

Utilisation du portail Hotspot pour informer les utilisateurs sur la désactivation de la randomisation des adresses MAC

Contenu

[Introduction](#)

[Configuration](#)

[Instructions spécifiques au périphérique](#)

[Android :](#)

[Apple :](#)

[Fenêtres:](#)

Introduction

Avec la version d'Android 10 et d'iOS 14, l'Aléatoire des adresses MAC a été introduit pour tenter d'empêcher le suivi des utilisateurs en fonction de leur adresse MAC sans fil. Cela est bon pour la confidentialité lorsque vous rejoignez des réseaux hotspots, mais rend le suivi des périphériques difficile dans un environnement d'entreprise, en particulier lorsque vous essayez de profiler ces périphériques ou d'utiliser un Gestionnaire de périphériques mobiles pour vous assurer que le périphérique est conforme à la politique de sécurité d'une entreprise avant d'accéder au réseau.

Pour les services de profilage et MDM, les utilisateurs finaux peuvent être invités à désactiver la randomisation MAC sur le périphérique avant d'obtenir l'accès réseau prévu. Pour ce faire, vous pouvez rediriger les utilisateurs vers une page hotspot modifiée qui fournit des instructions pour désactiver la randomisation MAC lorsque le périphérique utilise une adresse MAC aléatoire pour se connecter au réseau. Une fois la randomisation MAC désactivée, l'utilisateur peut se connecter normalement.

Configuration

1. Accédez à **Administration > Identity Management > Groups**, sélectionnez **Endpoint Identity Groups** et sélectionnez **Add** pour créer un nouveau groupe de terminaux appelé **Points de terminaison MAC aléatoires**

The screenshot shows the Cisco Identity Services Engine (ISE) configuration interface. The breadcrumb navigation is: Administration > Identity Management > Groups > Endpoint Identity Group List > New Endpoint Group. The main form is titled 'Endpoint Identity Group' and contains the following fields:

- Name:** Random_MAC_Endpoints
- Description:** To temporarily store random MAC addresses for endpoint purge policy
- Parent Group:** (empty dropdown menu)

At the bottom of the form, there are two buttons: 'Submit' and 'Cancel'.

2. Accédez à **Centres de travail > Accès invité > Portails et composants**, sélectionnez **Ports invités** et sélectionnez **Créer** pour créer un nouveau portail invité de hotspot appelé **Détection MAC aléatoire**.
3. Sous **Paramètres du portail**, sélectionnez le groupe de points de terminaison créé ci-dessus pour le **groupe d'identité de point de terminaison**
4. Sélectionner la **personnalisation de la page du portail**
5. Sous **Éléments de texte**, modifiez le **titre de la bannière** en **MAC aléatoire détectée**
6. Sélectionner une **stratégie d'utilisation acceptable**
7. Remplacer le **titre du contenu** par : **Votre périphérique utilise une adresse MAC aléatoire**
8. Ajouter le texte suivant à la page **Texte d'instruction** : **Modifiez le paramètre réseau de votre périphérique pour utiliser l'adresse MAC globale au lieu de l'adresse MAC aléatoire pour accéder au réseau.**D'autres instructions peuvent également être fournies avec des détails sur la désactivation de l'aléatoire MAC par SSID ou globalement sur le périphérique.
9. Ajoutez le contenu facultatif suivant sur la page AUP pour supprimer les éléments du portail hotspot (assurez-vous de sélectionner **Basculer la source HTML** avant et après le collage dans le script) :
10. D'autres paramètres de cette page peuvent être modifiés pour fournir des instructions sur la modification du paramètre de randomisation MAC sur les périphériques. Une fois terminé, sélectionnez **Enregistrer**.
11. Créer un profil d'autorisation appelé **Random_MAC** pour rediriger vers la page créée ci-dessus

12. Créez une règle de stratégie d'autorisation pour utiliser **Random_MAC** avec une condition qui correspond à n'importe quelle adresse MAC Randomisée pour que les SSID refusent l'adresse MAC aléatoire. Ici, la condition de correspondance de chaînes regex (**CORRESPOND $^{\wedge}$. $[26AEae]$.***) est utilisée pour identifier une adresse MAC aléatoire qui utilise un bit significatif localement de l'adresse MAC que suivent les périphériques Android et iOS

Instructions spécifiques au périphérique

Voici les étapes que l'utilisateur peut être invité à effectuer pour certains périphériques courants. Les fournisseurs de périphériques spécifiques peuvent avoir des étapes légèrement différentes pour désactiver l'aléatoire MAC sur leurs périphériques.

Android :

1. Ouvrez l'application **Paramètres**.
2. Sélectionnez **Réseau et Internet**.

3. Sélectionnez **WiFi**.
4. Vérifiez que vous êtes connecté au SSID d'entreprise.
5. Effleurez l'icône de rapport en regard de la connexion WIFI actuelle.
6. Sélectionnez **Avancé**.
7. Sélectionnez **Confidentialité**.
8. Sélectionnez **Utiliser l'adresse MAC du périphérique**.

Apple :

Apple a publié un article contenant des instructions sur la désactivation de la randomisation MAC sur leurs périphériques :

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

Fenêtres:

Au moment de la rédaction de cet article, les adresses MAC aléatoires sont désactivées par défaut sous Windows, mais un utilisateur peut choisir de les activer. Voici des instructions sur la désactivation de la fonctionnalité si activée :

- Désactivez l'option Utiliser des adresses matérielles aléatoires pour tous les réseaux :
- Désactivez l'option Utiliser des adresses matérielles aléatoires pour un réseau spécifique :