

ESU VPN SETUP AND PROCESS

FOR OFFICIAL USE ONLY

TABLE OF CONTENTS

Document Scope:	4
In-Scope:	4
FortiClient Configuration:	4
Single Sign-On (SSO) Configuration:	4
Uninstallation and Re-installation:	4
Out-of-Scope:	4
Advanced Administrative Tasks:	4
Detailed Technical Explanations:	4
Network or Security Policy Adjustments:	4
1. FortiClient Access Authorization:	5
1.1 Introduction:	5
1.2 Role-Based Access Request:	5
Discuss with Your Supervisor:	5
Supervisor Role Evaluation:	5
Supervisor Submits Helpdesk Ticket:	5
1.3 Helpdesk Processing:	5
Ticket Resolution Timeframe:	5
Communication from Helpdesk:	5
2. FortiClient Windows Installation	6
2.1 Prerequisites:	6
2.2 Installation Steps:	6
Download FortiClient:	6
2.3 Verification:	9
2.4 Conclusion:	10
3. FortiClient Configuration:	10
3.1 First Time Operation & Configuration:	10
3.2 Re-Configuring the VPN:	12
3.3 Connecting to Campus:	14
4. Uninstalling FortiClient:	16

4.1 Prerequisites: 16

4.2 Download & Run Revo Uninstaller Portable:..... 16

4.3 Summary: 22

5. Technical Resources:..... 22

FOR OFFICIAL USE ONLY

DOCUMENT SCOPE:

This document is intended for end-users seeking guidance on the configuration of FortiClient, a virtual private network client used to connect to university network(s). The scope is limited to the basis of configuration, un-installation, installation, and notation of process to gain access.

IN-SCOPE:

FORTICLIENT CONFIGURATION:

- Step-by-step guidance on installing FortiClient on your device.
- Basic configuration steps tailored for end-users.
- Instructions for connecting to Fortinet gateways securely.

SINGLE SIGN-ON (SSO) CONFIGURATION:

- Enabling Single Sign-On (SSO) within FortiClient for a simplified login experience.

UNINSTALLATION AND RE-INSTALLATION:

- User-friendly steps for uninstalling FortiClient if necessary.
- Guidance on safely reinstalling the application.

OUT-OF-SCOPE:

ADVANCED ADMINISTRATIVE TASKS:

- Configuration or administration of policies beyond end-user capabilities.
- In-depth troubleshooting that requires administrative access.

DETAILED TECHNICAL EXPLANATIONS:

- Elaborate technical details or backend functionalities.

NETWORK OR SECURITY POLICY ADJUSTMENTS:

- Modifying network configurations or security policies beyond the FortiClient application.

1. FORTICLIENT ACCESS AUTHORIZATION:

1.1 INTRODUCTION:

Before proceeding with the installation of FortiClient, it is crucial to obtain access authorization through the request process. This ensures that access aligns with your job duties and responsibilities within the university.

1.2 ROLE-BASED ACCESS REQUEST:

DISCUSS WITH YOUR SUPERVISOR:

- Engage in a conversation with your immediate supervisor to express the need for VPN access based on your role responsibilities.

SUPERVISOR ROLE EVALUATION:

- Your supervisor, understanding your role requirements, will assess whether FortiClient access is necessary for your tasks.

SUPERVISOR SUBMITS HELPDESK TICKET:

- If access is deemed necessary, your supervisor will submit a formal request to the IT helpdesk.
- This request will be in the form of a helpdesk ticket, providing all relevant details.

1.3 HELPDESK PROCESSING:

- The IT helpdesk will review the submitted ticket, verifying the necessity of FortiClient access based on your submittal.

TICKET RESOLUTION TIMEFRAME:

- Understand that all access requests are managed through a ticketing system to ensure accountability.
- Reaching out personally to IT personnel may not guarantee a speedy response. The established ticketing system ensures requests are tracked, prioritized, and addressed within a defined timeframe.

COMMUNICATION FROM HELPDESK:

- The IT helpdesk will communicate the status of your access request through the established channels, typically via email, telephone, or instant messaging.

2. FORTICLIENT WINDOWS INSTALLATION

2.1 PREREQUISITES:

Before you begin the installation, ensure that your system meets the following prerequisites:

OPERATING SYSTEM: Windows 10, Windows 11 (MAC OS Coming Soon)

INTERNET CONNECTION: Required for downloading FortiClient.

ADMINISTRATIVE PRIVILEGES: You need administrative rights on your device.

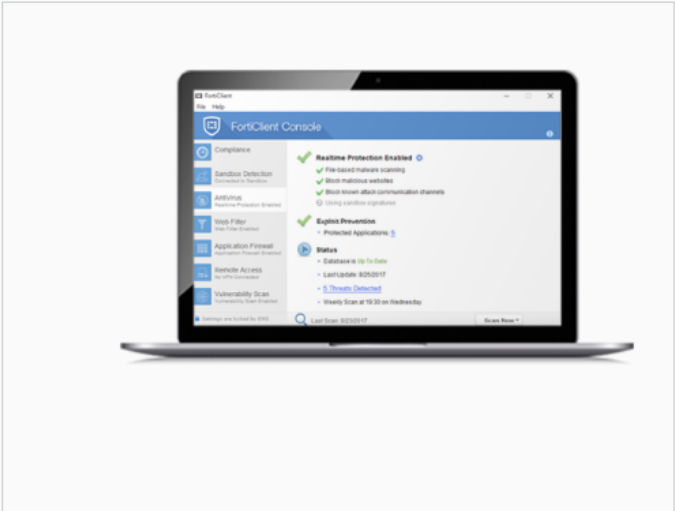
INTUNE MANAGED LAPTOPS: If your device is managed by Microsoft Intune, please reference step 2.4.

2.2 INSTALLATION STEPS:

DOWNLOAD FORTICLIENT:

- Visit the official Fortinet website or use the [provided link](#).
- Click on “FortiClient VPN only” as other installable versions aren't compatible.

FortiClient

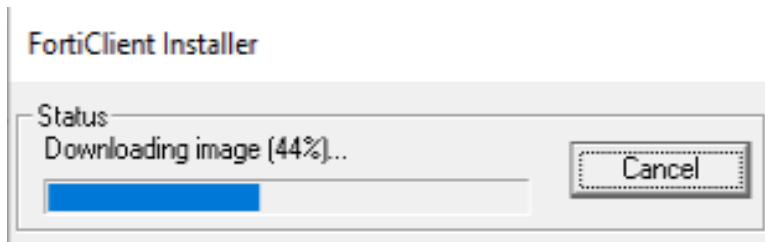


FortiClient 7.2
ZTNA Edition
EPP/APT Edition
FortiClient EMS
FortiClient VPN only

