Migratie Android Device Administrator (ADA) naar Android Open Source Project (AOSP)

Mei 2025

Index

1. Inleiding

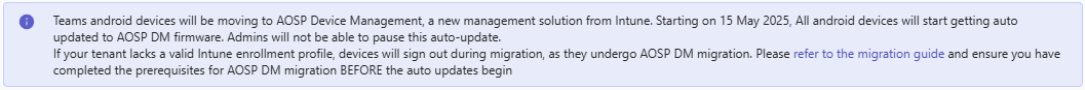
Microsoft gaat het beheersysteem van Android Teams toestellen veranderen. De belangrijkste reden hiervoor is, dat Google gaat stoppen met de oude Android Device Administrator (ADA) API koppelingen omdat deze niet meer te gebruiken zijn in combinatie met de moderne standaard voor beveiligde communicatie.

Ter vervanging heeft Microsoft het Android Open Source Project (AOSP) opgezet om deze taken over te nemen. Hiermee is de communicatie weer toekomstbestendig en veilig.

Enkele voordelen:

- Verbeterde beveiliging: AOSP biedt een modernere en veiligere manier om apparaten te beheren in vergelijking met de oudere Device Administrator-methode.
- Nieuwe functies: Door te migreren naar AOSP, kunnen organisaties profiteren van nieuwe functies en verbeterde functionaliteit die niet beschikbaar zijn in de oude beheeromgeving.
- Betere integratie met Intune: AOSP maakt gebruik van Intune voor apparaatbeheer, wat zorgt voor een naadloze integratie en betere controle over de apparaten.
- Automatische updates: Teams Android-apparaten zullen automatisch firmware-updates ontvangen, wat zorgt voor een up-to-date en goed functionerend systeem.

Microsoft heeft aangegeven dat deze migratie vanaf 15 mei doorgevoerd zal worden voor alle klanten, zonder mogelijkheid voor Rollback. Onderstaande melding is nu in het Teams Admin Center terug te vinden:



Om ervoor te zorgen dat bestaande hardware soepel blijft werken na deze automatische migratie, dient de Tenant beheerder diverse zaken voor te bereiden.

Let op: Deze migratie is bedoeld voor alle teams Android devices zoals bureautoestellen, rooms devices en andere Android based teams devices.

In dit document bieden wij diverse links, en tips om u op weg te helpen.

2. Voorbereiding tenant

Microsoft heeft een uitgebreid stappenplan gemaakt voor systeembeheerders om ervoor te zorgen dat de migratie soepel verloopt.

Ga hiervoor naar:

Migration guide Android AOSP management for Microsoft Teams Android devices - Microsoft Teams | Microsoft Learn

Stapsgewijs betekent dit dat de volgende punten doorlopen moeten worden:

1. Nieuwe Enrollment Policies maken:
   Moving Teams Android Devices to AOSP Device Management | Microsoft Community Hub

2. Indien er nu Compliance Policies zijn, dienen er ook AOSP devices compliance policies gemaakt te worden:
   Migration guide Android AOSP management for Microsoft Teams Android devices - Microsoft Teams | Microsoft Learn

3. Check je huidige firmware versies op je devices. Bij onjuiste of te oude firmware kan het zijn dat de automatisch uitrol van nieuw nieuwe firmware niet goed gaat. Meer firmware info vind je op:
   Moving Teams Android Devices to AOSP Device Management | Microsoft Community Hub

4. Als laatste kan je nu de toestellen gaan migreren.
   Migration guide Android AOSP management for Microsoft Teams Android devices - Microsoft Teams | Microsoft Learn

Let op: Het is aan te raden om vóór de geforceerde migratie van Microsoft zelf al 1 of meerdere toestellen handmatig over te zetten op de AOSP firmware. Hiermee voorkom je onnodige downtime als de voorbereiding niet correct/volledig is gedaan

3. Zaken om rekening mee te houden

In dit hoofdstuk behandelen we de belangrijkste zaken, die we in de eerste aanpassingen zijn tegen gekomen bij klanten. Hou er rekening mee dat er in andere omgevingen ook andere zaken kunnen voorkomen.

- Indien Microsoft-accounts met MFA gebruikt worden op de te migreren toestellen, dan zal de gebruiker zich opnieuw op het toestel zelf moeten aanmelden na de migratie.

- Indien geen MFA gebruikt wordt, zal het toestel na de migratie met hetzelfde account weer opgestart en geactiveerd worden.

- Als een device ingelogd is met een DeviceEnrollmentManager Account, dan dient dit eerst ongedaan gemaakt worden: Enroll devices using a device enrollment manager account - Microsoft Intune | Microsoft Learn

- Remote login vanuit de webbrowser via https://microsoft.com/devicelogin in combinatie met MFA is niet langer ondersteund. Gebruikers waarbij MFA aan staat dienen op het apparaat zelf in te loggen.

