How to configure Android Enterprise – Corporate-owned, fully managed user devices mode with Microsoft Intune

In the last two months I [wrote some blogs regarding different type of Android Enterprise modes](https://www.robinhobo.com/tag/android/). It’s now time for the last mode; Android Enterprise – Corporate-owned, fully managed user devices. And as the name of this mode indicates, this mode is for user based scenario’s. The enrollment process is more or less the same as with the dedicated device mode. The enrollment process also start with scanning a QR code. However, a user needs to enter his or her credentials during enrollment and all applications and profiles needs to be published user based (see also step 6: testing the results).

In this blog I will show you step-by-step how to configure the Android Enterprise – Corporate-owned, fully managed mode within Microsoft Intune. Note that by the time of writing, this mode is still in (public) preview.

Before you can start with the configuration of this mode, make sure you have the following in place;

* Microsoft Azure tenant with Microsoft Intune up and running
* Linked your Managed Google Play account with this Azure tenant
* Android test device(s)

In this blog I will cover the following topics;

* Step 1 : Create a Corporate-owned, fully managed user device Enrollment Token
* Step 2 : Create an User Group
* Step 3 : Publish Google Managed Applications
* Step 4 : Configure App Protection Policies
* Step 5 : Create a device restriction profile
* Step 6 : Test the results

Let’s get started.

**Step 1 : Create a Corporate-owned, fully managed user device Enrollment Token**

For the following steps, login to the [Microsoft Azure Portal](https://portal.azure.com/) first.

[Graphical user interface, text, application, email

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2019/03/How-to-configure-Android-Enterprise-%E2%80%93-Corporate-owned-fully-managed-user-devices-mode-with-Microsoft-Intune-001.jpg)

Navigate to **Microsoft Intune > Android enrollment**and click **Corporate-owned, fully managed user devices (Preview)**

[Graphical user interface

Description automatically generated with low confidence](https://www.robinhobo.com/wp-content/uploads/2019/03/How-to-configure-Android-Enterprise-%E2%80%93-Corporate-owned-fully-managed-user-devices-mode-with-Microsoft-Intune-002.jpg)

Set **Allow users to enroll corporate-owned user devices**to **Yes**

An Enrollment token will now be generated and displayed below. During the enrollment of the corporate device, this enrollment token is needed in one of the first steps.

**Step 2 : Create an User Group**

As mentioned before, with Android Enterprise – Corporate-owned, fully managed mode, everything is user based. Therefor I will create a new user group to publish all resources to.

[Graphical user interface, text, application

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2019/03/How-to-configure-Android-Enterprise-%E2%80%93-Corporate-owned-fully-managed-user-devices-mode-with-Microsoft-Intune-003.jpg)

Navigate to **Azure Active Directory > Groups**and click the **+ New group** button

[Graphical user interface, text, application, email

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2019/03/How-to-configure-Android-Enterprise-%E2%80%93-Corporate-owned-fully-managed-user-devices-mode-with-Microsoft-Intune-004.jpg)

Select **Security** as Group type and give the new group a name and a description. Select **Assigned**as Membership type.

Make the relevant users a member of this group.

Click **Create**

**Step 3 : Publish Google Managed Applications**

In Android Enterprise – Corporate-owned, fully managed mode you can publish applications as required (mandatory) or optional (available for install). For this blog I will show you both ways and how it looks like on the end point device.

[Graphical user interface, text, application, email

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2019/03/How-to-configure-Android-Enterprise-%E2%80%93-Corporate-owned-fully-managed-user-devices-mode-with-Microsoft-Intune-005.jpg)

Navigate to **Microsoft Intune > Client apps > Apps** and click the **+ Add** button

[Graphical user interface, application, website

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2019/03/How-to-configure-Android-Enterprise-%E2%80%93-Corporate-owned-fully-managed-user-devices-mode-with-Microsoft-Intune-006.jpg)

Select **Managed Google Play** as App type**.**Click **Managed Google Play / Approve** and search for the application you want to publish to the end point devices.