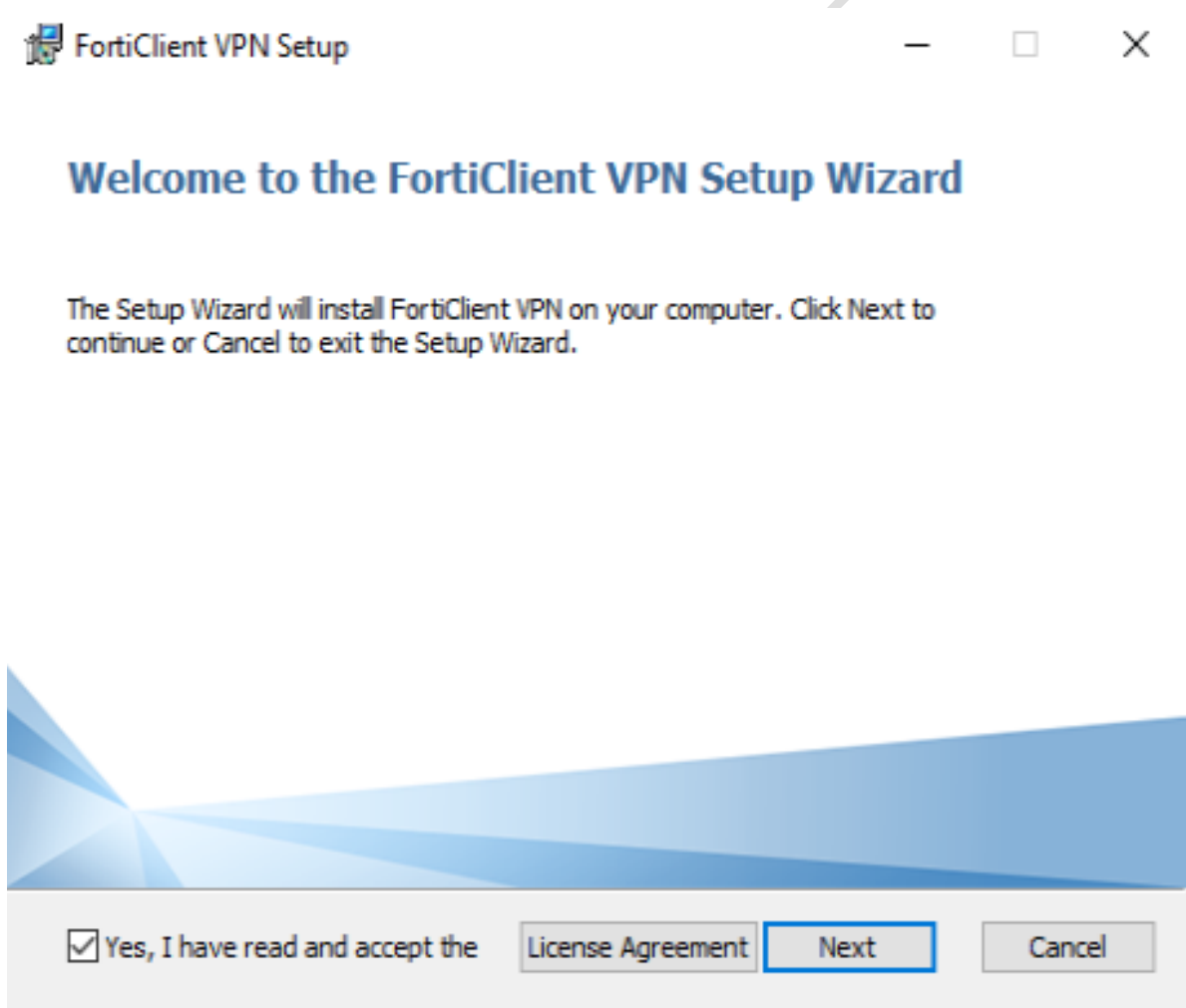
Click to See Larger Image

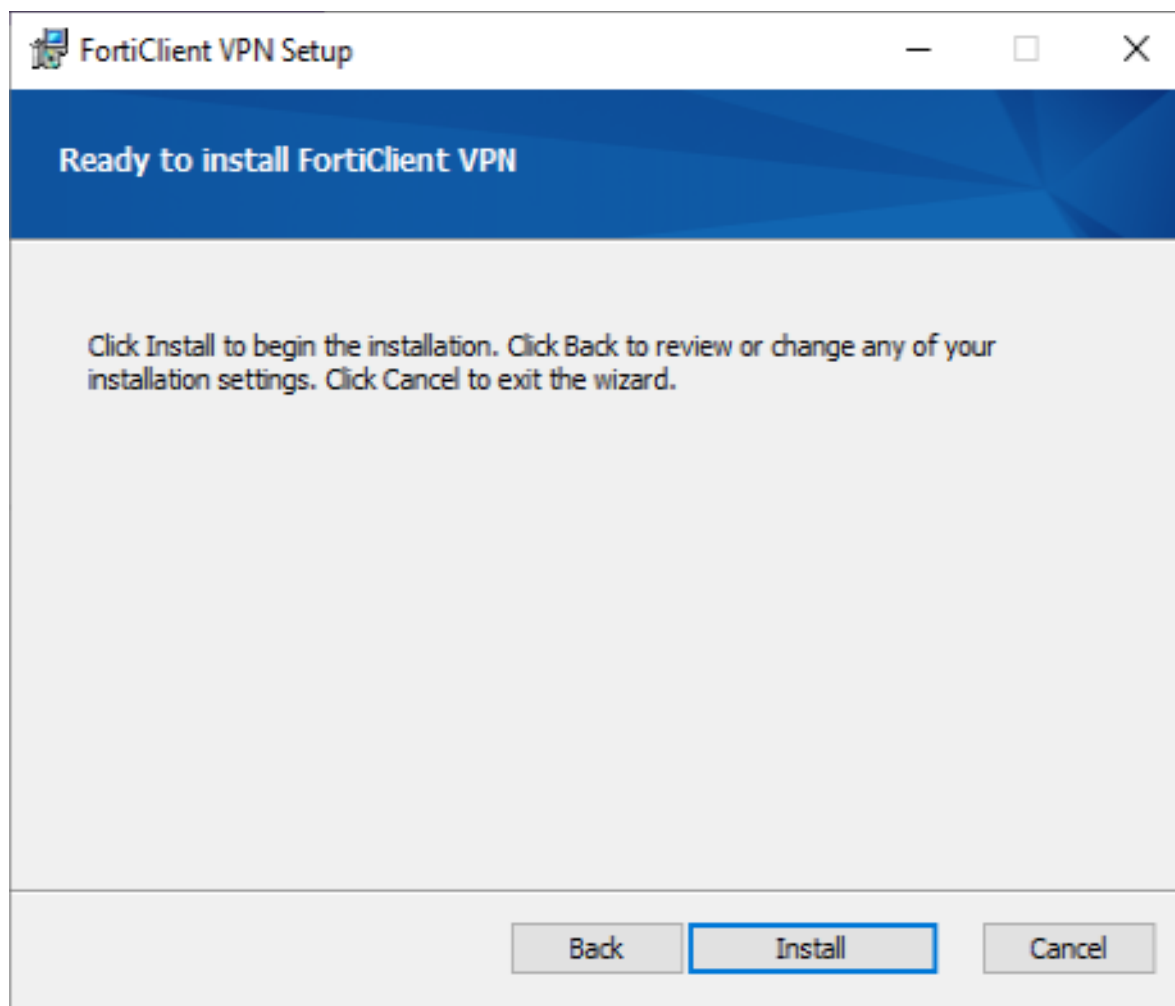
- Select the “Download VPN for Windows.”

- Run the Installer and allow it to download and un-pack.



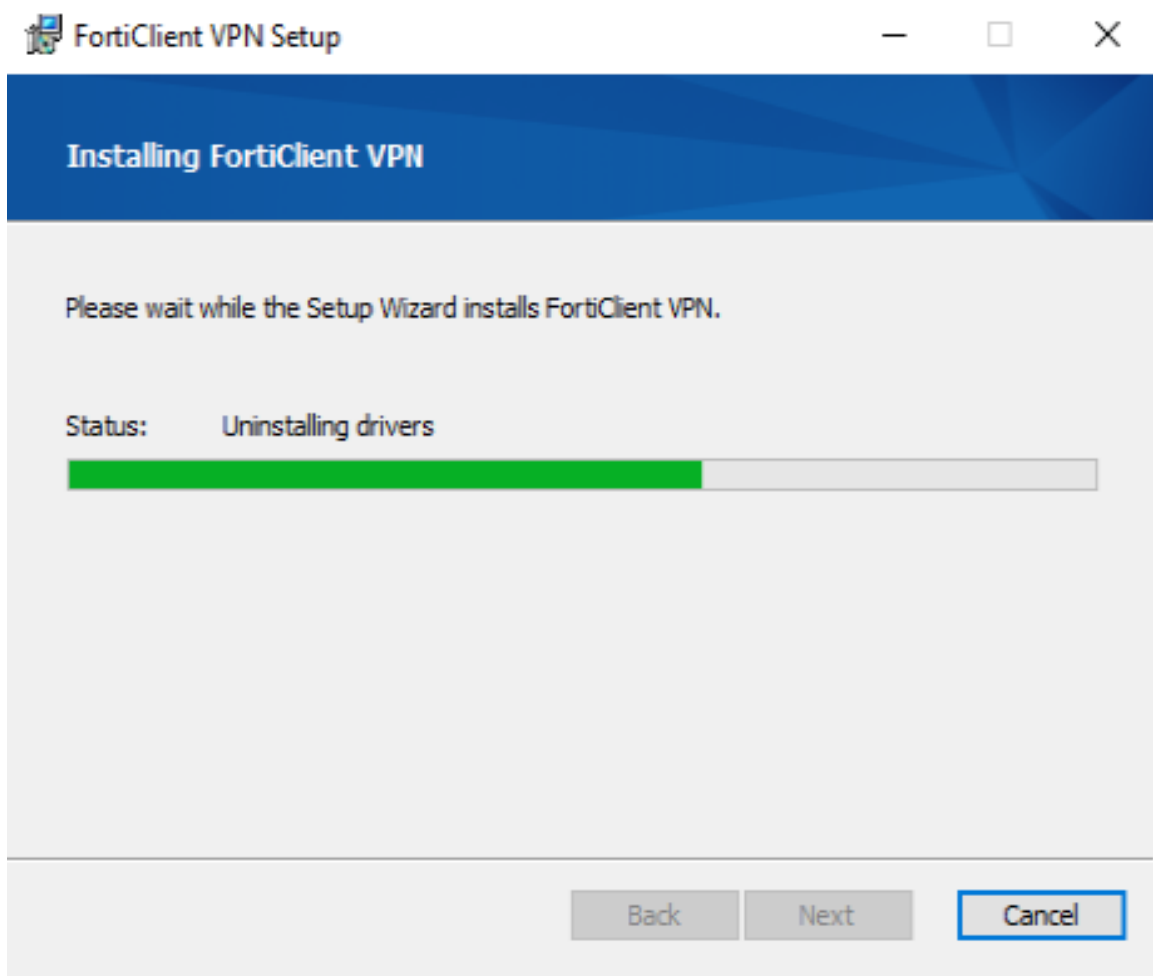
- Check the box to agree to the EULA and hit "next", followed by "Install."





