**Using GlobalProtect**

GlobalProtect is the future remote access VPN solution for Lumen Technologies. GlobalProtect provides Employees a secure connection to the Lumen corporate network while working remotely. This document will demonstrate how to login to GlobalProtect as well as provide a self service steps on how to troubleshoot common situations.

We will also demonstrate how to use the Start Before Logon Procedure for new employees or those employees who receive a replacement workstation and are required to login for the first time remotely.

Optionally skip to each section as desired:

[Connect using GlobalProtect](#_How_to_Use)

[Using Microsoft Authenticator with GlobalProtect](#_Microsoft_Authenticator)

[Using MobilePass+ with GlobalProtect](#_Mobile_Pass+)

[Successfully Authenticated](#_Once_successfully_authenticated)

[Resolve Connection or Authentication Issues](#_The_following_will)

[How To Contact the Help Desk](#_Lumen_Help_Desk)

[How to use Start Before Logon with GlobalProtect](#_The_following_will_1)

[Important Things to Know for GlobalProtect](#_Important_Things_to)

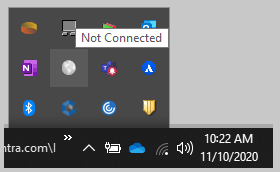
# **How to Use GlobalProtect**

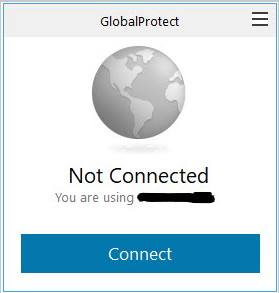


Every workstation should have GlobalProtect already installed, if not, please follow the instructions located at <https://mfa.centurylink.com/Documents/WrittenInstructions/GlobalProtect.docx>

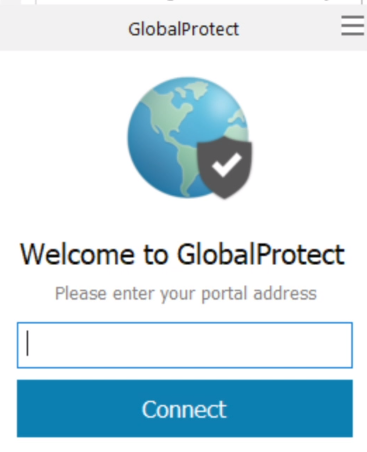
GlobalProtect uses Microsoft Authenticator or Mobile Pass+ tokens to securely authenticate users. Instructions on how to setup Microsoft Authenticator and Mobile Pass+ can be found on the MFA Website located at <https://mfa.centurylink.com>.

Once the authentication method is determined, locate the GlobalProtect app within the taskbar and click connect





If the option to enter a portal address is presented, please enter the respective address, then click connect:



1. roc.centurylink.com - North America (CTL Network)
2. roc-portal-idc2.centurylink.com - North America (fLVL3 Network)
3. roc-emea.centurylink.com - EMEA
4. roc-apac.centurylink.com - APAC
5. roc-latam.centurylink.com - LATAM

Option 1 is suggested for those who typically work out of a former CenturyLink location or may have formally used the Cisco AnyConnect VPN client

Option 2 is suggested for those who typically work out of a former Level3 location or may have formally used the Checkpoint VPN Client

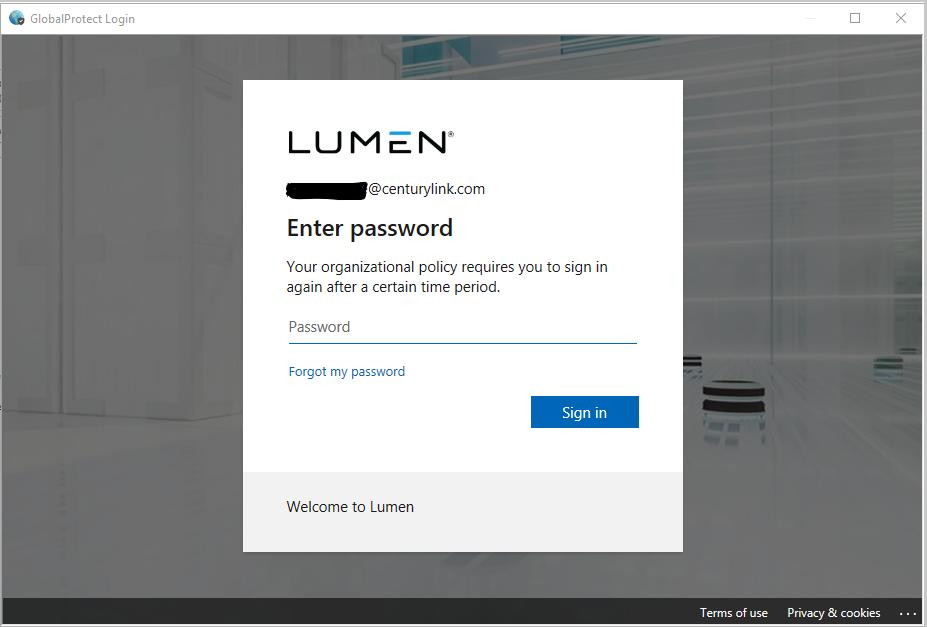
Option 3 is suggested for those who are located within the EMEA region

Option 4 is suggested for those who are located within the APAC region

Option 5 is suggested for those who are located within the LATAM region

Generally speaking, any of the portals are available for use, however, for the best user experience, it is recommended to connect to most appropriate portal listed for the individual user situation

Once connect is clicked, a prompt for user credentials will be displayed, enter email and password then click sign in.

