How to setup Android Enterprise – Corporate-owned dedicated devices with Microsoft Intune

Earlier I wrote about[how to configure 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/). This Android Enterprise mode is designed for personal-owned mobile devices. For corporate-owned devies there are two Android Enterprise modes, one for dedicated devices and one for fully managed user devices. In this blog I will show you how to configure Android Enterprise – Corporate-owned dedicated device mode within Microsoft Intune.

As the name suggests, Corporate-owned dedicated device mode is for devices without user affinity. For example, Kiosk devices and hand scanners.

**Requirements**

Before you can start with the configuration of the Corporate-owned dedicated device mode, make sure you have the following in place;

* An Azure tenant with Microsoft Intune up and running
* A Google Account linked to Microsoft Intune like described in Step 1 of [this blog](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/)
* Android test device(s)

**In this blog**

In this blog I will cover the following topics;

1. Create an Android Enterprise Corporate-owned dedicated device enrollment profile
2. Created an Azure AD Dynamic group
3. Assign Managed Google Play app(s)
4. Create and Assign a Restriction Profile (optional)
5. Test the results

**Step 1: Create an Android Enterprise Corporate-owned dedicated device enrollment profile**

Let’s start with creating the Android Enterprise Corporate-owned dedicated device enrollment profile. To do this, login to the [Microsoft Azure Portal](https://portal.azure.com/).

[Graphical user interface, text, application, email

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2019/02/How-to-setup-Android-Enterprise-%E2%80%93-Corporate-owned-dedicated-devices-with-Microsoft-Intune-001.jpg)

Navigate to: **Microsoft Intune > Device enrollment > Android enrollment** and click **Corporate-owned dedicated devices**

[Graphical user interface, text, application, email

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2019/02/How-to-setup-Android-Enterprise-%E2%80%93-Corporate-owned-dedicated-devices-with-Microsoft-Intune-002.jpg)

Click the **+ Create profile** button

[Graphical user interface, application

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2019/02/How-to-setup-Android-Enterprise-%E2%80%93-Corporate-owned-dedicated-devices-with-Microsoft-Intune-003.jpg)

Fill in a **Name** and optional a **Description**. A token will be created in the next step with an expire date. A token can be valid for maximum 90 days (Policy of Google). Select your expiration date and click **Create**

[Graphical user interface, text, application, email

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2019/02/How-to-setup-Android-Enterprise-%E2%80%93-Corporate-owned-dedicated-devices-with-Microsoft-Intune-004.jpg)

Click **Token**

[Graphical user interface, text, application, email

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2019/02/How-to-setup-Android-Enterprise-%E2%80%93-Corporate-owned-dedicated-devices-with-Microsoft-Intune-005.jpg)

Click **Show token**.

[Graphical user interface, qr code

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2019/02/How-to-setup-Android-Enterprise-%E2%80%93-Corporate-owned-dedicated-devices-with-Microsoft-Intune-006.jpg)

This token is needed when enrolling the Corporate-owned dedicated devices.

**Step 2: Created an Azure AD Dynamic group**

Second step is to create an Azure AD Dynamic group to scope the Android devices that are enrolling with the token from step one. All policies (profiles) and applications needs to be assigned to this group.

[Graphical user interface, application, Teams

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2019/02/How-to-setup-Android-Enterprise-%E2%80%93-Corporate-owned-dedicated-devices-with-Microsoft-Intune-007.jpg)

Navigate to: **Microsoft Intune > Groups > All groups** and click the **+New group** button

[Graphical user interface

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2019/02/How-to-setup-Android-Enterprise-%E2%80%93-Corporate-owned-dedicated-devices-with-Microsoft-Intune-008.jpg)

Select **Security** as Group type. Give this group a name and description and select **Dynamic Device** as Membership type**.**

Click **Dynamic device members**

[Graphical user interface, text, application, email

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2019/02/How-to-setup-Android-Enterprise-%E2%80%93-Corporate-owned-dedicated-devices-with-Microsoft-Intune-009.jpg)

Create the following **Simple rule**;

Add devices where: **enrollmentProfileName – Match** – And then the name of the profile created in step 1. In my case this is **AE-Kiosk**.

