Enrollment of AudioCodes Phones and Collaboration Bars in Microsoft Endpoint Manager

1.4

@ Farhad Niat

CONTENTS

1. Introduction 3
2. Understanding device sign-in 3
3. Understand sign-in flows 3
4. User sign-in conditional access (Intune Compliance) 4
5. Device enrollment 4
6. Example configuration in AudioCodes lab environment 5

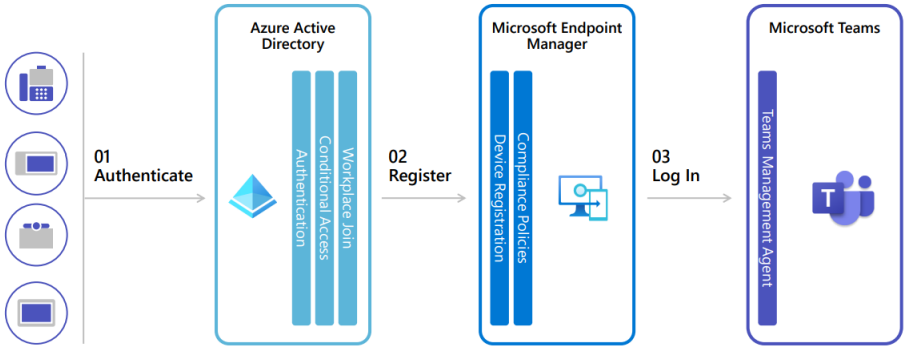
6.1 Creation of dynamic device group in AAD 5
6.2 Add dynamic query for Dynamic device members 5
6.3 Validation of Dynamic membership rules 6
6.4 Creation of Conditional Access Policy in AAD 6
6.5 Assignment of conditional access policy to dynamic device group 7
6.6 Select cloud apps 8
6.7 Select Device Platform 9
6.8 Grant access to devices which are marked as compliant 11
6.9 Compliance policy settings (Built-in Device Compliance Policy) in Endpoint Manager 11
6.10 Creation of Compliance policy 13
6.11 Overview Compliance settings in Endpoint Manager 14
6.12 Actions for noncompliance devices 15
6.13 Assign Compliance Policy to group 16
6.14 Identify devices as corporate-owned with serial number via Coporate device identifiers 16
6.15 Provisioning devices via Teams Admin Center for initial Login in BULK 18
6.16 Monitoring your compliance policy in endpoint Manager 20
6.17 Monitoring of enrolled/ registered devices in AAD 21

1. Introduction

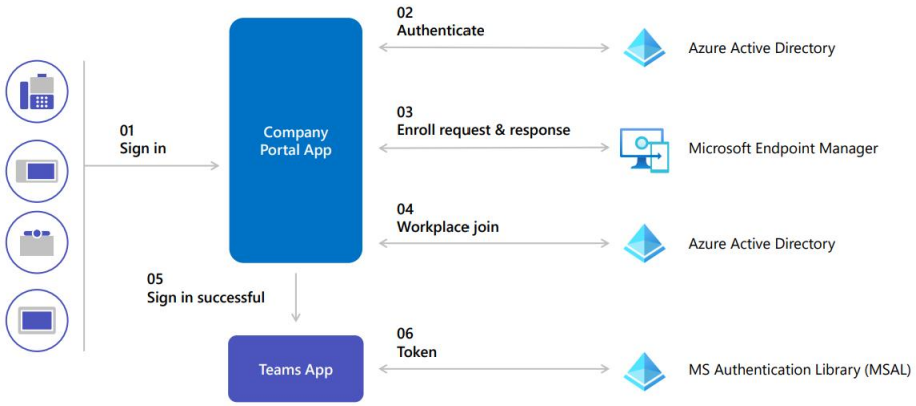
Please find a configuration summary how AudioCodes Phones and Collaboration Bars can be enrolled and managed via Microsoft Endpoint Manager. Keep in mind that not all settings which are available can be set within Endpoint Manager and/or Azure Active Directory. Currently no other settings are applicable except the configuration example which is described in this document.

2. Understanding device sign-in

Sign-in and registration components



Sign-in and registration Flow



3. Understand sign-in flows

User sign in

User sign in using existing conditional access rules.
May include Multi Factor authentication and/or device compliance.

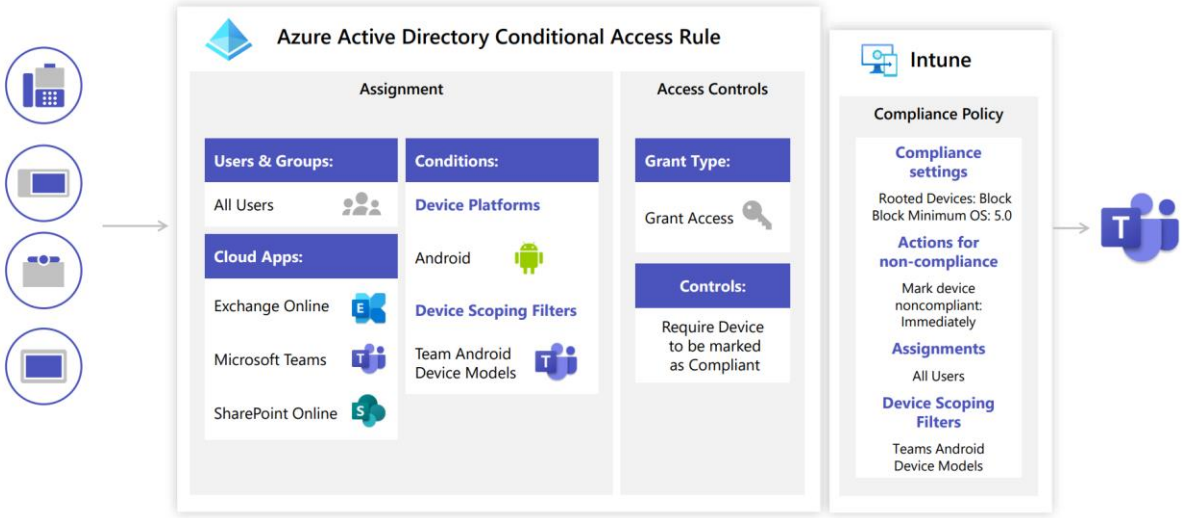
Common area devices

Evaluate trusted location and/or device compliance-based controls.
Target common area accounts with Azure AD groups in conditional access rules.
Do not use Multi Factor Authentication where possible and avoid using device compliance-based controls with hotdesking.

Meeting rooms

Evaluate trusted location, device compliance, or device scoping filter-based controls.
Target meeting room accounts with Azure AD Groups on conditional access rules.
Do not use Multi Factor Authentication.

4. User sign-in conditional access (Intune Compliance)



5. Device enrollment

Android enrollment

These devices do not run Google Play Services and run Android Open-Source versions. Firmware is built and supported by Microsoft OEM partners. It is highly recommended to update devices after enrollment via Teams Admin Center or AudioCodes OVOC.

Enrollment restrictions

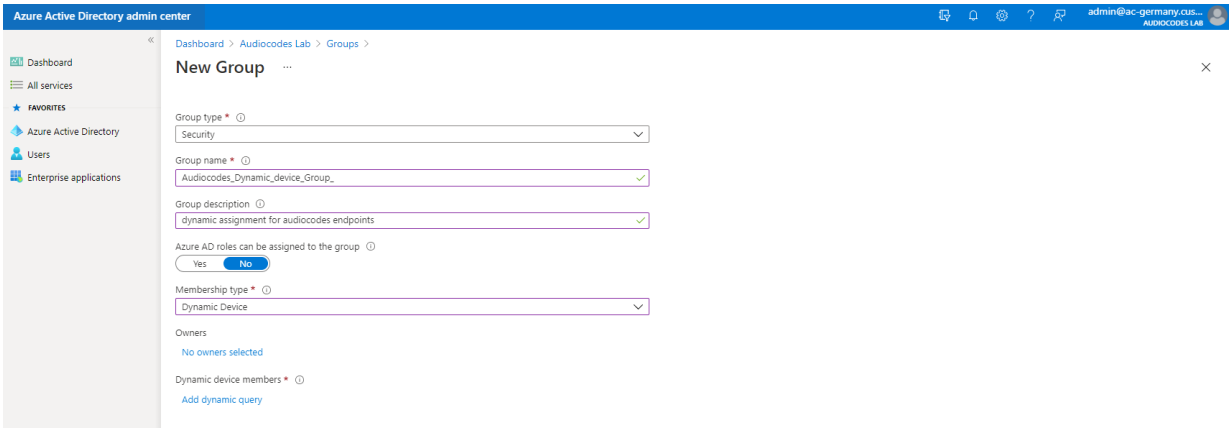
By default, users can only enroll up to 5 devices.
If using hotdesking, this number may need to be increased.
Consider any existing device type restrictions and if changes need to be made.

Corporate Device Management

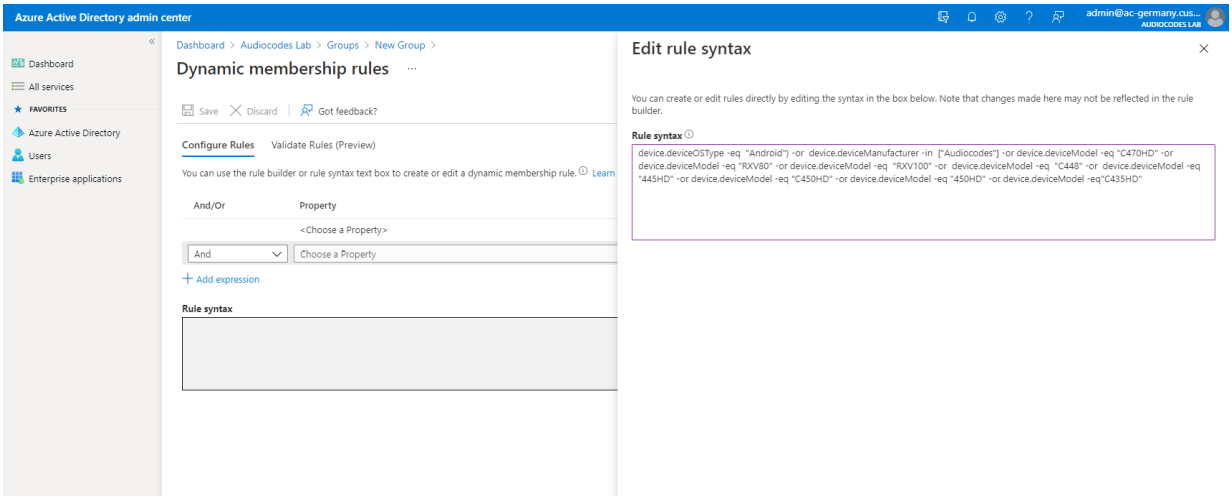
Importing device serial numbers into Microsoft Endpoint Manager lets you identify them as corporate devices identifiers. Ensures that only authorized devices are used.

