

# **Enrollment of AudioCodes Phones and Collaboration Bars in Microsoft Endpoint Manager**

## **1.4**

## CONTENTS

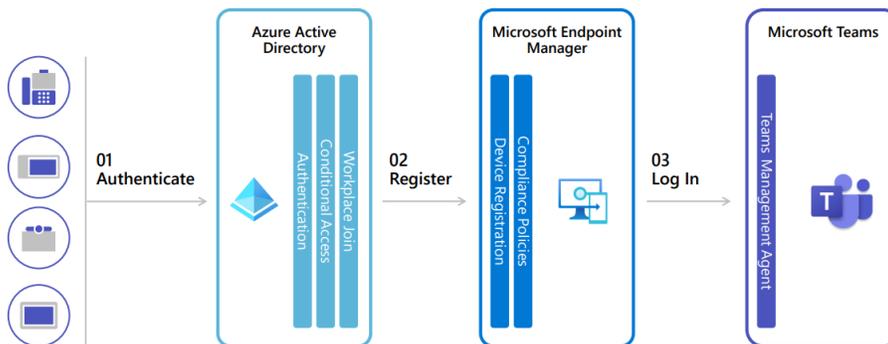
1.	Introduction .....	3
2.	Understanding device sign-in.....	3
3.	Understand sign-in flows .....	3
4.	User sign-in conditional access (Intune Compliance) .....	4
5.	Device enrollment.....	4
6.	Example configuration in AudioCodes lab environment .....	5
6.1	Creation of dynamic device group in AAD .....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

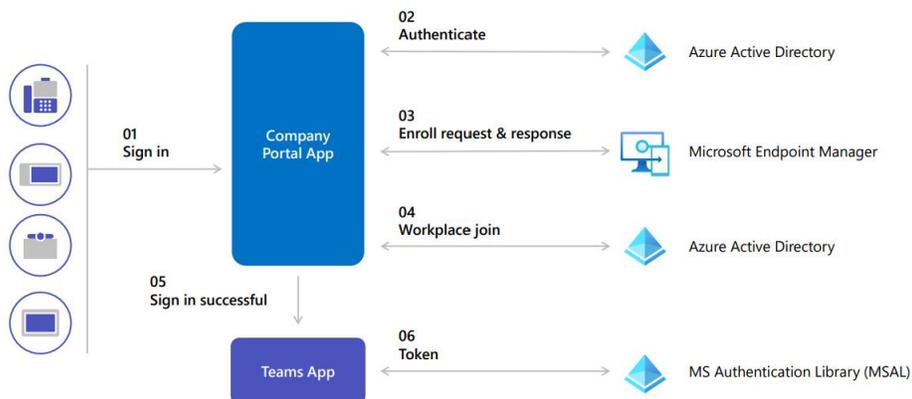
Please find a configuration summary how AudioCodes Phones and Collaboration Bars can be enrolled and managed via Microsoft Endpoint Manager. Keep in mind that not all settings which are available can be set within Endpoint Manager and/or Azure Active Directory. Currently no other settings are applicable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

