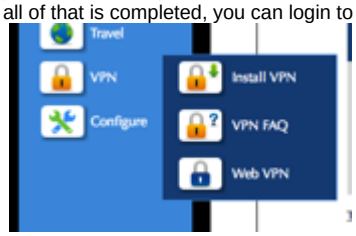
# How to gain JHU VPN access

## NOTE: Do not use the Web VPN as it won't allow you to SSH to the test nodes.

https://cds.johnshopkins.edu/vpn/

1) You will see references to a web based VPN in the above link. This will not work for connecting to the HLTCOE resources
2) To connect to the VPN, the user must have a JHED (Hopkins ID)
3) 2-Factor Authentication is required
    a. Users requesting VPN access at this time will be required to use Azure MFA (Multi-factor authentication) To enroll in Azure MFA go to https://aka.ms/mfasetup (Use your JHED login JHED@jh.edu )
    b. If you have setup MFA already with Google authenticator, OTP manager, or other methods, they will still work for now, but JHU Enterprise IT will be asking you to move to Azure MFA in the future.
4) Once 2-Factor Authentication is setup, the user must request VPN access at the below link
    a. https://johnshopkins.service-now.com/serviceportal?id=sc_cat_item&sys_id=8446c8800fe00600976b9bd692050e4c
        i. Ensure “VPN Client Access (Access includes Web VPN and VPN Mobile App)” option is checked and complete “Justification” section along the lines of “Required to access HLTCOE resources per jmckni10”
5) Once all of that is completed, you can login to the my.jhu.edu portal and select “VPN – Install VPN” and follow its instructions for the appropriate OS
    a. 


JHU Enterprise IT distributed a Remote Access Guidelines, which can be read below.

**HLTCOE IT highly recommends you use the Pulse VPN on Windows or Mac operating systems. Linux and Google Chromebook support are best effort support only.**