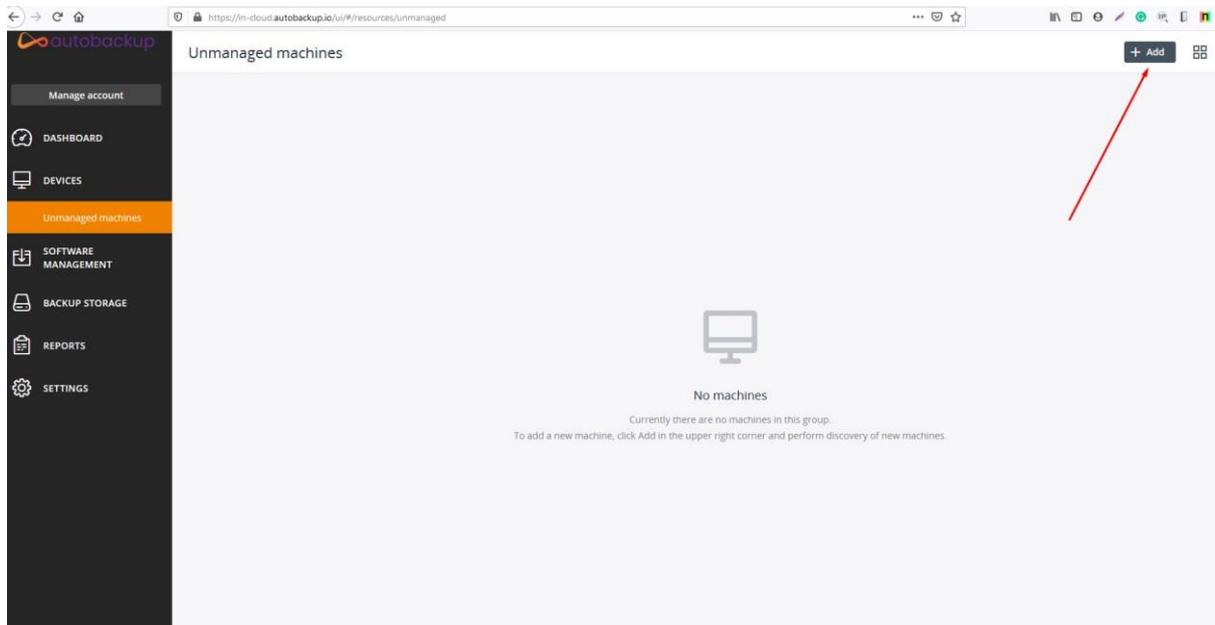
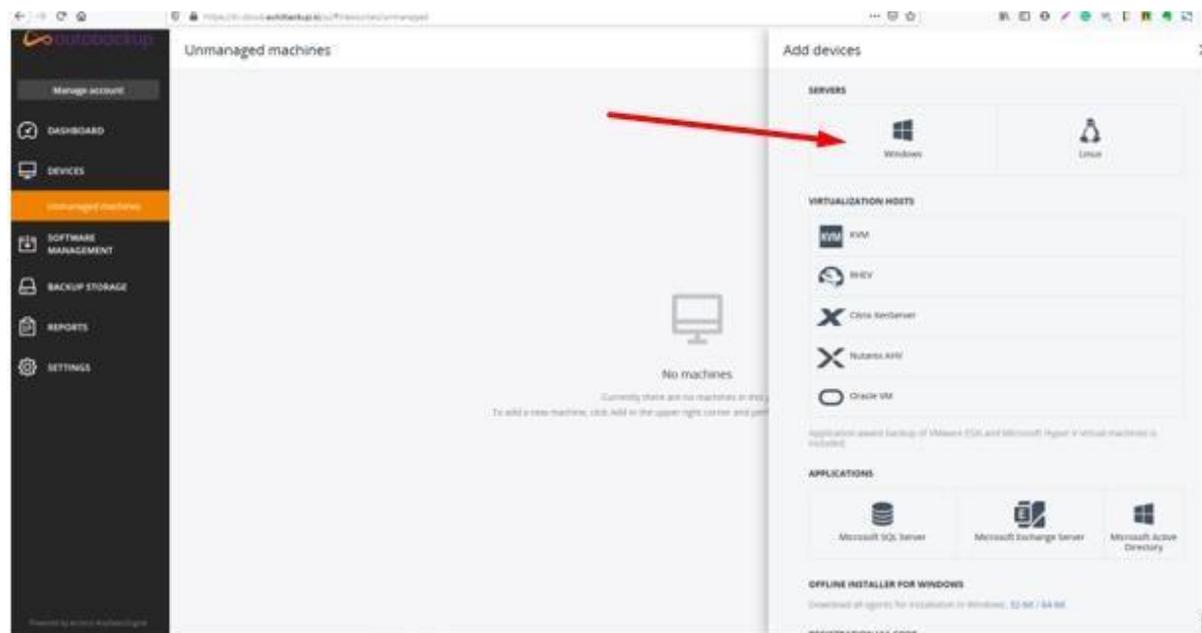


