**What is the difference between management scenarios for mobile devices?**

A quite common discussion topic when it comes to mobile device management is the different approaches you can take. Therefore, I’ve written down a little something to try to simplify a little bit.

I’ve intentionally left out any preview features and user enrollment for Apple device to focus on the most common scenarios. I will look to cover that in a separate post.

There are of course more technical aspects to this, but from a high level this is something that is good to keep in mind!

**Flow description Android**

For Android, there are three different type of management:

* Work Profile
* Corporate owned fully managed
* Corporate owned dedicated device

These are used for three different scenarios which are based on the requirements in the environment. Moving existing devices into Microsoft Intune management also affect which management method which should be used.

**Personally owned with work profile**

Personally owned with work profile is mostly referred to handle Bring Your Own Device (BYOD) scenarios. This is also often used to transition from either no management or legacy management into a Microsoft Intune enrolled device since it does not require the device to be reset to factory default before getting started.

To register a device using Work Profile, the user will need to download the Company Portal application from the Google Play store. When the application is downloaded and installed, user signs into the Company Portal app using the corporate credentials and follows the on-screen wizard how to enroll.

When the device is enrolled, a corporate container is created on the device where all corporate data is stored separately from the personal data. The user will see a new tab on the application pane called Work and all applications will have a small briefcase on them indicating they are work applications.

The IT department can only manage the Work Profile part but can put some restrictions and requirements on the device regarding e.g., PIN-code and Wi-Fi settings. Limited number of remote actions can also be performed such as PIN recovery or removal of corporate data. Applications in the Work Profile part is managed through a Managed Google Play store which is controlled by the Microsoft Intune administrators. Since the applications in the managed Google Play store are centrally managed and assigned, no corporate Google account is needed for the end-user to download and consume applications in the Work Profile.

The personal part of the phone still functions as expected by the user since data is separated and not allowed to stream between the containers.

[Diagram

Description automatically generated](https://www.olastrom.com/wp-content/uploads/2021/01/image.png)Personally owned with work profile

**Corporate owned fully managed**

A corporate owned fully managed device is used where the company buys the device and there is a 1:1 relationship between device and user. To enroll the device as fully managed, the device needs to be new out of the box or been reset to factory default.

Devices could be pre-registered to the customer by the hardware vendor in Google Zero touch to ease the enrollment procedure for the end-user.

When the user receives the device, and the user follows the on-screen onboarding process for initial setup.

If the device is not pre-registered using Google Zero Touch, the user will be asked to scan a QR code which is unique to each customer and must be made available by the IT department.

During the enrollment, the user will be asked to login using their corporate credentials. The user will also be asked to set a PIN-code. As part of the enrollment in Microsoft Intune, configurations, policies, and applications will be applied to the device which has been assigned to the user and/or device.

When the enrollment has finished, the device is ready to be used by the user.

The fully managed device does not separate corporate and personal data as the Work Profile method does, which means that corporate data and personal data is mixed on the device. On the other hand, since the device is fully managed, the IT department has much more control over the device and applied configurations and policies.

Applications are centrally managed by IT, but the public Google Play Store can be made available for the end user. For applications distributed through Microsoft Intune, no Google account is needed for the end user.

IT can also perform remote actions on the device, such as PIN recovery or data removal.

[Diagram

Description automatically generated](https://www.olastrom.com/wp-content/uploads/2021/01/image-1.png)Corporate owned fully managed

**Corporate owned dedicated devices**

Corporate-owned dedicated devices are used when there is not a 1:1 relationship between user and device, in a scenario where multiple users use one device. A good example of this is a kiosk device.

Devices could be pre-registered to the customer by the hardware vendor in Google Zero touch to ease the enrollment procedure.

When the user receives the device, and the user follows the on-screen onboarding process for initial setup.

If the device is not pre-registered using Google Zero Touch, the user will be asked to scan a QR code which is unique to each customer and must be made available by the IT department. These QR codes are unique to each enrollment profile and are valid for 90 days.

During the enrollment, no user sign in is required. Device will be automatically enrolled towards Microsoft Intune and no user affinity is applied. PIN-code can be set as part of the enrollment flow.

During the enrollment to Microsoft Intune, configurations, policies, and applications will be applied to the device which has been assigned to the device.

