Vérification de l'exclusion du client 802.1X sur un WLC AireOS

Table des matières

Introduction

Ce document décrit l'exclusion du client 802.1X sur un contrôleur LAN sans fil (WLC) AireOS.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- WLC Cisco AireOS
- Protocole 802.1X
- RADIUS (Remote Authentication Dial-In User Service)
- Identity Service Engine (ISE)

Composants utilisés

Les informations contenues dans ce document sont basées sur AireOS.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Informations générales

L'exclusion du client 802.1X est une option importante à avoir sur un authentificateur 802.1X tel qu'un WLC. Ceci afin d'éviter une surcharge de l'infrastructure du serveur d'authentification par les clients EAP (Extensible Authentication Protocol) qui sont hyperactifs ou fonctionnent de manière incorrecte.

Cas d'utilisateurs

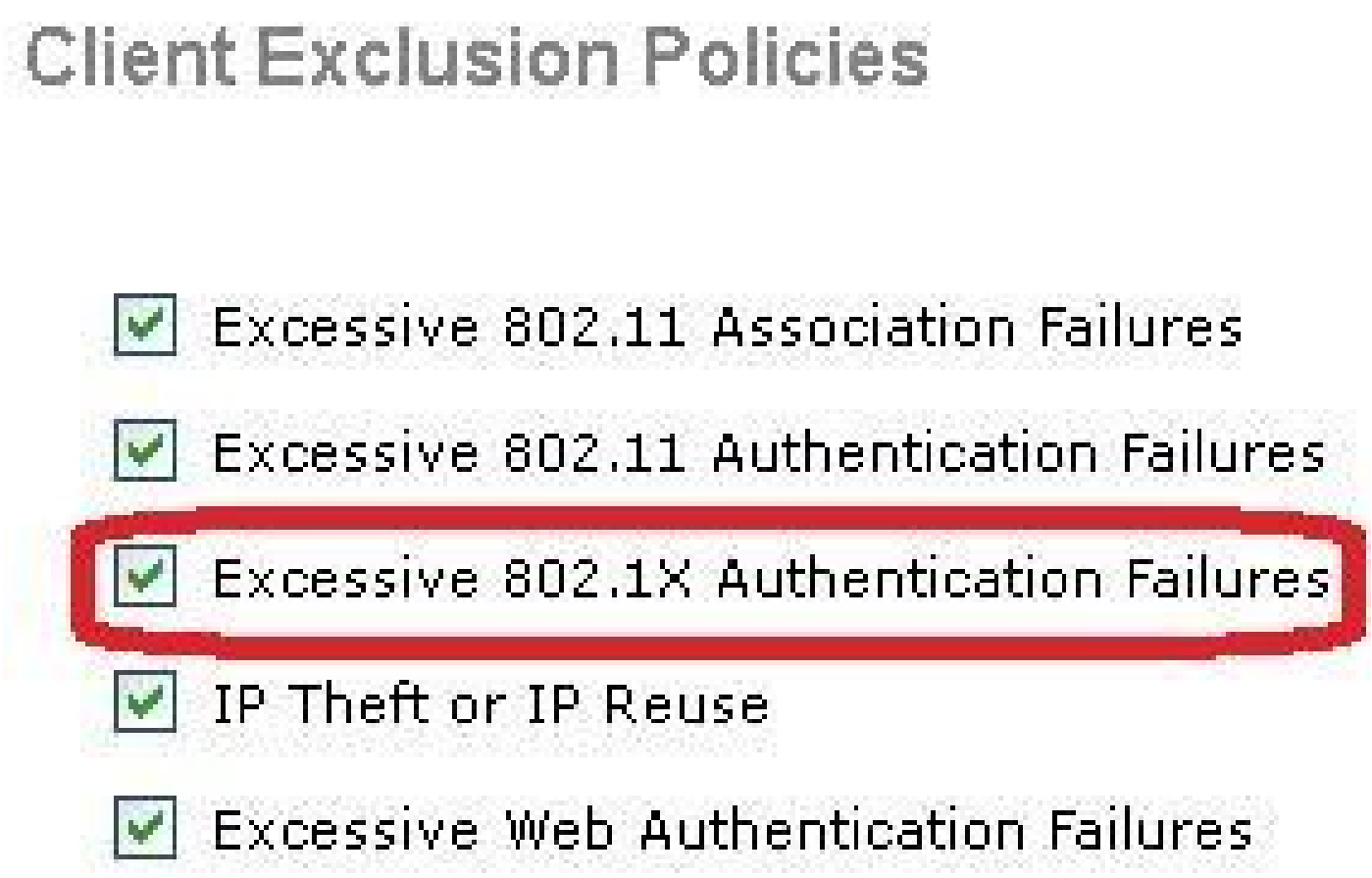
Exemples d'utilisation :

