Tellus eVV Hardware and Software Requirements

Introduction

This document specifies the hardware and software requirements for the following end-users of the Tellus eVV Solution:

1. **Caregivers** - Use the Tellus eVV Solution on their Mobile Device.
2. **Provider Agency Users** - Typically use the portal solution using a PC browser.

Supported Operating Systems and Browsers

Tellus certifies support for the eVV Portal (browser based), Claims Portal (browser based), and eVV App (mobile device app) on the following browsers and phone/PC operating systems.

Important Note: Tellus will support any operating system and browser listed below only as long as supported by the product supplier, and only so long as Tellus determines that there are no security flaws that could compromise Tellus information security.

Supported PC Operating Systems:

1. Windows OS (32 or 64 bit) Version 7 or higher.
2. Mac OS Version X (10) or higher.

Supported Mobile Operating Systems:

1. iOS Version 9 or higher.
2. Android Version Lollipop (5.0) or higher.

Supported PC Browsers:

1. Microsoft Edge Version 16 or higher.
2. Google Chrome Version 4 or higher.
3. Apple Safari Version 10 (Mac)/4 (Windows) or higher.
4. Mozilla Firefox Version 57 or higher.

Supported Mobile Browsers:

1. Google Chrome Version 4 or higher on Android.
2. Apple Safari Version 4 or higher on iOS.

Mobile Device Hardware Requirements

Tellus certifies our mobile apps on devices that meet the following specifications:

1. Form factor: Tablet of phone.
2. Operating System: Android or iOS (see above).
3. Bluetooth required: No
4. GPS required: Yes
5. Voice support required: No
6. Min Memory of Phone: No minimum
7. Min storage of phone: 50 MB

MDM Requirements

Mobile device management (MDM), is the process of managing and controlling a broad set of mobile device characteristics. MDM solutions are typically used to ensure security and valid use of a device that is provisioned by a business to an employee, or by a business to safeguard a business that has a bring-your-own-device (BYOD) policy. MDM may:

- Control which apps can be present on the devices.
- Control app access to device resources such as storage, mobile data usage, and camera.
- Allow for device location.
- Allow for securing devices if lost or stolen.

Many businesses use a third-party mobile device management software. Some of the most popular providers are:

- Google MDM.
- Microsoft Intune
- Cisco Meraki
- IBM MaaS360.
- AirWatch
- Citrix XenMobile
- SAP Mobile Secure
- Jamf Pro
- Samsung Knox

If the Tellus eVV+ mobile app is to operate on an MDM-managed solution, then the MDM solution must be configured to allow the following app access. If Optional, then eVV will still be possible. If required, then eVV will not work effectively without the privilege.

Access	Required/Optional	Reason
Camera	Optional	For user to take avatar picture.
Face ID (when available)	Optional	For biometric app login.
Fingerprint ID (when available)	Optional	For biometric app login.
Location Services	Required	For geo-location of visit check-in/check-out.
Photo Library	Optional	To allow user to select avatar picture.
Mobile Data	Required (unless user accesses internet only via WiFi network)	For internet access.
WiFi Data	Required (unless user accesses internet only mobile network)	For internet access.
File Storage	Required	For local encrypted storage of working data.