Ryerson University Computing & Communications Services

RU-VPN2 - GlobalProtect Installation for Windows

Use RU-VPN2 for a secure connection to Ryerson's Administrative system via the Internet. To use RU-VPN2, you will need to install and use client software called GlobalProtect which allows authorized user's access. It 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. GlobalProtect runs on your PC, laptop computer or mobile device, protecting you with the same security policies that protect the sensitive resources on Ryerson University network.

Requirements

- Access to the Internet
- A valid my.ryerson username and password
- VPN access enabled by the CCS Help Desk
- Two-factor authentication enabled for "applications that require two-factor authentication"

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

Download, Install and use RU-VPN2

Connect and Disable VPN Access

Download, Install and use RU-VPN2

Step 1.
Contact CCS to Request VPN Access

Before you download and install RU-VPN2, you will need to request VPN access by visiting https://my.ryerson.ca, navigate to the Self Service in your Personal Account where you can manage your VPN access and requests.

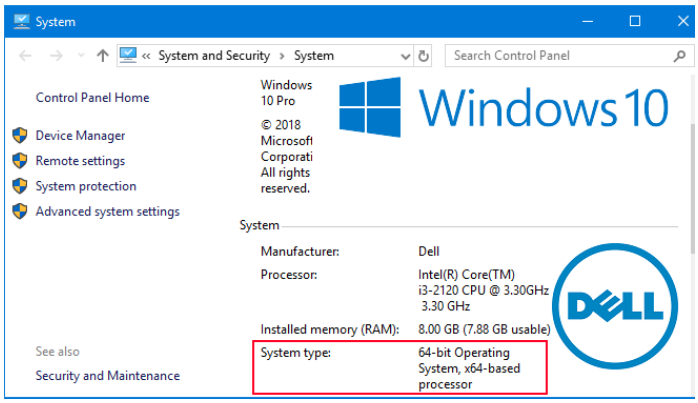
Step 2.
Setup Two-Factor Authentication

To use RU-VPN2, you will need to setup two-factor authentication. Please complete the instructions outlined on the two-factor authentication webpage before proceeding with the download and install of RU-VPN2, GlobalProtect.

Step 3.
Download the RU-VPN2, GlobalProtect Software Client

1. There are two versions of the RU-VPN2 client for Windows available for download. Please select either RU-VPN2 (64bit) or RU-VPN2 (32bit).

   Determine which version of Windows your computer is running and select the correct RU-VPN2 client software. You cannot install the 64-bit client on a 32-bit version of the Windows or vice versa.

   Check operating system in Windows 7
   Click on **Windows Control Panel** and click **System**. On the View basic information about your computer screen, the **System type** shows which version of Windows is installed.

   Check operating system in Windows 10

   Locate on your desktop, 

   icon. Right click and select **Properties**. Look for **System type** to see if you are running a 32-bit or 64-bit version of Windows.

   Select the appropriate software for your computer.
   - 32-bit Operation System, download RU-VPN2 32-bit.
   - 64-bit Operating System, download RU-VPN2 64-bit.

2. Save this file to your desktop or your Local Disk (C:).

Step 4.
Install RU-VPN2 using GlobalProtect

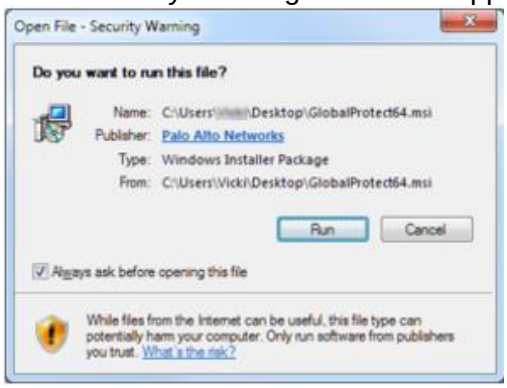
To use RU-VPN2, you will need to install and use the GlobalProtect client software. This is the software included in the files you downloaded.

