Troubleshooting with MobiVisor MDM for Android devices: Handbook

Android devices integrated into an MDM can be fully secured. However, end users may still report some issues to the IT administrator. In this guide, we will look at the most common issues and explain how you can solve them using MobiVisor MDM.

MOBIVISOR

Android Enterprise
Silver partner

IOTIQ GmbH • Emilienstraße 13 • 04107 Leipzig • Phone: +49 341 99160100 • Mail: info@iotiq.de • Web: iotiq.de

Password and Security

With MobiVisor MDM, you can configure a password policy that requires the user to set a password before using the device.

Forgotten Password

If the user has forgotten their device password, the admin can reset it. To do this, go to **Device details > Change passcode**. You can either assign a new one here or simply **send an empty field**.
Sending the empty field deletes the password and the user can set a new one.
Note: First, you must remove the password policy from the device, if one exists.

Password token not active

Usually, the password token is activated during device setup. However, sometimes problems occur at this point and the token is not active. You will see this as a warning in both the domain and the MobiVisor app.
We recommend fixing this, as the password can otherwise not be reset via MDM, for example.

Fixing this

Open the MobiVisor Client app on your device and select the three-dot menu in the top right corner.
Select **"Reset Password Token"**.
If a password policy has been assigned, the user must confirm the token update with the device's PIN (applies to BYOD, COWP and DO devices).

Password and Security

Forgotten SIM PIN and PUK

The SIM PIN is assigned by the mobile operator and may not be read by the MDM for data protection reasons. To prevent the SIM PIN from being lost, we recommend that you **enter it in the notes of the respective device** in MobiVisor MDM.

If the SIM PIN is forgotten, the device can still be accessed via MobiVisor. We recommend temporarily removing the SIM card to make the device accessible again. You will then need to **contact your mobile phone provider**.

Despite password, apps remain grayed out

If a password policy is assigned to the devices via MDM, the apps will only be unlocked when the user assigns a password. Sometimes the apps remain grayed out after a password has been assigned. If this happens, you must first **create a new group**.

To do this, you can simply copy the device's previous group.

Now create a policy in the policies called **“Blocklist apps”**, add the apps to this list and apply the policy.

Wait until the policy is applied to the device.

Then remove the policy.

The user should then try to set a password again.

Connection to the MDM

In order for devices enrolled in MDM to receive all security policies and apps, they require a connection to the MDM.
Don't worry: Even if the connection to the MDM is lost, the policies applied to date remain active.

Commands from the MDM do not reach the device

If commands don't make it through to the MDM, this is usually quickly noticed because users provide feedback about missing apps and more. However, you can always check the current status of a command in your MobiVisor domain.
To do this, go to the tab Commands, where you'll see a list of all outgoing commands, which you can also filter by user, date, etc. There are different command statuses:

For the push server:

The command is still on its way to the device via the Android server. This status will usually change automatically to "**Success**" after some time. If the command is set to "**At the push server**" for a long time, you must check the device's connection to the Internet and to MobiVisor.
To do this, open the MobiVisor app on the affected device, click on the 3-dot menu in the top right corner and tap "**Synchronize Push Token**".

Server Error:

In this case, a debug log of the device must be created. Please contact your MobiVisor team directly for this.

Connection to the MDM

Guidelines are not applied to the device

When you change policies and assign them to devices, they are sometimes not applied immediately. To speed up the process, you can go to the device list in the **MobiVisor domain** and select the affected devices there.
The “**Actions**” button will then appear in the top left corner. Click on it and select “**Update policies**”. Alternatively, you can also use the “**Sync**” button directly in the MobiVisor app.

The device is no longer connected to MobiVisor:

1. Due to prolonged non-use:

If the device is not used for a longer period of time, the connection to the MDM may be lost. If the device is not used for a long period of time, the connection to the MDM may be lost. In this case, the device will be marked in **red** in the device list in the MobiVisor domain.
You can restore the connection by going to the device details and selecting “**Renew session.**”
If you have the device, it's often sufficient to reopen the MobiVisor app. Please note that commands you sent to the device while offline may not be received. In this case, **resend the commands** once the device is back online.

2. By logging out of the user:

Here, the end user can scan the user QR code again to renew their login. Alternatively, they can execute the "**Renew Session**" command on the device details page in the MobiVisor domain.

