# Guide for Windows users to Access the NISER Campus LAN at Jatni through by Tunneling through VPN

**Purpose:**

To support staff, students and faculty members who may be conducting work either remotely or without a direct connection to the institute's network. Whilst the use of a secure virtual private network (VPN) will provide better assurances against the potential of data leakage than previously offered, it will not, however, ensure that data is completely safe, as various forms of malware and keyloggers could still be active. Computer Centre strongly advocate that any device used to undertake any work of the institute must be completely up to date with operating system and application security patches as well as having an anti-malware product installed and active.If you are working with personal, confidential or commercially sensitive data, you must ensure that you are using a secure connection (VPN), especially if you are using an unsecured public network, such as in a hotel or train station or airport. You should not connect to any unsecured wireless network unless you are sure of its

legitimacy.

1. Download the latest version of FortiClientVPN from fortinet.com site for windows OS. You may download the installer from this link:
https://www.niser.ac.in/docs/FortiClientVPNOnlineInstaller.exe

Please install the above and then do the following:
Give a name to the connection. Give the Server Address: **103.160.128.1** with port **10443**, give your **username** and **password** (your own WiFi access credentials or shell account credentials for home folder access) for SSL-VPN. Then click Connect to access the NISER Campus LAN resources.

You may also try the steps given below:
1. Download the tar ball for Forticlient SSL VPN Client installation on Windows from this link:
For 64 bit Windows:
https://www.niser.ac.in/docs/sslvpnclient64pkg_4.4.2332.tar.gz
For 32 bit Windows:
https://www.niser.ac.in/docs/sslvpnclient32pkg_4.4.2332.tar.gz
Then extract the tar ball using any compression/decompression software like Winzip, 7-Zip, WinRAR, etc. with option "**Extract to sslvpnclient64pkg_4.4.2332**"
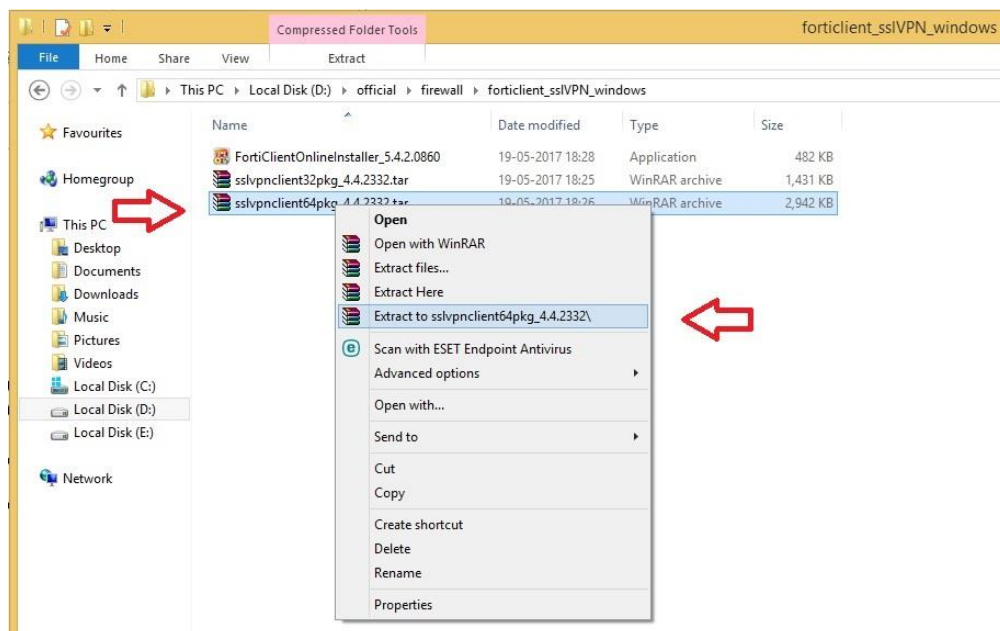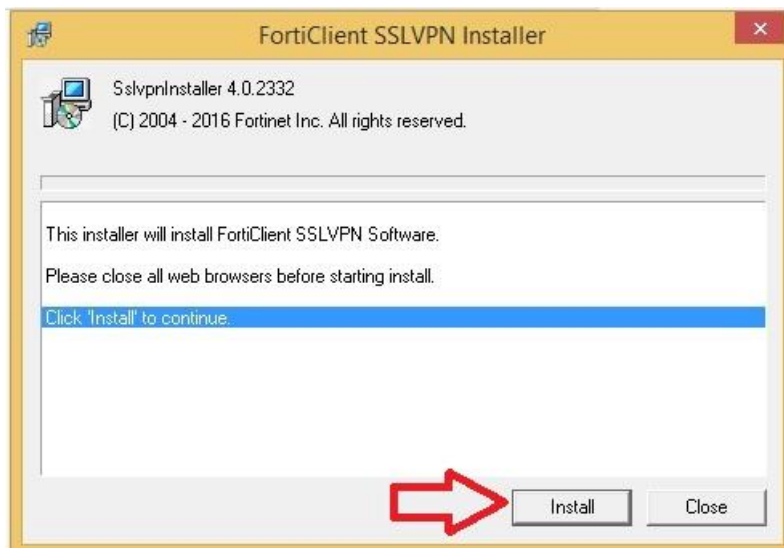