1. Before install, make sure that the GlobalProtect.msi or GlobalProtect64.msi file is located on your desktop.

2. Locate the downloaded file. Install the GlobalProtect client by double-clicking on the file **GlobalProtect.msi** or **GlobalProtect64.msi** and select **Run as administrator**.

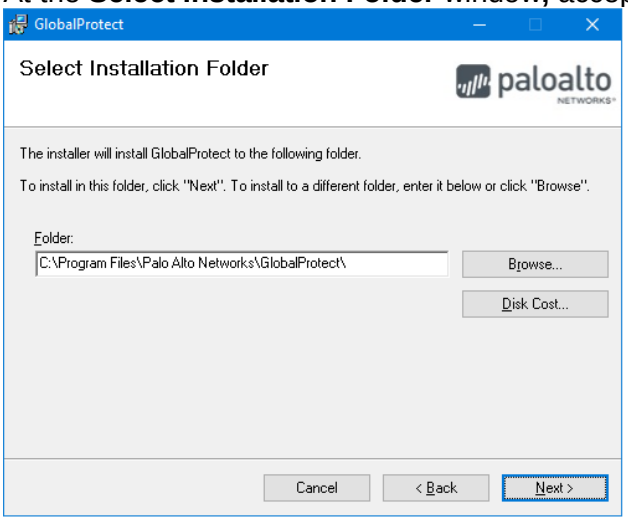
   Note: Running as administrator is mandatory. If you are not in the administrator group, please get help from your system administrator.

3. If the Security Warning screen will appear, click **Run** to continue.

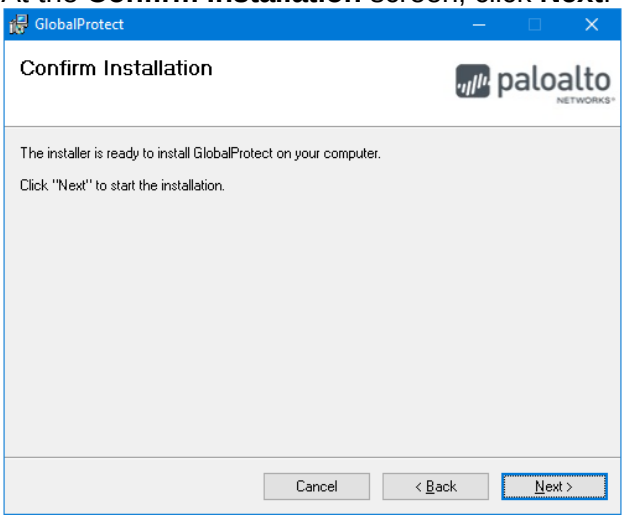


4. At the **Welcome to the GlobalProtect Setup Wizard** screen, click **Next.**

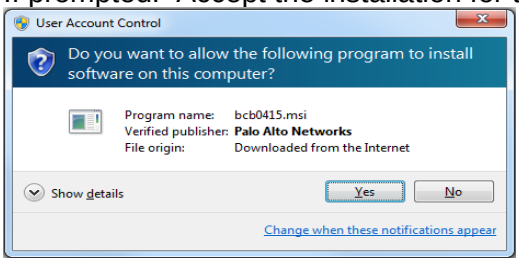
5. At the **Select Installation Folder** window**,** accept the folder and click **Next**.



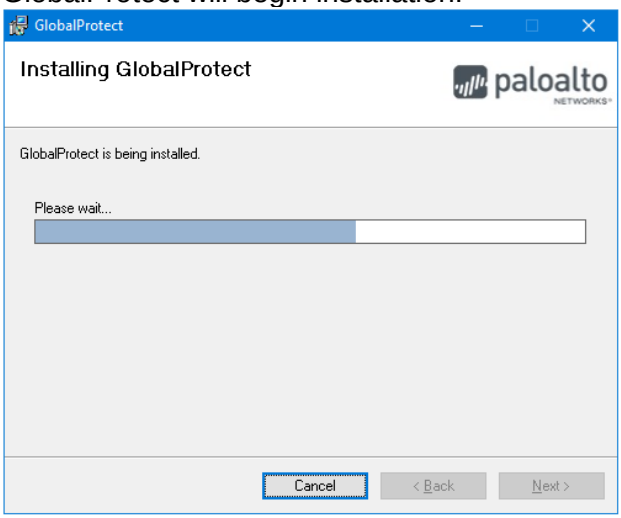
6. At the **Confirm Installation** screen, click **Next**.



