

# MotionPro Windows 1.2.19

## Release Note

Release Date: April 29, 2022

### Introduction

This release document summarizes the device requirements, enhancements and fixes, and limitations for the release of the MotionPro client 1.2.19 for Windows.

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

### Device Requirements

- Windows 8/8.1 32/64bit (software)
- Windows 10 Pro 64bit (software)
- Windows 11 Pro 64bit (software)

The MotionPro client for Windows has been tested on the following operating systems:

- Windows 10 Pro 64bit

It is expected that the client can work properly on most Windows devices that meet the minimal software requirement.

## ENHANCEMENTS AND FIXES

---

### Enhancements

- MotionPro client now supports Win10 v21H2. (113541)
- The value of parameter “Browser Type” in OEM.ini file is changed from “ICEF3Q” to “CEIF3Q”.(118529)
- The authentication type is changed from “SAML” to “Microsoft SAML”. (115768)

### Fixes

- Solved the issue that OpenSSL denial of Service Vulnerability reported by CVE-2022-0778. (117904)
- Solved the issue that after the power function wake-up function was enabled, the account password output in the log was plain text. (117713)
- 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 on Windows 10, after the VPN was successfully connected, it failed to reconnect normally after the PC slept and woke up again. (116553)
- Solved the issue that some users could not access VPN normally after introducing TLS 1.2. (115395)

## KNOWN LIMITATIONS

---

### AAA

- The MotionPro Device ID authentication will fail when end users choose auto detection for the certificate authentication type in the advanced settings of the profile on the client. Please use manual mode in this case.
- SMX v11 does not support changing password when the user logs into the system for the first time.

### L3VPN

- Does not support disabling the AAA function.
- Does not support proxy for IPv6.
- Does not support excluded network list for IPv6.
- Does not support DNS hostmap for IPv6.
- Does not support DNS search domain for IPv6.
- Does not support DNS proxy for IPv6.
- The priority of the IPv4 DNS server is higher than that of the IPv6 DNS server.
- Does not support script rewriting for the outside proxy. That is, the proxy script of the browser cannot be rewritten dynamically after the VPN tunnel is established.
- The MotionPro client supports “http://”, “file://” or “file:///” by automatically detecting proxy settings of the browser, but does not support dynamically rewriting the proxy script after the VPN tunnel is established.
- The VPN tunnel of the SSTP type does not support the inside proxy of the “manual” type.

## MotionPro Desktop

### Remote Desktop/VDI/Published Applications

- Does not support access to the remote desktop if the name and description attributes of the Published Applications contain Japanese or Chinese characters.
- In rare cases, access to a remote desktop will fail and a prompt “connection refused” will be displayed on the Microsoft RD client.
- Does not support the setting of the XenApp resource folder name.

- If the Google or WeChat OAuth authentication is used for authentication, when the end user adds the virtual site on the MotionPro client, the username parameter must be specified. Otherwise, the desktop resources cannot be displayed.

### **Client Verification**

- Does not support client verification.

### **Desktop Direct Portal**

- Does not support the registration portal.

## **Others**

- Does not support session reconnection.
- Does not support session warning for life/idle timeout.
- After the Web-launched client is installed on Firefox 90.x, the system skips to the page for downloading the client when the user clicks the Start VPN button. To solve this issue, please follow the following steps:
  - Access <https://127.0.0.1:60012>, the alert message is displayed on the page. Click the Advanced button.
  - Click the “Accept the risk and Continue” button.
  - Restart the client. You can successfully connect to VPN.