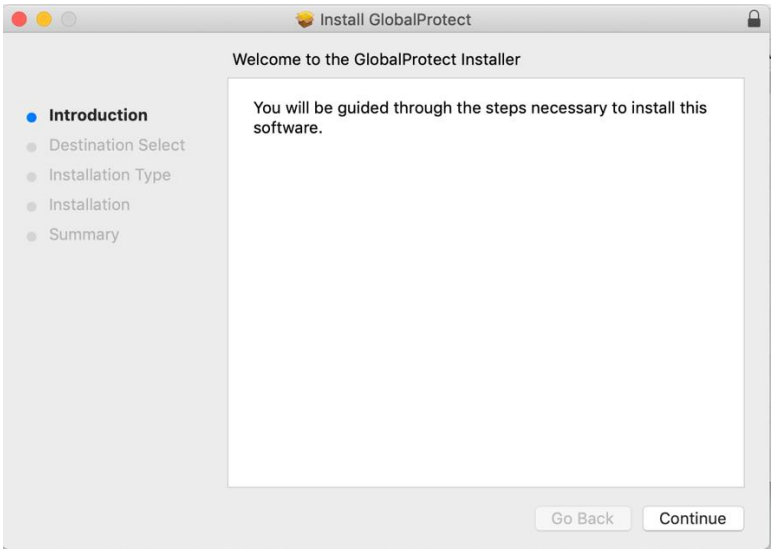
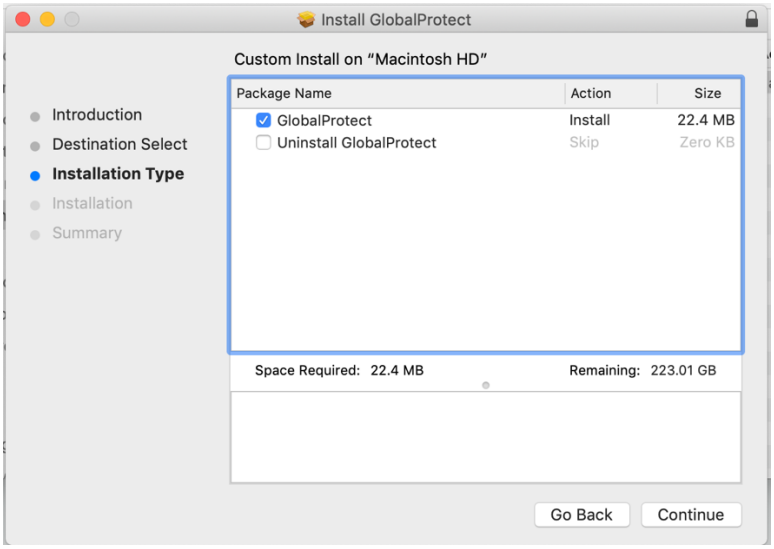
Installation and Configuration of Global Protect on Mac OSx

Installation of GlobalProtect Client for Mac:

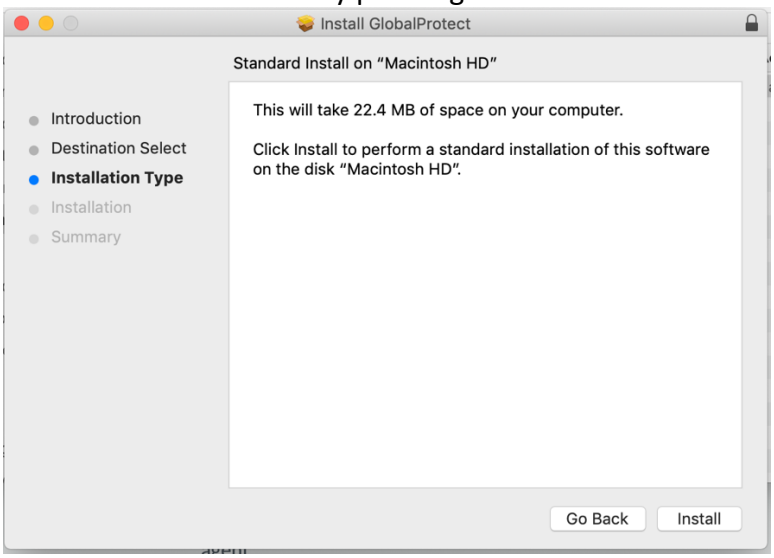
1. Log into the GlobalProtect Portal, download and run the installer for Mac OSx.
2. On the Introduction Screen, press “Continue”.