How to add Windows Server in Autobackup

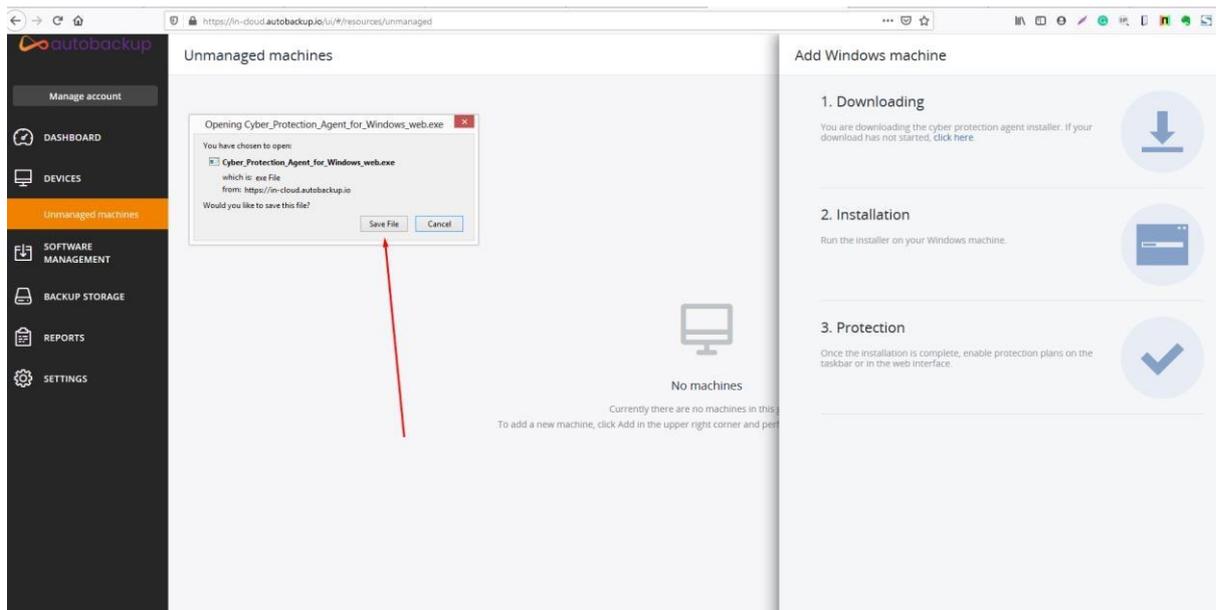
Step 1: Click on Add Button



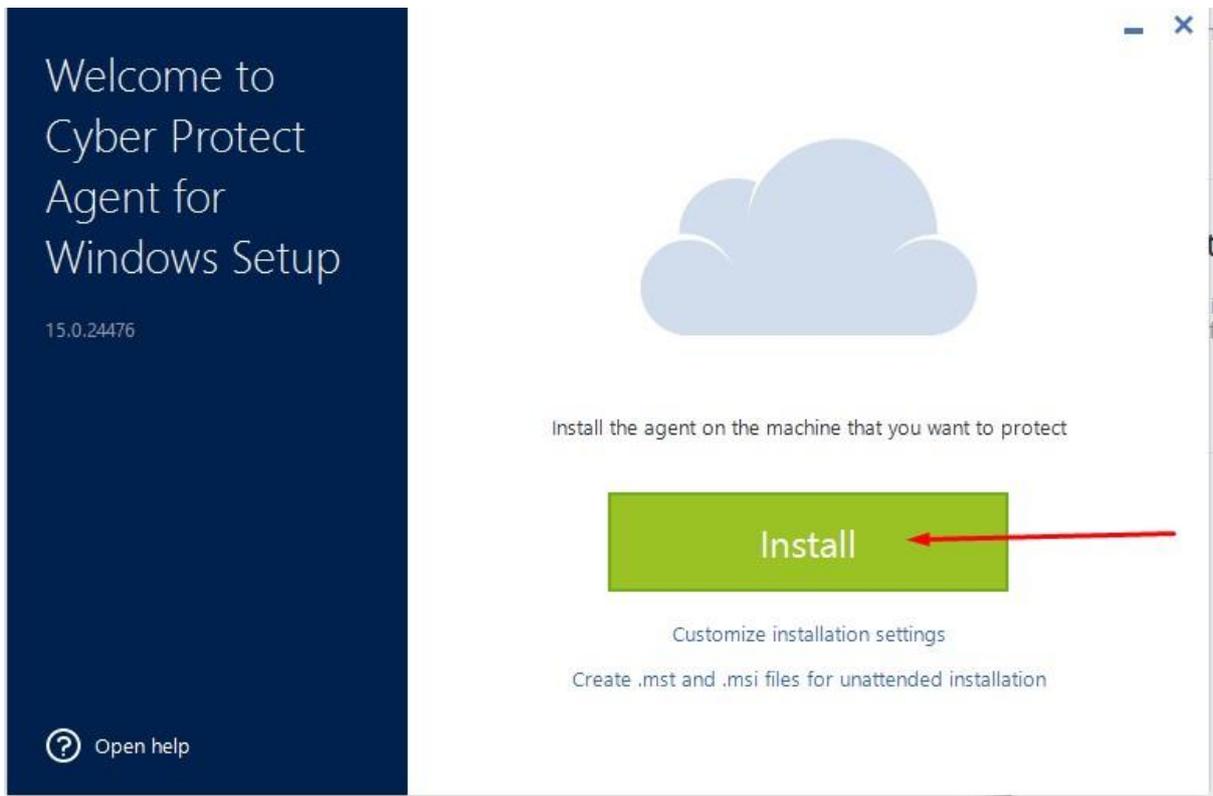
