信は、カード保有者のデータ環境のために必要なプロトコルを除いて拒否します。 このレポートは、レポートの合間で検知された、不正 または 誤設定された無線アクセスポイントのリストを表示します。 未承認の、カード保有者データへのアクセスは、これらのアクセスポイントを介して可能です。
  2. 要件 2.1.1: 無線機材の、業者発行の初期設定を変更します。 無線機材に関しては、初期設定のパスワード、SSID、WEP キー、セキュリティ設定は変更するべきです。 可能な限り WPA または WPA2 を使用するべきです。 このレポートは、初期設定の SSID または、セキュリティ設定を使用している無線アクセスポイントのリストを表示します。
  3. 要件 2.2: すべてのシステムコンポーネント（無線アクセスポイントと端末を含む）のための設定基準を開発します。 その基準が、知る限りのすべてのセキュリティの脆弱性に焦点を当てていること、 更に業界承認のシステムを強固にする取り組みと一致するものであることを、企業が保証することも必要となります。 このレポートは、現在の設定に相対し、新たに発見された脆弱性とよく知られる脆弱性 の存在する無線アクセスポイントとクライアントのリストを表示します。
  4. 要件 4.1.1: カード保有者データを送信する無線ネットワークは、適切な暗号化方法を使用していることを確認してください。 カード保有者データの保護を WEP に頼るのは避けるべきです。 このレポートは、オープン状態または、安全性の低い暗号化方法を使用して通信している、 無線のアクセスポイントと端末のリストを表示します。
  5. 要件 6.2: 新たに発見された脆弱性を特定するプロセスを確立して、その新しい脆弱問題に取り組むために設定基準を更新します。 このレポートを作成し、その内容を定期的に見直してください。 そうすれば新たに発見された脆弱性は特定され、行動に移すことができます。
  6. 要件 10.5.4: 無線ネットワークのログ(記録)を、集中管理されている内部のログサーバー、 または修正することが難しいメディアにコピーします。 このレポートの作成エンジンは、記録保管目的のため、すべての無線活動の記録を保管します。
  7. 要件 11.1: 稼働しているすべての無線機器を識別するために、無線アナライザを少なくとも 1 年に 4 回使用してください。 更に、スキャナーは継続的に使用中のすべての無線機器をモニタリングし、 サーバーで管理されている無線機器のリストを自動的に更新します。

8. 要件 11.2: ネットワーク脆弱性のスキャンを 1 年に 4 回と、ネットワークに重大な変化が起きたときに行います。 このレポートは、レポート作成の間隔に発見された無線の脆弱性のリストを表示しています。 このレポートは、要求に応じて（オン･デマンド）またはスケジュールされた間隔で作成することができます。
9. 要件 11.4: ネットワーク通信をモニタリングし、疑われる障害について担当人員に警告するための、 ネットワーク侵入検知と防止システムの使用します。 無線経由ででも侵入は起こりうる可能性があります。 無線スキャナーは、継続してモニタリングを行い、記録をし、警告を行い（オプション）、更に無線侵入の試みを阻止します。
10. 要件 12.9: インシデントレスポンス計画を実施します。 セキュリティ違反に直ちに対応できるよう準備します。 （無線バックドアを通って起こっているものを含む） 無線スキャナーは、1 日 24 時間 週 7 日 電波をモニタリングして、どのような不許可無線活動も即座に検知します。 事象の対応は、無線スキャナーを使用して、手動、自動、どちらででも行うことができます。無線環境は絶えず変化するので、 少なくとも 15 日ごとに 1 回、PCI 無線脆弱性査定を行うことが推奨されます。 PCI 無線コンプライアンスレポートを記録保管してください。 1 番の脆弱性を修正し、あなたの無線セキュリティの露見を最小限に留めるために、 継続的な無線安全対策を確立させます。このレポートのセクションでは、あなたのネットワークで検知された無線の脆弱性と、 それらの脆弱性によって生じた安全危機の度合いを一覧にします。

- **PCI DSS 1.1 無線コンプライアンスレポート** - 2006 年 9 月に発行された、 ペイメント カード インダストリー データ セキュリティ スタンダード (PCI DSS) バージョン 1.1 は、カード保有者のデータを保護するための、 推奨されるセキュリティ コントロールを定義します。 PCI スタンダードの要件は、すべての会員、およびカード保有者のデータを保持、 プロセス、送信するすべての業者とサービス提供者に適用されます。 PCI DSS バージョン 1.1 の以下のセクションは、 不許可の無線アクセスからカード保有者データを守るという観点に関連しています。 このレポートは、単に、無線 LAN 配備の PCI DSS 1.1 準拠を見直す助けになるよう意図されたものであり、 あなたの無線 LAN ネットワークに関連する要件 PCI DSS 1.1 を自動的に満たすものではありません。 準拠証明の取得に関しては、PCI 有資格セキュリティ監査官（QSA）に相談してください。
  1. 要件 1.2: 信用できないネットワークやホストからの通信は、 カード保有者のデータ環境のために必要なプロトコルを除いて拒否します。 このレポートは、レポートの合間で検知された、不正 または 誤設定された無線アクセスポイントのリストを表示します。 未承認の、カード保有者データへのアクセスは、これらのアクセスポイントを介して可能です。
  2. 要件 2.1.1: 無線機材の、業者発行の初期設定を変更します。 無線機材に関しては、初期設定のパスワード、SSID、WEP キー、セキュリティ設定は変更するべきです。 可能な限り WPA または WPA2 を使用するべきです。 このレポートは、初期設定の SSID または、セキュリティ設定を使用している無線アクセスポイントのリストを表示します。
  3. 要件 2.2: すべてのシステム コンポーネント（無線アクセスポイントと端末を含む）のための設定基準を開発します。 その基準が、知る限りのすべてのセキュリティの脆弱性に焦点を当てていること、 更に業界承認のシステムを強固にする取り組みと一致するものであることを、 企業が保証することも必要となります。 このレポートは、現在の設定に相対し、新たに発見された脆弱性とよく知られる脆弱性の存在する 無線アクセスポイントとクライアントのリストを表示します。
  4. 要件 4.1.1: カード保有者データを送信する無線ネットワークは、適切な暗号化方法を使用していることを確認してください。 カード保有者データの保護を WEP に頼るのは避けるべきです。 このレポートは、オープン状態または、安全性の低い暗号化方法を使用して通信している、 無線のアクセスポイントと端末のリストを表示します。
  5. 要件 6.2: 新たに発見された脆弱性を特定するプロセスを確立して、その新しい脆弱問題に取り組むために設定基準を更新します。 このレポートを作成し、その内容を定期的に見直してください。 そうすれば新たに発見された脆弱性は特定され、行動に移すことができます。

