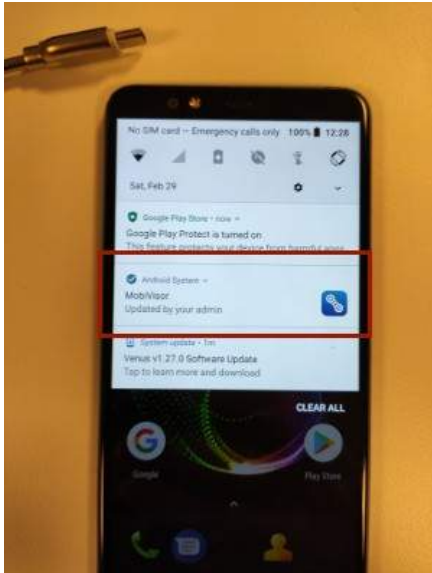
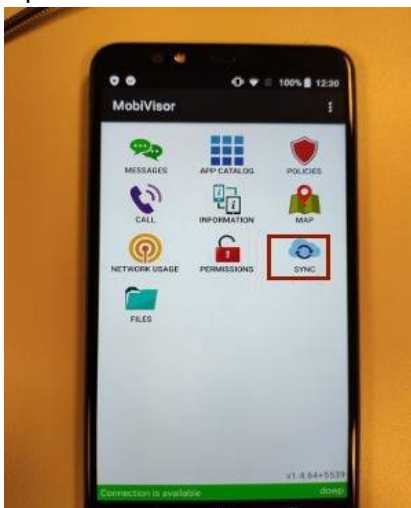


Device Owner + Work Profile Device Setup

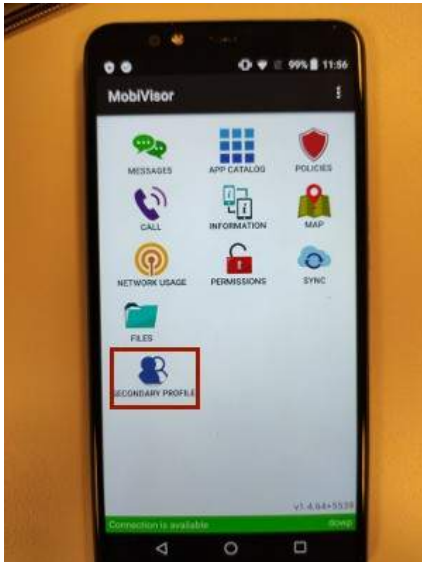
1. Run the Device Owner Setup (Android for Work).
 - Anleitung: <https://www.youtube.com/watch?v=872JIU3YyAY>
2. Wait, until MobiVisor is updated.



3. Open MobiVisor and click **SYNC**.



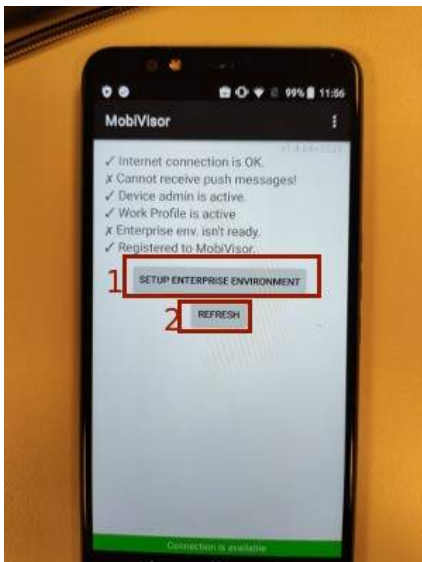
4. Close MobiVisor and open the app again. Now click on **SECONDARY PROFILE**.



5. The work profile will now be installed. After the installation please click the following buttons:

1. **SETUP ENTERPRISE ENVIRONMENT**

2. **REFRESH**



6. The update can take a few minutes. Click **REFRESH** again and wait, until MobiVisor is updated



7. After the successful update, the device can now be used.

Web Interface

1. Allow all apps in the private container, while the work profile only allows apps, that are enabled in the Whitelist feature. To adopt this setting, click **Config** **Android Enterprise** **Access Permissions** and take action with following settings:

1. **Access Permissions** **Include All**
2. **Work Profile Access Permissions** **Whitelist**

Completed! Android Enterprise is created and associated with MobiVisor

Name: Erste
Enterprise ID: LC01hzv6pn
Administrators: ademekici90@gmail.com

[Unenroll](#)

Applications + Add Applications **Access Permissions**

Default Access Permissions

The access level defines how your users see applications on google play store.
You can specify different access levels to specific devices using Groups.