2. Then double click on the extracted folder "**sslvpnclient64pkg_4.4.2332**".
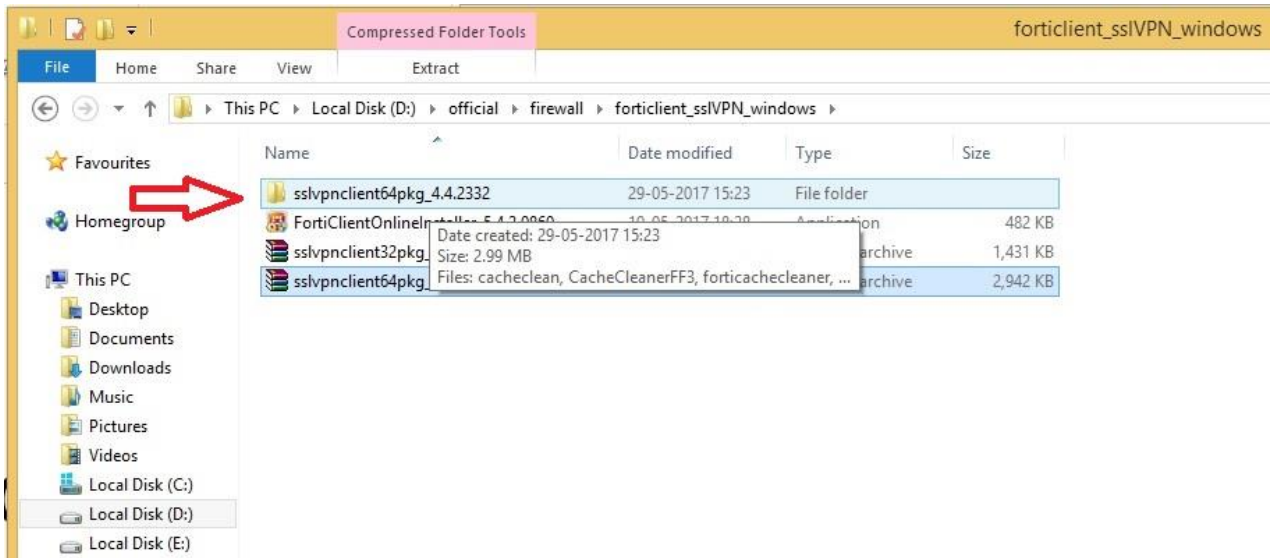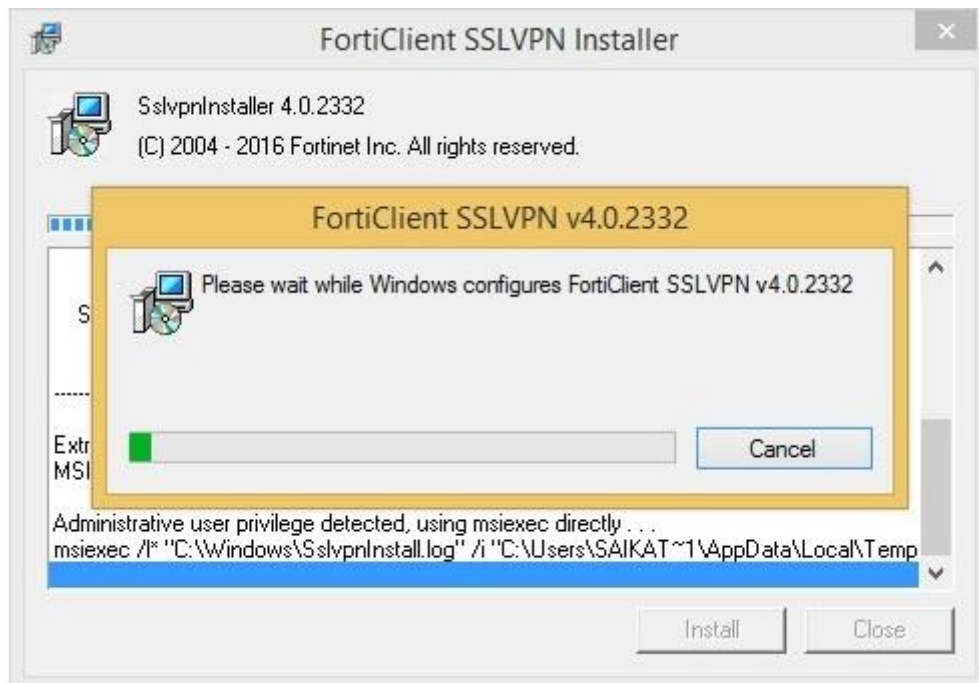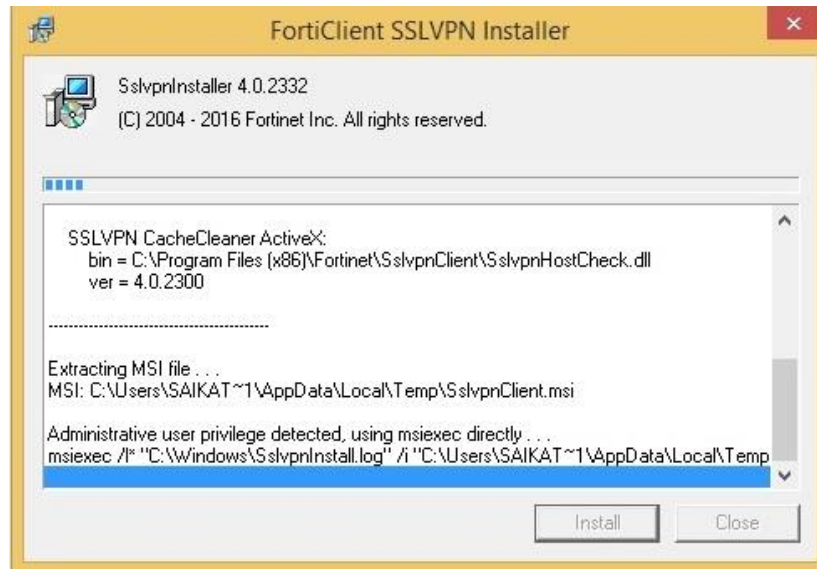
3. Then install the application named SslvpnClient.exe (*Run as Administrator* ).
