UNIVERSITY OF EXETER

VPN – Windows 10

To create the VPN connection to the UoE network you will need to connect to the secure website and install Pulse Secure. The VPN software allows you to connect securely to the University network as if your device was directly connected.

IMPORTANT - You will require administrative rights on *your computer* to complete the initial installation of Pulse Secure. These are not required once the installation is complete.

Initial setup of VPN service.

Open your web browser and navigate to http://as.exeter.ac.uk/it/network/vpn/
Look for the correct version of windows 10 – the majority of windows machines are 64bit ones.

Latest Version Operating System 9.1r3	Pulse Secure Client Software	How to Connect to the VPN
Windows XP / 7 / 8 / 8.1 32-bit	ps-pulse-win-9.1r3.0-b1313-32bitinstaller	Click here for instructions
Windows XP / 7 / 8 / 8.1 64-bit	ps-pulse-win-9.1r3.0-b1313-64bitinstaller	Click here for instructions
Windows 10 32 bit	ps-pulse-win-9.1r3.0-b1313-32bitinstaller	Click here for instructions
Windows 10 64 bit	ps-pulse-win-9.1r3.0-b1313-64bitinstaller	Click here for instructions
Mac OS X	ps-pulse-mac-9.1r3.0-b1313-installer	Click here for instructions
CentOS 6/7 32 bit	ps-pulse-linux-9.1r3.0-b85-centos-rhel-32-bit-installer	Click here for instructions
CentOS 6/7 64 bit	ps-pulse-linux-9.1r3.0-b85-centos-rhel-64-bit-installer	Click here for instructions
Ubuntu 14.04 to 16.04 32bit	ps-pulse-linux-9.1r3.0-b85-ubuntu-debian-32-bit-installer	Click here for instructions
Ubuntu 14.04 to 16.04 64bit	ps-pulse-linux-9.1r3.0-b85-ubuntu-debian-64-bit-installer	Click here for instructions

Click on the correct version of software (highlighted)**.** This will begin the downloading of the required software.

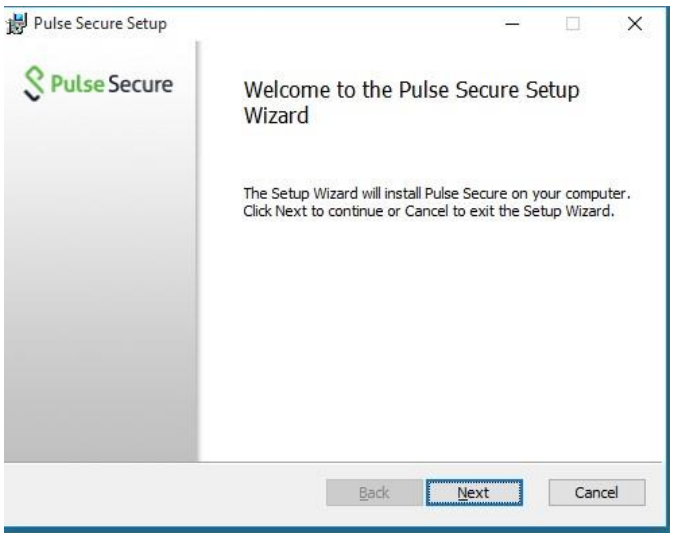
Obtaining Pulse Secure

Once you have clicked on the software it will download by default to the "Download" folder. This is located by clicking on the "This PC" icon.

