

MotionPro Android 3.0.22

Release Note

Release Date: April 29, 2022

Introduction

This release document summarizes the device requirements, improvements, fixes and limitations for the release of the MotionPro Android Client 3.0.22.

The MotionPro client is compatible with AG 9.4 versions and later.

To use the MotionPro Desktop feature, AG 9.3.0.79 or later is required.

Device Requirements

- Android 7.0 to 11.0 (software)
- Multi-touch screen
- ARM, ARM v7 and ARM v8 CPU

The MotionPro client has been tested on the following devices:

- Galaxy S21 5G (Android 11)

It is expected that the MotionPro client can work properly on most Android devices meeting the minimal software requirement.

IMPROVEMENTS AND FIXES

Improvements

- This release modifies support for Microsoft RD client. Android 8.x and previous systems need to use Microsoft RD 8.0. Android 9.x and later systems need to use Microsoft RD 10.0. (116449)
- The client security function provides support for “OS” device, which can be Android 8.x, Android 9.x, Android 10.x and Android 11.x. (109131)

Fixes

- Solved the issue that OpenSSL denial of service vulnerability reported by CVE-2022-0778. (117904)
- Solved the issue that sites with the same domain name and different ports could not be configured on the MotionPro client. (117021)
- Solved the issue that if client security checks were configured and hostname checks were added on AG device, the MotionPro client obtained and processed the domain name each time, resulting in too slow client security check. (116782)
- Solved the issue that the client could not open the Google browser APP on Android 11. (116294)
- Solved the issue that after the client security check function was enabled, it could not pass radius SMS authentication. (110092)

KNOWN LIMITATIONS

Enterprise Application Portal

General

- The MotionPro client does not support the VPN policy of “both mode” (**motionpro portal vpnpolicy both**). The MotionPro client supports only the L3VPN mode (**motionpro portal vpnpolicy l3vpn**). If “both” mode is configured, the client will still use the default VPN policy.

AAA

- It is highly recommended to enable the “Auto Register” function to avoid the following limitations:
 - If DeviceID+RADIUS SecureID authentication is enabled, the device cannot be registered on the MotionPro client, the administrator must register it manually on the MotionPro Pilot.
 - If DeviceID+SMX authentication is enabled, a user has to input SMX password again after device registration on their first login.
- The MotionPro client only supports “machineid” in the Hardware ID rule when Hardware ID authorization is used.

Secure Browser

- Secure Browser downloads are not cleared when the MotionPro process is killed or the MotionPro client is uninstalled before logout of the current session.

L3 VPN

- Split DNS is not supported on Android 4.4 or higher.
- If only desktop or remote application resources are configured, the L3VPN tunnel will not be established, so the Secure Browser and Native Application cannot function.
- The Web ACL function is not supported.
- On HuaWei P7, due to the enabling L3 VPN tunnel, the added DNS servers will not be cleared from the routing table after user logout until the network changes.
- The MotionPro client does not support DNS hostmap.

Enterprise Application Store

- After an application is downloaded, the user has to confirm the installation (this is required by the Android system).

Enterprise Application Security

Security Policy

- Nesting Client Verification conditions are not supported.
- When the Client Verification condition is “Device Passcode State: ON”, only “Pattern” can be used as the passcode lock.

MotionPro Desktop

- MotionPro Desktop does not support NLA (Network Level Authentication).
- MotionPro Desktop does not support ART Device Identification.
- MotionPro Desktop does not support ART Client Verification.
- MotionPro Desktop does not support accessing multiple remote desktops at the same time.
- MotionPro Desktop does not support the SSO function for remote desktop. The MotionPro login password cannot be posted to the Microsoft RD client for authentication, so users need to enter the password manually to access the remote desktop.
- The Microsoft RD client does not support the Gestures in the DesktopDirect client.
- The Microsoft RD client cannot automatically reconnect to the remote desktop after the MotionPro client reconnects to a server successfully.
- The Microsoft RD client cannot disable the clip board redirection.
- The following settings in the Client Settings of DD Pilot are not supported:
 - Keep Alive Interval
 - Console Connections
 - Resolution
 - Color Depth
 - Enable Bitmap Caching
 - Hide Connection Bar
 - RDP Agent

- Citrix Client
- Idle Timeout
- Life Timeout
- Please do not input a 2-bytes username. Otherwise, the end user may fail to obtain the assigned desktop resources.
- Published Applications cannot be accessed using the Microsoft RD client (version 8.1.x).
- “performance tuning” in client setting does not work if the remote desktop is Windows 10 or Windows 8.1.

Others

- With the framework ARMv8, the MotionPro client might fail to properly function when the VPN is connected and the screen is locked for more than 15 minutes.
- On Android 11, the MotionPro client failed to obtain the local certificate.

REFERENCES

Microsoft RD Client

<https://play.google.com/store/apps/details?id=com.microsoft.rdc.android>