   When done close the window from **Close** button.
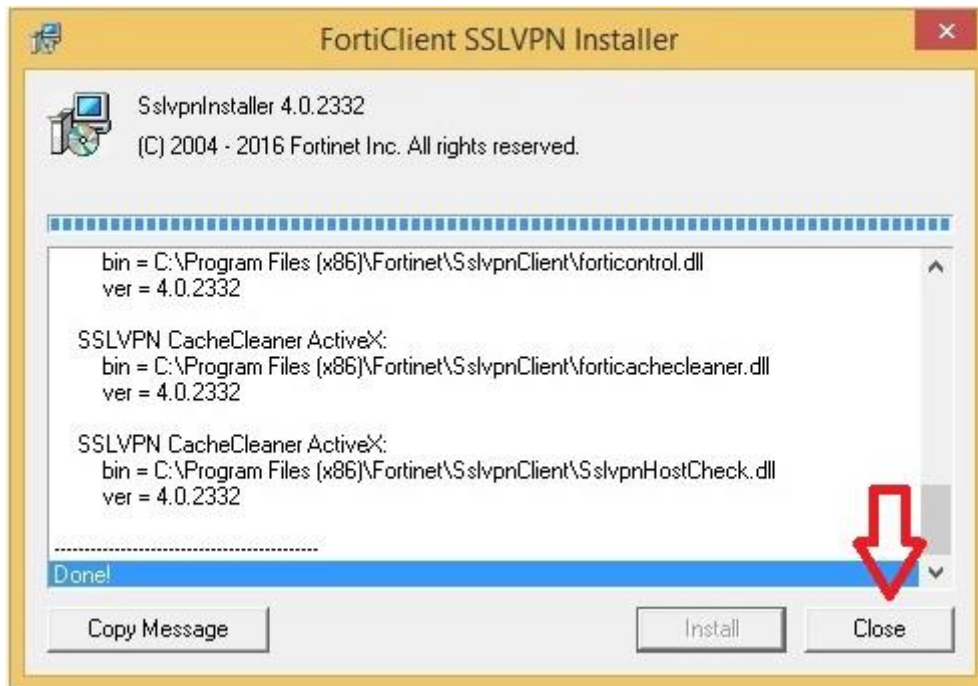   Right click >> Run as administrator   **OR**   Double click >> Run as administrator
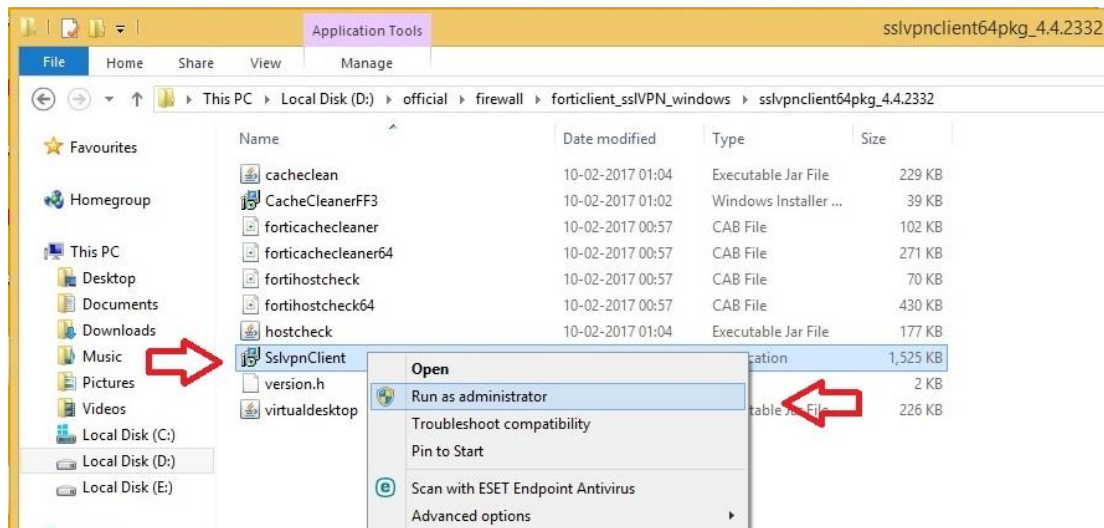


