How to Enable Android Enterprise and configure Personal devices with a Work Profile in Microsoft Intune – The ultimate Step-By-Step Guide

This year Google will stop with the support of Android Device Admin API’s with the release of Android 10. This means that the traditional way to manage Android devices is no longer possible with new Android 10 devices or older Android devices that are upgrading to Android 10 (or higher). Android Enterprise is the new way to manage Android devices.

With Microsoft Intune you can manage Android devices with Android Enterprise in different modes. In this blog I will show you step-by-step how to enable Android Enterprise and configure the Work Profile mode (I will write a separate blog for the other modes).

There are a lot of things that needs to be taken into account and I want to deal with them all in this blog. It has become quite a long blog and I think I have included all the necessary steps. That is why I have labeled this blog as The ultimate Step-by-Step guide.

**Topics in this blog**

In this blog I will cover the following topics;

1. [Link a Google Account with Microsoft Intune](https://www.robinhobo.com/how-to-enable-android-enterprise-and-configure-personal-devices-with-a-work-profile-in-microsoft-intune-the-ultimate-step-by-step-guide/#chapter1)
2. [Approve, Sync and Assign applications](https://www.robinhobo.com/how-to-enable-android-enterprise-and-configure-personal-devices-with-a-work-profile-in-microsoft-intune-the-ultimate-step-by-step-guide/#chapter2)
3. [Create and assign an Android Enterprise Work Profile](https://www.robinhobo.com/how-to-enable-android-enterprise-and-configure-personal-devices-with-a-work-profile-in-microsoft-intune-the-ultimate-step-by-step-guide/#chapter3)
4. [Configure App Protection Policies (MAM)](https://www.robinhobo.com/how-to-enable-android-enterprise-and-configure-personal-devices-with-a-work-profile-in-microsoft-intune-the-ultimate-step-by-step-guide/#chapter4)
5. [Configure Device Compliance settings](https://www.robinhobo.com/how-to-enable-android-enterprise-and-configure-personal-devices-with-a-work-profile-in-microsoft-intune-the-ultimate-step-by-step-guide/#chapter5)
6. [Configure Conditional Access](https://www.robinhobo.com/how-to-enable-android-enterprise-and-configure-personal-devices-with-a-work-profile-in-microsoft-intune-the-ultimate-step-by-step-guide/#chapter6)
7. [Enable Android Enterprise in Microsoft Intune](https://www.robinhobo.com/how-to-enable-android-enterprise-and-configure-personal-devices-with-a-work-profile-in-microsoft-intune-the-ultimate-step-by-step-guide/#chapter7)
8. [Test the results by enrolling an Android device](https://www.robinhobo.com/how-to-enable-android-enterprise-and-configure-personal-devices-with-a-work-profile-in-microsoft-intune-the-ultimate-step-by-step-guide/#chapter8)

**What is Android Work Profile?**

Android Work Profile is an Android Enterprise mode to manage corporate data and apps on a personal enabled Android devices. With an Android Enterprise Work Profile, a work container is created on the device in which all business applications end up. You can secure this work container to protect corporate data with security settings like, conditional access, disable the Copy and Past actions between applications inside and outside the work container and an access passcode.

**Preparation / Requirements**

The following requirements are needed for the steps in this blog;

* An Azure tenant
* Microsoft EM+S licenses (E3 or E5)
* A Google account that has not been assigned to a MDM solution
* An Android test device

**1.  Link a Google Account with Microsoft Intune**

The first step is to link a Google Account to Microsoft Intune. Login to the [Microsoft Azure portal](https://portal.azure.com/) for the following steps.

[Graphical user interface, application

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2019/01/How-to-Enable-Android-Enterprise-and-configure-Personal-devices-with-a-Work-Profile-in-Microsoft-Intune-001.jpg)

Navigate to **Microsoft Intune > Device enrollment > Android enrollment**. Click **Managed Google Play – Link your managed Google Play account to Intune**

[Graphical user interface, text, application, email

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2019/01/How-to-Enable-Android-Enterprise-and-configure-Personal-devices-with-a-Work-Profile-in-Microsoft-Intune-002.jpg)

Checkmark **I agree** (if you do) and click **Launch Google to connect now**

[Graphical user interface, application

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2019/01/How-to-Enable-Android-Enterprise-and-configure-Personal-devices-with-a-Work-Profile-in-Microsoft-Intune-003.jpg)

Click **Get started**

[Graphical user interface, application

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2019/01/How-to-Enable-Android-Enterprise-and-configure-Personal-devices-with-a-Work-Profile-in-Microsoft-Intune-004.jpg)

Fill in your Company/Business name and click **Next**

[Graphical user interface, text, application

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2019/01/How-to-Enable-Android-Enterprise-and-configure-Personal-devices-with-a-Work-Profile-in-Microsoft-Intune-005.jpg)

This form is optional, you can skip it or fill it in. Scroll down this page.