6. 要件 10.5.4: 無線ネットワークのログ(記録)を、集中管理されている内部のログサーバー、 または修正することが難しいメディアにコピーします。 このレポートの作成機関は、記録保管目的のため、すべての無線活動の記録を保管します。
7. 要件 11.1: 稼働しているすべての無線機器を識別するために、無線アナライザを少なくとも 1 年に 4 回使用します。 このレポートは、使用中のすべての無線機器のリストを表示します。 更に、スキャナーは継続的に使用中のすべての無線機器をモニタリングし、サーバーで管理されている無線機器のリストを自動的に更新します。
8. 要件 11.2: 8. 要件 11.2: ネットワークの脆弱性のスキャン(走査)を年に 4 回、およびネットワーク内で重大な変更が起きたあとに行います。 このレポートは、レポート作成の間隔に発見された無線の脆弱性のリストを表示しています。 このレポートは、要求に応じて（オン･デマンド）またはスケジュールされた間隔で作成することができます。
9. 要件 11.4: ネットワーク通信をモニタリングし、疑われる障害について担当人員に警告するための、 ネットワーク侵入検知と防止システムを使用します。 無線経由でも侵入行為は起こりうる可能性があります。 無線スキャナーは、継続してモニタリングを行い、記録をし、警告を行い（オプション）、更に無線侵入の試みを阻止します。
10. 要件 12.9: インシデントレスポンス計画を実施します。 セキュリティ違反に直ちに対応できるよう準備します。 （無線バックドアを通って起こっているものを含む） 無線スキャナーは、1 日 24 時間 週 7 日 電波をモニタリングして、どのような不許可無線活動も即座に検知します。 事象の対応は、無線スキャナーを使用して、手動、自動、どちらで行うことができます。

- **SOX 無線コンプライアンスレポート** - サーベンズ・オックスリー法（SOX） 2002 年は、2002 年に米国議会によって、会計のやりかた、財政の開示、および公共企業の組織管理を改正するための、 総合的な法律として議決されました。 SOX 法は、米国内で公に証券取引が行われているすべての会社に適用され、 証券取引委員会（SEC）によって取り締まりが行われています。
  SOX 法のセクション 302、404、および 409 は、 承認されていないユーザーへの非公共データの漏洩をコントロールすることを追求しています。 このレポートは、企業の無線安全状況を査定し、 あなたの企業をこのような非公共データ漏洩の危機にさらす可能性のある無線の脆弱性を特定します。
  1. セクション 302: このセクションは、 非公共情報を漏洩から守るために、内部コントロールを確立し、維持し、そして定期的に見直しをする責任者に、 CEO や CFO を任命します。 このレポートは、無線を通して非公共データが漏洩することを防止するために、 内部コントロールを確立する最初のステップです。
  2. セクション 404: このセクションは、 会社が、非公共データの電子情報公開を、モニタリング、検知、記録できる能力があることを要求しています。 この SOX レポートを定期的に生成し記録を保管することは、あなたの企業には、 無線経由での非公共データの漏洩事象を、モニタリング、検知、 記録できる能力があることを確立します。
  3. セクション 409: このセクションは、 もし非公共情報が、あなたのネットワーク上で不適切に公表された場合、 迅速な対応と露出査定のプログラムを要求しています。 この SOX レポートを定期的に生成し記録を保管することは、あなたの企業には、 もし非公共情報が無線経由で漏洩した場合にも、 迅速な対応と露出査定のプログラムあることを確立します。無線環境は絶えず変化するので、少なくとも 15 日ごとに 1 回、 SOX 無線脆弱性査定を行うことが推奨されます。 SOX 無線コンプライアンスレポートを記録保管してください。 1 番の脆弱性を修正し、あなた無線セキュリティの露見を最小限に留めるために、 継続的な無線安全対策を確立させます。このレポートのセクションでは、 あなたのネットワークで検知された無線の脆弱性と、 それらの脆弱性によって生じた安全危機の深刻度を一覧にします。

パフォーマンスレポート

- **周波数帯域幅 検査レポート** - このレポートは、無線ネットワークにおいて検知された 周波数帯域幅に関連するパフォーマンスの問題をまとめたものです。 これらのパフォーマンスの問題は、無線ネットワークを本来の機能以下で稼働させる原因になる可能性があります。 これらの問題点を取り除く是正措置を考慮すべきです。
- **コンフィグレーション 監査レポート** - このレポートは無線ネットワークで検出された、無線ネットワークを 最大能力以下で稼働させる要因になりうるコンフィグレーション設定をまとめたものです。 これらのコンフィグレーション設定の修正を考慮すべきです。
- **RF 監査レポート**-このレポートは、無線ネットワークで検知された RF の問題をまとめたものです。 これらのパフォーマンスの問題は、無線ネットワークを 本来の機能以下で稼働させる原因になる可能性があります。 これらの問題点を取り除く是正措置を考慮すべきです。

