How to add Windows Server in Autobackup

Step 1: Click on Add Button

()-	→ C' û	🛛 🗎 https://in-doud.autobackup.io/ui/#/resources/unmanaged 🛛 💀 🖓	9 G IN 🖸 O 🗡 😁 🔍 🖡	n
0	autobackup	Unmanaged machines	+ Add	88
	Manage account			
ග	DASHBOARD			
Ð	DEVICES			
	Unmanaged machines		/	
U	SOFTWARE MANAGEMENT			
⊜	BACKUP STORAGE			
¢	REPORTS			
ŝ	SETTINGS	No machines		
		Currently there are no machines in this group. To add a new machine, click Add in the upper right corner and perform discovery of new machin	ies.	

Step 2: Click on Windows

+ - C Q	9 & republication address block interview over		10 th	N D O / O	N. D. M. M. M.
Columbia	Unmanaged machines		Add devices		
Manage account			SERVERS		
🔿 оконаснао				2	2
E DEVICES			Windowy	Lin	
Internet destrict	-		VIRTUALIZATION HOITS		
MANAGEMENT			NAME AND A		
		_	(C) ==v		
🖨 serores			X Chris Kerdenset		
G ATTINGS		No machines	× Notamon and		
		Conversity theirs are not marked as the To add a new marking which add as the paper rates are not as	O OWNER MARK		
			Application assets factory of the material	neri 150. ati 100 mili 1450 vi 10	ad machines in
			APPLICATIONS		
			Managarit SQL Server	Mercardt Incharge Server	Monauth Active Directory
			OFFLINE INSTALLER FOR WIND Described of open for regular	own or in tendence, 12 art / MA MA	
			REFERENCE VIA CODE		

Step 3: A 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

Please confirm th	ne device registration	
Registration code		
Register for:	Test_Server	
Machine name:		

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

Welcome to Cyber Protect Agent for Windows Setup	
	The installation was successful.
	The machine will appear in the web console shortly.
	CLOSE
⑦ Open help	

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

	indig at overo the	
What to back up	Entire machine	^)
Where to back up	Entire machine	
Schedule	Disks/volumes	
How long to keep	Files/folders System state	
Encryption		0
Application backup	Disabled	0
Backup options	Change	
Active Protection Revert using cache, Self-protection on		•

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

↔	Active Protection Revert using cache, Self-protection on	
	Action on detection	Revert using cache
6	Self-protection	On
0	Network folder protection	On
()	Server-side protection	Off
\otimes	Cryptomining process detection	On
	Exclusions	None
	Vulnerability assessment Microsoft products, Windows third-party products	s, at 09:20 AM, Sunday through

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:

C:\ProgramData\Acronis\Restored Network Files

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.

х

х

d) Server-Side Protection:



f) Exclusions:

Exclusions	×				
i Environment variables are currently supporte	ed 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 monit	ored.				
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 pro	ducts, 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:



Windows third-party products

C Supported products

b) Schedule

Schedule

Schedule the task run usi	ng the follo	wing events							
Schedule by time	ing the rollo	ing crents	,						~
Schedule type				Tur	Mad	Thu	E.	Cat	
Daily	~	Sun	Mon	Tue	wea	Inu	Fri	Sat	J
Start at									
09:20 AM	~								
 Run within a date range Start conditions (i) 									
Distribute task s	start time	within a ti	me windo	w					
- 1	+	Hour(s)		~					
If the machine is	s turned o	off, run mis	ssed tasks	at the m	achine sta	artup			
Prevent the sleep	en or hihe	rnate mod	le during t	ask runn	inσ				

×

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