[Graphical user interface, application

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2019/01/How-to-Enable-Android-Enterprise-and-configure-Personal-devices-with-a-Work-Profile-in-Microsoft-Intune-006.jpg)

Select **I have read and agree to the Managed Google Play agreement**(if you do) and click **Confirm**

[Graphical user interface

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2019/01/How-to-Enable-Android-Enterprise-and-configure-Personal-devices-with-a-Work-Profile-in-Microsoft-Intune-007.jpg)

Click **Complete Registration**

**2.  Approve, Sync and Assign applications**

Go back to the [Microsoft Azure portal](https://portal.azure.com/).

[Graphical user interface, application, Teams

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2019/01/How-to-Enable-Android-Enterprise-and-configure-Personal-devices-with-a-Work-Profile-in-Microsoft-Intune-008.jpg)

Navigate to; **Microsoft Intune > Client apps > Managed Google Play**. Click **Open the managed Google Play store**

[Graphical user interface, application, Teams

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2019/01/How-to-Enable-Android-Enterprise-and-configure-Personal-devices-with-a-Work-Profile-in-Microsoft-Intune-009.jpg)

Search for an application you want to publish / push to Android devices. In this example I will add Microsoft Word to My managed apps.

[Graphical user interface, application

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2019/01/How-to-Enable-Android-Enterprise-and-configure-Personal-devices-with-a-Work-Profile-in-Microsoft-Intune-010.jpg)

Click **Approve**

[Graphical user interface, application

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2019/01/How-to-Enable-Android-Enterprise-and-configure-Personal-devices-with-a-Work-Profile-in-Microsoft-Intune-011.jpg)

Click **Approve**

[Graphical user interface, text, application, email

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2019/01/How-to-Enable-Android-Enterprise-and-configure-Personal-devices-with-a-Work-Profile-in-Microsoft-Intune-012.jpg)

Select **Keep approved when app requests new permissions** and click **Save**

Note 1: **Repeat this step for all applications you want to push/publish to Android devices.**

Note 2: **Add the Intune Company Portal app and push this app mandatory to all Android devices. This is required to get the latest updates automatically.**

[Graphical user interface, text, application, email, Teams

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2019/01/How-to-Enable-Android-Enterprise-and-configure-Personal-devices-with-a-Work-Profile-in-Microsoft-Intune-013.jpg)

Go back to the Microsoft Intune console and click **Sync**

[Graphical user interface, table

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2019/01/How-to-Enable-Android-Enterprise-and-configure-Personal-devices-with-a-Work-Profile-in-Microsoft-Intune-014.jpg)

When the sync is finished (status: success) open the **Apps** page. Here you can see all the apps that you approved in the previous step (App type is **Managed Google Play**app). The next step is to assign the application to a group.

[Graphical user interface, application, Teams

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2019/01/How-to-Enable-Android-Enterprise-and-configure-Personal-devices-with-a-Work-Profile-in-Microsoft-Intune-015.jpg)

Click on the app and open the **Assignment** page. Click **Add group**

[Graphical user interface, text, application, email

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2019/01/How-to-Enable-Android-Enterprise-and-configure-Personal-devices-with-a-Work-Profile-in-Microsoft-Intune-016.jpg)

Select the Assignment type and click **Included Groups**. Select the group you want to publish this application to. Click **OK** twice and click **Save**

**3.  Create and assign an Android Enterprise Work Profile**

The next step is to create the Android Enterprise Work Profile itself.

[Graphical user interface, text, application, email

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2019/01/How-to-Enable-Android-Enterprise-and-configure-Personal-devices-with-a-Work-Profile-in-Microsoft-Intune-017.jpg)

Navigate to; **Microsoft Intune > Device Configuration > Profiles** and click the **+ Create profile**button.