- **Whitelist:** The user has access to a specific set of apps that you define.
- **All Approved:** The user has access to all apps that are approved for the enterprise.
- **Include All:** The user has access to all apps that are publicly available in the Google Play store.

Beware: Make sure that this is a necessary change. Change of access level might lead to notifications being sent to all your devices.

Access Permissions
Include All ← Device Owner Access Permission
[Save Access Level](#)

Work Profile Access Permissions
Whitelist ← Work Profile Access Permission
[Save Work Profile Access Level](#)

2. To install apps on the work profile, click **Applications** **List** and choose the desired Android Enterprise app

After the selection of desired apps, you can delete the apps or send install/uninstall requests to devices

SELECT AN APP [Send Install or Remove](#)

App Name Environment

| Delete | Environment | Application Name | Management Options | Version Code | Version Name | Created At | Image | Application Type | Actions |
|-------------------------------------|--------------------|--|--|--------------|----------------|------------------|-------|---------------------|------------------------------|
| <input checked="" type="checkbox"/> | Android Enterprise | Adobe Acrobat Reader: PDF Viewer, Editor & Creator Work together @. Comment and edit in real-time ☑ Stay connected on all devices ↻ | Remove App On MDM Removal: <input checked="" type="checkbox"/> Silent Install After Signin: <input checked="" type="checkbox"/> | | Latest Version | 02/29/2020 11:42 | | Store App | Edit Details Configure |
| <input type="checkbox"/> | Android | MobiVisor DOWP | Remove App On MDM | 264 | 1.4.64+5539 | 02/29/2020 11:44 | | File App 4.24 MB | Edit Details |

3. Select a device with DO+WP settings and install the application on the work profile of the device.

After the selection of desired apps, you can delete the apps or send install/uninstall requests to devices

SELECT AN APP
← Select More Apps

Install Apps To Devices
Uninstall Apps From Devices

- Send A Request
- Install Directly
- Send App Request to Work Profile
- Install Directly to Work Profile

ENROLLED DEVICES
5 Total 4 Active 0 Semi Active 0 Inactive
Inactivity timeout: 120 Minutes

| Environment | User Name | Date Enrolled | Last Connection Time | Model/Make | Actions |
|--|------------------------------|------------------|----------------------|-----------------------------|------------------------|
| <input checked="" type="checkbox"/> Android Enterprise | Dowp <small>DO+WP</small> | 29/02/2020 11:53 | 29/02/2020 12:15 | Vestel - Venus Z20 | Manage |
| <input type="checkbox"/> iOS | no-user - Burak (iPad) | 25/02/2020 16:31 | 25/02/2020 16:31 | Apple - iPad 6th Gen (WiFi) | Manage |
| <input type="checkbox"/> Android | Serhan | 10/02/2020 14:27 | 13/02/2020 11:31 | Samsung - SM-G532F | Manage |
| <input type="checkbox"/> Android | admin | 11/02/2020 17:36 | 11/02/2020 18:44 | TP-Link - NetXos X1 Max | Manage |
| <input type="checkbox"/> iOS | Ali (Phone) | 03/10/2019 17:40 | 08/10/2019 19:06 | Apple - iPhone 6 | Manage |