Click **Add query**and **Create**

**Step 3: Assign Managed Google Play app(s)**

To publish applications to Android devices that are in Corporate-owned dedicated device mode, Google Managed apps needs to be assigned as **Required** to the group created in step 2. For this blog I will assign Microsoft Edge as a required application. For step-by-step instructions on how to publish Google Managed apps, see step 2 in [this blog](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).

[Graphical user interface, text, application

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2019/02/How-to-setup-Android-Enterprise-%E2%80%93-Corporate-owned-dedicated-devices-with-Microsoft-Intune-010.jpg)

**Step 4: Create and Assign a Restriction Profile (optional)**

An Android device in Corporate-owned dedicated device mode is already pretty locked down. There is not much a user can do on the device other than starting the published applications (and make phone calls if it is a phone). However, there are some possibilities the user can do that maybe you want to block as administrator. Examples are use of the camera and performing a factory reset.

To block these functionalities, you can create and assign a restriction profile. I show you step-by-step how to do this below;

[Graphical user interface, text, application, email

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2019/02/How-to-setup-Android-Enterprise-%E2%80%93-Corporate-owned-dedicated-devices-with-Microsoft-Intune-011.jpg)

Navigate to: **Microsoft Intune > Device configuration > Profiles** and click **+Create profile**

[Graphical user interface, application

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2019/02/How-to-setup-Android-Enterprise-%E2%80%93-Corporate-owned-dedicated-devices-with-Microsoft-Intune-012.jpg)

Fill in a **Name**and a **Description** and select **Device restrictions (Under Device Owner Only)** as Profile type.

[Graphical user interface, application

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2019/02/How-to-setup-Android-Enterprise-%E2%80%93-Corporate-owned-dedicated-devices-with-Microsoft-Intune-013.jpg)

Click **Settings**and configure the settings that apply to you. For this blog I will **Block** the **Factory reset.**Click **OK** and **Save**.

[Graphical user interface, text, application, email

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2019/02/How-to-setup-Android-Enterprise-%E2%80%93-Corporate-owned-dedicated-devices-with-Microsoft-Intune-014.jpg)

Open the **Assignments** page

[Graphical user interface, text, application, email

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2019/02/How-to-setup-Android-Enterprise-%E2%80%93-Corporate-owned-dedicated-devices-with-Microsoft-Intune-015.jpg)

Select the group created in step 2 and click **Save**

**Step 5: Test the results**

Lets test the results by enrolling a new Android device.

[Graphical user interface, application

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2019/02/How-to-setup-Android-Enterprise-%E2%80%93-Corporate-owned-dedicated-devices-with-Microsoft-Intune-016.jpg)

**Left:** Tab 7 times a white space on the screen

**Right:** Tab **Next**

[Graphical user interface, application

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2019/02/How-to-setup-Android-Enterprise-%E2%80%93-Corporate-owned-dedicated-devices-with-Microsoft-Intune-017.jpg)

**Left:**Select the **Wi-Fi** you want to connect with or select **Use Mobile network for setup**

**Right:**Updates and the QR reader will be installed

[Graphical user interface, application

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2019/02/How-to-setup-Android-Enterprise-%E2%80%93-Corporate-owned-dedicated-devices-with-Microsoft-Intune-018.jpg)

**Left:** This is the moment where you need to scan the QR Code

**Right:** After you scan the QR code select **I 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/2019/02/How-to-setup-Android-Enterprise-%E2%80%93-Corporate-owned-dedicated-devices-with-Microsoft-Intune-019.jpg)

**Left:**Select at least **End User License Agreement** and tab **Next**

**Right:**The device will now be configured in Android Enterprise – Corporate-owned dedicated device mode

[Graphical user interface, application

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2019/02/How-to-setup-Android-Enterprise-%E2%80%93-Corporate-owned-dedicated-devices-with-Microsoft-Intune-020.jpg)

**Left:** As you can see, only some basic apps are available like the **Phone, Contacts and Settings**. As you also can see, the **Microsoft Edge** browser is installed.

**Right:** It is not possible for the end user to perform a **Factory reset**, this indicates that the Restriction policy is applied successful.