[Graphical user interface, application

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2019/01/How-to-Enable-Android-Enterprise-and-configure-Personal-devices-with-a-Work-Profile-in-Microsoft-Intune-018.jpg)

Fill in a Name and a Description (optional). Select **Android enterprise** as Platform and select **Work Profile Only – Device restrictions** as Profile type.

[Graphical user interface, application

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2019/01/How-to-Enable-Android-Enterprise-and-configure-Personal-devices-with-a-Work-Profile-in-Microsoft-Intune-019.jpg)

Now you can configure the **Work profile settings, Device password, System security** and **Connectivity**. I always block **Copy and Past between work and personal profiles**, block **Add and remove accounts**and **Require Work Profile Password**. However, what and how to configure settings is depending on the customer use cases.

Click **OK**twice and click **Save**

[Graphical user interface, text, application, email

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2019/01/How-to-Enable-Android-Enterprise-and-configure-Personal-devices-with-a-Work-Profile-in-Microsoft-Intune-020.jpg)

Open the **Assignment**page and add the group you want to publish this profile to.

**4.  Configure App Protection Policies (MAM)**

When you include Microsoft Office 365 applications in your Android Enterprise Work Profile, it is also necessary to configure App Protection Policies, a.k.a. Mobile Application Management (MAM) policies. The Microsoft Office 365 applications are enabled for multi account use, meaning that you can add other accounts next to your business account. And not only email accounts, you can, for example, in Microsoft Word add Storage Accounts like Dropbox. With App Protection Policies you can prevent users from saving business mail attachments to private Storage accounts like Dropbox. In the following steps I show you how to configure this.

[Graphical user interface, text, application, email

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2019/01/How-to-Enable-Android-Enterprise-and-configure-Personal-devices-with-a-Work-Profile-in-Microsoft-Intune-021.jpg)

Navigate to **Microsoft Intune > Clients apps > App protection policies** and click the **+Create policy**button.

[Graphical user interface, application

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2019/01/How-to-Enable-Android-Enterprise-and-configure-Personal-devices-with-a-Work-Profile-in-Microsoft-Intune-022.jpg)

Give the App protection policy a name and a description you like. Select **Android**as the Platform.

Set **Target to all app types** to **No** and select **Apps in Android Work Profile**as **App type**.

[Graphical user interface, application

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2019/01/How-to-Enable-Android-Enterprise-and-configure-Personal-devices-with-a-Work-Profile-in-Microsoft-Intune-023.jpg)

Click **Select required apps** and select the applications that you are making available within the Android Enterprise Work Profile.

[Graphical user interface, text, application

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2019/01/How-to-Enable-Android-Enterprise-and-configure-Personal-devices-with-a-Work-Profile-in-Microsoft-Intune-024.jpg)

Click **Settings**. On the **Data protection**page set **Save copies of Org data**to **Block**. Next to **Allow users to save copies to selected services**select **OneDrive for Business**and **SharePoint** (when it applies for your company).

[Graphical user interface, text, application, email

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2019/01/How-to-Enable-Android-Enterprise-and-configure-Personal-devices-with-a-Work-Profile-in-Microsoft-Intune-025.jpg)

Since this App protection policy will only apply within the Android Enterprise Work Profile (which is protected with a own password) I disable a PIN for this managed applications on the **Access requirements** page. Click **OK** twice and click **Create**.

[Graphical user interface, text, application, email

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2019/01/How-to-Enable-Android-Enterprise-and-configure-Personal-devices-with-a-Work-Profile-in-Microsoft-Intune-026.jpg)

Click the just created App protection policy.

[Graphical user interface, text, application

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2019/01/How-to-Enable-Android-Enterprise-and-configure-Personal-devices-with-a-Work-Profile-in-Microsoft-Intune-027-a.jpg)

Open the **Assignment**tab and assign this policy to the group with the Android users.

**5.  Configure Device Compliance settings**

In steps 6 of this blog we are going to create Conditional Access policies. One of the checks that we are going to configure will be when the devise is **Marked As Compliant**. Before we can configure that, we have to determine when a devices really is compliant. Let’s start by looking at the standard behavior settings.

[Graphical user interface, text, application, email

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2019/01/How-to-Enable-Android-Enterprise-and-configure-Personal-devices-with-a-Work-Profile-in-Microsoft-Intune-027-b.jpg)

Navigate to: **Microsoft Intune > Device compliance > Compliance policy settings**

On this page you can configure conditions to mark a device compliant or not.