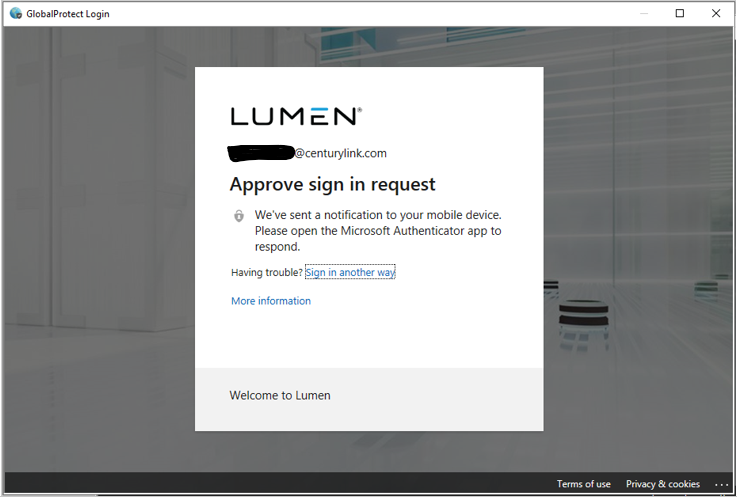


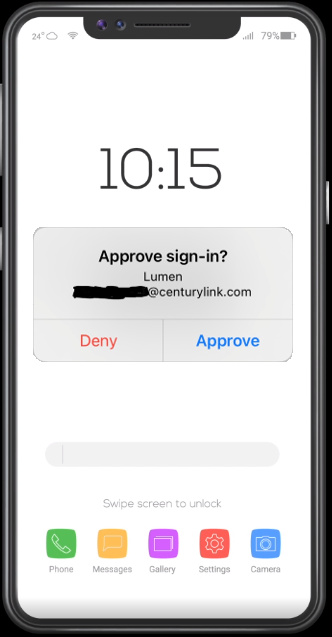
# **Microsoft Authenticator**

The following screens will demonstrate the steps for Microsoft Authenticator:



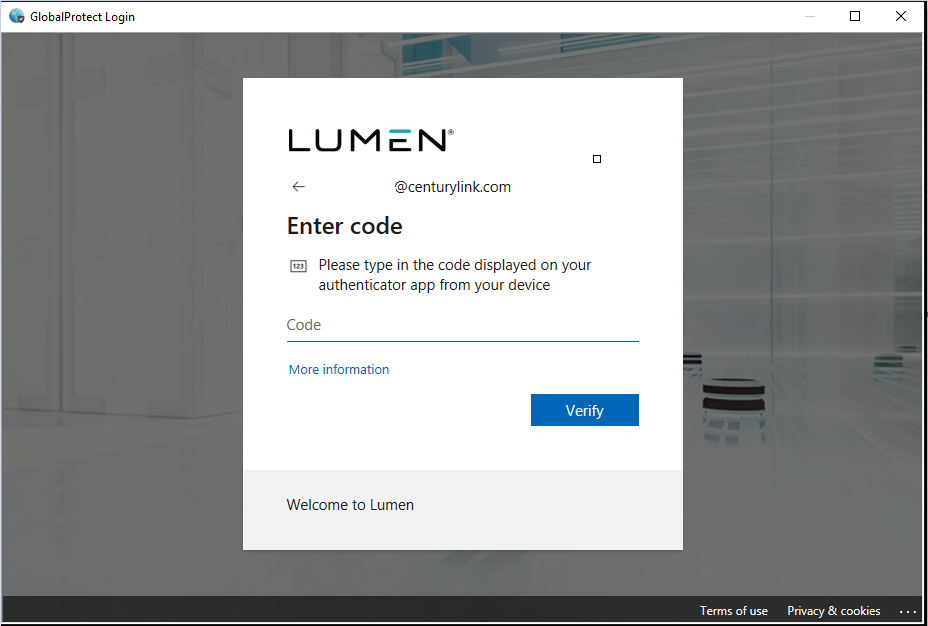
When Microsoft Authenticator app is setup to approve requests, the screen below will display until the individual approves the request on the phone.

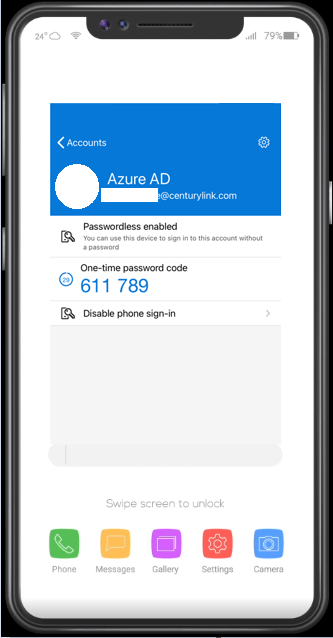




\*\*This is not a representation of what all phones will look like, it is provided as an example only

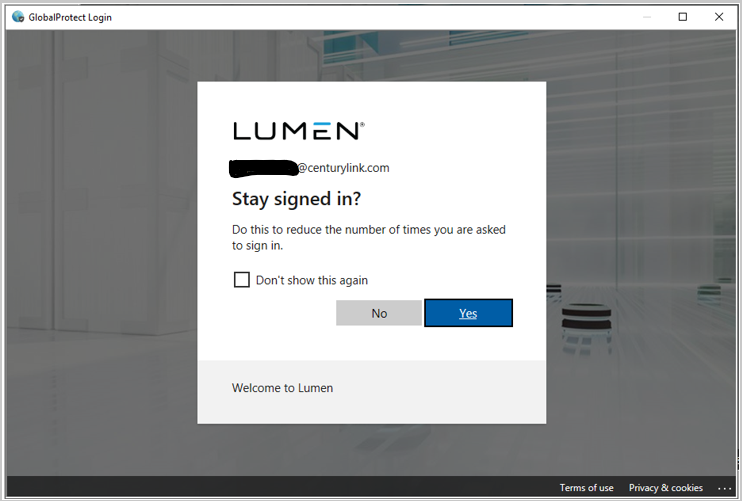
When Microsoft Authenticator app is setup to use a passcode, the screen below will display until the user enters the code displayed within the Microsoft Authenticator app on the phone. Next, Click Verify on the workstation screen.





\*\*This is not a representation of what all phones will look like, it is provided as an example only

Select yes or no, keep in mind, this message will display in the future regardless of which option is selected.