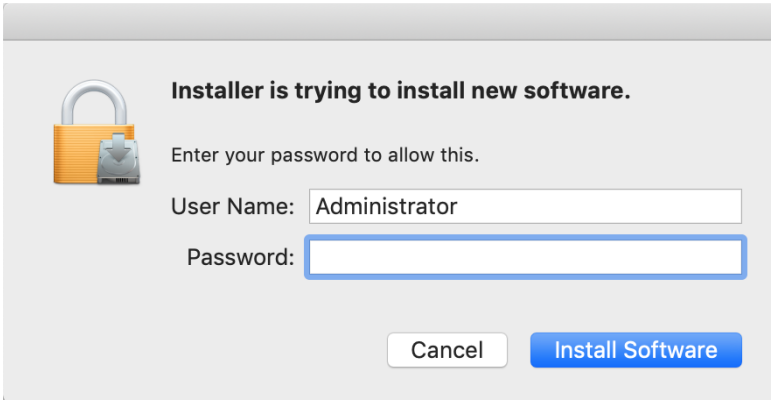
3. On the Destination Select screen choose the default by pressing “Continue”
4. On the Installation Type screen, ensure GlobalProtect Package Name is selected with the checkbox. Press “Continue”.



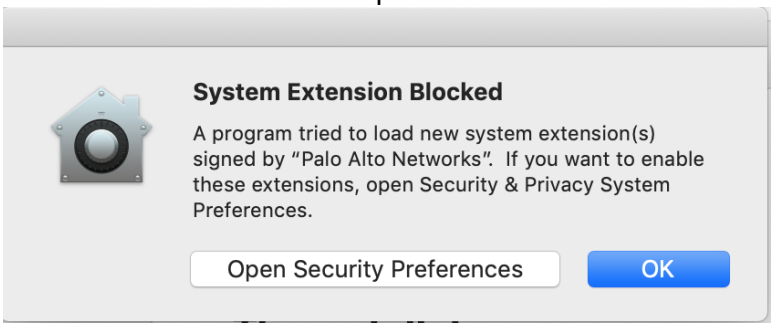
5. Confirm the Installation by pressing “Install”.



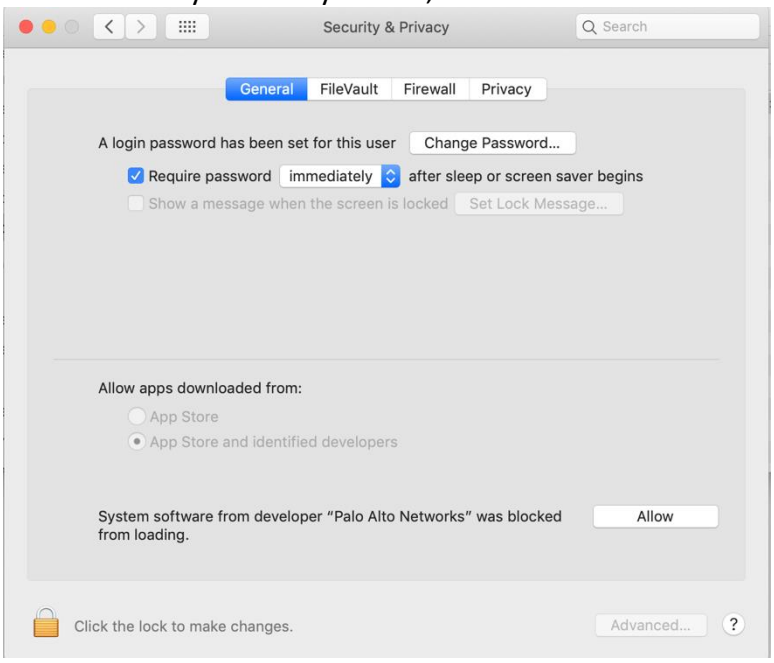
6. Enter the computer Administrator’s name and password to begin installation and press “Install Software”.



