

# Microsoft Intune Mobile Device Management (MDM) deployment in an iPhone in use

## Table of Contents

1. General.....	1
2. Start to use the Authenticator app.....	1
3. Delete Company Portal app .....	2
4. Install and setup Intune Company Portal .....	2
4.1. Option 1: Employer's phone .....	2
4.2. Option 2: Your own phone .....	6
5. Installation of work apps.....	10
6. Settings .....	11
6.1. Check the compliance with requirements .....	11
6.2. Notifications from Company Portal .....	13
7. Removing a phone from Intune MDM .....	13

## 1. General

For the sake of simplicity, our Intune MDM instructions only discuss phones and iPhone, but the system is also applied to iPads and all iPhone instructions work in them as well.

This instruction is for an iPhone that is already in use. If you are setting up Intune in a new iPhone, you can find instructions on the page [MDM – Instructions for new phone](#).

When MDM is enabled on an Android phone, the operating system enables the split into a personal profile with all previous applications and a work profile in which work applications and their data are installed. iPhones have a similar function for protecting work apps, but not a visible split to profiles as in Android phones. Since most of the phones in the Universities community are Android phones, we use the term work profile also in the general MDM guidelines. From the iPhone perspective, a work profile means only a set of work apps and their management.

## 2. Start to use the Authenticator app

If you are using text messages as the primary authentication method for two-step authentication (MFA), instead, start using Authenticator as the primary authentication method, as instructed on the page [Setting up multifactor authentication](#). There are two reasons for this: SMS is not a safe enough way for two-step authentication, and there is a bug on iPhone that causes an error in SMS authentication after changing the TUNI password. You can use SMS as a secondary authentication method in case there is a problem with the Authenticator application (as instructed on the page [Setting up multifactor authentication](#)).

### 3. Delete Company Portal app

If you already have the app Company Portal installed on your phone, you should delete it first. The easiest way to do this is to search your phone's app list for the "Company Portal" app, touch it long enough until a menu appears above or below the app, with the option "Remove app". Then lift your finger, tap "Delete App" and tap "Delete" to confirm the removal.

### 4. Install and setup Intune Company Portal

You must first delete all those apps that will be installed to your phone as work apps. Therefore, delete the following apps from your phone (all Microsoft products): Word, Excel, PowerPoint, Outlook, Teams, OneDrive, OneNote, Edge. App deletion is explained in the previous chapter.

Then update the phone software version by launching Settings and tapping *General - Software Update*. This setup guide is for the iOS version 15.

The deployment of Intune happens slightly differently in employer's phone than in your own phone.

- The employer's phone will be more widely protected than your own phone. Further information is available in the document Microsoft Intune MDM General info on the page [Mobile Device Management](#).
- In your own phone, the management system works with the new Apple ID, which is provided for each user with a tuni.fi address. The Apple ID contains 200 GB iCloud space.

So, follow the steps of only one of the following procedures:

- 4.1 Option 1: Employer's phone
- 4.2 Option 2: Your own phone

#### 4.1. Option 1: Employer's phone

Open App Store on the phone, find the Intune Company Portal and install the app according to the instructions below. Please note that, to keep the instructions brief, several notifications indicating the progress of the installation have been left out.

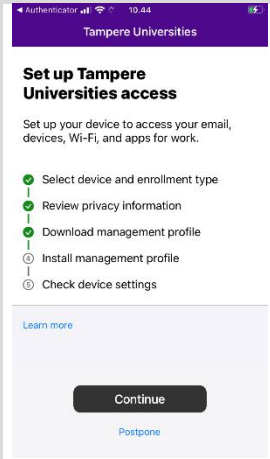
The screenshots were mainly taken with iPhone SE. With different kinds of iPhones, the screens may look slightly different.