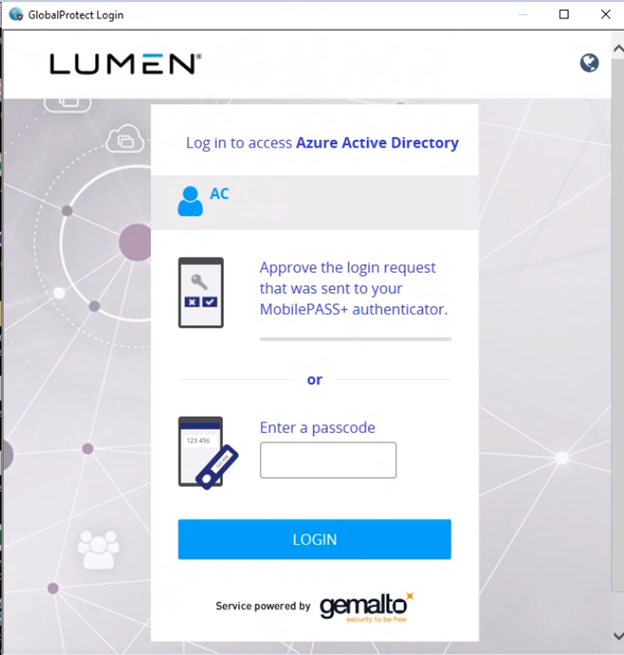


# **Mobile Pass+**

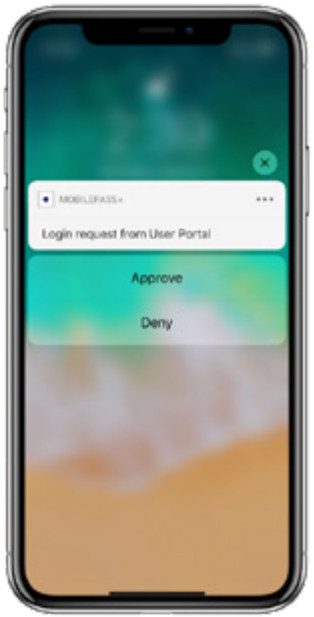
The following screens will demonstrate the steps for Mobile Pass+:



When the Mobile Pass+ app is setup to approve requests, the screen below will display until the individual approves the request on the phone.

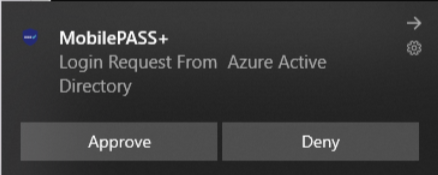


Phone App Notification:

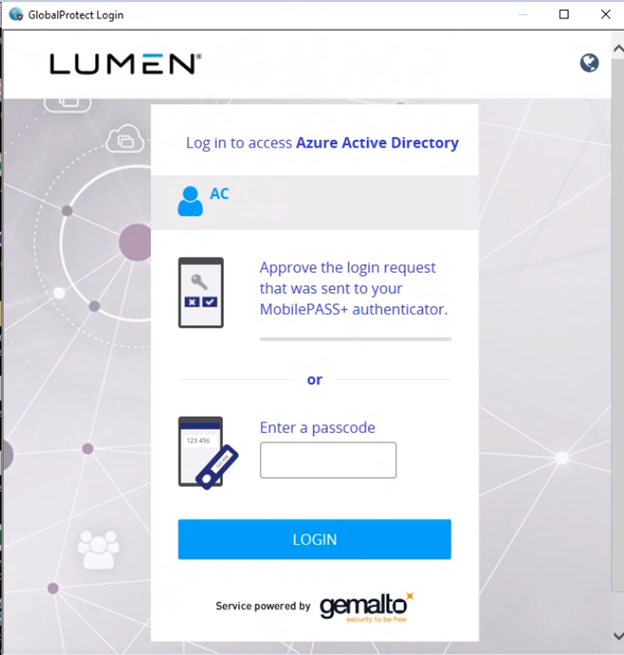


\*\*This is not a representation of what all phones will look like, it is provided as an example only

Workstation APP Notification



When MobilePass+ app is setup to use a passcode, the screen below will display until the user enters the passcode displayed within the MobilePass+ app on the phone. Next, Click Login on the workstation screen.

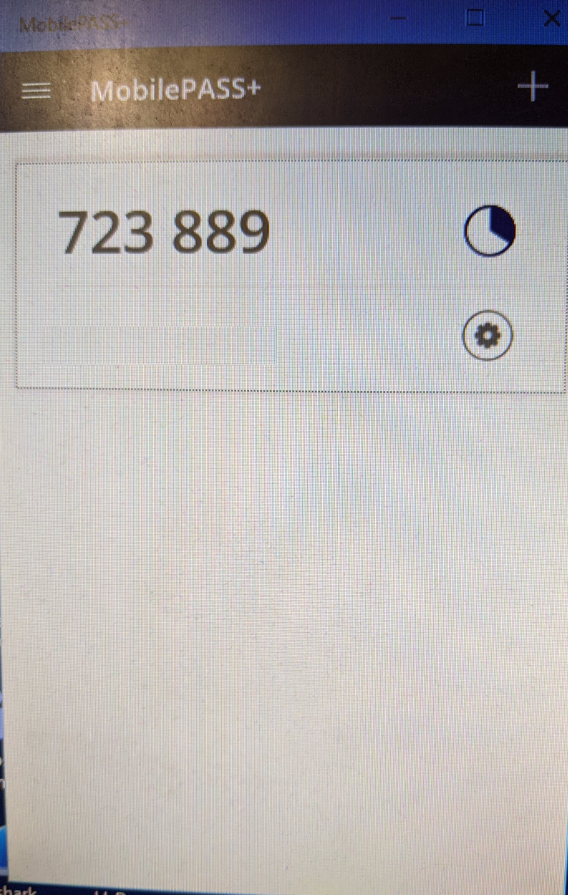


Phone APP Display



\*\*This is not a representation of what all phones will look like, it is provided as an example only

Workstation App Display:

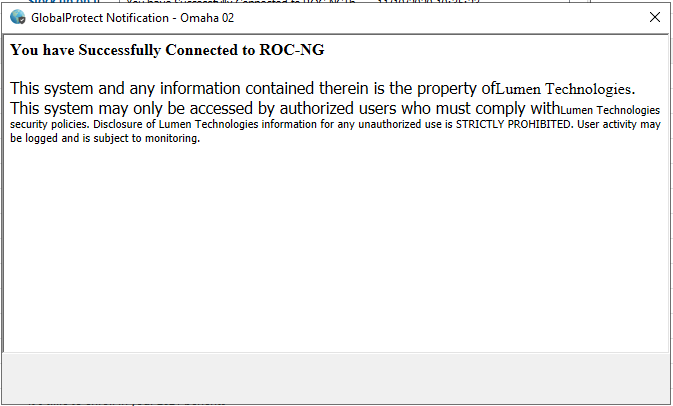


# Once successfully authenticated with email, password and token, two banners are expected.

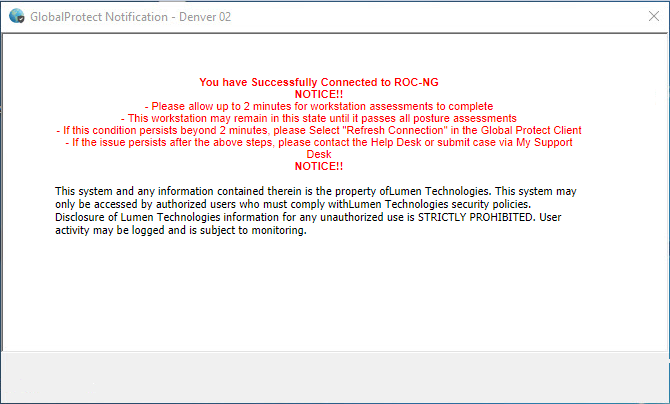
The first banner displays once initially connected. In the background, the GlobalProtect client is receiving any new configurations as well as gathering details about the PC and forwarding to the VPN system to ensure the workstation passes the required posture assessments to establish a full connection to corporate network.



