J-VMP

Join-Virtual Mobile Platform 6.1.0(J-VMP) USER's Guide

Ver.6.1.10
01/25/24

TheJOIN

Table of Contents

1. About J-Virtual Mobile Platform

J-VMP is a Virtual Mobile Infrastructure(VMI) solution that hosts independent workspaces for all users. The mobile user virtual workspace is based on the Android operating system and can be accessed via the mobile client application(J-VMP) installed on an Android or iOS mobile device.

Mobile client applications(J-VMP) allow users to access the same mobile environment, including all applications and data they use at work from anywhere, without being tied to a single mobile device.

The mobile client application provides users with all Android features and controls to provide the original Android user UI experience.

All mobile workspaces are hosted on the server and maintained by the administrator, so you can clearly separate the personal and corporate data available to you.

This clear separation of usage areas makes it easier to manage and maintain by ensuring data safety within the enterprise and providing a centralized, efficient workspace.

2. Why Use Mobile Virtualization Products

J-Virtual Mobile Platform provides the following benefits:

Benefit	Description
Data Protection	All enterprise applications and data are saved in secure corporate servers under administrator's control
Good User Experience	Users can use their personal mobile device to access corporate data, and therefore the mobile OS user experience is preserved.
	Easy-to-use system to access corporate virtual workspace.
	Natural screen touch experience for Smartphones and tablets.
Simplified Management	Administrator can centrally manage all users from single Web console.
Single Sign-On	Reducing time spent in re-entering passwords in virtual workspace.
	Reducing administration cost due to lower number of IT help desk calls about passwords.
Workspace Customization	Administrator can create a personal virtual mobile workspace for each employee.
	Administrator can centrally customize applications for employees in their virtual workspaces from the server.
User-based Profile	Provides user based profile management.
	Users can use their own virtual workspace from any of their mobile devices.
Manageable Life Cycle	Administrator can remotely manage a workspace's entire life cycle-from provisioning to the end of life.
Easy Deployment	Provides on-premise deployment.
	Provides self-contained Linux-based operating system for easy deployment.
Integration with Enterprise Infrastructure	Provides integration with LDAP and external storage.

3. Minimum Requirement for Mobile User Devices

Before installing the J-VMP App, check the requirements for the following systems:

Component	Minimum Specifications	
iOS	Mobile OS	iOS 16.0 minimum
	Storage space	128-MB minimum
	Memory	100-MB minimum
Android	Mobile OS	Android 13 minimum
	Storage space	128-MB minimum
	Memory	100-MB minimum

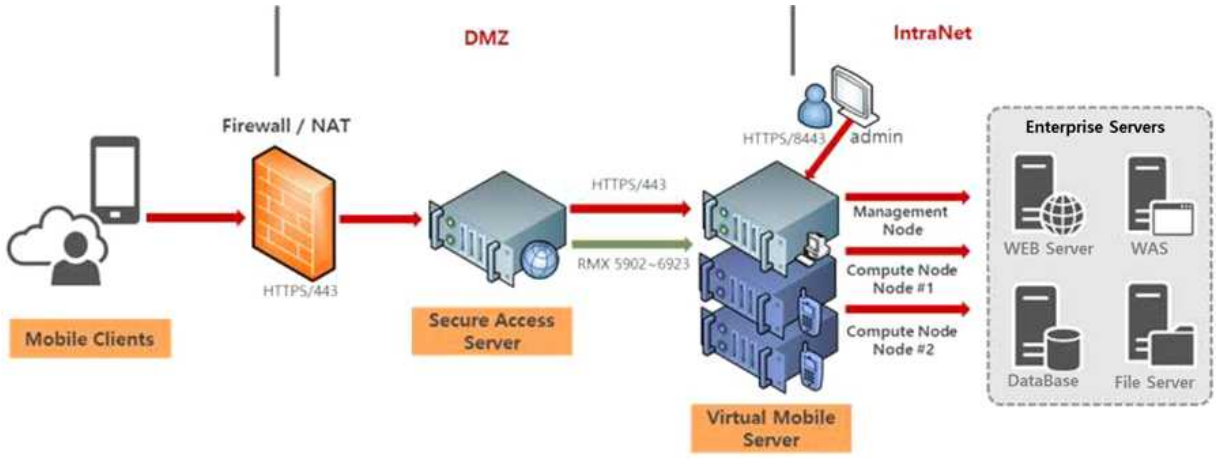
4. Architecture of J-Virtual Mobile Platform

Depending on your company's size, environment, and requirements, the J-Virtual Mobile Platform allows you to deploy a single or multiple servers for secure service.

