

CryptoStopper – Installation and User Guide

Table of Contents

Helpful Links.....	2
Overview	3
Installation Instructions	3
Whitelisting Programs.....	12
CryptoStopper Service	13
Remediation/Windows Firewall	14
Change Email Address.....	14
Watcher Files	15
GPO Deployment	16
JSON Configuration Template.....	16
Explanation of JSON config file	17
How to use Group Policy to remotely install software in Windows Server 2003 and Windows Server 2008	17
Troubleshooting GPO Installation.....	18
Frequently Asked Questions (FAQ).....	19



Helpful Links:

Two-Minute Install Video:

<https://www.watchpointdata.com/cryptostopper/cryptostopper-installation-video/>

Schedule Install Assistance:

<https://go.watchpointdata.com/get-a-demo>

Weekly Webinar Demo Signup:

<https://go.watchpointdata.com/weekly-live-demo-registration>

Overview: This document explains how to install CryptoStopper software on a Windows workstation or server. The document also covers configuring CryptoStopper settings and GPO deployment.

Installation Instructions

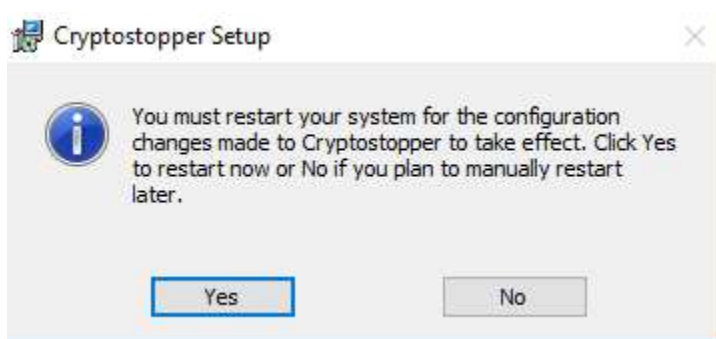
- 1) Double-click CryptoStopper.exe to start the software installation.



- 2) Review the CryptoStopper License Agreement then check the box "I accept the terms in the License Agreement."
- 3) Next, click the "Install" button.
- 4) Click "Finish" once the installation is complete.



- 5) Click “Yes” to reboot when the installation has completed.



- 6) The CryptoStopper Installation is complete.

User Guide

Protecting Data Folders with CryptoStopper

CryptoStopper can be installed on a workstation or server. Adding folders or server shares to CryptoStopper protection is very straightforward. When a folder is protected, CryptoStopper will deploy hidden “watcher files” to the selected folders that continuously monitor for ransomware activity. If any of the “watcher files” are touched, CryptoStopper will activate its defenses.

WatchPoint highly recommends installing CryptoStopper on both your network servers and workstations. Ransomware almost always starts at the workstation, but not all ransomware behaves the same way. Some variants attack the workstation only. Others attack the workstation and then enumerate the network share while others skip the workstation altogether and immediately attack mapped drives. Having both CryptoStopper Workstation and CryptoStopper Server installed will mitigate both potential ransomware scenarios.

There are three options when adding or removing folders from CryptoStopper Ransomware protection.

Option 1. Single-Click to protect the folder three layers deep. This provides what we call “Blanket Protection” that watches the top layer directories where ransomware starts. This is the recommended installation method.

Option 2. Shift-Click to select all the folders in a directory or share. Only use this option when you have less than 1000 child-folders in the selected directory or share.

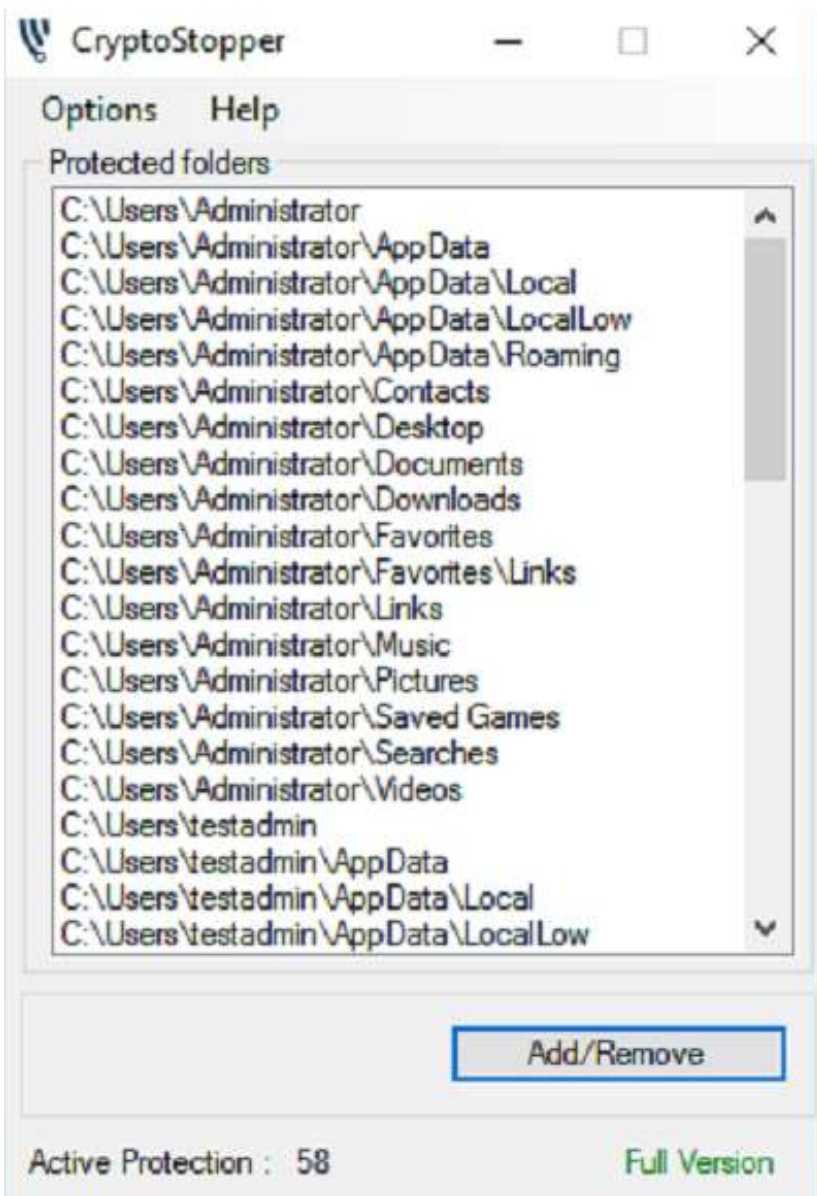
Option 3. Single-Click to select or deselect additional child folders beyond those selected in Option 1.

Add/ Modify Protected Folders

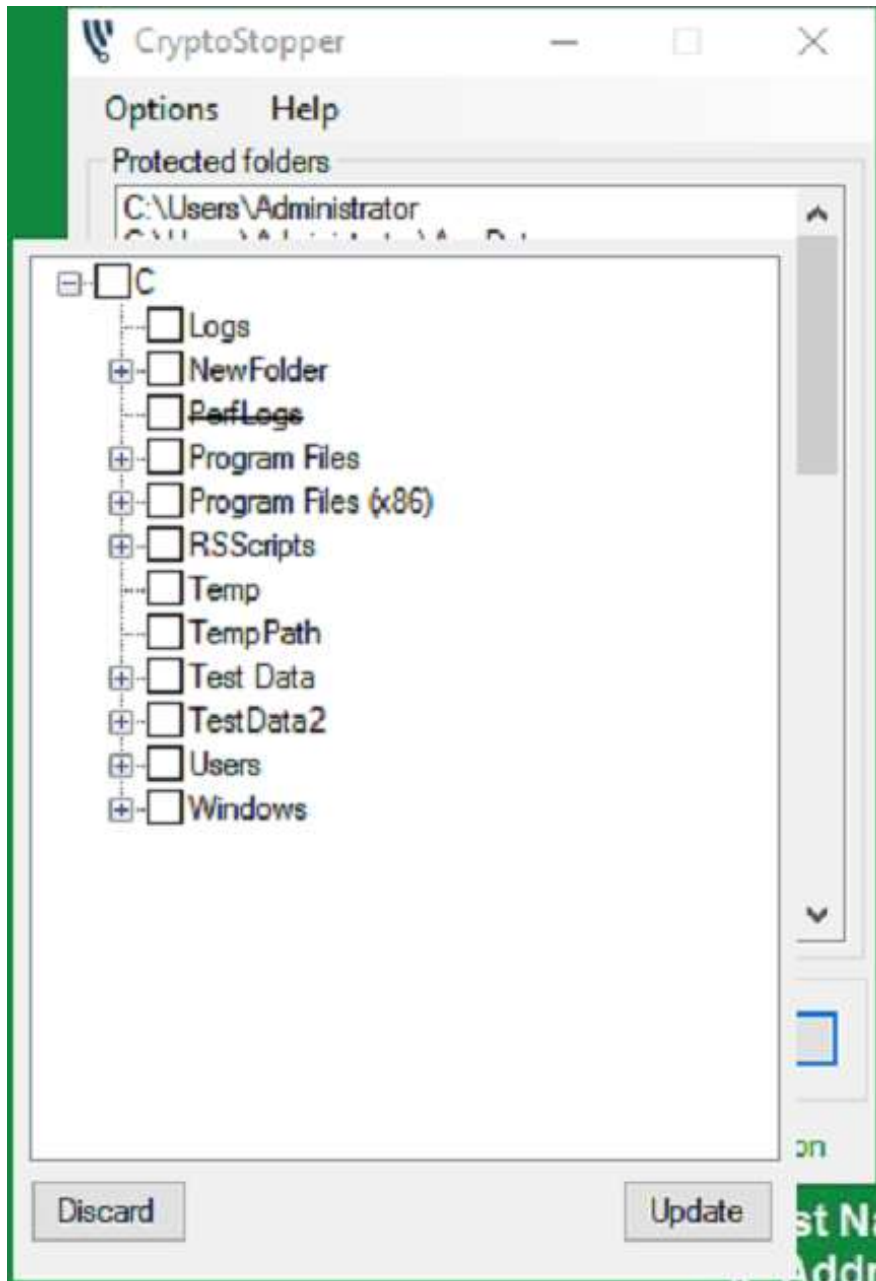
- 1) Open CryptoStopper from the desktop icon or the tray icon.



- 2) Click the "Add/Remove" button.

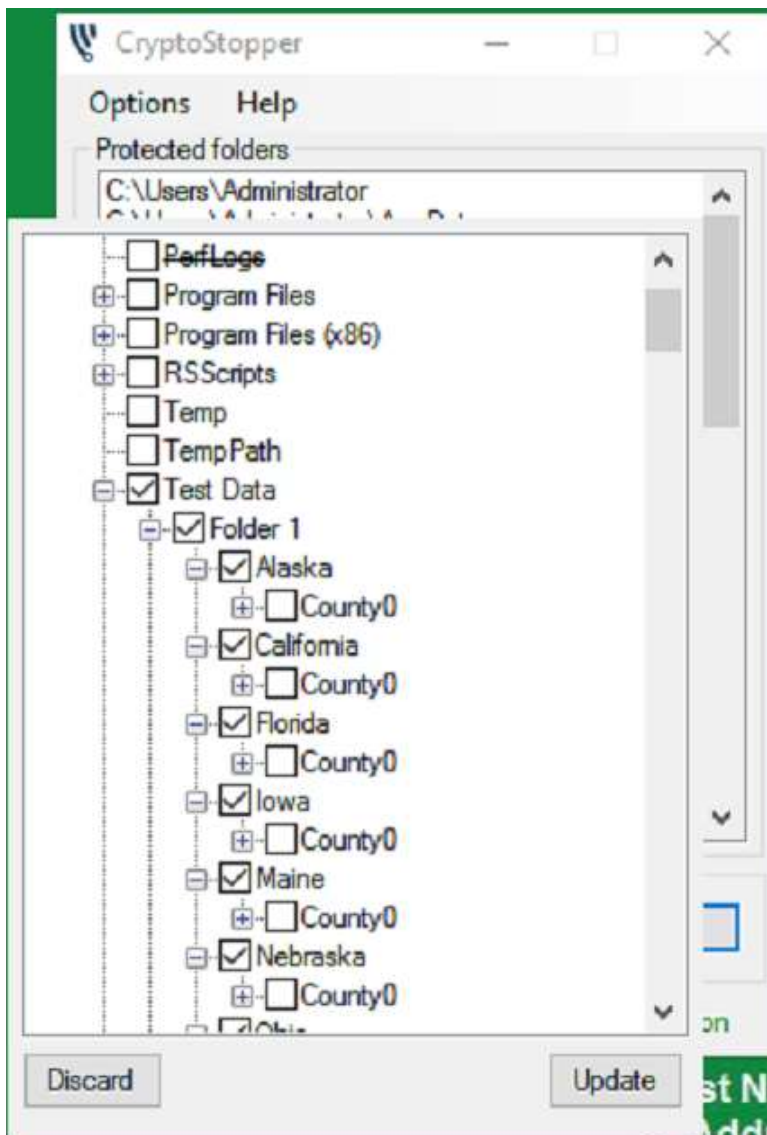


3) Expand the drive that contains the folders that you want to protect.

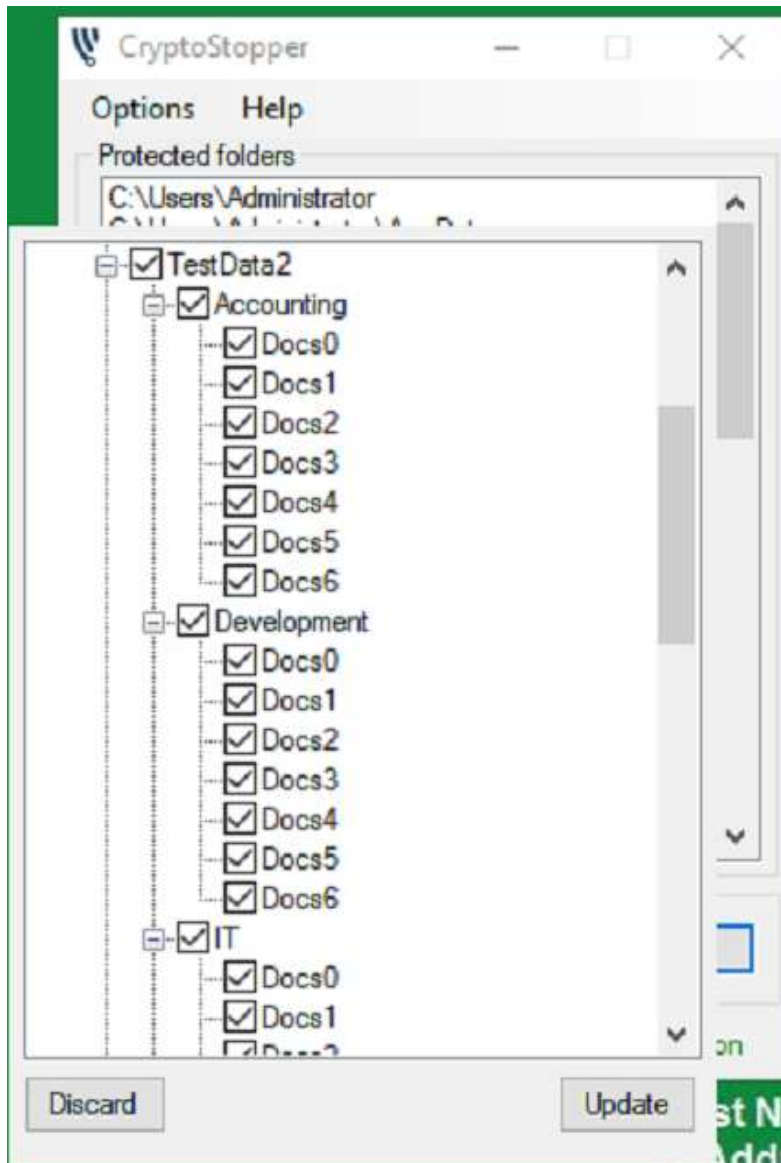


4) Single-click any folder on a workstation or any file share on a server to protect the root of that folder, the child folders in the root and the child(ren) of the child folder(s). In this example, single-click the server share called “Test Data.” Test Data contains 100,000 folders.

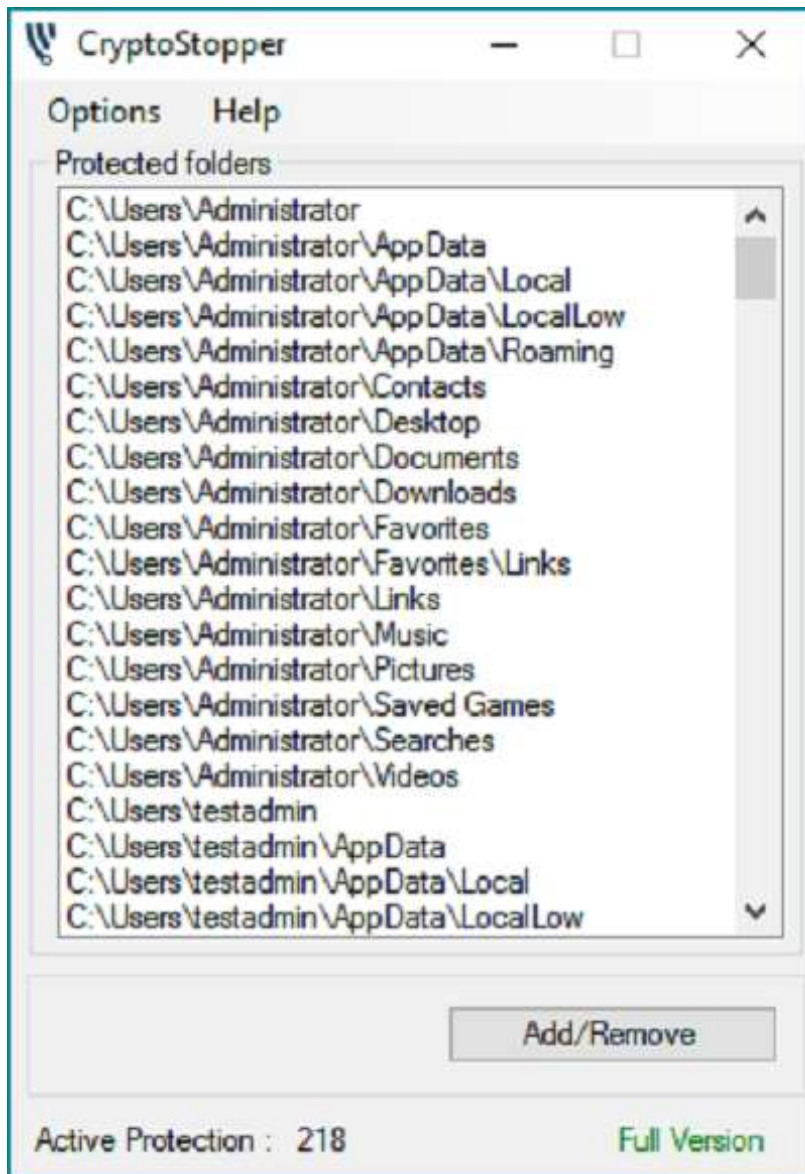
In the following screenshot, you’ll see that Test Data is the folder share. Folder 1 is the first child folder, and the folders with state names like Alaska, California, and Florida are the 2nd level child folders. This is three-layer protection. (Root – Children – Children)



5) Shift-Click a folder on a workstation or any file share on a server to protect the root and all the child folders. In this second folder selection example, shift-click the folder “Test Data2” to protect the root and all the child folders.



6) Once you have finished with your selection you can press “Discard” to exit without making any changes, or you can press “Update” to add those selected folders to the protection list. The number of folders protected is listed as “Active Protection: XXX” in the lower left corner of the application.



Configure CryptoStopper Settings Button

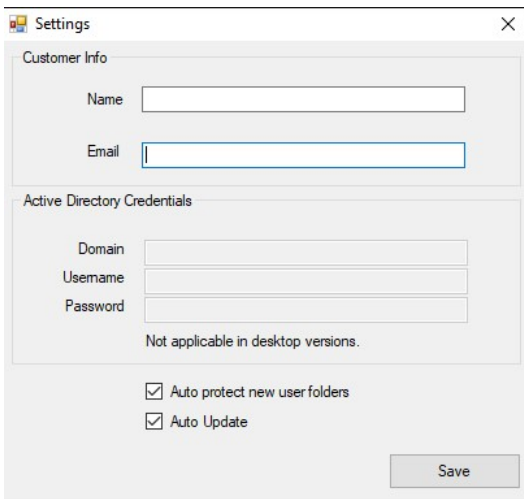
Customer Information: Configuring the settings is necessary for CryptoStopper to work properly. You must configure the company name and email address. This email address is the address that will receive alerts in the event of a ransomware attack. This email can be different than the address you used to register the software. WatchPoint suggests setting up a distribution group for email notification so that more than one person receives the ransomware attack notification.

Active Directory Credentials: When installing on a server, you should also configure the domain settings. Configuring the domain settings will allow CryptoStopper Server to send a shutdown command to the workstation after it has been isolated from the network share. If the domain settings are not configured, CryptoStopper will still stop the attack against the network share by isolating the infected host from the share, but the workstation will not get shut down.

Auto protect new user folders: This box is selected by default. Checking this box protects new user profiles added after the installation of CryptoStopper.

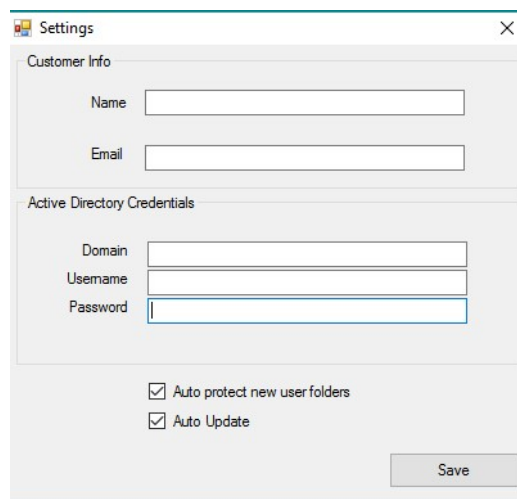
Auto Update: This box is selected by default. Checking this box allows CryptoStopper to update automatically.

Workstation Settings



The screenshot shows the 'Settings' dialog box for a workstation. It has a title bar with a close button. The 'Customer Info' section contains 'Name' and 'Email' text boxes. The 'Active Directory Credentials' section contains 'Domain', 'Username', and 'Password' text boxes, with a note below stating 'Not applicable in desktop versions.' At the bottom, there are two checked checkboxes: 'Auto protect new user folders' and 'Auto Update'. A 'Save' button is located at the bottom right.

Server Settings



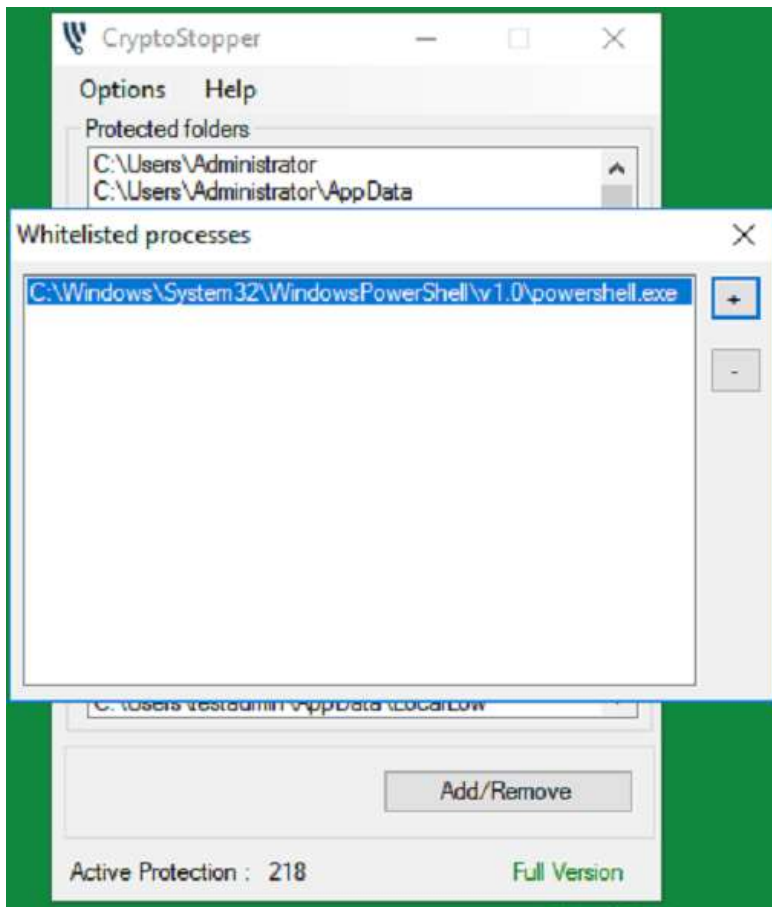
The screenshot shows the 'Settings' dialog box for a server. It has a title bar with a close button. The 'Customer Info' section contains 'Name' and 'Email' text boxes. The 'Active Directory Credentials' section contains 'Domain', 'Username', and 'Password' text boxes. At the bottom, there are two checked checkboxes: 'Auto protect new user folders' and 'Auto Update'. A 'Save' button is located at the bottom right.

Make sure and click “Save” after entering the settings and close the Settings window. CryptoStopper will verify and alert you if your credentials are invalid.

Now that you have protected folders and configured settings, CryptoStopper is fully configured and ready to detect and stop ransomware.

Whitelisting Programs

If you need to whitelist any program that is creating false positive alerts, you can do that in the CryptoStopper GUI. CryptoStopper will ignore any process that is whitelisted. You will rarely use this feature, but WatchPoint made it available if you do need it.



There are two ways to whitelist a process. One is from CryptoStopper GUI. The second option is to whitelist a running process for which CryptoStopper has generated a false positive alert.

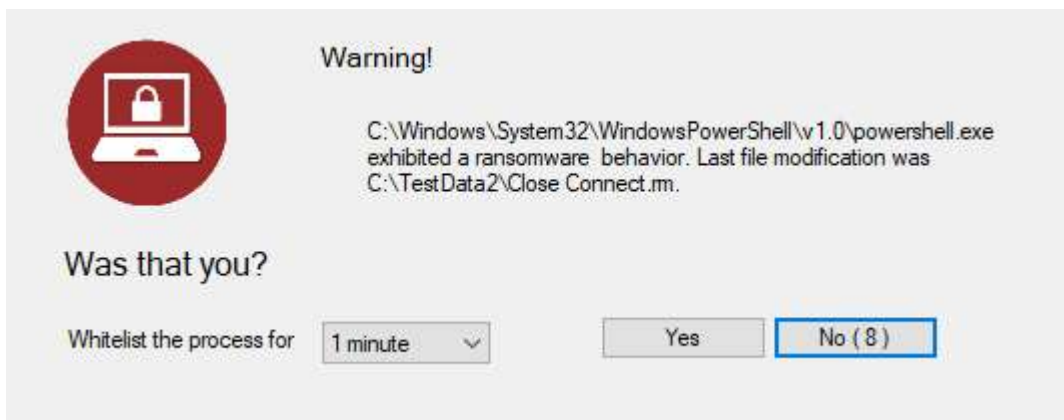
From CryptoStopper GUI

1. Open CryptoStopper.
2. Click the "Whitelist" button.
3. Click the "+" symbol and navigate to the process you want to whitelist.

