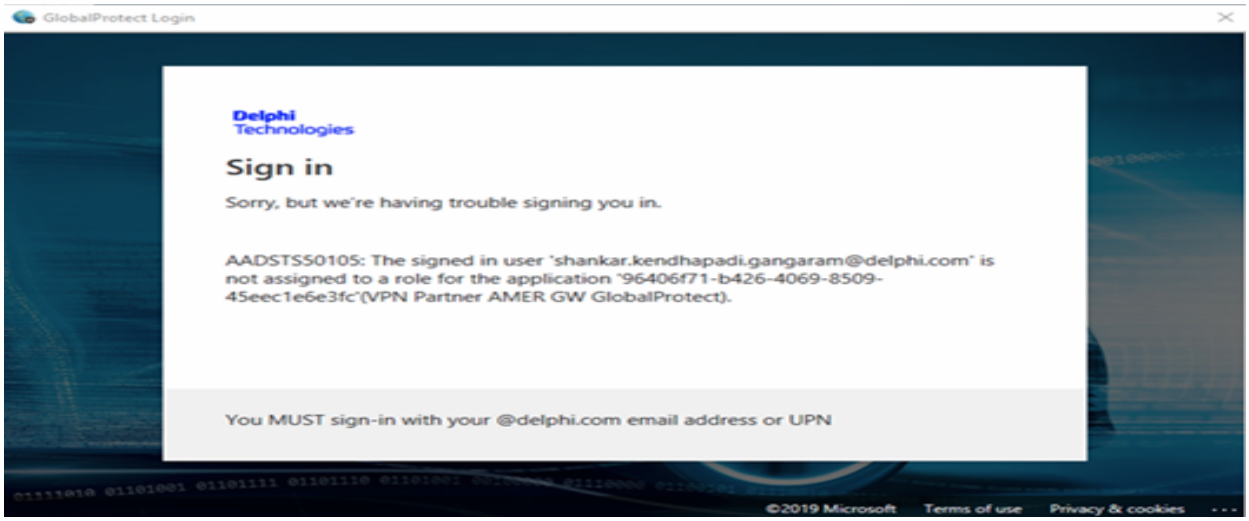
1. Acronyms and Abbreviations

- DGD : Delphi Global Desktop
- DT : Delphi Technologies
- GPO : Group Policy Object
- FQDN : Fully qualified domain name
- MFA : Multi-Factor Authentication
- AD : Active Directory
- APAC : Asia Pacific
- EMEA : Europe Middle East & Africa
- NA : North America
- SMS : Short Message Service
- SSL : Secure Sockets Layer
- UPN : User Principle Name
- VPN : Virtual Private Network
- URL : Uniform Resource Locator

Global Protect notes:
Most incidents that were reported were linked to the fact that partners were not in the proper groups. The document shows what is required for partners to be able to connect via GP successfully. If error message is about a role not to be assigned to the users, it is to be fixed by the **DT-AD team**.

For partners, there are 2 steps to be checked by AD team
Failing which the partner would not be able to connect resulting in the below error



1. **GlobalProtect for Partners:**
    a. **SAML Authentication in Azure AD: Make sure the users are added to the appropriate AD Groups.**
        i. **ASIA : VPN_Partner_ASIA, this provides access to the following GP Apps in Azure AD:**
            - **VPN Partner Portal GlobalProtect**
            - **VPN Partner ASIA GW GlobalProtect**
        ii. **EMEA : VPN_Partner_EMEA, this provides access to the following GP Apps in Azure AD:**
            - **VPN Partner Portal GlobalProtect**
            - **VPN Partner EMEA GW GlobalProtect**
        iii. **AMER : VPN_Partner_AMER, this provides access to the following GP Apps in Azure AD:**
            - **VPN Partner Portal GlobalProtect**
            - **VPN Partner AMER GW GlobalProtect**
    b. **In addition:**
        - **Firewall rule Authorizatin for On-prem Delphidrive AD group:**
            - **Add partner to DLG_VPN_<Partner_name> as per the groups below**
                - **DLG_VPN_GENPACT,**
                - **DLG_VPN_TCS**
                - **DLG_VPN_Avelabs**
                - **DLG_VPN_BARTECH**
                - **DLG_VPN_BASS**
                - **DLG_VPN_BMW_AG**
                - **DLG_VPN_Cadmaxx**
                - **DLG_VPN_Calibrate_Consulting**
                - **DLG_VPN_CANNON_PACKING_AND_LOGISTICS_LTD**
                - **DLG_VPN_CBI**
                - **DLG_VPN_Cogiscan**
                - **DLG_VPN_Corporate**
                - **DLG_VPN_Datelka**
                - **DLG_VPN_DCS**
                - **DLG_VPN_Digitalsoft**
                - **DLG_VPN_DilT-AG**
                - **DLG_VPN_Donyati**
                - **DLG_VPN_DPSS**
                - **DLG_VPN_DTSS**
                - **DLG_VPN_DTVS**
                - **DLG_VPN_DXC**
                - **DLG_VPN_DXC_technologies**

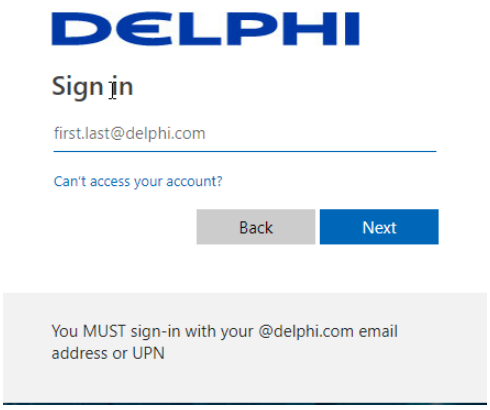
2. Download and Install GlobalProtect Agent for Windows

The download and installation procedure outlined in this document is only applicable for Delphi Business Partners. If you are a Delphi employee, please check GlobalProtect user guide for DGD or non-DGD machines.

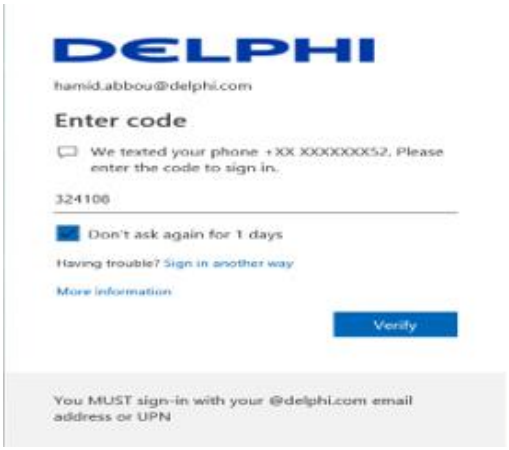
1. Log in to the GlobalProtect portal.

   Launch a web browser and go to the following URL:

   https://partner-access.delphi.com
2. You will be redirected to Azure MFA authentication. Enter your DELPHI.COM email address or UPN, then click **Next**:



3. Depending on your profile in Azure AD you should get a SMS on your mobile phone or a notification to validate via mobile app.

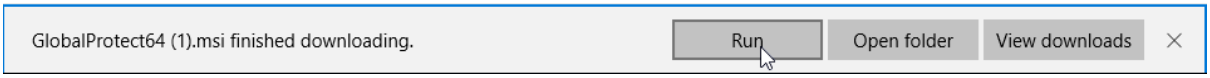


4. You will be redirected to the download site for GlobalProtect agent.

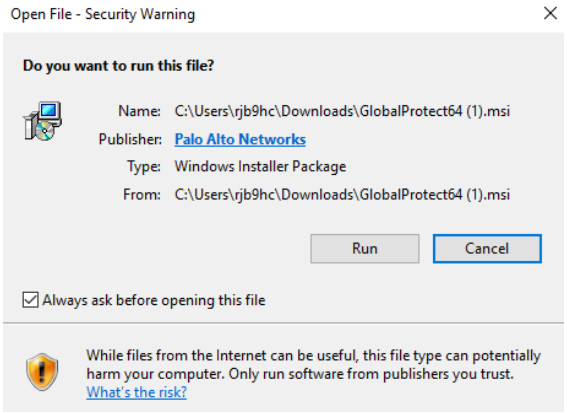
   To begin the download, click the software link that corresponds to the operating system running on your computer. If you are not sure whether the operating system is 32-bit or 64-bit, ask your system administrator before you proceed.

