AireOS WLCでの802.1Xクライアント除外の確認

内容

はじめに

このドキュメントでは、AireOSワイヤレスLANコントローラ(WLC)での802.1Xクライアント除外について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco AireOS WLC
- 802.1Xプロトコル
- Remote Authentication Dial-In User Service（RADIUS）
- アイデンティティサービスエンジン(ISE)

使用するコンポーネント

このドキュメントの情報は、AireOSに基づくものです。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

802.1Xクライアント除外は、WLCなどの802.1Xオーセンティケータで使用する重要なオプションです。これはactivities overloadまたは不適切な機能の拡張認証プロトコル（EAP ）クライアントが認証サーバのオーバーロードを防止するためです。

ユーザケース

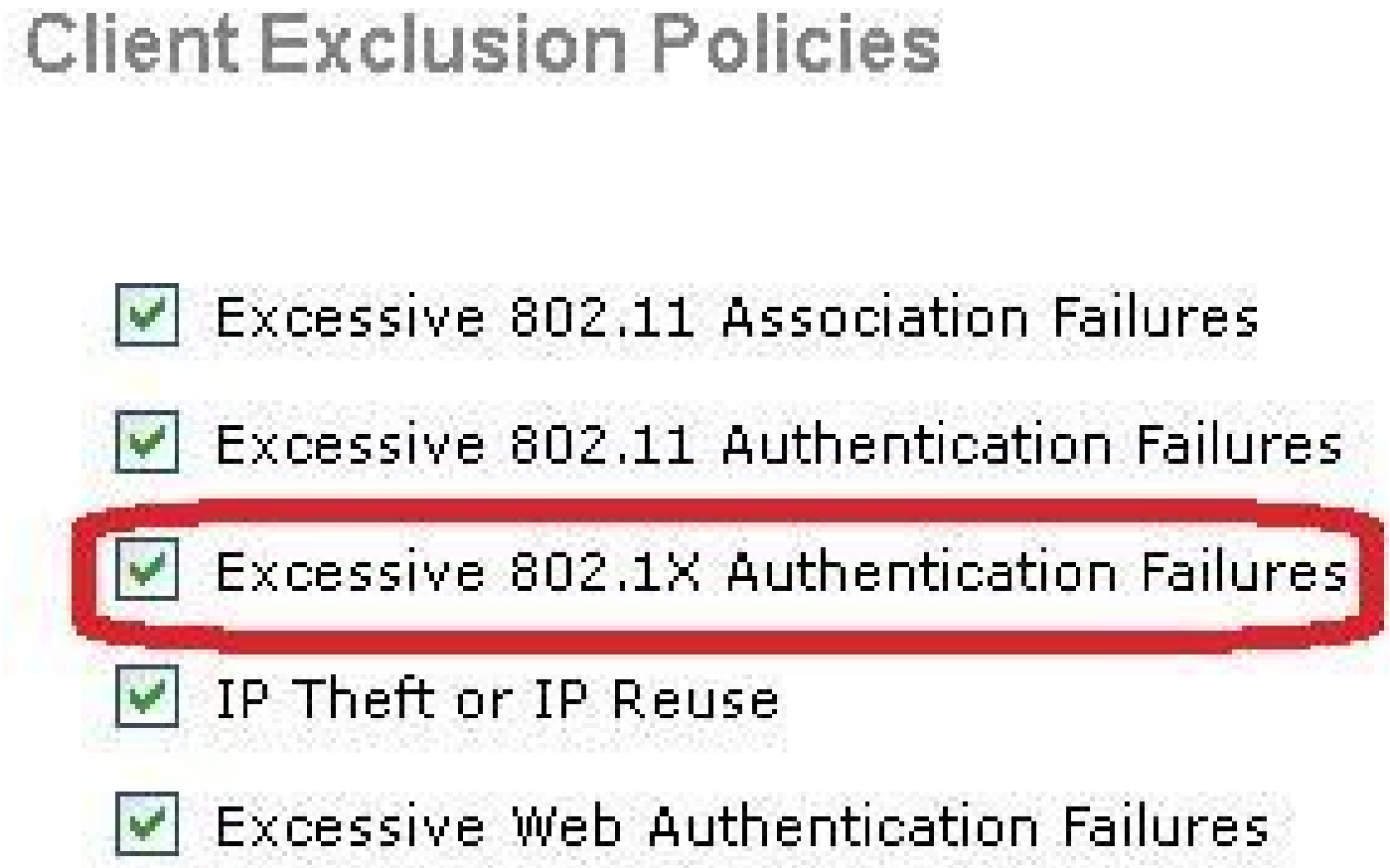
使用例を以下に示します。

- 誤ったクレデンシャルで設定されたEAPサプリカント。EAP サプリカントなど、ほとんどのサプリカントは、失敗が何回か続いたら認証の試みを中止します。ただし、一部の EAP サプリカントは何回でも再認証を試みます。このようなクライアントが RADIUS サーバを過負荷にして、ネットワーク全体のサービス妨害（DoS）を引き起こします。
- 主要なネットワークフェールオーバーの後、何百または何千ものEAPクライアントが同時に認証を試みることができます。その結果、認証サーバが過負荷になり、応答が遅くなる可能性があります。応答の遅れを処理する前にクライアントまたはオーセンティケータがタイムアウトすると、認証の試みがタイムアウトするまで続いてから、再び応答を処理しようとして悪循環に陥る可能性があります。

