

RU-VPN Installation Instructions (Windows Vista and Windows 7)

An RU-VPN id allows authorized users to access Ryerson's Administrative Systems via the internet. RU-VPN utilizes a digital "certificate" that is installed on your PC together with a login password. RU-VPN provides further security by creating a Virtual Private Network (VPN), which is like a "secure tunnel" through which all communication between the user PC and Ryerson must pass. All data transmissions are "encrypted" so that they cannot be read while traveling across the Internet.

Hardware and Software Requirements

- Pentium PC running **Windows VISTA** or **Windows 7**
- 10 MB of free hard disk space
- An **RU-VPN certificate/ID** and **password**
- Access to the Internet
- A valid **my.ryerson username** and **password**

Note: If you do not meet or understand the above requirements, contact the CCS Help Desk for information before proceeding.

Instruction

Diagram

If you previously installed **OpenVPN** on your PC, please uninstall OpenVPN and reboot your system. You can use the OpenVPN, .p12 certificate you previously received from the CCS Helpdesk for RU-VPN.

Step 1 - Getting an RU-VPN ID and Password

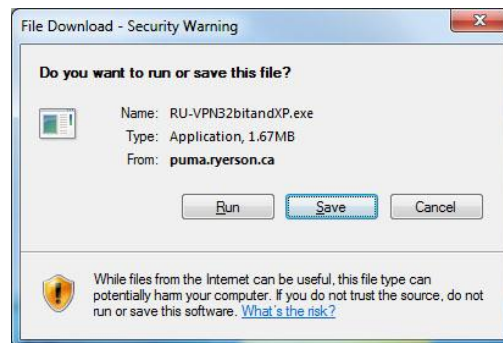
1. Once your request for RU-VPN has been processed by the CCS Help desk, you will receive a confirmation email containing an attachment **username.p12** (where username is your RU-VPN certificate/ID eg. jdoe.p12).
2. Save the file received from the CCS Help desk to a USB drive or on your local drive (on your local desktop). You will need this to install RU-VPN.

Instruction

Diagram

Step 2 - Downloading the RU-VPN software

1. From the CCS download web page <http://www.ryerson.ca/ccs/software/downloads/security/> find **RU-VPN** and click **Download for Windows Vista or Windows 7**. Check your Operating System before selecting the file to download.
2. At the **Connect to puma.ryerson.ca** screen, type in your my.ryerson username and password. Click **OK**.
3. At the **File Download** screen, click **Save**. Save this file to your desktop or your Local Disk (C:).



Step 3 – Installing RU-VPN

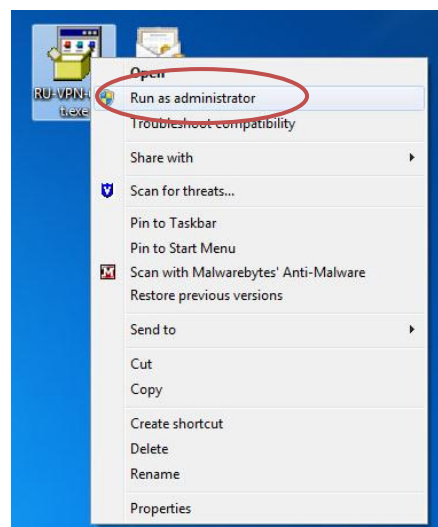
1. Before install, make sure that the **RU-VPN32bitandXP.exe** or **RU-VPN64bit.exe** file and your .p12 file are located on your desktop. Check your Operating System when selecting the exe file.



Note: If an old version of OpenVPN is already installed on the computer, please uninstall first and reboot before proceeding.

2. Locate the downloaded file. Right click **RU-VPN32bitandxp.exe** or **RU-VPN64bit.exe** and select **Run as administrator**.

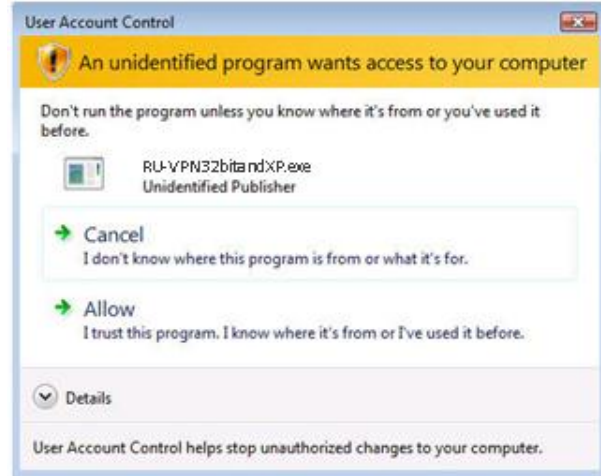
Note: Running as administrator is mandatory.