<p>Tap the installation button and Open once the installation is complete.</p>	<p>Tap Sign in.</p>	<p>Enter your TUNI email address and tap next.</p>	<p>Enter your TUNI password and tap Sign in.</p>

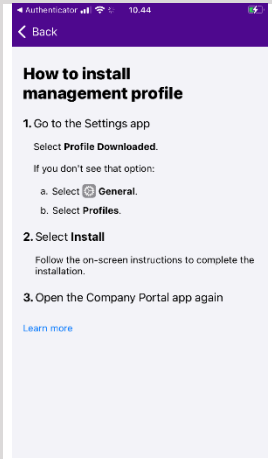
<p>Approve multi-factor authentication.</p>	<p>Tap OK.</p>	<p>Tap Allow.</p>	<p>Tap Begin.</p>

<p>Choose the topmost option and tap Continue.</p>	<p>If you have not already installed Microsoft Authenticator, install it. After that, press the home button and open Company Portal.</p>	<p>Tap Continue.</p>	<p>You may check the use of your data by tapping Can/Can't. Tap Continue.</p>

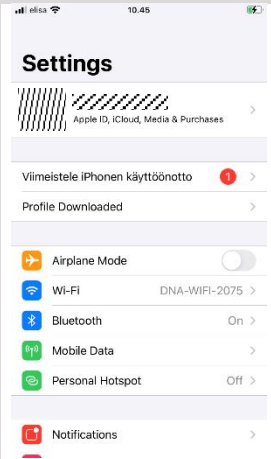
<p>Tap Continue.</p>	<p>Tap Allow.</p>	<p>Tap Close.</p>	<p>Tap Continue.</p>



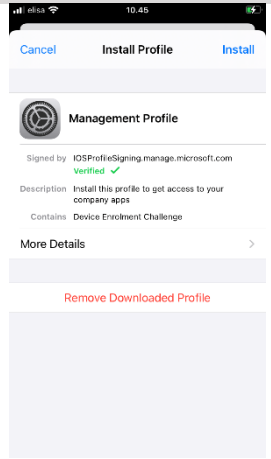
Tap Continue.



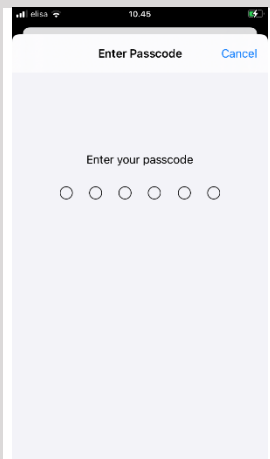
Press the home button and open Settings app.



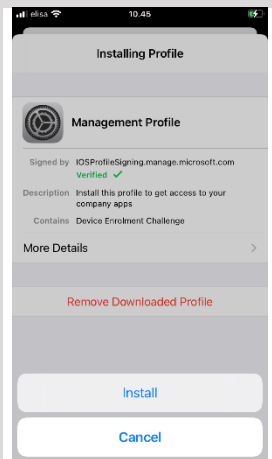
Tap Profile Downloaded.



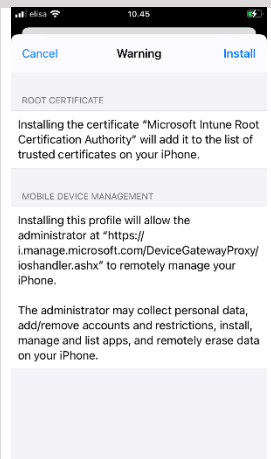
Tap Install.



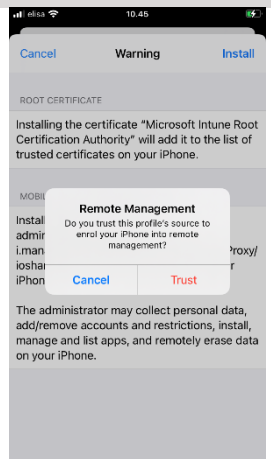
Enter your passcode.



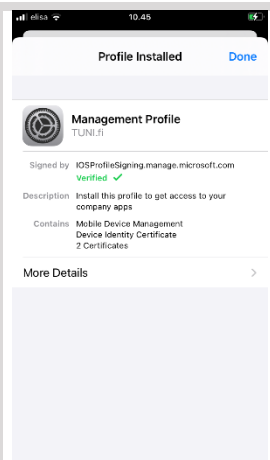
Tap Install.