デバイスインベントリレポート

- **全デバイス一覧** - システムによって検知されたすべてのアクセスポイント、 クライアント、センサーの一覧がこのレポートに記載されています。 アクセスポイント、クライアント、センサーについての情報は、 更にデバイスフォルダーに基づいてさまざまなセクションに分類されます。
- **ブリング・ユア・オウン・デバイス（BYOD）個人機器の持ち込み** - このレポートでは、Wi-Fi を介して企業のネットワークに侵入する スマートフォンとタブレットについての情報を提供します。 また、許可なく企業の敷地内で稼働している可能性のある、ソフトアクセスポイントと モバイル Wi-Fi ホットスポットについての情報も提供します。
- **詳細な AP 一覧表** - システムによって検知されたすべてのアクセスポイントの一覧はこのレポートに記載されています。 AP についての情報は、 更に AP フォルダーに基づいてさまざまなセクションに分類されます。
- **詳細な クライアントのリスト** - 製品で検出されるすべてのクライアントの完全な明細は、 このレポートに記載されています。クライアントに関する情報は、 更にクライアントのフォルダーに基づいてさまざまなセクションに分類されます。
- **詳細な センサー一覧表** - 製品によって検知されたすべてのセンサーの一覧は、 このレポートに記載されています。

カスタムレポート

あなたは必要に基づいてレポートをデザインすることができます。 これらのレポートは、 **カスタム** レポートです。 カスタムレポートは管理コンソールサーバーで作成され、管理コンソール(Management Console)にインポートすることができます。あなたは、 .zip ファイル形式で管理コンソールサーバーからレポートをエクスポートして、管理コンソール(Management Console)に、.zip ファイルをインポートすることができます。

レポートのインポート をクリックし、インポートするレポートのパスとファイル名を指定します。 それをインポートするときに、レポート名を変更することができます。 管理コンソールサーバーによって生成されていないファイルをインポートすることができません。

マイレポート

コンプライアンスレポートなどの共有レポートとは異なり、 **マイレポート** はそれらを作成したユーザーのみに表示されます。
あなたは自分のレポートを取得することができます。また、名前を変更しこれらのレポートを削除することができます。

アナリティクス

アナリティクスデータは、WIPS センサーに認識できる Wi-Fi クライアントとアクセスポイント(AP)とアソシエイトする Wi-Fi クライアントに関して利用可能です。

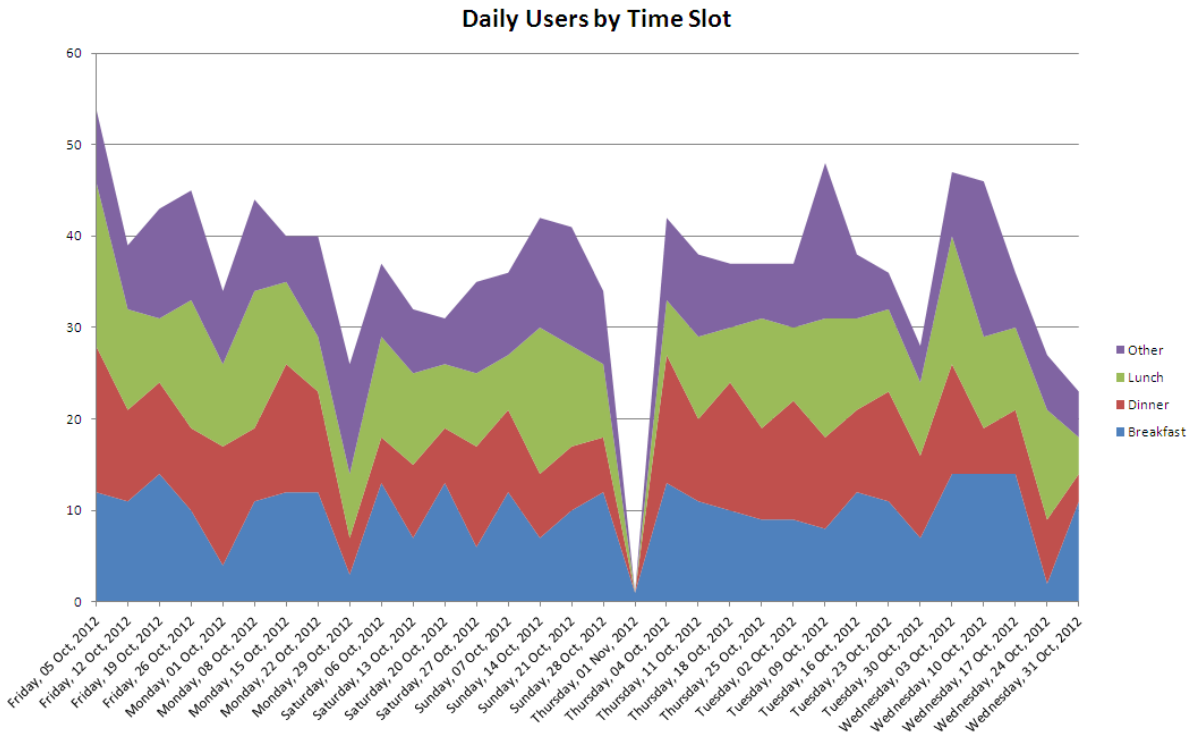
可視性アナリティクスは、管理デバイス(Management Device)付近のクライアントに関する情報を提供します。

アソシエーション分析は、アクセスポイント(AP)と接続するまたはアソシエイトするクライアントについての情報を提供します。

コンテンツアナリティクスは、アクセスポイント(AP)にアソシエイトするクライアントがアクセスしたインターネットドメインに関する情報をキャプチャします。 この情報は、レポート>アナリティクスからダウンロードすることができるアソシエーション分析のファイル内に存在します。
アナリティクスのレポートを生成するには、管理者権限が必要です。

