Guide to TT Network Update & Install (for Version 2.8)

General Installation Notes

- You must be logged in as “Administrator” or have admin rights to install.
- Make sure all Microsoft patches are up to date prior to install.
- You must turn off User Access Controls during the install.
- Disable all toolbars and pop-up blockers prior to install.
- You must have an Internet connection during the install and ensure that firewall and proxy requirements are met prior to the install.
- If the machine is locked down by domain policies (folder or registry write permissions, BIOS read, MS-SQL password complexity restrictions, etc), you’ll need to do the install off the domain with these restrictions removed.
- Some anti-virus products will view the code used during install as malware, blocking the install. Disable your antivirus prior to beginning the install and re-enable when complete.

Firewall Openings

Tech Tool requires that the firewall be open for outbound connections on ports 2010, 80 and 443 for the following URLs/IP addresses:

- secureweb.volvo.com (IP 153.112.167.191)
- sws.it.volvo.com (IP 153.112.167.146)
- networkupdatemetadata.it.volvo.com (IP 153.112.163.252)
- networkupdatefilespublic.it.volvo.com (IP 153.112.162.194)
- hmg.it.volvo.com (IP 153.112.166.184)
- viftng.volvo.com (IP 153.112.167.185)
- hmgmobile.it.volvo.com
- msftncsi.com/ncsi.txt
- *.msappproxy.net
  - baldoauthserviceprod-volvogroup.msappproxy.net
  - embla-volvogroup.msappproxy.net
  - ppd-volvogroup.msappproxy.net
  - genericlogger-volvogroup.msappproxy.net
  - namsppd-volvogroup.msappproxy.net
  - namsadmin-volvogroup.msappproxy.net
  - gdsp-volvogroup.msappproxy.net
  - wbimb1-volvogroup.msappproxy.net
  - wbimb2-volvogroup.msappproxy.net

Important Note: The development group strongly recommends that access is “permitted by domain name” (*.volvo.com) rather than by IP address in both the firewall and proxy. The above specific addresses are provided (and may change) if your organization’s security policies do not allow this.

Proxy Requirements

Tech Tool runs as 2 different users: the human that is at the keyboard and 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 userid 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” web sites. 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 userid and for LOCAL SYSTEM (or the userid employed to start” baf”):

- secureweb.volvo.com/* (IP 153.112.167.191)
- sws.it.volvo.com/* (IP 153.112.167.146)
- networkupdatemetadata.it.volvo.com/* (IP 153.112.163.252)
- networkupdatefilespublic.it.volvo.com/* (IP 153.112.162.194)
- hmg.it.volvo.com/* (IP 153.112.166.184)
- viftng.volvo.com/* (IP 153.112.167.185)
- 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 is 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, 2010 port is blocked/disabled and you will not be able to login