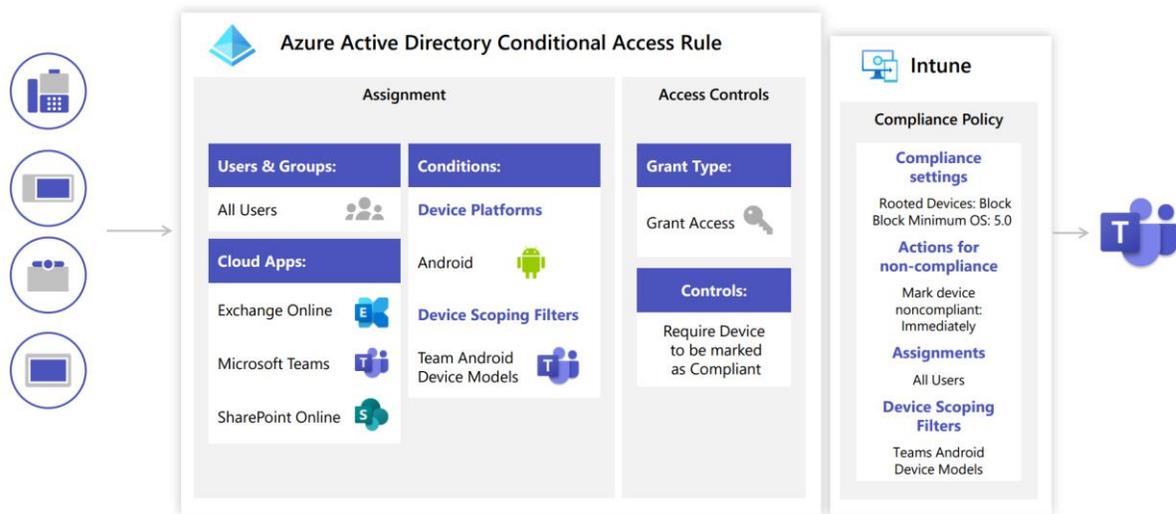
### Common area devices

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

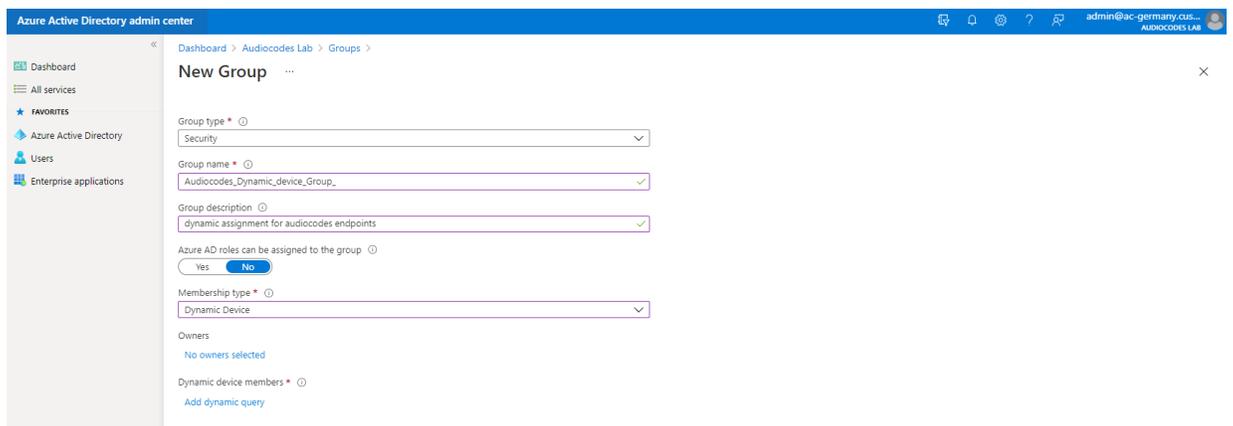
By default, users can only enroll up to 5 devices.  
 If using hotdesking, this number may need to be increased.  
 Consider any existing device type restrictions and if changes need to be made.

## Corporate Device Management

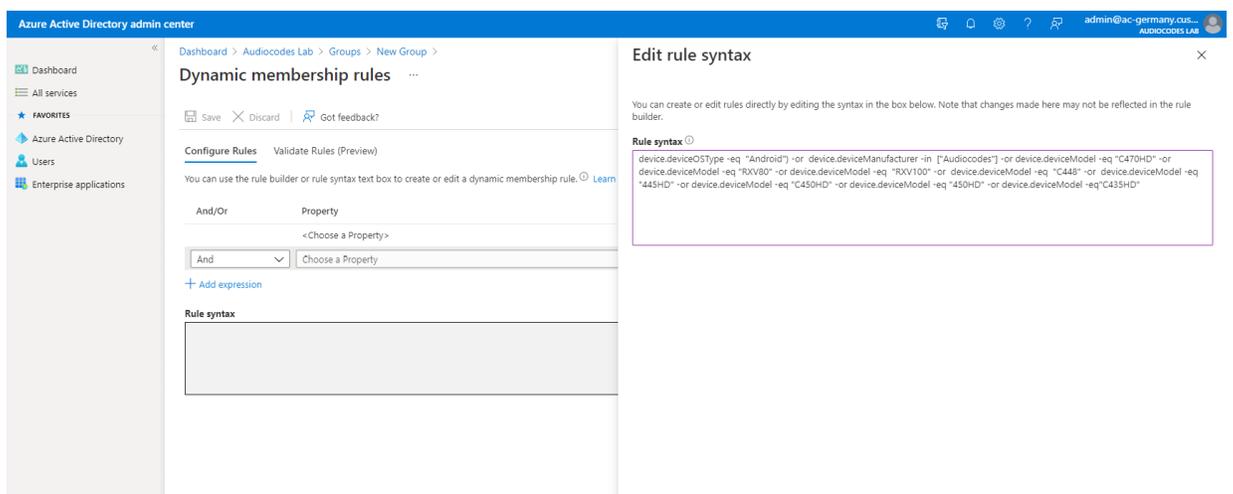
Importing device serial numbers into Microsoft Endpoint Manager lets you identify them as corporate devices identifiers. Ensures that only authorized devices are used.

## 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

The screenshot shows the 'Audiocodes\_Dynamic\_Device\_Group | Dynamic membership rules' page in the Azure Active Directory admin center. The 'Validate Rules (Preview)' tab is active, displaying a table of devices and their status relative to the rule.

**Rule syntax:**  
`(device.deviceOSType -eq "Android") -or device.deviceManufacturer -in ["Audiocodes"] -or device.deviceModel -eq "C470HD" -or device.deviceModel -eq "RXV80" -or device.deviceModel -eq "RXV100" -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"`

Name	Status
435_Android_7/8/2021_5:56 AM	In group
AudioCodesC435HD	In group
AudiocodesC448HD	In group
AudioCodesC470HD	In group
RXV80_Android_7/22/2021_3:55 PM	In group
C450HD_Android_7/16/2021_9:57 AM	In group

### 6.4 Creation of Conditional Access Policy in AAD

The screenshot shows the 'Conditional Access | Policies' page in the Azure Active Directory admin center. It displays a list of existing policies.