- Allow the program to complete the installation and after hit "finish."

FOR OFFICIAL USE ONLY



2.3 VERIFICATION:

To ensure a successful installation, perform the following verification steps:

CONFIRM THAT FORTICLIENT IS INSTALLED WITHOUT ERRORS.

- Verify the FortiClient shield, and check mark are displayed in the tray by date & time.



2.4 CONCLUSION:

- Congratulations! You have successfully installed FortiClient on your device.

Note: If you encounter any issues during installation, please refer to the Troubleshooting section in this document or contact our help desk via telephone, email or submit a ticket on the intranet.

3. FORTICLIENT CONFIGURATION:

3.1 FIRST TIME OPERATION & CONFIGURATION:

SYSTEM TRAY ICON:

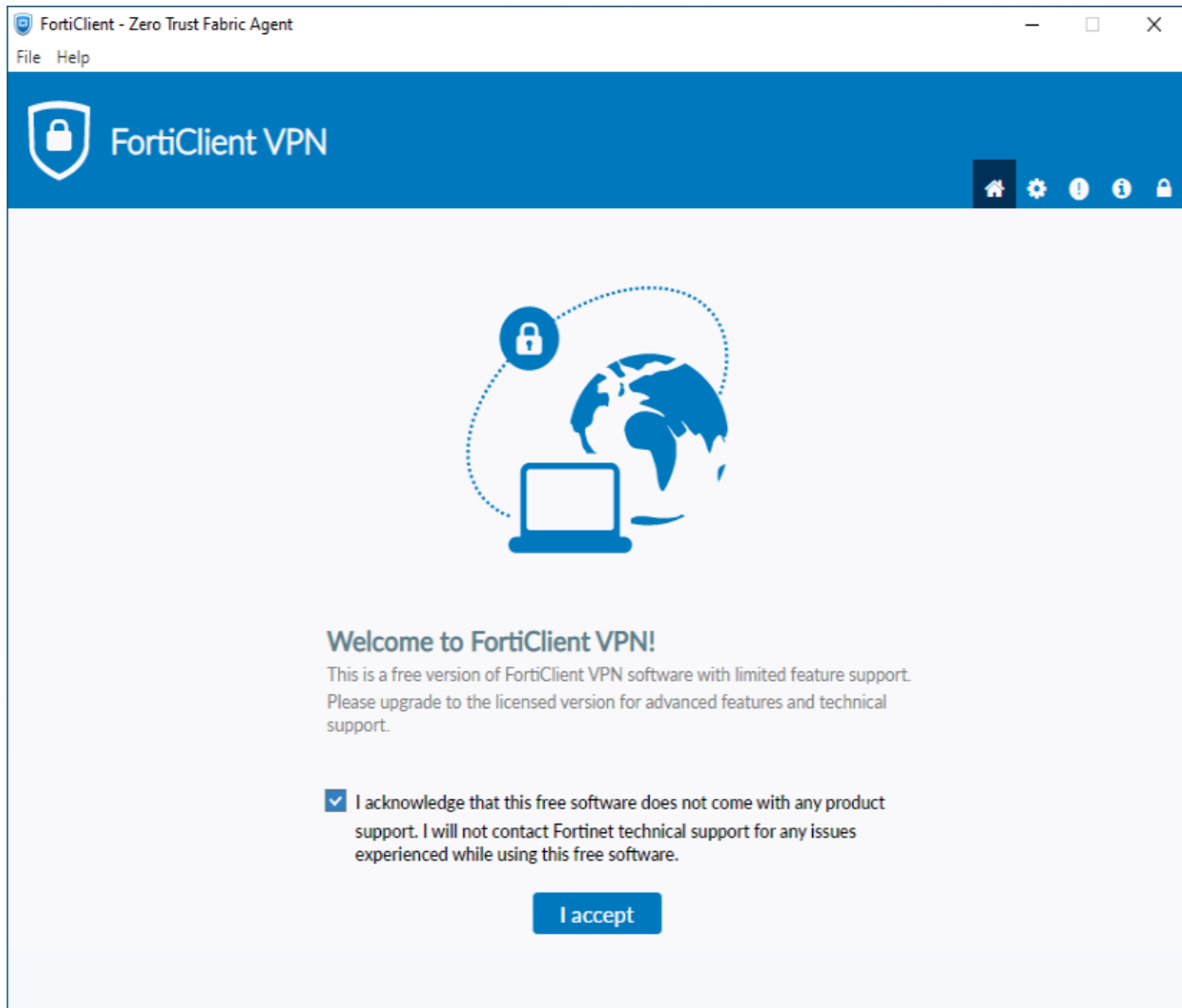
- Locate the FortiClient icon in the system tray at the bottom right of your screen (near the clock).
- *Note: If you don't see the FortiClient icon in the system tray, you can open FortiClient from the Start menu or desktop shortcut.*



Right-click on the FortiClient icon.

LAUNCH IT:

- Double click on the icon to launch the program, if it was the first time doing so, please accept the license agreement.



CONFIGURE VPN:

- o Click on "Configure VPN"

INSERT THE VARIOUS CONFIGURATION INTO THE PROGRAM:

Connection Name: ESU VPN

Remote Gateway: ssltunnel.admin.esu.edu

Customize Port:

Port Number: 9443

Enable Single Sign On (SSO) for VPN Tunnel:

Use external browser as user-agent for SAML user authentication:

New VPN Connection

VPN: SSL-VPN IPsec-VPN XML

Connection Name:

Description:

Remote Gateway: ✕
+Add Remote Gateway

Customize port:

Enable Single Sign On (SSO) for VPN Tunnel

- Use external browser as user-agent for saml user authentication
- Enable auto-login with Azure Active Directory

