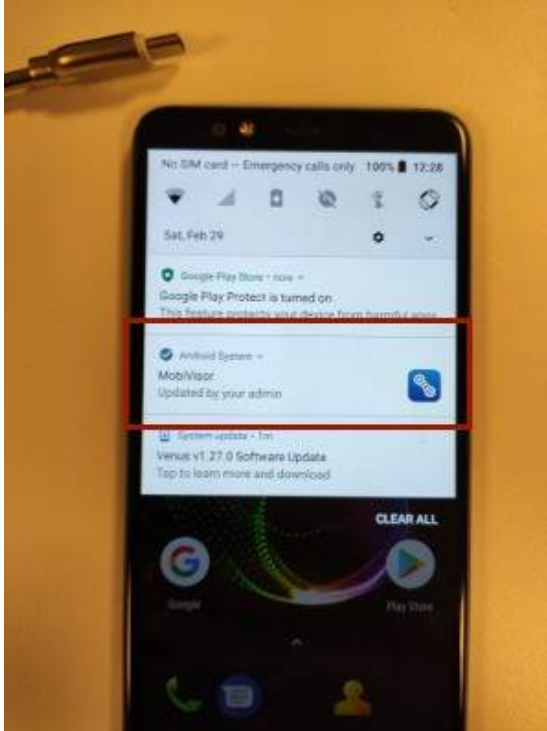
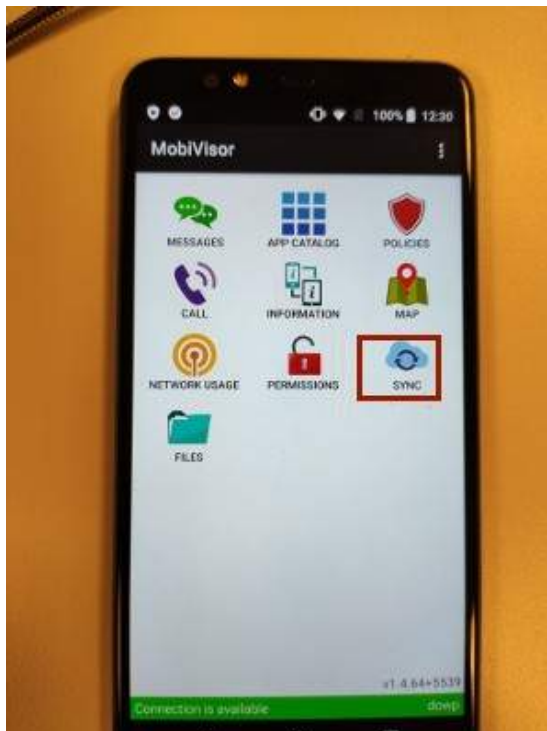


## Device Owner + Work Profile Device Setup

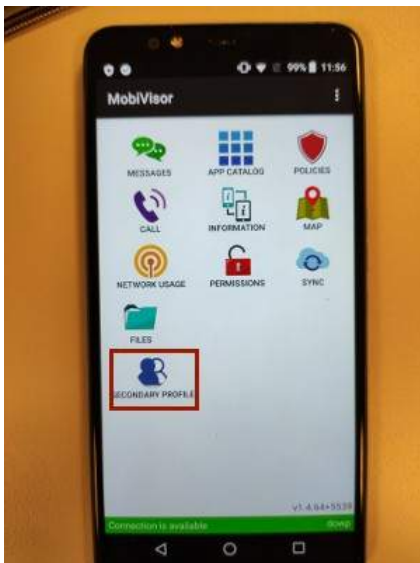
1. Führen Sie das Device Owner Setup (Android for Work) durch.
  - Anleitung: <https://www.youtube.com/watch?v=872JIU3YyAY>
2. Warten Sie, bis sich MobiVisor aktualisiert.



3. Öffnen Sie MobiVisor und klicken Sie **SYNC**.

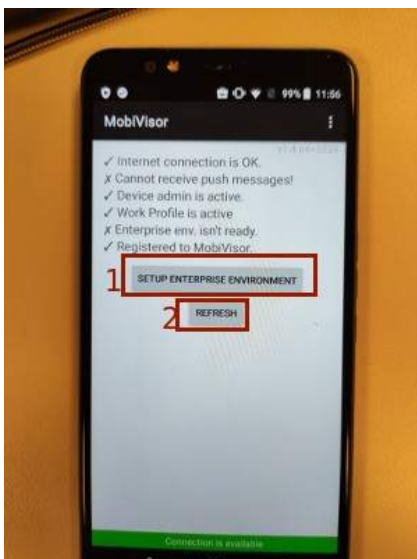


4. Schließen Sie MobiVisor und öffnen Sie die App erneut. Klicken Sie jetzt auf **SECONDARY PROFILE**.

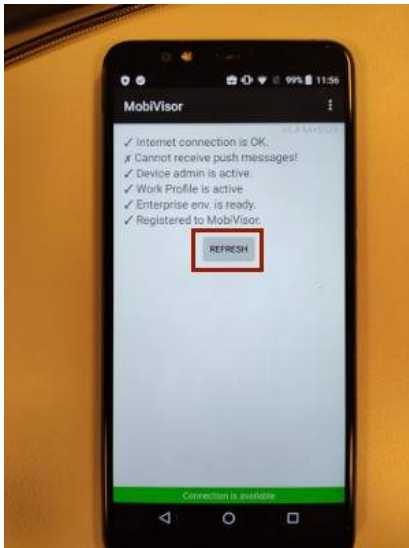


5. Das Work Profile wird jetzt installiert. Nach der Installation klicken Sie bitte folgende Buttons:

- 1. SETUP ENTERPRISE ENVIRONMENT**
- 2. REFRESH**



6. Die Aktualisierung kann wenige Minuten dauern. Klicken Sie erneut auf **REFRESH** und warten Sie, bis sich MobiVisor aktualisiert.



