Configuration Note

AOSP Migration for AudioCodes Teams Devices

audiocodes

Table of Contents

Notice

Information contained in this document is believed to be accurate and reliable at the time of printing. However, due to ongoing product improvements and revisions, AudioCodes cannot guarantee accuracy of printed material after the Date Published nor can it accept responsibility for errors or omissions. Updates to this document can be downloaded from https://www.audiocodes.com/library/technical-documents.

This document is subject to change without notice.

Date Published: May-28-2026

Document Revision Record

LTRT	Description
21902	Initial release

Security Vulnerabilities

All security vulnerabilities should be reported to vulnerability@audiocodes.com.

WEEE EU Directive

Pursuant to the WEEE EU Directive, electronic and electrical waste must not be disposed of with unsorted waste. Please contact your local recycling authority for disposal of this product.

Customer Support

Customer technical support and services are provided by AudioCodes or by an authorized AudioCodes Service Partner. For more information on how to buy technical support for AudioCodes products and for contact information, please visit our website at https://www.audiocodes.com/services-support/maintenance-and-support.

Stay in the Loop with AudioCodes

Abbreviations and Terminology

Each abbreviation, unless widely used, is spelled out in full when first used.

Documentation Feedback

AudioCodes continually strives to produce high quality documentation. If you have any comments (suggestions or errors) regarding this document, please fill out the Documentation Feedback form on our website at https://online.audiocodes.com/documentation-feedback.

1 Guidelines

Android Open Source Project (AOSP) is the foundation of the Android operating system, providing an open-source framework that manufacturers and developers can use to build and customize Android devices. In the context of Teams Android Devices, AOSP Management allows organizations to enroll and manage these devices without relying on Google Mobile Services (GMS). This enables enterprises to maintain control over device security, updates, and compliance policies while ensuring a seamless sign-in experience for Teams users.

Intune provides a hand full of conditional access and security methods to secure the connection of external devices such as phones, meeting room devices etc., to the organization environment.

- Please make sure that your tenant is ready with AOSP policies, before deploying any device running this method.
- Your previous Device Administration method can remain and there's no need to delete it from Intune.

Important: *If your organization does not enroll Teams Android Devices in Intune, no enrollment profile or AOSP policies are required. Simply upgrade the devices to AOSP Management capable firmware when available.*

2 Step 1: Set Up New AOSP Management Enrollment Profiles

2.1 Prerequisites

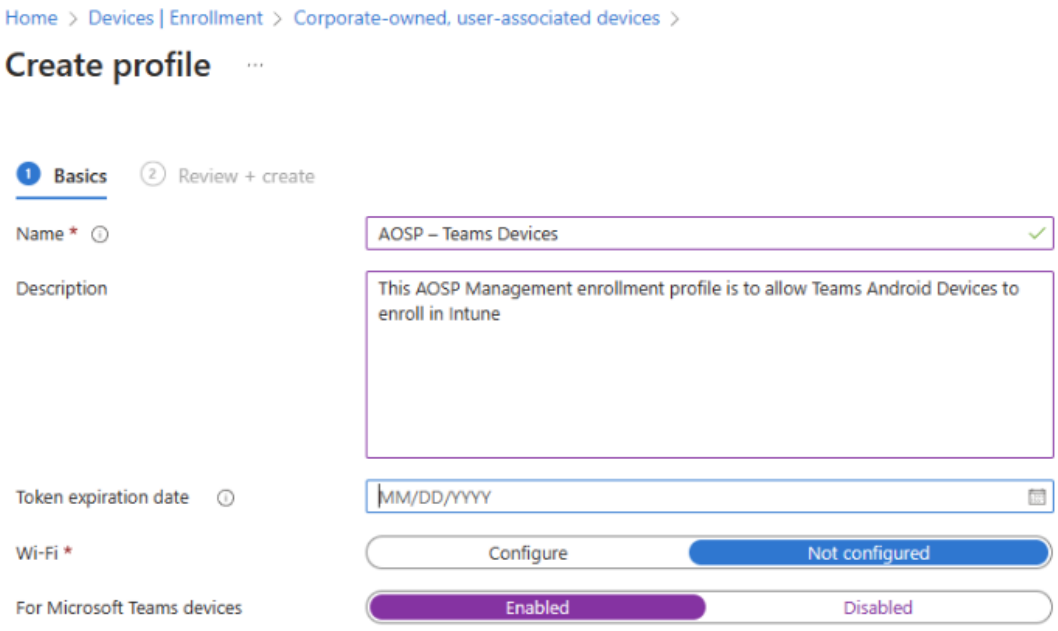
- Teams Android Devices enrolled using Device Administrator.
- Teams Android Devices that support AOSP Management.
- Intune admin permissions in your Microsoft 365 environment.

