# 验证AireOS WLC上的802.1X客户端排除

## 目录


简介

先决条件

- 要求
- 使用的组件

背景信息

用户案例

802.1X客户端排除如何工作？

用于保护RADIUS服务器免于过载的排除设置

阻止802.1X排除正常运行的问题

- 由于WLC EAP计时器设置，未排除客户端
- 由于ISE PEAP设置而未排除的客户端

相关信息


## 简介

本文档介绍AireOS无线局域网控制器(WLC)上的802.1X客户端排除。

## 先决条件

### 要求

Cisco 建议您了解以下主题：

- 思科AireOS WLC
- 802.1X协议
- 远程用户拨入认证系统(RADIUS)
- 身份服务引擎(ISE)

### 使用的组件

本文档中的信息基于AireOS。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

## 背景信息

802.1X Client Exclusion是802.1X身份验证器（例如WLC）的重要选项。这是为了防止超级活动或功能不当的可扩展身份验证协议(EAP)客户端造成身份验证服务器基础设施过载。

## 用户案例

示例使用案例包括：

- 配置了错误凭证的EAP请求方。大多数Supplicant客户端（例如EAP客户端）在连续几次失败后停止身份验证尝试。但是，有些EAP请求方在失败时仍会继续尝试重新进行身份验证，可能每秒多次进行。某些客户端会使RADIUS服务器过载并导致整个网络的拒绝服务(DoS)。
- 在发生主要网络故障转移后，成百上千个EAP客户端可以同时尝试进行身份验证。因此，身份验证服务器可能过载并且响应缓慢。如果客户端或身份验证器在处理缓慢响应之前超时，则会出现恶性循环，其中身份验证尝试继续超时，然后再次尝试处理响应。