Step 2: Click on Windows



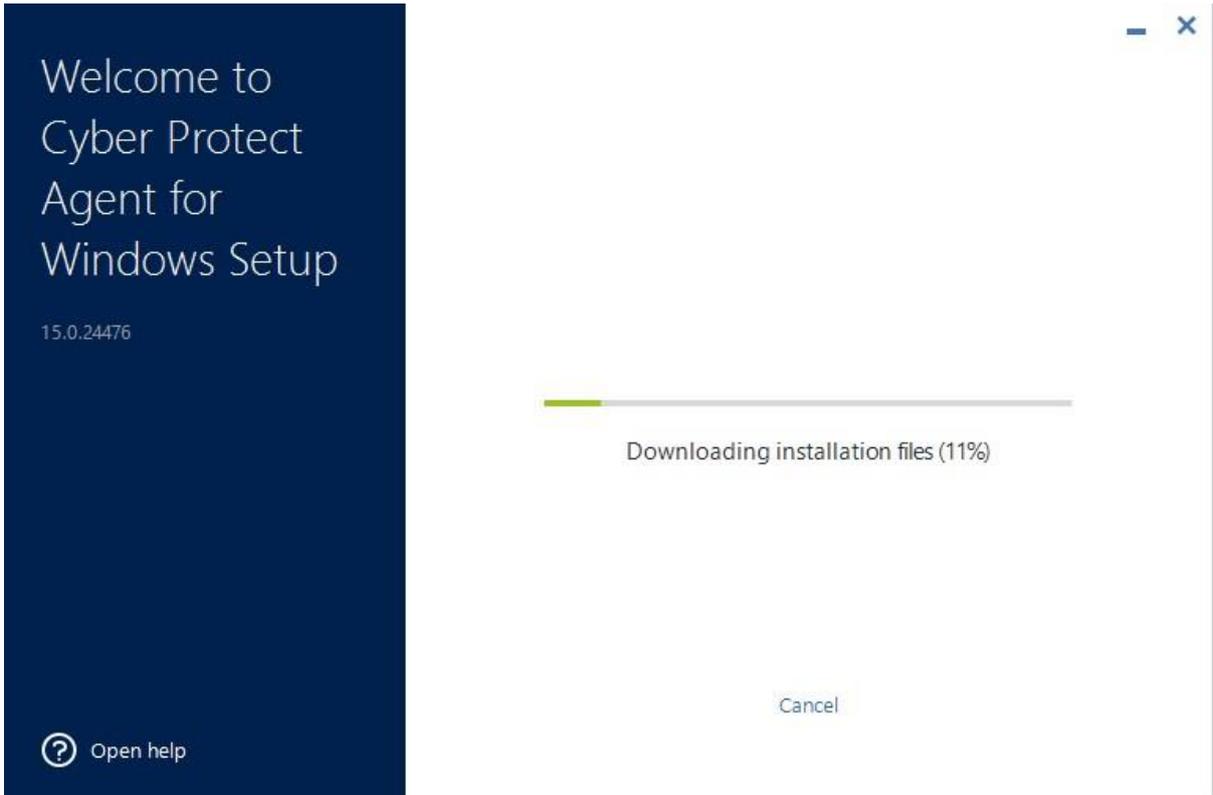
Step 3: An installer is downloaded in your machine that you want to add for cyber backup