For multiple servers, Virtual Mobile Platform can maximize efficiency through load balancing between servers.

The systems configured in the assessment are as follows:

A multi-server installation model is a model that installs and operates two or more virtualized and Secure Access servers.



5. Components of J-Virtual Mobile Platform

J-Virtual Mobile Platform system includes the following components:

Component	Description	Options
Virtual Mobile Infrastructure Server	The Virtual Mobile Platform server contains management node and compute node. • Management node provides management console for administrator and web service for user logon, logoff and connection to users's workspace. • Compute node hosts workspaces. Each workspace runs as a Virtual Mobile Platform instance.	Required
Virtual Mobile Platform Mobile Client Application(J-VMP)	The mobile client application is installed on the mobile devices. The client application connects with the Virtual Mobile Infrastructure server to allow users to use their workspaces hosted on the server.	Required
Secure Access	The Virtual Mobile Platform Secure Access enables mobile clients to access Virtual Mobile Platform server via Internet.	Strongly recommended
Active Directory	The Virtual Mobile Platform server imports groups and users from Active Directory.	Optional
External Database	External Database provides scalable data storage for user data. By default, Virtual Mobile Platform server maintains a database on its local hard drive. However, if you want to store the data on an external location, then you will need to configure External Database.	Optional
External Storage	Using this option will enable you to store the user data in an external storage.	Optional

6. Common Criteria Evaluation

The functionality described in this guidance documentation is limited to the security functionality described in the Security Target.

Other product functionality is not applicable to the claimed Protection Profile and was therefore not examined as part of the Common Criteria evaluation of the J-VMP product.

The evaluated configuration also includes several assumptions and requirements that must be met by the intended environment in order for the installed J-VMP Client to be in the evaluated configuration. These are as follows:

- The J-VMP Server relies upon a trustworthy computing platform for its execution.
- The administrator of the application software should administer the software within compliance of the applied enterprise security policy.
- The Security Target is the J-Virtual Mobile Platform (J-VMP), Version 6.1.0.

The J-Virtual Mobile Platform (J-VMP) 6.1.0 was tested on the following mobile devices.

Device Name	Processor	Operating System
Samsung Galaxy S22	Qualcomm Snapdragon 8	Android 13
Apple iPhoneX	Apple A11	Apple iOS 16

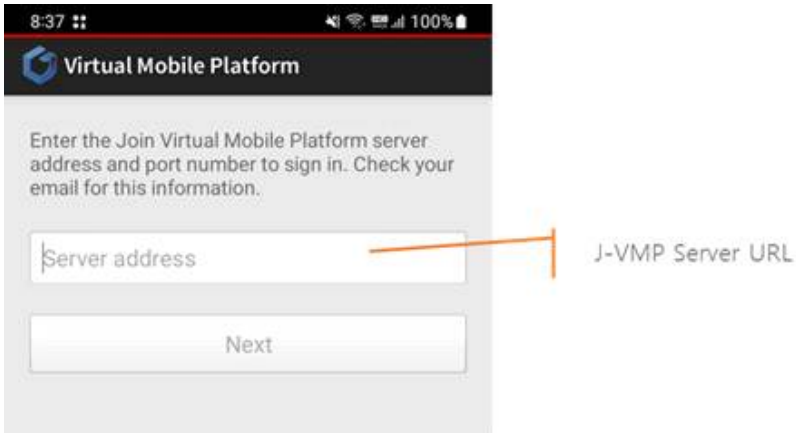
7. Guidance

J-VMP applies in the evaluated configuration along with this Common Criteria specific guidance. No configuration is needed for evaluated cryptography to be used.

7.1 Features

7.1.1 Specify server information

After launch the app, server information should be specified with a DNS name or a network address.



this information is used for TLS certificate validation.

