INSTRUCTIONS FOR CONFIGURING VPN SETTINGS FOR WINDOWS OPERATING SYSTEM DEVICES

Written by Area Sistemi Informativi
1. Requirements

This document explains how to configure a Microsoft Windows machine to access the University VPN data network.

The user device must meet the following requirements:

- Microsoft Window operating system currently supported (Windows 8.1 or higher);
- Access with system administrator roles.

Important notes about using VPN connection:

- VPN connection is reserved for computers that are located outside the University network (VPN connection assigns an IP address belonging to the Bicocca network);
- the use of the University VPN connection, the Bicocca network, and the Italian University and Research Network, are subject to acceptance of the GARR-AUP policies (available at the following link).

2. Settings

Install the Palo Alto GlobalProtect software (agent) in your operating system:

- Access, with your university credentials, the following link
- Download the specific agent for your operating system
- Install the downloaded package (GlobalProtect64.msi) by clicking on the Run button
- For devices with Windows 10 operating system, a screen will appear in which Microsoft recommends installing this app from the Microsoft Store to protect your PC (NOT RECOMMENDED); click on Continue to Install outside the Store
To complete the installation, click on the **Next** button and accepting all the installation confirmation requests that are proposed.

When finished, click **Close**.
Configure the University VPN connection:

- Enter in the form portal ravpn.unimib.it e click on the Connect button

Once redirected to the University authentication system, change the settings as indicated, inserting your credentials (the complete e-mail address and the relative password)
Click on Sign in button and authentication will be performed.

The VPN connection will be correctly established.