アナリティクスデータは、さまざまな方法で使用することができます。 例えば、管理コンソール(Management Console)が小売店で配置されているならば、可視性アナリティクスを使用することにより小売店とその周辺のクライアント数を見ることができます。 同様に、アソシエーション分析を使用すると、許可クライアント、ゲストクライアント、およびこれらのクライアントが使用している SSID の利用状況を分析することができます。 アソシエーションと可視性アナリティクスを使用して、ストアへの訪問客に限らず、1 日のいろいろな時間帯の小売店への来客数、ネットワークの使用パターンを確認することができます。

以下のアソシエーション分析・グラフは、朝食、ランチ、ディナー、他の時間帯のタイムスロットあたりの 1 日のユーザー数を一般的な例として示しています。 これらの情報は、アソシエーションと可視性アナリティクスエンジンを使用して得られます。
アナリティクスは、カンマで区切られた値の（.csv）ファイルで提供されます。次のグラフは.csv ファイルのデータから生成したものです。



Daily Users by Time Slot derived from Analytics Data

サンプルマクロは、リクエストに応じて利用可能です。

アナリティクスはライセンスベースの機能です。 サーバーにアナリティクスライセンスの適用後に、レポートページのアナリティクスタブが有効になり表示されます。

アナリティクスデータのダウンロード

可視性アナリティクスデータをダウンロードするには、次の操作を行います。
1. **可視性アナリティクス**を選択します。
2. このデータをダウンロードしたい過去の日数を入力します。
3. **ダウンロード**をクリックします。

可視性分析データは、カンマ区切りのファイル(.csv)としてダウンロードされます。 データをダウンロードした際にポップアップがブラウザで有効になっていることを確認します。

.csv ファイルは、通常、'Downloads' フォルダーに保存されます。それには次のデータが含まれています。
- クライアントの MAC アドレス（Client MAC address）
- クライアントのロケーション（Location of the client）
- 最良の受信信号強度（Best received Signal Strength indication） (RSSI)
- 最良の RSSI をレポートするセンサーの MAC アドレス（MAC address of the sensor reporting best RSSI）
- クライアントセッションの継続時間（Client session duration）
- アクティビティ停止時間（Activity stop time） (GMT)
- ユーザーのローカルタイムゾーンごとのアクティビティ停止時間 - アナリティクスデータがロケーションフロアに関連する場合には、その直接の親ロケーションフォルダーに設定されたローカルタイムゾーンが考慮されます。 ロケーションフォルダーのタイムゾーンが設定されていない場合、このフィールドはサーバーのタイムゾーンに基づいたアクティビティ停止時間を示しています。 アナリティクスデータがロケーションのフォルダーに関係する場合も同様に、ロケーションフォルダーに設定されたローカルタイムゾーンが考慮されます。 ロケーションフォルダーのタイムゾーンが設定されていない場合、このフィールドはサーバーのタイムゾーンに基づいたアクティビティ停止時間を示しています。
- ローカルタイムゾーン - アナリティクスデータがロケーションフロアに関連する場合には、その直接の親ロケーションフォルダーに設定されたローカルタイムゾーンが考慮されます。 ロケーションフォルダーのタイムゾーンが設定されていない場合、このフィールドはサーバーのタイムゾーンを示しています。 アナリティクスデータがロケーションのフォルダーに関連する場合も同様に、ロケーションフォルダーに設定されたローカルタイムゾーンが考慮されます。 ロケーションフォルダーのタイムゾーンが設定されていない場合、このフィールドはサーバーのタイムゾーンを示しています。

ご注意： クライアントが複数のセンサーから見える場合、センサーがレポートした最良の RSSI 値が.csv ファイルに記録されます。

アソシエーション分析データをダウンロードするには、次の操作を行います。
1. **アソシエーションアナリティクス** を選択します。
2. このデータをダウンロードする日付を入力してください。
3. **ダウンロード**をクリックします。

ご注意： アソシエーションアナリティクス のチェックボックスにチェックを入れるには、アクセスポイント(AP)に関連付けられた SSID プロファイルを編集します。 このチェックボックスが選択されていない場合、それぞれの SSID に関連付けられたアクセスポイント(AP)に関連するデータの csv ファイルに、アソシエーション分析データは表示されません。

アソシエーション分析データは、カンマ区切りのファイル（.csv）としてダウンロードされます。
データをダウンロードした際にポップアップがブラウザで有効になっていることを確認します。
ファイルは、通常、'Downloads' フォルダーに保存されます。
.csv ファイルには、次のデータが含まれています。

- クライアント MAC アドレス（Client MAC address）
- プロトコル（Protocol）
- SSID
- ロケーション（Location）
- クライアントのアソシエーション開始時間（Association start time 〈GMT〉 of the client）
- アソシエーション終了時間（Association end time〈GMT〉）
- ユーザーのローカルタイムゾーンごとのクライアントのアソシエーション開始時間 - アナリティクスデータがロケーションフロアに関連する場合には、その直接の親ロケーションフォルダーに設定されたローカルタイムゾーンが考慮されます。 ロケーションフォルダーのタイムゾーンが設定されていない場合、このフィールドのクライアントアソシエーション開始時間はサーバーのタイムゾーンを示します。 アナリティクスデータがロケーションのフォルダーに関連する場合も同様に、ロケーションフォルダーに設定されたローカルタイムゾーンが考慮されます。 ロケーションフォルダーのタイムゾーンが設定されていない場合、このフィールドはサーバーのタイムゾーンに基づいたクライアントのアソシエーション開始時刻を示しています。
- ユーザーのローカルタイムゾーンごとのクライアントのアソシエーション終了時間 - アナリティクスデータがロケーションフロアに関連する場合には、その直接の親ロケーションフォルダーに設定されたローカルタイムゾーンが考慮されます。 ロケーションフォルダーのタイムゾーンが設定されていない場合、このフィールドは、サーバーのタイムゾーンに基づいたクライアントのアソシエーション終了時刻を示しています。 アナリティクスデータがロケーションのフォルダーに関連する場合も同様に、ロケーションフォルダーに設定されたローカルタイムゾーンが考慮されます。 ロケーションフォルダーのタイムゾーンが設定されていない場合、このフィールドはサーバーのタイムゾーンに基づいたクライアントアソシエーション終了時刻を示しています。
- セッション期間（Session duration）
- バイト単位のクライアントデバイスからのデータ転送（Data Transfer from client device in bytes）
- バイト単位のクライアントデバイスへのデータ転送（Data Transfer to client device in bytes）
- データレート（Data Rate in Kbps ）
- スマートデバイスの種類（Smart device type）
- ローカルタイムゾーン（Local Time Zone）
- ロケーション ID（Location ID）
- アクセスしたドメイン（Domains Accessed）