[Graphical user interface, application

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2019/03/How-to-configure-Android-Enterprise-%E2%80%93-Corporate-owned-fully-managed-user-devices-mode-with-Microsoft-Intune-007.jpg)

For this blog I will publish a few Microsoft Office 365 applications, starting with Microsoft Outlook. Click **Approve**

[Graphical user interface, application

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2019/03/How-to-configure-Android-Enterprise-%E2%80%93-Corporate-owned-fully-managed-user-devices-mode-with-Microsoft-Intune-008.jpg)

Click **Approve**once again

[Graphical user interface, text, application, email

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2019/03/How-to-configure-Android-Enterprise-%E2%80%93-Corporate-owned-fully-managed-user-devices-mode-with-Microsoft-Intune-009.jpg)

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

Repeat these steps for every app you want to make available.

[Graphical user interface, application

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2019/03/How-to-configure-Android-Enterprise-%E2%80%93-Corporate-owned-fully-managed-user-devices-mode-with-Microsoft-Intune-010.jpg)

When finished with all the apps, click **OK**

[Graphical user interface, text, application, email

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2019/03/How-to-configure-Android-Enterprise-%E2%80%93-Corporate-owned-fully-managed-user-devices-mode-with-Microsoft-Intune-011.jpg)

Click **Sync**

[Graphical user interface, text, application, email

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2019/03/How-to-configure-Android-Enterprise-%E2%80%93-Corporate-owned-fully-managed-user-devices-mode-with-Microsoft-Intune-012.jpg)

Navigate to **Microsoft Intune > Client apps > Apps**. After the sync is finished, all new apps will appear here.

Select an application to publish it to the user group created in the previous step.

[Graphical user interface, application

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2019/03/How-to-configure-Android-Enterprise-%E2%80%93-Corporate-owned-fully-managed-user-devices-mode-with-Microsoft-Intune-013.jpg)

Open the **Assignments** page and click **Add group**

[Graphical user interface, text, application, email

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2019/03/How-to-configure-Android-Enterprise-%E2%80%93-Corporate-owned-fully-managed-user-devices-mode-with-Microsoft-Intune-014.jpg)

For the Assignment type, select **Required**when you want to publish the application as a mandatory application and **Available or enrolled device** or **Available with or without enrollment** if you want to publish the application as an optional application.

Click **Include Groups** and select the user group created in previous step.

Click **OK**twice and then click **Save**

**Step 4 : Configure App Protection Policies**

This step is optionally but I always configure this as my own best practice. To prevent the end user from saving Microsoft Office documents and Microsoft Outlook attachments to storage accounts like Dropbox, we need to prevent the save as option in the Microsoft Office applications. This is possible with an App Protection Policy. I will show you this step-by-step.

**NOTE: If you are deploying App Protection Policies, make sure you have deployed the Intune Company Portal app as mandatory!**

[Graphical user interface, text, application, email

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2019/03/How-to-configure-Android-Enterprise-%E2%80%93-Corporate-owned-fully-managed-user-devices-mode-with-Microsoft-Intune-015.jpg)

Navigate to: **Microsoft Intune > Client apps > App protection policies**. Click the **+ Create policy** button

[Graphical user interface, application

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2019/03/How-to-configure-Android-Enterprise-%E2%80%93-Corporate-owned-fully-managed-user-devices-mode-with-Microsoft-Intune-016.jpg)

Fill in a name. Select **Android** as Platform. Set **Target to all app types**to **NO** and select **Apps on Intune managed devices** as App types.

[Graphical user interface

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2019/03/How-to-configure-Android-Enterprise-%E2%80%93-Corporate-owned-fully-managed-user-devices-mode-with-Microsoft-Intune-017.jpg)

Open the **Select required apps** page and select the Microsoft Office applications (and other apps that can be managed by Intune) and click the **Select** button.

