TROUBLESHOOTING WITH MOBILE DEVICE MANAGEMENT

About us

IOTIQ GmbH has been providing innovative software solutions for various application areas since 2017. Our mission is to support companies of all industries and sizes in taking the path towards digitalization with the right tools at hand and the right partner at their side.
In a world that is mobile and constantly becoming more so, security remains the top priority. To ensure this, we have developed MobiVisor - the mobile device management system that is just right for you.

**IOTIQ**

Smartly Done.

FACTORS TO CONSIDER

All kinds of MDM users as well as employers in this digital business world come across problems like malfunctioning devices, failed client installations, constantly crashing apps, and many more. To cope with these challenges, people used to take shelter in conventional methods such as emails, chat, and phone calls. But these traditional methods are not useful, especially if an employee is not able to follow the instructions for troubleshooting in complicated situations. Instead, we are here to guide you with simpler and more efficient solutions through troubleshooting with an MDM!

Let's talk about the ways you can tackle trouble in your MDM system:

KIOSK Mode

Troubleshooting a KIOSK provisioned device could happen by either invoking or revoking the KIOSK Mode on the device. The former is efficient because you can temporarily remove the KIOSK mode, fix the issue, then open it again. The latter is helpful whenever apps start continuously crashing. You can activate the KIOSK Mode to stabilize app screening.

e.g. Case Study: In one of the companies we work with, an employee activated the flight mode on the device – probably to save some battery – but later could not deactivate it. We simply removed the policy with the KIOSK Mode remotely and told the employee to turn off the flight mode in that time frame. After they had deactivated the flight mode, we installed the KIOSK Mode again and the device worked as it did before.
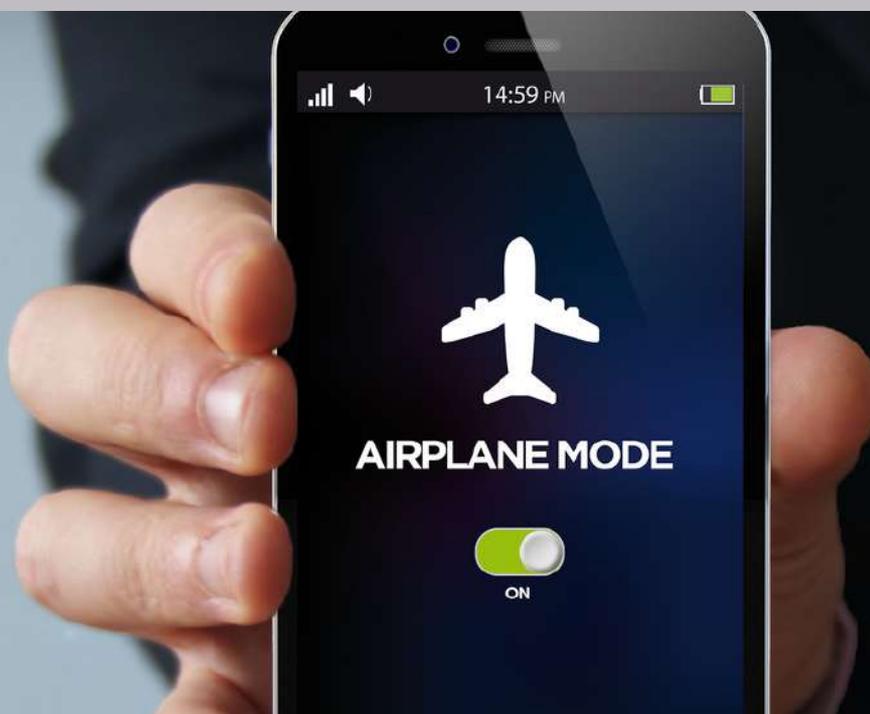
Remote Commands

Not only do office employees often work remotely, but their MDM administrators do not need to be in the office physically either to be able to help with problems. Sometimes employees are so far apart, especially when they work on construction sites, homecare, or nursing, that it's simply not possible for the administrator to reach them.