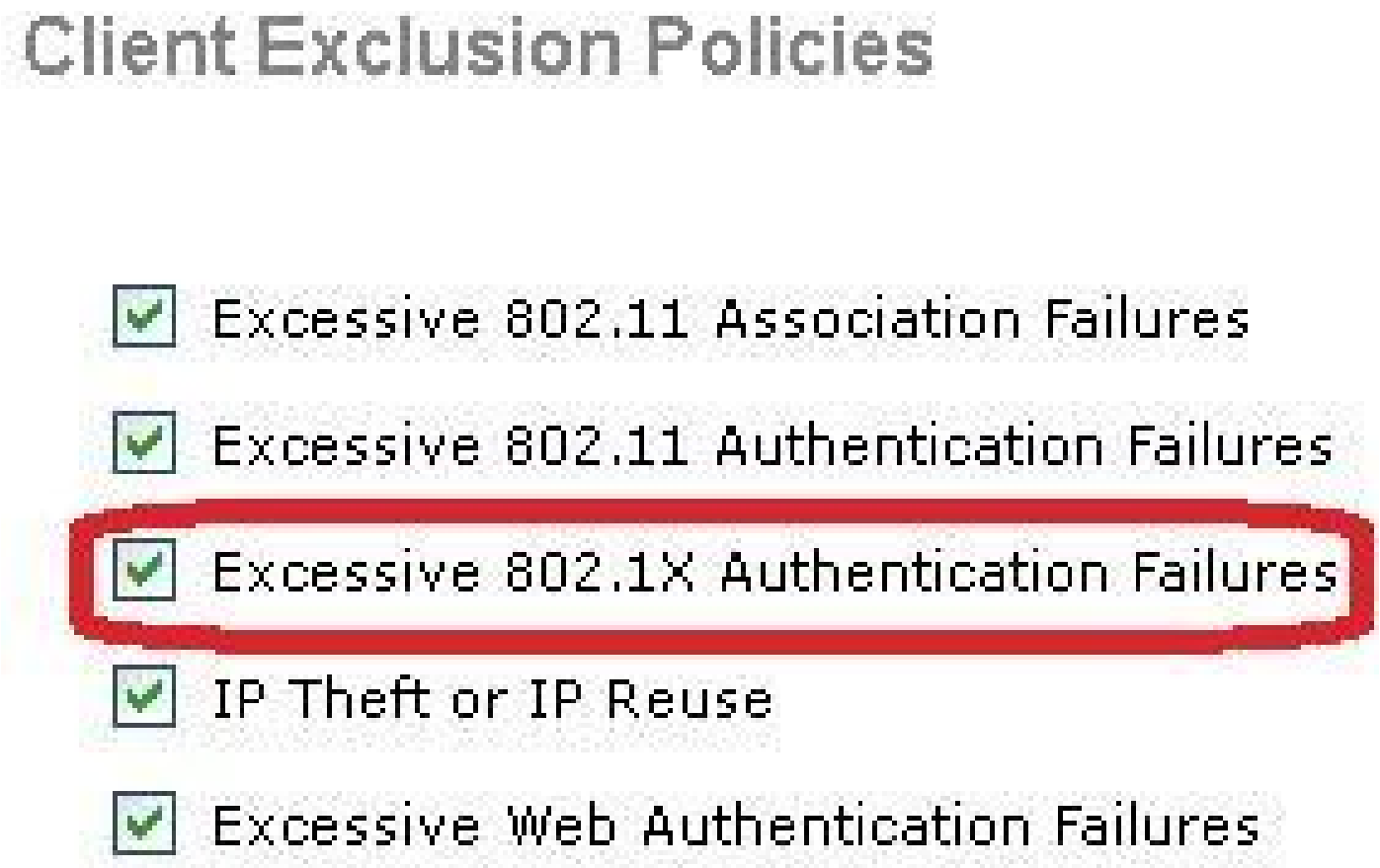
---

注意：为使身份验证尝试成功，需要准入控制机制。

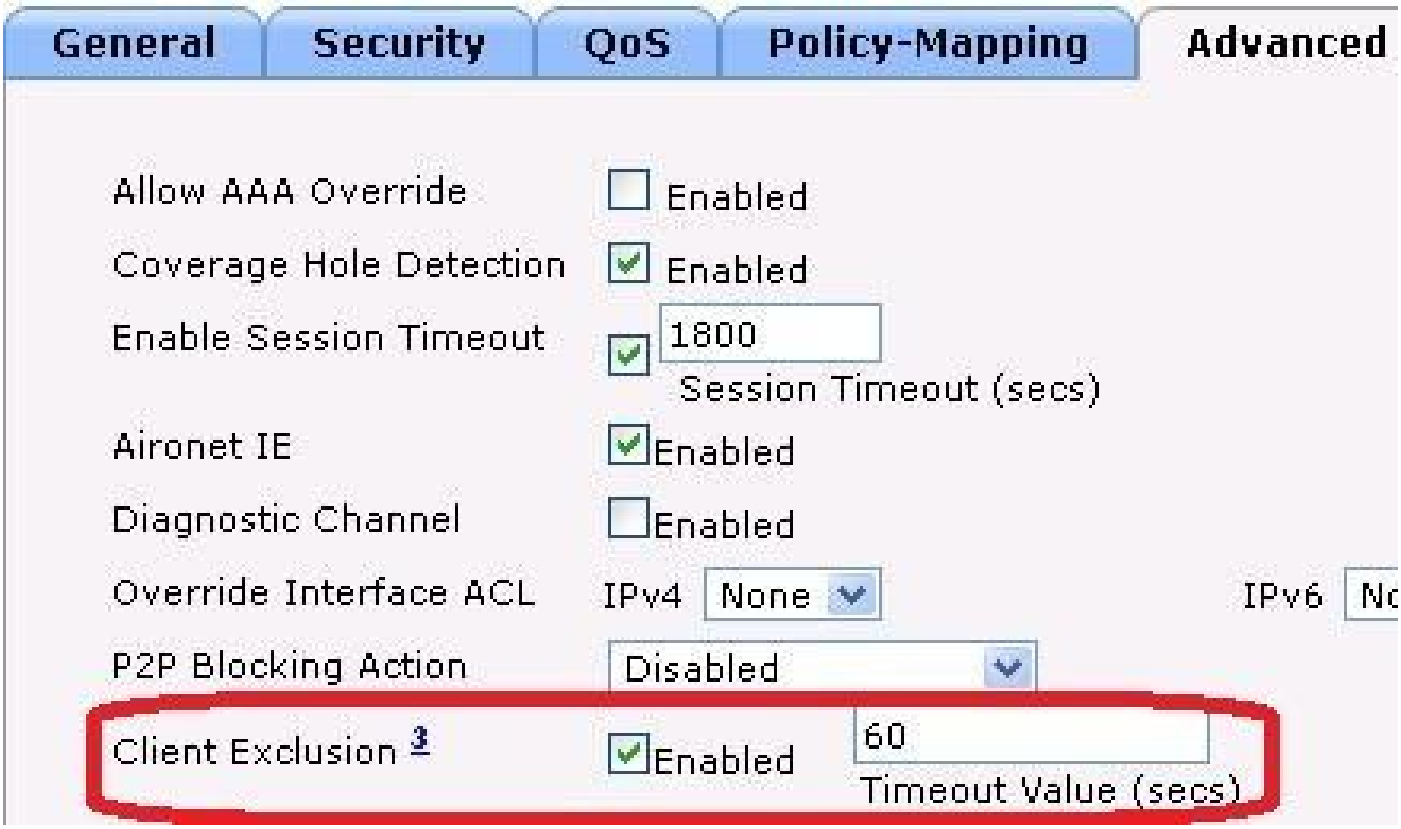
---

## 802.1X客户端排除如何工作？

802.1X客户端排除在802.1X身份验证失败次数过多之后的一段时间内阻止客户端发送身份验证尝试。在AireOS WLC 802.1X上，默认情况下通过导航到Security > Wireless Protection Policies > Client Exclusion Policies全局启用客户端排除，在此映像中可以看到。




