ZotDefend Compliance

ZotDefend Compliance Instructions for End-Users (School of Physical Sciences ONLY)

- ZotDefend Apple Instructions
- ZotDefend Windows Instructions
- ZotDefend Linux Instructions

ZotDefend Apple Instructions

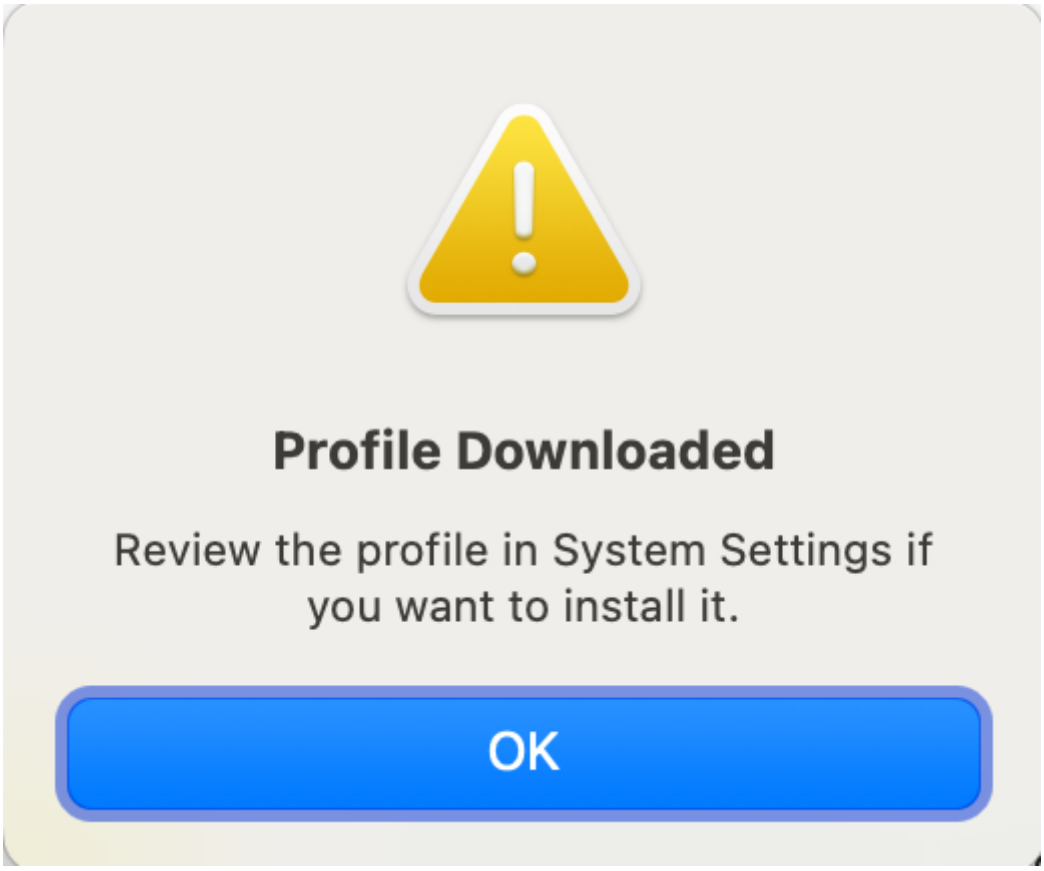
This page contains instructions to install software to ensure an Apple computer is UCI ZotDefend compliant. School of Physical Sciences ONLY

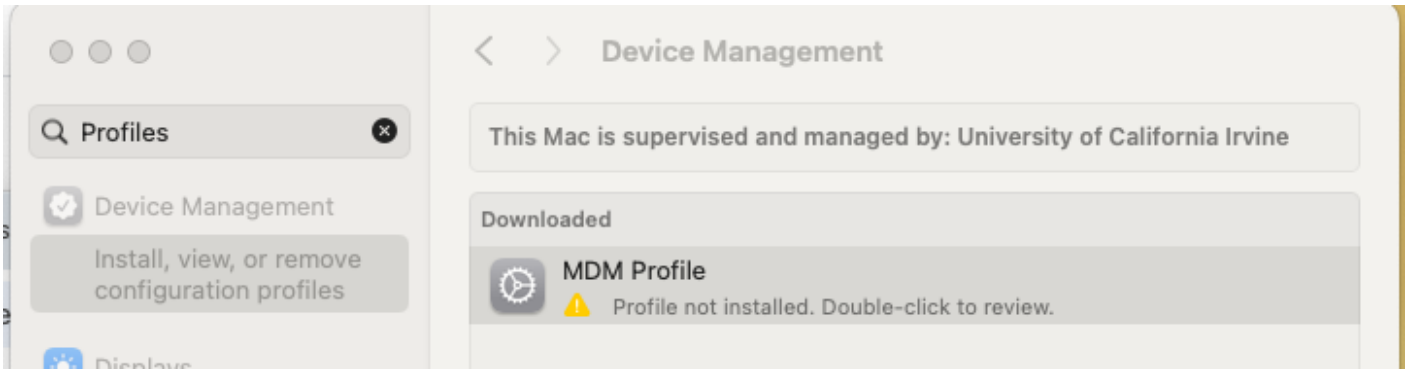
1. Install Jamf Client (Instructions below)

https://tools.ps.uci.edu/downloads/download/enrollmentProfile.mobileconfig

After you log in with your UCInetID and password, it will automatically download a file.

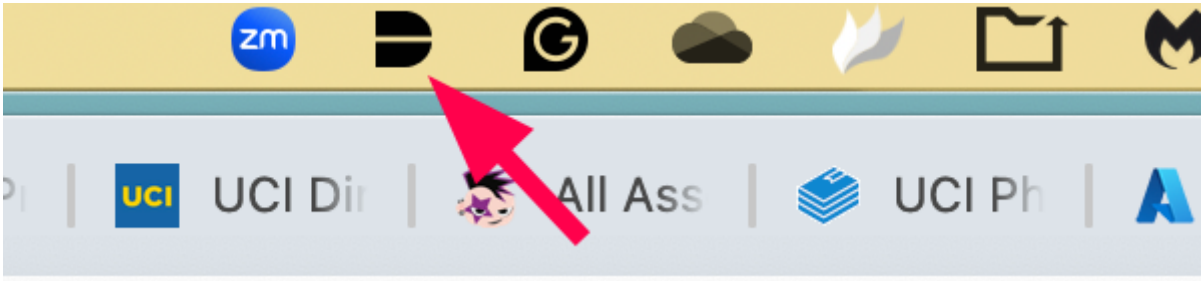
Then go to your "Downloads" folder, and click on "enrollmentProfile.mobileconfig"



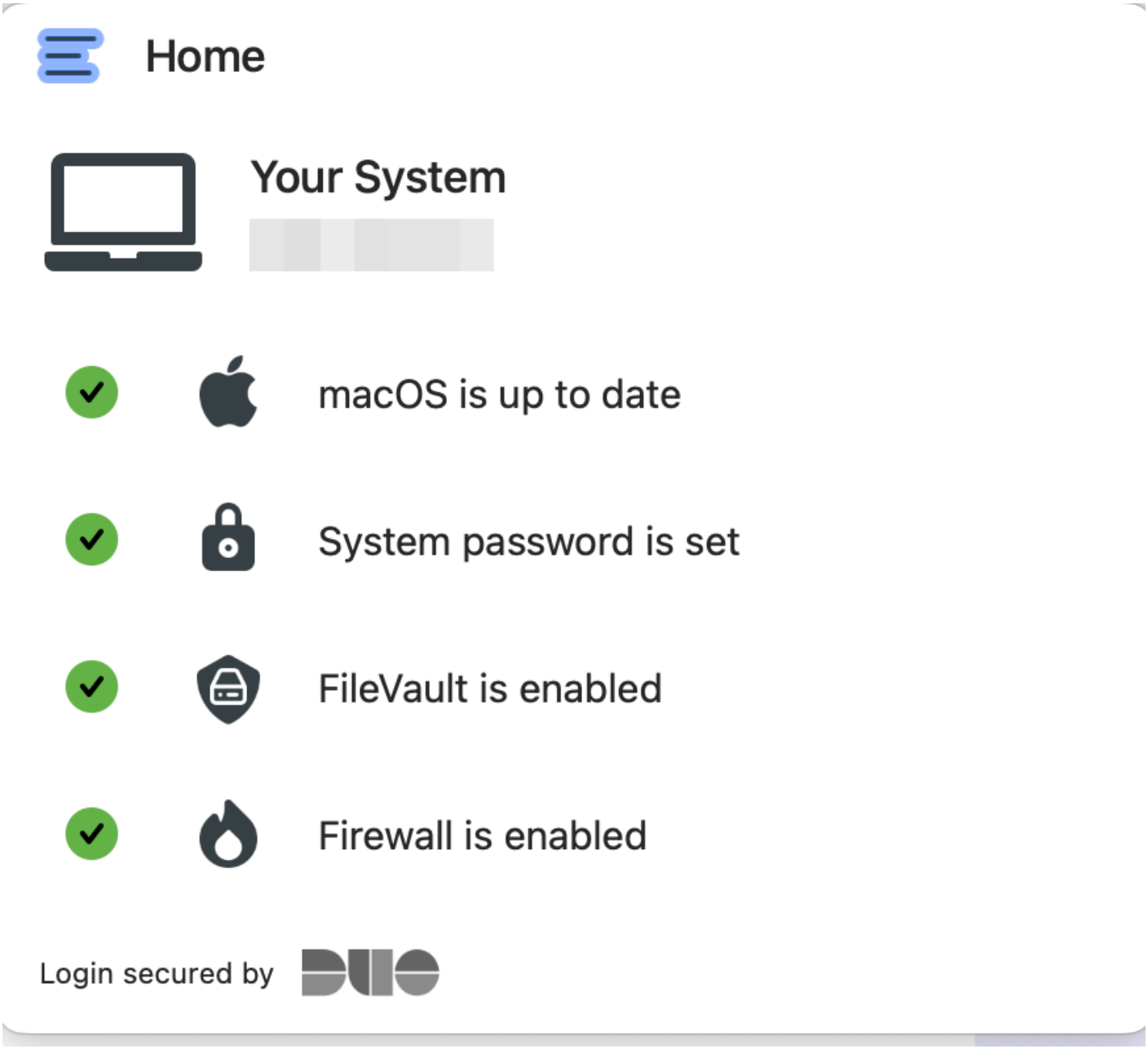


2. **Double click on the profile and enroll the computer. Wait 5-10 minutes** for Jamf to install the required software. You will need to leave your computer on and connected to the internet for this step.

