

## Requisiti tecnici (V240306)

I seguenti requisiti, indipendentemente dalla tecnologia utilizzata nella SCUOLA/CLIENTE, sono necessari per il corretto funzionamento di IMTLazarus:

- È necessario che l'infrastruttura Wi-Fi del centro funzioni correttamente e senza micro-tagli.
- Se esiste un firewall di rete, consentire la comunicazione bidirezionale in TCP, UDP e Secure WebSockets (WSS) con gli indirizzi di **manager.imtlazarus.com** (**manager-usa1.imtlazarus.com** negli Stati Uniti) e [scuola\_server].imtlazarus.com
- Le porte utilizzate sono:  
443 e 80  
9001-9004 TCP (9001-9002-9003-9004) "porta di collegamento"  
8991-8994 TCP (8991-8992-8993-8994) "porta di archiviazione online"  
8999 TCP

### Specifiche tecniche per i dispositivi Chromebook/Google Workspace:

- IMTLazarus Deployment Manager deve avere accesso come amministratore a Google Workspace per installare l'estensione IMTLazarus.
- L'estensione IMTLazarus verrà caricata solo sulle Unità organizzative / Gruppi licenziati. (Vedere il documento in [imtlazarus.com/en](https://imtlazarus.com/en) → Risorse → Amministratori → Guide per l'installazione e l'uso → INSTALLAZIONE DELL'ESTENSIONE GOOGLE WORKSPACE).
- Avere una licenza educativa Google Workspace gestita dal centro scolastico.  
Si consiglia:
  - Avere un collegamento a Google Workspace correttamente attivato per l'importazione di dati. (Vedere il documento in [imtlazarus.com/en](https://imtlazarus.com/en) → Risorse → Amministratori → Guide per l'installazione e l'uso → IMPORTARE DATI DA GOOGLE WORKSPACE).

### Specifiche tecniche per i dispositivi Android/Samsung:

- La versione del dispositivo deve essere Android 8.0 o superiore (maggiore sicurezza sui dispositivi Samsung con tecnologia Knox).
- Il dato di campo richieste è l'e-mail.
- L'unica applicazione del browser consentita sarà IMTGo.

### Specifiche tecniche per i dispositivi Windows/Intune:

- La versione del dispositivo deve essere Windows 10 o superiore.
- I dati richiesti sono: il numero di serie del dispositivo o l'utente Azure sempre con MDM Intune.
- Gli unici browser consentiti saranno: Google Chrome e MS Edge Chromium (altri browser o versioni portatili saranno bloccati).
- L'unico antivirus utilizzato deve essere Windows Defender.

Si consiglia:

- Che l'account utilizzato dallo studente deve essere limitato, senza autorizzazioni di amministratore di sistema.
- Che lo studente non conosca la password dell'account amministratore.

### **Specifiche tecniche per i dispositivi iOS:**

- La versione del dispositivo deve essere iOS 15 o superiore.
- L'unica applicazione del browser consentito per garantire la sicurezza sarà IMTGo.
- I dati richiesti sono: l'e-mail e il numero di serie per il dispiegamento automatico tramite MDM.

Si consiglia:

- Che i dispositivi siano monitorati con l'obiettivo di gestire la navigazione in altri browser e controllare i profili che gestiscono le diverse applicazioni.
- Che quando i dispositivi NON sono monitorati (dispositivi BYOD) dovremmo fare affidamento sul sistema "Time of Use" per limitare l'uso di applicazioni non autorizzate.
- Che sono collegati al MDM attraverso il DEP.