驗證AireOS WLC上的802.1X客戶端排除

目錄

簡介

本檔案將說明AireOS無線LAN控制器(WLC)上的802.1X使用者端排除。

必要條件

需求

思科建議您瞭解以下主題：

- Cisco AireOS WLC
- 802.1X通訊協定
- 遠端驗證撥入使用者服務(RADIUS)
- 身分識別服務引擎 (ISE)

採用元件

本文檔中的資訊基於AireOS。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

802.1X客戶端排除是802.1X身份驗證器（如WLC）上必須具備的重要選項。這是為了防止可延伸驗證通訊協定(EAP)使用者端過度使用或功能不當造成驗證伺服器基礎架構超載。

使用者案例

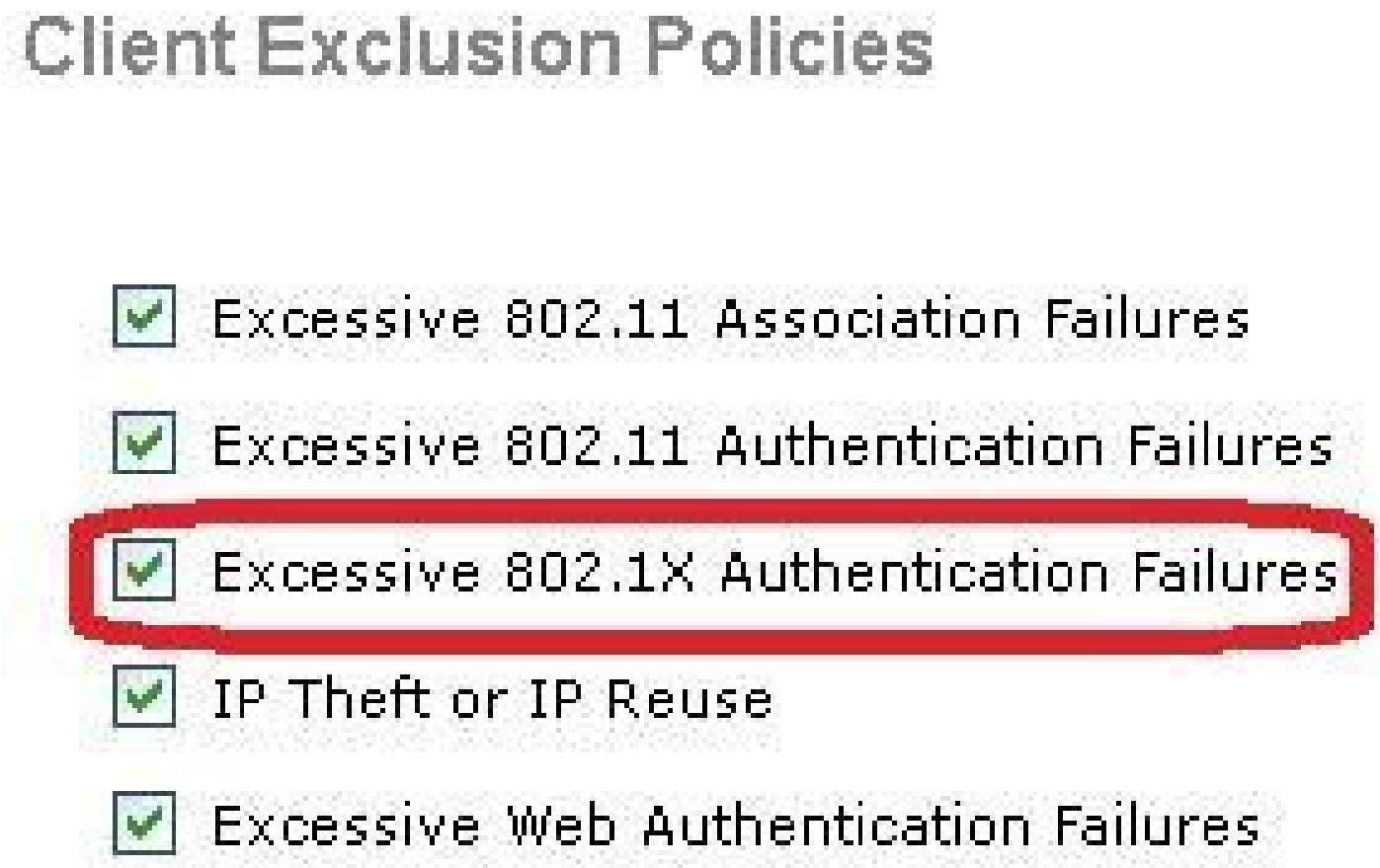
示例使用情形包括：

- 使用不正確的憑證配置的EAP請求方。大多數請求方（例如EAP請求方）在連續幾次失敗後停止身份驗證嘗試。但是，有些EAP請求方在失敗時仍會嘗試重新進行身份驗證，可能每秒多次進行。某些使用者端造成RADIUS伺服器超載，並造成整個網路的拒絕服務(DoS)。
- 在主要網路容錯移轉之後，數以百計或數以千計的EAP使用者端可以同時嘗試進行驗證。因此，身份驗證伺服器可能過載並且響應緩慢。如果客戶端或身份驗證器在處理緩慢響應之前超時，則會出現惡性循環，其中身份驗證嘗試繼續超時，然後再次嘗試處理響應。

