MotionPro

Release Notes

Last Update: November 7, 2023

Contact us:
Array Networks Inc.
1371 McCarthy Boulevard Milpitas,
California 95035, USA
Email: info@arraynetworks.com
Telephone: (408)240-8700 (Monday through Friday, 9 A.M. to 5 P.M. PST)
Toll Free: 1-866-692-7729 (1-866-MY-ARRAY)
Support: 1-877-992-7729 (1-877-99-ARRAY)
Fax: (408)240-8754
http://www.arraynetworks.com/

Legal Notice

Documentation is provided “as is” without warranty of any kind, either express or implied, including any kind of implied or express warranty of non-infringement or the implied warranties of merchantability or fitness for a particular purpose.

Array Networks reserves the right to change any products described herein at any time, and without notice. Array Networks assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by Array Networks. The use and purchase of this product does not convey a license to any patent copyright, or trademark rights, or any other intellectual property rights of Array Networks.

WARNING:
Modifications made to the Array Networks unit, unless expressly approved by Array Networks, could void the user’s authority to operate the equipment.

Document Feedback

Array Networks values your opinion and strives to ensure that the documentation you receive is clear, concise, and provides the appropriate information required for you to use each Array Networks application efficiently.

If you would like to provide feedback on this document, you can submit your questions or suggestions to the Array Networks Support team and they will be forwarded to the appropriate development teams for review and consideration in a future release.

In addition to the provided documentation, many additional resources are available to help you understand and work with your Array Networks applications. For more information on these resources, see the Array Networks website.

Array Customer Support

To contact Array Networks Customer Support, please call 1-877-992-7729 or email the support team at support@arraynetworks.com.

Contents

Release Overview

This release note summarizes the system requirements, updates, resolved issues, and known limitations for the release of the client of MotionPro Windows, macOS, Android, and iOS, and that of MotionPro OTP Android and iOS.

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

Related Documentation

- Previous Release Notes
- User Guide
- Administration Guide

Note: You can access all the related documents through the support portal. Please connect Array Networks Support team if you are facing issues in log in to the support portal.

MotionPro Windows 1.2.24

The following sections give an overview of the requirements, updates, and limitations for MotionPro Global Windows 1.2.24.

System Requirements

- Windows 11
- Windows 10 64-bit

Testing Environment

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

- Windows 11 Home 23H2
- Windows 10 Pro 64-bit

Updates

Added support for Windows 11 23H2. (323)

Resolved Issues

- Solved the issue that after the client was upgraded to the latest version, the status bar kept showing connecting when users connected to the site. (135345 and 141907)
- Solved the issue that after the VPN connection was successful, the route couldn’t be added and users were unable to access internal resources. (138796)
- Solved the issue that the client version was displayed incorrectly after **client automatic upgrade** was enabled on the server. (140813)

Known Limitations

AAA (Authentication, Authorization, Accounting)

- Once the MotionPro client is launched, navigate to the menu bar, select **Profile** > **Add** and expand **Advanced Setting**. In the **Authentication Type** list, if users select **Certificate** and then select **Auto Detect**, it results in the inability to authenticate the MotionPro Device ID. To address this issue, select **Manual** option instead.
- In SMX v11, users are unable to modify their passwords upon initial (first time) sign-in to the system.

L3VPN

- Disabling AAA is not supported.
- IPv6 proxy is not supported.
- The excluded network list for IPv6 is not supported.
- IPv6 DNS hostmap is not supported.
- IPv6 DNS search domain is not supported.
- IPv6 DNS proxy is not supported.
- The priority of an IPv4 DNS server is higher than that of an IPv6 DNS server.
- The external proxy does not support script rewriting. As a result, after a VPN tunnel is established, the browser's proxy script cannot be dynamically rewritten.
- The MotionPro client supports "http://," "file://," or "file:///" by automatically detecting a browser's proxy setting, but it does not support dynamically rewriting proxy script after a VPN tunnel is established.
- SSTP VPN tunnels do not support the "manual" inside proxy.