2.2 Instructions

1. Sign in to Intune Management Console at https://intune.microsoft.com/.
2. Navigate to Enrollment Profiles: Select **Devices** > **Enrollment** > **Android**).
3. Create an Enrollment Profile: Under **Enrollment Profiles**, select **Corporate-owned, user-associated device**, then click **Create policy**.

2.3 Profile Configuration

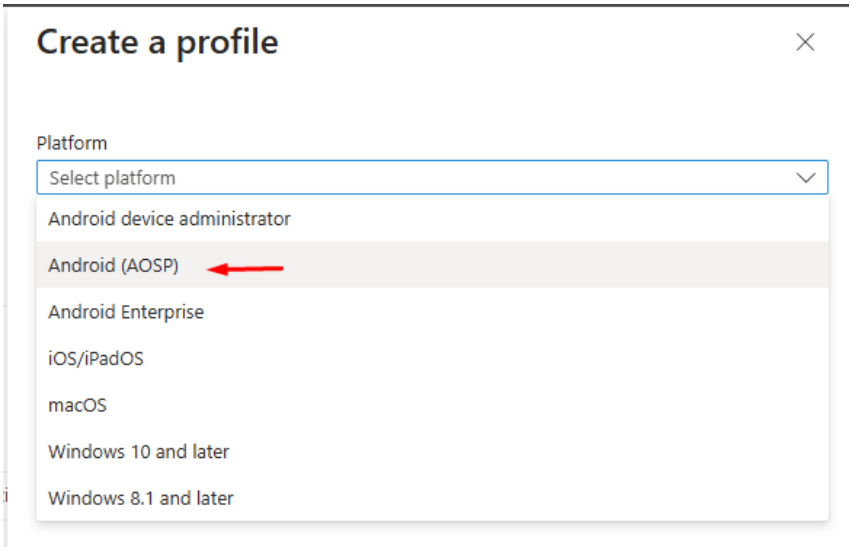
1. In the Name field, type "AOSP – Teams Devices".
2. In the Description field, type "This AOSP Management enrollment profile allows Teams Android Devices to enroll in Intune".
3. In the Token expiration date field, default to 65 years.
4. For Wi-Fi, select **Not configured**.
5. For Microsoft Teams devices, select **Enabled**.
6. Click **Next**, review your settings, and then click **Create**.



