

G-Lock / G-Lock Pryme App Issues

G-Lock & Pryme Issues

1. Not yet getting updates on **android 15(OPPO,REALME,ONEPLUS)**,the no of installation on these devices are huge according to the market **but from last 3 -4 months backend told us they are developing but no results yet received.**
the issue seems to be at Oppo/Realme/OnePlus (ColorOS) end, Also it's been only 2 months since 2.0 is Pushed
2. The **"Software Remove Online" command fails** on approximately **30% of devices**. In certain models (especially **Realme** and **Oppo**), it requires a **hard reset** to complete the process. It has been noticed that support team is Inactivating the devices without properly Uninstalling the Locker via Offline/Online Attempts
3. **Location and SIM details are not fetched correctly** on the majority of devices.
Sim Is Fetched from the Device itself, if device is unable to read, Locker app won't read either
Also, Location can only be accessed when device is LOCKED (Privacy Concerns)
in PRYME Location toggle can be turned of by customer to avoid Location Update
4. In **40%** of the **Lock and Unlock Cases, Online command Doesn't Work** even if the Internet is connected through broadband with good Internet Speed. Kindly Check DATA Restrictions which customers enable to Avoid Networking via Server
5. After adding customer details, **IMEI 1 and IMEI 2 get swapped** on some devices (especially **POCO** and **Mi** phones).
Swapping of IMEI is Not a concern, and it done to match a certain IMEI Storing Pattern, THIS DOESN'T AFFECT THE SOFTWARE AT ALL

iLock Issues

1. The **iLock unlock command doesn't work** as expected. Locked iPhones remain locked even after issuing the unlock command via **dialing 112 (E-Call)** or using an **Ethernet cable**. iPhones Follow a strict Policy in LOCK MODE, Either the device should be connected to a known wifi network & or be in state of EMERGENCY
2. **Face ID functionality fails intermittently**, causing authentication issues for users.
After the 2.0 Update, there is no involvement of FACE ID & Passcode for iLock devices, Devices Installed before the Update can be resolved using the Enable Passcode Command.

Retailer App Issues

1. **Login OTPs are often not received** on registered mobile numbers, preventing login for many retailers.
MCops Series Uses Google Authentication for Mobile Devices, And Verifies a Login request using Phone number & a Captcha, While Some retailers Press Back on Verification Screen which results in Bogus Attempts to login and thus number getting Blocked temporarily for OTPs

2. Users frequently encounter a **"Something went wrong"** error while attempting to log into the Retailer app.
Happens when network fluctuations, Invalid Login Credentials & Multiple Login attempts
3. During the process of adding a customer, the **MPIN page appears unexpectedly** when clicking photos, disrupting the flow.
Make sure devices are in proper internet connection, Any Distruption During the application usage will trigger a security mechanism of MPIN Screen to avoid unauthorized access.

Post-Solution Issues Observed

Even after applying all standard solutions and troubleshooting steps, the following issues continue to occur across multiple devices and scenarios:

Software Remove Issues

1. **Software remove command fails** intermittently even after using both **online and offline methods**.
Do Not Pre-Inactive device before Uninstall Confirmation
2. In some cases, the software is **not removed even after changing the SIM card twice**.
No Point of chaning sim cards if Offline message is sent via Unauthorized SIM

iLock Unlock Issues

1. **iLock unlock fails** even after attempting **all known methods**, including:
 - Dialing **112 (E-Call)** Mentioned already about iPhone LOCK MODE policy
 - Using **Ethernet cables** Apple Recommends this method to provide internet on LOCK MODE devices
 - Reapplying unlock commands multiple times
Multiple Commands at once will cause the server to rate limit the requests thus cancelling all the Queued Commands

FRP (Factory Reset Protection) Issues

1. Devices get **stuck on the FRP page**, and the **FRP unlock using the registered email fails** to bypass the screen on certain devices.

Make Sure you have installed GLOCK, and use the appropriate Account for Unlock, FRP Screen Doesn't Comes in PRYME, even if it comes it has nothing to do with MCOPS Series unless device has GOOGLE POLICY INSTALLED while Automatic REINSTALL

Retailer App Issues

1. The **Retailer app freezes** and unexpectedly **navigates back to the MPIN setup page** during the customer registration or login process.

Already Mentioned about this NETWORK FLUCTUATIONS

Market Expectations Regarding M-Series

Based on multiple user inputs, the following improvements are expected in the **M-Series (GLock & Pryme)** functionality:

Location & SIM Details

1. **Lock the GPS Location tab permanently** to ensure accurate and consistent location tracking. **Not Possible due to Potential Legal Troubles & Compliance with IT LAWS**
2. Ensure that the system **fetches correct SIM details and location information** on all devices without failure.

SIM Fetching depends on the DEVICE CAPABILITY itself, Also the SIM should Support Showing Self Number

IMEI Handling

3. Resolve the issue of **automatic IMEI swapping or replacement** during the installation of the GLock or Pryme kits. This affects the integrity of device tracking and customer recor **Swapping of IMEI is Not a concern, and it done to match a certain IMEI Storing Pattern, THIS DOESN'T AFFECT THE SOFTWARE AT ALL**

Permission Management

4. **Restrict the installation** of the Pryme kit if **any required permission is skipped** during setup. Alternatively, display a **clear warning message** indicating that the kit lacks necessary permissions for proper functioning.

Core Android Permissions can't be skipped as it is technically possible to check,

Brand Specific permissions shall be given Manually as it lacks the technical capabilities of Checking them

5. After activation of the Pryme kit, **allow users to access the "App Info" section of all other apps(except battery,location)** on the device for better control and configuration.

Having Lenient restrictions will put the security of PRYME in jeopardy thus effecting the Performance and Security of the Software & Locking Mechanism,

Pryme only restricts risky permissions which can stop it from working or getting uninstalled

AGREEMENT PHOTO UPDATE

6. User agreement should come with customer photo