Troubleshooting mit MobiVisor MDM für Android-Geräte: Handbuch

Android-Geräte, die in einem MDM eingebunden sind, können über dieses vollumfänglich abgesichert werden. Dennoch kann es dazu kommen, dass die Enduser dem IT-Admin einige Probleme melden. In diesem Guide beleuchten wir die häufigsten Anfragen dieser Art und erklären, wie Sie diese mithilfe von MobiVisor MDM lösen können.

MOBIVISOR

Android Enterprise
Silver partner

IOTIQ GmbH • Emilienstraße 13 • 04107 Leipzig • Telefon: 0341 99160100 • Mail: info@iotiq.de • Web: iotiq.de

Passwort und Sicherheit

Mit MobiVisor MDM können Sie eine Passwortrichtlinie konfigurieren, die vorgibt, dass der User vor Nutzung des Gerätes ein Passwort festlegen muss.

Passwort vergessen

Hat der User sein Gerätepasswort vergessen, kann dies vom Admin zurückgesetzt werden.
Gehen Sie dazu zu den **Gerätedetails > Passcode** ändern.
Sie können hier entweder ein neues vergeben oder einfach das leere Feld senden. Das Senden des leeren Feldes löscht das Passwort und der User kann sich ein Neues vergeben.
Achtung: Im Vorfeld müssen Sie, sofern vorhanden, die Passwortrichtlinie vom Gerät entfernen.

Passwort-Token nicht aktiv

Im Normalfall aktiviert sich das Passwort-Token bei der Einrichtung des Gerätes. Manchmal kommt es allerdings an dieser Stelle zu Problemen und das Token ist nicht aktiv – dies sehen Sie sowohl in der Domain, als auch in der MobiVisor App als Warnhinweis.
Wir empfehlen dies zu beheben, da sonst z.B. das Passwort nicht per MDM zurückgesetzt werden kann.

Behebung

Öffnen Sie die MobiVisor Client App auf dem Gerät und wählen Sie das 3-Punkte Menü oben rechts. Wählen Sie hier “Passwort Token zurücksetzen”.
Wurde eine Passwortrichtlinie vergeben, muss der User die Aktualisierung des Token mit der PIN des Gerätes bestätigen (gilt für BYOD-, COWP- und DO-Geräte).

Passwort und Sicherheit

SIM-PIN und PUK vergessen

Der SIM-PIN wird vom Mobilfunkbetreiber vergeben und darf aus Datenschutzgründen nicht vom MDM ausgelesen werden. Um zu verhindern, dass der SIM-PIN verloren geht, empfehlen wir, diesen bei Einrichtung der Geräte in den **Notizen des jeweiligen Gerätes** in MobiVisor MDM abzulegen.

Wurde der SIM-PIN vergessen, ist das Gerät dennoch per MobiVisor MDM erreichbar. Wir empfehlen dazu, dass die SIM-Karte temporär entfernt wird, um das Gerät wieder zugänglich zu machen. Im Anschluss müssen Sie sich zur Abfrage von PIN und PUK an Ihren **Mobilfunkanbieter** wenden.

Trotz Passwort bleiben Apps ausgegraut

Wird eine Passwortrichtlinie per MDM an die Geräte vergeben, schalten sich die Apps erst frei, wenn der User ein Passwort vergibt. Manchmal bleiben die Apps noch immer grau, nachdem ein Passwort vergeben wurde.

Wenn dies passiert, müssen Sie das betroffene Gerät zunächst in eine **extra angelegte Gruppe** umziehen. Dafür können Sie zum Beispiel die bisherige Gruppe des Gerätes einfach kopieren.
Erstellen Sie nun in den Richtlinien eine Richtlinie mit “Sperrliste Apps”, setzen Sie die Apps auf diese Liste und wenden Sie die Richtlinie an.
Warten Sie, bis die Richtlinie vom Gerät angewendet wird. Danach entfernen Sie die Richtlinie wieder.
Im Anschluss soll der User nochmal versuchen, ein Passwort zu vergeben.