The second banner displays once all posture assessments are complete, as explained in the initial banner, this process can take up to two minutes to complete.

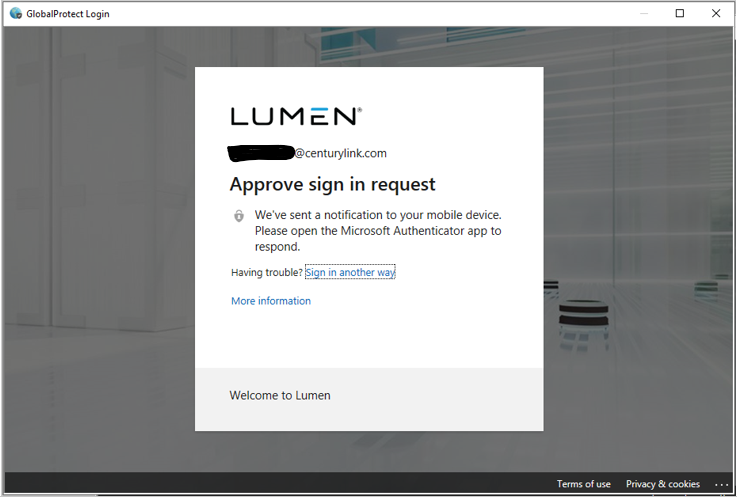


If this banner is received, the posture assessment did not pass or complete and the workstation requires attention.

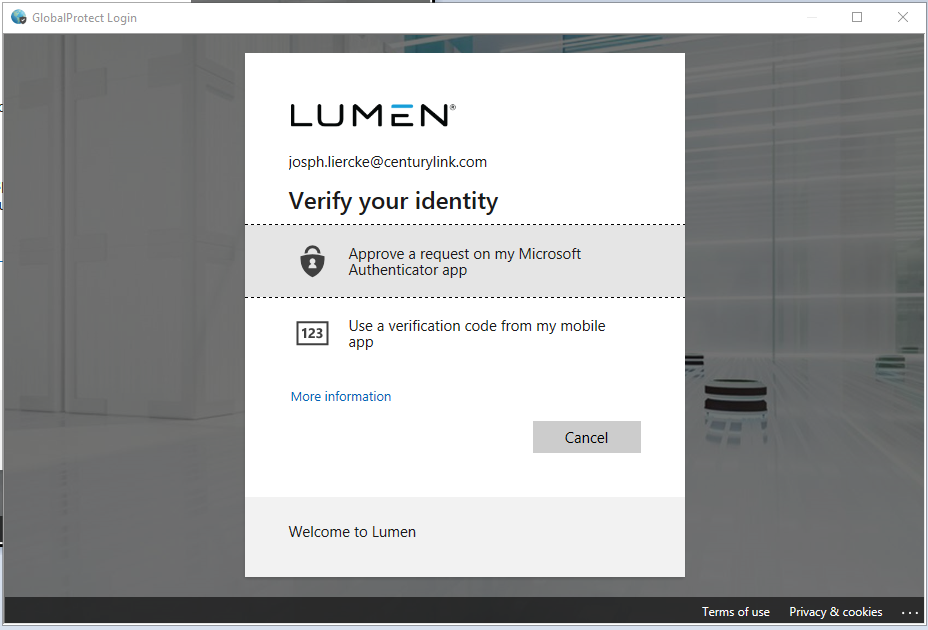


# The following will demonstrate remediation steps a user can take prior to contacting the Help Desk.

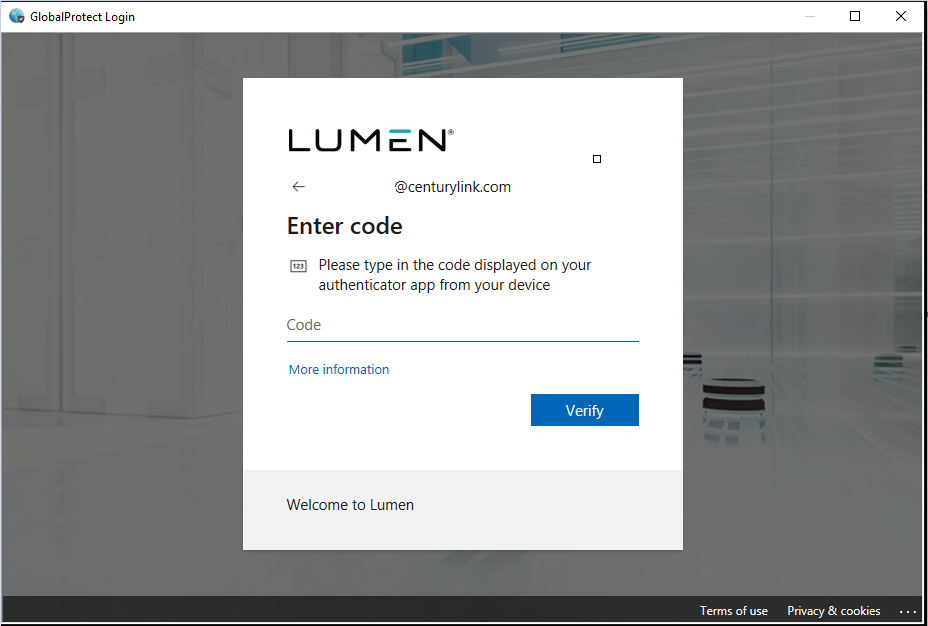
There are times where a delay of the approval message to the Microsoft Authenticator phone app may occur. If this happens, a new code can be sent or use a code displayed within the app instead. To do this, click on Sign in another way