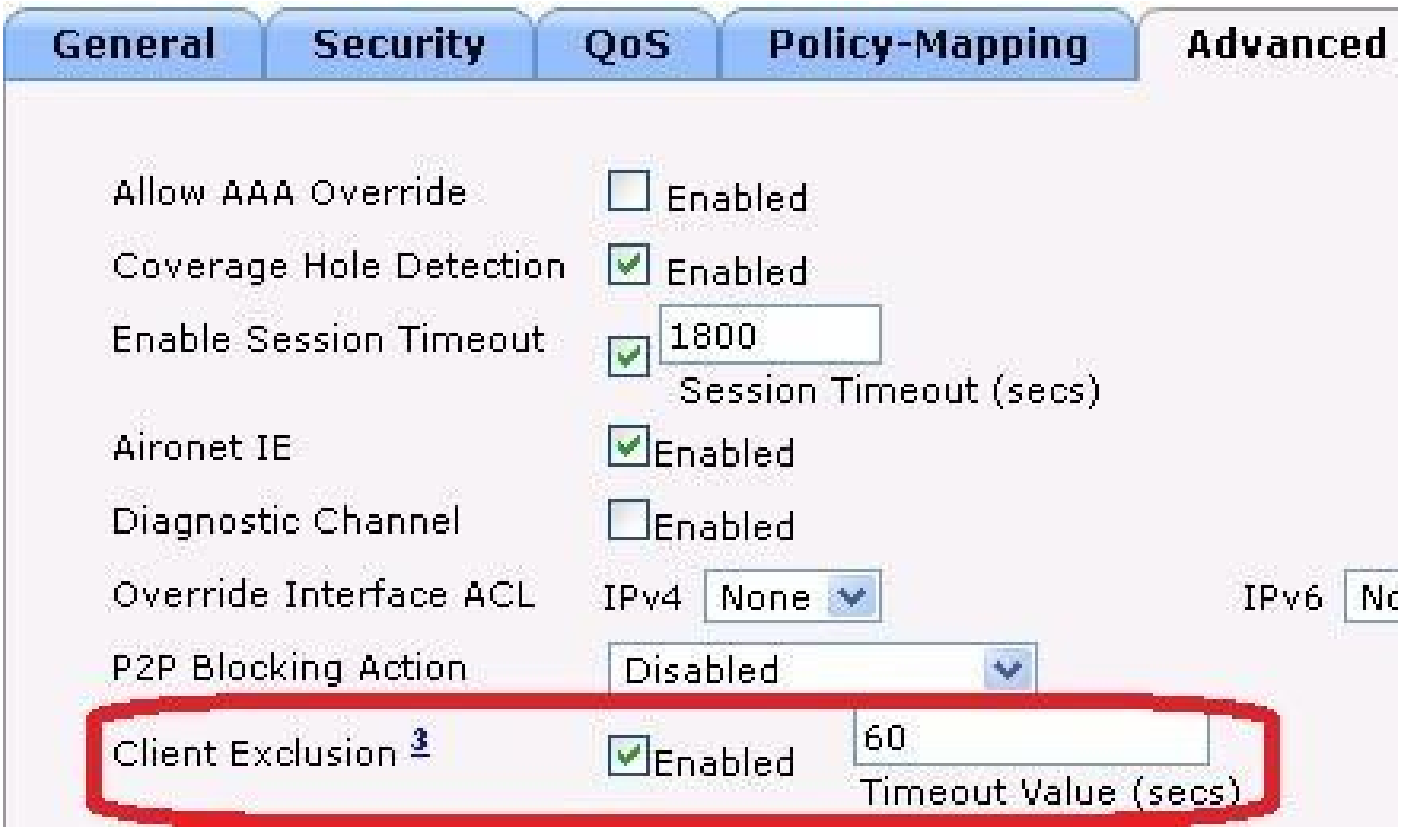
注：認証の試行を成功させるには、アドミッション制御メカニズムが必要です。

802.1Xクライアント除外の動作

802.1Xクライアント除外は、過剰な802.1X認証の失敗後、一定時間、クライアントが認証試行を送信することを防止します。AireOS WLC 802.1Xでは、クライアントの除外は、デフォルトで Security > Wireless Protection Policies > Client Exclusion Policiesの順に移動してグローバルに有効になり、次の図で確認できます。



クライアント除外は、WLANごとに有効または無効にできます。デフォルトでは、AireOS 8.5より前の60秒、およびAireOS 8.5より前の180秒のタイムアウトで有効になっています。



RADIUSサーバを過負荷状態から保護するための除外設定

ワイヤレスクライアントが正しく機能しないために発生する過負荷からRADIUSサーバが保護されていることを検証するには、次の設定が有効であることを確認します。

- Excessive 802.1X Authentication FailuresがWLCグローバルクライアント除外ポリシーで選択されている。
- Client Exclusionは、WLAN advanced settingsでEnabledに設定されています。
- Client Exclusion Timeout Valueは、60 ~ 300秒に設定されています。