Policy Name	State	Creation Date	Modified Date
Exchange Online Requires Compliant Device	On	6/25/2021, 3:57:47 PM	7/12/2021, 10:50:17 AM
Office 365 App Control	On	6/25/2021, 3:57:54 PM	7/12/2021, 10:50:00 AM
Intune_Comppliance_Conditional_Access	On	7/6/2021, 12:04:15 PM	7/7/2021, 4:05:30 PM
MFA_Enabled_User	On	7/22/2021, 12:12:59 PM	

## 6.5 Assignment of conditional access policy to dynamic device group

The screenshot shows the Azure Active Directory admin center interface for configuring a Conditional Access policy named 'Intune\_Compliance\_Conditional\_Access'. The interface is divided into several sections:

- Name:** 'Intune\_Compliance\_Conditional\_Access'
- Assignments:**
  - Users and groups:** 'Specific users included' (expanded to show 3 apps included)
  - Cloud apps or actions:** '3 apps included'
  - Conditions:** '2 conditions selected'
  - Access controls:** '1 control selected'
  - Session:** '0 controls selected'
- Include/Exclude options:**
  - Include:**  Select users and groups
  - Exclude:**  All guest and external users,  Directory roles,  Users and groups
- Select:** '1 group' (expanded to show 'AU Audiocodes\_Dynamic\_Device\_...')
- Enable policy:** 'Report-only' mode, 'On' status

At the bottom, there is a 'Save' button.

## 6.6 Select cloud apps

Azure Active Directory admin center

Dashboard > Audiocodes Lab > Security > Conditional Access >

### Intune\_Compliance\_Conditional\_Access

Conditional Access policy

Delete

Control user access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Control user access based on all or specific cloud apps or actions. [Learn more](#)

Select what this policy applies to

Cloud apps

**Include** Exclude

None

All cloud apps

Select apps

Select

Microsoft Teams and 2 more

- Office 365 Exchange Online
- Office 365 SharePoint Online
- Microsoft Teams

**At least one of the apps selected is part of Office 365. We recommend setting the policy on the Office 365 app instead.**

Selecting SharePoint Online will also affect apps such as Microsoft Teams, Planner, Delve, MyAnalytics, and Newsfeed.

Selecting Office 365 Exchange Online will also affect apps such as OneDrive and Teams.

Enable policy

Report-only  On  Off

Save

## 6.7 Select Device Platform

**Azure Active Directory admin center**

Dashboard > Audiocodes Lab > Security > Conditional Access > Intune\_Compliance\_Conditional\_Access

### Intune\_Compliance\_Conditional\_Access

Conditional Access policy

Delete

Control user access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

**Name \***  
Intune\_Compliance\_Conditional\_Access

**Assignments**

Users and groups   
Specific users included

Cloud apps or actions   
3 apps included

**Conditions**   
2 conditions selected

**Access controls**

Grant   
1 control selected

Session   
0 controls selected

**User risk**   
Not configured

**Sign-in risk**   
Not configured

**Device platforms**   
1 included

**Locations**   
All trusted locations

**Client apps**   
Not configured

**Device state (Preview)**   
Not configured

**Filters for devices (Preview)**   
Not configured

**Enable policy**  
Report-only

Save

### Device platforms

Apply policy to selected device platforms. [Learn more](#)

Configure

**Include** **Exclude**

Any device

Select device platforms

Android

iOS

Windows Phone

Windows

macOS

Done

Microsoft Entra admin center Search

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](#)

Control access based on signals from conditions like risk, device platform, location, client apps, or device state. [Learn more](#)

Control user access based on their physical location. [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](#)

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](#)

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.

The screenshot shows the Microsoft Entra admin center interface for configuring a Conditional Access policy named "AudioCodes\_IPP\_Conditional\_Access". The policy is currently set to "Report-only" and is "On". The "Grant" section is expanded, showing the following settings:

- Control access enforcement to block or grant access:**
  - Block access
  - Grant access
- Require multifactor authentication:**
- Require authentication strength (Preview):**  (Dropdown: Passwordless MFA)
- Require device to be marked as compliant:**  (Warning: "Don't lock yourself out! Make sure that your device is compliant.")
- Require Hybrid Azure AD joined device:**
- Require approved client app:**  (See list of approved client apps)
- Require app protection policy:**  (See list of policy protected client apps)
- Require password change:**

**For multiple controls:**

- Require all the selected controls
- Require one of the selected controls

At the bottom, the "Enable policy" toggle is set to "On", and a "Save" button is visible.

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

*\*Prerequisites: Enabled Android device administrator*

- Home
- Dashboard
- All services
- Devices
- Apps
- Endpoint security
- Reports
- Users
- Groups
- Tenant administration
- Troubleshooting + support

Dashboard > Android

## Android | Android enrollment

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.