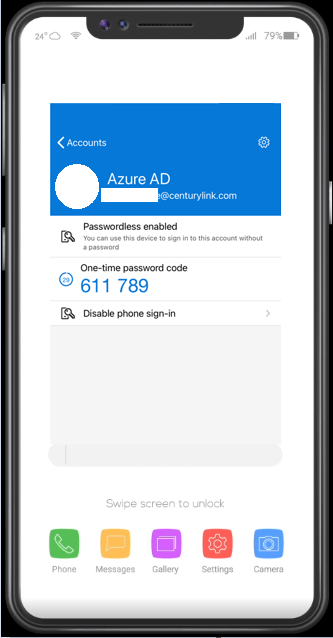


Then choose the desired option. If the approval method has been attempted multiple times without success, using the verification code option is recommended



Then open the app on the phone, select the proper account, type the one-time password code displayed within the app and click verify

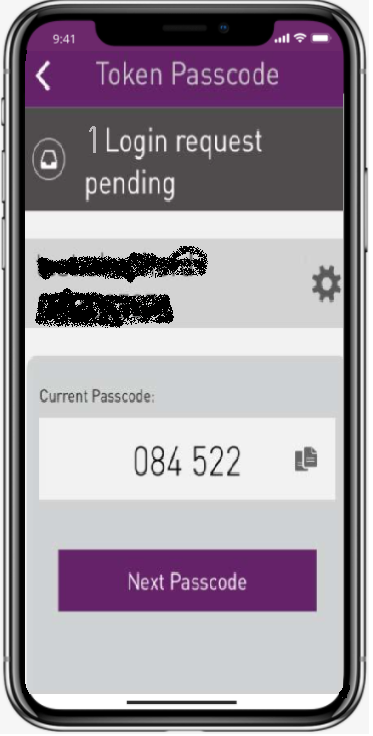


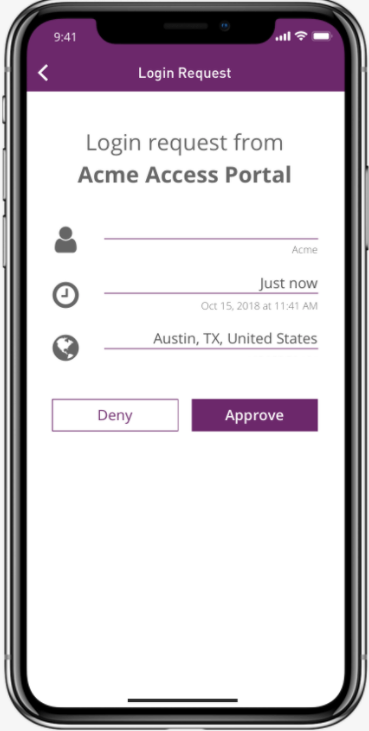


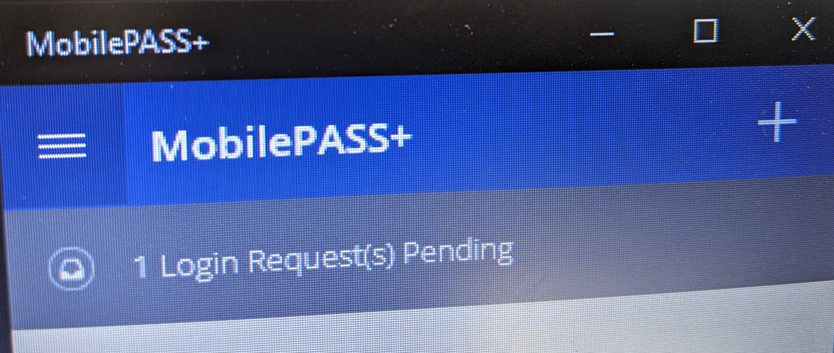
\*\*This is not a representation of what all phones will look like, it is provided as an example only

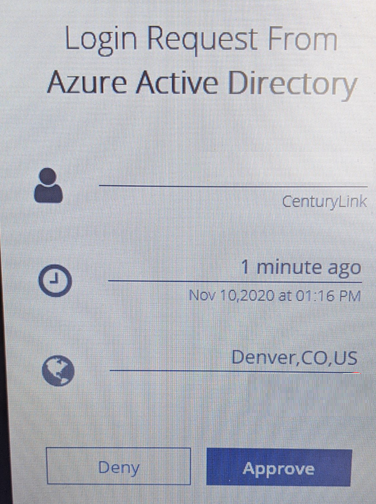
Similarly, MobilePass+ App might experience these delays, when this occurs, there will be Pending requests within the App. Click on the pending request and Approve

Phone App Display

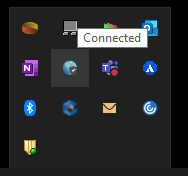


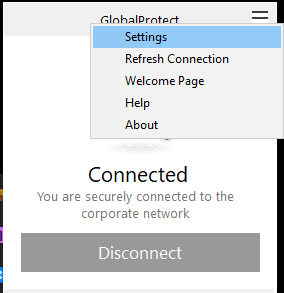


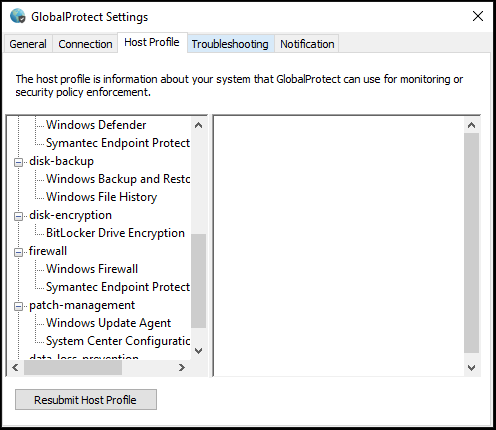
PC App Display:



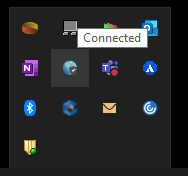
Once authenticated and the first banner is displayed, if longer than two minutes without receiving the second banner OR full network access is not established, please try to remediate these issues by going to the GlobalProtect Settings and resubmitting the host profile information.

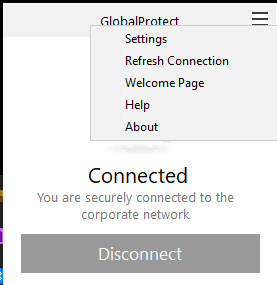






After completing this step and the second banner does not display OR full network access is not established, please attempt to refresh the connection within the GlobalProtect Application.