7.1.2 Appling server configuration:

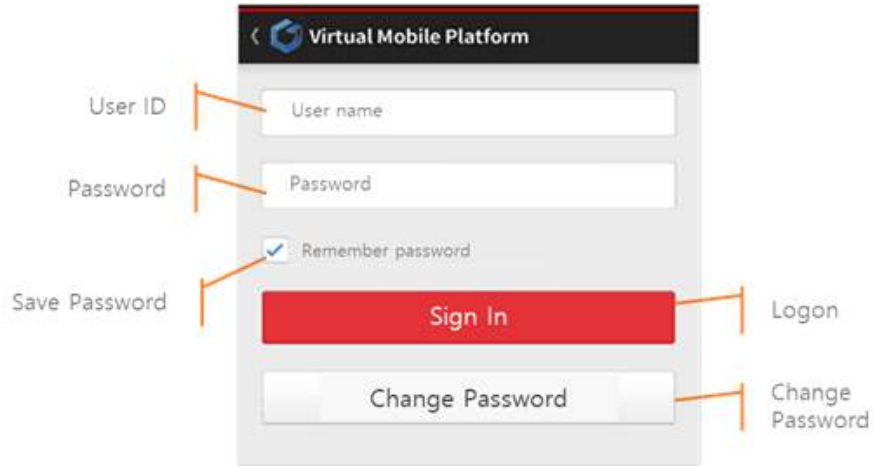
Launch the application and input the server address, client will communicate with the server to get some configurations from server.

The following is an example for partial configurations from VMP server.

Component	Example
Final Version of the Client App	"current_ios_client_version": "6.1.0" "current_android_client_version": "6.1.0"
Graphic Settings Options	"graphic_quality": 1
Save Password Options	"remember_passwd": true
rooted or jailbroken blocked	"enable_csr": false
Initial password status	"change_password": false

7.1.3 Login

After get configuration, we can input our account and password to login the server via https protocol.

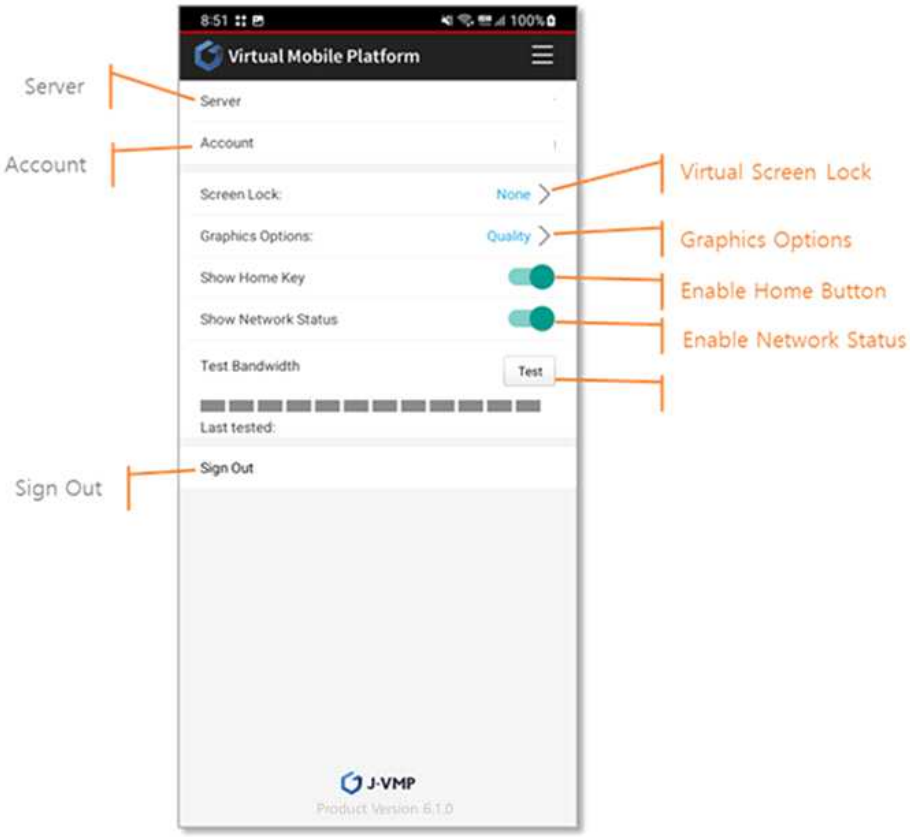


7.1.4 Operate the workspace

Client can operate the virtual mobile, send email, take photo, add contacts and any other application they want.