4. Click on **Install**. The installation of SSL VPN Client software shall start.

**5.** a) If you are installing a fresh Forticlient SSL VPN installer then you will get the following screen and click "**Close**".
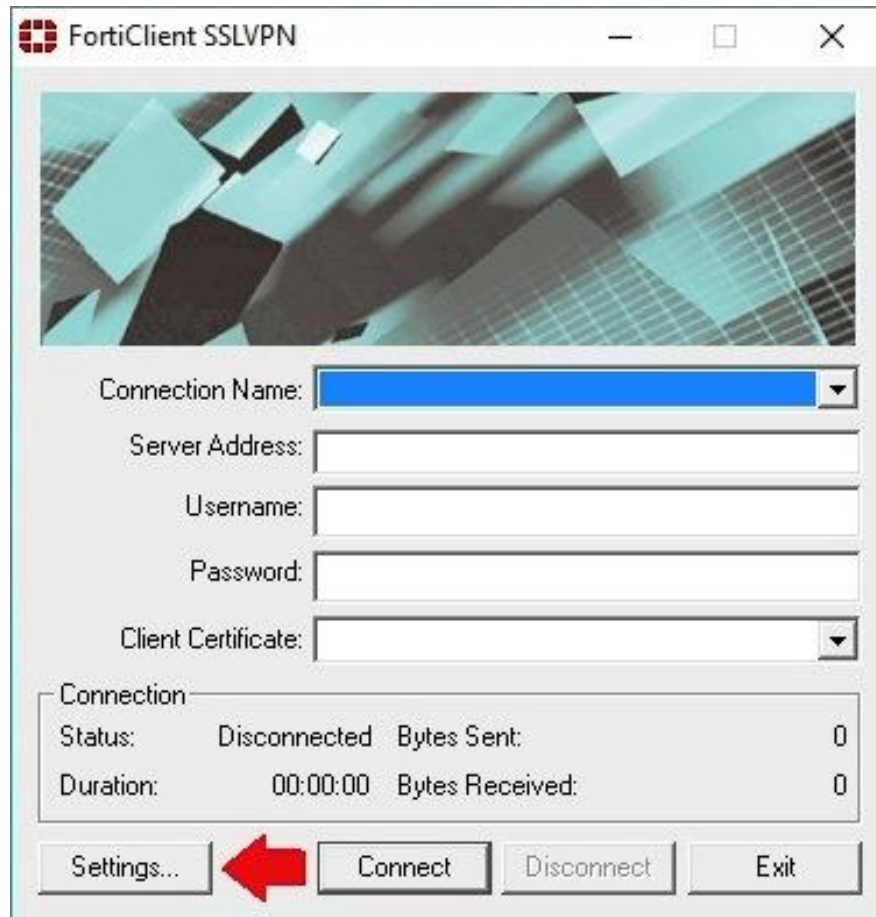