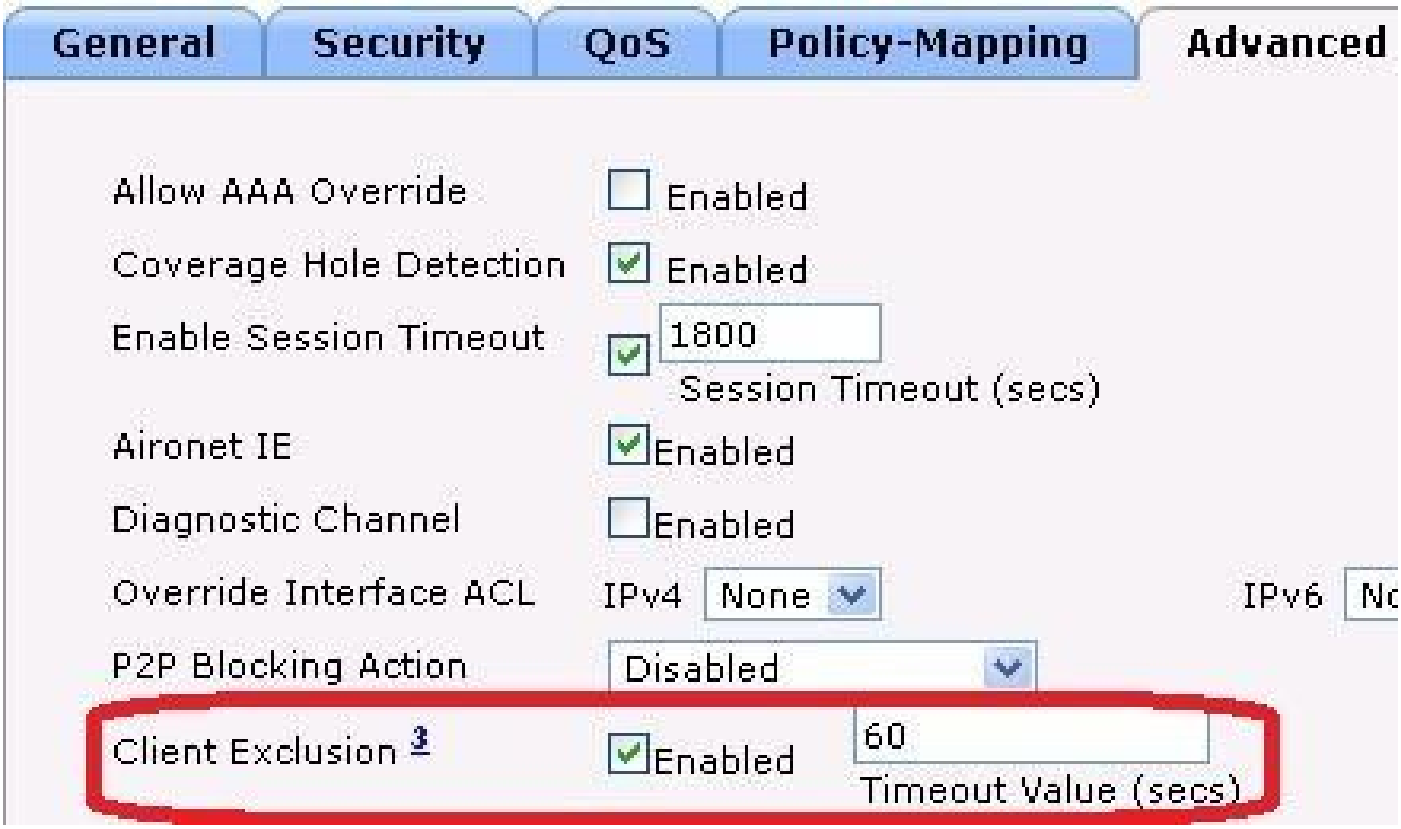
注意：需要准入控制機制以允許身份驗證嘗試成功。

802.1X客戶端排除如何工作？

802.1X使用者端排除可防止使用者端在802.1X驗證失敗次數過多之後傳送驗證嘗試。在AireOS WLC 802.1X上，客戶端排除功能透過導航到安全 > 無線保護策略 > 客戶端排除策略全局啟用，如下圖所示。



