

Stony Brook Medicine GlobalProtect VPN Initial Setup & Use Instructions

V23-12-11

Before you begin the GlobalProtect VPN client installation, please read these requirements!

1) You must have already set up Microsoft MFA (Multi-Factor Authentication). If you have not, please visit: [MFA Setup Instructions](#)

2) Make sure your computer complies with the requirements below:

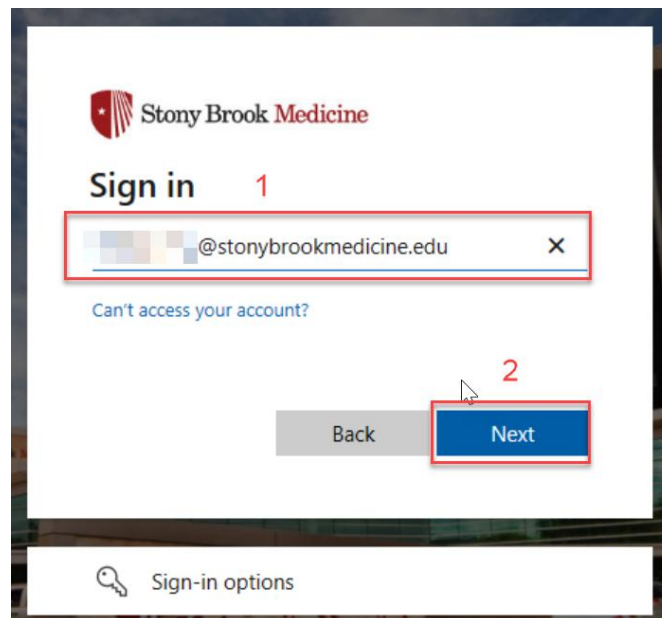
- Operating System: Windows 10 or above, MacOS 11 or above.
- You must have admin rights to your computer to complete the install.
- Required Anti-Malware Application: Real-time protection enabled, updated definitions and from one of the vendors below:
 - Palo Alto, Symantec, Avast, Bitdefender, CarbonBlack, Cisco, Crowdstrike, Cylance, Cybereason, Fortinet, Kaspersky, McAfee, Malwarebytes, Norton, Sophos, SentinelOne, Trend Micro, Webroot.
- Computer must be up-to-date with latest operating system patches and have its firewall enabled.

3) **Important Note:** When connected to the SBM VPN, all traffic (including Internet) will be sent to SBM for connectivity. This traffic is logged and subject to web-filtering rules just as if you were onsite. Please be mindful of this and disconnect when needing to access non-SBM resources.

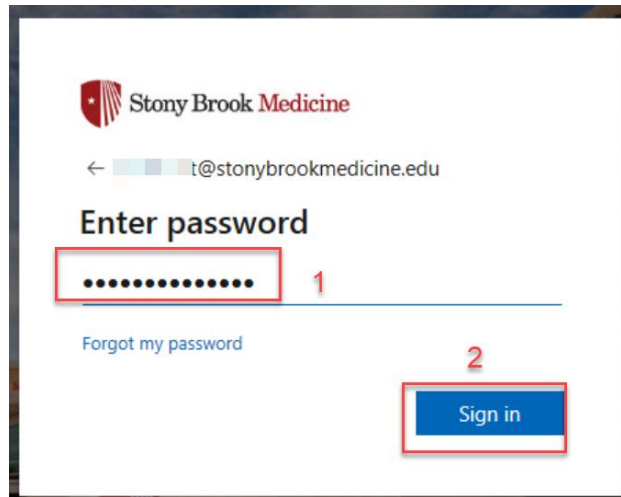
Installation of GlobalProtect Client

1) Please open a web-browser and visit: <https://sbmvpn.stonybrookmedicine.edu>

You should see the screen below. Please enter your SBM e-mail address here and click “Next”.

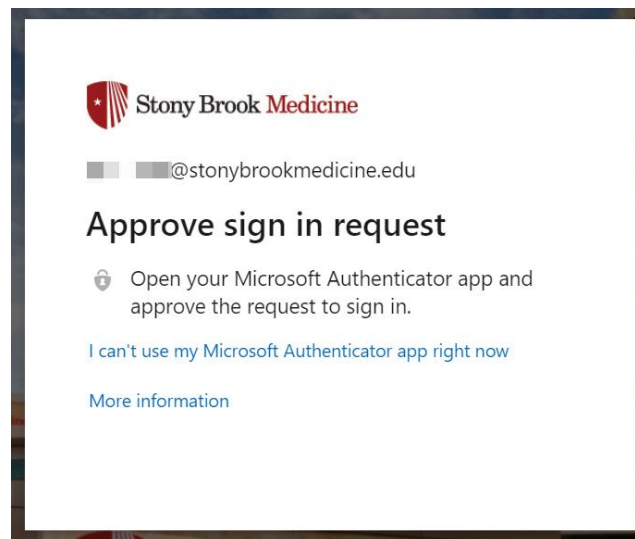


- 2) You should then be asked to enter your SBM Password and click “Sign In” (below):



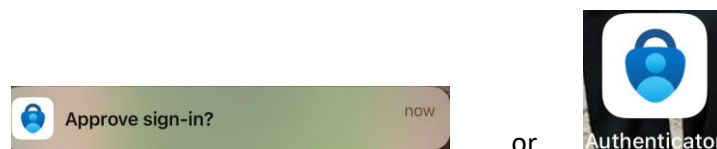
The image shows the Stony Brook Medicine login page. At the top is the Stony Brook Medicine logo. Below it is a back arrow and a partially obscured email address ending in @stonybrookmedicine.edu. The main heading is "Enter password". Below this is a password input field with a red box around it and a red number "1" to its right. Under the password field is a link that says "Forgot my password". At the bottom right is a blue "Sign in" button with a red box around it and a red number "2" above it.

- 3) This process should now show it is awaiting confirmation of the MFA (multi-factor authentication) you have configured on your mobile device (below)

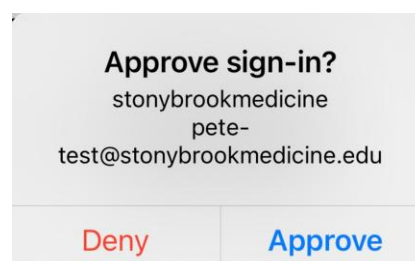


The image shows the "Approve sign in request" screen. At the top is the Stony Brook Medicine logo. Below it is a back arrow and a partially obscured email address ending in @stonybrookmedicine.edu. The main heading is "Approve sign in request". Below this is a lock icon followed by the text "Open your Microsoft Authenticator app and approve the request to sign in." Underneath is a link that says "I can't use my Microsoft Authenticator app right now" and another link that says "More information".

- 4) Please use your mobile device where you should either see a notification to click on or open the Microsoft Authenticator app as shown below.

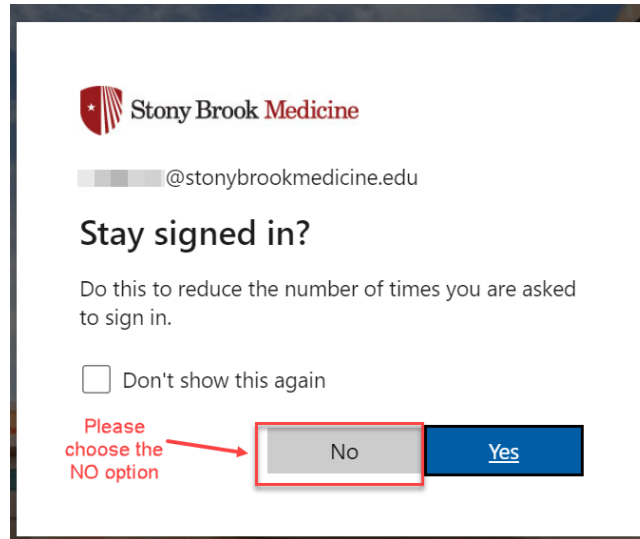


- 5) After you open the app, you should Approve the sign-in (below):