- Home
- Dashboard
- All services
- Devices
- Apps
- Endpoint security
- Reports
- Users
- Groups
- Tenant administration
- Troubleshooting + support

Dashboard > Devices | Android > Android | Android enrollment

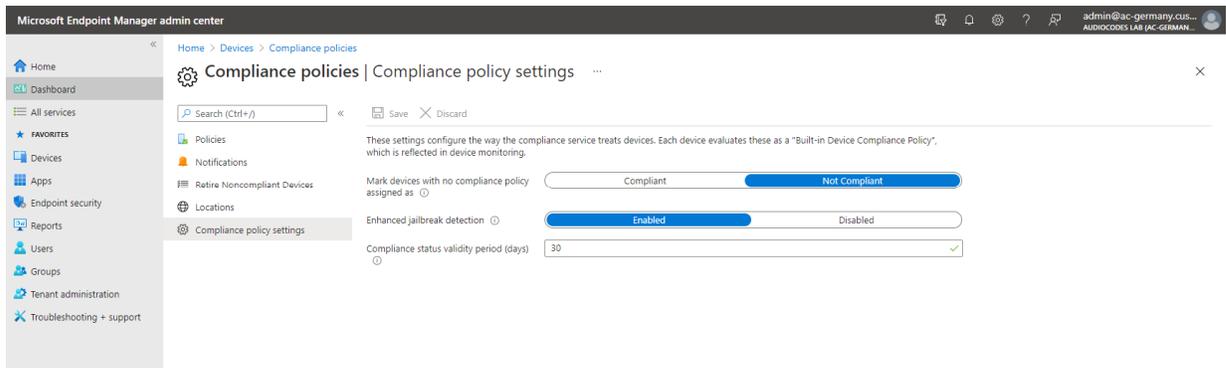
## Personal and corporate-owned devices with device administrator privileges

⚠️ 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.](#) →

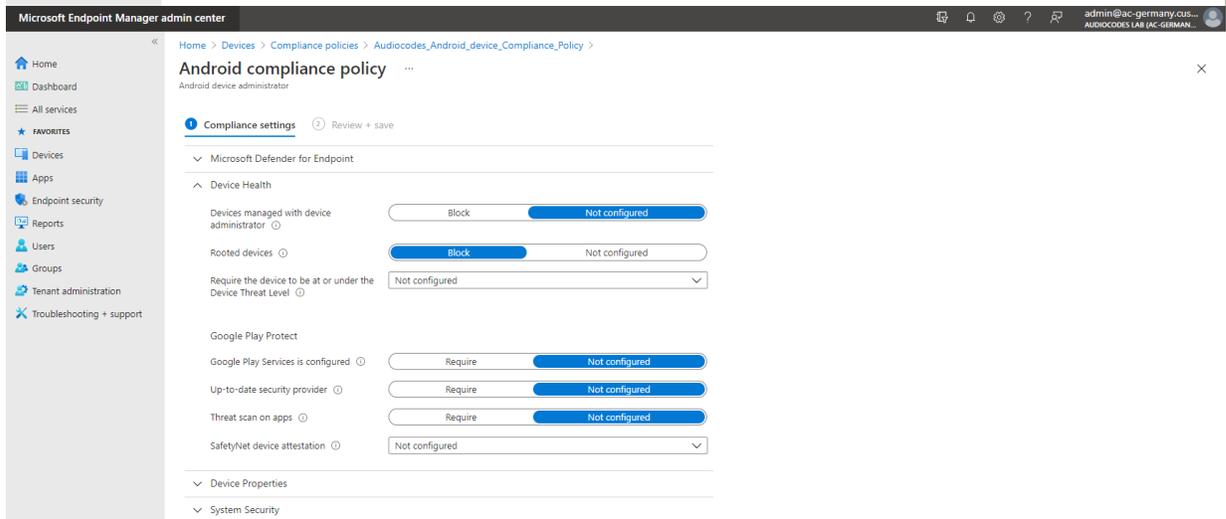
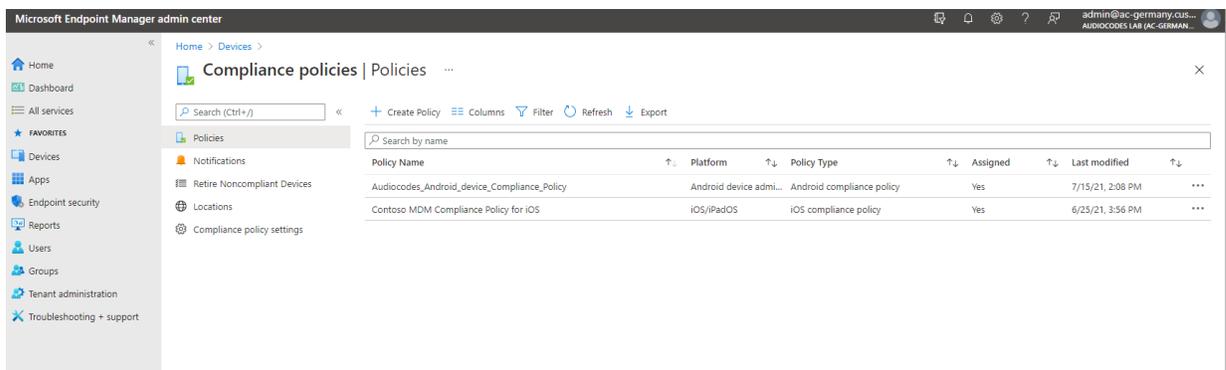
This setting enables Android's older management method, device administrator, to manage corporate data and apps. You can still manage your devices with device administrator, but we recommend that you switch to Android Enterprise for the most up-to-date and secure features. [Learn more.](#)

