Table of Contents

Helpful Links

Schedule Install Assistance:
https://go.getcryptostopper.com/get-a-demo

CryptoStopper Portal:
https://portal.getcryptostopper.com

CryptoStopper Download:
https://getcryptostopper.com/download

Video - Two-Minute Install:
https://www.getcryptostopper.com/cryptostopper/cryptostopper-installation-video/

Video - CryptoStopper Portal – Adding a new customer:
https://www.getcryptostopper.com/msp-resources/portal/cryptostopper-portal-adding-a-new-customer

Video - CryptoStopper install via Group Policy:
https://www.getcryptostopper.com/msp-resources/cryptostopper/cryptostopper-gpo-deployment/

Video - CryptoStopper Install via Powershell Script:
https://www.getcryptostopper.com/msp-resources/cryptostopper/cryptostopper-install-via-powershell-script

Overview

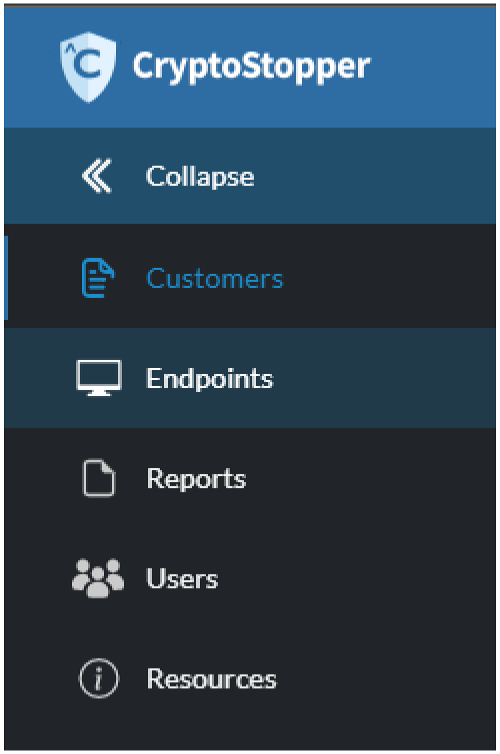
CryptoStopper was desiged to detect and stop actively running ransomware. It is your best line of defense in stopping actively running ransomware that has bypassed other products in the security stack. CryptoStopper protects endpoints by deploying hidden honeypot files to the protected folders. CryptoStopper monitors these hidden honeypot files for ransomware activity and reacts in the event of a ransomware attack. CryptoStopper also has advanced monitoring features like native file monitoring and extension change monitoring that provide additional protection on top of the hidden honeypot files. Lastly, CryptoStopper's advanced driver protection provides faster detection and better intelligence that complements our original honeypot file detection method.

This document outlines how to create and configure new customer accounts in the CryptoStopper web portal and assumes the perspective of the MSP. It also covers configuring CryptoStopper settings, manual installation of the product and mass deployments using Group Policy or an RMM.

CryptoStopper Portal

The CryptoStopper Portal URL is https://portal.getcryptostopper.com. The portal is the central management system for CryptoStopper agents. You can create new customer accounts, update notification and endpoint settings and monitor agent status from the portal.

Partners have access to the Customers list, Endpoints list, Reports, User Management and Resources menus via the left sandwich menu.



View the customer list

View activated endpoints

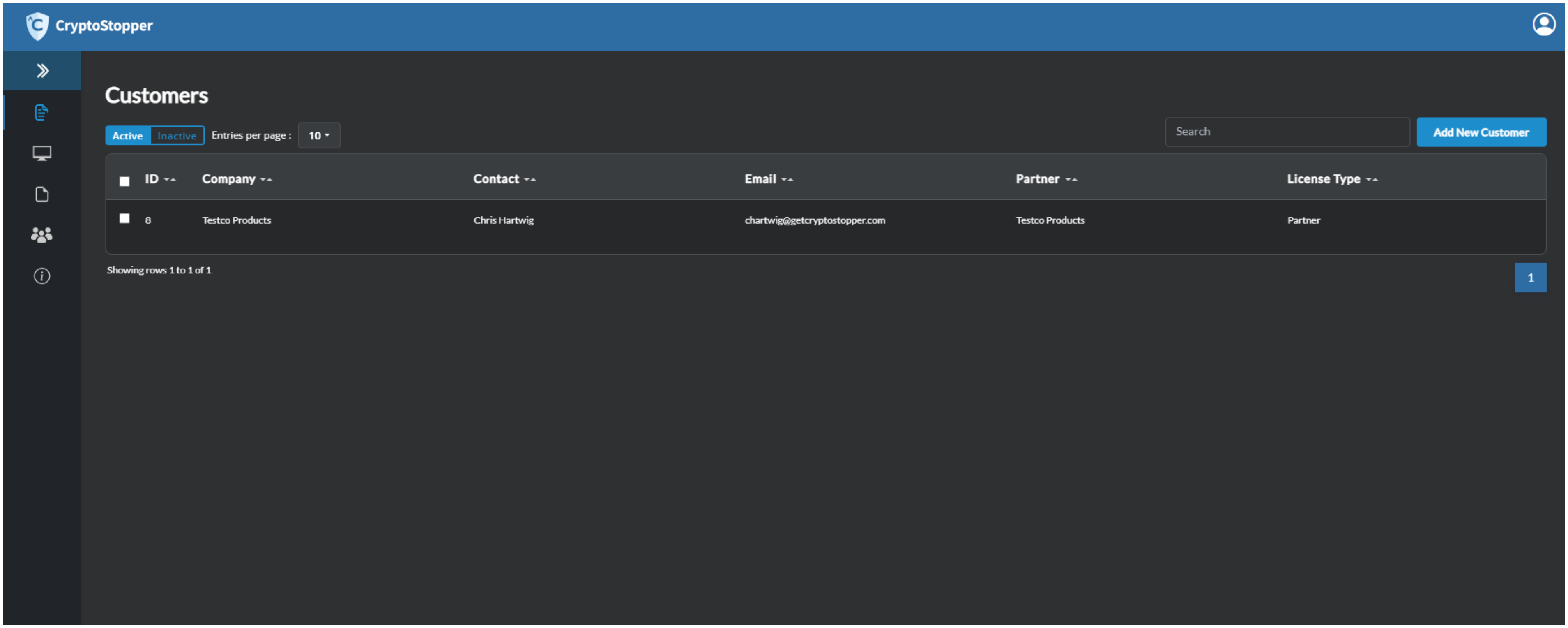
Run reports

Configure user accounts

Access training manuals and videos

Creating Customer Accounts

Login to the CryptoStopper Portal with the credentials provided to you. (If this is the first time you have logged in, you will be required to set up 2FA for secure account logins.)