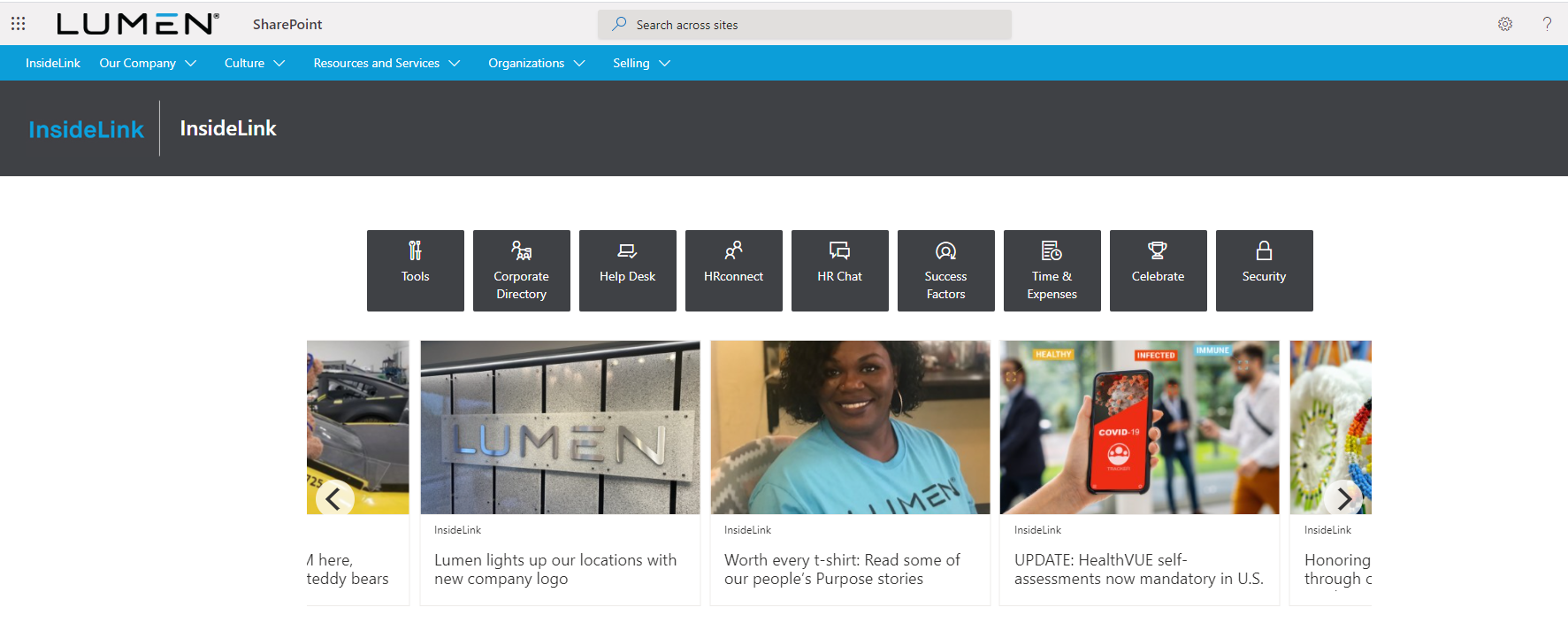




After completing this step and the second banner does not display OR full network access is not established, it is recommended to contact the Help Desk.

# Lumen Help Desk Contact information

The Help Desk information can be located on Inside Link By Navigating to <https://centurylink.sharepoint.com/> within your browser and Selecting Help Desk



Or by navigating to <https://centurylink.sharepoint.com/sites/ILSystems/SitePages/Help-Desk.aspx> within your browser.

Here is a list of Numbers for the Lumen Help Desk:

North America: 877-828-4357

EMEA: +441256732999

LATAM Española: +541151706410

LATAM Portuguese +551139572040

Singapore: +6565055215

All other Int'l locations: 1-303-738-2001

The My Support Desk Link is displayed below:

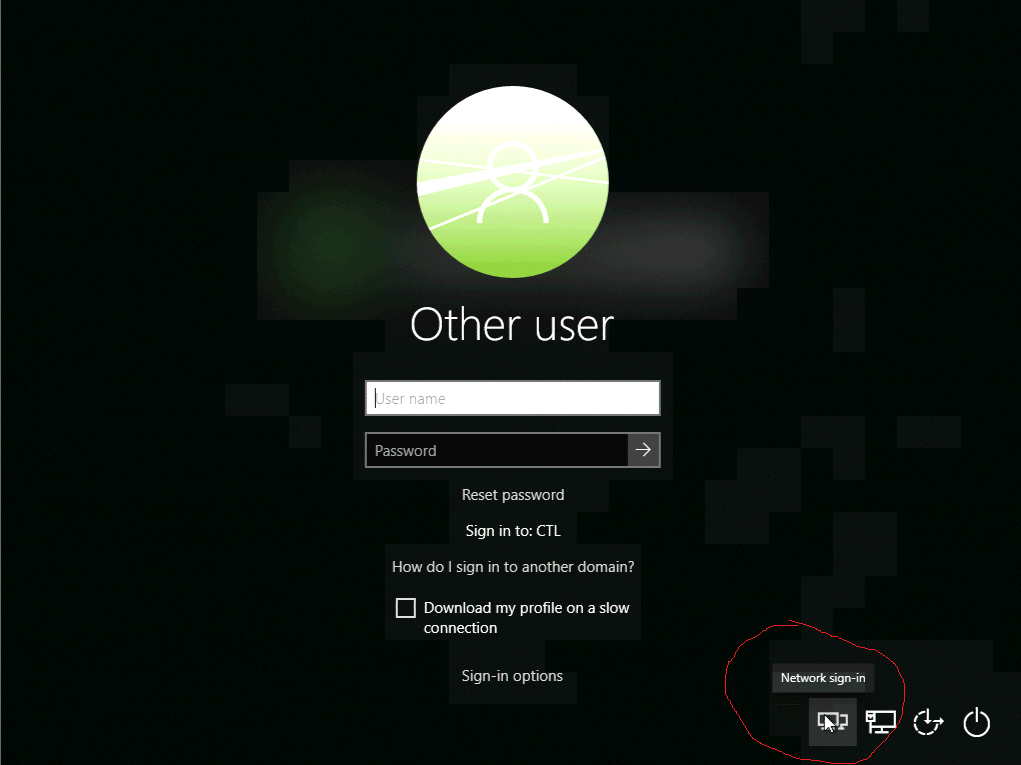
<https://mysupportdesk.service-now.com/msd>

