

ワイヤレス LAN コントローラの信頼された AP ポリシー

目次

[概要](#)

[前提条件](#)

[要件](#)

[表記法](#)

[信頼された AP ポリシー](#)

[信頼された AP とは何か。](#)

[WLC GUI からの信頼された AP で AP の設定方法か。](#)

[信頼された AP ポリシー設定の概要](#)

[設定する方法 WLC の AP ポリシーを信頼しましたか。](#)

[信頼された AP ポリシーの違反 警告メッセージ](#)

[関連情報](#)

概要

この資料はワイヤレス LAN コントローラ (WLC) の信頼された AP ワイヤレス保護ポリシーを記述し、信頼された AP ポリシーを定義し、すべての信頼された AP ポリシーの簡潔な説明を提供したものです。

前提条件

要件

ワイヤレス LAN セキュリティ パラメータの基本的な知識があることを確認して下さい (SSID のような、暗号化、認証、等) 。

表記法

ドキュメント表記の詳細は、『[シスコテクニカルティップスの表記法](#)』を参照してください。

信頼された AP ポリシー

信頼された AP ポリシーは顧客にコントローラと共に平行自律 AP ネットワークがあるシナリオで使用するよう設計されているコントローラのセキュリティ機能です。シナリオがコントローラの信頼された AP として、自律 AP マークすることができることおよびユーザ使用する WEP か WPA 必要がある信頼された AP (、自身の SSID だけ、短いプレアンプル、等) はこれらのためのポリシーを定義できます。アラームがそのネットワーク管理デバイス (Wireless Control

System) にこれらのポリシーに適合するこれらの AP 失敗のうちのどれかによってコントローラ状態発すれば信頼された AP は設定されたポリシーに違反しました。

信頼された AP とは何か。

信頼された AP は組織の一部の AP です。ただし、それらによりネットワークへのセキュリティの脅威を引き起こしません。これらの AP はまた友好的な AP と呼ばれます。複数のシナリオによってはどこに信頼された AP で AP を設定したいと思うかもしれませんがあります。

たとえば、ネットワークの AP の異なるカテゴリがあるかもしれません (以下を参照) :

- 所有する LWAPP (多分 IOS か VxWorks を実行します) を実行しない AP
- 従業員が持って来る LWAPP AP (管理者のナレッジと)
- LWAPP AP は存在するネットワークをテストするのが常でありました
- その LWAPP AP は相手所有します

通常、信頼された AP はカテゴリ 1 に分類される AP です、所有する LWAPP を実行しない AP の。それらは VxWorks か IOS を実行する古い AP であるかもしれません。これらの AP がネットワークに害を与えないようにするために、ある特定の機能は正しい SSID および認証種別のような、実施することができます。WLC の信頼された AP ポリシーを設定し、信頼された AP がこれらのポリシーに適合することを確かめて下さい。そうでなかったら、コントローラをネットワーク管理デバイス (WCS) に発生のような複数の処置を、アラームとるために設定できます。

相手に属する既知 AP は信頼された AP で設定することができます。

通常、MFP (管理 フレーム 保護) は WLC の加入からの正当ではない LWAPP AP ではない AP を防ぐ必要があります。NIC カード サポート MFP が、それら実質 AP 以外デバイスからの deauthentications を受け入れればことができなければ。MFP に関する詳細については [WLC および LAP 設定例のインフラストラクチャ 管理 フレーム 保護 \(MFP \)](#) を参照して下さい。

持っていれば VxWorks か IOS (1) 次 カテゴリを、実行する AP は決して LWAPP グループ加入しませんし、MFP を、あなたをそのページにリストされているポリシーを実施したいと思うかもしれませんしません。このような場合、信頼された AP ポリシーは対象の AP のためのコントローラで設定される必要があります。

一般に不正な AP について確認し、それはネットワークへ脅威ではないこと識別すれば、既知信頼された AP としてこと AP 識別できます。

WLC GUI からの信頼された AP で AP の設定方法が。

信頼された AP で AP を設定するためにこれらのステップを完了して下さい:

1. HTTP か https を通して WLC の GUI にログインしますログインして下さい。
2. コントローラ メインメニューから、『Wireless』をクリックして下さい。
3. theWireless ページの左側にあるメニューでは不正な AP をクリックして下さい。不正な AP ページはネットワークの不正な AP として検出するすべての AP をリストします。
4. 不正な AP のこのリストから、カテゴリ 1 の下で下る信頼された AP で設定されてほしいと思う AP を見つけて下さい (前のセクションで説明されているように)。不正な AP ページでリストされている MAC アドレスの AP を見つけることができます。望ましい AP がこのページにない場合、Next ページからの AP を識別するために『Next』をクリックして下さい。