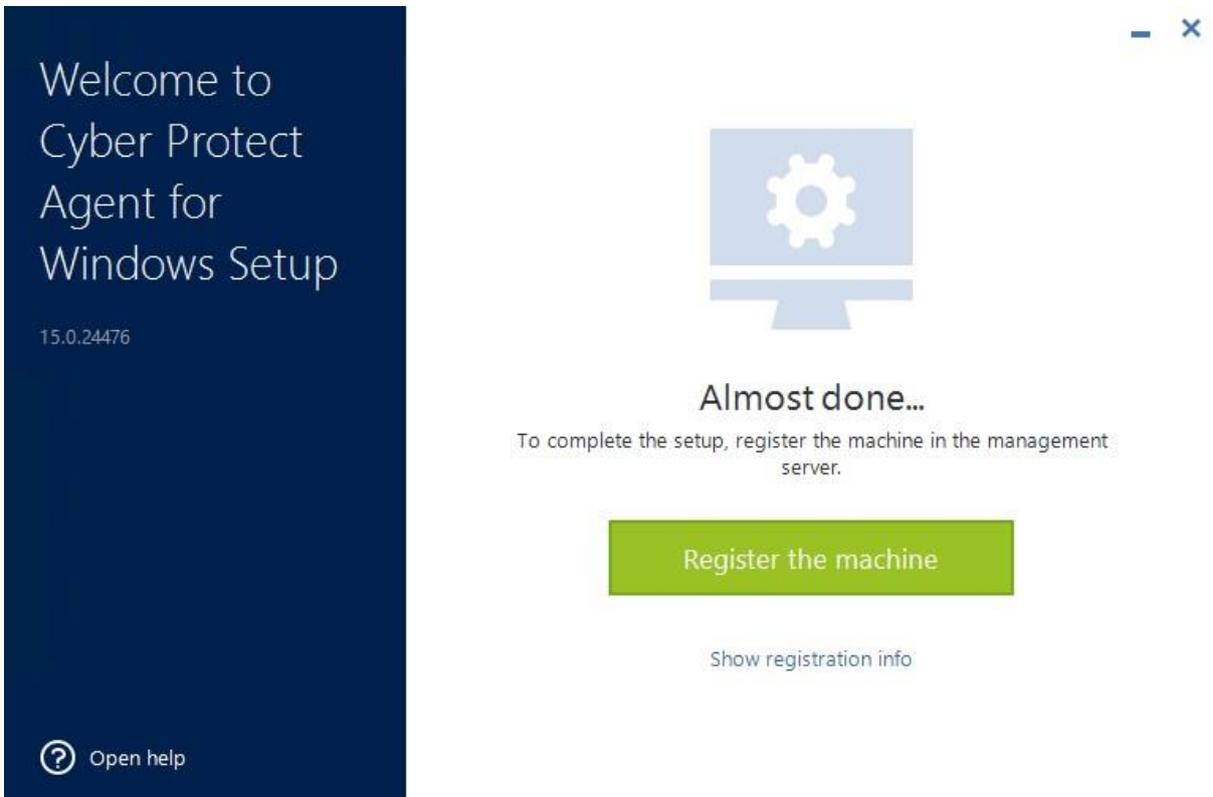
Step 4: Run that installer file in your machine and then click on the install button



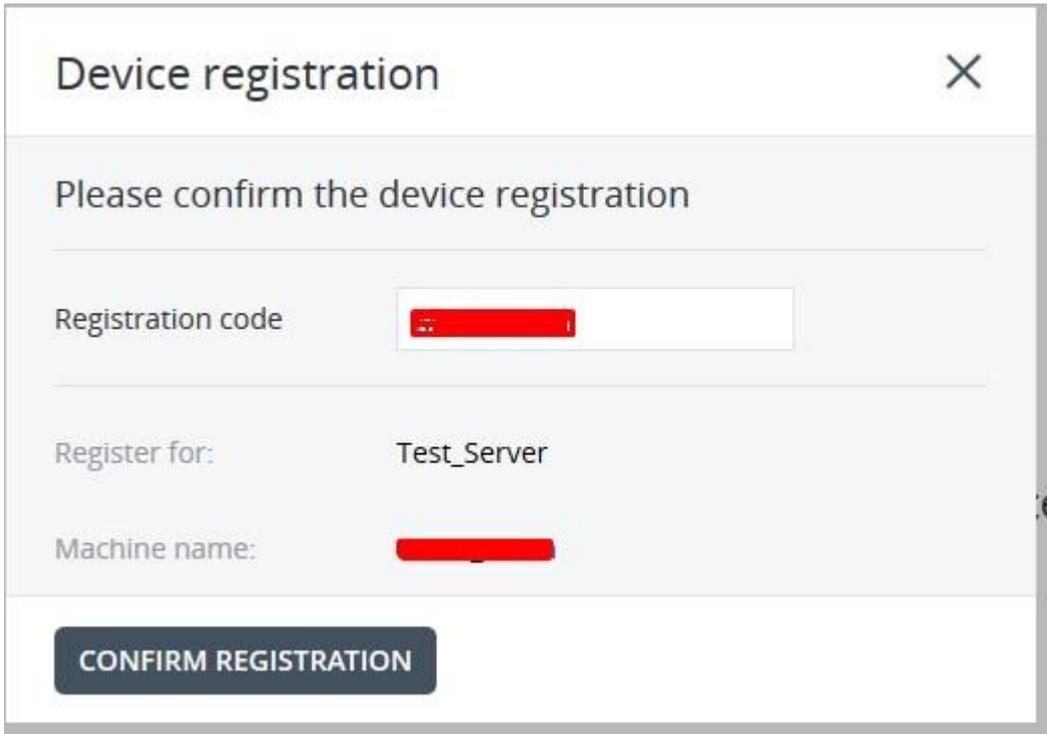
Step 5: Now agent is installing in your machine