> 注:300秒を超える値を設定すると保護は向上しますが、ユーザから苦情が寄せられる可能性があります。

- AireOS EAPタイマーとISE Protected Extensible Authentication Protocol(PEAP)設定の設定

802.1X除外の動作を妨げる問題

WLCとRADIUSサーバのいくつかの設定によって、802.1Xクライアント除外の動作が妨げられる可能性があります。

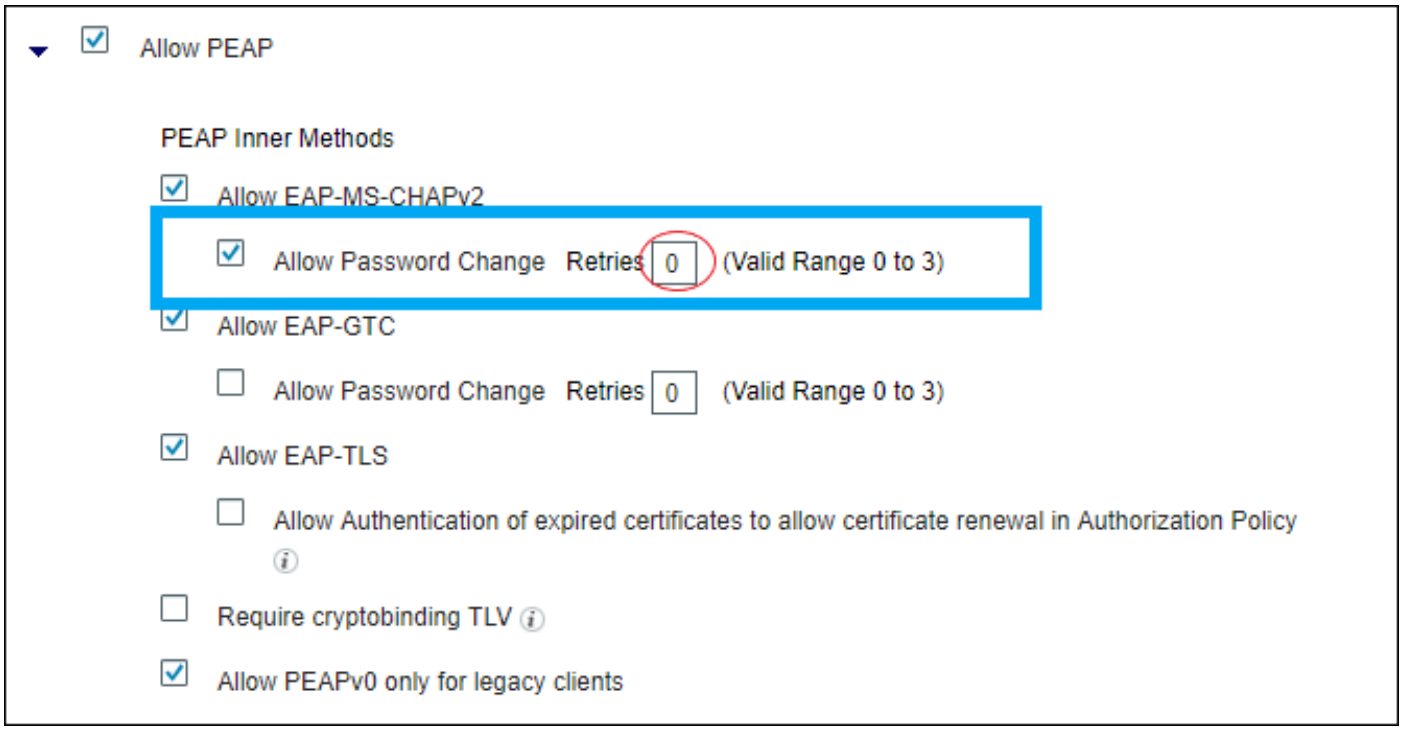
WLCのEAPタイマー設定が原因で除外されないクライアント

デフォルトでは、WLANでClient ExclusionがEnabledに設定されている場合、ワイヤレスクライアントは除外されません。これは、デフォルトのEAPタイムアウトが30秒と長く、誤動作しているクライアントが除外をトリガーするのに十分な失敗を連続してヒットしないことが原因です。802.1Xクライアント除外を有効にするために、EAPタイムアウトを短くし、再送信の数を増やします。タイムアウトの例を参照してください。

```
config advanced eap identity-request-timeout 3
config advanced eap identity-request-retries 10
config advanced eap request-timeout 3
config advanced eap request-retries 10
```