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



Microsoft Endpoint Manager admin center

Home > Android | Compliance policies > AudioCodes\_Android\_Device\_Compliance\_Policy | Properties >

## Android compliance policy

Android device administrator

**Compliance settings** Review + save

- Microsoft Defender for Endpoint
- Device Health
- Device Properties
  - Operating System Version
    - Minimum OS version
    - Maximum OS version
- System Security

Microsoft Endpoint Manager admin center

Home > Android | Compliance policies > AudioCodes\_Android\_Device\_Compliance\_Policy | Properties >

## Android compliance policy

Android device administrator

Require encryption of data storage on device.   Not configured

Device Security

Block apps from unknown sources   Not configured

Company Portal app runtime integrity  Require  Not configured

Block USB debugging on device  Block  Not configured

Minimum security patch level

Restricted apps

App name  App bundle ID

**!** Beginning in October 2020, some settings will not be supported on Android devices that are running Android 10 and later and are not Samsung Knox. These settings are labeled with Android 9 and earlier or Samsung Knox. Click to learn more.

**All Android devices**

These settings work for all Android OS versions and manufacturers.

Maximum minutes of inactivity before password is required

Require a password to unlock mobile devices   Not configured

**Android 10 and later**

These settings work for devices running Android 10 or later.

Password complexity

**Android 9 and earlier or Samsung Knox**

These settings work for devices running Android 9 or earlier, and will also work on all Samsung Knox devices running any Android OS version.

[Learn more](#)

Required password type

## 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
11							

## 6.12 Actions for noncompliance devices

Microsoft Endpoint Manager admin center

Home > Devices > Compliance policies > Audiocodes\_Android\_device\_Compliance\_Policy >

### Android compliance policy

Android device administrator

1 Actions for noncompliance (2) Review + save

Specify the sequence of actions on noncompliant devices

Action	Schedule (days after noncompliance)	Message template	Additional recipients (...)
Mark device noncompliant	Immediately		
Remotely lock the nonco...	Immediately		...
Retire the noncompliant ...	30 days		...

## 6.13 Assign Compliance Policy to group

Microsoft Endpoint Manager admin center

All services > Devices > Android > Audiocodes\_Android\_device\_Compliance\_Policy >

### Android compliance policy

Android device administrator

**Assignments** Review + save

Included groups

Add groups Add all users

Groups Filter (preview) Filter mode (preview)

No groups selected

Excluded groups

When excluding groups, you cannot mix user and device groups across include and exclude. Click here to learn more.

+ Add groups

Groups

No groups selected

**Select groups to include**

Azure AD Groups

Search

- AU** Audiocodes\_Dynamic\_Device\_Group Selected
- CT** Contoso Team contosoteam@M365x416887.onmicrosoft.com
- DI** Digital Initiative Public Relations DigitalInitiativePublicRelations@M365x416887.onmicrosoft.com
- MP** Mark & Project Team Mark&ProjectTeam@M365x416887.onmicrosoft.com
- MF** MFA\_Enabled
- RE** Retail Retail@M365x416887.onmicrosoft.com
- SM** Sales and Marketing SalesAndMarketing@M365x416887.onmicrosoft.com
- SG** sg-Engineering
- SE** sg-Executive

**Selected items**

- AU** Audiocodes\_Dynamic\_Device\_Group Remove

Review + save Cancel

Select

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

Microsoft Endpoint Manager admin center

Home > Devices > Enroll devices

### Enroll devices | Corporate device identifiers

Search (Ctrl+) Add Delete Refresh Filter Columns Export

- Windows enrollment
- Apple enrollment
- Android enrollment
- Enrollment restrictions
- Corporate device identifiers**
- Device enrollment managers