5. After the download is completed, start the installation process:

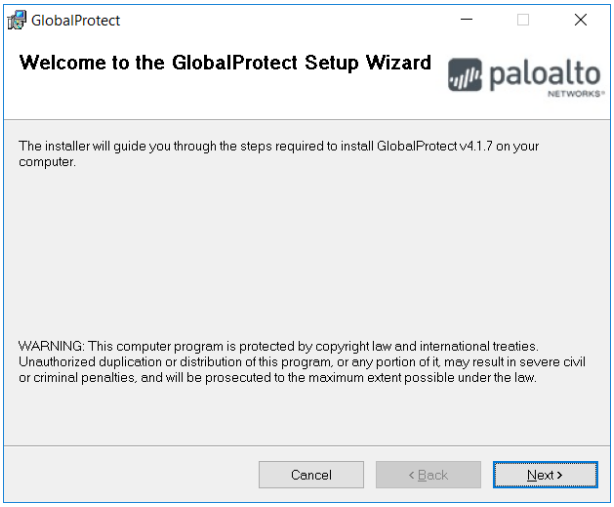
   a. Click on **run** to start the installation process



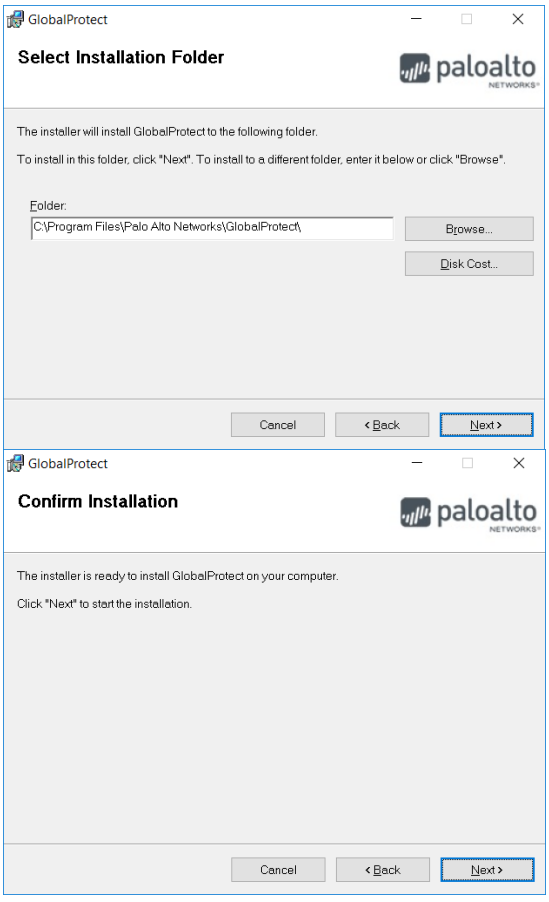
   b. Confirm the Security Warning – **Run**.