5. 望ましい AP が不正な AP リストからあったら、AP の Detail ページに連れて行く、AP に対応する **Edit ボタン** をクリックして下さい。Details ページ不正な AP ではこの AP についての詳細な情報を見つけることができます (のようなかどうか有線ネットワークに、また AP の現在のステータス等接続されるその AP)。
6. この AP を信頼された AP で設定するために、**既知 内部** をアップデートステータス ドロップダウン リストから選択し、『Apply』 をクリックして下さい。既知 内部に AP ステータスをアップデートするとき、この AP はこのネットワークの信頼された AP で設定されます。
7. 信頼された AP で設定したいと思うすべての AP のためのこれらのステップを繰り返して下さい。

信頼された AP 設定を確認して下さい

AP がコントローラ GUI からの信頼された AP で正しく設定されることを確認するためにこれらのステップを完了して下さい:

1. 『Wireless』 をクリックして下さい。
2. theWireless ページの左側にあるメニューでは**既知悪党 AP** をクリックして下さい。望ましい AP は **既知** としてリストされているステータスの既知悪党 AP ページで書かれる必要があります。

信頼された AP ポリシー設定の概要

WLC にこれらの信頼された AP ポリシーがあります:

- [実施された暗号化ポリシー](#)
- [実施されたプリアンブル ポリシー](#)
- [実施された無線型ポリシー](#)
- [SSID を検証して下さい](#)
- [信頼された AP が抜けていれば場合アラート](#)
- [信頼された AP エントリ \(秒 \) のための有効期限タイムアウト](#)

実施された暗号化ポリシー

このポリシーが使用する信頼された AP が必要がある暗号化タイプを定義するのに使用されています。 実施された暗号化ポリシーの下でのこれらの暗号化タイプ設定できます:

- なし
- オープン
- WEP
- WPA/802.11i

WLC は信頼された AP で設定される暗号化タイプが「**実施された暗号化ポリシー**」設定で設定される暗号化タイプと一致するかどうか確かめます。 信頼された AP が指定暗号化タイプを使用しない場合、WLC によっては管理 システムに適切な行動を奪取 するためにアラームが発します。

実施されたプリアンブル ポリシー

無線プリアンブルは (時々ヘッダと呼ばれる) ワイヤレス デバイスが必要とする情報が含まれて

いるパケットを送信し、受信するときパケットのヘッダーにデータのセクションです。短いプリアンブルはスループット パフォーマンスを改善します、従ってデフォルトで有効になります。一方、SpectraLink NetLink 電話機のようないくつかの無線デバイスでは、ロングプリアンブルが必要です。実施されたプリアンブル ポリシーの下でのこれらのプリアンブル オプション設定できます:

- なし
- Short
- Long

WLC は信頼された AP で設定されるプリアンブル型が「**実施されたプリアンブル ポリシー**」設定で設定されるプリアンブル型と一致するかどうか確かめます。信頼された AP が規定されたプリアンブル型を使用しない場合、WLC によっては管理 システムに適切な行動を奪取するためにアラームが発します。

実施された無線型ポリシー

このポリシーが使用する信頼された AP が必要がある無線型を定義するのに使用されています。実施された無線型ポリシーの下でのこれら無線型設定できます:

- なし
- 802.11b だけ
- 802.11a だけ
- 802.11b/g だけ

WLC は信頼された AP で設定される無線型が「**実施された無線型ポリシー**」設定で設定される無線型と一致するかどうか確かめます。APdoes 信頼されたアラームが管理 システムに適切な行動を奪取するためにない使用によってが規定された無線、WLC 発すれば。

SSID を検証して下さい

コントローラで設定される SSID に対してコントローラを信頼された AP SSID を検証するために設定できます。信頼された AP SSID がコントローラ SSID の 1 つと一致する場合、コントローラによってはアラームが発します。

信頼された AP が抜けていれば場合アラート

このポリシーが有効になる場合、WLC は信頼された AP が既知悪党 AP リストから抜けている場合管理 システムを警告 します。

信頼された AP エントリ (秒) のための有効期限タイムアウト

この有効期限タイムアウト値は信頼された AP が WLC エントリから切られ、フラッシュされたと考えられる前に秒数を規定 します。秒のこのタイムアウト値を規定 できます (120 - 3600 秒)。