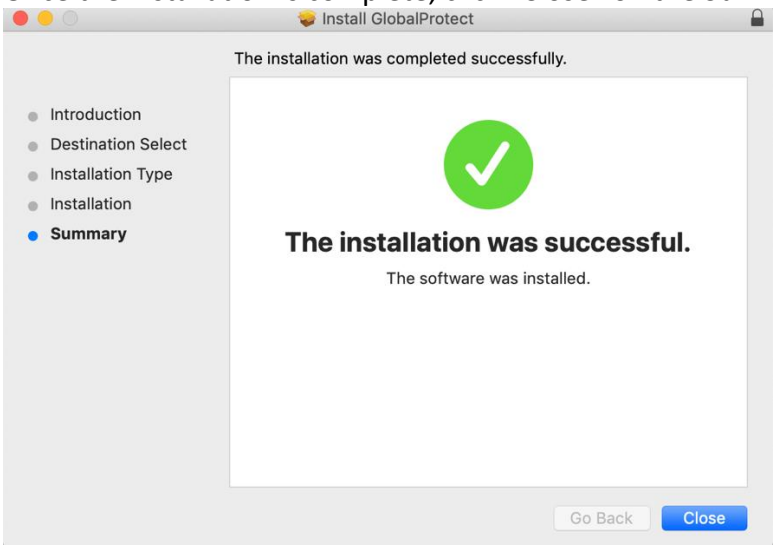
7. System Extension Blocked: Click on “Open Security Preferences” to allow the GlobalProtect installation to proceed.



8. On the Security & Privacy screen, Press “Allow” to continue the installation.

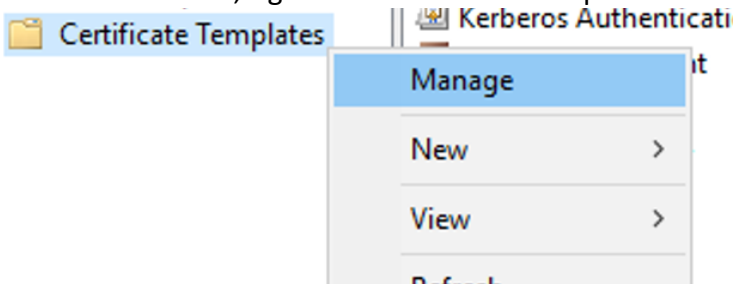


9. Once the installation is complete, click “Close” on the Summary screen.

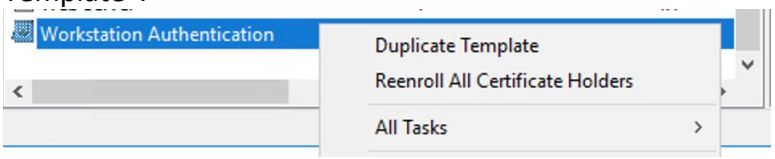


Certificate Configuration for GlobalProtect

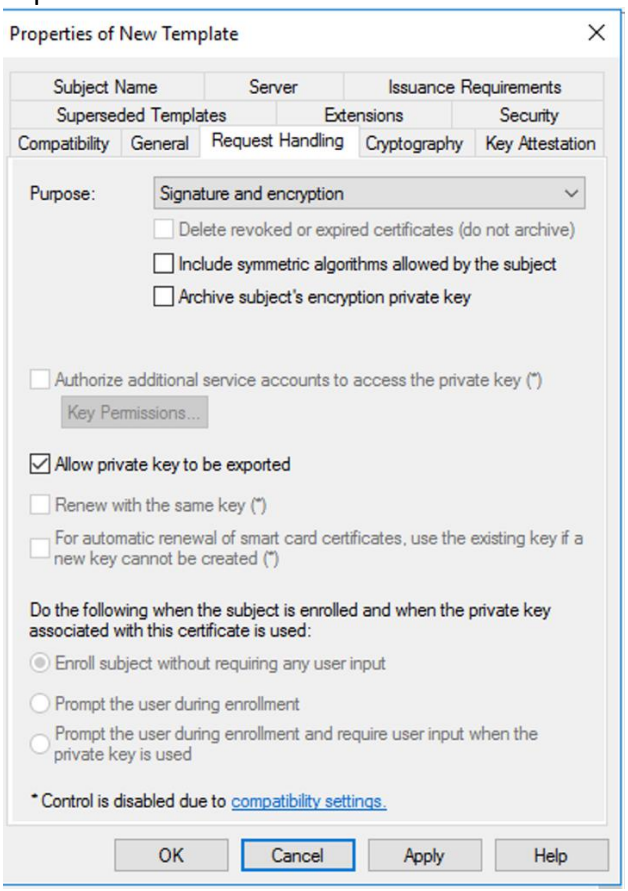
1. Configure the Certificate Template
    a. From the CA console, right-click Certificate Templates and select “Manage”



    b. Right-click the “Workstation Authentication” template, then select “Duplicate Template”.