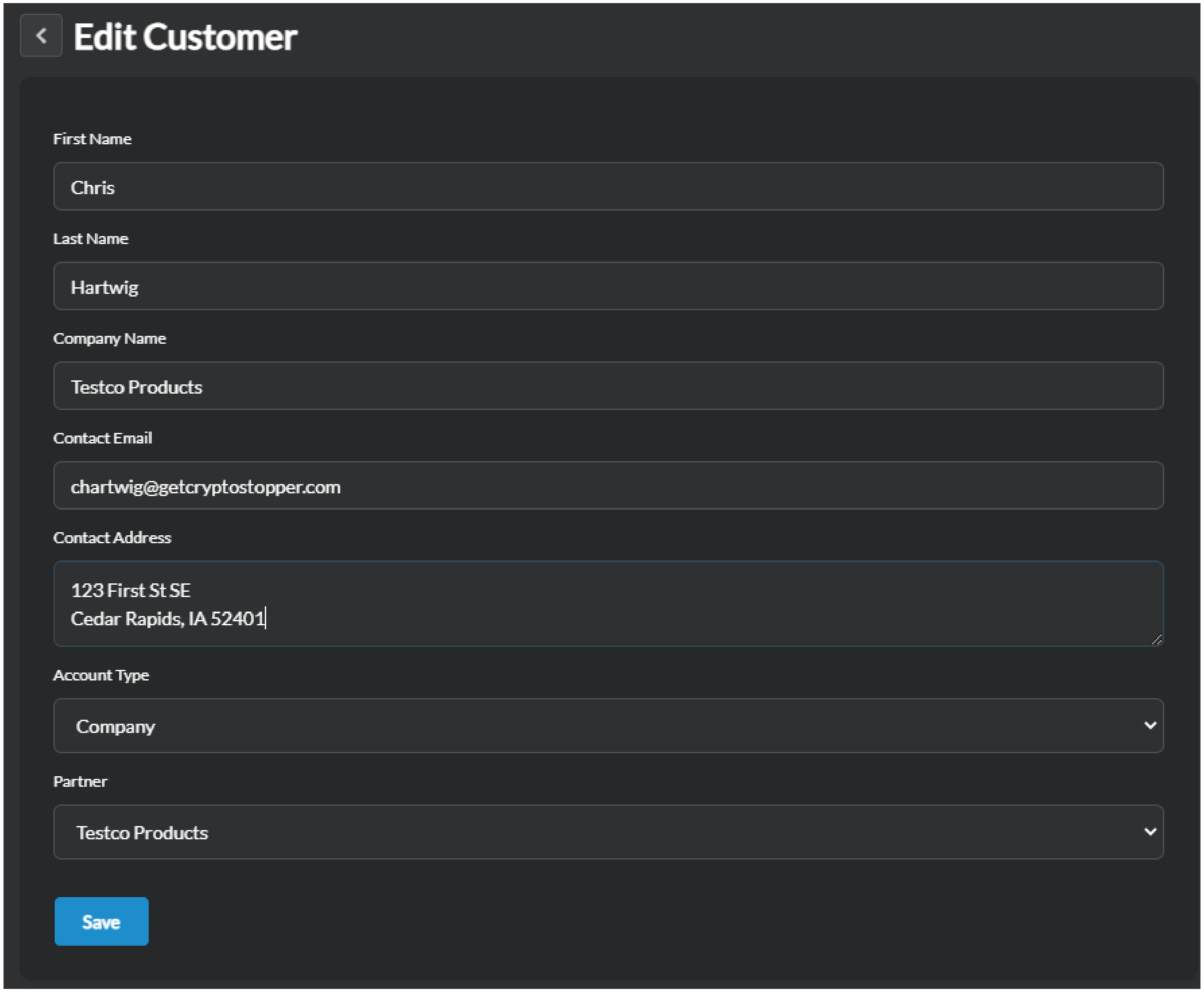
Customers

ID	Company	Contact	Email	Partner	License Type
8	Testco Products	Chris Hartwig	chartwig@getcryptostopper.com	Testco Products	Partner

Showing rows 1 to 1 of 1

Select "**Add New Customer**" and fill out the required information. A unique email address is required per customer.

Click “Save” when you are finished entering the customer information.



Edit Customer

First Name

Chris

Last Name

Hartwig

Company Name

Testco Products

Contact Email

chartwig@getcryptostopper.com

Contact Address

123 First St SE
Cedar Rapids, IA 52401

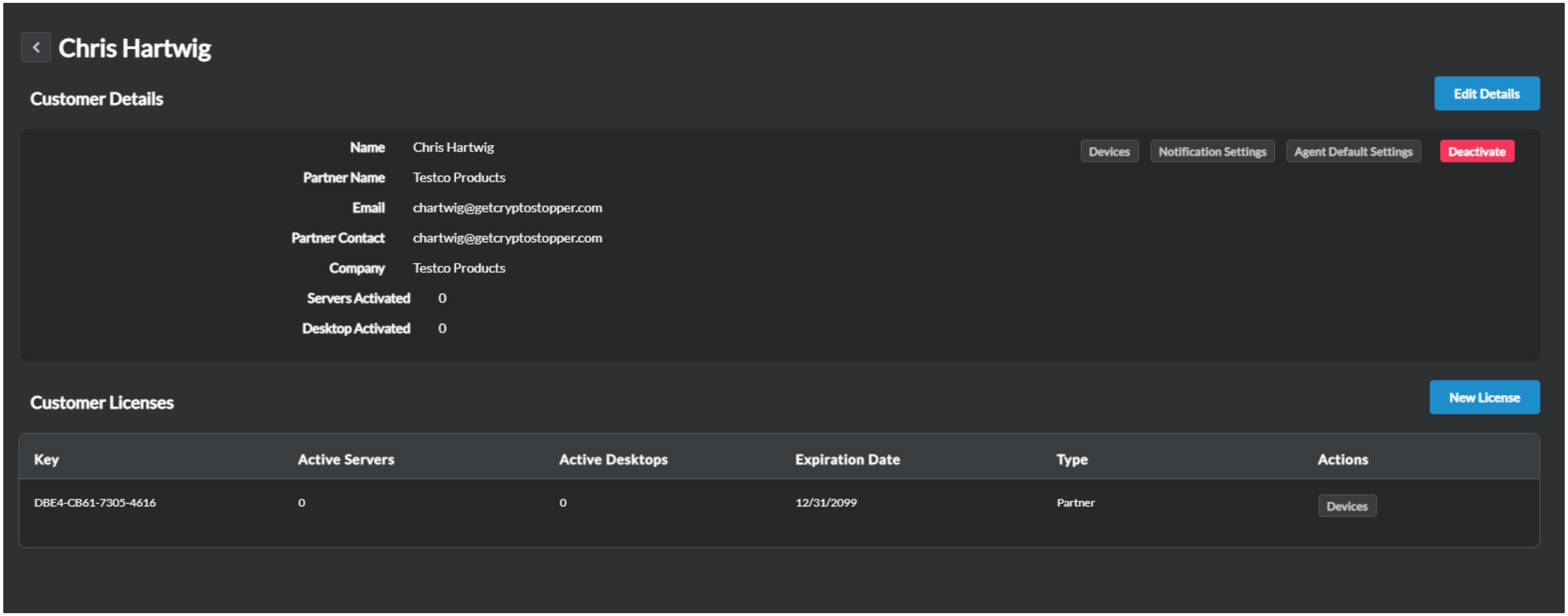
Account Type

Company

Partner

Testco Products

A new customer with a unique license key is created. Now you will configure the “Notification Settings” and “Agent Default Settings”



Chris Hartwig

Customer Details

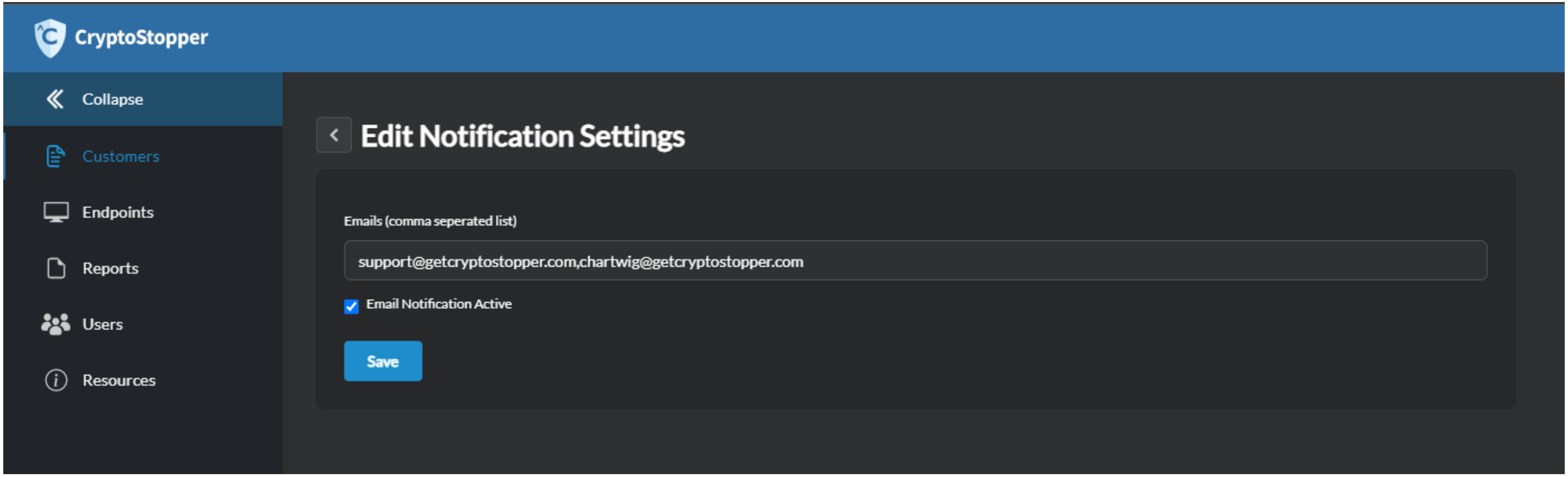
Name	Chris Hartwig
Partner Name	Testco Products
Email	chartwig@getcryptostopper.com
Partner Contact	chartwig@getcryptostopper.com
Company	Testco Products
Servers Activated	0
Desktop Activated	0

Customer Licenses

Key	Active Servers	Active Desktops	Expiration Date	Type	Actions
DBE4-CB61-7305-4616	0	0	12/31/2099	Partner	Devices

Notification Settings

When an alert is generated by CryptoStopper, the agent checks in with the portal to verify the proper email address for notification. If the portal cannot be reached, the CryptoStopper agent will use its internal SMTP server to send an email to the address listed under “Agent Default Settings.” The “Notification Settings” email field will accept a comma separated list of emails.



Edit Notification Settings

Emails (comma seperated list)

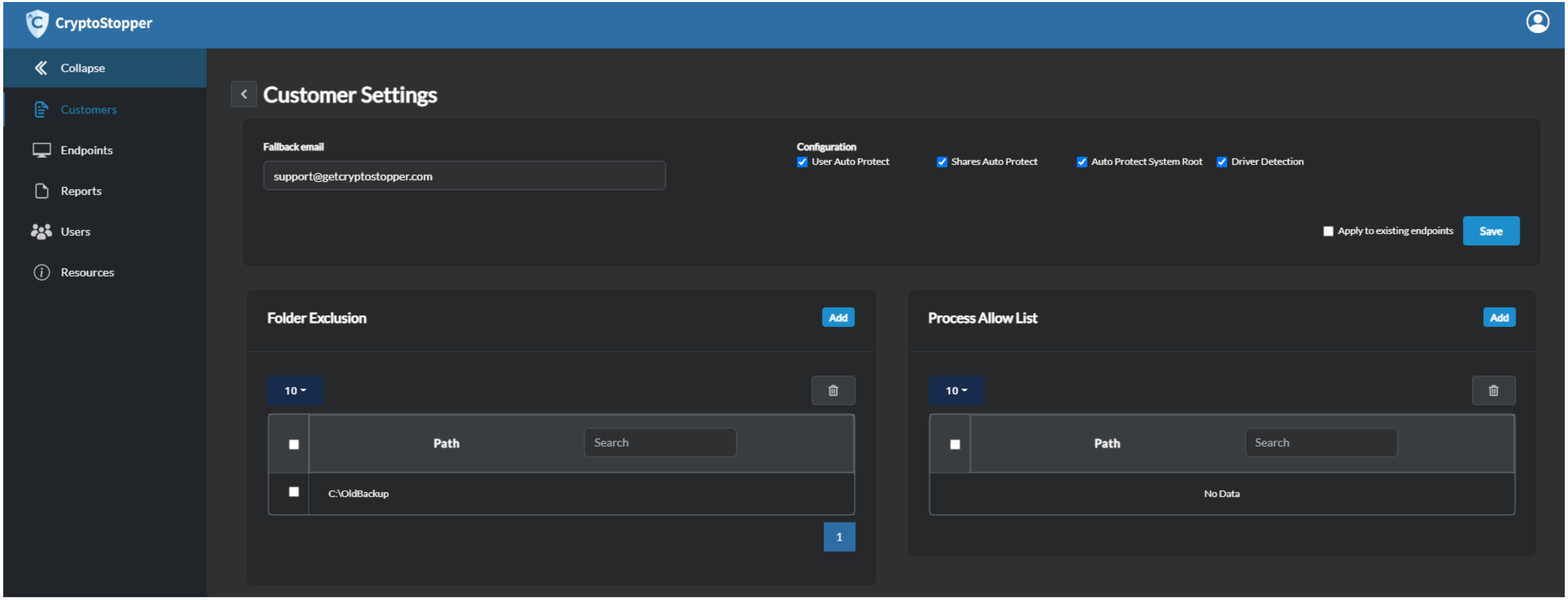
support@getcryptostopper.com,chartwig@getcryptostopper.com

☑ Email Notification Active

Agent Default Settings

These settings will be pushed to the agent after installation. These settings can also be updated and pushed down to existing agents. We recommend configuring agent settings and folder exclusions first, then install CryptoStopper to your endpoints.

Fallback email – The email is pushed to the agent and will be used if the agent cannot communicate with the portal to send the email.
User Auto Protect – When checked, CryptoStopper will protect all user profiles automatically.
Shares Auto Protect – When checked, CryptoStopper will protected the shared folders automatically.
Auto Protect System Root – When checked, CryptoStopper will protect the default volume automatically.
Driver Detection – Enable the agent Windows driver for faster detection.
Apply to existing endpoints – Apply setting to some or all of the existing endpoints.
Folder Exclusion – Exclude a folder from protection if an application is generating false positives.
Process Allow List – Whitelist a process and allow it to run even if it triggers the CryptoStopper detection mechanism.



Customer Settings

Fallback email: support@getcryptostopper.com

Configuration
☑ User Auto Protect ☑ Shares Auto Protect ☑ Auto Protect System Root ☑ Driver Detection

☐ Apply to existing endpoints

Folder Exclusion

☐	Path
☐	C:\OldBackup

Process Allow List

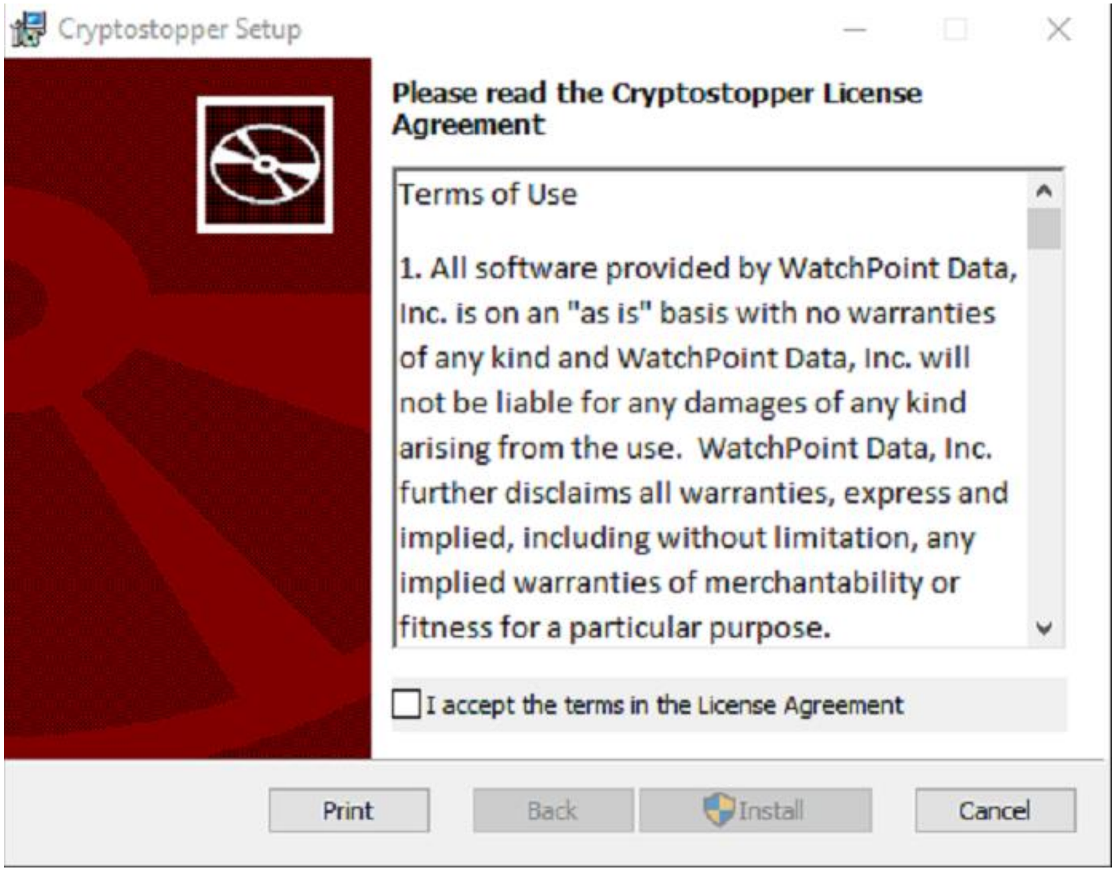
☐	Path
	No Data

Installing CryptoStopper

After the customer account has been created you will open the account and copy the installation key. Next you can install CryptoStopper manually on each endpoint, or you have a number of options to automate the install. Automated methods include deployment via Group Policy, powershell scripting, RMM tools and third party installers.