MotionPro Desktop

Remote Desktop/VDI/Published Applications

- If the names and descriptions of Published Applications contain Japanese and Chinese characters, remote desktop access will not be supported.
- In rare cases, remote desktop access might fail with "connection refused" displayed in the Microsoft RD client.
- If Google or WeChat OAuth is used for authentication, when users add virtual sites on the MotionPro client, the username parameter must be specified, otherwise desktop resources cannot be displayed.

Client Verification

- Client verification is not supported.

DesktopDirect Portal

- Registering a PC on the AG portal is not supported.

Others

- Session reconnection is not supported.
- Session warnings for lifetime or idle timeout is not supported.

- After the web-launched client is installed on a Firefox 90.x browser, clicking **Start VPN** will lead the system to switch to the client download page. This issue can be resolved using the following steps:

  1. Go to https://127.0.0.1:60012. When a warning message displays, click **Advanced**.
  2. Click **I accept the risk and want to continue**.
  3. Restart the client and the VPN can be connected successfully.

MotionPro macOS 1.2.20

The following sections give an overview of the requirements, updates, and limitations for MotionPro Global macOS 1.2.20.

System Requirements

macOS 11–14.0

Testing Environment

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

- macOS Sonoma 14.0
- macOS Ventura 13.1

Updates

Added support for macOS 14. (290)

Known Limitations

AAA (Authentication, Authorization, Accounting)

SMX authentication is not supported.

L3VPN

- Disabling AAA is not supported.
- After a VPN tunnel is established, automatic proxy detection and script rewriting are not supported.
- The excluded network list for IPv6 is not supported.
- IPv6 DNS hostmap is not supported.
- IPv6 DNS search domain is not supported.
- IPv6 DNS proxy is not supported.
- DNS filtering is not supported.
- The priority of an IPv4 DNS server is higher than that of an IPv6 DNS server.
- After configuring an external proxy, opening the Web portal requires setting up an HTTPS proxy in Safari browsers.

- On Mac OS 11 Big Sur, if users connect to the VPN and subsequently modify the DNS resolution rules, clicking **Disconnect** or the red A, does not successfully disconnect the VPN in the MotionPro client. To disconnect the VPN, users must click **Quit** from the Start menu.

MotionPro Desktop

Remote Desktop/VDI/Published Applications

- If the names and descriptions of Published Applications contain Japanese and Chinese characters, remote desktop access will not be supported.
- If Google or WeChat OAuth is used for authentication, when users add virtual sites on the MotionPro client, the username parameter must be specified, otherwise desktop resources cannot be displayed.
- The MotionPro client supports Microsoft Remote Desktop 8.0 and 10.x, both of which can be acquired from the Apple App store.
- VDI resources cannot be displayed after the VDI authentication is disabled.
- The web-launched MotionPro client does not support external proxies.

Client Verification

Client verification is not supported.

Client Settings

Idle and lifetime timeouts are not supported.

DesktopDirect Portal

Registering a PC on the AG portal is not supported.

Others

- The VPN connection cannot be established using WebAuth in the WebView. During the connection establishment WebView stops responding and is stuck on the loading screen. (290)
- Session warnings for lifetime or idle timeout are not supported.
- Custom profiles and logos are not supported.
- Automatic upgrade is not supported.
- The Web-launched MotionPro client consistently opens the Web portal through Safari browsers.

- Clicking **Quit MotionPro** or **Quit**, does not successfully close the macOS MotionPro client.

- To access resources using Firefox on macOS, follow the steps below:

    1. Enable **network.websocket.allowInsecureFromHttps**.

    2. In the Firefox address bar, enter "about:config." In the search box, enter "websocket," and in the list, double-click "network.websocket.allowInsecureFromHttps" to change the value from **false** to **true**.

    3. Accept the settings.

    4. In the Firefox address bar, enter "https://127.0.0.1:60012/." Click **Advanced** and then click **Accept the risk and add exceptions**.

- Warning messages will appear upon installing the MotionPro client on macOS. To resolve this issue, follow the steps below:

    1. In System Settings, click **Privacy and Security** on the left.

    2. "iSecSPSetup.pkg installation has been blocked" is displayed in the security on the right. Click the button below to open it.

