Trend Micro Virtual Mobile Infrastructure (TMVMI) USER's GUIDE

Version 0.2

01/13/20

Table of Contents

1 Introducing Virtual Mobile Infrastructure

Trend Micro Virtual Mobile Infrastructure is a service that hosts independent workspaces for every user. A user workspace is based on the Android operating system, which is accessible via the Virtual Mobile Infrastructure mobile client application installed on an Android or iOS mobile device. Using the mobile client application, users can access the same mobile environment that includes all their applications and data from any location, without being tied to a single mobile device. The mobile client application preserves the original Android user experience by providing all the Android features and their controls to the user.

Since all the workspaces are hosted onto the server and maintained by the administrator, Virtual Mobile Infrastructure enables a clear separation between the personal and corporate data available to the users. This clear separation ensures data safety and provides more centralized and efficient workspaces that are easier to manage and maintain.

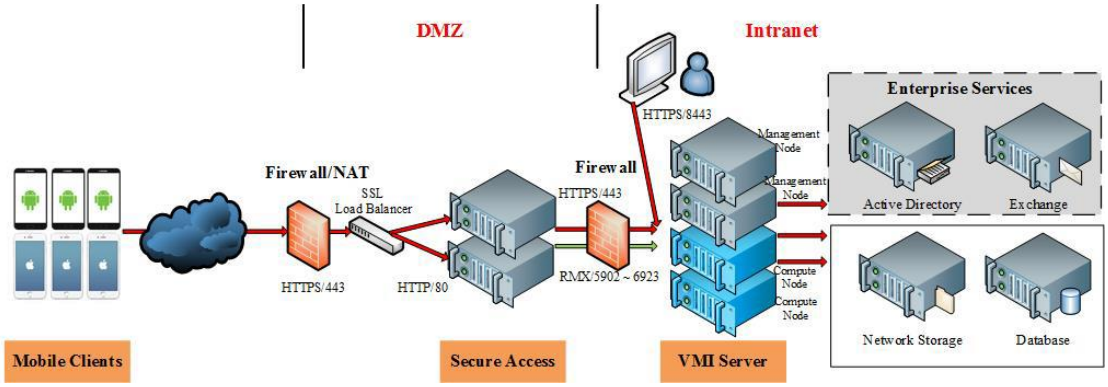


FIGURE1-1: Trend Micro Virtual Mobile Infrastructure High Availability architecture

Components of Virtual Mobile Infrastructure

The Virtual Mobile Infrastructure system includes the following components:

TABLE 1-4. Virtual Mobile Infrastructure Components

Component	Description
Virtual Mobile Infrastructure Server	The Virtual Mobile Infrastructure 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' workspace. • Compute node hosts workspaces. Each workspace runs as a Virtual Mobile Infrastructure instance.
Virtual Mobile Infrastructure Mobile Client Application	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.

Secure Access	The Virtual Mobile Infrastructure Secure Access enables mobile clients to access Virtual Mobile Infrastructure server via Internet.
External Database	External Database provides scalable data storage for user data. By default, Virtual Mobile Infrastructure 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.
External Storage	Using this option will enable you to store the user data in an external storage.
Active Directory	The Virtual Mobile Infrastructure server imports groups and users from Active Directory.

2 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 TMVMI product.

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

- The VMI 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.

3 Guidance

TMVMI applies in the evaluated configuration along with this Common Criteria specific guidance. This guidance covers Android 5.1 and above, and for iOS versions 10.0 and above. There is no extra configuration needed to evaluated cryptography

3.1 Features

3.1.1 Specify server information

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

3.1.2 Appling server configuration:

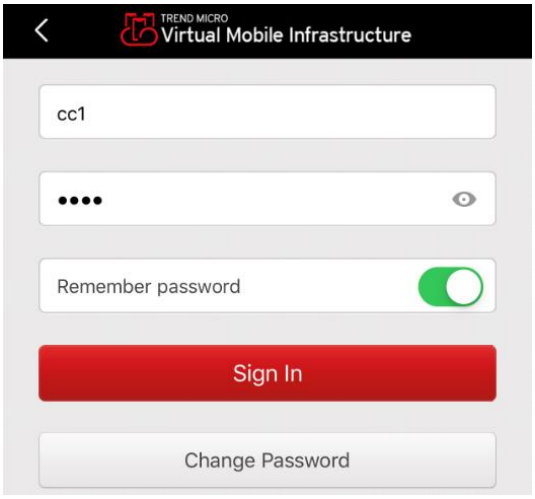
Launch the application and input the server address, client will communicate with the server to get some configurations from server.