3. Check for the **Duo Desktop** icon in the notification area. Once you see it, click on it to open Duo Desktop.

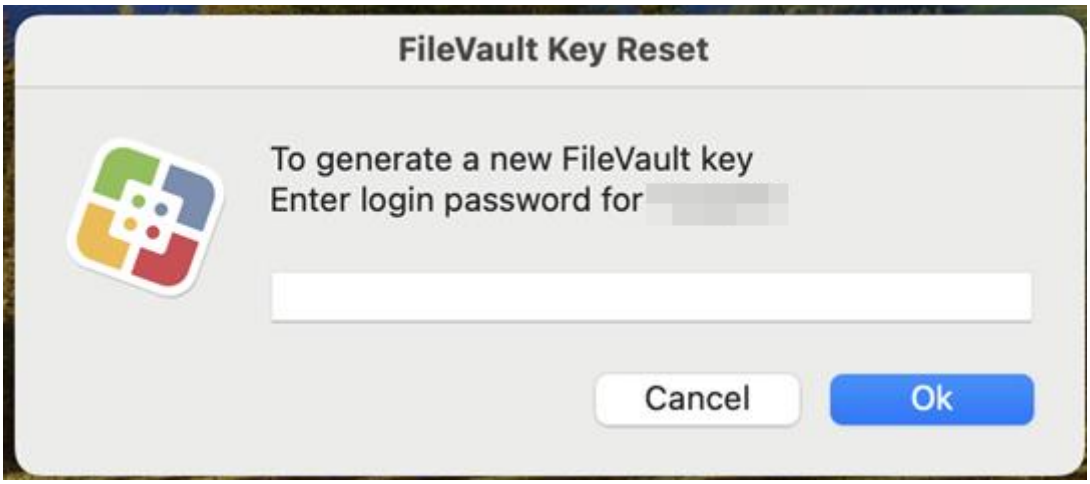


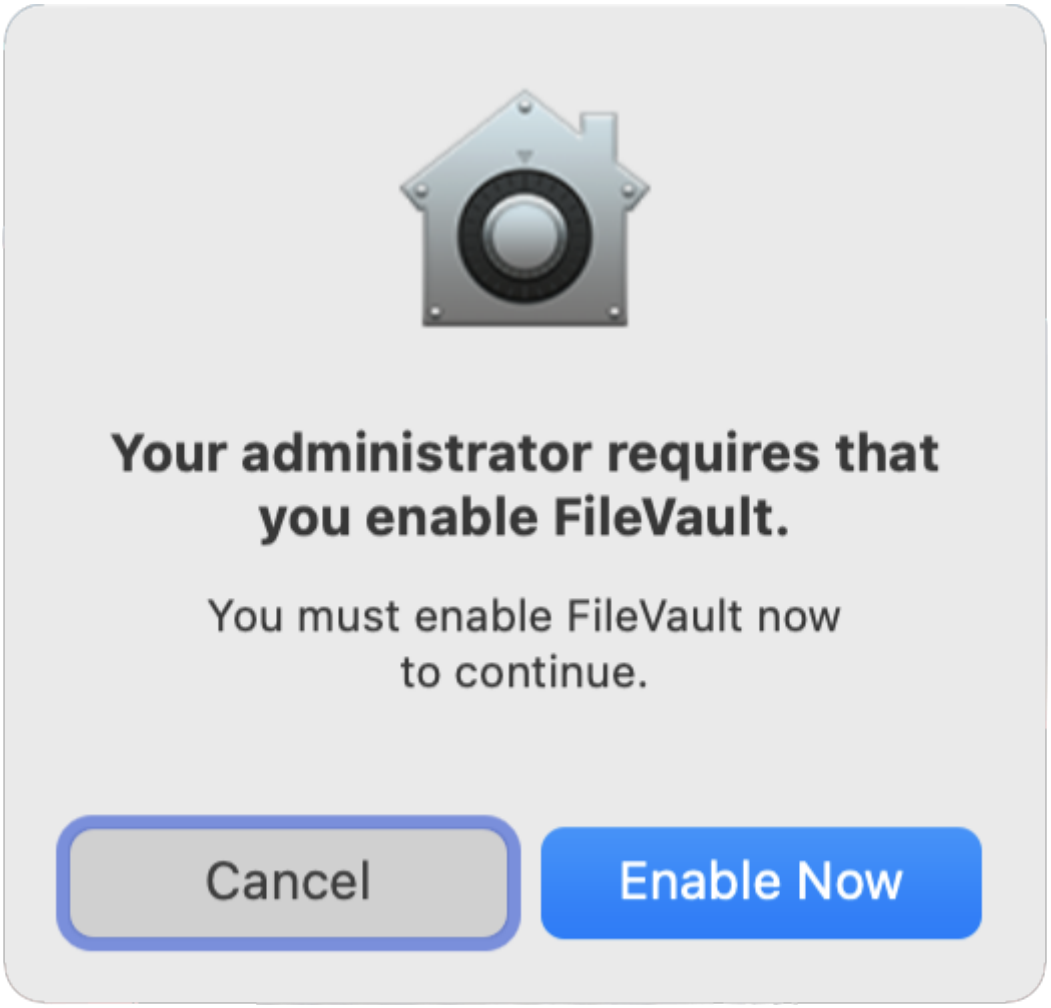
4. Duo Desktop will check for compliance, and will show you green check-marks for each requirement. If you do not have encryption enabled yet, **reboot** and you should be prompted for a password to enable encryption.



5. After a reboot if your device did not have all green checkmarks, you may see the following screens, please click "Enable Now" and enter your password if prompted. This will turn on encryption:

If FileValut Key Reset is having you generate a new FileVault key multiple times, go to Terminal -> type in "jamf recon"


FileVault Key Reset
To generate a new FileVault key
Enter login password for
Cancel
Ok

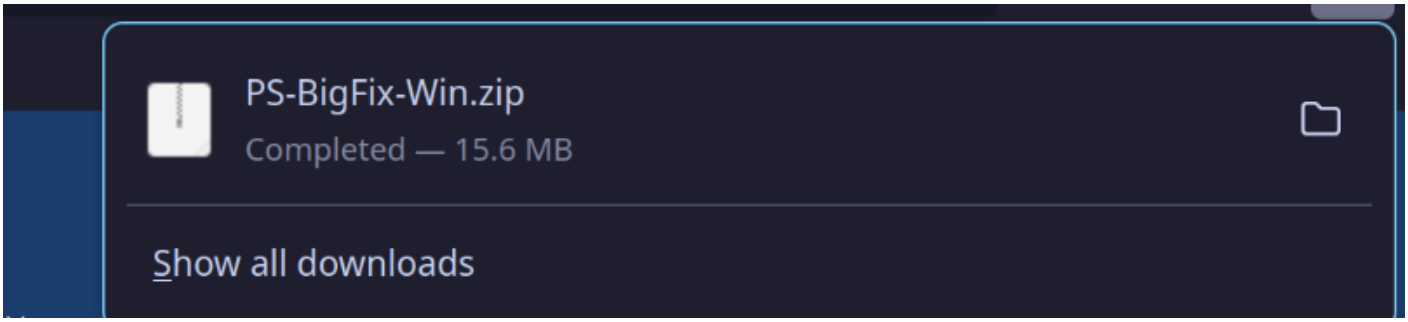

Your administrator requires that you enable FileVault.
You must enable FileVault now to continue.
Cancel
Enable Now