Verbindung mit dem MDM

Damit die im MDM registrierten Geräte alle Sicherheitsrichtlinien und Apps empfangen, benötigen Sie eine Verbindung mit dem MDM.
Keine Sorge: Auch wenn die Verbindung mit dem MDM mal verloren geht, bleiben die bis dato angewandten Richtlinien aktiv.

Befehle vom MDM kommen nicht zum Gerät durch

Kommen Befehle nicht zum MDM durch, fällt dies in der Regel schnell auf, weil die User eine Rückmeldung bezüglich fehlender Apps etc. geben. Sie können den aktuellen Stand eines Befehls jedoch auch immer in Ihrer MobiVisor Domain überprüfen.
Gehen Sie dazu zum Tab **Befehle**. Dort sehen Sie eine Liste mit allen ausgehenden Befehlen, die Sie auch nach User, Datum usw. Filtern können. Es gibt verschiedene Befehlsstati:

Beim Push Server:

Der Befehl befindet sich noch über den Android-Server auf dem Weg zum Gerät. Dieser Status wird sich in der Regel nach einiger Zeit von selbst zu "**Erfolg**" wandeln.
Steht der Befehl lange auf "**Beim Push Server**", müssen Sie die Verbindung des Gerätes zum Internet und zu MobiVisor überprüfen.
Öffnen Sie hierzu die MobiVisor App auf dem betroffenen Gerät, klicken Sie auf das 3-Punkte Menü oben rechts und tippen sie "Push Token synchronisieren" an.

Server Error:

In diesem Fall muss ein Debuglog des Gerätes angefertigt werden. Wenden Sie sich daher direkt an Ihr MobiVisor Team.

Verbindung mit dem MDM

Richtlinien werden nicht auf das Gerät angewandt

Ändern Sie Richtlinien und weisen diese den Geräten zu, werden diese manchmal nicht sofort angewandt.
Um den Prozess zu beschleunigen, können Sie in der **MobiVisor-Domain** in die **Geräteliste** gehen und dort die betroffenen Geräte auswählen.
Im Anschluss erscheint oben Links der Button "**Aktionen**". Diesen klappen Sie einmal aus und wählen "**Richtlinien aktualisieren**".
Alternativ können Sie auch direkt in der **MobiVisor App** den "**Sync**" Button verwenden.

Das Gerät ist nicht mehr mit MobiVisor verbunden

1. Durch längere Nichtbenutzung:

Wird das Gerät längere Zeit nicht mehr genutzt, kann es sein, dass die Verbindung zum MDM verloren geht. In diesem Fall wird Ihnen das Gerät in der Geräteliste in der **MobiVisor-Domain** in rot markiert angezeigt.
Sie können die Verbindung wiederherstellen, indem Sie in die Gerätedetails gehen und "**Sitzung erneuern**" auswählen.
Liegt Ihnen das Gerät vor, reicht es zudem oft, die MobiVisor App erneut zu öffnen. Bitte beachten Sie, dass Befehle, die Sie an das Gerät während der Offline-Phase gesendet haben, unter Umständen nicht zum Gerät durchkommen. In diesem Fall senden Sie die Befehle erneut, wenn das Gerät wieder online ist.

2. Durch Abmelden des Nutzers:

Hier kann der Endnutzer erneut den User-QR-Code scannen, um die Anmeldung zu erneuern. Alternativ können Sie in der MobiVisor Domain auf der Gerätedetailseite den Befehl "Sitzung erneuern" ausführen.

App-Installation

Eine der Hauptaufgaben eines MDMs ist die zentralisierte App-Verwaltung. Es können nicht nur die Apps gleichzeitig an alle Unternehmensgeräte verteilt werden, sondern es kann auch festgelegt werden, welche Apps die User verwenden dürfen.