Client Certificate: ▼

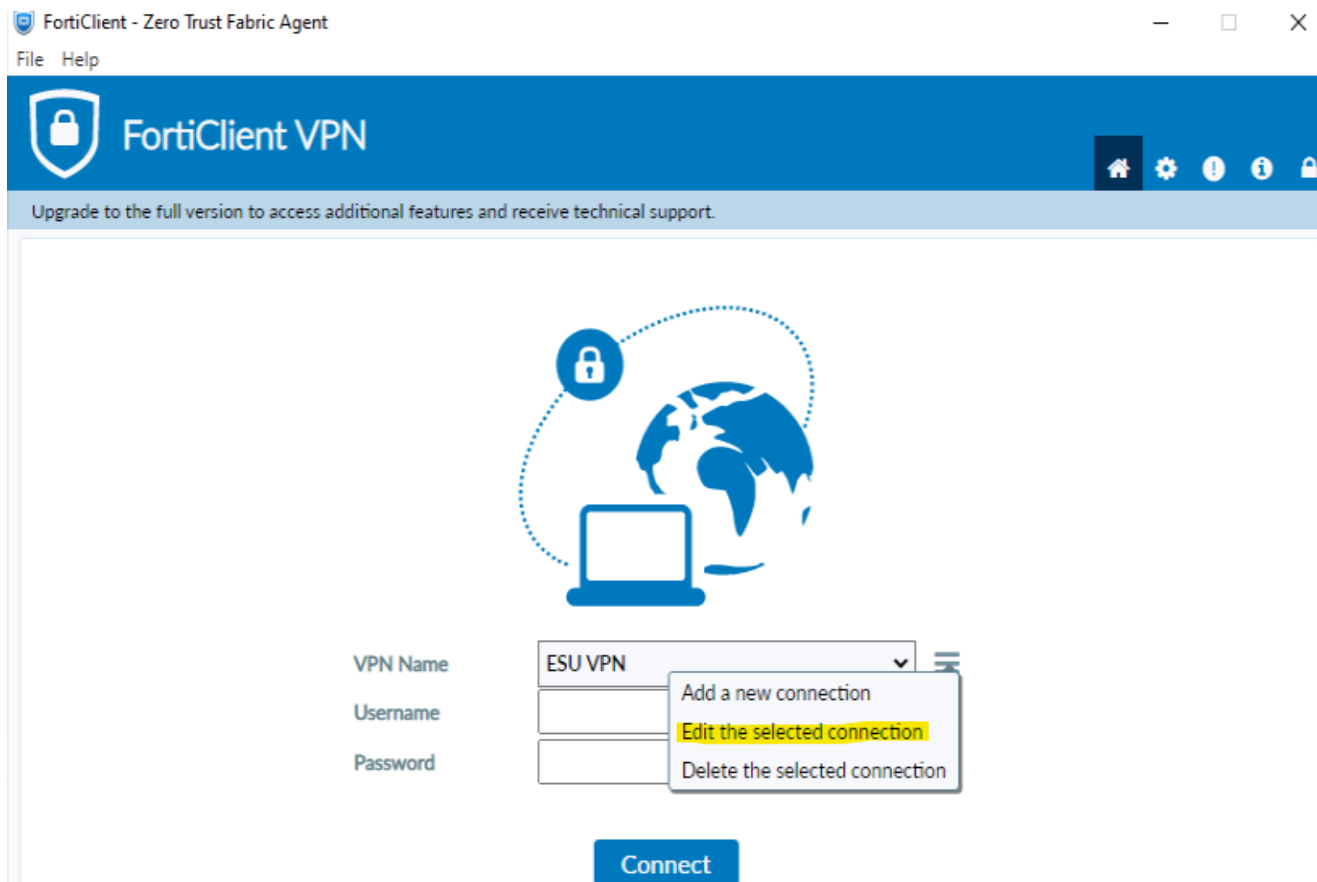
Enable Dual-stack IPv4/IPv6 address

3.2 RE-CONFIGURATING THE VPN:

- If you already have Forti-Client installed and were using it prior, you are going to want to follow these steps to change the configuration.

EDIT THE CONNECTION:

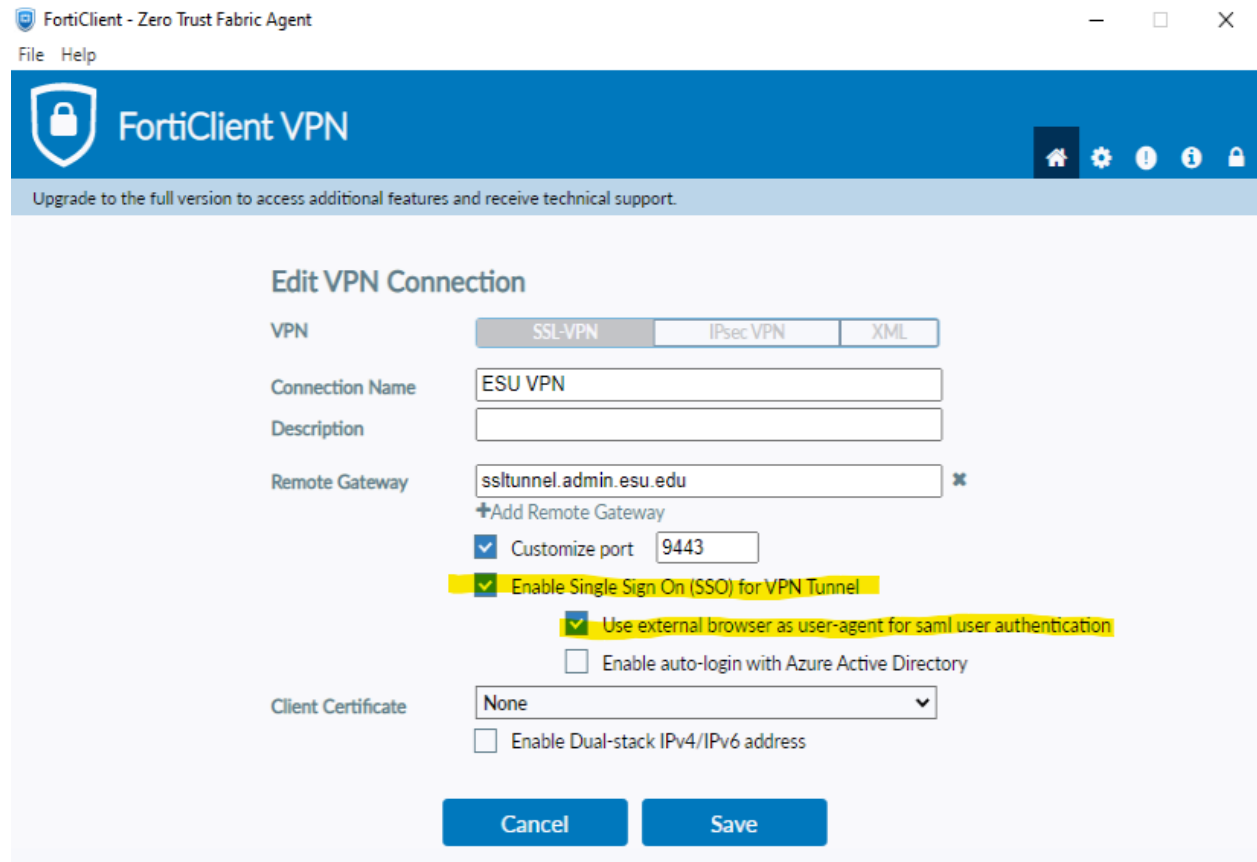
- Click on the stacked bars and in the drop down, click "Edit the selected connection."



ADDING SSO VARIABLES:

- o Place a check mark in the two locations: "Enable Single Sign On" & "Use external browser...." and click "Save."

FOR OFFICIAL USE ONLY

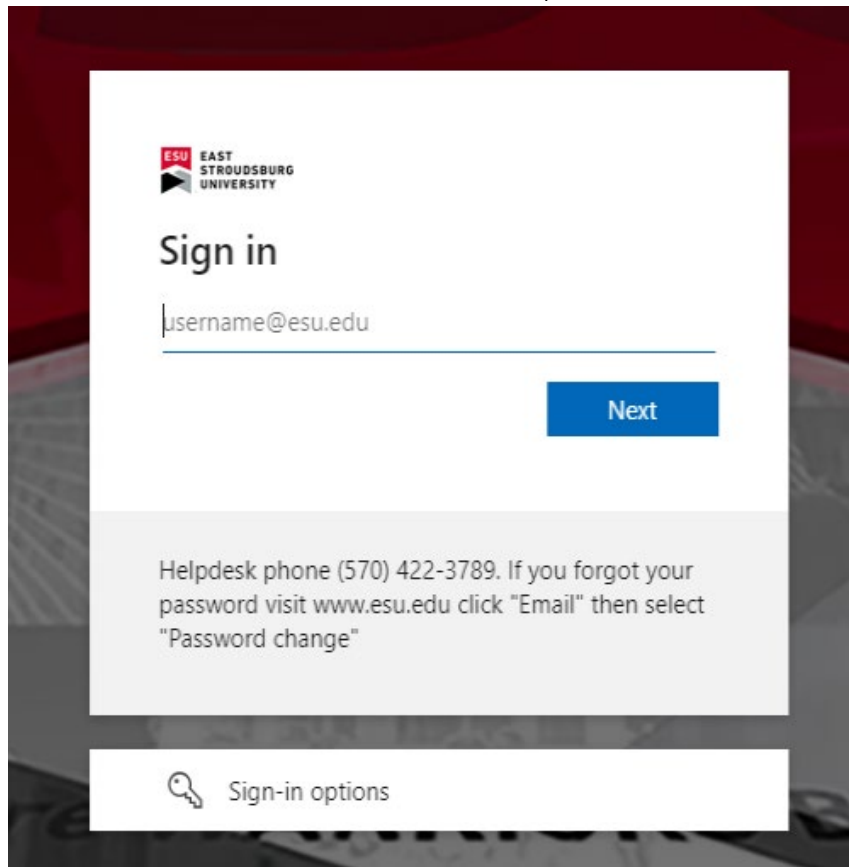


Notice: **If the SSO options are not present in your application, this means you are running an unsupported version of FortiClient, please refer to section 4 for the clean uninstallation procedure, followed by installation and configuration.**