6. Example configuration in AudioCodes lab environment

6.1 Creation of dynamic device group in AAD



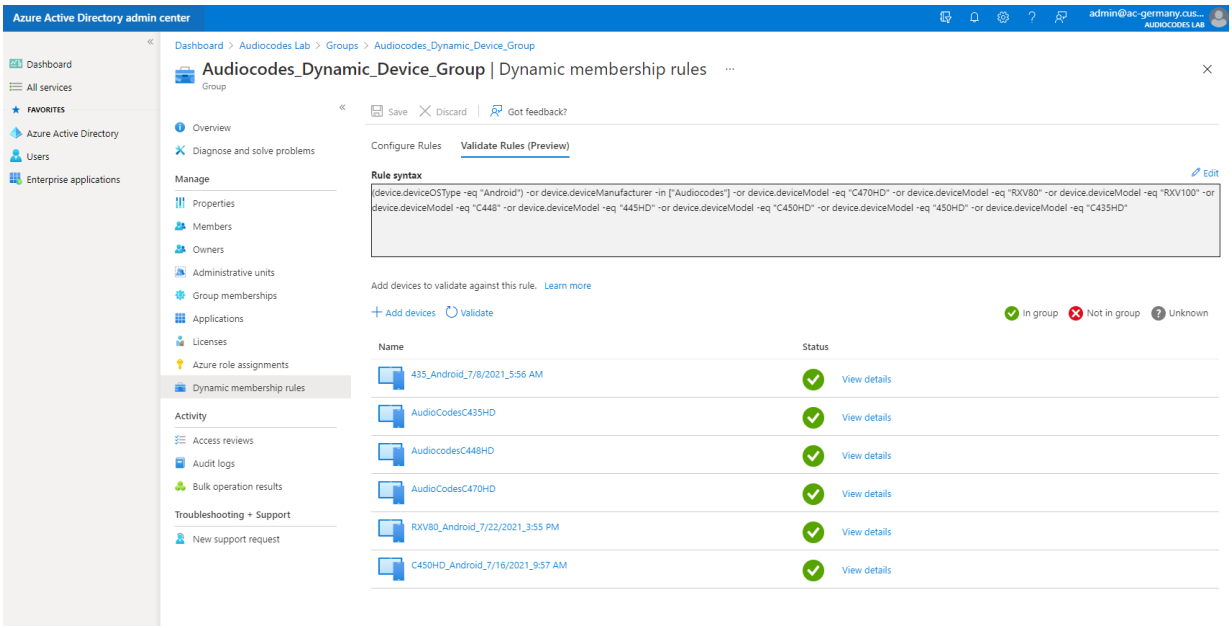
6.2 Add dynamic query for Dynamic device members



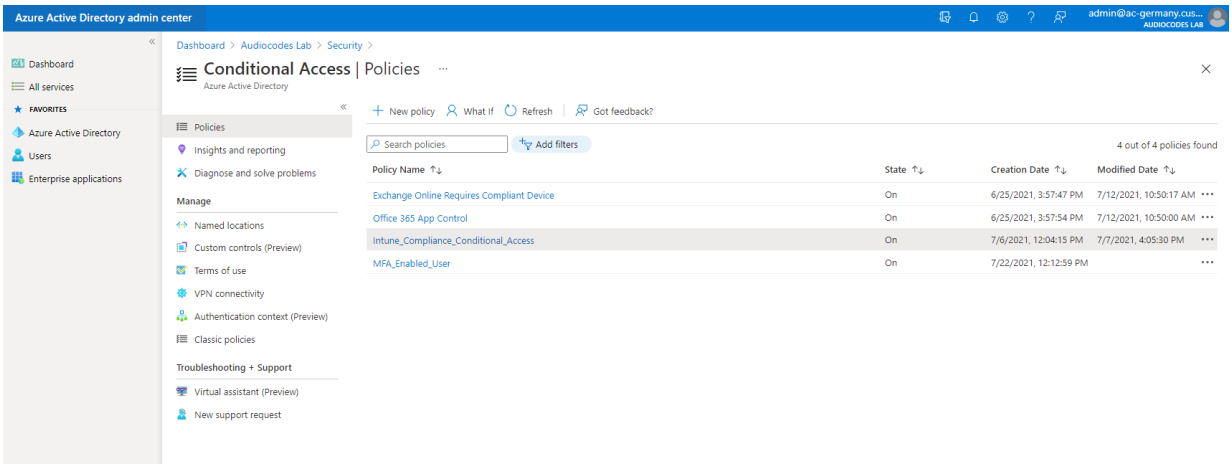
Rule syntax:

device.deviceOSType -eq "Android") -and device.deviceManufacturer -in ["Audiocodes"] -or device.deviceModel -eq "C470HD" -or device.deviceModel -eq "RXV80"-or device.deviceModel -eq "RXV81" -or device.deviceModel -eq "C448" -or device.deviceModel -eq "445HD" -or device.deviceModel -eq "C450HD" -or device.deviceModel -eq "450HD" -or device.deviceModel -eq"C435HD" -or device.deviceModel -eq "C455HD"

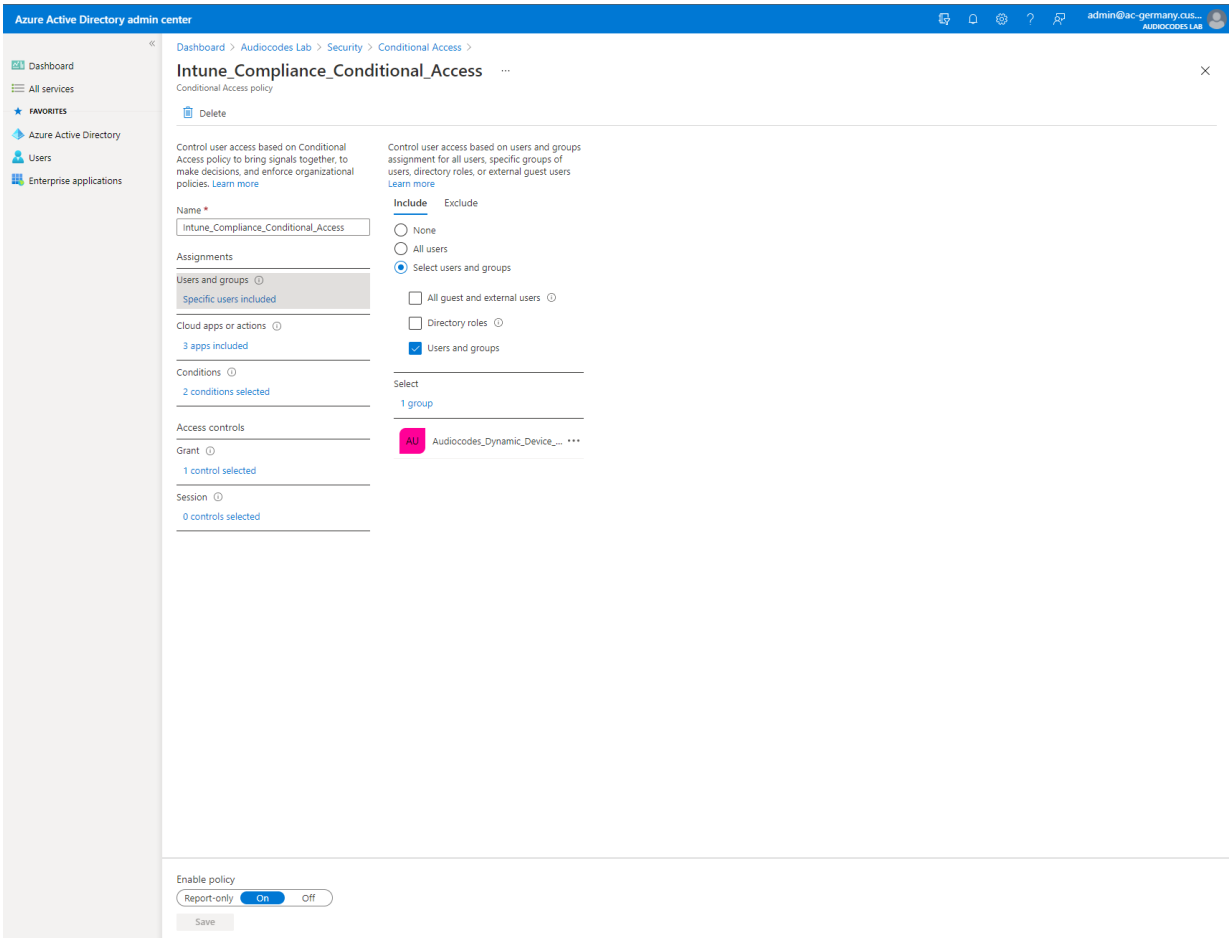
6.3 Validation of Dynamic membership rules



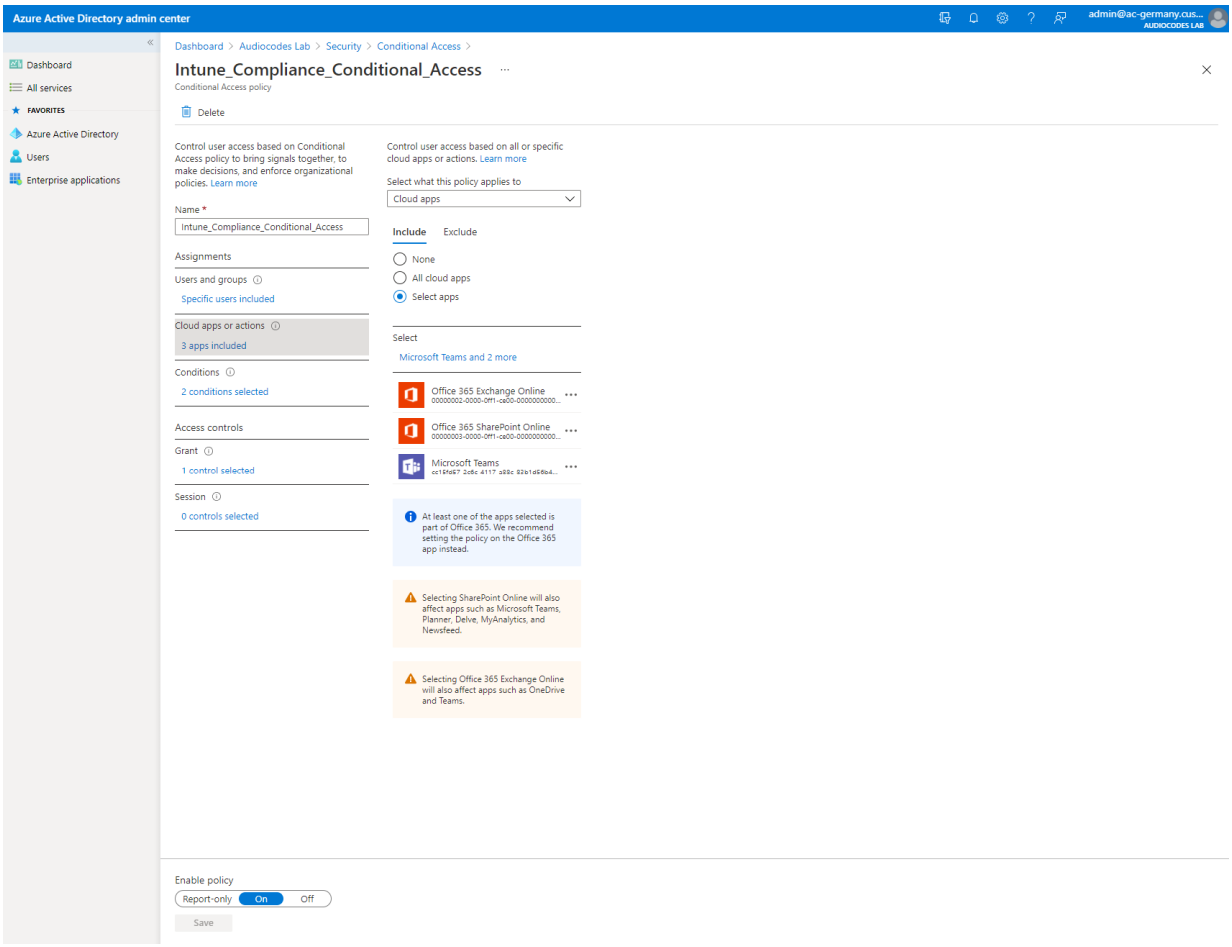
6.4 Creation of Conditional Access Policy in AAD