データ交換に基づいて上位ドメインが csv ファイルの Domains Accessed の列に提示されます。
Domains Accessed 列のデータは次の形式で表示されます： :<ドメイン名> (<ドメインに転送されたデータ>/<ドメインから受信したデータ>)。 複数のドメインは | で区切られています。

ご注意： インターネットドメイン関連の情報は、SSID プロファイルの設定時に**コンテンツアナリティクス**のチェックボックスにチェックを入れた場合のみ収集されます。 それ以外の場合は、csv ファイル内の Domains Accessed の列は空白になります。

セッション継続時間は、クライアントがアクセスポイント(AP)を介してネットワークリソースに活発にアクセスした継続時間として計算されるため、 アソシエーション開始時間と終了時間の差分よりも少ない可能性があります。

アナリティクスデータのバックアップ

バックアップを取りたいときは、`set dB backup info` または `dB backup` コマンドを実行することで、 アナリティクスデータのバックアップが可能です。 アナリティクスデータがバックアップされる場合、バックアップしたデータベースのサイズが大きくなる可能性がありますので注意してください。

レポートのアーカイブ表示

レポートの Archives タブでは、管理コンソール(Management Console)で保存または生成されたアーカイブレポートを表示することができます。 これらのレポートは、トレンド分析に役立ちます。 アーカイブされたレポートは、以前このレポートを生成したユーザーに表示されます。 スーパーユーザーは、すべてのアーカイブされたレポートを見ることができます。

アーカイブされたレポートロケーション固有のものではありません。 管理コンソール(Management Console)にログインしたユーザーの特権または権利に依存します。 スーパーユーザーはすべてアーカイブされたレポートを見ることができます。 パワーユーザーは、彼らが管理する顧客のアカウントのすべてのアーカイブされたレポートを見ることができます。 管理者、オペレータ、およびビュアーは、自身でアーカイブされたレポートのみ見ることができます。

サーバークラスタの親サーバーにログインしている場合、（自分の役割に基づいて）あなたは親と子のサーバーからアーカイブされたレポートの集約されたセットを確認することができます。

アーカイブされたレポートの取り出し、名前変更、および削除を行うことができます。 ロケーションでアーカイブされたレポートの一覧を印刷することができます。

アーカイブされたレポートが、サーバークラスタの親サーバー上で生成された場合は、親と子のサーバーから集約されたデータを示します。

アーカイブされたレポートの取出

アーカイブされたレポートを取り出して表示するには、次の手順を実行します。
1. **レポート>アーカイブ** タブへ移動します。
2. レポートがアーカイブされているロケーションを選択します。
3. アーカイブされたレポートリストからレポートのチェックボックスを選択します。
4. レポートを取り出すには、取得アイコンをクリックします。

アーカイブされたレポートの名前変更

アーカイブされたレポートの名前を変更するには、次の手順を実行します。
1. **レポート>アーカイブ** タブへ移動します。
2. レポートがアーカイブされているロケーションを選択します。
3. アーカイブされたレポートリストからレポートのチェックボックスを選択します。
4. 名前変更アイコンをクリックし、レポートの新しい名前を入力します。

ロケーションのアーカイブされたレポート一覧を印刷

アーカイブされたレポートの一覧を印刷するには、次の手順を実行します。
1. **レポート>アーカイブ** タブへ移動します。
2. アーカイブされたレポートリストを印刷したいロケーションを選択します。
3. リストに印刷される列を選択します。 列の選択または解除をするには、任意の列名をクリックします。
4. 印刷アイコンをクリックします。 アーカイブされたレポートリストの印刷プレビューが表示されます。
5. リストを印刷するには、**印刷** をクリックします。

アーカイブされたレポートの削除

アーカイブされたレポートを削除するには、次の手順を実行します。
1. **レポート>アーカイブ** タブへ移動します。
2. レポートがアーカイブされているロケーションを選択します。
3. アーカイブされたレポートリストからレポートのチェックボックスを選択します。
4. 削除アイコンをクリックします。削除を確認するメッセージが表示されます。
5. アーカイブされたレポートの削除を実行するには、**Yes** をクリックします。