App wird nicht installiert

Dass eine bestimmte App oder gleich mehrere Apps sich über den gewohnten Weg nicht installieren, kann verschiedene Gründe haben. Deshalb ist es oft hilfreich, die folgende Checkliste durchzugehen:

1. Wurde die App im Google Play Store für das Unternehmen freigegeben? *(Einsehbar in Appliste)*
2. Ist die App eine Android Enterprise App? *(Einsehbar in Appliste)*
3. Befindet sich die App unter Umständen auf einer Blacklist? *(Einsehbar in den Richtlinien)*
4. Wurde die App der richtigen Gruppe in der MobiVisor Domain hinzugefügt? *(Einsehbar in Gruppen)*
5. Erscheint die App im App-Katalog der MobiVisor Client-App des Geräts? Falls ja, versuchen Sie die App hierüber zu installieren.

Wenn keiner der oben genannten Punkte zur Lösung beiträgt, wenden Sie sich bitte an das MobiVisor Team.

APKs werden nicht installiert

Um APKs zu installieren, müssen Sie in den Richtlinien "**Apps außerhalb des Play Stores**" aktivieren. Ist dies bereits geschehen und die App installiert sich trotzdem nicht, weist dies auf Kompatibilitätsprobleme mit der APK hin. Diese kann zum Beispiel zu groß sein, um sie in MobiVisor hochzuladen. Sollte der APK-Upload wiederholt nicht funktionieren, wenden Sie sich bitte an das MobiVisor MDM Team.

App-Installation

Apps werden auf einzelnen Geräten nicht deinstalliert

Wurde eine App zu einer Gruppe hinzugefügt, kann sie von einem Gerät nicht deinstalliert werden, solange dieses Gerät in der Gruppe ist.
Um nur eine bestimmte App zu deinstallieren, kopieren Sie die Gruppe zunächst. Entfernen Sie dann alle anderen Geräte aus der kopierten Gruppe, sodass nur das betreffende Gerät in dieser verbleibt.
Entfernen Sie nun das betreffende Gerät aus der Original-Gruppe.
Anschließend rufen Sie wieder die kopierte Gruppe auf und entfernen von dort die App. Dies geschieht über den Tab “Anwendungen”.
Speichern Sie Ihre Einstellungen.

Entfernen Sie eine App aus einer Gruppe, dann wird diese automatisch bei allen Geräten deinstalliert. Wir empfehlen daher oberes Vorgehen, wenn die Änderung nur einzelne Geräte betrifft.

Apps funktionieren nicht wie vorgesehen

Können Apps trotz erfolgreicher Installation nicht wie gewünscht bedient werden, können ebenfalls vielfältige Ursachen dahinterstecken. Als MDM haben wir leider keinen vollumfänglichen Zugriff auf die Apps selbst, weswegen wir nur einige Tipps geben können.

App kann nicht geöffnet werden

Kann eine App nicht geöffnet werden, obwohl sie auf dem Gerät installiert wurde, kann dies zwei mögliche Auslöser haben. Zum einen kann die App auf einer Blacklist sein, was in den Richtlinien im MDM überprüft werden kann. Wurde die **App auf eine Blocklist** gesetzt, nachdem sie installiert wurde, wird sie nicht automatisch deinstalliert, weshalb sie noch auf dem Gerät zu finden ist.
Eine andere mögliche Ursache sind **Kompatibilitätsprobleme** der App. Überprüfen Sie hier, ob die **aktuellste Version** installiert wurde.

App crashed immer wieder unvorhergesehen

Auch hier ist die wahrscheinlichste Ursache, dass die installierte App-Version nicht mit dem Gerät kompatibel ist. Überprüfen Sie, ob Sie das Betriebssystem des Gerätes ggf. updaten müssen *(einsehbar in den Gerätedetails)* und installieren Sie die neueste Version der App.

