Microsoft Intune Mobile Device Management instructions - general

1. Background and terminology

We use a device management product called Microsoft Intune. The name of the device management app to be installed on the device is Company Portal. The name of this app in the Google Play Store and in the Apple App Store is slightly different: Intune Company Portal.

The terms Mobile Device Management, Management System, Intune, and Company Portal are used in our instructions in a slightly mixed way depending on the situation, but they all refer to the same system from different points of view.

2. What information related to my device can be accessed by the management system?

The privacy of all systems and devices used by the Tampere Universities community is taken seriously, which is of course the case regarding Intune mobile device management as well. Here is a list of information the management system can and cannot access. All information is processed confidentially and only for a justified need.

Any kind of control and management is naturally suspicious when it seems to target personal things like your own data and files on your phone. You may be worried by many aspects: Does the management system do exactly what it promises and nothing else? Are there any faults in the management system? Is the management system configured correctly? Can I trust that the maintenance personnel do not access my data and files? A critical attitude is always in place, but there are several reasons why you can trust this system:

- Microsoft Intune is a widely used system, used by about 3,000 companies.
- Intune's documentation (see Chapter 2) tells you exactly what Intune sees and what it doesn't. Intune does not ever access any information in your personal profile, that is, your own applications, their data and files.
- Intune is a management system monitored by IT professionals in all organizations. Deviations from the documentation and faults in the system are therefore much more likely to be found than in consumer systems.
- Much of the MDM functionality on the device is in operating systems made by Google and Apple, and the continuous monitoring mentioned above helps to detect their relevant faults as well.
- You probably use a lot of apps to store and transmit even your confidential information, such as: Google Drive, OneDrive, iCloud, WhatsApp, Signal, email. If you can rely enough on their flawlessness and maintenance staff, why couldn't you trust similarly Intune and MDM?
- The employees of the Tampere University IT Services adhere to strict data protection and professional ethics. The work of the maintenance personnel is strictly regulated in the IT Services Maintenance Rules and in the University Group's Log Policy. We follow naturally Principles of Good Governance at Tampere University, in which data protection and information security are the most relevant in this context. Your data is secured in good hands.

The management system can access the following information related to your device:

- Device model and manufacturer
- Operating system and version
- Name of the owner of the device
- Name, serial number and IMEI of the device
- The last four digits of the phone number registered on the device (except on a device owned by your employee, please see below)
- Names of the apps installed by the management system

On a device owned by your employee, the management system can access the following additional information:

- Full phone number
- The names of all the apps you have installed on an iPhone or iPad. The IT Services only use this information for automated data security management purposes, primarily malware protection.
- Location: If an iPhone or an iPad goes missing or is stolen, the user of the device can set the status of the device to “Managed Lost Mode”. Also IT Helpdesk can do this if requested by the user. This mode displays a notification on the device that it has been tracked and the device’s location is displayed also on Intune. This is the only situation in which IT Services can access the location of the device.

The management system cannot access the following information related to your device:

- Call and browsing history
- E-mail and text messages
- Contacts
- Calendar
- Passwords
- Photos
- Files
- Apps installed by you and the related information (exception: Intune can access the names of apps on iOS devices owned by the employer, but the IT Administration only use this information for automated data security management purposes, primarily malware protection.)

Microsoft’s documentation about this matter is available at https://docs.microsoft.com/fi-fi/mem/intune/user-help/what-info-can-your-company-see-when-you-enroll-your-device-in-intune.

3. Work apps

Employees can access the M365 services (formerly: Office 365) only using managed work apps installed in the work profile of your device. The set of work apps will be modified over time and that information will be updated to this list. Some work apps are installed in all devices, and some apps are optional so that you can choose which to install. The M365 services can be accessed not only with the M365 apps but also with a browser installed in work profile.

If you need an app to be installed in your device as a work app, you can send a request about it with good justifications. The typical justification is that you receive a link to a service via work email and the services does not work well enough on a browser, but you need to launch the app using the link.