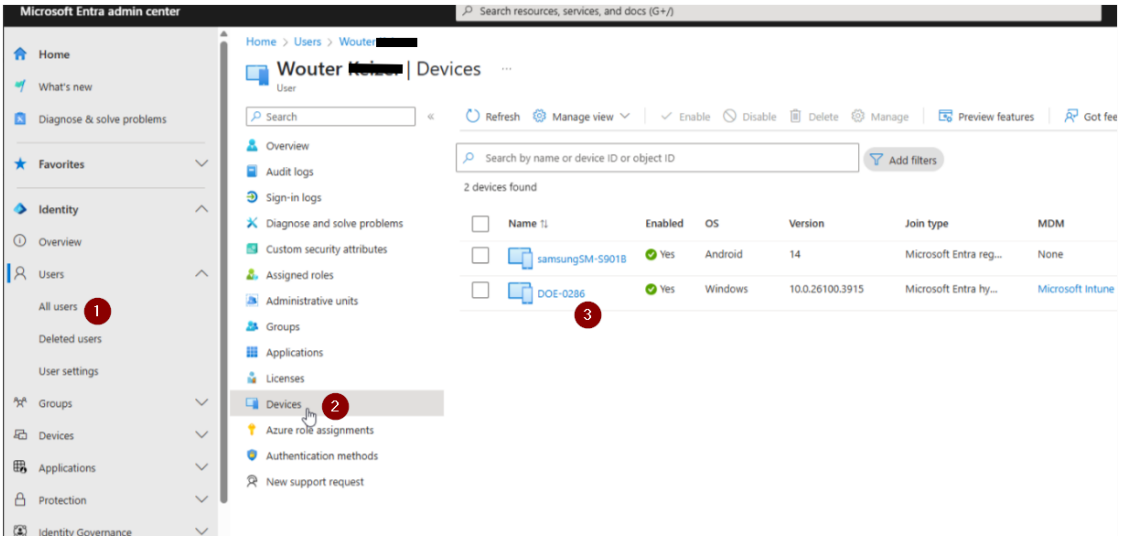
- Op het moment van schrijven hebben wij gemerkt dat de Poly CCX350 (nog) geen optie heeft om lokaal in te loggen met als gevolg dat je op dit type toestel dus niet met een MFA enabled account kan inloggen! Hiervan is melding gemaakt bij Microsoft.
  Update: Teams App update van 26-5-2025 versie 1449/1.0.94.2025165302 heeft dit issue verholpen.

- Het kan zijn dat u tijdens upgraden geen AOSP-firmware ziet, deze wordt namelijk pas zichtbaar als de laatste NON-AOSP firmware op het apparaat staan. Het kan dus noodzakelijk zijn om meerdere updates te doen.

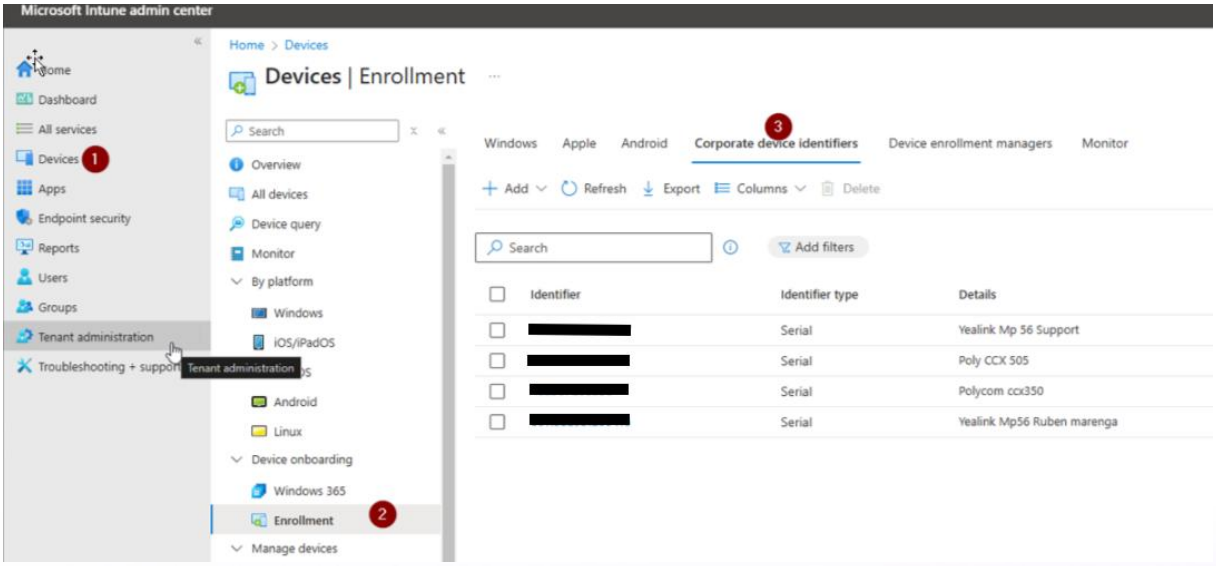
- Als toestellen niet op de laatste NON-AOSP firmware draaien, bestaat de kans dat de geforceerde migratie niet goed verloopt en toestellen niet updaten naar AOSP firmware.

- Om alle voorbereidingen goed te doorlopen zijn administrator rechten vereist voor meerdere beheer portalen van Microsoft. Een Global Administrator heeft deze rechten.

- Inlog problemen na de migratie - terwijl wel aan alle voorbereiding is voldaan - is vaak te wijten aan limieten die ingesteld zijn. Bijvoorbeeld een maximum aantal geregistreerde apparaten onder 1 gebruiker. Een gemigreerd apparaat wordt als een extra/nieuw device gezien. Verwijder in dat geval de oude geregistreerde devices van de gebruiker onder Entra of Intune bij Users à “user” à Devices.



- Als er gekozen wordt voor een setup waarbij alleen “Enterprise Managed devices” zijn toegestaan, dan dienen de “Android devices” handmatig toegevoegd te worden aan de “Corporate Device Identifiers”.



Hiermee worden de apparaten als “Enterprise Managed” behandeld.