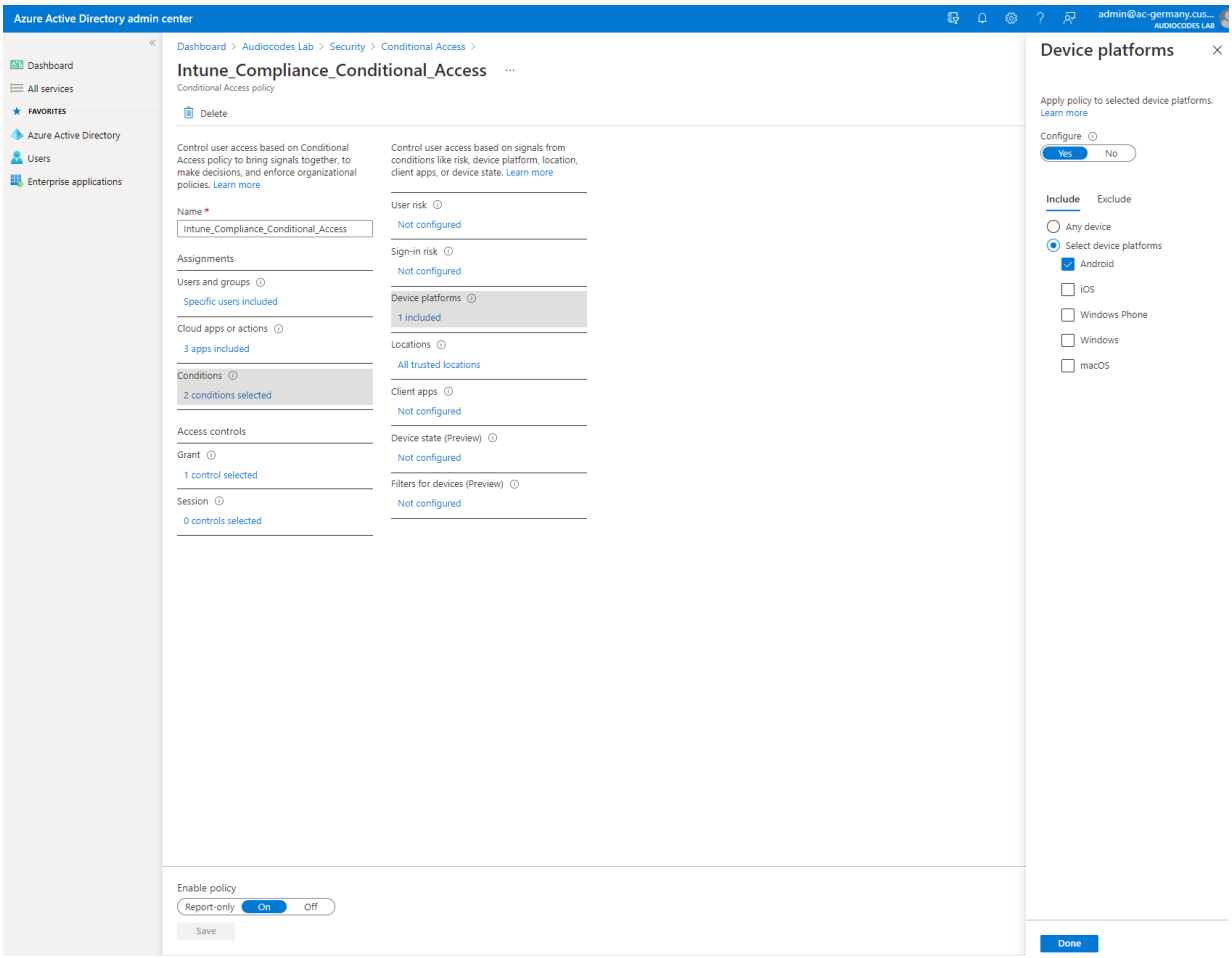
6.5 Assignment of conditional access policy to dynamic device group