Instruction

Diagram

3. If a **Security Warning** screen appears, click **Allow (I Trust this program)** or **Run** to continue.



4. When prompted **Beginning RU-VPN installation**, click **Yes**.



5. If the TAP-Win32 screen displays with, **Would you like to install this device software?**, click **Install**.



Instruction

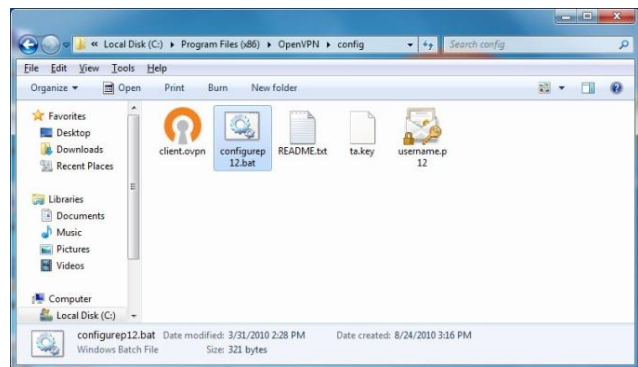
Diagram

- At the **Installation successful** screen, click **OK**.



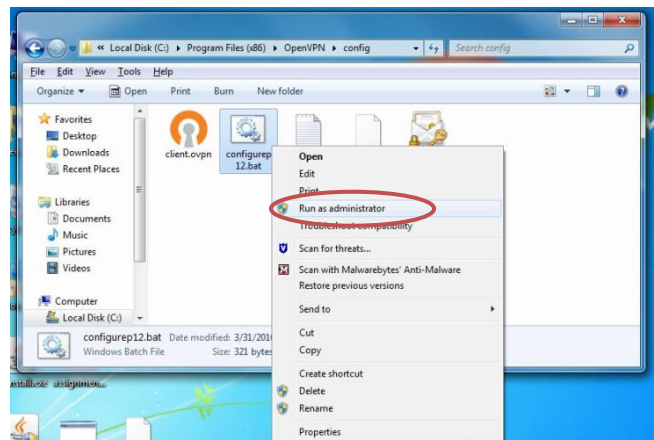
Installed RU-VPN before receiving p12 file?

- If you installed the RU-VPN software before you received your p12 file. Place the p12 on desktop.
- Using Windows Explorer go to:
 - For 32-bit Operating System:
c:\Program Files\OpenVPN\config
 - For 64-bit Operating System use:
c:\Program Files (x86)\OpenVPN\config



- Right click **configurep12.bat** and select **Run as Administrator**. This will copy p12 file into this directory

Note: Running as administrator is mandatory.



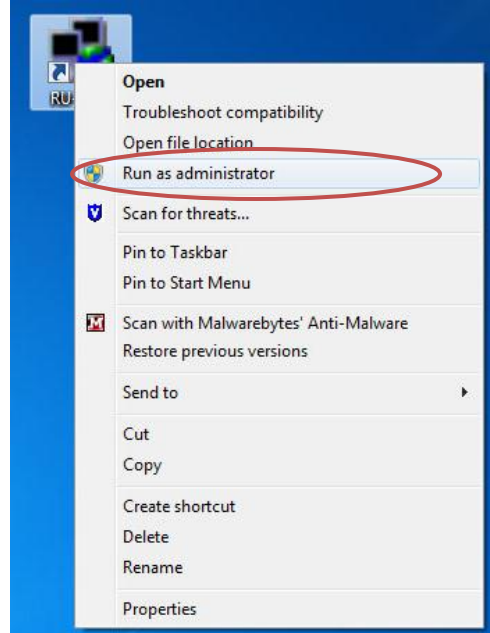
Instruction

Diagram

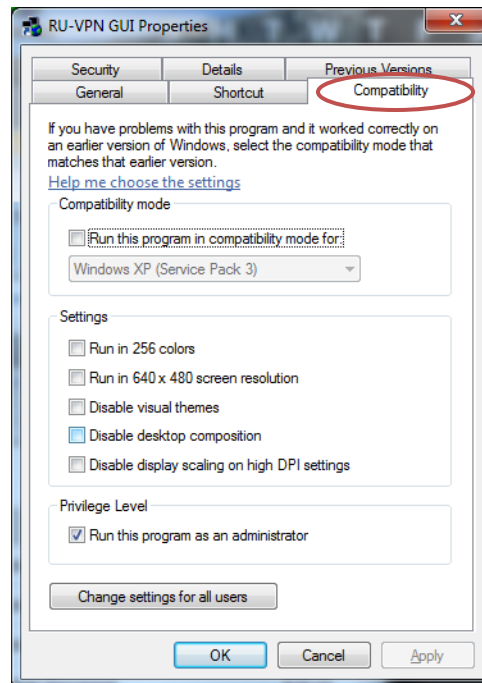
Step 4 - Running RU-VPN

1. If you are at home, make sure you are connected to the Internet. If you are at Ryerson, make sure you are connected to the Ryerson Internal Network, RIN.
2. From the desktop, find the **RU-VPN** icon. Right click on the icon and click **Run as Administrator**. A new icon will display in the taskbar at the bottom of your screen.

