使用熱點門戶指導使用者禁用MAC地址隨機化

目錄

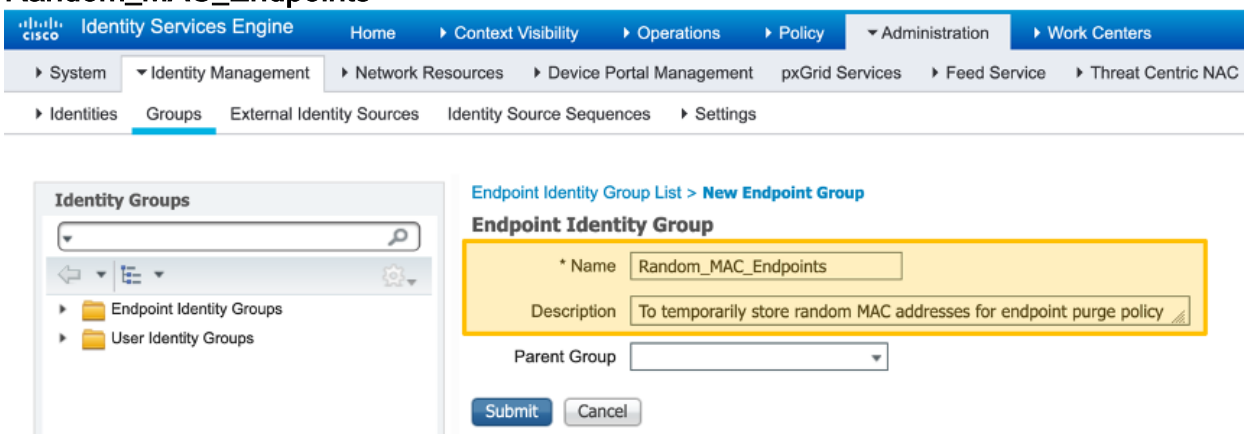
簡介

隨著Android 10和iOS 14的發佈，引入了MAC地址隨機化來嘗試防止使用者根據他們的無線MAC地址被跟蹤。在加入熱點網路時，這有利於保護隱私，但會使企業環境中的裝置跟蹤變得困難，特別是在嘗試分析這些裝置或使用流動裝置管理器以確保裝置在獲取網路訪問之前符合組織的安全策略時。

對於分析和MDM服務，可指示終端使用者在獲得預期的網路訪問之前禁用裝置上的MAC隨機化。這可以通過將使用者重定向到修改後的熱點頁面來實現，該熱點頁面提供在裝置使用隨機MAC地址連線到網路時禁用MAC隨機化的指令。禁用MAC隨機化後，使用者可以正常連線。

組態

1. 導航到**Administration > Identity Management > Groups**，選擇**Endpoint Identity Groups**，然後選擇**Add**以建立新的終端組，該組名為**Random_MAC_Endpoints**



2. 導航到**工作中心(Work Centers)>訪客接入(Guest Access)>門戶和元件(Portals & Components)**，選擇**訪客門戶**，然後選擇**建立(Create)**以建立新的熱點訪客門戶，名為**Random MAC Detected**
3. 在**Portal Settings**下，為**Endpoint identity**組選擇上面建立的**終端組**
4. 選擇**Portal Page Customization**
5. 在**Text Elements**下，將**Banner title**更改為**Random MAC detected**
6. 選擇**可接受使用策略**
7. 將**內容標題**更改為：**裝置正在使用隨機MAC地址**
8. 將以下文本新增到「**說明文本**」頁： **請更改裝置上的網路設定以使用全域性MAC地址而**

不是隨機MAC地址來獲取網路訪問。還可以提供有關在裝置上禁用每個SSID的MAC隨機化或全域性化的具體說明。

9. 在AUP頁上新增以下可選內容以刪除熱點門戶元素(確保在指令碼中貼上之前和之後選擇**Toggle HTML Source**按鈕):

10. 此頁面上的其他設定可以更改，以便提供如何修改裝置上的MAC隨機設定的說明，一旦完成選擇**儲存**
11. 建立名為**Random_MAC**的授權配置檔案，以重定向到上面建立的頁面

12. 建立授權策略規則，以使用**Random_MAC**，條件與任何SSID的任何隨機MAC地址相匹配，以拒絕隨機MAC地址。這裡，正規表示式字串匹配條件(**MATCHES ^.[26AEae].***)用於標識隨機MAC地址，該地址利用Android和iOS裝置都遵循的MAC地址的本地有效位

裝置特定說明

以下是一些常見裝置可以指導使用者完成的步驟。特定裝置的供應商可以在其裝置上禁用MAC隨機化的步驟略有不同。

Android:

1. 開啟**設定**應用。
2. 選擇**Network and Internet。**
3. 選擇**WiFi。**
4. 確保您已連線到公司SSID。
5. 輕按當前WIFI連線旁邊的齒輪圖示。
6. 選擇**Advanced。**
7. 選擇**Privacy。**
8. 選擇**使用裝置MAC。**

蘋果：

蘋果公司發表了一篇文章，介紹了如何在他們的裝置上禁用MAC隨機化：

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

Windows:

在撰寫本文時，Windows預設禁用隨機MAC地址，但使用者可以選擇將其開啟。以下是啟用此功能後禁用該功能的說明：

- 為所有網路禁用「使用隨機硬體地址」：
- 禁用特定網路的「使用隨機硬體地址」：