Tech Tool Network Setting Guidelines

Version 2.2

Last Modified – 21/05/2025

Abstract

This document describes the Tech Tool network environment and connectivity methods.

Tech Tool Network Setting Guideline

Introduction

This document describes the Tech Tool network environment and connectivity methods. It is intended to assist external network administrators with setting up and troubleshooting Tech Tool connectivity issues.

Network Overview

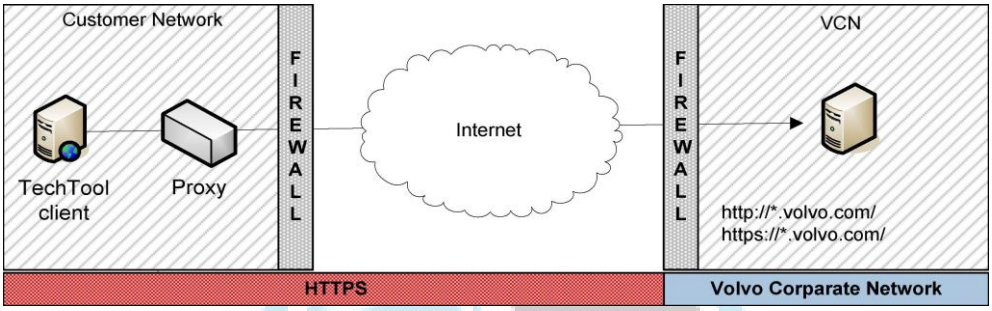

Figure 1: Network Overview

Note: The proxy component is not always implemented at customer sites.

Network Components

Network settings and software requirements are updated with every Tech Tool release.

See *Client HW and SW requirements* for more information.

1. Customer Network Firewall

The customer network firewall must be configured to allow the Tech Tool client to connect to the following:

- *.volvo.com
- port 80 (HTTP)
- port 443 (HTTPS)
- *.msappproxy.net
- port 8891 (HTTP)
- port 8893 (HTTP)
- port 8895 (HTTP)
- port 2010 (HTTP)

SSL Inspection

Customers implementing SSL inspection using firewall products that replace the certificate path for custom certificate authorities need to include exceptions for all volvo.com domain and there should not be SSL inspection for *.msappproxy.net

2. Customer Network Proxy

The customer network proxy must be configured to allow outgoing HTTP and HTTPS traffic and allow the client to tunnel outbound SSL requests.

The reverse proxy webserver requires that the Tech Tool client is authenticated using the SSL server certificate. Any setup which terminates SSL connections is not supported.

If Team Viewer is used for remote support, it must be configured using local proxy settings. See Local Software Firewall Configuration.

3. Installation

Before installing Tech Tool, ensure the following prerequisites are met:

- Active internet connection (mandatory for all installation methods).
- Client ID, User Principal Name (UPN), and Password.

General Installation Notes

- Ensure you are logged in as "Administrator" or have administrative rights to perform the installation.
- Verify that all Microsoft patches are up to date before starting the installation.
- Temporarily disable User Access Controls (UAC) during the installation process.
- Turn off any toolbars and pop-up blockers before installing.
- Maintain an active Internet connection throughout the installation and confirm that firewall and proxy settings meet installation requirements.
- If the machine is controlled by domain policies (e.g., restricted folder or registry access, BIOS read permissions, MS-SQL password complexity requirements), install outside of the domain with these restrictions lifted.
- Some antivirus software may flag installation code as malware, which can block the process. Disable antivirus software temporarily before installing and re-enable it afterward.

Network installation

Network installation is also supported. A small generic installer component is downloaded by the user. This component manages the encryption and download of all other packages required for the current installation. At the end of the installation, the installer will search for new applicable updates.

4. Prerequisite .Net Components

Tech Tool uses Windows Communication Foundation (WCF) to host local services. WCF is a part of the Microsoft .NET Framework. The required .NET framework is installed automatically by Tech Tool if it is not present on the client.