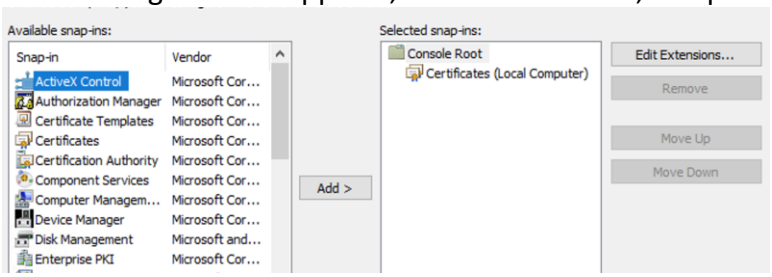


    c. On the “General” Tab, enter a template name that is recognizable.
    d. On the “Request Handling” tab, make sure the “Allow private key to be exported” is selected.

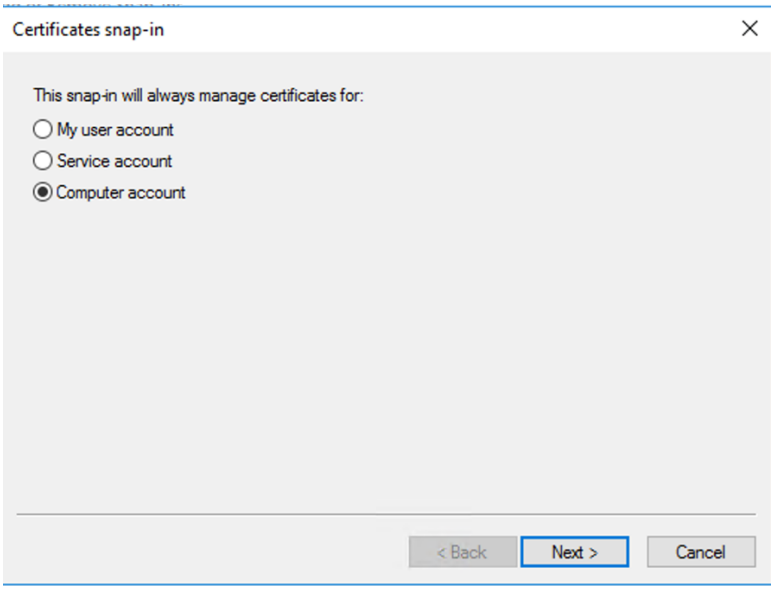


e. Click the “Subject Name” tab and select “Supply in the request”. Press “OK” in the warning dialog to acknowledge the security risk.
f. Click the “Security” tab and remove the “Enroll” permission from the security groups **Domain Admins** and **Enterprise Admins**.
g. Click “Add”. In the “Select Users, Computers, Service Accounts, or Groups” dialog box, click “Object Types”, then “Computers”, then click “OK”. Specify the name of a Windows computer that will request the certificate on behalf of the Mac Computers (it can be the CA itself), click “Check Name” to verify, finally click “OK”.
h. Select Enroll permission for this computer. **DO NOT CLEAR READ PERMISSIONS**
i. Click “OK” and close the **Certificate Templates Console**.

2. Issue Certificate to Mac Workstation
   a. From the computer that was configured in step 1 above, click “Start”, click “Run”, type *mmc.exe*.
   b. Click “File”, then “Add/Remove Snap-In”
   c. In the dialog box that appears, select Certificates, and press “Add”

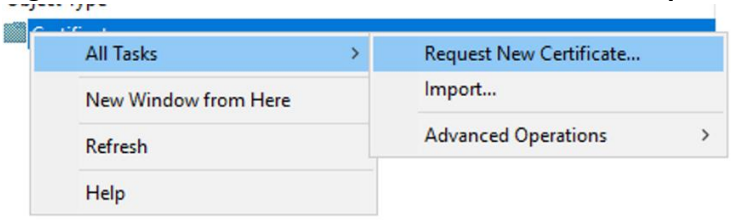


   d. In the “Certificate Snap-In” dialog box, select **Computer Account** and press “Next”



   e. In the “Select Computer” dialog box, ensure **Local Computer** is selected and press “Finish”.
   f. Click “OK”