    3. In the pop-up dialog box, enter your macOS password.

    4. The message ""iSecSPSetup.pkg" cannot be opened because Apple cannot check whether it contains malicious software" appears. Click **Open**.

    5. Click **Continue** to install.

    6. Enter your macOS password again. Click **Install Software** to complete the installation.

MotionPro Global Android 3.1.3

The following sections give an overview of the requirements, updates, and limitations for MotionPro Global Android 3.1.3.

System Requirements

- Android 7.0 to 14.0 compatible
- ChromeOS 105 and later compatible

Testing Environment

The MotionPro Global Android client has been tested on the following operating systems:

- ASUS ChromeBook C436F, ChromeOS 105, 117, and 118
- Pixel 7a, Android 14
- Samsung Galaxy A33 5G, Android 13.0
- SHARP AQUOS V, Android 9.0
- Sony G3125, Android 8.0

Updates

- Added support for Android 14. (302)
- For Android 13 (API level 33), notification runtime permission has been added. After MotionPro Global is started, it will ask your permission to push notifications. (278)
- Added support for ChromeOS. (209)

Resolved Issues

Solved the issue that MotionPro Global could not be started from browsers. Now you can start MotionPro Global on a web page. After it is started, it will connect to the VPN automatically. (309)

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 ended 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

- NLA (Network Level Authentication) is not supported.

- ART Device Identification is not supported.
- ART Client Verification is not supported.
- Accessing multiple remote desktops at the same time is not supported.
- SSO function for remote desktop is not supported. The MotionPro account password cannot be posted to the Microsoft RD client for authentication, so users need to enter their passwords 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
- Two-byte usernames are not supported. Using them may cause end users to 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

- The MotionPro client might crash when you sign in using fingerprint, because fingerprint authentication is not supported by all Chromebooks. (209)
- With the framework ARMv8, the MotionPro client might fail to properly function when it connects to the VPN and the screen is locked for more than 15 minutes.
- On Android 11, the MotionPro client fails to obtain the local certificate.

MotionPro OTP Global Android 3.1.0

The following sections give an overview of the requirements, updates, and limitations for MotionPro OTP Global Android 3.1.0.

System Requirements

- Android 7.0 to 14.0 compatible
- ChromeOS 105 and later compatible
- Multi-touch screen
- ARM, ARMv7, and ARMv8 CPU

Testing Environment

The MotionPro OTP Global Android client has been tested on the following operating systems:

- ASUS ChromeBook C436F, ChromeOS 105, 117, and 118
- Pixel 7a, Android 14
- Samsung Galaxy A33 5G, Android 13.0
- SHARP AQUOS V, Android 9.0
- Sony G3125, Android 8.0

Updates

- Added support for Android 14. (302)
- Added support for ChromeOS. (209)
- The Chinese text 华耀 was changed to 安瑞.
- MotionPro OTP was renamed MotionPro OTP Global.

Resolved Issues

Solved the issue that MotionPro OTP Android 2.9 cannot be installed from Google Play on Android 12. (137262)

Known Limitations

There are no known limitations applicable to this release.

MotionPro Global iOS 3.1.1

The following sections give an overview of the requirements, updates, and limitations for MotionPro Global iOS 3.1.1.

System Requirements

- iPadOS 14.x to 16.x compatible
- iOS 14.x to 17.x compatible

Testing Environment

The MotionPro Global iOS client has been tested on the following operating systems:

- iPad Air 3, iOS 16.7.2
- iPhone 12, iOS 16.7
- iPhone SE2, iOS 15.4.1
- iPhone XR, iOS 17.0.2

Updates

Added support for iOS 17. (205)

Resolved Issues

- Solved the issue that Microsoft Remote Desktop Mobile could not be detected on iOS 17. (205)
- In MotionPro Global, after you selected a machine to connect, Microsoft Remote Desktop Mobile (RD client) would not open automatically to connect to the selected machine. You needed to open the RD client first, and then it could connect to the machine you selected in MotionPro Global. This was limited to the RD client's behavior. This issue has been resolved in Microsoft Remote Desktop Mobile 10.5.2. (149)

Known Limitations

Enterprise Application Portal and Secure Access

General

The MotionPro Plus client does not support the VPN policy of "both mode" (**motionpro portal vpnpolicy both**). The MotionPro Plus 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 SecurID authentication is enabled, the device cannot be registered on the MotionPro Plus client, and the administrator must register it manually.
  - If DeviceID+SMX authentication is enabled, a user has to input the SMX password again after device registration on their first login.
- The MotionPro Plus client does not support changing password for multi-factor authentication.