The fist setting is **Mark devices with no compliance policy assigned as**(Compliant or Not Compliant). This depends on the company requirements. If there are some security baselines that needs to be applied to every mobile device, you can configure these guidelines into a Compliance Policy and apply this policy to all the devices. If the device meets the requirements, the device is marked as compliant and otherwise not. But if there is no need to configure a Compliance Policy, make sure that the answer to the first option is set to **Compliant**.

Second option is to **Enhanced jailbreak detection**(Enabled or Disabled). I think, for security reasons, this should always be set to **Enabled** (jailbroken devices will be marked as not compliant device).

Last option is **Compliance status validity period (days)**. After how many days of inactivity must a device be marked as not compliant? In my case I will fill in 90 days.

**6.  Configure Conditional Access**

With this current configuration so far, we have secured the Android Enterprise Work container. Now we have to make sure that company data is not accessible outside this work container on a Android device. Therefor we need to configure Azure AD Conditional Access.

[Graphical user interface, application

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2019/01/How-to-Enable-Android-Enterprise-and-configure-Personal-devices-with-a-Work-Profile-in-Microsoft-Intune-028.jpg)

Navigate to: **Microsoft Intune > Conditional access > Policies** and click the **+ New policy**  button

[Graphical user interface, application

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2019/01/How-to-Enable-Android-Enterprise-and-configure-Personal-devices-with-a-Work-Profile-in-Microsoft-Intune-029.jpg)

Give the new Conditional Access policy a name (in my case **Android Enterprise CA**). Click on **Users and groups** to target this Conditional Access to a group of users (in my case the same group as all the other resources I publish for Android Enterprise). Click **OK**.

[Graphical user interface, application

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2019/01/How-to-Enable-Android-Enterprise-and-configure-Personal-devices-with-a-Work-Profile-in-Microsoft-Intune-030.jpg)

Click on **Cloud apps** and select the Cloud Applications you use within your company and where you want to avoid that these applications can access corporate data outside the secure Android container. Most common are **Office 365 Exchange Online** (for access to email) and **Office 365 SharePoint Online** (which also includes OneDrive for Business).

Click **OK**

[Graphical user interface, application

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2019/01/How-to-Enable-Android-Enterprise-and-configure-Personal-devices-with-a-Work-Profile-in-Microsoft-Intune-031.jpg)

Open the **Conditions** tab and open the **Device platforms** settings. In my case I only select **Android** as platforms. You can select multiple platforms or just select **Any device**, but if you select different platforms, make sure that you at least select Android in this case.

[Graphical user interface, application

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2019/01/How-to-Enable-Android-Enterprise-and-configure-Personal-devices-with-a-Work-Profile-in-Microsoft-Intune-032.jpg)

Click on **Client apps (preview)**. Here you can select which client apps this policy must apply to. In my case I select every option except “Apply policy only to supported platforms”. In this way every kind of email application outside the Android Secure Container is blocked from accessing corporate email. Even with an  unmanaged browser. Click **OK**

[Graphical user interface, application

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2019/01/How-to-Enable-Android-Enterprise-and-configure-Personal-devices-with-a-Work-Profile-in-Microsoft-Intune-033.jpg)

Under **Access controls** open the **Grant** tab. Select **Grant access** and make sure you select both **Require device to be marked as compliant**and **Require approved client apps**. In this way, the device must be enrolled with Intune (and be compliant) and the Intune Managed apps must be used to access the corporate data (assuming that Outlook will be used as mail client, otherwise don’t select the last option). Make sure that **Require all the selected controls** is selected.

[Graphical user interface, application

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2019/01/How-to-Enable-Android-Enterprise-and-configure-Personal-devices-with-a-Work-Profile-in-Microsoft-Intune-034.jpg)

Make sure that **Enable policy** is set to **On** and click **Create**

**7.  Enable Android Enterprise in Microsoft Intune**

The final step is to enable Android Enterprise so that new devices will be enrolled with a Android Enterprise Work Profile.

[Graphical user interface, application

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2019/01/How-to-Enable-Android-Enterprise-and-configure-Personal-devices-with-a-Work-Profile-in-Microsoft-Intune-035.jpg)

Navigate to: **Microsoft Intune > Enrollment restrictions** and open the **Default** restriction profile.

