Data separation on Apple devices

Separating data into private and business areas makes sense if a device is not only used for work but can also be used for private purposes. Companies create a benefit for their employees by enabling this dual usage.

Apple offers two versions for business and private use: **BYOD (Bring your Own Device)** and the **establishment of a private area** on Apple DEP devices.

How it works

Fundamentally, the separation of the areas is based on a separation of Apple IDs. In addition to the personal Apple ID, an Apple ID managed by the company or educational institution is installed on the device. This separates data and apps, preventing them from accessing each other. Apple generally distinguishes between two types of apps:

- Apps installed by MDM **(Managed Apps)**, which can be managed by the IT administrator. These are linked to the company's Apple ID.
- Apps downloaded by the user from the App store (**unmanaged apps**) that cannot be managed with MDM. These are linked to the private Apple ID.

Requirements:

- Apple DEP account for company-owned devices
- MDM to manage the business area

MOBIVISOR

BYOD with Apple devices

BYOD means that employees use their own device for work. However, this device must still meet the company's security standards to avoid GDPR violations. In principle, all iOS devices, iPads, and MacBooks can be turned into BYOD devices.

Setup:

The devices are equipped with a private Apple ID. The end user downloads the MDM client app (for example MobiVisor MDM) from the App Store and logs in.

A separate workspace is set up on the device. However, this is not specifically labeled. After the MDM profile has been successfully installed, the IT administrator can install apps on the device via MDM. These are considered “managed apps”.

How it works:

- Managed Apps and MDM Client App can be removed by the end user at any time
- IT admin can manage managed apps via MDM policies
- In MDM, apps downloaded by the end user can be viewed, but not managed or uninstalled
- Apps can be managed or unmanaged, but never exist twice on a device

Notes on data protection:

- Prevent copying data from unmanaged to managed apps by policy
- Disable access of unmanaged apps to managed contacts
- Prohibit opening content from managed apps in unmanaged apps
- Apps that are on a blacklist can still be downloaded by the end user as an unmanaged app

Setting up a private area on the DEP device

Apple DEP devices are all company-owned devices that have been assigned to the company and an MDM server via Apple Business Manager.The device is supplied with the company-owned Apple ID and the MDM profile cannot be removed.

Setup:

To set up a private area on the company's Apple device, the MDM policy must allow the end user to additionally add a private Apple ID. The end user can then install unmanaged apps.

How it works:

- Apps can be blacklisted and then cannot be installed by the user
- MDM profile and managed apps cannot be removed by the user
- Here too, apps are either managed or unmanaged.
    - Unmanaged apps can be replaced by a managed app if the same app is installed via MDM

Notes on data protection:

- Blacklist unwanted apps
- Use MDM policies to manage end-user access and rights and set up devices in compliance with GDPR
- Use passcode policies to increase device security

Would you like more information or have questions about integrating Apple devices into MDM?

Visit our YouTube Channel @iotiq

Contact us by email: mds@iotiq.de

MOBIVISOR