In this case, the administrator can send remote commands like the so-called 'lock and wipe' function: The admin uses the lock command in case the employee might cause more damage. They can remotely lock the device, being sure that the employee can solve their device's problem. If nothing else helps, the admin can use the wipe command and re-enroll the device again, often solving bigger problems. They can also put the device in the lost mode when the device is literally lost or was stolen.
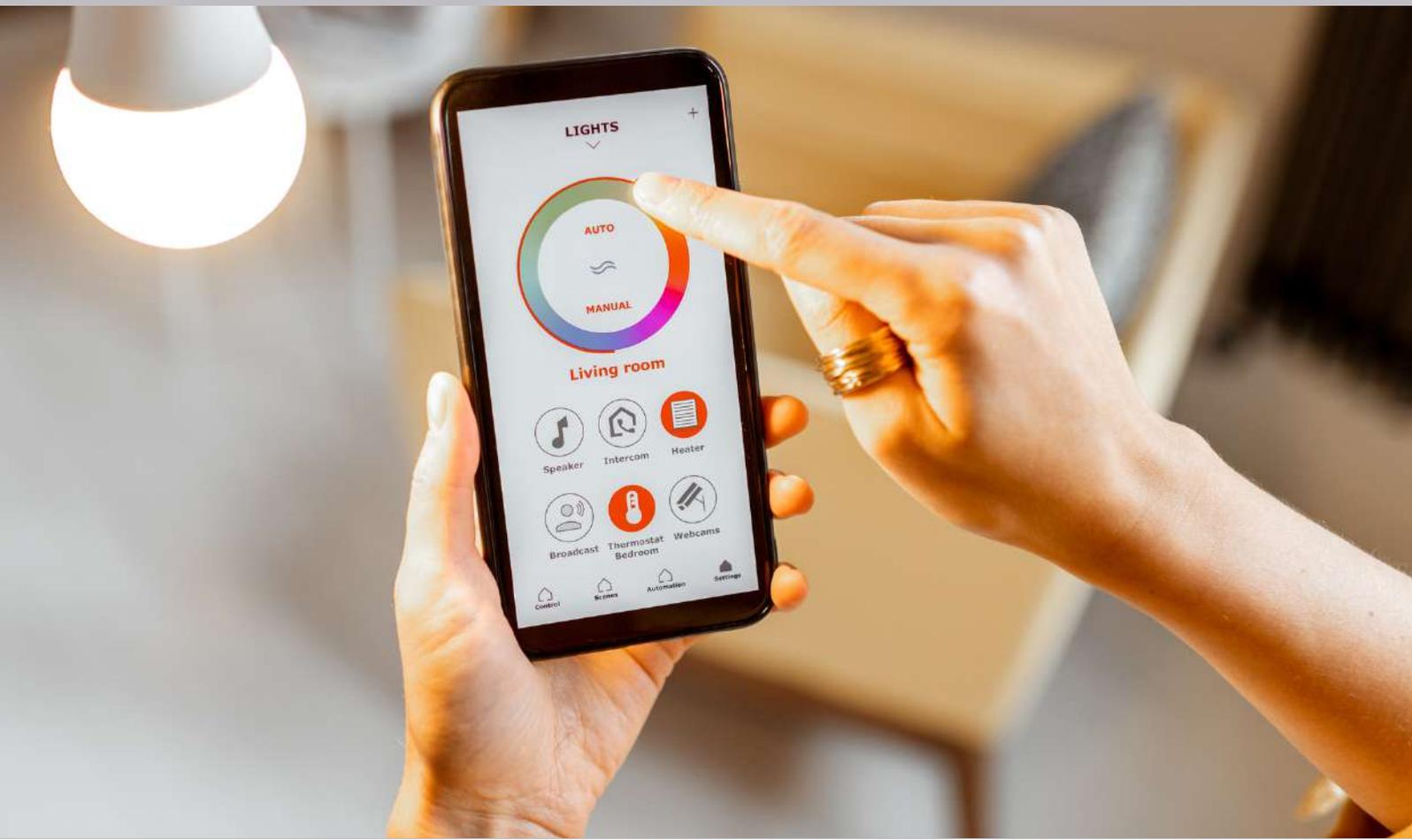
Backup Deduplication

Companies may confuse backup with duplication. But in the former, MDM works with a cloud computing system that enables you to backup your MDM-related data under one cloud. This means that two records of the data exist in two different places. Backing up the data keeps your storage place in relief and you will have more space for more complex data whereas the duplication of the data leads to wasted space and thus the lower and slower performance of the system.

Hotspots

Hotspots are physical locations where you can access the Internet via Wifi or a wireless local-area network. Since hotspots are complex designs, sometimes the system may have difficulty carrying them. If you especially use mobile phones or tablets in your business, you may be hesitant to create hotspots due to:

- Slower speed than Wifi
- Crowded storage space
- Data overcharges
- Higher consumption of battery
- Limitations on mobile phone's own functions (e.g. Your device might not be capable of supporting voice-phone calls and data simultaneously with the mobile hotspot.)
- Security concerns

Security Concerns

MDM, on the other hand, can help you monitor your hotspot. Alternatively, it can configure a virtual private network (VPN) for your company and all the control will be in your hands as an administrator. This way, you can create flexible data use restrictions, limit users to alter settings, restrict device connections and specify security protocols. You can also organize devices into groups and apply regulations based on roles, locations, or departments.

Do you want to know more?

Do you have questions about how MobiVisor and our extensions work, or are you unsure whether MobiVisor MDM fits your company and its challenges?

We are happy to assist you with advice and support! Just contact us by phone or e-mail.
We would also be happy to arrange a personal presentation appointment with you and provide you with a test environment of MobiVisor without obligation.

Toni Voß
toni@iotiq.de
+49 1578 3020995

Saskia Riechers
saskia@iotiq.de
+49 176 1500 6080