不正管理および aWIPS ワークフローの構築と展開

不正管理と aWIPS ワークフローの概要

Cisco DNA Center 不正管理および aWIPS ワークフローを使用すると、許可リストに一括で移動する不正アクセスポイントの MAC アドレスを確認してマークを付け、選択したアクセスポイントの MAC アドレスの一括許可リストを処理できます。

不正管理および aWIPS ワークフローは、Cisco AireOS コントローラおよび Cisco Catalyst 9800 シリーズワイヤレスコントローラに関連付けられている AP をサポートします。

このワークフローでは、次の不正 AP タイプを許可リストに移動できます。

- Rogue on Wire
- ハニーポット
- Interferer
- Neighbor

このワークフローでは、次の不正 AP タイプを許可リストに移動することはできません。

- AP Impersonation
- Friendly

不正管理と aWIPS ワークフローの設定

この手順では、不正 AP の MAC アドレスを許可リストに一括で移動する方法を示します。これらのアドレスは、Cisco DNA Center で高脅威として報告しないアドレスです。

始める前に

次のタスクを実行するには、SUPER-ADMIN-ROLE または NETWORK-ADMIN-ROLE 権限が必要です。

ステップ 1 メニューアイコン（☰）をクリックして、**ワークフロー** > **不正管理と aWIPS ワークフローの設定**。

[Set up Rogue Management and aWIPS] ウィンドウが表示されます。

ステップ 2 [Let's Do it] をクリックします。

今後この画面をスキップするには、[Don't show this to me again] チェックボックスをオンにします。

[Bulk upload allowed access Points] ウィンドウが表示されます。

ステップ 3 [Search] フィールドでは、前のワークフローですでに追加されている MAC アドレスを検索できます。

[Export] をクリックし、許可リストをエクスポートします。

ステップ 4 サンプル CSV テンプレートファイルをダウンロードし、MAC アドレス、操作、およびカテゴリを手動で追加して、一括許可リストテンプレートを作成できます。[Download the sample CSV template from here] リンクをクリックします。

通知記号にカーソルを合わせると、許可されている MAC アドレス、操作、およびカテゴリの形式を表示できます。

ステップ 5 CSV ファイルをボックス領域にドラッグアンドドロップするか、[Choose a file] をクリックしてシステム上の CSV ファイルを参照します。CSV ファイルの最大サイズは 1.2 MB です。

（注） Cisco DNA Center で検証チェックが実行されます。アップロードされた CSV ファイルが次の要件を満たしていない場合、エラーメッセージが表示されます。

- MAC アドレスが有効な不正ポイント MAC アドレスではありません。
- すべての不正アクセスポイントの MAC アドレスがシステムにすでに存在しているか、または削除操作の対象となる不正アクセスポイントの MAC アドレスがありません。

緑色のチェックマークは、アップロードされた CSV ファイルの内容が有効であることを示します。

ステップ 6 [Next] をクリックします。

ステップ 7 [Summary] ウィンドウの [Uploaded bulk allowed list MAC addresses] テーブルに、許可された MAC アドレスのリスト、およびそれぞれの動作とアクションが表示されます。

- [All]：すべての MAC アドレスのリスト、およびそれぞれの動作とアクションを一括して表示します。
- [Create]：作成された MAC アドレスのリスト、およびそれぞれの操作とアクションをまとめて表示します。
- [Delete]：削除された MAC アドレスのリスト、およびそれぞれの動作とアクションが一括して表示されます。

- [No Action]：すでに削除されている MAC アドレスのリスト、およびそれぞれの操作とアクションが表示されます。

ステップ 8 [Continue to allowed list] をクリックし、後続の警告ポップアップウィンドウで [Yes] をクリックします。

タスク完了**[Allowed List Updated]** ウィンドウが表示されます。

ステップ 9 [Go to Rogue and aWIPS Home Page] リンクをクリックします。

[Rogue and aWIPS] ダッシュボードが表示されます。

[Threat] テーブルで、Cisco DNA Center により指定した不正 AP MAC アドレスが [Type] 列の下の [Allowed List] に分類されます。

ステップ 10 許可リストに不正 AP MA Cアドレスを個別に追加または削除するには、[Threat MAC address] 列の下にリストされている不正 MAC アドレスをクリックします。

[Threat 360] ウィンドウが表示されます。

ステップ 11 [Action] ドロップダウンリストをクリックし、[Add to Allowed list] を選択します。

許可リストから不正 AP MAC アドレスを個別に削除するには、[Action] ドロップダウンリストで [Remove from Allowed] リストを選択します。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。