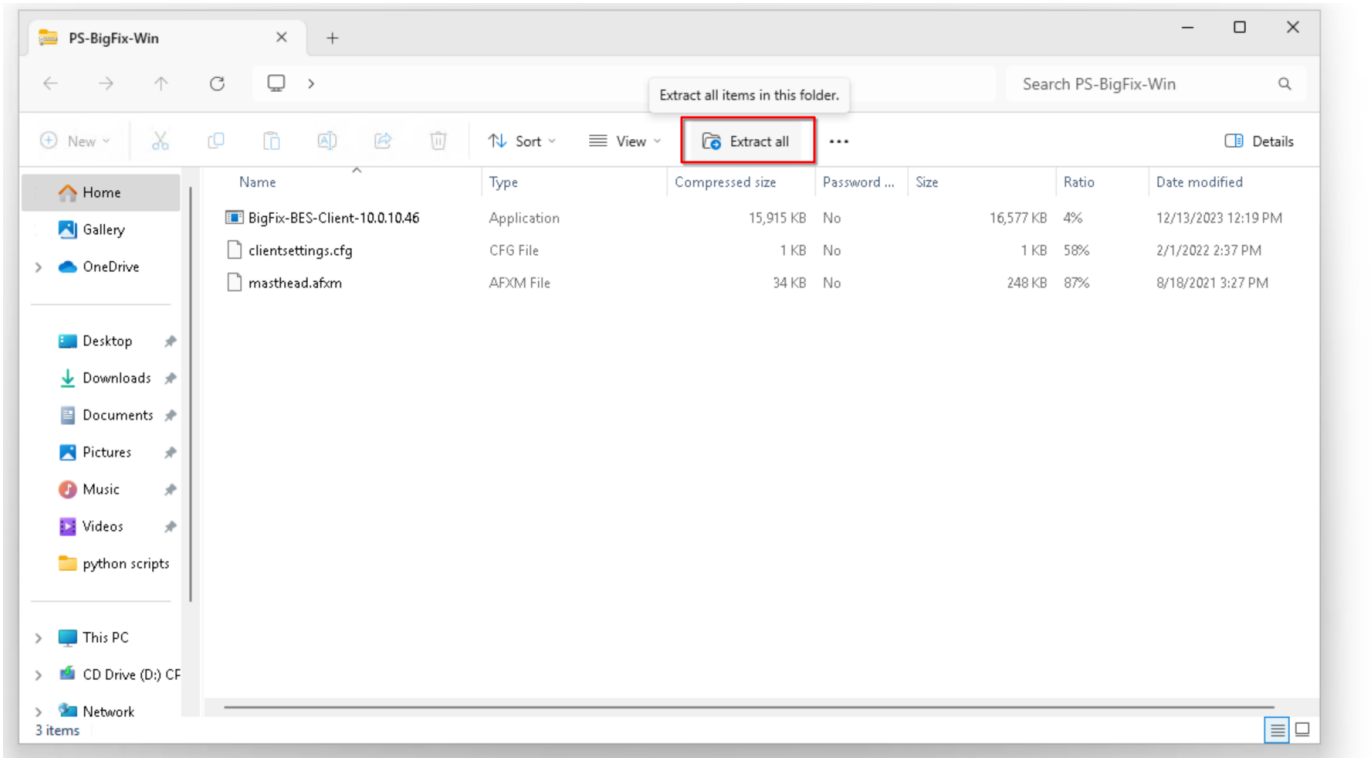
ZotDefend Windows Instructions

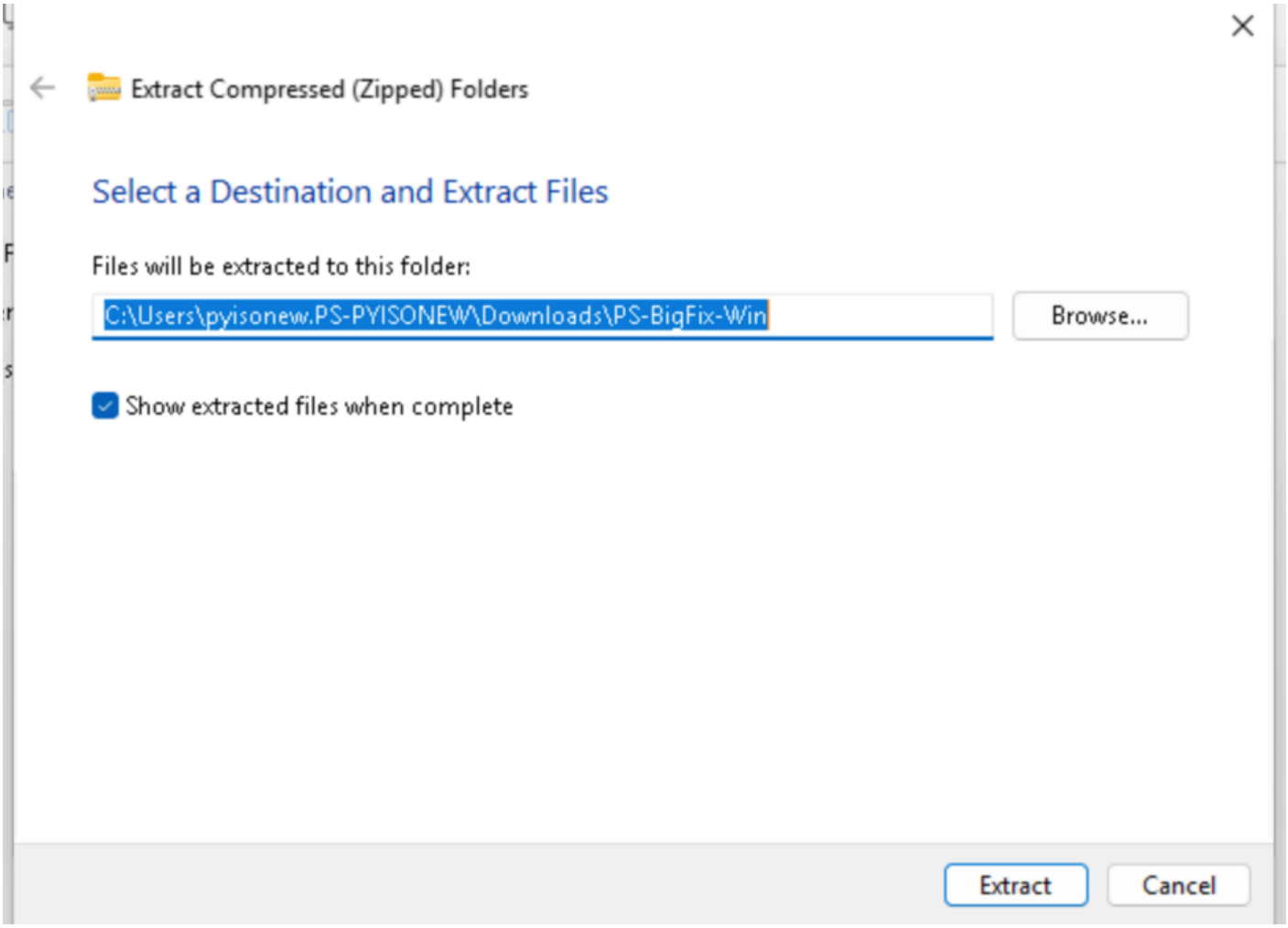
This page contains instructions to install software to ensure a Windows computer is UCI ZotDefend compliant. School of Physical Sciences ONLY

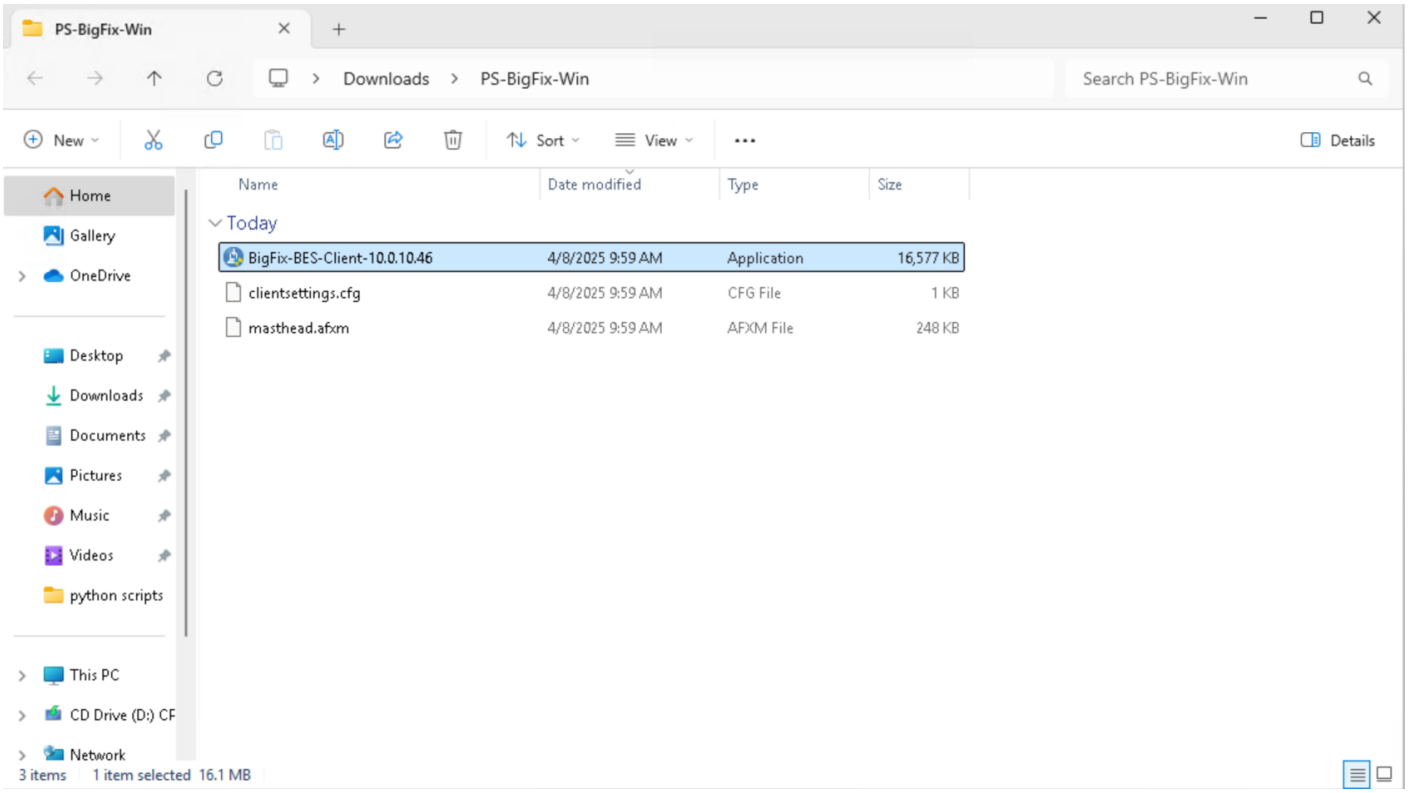
1. Install BigFix (Instructions below)