レポート生成のスケジュール

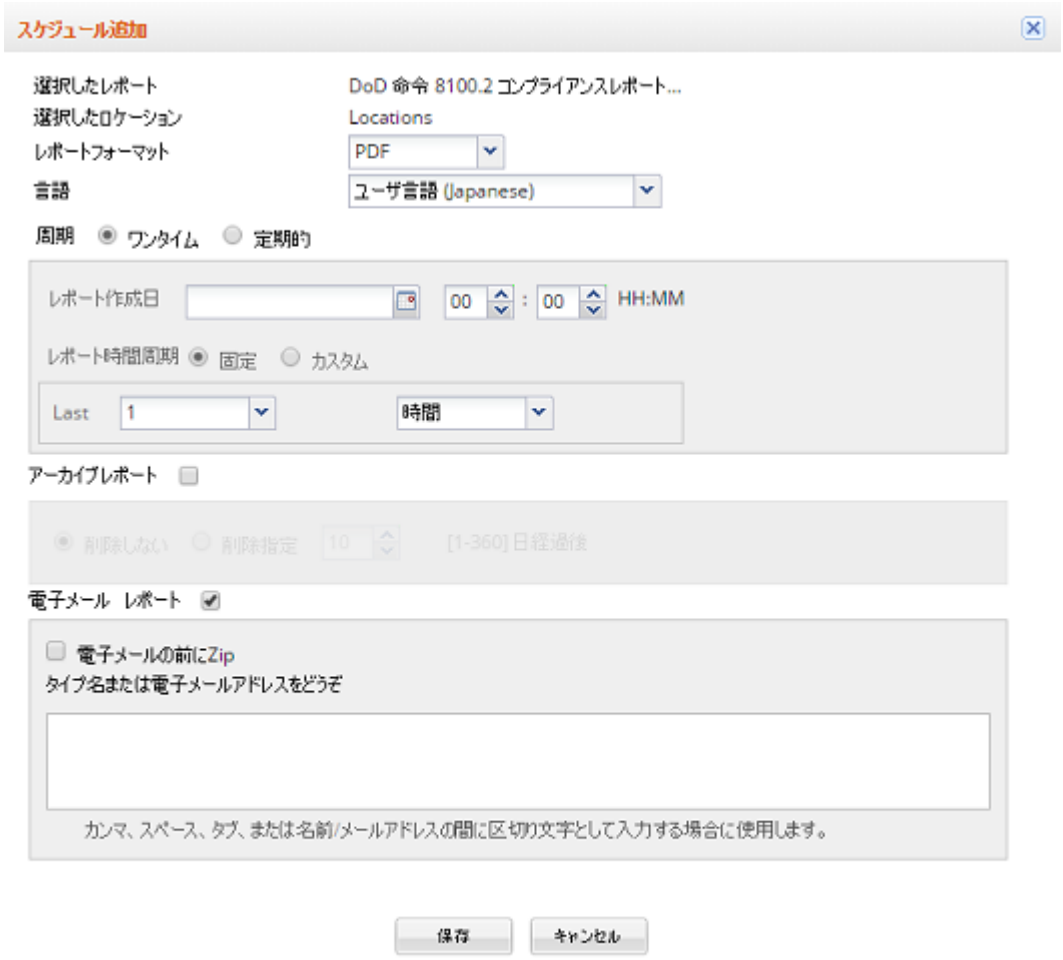
1 回限りの生成(One Time)または定期的な生成(Recurring)でレポートをスケジュール設定できます。電子メールにレポートを送信することができます。 また、レポート生成のスケジュール時にレポートのアーカイブの詳細を指定することができます。 いったんレポート作成スケジュールが設定されると、レポートをスケジュールしたユーザーに対して **自分によってスケジュールされたレポート** で確かめられます。

ご注意： 誤ったタイムゾーン設定がサーバー設定シェルからサーバーの初期化と設定ウィザードで設定されている場合は、スケジュールされたレポートは誤った時刻に電子メールで送信されます。適切に配信されるように正しいタイムゾーンを選択してください。

ご注意： サーバーがサーバークラスタ内の親サーバーでかつ親サーバーのロケーションツリーにマウントされた子サーバーが存在する場合、子サーバー上でレポートをスケジュールすることはできません。 スケジューリングは、親サーバーに対するローカルでのレポートのみ許可されます。 通常はリモートロケーション上でのレポートスケジュールは許可されていません。

レポート生成をスケジュール設定するには、次の手順を実行します。
1. レポートで、適切なレポートカテゴリを選択します。
2. スケジュールするレポートの **スケジュール追加**をクリックします。
3. 以下の画像に表示されるように、**スケジュール追加**が表示されます。
4. **レポートフォーマット**を選択します。 使用可能なオプションは、pdf、html、xml です。

