

Uso del portale hotspot per istruire gli utenti sulla disabilitazione della casualizzazione degli indirizzi MAC

Sommario

[Introduzione](#)

[Configurazione](#)

[Istruzioni specifiche del dispositivo](#)

[Android:](#)

[Apple:](#)

[Windows:](#)

Introduzione

Con il rilascio di Android 10 e iOS 14, è stata introdotta la casualizzazione degli indirizzi MAC per impedire agli utenti di essere tracciati in base al loro indirizzo MAC wireless. Ciò è utile per la privacy quando si accede alle reti degli hotspot, ma rende difficile il monitoraggio dei dispositivi in un ambiente aziendale, in particolare quando si tenta di creare un profilo di questi dispositivi o si utilizza Gestione dispositivi mobili per verificare che il dispositivo sia conforme ai criteri di sicurezza dell'organizzazione prima di ottenere l'accesso alla rete.

Per i servizi di profiling e MDM, agli utenti finali può essere richiesto di disabilitare l'assegnazione casuale di indirizzi MAC sul dispositivo prima di ottenere l'accesso alla rete desiderato. Questo può essere ottenuto reindirizzando gli utenti a una pagina di hotspot modificata che fornisce istruzioni per disabilitare l'assegnazione casuale di indirizzi MAC quando il dispositivo utilizza un indirizzo MAC casuale per connettersi alla rete. Una volta disattivata l'assegnazione casuale di indirizzi MAC, l'utente può connettersi normalmente.

Configurazione

1. Passare a **Amministrazione > Gestione delle identità > Gruppi**, selezionare **Gruppi di identità degli endpoint** e selezionare **Aggiungi** per creare un nuovo gruppo di endpoint denominato

Endpoint_MAC_casuali

The screenshot displays the Cisco Identity Services Engine (ISE) Administration interface. The breadcrumb navigation path is: Administration > Work Centers > Identity Management > Groups > Endpoint Identity Groups > New Endpoint Group. The main content area shows the 'Endpoint Identity Group' configuration form. The 'Name' field is set to 'Random_MAC_Endpoints' and the 'Description' field is set to 'To temporarily store random MAC addresses for endpoint purge policy'. The 'Parent Group' dropdown is empty. The 'Submit' and 'Cancel' buttons are visible at the bottom of the form.

2. Passare a **Centri di lavoro > Accesso guest > Portali e componenti**, selezionare **Portali guest** e selezionare **Crea** per creare un nuovo portale guest di hotspot chiamato **MAC casuale rilevato**
3. In **Impostazioni portale**, selezionare il gruppo di endpoint creato in precedenza per il **gruppo di identità degli endpoint**
4. Seleziona **personalizzazione pagina portale**
5. In **Elementi di testo**, modificare il titolo del banner in **MAC casuale rilevato**
6. Seleziona **criteri di utilizzo accettabili**
7. Cambia titolo contenuto in: **Il dispositivo usa un indirizzo MAC casuale**
8. Aggiungere il testo seguente alla pagina **Testo istruzioni: Modificare le impostazioni di rete sul dispositivo in modo che utilizzi l'indirizzo MAC globale anziché l'indirizzo MAC casuale per ottenere l'accesso alla rete.**Ulteriori istruzioni possono essere fornite con le specifiche sulla disattivazione della casualizzazione MAC per SSID o globalmente sul dispositivo.
9. Aggiungere il seguente contenuto facoltativo nella pagina AUP per rimuovere gli elementi del portale degli hotspot (assicurarsi di selezionare il pulsante **Attiva/disattiva origine HTML** prima e dopo aver incollato lo script):
10. È possibile modificare altre impostazioni in questa pagina per fornire istruzioni su come modificare l'impostazione di casualità MAC sui dispositivi, dopo aver selezionato **Salva**
11. Crea profilo di autorizzazione denominato **Random_MAC** per reindirizzare alla pagina creata in precedenza



12. Creare una regola dei criteri di autorizzazione per utilizzare **Random_MAC** con una condizione che corrisponda a qualsiasi indirizzo MAC casuale affinché gli SSID neghino l'utilizzo di un indirizzo MAC casuale. In questo caso, la condizione di corrispondenza della stringa regex (**MATCHES ^.[26AEae].***) viene utilizzata per identificare l'indirizzo MAC casuale che utilizza il bit localmente significativo dell'indirizzo MAC seguito sia dai dispositivi Android che iOS



Istruzioni specifiche del dispositivo

Di seguito sono riportati i passaggi che l'utente può completare per alcuni dispositivi comuni. I fornitori di dispositivi specifici potrebbero avere passaggi leggermente diversi per disabilitare la Randomizzazione MAC sui loro dispositivi.

Android:

1. Aprire l'app **Settings**.
2. Selezionare **Rete e Internet**.
3. Selezionare **WiFi**.

4. Assicurarsi di essere connessi all'SSID aziendale.
5. Toccare l'icona dell'ingranaggio accanto alla connessione WIFI corrente.
6. Selezionare **Avanzate**.
7. Selezionare **Privacy**.
8. Selezionare **Use Device MAC**.

Apple:

Apple ha pubblicato un articolo con le istruzioni su come disabilitare la Randomizzazione MAC sui propri dispositivi:

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

Windows:

Al momento della stesura di questo articolo, gli indirizzi MAC casuali sono disabilitati per impostazione predefinita in Windows, ma un utente può scegliere di attivarlo. Di seguito sono riportate le istruzioni per disabilitare la funzione se abilitata:

- Disabilita 'Usa indirizzi hardware casuali' per tutte le reti:
- Disabilita 'Usa indirizzi hardware casuali' per una rete specifica: