Tech Tool Network Setting Guidelines

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

The Tech Tool client uses HTTP and HTTPS protocols to connect to the systems located on the Volvo Corporate Network (VCN). These systems are referred to as Volvo Central Systems (VCS).

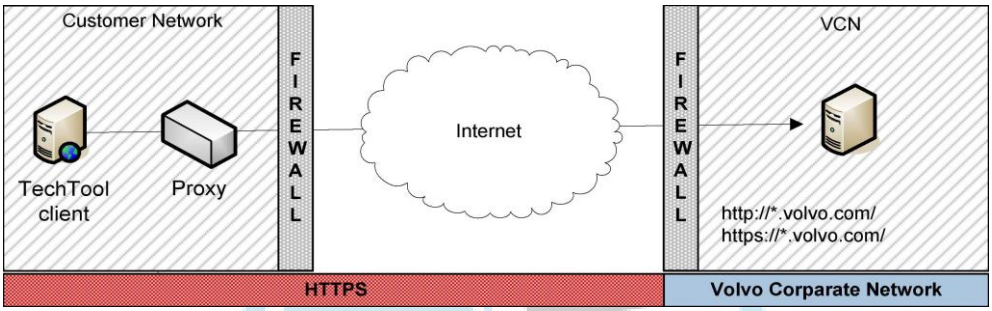


Figure 1: Network Overview

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 on a USB drive.

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)
- port 8891 (HTTP)
- port 8893 (HTTP)
- port 8895 (HTTP)
- port 2010 (HTTPS)
- http://www.msftncsi.com/ncsi.txt
- *.msappproxy.net
- secureweb.volvo.com
- viftng.volvo.com
- hmgmobile.it.volvo.com
- sws.it.volvo.com
- networkupdatemetadata.it.volvo.com
- networkupdatefilespublic.it.volvo.com
- hmg.it.volvo.com
- msftncsi.com/ncsi.txt

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 sub-domain certificates.

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.

Secure Web

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

Team viewer

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

Internet

The Tech Tool client connects to VCS over the internet. For information on optimizing this connection, refer to Configuring MTU.

3. Installation

Tech Tool can be installed from a network

Prerequisites

An internet connection is required for all installation methods. Client Id, User Id, and Password are verified by the Installer.

General Installation Notes

- Ensure you are logged in as an “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 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. Client Components

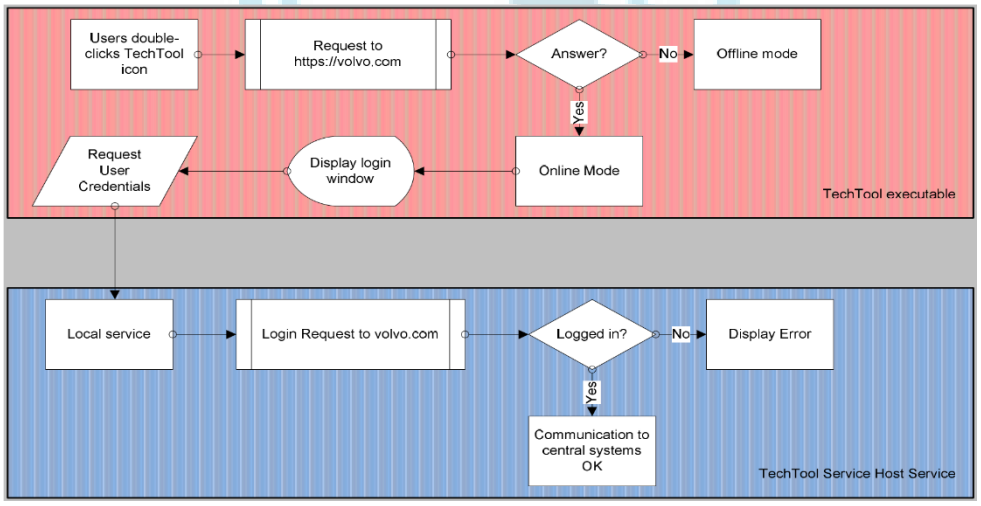
Tech Tool uses Windows Communication Foundation (WCF) to host local services. WCF is a part of the Microsoft .NET Framework. The required .NET framework is installed automatically by Tech Tool if it is not present on the client.

- Tech Tool 2
  - .NET Framework 4.8
- Client Update & FIDO
  - .NET Framework 4.6

5. Client Components

The Tech Tool client has three communication components:

- Tech Tool executable (VolvoIt.Baf.CoreUi.exe)
- Tech Tool Service Controller (VolvoIt.Baf.ServiceHostController.exe)



- Tech Tool Service Host (VolvoIt.Baf.ServiceHostProcess.exe)

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.

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

3. Configuring MTU

If large data packets are sent over a network, the router splits the packets into smaller chunks, causing packet fragmentation. Fragmentation depends on the Maximum Transfer Unit (MTU) size. A slow network connection can cause packet fragmentation, and this can result in poor network performance and timeouts in Tech Tool.

To discover the optimal MTU value, do the following:

1. Open the Command Prompt on the Tech Tool client
2. Execute the following command: ping secureweb.volvo.com -f -l 1492, where 1492 represents the MTU value.
3. If the response is: that the packet needs to be fragmented but DF set, then the MTU is too high.
4. Repeat steps 1. and 2. using a lower MTU value until a response similar to the following is shown: Reply: bytes=1200 time=1ms TTL=61
5. The MTU value can be increased in smaller increments until the correct value is found.
6. Set the MTU on the client and network routers to this value.

Proxy Requirements

Tech Tool runs as 2 different users: the human that is at the keyboard and the LOCAL SYSTEM (i.e., the machine name). This can create connectivity problems with both the central systems and the network update sites, particularly at fleet sites with web filtering proxies and authentication requirements. While PTT provides a means of letting the end user automatically authenticate, it doesn't allow the LOCAL SYSTEM to do the same. The result is that network updates don't work, or verification of Internet connectivity fails (no option to "Connect to Central Systems").

There are two methods to fix this problem:

1. The LOCAL SYSTEM, i.e., machine name, MUST be allowed to pass through or bypass the proxy without authentication (This may require Active Directory setup and/or proxy rule changes.).
2. The "baf" system service can be started with a user ID that is allowed to access the Internet without authentication (i.e., not the service tech's ID).

The service tech's User ID can still be forced to authenticate, so he can't surf to "less than desirable" websites. If the proxy software is capable, it may be possible to configure it to allow unauthenticated access to *.volvo.com sites. The proxy must permit access to these URLs (HTTP and HTTPS) for both the service tech's user id and for LOCAL SYSTEM (or the user id employed to start" baf"):

- http://*.volvo.com/* ; port 80
- https://*.volvo.com/* ; port 443
- https://*.volvo.com/* ; port 2010
- https://*.volvo.com/*
- http://www.teamviewer.com
- secureweb.volvo.com/*
- sws.it.volvo.com/*
- networkupdatemetadata.it.volvo.com/*
- networkupdatefilespublic.it.volvo.com/*
- hmg.it.volvo.com/*
- viftng.volvo.com/*
- msftncsi.com/ncsi.txt
- *.msappproxy.net

Finally, proxied DNS is not supported (PTT must be able to resolve the above URLs directly), and proxy configurations that terminate HTTPS tunnels (man-in-the-middle) and forward after decryption/re-encryption will cause PTT to fail. The application must be allowed to tunnel HTTPS using the CONNECT method for SYSTEM CONTENT.

Test URLs (verify that the USER has access through proxy and firewall; there are no means of testing if the MACHINE as LOCAL SYSTEM has access, other than review of drops/denies in the proxy and firewall logs):

Using IE, surf to these sites. You should get a splash page or XML code.

- **http://secureweb.volvo.com –** if this fails, you will not be able to log into Central Systems
- **https://hmg.it.volvo.com/hmgLite/ws/wsmq?wsdl -** if this fails, so will client updates
- **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
- **https://viftng.volvo.com/ -** if this fails, so will VCADS updates
- **https://hmgmobile.it.volvo.com:2010 –** if you get a response "401 Unauthorized", means 2010 is enabled. If not, the 2010 port is blocked/disabled and you will not be able to login