- Un demandeur EAP qui est configuré avec des informations d'identification incorrectes. La plupart des demandeurs, tels que les demandeurs EAP, cessent leurs tentatives d'authentification après quelques échecs successifs. Cependant, certains demandeurs EAP continuent de tenter de se réauthentifier en cas d'échec, peut-être plusieurs fois par seconde. Certains clients surchargent les serveurs RADIUS et entraînent un déni de service (DoS) pour l'ensemble du réseau.
- Après un basculement de réseau majeur, des centaines ou des milliers de clients EAP peuvent simultanément tenter de s'authentifier. Par conséquent, les serveurs d'authentification peuvent être surchargés et fournir une réponse lente. Si le délai d'attente des clients ou de l'authentificateur est dépassé avant le traitement de la réponse lente, un cercle vicieux peut se produire lorsque les tentatives d'authentification continuent à expirer, puis tentent de traiter à nouveau la réponse.

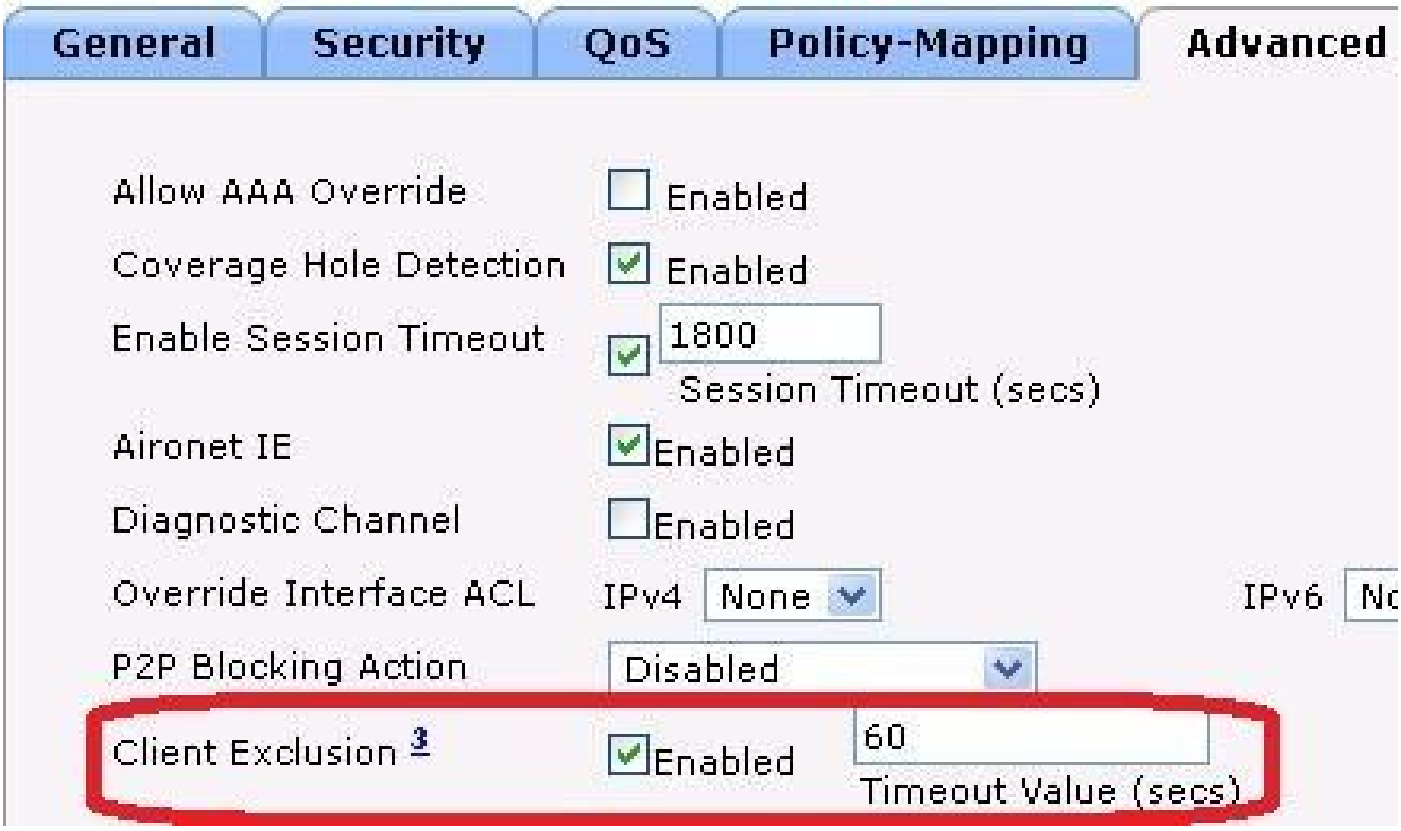
Remarque : un mécanisme de contrôle d'admission est requis pour permettre aux tentatives d'authentification de réussir.