[Graphical user interface, text, application

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2019/03/How-to-configure-Android-Enterprise-%E2%80%93-Corporate-owned-fully-managed-user-devices-mode-with-Microsoft-Intune-018.jpg)

Open the **Settings / Default settings configured**page and then the **Data protection** page. You can configure the settings you want. For preventing end user from saving Outlook attachments to storage accounts like Dropbox, set **Save copies of Org data** to **Block**. After this, you have the option to acceptations for OneDrive for Business and SharePoint**.**

[Graphical user interface, application

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2019/03/How-to-configure-Android-Enterprise-%E2%80%93-Corporate-owned-fully-managed-user-devices-mode-with-Microsoft-Intune-019.jpg)

Open the **Access requirements** page, since this profile will be applied to Android Enterprise, Corporate Owned, Fully managed user devices, I will disable the **PIN for access**.

Click **OK** twice and click **Create**

[Graphical user interface, text, application, email

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2019/03/How-to-configure-Android-Enterprise-%E2%80%93-Corporate-owned-fully-managed-user-devices-mode-with-Microsoft-Intune-020.jpg)

Open the **Assignments** page and select the User Security Group created in step 2. Click **Save**

**Step 5 : Create a device restriction profile**

This is an optional step in case you want to disable some features on the device or want to enforce some security settings. In this case I will disable the factory reset option for the end user and block USB file transfer.

[Graphical user interface, text, application, email

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2019/03/How-to-configure-Android-Enterprise-%E2%80%93-Corporate-owned-fully-managed-user-devices-mode-with-Microsoft-Intune-021.jpg)

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

[Graphical user interface

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2019/03/How-to-configure-Android-Enterprise-%E2%80%93-Corporate-owned-fully-managed-user-devices-mode-with-Microsoft-Intune-022.jpg)

Give this profile a name and optionally a description. Select **Android enterprise** as Platform and select **Device restrictions** as Profile type. On the **Settings / Configure** page you can set de restrictions you want, for this blog I will disable the Factory reset function and the USB file transfer.

Click **OK**twice and click **Create**

[Graphical user interface, text, application, email

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2019/03/How-to-configure-Android-Enterprise-%E2%80%93-Corporate-owned-fully-managed-user-devices-mode-with-Microsoft-Intune-023.jpg)

Open the **Assignments**page and publish this Profile to the user security group created in step 2 of this blog.

**Step 6 : Test the results**

Let’s test the results by enrolling a new Android device.

[A picture containing text, electronics

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2019/03/How-to-configure-Android-Enterprise-%E2%80%93-Corporate-owned-fully-managed-user-devices-mode-with-Microsoft-Intune-024.jpg)

**Left :**Start an Android device. On the “language select page”, tab 7 times a white space.

**Right :**Tab **Next**

[A picture containing text, electronics, cellphone

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2019/03/How-to-configure-Android-Enterprise-%E2%80%93-Corporate-owned-fully-managed-user-devices-mode-with-Microsoft-Intune-025.jpg)

**Left :**Connect with a WiFi network

**Right :**The QR reader will now be installed

[A picture containing text, electronics

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2019/03/How-to-configure-Android-Enterprise-%E2%80%93-Corporate-owned-fully-managed-user-devices-mode-with-Microsoft-Intune-026.jpg)

**Left :**Select **I have read and agree to all of the above** (if you do) and tab **Next**

**Right :**Select at least **End User License Agreement** and tab **Agree**

[A picture containing text, electronics

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2019/03/How-to-configure-Android-Enterprise-%E2%80%93-Corporate-owned-fully-managed-user-devices-mode-with-Microsoft-Intune-027.jpg)

**Left :**Tab **Accept & Continue**

**Right :**Login with your user credentials

[A picture containing text, monitor, different, electronics

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2019/03/How-to-configure-Android-Enterprise-%E2%80%93-Corporate-owned-fully-managed-user-devices-mode-with-Microsoft-Intune-028.jpg)

**Left :**Tab **Please click here to continue**

**Right :**All mandatory (required) applications will be installed automatically, without the need of any Google Play Store ID

[Graphical user interface, application

Description automatically generated](https://www.robinhobo.com/wp-content/uploads/2019/03/How-to-configure-Android-Enterprise-%E2%80%93-Corporate-owned-fully-managed-user-devices-mode-with-Microsoft-Intune-029.jpg)

**Left :**When opening the Google Play Store on the device. Only the applications published from Microsoft Intune are visible, other apps cannot be installed on the device

**Right :**Optional (available) applications can be installed manually