[Graphical user interface, application

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2019/01/How-to-Enable-Android-Enterprise-and-configure-Personal-devices-with-a-Work-Profile-in-Microsoft-Intune-036.jpg)

Click **Properties** and then **Select platforms**.

Make sure Android is set to **Block**, and Android work profile is set to **Allow**

**8.  Test the results by enrolling an Android device**

Final step is to test the results of the just created configuration. Therefor I will enroll a new Android 8 device to see if everything is working fine.

[Graphical user interface, application

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2019/01/How-to-Enable-Android-Enterprise-and-configure-Personal-devices-with-a-Work-Profile-in-Microsoft-Intune-037.jpg)

Left: Search for the **Intune Company Portal**app and click **Install**

Right: After the installation, click **Open**

[Graphical user interface, application

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2019/01/How-to-Enable-Android-Enterprise-and-configure-Personal-devices-with-a-Work-Profile-in-Microsoft-Intune-038.jpg)

Left: Click **Sign in**

Right: Fill in your email address and password and login

[Graphical user interface, text, application

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2019/01/How-to-Enable-Android-Enterprise-and-configure-Personal-devices-with-a-Work-Profile-in-Microsoft-Intune-039.jpg)

Left: Click **Continue**

Right: Click **Continue**

[Graphical user interface, text, application

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2019/01/How-to-Enable-Android-Enterprise-and-configure-Personal-devices-with-a-Work-Profile-in-Microsoft-Intune-040.jpg)

Left: Click **Next**

Right: Select **U have read and agree to all of the above**(if you do) and click **Next**

[Graphical user interface, text, application

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2019/01/How-to-Enable-Android-Enterprise-and-configure-Personal-devices-with-a-Work-Profile-in-Microsoft-Intune-041.jpg)

Left: Click **Continue**

Right: Click **Continue**

[Graphical user interface, application

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2019/01/How-to-Enable-Android-Enterprise-and-configure-Personal-devices-with-a-Work-Profile-in-Microsoft-Intune-042.jpg)

Left: I did not have configured a pincode on the device (for this demo) so at this point I’m forced to create a pincode before I can continue with the device enrollment.

Right: Set a pincode

[Graphical user interface, text, application, chat or text message

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2019/01/How-to-Enable-Android-Enterprise-and-configure-Personal-devices-with-a-Work-Profile-in-Microsoft-Intune-043.jpg)

Left: Click **Continue**to re-check the device settings requirements

Right: Click **Done**

[A picture containing text, electronics, different, several

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2019/01/How-to-Enable-Android-Enterprise-and-configure-Personal-devices-with-a-Work-Profile-in-Microsoft-Intune-044.jpg)

Left: The device is now enrolled and mandatory apps will now be installed in the background

Right: A **Workspace**folder is created. Open this folder to see all the business applications.

[Graphical user interface, application

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2019/01/How-to-Enable-Android-Enterprise-and-configure-Personal-devices-with-a-Work-Profile-in-Microsoft-Intune-045.jpg)

Left: When opening a managed application (with an App Protection policy applied to it) for the first time (like Microsoft Outlook of Microsoft Word) this message will appear once. After this, the configured App protection policies are applied.

Right: For the test I have added my Dropbox storage account to Microsoft Word and try to save a business document to it. As you can see, this action is blocked bij the App protection policies.

[Graphical user interface, application

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2019/01/How-to-Enable-Android-Enterprise-and-configure-Personal-devices-with-a-Work-Profile-in-Microsoft-Intune-046.jpg)

Left: As a test, I will now install the Microsoft Outlook application outside the secure Android Enterprise Work profile to see if the conditional access policies are working. Open the app store, search for Microsoft Outlook and click **Install**

Right: After the installation, click **Open**

[Graphical user interface, application

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2019/01/How-to-Enable-Android-Enterprise-and-configure-Personal-devices-with-a-Work-Profile-in-Microsoft-Intune-047.jpg)

Left: Click **Get Started**

Right: Fill in your email address and password to **Sign in**

[Graphical user interface, text, application

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2019/01/How-to-Enable-Android-Enterprise-and-configure-Personal-devices-with-a-Work-Profile-in-Microsoft-Intune-048-a.jpg)

Access to corporate email is blocked as expected.