Comment fonctionne l'exclusion du client 802.1X ?

L'exclusion de client 802.1X empêche les clients d'envoyer des tentatives d'authentification pendant un certain temps après des échecs d'authentification 802.1X excessifs. Sur un AireOS WLC 802.1X, l'exclusion de client est globalement activée en naviguant vers Security > Wireless Protection Policies > Client Exclusion Policies par défaut et peut être vu dans cette image.



L'exclusion de client peut être activée ou désactivée pour chaque WLAN. Par défaut, il est activé avec un délai d'attente de 60 secondes avant AireOS 8.5 et de 180 secondes à partir d'AireOS 8.5.



Paramètres d'exclusion pour protéger les serveurs RADIUS contre la surcharge

Afin de valider que le serveur RADIUS est protégé contre la surcharge due à des clients sans fil qui ne fonctionnent pas correctement, vérifiez que ces paramètres sont en vigueur :

- Des échecs d'authentification 802.1X excessifs sont sélectionnés dans les stratégies d'exclusion client globales du WLC.
- L'exclusion du client est définie sur Activé dans les paramètres avancés du WLAN.
- La valeur du délai d'exclusion du client est définie sur 60 à 300 secondes.

> Remarque : les valeurs supérieures à 300 secondes offrent une meilleure protection, mais peuvent déclencher des plaintes des utilisateurs.

- Configurer les compteurs AireOS EAP et les paramètres PEAP (Protected Extensible Authentication Protocol) d'ISE

Problèmes empêchant l'exclusion 802.1X de fonctionner

Plusieurs paramètres de configuration, dans le WLC et dans le serveur RADIUS, peuvent empêcher l'exclusion du client 802.1X de fonctionner.