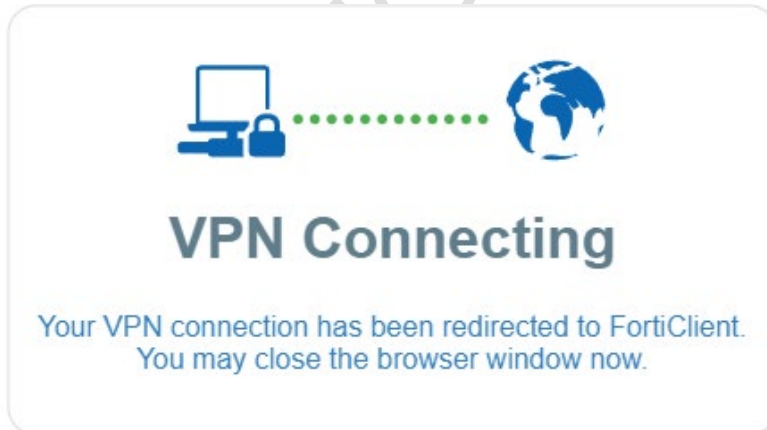
3.3 CONNECTING TO CAMPUS:

- The VPN is now configured, and you are ready to hit connect.
- Once you've hit connect, the browser of preference will be launched.
 - If you have not logged in from this computer before, Microsoft will want to authenticate you with your campus email address and password, along with your

- Microsoft authenticator code, SMS or telephone number.



- If you've logged in before, you will notice that FortiClient will show up in the browser letting you know it's connecting. You can close this browser window.



- You're now connected to the campus network!

4. UNINSTALLING FORTICLIENT:

4.1 PREREQUISITES:

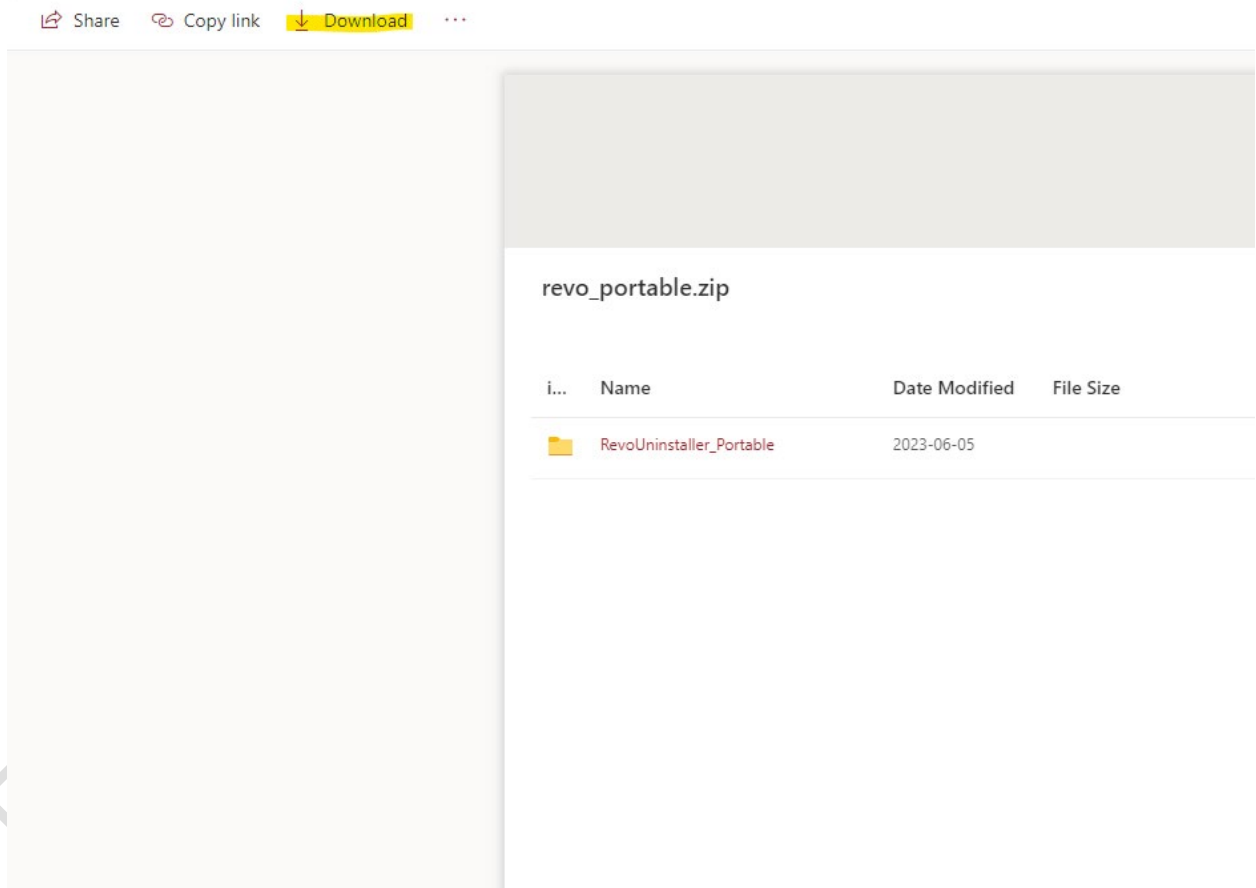
Before you begin the removal, ensure that your system meets the following prerequisites:

INTERNET CONNECTION: Required for downloading Revo Uninstaller

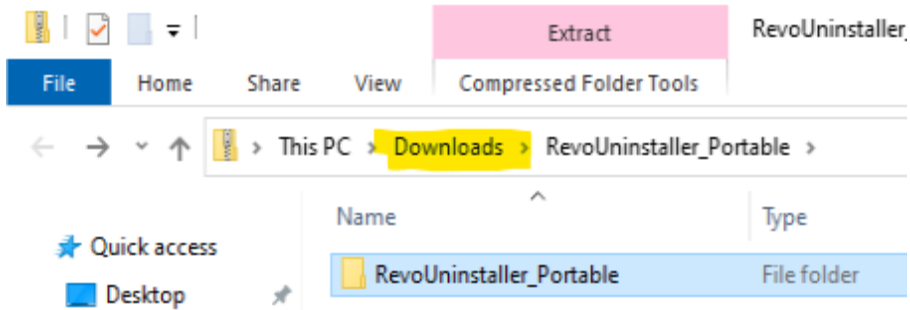
ADMINISTRATIVE PRIVILEGES: You need administrative rights on your device.

4.2 Download & Run Revo Uninstaller Portable:

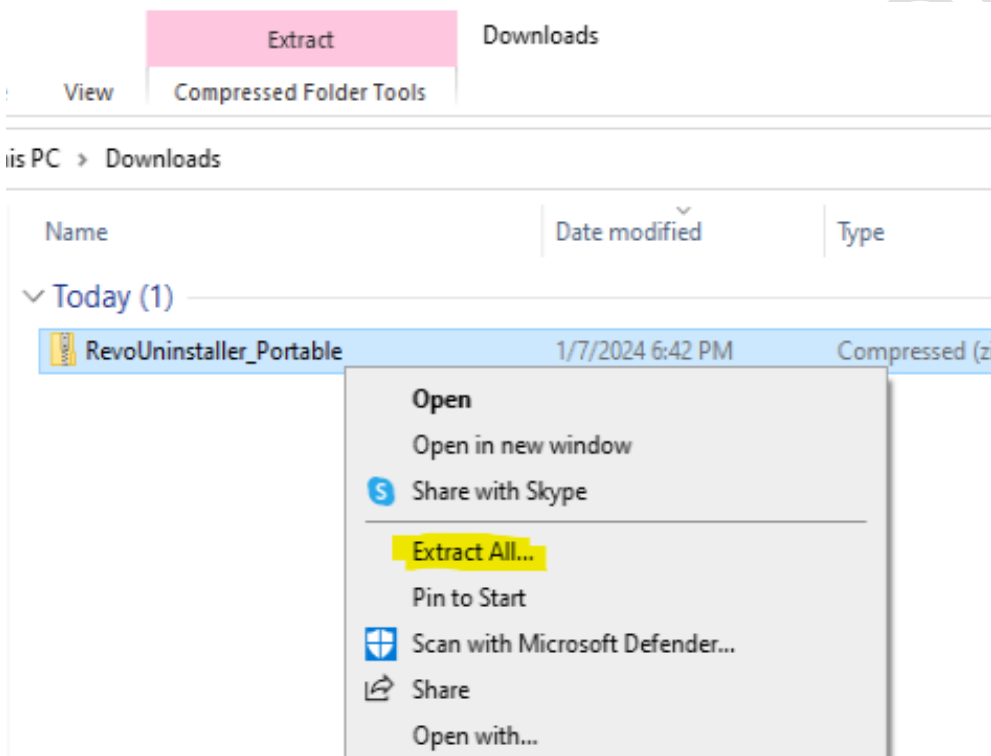
- o Visit the site with the [link](#), right click "Download" at the top left.