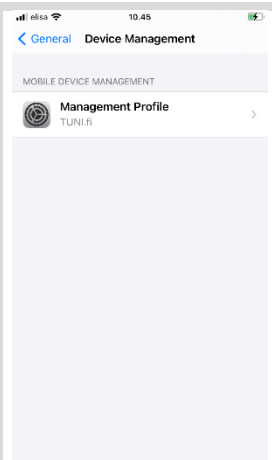
Tap Install.



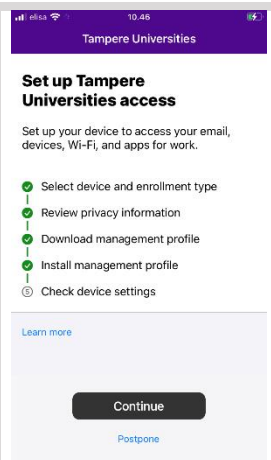
Tap Trust.



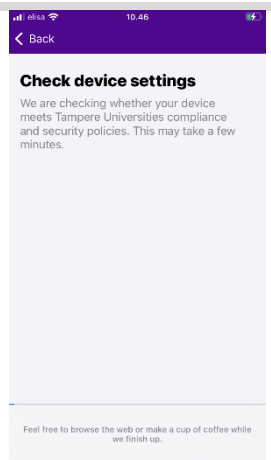
Tap Done.



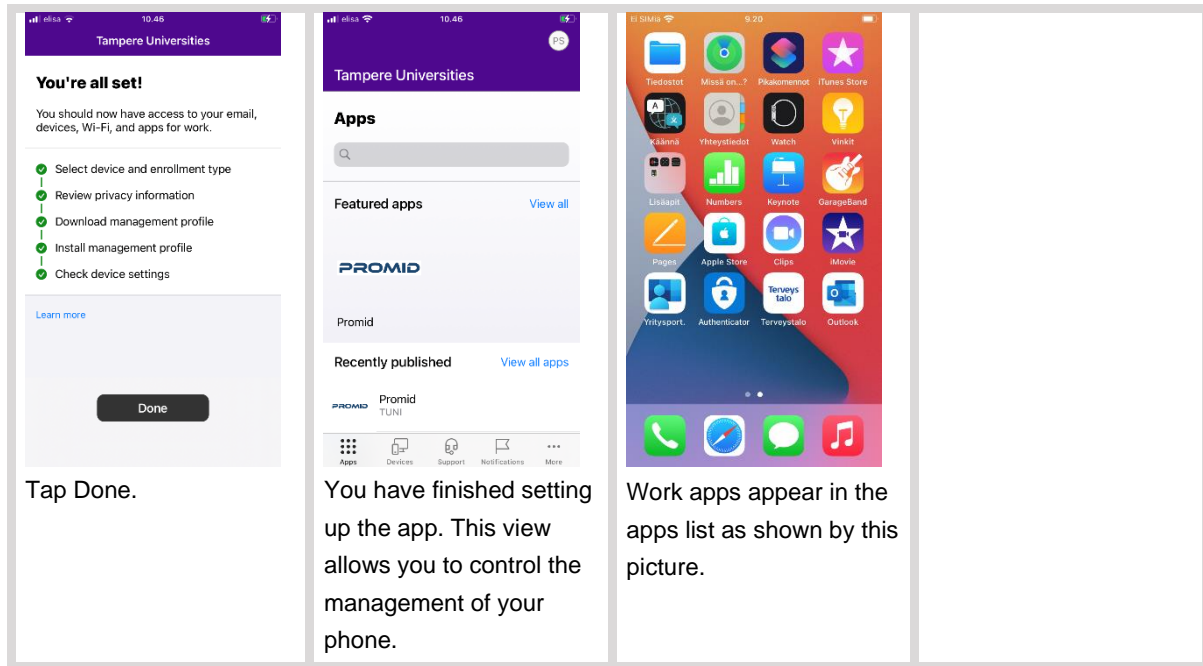
Press home button and open Company Portal.



Tap Continue.



Wait a moment.



## 4.2. Option 2: Your own phone

Launch the Settings app and tap the top item that should show your name. On the next screen, your Apple ID will appear below your name.