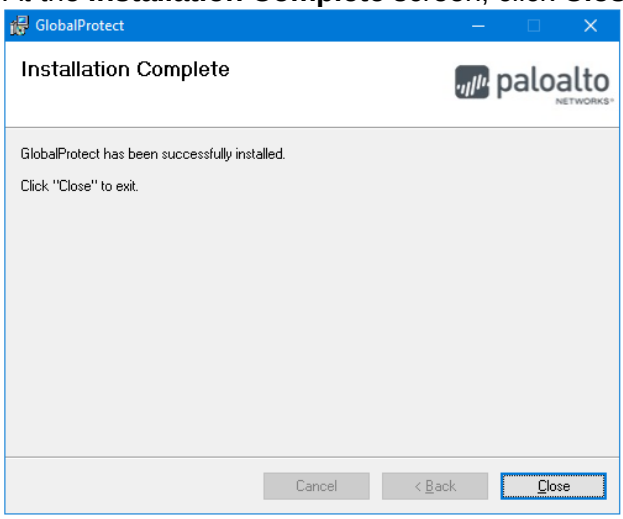
7. If prompted. Accept the installation for the Palo Alto Networks software, click **Yes**.



8. GlobalProtect will begin installation.



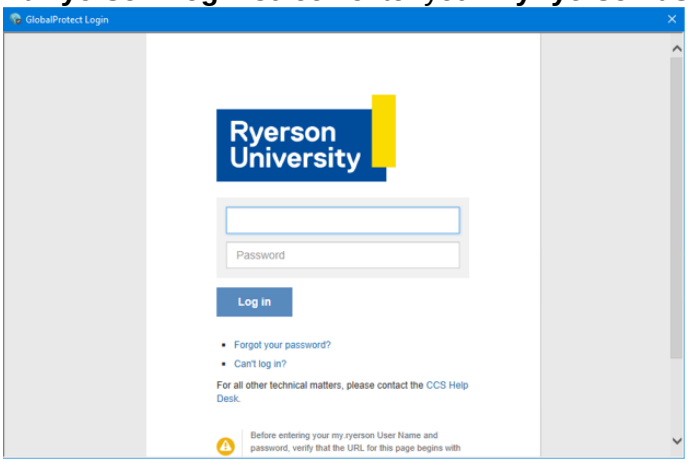
9. At the **Installation Complete** screen, click **Close** to end the installation.



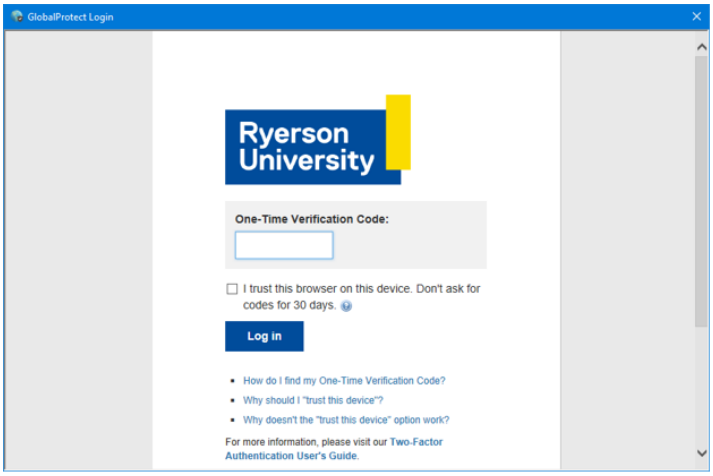
Step 5.
Configure and Run GlobalProtect for the first time

1. After installation, please wait and GlobalProtect will open a Welcome window. At the **Welcome to GlobalProtect** window enter the portal address as **net.ryerson.ca** and click **Connect**.