From the Ransomware Alert Message

When a ransomware attack is detected, this alert message will pop-up. If you are not expecting this alert, click “No” immediately. If you are running a program that generates a false positive, you can whitelist the process for 1 minute, 5 minutes, or 10 minutes depending on the selection that you choose from the Whitelist dropdown.

1. Click the “Whitelist the process for” dropdown.
2. Select 1 minute, 5 minutes or 10 minutes.
3. Click “Yes.”



You will now be able to run the process during the time window you selected.

CryptoStopper Service

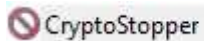
By default, CryptoStopper is running in the background. If you’d like to confirm that it’s running, you can do so via the Windows services. Verify that ‘WatchPointCryptoStopper’ service is running.



Remediation/Windows Firewall

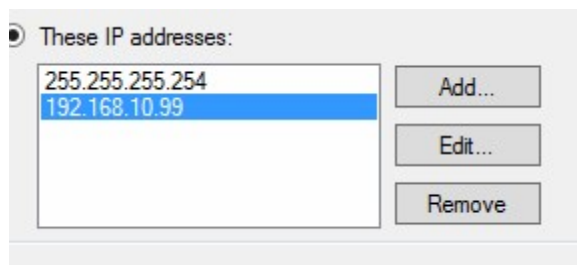
You should know what to do once an infected computer is identified and disconnected from the server. CryptoStopper creates a Windows firewall rule that blocks an infected computer and prevents it from connecting to the server.

The firewall rule will not be visible until ransomware activity is identified for the first time. After the first attack or attack test, you will see this listed as an inbound firewall rule.



Once an infected computer is identified, you'll right-click, select the scope tab to remove the infected computer's IP address. Please note that 255.255.255.254 is there by default.

Select the infected computer's IP address and click "Remove" then "OK."



Change Email Address

To change the email address for the alert mechanism, open CryptoStopper, and click the "Settings" button. Update the email address and click the "save" button.

Watcher Files

CryptoStopper creates 'Watcher Files' within the directories selected for protection. The watcher files are used as bait by CryptoStopper as it continuously monitors the files for signs of ransomware activity. Below is an example of the watcher files created by CryptoStopper:

This PC ▶ Local Disk (C:) ▶ share

Name	Date modified	Type
AddUndo.doc	6/29/2016 4:36 PM	DOC File
AssertProtect.mp4	6/27/2016 4:32 PM	MP4 File
AssertPublish.mov	6/23/2016 1:24 PM	MOV File
BackupExport.pptx	6/27/2016 4:32 PM	PPTX File
BlockAdd.doc	6/27/2016 4:32 PM	DOC File
BlockInvoke.mpg	6/23/2016 1:24 PM	MPG File
CheckpointOptimize.pdf	6/29/2016 4:36 PM	PDF File
CheckpointRead.mpg	6/27/2016 4:32 PM	MPG File
CheckpointRepair.doc	6/23/2016 1:24 PM	DOC File
ClearHide.ram	6/29/2016 4:36 PM	RAM File
ClearSet.docx	6/23/2016 1:24 PM	DOCX File
CloseMeasure.mp4	6/29/2016 4:36 PM	MP4 File
CompareGrant.docx	6/29/2016 4:36 PM	DOCX File
CompareRead.dot	6/29/2016 4:36 PM	DOT File
CompleteInvoke.dot	6/27/2016 4:32 PM	DOT File
CompressCompare.ram	6/29/2016 4:36 PM	RAM File

The watcher files have random file names, random file extensions, and random file sizes. This allows the watcher files to comeingle between company data files and detect the ransomware attack wherever it may start in the protected folder.

The hidden attribute hides the watcher files from end users but not from ransomware. It's important to make sure that workstations on your network do not have "View hidden files" turned on, so users avoid generating a false positive alert by deleting the hidden watcher files. If a user deletes any of the files, CryptoStopper will redeploy those files automatically as long as the directory hasn't been deleted as well.

GPO Deployment

CryptoStopper can be pushed out using GPO or another third-party software program. To push CryptoStopper, you need the CryptoStopper executable and a JSON config file. The next page contains text from a JSON config that you can use as a template to get started. When finished, make sure to validate your JSON using the JSON validator here:

<https://jsonlint.com/>

JSON Configuration Template

```
{ "CompanyName": "Test Company",  
  
  "Email": "user1@testcompany.com",  
  
  "DefaultProtection": "True",  
  
  "DefaultProtectionDeep": "3",  
  
  "FolderListToAdd": [  
  
    { "folder": "C:\\Program Files", "deep": "3" },  
  
    { "folder": "C:\\Program Files (x86)", "deep": "3" },  
  
    { "folder": "C:\\ProgramData", "deep": "3" }  
  
  ],  
  
  "FolderListToRemove": [  
  
    { "folder": "C:\\Program Files\\WindowsApps\\Deleted", "deep": "3"},  
  
    { "folder": "C:\\Program Files (x86)\\Google\\Update", "deep": "3"},  
  
    { "folder": "C:\\ProgramData\\LabTech", "deep": "3" }, { "folder": "C:\\Program Files\\WindowsApps", "deep": "3" }  
  
  ],  
  
  "AddToWhitelist": "",  
  
  "RemoveWhitelist": "",  
  
  "Serialkey": "XXXX-XXXX-XXXX-XXXX" }
```