Search by identifier

Identifier Type	Identifier	Details	Date Added	Status	Last Contacted
No Results					

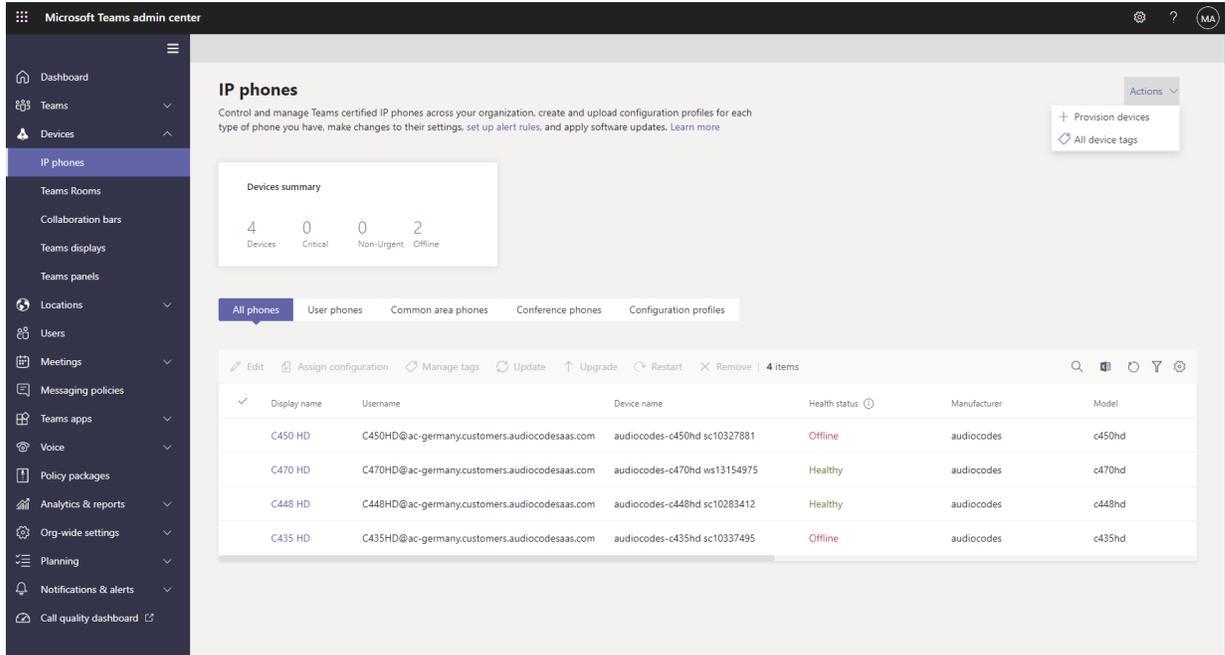
Upload CSV file with following format. Do not name the columns.

Identifier Type	Identifier	Details	Date Added	Status	Last Contacted
<input type="checkbox"/> Serial	SC10283412	device details	7/26/21, 8:48 AM	Not Contacted	Not Applicable
<input type="checkbox"/> Serial	SC10327881	device details	7/26/21, 8:48 AM	Not Contacted	Not Applicable
<input type="checkbox"/> Serial	WS13154975	device details	7/26/21, 8:48 AM	Not Contacted	Not Applicable

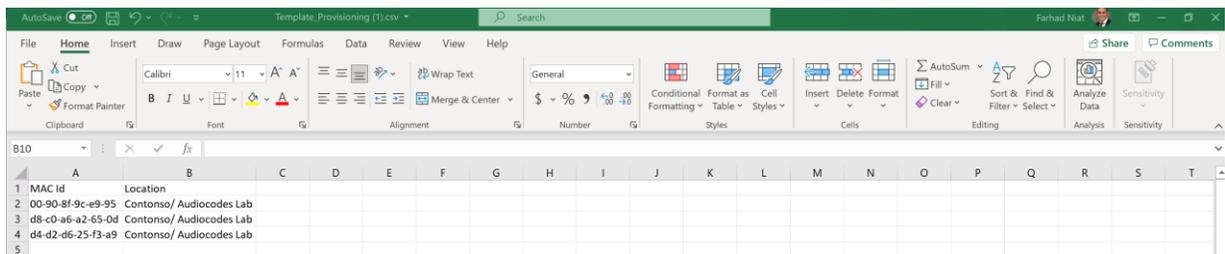
It can take up to 6 hours after sign in until devices are shown as Enrolled.

Identifier Type	Identifier	Details	Date Added	Status	Last Contacted
<input type="checkbox"/> Serial	SC10283412	device details	7/23/21, 9:18 PM	Enrolled	07/23/21, 9:34 PM
<input type="checkbox"/> Serial	SC10327881	device details	7/23/21, 9:18 PM	Enrolled	07/23/21, 9:39 PM
<input type="checkbox"/> Serial	WS13154975	device details	7/23/21, 9:18 PM	Enrolled	07/23/21, 9:34 PM

## 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.



Microsoft Teams admin center

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**

- 1 Manually add or upload a file with new MAC addresses.
- 2 Generate a verification code.
- 3 Export the verification codes for your devices.

**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... X

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.