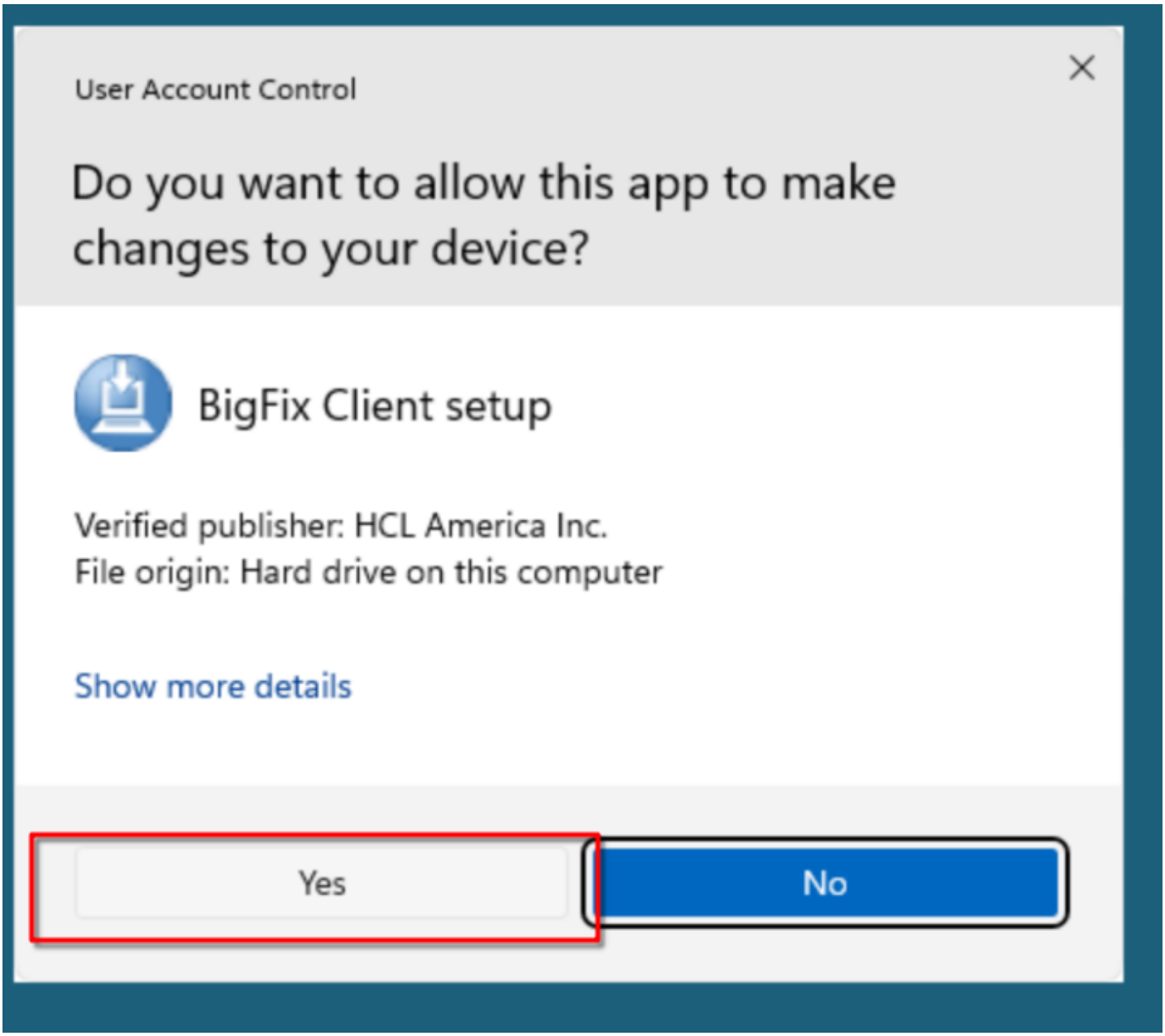
https://tools.ps.uci.edu/downloads/download/PS-BigFix-Win.zip

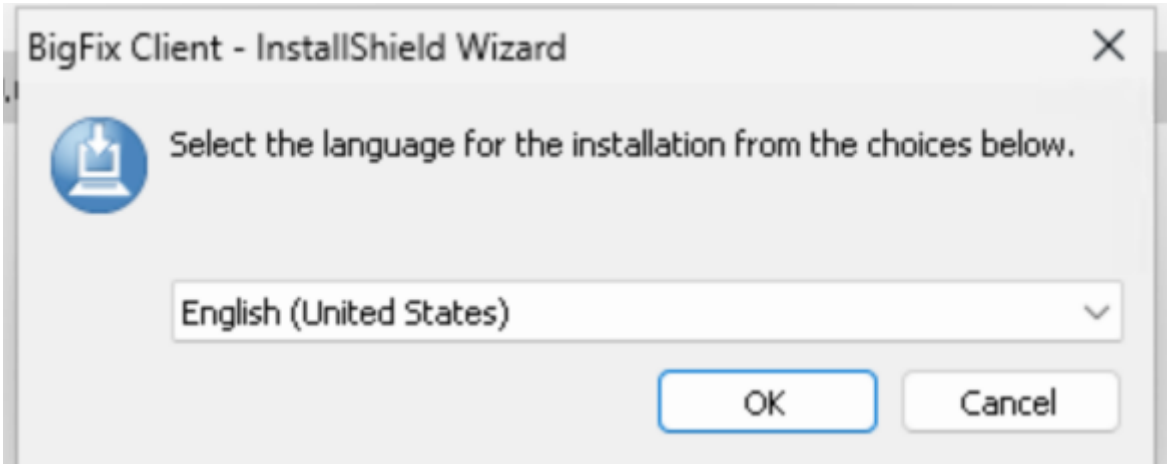


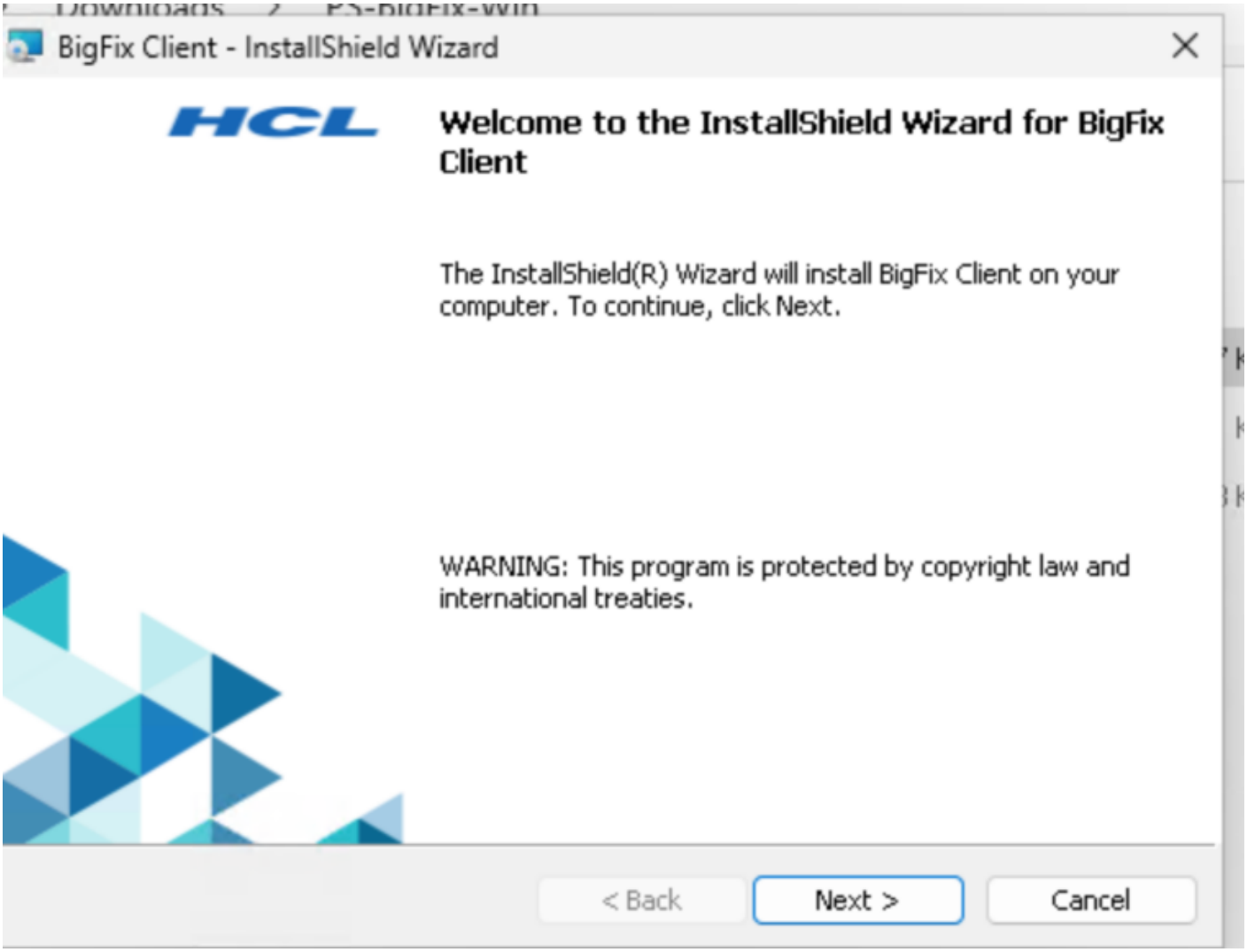

PS-BigFix-Win
Search PS-BigFix-Win
Extract all items in this folder.
New
Sort
View
Extract all
Details
Home
Gallery
OneDrive
Desktop
Downloads
Documents
Pictures
Music
Videos
python scripts
This PC
CD Drive (D:) CF
Network
Name
Type
Compressed size
Password ...
Size
Ratio
Date modified
BigFix-BES-Client-10.0.10.46
Application
15,915 KB
No
16,577 KB
4%
12/13/2023 12:19 PM
clientsettings.cfg
CFG File
1 KB
No
1 KB
58%
2/1/2022 2:37 PM
masthead.afxm
AFXM File
34 KB
No
248 KB
87%
8/18/2021 3:27 PM
3 items