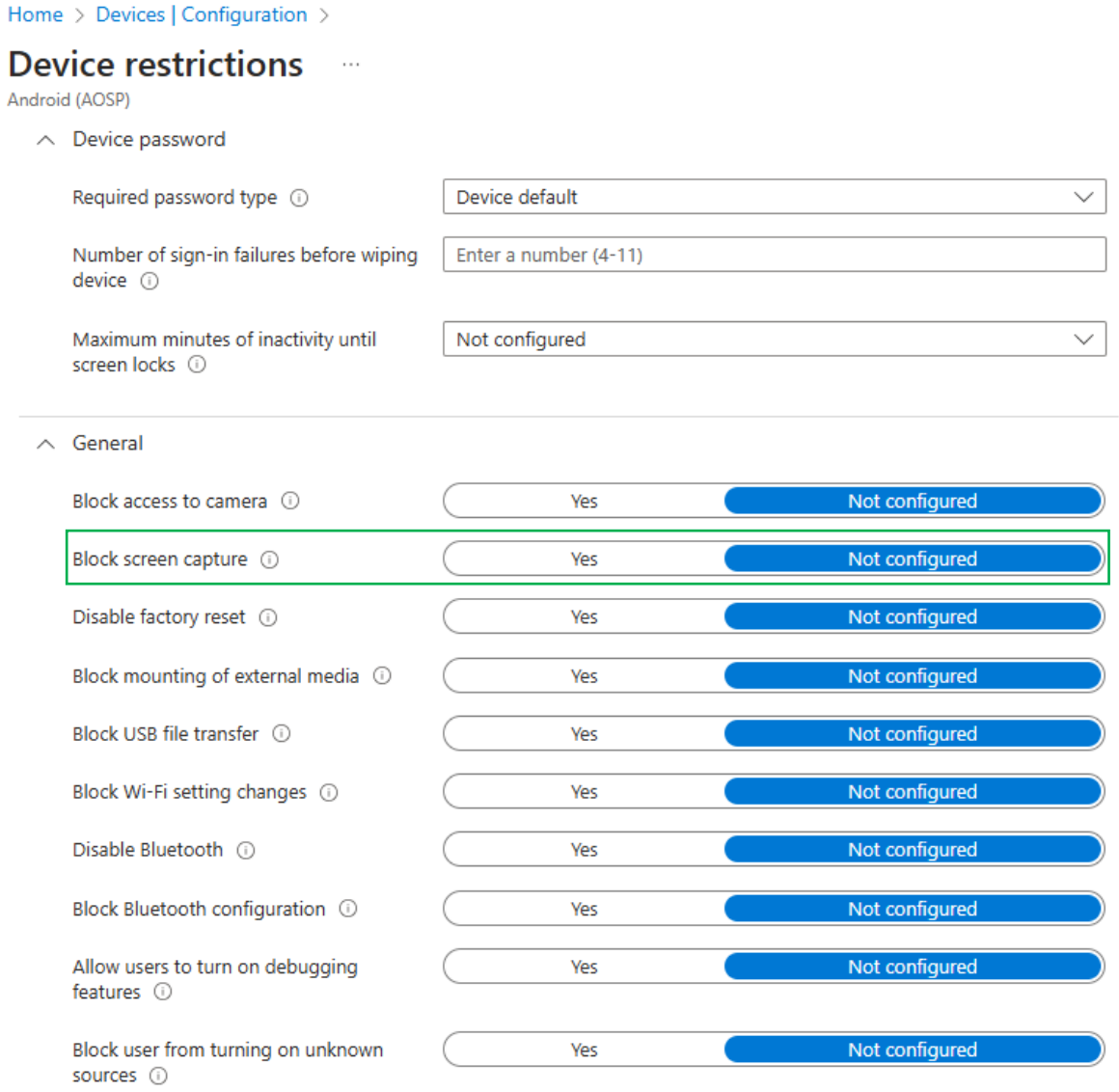
3 Step 2: Set Up AOSP Management Configuration and Compliance Policies

3.1 Configuration Policies

1. Sign in to Intune Management Console at https://intune.microsoft.com/.
2. Navigate to Configuration Policies: Select **Devices** > **Configuration**.
3. Create a new policy: Click **Create** > **New Policy**.
4. Platform: Select **Android (AOSP)**.