可以针对每个WLAN启用或禁用客户端排除。默认情况下，在AireOS 8.5之前会启用超时60秒，在AireOS 8.5中会启用超时180秒。




## 用于保护RADIUS服务器免于过载的排除设置

要验证RADIUS服务器是否因无线客户端功能不正确而免于过载，请验证以下设置是否有效：

- Excessive 802.1X Authentication Failures。
- Client Exclusion在WLAN高级设置中设置为Enabled。
- Client Exclusion Timeout Value设置为60到300秒。

> 注意：高于300秒的值可提供更好的保护，但可能触发用户投诉。

- 配置AireOS EAP计时器和ISE受保护的可扩展身份验证协议(PEAP)设置

## 阻止802.1X排除正常运行的问题

WLC和RADIUS服务器中的多个配置设置可能会阻止802.1X客户端排除正常工作。

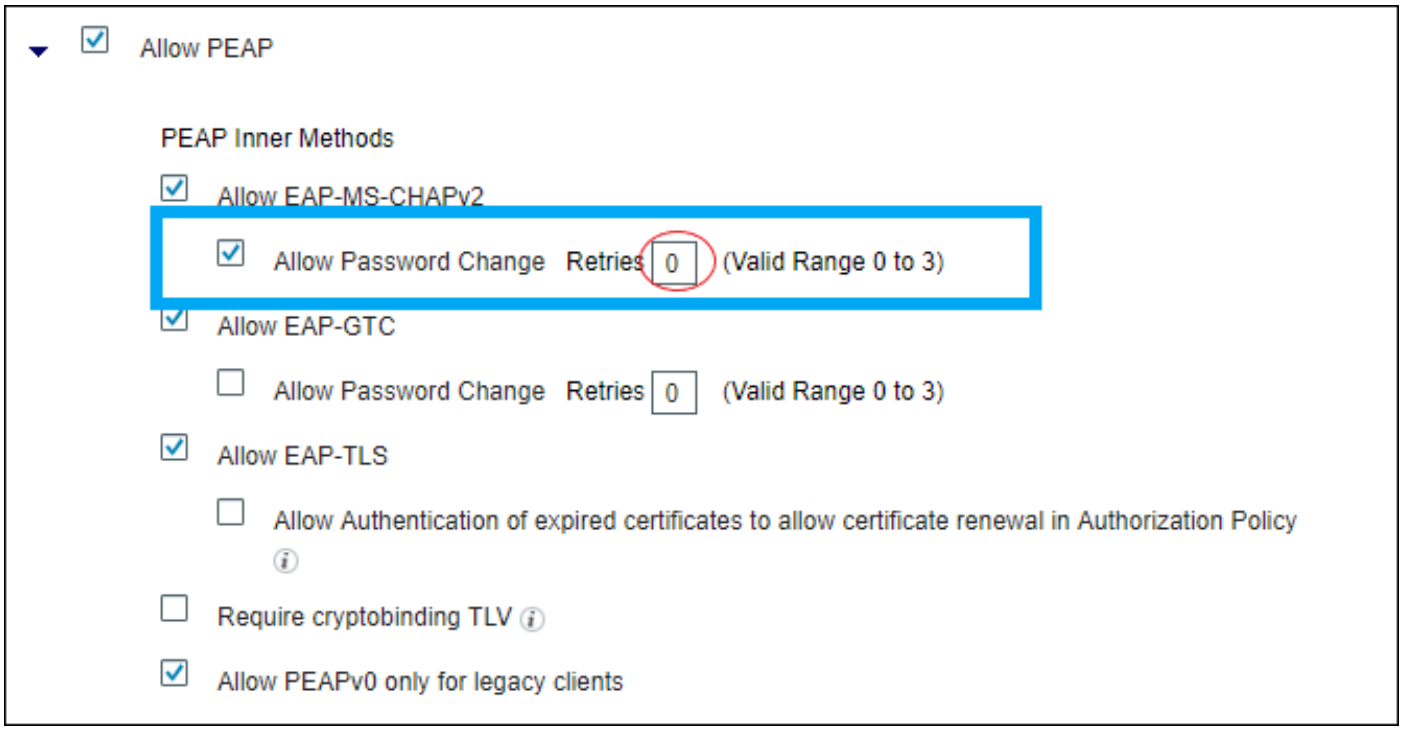
### 由于WLC EAP计时器设置，未排除客户端

默认情况下，在WLAN上将Client Exclusion设置为Enabled时，不会排除无线客户端。这是因为，默认的EAP超时较长，为30秒，导致客户端行为不当，永远达不到触发排除的连续失败次数。配置更短的EAP超时和更多的重新传输数量，以使802.1X客户端排除生效。请参阅超时示例。

```
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
```