b) **OR** if you are upgrading from previous version then you may be asked to restart your device as follows and "**Yes**" button has to be clicked to reboot the device and thereby completing the installation.
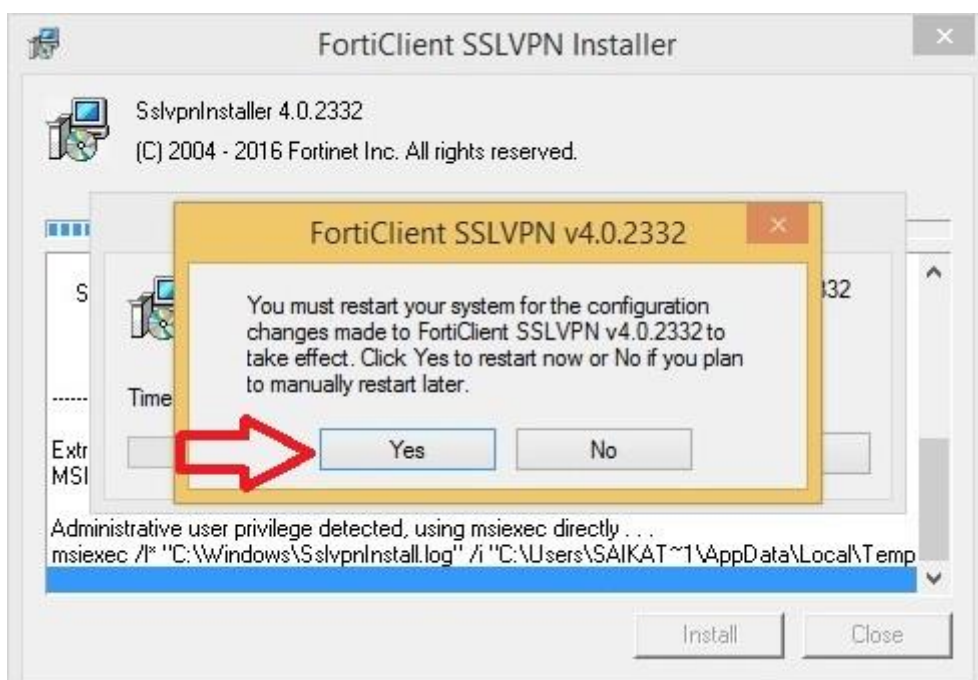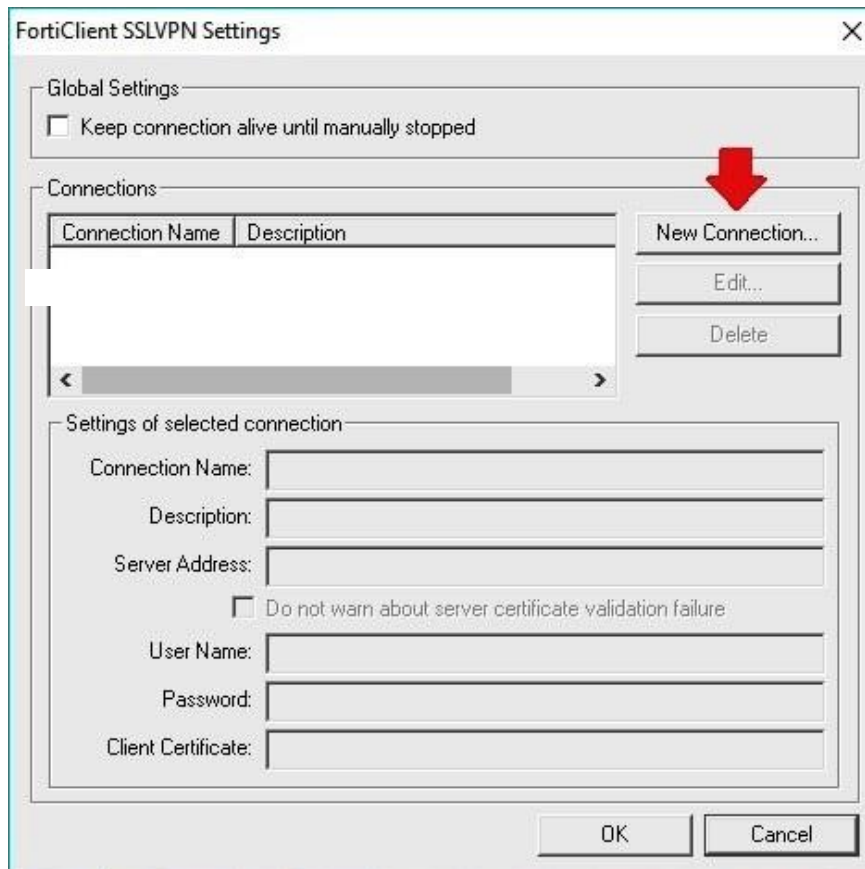