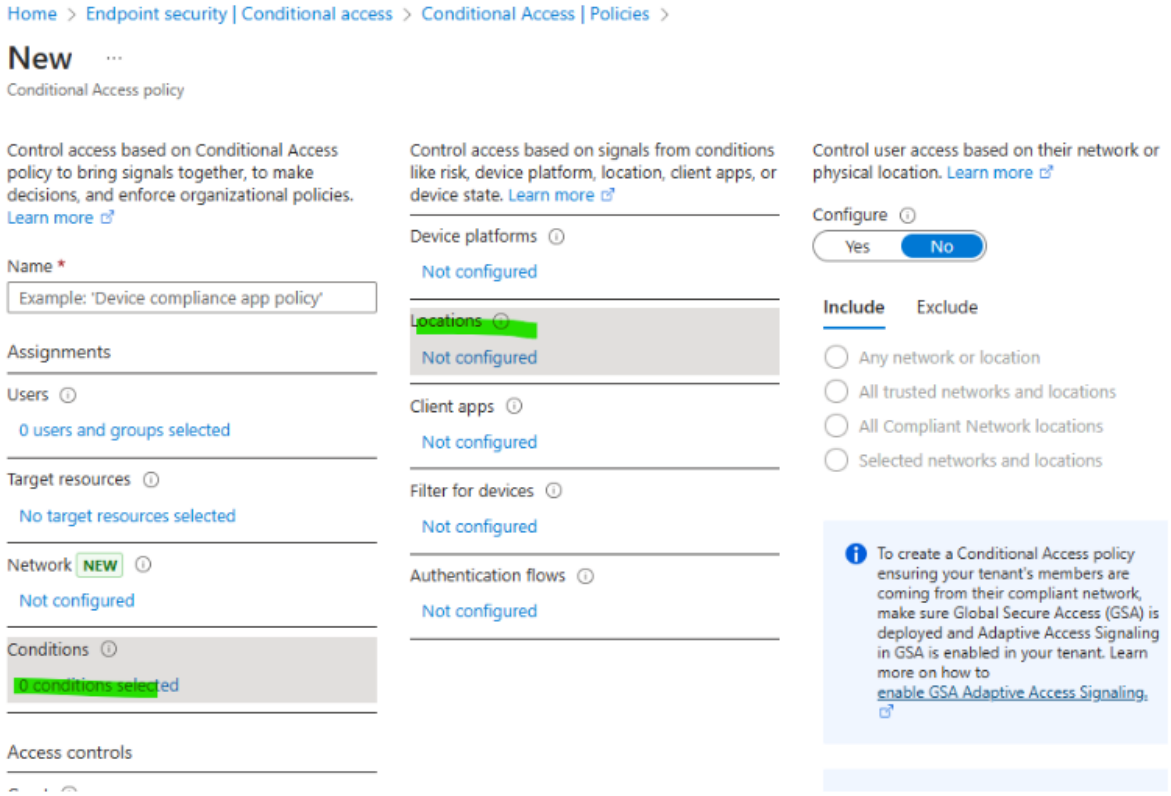


5. Profile Type: Select **Device Restrictions**, and then click **Create**.
6. Name & Description: Enter appropriate values.
7. General Settings: Set Block screen capture to **Yes**.



3.1.1 Location-based Policies Removal Recommendation

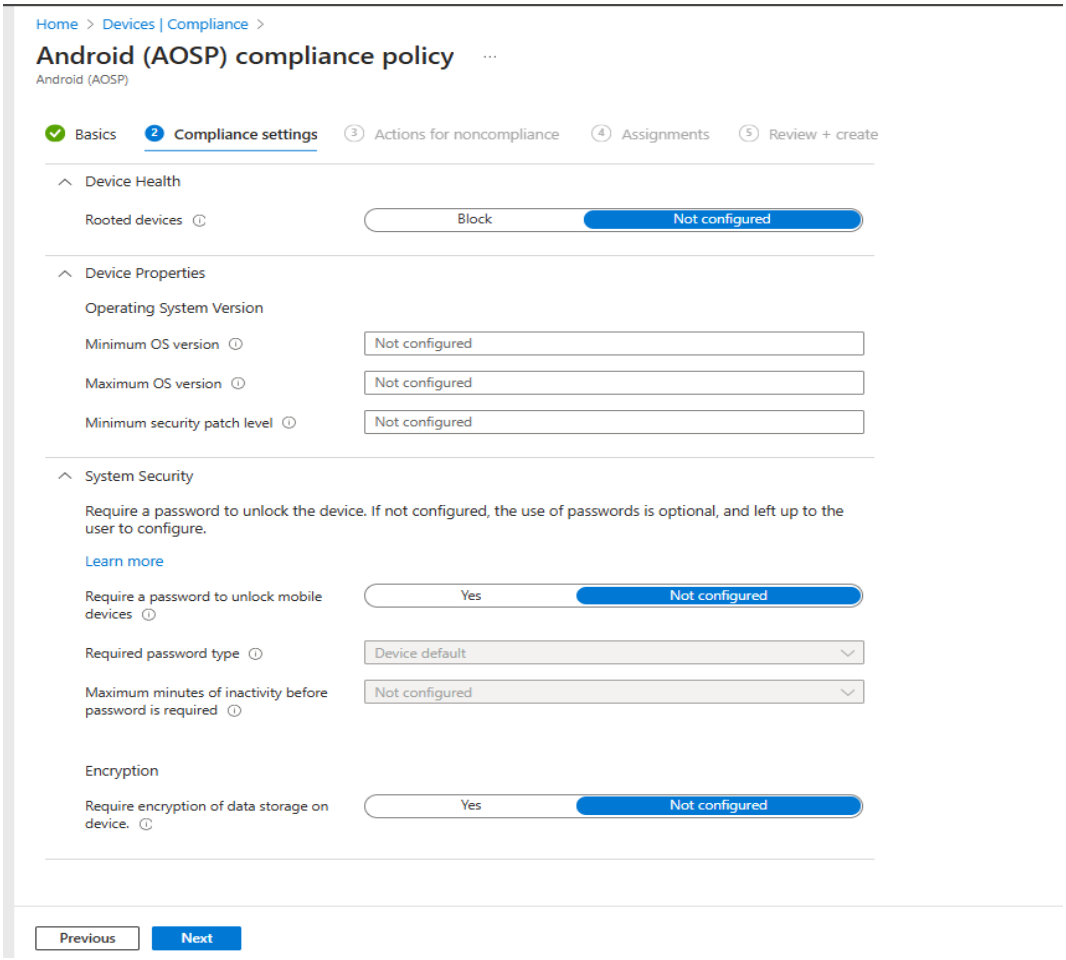
If the current Intune policies include a conditional access that also checks the location of the enrolled device, it's recommended that you set it to **Not Configured**, as shown in the figure below.



