

使用热点门户指导用户禁用MAC地址随机化

目录

[简介](#)

[配置](#)

[设备特定说明](#)

[Android:](#)

[苹果:](#)

[Windows 窗口版本:](#)

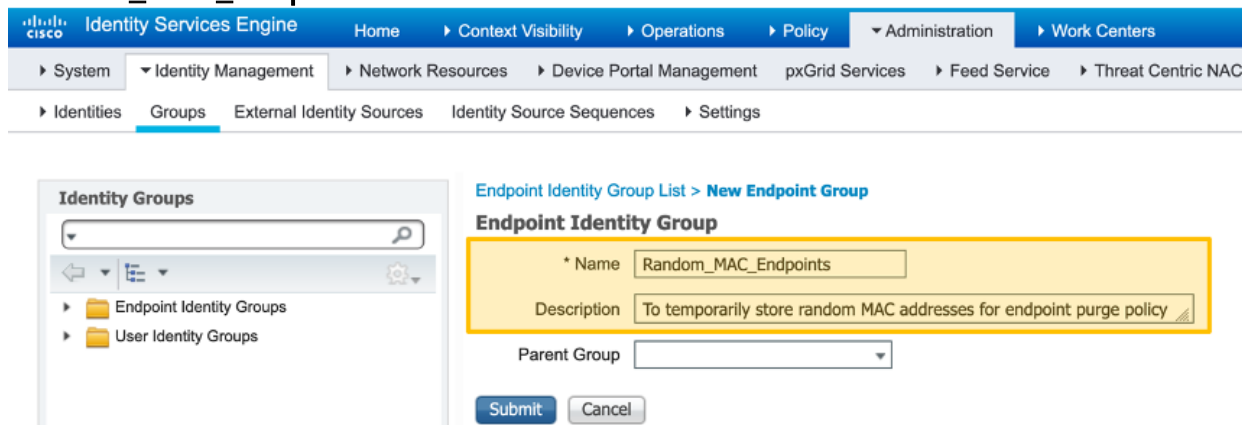
简介

随着Android 10和iOS 14的发布，引入了MAC地址随机化，以防止用户根据其无线MAC地址进行跟踪。这在加入热点网络时有利于隐私，但在企业环境中会使设备跟踪变得困难，特别是在尝试分析这些设备或使用移动设备管理器来确保设备在获得网络访问权限之前符合组织的安全策略时。

对于分析和MDM服务，可以指示最终用户在获得预期网络访问之前禁用设备上的MAC随机化。这可以通过将用户重定向到修改的热点页面来实现，该热点页面提供在设备使用随机MAC地址连接网络时禁用MAC随机化的指令。禁用MAC随机化后，用户可以正常连接。

配置

1. 导航至**管理>身份管理>组**，选择**终端身份组**，然后选择**添加**以创建名为**Random_MAC_Endpoints**



2. 导航至**工作中心>访客接入>门户和组件**，选择**访客门户**，然后选择**创建**以创建名为“Random MAC Detected”的新热点访客门户
3. 在“门户设置”下，为“终端身份组”选择上面创建的终端组
4. 选择门户页面自定义
5. 在“文本元素”下，将“横幅标题”更改为“检测到随机MAC”
6. 选择可接受使用策略
7. 将内容标题更改为：您的设备使用随机MAC地址
8. 在“说明文本”页中添加以下文本：请更改设备上的网络设置，以使用全局MAC地址而不是随机MAC地址来获取网络访问。此外，还可以提供有关在设备上全局禁用每个SSID的MAC随机化的详细说明。
9. 在AUP页面上添加以下可选内容以删除热点门户元素(确保在脚本中粘贴之前和之后选择

“切换HTML源”按钮):

10. 可以更改此页面上的其他设置，以提供有关如何修改设备上的MAC随机化设置的说明，完成后选择**Save**
11. 创建名为Random_MAC的**授权配置**文件，以重定向到上面创建的页面



12. 创建授权策略规则以使用**Random_MAC**，并将任何SSID的任何随机MAC地址上的匹配条件用于拒绝随机MAC地址。此处，正则表达式字符串匹配条件(**MATCHES ^.[26Aeae].***)用于标识随机MAC地址，该MAC地址利用Android和iOS设备都遵循的MAC地址的本地有效位



设备特定说明

以下步骤可指导用户完成某些常见设备。特定设备的供应商在其设备上禁用MAC随机化时可采取稍有不同的步骤。

Android:

1. 打开“**设置**”应用。
2. 选择**网络和Internet**。
3. 选择**WiFi**。
4. 确保您已连接到企业SSID。
5. 轻触当前WiFi连接旁边的齿轮图标。
6. 选择**Advanced**。
7. 选择“**隐私**”。
8. 选择**使用设备MAC**。

苹果：

苹果发布了一篇文章，说明在其设备上禁用MAC随机化：

<https://support.apple.com/en-us/HT211227>

Windows 窗口版本:

自撰写本文起，随机MAC地址在Windows上默认禁用，但用户可以选择将其打开，以下是有关禁用此功能（如果启用）的说明：

- 对所有网络禁用“使用随机硬件地址”：
- 对特定网络禁用“使用随机硬件地址”：