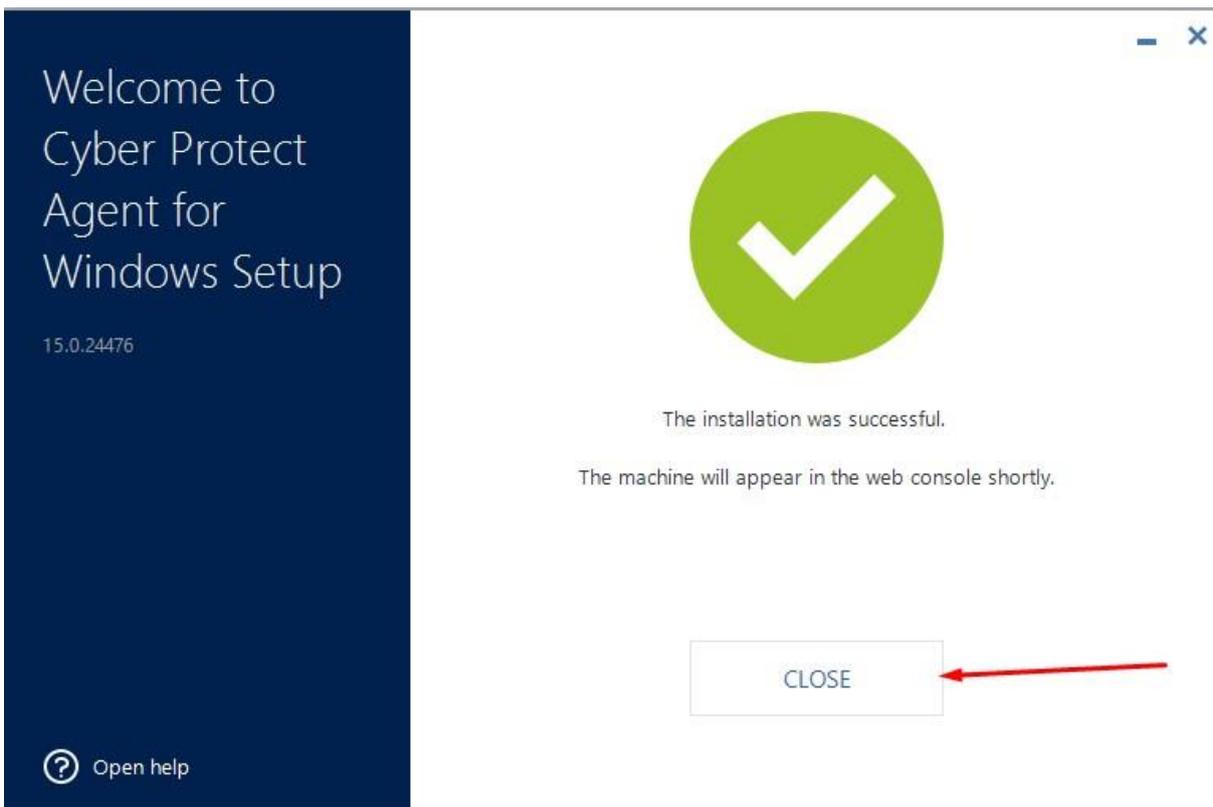
Step 6.1: Now you just need to register your machine at cloud management portal for that click on **Register the Machine** button



Step 6.2: After that you will get the registration Code, you just need to click on Confirm Registration