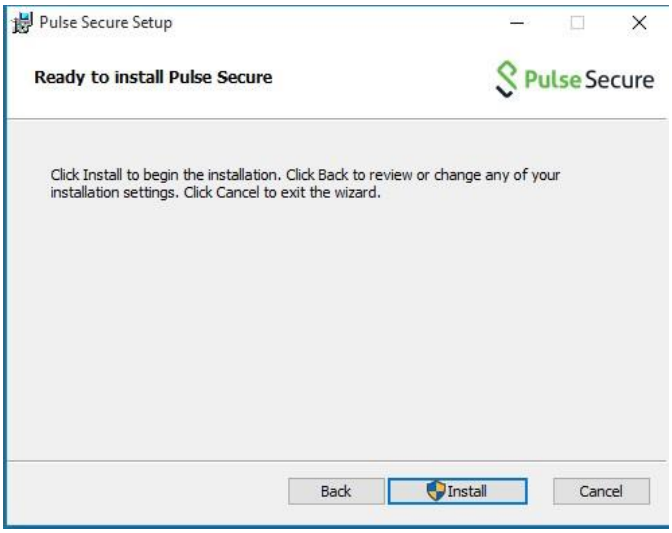
In the window opened by clicking the above icon look for the folder called "Downloads". Once located double click it to install.

Installing Pulse Secure

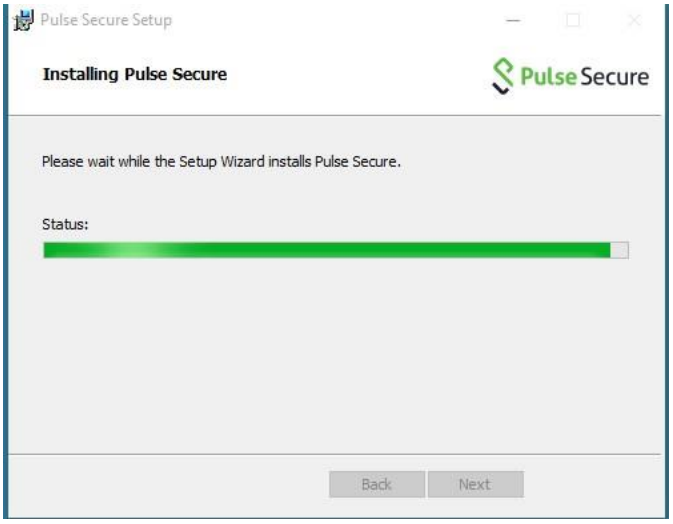
The install procedure will begin.
Choose next,



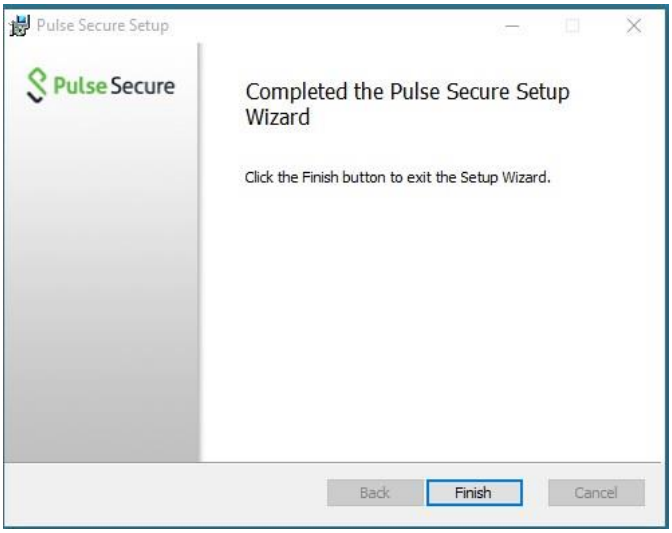
Then choose Install



The installation should only take a few minutes.



Click on Finish.

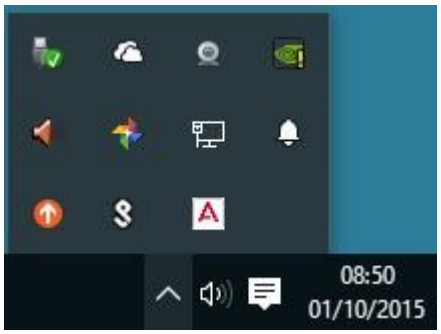


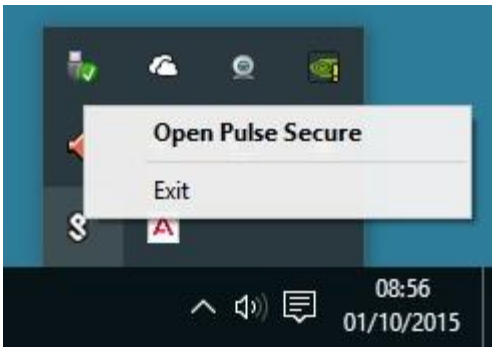
Pulse secure is now installed on your Windows 10 machine.