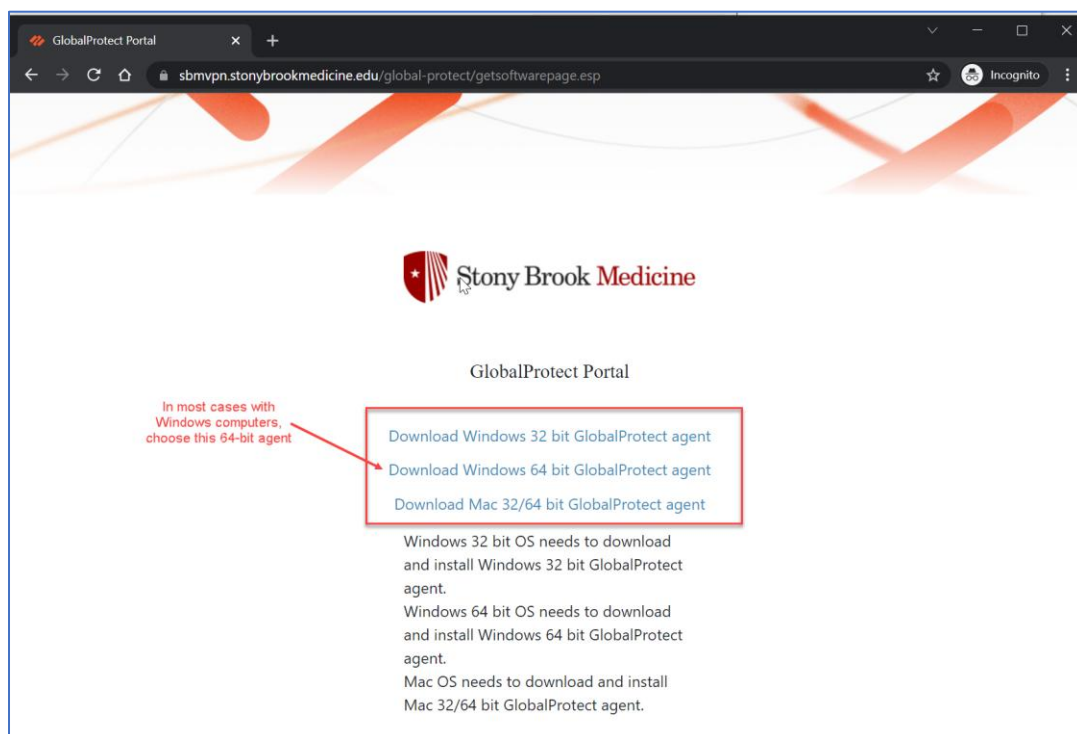


The image shows a dialog box titled "Approve sign-in?". Below the title is the text "stonybrookmedicine", "pete-", and "test@stonybrookmedicine.edu". At the bottom of the dialog box are two buttons: "Deny" in red text and "Approve" in blue text.

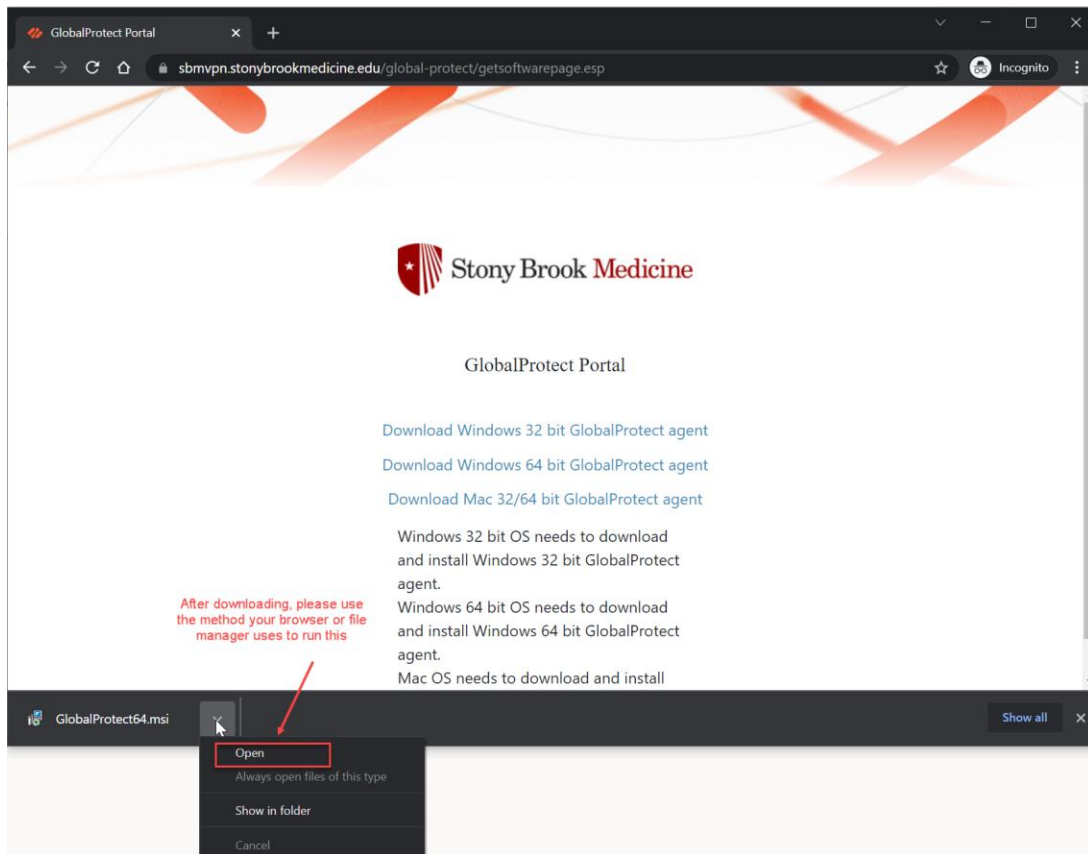
- 6) Once you have approved the MFA, the webpage on your computer should change to the screen below. Please choose "No" below.



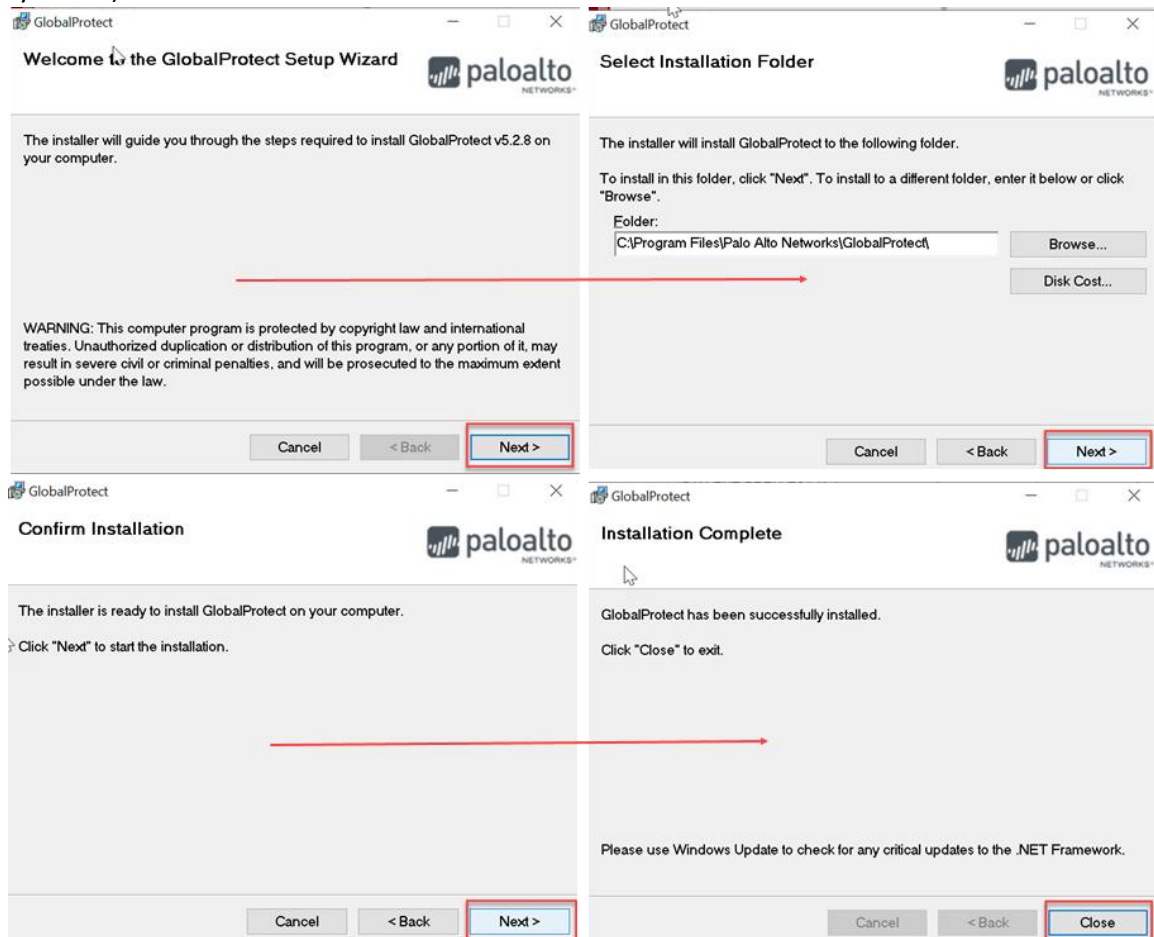
- 7) At this point you have authenticated to the GlobalProtect portal that allows you to download the client (below). You will choose the client you wish to download by choosing the appropriate link. NOTE: Most people will use the Windows 64-bit link. If you wish to confirm type "about your pc" (without the quotes) into the Windows search box and under System Type it will show either 64- or 32-bit.



- 8) After the file downloads, use the method your browser or file manager provides to run this file (GlobalProtectxx.msi). See below for example:



- 9) Please follow through the installation of the GlobalProtect client by clicking on Next through each of the steps (summary below):

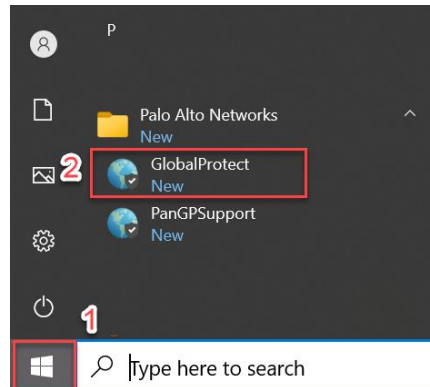


10) You can now proceed to the use instructions below.

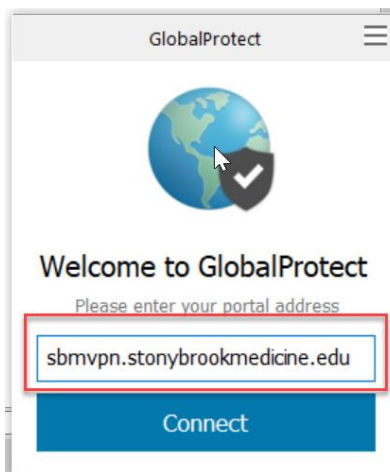
GlobalProtect Use Instructions

The GlobalProtect VPN client is designed in our environment to be used on-demand (only when needed). Therefore the client should only be enabled when actual SBM resources are needed. Do not leave running all the time. **This is especially important because all Internet and home network traffic will be passed through Stony Brook Medicine when connected. This may impact certain Internet or home sites you can reach from your computer when connected. Please disconnect the VPN if you wish to reach these sites.**

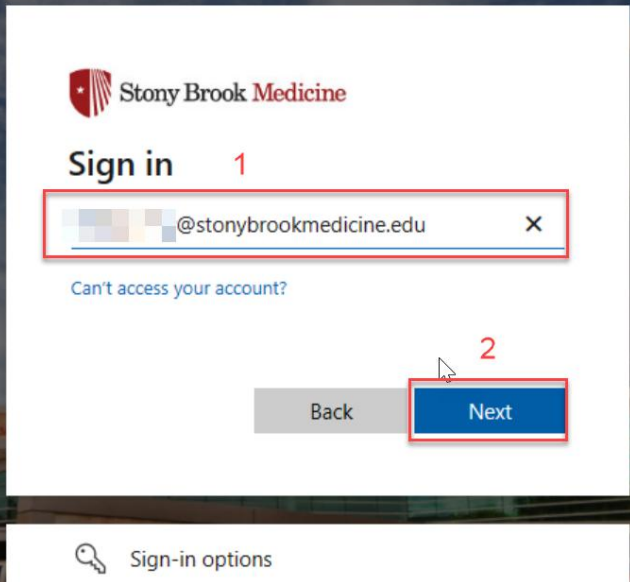
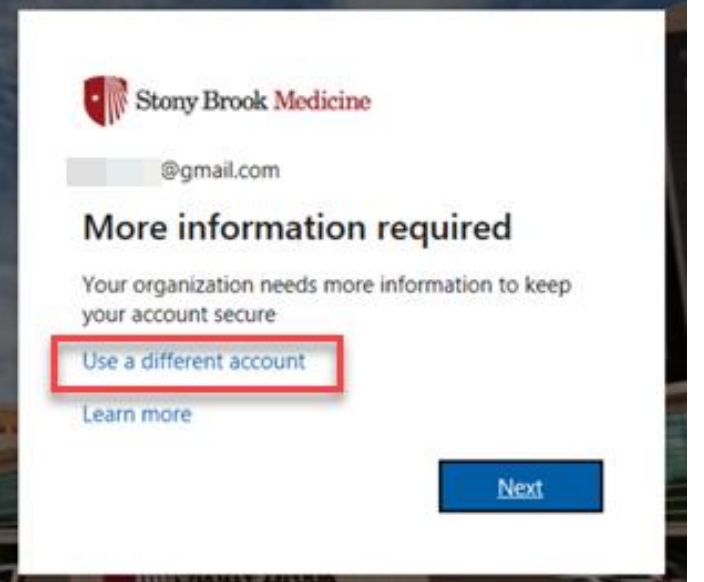
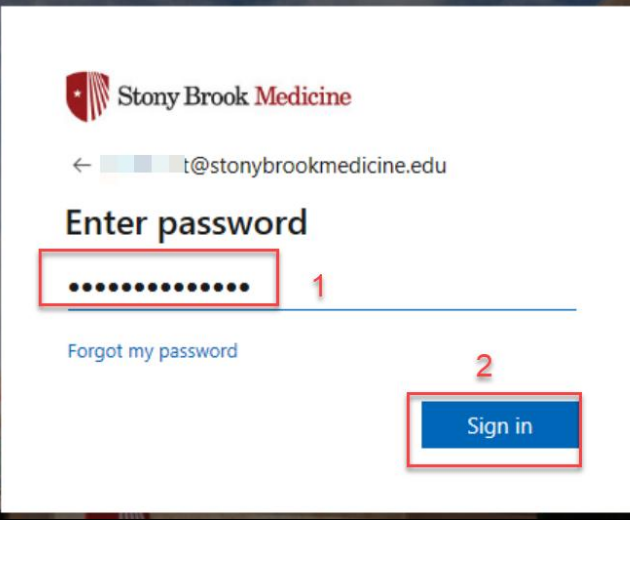
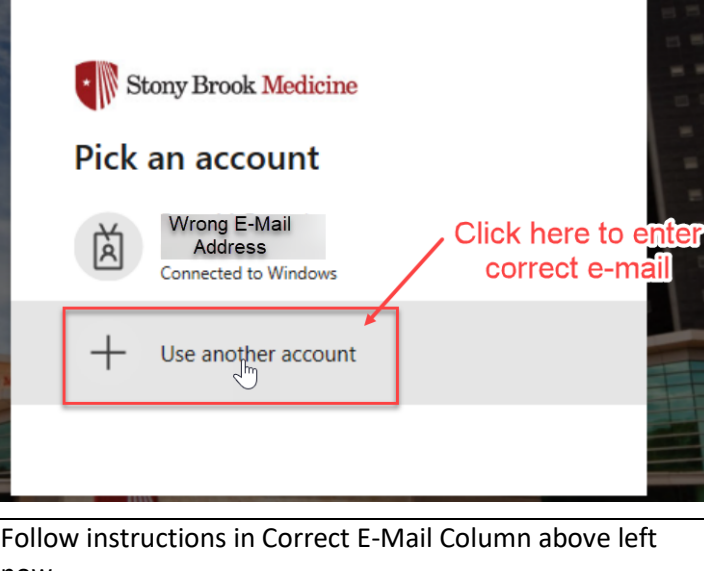
- 1) After you have installed the GlobalProtect client, you can now run for the first time by choosing the Windows Start menu and selecting “GlobalProtect” client as show below.




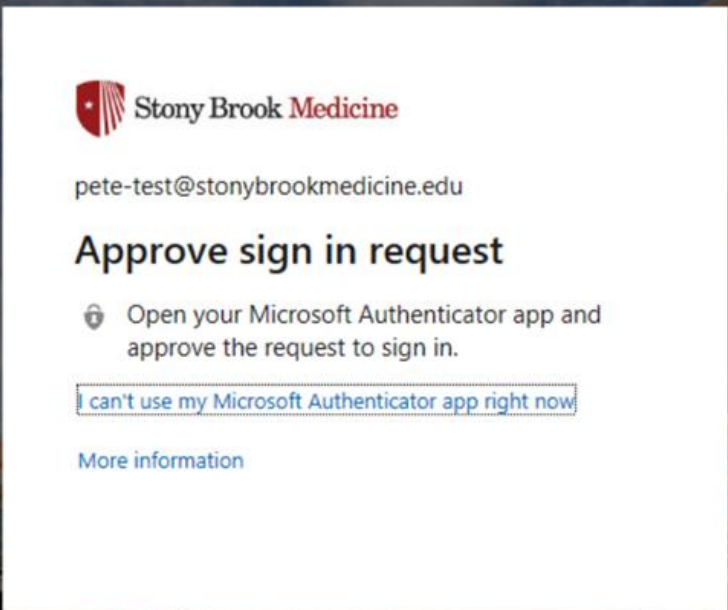

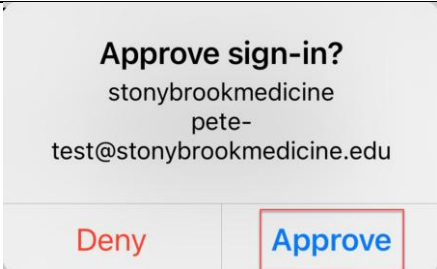
- 2) The main GlobalProtect window should pop-up on the right-hand side of your computer by the task bar (below). Please enter, sbmvpn.stonybrookmedicine.edu in the box and click “Connect”.



