Verifica dell'esclusione del client 802.1X su un WLC AireOS

Sommario

[Introduzione](#)

[Prerequisiti](#)

- [Requisiti](#)
- [Componenti usati](#)

[Premesse](#)

[Casi utente](#)

[Come funziona l'esclusione dei client 802.1X?](#)

[Impostazioni di esclusione per proteggere i server RADIUS dal sovraccarico](#)

[Problemi che impediscono il funzionamento dell'esclusione 802.1X](#)

- [Client non esclusi a causa delle impostazioni del timer EAP WLC](#)
- [Client non esclusi a causa delle impostazioni ISE PEAP](#)

[Informazioni correlate](#)

Introduzione

Questo documento descrive l'esclusione del client 802.1X su un controller WLC (AireOS Wireless LAN Controller).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

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

Componenti usati

Le informazioni fornite in questo documento si basano su AireOS.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

L'esclusione di client 802.1X è un'opzione importante da includere in un autenticatore 802.1X come un WLC. In questo modo è possibile evitare un sovraccarico dell'infrastruttura del server di autenticazione da parte dei client EAP (Extensible Authentication Protocol) iperattivi o che non funzionano correttamente.

Casi utente

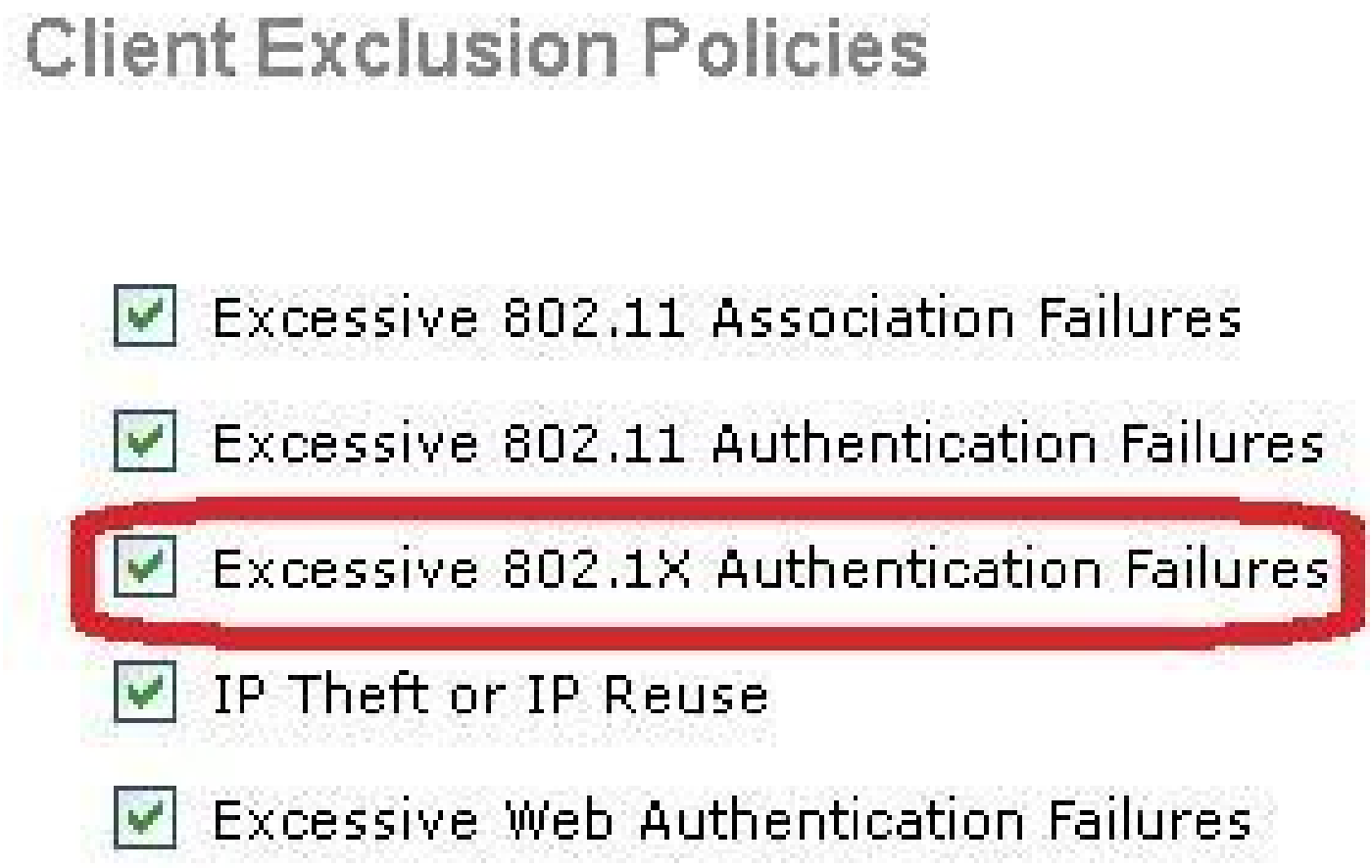
Esempi di casi di utilizzo includono:

- Supplicant EAP configurato con credenziali non corrette. La maggior parte dei supplicant, ad esempio i supplicant EAP, interrompe i tentativi di autenticazione dopo alcuni errori successivi. Tuttavia, alcuni supplicant EAP continuano i tentativi di riautenticazione in caso di errore, probabilmente molte volte al secondo. Alcuni client sovraccaricano i server RADIUS e causano un DoS (Denial of Service) per l'intera rete.
- Dopo un failover di rete di grandi dimensioni, centinaia o migliaia di client EAP possono tentare di eseguire l'autenticazione contemporaneamente. Di conseguenza, i server di autenticazione possono essere sovraccarichi e fornire una risposta lenta. Se si verifica il timeout dei client o dell'autenticatore prima dell'elaborazione della risposta lenta, potrebbe verificarsi un ciclo vizioso in cui i tentativi di autenticazione continuano a scadere e quindi si tenta di elaborare di nuovo la risposta.

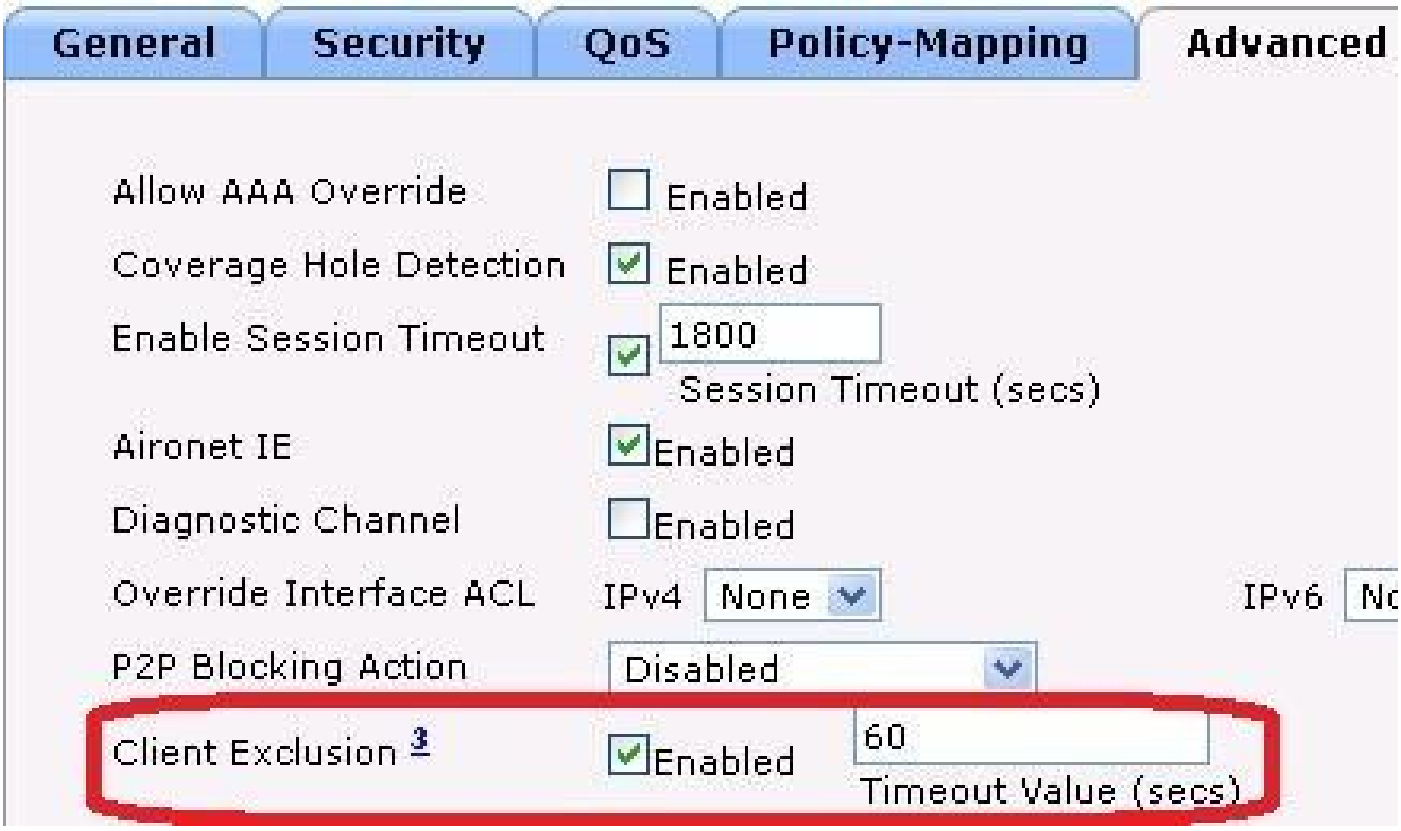
Nota: per consentire la riuscita dei tentativi di autenticazione, è necessario un meccanismo di controllo dell'ammissione.