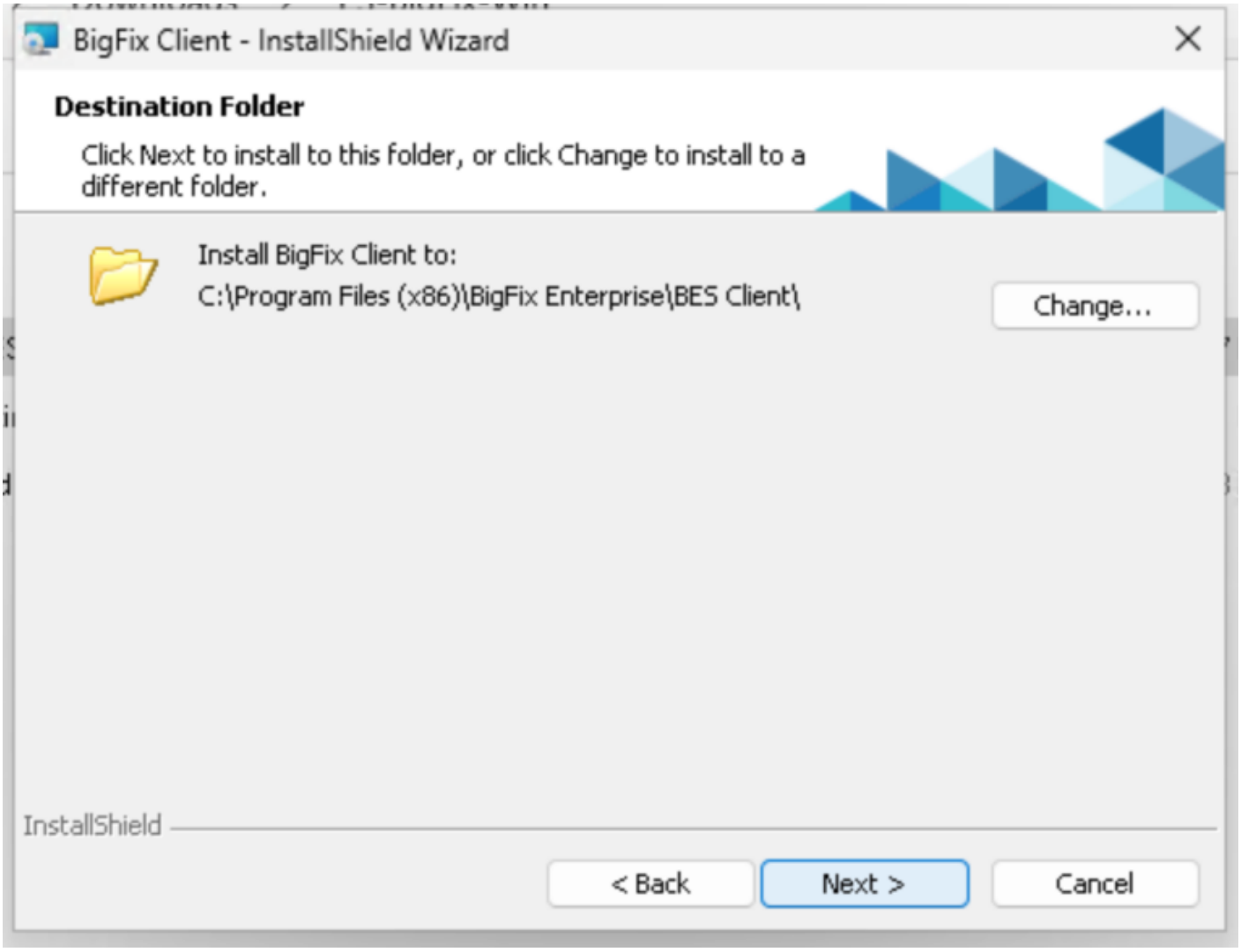

Extract Compressed (Zipped) Folders
Select a Destination and Extract Files
Files will be extracted to this folder:
C:\Users\pyisonew.PS-PYISONEW\Downloads\PS-BigFix-Win
Browse...
Show extracted files when complete
Extract
Cancel

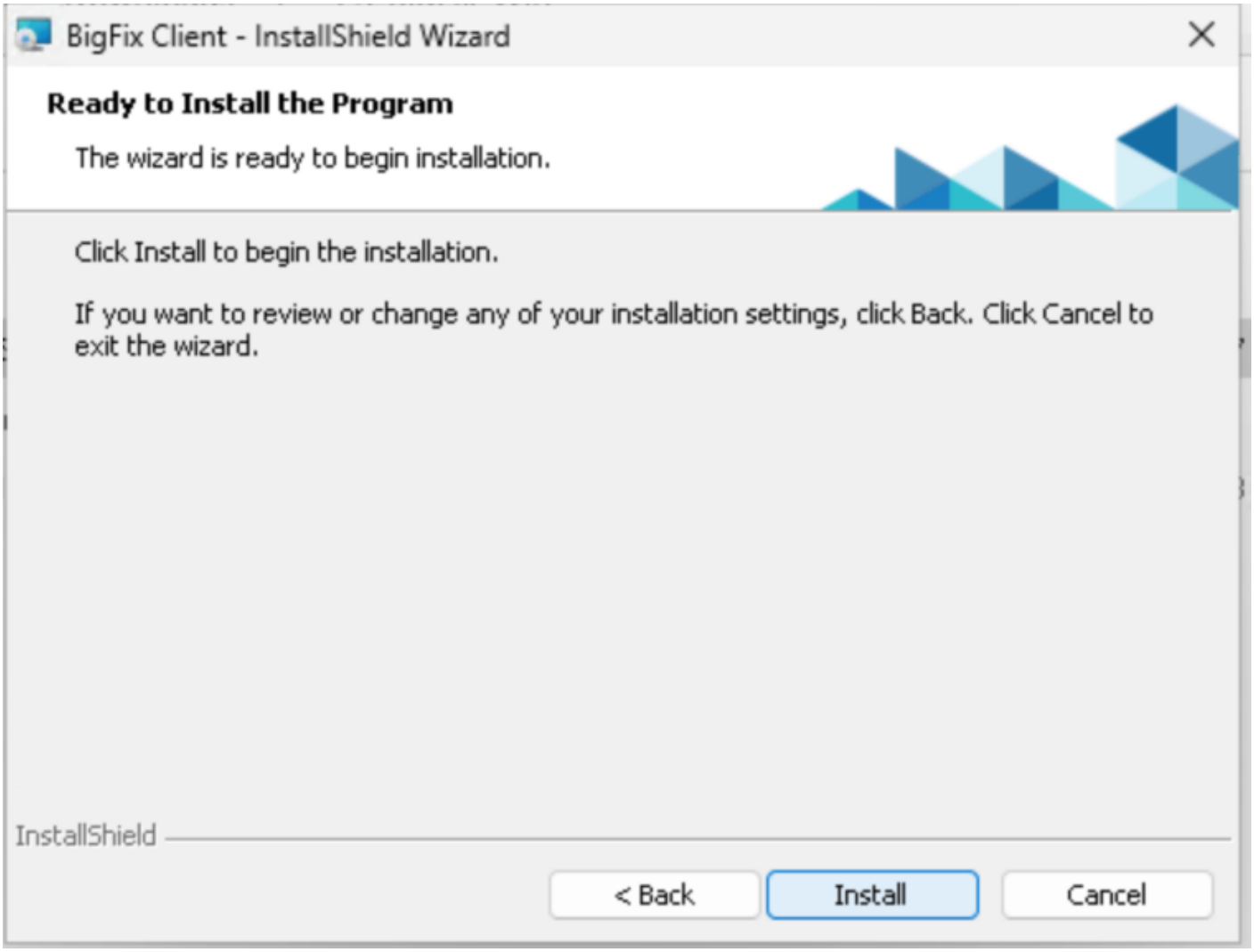

PS-BigFix-Win
Downloads
PS-BigFix-Win
Search PS-BigFix-Win
New
Sort
View
Details
Home
Gallery
OneDrive
Desktop
Downloads
Documents
Pictures
Music
Videos
python scripts
This PC
CD Drive (D:) CF
Network
Name
Date modified
Type
Size
Today
BigFix-BES-Client-10.0.10.46
4/8/2025 9:59 AM
Application
16,577 KB
clientsettings.cfg
4/8/2025 9:59 AM
CFG File
1 KB
masthead.afxm
4/8/2025 9:59 AM
AFXM File
248 KB
3 items
1 item selected 16.1 MB