Note: Running as administrator is mandatory.



3. To setup the RU-VPN icon to always run as administrator; right click on the icon and click **Properties**. Select the **Compatibility** tab and check **Run this program as an administrator**. Click **OK**.



4. Double click the RU-VPN icon.



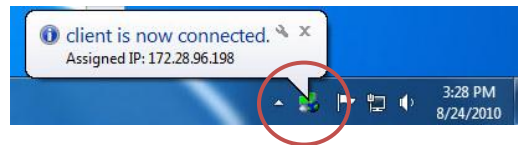
Instruction

Diagram

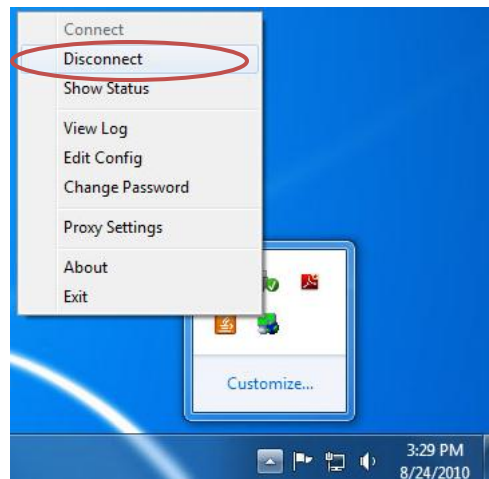
- At the OpenVPN window, you will be prompted for your password. This is the RU-VPN password that was provided by the CCS Help desk. Type in your password and click **OK**.



- After the password is entered, RU-VPN will begin to connect. The transactions between client and server will take up to 20 seconds. Once the process is completed the icon will turn green and you will see a message **Client is now connected**.



- When you are finished with RU-VPN you can disconnect by right clicking on the green icon. Click **Disconnect**.



This will end your connection to RU-VPN.

You can now delete from your desktop the username.p12 and RU-VPN.exe files.

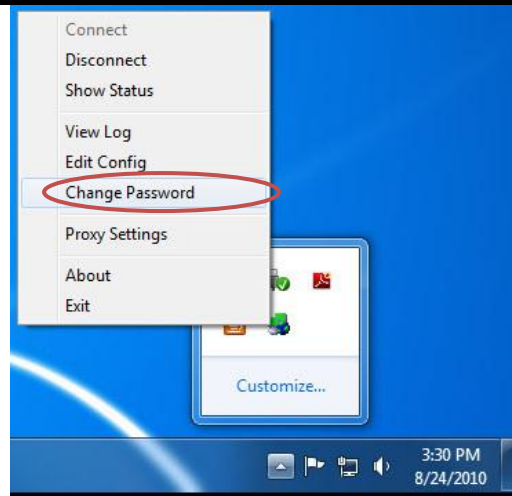
Instruction

Diagram

Changing RU-VPN Password

1. Although you have been assigned a temporary password, it is advisable to change that password to your own password now. Right click the RU-VPN icon, at the bottom of your screen and select change password.

Note: If RU-VPN is installed on more than one computer, please reset the password on all machines.



2. Enter your assigned temporary password in the **Old Password** area. Then enter your own new password in the **New Password** area and enter it again in the **Confirm New Password** area and click **OK**.

Note: The rules for the password are: minimum 8 characters in length must contain at least one numeric character and at least one capitalized letter.



IMPORTANT NOTE:

Ryerson is taking the issue of security very seriously. It is imperative that you disconnect your RU-VPN session when you are finish with accessing any of the Ryerson systems or when your computer will be left unattended and unsecured for some period of time during the day.

Leaving your active RU-VPN session open and unattended provides others with the opportunity for message forgery and other misuse, attributing them to you and creating an embarrassment to you and possibly compromising the integrity of Ryerson. This is especially important for people who share computers or have their computer located in a public area.

Some basic safeguards which can be used to aid data security are:

- Disconnect your RU-VPN session and logout from your PC during periods of absence. (e.g. coffee break, lunch, meetings etc.)
- Lock your office or room during periods of absence during normal working hours.
- Always use a screen saver password and a computer power-on password.