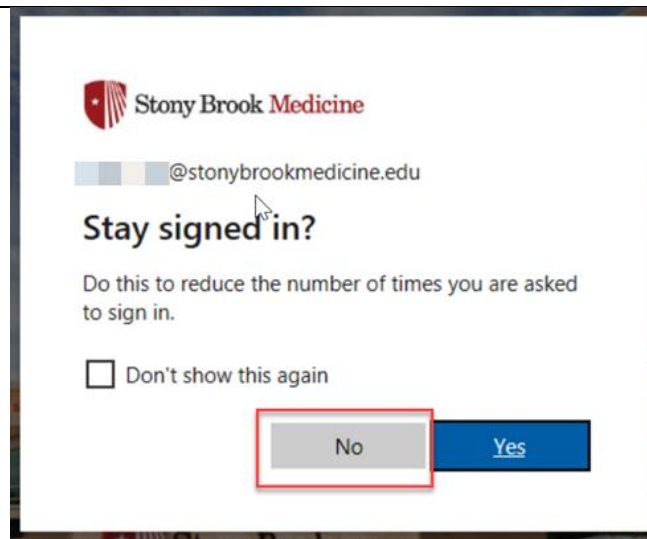
- 3) You should now receive a pop-up window asking for your credentials. Depending on how your computer is configured, you may find that the proper email address is in this field. In this case you can click “Next”, if it is not your proper SBM email, choose the “use different account” selection to enter the correct account (see samples below).

Correct SBM E-Mail	Incorrect SBM E-Mail
 <p>Stony Brook Medicine</p> <p>Sign in 1</p> <p>@stonybrookmedicine.edu X</p> <p>Can't access your account?</p> <p>Back Next 2</p> <p>Sign-in options</p>	 <p>Stony Brook Medicine</p> <p>@gmail.com</p> <p>More information required</p> <p>Your organization needs more information to keep your account secure</p> <p>Use a different account</p> <p>Learn more</p> <p>Next</p>
 <p>Stony Brook Medicine</p> <p>← @stonybrookmedicine.edu</p> <p>Enter password</p> <p>Forgot my password</p> <p>Sign in 2</p>	 <p>Stony Brook Medicine</p> <p>Pick an account</p> <p>Wrong E-Mail Address Connected to Windows</p> <p>Use another account</p> <p>Click here to enter correct e-mail</p>
	<p>Follow instructions in Correct E-Mail Column above left now.</p>

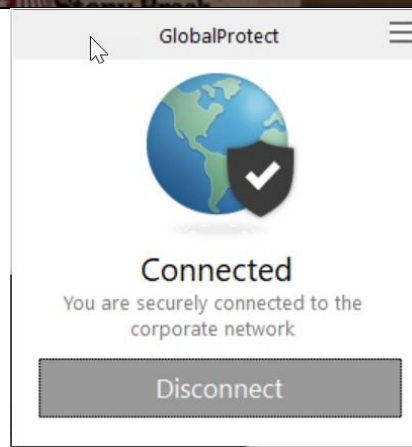
- 4) After clicking “Sign In” above you should now be presented with a prompt to enter your password and accept the MFA (Multi-Factor Authentication) on your mobile device. Please follow the detail steps below.

<p>4a) Enter your email password and click Sign-In</p>	
<p>4b) The system has now sent the MFA (multi-factor authentication) to your mobile device. Leave this screen open and view your mobile device.</p>	
<p>4c) On mobile device click on the notification or open the Microsoft Authenticator App.</p>	
<p>4d) In the Authenticator, please click the "Approve" menu item.</p>	

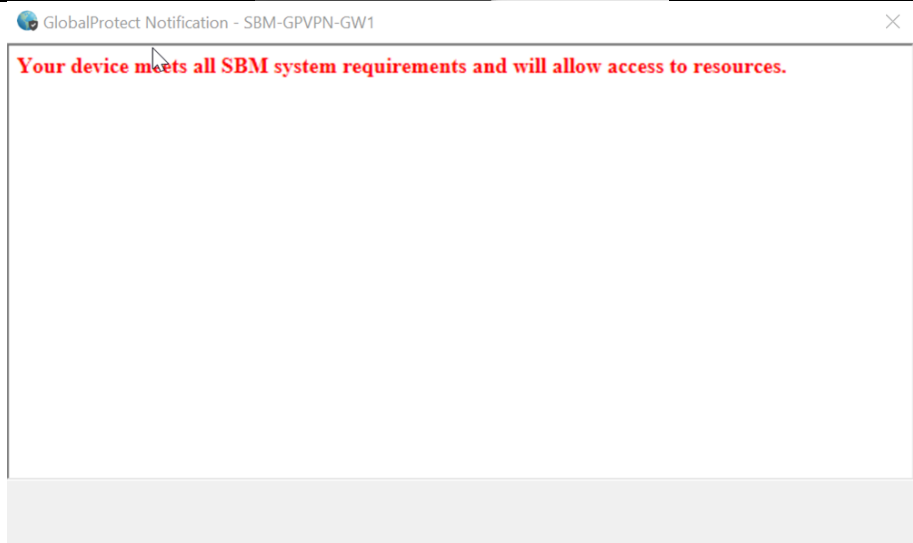
4e) On the Stay Signed In page, choose the "No" option.