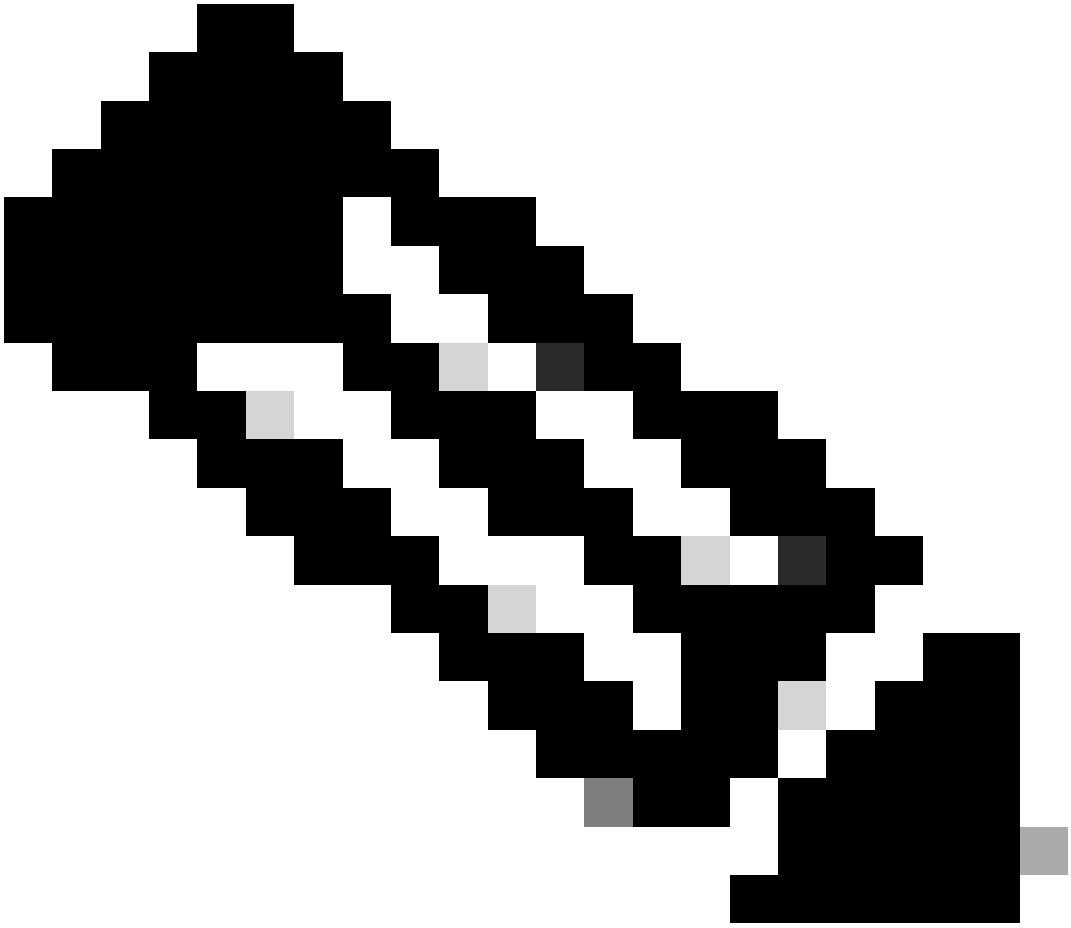
## 由于ISE PEAP设置而未排除的客户端

为使802.1X客户端排除正常运行，身份验证失败时，RADIUS服务器必须发送Access-Reject。如果RADIUS服务器为ISE且正在使用PEAP，则无法进行排除，具体取决于ISE PEAP设置。在ISE中，导航到策略>结果 > 身份验证 > 允许的协议 > 默认网络访问，如图所示。




如果将Retries（在右边用红色圈出）设置为0，则ISE必须立即向WLC发送Access-Reject，该WLC必须启用WLC以排除客户端（如果尝试三次进行身份验证）。

注意：Retries 的设置与Allow Password Change复选框有些无关，也就是说，即使取消选中Allow Password Change，仍可以接受Retries 值。但是，如果Retries 设置为0，则Allow Password Change不起作用。



注意：有关详细信息，请参阅思科漏洞ID CSCsq16858。只有注册的思科用户才能访问思科漏洞工具和信息。

## 相关信息

- 防止大规模无线RADIUS网络崩溃
- 思科技术支持和下载

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。