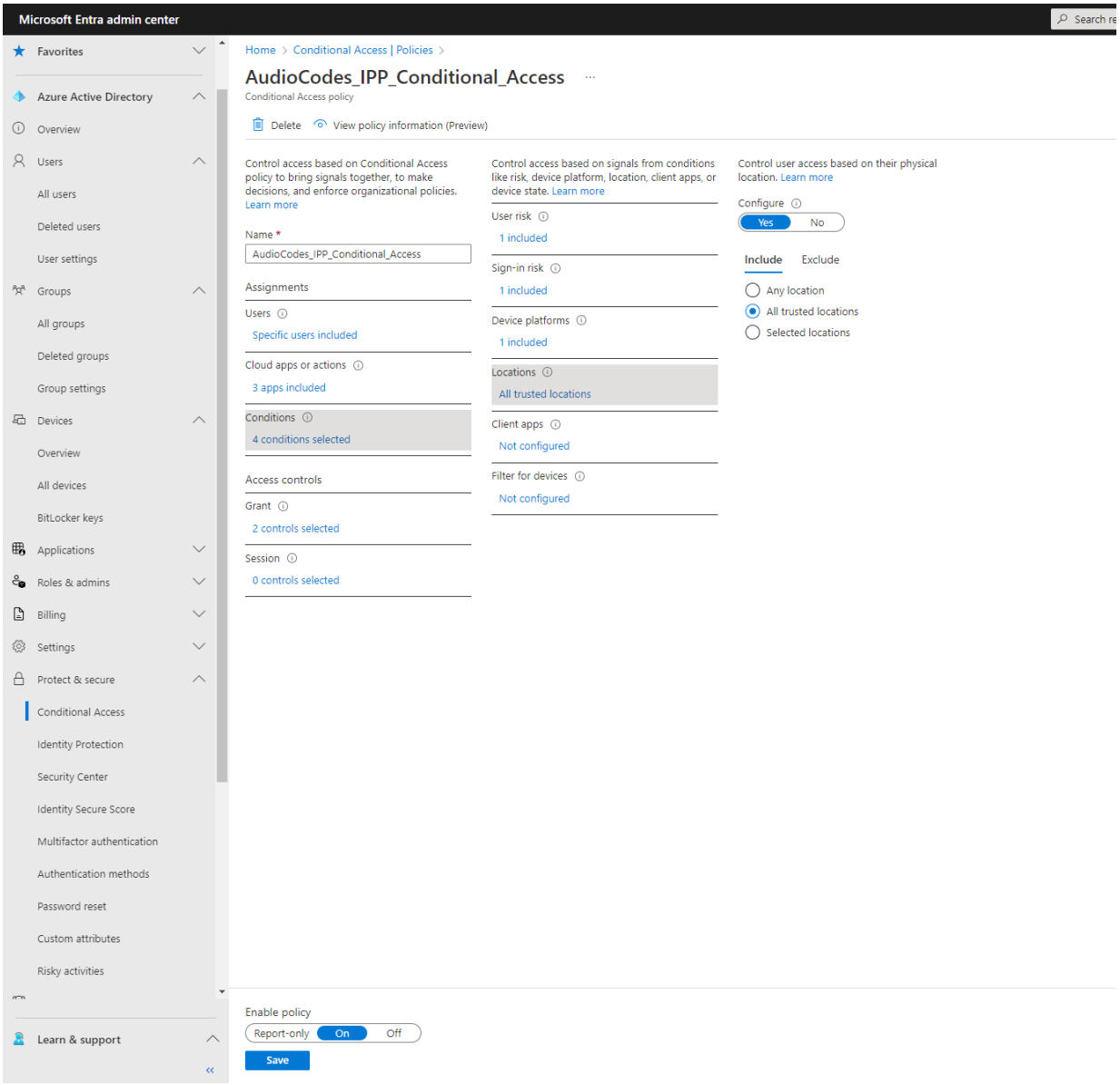


6.6 Select cloud apps

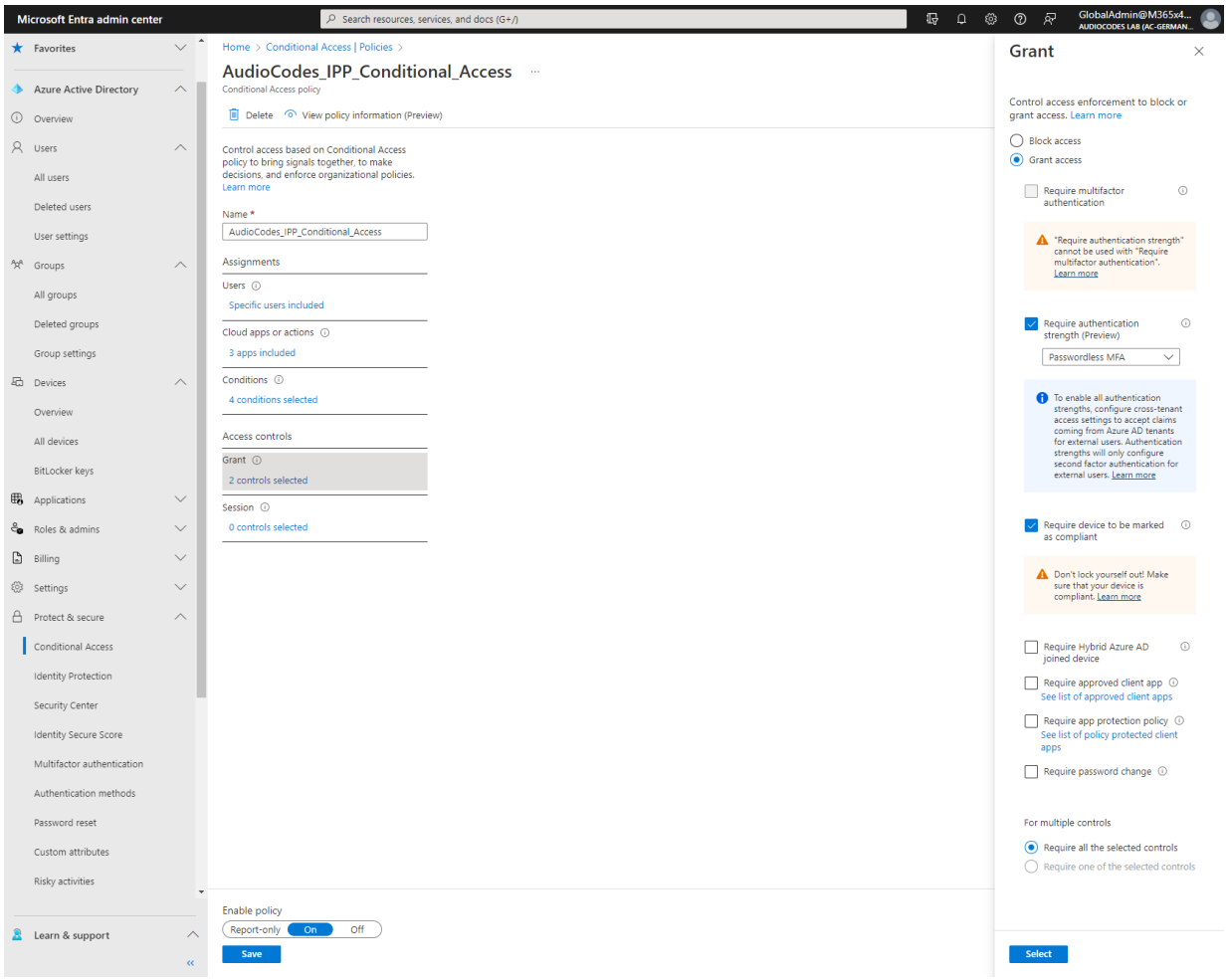


6.7 Select Device Platform



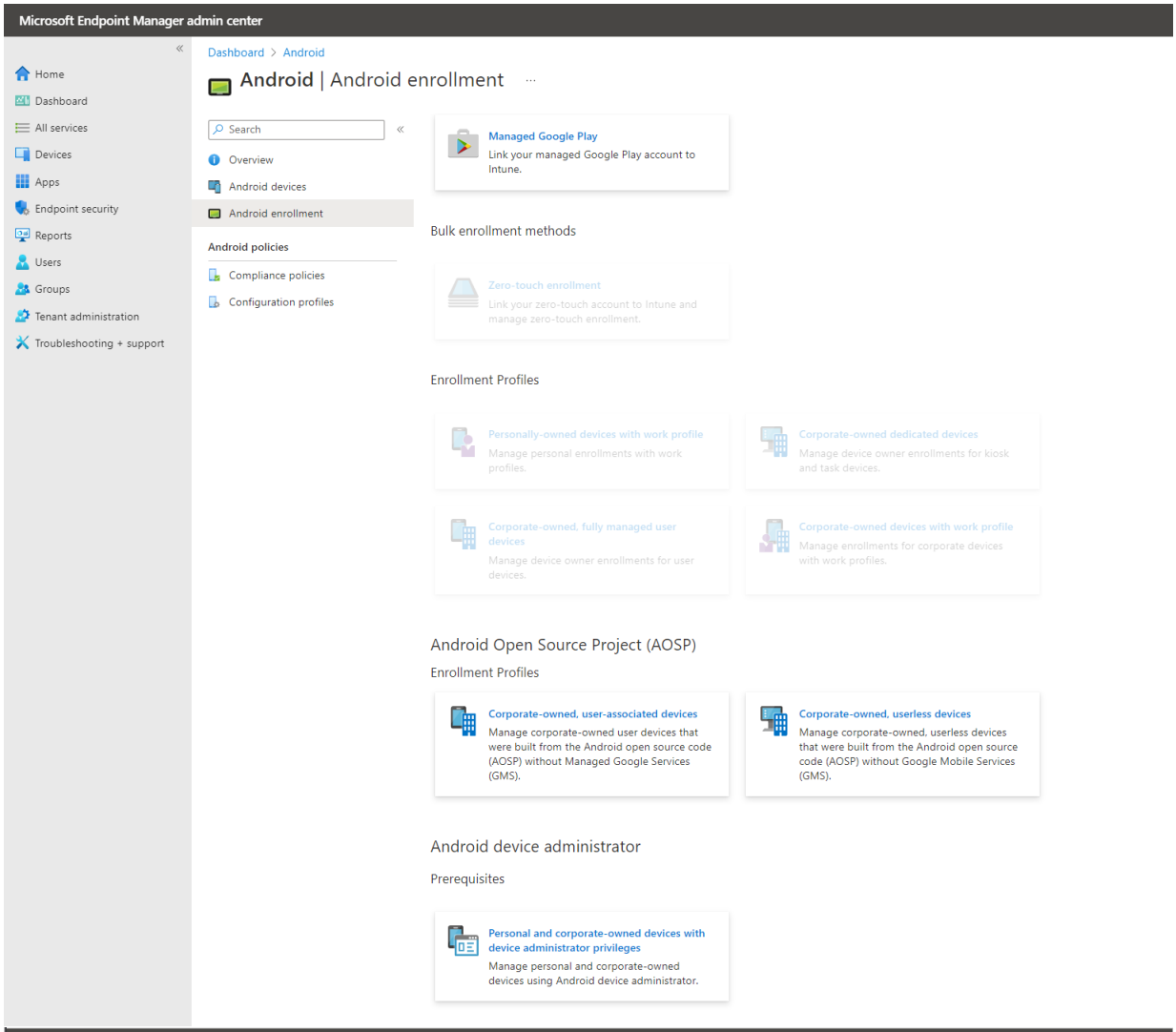

Microsoft Entra admin center
Search re
Favorites
Azure Active Directory
Overview
Users
All users
Deleted users
User settings
Groups
All groups
Deleted groups
Group settings
Devices
Overview
All devices
BitLocker keys
Applications
Roles & admins
Billing
Settings
Protect & secure
Conditional Access
Identity Protection
Security Center
Identity Secure Score
Multifactor authentication
Authentication methods
Password reset
Custom attributes
Risky activities
Learn & support
Home > Conditional Access | Policies >
AudioCodes_IPP_Conditional_Access
Conditional Access policy
Delete
View policy information (Preview)
Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. Learn more
Name *
AudioCodes_IPP_Conditional_Access
Assignments
Users
Specific users included
Cloud apps or actions
3 apps included
Conditions
4 conditions selected
Access controls
Grant
2 controls selected
Session
0 controls selected
Control access based on signals from conditions like risk, device platform, location, client apps, or device state. Learn more
User risk
1 included
Sign-in risk
1 included
Device platforms
1 included
Locations
All trusted locations
Client apps
Not configured
Filter for devices
Not configured
Control user access based on their physical location. Learn more
Configure
Yes
No
Include
Exclude
Any location
All trusted locations
Selected locations
Enable policy
Report-only
On
Off
Save

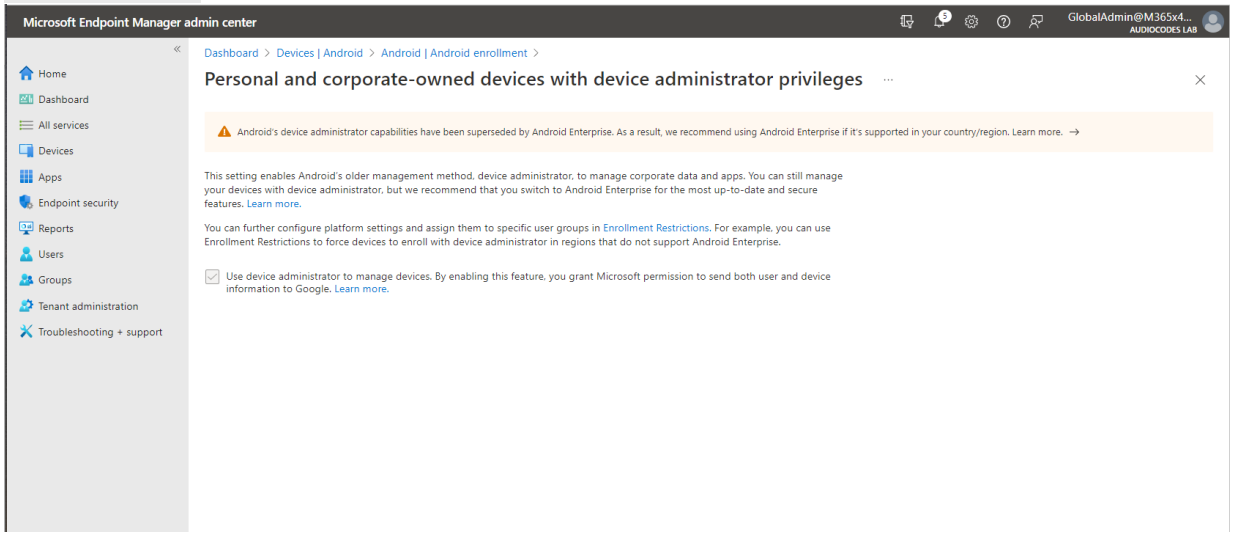
6.8 Grant access to devices which are marked as compliant.

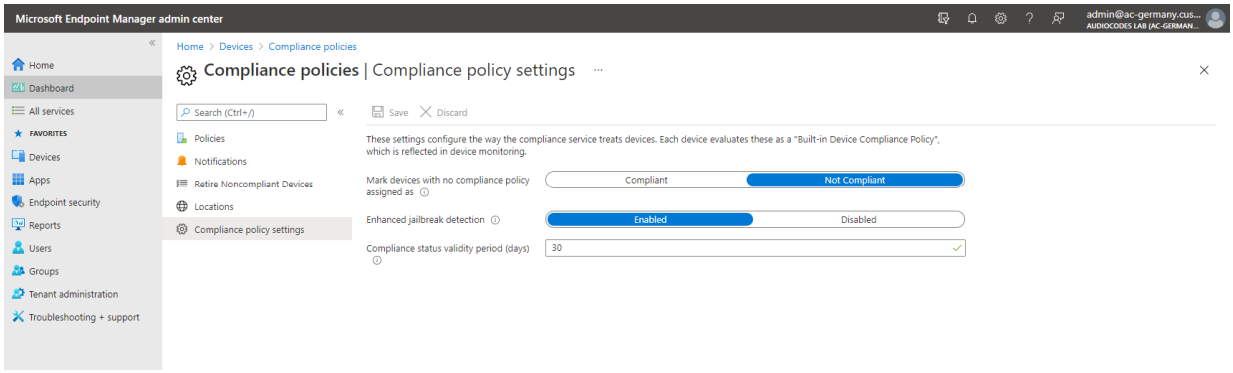


6.9 Compliance policy settings (Built-in Device Compliance Policy) in Endpoint Manager

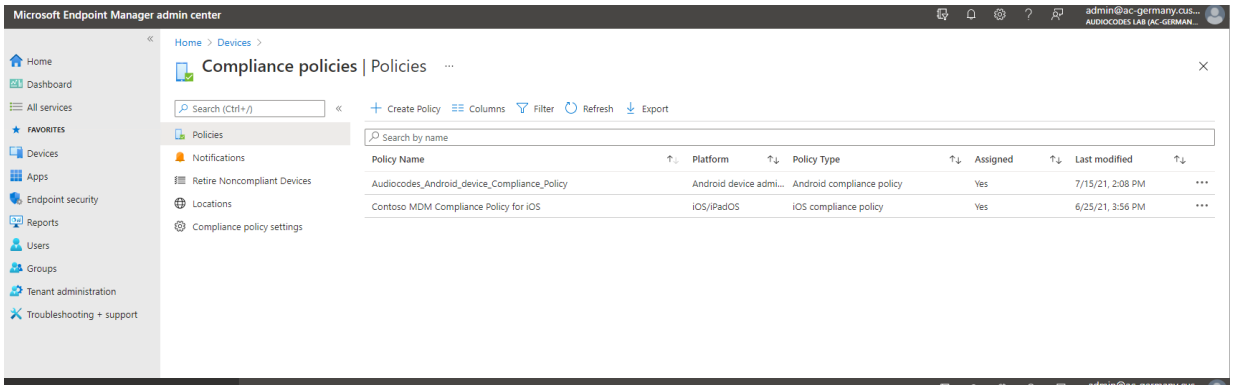
**Prerequisites: Enabled Android device administrator*