設定する方法 WLC の AP ポリシーを信頼しましたか。

GUI によって WLC の信頼された AP ポリシーを設定するためにこれらのステップを完了して下さい:

注: 同じ WLC ページのすべての信頼された AP ポリシー常駐する。

1. WLC GUI メインメニューから、『Security』をクリックして下さい。
2. セキュリティのページの左側にあるメニューからワイヤレス保護ポリシー先頭に立の下にリストされている**信頼された AP ポリシー**をクリックして下さい。
3. Policies ページ信頼された AP で実施された暗号化ポリシー ドロップダウン リストから望ましい暗号化タイプを (どれも、WEP、WPA/802.11i 開きません) 選択して下さい。
4. 実施されたプリアンブル型ポリシー ドロップダウン リストから望ましいプリアンブル型を (どれも、短く、長い) 選択して下さい。
5. 実施された無線型ポリシー ドロップダウン リストから望ましい無線型を (どれも、802.11b だけ、802.11a だけ、802.11b/g だけ) 選択して下さい。
6. **検証 SSID Enabled チェックボックス**をチェックするか、または検証 SSID 設定を有効にするか、またはディセーブルにするためにチェックを外して下さい。
7. 信頼された AP が抜けた設定である場合**信頼された AP が抜けた Enabled チェックボックス**アラートをディセーブルにするために有効にするか、または**である場合アラート**をチェックするか、またはチェックを外して下さい。
8. **信頼された AP エントリ オプションの有効期限タイムアウト**の値を (秒で) 入力して下さい。
9. [Apply] をクリックします。

注: WLC CLI からのこれらの設定を行うために、適切なポリシー オプションと構成 **wps 信頼 ap** コマンドを使用できます。

```
Cisco Controller) >config wps trusted-ap ? encryption Configures the trusted AP encryption policy to be enforced. missing-ap Configures alert of missing trusted AP. preamble Configures the trusted AP preamble policy to be enforced. radio Configures the trusted AP radio policy to be enforced. timeout Configures the expiration time for trusted APs, in seconds.
```

信頼された AP ポリシーの違反 警告メッセージ

コントローラが表示する信頼された AP ポリシーの違反 警告メッセージの例はここにあります。

```
Thu Nov 16 12:39:12 2006 [WARNING] apf_rogue.c 1905: Possible AP impersonation of xx:xx:xx:xx:xx:xx, using source address of 00:16:35:9e:6f:3a, detected by 00:17:df:7d:e1:70 on slot 0
Thu Nov 16 12:39:12 2006 [SECURITY] apf_rogue.c 1490: Trusted AP Policy failed for AP xx:xx:xx:xx:xx:xx - invalid SSID 'SSID1' Thu Nov 16 12:39:12 2006 [SECURITY] apf_rogue.c 1457: Trusted AP Policy failed for AP xx:xx:xx:xx:xx:xx - invalid encryption type Thu Nov 16 12:39:12 2006 Previous message occurred 6 times
```

強調表示されたエラーメッセージにここに注意して下さい。これらのエラーメッセージは信頼された AP で設定される SSID および暗号化タイプが信頼された AP ポリシー 設定を一致することを示します。

同じ警告メッセージは WLC GUI から見られる場合があります。このメッセージを表示するために、WLC GUI メインメニューに行き、『Monitor』をクリックします。Monitor ページの最新トラップ セクションでは、完全に最近を表示するために**すべてを警告**します WLC の『View』をクリックして下さい。

最新トラップ ページで、このイメージに示すように信頼された AP ポリシーの違反 警告メッセージを生成するコントローラを識別できます:

関連情報

- [Ciscoワイヤレス LAN コントローラ設定 ガイド、リリース 5.2 - RF グループの弁柄アクセスポイント 検出を有効に すること](#)
- [Ciscoワイヤレス LAN コントローラ設定 ガイド、リリース 4.0 -セキュリティソリューションを設定すること](#)
- [Unified Wireless Network における不正検出](#)
- [SpectraLink 電話器の設計および展開ガイド](#)
- [基本的な無線 LAN 接続の設定例](#)
- [ワイヤレス LAN ネットワークの接続に関するトラブルシューティング](#)
- [ワイヤレス LAN コントローラでの認証の設定例](#)
- [テクニカルサポートとドキュメント - Cisco Systems](#)