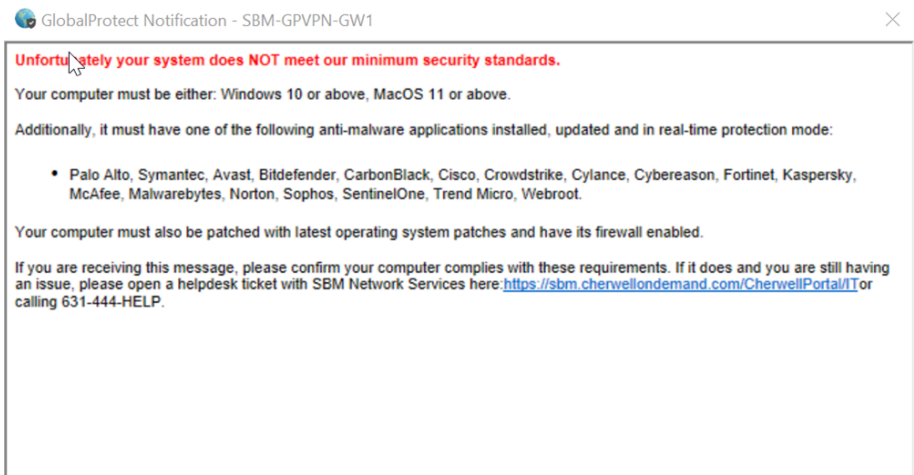
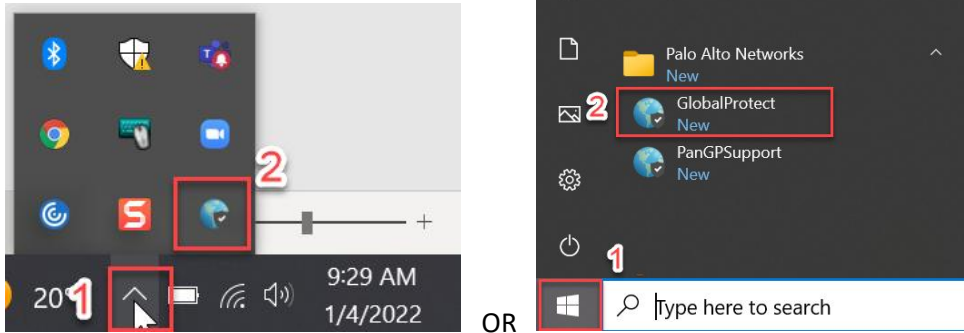
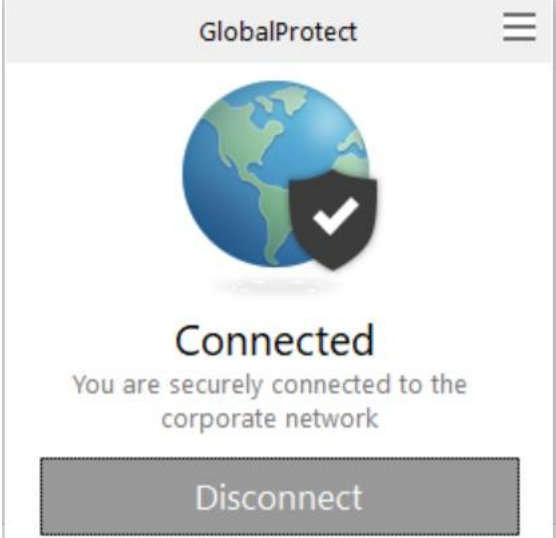


4f) The GlobalProtect app should now change to "Connected" just above the taskbar.



4g) A pop-up will appear to show the security status of your computer. If you see the message to the right, you are ready to access all resources, however if you see a different message see below.



<p>4h) If you see the message to the right, your system does not meet the minimum security standards and will not be able to access most resources. Please see the requirements at the beginning of this document and make sure your system meets these requirements before connecting again.</p>	
<p>4i) At this point, the VPN is connected and should be able to access necessary resources. If you want to check the status you can choose one of the two methods to the right to click to open the client or see the status.</p>	
<p>4j) When you open the client you will see the menu to the right which will allow you to disconnect the SBM VPN and restore direct access to the Internet. We strongly recommend disconnecting when done working with SBM resources. NOTE: The VPN will timeout after 2 hours of inactivity and force reauthentication after 8 hours.</p>	

If you have any questions or issues, please open a helpdesk ticket at:
<https://sbm.cherwellondemand.com/CherwellPortal/>