- If it ends in @tuni.fi, ie in the format firstname.lastname@tuni.fi, you are using an account managed by TUNI, in which case you must sign out by tapping *Sign Out* at the bottom of the screen and then sign in into another Apple ID account on your phone. If you don't have an Apple ID account, you can create a new one, for example using the format firstname.lastname.tuni@icloud.com.
- If your Apple ID doesn't end at @tuni.fi, then you don't need to sign out.

Open App Store on your phone, find the Intune Company Portal and install the app according to the instructions below. Please note that, to keep the instructions brief, several messages indicating the progress of the installation have been left out.

The screenshots were mainly taken with iPhone SE. With different kinds of iPhones, the screens may look slightly different.

The first screenshot shows the App Store search results for 'Intune Company Portal' with a 'GET' button highlighted. The second screenshot shows the app's splash screen with a 'Sign in' button. The third screenshot shows the Microsoft sign-in page with the email address entered and the 'Next' button highlighted. The fourth screenshot shows the password entry screen with the 'Sign in' button highlighted.

Tap the installation button and Open once the installation is complete.

Tap Sign in.

Enter your TUNI email address and tap next.

Enter your TUNI password and tap Sign in.

The first screenshot shows a 'Approve sign in request' dialog with a blue box around the 'I can't use my Microsoft Authenticator app right now' link. The second screenshot shows a 'Get notified so you don't lose access' dialog with an 'Ok' button. The third screenshot shows a 'Send You Notifications' dialog with an 'Allow' button. The fourth screenshot shows the 'Set up Tampere Universities access' screen with a 'Begin' button.

Approve multi-factor authentication.

Tap OK.

Tap Allow.

Tap Begin.

The first screenshot shows the 'Select device and enrollment type' screen. The user has selected 'Tampere Universities owns this device' and 'I own this device'. The second screenshot shows the same screen with 'Secure work-related apps and data only' selected. The third screenshot shows the 'Asenna Microsoft Authenticator' screen with the 'Asenna App Storesta' button. The fourth screenshot shows the 'Set up Tampere Universities access' screen with the 'Continue' button.

Choose "I own this device".

Choose Protect only work-related apps and data. Tap Continue.

Install Microsoft Authenticator if you have not already done so. After that, press home button and open Company Portal.

Tap Continue.

The first screenshot shows the 'Device management and your privacy' screen with 'Can't' selected. The second screenshot shows the 'Set up Tampere Universities access' screen with the 'Continue' button. The third screenshot shows the 'Continue to Company Portal' screen with the 'Allow' button. The fourth screenshot shows the 'Continue to Company Portal' screen with the 'Close' button.