7.1.5 Setting Configuration Options

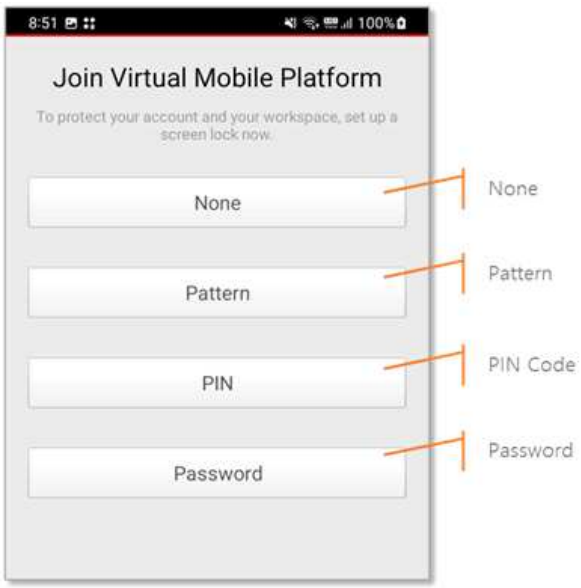
The client can set up a virtual mobile environment by touching the upper right setting button.



• **Virtual Screen Lock**

At the first login, client will ask use to set a virtual screen lock to protect the workspace. There are four kind of screen lock,

If we enable touch/face ID in iPhone and fingerprint recognition in Android, screen lock can be skipped by input that information.

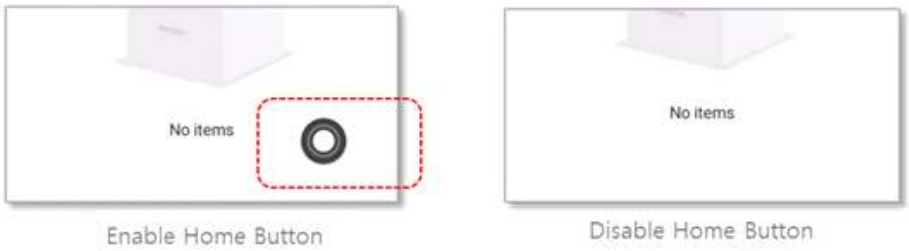


• **Graphics Options**

The Graphics option can be modified. It includes quality, balance, performance. The three modes are with different resolution and frame rate, so user can modify the graphics mode according to the network bandwidth for a better experience.

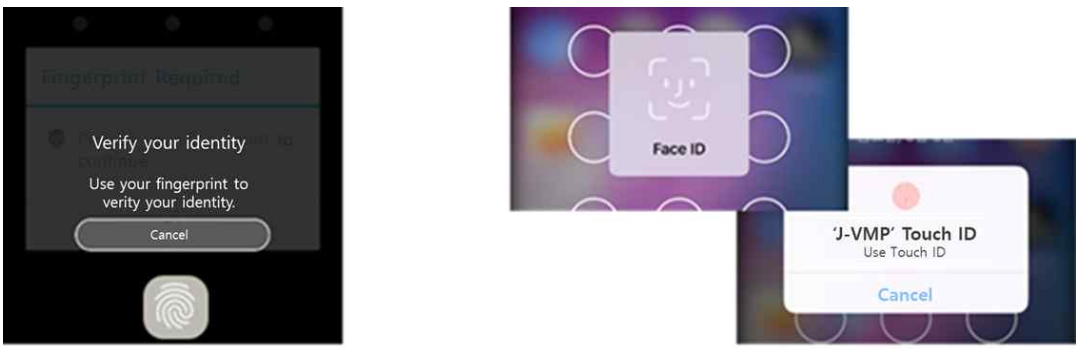
• **Enable Home Button**

Available when moving to the virtualization workspace home (not the Mobile Device home button)



• **Enable Touch ID / Fingerprint**

J-VMP client can enable Touch ID/Fingerprint for quick authentication to connect the virtual mobile after login successfully



• **Test Bandwidth**

A build-in tools to test the network bandwidth between virtual mobile and mobile device.

8. Required Permissions

8.1 Android Permissions

The J-VMP Client for Android requires permission for installation and using. The following permissions are requested during the Client installation and using on Android devices:

Permissions	Description
Access network state	The J-VMP client access the state of the network interface to get connectivity.
Access WiFi state	The J-VMP client access the state of the network interface to get connectivity.
Bluetooth / Bluetooth admin	The J-VMP client provide access to device's Bluetooth to enables bluetooth connection in virtual mobile or access to device's Bluetooth to enables application discover or pair Bluetooth devices in virtual mobile
Change WIFI state	The J-VMP client provide access to Wi-Fi state to enable turn ON/OFF device's WiFi in virtual mobile
Internet	The J-VMP Client must access networks to communicate with the Virtual Mobile running in J-VMP server. It can use any of the provided networks (Wi-Fi, 5G, 4G/LTE, 3G) when they are active.
Use fingerprint	The J-VMP Client uses the fingerprint permission to enable a Biometric Authentication Factor in the form of a fingerprint. The J-VMP Client supports biometric fingerprint ID capabilities if the mobile device's underlying platform supports biometric authentication.
Vibrate	The J-VMP Client uses the mobile device's vibrator to provide silent notification alerts.
Wake lock	The J-VMP client need to use Power Manager Wake Locks to keep processor from sleeping or screen from dimming.
Access coarse location	The J-VMP Client provides access to the coarse location for apps in the Virtual Mobile that require device's location.
Access fine location	The J-VMP Client provides access to fine location for apps in the Virtual Mobile that require device's location.
Camera	The J-VMP Client provides remote access to the device's camera to multimedia apps that use the camera in the Virtual Mobile.
Record audio	The J-VMP Client provides access to the device's microphone to enables voice recording and phone apps in the Virtual Mobile.

8.2 iOS Permissions

The J-VMP Client for IOS requires permission for installation and using. The following permissions are requested during the Client installation and using on IOS devices:

Permissions	Description
Background operation	The J-VMP Client can be configured to refresh in background. The background operations permission is required to retrieve necessary information when the application is not active. To enable this capability, the user must enable the permission in the iOS settings – it is disabled by default.
Camera	The J-VMP Client uses remote access to the device's camera to support multimedia applications that use the camera in the Virtual Mobile. The user is prompted for access to the camera when the application is first started.
Location	The J-VMP Client provides access to the GPS sensors, the Wi-Fi location services of the mobile device for authentication with the J-VMP server and for apps in the Virtual Mobile that require location services. The user is prompted for access to location information when the application is first started.
Microphone	The J-VMP Client provides access to the microphone and audio recording capabilities on the mobile device to support apps in the Virtual Mobile that require audio input. Access to the microphone is requested the first time an application in the virtual device needs to use the microphone.
Photo library	The J-VMP Client supports access to the camera for video recording and taking pictures. This function in iOS requires the application register for permission to access the photo library – iOS will prompt the user for this permission when a photo or video is stored on the device. However, the J-VMP Client only use UIImagePickerControllerSourceTypeCamera from iOS platform to take photos under this permission, the J-VMP client will not read/write photo library, and The user is prompted for access to photo library when the application is trying to take photos.
Notifications	The J-VMP Client uses the mobile device's notifications permission to support notification display features. The user is prompted for permission to post notifications when the application is first started.
Bluetooth	The J-VMP Client provides access to the Bluetooth service on the mobile device to support apps in the Virtual Mobile that require Bluetooth Information. Access to the Bluetooth is requested the first time an application in the virtual device needs to use the microphone.

9. Updates and Update Verification

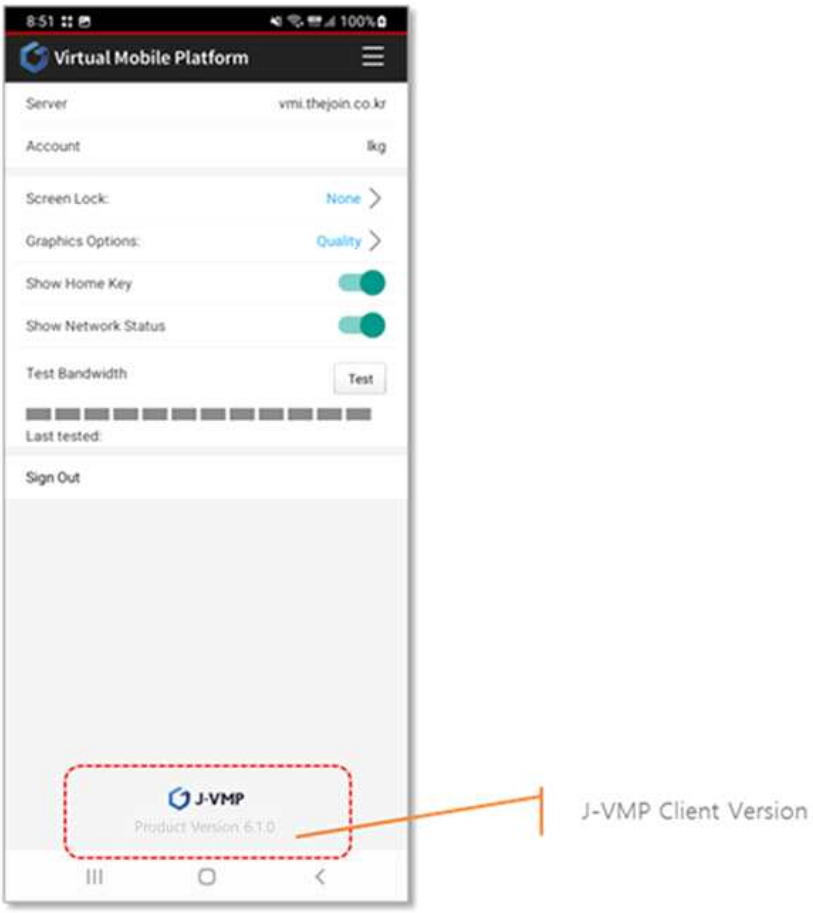
Users obtain J-VMP Client updates using Android or iOS update mechanisms or from J-VMP server.