Portal

Screen rotation is not supported by the MotionPro Plus client.

Secure Browser

- Online video cannot be played in Secure Browser.
- Some Web applications of the HTTPS type cannot be opened through Secure Browser.

VPN

- On iOS 9, when the SSL protocol is set to “SSLv3,” the end user cannot access the portal via the MotionPro Plus client.
- For the DNS Filter function, only the virtual DNS filter rule is supported. When the hostname to be resolved matches the virtual DNS filter rule, the Array Client will use only the virtual DNS server to perform the DNS resolution. When not match, the Array Client will use only the local DNS server (flag=1) to perform the DNS resolution according to the setting of the virtual DNS filter rule.
- When the user accesses the Web resources via the split tunnel, the DNS search function can take effect after the “**motionpro client flag** 16” is configured on the AG appliance.
- The MotionPro Plus client does not support DNS hostmap.
- After the Motionpro Plus client connected to VPN, when the administrator manually killed the session or the session timed out, the VPN was disconnected but the MotionPro Plus client did not log out.
- On iPadOS 14.2, the user fails to start VPN via Web-launched MotionPro Plus client. The Safari browser prompts the user to download MotionPro Mac OS client when the user tries to connect to the VPN server via Safari.

Client Security

- When the success URL and failure URL are configured, the end user cannot log into the portal.
- L3VPN is not supported when the Client Security level is set to “low” or “none.”

Enterprise Application Store

- User permission is required during the installation.
- Now, on iOS 9, the installation status of applications will not be displayed on the application list. Users need to click the application to obtain the installation status of an application.
- RootCA cannot be installed on iOS 10.3.1.
- If the certificate of the virtual site cannot be trusted, the Apple App Store function will fail to work.

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 Plus 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 PubApp connects to the remote desktop after the Microsoft RD client is updated to 8.1.0 - 8.1.4.
- The Microsoft RD client does not support the Gestures in the DesktopDirect client.
- The Microsoft RD client cannot remove access history until the process is killed.
- The Microsoft RD client cannot automatically reconnect to the remote desktop after the MotionPro Plus 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

- Do not use 2-bytes characters to enter the username. Otherwise, the end user may fail to obtain the assigned desktop resources.
- Do not use the equal sign (=) and ampersand (&) in the DesktopDirect configurations. Otherwise, the end user may fail to obtain the assigned desktop resources.
- "performance tuning" in client setting does not work if the remote desktop is Windows 10 or Windows 8.1.

IPv6 Support

The MotionPro Plus client cannot work in NAT64 network environment.

Others

- If you use Array IDpass for authentication, MotionPro Global will switch to IDpass to sign in automatically, but it won't switch back to MotionPro to show the status of the VPN connection. (205)
- After the upgrade of the client compilation environment, iOS 13.x is not supported because the new interface is required to support iOS 15.x.

MotionPro OTP Global iOS 3.1.0

The following sections give an overview of the requirements, updates, and limitations for MotionPro OTP Global iOS 3.1.0.

System Requirements

- iPadOS 14.x to 16.x compatible
- iOS 14.x to 17.x compatible

Testing Environment

The MotionPro OTP Global iOS client has been tested on the following operating systems:

- iPad Air 3, iOS 16.7.2
- iPhone 12, iOS 16.7
- iPhone SE2, iOS 15.4.1
- iPhone XR, iOS 17.0.2

Updates

- Added support for iOS 17. (205)
- Binding one-time password (OTP) authentication.
  - Using dynamic code which is updated every 30 seconds to enhance security.
  - Online registration and offline usage.

Resolved Issues

There are no resolved issues applicable to this release.

Known Limitations

There are no known limitations applicable to this release.