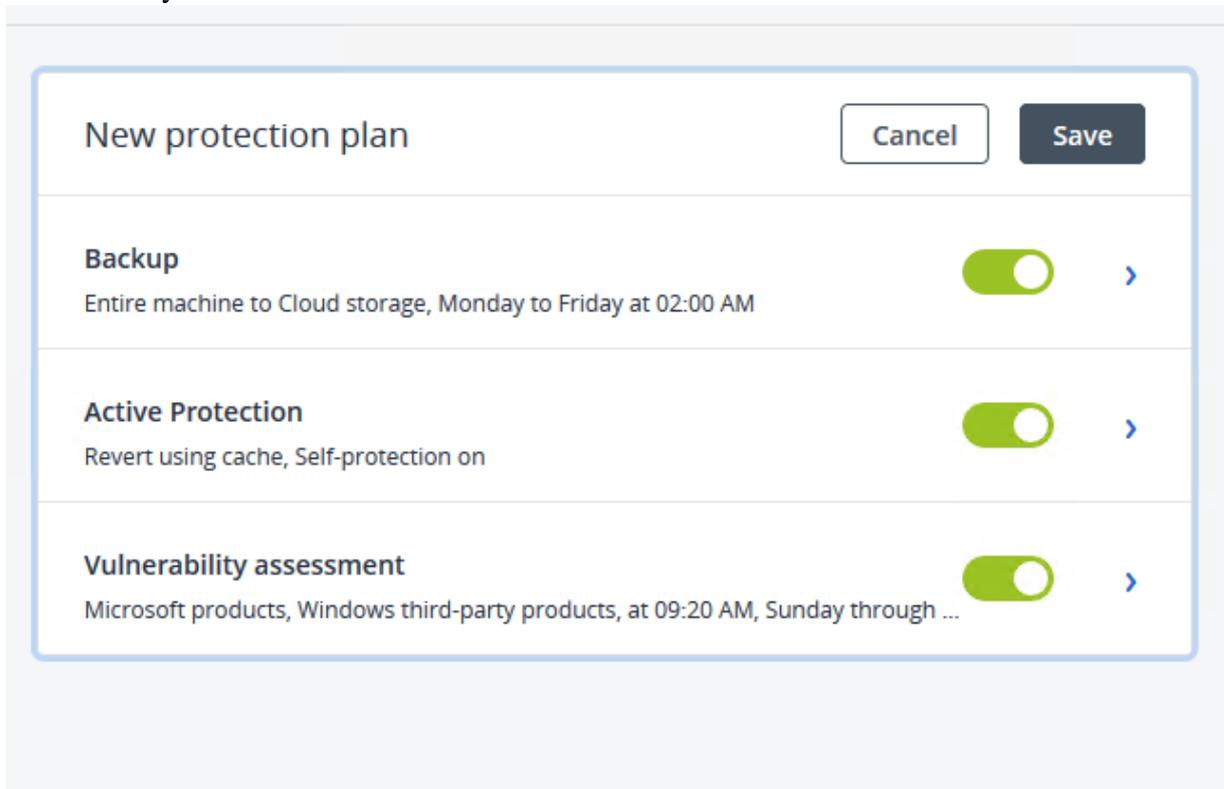


Step 6.3: After that you will get this popup just close this window.