If the application is installed using the Apple App Store or the Google Play Store, it may be updated automatically if your App Store or Play Store is configured to do so. If it is not, selecting the "update" option for the application in the Store application will verify that the application package is valid and install it over the older version.

If users are using an enterprise version client, they will install and upgrade the application form J-VMP server. J-VMP server can set the current version and min version supported. in this case the administrator need to follow Apple's guidance for enterprise installations and Google's guidance for installing an application from "unknown sources". iOS and Android will only replace the existing application with the updated one if the signing keys are the same and that the new applications are signed properly and have not been tampered with.

10. Verify Version of the J-VMP Client

To verify the version of the J-VMP Client, open the J-VMP Client, On the J-VMP Client Login or Setting screens, the footer at the bottom of the J-VMP Client app displays the version number.



11. Installing and Setting up the J-VMP Client

Your smartphone need to be connected to the Internet. It is better to use a wi-fi connection, to save traffic.

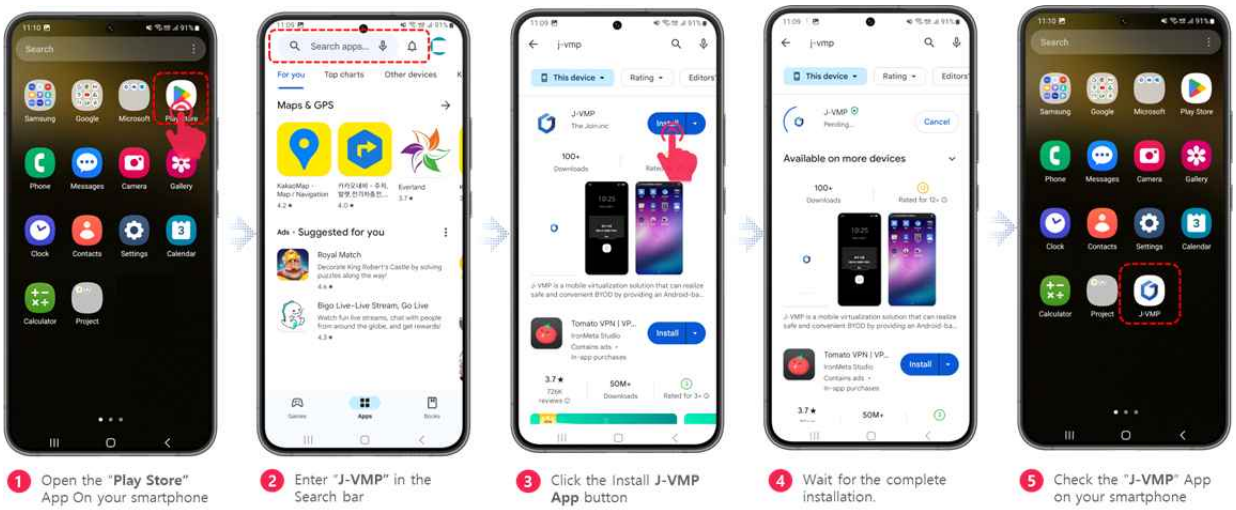
11.1 How to Install the J-VMP Client for Android users

You can search for, download, and install J-vmp in the Google Play Store.

1) Check Android phone installation specifications.

Operating System	Storage space	Memory
Android 13	Minimum 128-MB	Minimum 100-MB

2) Installing J-VMP Downloads from the Google Play Store.