可以針對每個WLAN啟用或停用客戶端排除。預設情況下，該模式在AireOS 8.5之前為60秒，在AireOS 8.5中開始為180秒。



用於保護RADIUS伺服器免於過載的排除設定

要驗證RADIUS伺服器是否因無線客戶端不正確工作而超載，請驗證以下設定是否有效：

- Excessive 802.1X Authentication Failures。
- Client Exclusion在WLAN advanced settings中設定為Enabled。
- Client Exclusion Timeout Value設定為60到300秒。

> 注意：高於300秒的值可提供更好的保護，但可能會觸發使用者投訴。

- 配置AireOS EAP計時器和ISE保護的可擴展身份驗證協定(PEAP)設定

導致802.1X排除無法運作的問題

在WLC和RADIUS伺服器中的若干配置設定可能會使802.1X客戶端排除無法正常工作。

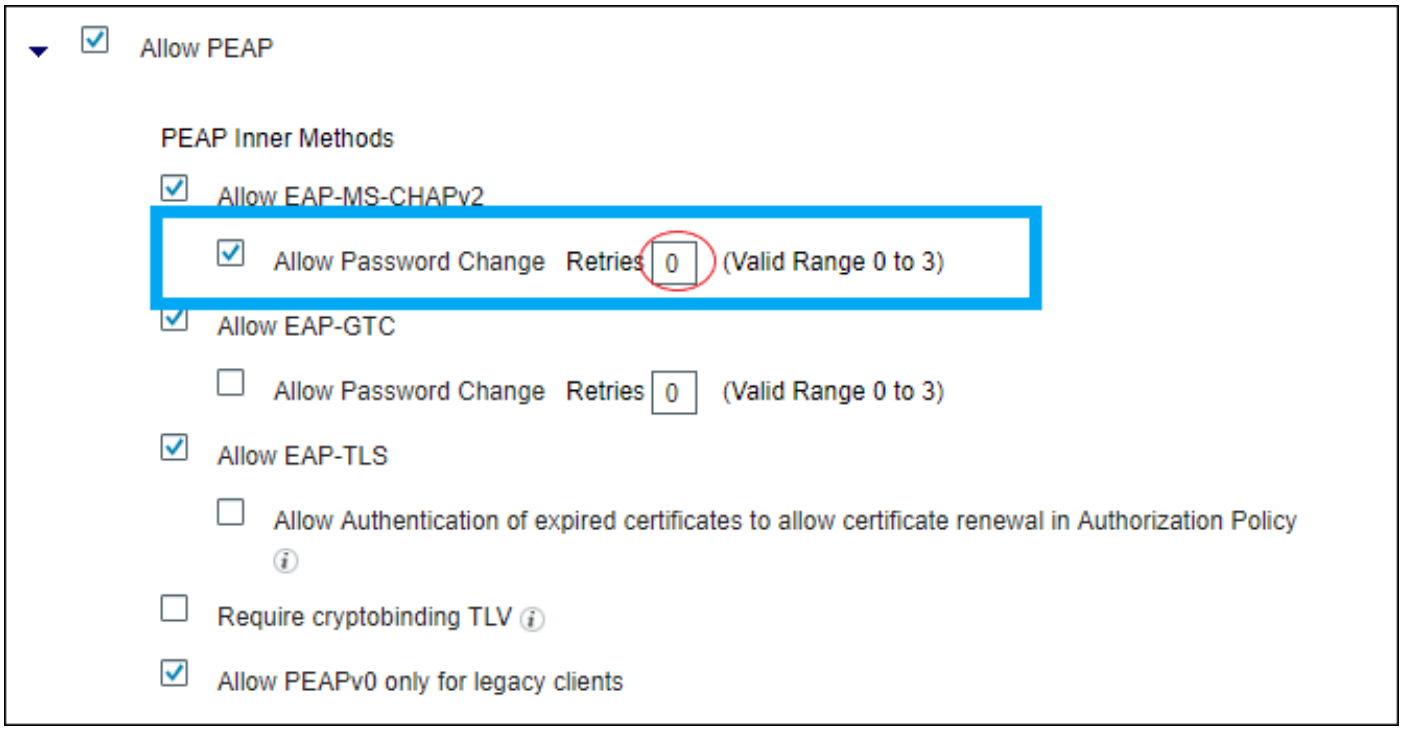
由於WLC EAP計時器設定未排除的客戶端

預設情況下，在WLAN上Client Exclusion設定為Enabled時，不會排除無線客戶端。這是因為預設EAP超時時間較長，為30秒，這會導致客戶端行為不當時永遠不會遇到足夠的連續故障來觸發排除。設定較短的EAP逾時，並增加重新傳輸次數，讓「802.1X使用者端排除」生效。請參閱逾時範例。

```
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
```

