Controleer de uitsluiting van 802.1X-clients op een AireOS WLC

Inhoud

Inleiding

Voorwaarden

- Vereisten
- Gebruikte componenten

Achtergrondinformatie

Gebruikerscases

Hoe werkt 802.1X Client Exclusion?

Uitsluitingsinstellingen om RADIUS-servers te beschermen tegen overbelasting

Problemen die verhinderen dat 802.1X wordt uitgesloten van het werken

- Clients niet uitgesloten vanwege WLC EAP Timer-instellingen
- Clients niet uitgesloten vanwege ISE-PEAP-instellingen

Gerelateerde informatie

Inleiding

Dit document beschrijft de 802.1X-clientuitsluiting op een AireOS draadloze LAN-controller (WLC).

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Cisco AireOS WLC
- 802.1X-protocol
- Remote Verificatie-inbelgebruikersservice (RADIUS)
- Identity Service Engine (ISE)

Gebruikte componenten

De informatie in dit document is gebaseerd op AireOS.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

De 802.1X Client Exclusion is een belangrijke optie om te hebben op een 802.1X authenticator zoals een WLC. Dit om overbelasting van de infrastructuur van de verificatieserver te voorkomen door EAP-clients (Extensible Authentication Protocol) die hyperactief zijn of niet correct functioneren.

Gebruikerscases

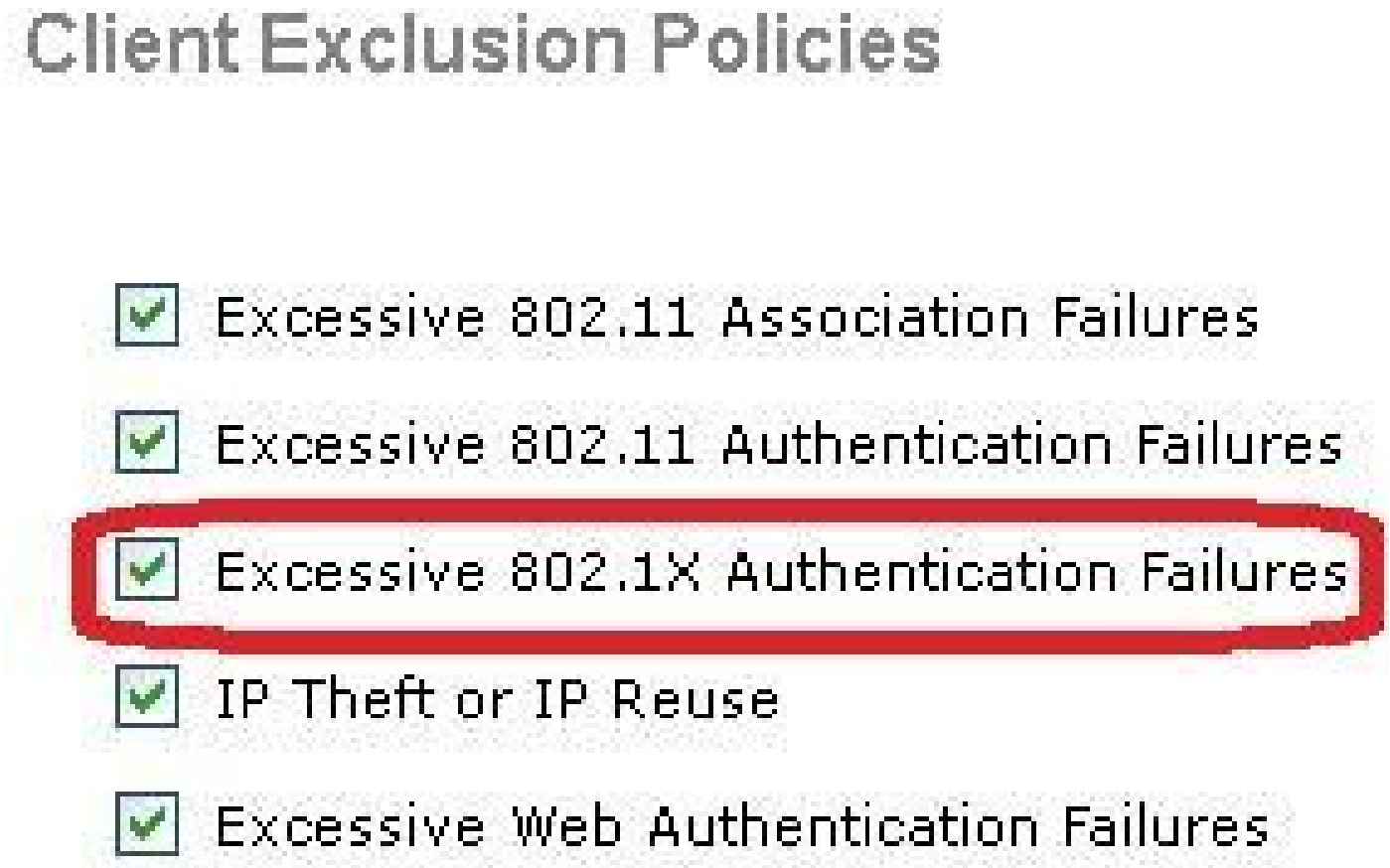
Voorbeelden van gebruiksmogelijkheden zijn:

- Een EAP-supplicant die is geconfigureerd met onjuiste referenties. De meeste smeekbedes, zoals EAP smeekbedes, houden authentificatiepogingen na een paar opeenvolgende mislukkingen op. Echter, sommige EAP supplicants blijven pogingen om opnieuw te authenticeren bij falen, mogelijk vele malen per seconde. Sommige clients overladen RADIUS-servers en veroorzaken een Denial of Service (DoS) voor het hele netwerk.
- Na een grote netwerkfailover kunnen honderden of duizenden EAP-clients tegelijkertijd proberen te verifiëren. Hierdoor kunnen de verificatieservers worden overbelast en kan een langzame respons worden gegeven. Als de clients of de authenticator time-out voordat de trage reactie wordt verwerkt, kan een vicieuze cyclus optreden waar de verificatiepogingen tot time-out worden voortgezet, en probeer dan de respons opnieuw te verwerken.

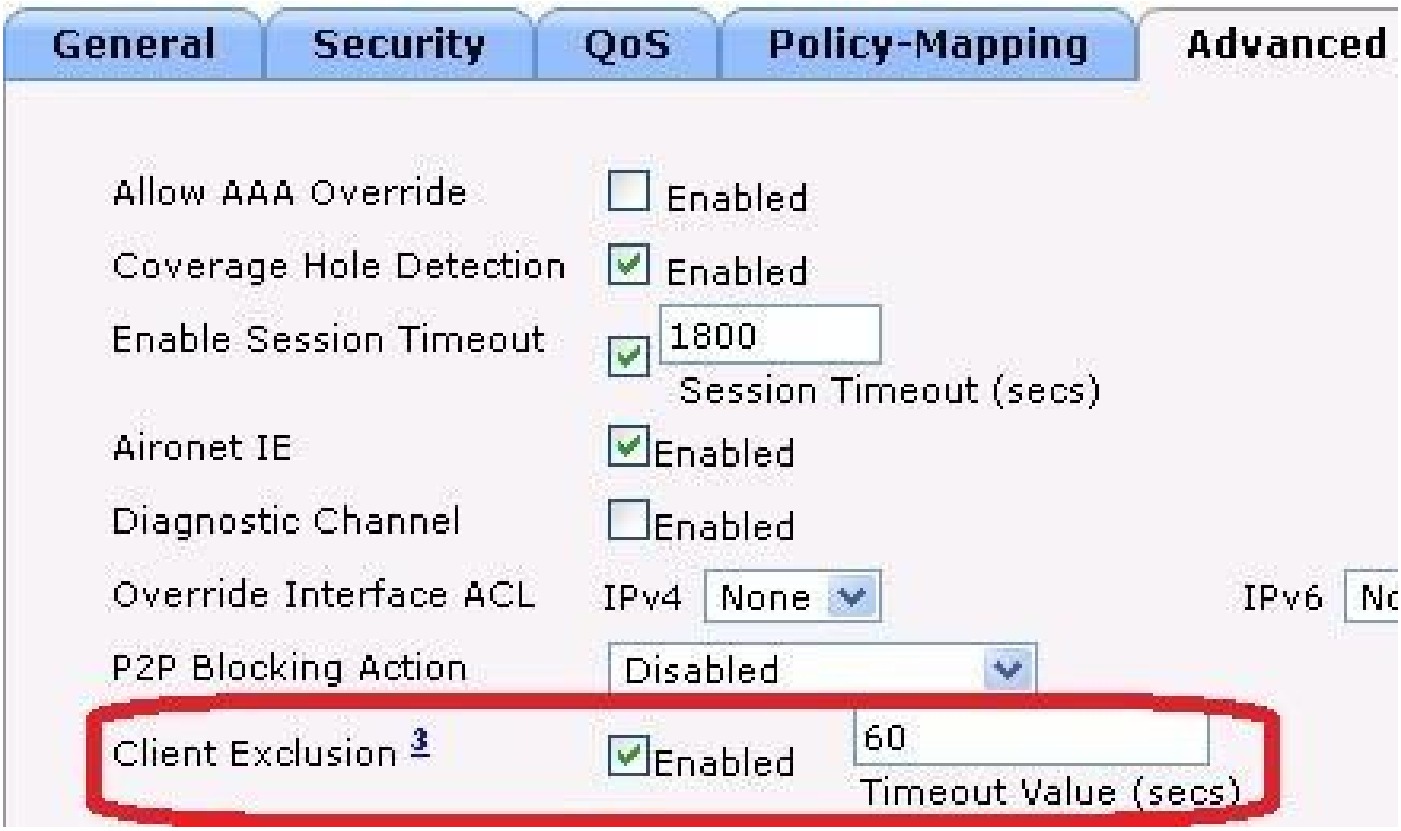
Opmerking: een toegangscontrolemechanisme is vereist om authenticatiepogingen te laten slagen.