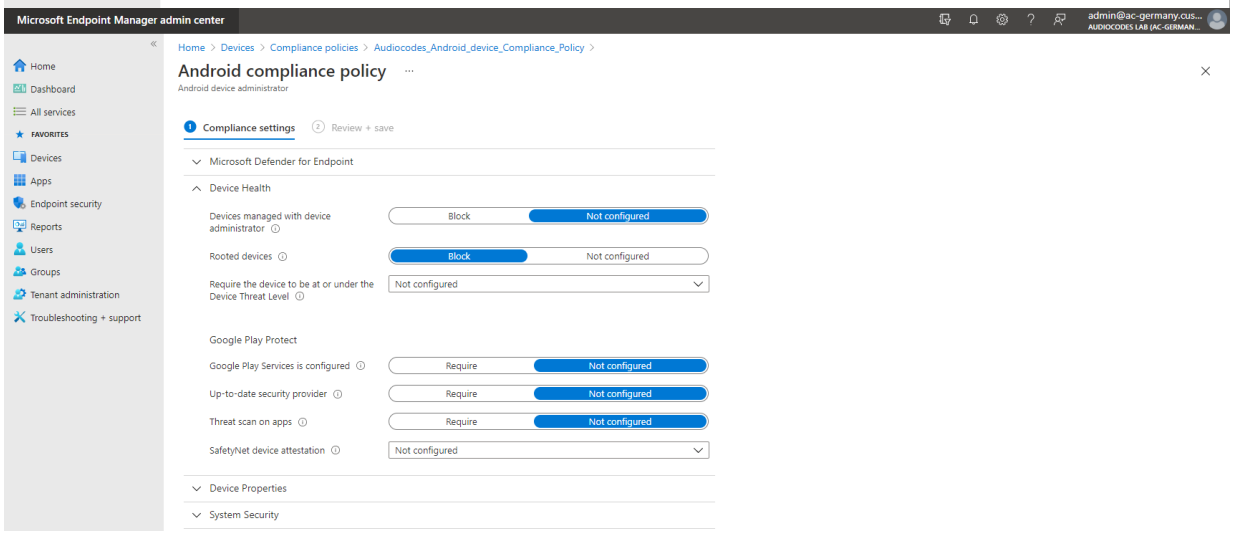

Microsoft Endpoint Manager admin center
Dashboard > Android
Android | Android enrollment
Home
Dashboard
All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Search
Overview
Android devices
Android enrollment
Android policies
Compliance policies
Configuration profiles
Managed Google Play
Link your managed Google Play account to Intune.
Bulk enrollment methods
Zero-touch enrollment
Link your zero-touch account to Intune and manage zero-touch enrollment.
Enrollment Profiles
Personally-owned devices with work profile
Manage personal enrollments with work profiles.
Corporate-owned dedicated devices
Manage device owner enrollments for kiosk and task devices.
Corporate-owned, fully managed user devices
Manage device owner enrollments for user devices.
Corporate-owned devices with work profile
Manage enrollments for corporate devices with work profiles.
Android Open Source Project (AOSP)
Enrollment Profiles
Corporate-owned, user-associated devices
Manage corporate-owned user devices that were built from the Android open source code (AOSP) without Managed Google Services (GMS).
Corporate-owned, userless devices
Manage corporate-owned, userless devices that were built from the Android open source code (AOSP) without Google Mobile Services (GMS).
Android device administrator
Prerequisites
Personal and corporate-owned devices with device administrator privileges
Manage personal and corporate-owned devices using Android device administrator.

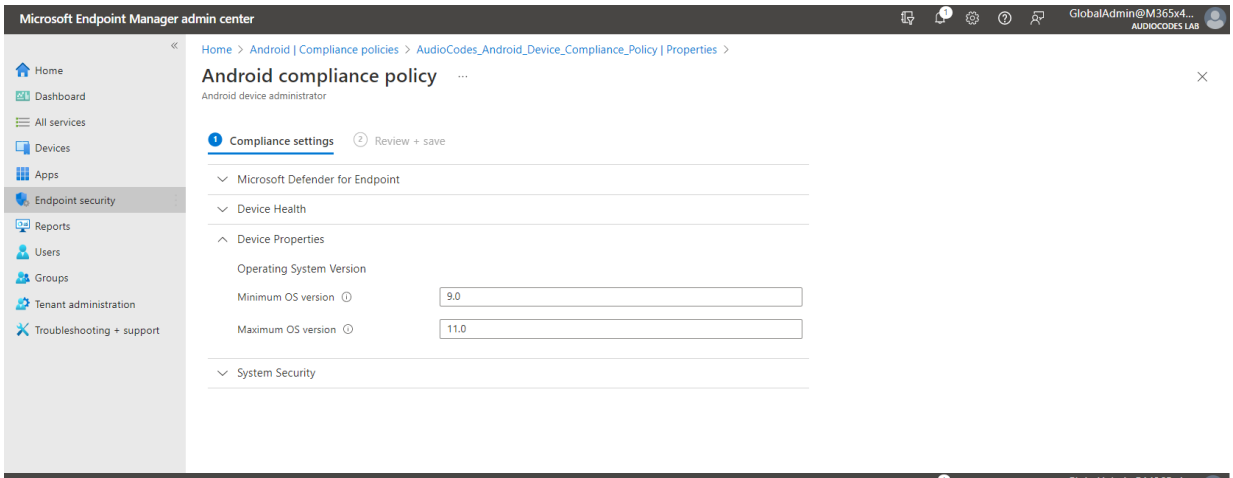

Microsoft Endpoint Manager admin center
GlobalAdmin@M365x4...
AUDIOCODES LAB
Dashboard > Devices | Android > Android | Android enrollment >
Personal and corporate-owned devices with device administrator privileges
Home
Dashboard
All services
Devices
Apps
Endpoint security
Reports
Users
Groups
Tenant administration
Troubleshooting + support
Android's device administrator capabilities have been superseded by Android Enterprise. As a result, we recommend using Android Enterprise if it's supported in your country/region. Learn more.
This setting enables Android's older management method, device administrator, to manage corporate data and apps. You can still manage your devices with device administrator, but we recommend that you switch to Android Enterprise for the most up-to-date and secure features. Learn more.
You can further configure platform settings and assign them to specific user groups in Enrollment Restrictions. For example, you can use Enrollment Restrictions to force devices to enroll with device administrator in regions that do not support Android Enterprise.
Use device administrator to manage devices. By enabling this feature, you grant Microsoft permission to send both user and device information to Google. Learn more.