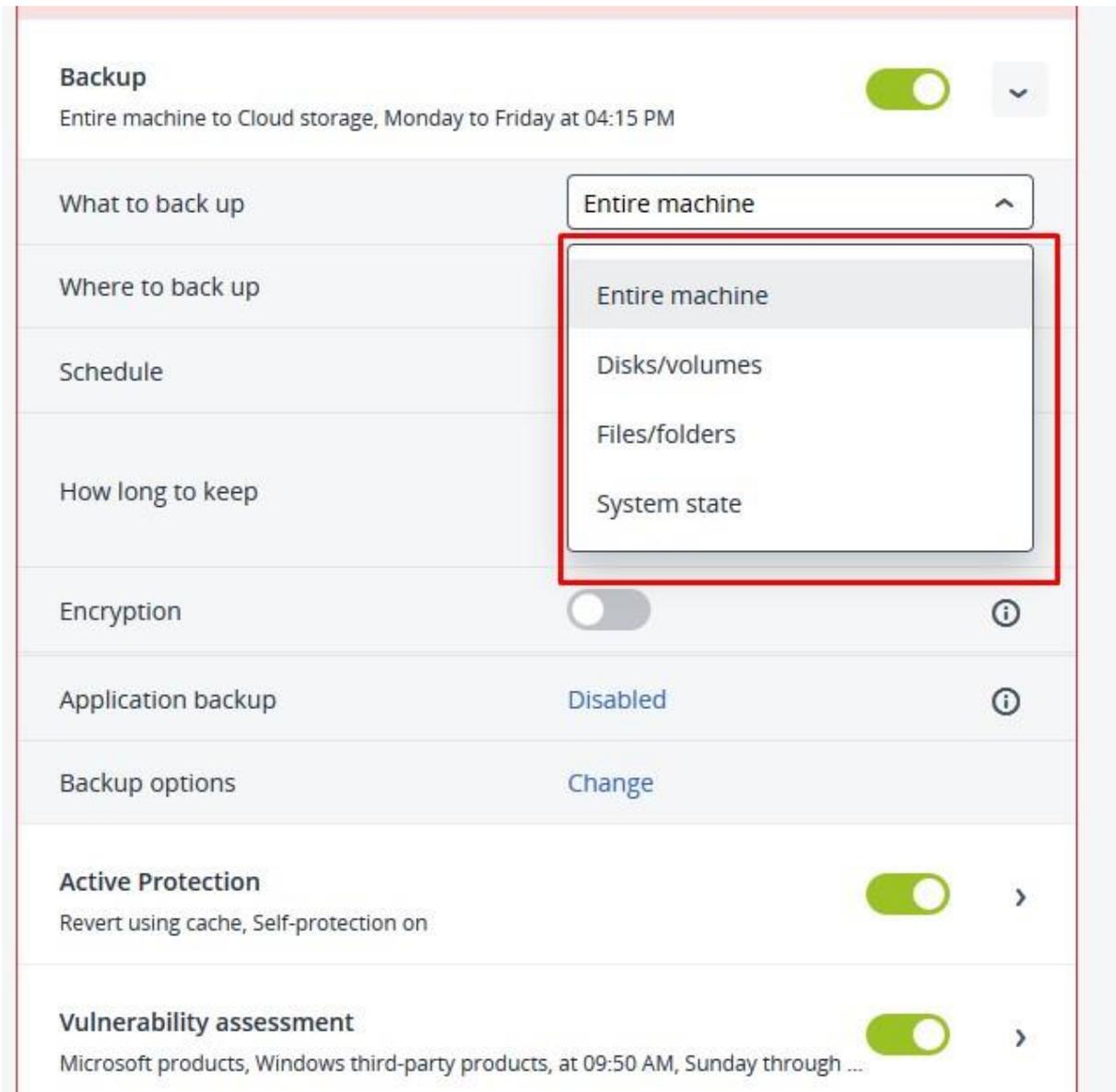
Step 7: When you Enable Protection there are 3 different options that we need to understand clearly for the protection of our data and proper backup.