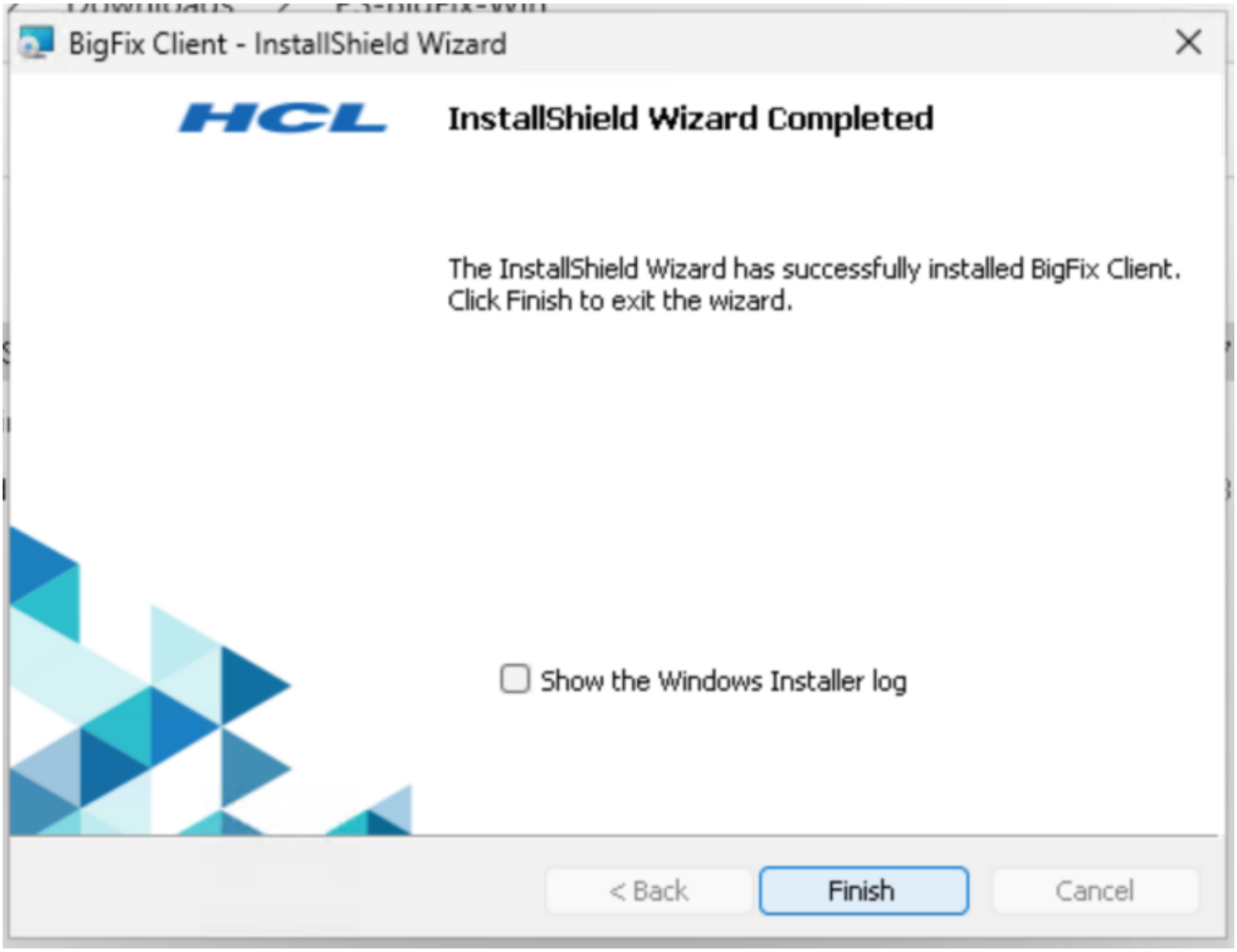

User Account Control
Do you want to allow this app to make changes to your device?
BigFix Client setup
Verified publisher: HCL America Inc.
File origin: Hard drive on this computer
Show more details
Yes
No


BigFix Client - InstallShield Wizard
Select the language for the installation from the choices below.
English (United States)
OK
Cancel


BigFix Client - InstallShield Wizard
HCL
Welcome to the InstallShield Wizard for BigFix Client
The InstallShield(R) Wizard will install BigFix Client on your computer. To continue, click Next.
WARNING: This program is protected by copyright law and international treaties.
< Back
Next >
Cancel

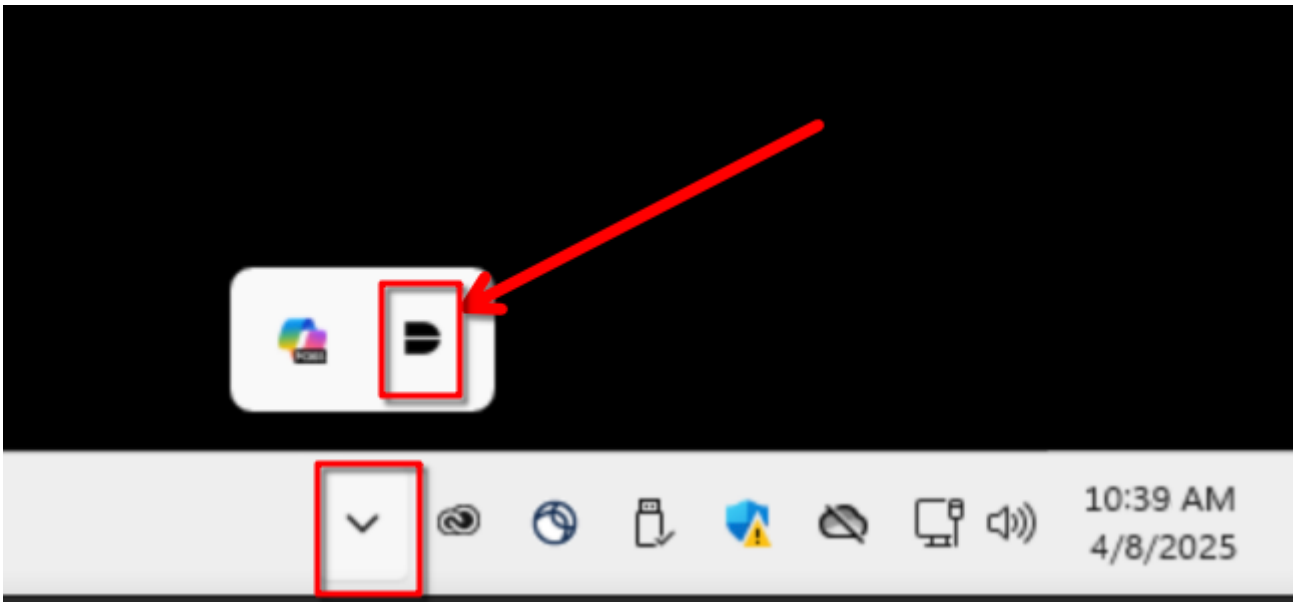

BigFix Client - InstallShield Wizard
Destination Folder
Click Next to install to this folder, or click Change to install to a different folder.
Install BigFix Client to:
C:\Program Files (x86)\BigFix Enterprise\BES Client\
Change...
InstallShield
< Back
Next >
Cancel


BigFix Client - InstallShield Wizard
Ready to Install the Program
The wizard is ready to begin installation.
Click Install to begin the installation.
If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.
InstallShield
< Back
Install
Cancel

