OCIO Knowledge

How to Connect to VPN on an HHS Laptop

VPN stands for **Virtual Private Network** and allows users to use a public internet connection to connect to the HHS network securely. While connected to VPN, your laptop will be able to access HHS network resources as well as be protected by HHS network security features.

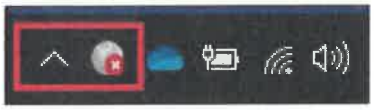
There are currently two VPN applications in use by HHS. The Endpoint Security VPN application is in the process of transitioning to the GlobalProtect VPN application. During that transition, both applications will be available to use.

How to connect to GlobalProtect VPN:

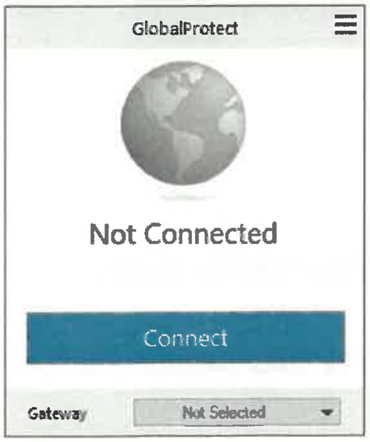
GlobalProtect VPN requires a PIV card to connect. If no PIV is available and you are on an active PIV exception, Azure Multi-factor Authentication (MFA) login will be required in place of a PIV login. There is no other change in the connection process. For more information, refer to KB0011728 - How to Use Multi-factor Authentication with Microsoft 365. If you require a PIV exception, contact the OCIO Service Desk for assistance.

For a video tutorial on how to connect to the VPN service using GlobalProtect, please reference the Connecting to the VPN Service Using GlobalProtect guidance video.

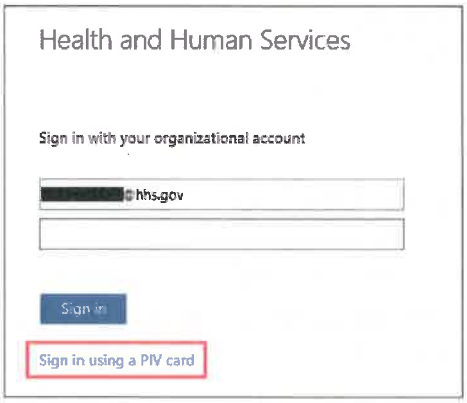
1. Verify your system is connected to the internet. For more information, review KB0010311 - How to Connect a Laptop to a Wi-Fi Network.
2. Locate the grey globe icon in the lower right of your screen. If it does not display there, click the Up Arrow icon to expand the displayed icons.



3. Click on the grey globe icon to open the GlobalProtect application and click the **Connect** button.



4. Enter your **HHS.gov** email address and select the option to **Sign in using a PIV card**. Enter your PIN when prompted.

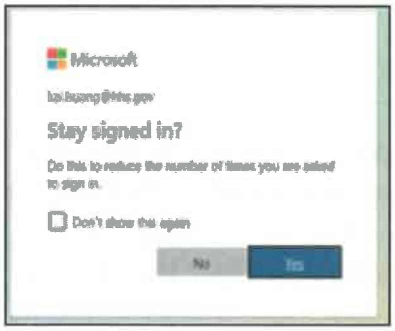


Health and Human Services

Sign in with your organizational account

[redacted]@hhs.gov

5. If asked to stay signed in, click **Yes**.



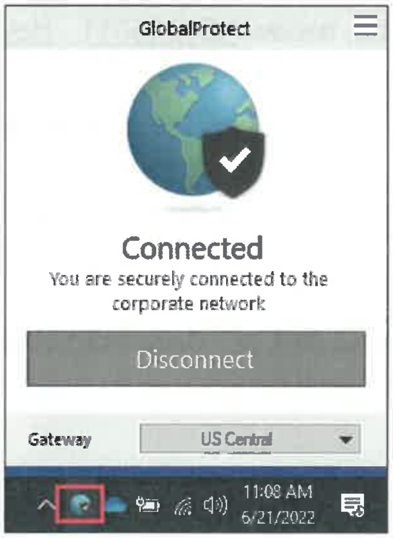
kai.huang@hhs.gov

Stay signed in?

Do this to reduce the number of times you are asked to sign in.

□ Don't show this again

6. If successful, the status screen will change to **Connected** and the globe icon will change color with a checkmark on it.