The following work apps will be installed automatically to your device:

Android:

- Microsoft Office
- Microsoft Outlook
- Microsoft Teams
- Microsoft OneDrive
- Microsoft Edge
- Microsoft Authenticator

iPhone/iPad:

- Microsoft Word
- Microsoft Excel
- Microsoft PowerPoint
- Microsoft Outlook
- Microsoft Teams
- Microsoft OneDrive
- Microsoft Edge
- Microsoft Authenticator

You can install these work apps if you want:

Android:

- 112 Suomi
- Elisa Ring
- eParking (link)
- Gboard
- Google Chrome
- Microsoft OneNote
- Microsoft SwiftKey Keyboard
- Moodle
- Promid (link)
- Signal
- ZOOM Cloud Meetings

iPhone/iPad:

- 112 Suomi
- Elisa Ring
- eParking.fi
- Google Chrome
- Microsoft OneNote
- Promid (link)
- Signal
- ZOOM Cloud Meetings

4. If you do not deploy mobile device management

Employees can access the M365 services (formerly: Office 365) only on those mobile devices that have the MDM deployment in good standing. In addition to regular employees with employment contract, employee also means those resource agreement holders who have been given a mobile device for work use from Tampere university or TAMK. Employee means here also those employees who are also students at the Tampere university or TAMK.

When the deadline of the deployment of MDM is reached in your faculty or unit, your TUNI account will stop working in M365 apps (such as Outlook, Office, OneDrive, Teams) on your mobile device.

The two-phase authentication using for example the app Microsoft Authenticator will continue to work as previously. However, other functions of the Authenticator, such as “Review recent activity”, will stop working.

The deployment of MDM has started in December 2021 and will continue in phases during spring 2022. A request for deployment will be emailed to users when the deployment is timely. MDM should be deployed within 6 weeks of receiving the request for deployment. Thereafter, the system will be blocked to prevent access to the Universities community’s M365 services by any phone and tablet in which MDM is not enabled.

5. Student as employee

The requirements described above for using MDM apply to all employees, also students. Studying or short employment are not valid reasons to compromise on security.

The obligation to use mobile device management is managed on a user-ID basis. Every person has only one user-ID, there are no separate user-IDs for studying and working. Employee’s obligation to use MDM therefore also applies also to studying purposes and all mobile devices, including own equipment.

Therefore, if you are a student and starting an employment at a university or TAMK, you have to deploy MDM on all mobile devices in which you want to use M365 apps or services (such as Outlook, Teams, Office, OneDrive). The obligation to use is determined by the employment status and takes effect automatically at the beginning of the employment.

When the employment is terminated, the obligation to use MDM is automatically terminated and the M365 applications run again in a personal profile or without MDM like they did before employment. When employment finishes, you may continue to use MDM and the apps it has installed, but new work apps cannot be installed.

6. Microsoft Intune in more detail

The documentation for users of the Intune system is available at https://docs.microsoft.com/fi-fi/mem/intune/user-help/ and it applies also to our deployment. A part of the functions of Intune and the devices can be modified by the IT Services and we develop that continuously. If you find something that you would like to be changed in the configuration, please contact IT Helpdesk and justify your request well.

To enable you to study the Microsoft Intune documentation, the deployment of Intune at Tampere Universities is done in the following way:

Android:

- If you have installed the Company Portal yourself and performed the deployment, the Intune enrollment profile is called ”personally-owned with a work profile”.
    - If the device is owned by your employer, the ownership of the device is ”corporate”.
    - If the device is owned by you, the ownership of the device is ”personal”.
- If you received a new mobile device and the deployment of the Intune Company Portal started automatically, the enrollment profile is called ”corporate-owned with a work profile” and the the ownership of the device is ”corporate”.

iOS:

- If you have installed the Company Portal yourself and performed the deployment, the device is not “Supervised”.
    - If the device is owned by your employer, the ownership of the device is ”corporate” and the type of deployment is ”Device enrollment”.
    - If the device is owned by you, the ownership of the device is ”personal” and the type of deployment is ”User enrollment”.
- If you received a new mobile device and the deployment of the Intune Company Portal started automatically, the device is “Supervised”, the ownership of the device is ”corporate” and the type of deployment is Automated Device Enrollment”