LEWIS CLARK STATE COLLEGE
INFORMATION TECHNOLOGY

Virtual Private Network (VPN) Instructions for Staff and Faculty

***Note**: This documentation assumes that an employee has been approved to have access to VPN. This approval starts with a Help Desk ticket from a director requesting VPN for a particular employee.*

The VPN system allows you to access secure campus resources such as Ellucian Colleague, Ellucian Recruit, WebNow, as well as file servers such as Redwood and Alder. You can use LCSC's VPN while you are at home or at any other location with Internet bandwidth.

You will **not** be able to use campus printers and scanners. You **cannot** connect to the VPN while on campus.

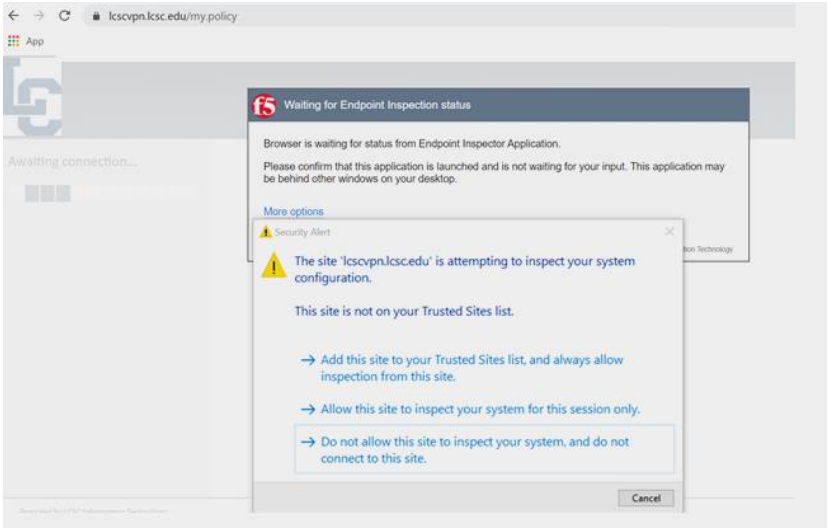
IT recommends using an LCSC owned computer to access the VPN. While VPN should work on your own computer, the department cannot provide support for non-college computing devices. The computer should be connected each month to ensure the computer receives updates and will continue to successfully connect to the VPN.

Please ensure you are up to date on Windows updates and that your antivirus is up to date. Windows computers require a full antivirus scan every two weeks. Refer to the troubleshooting section on how to run a full antivirus scan for Windows computers.

Connecting to the VPN

Once you are on a computer with Internet access, open a web browser such as Edge, Chrome or Firefox and go to LC State VPN access (https://lcscvpn.lcsc.edu/). You will be prompted to log in. Use the same username and password as your email (*you will not need the @lcsc.edu for the username*).

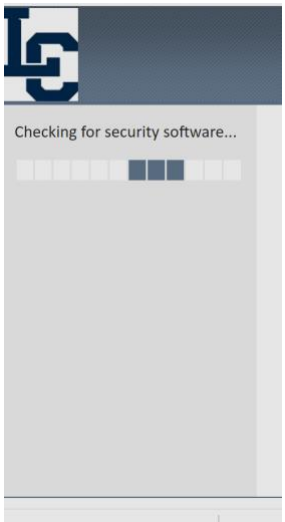
On first time login, you will be asked to install the F5 Endpoint Inspector and run a system check. Click the first option – ‘Add this site to your Trusted Sites list…”.



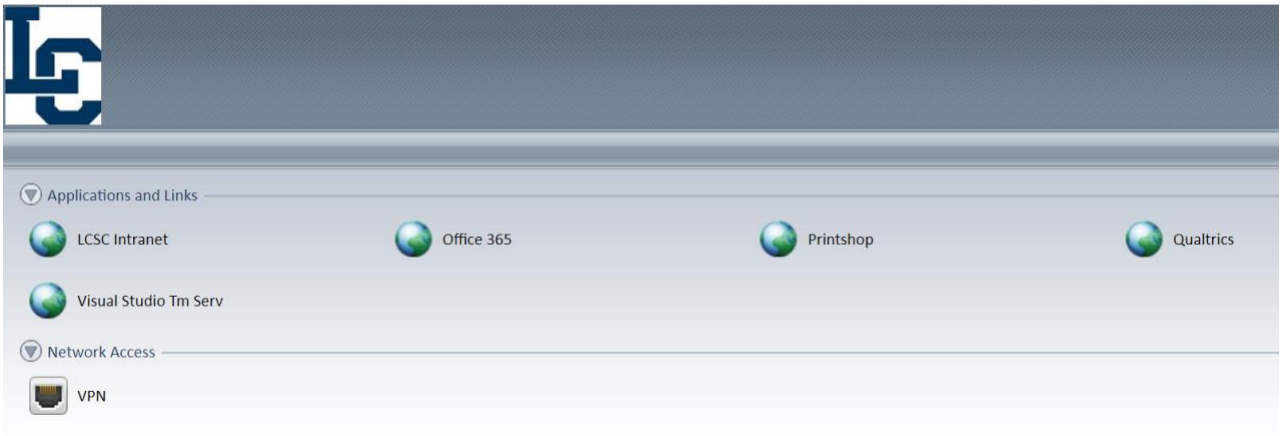
F5 Endpoint Inspector will determine if your computer’s operating system and antivirus software are up to date. This verification protects LCSC’s resources once you connect. The inspection process occurs every time you connect to the VPN.