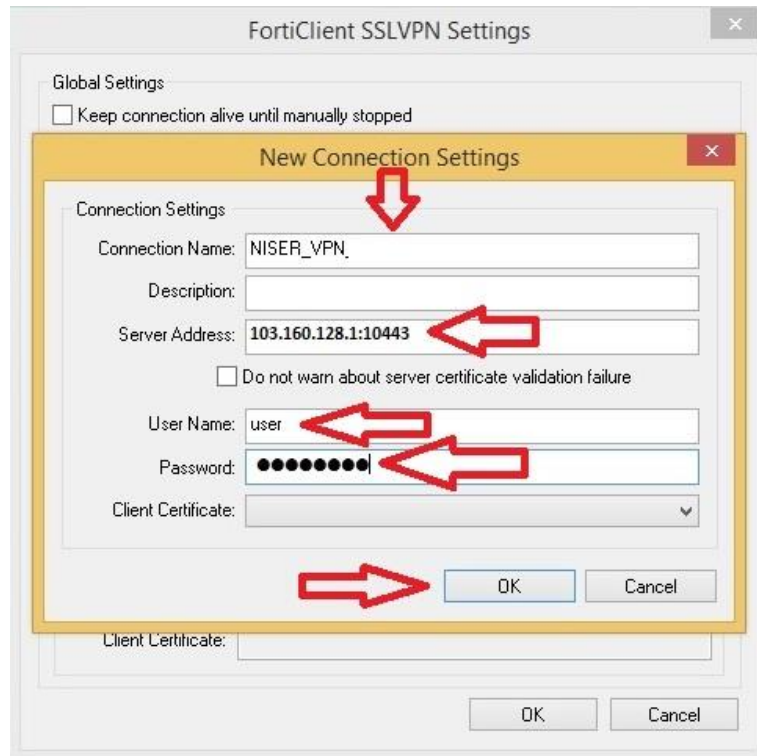6. Run the application [ Start >>Programmes >>**FortiClient SSL VPN** ]