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


```
{
    "current_ios_client_version": "6.0.1060",
    "graphic_quality": 1,
    "remember_passwd": true,
    "current_android_client_version": "6.0.1155",
    "root_or_jailbreak": 1,
    "enable_csr": false,
    "change_password": false,
}
```

3.1.3 Login

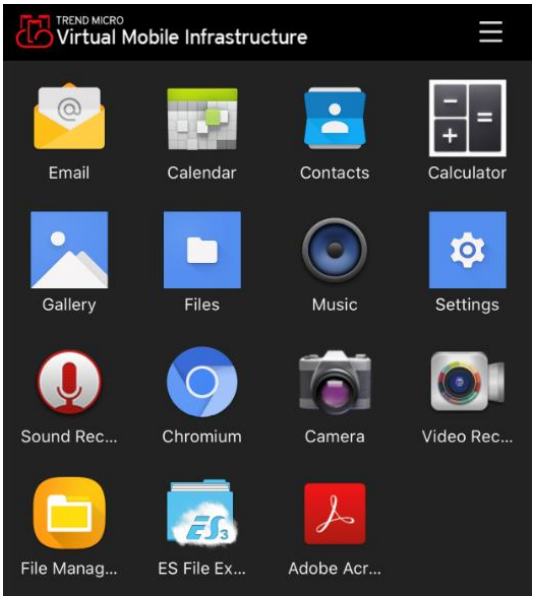
After get configuration, we can input our account and password to login the server via https protocol.



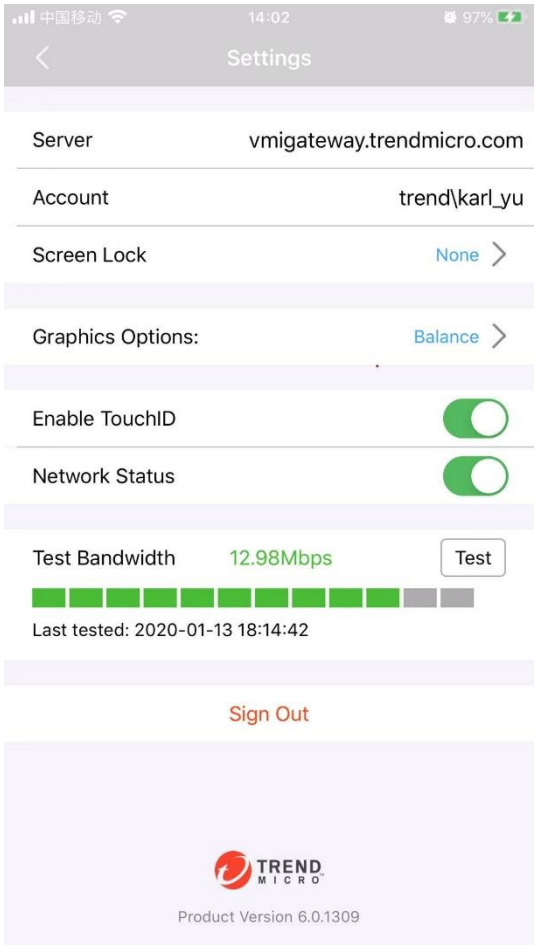
If login successfully, client will connect to the virtual mobile(workspace) in server, using a customized trusted channel (~~a module similar to WBERTC~~) based on OPENSSL.

3.1.4 Operate the workspace

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



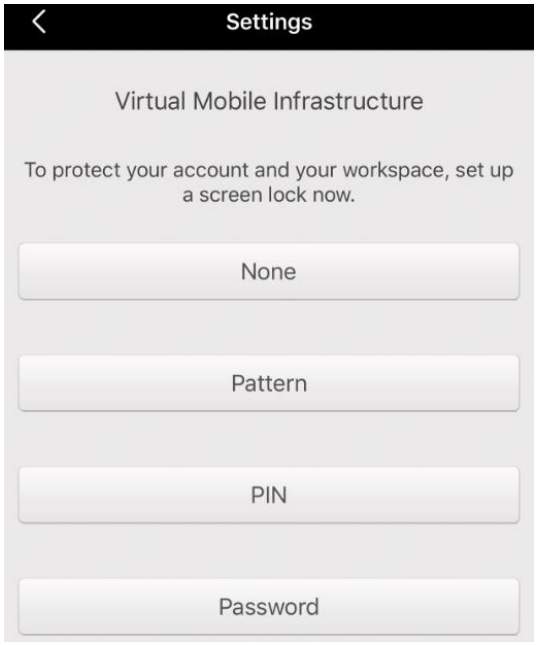
3.1.5 Setting configuration options



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/face recognition in Android, screen lock can be skipped by input that information.