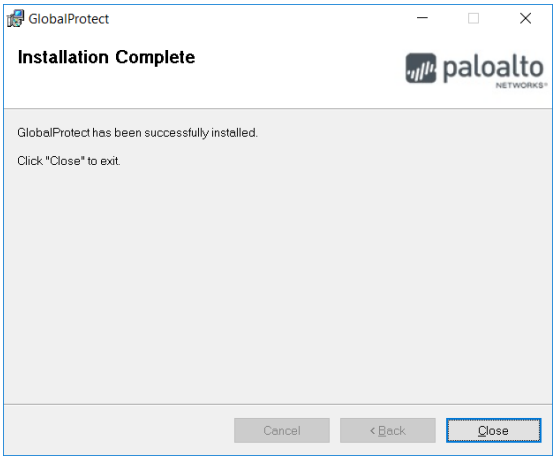
c. In the GlobalProtect Setup Wizard, click **Next.**



d. Click **Next** to accept the default installation folder (C:\Program Files\Palo Alto Networks\GlobalProtect), or click **Browse** to select a new location and then click **Next twice**.



e. After installation is complete, **Close** the wizard.

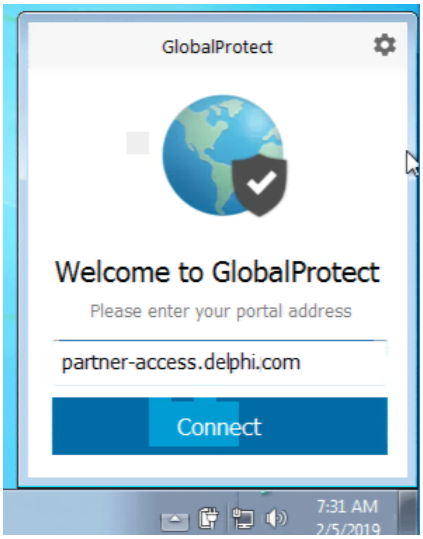


3. How to use GlobalProtect Agent for Windows

3.1. Connect to the GlobalProtect portal

a. Launch the GlobalProtect agent by clicking the system tray icon. The status will open.

b. Enter the FQDN of the portal **partner-access.delphi.com,** and then click **Connect**.



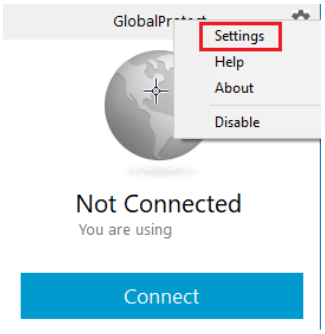
c. GlobalProtect client will redirect you to Azure MFA for authentication. Complete authentication process similar to Section 2, Step 2 & 3.

3.2. Open the GlobalProtect Agent

a. Click the GlobalProtect system tray icon to launch the app interface.

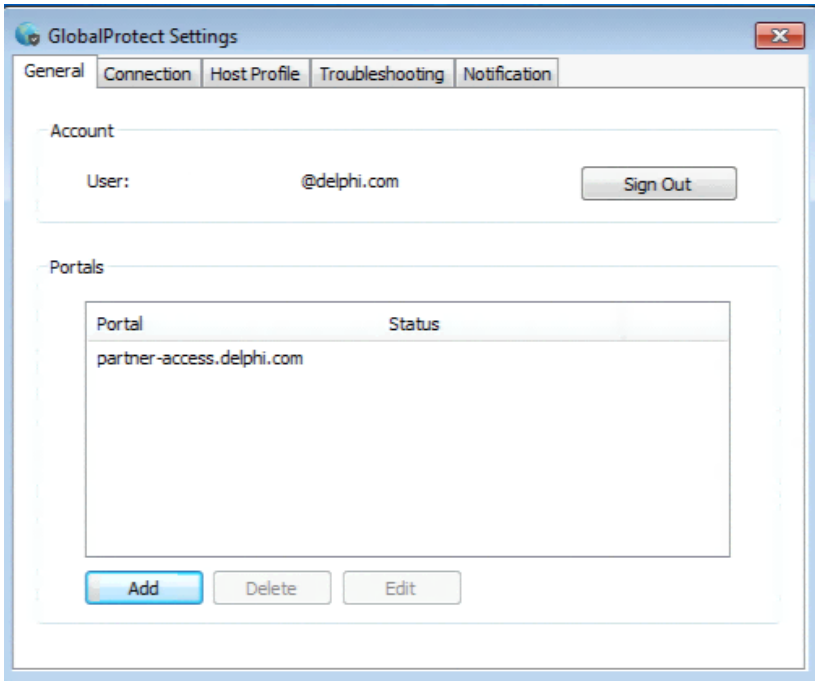
b. View the information about your network connection.