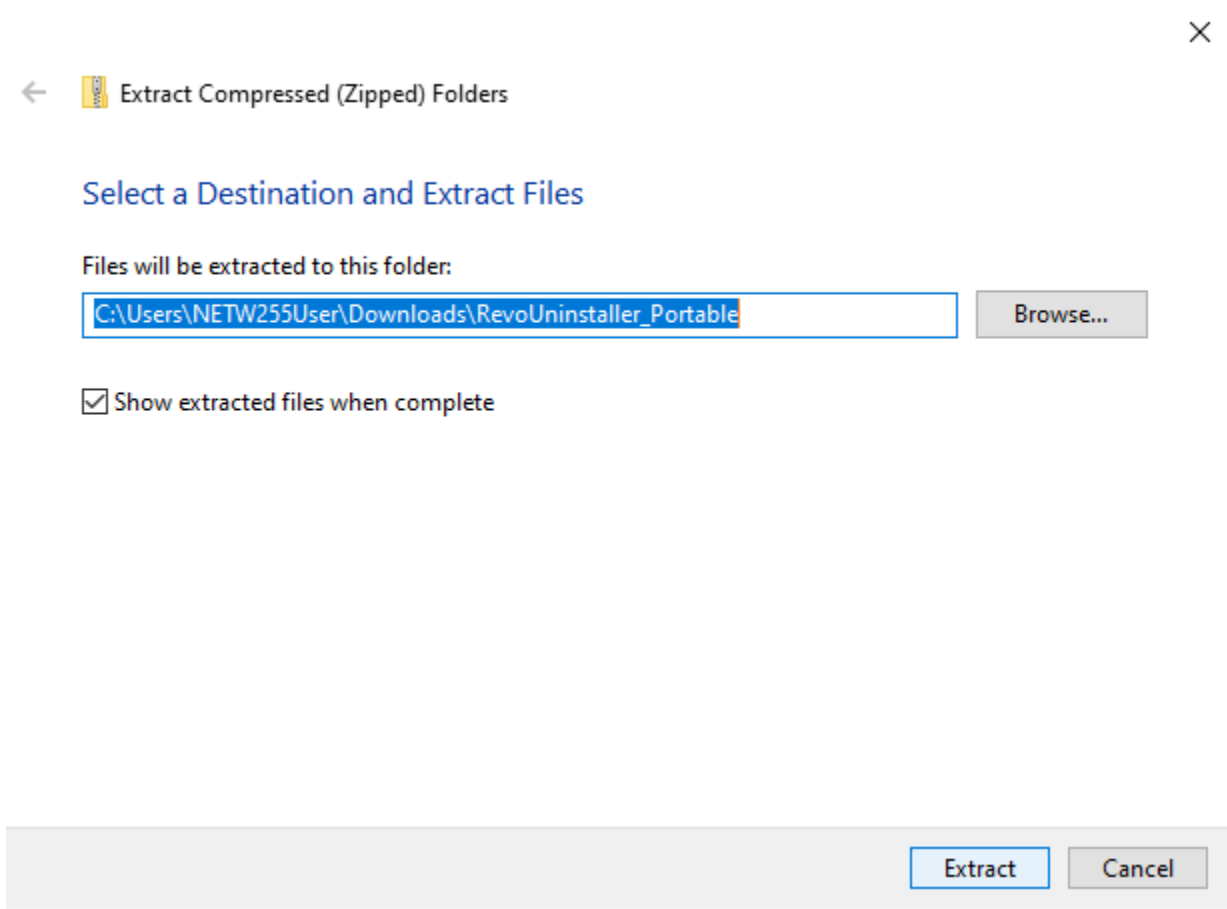
- o Open the downloaded zip file and click back a directory to "Downloads."



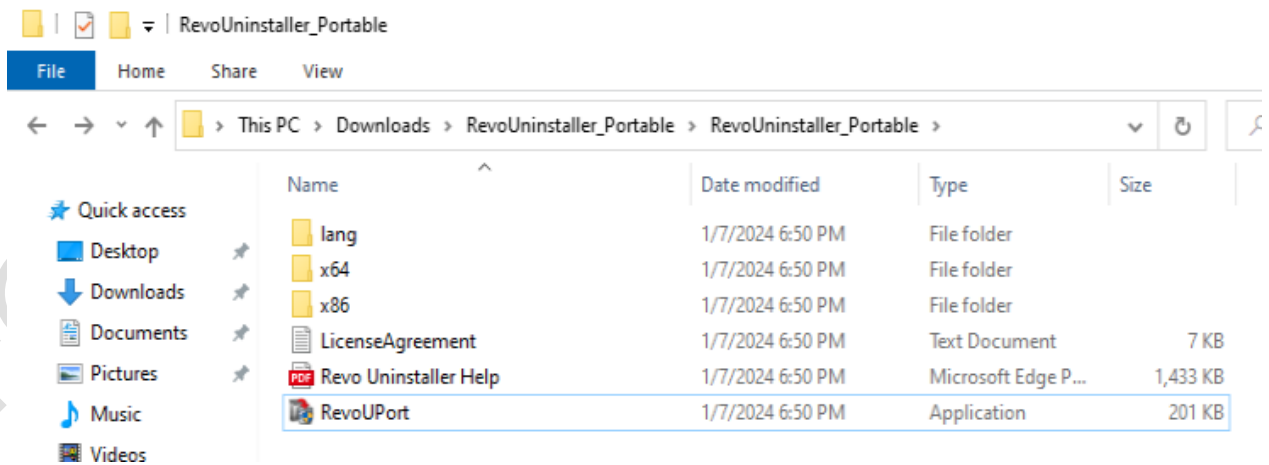
- o Right click on the folder, navigate to “Extract All” and click on that.



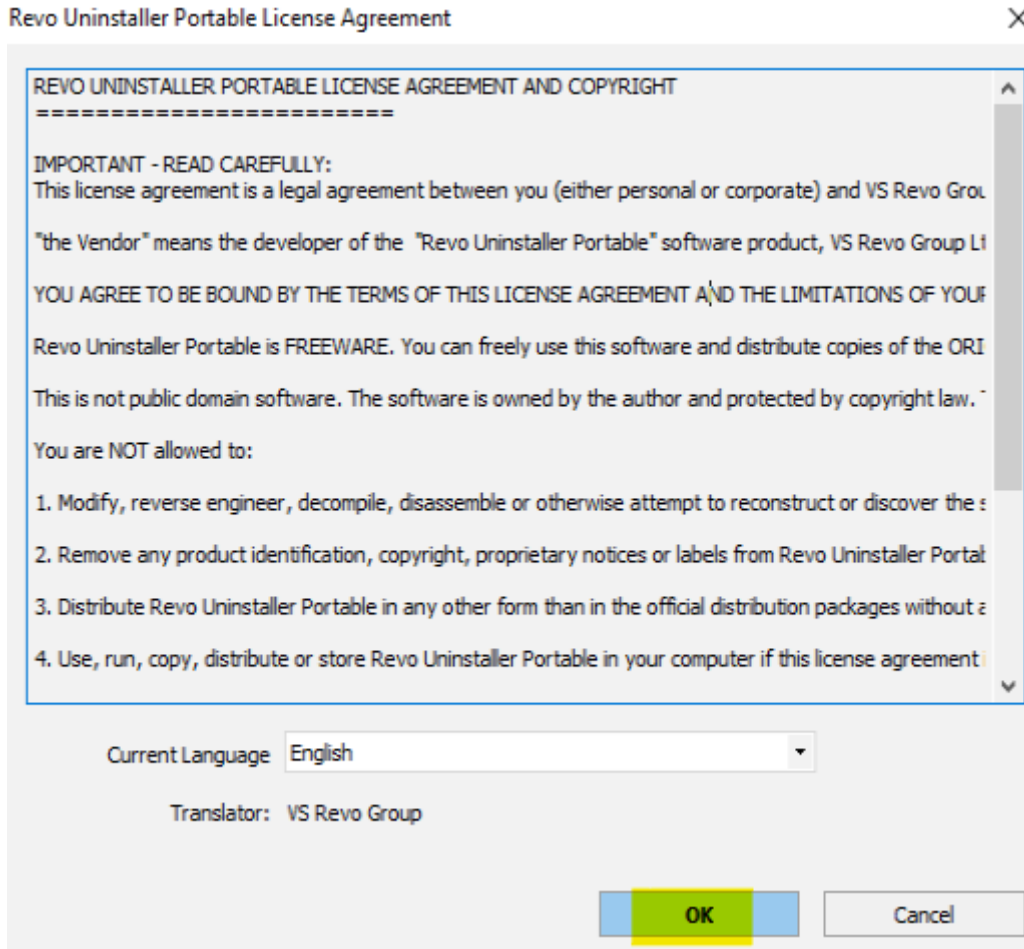
- o Next, click on “Extract” without changing anything and ensure the box is checked.