Hoe werkt 802.1X Client Exclusion?

802.1X Client Exclusion voorkomt dat clients verificatiepogingen kunnen verzenden voor een bepaalde tijd na buitensporige 802.1X-verificatiefouten. Op een AireOS WLC 802.1X, client-uitsluiting wordt wereldwijd mogelijk gemaakt door te navigeren naar Security > Wireless Protection Policies > Client Exclusion Policies by default en kan worden gezien in deze afbeelding.



Clientuitsluiting kan per WLAN worden in- of uitgeschakeld. Standaard is deze ingeschakeld met een time-out van 60 seconden vóór AireOS 8.5 en 180 seconden vanaf AireOS 8.5.



Uitsluitingsinstellingen om RADIUS-servers te beschermen tegen overbelasting

Controleer of deze instellingen zijn ingeschakeld om te controleren of de RADIUS-server is beveiligd tegen overbelasting door onjuist functionerende draadloze clients:

- Excessieve 802.1X-verificatiefouten worden geselecteerd in het WLC global client exclusion policies.
- Clientuitsluiting is ingesteld op Ingeschakeld in de geavanceerde WLAN-instellingen.
- Time-outwaarde voor uitsluiting client is ingesteld op 60 tot 300 seconden.

> Opmerking: waarden hoger dan 300 seconden bieden een betere bescherming maar kunnen klachten van gebruikers veroorzaken.

- AireOS EAP-timers en ISE Protected Extensible Verification Protocol (PEAP)-instellingen configureren

Problemen die verhinderen dat 802.1X wordt uitgesloten van het werken

Verschillende configuratie-instellingen, in de WLC en in de RADIUS-server, kunnen voorkomen dat 802.1X Client Exclusion werkt.