After you launch the app, click the settings icon ( ) on the status panel to open the settings menu.



Select **Settings** to open the GlobalProtect Settings panel:

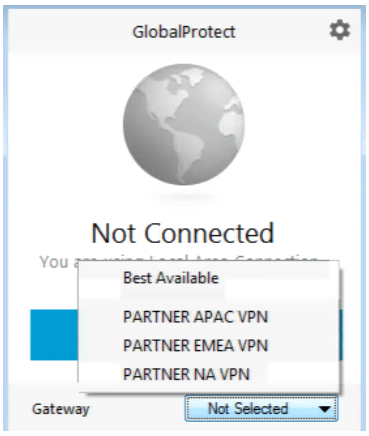
c. GlobalProtect Settings panel will be displayed:



In the "**General**" tab, the username and portal(s) associated with the GlobalProtect account are displayed.

3.3. Connect to a regional SSL VPN gateway

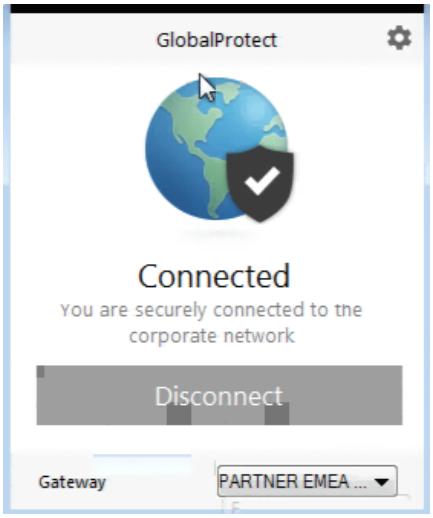
a. Manually select one of the gateways available from the list:



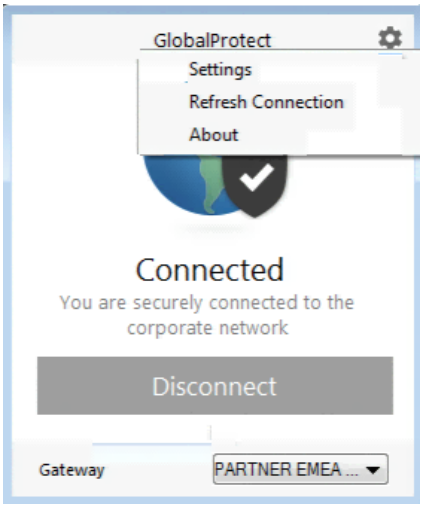
b. If you are in EMEA, please select PARTNER EMEA VPN.

If the client will redirect you to Azure MFA for authentication, complete the authentication process similar to Section 2, Step 2 & 3.

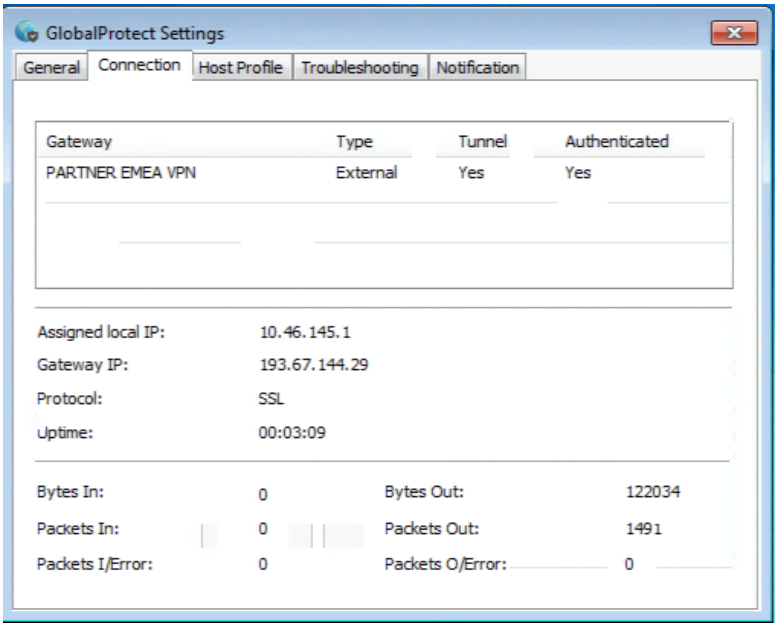
c. Once successfully connected to one of the gateways you should see the following (PARTNER EMEA VPN for example):