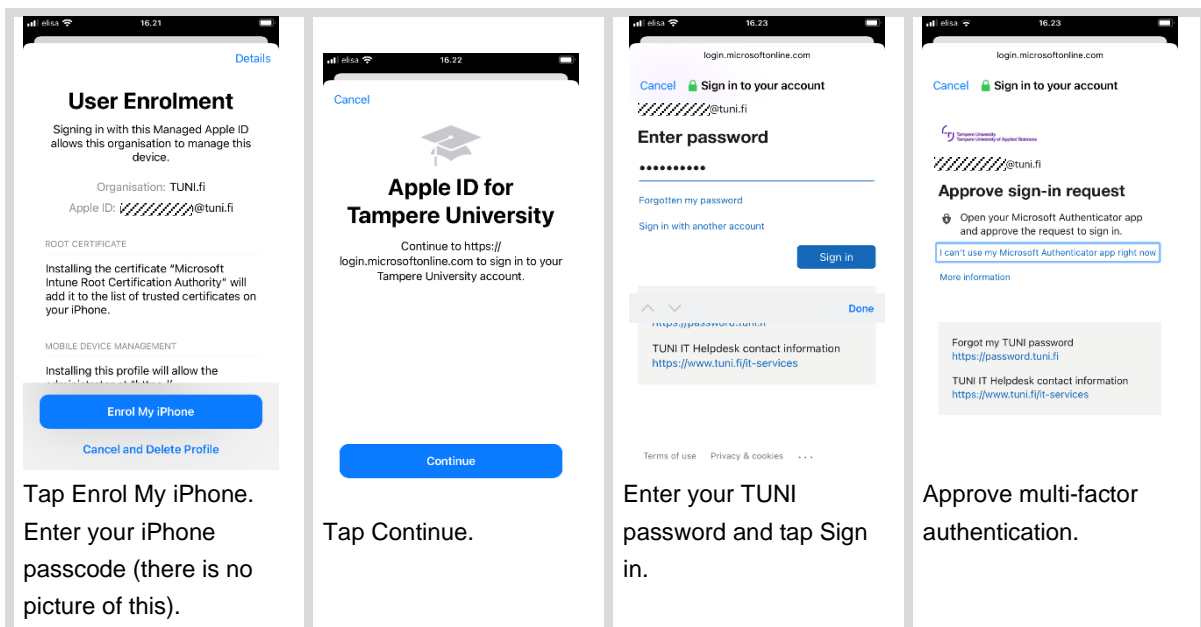
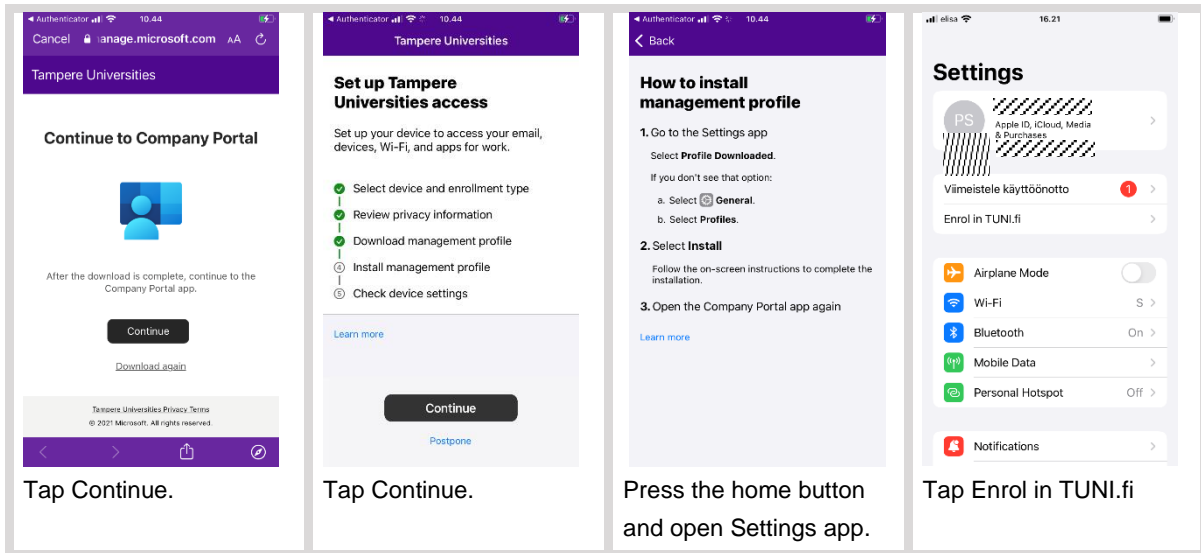
You may check the use of your data by tapping Can/Can't. Tap Continue.