App-Konfigurationen funktionieren nicht

Sie können bestimmte Apps per MDM konfigurieren. Dabei gibt es verschiedene Möglichkeiten. Betrifft das Problem Ihre **Exchange-Konfiguration für Ihre E-Mail App**, überprüfen Sie zunächst, ob Sie die Exchange-Konfig einer Richtlinie zugewiesen und auch ob die E-Mail-App installiert ist.
Ist dies der Fall, wenden Sie sich mit Problemen mit der Konfiguration direkt an das MDM-Team. Wenn Sie eine App wie zum Beispiel Google Chrome konfigurieren wollen, müssen Sie die App im Anschluss noch einmal per Installationsbefehl an die Geräte senden, damit die Konfiguration wirksam wird.

Apps funktionieren nicht wie vorgesehen

Eine App kann ihre Grundfunktionen nicht ausführen

Manche Apps benötigen Zugriff auf bestimmte Berechtigungen, wie zum Beispiel Kontakte, Kamera oder Galerie. Kann eine App, wie etwa ein Messenger, keine Fotos versenden, überprüfen Sie zunächst die **Berechtigungen in den Einstellungen des Gerätes**. Aktivieren Sie diese gegebenenfalls.

Sind die Berechtigungen bereits gegeben, kann es sein, dass Sie die entsprechenden **System-Apps aktivieren** müssen:
1. Rufen Sie in der MobiVisor Domain **Einstellungen > Allgemeine Systemeinstellungen** auf
2. Suchen Sie die **Anwendungsfunktionen**
3. Wählen Sie “Aktivieren Sie System-Apps” um **alle** System-Apps zu aktivieren
4. Um **einzelne** System-Apps zu aktivieren, wählen Sie “Aktivierte Systemanwendungen” und wählen Sie die entsprechenden Package-Names aus.

Die **Package-Names der System-Apps** können Sie unter den Gerätedetails aufrufen:
1. Wählen Sie “System-Apps auslesen”
2. Klicken Sie “Geholte System-Apps anzeigen”
3. Suchen Sie z.B. nach Telefon, um alle Package-Names, die zur Telefon-App gehören, anzuzeigen. Über das kleine + fügen Sie diese den vordefinierten Apps hinzu und können somit die Package-Names in den System-App Einstellungen (s.oben) hinzufügen.

Sie können dieses **Vorgehen auch für einzelne Geräte** vornehmen. In diesem Fall ist das Vorgehen ähnlich:
1. Package-Name suchen und zu vordefinierten Apps hinzufügen
2. In den Richtlinien die System-App aktivieren
3. Aktualisierte Richtlinie an die Geräte senden und ggf. Sync in MobiVisor Client-App (auf dem Gerät) nutzen

KIOSK-Modus

Der KIOSK-Modus wird verwendet, um die Benutzeroberfläche der Geräte einzuschränken. Dies ist insbesondere dann sinnvoll, wenn die Geräte nur für einen bestimmten Zweck, zum Beispiel als Point of Sales, eingesetzt werden sollen.

Eine App erscheint nicht im KIOSK-Modus

Überprüfen Sie in diesem Fall, ob die App der **entsprechenden Gruppe** und dem gewünschten **KIOSK-Modus zugewiesen** wurde.
Ist die App noch in der Gruppe, dann müssen Sie diese zunächst hinzufügen. Gehen Sie dazu in Ihrer MobiVisor Domain auf Gruppen und klicken Sie bei der gewünschten Gruppe auf "**bearbeiten**". Fügen Sie im Tab "**Anwendungen**" die App aus der Appliste hinzu.