Clients non exclus en raison des paramètres du minuteur EAP WLC

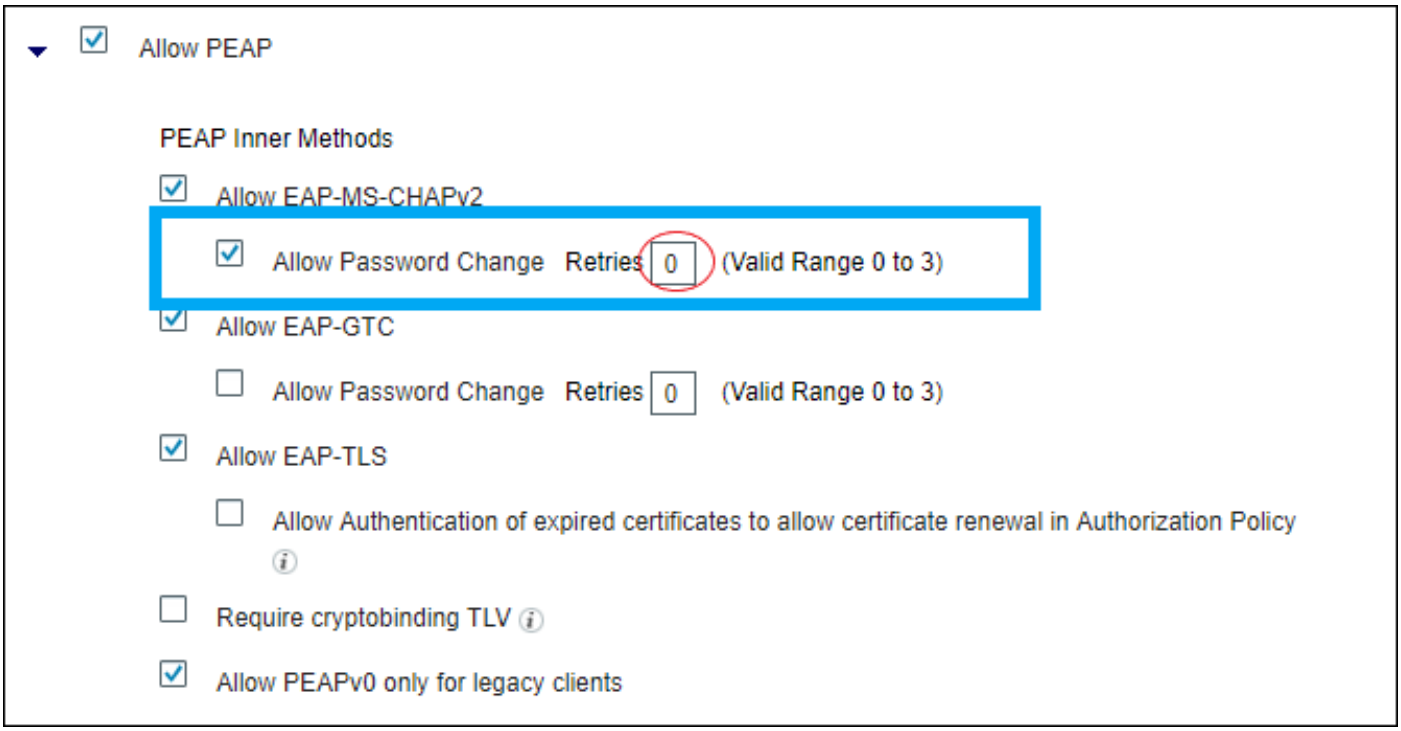
Par défaut, les clients sans fil ne sont pas exclus lorsque l'option Client Exclusion est définie sur Enabled sur le WLAN. Cela est dû à de longs délais d'expiration EAP par défaut de 30 secondes, qui font qu'un client qui se comporte mal n'a jamais atteint assez de défaillances successives pour déclencher une exclusion. Configurez des délais d'expiration EAP plus courts avec un nombre accru de retransmissions pour permettre à l'exclusion du client 802.1X de prendre effet. Voir l'exemple de délai d'attente.

```
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
```