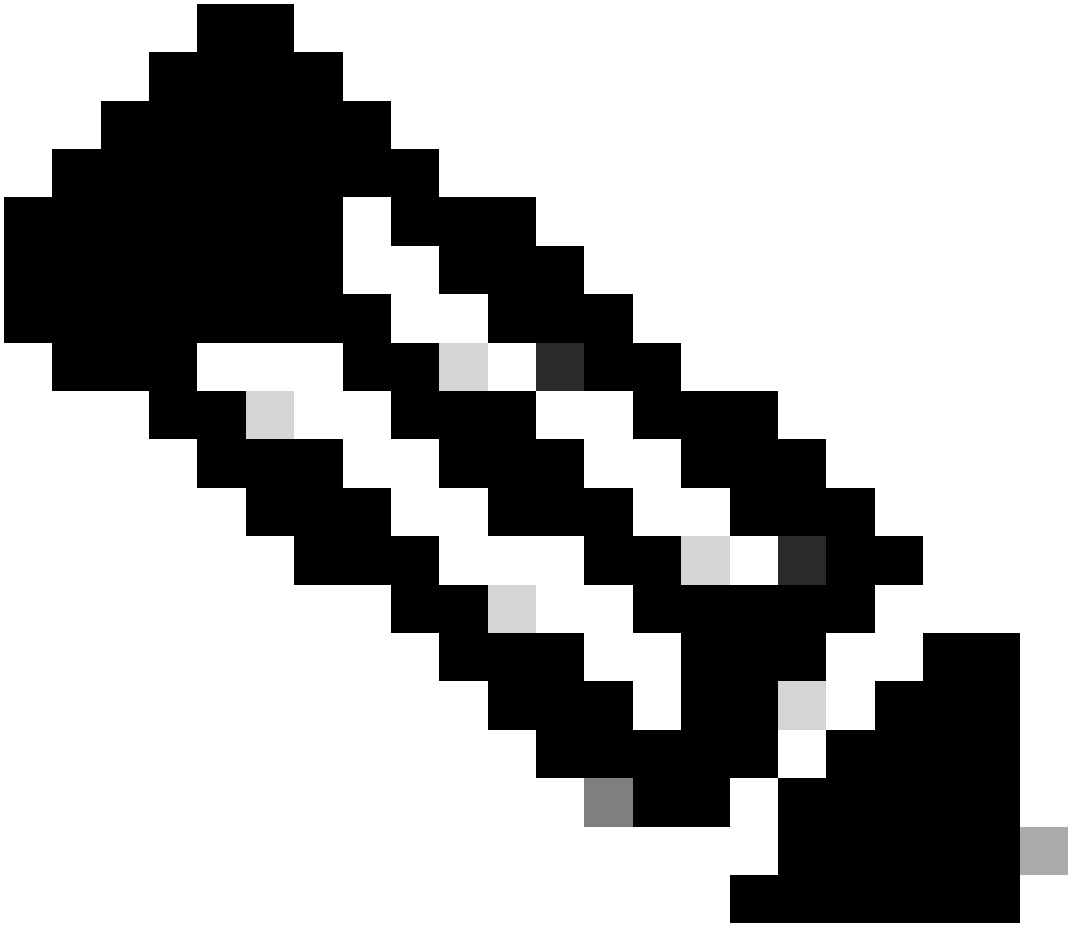
由於ISE PEAP設定未排除的客戶端

為使802.1X客戶端排除正常運行，身份驗證失敗時，RADIUS伺服器必須傳送Access-Reject。如果RADIUS伺服器是ISE並且正在使用PEAP，則無法進行排除，這取決於ISE PEAP設定。在ISE中，導航到策略>結果 > 身份驗證 > 允許的協定 > 預設網路訪問，如圖所示。



如果將Retries（在右邊紅色圓圈）設定為0，則ISE必須立即向WLC傳送Access-Reject，而後者必須啟用WLC以排除客戶端（如果它嘗試三次進行身份驗證）。

注意：Retries 的設定與Allow Password Change覈取方塊有些獨立，也就是說，即使取消選中Allow Password Change，也可以接受Retries 值。但是，如果Retries 設定為0，則Allow Password Change不起作用。



注意：有關詳細資訊，請參閱思科漏洞ID CSCsq16858。只有已註冊的思科使用者可以存取思科錯誤工具和資訊。

相關資訊

- 防止大規模無線RADIUS網路崩潰
- 思科技術支援與下載

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。