2. At **Ryerson Login** screen enter your **my.ryerson username** and **password.** Click **Log in**.

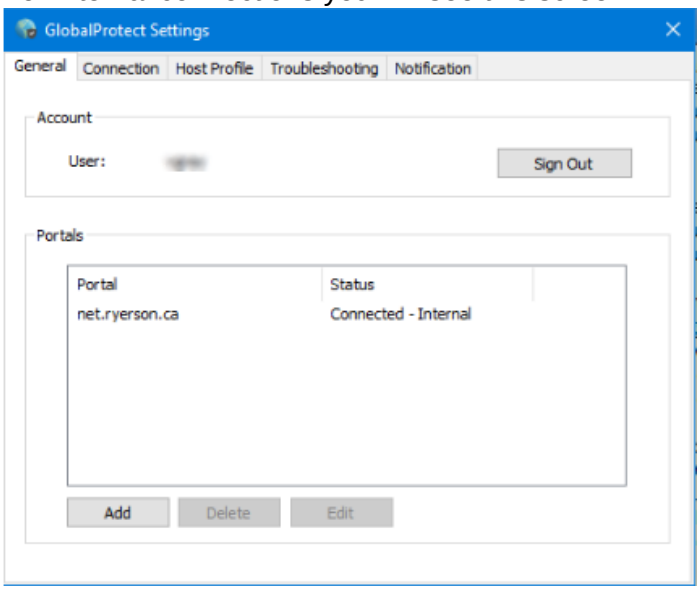


3. Next you will be prompted for your Two-Factor **Verification Code**. You can select the checkbox to trust this browser for 30 days, so that you will not be prompted during that time period.

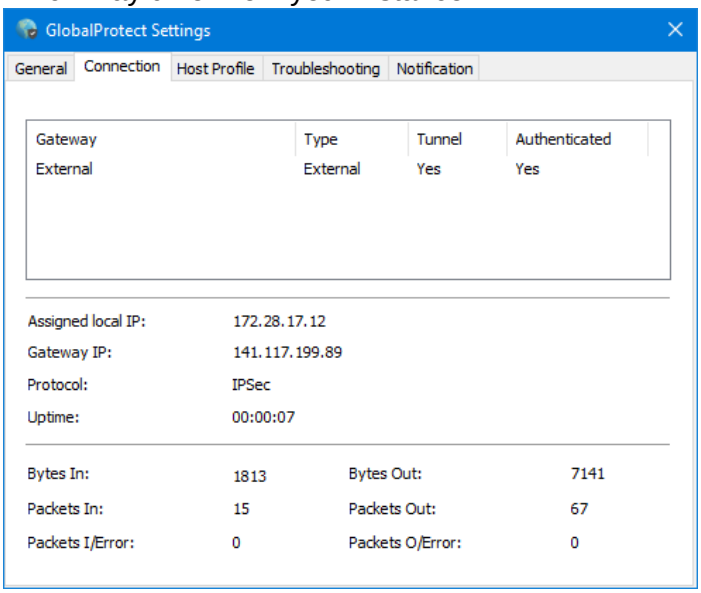


4. A Global Protect **Connected** window displays when connection is made. You can now access sites that require VPN.

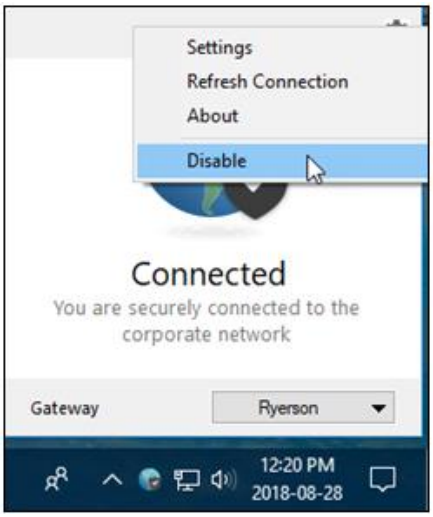
For internal connections you will see this screen:



5. For external connections, a detailed view is provided that includes the IP and statistics information which may differ from your instance:



6. When you are finished using GlobalProtect, click on the GlobalProtect icon found on your taskbar. Next click on the setting gear at the top right of the screen. Select **Disable**. This will end your connection to VPN.



7. You can now delete from your desktop the GlobalProtect.msi or GlobalProtect64.msi file.

Step 6.
Uninstall old RU-VPN

Remove old RU-VPN2, GlobalProtect

If you need to remove an old version of GlobalProtect, open the Windows Control Panel or Settings panel.

1. For Windows 7, click on **Programs and Features**.
2. For Windows 8.x, click on **Uninstall A Program**.
3. For Windows 10, click on **Apps.**

Select **GlobalProtect.** Click **Uninstall**.

Remove OpenVPN

Once you have the new RU-VPN2 up and running you should uninstall the old RU-VPN. Open the Windows Control Panel or Settings panel.

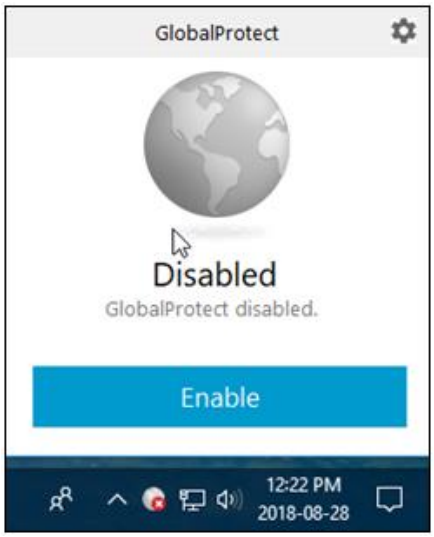
1. For Windows 7, click on **Programs and Features**.
2. For Windows 8.x, click on **Uninstall A Program**.
3. For Windows 10, click on **Apps.**

Select **OpenVPN**. Click **Uninstall**.

