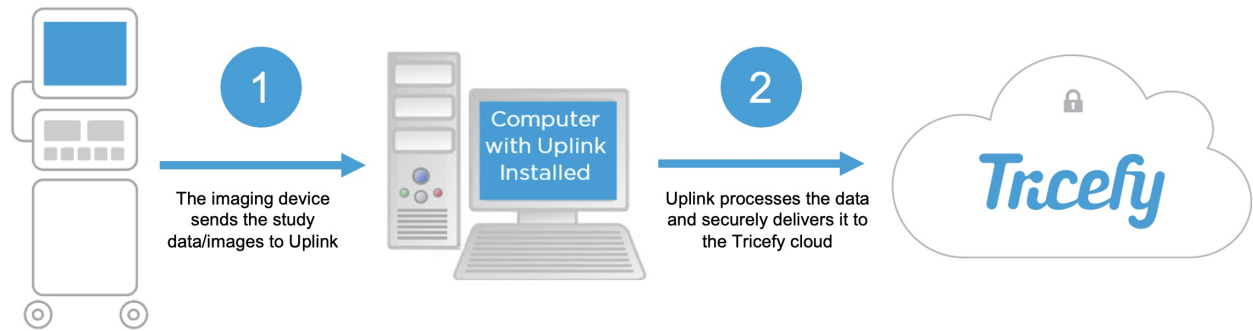




Network Setup and Firewalls

Last Modified on 2025-04-15 16:15



In some cases, firewall changes may be needed in order to allow the local Tricefy Uplink to communicate out to the 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 only needs outbound access in the firewall

Note: **legacy** uplink will connect through a different domain (receiving.trice.io) but resolves to the same 2 public IPs above

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

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
-