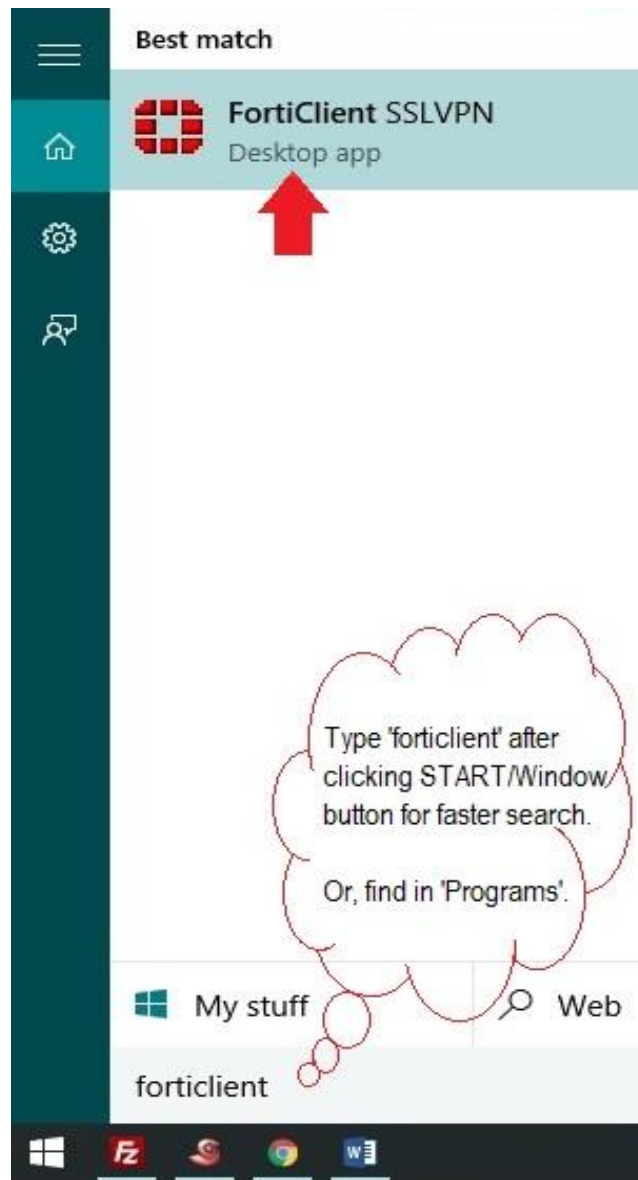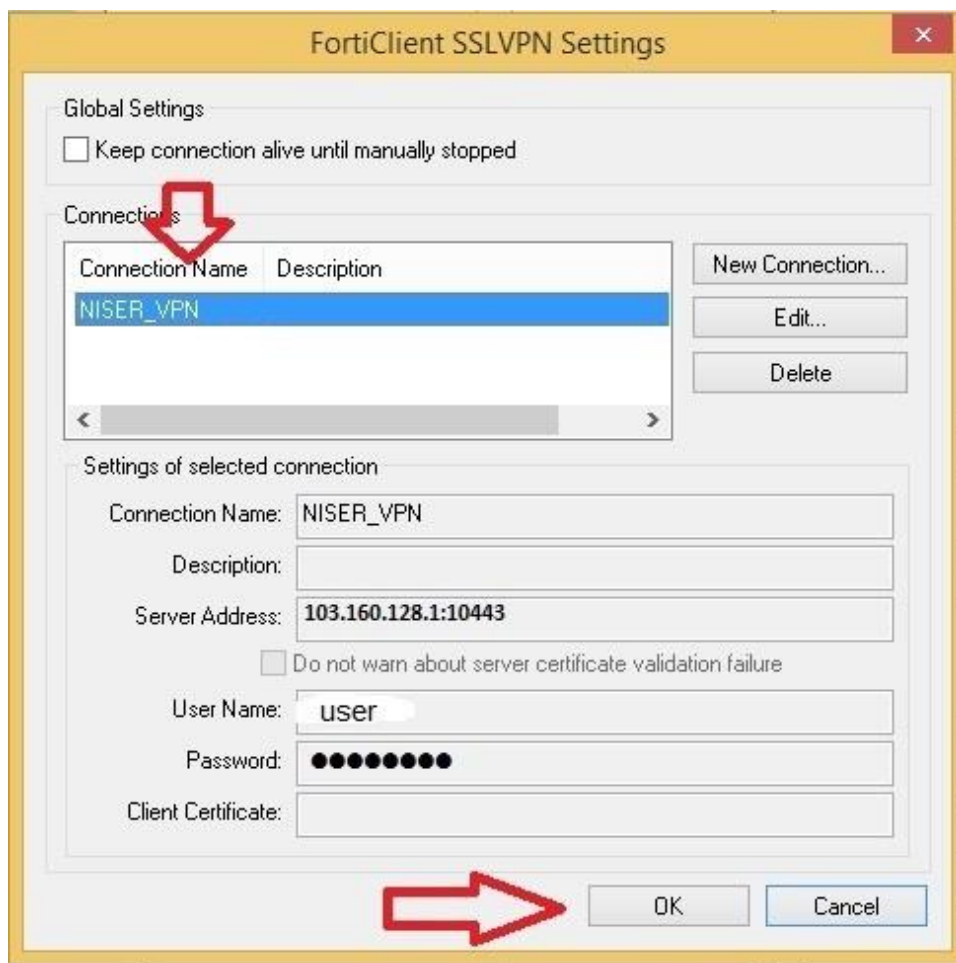
7.  Then Click on **Settings...**