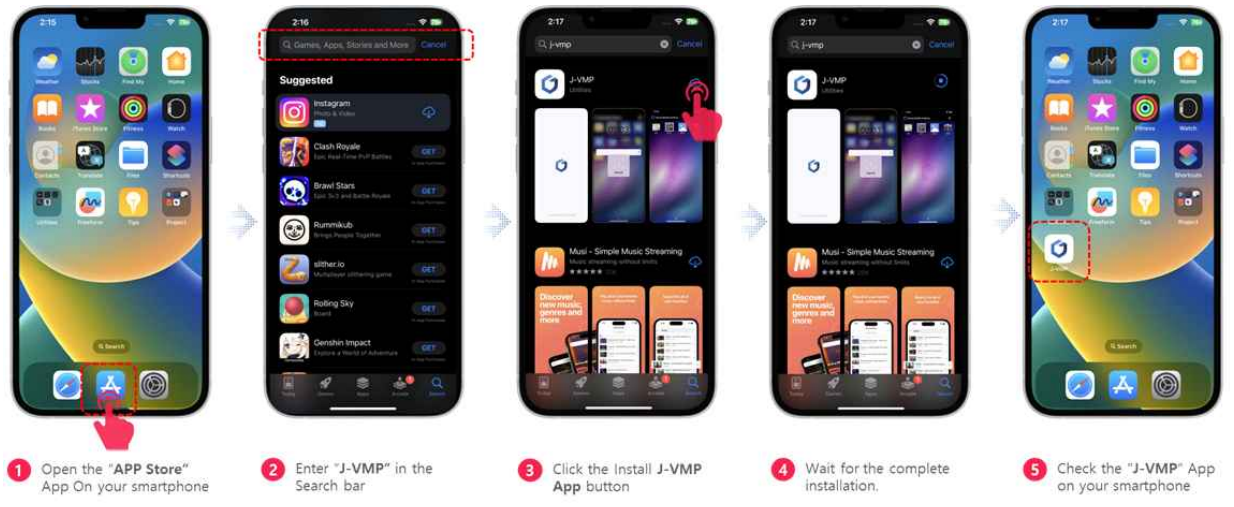
11.2 How to Install the J-VMP Client for iOS users

You can search for, download, and install J-VMP in the App Store.

1) Check iPhone installation specifications.

Operating System	Storage space	Memory
iOS 16	Minimum 128-MB	Minimum 100-MB

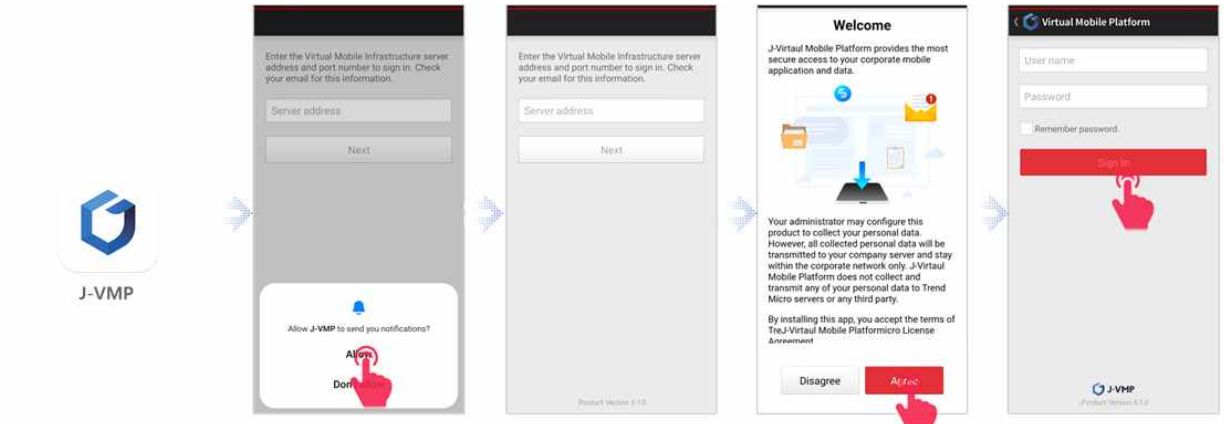
2) Installing J-VMP Downloads from the App Store.



11.3 How to set up a J-VMP Client connection

Describes how to set up and log in to the mobile virtualization server after installation.