Connected

You are securely connected to the corporate network

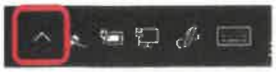
Gateway US Central

How to connect to Endpoint Security VPN:

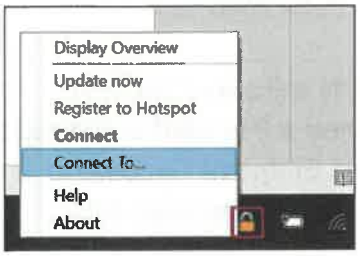
Endpoint Security VPN requires a PIV card to connect. If a PIV card is not available, review KB0011803 - How to Connect to VPN without a PIV Card.

For a video tutorial on how to connect to Endpoint Security VPN with a PIV card, please reference the Connecting to VPN with a PIV Card guidance video.

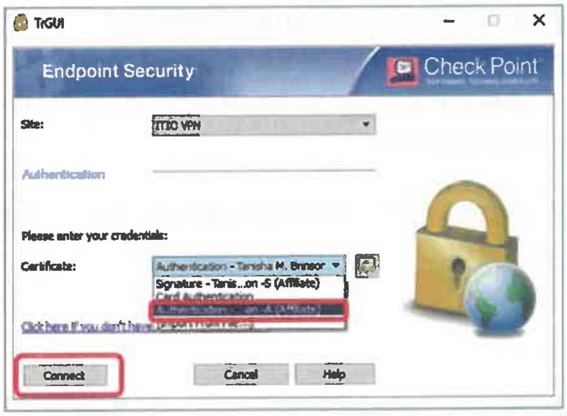
1. Verify your system is connected to the internet. For more information, review KB0010311 - How to Connect a Laptop to a Wi-Fi Network.
2. Click the Up Arrow icon in the system tray in the lower right corner to view hidden icons.



3. Right-click on the gold padlock icon and select **Connect To...**.



4. Next to Certificate, use the dropdown menu to select the certificate that starts with **Authentication** or ends with **-A**. Then, click **Connect**.

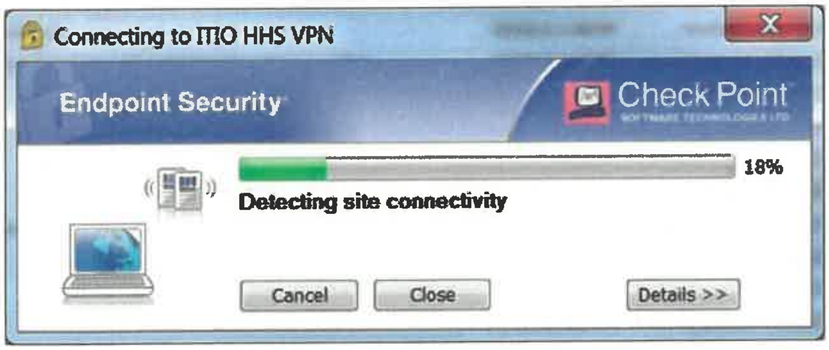


Site: ITIO VPN

Please enter your credentials:

Certificate: Authentication - Tanisha M. Brnnor

5. A connection progress screen will appear and you will be prompted to enter your PIV card PIN.



Connecting to ITIO HHS VPN

18%

Detecting site connectivity

Once your PIN is entered and accepted, a "whistle" sound will be made and a message indicating a successful connection should display.

Be sure to disconnect the VPN by right clicking the padlock icon and selecting **Disconnect** when no longer needed to free up network bandwidth for active users.

Troubleshooting VPN Connection issues:

If VPN fails to connect or fails to stay connected, you can do the following to troubleshoot connection issues.

Verify the internet connection is active. The easiest way to do so is to try and go to a public website like Google. If the site does not load, that can indicate the system is not connected to the internet. If the system shows it is connected to a Wi-Fi router, try restarting the router. If issues persist, contact the Internet Service Provider to troubleshoot internet connectivity issues or to determine if there is an outage in your area.

Try a different Authentication certificate. By default, Endpoint Security VPN will select the last authentication certificate that it was able to successfully connect with. When a PIV card is renewed or replaced, the old authentication certificate will no longer be valid, however Endpoint Security VPN will still try and connect with it. If that happens, use the dropdown menu to select the second active Authentication certificate.

VPN disconnects frequently. Unlike other internet applications like websites or streaming video that will wait for internet to become available and continue where it left off, VPN has a very short time-out period. Frequent VPN Disconnects is usually caused by brief and sporadic loss of internet connectivity that may not be apparent in other internet apps. Try and restart the internet router to clear the issue. If the issue persists, contact the Internet Service Provider to run a test on your line to identify and fix any packet loss or instability in your internet connection.

If you have any questions or would like further assistance, please call the OCIO Service Desk at your convenience at 1-866-699-4872 or email the OCIO Service Desk.