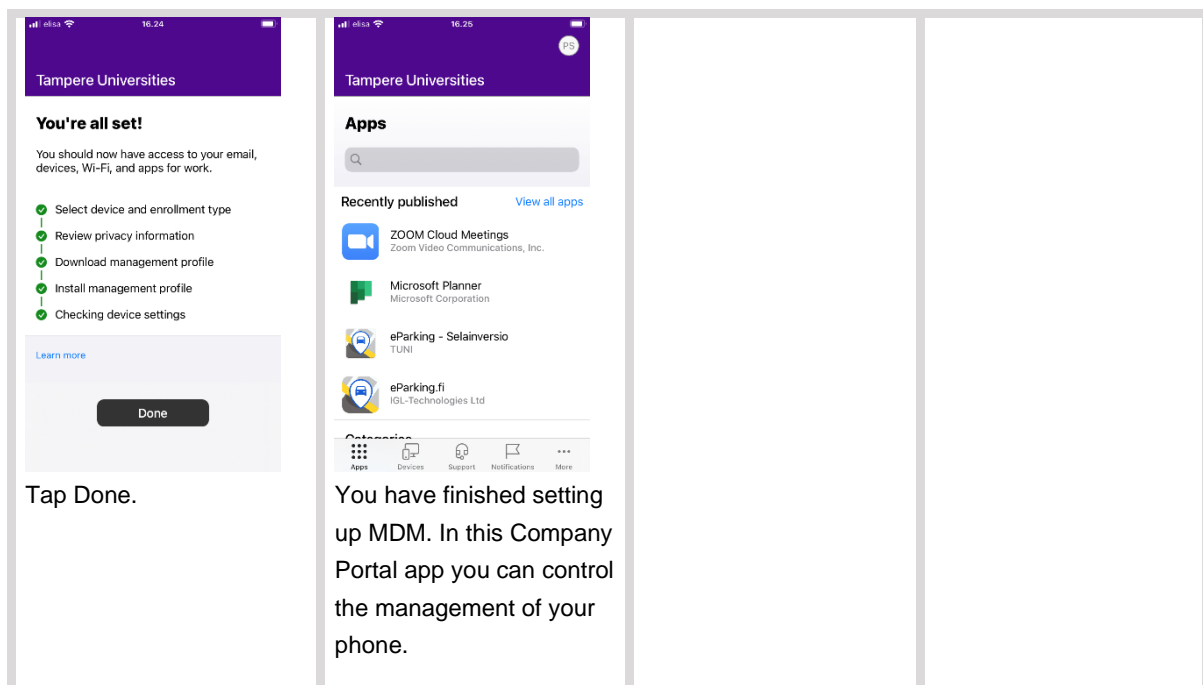
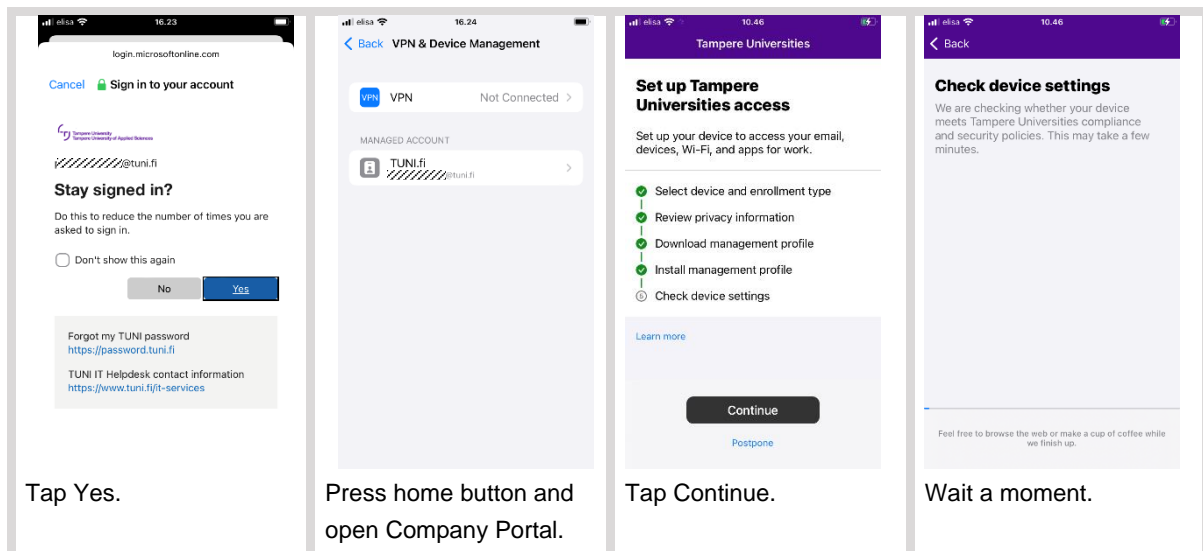
Tap Continue.

Tap Allow.

Tap Close.