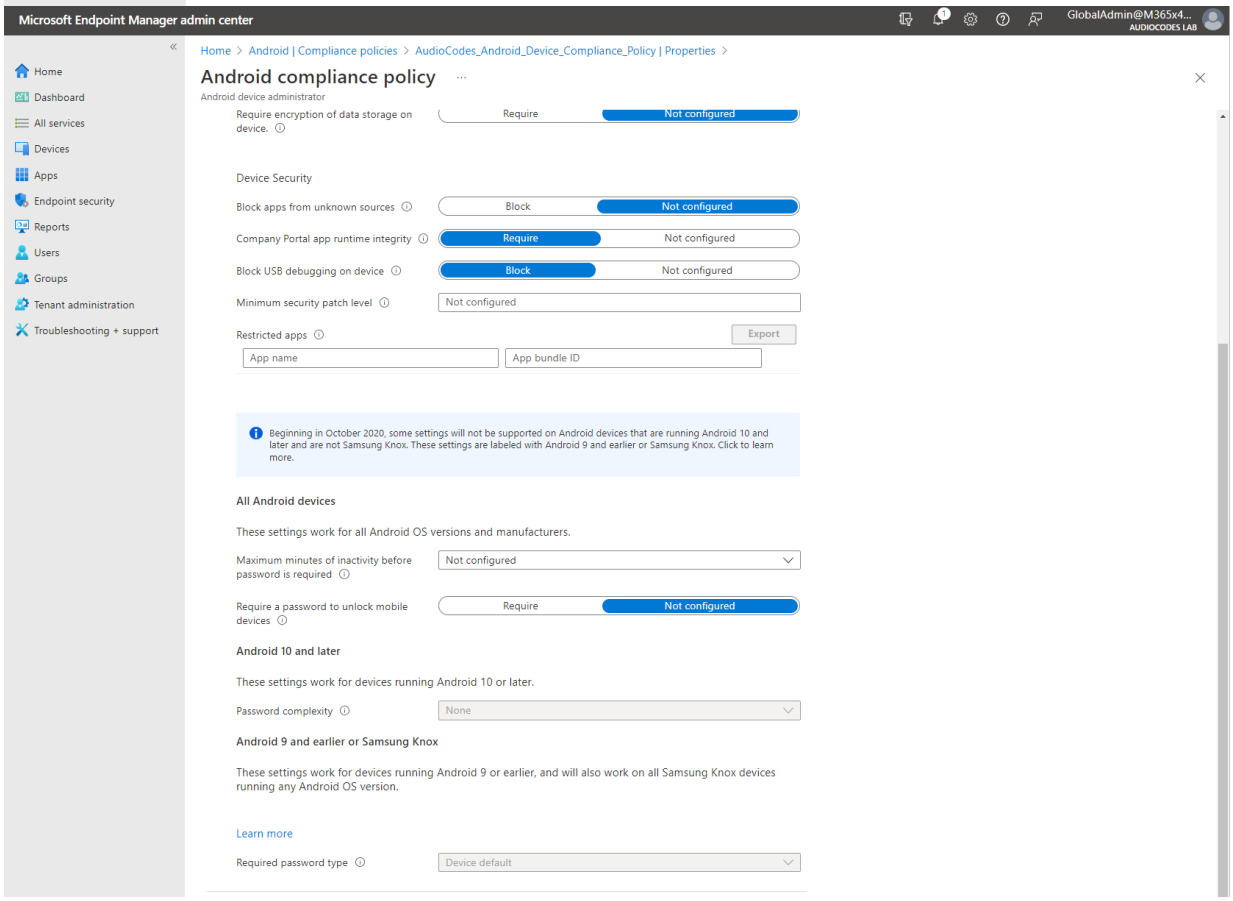


6.10 Creation of Compliance policy

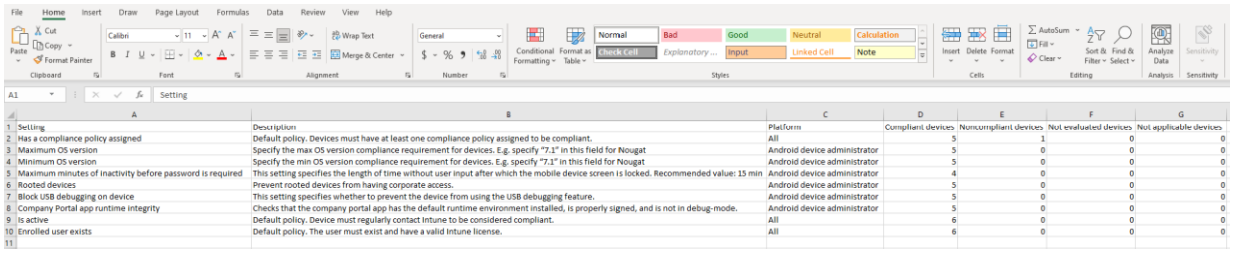






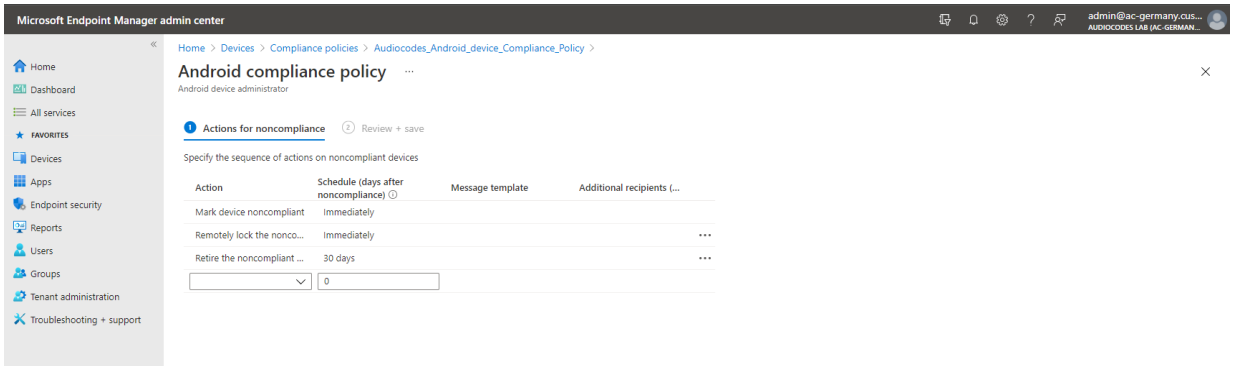


6.11 Overview Compliance settings

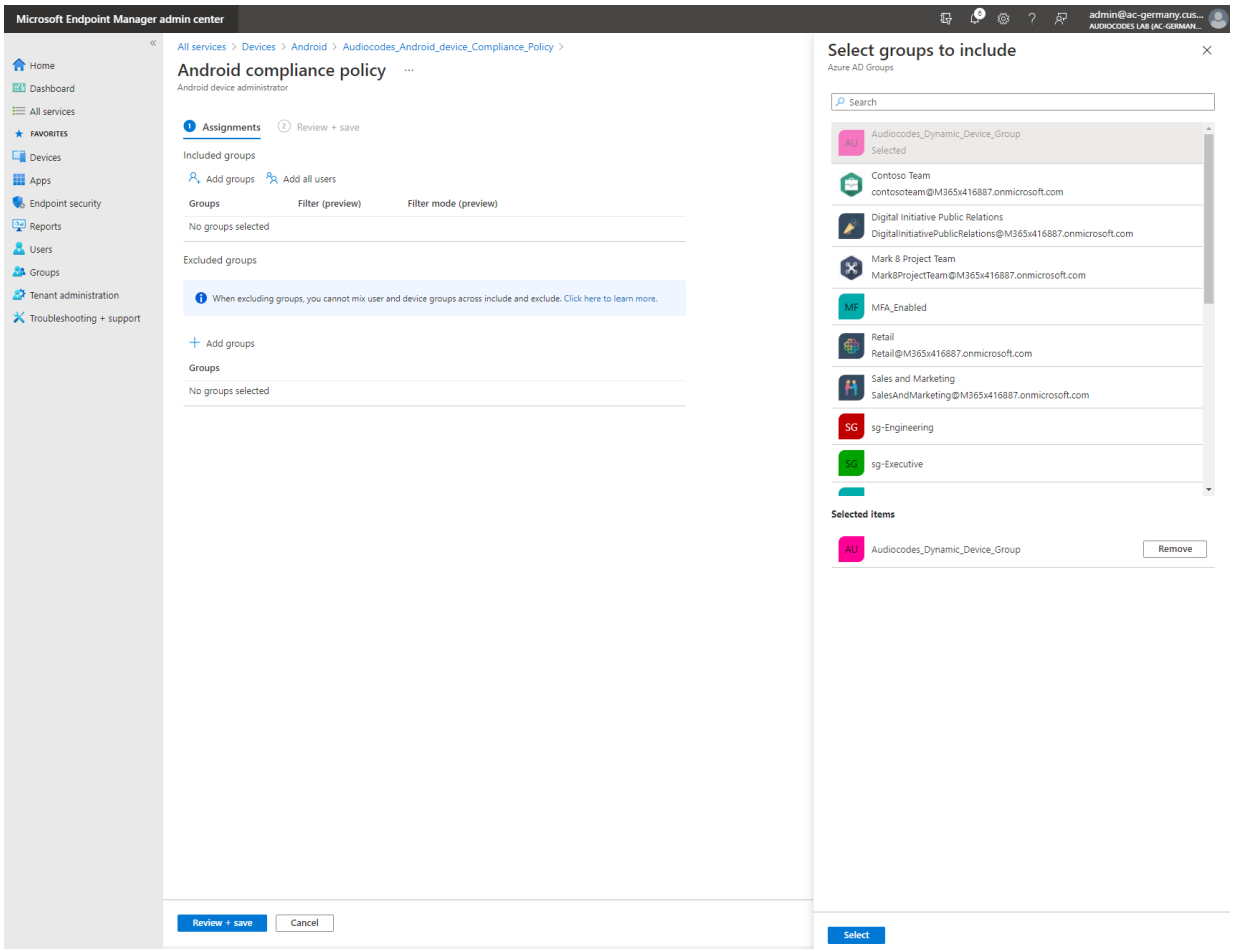


	A	B	C	D	E	F	G
1	Setting	Description	Platform	Compliant devices	Noncompliant devices	Not evaluated devices	Not applicable devices
2	Has a compliance policy assigned	Default policy. Devices must have at least one compliance policy assigned to be compliant.	All	5	1	0	0
3	Maximum OS version	Specify the max OS version compliance requirement for devices. E.g. specify "7.1" in this field for Nougat	Android device administrator	5	0	0	0
4	Minimum OS version	Specify the min OS version compliance requirement for devices. E.g. specify "7.1" in this field for Nougat	Android device administrator	5	0	0	0
5	Maximum minutes of inactivity before password is required	This setting specifies the length of time without user input after which the mobile device screen is locked. Recommended value: 15 min	Android device administrator	4	0	0	0
6	Rooted devices	Prevent rooted devices from having corporate access.	Android device administrator	5	0	0	0
7	Block USB debugging on device	This setting specifies whether to prevent the device from using the USB debugging feature.	Android device administrator	5	0	0	0
8	Company Portal app runtime integrity	Checks that the company portal app has the default runtime environment installed, is properly signed, and is not in debug-mode.	Android device administrator	5	0	0	0
9	Is active	Default policy. Device must regularly contact Intune to be considered compliant.	All	6	0	0	0
10	Enrolled user exists	Default policy. The user must exist and have a valid Intune license.	All	6	0	0	0