Um zu überprüfen, ob die App auch dem KIOSK-Modus zugewiesen ist, gehen Sie zu **Richtlinien > Kioskmodus**. Scrollen Sie ganz nach rechts und bewegen Sie den Scrollbar ganz nach rechts, bis Sie die Package Names der Apps sehen. Ist das entsprechende Package noch nicht dort zu sehen, müssen Sie es noch zum KIOSK-Modus hinzufügen. Klicken Sie dafür beim entsprechenden KIOSK-Modus "**Bearbeiten**" an. In der rechten Spalte finden Sie alle Package Names, aus denen Sie auswählen können, welche zum KIOSK-Modus hinzugefügt werden sollen.

Nachdem Sie die App zum KIOSK-Modus hinzugefügt haben, müssen Sie die Richtlinien bzw. den KIOSK-Modus auf den Geräten aktualisieren. Gehen Sie dazu in die Geräteliste, wählen Sie die entsprechenden Geräte aus und wählen Sie bei "**Aktionen**" (oben links) "**Kioskmodus aktualisieren**" aus.

KIOSK-Modus

KIOSK-Modus wird nicht angewendet

Für dieses Problem kann es verschiedene Ursachen geben. Gehen Sie daher wie folgt vor:

1. Überprüfen Sie, ob das Gerät eine stabile Internetverbindung hat.
2. Wird das Gerät bei MobiVisor als online angezeigt? Wenn nein, muss erst wieder eine Verbindung zum MDM hergestellt werden *(In MobiVisor App "Push Token" aktualisieren).*
3. Wurde der KIOSK-Modus einer Richtlinie zugewiesen und diese Richtlinie einer Gruppe zugewiesen?
4. Treffen diese Dinge zu und der KIOSK-Modus wird nicht angewandt, öffnen Sie die MobiVisor-App auf dem Gerät und betätigen Sie "Sync".

Wenn Sie all dies durchgeführt haben und der KIOSK-Modus noch immer nicht auf dem Gerät angewandt wird, wenden Sie sich bitte an das MDM-Team.

KIOSK-Modus lässt sich nicht entfernen

Im Regelfall können Sie den KIOSK-Modus einfach entfernen, indem Sie diesen aus den Richtlinien der jeweiligen Gruppe entfernen. Wird der KIOSK-Modus mit diesem Vorgang nicht entfernt, empfehlen wir, zunächst die Richtlinien zu aktualisieren.

Stellen Sie zudem sicher, dass das Gerät eine stabile Internetverbindung aufweist. Sollte der Vorgang ungewöhnlich lange dauern, können Sie auch die Befehlsliste überprüfen, ob der Befehl ordnungsgemäß durchläuft.

KIOSK-Modus

Home & Back Button

Der sogenannte Device Owner bzw. Gerätebesitzer KIOSK-Modus schränkt die Funktionalität des Gerätes entsprechend der Vorgaben des Admins ein. Dementsprechend verhalten sich auch der Home- und der Back-Button unterschiedlich, was jedoch keinen Fehler darstellt.

Home-Button im KIOSK-Modus:

Im KIOSK-Modus Start Screen: Löst keine Aktion aus
App geöffnet: Führt zurück zu KIOSK Start Screen.

Back-Button im KIOSK-Modus:

Im KIOSK-Modus Start Screen: Löst keine Aktion aus
App geöffnet im Start Screen: Führt zurück zum KIOSK-Modus Start Screen
App geöffnet in einem Aktionsscreen, z.B. Chatverlauf: Führt zurück zu vorheriger Seite

Gerät ist zu stark eingeschränkt

Mobile Geräte werden mit Richtlinien so abgesichert, dass kein Missbrauch mit diesen geschehen kann. Dies bedeutet aber auch, dass abhängig von den Datenschutzrichtlinien des Unternehmens viele Funktionen eingeschränkt werden. So zum Beispiel: Die Möglichkeit, die Systemeinstellungen zu verändern, eine nicht genehmigte Internetverbindung zu verwenden oder USB-Debugging zu verwenden. Sind die Geräte zu stark eingeschränkt, zeigt Ihnen MobiVisor die entsprechende Warnung auf der Geräteseite an.

