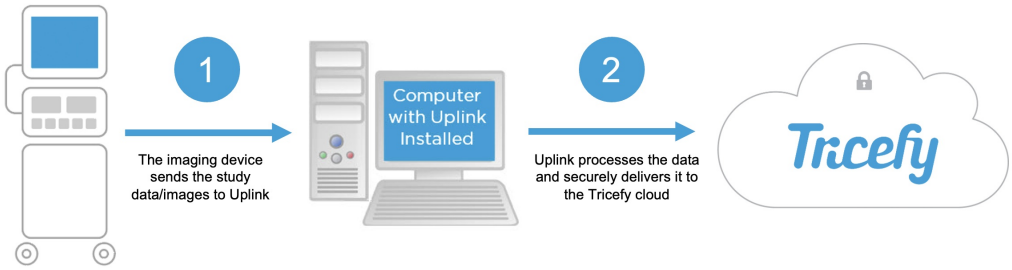
Network Setup and Firewalls

Last Modified on 2025-07-17 21:23



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 Firewall Settings

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, however a network firewall can still be blocking the traffic.

If you have an IT department, confirm with IT that firewalls are configured to allow the Tricefy Uplink process with the communication details above.

If you don't have an IT department, try the following troubleshooting steps:

- Temporarily turn off Windows firewall
  - Test the ultrasound connection using Ping/Verify - if it works, firewall needs to be configured to allow the Tricefy Uplink process
- Temporarily turn off anti-virus software

- Test the ultrasound connection Ping/Verify - if it works, an AV software exception needs to be configured to allow the Tricefy Uplink process