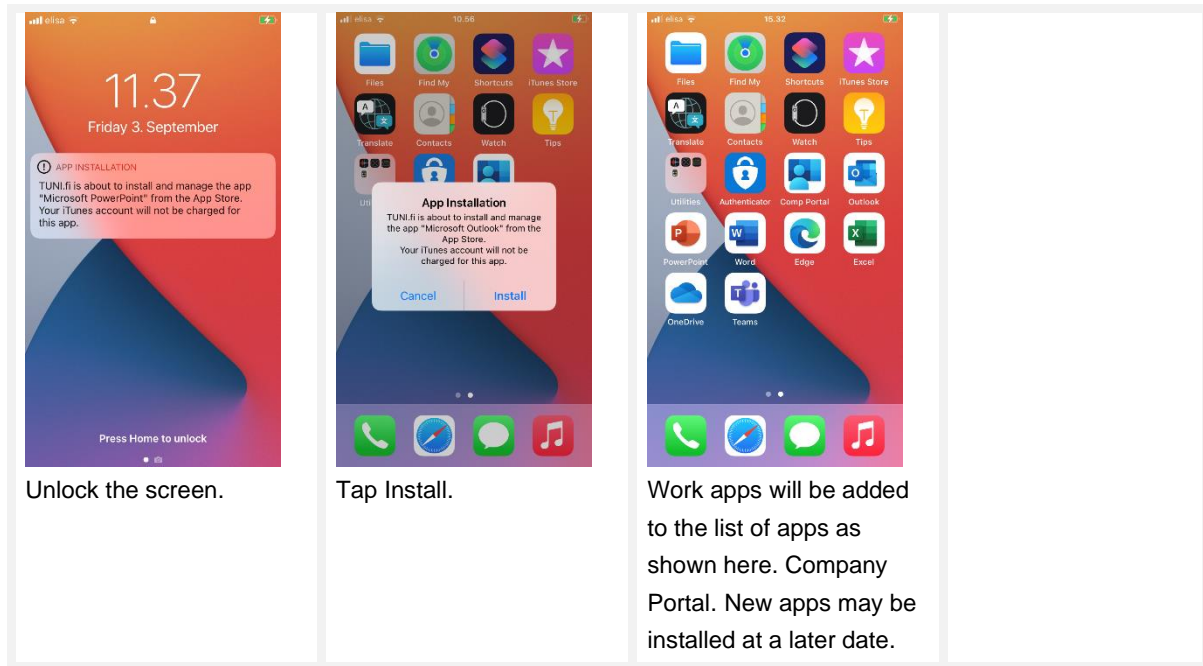




## 5. Installation of work apps

After the deployment of the MDM, it will automatically install the work apps. The installation starts usually after 15 minutes. A notification described below will be displayed for each app to be installed, please accept all of them.

If there are any apps that Company Portal is set to install and which have already been installed on the phone, Company Portal will ask “Would you like to let TUNI.fi take management of the app...” for each of these apps. Please tap Manage for each of these requests to give this permission in order to protect the data of the apps. Additional copies of the apps will not be installed.



In addition to the automatically installed work apps, you can install other work apps in the Company Portal like this: open the tab Apps, tap “View all apps”, tap an app you want to install and tap then Install. The sets of work apps are updated over time as needed.

Sign in the work apps in a normal manner using your TUNI email address.

In addition to the TUNI account, you can also add your other email accounts into the Outlook app in work profile. That allows you to access all your emails in the same Outlook app and to see all your calendars in the same Outlook calendar view.

Unlike with Android, there are no identifiers for work apps on iPhones that would separate them from personal apps in the list of apps or in the actual apps. The work apps are just added to the list of apps, looking exactly the same.

## 6. Settings

### 6.1. Check the compliance with requirements

Intune MDM monitors that the phone fulfils the defined information security requirements. If a requirement is not met in a phone, the MDM prevents the access for an employee from this phone to the M365 services.

This is how you can check if your phone fulfils the requirements and what you have to do fix the possible issues:

- Launch Company Portal app, switch to tab “Devices”
- Tap the name of your phone. It is normally at the top of the list.
- If the status after the title “Device settings status:” says “Can access company resources”, everything is OK now and you do not need to anything regarding this chapter (6).