This step can take a few minutes as it scans your computer.

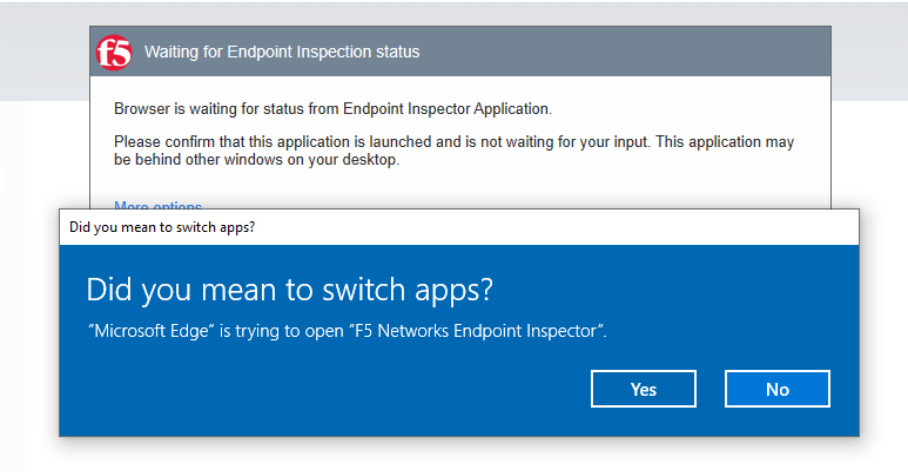
If the scan produces a failure with an error message, jump down to the “**Troubleshooting**” section of this document on the last page.



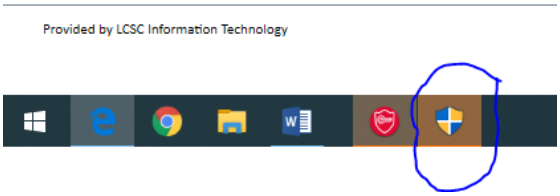
If your computer passes the inspection, then you will be presented with the following screen. Click on the VPN icon.



A box will pop up asking you to confirm the Endpoint Inspection. Click Yes.



Pay close attention to the task bar. Click on the blue and yellow shield if it appears.

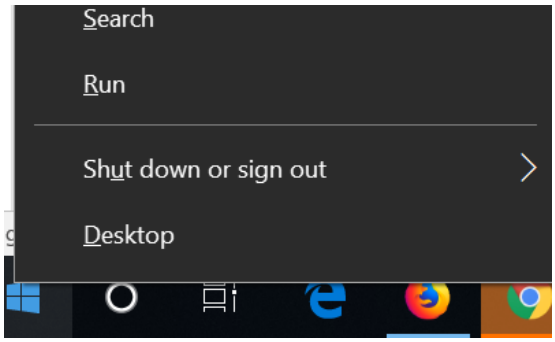


Clicking on the shield will produce the following message. Click “Yes.”

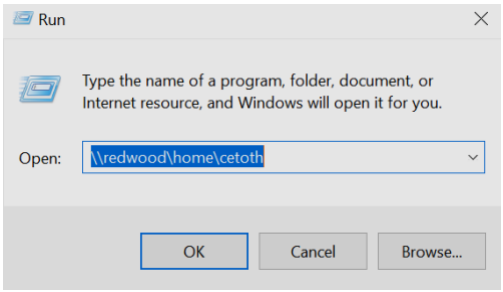
In the lower right corner, you should see a red shield. Hover your mouse over the shield and it should say “Connected to /Common/VPN.” If that’s what you see, you are connected to LCSC’s VPN and can access your network shared drives, Colleague, WebNow, etc.

Network Shared Drives

To access network shared drives, you need to know the exact file pathway. Once known, right click the start button, and click run.

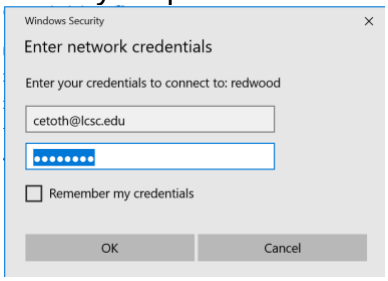


To access Redwood or Alder file shares, type \\redwood or \\alder and then the share name. To access a Redwood home drive type \\redwood\home\<userid> and click Ok. For example:



For Department shares, type in \\redwood\(insert your department share name).

