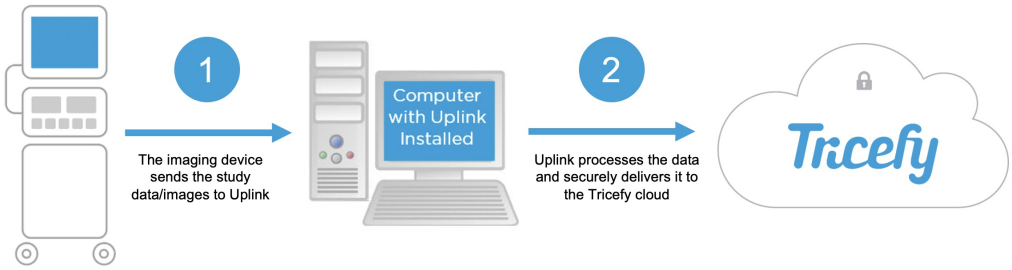
Network Setup and Firewalls

Last Modified on 2025-07-31 13:24



Firewall changes may be needed in order to allow the local Uplink to reach Tricefy Cloud

Tricefy Uplink Connection to Tricefy Global Cloud

Outbound port: **443**
Domain: **receiving.tricefy.com**
Public IPs: **54.72.5.235 || 54.171.0.176**
Encryption: TLS 1.3

Tricefy Uplink Connection to Tricefy USA Cloud

Outbound port: **443**
Domain: **receiving.us.tricefy.com**
Public IPs: **35.169.253.152 || 18.207.44.115**
Encryption: TLS 1.3

**Tricefy uplink only needs outbound access in the firewall. While the Tricefy Uplink service utilizes TLS appropriately, the protocol used within is not HTTP-based. Firewall systems with [deep] packet inspection enabled may continue to block the Uplink traffic. As a result, it may be necessary to disable packet inspection if Uplink cannot communicate with Tricefy cloud.

Local Windows Settings & Anti-Virus

When Uplink is installed, a Windows service called – Tricefy Uplink – will run in the background. The installation process is designed to apply local Windows firewall rules to avoid from blocking the local uplink process/service.

Systems with anti-virus software may also prevent the Uplink from communicating with Tricefy cloud, and very commonly will block the Uplink installer from running or successfully completing. It may be necessary to whitelist the Tricefy Uplink service/process/folder in the anti-virus admin settings. If possible, temporarily disabling the anti-virus software altogether on the host can help to rule it out.