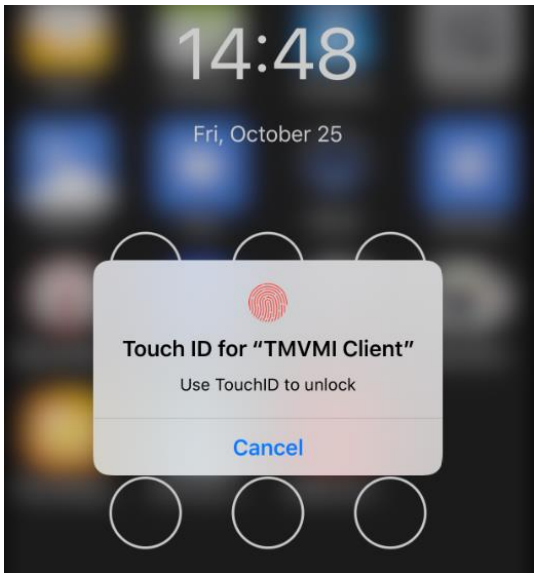


Graphics Options:

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 Touch ID/Fingerprint

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



Network Status

Virtual mobile can show the network connection status with the mobile device.

Green: quick

Yellow: slowly

Red: very slowly

Test Bandwidth

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

4 Reference Identifier for TLS

TBD

5 Required Permissions

5.1 Android Permissions

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

- **Access network state**
- **Access WIFI state**
- **Bluetooth**
- **Change WIFI state**
- **Internet**
- **Request install packages**
- **Use fingerprint**
- **Vibrate**
- **Wake lock**
- **Foreground service**
- **Access coarse location**
- **Access fine location**
- **Camera**
- **Record audio**

A brief summary that describes how these Android permissions are used is given in the following subsections.

5.1.1 Access network state

The TMVMI client access the state of the network interface to get connectivity.

5.1.2 Access WIFI state

The TMVMI client access the state of the network interface to get connectivity.

5.1.3 Bluetooth

The TMVMI client provide access to device's Bluetooth to enables bluetooth connection in virtual mobile

5.1.4 Bluetooth admin

The TMVMI client provide access to device's Bluetooth to enables application discover or pair Bluetooth devices in virtual mobile

5.1.5 Change WIFI state

The TMVMI client provide access to Wi-Fi state to enable turn ON/OFF device's WIFI in virtual mobile

5.1.6 Internet

The TMVMI Client must access networks to communicate with the Virtual Mobile running in TMVMI server. It can use any of the provided networks (Wi-Fi, 4G/LTE, 3G) when they are active.

5.1.7 Request install packages

The TMVMI client need to request installing package for installation.

5.1.8 Fingerprint

The TMVMI Client uses the fingerprint permission to enable a Biometric Authentication Factor in the form of a fingerprint. The TMVMI Client supports biometric fingerprint ID capabilities if the mobile device's underlying platform supports biometric authentication.

5.1.9 Vibrate

The TMVMI Client uses the mobile device's vibrator to provide silent notification alerts.

5.1.10 Wake lock

The TMVMI client need to use Power Manager Wake Locks to keep processor from sleeping or screen from dimming.

5.1.11 Foreground service

The TMVMI client need to use foreground service to keep active

5.1.12 Access coarse location

The TMVMI Client provides access to the coarse location for apps in the Virtual Mobile that require device's location.

5.1.13 Access fine location

The TMVMI Client provides access to fine location for apps in the Virtual Mobile that require device's location.

5.1.14 Camera

The TMVMI Client provides remote access to the device's camera to multimedia apps that use the camera in the Virtual Mobile.

5.1.15 Record audio

The TMVMI Client provides access to the device's microphone to enables voice recording and phone apps in the Virtual Mobile.

5.2 iOS Permissions

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

- **Background operation**
- **Camera**
- **Location**
- **Microphone**
- **Photo library**
- **Notifications**
- **Bluetooth**

Some permissions must be granted expressly by the user. In some cases, the permission is requested when the Client application is first launched. In other cases, the user may be prompted when the permission is first needed. In one case, it must enable the permission manually if it is required.
A brief summary that describes how these iOS permissions are used is given in the following subsections.

5.2.1 Background operation

The TMVMI 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.

5.2.2 Camera

The TMVMI 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.

5.2.3 Location

The TMVMI Client provides access to the GPS sensors, the Wi-Fi location services of the mobile device for authentication with the TMVMI 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.

5.2.4 Microphone

The TMVMI 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.

5.2.5 Photo library

The TMVMI 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 TMVMI Client only use *UIImagePickerControllerSourceTypeCamera* from iOS platform to take photos under this permission, the TMVMI 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.

5.2.6 Notifications

The TMVMI 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.

5.2.6 Bluetooth

The TMVMI 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.

6 Updates and Update Verification

Users obtain TMVMI Client updates using Android or iOS update mechanisms or from TMVMI 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 TMVMI server. TMVMI 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.

7 Verify Version of the TMVMI Client

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