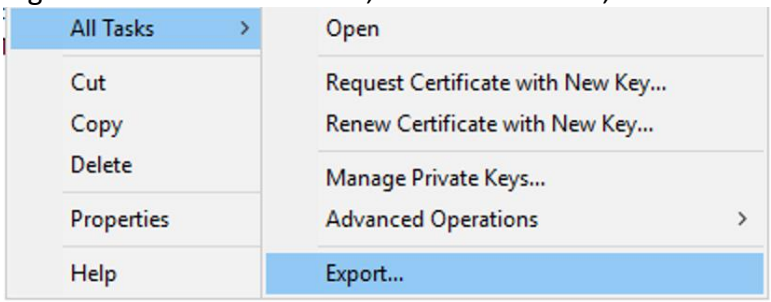
g. Expand “Certificates (Local Computer)”, then click “Personal”.
h. Right-click **Certificates;** click **All Tasks**; and click **Request New Certificate**.



i. On the **Before You Begin** screen, press “Next”
j. Press “Next” on the **Certificate Enrollment** Screen
k. Select the Certificate template created in the previous steps.
    i. Click the hyperlink under the Certificate

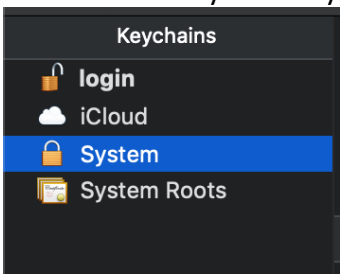
l. On the **Certificate Properties** dialog box, enter the value in the Subject name box. Use the FQDN (hostname.domain.com).
m. Press the “Add” button and press “OK”.
n. Press the “Enroll” button.

3. Export the needed certificates
    a. Both the newly added certificate and root certificates need to be exported.
    b. Right-click on the certificate, select “All Tasks”, then click “Export”.

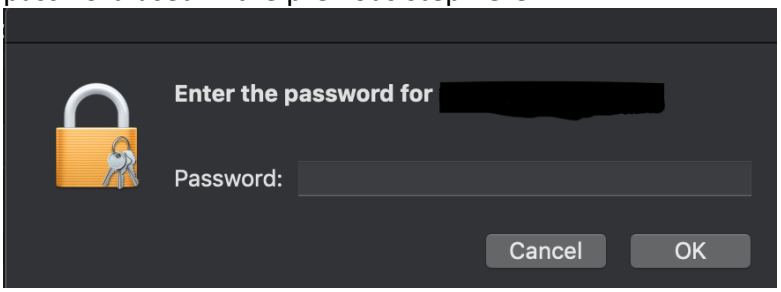


    c. On the Export Certificate Wizard Welcome page, press “Next”
    d. Select “Yes, export the private key” and press “Next”.
    e. On the **Export File Format** screen, make sure the file format is “PKCS #12 (.PFX)” and press “Next”.
    f. On the **Security** screen, give the file a secure password. This will be used when importing the certificate into the Mac.
    g. On the **File to Export** page, give the certificate a file name and press “Next”.
    h. Finally, click “Finish” to close the wizard, and “OK” in any dialog boxes that appear.
    i. Copy the certificate(s) to the Mac.
4. Import the certificates into the System Keychain
    a. As an administrator, open the KeyChain application on the Mac.
        i. Press Command + Space bar and type Keychain

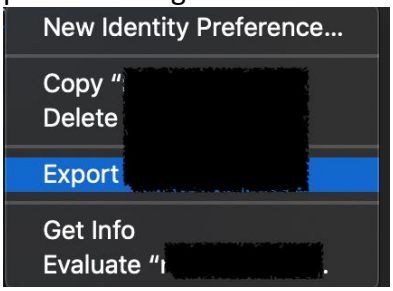
b. Browse to the System keychain.



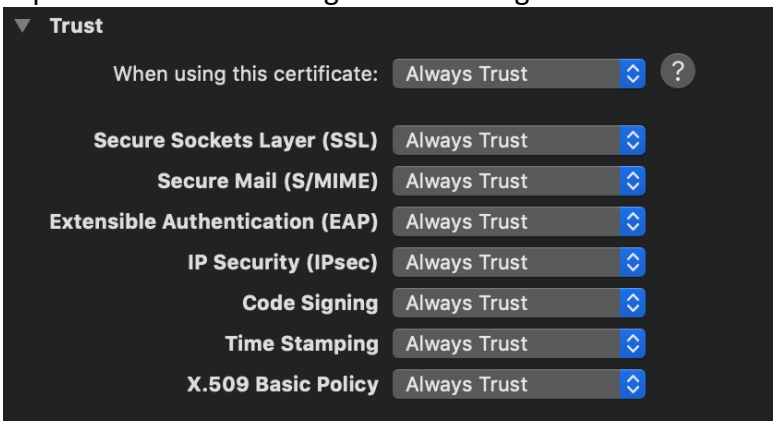
c. Go to File -> Import Items
d. Select the .pfx file from the previous step and press “Open”
e. On the Keychain Access popup, allow access to modify the System keychain by entering the administrator’s password.
f. The next pop up window will be the password for the certificate. Enter the password used in the previous step here.



g. Once the certificate(s) are loaded ensure they are trusted by all users and processes. Right-click on the certificate and select “Get Info”.