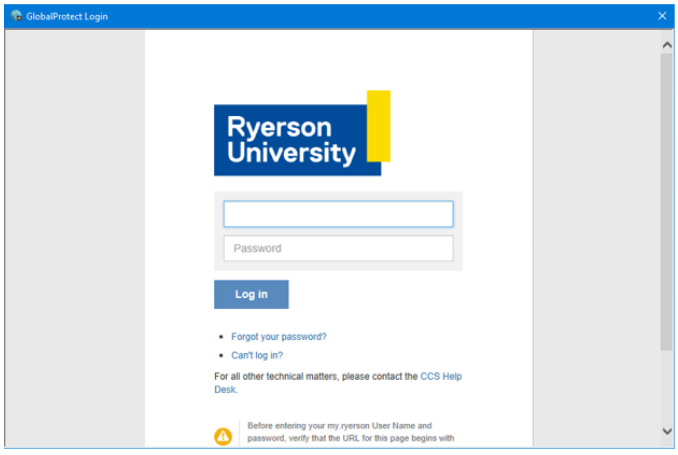
Connect and Disable VPN Access

Connect to Ryerson using GlobalProtect

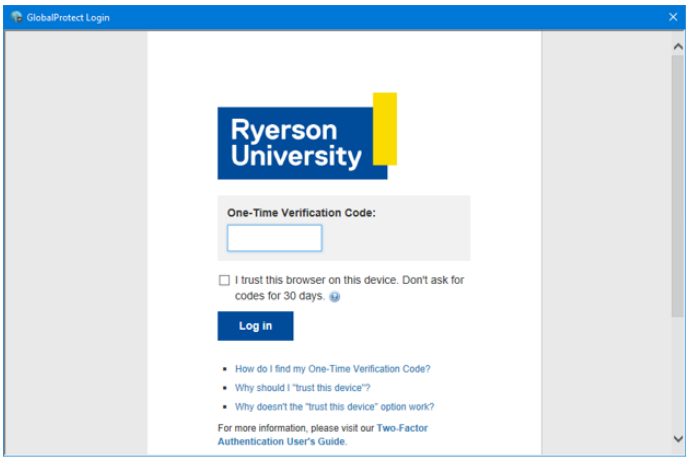
1. Click on the GlobalProtect icon found on your taskbar. Select **Enable**.



2. At the **Ryerson Login** screen enter your **my.ryerson, username** and **password**. Click **Log in**.



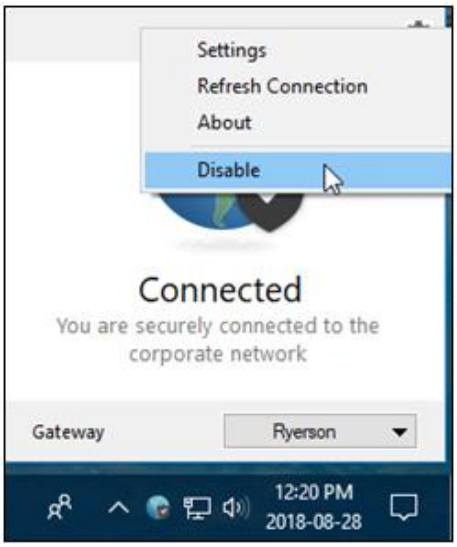
3. Next, you will be asked for your Two-Factor **Verification Code**. You can select the checkbox to trust this browser for 30 days, so that you will not be prompted during that time period.



4. A Global Protect **Connected** window displays when connection is made. You can now access sites that require VPN.

Disable GlobalProtect

Click on the GlobalProtect icon found on your taskbar. Click on the settings gear found at the top right of the GlobalProtect screen and select **Disable**. This will end your connection to VPN.



FAQ

How can I tell that I am definitely connected to the GlobalProtect VPN?

The VPN status icon, that displays on the taskbar, at the bottom right of the screen, will indicate the current connection state:

-  GlobalProtect is connected successfully.
-  GlobalProtect is not connected, either because authentication failed or you chose to disable your connection.

How do I uninstall RU-VPN on Windows computer?

Remove old RU-VPN2, GlobalProtect

Steps to uninstall RU-VPN:

1. Open the Windows Control Panel.
2. For Windows 7, click on **Programs and Features.**
3. For Windows 8.x, click on **Uninstall A Program.**
4. For Windows 10, click on **Apps.**

Select **GlobalProtect**. Click **Uninstall**.

Remove OpenVPN

If you need to uninstall the old OpenVPN, open the Windows Control Panel or the Settings Panel.

1. For Windows 7, click on **Programs and Features**.
2. For Windows 8.x, click on **Uninstall A Program**.
3. For Windows 10, click on **Apps.**

Select **OpenVPN**. Click **Uninstall**.

The GlobalProtect client will not install and is asking for Administrator password?

If your computer is a Ryerson computer and supported by CCS, please contact the CCS Help Desk at help@ryerson.ca or extension 556806. Otherwise, you must contact the person who has administrator rights on the computer.

When I try and make a VPN connection, I keep being taken back to the username/password or verification code screen?

This may be caused by entering an incorrect or invalid my.ryerson username, password or verification code. Make sure you are entering your my.ryerson username and password. Remember that usernames and passwords are case-sensitive. If you are able to log on http://my.ryerson.ca using your my.ryerson username and password, the problem may be your two-factor authentication setup. Try resetting your two-factor authentication by revoking your two-factor authentication and then reactivating two-factor authentication.