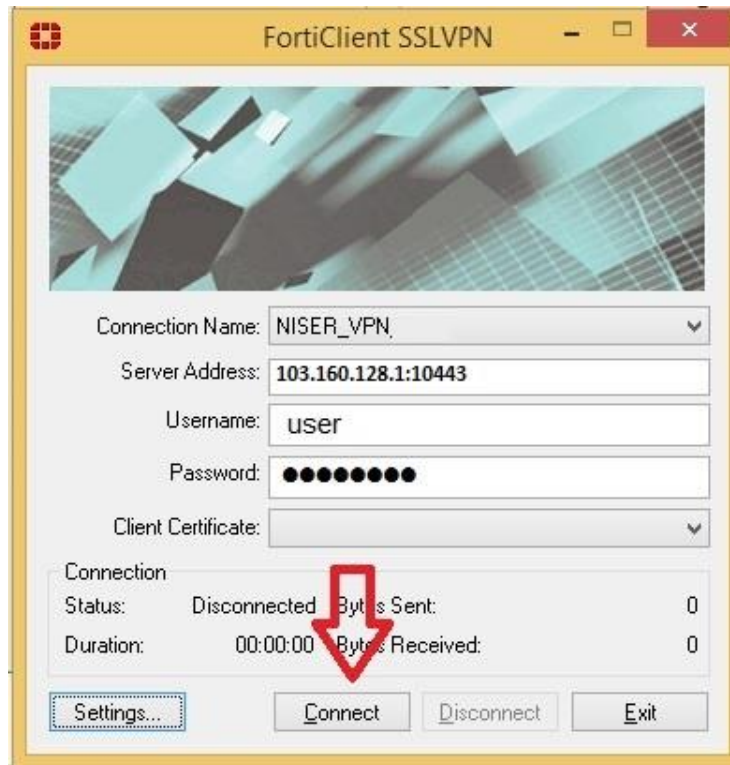8.  a) Then click on **New Connection…** and fill as shown below.



b) Give a name to the connection. Give the Server Address: **103.160.128.1** with port **10443**, give your **username** and **password** (your own WiFi access credentials or shell account credentials for home folder access) for SSL-VPN.

9. Then click on choose a 'connection', provide password and click **Connect**.

**10.** Click on **Yes** in Security Alert box.



**11.** Now you are connected. Status should show **"Connected".** "Bytes Sent" and "Bytes Received" should increase with time.