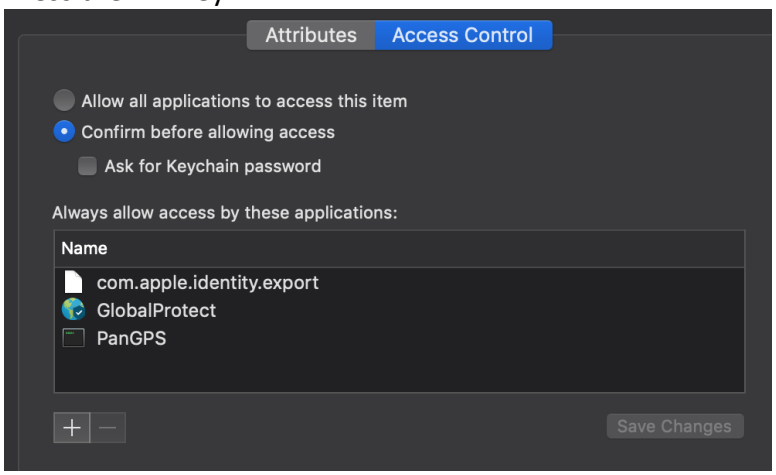


h. Expand “Trust” and change “When using this certificate:” to “Always Trust”.

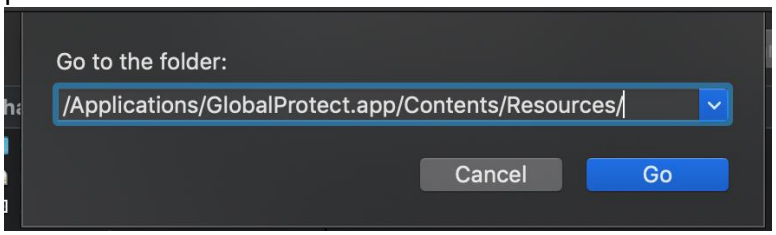


5. Ensure GlobalProtect has access
    a. Expand the computer certificate and right-click on the private key.

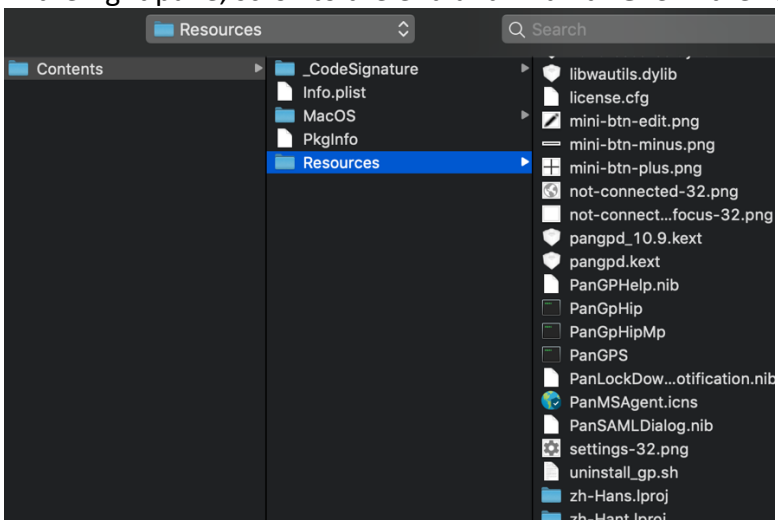
    b. Click “Get Info”
    c. Go to the “Access Control” tab.
    d. Press the “+” key.



    e. On the Pop up, press “Command + Shift + G” to enter the path directly.
    f. Enter the path of */Applications/GlobalProtect.app/Contents/Resources* and press “Go”.



    g. In the right pane, scroll to the end and find **PanGPS** in the list of resources.



    h. Click “Save Changes” and enter the Administrator’s password in the popup.