- a) Backup
- b) Active Protection
- c) Vulnerability Assessment

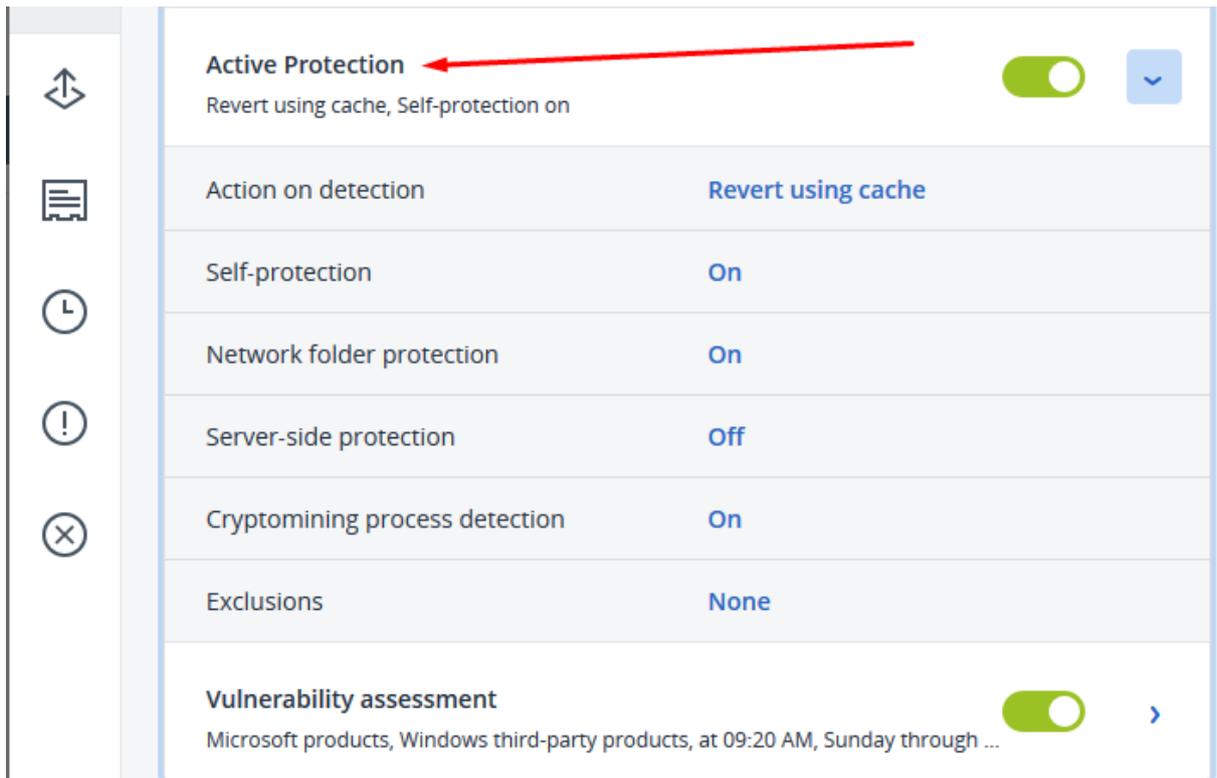


Step 7.1(Backup): After registering your machine at autobackup you need to select backup plan according to your requirement.

Devices >> All Devices >> Enable Protection



Step 7.2(Active Protection): This step is very important for us as it is used to protect our data from ransomware.



a) Action on Detection: -

Action on detection

- Notify only
Generate an alert about the process suspected of ransomware activity.
- Stop the process
Generate an alert and stop the process suspected of ransomware activity.
- Revert using cache
Generate an alert, stop the process, and revert file changes by using the service cache.

b) Self-Protection:

Self-protection ✕

Self-protection prevents unauthorized changes to the software's own processes, registry records, executable and configuration files, and backups located in local folders.

Self-protection

Allow specific processes to modify backups

Request password on an attempt to modify components list locally on the device

Password protection [Generate new password](#)

c) Network Folder Protection:

Network folder protection ✕

This option defines whether Antivirus & Antimalware protection protects network folders that are mapped as local drives. The protection applies to folders shared via SMB or NFS protocols.

Protect network folders mapped as local drives

Files restored by using the 'Revert using cache' operation will be saved to the following local folder:

The 'Revert using cache' operation does not support file recovery to network folders or mapped drives. You can restore files only to a local disk.

d) Server-Side Protection:

Server-side protection ✕

This option defines whether Antivirus & Antimalware protection protects network folders that are shared by you from the external incoming connections from other servers in the network that may potentially bring threats.

Server-side protection

e) Cryptomining Process Detection:

Cryptomining process detection ✕

This option protects against cryptomining malware to prevent unsanctioned using of computer resources.

Detect cryptomining processes

Notify only
Generate an alert about the process suspected of cryptomining activities.

Stop the process
Generate an alert and stop the process suspected of cryptomining activities.

f) Exclusions:

Exclusions ✕

ℹ Environment variables are currently supported on Windows only

Trusted	Blocked
---------	---------

Specify processes that will never be considered malware. Processes signed by Microsoft are always trusted.

Processes + Add

Specify folders where file changes will not be monitored.

Folders + Add

Step: 7.3(Vulnerability Assessment): With this step we're going to configure to check whether there is any vulnerability in your server or not (Process of Identifying, Quantifying, and Prioritizing the vulnerabilities in a system).

Applied protection plan: 1

 Add plan

New protection plan

Cancel

Save

Backup

Entire machine to Cloud storage, Monday to Friday at 02:00 AM



Active Protection

Revert using cache, Self-protection on



Vulnerability assessment

Microsoft products, Windows third-party products, at 09:20 AM, Sunday through ...



Vulnerability assessment scope

Microsoft products, Windows third-party products

Schedule

At 09:20 AM, Sunday through Saturday

a) Vulnerability Assessment Scope:

What to scan

Select the items that you want to scan for vulnerabilities.

Windows machines:

- Microsoft products
 - Windows third-party products
-

[Supported products](#)

b) Schedule

Schedule ✕

Schedule the task run using the following events

Schedule by time ▼

Schedule type ▼

Daily

Sun	Mon	Tue	Wed	Thu	Fri	Sat
-----	-----	-----	-----	-----	-----	-----

Start at ▼

09:20 AM

Run within a date range

Start conditions ⓘ

Distribute task start time within a time window

− 1 + Hour(s) ▼

If the machine is turned off, run missed tasks at the machine startup

Prevent the sleep or hibernate mode during task running

- If the machine is turned off, run missed tasks at the machine startup
 - Prevent the sleep or hibernate mode during task running
 - Wake up from the sleep or hibernate mode to start a scheduled task
 - User is idle
 - Users logged off
 - Fits the time interval
 - Save battery power
 - Do not start when on metered connection
 - Do not start when connected to the following Wi-Fi networks
 - Check device IP address
-
- If start conditions are not met, run the task anyway after

So, this is the process through which you can add your windows server and select the backup plan with relevant security features. according to your needs.