d. Check the connection details in the GlobalProtect Settings panel as described in Section 3.2.b



e. Connection details are displayed in the "**Connection**" Tab



3.4. (Optional) Log in using a new password

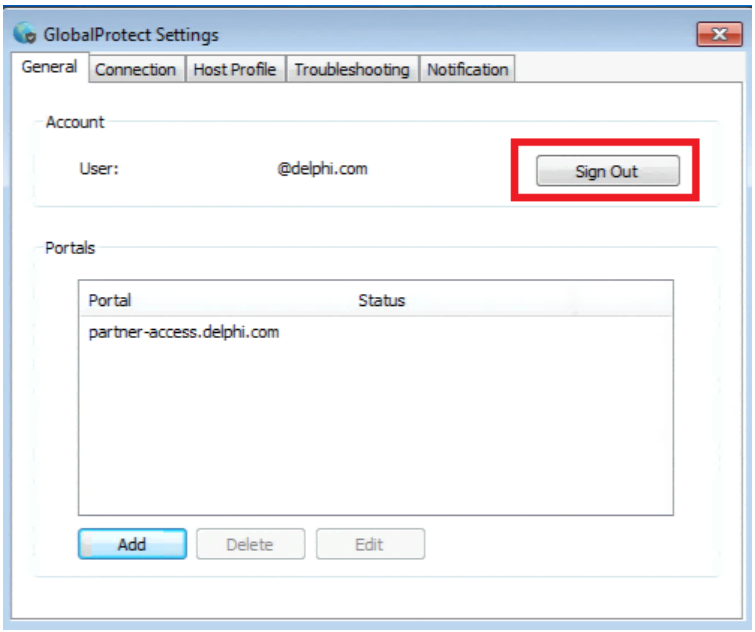
GlobalProtect agent is configured to Save User Credentials. If your password changes, you must log in to GlobalProtect using your new password.

a. Launch the GlobalProtect agent by clicking the system tray icon.

b. Click the settings icon (⚙) to open the settings menu.

c. Select **Settings** to open the GlobalProtect Settings panel.

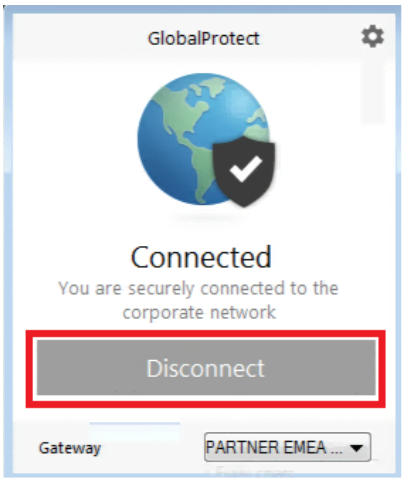
d. On the **General** tab of the GlobalProtect Settings panel click **Sign Out** to clear your current credentials.



e. After you clear your user credentials, GlobalProtect will prompt you to reconnect using the new credentials.

3.5. Disconnect From GlobalProtect agent

GlobalProtect is configured with “Manually Only” connect method, so to disconnect you can click on “Disconnect” after launching the GlobalProtect App interface from system tray icon:



After disconnecting from the GlobalProtect agent, you can connect to the Internet using unsecured communication (without a VPN) or connect to your corporate network.