In Bezug auf das Troubleshooting bedeutet dies, dass für solche Geräte besondere Vorsicht geboten ist und Vorbeugung einfacher ist, als die Probleme zu suchen. Dies bedeutet:

1. Stellen Sie sicher, dass diese Geräte stets mit dem Internet verbunden sind (per Mobile Daten oder WLAN)
2. Achten Sie darauf, dass die MobiVisor App von Zeit zu Zeit geöffnet wird, um den Push-Token aktuell zu halten.
3. Wenn Sie eine Passwortrichtlinie vergeben haben, weisen Sie die Mitarbeitenden an, Ihnen das Passwort beim Verlassen des Unternehmens bzw. der Rückgabe des Gerätes mitzuteilen.

Gerät ist eingefroren (SAMSUNG)

In der Praxis kommt es leider immer wieder vor, dass ein Gerät nicht mehr entsperrt und auch durch die Sicherheitsrichtlinien nicht mehr zurückgesetzt werden kann. In diesem Fall wenden Sie sich bitte an das MDM-Team.

Diebstahl und Verlust

Nicht immer sind es technische Probleme, die ein Troubleshooting erfordern. In anderen Fällen, wie einem Diebstahl oder dem Verlust des Gerätes, muss schnell gehandelt werden, um zu verhindern, dass die Daten auf dem mobilen Gerät kompromittiert werden. Dazu können Sie folgende Funktionen nutzen:

1. Lost-Modus

Um den Lost-Modus zu aktivieren, müssen Sie auf die Geräte-Detailseite gehen. Dort können Sie bei Device Owner Geräten den “MDM Lost Modus” aktivieren. Sie können eine Nachricht und eine Telefonnummer angeben, um einem ehrlichen Finder die Möglichkeit zu geben, das Gerät zurückzugeben.
Mit dem Passwort, welches Sie ebenfalls vergeben, kann der Lost-Modus bei Auffinden des Geräts wieder entfernt werden. Der Lost-Modus verhindert, dass das Gerät in der Zwischenzeit verwendet werden kann.

2. Sperren

Bei Diebstahl oder Verlust oder auch wenn eine unerlaubte Handlung auf dem Gerät ausgeführt wird, kann das Gerät mit einem Befehl gesperrt werden. Hierbei kann das Gerät nicht mehr verwendet werden.
Diese Funktion ist zum Beispiel dann sinnvoll, wenn ein Dieb versucht, die SIM-Karte auszutauschen. Sie können für solche Fälle einen “Verstoß” im MDM konfigurieren, der die Sperrung des Gerätes auslöst.

3. Klingeln des Geräts

Diese Funktion kann zum Auffinden des Gerätes genutzt werden. Dabei klingelt das mobile Gerät und die Taschenlampe wirkt aktiviert, um auch über ein Lichtsignal auf sich aufmerksam zu machen. Dabei spielt es keine Rolle, ob das Gerät zuvor vom Nutzer stumm geschaltet wurde.

Diebstahl und Verlust

4. Remote Wipe

Ist das Gerät nicht mehr auffindbar, können Sie es mit dem Befehl “Löschen” per MDM auf die Werkseinstellungen zurücksetzen. Auch wenn die SIM-Karte ausgetauscht wird, bleibt das MDM auf dem Gerät und somit auch alle Einstellungen.
Sobald das Internet also wieder mit dem Internet verbunden wird, geht der Lösch-Befehl durch und es können keine Daten von Unbefugten missbraucht werden.

E-Mail Account lässt sich nicht hinzufügen

Um einen zweiten E-Mail Account auf einem Arbeitsgerät hinzuzufügen, muss die Richtlinienfunktion “**Konten ändern**” erlaubt werden.

Unsere Lösungsvorschläge führen nicht zum gewünschten Erfolg?

Benötigen Sie mehr Infos und Unterstützung? Sie können uns jederzeit unter mds@iotiq.de erreichen.