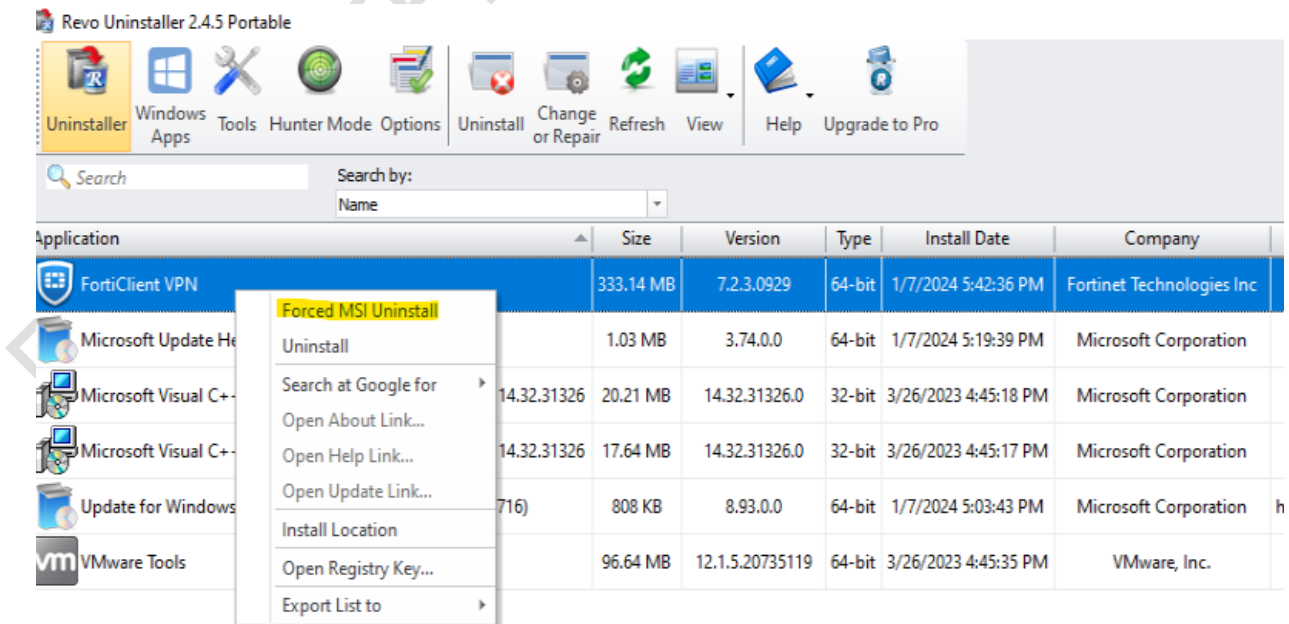
- o It will then open the folder where all the contents were extracted, keep clicking on the folder until you see the application "RevoUPort" and right-click, "Run as administrator" on it.



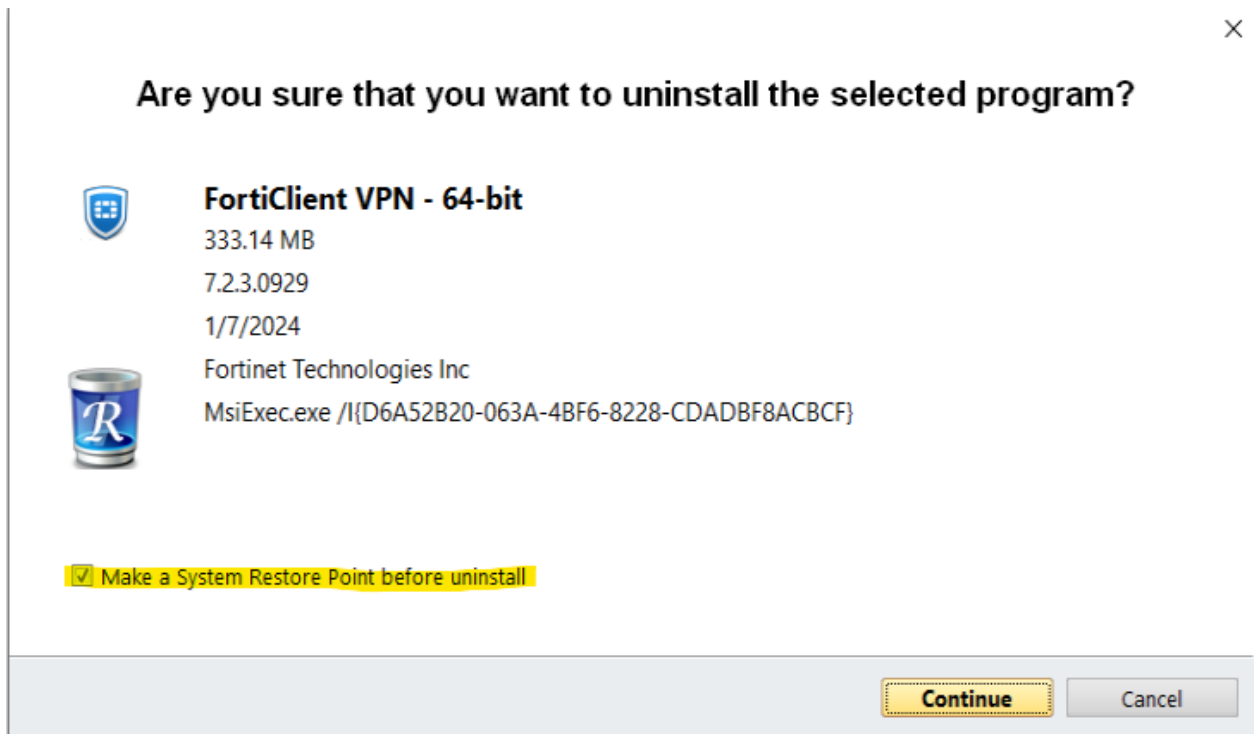
- o Accept the License Agreement



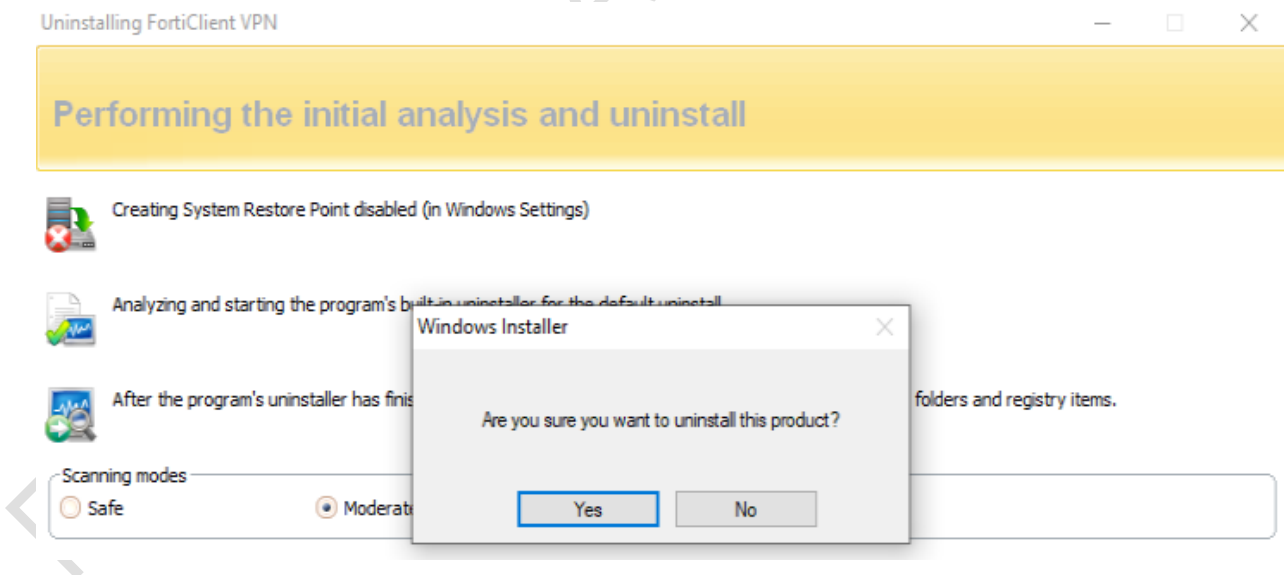
- o Navigate to FortiClient, then click on "Forced MSI Uninstall."