1) Follow these steps to connect to the mobile virtualization server*(Same as Android and iOS).*



1 Running the "**J-VMP**" installed On your smartphone

2 Click "**Allow**" to allow app Notifications

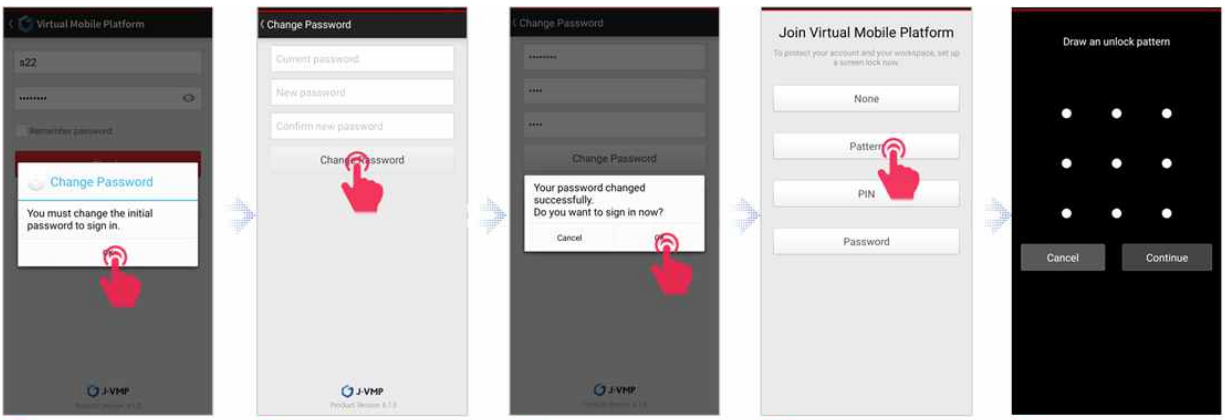
3 Enter Virtual Mobile Server Address

** you may need to contact your administrator for server information.*

4 Click "**Agree**" for a user license

5 Enter your user ID and initial password and click the "**Sign In**" button

** You may need to contact your administrator for your account information.*



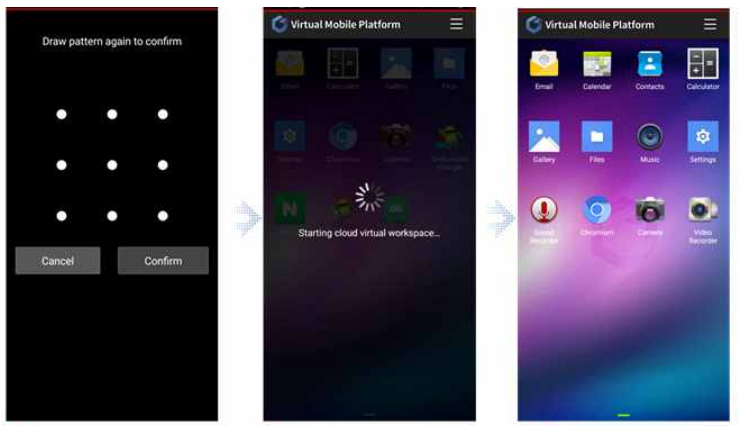
6 Click the "**OK**" button to change the initial password

7 Enter the initial password, enter the password you want to change, and click the "**Change Password**" button

8 Click the "**OK**" button to Sign In

9 Select how to unlock the virtualization screen (e.g. pattern)

10 Example: Pattern Settings



11 Example : Click the "**confirm**" button to complete the pattern setting

12 Starting Virtualization Workspace

13 Mobile Virtualization Workspace Access Complete

12. Cryptographic support

The J-VMP client utilizes platform APIs to provide secure network communication using HTTPS. The client also uses its own cryptography to establish trusted TLS channels to transmit data to the J-VMP Server.

1) TLS Cipher Suite:

The application employs the TLS_RSA_WITH_AES_128_GCM_SHA256 cipher suite for securing communication.

2) Certificate Checks:

The application conducts thorough certificate checks to ensure secure communication. Certificates are rigorously verified to establish the authenticity of the parties involved in the communication.

(Compliance with verification items such as RFC 6125)

3) Supported Signature Algorithms:

The application strictly supports SHA256 for signature algorithms. This ensures the robustness and integrity of the signatures used in the TLS communication.

J-VMP® User Guide

08/21/2021 Date Created

Product Name	J-VMP(Join-Virtual Mobile Platform)
Product Version	Ver 6.1.0
Vendor	The Join Co., Ltd
Postal code	06140
Address	63, Bongeunsa-ro 30-gil, Gangnam-gu, Seoul, Republic of Korea
Telephone	02-6949-0335
Fax	02-6949-0336
Web Site	http://www.thejoin.co.kr
Email	thejoin@thejoin.co.kr
Document Number	Join-JVMP-M-2021-001
Revised Number	6.1.10
Revised Date	2024. 01. 25.