# The following will demonstrate how to use the Start Before Logon Functionality with GlobalProtect

**\*\*\*\*\* KEEP IN MIND, THIS REQUIRES A TOKEN TO BE AVAILABLE ON A CELL PHONE. IF THE TOKEN IS ON THE PC, THIS FEATURE WILL NOT WORK UNLESS ACCESS TO AN ALTERNATE CORPORATE LAPTOP IS AVAILABLE WITH THE TOKEN APPLICATION STILL INSTALLED AND TOKEN AVAILABLE\*\*\*\*\***

At Windows Screen, press ctrl+alt+del simultaneously

At the bottom of your screen Click Network Sign In Button



If prompted for Portal, use the proper portal below, click the arrow to connect and enter the workstation user credentials and token (email + password, then token)

1. roc.centurylink.com - North America (CTL Network)
2. roc-portal-idc2.centurylink.com - North America (fLVL3 Network)
3. roc-emea.centurylink.com - EMEA
4. roc-apac.centurylink.com - APAC
5. roc-latam.centurylink.com - LATAM

Option 1 is suggested for those who typically work out of a former CenturyLink location or may have formally used the Cisco AnyConnect VPN client

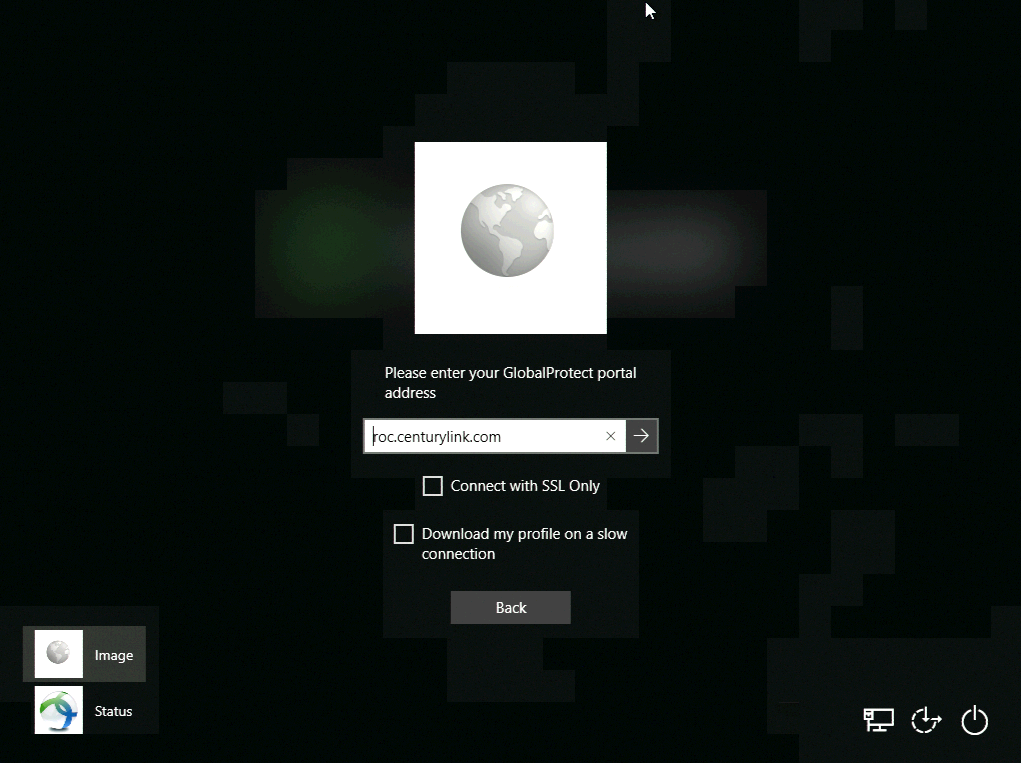
Option 2 is suggested for those who typically work out of a former Level3 location or may have formally used the Checkpoint VPN Client

Option 3 is suggested for those who are located within the EMEA region

Option 4 is suggested for those who are located within the APAC region

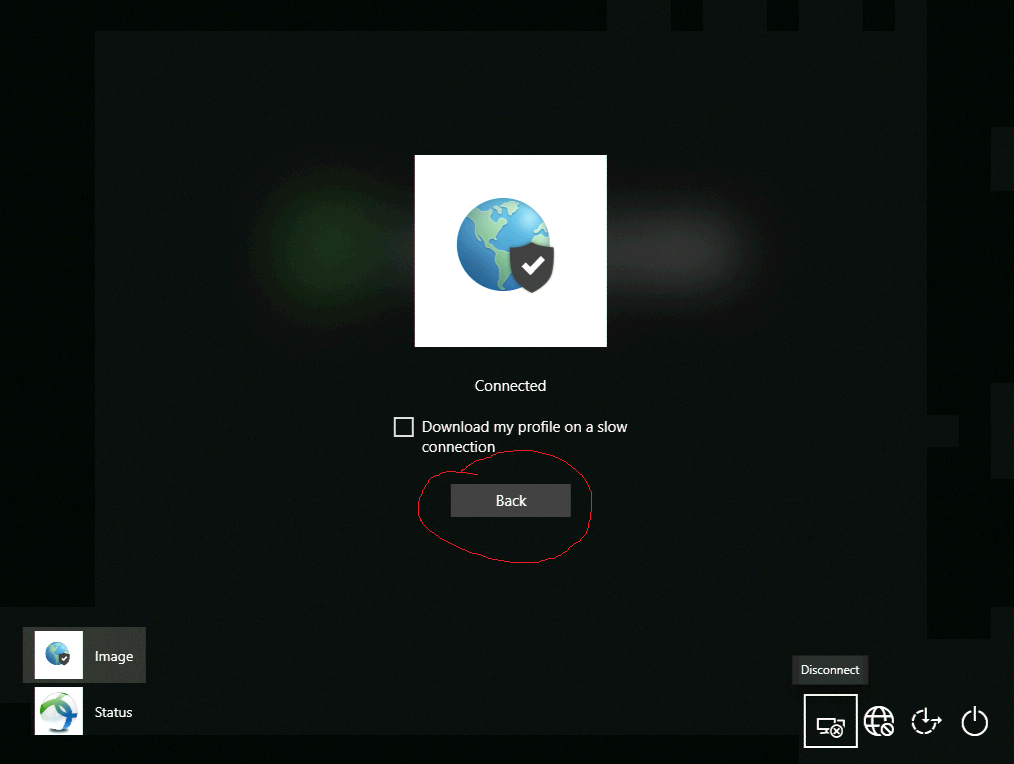
Option 5 is suggested for those who are located within the LATAM region

Generally speaking, you are able to connect to any of the portals, however, for the best user experience, it is highly recommended to connect to the portal designated for the various regions or network locations.