- Tech Tool 2
  - .NET Framework 4.8
- Client Update & FIDO
  - .NET Framework 4.6.2

5. Client Components

The Tech Tool client has following components:

- Tech Tool executable (VolvoIt.Baf.CoreUi.exe)
- Tech Tool Service Controller (VolvoIt.Baf.ServiceHostController.exe)
- Tech Tool Service Host (VolvoIt.Baf.ServiceHostProcess.exe)
- CodeMeter Runtime Server (CodeMeter.exe)

Note: For the restricted environment above mentioned components needs to be whitelisted.

Background services

Some Tech Tool services are required to be running in the background even when Tech Tool is not. These background services are hosted by the following Windows service hosts and are started at Windows start-up:

- *CLUP Agent* runs under the Windows Local System
- *FIDO Agent* runs under the Windows Local System

Note: "Tech Tool Service Control Service" will be running in the background if the user has opted for "Start services during the initial launch of Tech Tool" in the settings -> System Start-up of Tech Tool.

Troubleshooting

This chapter offers solutions to the most common networking and connectivity issues.

1. Active Directory Group Policies

Active Directory (AD) group policies are used to standardize client behavior. If outgoing proxy settings are deployed through group policies, these policies must be applied to both the COMPUTER and the USER account on the client.

Note: *This applies mostly to MyPlace PC.*

2. Local Software Firewall Configuration

Local software firewalls must be configured to allow communication from the following:

- Tech Tool application:
  - *VolvoIt.Baf.Core.Ui.exe, on port 8891*
  - *VolvoIt.Baf.Core.Ui.exe, on port 8895*
- Grade-X:
  - *GRADE-X TEA2+ APP.exe, on port 8893*
- Windows Service:
  - *Volvo Tech Tool Service Controller, on port 8891*
  - *Volvo Tech Tool Service Controller, on port 8895*
- WCF
  - http://*.volvo.com/* ; port 80
  - https://*.volvo.com/* ; port 443

- https://*.volvo.com/* ; port 2010

- Client Update
  - https://*.volvo.com/*

***Note**: Client Update must be configured using the above URLs, not using an IP address*

- TeamViewer
  - http://www.teamviewer.com

Proxy Requirements

Tech Tool operates under two different user contexts:

1. The logged-in user (typically the service technician).
2. The LOCAL SYSTEM account (i.e., the machine name).

This can lead to connectivity problems with central systems and network update sites—especially at fleet locations where web filtering proxies and authentication are required. While PTT allows the logged-in user to authenticate automatically, it does not enable the LOCAL SYSTEM account to do so. As a result, network updates may fail, or Internet connectivity checks may not pass (e.g., no option to “Connect to Central Systems”).

To resolve these issues, choose one of the following approaches:

1. Allow LOCAL SYSTEM to Bypass Proxy Authentication

Configure the proxy to allow the LOCAL SYSTEM (machine account) to bypass authentication. This may require changes in Active Directory settings and/or proxy rules.

2. Run the "BAF" Service Under a Different User Account

Start the “BAF” system service using a user ID that has unrestricted Internet access (not the service tech’s personal ID). This maintains security, as the technician’s account can still be restricted from accessing inappropriate websites.

Optional Proxy Configuration:

If the proxy allows, enable unauthenticated access to the following domains for both the service tech's user ID and the LOCAL SYSTEM account (or the account used to start "baf"):

- http://*.volvo.com/* – Port 80
- https://*.volvo.com/* – Ports 443 and 2010
- *.msappproxy.net

Note: PTT must be able to resolve these domains **directly**. **Proxied DNS is not supported**.

Also, PTT will fail if the proxy:

- **Performs HTTPS inspection** (i.e., decrypts and re-encrypts traffic).
- Does **not** allow HTTPS tunnelling via the CONNECT method.

The application must be allowed to tunnel HTTPS traffic without interference to ensure SYSTEM CONTENT access.

Test URLs

To verify that the **user** has proper Internet and proxy access (there is no direct way to test LOCAL SYSTEM access other than checking proxy/firewall logs for blocks) open these URLs in Microsoft Edge — a successful result will return a splash page or XML code.

- https://networkupdatefilespublic.it.volvo.com/ping.htm - if this fails, so will client updates.
- https://networkupdatemetadata.it.volvo.com/manifests_v21/Diagnostic%20Communication%20Database%20(M)%20000.009/master/mastermanifest.xml - if this fails, so will updates.