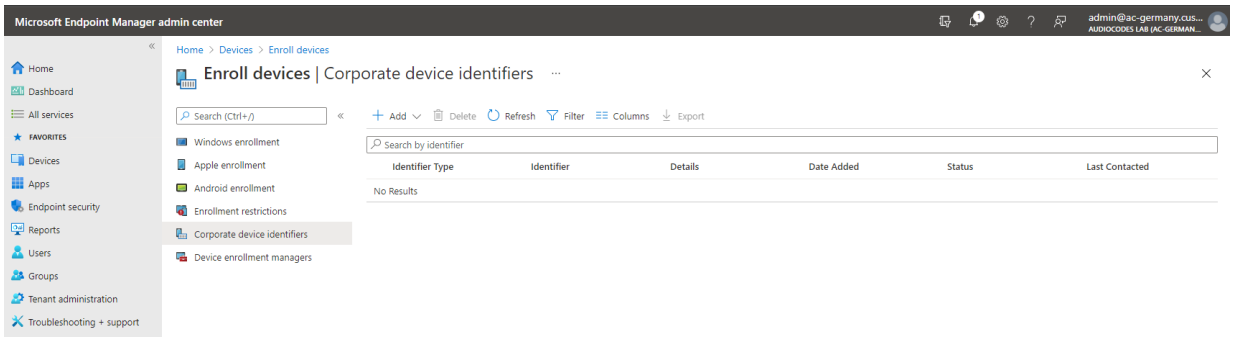
6.12 Actions for noncompliance devices

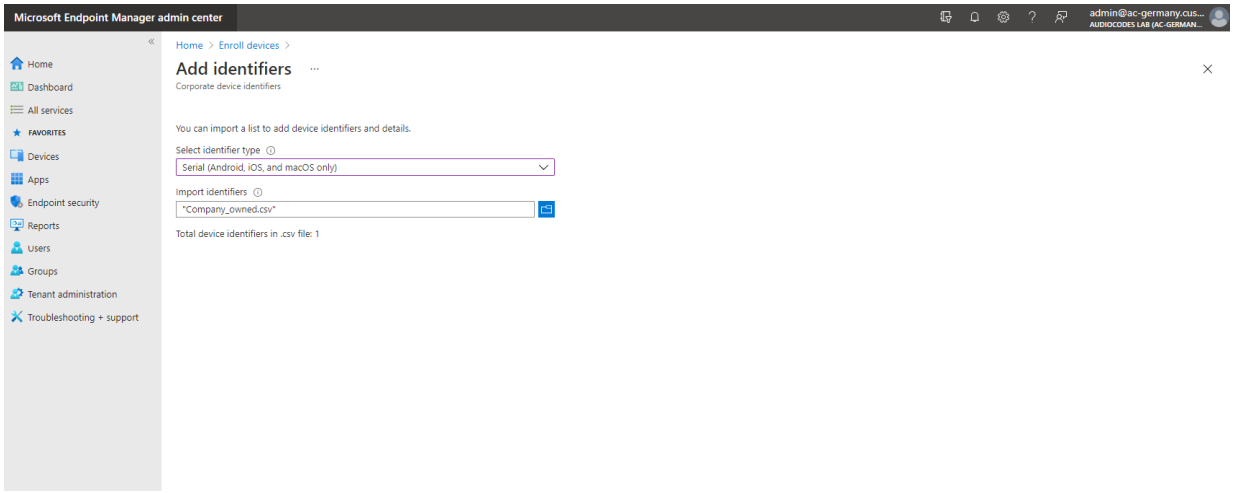


6.13 Assign Compliance Policy to group

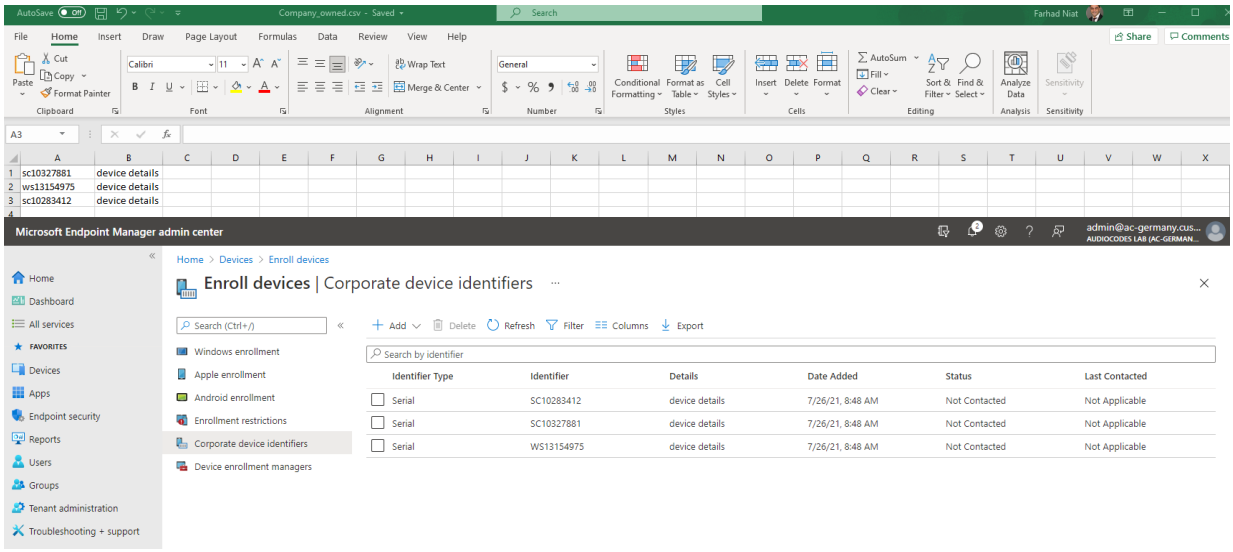


6.14 Identify devices as corporate-owned with serial number via Coporate device identifiers

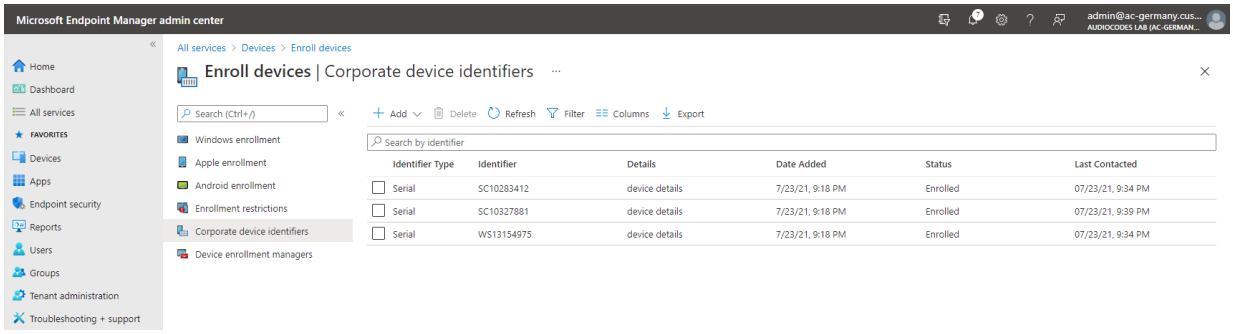




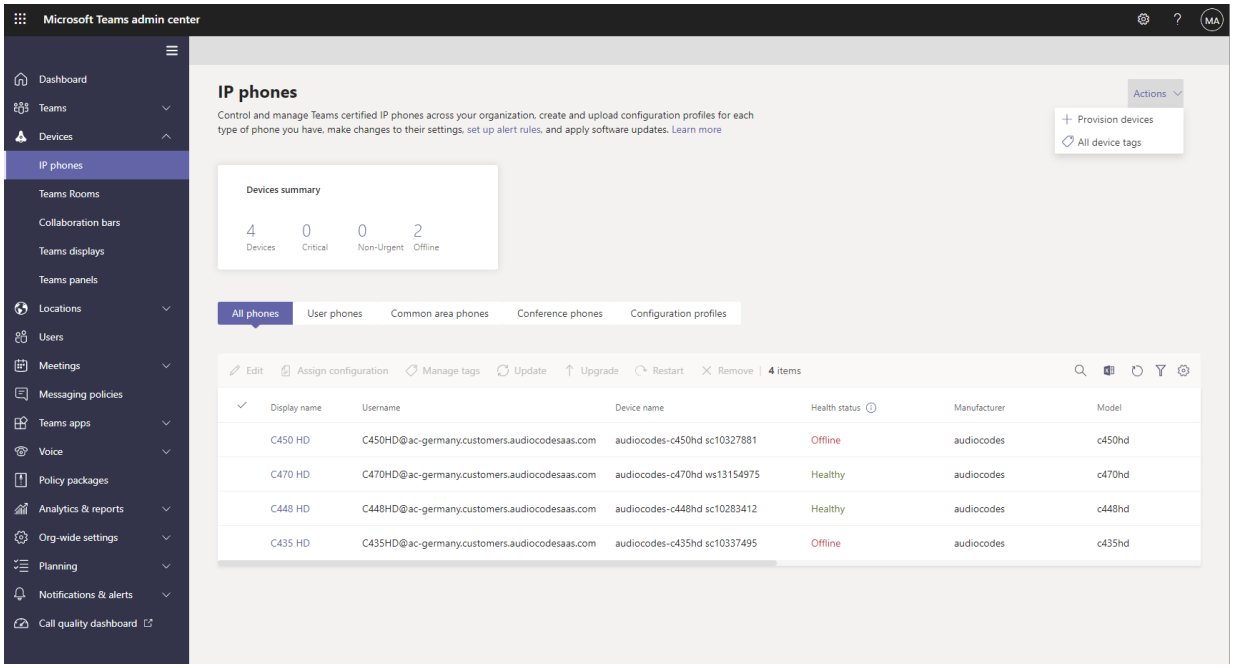
Upload CSV file with following format. Do not name the columns.



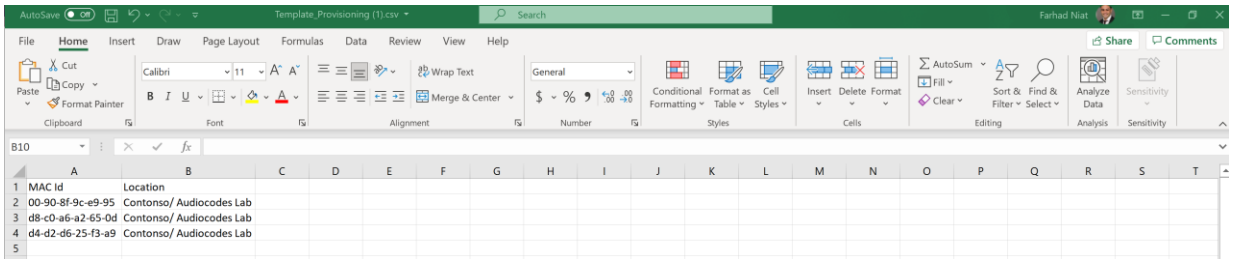
It can take up to 6 hours after sign in until devices are shown as Enrolled.

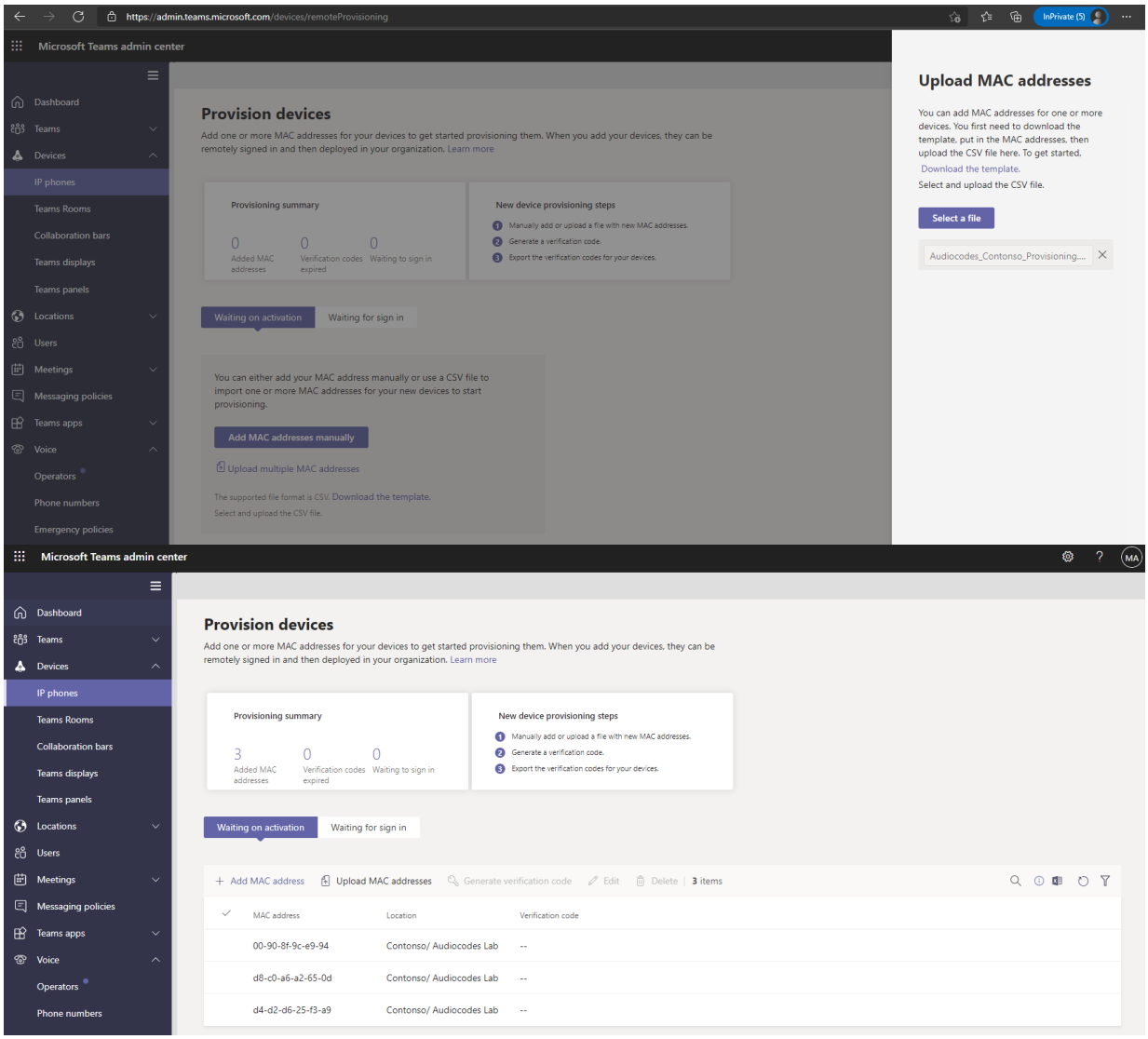


6.15 Provisioning devices via Teams Admin Center for initial Login in BULK

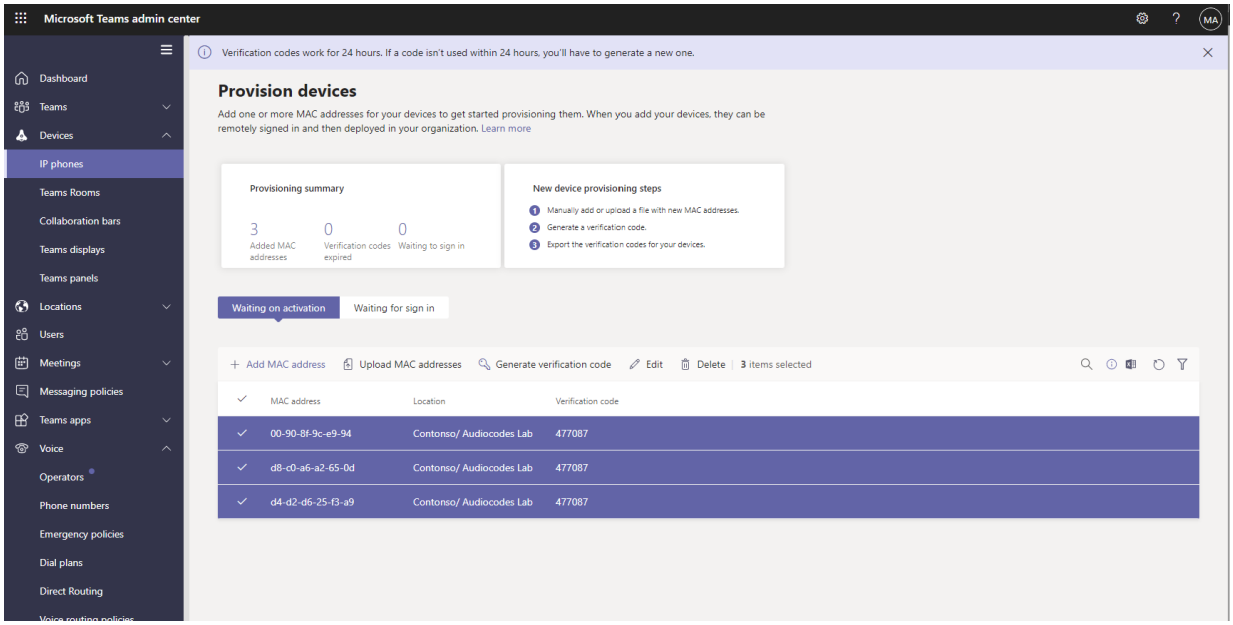


Click + Provision devices. Download the template. Put in MAC addresses and click Upload multiple MAC addresses.