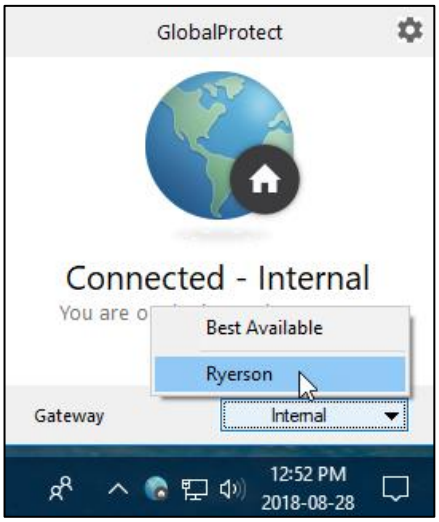
How do I stop getting prompted to enter a verification code, username or password when I do not need to connect to GlobalProtect?

Follow the Disable GlobalProctect instructions.

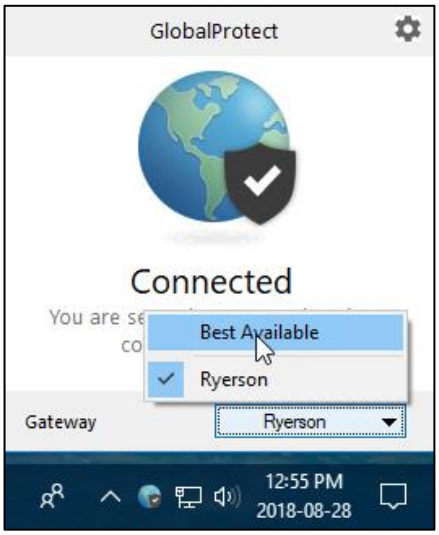
Connecting from an Administrative network, how do I access my application?

If you are connecting from an Administrative network, not Academic or from off campus or RU-Secure, and require full VPN to access your application please do the following:

1. Click on the GlobalProtect icon found on your taskbar. Next click on the Gateway dropdown selection and choose **Ryerson**. You will now have full VPN access.

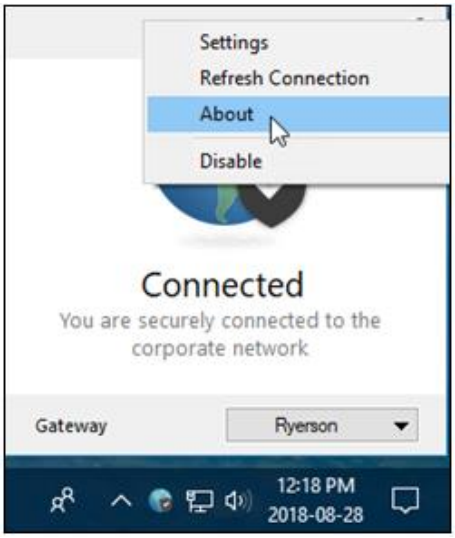


2. When you no longer need access to your application that required full VPN, you can disconnect. Click on the GlobalProtect icon found on your taskbar. Next click on the Gateway dropdown selection and choose **Best Available**.



How do I get the GlobalProtect client version information?

Find the GlobalProtect icon in the taskbar. Click the Settings gear at the top right of the screen and select **About**.



How does a new version of the GlobalProtect client get installed?

GlobalProtect is pre-set to check if there are new versions available. Once you have installed GlobalProtect and establish a VPN connection, the software will download the new version and put it in a queue. It will install by itself. You may see a message, "GlobalProtect agent upgrade is in progress. Please wait, application will restart once the upgrade is complete."

How do I get help with other GlobalProtect problems?

If the information here did not help to resolve your problem, you can contact the CCS Help Desk at help@ryerson.ca. Please include details of:

- Your operating system version, e.g. Windows 7 Professional with SP1, Mac OS X 10.10.2 etc. Your GlobalProtect Client version
- Your ISP (Internet Service Provider)
- Your Ryerson email address

Important Note

Ryerson is taking the issue of security very seriously. It is imperative that you disconnect your 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 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 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.