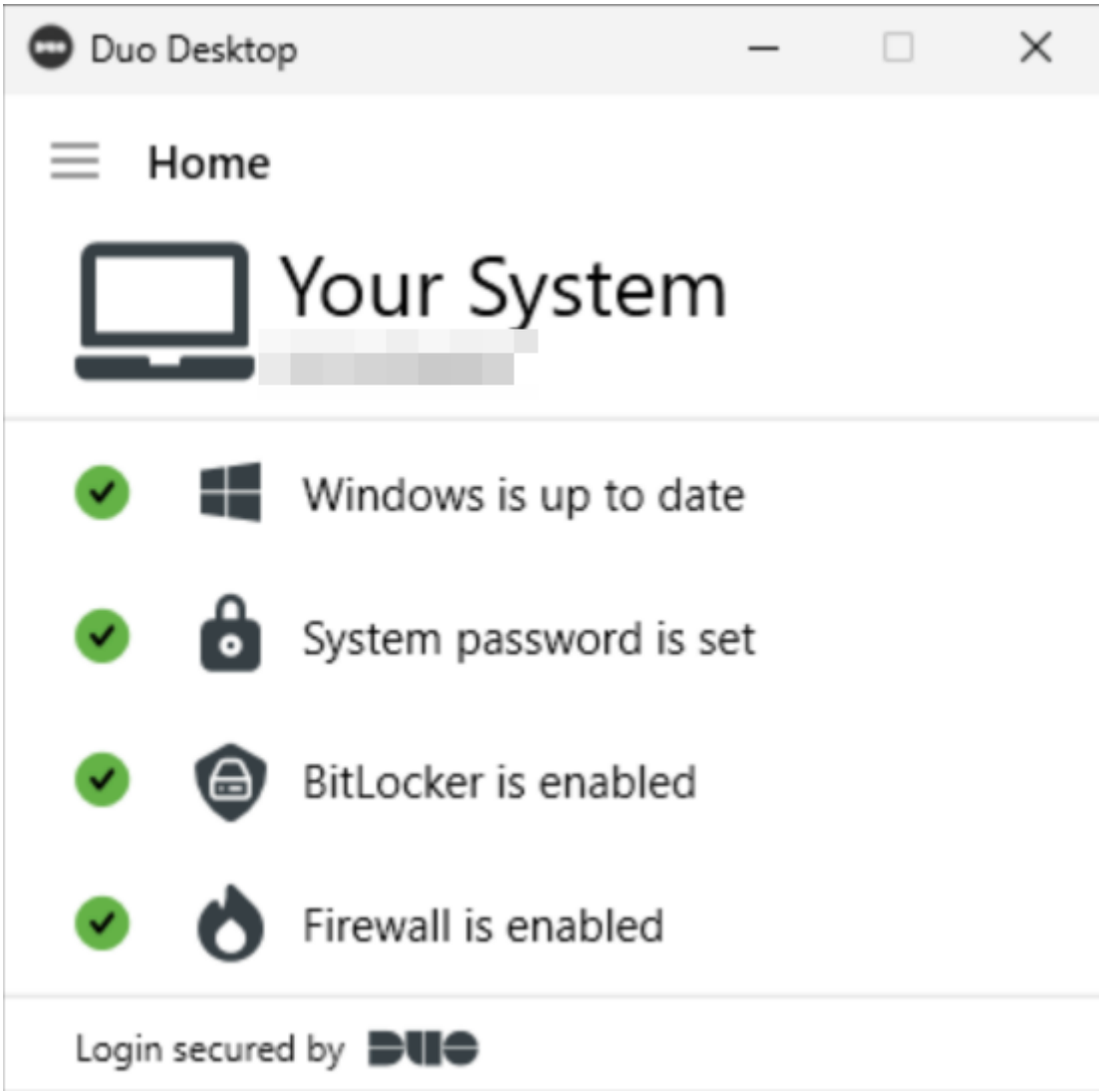


2. **Wait 5-10 minutes** for BigFix to install the required software. You will need to leave your computer on and connected to the internet for this step.

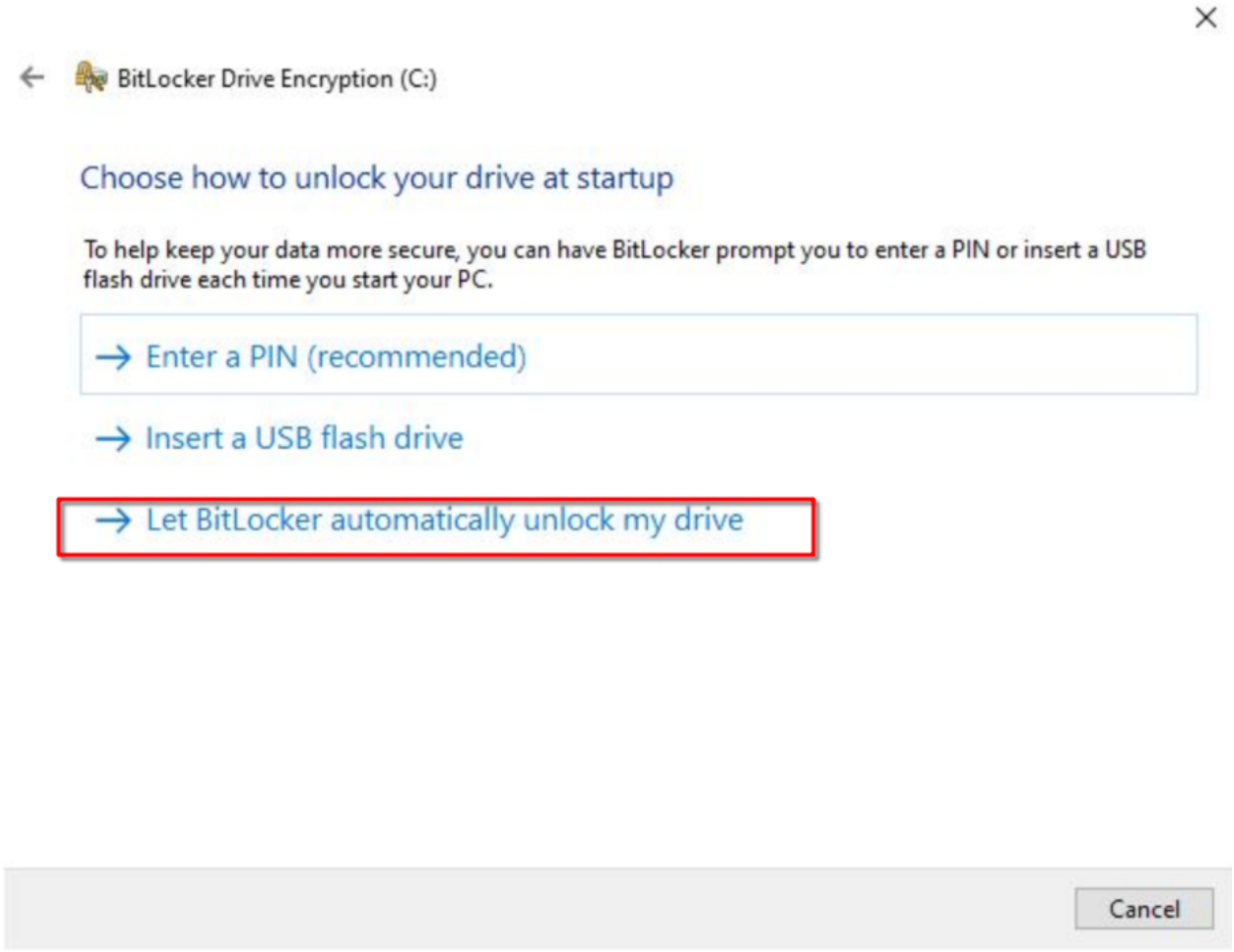
3. Check for the **Duo Desktop** icon in the task tray area. Once you see it, click on it to open Duo Desktop.