In addition, if there are App protection policies configured in Conditional Access, they are not supported on devices. This is by design, and they need to be removed.

3.1.2 Compliance Policies

1. Sign in to Intune Management Console.
2. Navigate to Compliance Policies: Select **Devices** > **Compliance**.
3. Create a new policy: Platform: Select **Android (AOSP)**.
4. Name & Description: Provide details.
5. Enable Compliance Settings:
   - Rooted devices: **Block**.
   - Minimum OS version.
   - Maximum OS version.
   - Require encryption of data storage.

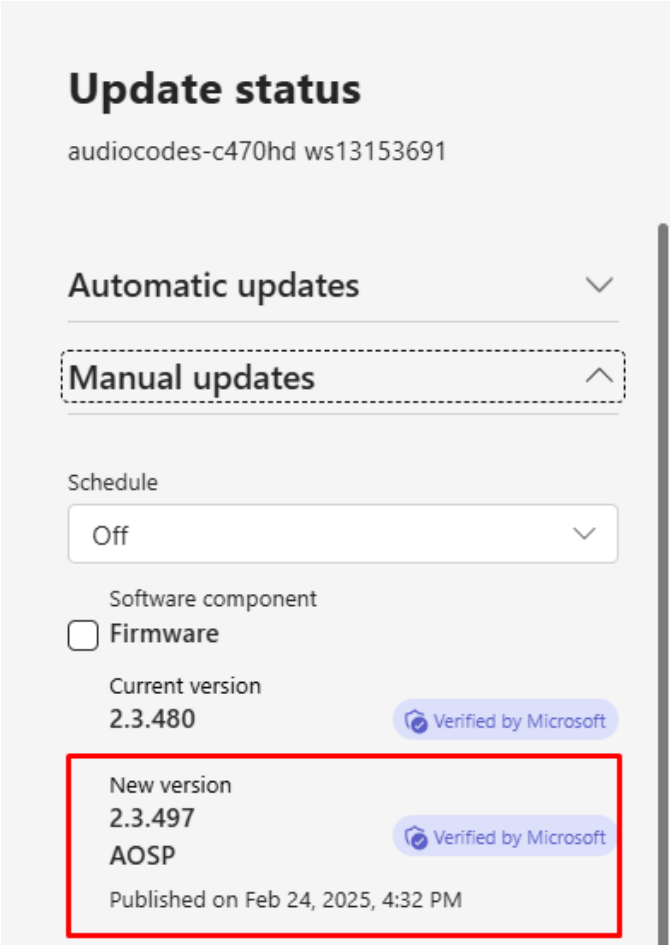


- Assign Policy: Assign to all devices or an Entra ID group, click **Next**, and then **Create**.