1 回限りのレポート生成をスケジュールしたい場合は、**ワンタイム**タブの下で詳細を指定します。

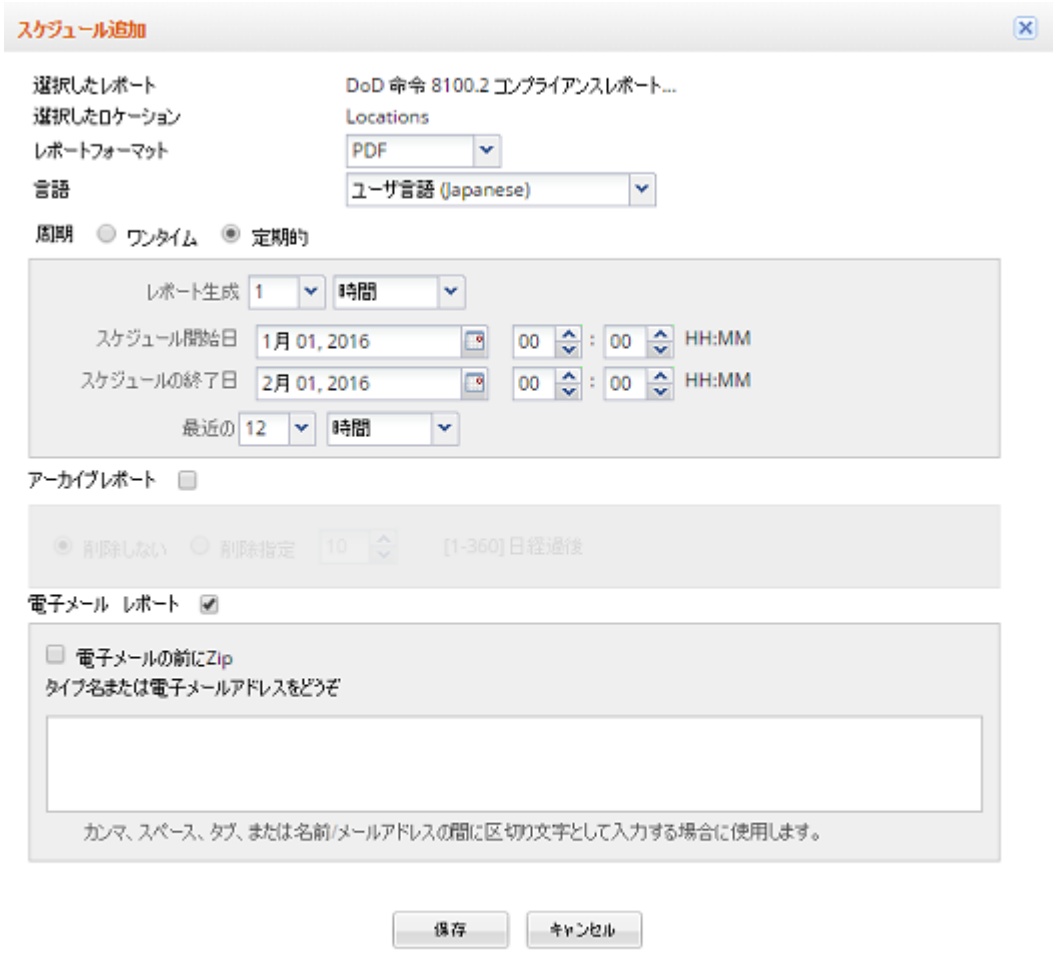


スケジュール追加 - One Time Generation

次の表は、**One Time Generation** タブ上のフィールドについて説明します。

One Time Generation タブのフィールド	
フィールド	**説明**
レポート作成日	レポート生成の日付を指定するには、カレンダーアイコンをクリックします。 また、レポート作成の時間を指定します。
レポート時間周期	レポート配信日時の前の期間を指定するには **固定** を選択します。 レポートを生成する対象の数時間、数日または数ヶ月前の数を指定します。
	レポートを日付単位で期間を指定するには、 **カスタム** を選択します。

定期的なレポート生成をスケジュールする場合は、 **定期的**タブの下で詳細を指定します。



スケジュール追加 - Recurring Generation

次の表は、**Recurring** タブ上のフィールドについて説明します。

Recurring Generation タブのフィールド	
フィールド	**説明**
レポート生成毎	レポート生成の時間、日、または月の数で周期を指定します。
スケジュール開始日	レポートを生成する対象の開始日時を選択します。
スケジュールの終了日	レポートを生成する対象の終了日時を選択します。
レポート時間周期	レポートが生成される時間、日数、または月数の期間を選択します。

電子メールでレポートを送信

生成時にレポートを電子メールで送信する場合は、**電子メールレポート**のチェックボックスにチェックを入れます。 電子メールで送信する前にレポートを圧縮したい場合は、**電子メールの前に Zip** のチェックボックスにチェックを入れます。

スケジュールで電子メールの ID が記述されている場合は、 **スケジュール** タブの **自分用にスケジュールされたレポート** でレポートを見ることができます。 スケジュールを追加した場合は、 **スケジュール** タブの **自分によってスケジュールされたレポート** でレポートを見ることができます。

アーカイブレポート

レポートを暗号化するには、アーカイブレポートのチェックボックスにチェックを入れます。 永続的にアーカイブされたレポートを削除しない場合は、**削除しない**を選択します。 固定期間アーカイブされたレポートを削除しない場合は、**削除指定**を選択し、アーカイブされたレポートがシステムから削除されるまでの期間を指定します。 アーカイブされたレポートを保持する最小と最大保有期間は、それぞれ 1 日と 360 日になります。

レポートスケジュールの表示

レポートスケジュールタブで あなたが定義したレポートスケジュールを表示することができます。メールアドレスがスケジュールに記載されている場合は、**レポート>スケジュール**タブの **自分用にスケジュール されたレポート**で見ることができます。スケジュールを追加した場合は、**レポート>スケジュール**タブの**自分によってスケジュールされたレポート**で見ることができます。

自分で定義したレポートスケジュールのリストを見るには、**自分によってスケジュールされたレポート**をクリックしてください。

自分によってスケジュールされたレポートのセクションでは、 レポート名、スケジュール情報、次のレポートの配信日時、レポートが生成されるロケーション 、このセクションで生成されるレポートの期間が表示されます。

自分のためにスケジュールされたレポートのリストを表示するためには **自分用にスケジュールされたレポート**をクリックしてください。

自分用にスケジュールされたレポートのセクションでは、 レポート名、スケジュール情報、次のレポート配信日時、レポートが生成されるロケーション 、レポートが生成さる期間、およびレポートのスケジュールを定義したユーザーの名前が表示されます。

アイコンの用語集

以下は、管理コンソール(Management Console)上で表示されるデバイス関連のアイコン一覧です。

アイコン	説明
	不正 AP-アクティブ： 不正 AP(Rogue AP)がアクティブでセンサーに認識されていることを示します。
	許可 AP(Authorized AP)： AP が許可されたアクセスポイントであることを示します。
	許可 AP(Authorized AP)-アクティブ： 許可された AP がアクティブでセンサーに認識されていることを示します。
	許可 AP(Authorized AP)-非アクティブ： センサーに認識されていた許可された AP が非アクティブであることを示します。
	外部 AP-アクティブ： 外部 AP がアクティブでセンサーに認識されていることを示します。
	隔離保留： AP/クライアントを隔離する必要があることを示していますが、隔離は保留されています。
	隔離中： AP/クライアントが隔離されていることを示します。
	隔離エラー： デバイスを隔離中に、なんらかのエラーが発生したことを示します。
	DoS 隔離： このデバイスの DoS 攻撃に対する検疫が実行中であること示します。
	DoS 隔離保留：このデバイスの DoS 攻撃に対する検疫が保留されていることを示します。
	禁止デバイス： AP/クライアントが禁止されたデバイスであることを示します。
	禁止リストから削除： AP /クライアントが禁止リストから削除されたことを示します。
	トラブルシューティング： トラブルシューティングがデバイス上で実行中であることを示します。
	許可クライアント-アクティブ： 許可されたクライアントがアクティブでセンサーに認識されていることを示します。
	許可クライアント - 非アクティブ： センサーに認識されていた許可されたクライアントが非アクティブであることを示します。
	不正クライアント(Rogue Client) - アクティブ： 不正クライアント(Rogue Client)がアクティブでセンサーに認識されていることを示します。
	不正クライアント - 非アクティブ(Rogue Client)： センサーに認識されていた不正クライアント(Rogue Client)が非アクティブであることを示します。
	外部クライアント(External Client) - アクティブ： 外部クライアント(External Client)がアクティブでセンサーに認識されていることを示します。
	外部クライアント(External Client) - 非アクティブ： センサーに認識されていた外部クライアント(External Client)が非アクティブであることを示します。
	ゲストクライアント - アクティブ： ゲストクライアントがアクティブでセンサーに認識されていることを示します。
	ゲストクライアント - 非アクティブ： センサーに認識されていたゲストクライアントが非アクティブであることを示します。
	未分類クライアント - アクティブ： 外部クライアント(External Client)がアクティブでセンサーに認識されていることを示します。
	未分類クライアント - 非アクティブ： センサーに認識されていた未分類クライアントが非アクティブであることを示します。
	DoS 攻撃者： DoS 攻撃が実行されているデバイスを示します。