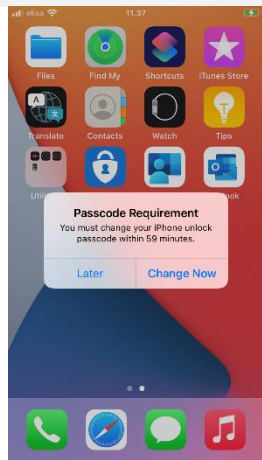
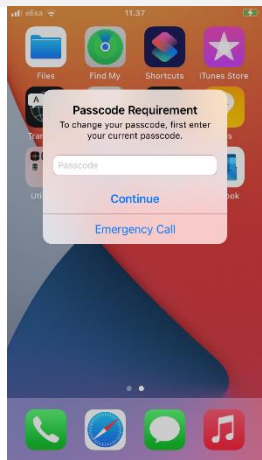
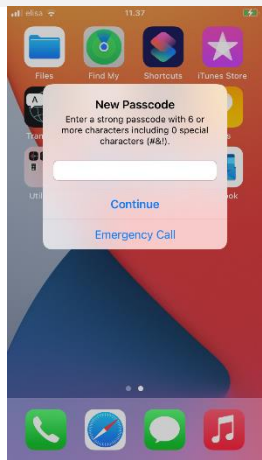
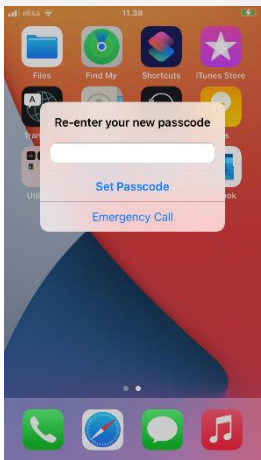
- If the status after the title “Device settings status:” says “May not be able to access company resources”, you will have to something to fix issues.
- Tap the text “You need to update settings on this device. See status for details”.
- Now you should see a list of issues that you will need to fix so make the phone fulfil the requirements. Under each issue description there is text “How to resolve this” which you can tap to get instructions how to resolve the issue. Follow the instructions to fix the issue. Repeat this checking process until there are no issues left.

At this moment, the following settings should be applied. The IT Services updates these requirements as needed. The current requirements may be tightened and there may be new requirements.

- Auto-Lock display timeout (Settings – Display & Brightness – Auto-Lock): 5 minutes or less
  - Note: Teams app prevents the display from getting locked during a meeting
- Passcode (Settings – Touch ID and passcode): Set a passcode with at least 6 digits (no consecutive or recurrent digits).
  - **Memorize the new passcode very carefully! If you forget it, the phone has to be reset, in which case you will lose all data and files in the phone.**
  - You can set up Touch ID to avoid needing to enter the passcode.
- The Software Version must be 14.0 or higher (Settings - General - Software Update).
  - If your phone does not fulfil this requirement, try to perform a software update in your phone (Settings - General - Software Update).
- The operating system of the phone must be original, that is, installed by the phone manufacturer. Thus, the phone cannot be “jailbroken”.
  - If your phone does not fulfil this requirement, you will have to install the original operating system in the phone. If that is not possible, the phone will have to be renewed.

## 6.2. Notifications from Company Portal

If the settings of the phone are not set as required by MDM, Company Portal will display notifications requesting you to change the settings. Please change the settings as requested by the notifications.

			
Tap Change Now.	Enter your current passcode.	Enter a new passcode. <b>Memorize the new passcode very carefully! If you forget it, the phone has to be reset, in which case you will lose all data and files in the phone.</b>	Re-enter the new passcode.

## 7. Removing a phone from Intune MDM

You can remove your phone from Intune MDM with Company Portal. After the removal, you can start using Intune MDM again according to the instructions provided earlier in this document. Here's how to remove your phone from Intune MDM.

Open the tab Devices.  
Tap the name of your phone.

Open the menu by tapping the three dots and tap "Remove device".

Tap Remove.

Apps installed by Intune will be automatically removed. The phone has now been removed from the Intune management system.