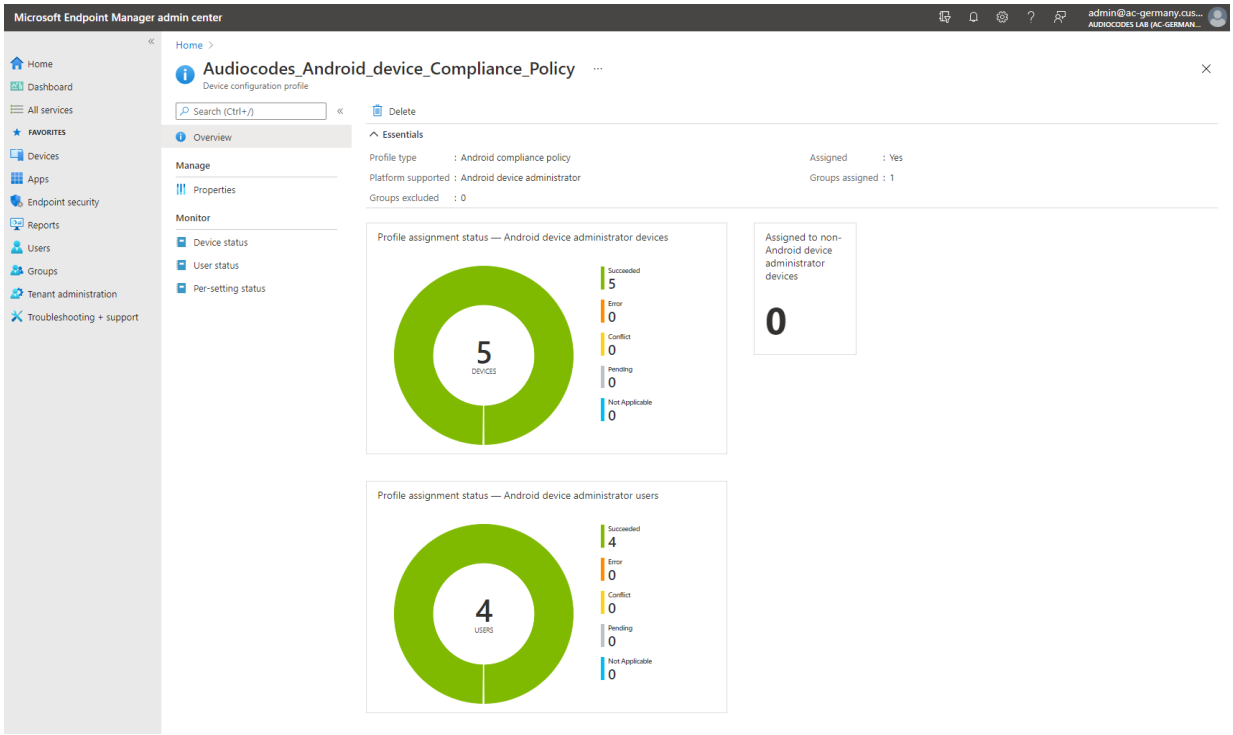


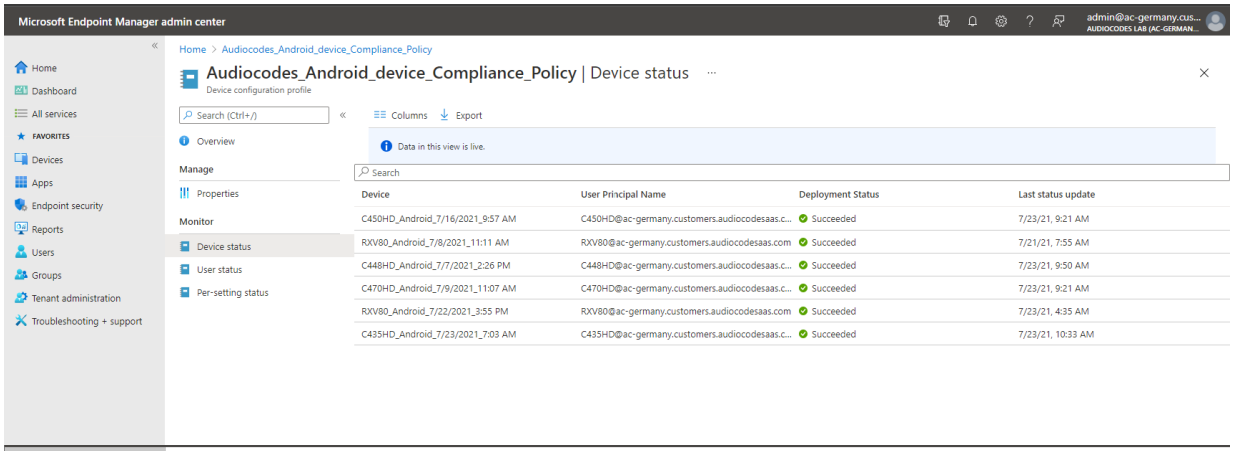

https://admin.teams.microsoft.com/devices/remoteProvisioning
Microsoft Teams admin center
Dashboard
Teams
Devices
IP phones
Teams Rooms
Collaboration bars
Teams displays
Teams panels
Locations
Users
Meetings
Messaging policies
Teams apps
Voice
Operators
Phone numbers
Emergency policies
Provision devices
Add one or more MAC addresses for your devices to get started provisioning them. When you add your devices, they can be remotely signed in and then deployed in your organization. Learn more
Provisioning summary
0
Added MAC addresses
0
Verification codes expired
0
Waiting to sign in
New device provisioning steps
Manually add or upload a file with new MAC addresses.
Generate a verification code.
Export the verification codes for your devices.
Waiting on activation
Waiting for sign in
You can either add your MAC address manually or use a CSV file to import one or more MAC addresses for your new devices to start provisioning.
Add MAC addresses manually
Upload multiple MAC addresses
The supported file format is CSV. Download the template.
Select and upload the CSV file.
Upload MAC addresses
You can add MAC addresses for one or more devices. You first need to download the template, put in the MAC addresses, then upload the CSV file here. To get started.
Download the template.
Select and upload the CSV file.
Select a file
Audiocodes_Contonso_Provisioning....
Microsoft Teams admin center
Dashboard
Teams
Devices
IP phones
Teams Rooms
Collaboration bars
Teams displays
Teams panels
Locations
Users
Meetings
Messaging policies
Teams apps
Voice
Operators
Phone numbers
Provision devices
Add one or more MAC addresses for your devices to get started provisioning them. When you add your devices, they can be remotely signed in and then deployed in your organization. Learn more
Provisioning summary
3
Added MAC addresses
0
Verification codes expired
0
Waiting to sign in
New device provisioning steps
Manually add or upload a file with new MAC addresses.
Generate a verification code.
Export the verification codes for your devices.
Waiting on activation
Waiting for sign in
Add MAC address
Upload MAC addresses
Generate verification code
Edit
Delete
3 items
MAC address
Location
Verification code
00-90-8f-9c-e9-94
Contonso/ Audiocodes Lab
--
d8-c0-a6-a2-65-0d
Contonso/ Audiocodes Lab
--
d4-d2-d6-25-f3-a9
Contonso/ Audiocodes Lab
--

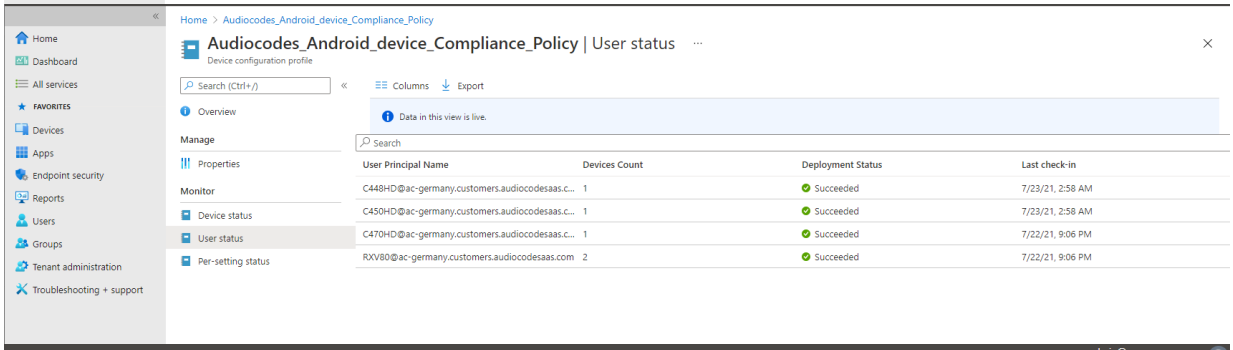
Select devices and click on Generate verification code. This is needed for first Login. (Verification codes works for 24 hours)

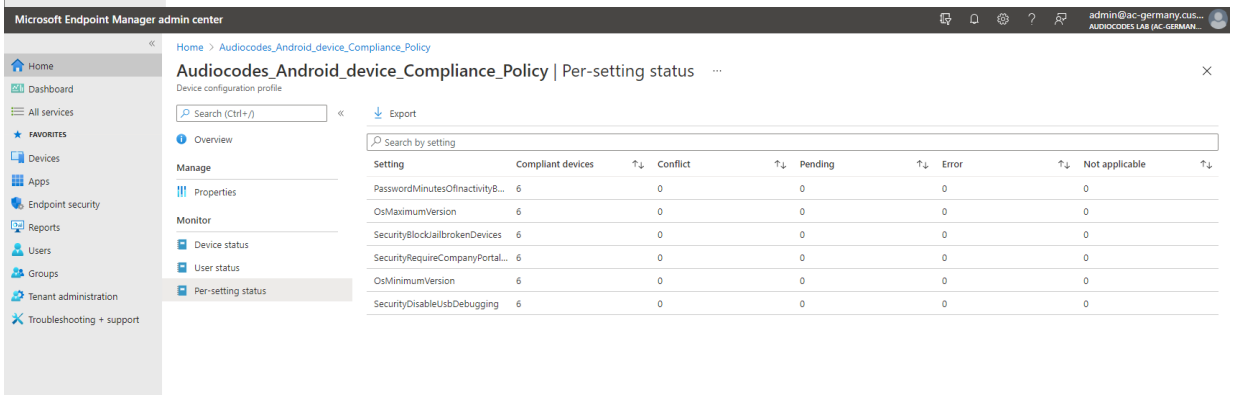


6.16 Monitoring of enrolled devices in Endpoint Manager









6.17 Monitoring of registered devices in AAD