4 Step 3: Deploy AOSP Management Capable Device Firmware

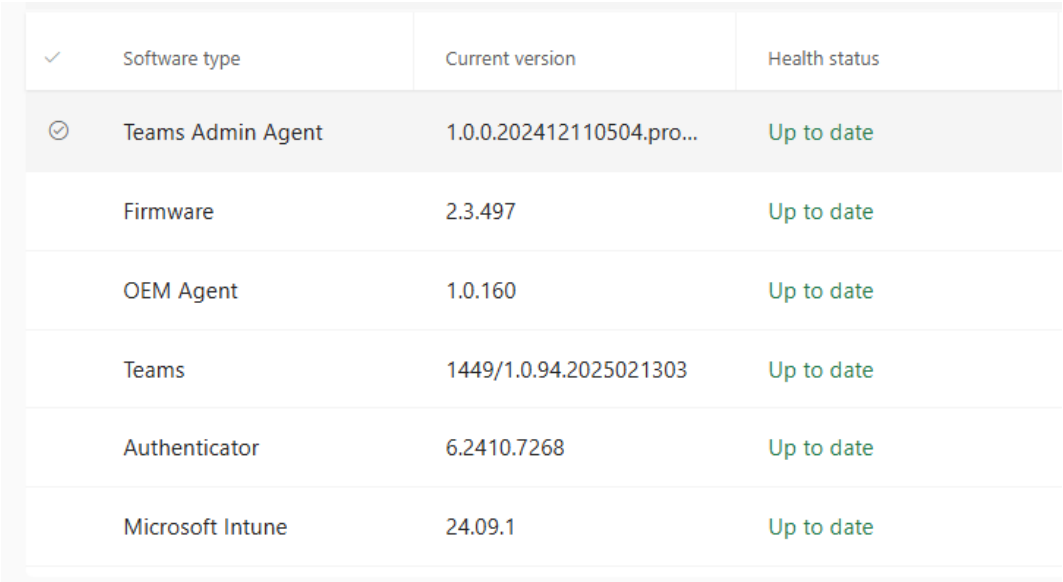
4.1 Firmware Deployment

1. Access Teams Admin Center at https://admin.teams.microsoft.com/.
2. Navigate to Device Updates: Select **Teams** > **Devices**.
3. Update Device Firmware:
   a. Select the device type.
   b. Click the display name of the device.
   c. Select **Update software**.
   d. Open Manual updates.
   e. Choose the new firmware update and schedule the update.
   f. Click **Update**.
4. Allow Time for the Update: The device automatically signs into Teams again after updating.



4.2 Confirming AOSP Management Update is Installed

1. Sign in to Teams Admin Center at https://admin.teams.microsoft.com/.
2. Navigate to Device Status: Select **Teams** > **Devices**.
3. Check Update History:
   a. Select the device.
   b. Click **History**.
   c. Confirm that the recent Software update status is "Successful".
4. Verify Software Type:
   a. Navigate to the **Health** tab.
   b. Make sure that the Health status field for the Microsoft Intune app and Authenticator app displays "Up to date".



Software type	Current version	Health status
Teams Admin Agent	1.0.0.202412110504.pro...	Up to date
Firmware	2.3.497	Up to date
OEM Agent	1.0.160	Up to date
Teams	1449/1.0.94.2025021303	Up to date
Authenticator	6.2410.7268	Up to date
Microsoft Intune	24.09.1	Up to date

5 References and Materials

- https://learn.microsoft.com/en-us/microsoftteams/rooms/android-migration-guide
- https://www.youtube.com/watch?v=caTvQnL_S_4
- https://www.linkedin.com/posts/thegrahamwalsh_microsoft-intune-aosp-activity-7300173564635152385-LdR6?utm_source=share&utm_medium=member_desktop&rcm=ACoAACoVce8BoNTKdTpLEjUSfi3ahcFySUdu1S0
- Intune Conditional Access policies support is same for Device Administrator and AOSP. Intune Conditional Access policies for Microsoft Teams devices are documented here: Supported Conditional Access and Intune device compliance policies for Microsoft Teams Rooms - Microsoft Teams | Microsoft Learn
- DEM stands for "device enrollment manager", which is a special Intune designation intended for accounts that aren't associated with normal users and thus are able to enroll up to 1000 devices (vs the normal 15 per user, see below link). Intune doesn't support DEM account enrollment for AOSP, which would extend to Teams Devices on AOSP as well.
  - AOSP doesn’t support DEM accounts: Enroll devices using a device enrollment manager account - Microsoft Intune | Microsoft Learn
  - If a customer wanted to remove the account from DEM list, here are the instructions to remove it, which are the inverse of adding them: Enroll devices using a device enrollment manager account - Microsoft Intune | Microsoft Learn

6 FAQ

6.1 Does the sign-in process for devices change after migration to AOSP?

Source: Microsoft Community Hub – Moving Teams Android Devices to AOSP Device Management

Except for the case of Device Code Flow (see the next topic), there is **no change** to the sign-in process or the user experience on devices following migration to AOSP management.

6.2 Why is sign-in failing when using microsoft.com/devicelogin (Device Code Flow - DCF)?

For **shared space devices** (e.g., Teams Rooms, Panels, and Common Area Phones) with **Teams resource accounts**, sign-in often fails due to enforcement of **user-interactive multi-factor authentication (MFA)**—which is **not supported** in this context.

Reference: Supported Conditional Access Policies

In addition, MS are forcing to block the usage of DCF (sign in code). For more information, including how to create an exclusion group to overcome this, see Policy changes for Microsoft Teams devices using device code flow authentication | Microsoft Community Hub

> Other MFA methods such as known network location or compliant device checks are supported for Teams resource accounts.