Come funziona l'esclusione dei client 802.1X?

L'esclusione dei client 802.1X impedisce ai client di inviare tentativi di autenticazione per un periodo di tempo dopo un numero eccessivo di errori di autenticazione 802.1X. Su un WLC AireOS 802.1X, l'esclusione dei client è abilitata a livello globale passando a Security > Wireless Protection Policies > Client Exclusion Policies (Policy di esclusione client) per impostazione predefinita, e può essere visualizzata in questa immagine.



L'esclusione dei client può essere abilitata o disabilitata per singola WLAN. Per impostazione predefinita, è abilitato con un timeout di 60 secondi prima che AireOS 8.5 e di 180 secondi a partire da AireOS 8.5.



Impostazioni di esclusione per proteggere i server RADIUS dal sovraccarico

Per verificare che il server RADIUS sia protetto dal sovraccarico a causa di client wireless che non funzionano correttamente, verificare che queste impostazioni siano attive:

- Errori di autenticazione 802.1X eccessivi selezionati nei criteri di esclusione client globali WLC.
- Nelle impostazioni avanzate della WLAN, l'esclusione del client è abilitata.
- Il valore di timeout di esclusione client è impostato su un valore compreso tra 60 e 300 secondi.

> Nota: i valori superiori a 300 secondi forniscono una migliore protezione ma possono provocare reclami da parte degli utenti.

- Configurazione dei timer EAP AireOS e delle impostazioni PEAP (ISE Protected Extensible Authentication Protocol)

Problemi che impediscono il funzionamento dell'esclusione 802.1X

Numerose impostazioni di configurazione, nel WLC e nel server RADIUS possono impedire il funzionamento dell'esclusione client 802.1X.

