Bring Your Own Device (BYOD) with Android Enterprise & MobiVisor MDM

In this data sheet:

1. Requirements for BYOD on your Android devices
2. Advantages of the BYOD model for your company
3. App deployment and management
4. Removing the managed profile
5. Possible security policies in the work profile

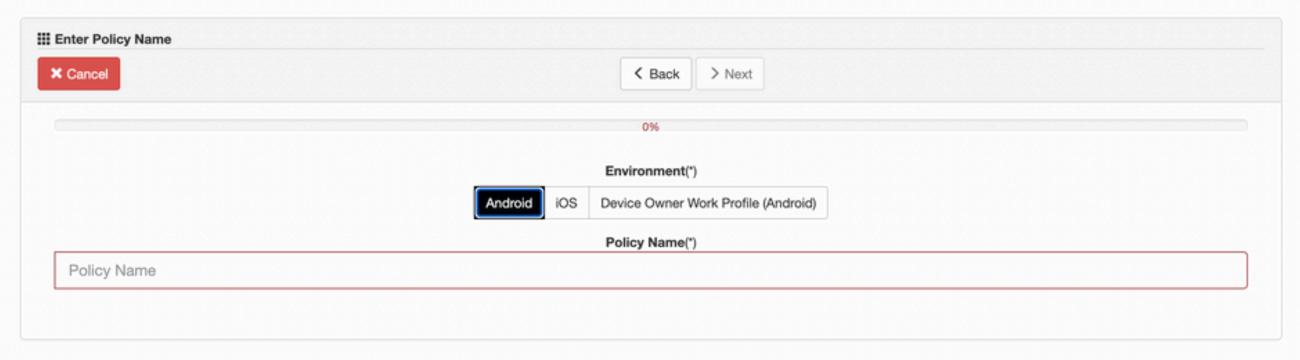
The Android work profile with MobiVisor MDM:
Security and flexibility for your BYOD implementation

BYOD (Bring Your Own Device) – the use of employees' private devices for mobile working is repeatedly promoted by IT managers as a worthwhile opportunity to save costs. Android's work profile creates a dedicated, secure area on the device that contains all company applications and data. It runs parallel to the private profile on the device, with business apps and notifications marked with a briefcase icon. Users can easily multitask between business and private apps, but the data remains completely separate.

Requirements for BYOD on your devices

In order to implement the BYOD model with Android devices, the use of a mobile device management system (MDM) such as MobiVisor is essential. Only an MDM can set up a so-called **managed work profile** that strictly separates business data from private data on the device. The MDM takes care of the configuration, assignment of policies, and ongoing management of the work profile—without an MDM, it is not possible to separate private and business content on BYOD devices.

To manage Android devices in the BYOD (Bring Your Own Device) model with MobiVisor, you first need to create a suitable policy in the system. You can do this by going to **“Policies > New > Android.”** In the policy settings, you'll find an overview of all available features, which are listed in the **“Supported Versions”** column.



Important: For BYOD devices, only the features marked with the note **“Work profile”** are used. The work profile separates business and personal data on the device and ensures that only the business area is managed by IT—a key element for data protection and user acceptance in the BYOD context.

Please also note that **Samsung-specific features cannot be used on BYOD devices**, as the Samsung API required for this is not active in this mode.

Advantages of the work profile for your business

Data loss prevention (DLP policies): MobiVisor MDM allows you to apply a set of data loss prevention (DLP) policies and settings to the work profile. These include:

- **Work profile security codes:** Enforce a minimum complexity level in the work profile with a PIN, pattern, password, or biometric method to prevent unauthorized access.
- **Copy control:** Prevent data from being copied from business apps and pasted into personal apps to protect sensitive information.
- **Sharing between apps:** Specify which business apps are allowed to share data with personal apps, or block this feature entirely.
- **VPN options:** Apps in the work profile can be protected on the network using a variety of VPN options. You have the option of ensuring that only apps in the work profile can use the VPN to secure all business data traffic.

Data protection (for users) and IT control: For private devices used for business purposes (BYOD), IT administrators use MobiVisor MDM to manage only company applications and data.

- **No access to private data:** Employees can continue to use their own apps in their private profile. Private apps and data cannot be checked or controlled by the IT department.
- **Selective remote deletion:** Business apps and data can be deleted remotely by the IT administrator without affecting private applications and data. This is crucial in the event of loss, theft, or an employee leaving the company.

Work-life balance: The work profile promotes a healthy work-life balance by enabling a clear separation between private and professional content on the same device. Business apps, emails, and data are located exclusively in the protected work area, while personal content remains untouched. This allows employees to consciously switch off outside of working hours without seeing work notifications or applications in their private environment.

App deployment and management
with MobiVisor MDM and Managed Play Store

Companies must equip employees with approved applications, ranging from publicly available apps to privately developed software. MobiVisor MDM uses the Managed Play Store as the standard option for secure app delivery.

- **Secure app delivery:** With the Managed Play Store, administrators can securely deliver and remotely configure internally developed and public applications.
- **Automated app distribution:** IT administrators can add applications to their approval list in the Managed Play Store or deploy them directly to employee devices via push. Apps can be deployed and configured remotely for specific employees without users having to do anything themselves.

Managed profile can be removed at any time

A key aspect of the BYOD strategy with Android is that **participation is voluntary.**

- Users retain control over their device at all times – the managed work profile set up by MobiVisor can also be removed independently if necessary.
- This completely deletes all business data and apps, while private content remains untouched.

Setup is also carried out by the users themselves:

- They download the MobiVisor client from the Google Play Store and log in with their personal access data (username and password).
- Step-by-step instructions for setup can be found here.

Security guidelines in the work profile

Various security policies can be applied within the managed work profile to ensure the protection of company data. These include, among others:

- Mandatory setup of a **secure lock code**
- **Encryption of all data** stored in the work profile
- Blocking of **unsecure apps**
- **Restriction of file transfers** between the private and business areas