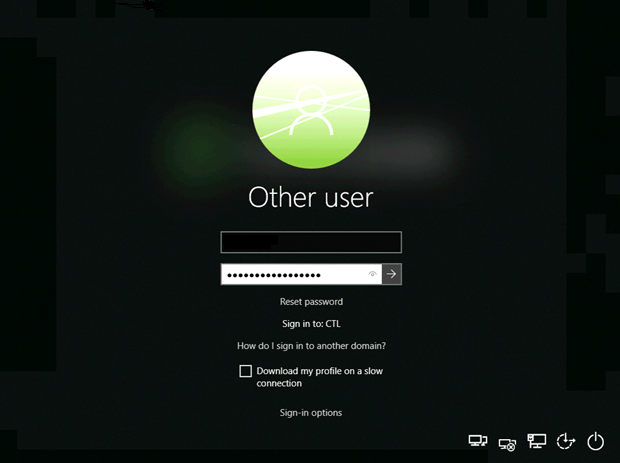


If there are issues connecting, try the “Connect with SSL Only” option, may require reboot to check the box after a failed attempt

Once connected, the Screen below will be displayed, Click Back



Now Login using with workstation user credentials (username + password)



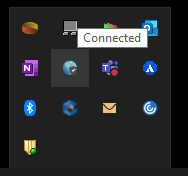
# Important Things to Know:

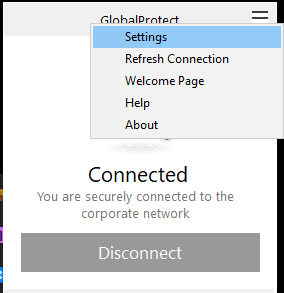


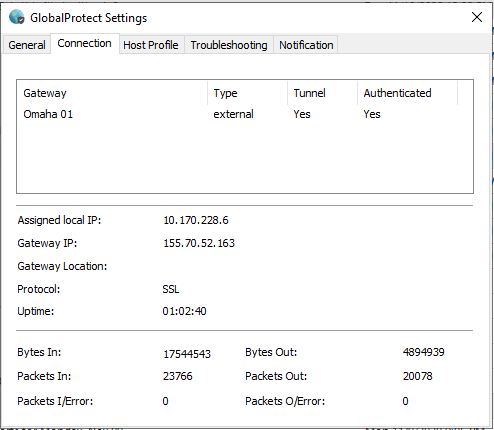
To change the Microsoft Authenticator App preferences (Approve on phone or Use Code), go to <https://mysignins.microsoft.com/security-info> and change the Default sign-in method



To identify which Gateway the PC is connected to, Navigate to the Settings of The GlobalProtect application. Similarly, this can identify the IP address assigned to the PC for the GlobalProtect session.

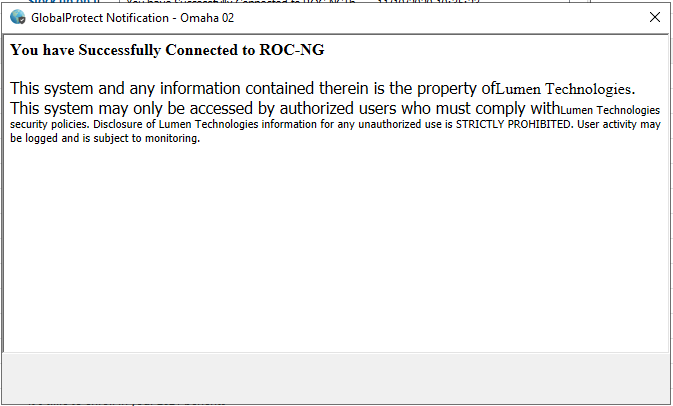




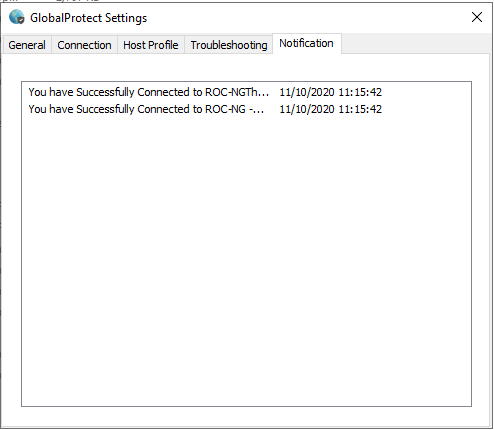


Similarly, the IP address assigned by GlobalProtect is displayed

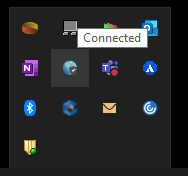
The second banner also displays the connected Gateway

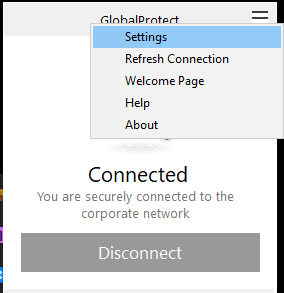


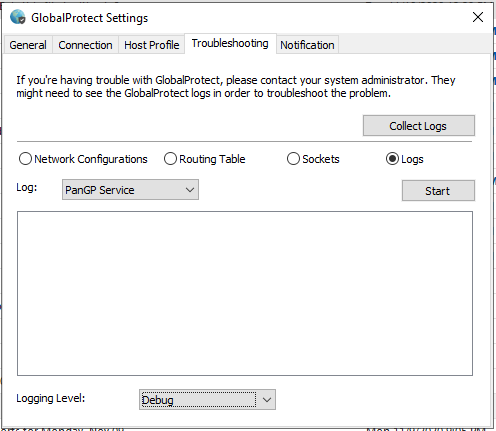
To view which banner(s) have been received by GlobalProtect once they are closed, they can be located within the GlobalProtect Settings, under the Notification Tab (Double click each notification to view to view)



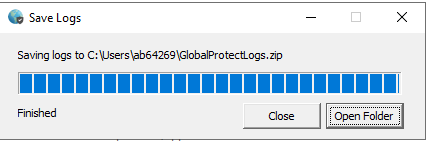
When requested, the logs for GlobalProtect can be gathered from the client Settings, under the Troubleshooting Tab then clicking Collect Logs.







Once the file is generated, Click Open Folder then email the file named GlobalProtectLogs.zip to the requesting support technician



\*Note, the file is saved under C:\Users\USERNAME\