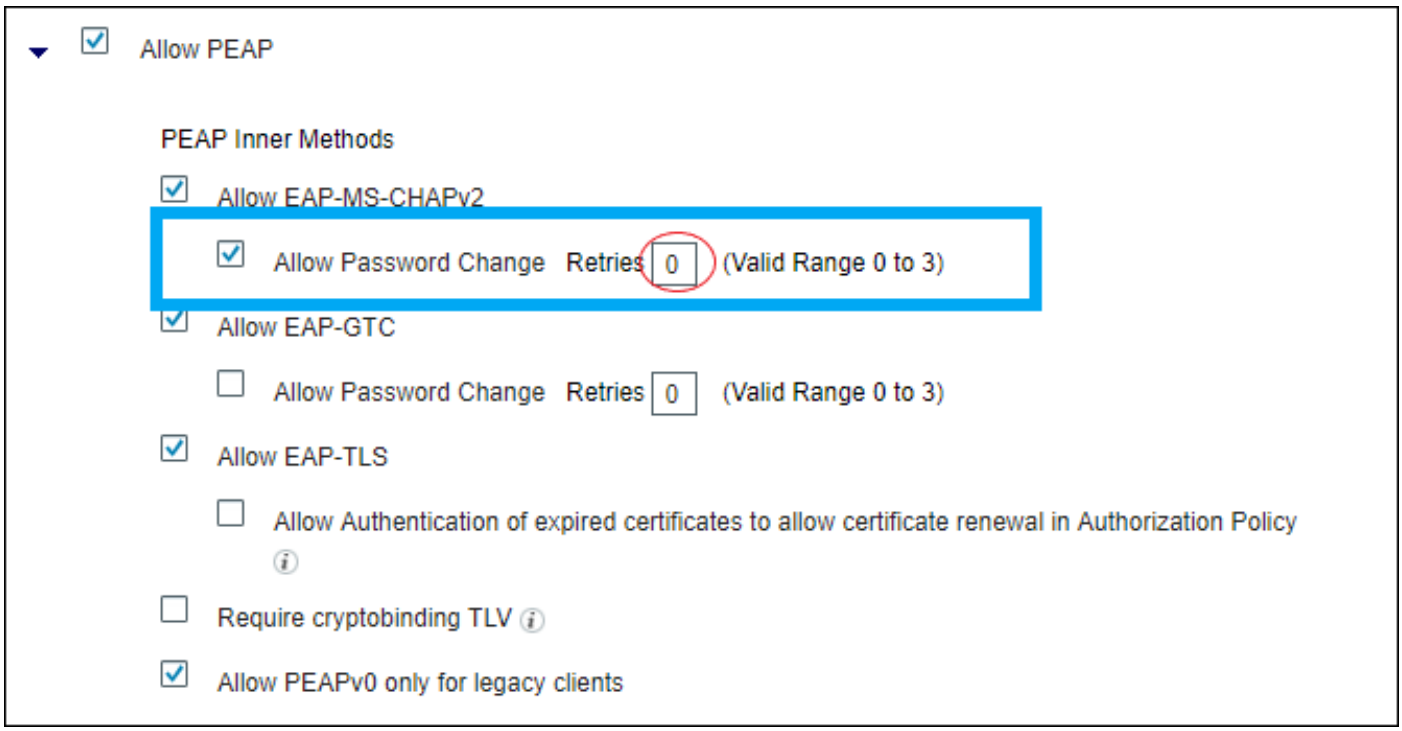
Client non esclusi a causa delle impostazioni del timer EAP WLC

per impostazione predefinita, i client wireless non vengono esclusi quando l'opzione Esclusione client è impostata su Attivata sulla rete WLAN. Ciò è dovuto ai lunghi timeout EAP predefiniti di 30 secondi che fanno in modo che un client che si comporta in modo errato non raggiunga mai il numero di errori successivi sufficiente per attivare un'esclusione. Configurare timeout EAP più brevi con un numero maggiore di ritrasmissioni per rendere effettiva l'esclusione del client 802.1X. Vedere l'esempio di timeout.

```
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
```