	アドホックモードのクライアント - アクティブ： アドホックモードのクライアントがアクティブでセンサーに認識されていることを示します。
	アドホックモードのクライアント - 非アクティブ： アドホックモードでセンサーに認識されていたクライアントが非アクティブであることを示します。
	センサーアクティブ： センサーがサーバーに接続されネットワークを活発にモニタしていることを示します。 このセンサーは、最新のソフトウェアバージョンで、アップグレードする必要はありません。
	センサー非アクティブ： センサーがサーバーに接続されておらず、現在のネットワークを監視していないことを示します。 このセンサーは、最新のソフトウェアバージョンで、アップグレードする必要はありません。
	センサーのアップグレード中： センサーのアップグレードが進行中であることを示しています。
	センサーのアップグレード要求： センサーを新しいバージョンにアップグレードする必要があることを示します。
	センサーのアップグレード失敗： 新しいバージョンへのセンサーのアップグレードが失敗したことを示します。
	センサー不定： センサーが不定または回復不能な状態にあることを示します。
	Network Detector-アクティブ： Network Detector(ND)がサーバーに接続されており、現在 AP の有線検出に寄与していることを示しています。
	Network Detector-非アクティブ： Network Detector(ND)がサーバーに接続されておらず、現在 AP の有線検出に寄与していないことを示しています。
	AP /センサーコンボ - アクティブ： AP/センサーのコンボデバイスがサーバーに接続され、ネットワークを監視していることを示します。
	AP /センサーコンボ - 非アクティブ： AP /センサーのコンボデバイスがサーバーに接続されておらず、非アクティブであることを示します。
	RSSI レベル 0： 利用可能な信号が非常に弱いことを示します。
	RSSI レベル 1： 弱い信号強度を示します。
	RSSI レベル 2： 中程度の信号強度を示します。
	RSSI レベル 3： 強い信号強度を示します。
	RSSI レベル 4： 非常に強い信号強度を示します。
	表示列： テーブル内のほとんどのフィールドは、表示に選択または必要に応じて非表示にすることができます。 このボタンは、パラメータの選択と設定が表示され、テーブルに非表示にすることができます。
	監視対象のネットワーク： ネットワークがセンサーによって監視されていることを示しています。
	監視対象外のネットワーク： ネットワークがセンサーによって監視されていないことを示します。
	承認されたスマートデバイス： 許可クライアントが承認されたスマートデバイスであることを示します。
	未承認のスマートデバイス： 許可クライアントが未承認のスマートデバイスであることを示します。
	デバイスタイプの変更：スマートデバイスタイプの変更を示します。
	スマートデバイス：ゲストクライアントがスマートデバイスであることを示します。

以下は、管理コンソール(Management Console)上で表示されるイベントリスト関連のアイコン一覧です。

アイコン	説明
	高： 重要度の高いイベントを示します。
	中： 重要度が中程度のイベントを示します。
	低： 重要度の低いイベントを示します。
	New： リードも承認もされていないイベントを示します。
	Read： イベントが読み出されたことを示します。
	承認済み： イベントが読み込まれ、承認されたことを示します。
	Live： イベントを発生させたトリガーが動作しているか、存続しているライブイベントを示し、 このイベントは有効な開始タイムスタンプを持っています。
	Live と更新： イベントが最後に読み込まれたあとに、なんらかのアクティビティが起きて、更新されたライブイベントを示します。
	瞬間的： 継続性を持っていないトリガーに基づいてトリガーされる瞬間的なイベントを示します。
	期限切れ： イベントを発生させたトリガーが動作していないか、存続していない期限切れのイベントを示し、 このイベントは有効な開始/停止タイムスタンプを持っています。
	安全： イベントがシステムの脆弱性ステータスに関与しないことを示します。
	脆弱： イベントがシステムの脆弱性ステータスに関与することを示します。
	干渉デバイス/ジャマー・アイコン： RF ジャマーまたは非 Wi-Fi 干渉の発生源であるデバイスを示します。

以下は、管理コンソール(Management Console)上で表示されるロケーションリスト関連のアイコン一覧です。

アイコン	説明
	ロケーションフォルダーを示します。
	ロケーションフロアを示します。
	不明なロケーションフロアを示します。
	ルートロケーションを示します。
	安全なロケーションフロアを示します。
	脆弱なロケーションフロアを示します。
	安全なロケーションフォルダーを示します。
	脆弱なロケーションフォルダーを示します。
	脆弱なルートロケーションを示します。
	安全なルートロケーションを示します。
	脆弱な不明ロケーションフロアを示します。
	安全な不明ロケーションフロアを示します。

NECプラットフォームズ株式会社
管理コンソール (Management Console) ユーザーガイド 第 5 版

2019 年 12 月
AM1-002924-005