For **personal accounts**, if user-interactive MFA is enforced by policy, the microsoft.com/devicelogin method will also fail.

This can be mitigated through the following methods:

- Use **Conditional Access filters** to exclude user-interactive MFA policies during sign-in (based on known network or device type).
- Sign in **locally on the Teams device**, where users can interact with the MFA prompt directly on-screen.

6.3 What happens to devices that don't migrate to AOSP?

Devices that are unable to migrate will remain on **Android Device Administrator**. These devices:

- Will be **considered legacy and unsupported** once Device Administrator is deprecated.
- May **lose feature compatibility** at any time.

To continue using these devices:

1. Unenroll from Intune.
2. Re-sign in to the device without an Intune license.

More info: Manage Intune Devices with Android Device Administrator

6.4 How do I unenroll a Teams-certified Android device using Device Administrator?

For devices like the **C450HD and C448** (which remain on OS9 and won't get AOSP firmware), follow these steps:

1. Sign in to the **Microsoft 365 admin center**.
2. **Remove the Intune license** from the Teams account assigned to the device.

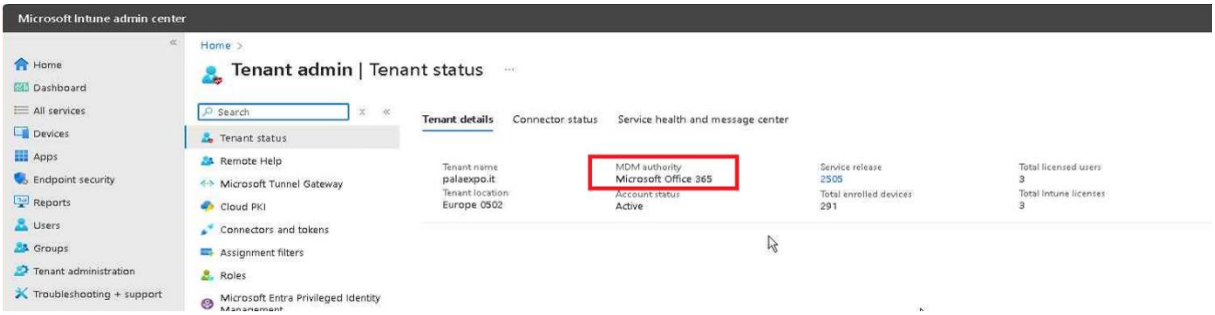
After license removal, there's a **30-day grace period** where the device still functions.

The device **must sign in again** during this period to avoid re-enrollment under Device Administrator.

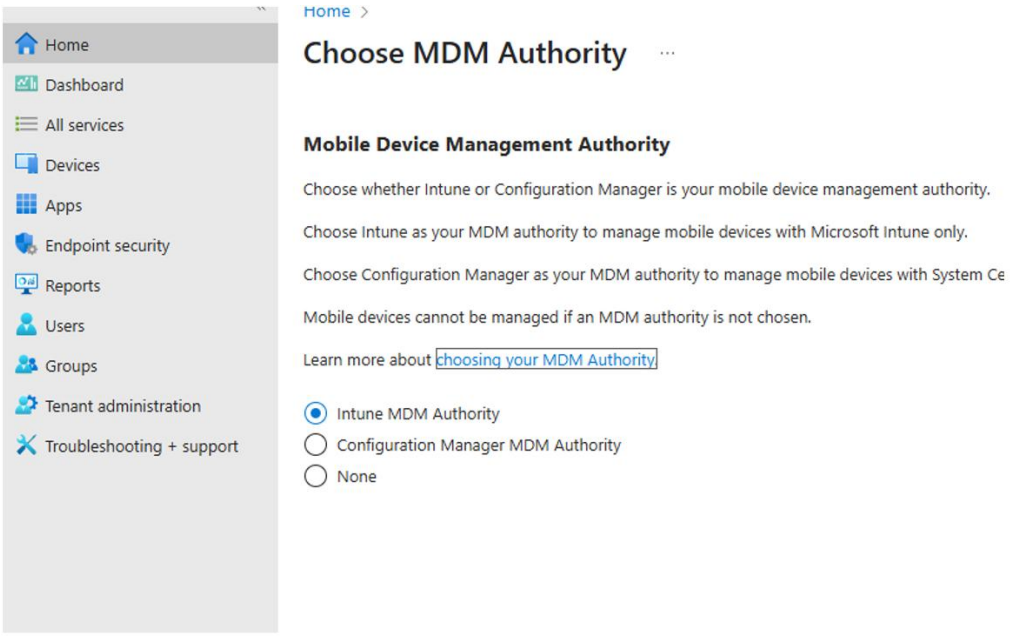
6.5 Checking MDM Authority settings in Intune

In rare occasions, the MDM (mobile device management) setting in Intune might be incorrect.