App Installation

One of the main features of an MDM is centralized app management. Not only can apps be distributed to all company devices simultaneously, but it can also be specified which apps users are allowed to use.

App is not installed

There can be various reasons why a particular app, or several apps, won't install using the usual method.
Therefore, it can be helpful to go through the following checklist:

1. Has the app been approved for the company in the Google Play Store? *(Viewable in the app list)*
2. Is the app an Android Enterprise app? *(Viewable in the app list)*
3. Is the app possibly blacklisted? *(See the guidelines)*
4. Has the app been added to the correct group in the MobiVisor domain? *(Viewable in groups)*
5. Does the app appear in the app catalog of the device's MobiVisor client app? If so, try installing the app from there.

If none of the above points help to resolve the issue, please contact the MobiVisor team.

APKs are not installed

To install APKs, you must activate the "**Apps outside the Play Store**" policy. If this has already happened and the app still won't install, this indicates compatibility issues with the APK. It may for example be too large to upload to MobiVisor.
If the APK upload fails repeatedly, please contact the MobiVisor MDM team.

App Installation

Apps are not uninstalled on individual devices

Once an app has been added to a group, it cannot be uninstalled from a device as long as that device is in the group.
To uninstall only a specific app, first **copy the group.**
Then remove all other devices from the copied group, leaving only the device in question in it.
Now **remove the device** in question from the original group.
Now go back to the copied group and remove the app from there.
You can do this via the "**Applications**" tab. Save your settings.

If you remove an app from a group, it will be automatically uninstalled from all devices. We therefore recommend the above procedure if the change only affects individual devices.

Apps do not work as intended

If apps cannot be used as intended despite successful installation, there can be a variety of reasons. Unfortunately, as an MDM, we don't have full access to the apps, so we can only offer a few tips.

App cannot be opened

If an app cannot be opened even though it has been installed on the device, there are two possible reasons for this.

Firstly, the **app may be on a blacklist**, which can be checked in the MDM guidelines.

If the app was blacklisted after it was installed, it will not be automatically uninstalled, which is why it can still be found on the device.

Another possible cause is **compatibility issues** with the app. Check to make sure that the latest version is installed.

App keeps crashing unexpectedly

Here, too, the most likely cause is that the installed app version is incompatible with the device. Check whether you need to **update the device's operating system** (visible in the device details) and install the latest version of the app.

App configurations do not work

You can configure specific apps using MDM. There are several options for doing this.

If the problem affects your **Exchange configuration for your email app**, first check whether you have assigned the Exchange configuration to a policy and whether the email app is installed.

If so, contact the MDM team directly if you have any configuration issues. If you want to configure an app such as Google Chrome, you must then send the app to the devices again using the **installation command** for the configuration to take effect.

Apps do not work as intended

An app cannot perform its basic functions

Some apps require access to certain permissions, such as contacts, camera, or gallery.
If an app, such as a messenger, cannot send photos, first check the permissions in the device settings. Activate these if necessary.

If the permissions are already granted, you may need to enable system apps:
1. In the MobiVisor domain, go to **Settings > General System Settings**.
2. Find the application functions.
3. Select “**Enable System Apps**” to enable all system apps.
4. To enable individual system apps, select “**Enabled System Applications**” and select the corresponding package names.

The package names of system apps can be accessed under the device details:
1. Select “**Read system apps**”
2. Click “**Show fetched system apps**”
3. Search for "**Phone**" to display all package names belonging to the phone app. Use the small “**+**” sign to add these to the predefined apps.
4. **Add the package names** in the system app settings (see above).

You can also perform this procedure for individual devices. In this case, the procedure is similar:
1. Search for the **package name** and add it to **predefined apps**
2. **Enable** the system app in the policies
3. **Send updated policy** to the devices and, if necessary, use sync in the MobiVisor client app (on the device).

KIOSK Mode

KIOSK mode is used to restrict the user interface of the devices. This is particularly useful when the devices are intended for a specific purpose, such as a point of sale.

An app does not appear in KIOSK mode

In this case, check whether the app has been assigned to the appropriate group and the desired KIOSK mode. If the app is still in the group, you'll need to add it first.
To do this, go to Groups in your MobiVisor domain and click "**Edit**" for the desired group.
Add the app from the app list in the "**Applications**" tab.