Device management

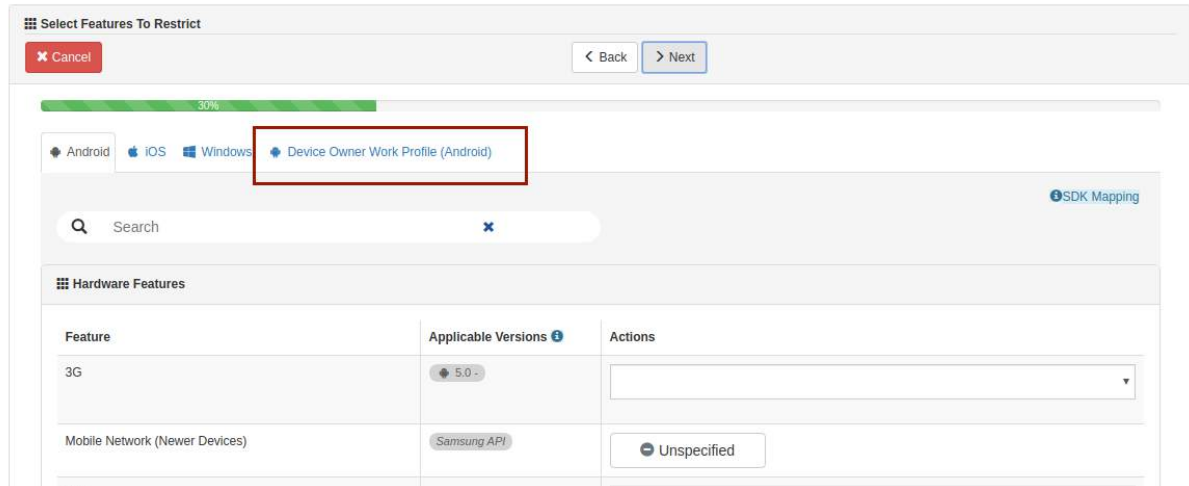
1. To execute commands on the different profiles, click on **Devices -> Manage**.
2. Now you can switch between the different profiles under Management Actions.

The screenshot displays the IOTIQ device management interface. On the left, the 'DEVICE DETAILS' section provides information about a device named 'dowp'. The 'Management Actions' section is highlighted with a red box, showing options for 'Personal Space' and 'Work Space'. Below this, various management actions are listed, including 'Change Password', 'Update Settings', 'Switch User', 'Renew Session', 'Logout User', 'Lock Screen Now', 'Debug Logs', 'Wipe', 'Lock Device', 'Unlock Device', and 'Ring Device'. The 'Requests' section includes 'Location' and 'Status' buttons. The 'Application Info Requests' section has a 'Fetch System Apps' button. The 'System Features' section shows 'Reboot' and 'Power Off' buttons.

| DEVICE DETAILS | |
|------------------------------|--------------------------|
| USER NAME | dowp |
| DISPLAY NAME | Dowp |
| DESCRIPTION | |
| DATE JOINED | 24/01/2020 16:49 |
| DATE ENROLLED | 29/02/2020 11:53 |
| LAST CONNECTION TIME | 29/02/2020 12:16 |
| GROUPS | DO-WP |
| LAST STATUS | |
| Ignore Battery Optimizations | ✖ |
| Power Save Mode | ✖ |
| Google Accounts | - |
| Policies | - |
| Rejected Permissions | |
| Build Flavor | Normal |
| Device Encryption Status | Active (Default Key) |
| Device Admin Status | ✔ |
| Brightness | 40% |
| Mock GPS Apps | |
| Mock GPS Enabled | ✖ |
| GPS Status | ✔ |
| Bluetooth Status | ✖ |
| Mobile Network Status | ✖ |
| Wi-Fi Status | ✔ |
| Network Country | |
| Sim Country | |
| Network Operator | |
| Installer Source | Unknown |
| Root Status | Not Rooted |
| Manufacturer API Status | No API |
| Manufacturer API Version | - |
| Device API Type | Device Owner (Venus Z20) |
| Model | Vestel |
| Kernel Version | 4.4.78-perf+ |
| Boot Loader | Unknown |
| IMEI | 354651090588650 |
| Build Number | 10021851 |
| Android Version | 8.0.0 |
| DNS | - |
| Serial Number | 2811389718001488 |
| MAC Address | 00:09:DF:B3:CF:CF |
| IP Address | 192.168.0.102 |
| Used Storage | 1% |

Policies

1. Create a new policy. To do this, click on **Policies** \square **Policies** \square **New**.
2. When creating the new policy, select **Device Owner Work Profile (Android)**



3. Assign the policy to users/groups (**Policies** \square **Assign Policies**).
4. The policy is now active for your work profile.