When the enrollment has finished, the device is ready to be used by the user.

Since the device is supposed to be dedicated to a specific task or function, the features in the OS are limited and can be locked by the IT department. Some built in applications can also be removed if needed.

Applications are centrally managed by IT using Microsoft Intune.

IT can also perform remote actions on the device, such as PIN recovery or data removal.

[Diagram

Description automatically generated](https://www.olastrom.com/wp-content/uploads/2021/01/image-2.png)Corporate owned dedicated devices

**Flow description IOS and iPadOS**

Management of iOS and iPadOS does not have the same number of variations as Android. There is however a difference in how you can handle devices based upon if you use Apple Automated Device Enrollment or not.

For iOS/iPadOS management, there are two different ways of managing the device, personal or shared. Shared device is only applicable to iPadOS.

There are however two different ways of enrollning a device depending on if Apple Automated Device Enrollment is used or not.

**Personal iOS/iPadOS devices with Apple Automated Device Enrollment**

The default management of iOS/iPadOS devices are personal devices where there is a 1:1 relationship between user and device.

If Apple Automated Device Enrollment is used, the devices are pre-registered by the vendor in Apple Business/School Manager. Apple Automated Device Enrollment is used to simplify the enrollment process for the end-user and provide an additional set of control for IT.

When Apple Automated Device Enrollment is used, IT can control the first run experience for the user to remove unnecessary steps. This control will also ensure that the device will be enrolled. When a user receives the device, they will follow the on-screen wizard to get started and register their device.

During the initial setup, the user will be asked to sign in using the corporate credentials and the device will enroll in Microsoft Intune and received the applicable configuration, polices and applications which has been assigned to the user and/or device. When the setup is done, the device is ready to use.

IT can manage configuration, policies, and applications centrally and perform some remote actions such as PIN recovery, data removal or resetting the device. If the devices are deployed in Supervised mode, there is also a possibility to trace lost devices and put them in a “lost mode” to prevent a lost device being used by an inappropriate person.

Applications are downloaded through the Apple App Store. For corporate applications and line-of-business applications, the Company Portal is used to initiate the download and the user will not require an Apple ID to download applications. IT can also do required installations of applications.

[Diagram

Description automatically generated](https://www.olastrom.com/wp-content/uploads/2021/01/image-5.png)Personal iOS/iPadOS devices with Apple Automated Device Enrollment

**Personal iOS/iPadOS devices without Apple Automated Device Enrollment**

The default management of iOS/iPadOS devices are personal devices where there is a 1:1 relationship between user and device.

If Apple Automated Device Enrollment is not used, user will have to download the Company Portal application from the Apple App Store to enroll the device. Users then sign into the application using their corporate credentials and follow the on-screen instructions on how to enroll the device.

IT can manage configuration, policies, and applications centrally and perform some remote actions such as PIN recovery, data removal or resetting the device.

Applications are downloaded through the Apple App Store. For corporate applications and line-of-business applications, the Company Portal is used to initiate the download and the user will not require an Apple ID to download applications. IT can also do required installations of applications.

[Diagram

Description automatically generated](https://www.olastrom.com/wp-content/uploads/2021/01/image-6.png)Personal iOS/iPadOS devices without Apple Automated Device Enrollment

**Shared iPadOS device**

Shared iPadOS devices are used when there is not a 1:1 relationship between user and device, in a scenario where multiple users use one device. A good example of this is a kiosk device.

To use the Shared iPadOS scenario, Apple Automated Device Enrollment needs to be used. Devices are registered in the Apple Business/School Manager to connect the device towards the customer.

When a device is to be registered, a user or coordinator starts the device and follows the on-screen instructions. No sign-in is required during this process since the device will not have user affinity.

During the enrollment, the device will receive configurations, policies and applications which has been assigned to the device.

When the registration is completed, the device is ready to use.

IT can manage configuration, policies, and applications centrally and perform some remote actions such as PIN recovery, data removal or resetting the device.

Applications are centrally managed by IT and are installed automatically by assigning them in Microsoft Intune without user interaction.

[Diagram

Description automatically generated](https://www.olastrom.com/wp-content/uploads/2021/01/image-4.png)Shared iPadOS device