While connecting to a network shared drive you may be prompted for your credentials. You will need to type in your full email address and your password to connect.



Troubleshooting

The following screenshot is an example of an error that can be received when trying to use the VPN.

If you receive the error "your session could not be established" then try the following:

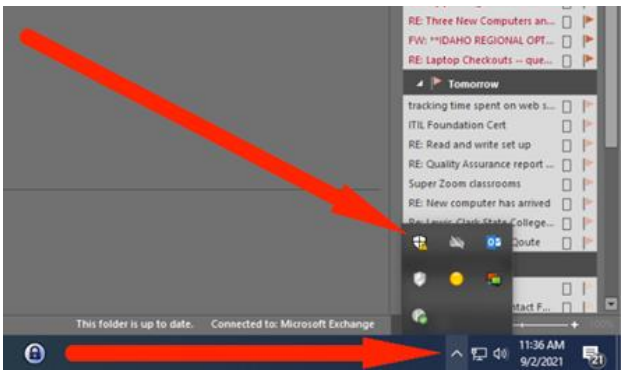
- **FOR PC USERS:**
  - Open Windows Updates (https://support.microsoft.com/en-us/hub/4338813/windows-help?os=windows-10) and make sure you have the latest updates.
  - Open your Antivirus, check for updates, and run a full scan. *A full scan is required every 2 weeks.* Instructions on how to run a full scan are shown below.
- **FOR MAC USERS:**
  - Ensure Mac OS updates have been installed.
  - Open Sophos, check for updates, and run a full scan.

If you still experience issues, contact the IT Help Desk with the session reference number as soon as you receive the error. IT can check the logs to see what is preventing you from connecting.

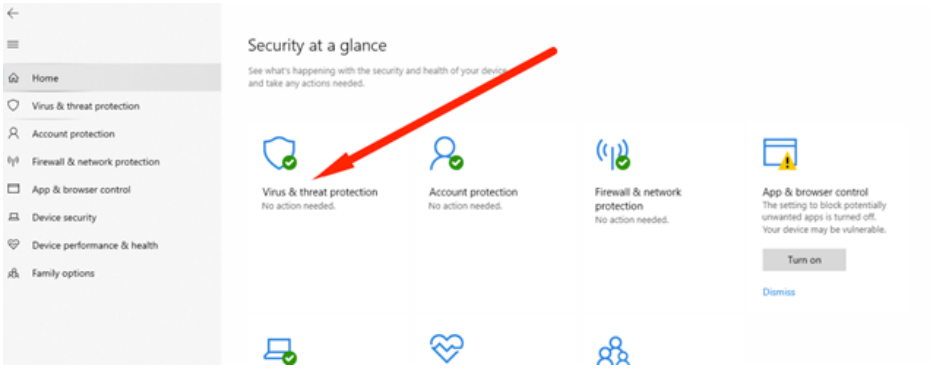
Running a full scan on Windows:

This will take around 45-60 minutes. If you still cannot connect, go back into the shield as shown on step one and make sure there isn't an error asking you to restart a service.

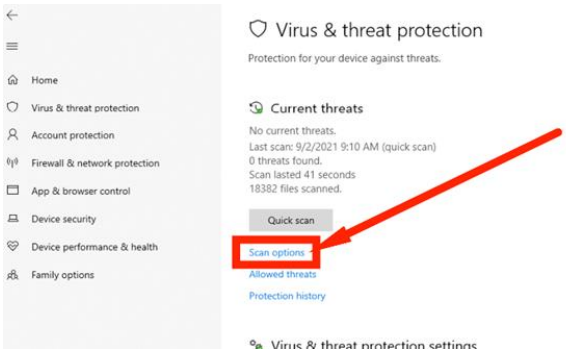
1. Click on the ^ icon down by your clock and then click the shield.



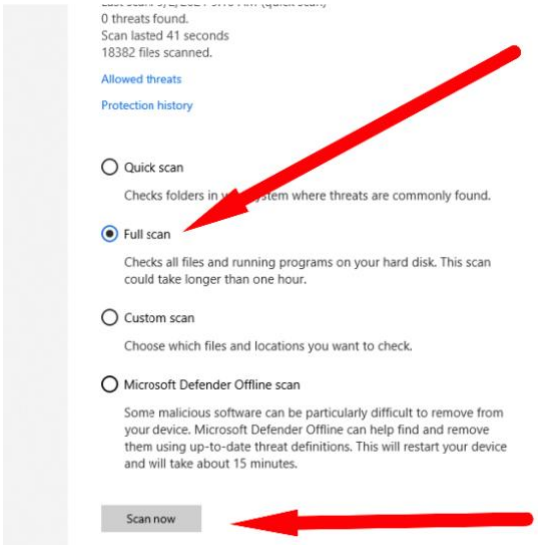
2. Click on Virus & threat protection.



3. Click on Scan Options



4. Choose Full scan and then click Scan now



5. Wait for scan to complete (this may take up to an hour) and then try to connect to VPN again.