The mobile device management (MDM) authority setting determines how you manage your devices. As an IT admin, you must set an MDM authority before users can enroll devices for management. You should also be assigned an Intune license to set the MDM Authority.



It must be set to Intune MDM authority –



Reference link - https://learn.microsoft.com/en-us/intune/intune-service/fundamentals/mdm-authority-set

6.6 Known issues in Teams devices

Refer to the following link by MS –

https://learn.microsoft.com/en-us/troubleshoot/microsoftteams/teams-rooms-and-devices/teams-rooms-known-issues-android

Explicitly, sign in issues and workaround are listed in the following resource –

https://learn.microsoft.com/en-us/troubleshoot/microsoftteams/teams-rooms-and-devices/signed-out-of-teams-android-devices

6.7 List of actions important to notice

Policies/Rules	Recommendation	Outcomes if recommendation not followed
CA Policy - with device compliance requirement	Ensure enrollment profile is created in Intune.	Devices may sign-out during migration. Further sign-ins will also be blocked with error AADSTS50002: "Device is required to be compliant" in AAD signin non-interactive logs.
CA Policy - Multi-factor Authentication (MFA)	1. Not supported at all for shared devices 2. For personal devices: not supported with DCF for Teams app version 1449/1.0.94.2025084203 (and earlier) • You may use per-user MFA to unblock DCF sign-in temporarily but this is deprecated in September 2025. 3. For personal devices (Teams Phones, Teams Displays): Supported for DCF with on screen keyboard for Teams app version 1449/1.0.94.2025087003 (and later).	DCF sign-in will fail with AADSTS50076/50079: "use/enroll multi-factor authentication" error code. more info can be found here - https://learn.microsoft.com/en-us/entra/identity/conditional-access/concept-conditional-access-cloud-apps#user-actions
CA Policy - with App Protection Policies	Not supported	Sign-in will fail with AADSTS53009/53005 error code.
CA Policy - exclude devices	Location filters or Device filters can be used to exclude devices from unsupported policies.	If not excluded from unsupported policies, devices may sign-out.
CA Policy - Terms of Use (ToU)	■ Not supported for shared devices ■ Not supported with DCF for Teams app version 1449/1.0.94.2025084203 and earlier ■ Supported for DCF with on screen keyboard for Teams app version 1449/1.0.94.2025087003 and later	DCF sign-in will fail with AADSTS50158 error code.
CA Policy - Sign-in Frequency	■ Not supported for shared devices ■ Sign-in Frequency for "1 hour" and "Every time" should not be used for Teams Devices undergoing AOSP migration	Requires reauthentication if configured (AADSTS70045), including causing sign-outs during migration.

Policies/Rules	Recommendation	Outcomes if recommendation not followed
Firewall rules	Teams and Intune URLs need to be allowed in firewalls 1. Allow Teams traffic, Office 365 endpoints 2. Allow Intune traffic, Intune endpoints	Devices may sign-out during migration and further sign-in may fail with error code: 20018 or discovery on login screen UI.
Dynamic Device Groups	Do not use Dynamic Device Groups that require attributes that are populated by Intune (e.g. device.deviceManufacturer -eq "Cisco").	Leads to replication delays on the Manufacturer and Model number attributes which can cause sign-in delays or require multiple sign in attempts.
Sign in fails/Calendar not synced/Account name not visible	Enable Office 365 SharePoint Online in Entra Admin Center	AADSTS500014: The service principal for resource '00000003-0000-0ff1-ce00-000000000000' is disabled

International Headquarters
Naimi Park
6 Ofra Haza Street
Or Yehuda, 6032303, Israel
Tel: +972-3-976-4000
Fax: +972-3-976-4040

AudioCodes Inc.
80 Kingsbridge Rd
Piscataway, NJ 08854, USA
Tel: +1-732-469-0880
Fax: +1-732-469-2298

Contact us: https://www.audiocodes.com/corporate/offices-worldwide
Website: https://www.audiocodes.com

Document #: LTRT-21902