Exigences techniques (V060324)

Les exigences suivantes, quelle que soit la technologie utilisée dans le
CLIENT/ÉCOLE, sont nécessaires au bon fonctionnement d'IMTLazarus :

● Il est nécessaire que l'infrastructure WiFi du centre fonctionne correctement et sans micro-coupures.

● S'il existe un pare-feu réseau, autorisez la communication bidirectionnelle en TCP, UDP et WebSockets sécurisés (WSS) avec adresses **manager.imtlazarus.com** (**manager-usa1.imtlazarus.com** aux États-Unis) et [**serveur_école].imtlazarus.com**

● Les ports utilisés sont :

- ● 443 et 80
- ● 9001-9004 TCP (9001-9002-9003-9004) « port websocket »
- ● 8991-8994 TCP (8991-8992-8993-8994) « port websocket »
- ● 8999 TCP

Spécifications techniques des appareils Chromebook/Google Workspace :

● Il est nécessaire que la personne responsable du déploiement d'IMTLazarus ait accès en tant que
administrateur de Google Workspace pour pouvoir installer l'extension IMTLazarus.

● L'extension IMTLazarus sera chargée uniquement dans les unités/groupes organisationnels avec permis. (Voir le document sur imtlazarus.com → Ressources → Administrateurs → Guides installation et utilisation → CHARGER L'EXTENSION GOOGLE WORKSPACE)

● Posséder une licence éducative Google Workspace gérée par le centre.

Nous recommandons:

● Avoir un lien vers Google Workspace correctement activé pour une importation
données. (Voir le document sur imtlazarus.com → Ressources → Administrateurs → Guides installation et utilisation → IMPORTATION DE DONNÉES DEPUIS GOOGLE WORKSPACE)

Spécifications techniques pour les appareils Android/Samsung :

● La version de l'appareil doit être Android 8.0 ou supérieure (sécurité renforcée sur
Appareils Samsung dotés de la technologie Knox).

● L'information obligatoire requise est l'email.

● La seule application de navigateur autorisée sera IMTGo.

Spécifications techniques pour les appareils Windows/Intune :

● La version des appareils doit être Windows 10 ou supérieure.

● Les données requises sont : le numéro de série de l'appareil ou l'utilisateur Azure toujours avec Intune MDM.

● Les seuls navigateurs autorisés seront : Google Chrome et MS Edge Chromium (le reste des navigateurs ou des versions portables seront bloqués)

● Le seul antivirus utilisé doit être Windows Defender.

Nous recommandons:

● Le compte utilisé par l'étudiant doit être limité, sans autorisations d'administrateur du système.

● Que l'étudiant ne connaît pas le mot de passe du compte administrateur.

Spécifications techniques pour les appareils iOS :

● La version des appareils doit être iOS 15 ou supérieure.

● La seule application de navigateur autorisée à assurer la sécurité sera IMTGo.

● Les données obligatoires requises sont : email et numéro de série pour un déploiement automatiquement via MDM.

Nous recommandons:

● Que les appareils soient supervisés afin de gérer la navigation dans d'autres navigateurs et contrôler les profils gérés par différentes applications.

● Que lorsque les appareils ne sont PAS supervisés (appareils BYOD), nous devons s'appuyer sur le système « Time of Use » dans le but de limiter l'usage des les candidatures ne sont pas autorisées.

● Qu'ils soient liés au MDM via DEP.