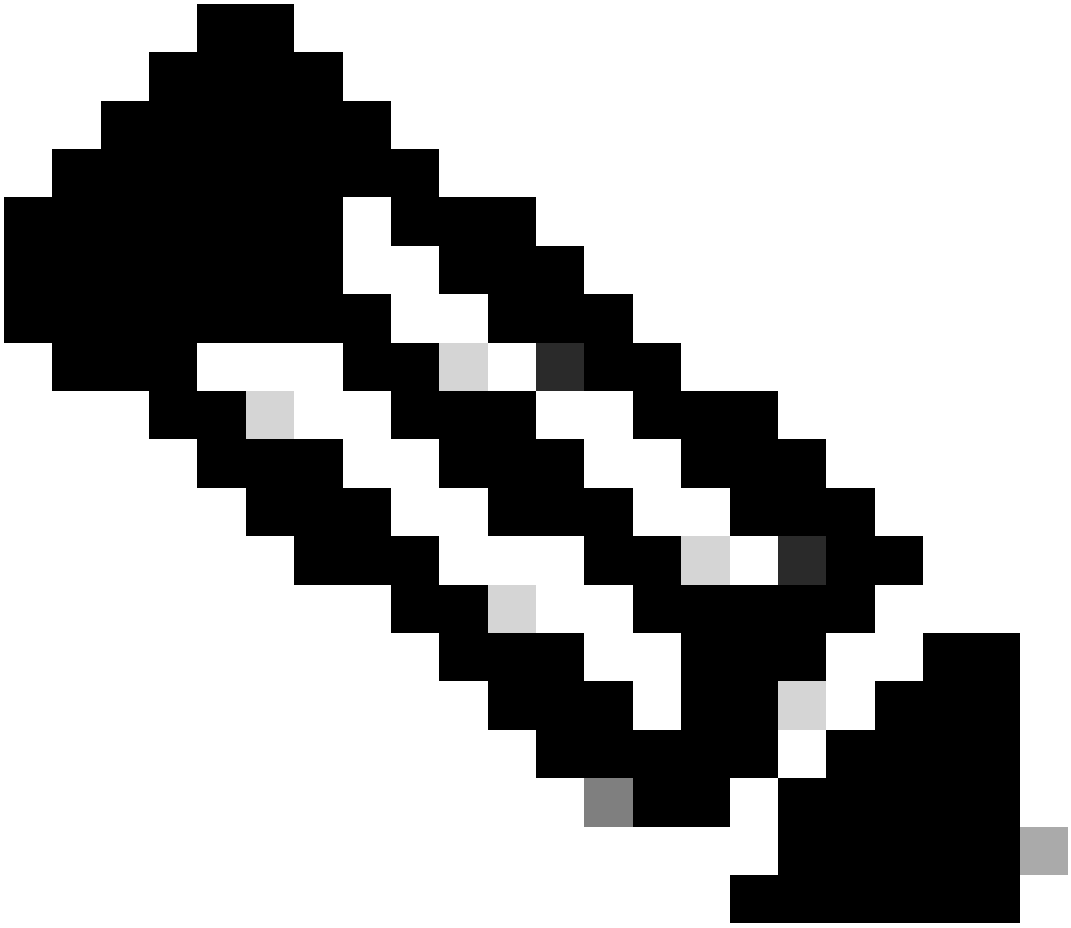
Client non esclusi a causa delle impostazioni ISE PEAP

Affinché l'esclusione del client 802.1X funzioni correttamente, il server RADIUS deve inviare un messaggio di rifiuto di accesso quando l'autenticazione non riesce. Se il server RADIUS è ISE e se PEAP è in uso, l'esclusione non può verificarsi e dipende dalle impostazioni ISE PEAP. All'interno di ISE, selezionare Policy > Results > Authentication > Allowed Protocols (Policy > Risultati > Autenticazione > Protocolli consentiti) > Default Network Access (Accesso di rete predefinito), come mostrato nell'immagine.



Se si imposta Retries (cerchiato in rosso a destra) su 0, ISE deve inviare immediatamente Access-Reject al WLC, che deve abilitare il WLC per escludere il client (se tenta tre volte di autenticarsi).

Nota: l'impostazione di Tentativi in qualche modo indipendente dalla casella di controllo Consenti modifica password, ovvero il valore Tentativi può essere rispettato, anche se Consenti modifica password è deselezionato. Tuttavia, se Retries (Tentativi) è impostato su 0, Allow Password Change (Consenti modifica password) non funziona.



Nota: per ulteriori informazioni, consultare l'ID bug Cisco CSCsq16858. Solo gli utenti Cisco registrati possono accedere agli strumenti e alle informazioni sui bug di Cisco.

Informazioni correlate

- Impedire il crollo di una rete RADIUS wireless su larga scala
- Supporto tecnico Cisco e download

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).