FortiClient 7.2.3 Installation – macOS Ventura and higher

Installation Instructions

- Go to www.concordia.ca
- Login to your My CU Account
- Go to Apps & software VPN client (FortiClient) to
- download the installer file.
- Double click on the downloaded dmg file to mount the installer



FortiClient .dmg file

• Double click on the FortiClient icon.



• Double click on installer.mpkg



• Click continue

• • •	🥪 Install FortiClient	۵
	Welcome to the FortiClient Installer	
 Introduction License Destination Select Installation Type Installation Summary 	FortiClient for macOS is a unified security agent for computers that integrates antivirus, SSL and IPsec VPN remote access, web filtering, application firewall and vulnerability scan into a single software package. FortiClient for macOS has a user-friendly interface that allows for quickly setting up protection for your computer.	
	Go Back Continue	

Read the Software License Agreement and click continue and then "Agree"



Click on install to begin the installation

	🥪 Install FortiClient	E
	Standard Install on "Macintosh HD"	
 Introduction License Destination Select Installation Type Installation Summary 	This will take 295 MB of space on your computer. Click Install to perform a standard installation of this software for all users of this computer. All users of this computer will be able to use this software.	

• macOS will prompt you for your password, enter it and click 'Install Software'

	R
	Installer
In	staller is trying to install new software.
	Enter your password to allow this.
0	lasaword .
0	Install Software
1	Cancel

• During the installation, you will be prompted to provide your password again so that FortiClientAgent can make changes to the System Trust Certificate settings. Immediately afterwards, macos security will also prompt for your password

FortiClientAgent	security
You are making changes to the System Certificate Trust Settings.	You are making changes to your Certificate Trust Settings.
Enter your password to allow this.	Enter your password to allow this.
	Doemanie
Password	Password
Update Settings	Update Settings
Cancel	Cancel

• Click "Allow" for FortiTray



- MacOS Ventura, click on open system settings to Allow "FortiClientNetwork".
- For older macOS versions please use "security preferences".



• Open system settings to Allow "FortiTray".



- Click on Details to allow the extensions.
- Enter your password and click on Modify Settings.



• Enable extensions

System software from the following developers was updated and the system needs to be restarted before it can be used.

FortiClientNetwork	\longrightarrow
FortiTray	\longrightarrow
	Cancel OK

Click OK and then enter your password and click on Modify Settings

• Enable Full Disk Access.



• Click close to complete the software installation



Configuring the VPN Connection and Licensing the Software

Click on "Remote Access" on the left side of the FortiClient window. In here, select 1. "Configure VPN"



- Configure the settings on this screen as below:
 - **Connection Name: Concordia VPN** •
 - Remote Gateway: vpn.concordia.ca •
 - Customize port: 443 ٠
 - Enable Single Sign On (SSO) for VPN Tunnel •

	Edit VPN Connection		×	
		VPN	SSE-VPN IPsec VPN XML	
		Connection Name	Concordia VPN]
	NETNAME	Description]
**	ZERO TRUST TELEMETRY	Remote Gateway	vpn.concordia.ca	×
<u> </u>	REMOTE ACCESS		Add Remote Gateway Customize port 443	
0	Notifications	Single Sign On Settings	 Enable Single Sign On (SSO) for VPN Tunnel Use external browser as user-agent for saml user auth 	entication
₽	Settings	Client Certificate	Enable auto-login with Azure Active Directory None	
۲	About		Enable Dual-stack IPv4/IPv6 address	
		[Cancel Save	

Afterwards, click Save.

3. Once the connection has been created, click on "Connect" and provide your credentials to establish a connection to the VPN

NETNAME	VPN Connected	UNLICENSED
X ZERO TRUST TELEMETRY	<u> </u>	🐔
Notifications	VPN N	ame Concordia VPN
	IP Add	ress 172.16.250.137
C Settings	Userna	me firstname.lastname@concordia.ca
	Dura	tion 00:00:11
About	Bytes Recei	ved 1.56 KB
	Bytes	Sent 6.75 KB
	C	Disconnect

4. Once successfully connected, click on the "Zero Trust Telemetry" tab and type in the EMS server address then click connect.

• Server Address: ems.concordia.ca

	FortiClient - Disconnected Zero Trust Fabric Agent
NETNAME	Register with Zero Trust Fabric Enter Server address or Invitation code: ems.concordia.ca Connect = X
REMOTE ACCESS Notifications Settings	
About	Disconnect

Once you have connected, you will see "Centrally Managed by EMS".
 *Please allow up to 60 seconds for the status to change



Once you have completed the above steps, you will not need to follow them again unless you are installing the VPN on another device.

Should you click "Disconnect" on the Zero Trust Telemetry tab, you will have to manually type in the EMS server address to properly connect again. Please be aware that connection to the EMS server is only possible while on the campus network or when currently connected to the VPN in the "Remote Access" tab.