- o Ensure "Make a System Restore Point...." Is checked before hitting continue.

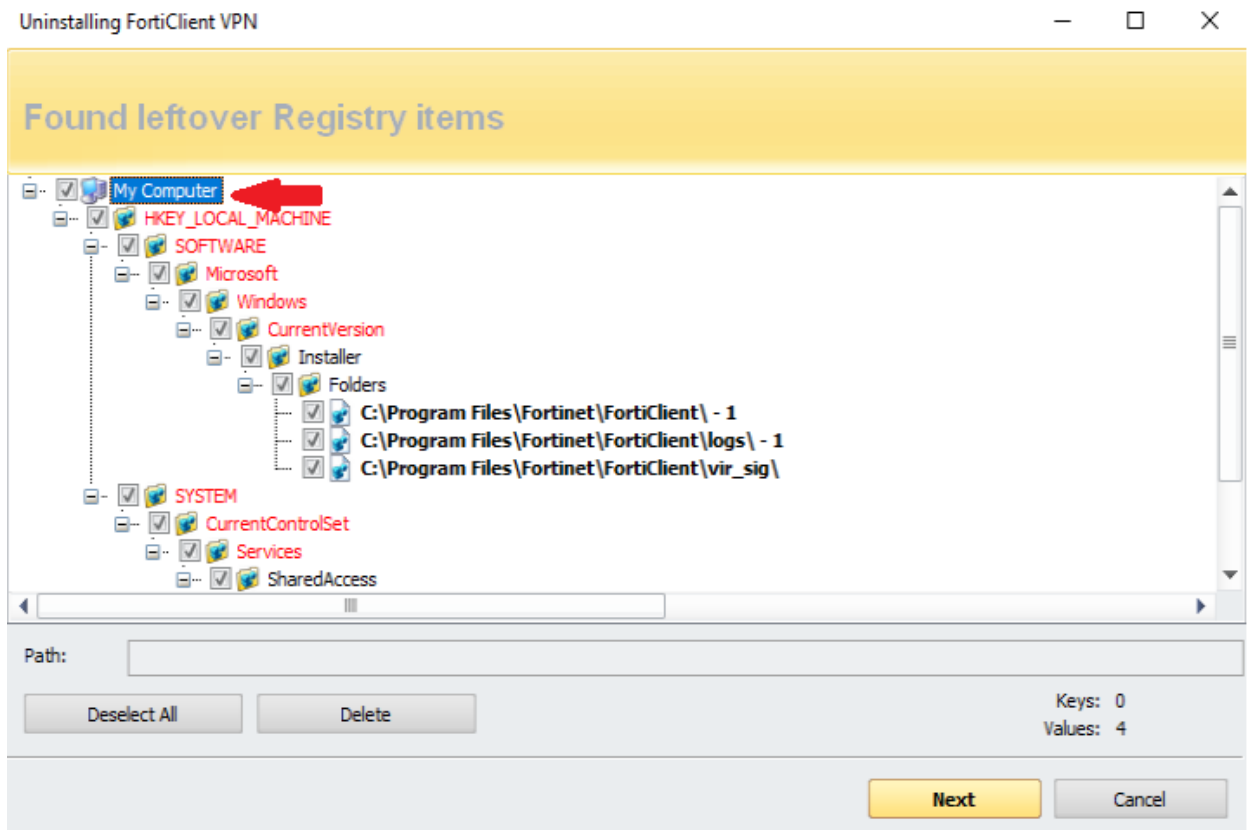


- o Hit "Yes" to ensure you want to uninstall the product.



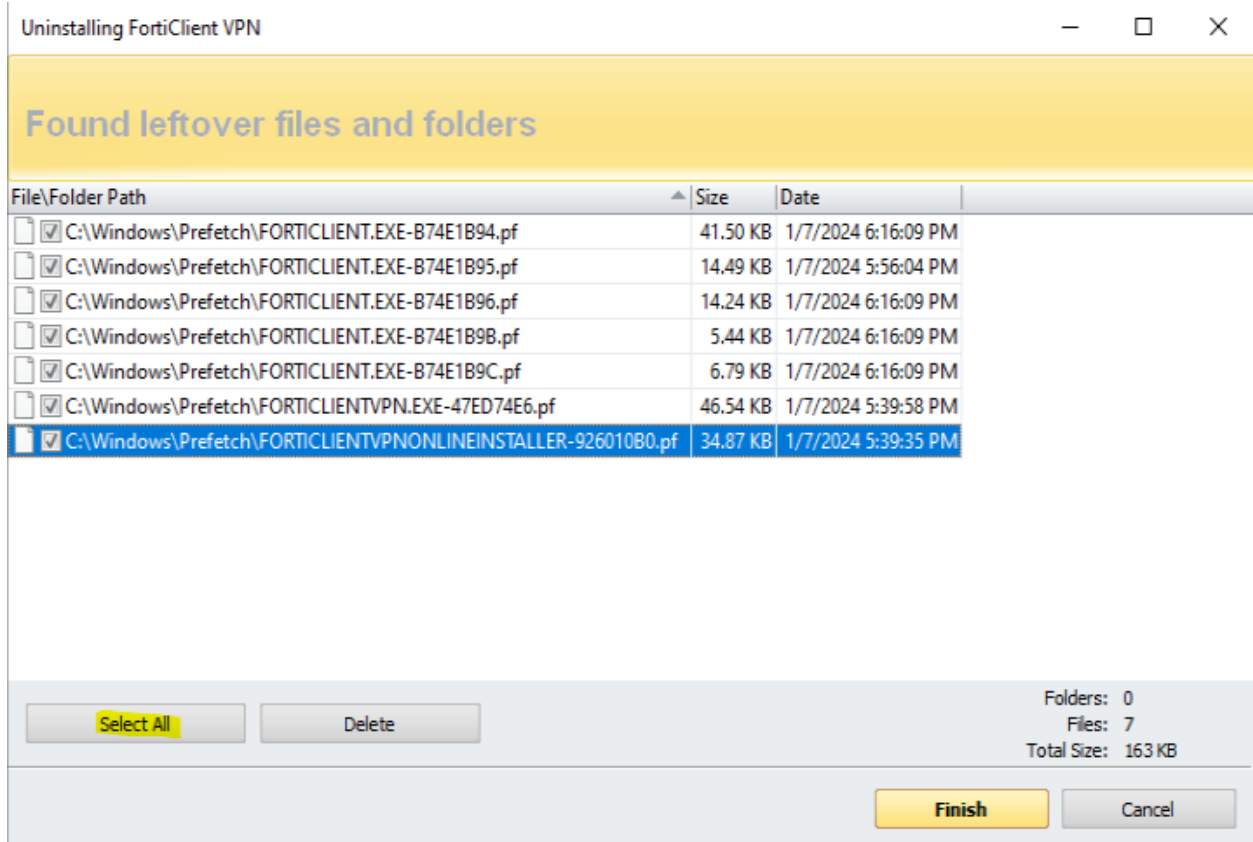
- o Wait for it to finish uninstalling the program, then make sure scanning modes is on "moderate" and hit "scan."

- Click the check box in the top of the tree that says “My Computer” it will highlight everything in the list, then hit “delete” and then “Next.”



- Hit “Select All” on all of the files at the bottom, then “Delete” and confirm with “Yes” if it prompts you.

FOR OFFICIAL USE ONLY



- o You can now close the application and associated folders or windows.

4.3 SUMMARY:

- o FortiClient is now uninstalled, you may refer to the installation steps followed by configuration of the application.

5. TECHNICAL RESOURCES:

ESU ACADEMIC AND ADMINISTRATIVE HELPDESK:

Submit a ticket: [ESU Work Orders](#)

Email: helpdesk@live.esu.edu

Telephone: 570-422-3789