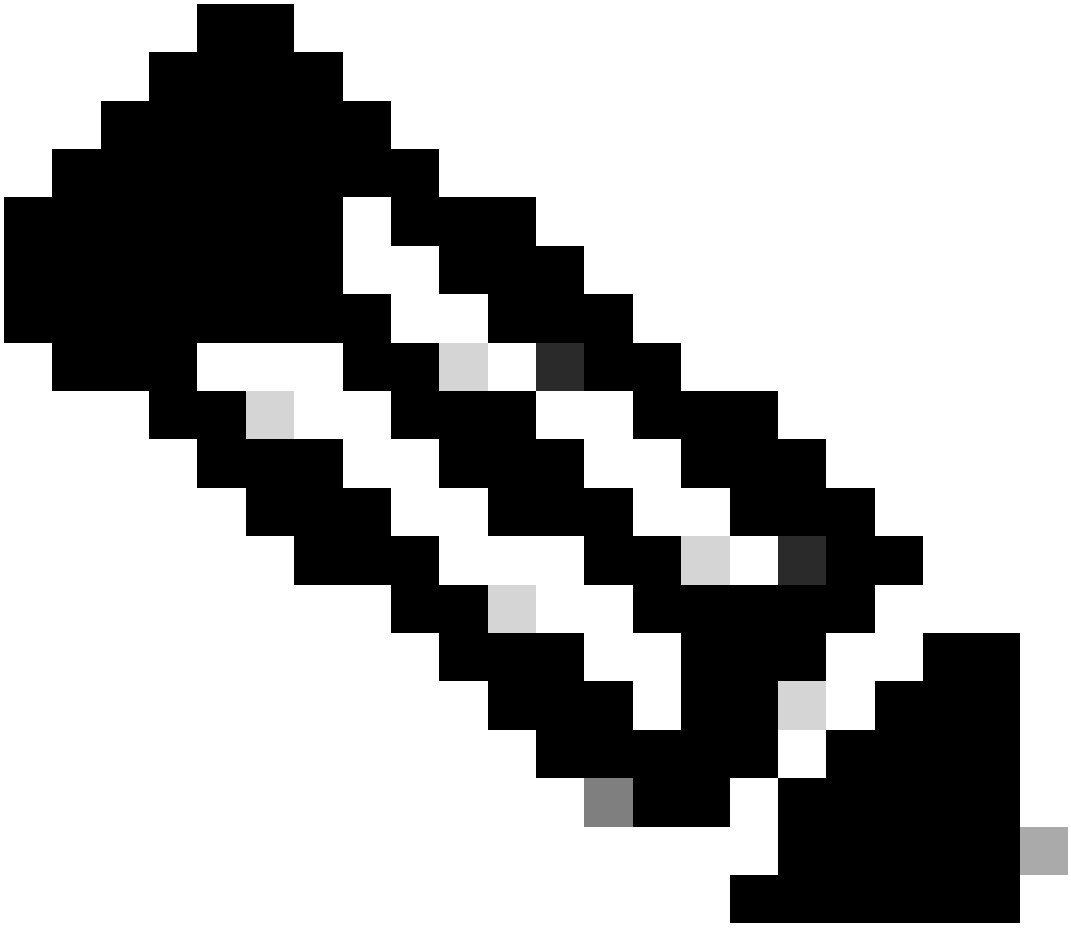
ISE PEAP設定が原因で除外されないクライアント

802.1Xクライアント除外が機能するためには、認証が失敗した場合にRADIUSサーバからAccess-Rejectが送信される必要があります。RADIUSサーバがISEで、PEAPが使用されている場合、除外は実行されず、ISE PEAPの設定に依存します。ISEで、図に示すように、Policy > Results > Authentication > Allowed Protocols > Default Network Accessの順に移動します。



Retries（右側は赤で囲まれている）を0に設定した場合は、ISEはWLCにただちにアクセス拒否を送信する必要があります。この場合、クライアントを除外するためにWLCを有効にする必要があります（認証を3回試行した場合）。

注：再試行の設定は、パスワードの変更を許可するチェックボックスとは多少関係ありません。つまり、パスワードの変更を許可するチェックボックスがオフの場合でも、再試行の値に問題がない可能性があります。ただし、再試行を0に設定すると、パスワードの変更を許可する機能は動作しません。



注：詳細については、Cisco Bug ID CSCsq16858を参照してください。シスコのバグツールおよび情報にアクセスできるのは、シスコの登録ユーザのみです。

関連情報

- 大規模なワイヤレス RADIUS ネットワークのメルトダウンを防止する
- シスコのテクニカルサポートとダウンロード

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。