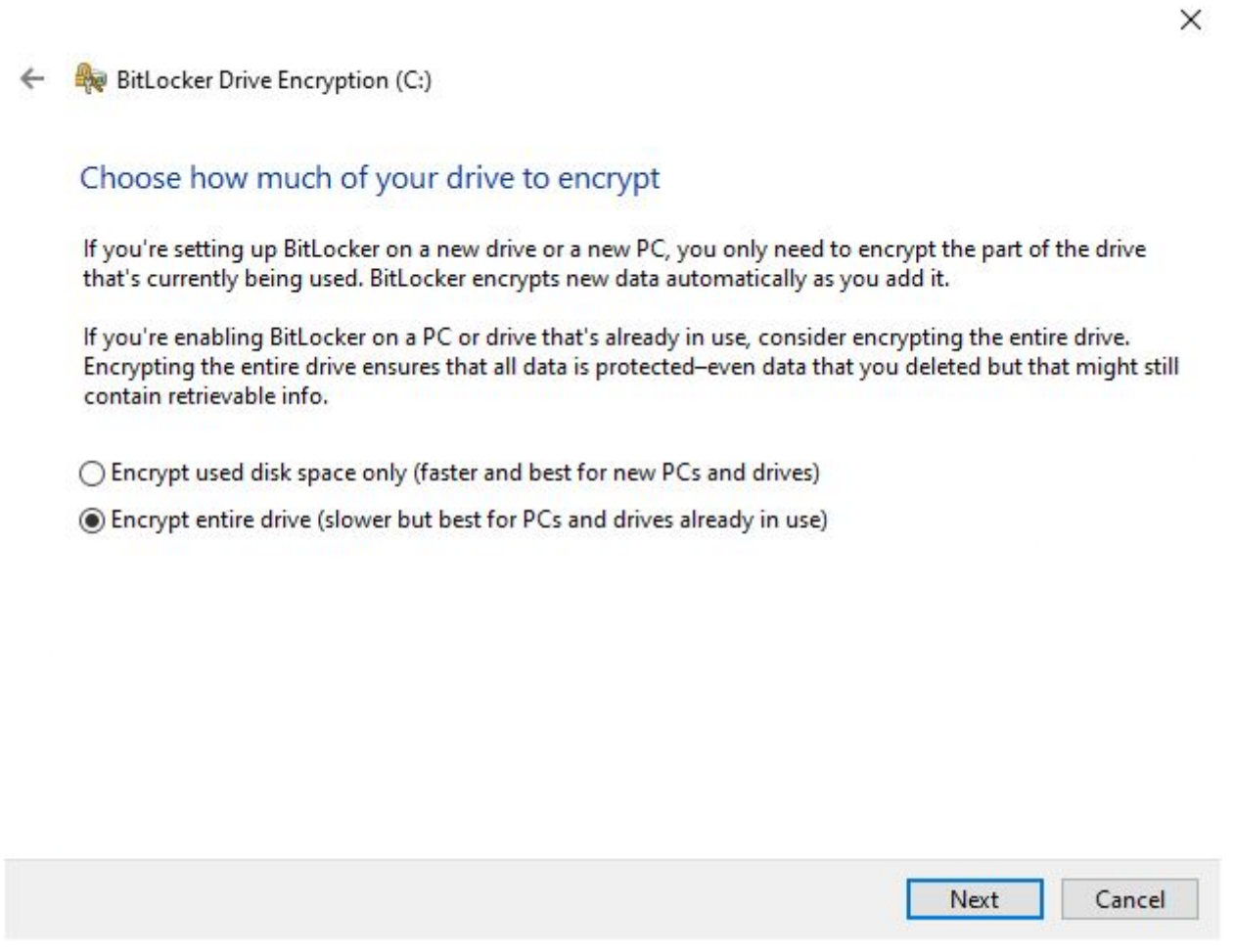


4. Duo Desktop will check for compliance, and will show you green check-marks for each requirement.

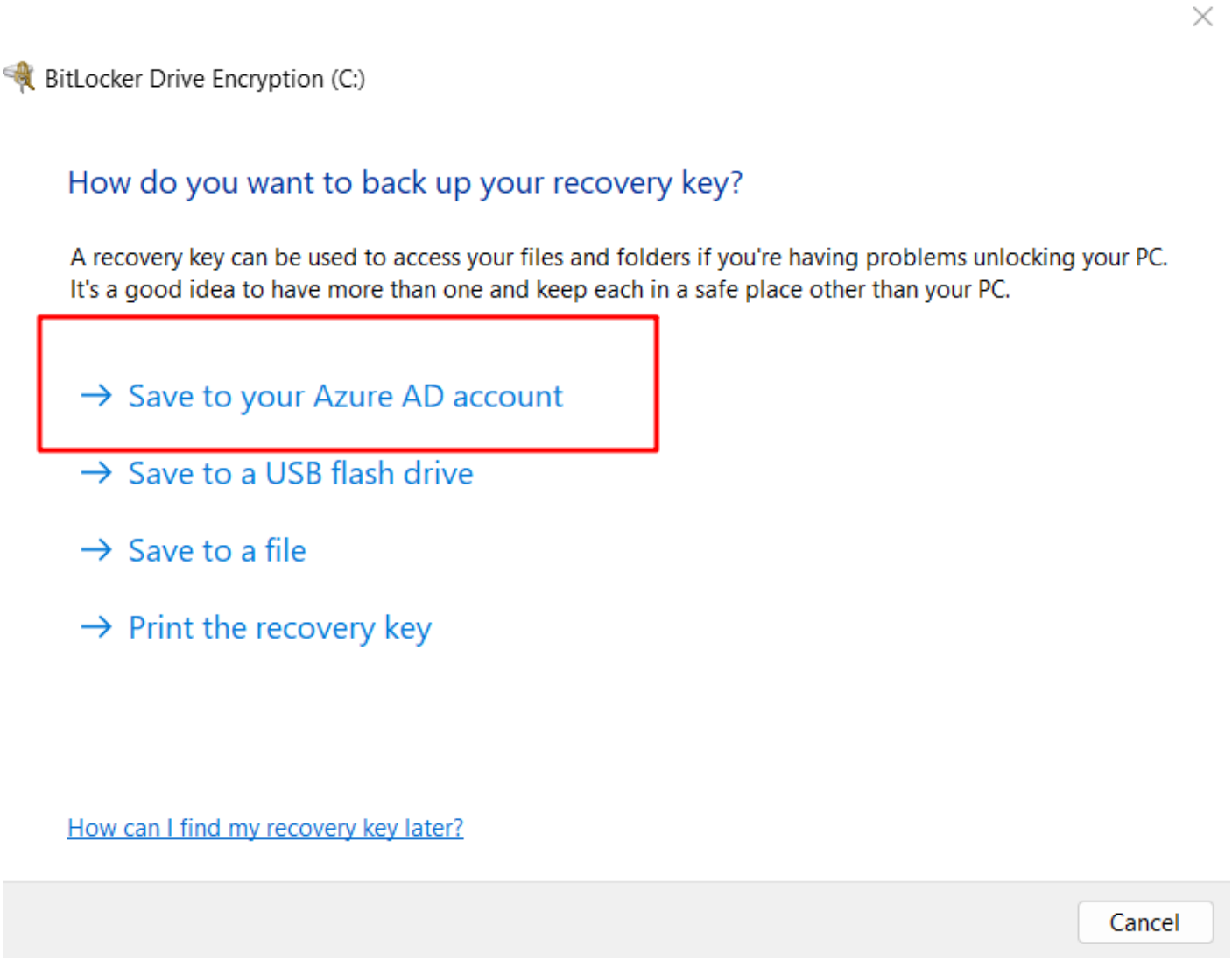


6. If you do not see a green check box for encryption, click on the message in Duo Desktop to go to Bitlocker Settings, and turn it on. Choose "Let BitLocker automatically unlock my drive"


BitLocker Drive Encryption (C:)
Choose how to unlock your drive at startup
To help keep your data more secure, you can have BitLocker prompt you to enter a PIN or insert a USB flash drive each time you start your PC.
Enter a PIN (recommended)
Insert a USB flash drive
Let BitLocker automatically unlock my drive
Cancel


BitLocker Drive Encryption (C:)
Choose how much of your drive to encrypt
If you're setting up BitLocker on a new drive or a new PC, you only need to encrypt the part of the drive that's currently being used. BitLocker encrypts new data automatically as you add it.
If you're enabling BitLocker on a PC or drive that's already in use, consider encrypting the entire drive. Encrypting the entire drive ensures that all data is protected–even data that you deleted but that might still contain retrievable info.
Encrypt used disk space only (faster and best for new PCs and drives)
Encrypt entire drive (slower but best for PCs and drives already in use)
Next
Cancel

NOTE: If you need to manually encrypt with BitLocker, choose "Save to AD account":



7. If any step is not green, click on it for for instructions to remediate it, and if you are unable to remediate it on your own, please send an email to pshelpdesk@uci.edu to open a help ticket. After all steps are green you can close the window

ZotDefend Linux Instructions

ZotDefend Linux Installation (School of Physical Sciences ONLY)

Trellix HX Agent

Trellix Installation Instructions

The .tgz package (Linux) includes the following files:
HX Client Software (tgz bundle)

1. Agent .rpm files.
2. Agent .deb files.
3. Agent .run file (xagtSetup_xx.x.x.run).
4. Agent configuration file (agent_config.json). It is critical that you import the configuration file following install to insure that the agent properly communicates with the server.

Supported Linux operations system versions:

	Linux OS	Version	File Type	Software Installation File
	Ubuntu	Ubuntu 12.04 and 14.04	.deb	xagt_34.x.x-1.ubuntu12_amd64.deb
		Ubuntu 16.04 and 18.04, 19.04, 20.04	.deb	xagt_34.x.x-1.ubuntu16_amd64.deb
	RHEL	RHEL 6.8, 6.9, and 6.10	.rpm	xagt-34.x.x-1.el6.x86_64.rpm
		RHEL 7.2, 7.3, 7.4, 7.5, 8+ 7.6, and 8 (64-bit)	.rpm	xagt-34.x.x-1.el7.x86_64.rpm
	CentOS	CentOS 6.8, 6.9, and 6.10	.rpm	xagt-34.x.x-1.el6.x86_64.rpm
		CentOS 7.2, 7.3, 7.4, 7.5, and 7.6, and 8 (64-bit)	.rpm	xagt-34.x.x-1.el7.x86_64.rpm
	Amazon	Amazon Linux AMI 2018.3, AM2	.rpm	xagt-34.x.x-1.el7.x86_64.rpm
	SUSE	SUSE 11.4	.rpm	xagt-34.x.x-1.sle11.x86_64.rpm
		SUSE 12.2, 12.3, and 15	.rpm	xagt-34.x.x-1.sle12.x86_64.rpm
	Oracle	Linux 6.10, 7.6		

Example: Installing on Ubuntu OS using .deb file

```
Open a Terminal session on the Linux endpoint that has the agent installation .tgz
package.
username@localhost:~/Desktop/FireEyeInstallDirectory$
Use the ls command to verify that the IMAGE_HX_AGENT_LINUX_33.46.0.tgz file has
been exists in the install directory.
Use the tar zxf command to unzip and extract the files from the Linux agent
Use the dpkg , medium-level package manager for Debian and the -i option to run
the .deb script and install the agent software on your Linux
endpoint. You must have sudo access.
username@localhost:~/Desktop/FireEye$ sudo dpkg -i xagt-
.ubuntu12_amd64.deb33.46.0
After the .deb installation script is complete, use the i option to import the
agent configuration file from the /opt/fireeye/bin/xagt binary path:
username@localhost:~/Desktop/FireEyeInstallDirectory$ sudo /opt/fireeye/bin/xagt -
i agent_config.json
Start the agent services on your Linux endpoint using the following command:
username@localhost:~/Desktop/ FireEyeInstallDirectory$ sudo systemctl enable --now
xagt
```

Nessus Tenable Agents

Nessus Tenable Agent Installation Instructions

1. Make sure outbound traffic from port 443 to nessus.oit.uci.edu is allowed through your firewall.
2. Install the Tenable agent with your package manager from the link above.
3. Contact pscsg@uci.edu to get the tenable key.
4. Run as root or with sudo: **/opt/nessus_agent/sbin/nessuscli agent link --host=nessus.oit.uci.edu --port=443 --key=KEY_PROVIDED_BY_PSCSG**

Duo Desktop Downloads:

- **Linux .deb Package (Debian Based eg Ubuntu)** https://desktop.pkg.duosecurity.com/duo-desktop-latest.amd64.deb
- **Linux .rpm Package (RHEL based)** https://desktop.pkg.duosecurity.com/duo-desktop-latest.x86_64.rpm

Duo Desktop Agent Installation Instructions

1. Download the appropriate package for your distribution from the above link.
2. Install the package.
3. Enable the service. Eg on systemd distributions, run

   ```
   sudo systemctl enable --now duo-desktop
   ```

4. Check to make sure the duo-desktop service is running. Eg. on systemd distributions, run

   ```
   sudo systemctl status duo-desktop
   ```

5. If you get SELinux erros relating to .NET services, it's most likely Duo Desktop. Create an exception via:

   ```
   ausearch -c '.NET TP Worker' --raw | audit2allow -M my-NETTPWorker
   semodule -X 300 -i my-NETTPWorker.pp
   ```