Microsoft Teams admin center

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**

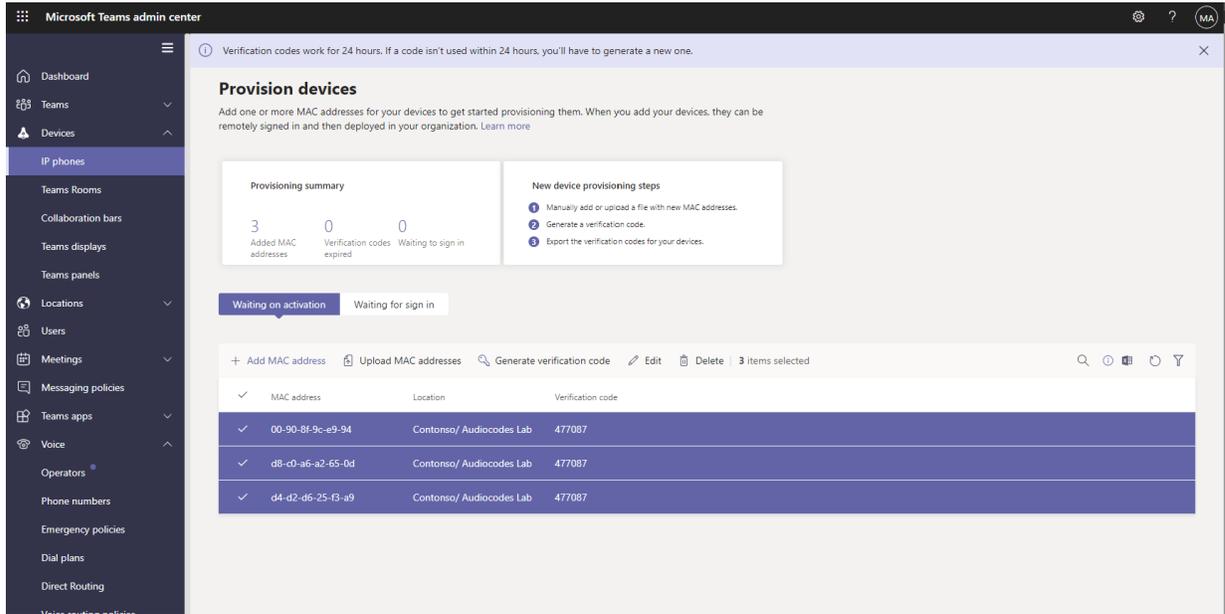
- 1 Manually add or upload a file with new MAC addresses.
- 2 Generate a verification code.
- 3 Export the verification codes for your devices.

Waiting on activation    Waiting for sign in

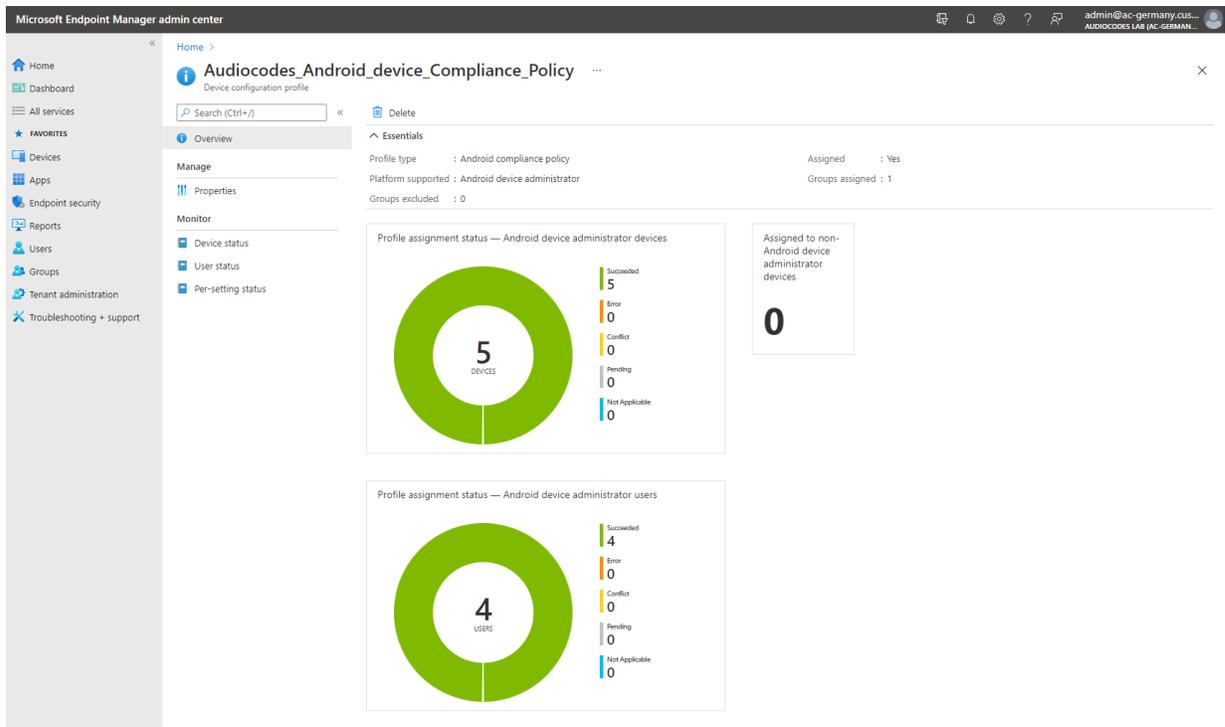
+ Add MAC address    Upload MAC addresses    Generate verification code    Edit    Delete | 3 items

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



Microsoft Endpoint Manager admin center

Home > Audiocodes\_Android\_device\_Compliance\_Policy

### Audiocodes\_Android\_device\_Compliance\_Policy | Device status

Device configuration profile

Search (Ctrl+/) Columns Export

Overview: Data in this view is live.