Explanation of JSON config file

Company Name: Name of Company protected by CryptoStopper

Email: Email address where you want to receive ransomware alert email messages

FolderListToAdd: File path of the folder or server share to be protected. “folder” is the exact path and “deep” represents the number of layers to protect. In this case, a number 4 instructs CryptoStopper to protect the root of the folder and three child layers deep.

FolderListToRemove: File path to the folder or server share that you want to be removed from protection.

DefaultProtection: “True” instructs CryptoStopper to protect the user profile directory.

DefaultProtectionDeep: Number of levels to protect. This includes the root and the child folders. I.E., A “4” means to protect the root and three additional layers of child folders.

AddToWhitelist: Used to whitelist executables and prevent them from generating a ransomware alert.

RemoveWhitelist: Used to remove executables that are currently whitelisted.

UserAutoProtect: “True” checks the auto protect folders checkbox in settings to ensure new user profiles are added to CryptoStopper protection automatically after the CryptoStopper installation.

If you are unsure about how to set up GPO; below is a link to an article from Microsoft to walk you through it. This article explains how to push software through GPO without a config file. To push CryptoStopper with the JSON configuration file, you save the configuration file in the same software deployment directory as the CryptoStopper executable and GPO will deploy the executable with the JSON configuration file.

How to use Group Policy to remotely install software in Windows Server 2003 and Windows Server 2008.

These instructions also apply to Windows Server 2012 and 2016.

<https://support.microsoft.com/en-us/help/816102/how-to-use-group-policy-to-remotely-install-software-in-windows-server>

Troubleshooting GPO Installation

Deploying software through GPO is rarely 100% due to a number of different factors that can make working with GPO software deployments frustrating. If you have a problem with a small number of devices in your GPO deployment, it is often better to push what you can through GPO and then manually install CryptoStopper on those problem endpoints. If you want to troubleshoot GPO, here are the most common issues.

1. Verify Network Discovery is turned on at the endpoint.
2. Verify the App Deployment folder containing CryptoStopper is shared with domain users.
3. Verify you can access the deployment folder from the UNC path.
4. If CryptoStopper was installed previously through GPO, there might be a registry key that needs to be deleted here: HKLM\Software\Microsoft\Windows\Current Version\Group Policy\AppMgmt
5. Enable GPO "Always wait for the network at computer startup and logon."
6. Configure wait time in GPO "Specify startup policy processing wait time."
7. After checking all of these steps, open an elevated command prompt and run the command: gpupdate /force
8. Reboot.

What port does CryptoStopper use to send alert messages?

CryptoStopper uses SMTP to connect to a mandrill server to send email. Smtplib.mandrillapp.com:587. Please ensure this port is open.

Will CryptoStopper automatically protect new folders?

CryptoStopper will check the share or protected folder each hour and add new folders as necessary.

What is CryptoStopper resource utilization?

CryptoStopper uses a minimal amount of CPU and RAM. Typically, less than 1% of CPU and 20MB of RAM.

Will CryptoStopper isolate the offending workstation automatically?

Yes. CryptoStopper uses an algorithm to monitor specially crafted watcher files. When ransomware attacks your server, CryptoStopper correlates the offending user and immediately isolates that user. It simultaneously notifies the specified email.

Do you have a PC version of CryptoStopper?

Yes. CryptoStopper Server and CryptoStopper Desktop are both available for download.

Does CryptoStopper automatically update?

Yes. WatchPoint provides automatic updates to CryptoStopper.

How long does it take to install CryptoStopper?

A typical server install will take 15 minutes or less. The workstation version installs in as little as 5 minutes.

Will my backup trigger CryptoStopper?

No. Your backup only updates the archive bit and doesn't modify the file.

How quickly will CryptoStopper work to stop a ransomware attack?

CryptoStopper detects and stops a ransomware attack in as little as 2 seconds.

Does CryptoStopper detect and stop all ransomware?

CryptoStopper will detect and stop all variants of ransomware whether new or zero-day.

What if the infection happens directly on the server?

CryptoStopper Server will stop a local attack running on the server. If you are the victim of a ransomware attack that happens directly on the server, you are the victim of a hack and attack. You should consider your entire network compromised and act accordingly.