Clients non exclus en raison des paramètres PEAP ISE

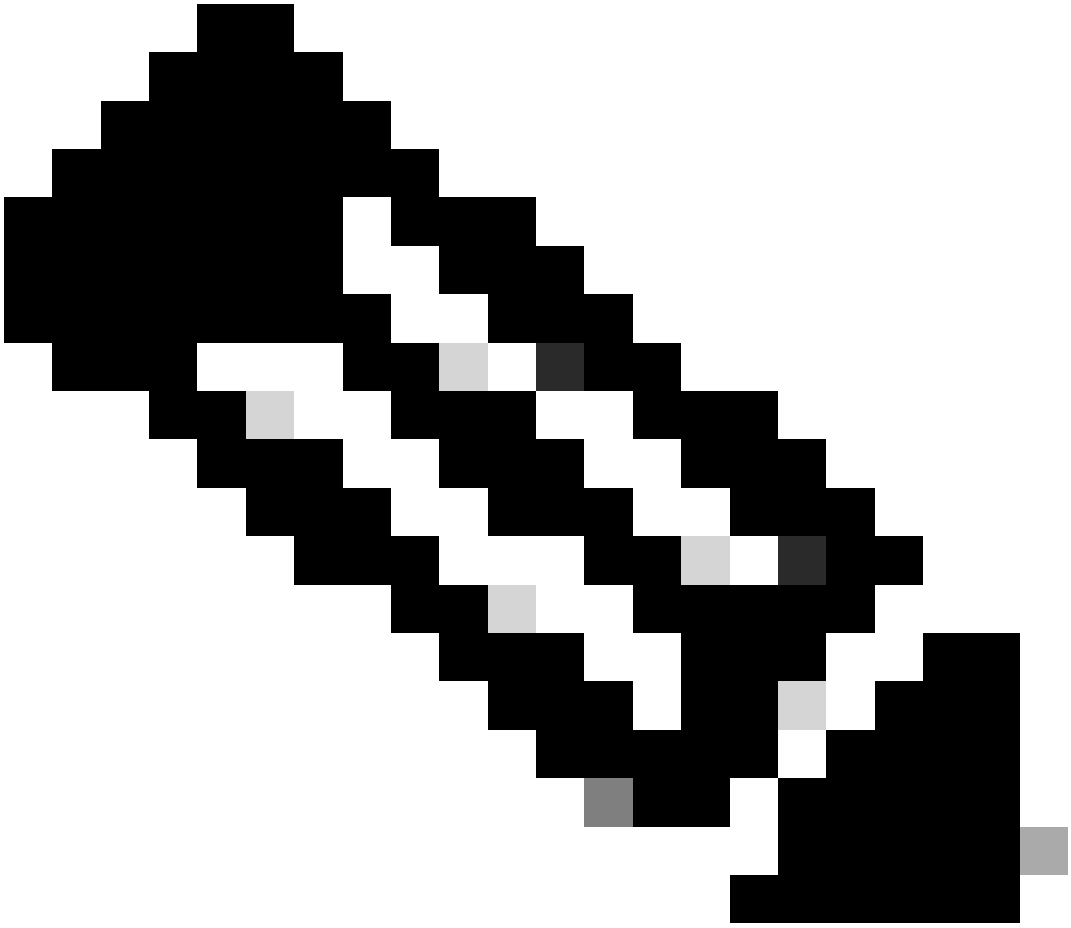
Pour que l'exclusion du client 802.1X fonctionne, le serveur RADIUS doit envoyer un refus d'accès lorsque l'authentification échoue. Si le serveur RADIUS est ISE et si PEAP est utilisé, l'exclusion ne peut pas se produire et dépend des paramètres PEAP ISE. Dans ISE, accédez à Policy >

Results > Authentication > Allowed Protocols > Default Network Access comme indiqué dans l'image.



Si vous définissez Retries (entouré en rouge sur la droite) sur 0, alors ISE doit envoyer Access-Reject immédiatement au WLC, qui doit activer le WLC afin d'exclure le client (s'il essaie trois fois de s'authentifier).

Remarque : le paramètre Retries est quelque peu indépendant de la case à cocher Allow Password Change, c'est-à-dire que la valeur Retries peut être respectée, même si la case à cocher Allow Password Change est désactivée. Cependant, si Retries est défini sur 0, alors Allow Password Change ne fonctionne pas.



Remarque : pour plus d'informations, consultez l'ID de bogue Cisco CSCsq16858. Seuls les utilisateurs Cisco enregistrés peuvent accéder aux informations et aux outils de bogue Cisco.

Informations connexes

- Empêcher la fusion du réseau RADIUS sans fil à grande échelle
- Assistance technique de Cisco et téléchargements

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.