Manage: Search

Device	User Principal Name	Deployment Status	Last status update
C450HD_Android_7/16/2021_9:57 AM	C450HD@ac-germany.customers.audiocodesaas.c...	Succeeded	7/23/21, 9:21 AM
RXV80_Android_7/8/2021_11:11 AM	RXV80@ac-germany.customers.audiocodesaas.com	Succeeded	7/21/21, 7:55 AM
C448HD_Android_7/7/2021_2:26 PM	C448HD@ac-germany.customers.audiocodesaas.c...	Succeeded	7/23/21, 9:50 AM
C470HD_Android_7/9/2021_1:107 AM	C470HD@ac-germany.customers.audiocodesaas.c...	Succeeded	7/23/21, 9:21 AM
RXV80_Android_7/22/2021_3:55 PM	RXV80@ac-germany.customers.audiocodesaas.com	Succeeded	7/23/21, 4:35 AM
C435HD_Android_7/23/2021_7:03 AM	C435HD@ac-germany.customers.audiocodesaas.c...	Succeeded	7/23/21, 10:33 AM

Microsoft Endpoint Manager admin center

Home > Audiocodes\_Android\_device\_Compliance\_Policy

### Audiocodes\_Android\_device\_Compliance\_Policy | User status

Device configuration profile

Search (Ctrl+/) Columns Export

Overview: Data in this view is live.

Manage: Search

User Principal Name	Devices Count	Deployment Status	Last check-in
C448HD@ac-germany.customers.audiocodesaas.c...	1	Succeeded	7/23/21, 2:58 AM
C450HD@ac-germany.customers.audiocodesaas.c...	1	Succeeded	7/23/21, 2:58 AM
C470HD@ac-germany.customers.audiocodesaas.c...	1	Succeeded	7/22/21, 9:06 PM
RXV80@ac-germany.customers.audiocodesaas.com	2	Succeeded	7/22/21, 9:06 PM

Microsoft Endpoint Manager admin center

Home > Audiocodes\_Android\_device\_Compliance\_Policy

### Audiocodes\_Android\_device\_Compliance\_Policy | Per-setting status

Device configuration profile

Search (Ctrl+/) Export

Overview: Search by setting

Setting	Compliant devices	Conflict	Pending	Error	Not applicable
PasswordMinutesOfInactivity8...	6	0	0	0	0
OsMaximumVersion	6	0	0	0	0
SecurityBlockAllBrokenDevices	6	0	0	0	0
SecurityRequireCompanyPortal...	6	0	0	0	0
OsMinimumVersion	6	0	0	0	0
SecurityDisableUsbDebugging	6	0	0	0	0

## 6.17 Monitoring of registered devices in AAD

Azure Active Directory admin center

Dashboard > Audiocodes Lab >

### Devices | All devices

Audiocodes Lab - Azure Active Directory

Enable Disable Delete Manage Download devices (Preview) Refresh Columns Preview features Got feedback?

This page includes previews available for your evaluation. View previews →

You can use the activity timestamp to efficiently manage stale devices in your environment. Learn more ⚡

Search by name or device ID or object ID Compliant: Yes Add filters

Name	Enabled	OS	Version	Join Type	Owner	MDM	Compliant	Registered	Activity
C448HD_Android_...	Yes	Android	7.1.2	Azure AD registered	C448 HD	Microsoft Intune	Yes	7/17/2021, 4:25:39 PM	7/17/2021, 3:11:52 AM
RXV80_Android_7/...	Yes	Android	9.0	Azure AD registered	RXV80	Microsoft Intune	Yes	7/8/2021, 1:11:08 PM	7/20/2021, 11:38:30 AM
C470HD_Android_...	Yes	Android	9.0	Azure AD registered	C470 HD	Microsoft Intune	Yes	7/9/2021, 1:07:26 PM	7/19/2021, 7:02:50 AM
C450HD_Android_...	Yes	Android	7.1.2	Azure AD registered	C450 HD	Microsoft Intune	Yes	7/16/2021, 11:57:20 AM	7/16/2021, 11:57:20 AM
RXV80_Android_7/...	Yes	Android	9.0	Azure AD registered	RXV80	Microsoft Intune	Yes	7/22/2021, 5:54:55 PM	7/22/2021, 5:54:55 PM
C435HD_Android_...	Yes	Android	9.0	Azure AD registered	C435 HD	Microsoft Intune	Yes	7/23/2021, 9:02:29 AM	7/23/2021, 9:02:29 AM