To check if the app is also assigned to KIOSK mode, go to **Policies > Kiosk Mode**. Scroll all the way to the right and move the scroll bar all the way to the right until you see the package names of the apps.
If the corresponding package isn't already there, you still need to add it to KIOSK mode. To do this, click "**Edit**" for the corresponding KIOSK mode.
In the right column, you'll find all the package names from which you can select which ones you want to add to KIOSK mode.

After adding the app to KIOSK mode, you need to update the policies or KIOSK mode on the devices. To do this, go to the device list, select the relevant devices, and then select “**Actions**” (top left) > “**Update Kiosk Mode**”.

KIOSK Mode

KIOSK mode is not applied

There are several possible causes for this problem.

Please proceed as follows:
1. Check if the device has a stable internet connection.
2. Does the device appear as online in MobiVisor? If not, you must first reconnect to the MDM (update the "**Push Token**" in the MobiVisor app).
3. Has KIOSK mode been assigned to a policy and this policy assigned to a group?
4. If these things apply and KIOSK mode is not applied, open the MobiVisor app on the device and press “**Sync**”.

If you have done all of this and KIOSK mode is still not applied to the device, please contact the MDM team.

KIOSK mode cannot be removed

Typically, you can simply remove KIOSK mode by removing it from the respective group's policies.

If this doesn't remove KIOSK mode, we recommend updating the policies first. Also, ensure the device has a stable internet connection.

If the process takes an unusually long time, you can also check the command list to see if the command is running correctly.

KIOSK Mode

Home & Back Button

The so-called Device Owner or KIOSK mode restricts the device's functionality according to the administrator's specifications. Accordingly, the Home and Back buttons also behave differently, but this is not a bug.

Home button in KIOSK mode:

In KIOSK mode start screen: Does not trigger any action
App opened: Returns to KIOSK Start Screen

Back button in KIOSK mode:

In KIOSK mode start screen: Does not trigger any action
App opened in the start screen: Returns to the KIOSK mode start screen
App opened in an action screen, e.g. chat history: Returns to previous page

Device is restricted too much

Mobile devices are secured with policies to prevent misuse. However, this also means that, depending on the company's privacy policy, many functions are restricted, like the ability to change system settings, use an unauthorized internet connection, or use USB debugging. If the device is too restricted, MobiVisor displays the corresponding warning on the device page.

In terms of troubleshooting, this means that special care is required for such devices, and prevention is easier than troubleshooting.

This means:
1. Make sure that these devices are **always connected to the Internet** (via mobile data or Wi-Fi)
2. Make sure to open the MobiVisor app from time to time to keep the **push token** up to date.
3. If you have a password policy, instruct employees to **tell you the password** when they leave the company or return the device.

Device is frozen (SAMSUNG)

In practice, unfortunately, it often happens that a device can no longer be unlocked and cannot be reset even by the security policies.
In this case, please contact the MDM team.

Theft and loss

It's not always technical issues that require troubleshooting. In other cases, such as theft or loss of a device, you need to act quickly to prevent the data on your mobile device from being compromised.
You can use the following features to help:

1. Lost Mode

To enable Lost Mode, you need to go to the device details page. There you can enable "**MDM Lost Mode**" for Device Owner devices. You can enter a message and a phone number to give an honest finder the opportunity to return the device.
You can also assign a password to remove Lost Mode once the device is found. Lost Mode prevents the device from being used in the meantime.

2. Lock

If the device is stolen, lost, or tampered with, you can lock it with a command. This makes it unusable. This feature is useful, for example, if a thief tries to replace the SIM card.
You can configure a "**breach**" in the MDM to trigger the device lock.

3. Ringing of the device

This feature can be used to locate the device. The mobile device will **ring** and the **flashlight** will be activated to attract attention with a light signal. It doesn't matter whether the device was previously muted by the user.

4. Remote Wipe

If the device can no longer be found, you can reset it to factory settings using the "**Erase**" command via MDM. Even if the SIM card is replaced, the MDM remains on the device, along with all its settings.
As soon as the internet connection is restored, the erase command is executed, preventing unauthorized access to any data.

Email account cannot be added

To add a second email account on a work device, the policy function “**Change account**s” has to be allowed.

Our proposed solutions do not lead to the desired success?

If you need more information and support, you can contact us at any time at mds@iotiq.de.