7. Nach der erfolgreichen Aktualisierung ist das Gerät einsatzbereit.

## Web Oberfläche

1. Erlauben Sie im privaten Container alle Apps, während für das Work Profile nur ausgewählte Apps via Whitelist freigegeben werden. Um diese Einstellung zu übernehmen, klicken Sie auf **Config → Android Enterprise → Access Permissions** und nehmen Sie folgende Einstellungen vor:

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. Um Apps auf dem Work Profile zu installieren, klicken Sie auf **Applications → List** und wählen Sie die gewünschte Android Enterprise Anwendung aus.

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

All

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: (🔄) Silent Install After Signin: (🔒)		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. Wählen Sie ein Gerät mit DO+WP Einstellungen und installieren Sie die Anwendung auf dem Work Profile des Geräts.

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

The screenshot shows the IOTIQ management interface. At the top, there is a 'SELECT AN APP' section with search filters for 'App Name' and 'Environment'. A dropdown menu is open, showing options: 'Install Apps To Devices', 'Uninstall Apps From Devices', 'Send A Request', 'Install Directly', 'Send App Request to Work Profile' (highlighted with a red box), and 'Install Directly to Work Profile'. Below this is the 'ENROLLED DEVICES' section, which includes a table of devices and their details.

Environment	User Name	Date Enrolled	Last Connection Time	Model/Make	Actions
Android Enterprise	Dowp DO+WP	29/02/2020 11:53	29/02/2020 12:15	Vestel - Venus Z20	Manage
iOS	no-user - Burak (iPad)	25/02/2020 16:31	25/02/2020 16:31	Apple - iPad 6th Gen (WiFi)	Manage
Android	Serhan	10/02/2020 14:27	13/02/2020 11:31	Samsung - SM-G532F	Manage
Android	admin	11/02/2020 17:36	11/02/2020 18:44	TP-Link - Neffos X1 Max	Manage
iOS	Ali (iPhone)	03/10/2019 17:46	08/10/2019 19:06	Apple - iPhone 6	Manage

## Geräteverwaltung

1. Um Befehle auf den verschiedenen Profilen auszuführen, klicken Sie auf **Devices** -> **Manage**.
2. Jetzt können Sie unter Management Actions zwischen den verschiedenen Profilen wechseln.

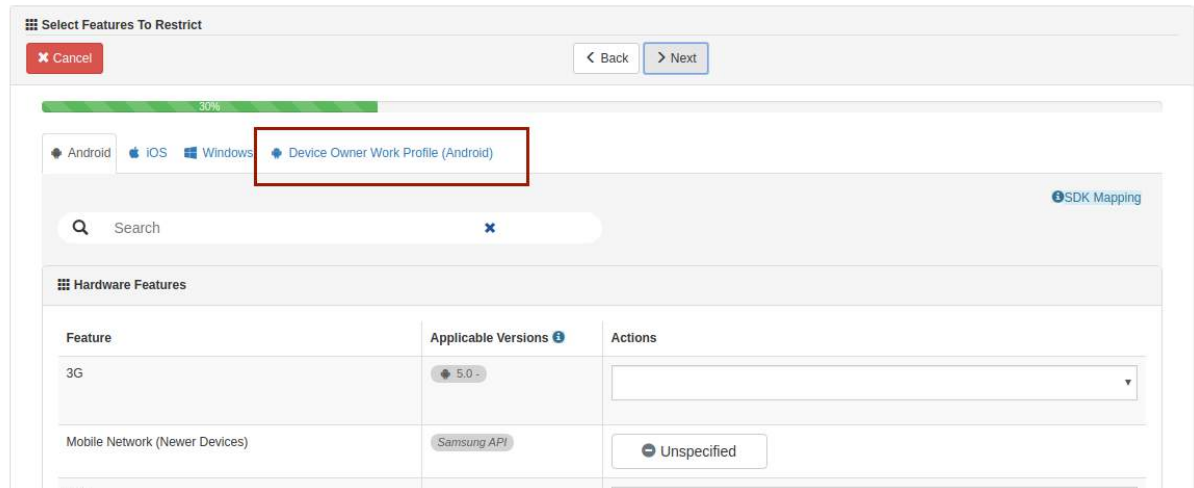
The screenshot displays the IOTIQ device management interface. On the left, the 'DEVICE DETAILS' section provides information about the device, including user name, display name, date joined, and various status indicators. The right side of the interface is divided into several sections: 'Common Android Features', 'Management Actions', 'Requests', 'Application Info Requests', and 'System Features'. The 'Management Actions' section is highlighted with a red box and contains two buttons: 'Personal Space' and 'Work Space'. Other actions include '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 includes '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	Off
Power Save Mode	Off
Google Accounts	0
Policies	0
Rejected Permissions	0
Build Flavor	Normal
Device Encryption Status	Active (Default Key)
Device Admin Status	On
Brightness	40%
Mock GPS Apps	Off
Mock GPS Enabled	Off
GPS Status	On
Bluetooth Status	On
Mobile Network Status	On
Wi-Fi Status	On
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
Model	(Venus Z20)
Manufacturer	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. Legen Sie eine neue Policy an. Klicken Sie dafür auf **Policies → Policies → New**.
2. Wählen Sie bei der Erstellung der neuen Richtlinie **Device Owner Work Profile (Android)** aus.



3. Weisen Sie die Richtlinie Benutzern/Gruppen zu (**Policies → Assign Policies**).
4. Die Richtlinie ist jetzt für Ihr Arbeitsprofil aktiv.