Clients niet uitgesloten vanwege WLC EAP Timer-instellingen

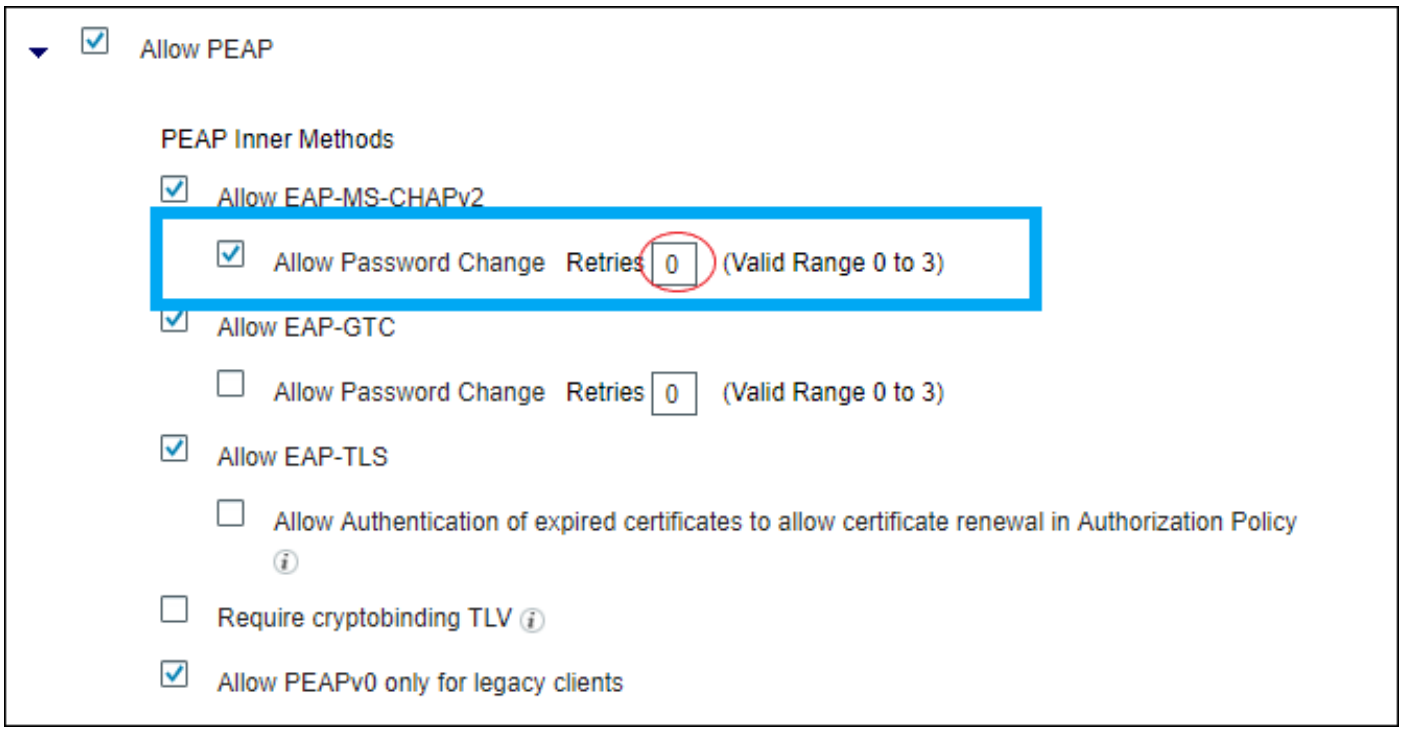
Draadloze clients zijn standaard niet uitgesloten wanneer Client Exclusion is ingesteld op Enabled op het WLAN. Dit is te wijten aan lange standaard EAP onderbrekingen van 30 seconden die ervoor zorgen dat een client die zich misdraagt nooit genoeg opeenvolgende mislukkingen te raken om een uitsluiting te veroorzaken. Configureer kortere EAP-onderbrekingen met een verhoogd aantal hertransmissies zodat de uitsluiting van de 802.1X-client van kracht kan worden. Zie het timeout voorbeeld.

```
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 niet uitgesloten vanwege ISE-PEAP-instellingen

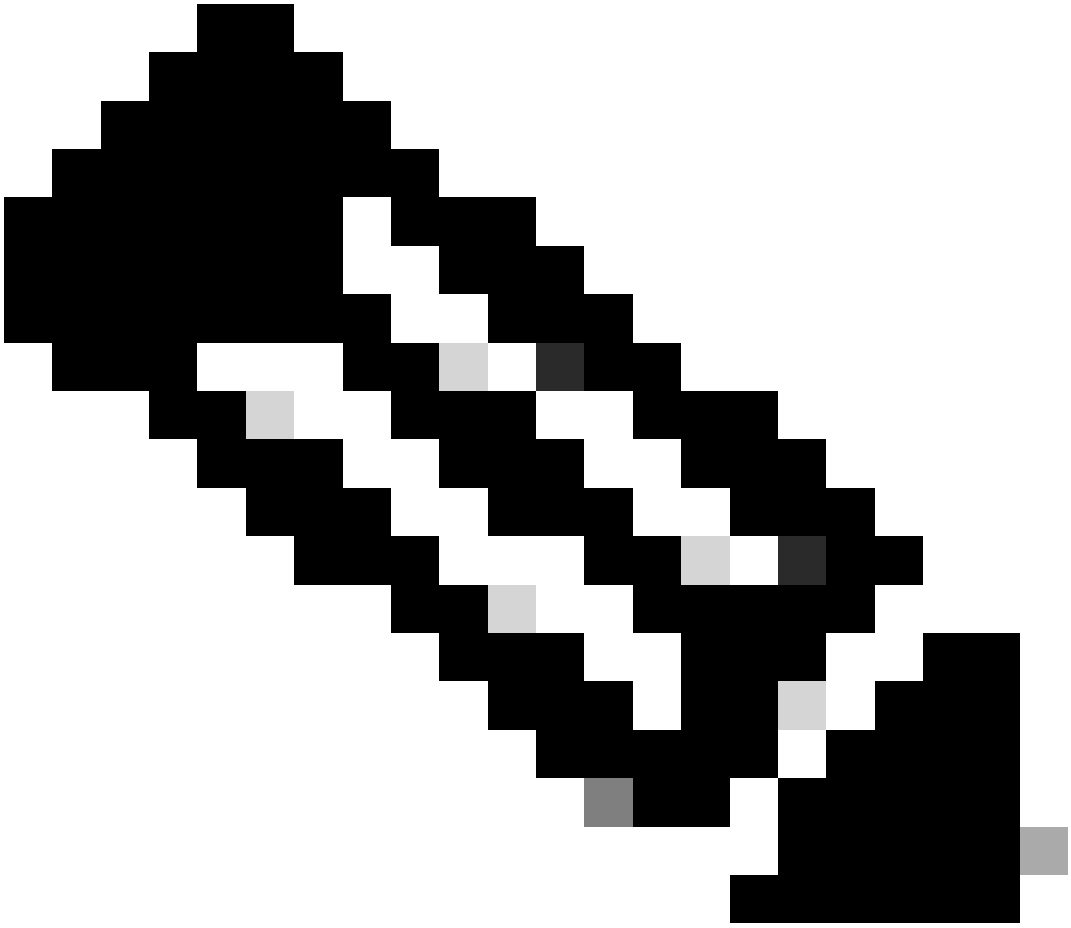
Om 802.1X Client Exclusion te kunnen laten werken, moet de RADIUS-server een Access-Reject

verzenden wanneer de verificatie mislukt. Als de RADIUS-server ISE is en PEAP wordt gebruikt, kan uitsluiting niet plaatsvinden en is dit afhankelijk van de ISE PEAP-instellingen. Ga binnen ISE naar Policy > Results > Verificatie > Toegestane protocollen > Default Network Access zoals in de afbeelding.



Als u Retries (rood omcirkeld op de rechterkant) op 0 instelt, dan moet ISE Access-Reject onmiddellijk naar de WLC sturen, die de WLC moet inschakelen om de client uit te sluiten (als het drie keer probeert om te authenticeren).

Opmerking: de instelling van Retries enigszins onafhankelijk van het aanvinkvakje Wachtwoordwijziging toestaan, dat wil zeggen, de waarde Retries kan worden gehonoreerd, zelfs als Wachtwoordwijziging toestaan niet is aangevinkt. Als deze optie echter op 0 wordt ingesteld, kunt u Wachtwoordwijziging niet toestaan.



Opmerking: bekijk voor meer informatie Cisco Bug ID CSC16858. Alleen geregistreerde Cisco-gebruikers kunnen toegang krijgen tot tools en informatie over Cisco-bugs.

Gerelateerde informatie

- Grootschalige draadloze RADIUS-netwerkmodules voorkomen
- Cisco Technical Support en downloads

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.