You may see it on the task bar as shown, or it may be in the hidden icon section of the task bar.

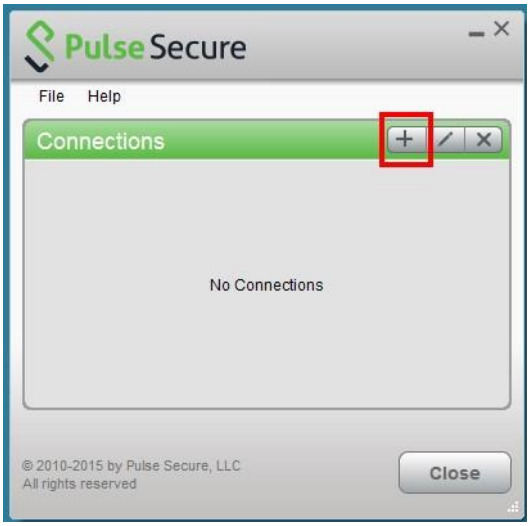
Once you have located the icon for Pulse Secure.

Left click on it and select **"Open Pulse Secure"**





From this screen you need to choose the **+** icon to add a new VPN connection.

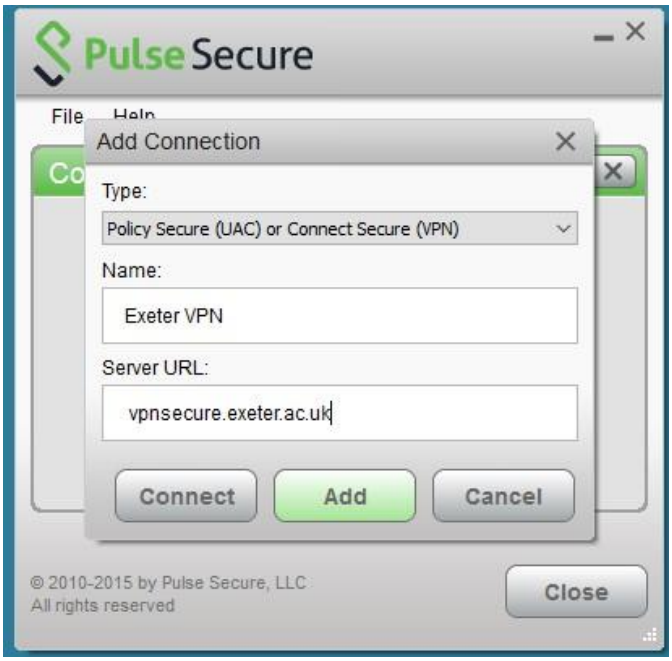


This will allow you to now manually enter the location for the VPN to connect to:

The settings are:

Name : **Exeter VPN**

Server URL: **vpnsecure.exeter.ac.uk**



Now **Click Add**.

This information will not need be added on subsequent connections.

To connect to the University VPN **click the connect** button.

You will be prompted for your University Username and Password. Keep these secure.

Using Pulse Secure

After installation, the Pulse Secure client will load automatically every time you start windows.

However, in the future, it will **not connect** to the University VPN unless prompted. You can connect in one of two ways:

Visit the vpnsecure.exeter.ac.uk website and enter your login details this will then start the software automatically.
Click on the Pulse Secure client on your computer and click Connect, for the Exeter entry.

You will be prompted for your username and password to complete the logging on.

- It is NOT recommended that you Save Settings for security reasons

Important information when using the VPN service

Once connected, your device will have a secure tunnel to the University network, and will be allocated a UoE network address. It will effectively be treated as directly connected to the University network.

Unless specifically requested otherwise, all the network traffic your device generates during an active VPN session will travel via the secure tunnel and the University network. This is useful to know when accessing external resources that will only permit access from known University network addresses.