Manual Installation Instructions

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



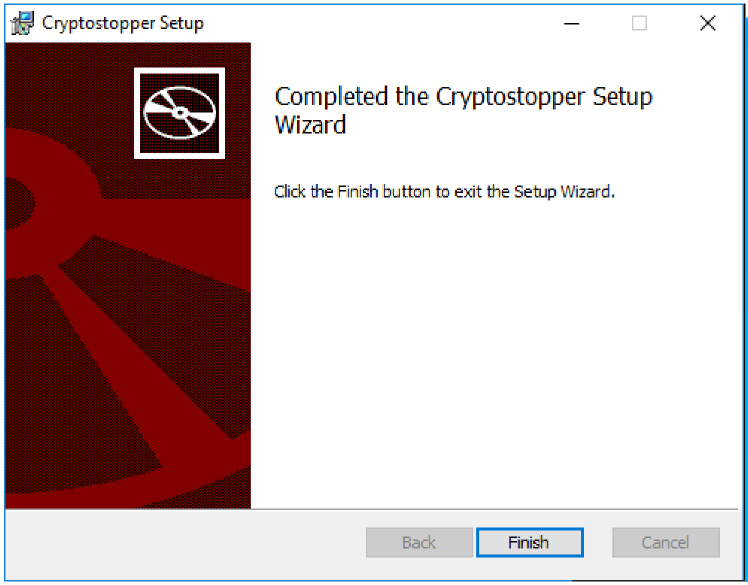
Please read the Cryptostopper License Agreement

Terms of Use

1. All software provided by WatchPoint Data, Inc. is on an "as is" basis with no warranties of any kind and WatchPoint Data, Inc. will not be liable for any damages of any kind arising from the use. WatchPoint Data, Inc. further disclaims all warranties, express and implied, including without limitation, any implied warranties of merchantability or fitness for a particular purpose.

□ I accept the terms in the License Agreement

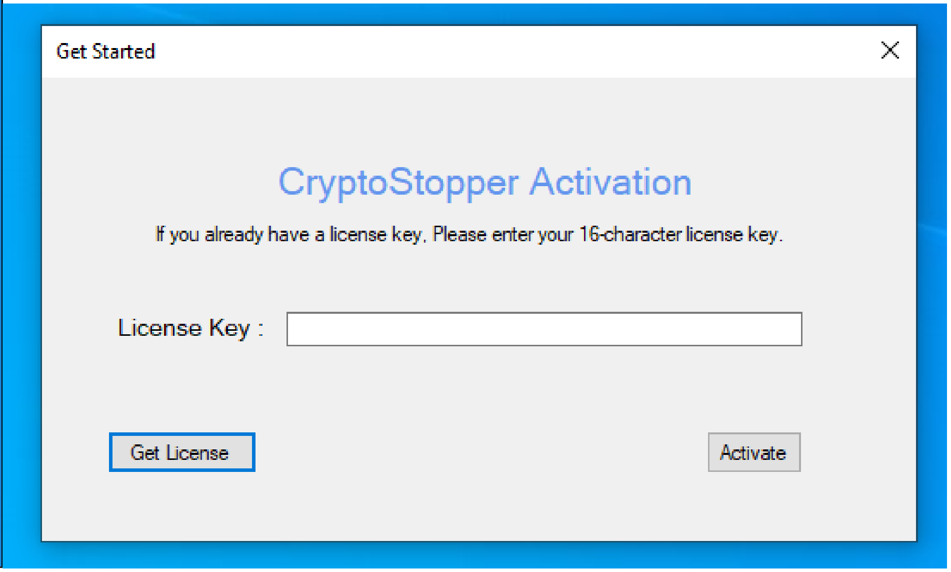
2) Review the CryptoStopper License Agreement then check the box “I accept the terms in the License Agreement.”
3) Next, click the “Install” button.
4) Click “Finish” once the installation is complete.
5) Enter the license key when prompted to activate CryptoStopper.



Cryptostopper Setup

Completed the Cryptostopper Setup Wizard

Click the Finish button to exit the Setup Wizard.



Get Started

CryptoStopper Activation

If you already have a license key, Please enter your 16-character license key.

License Key :

6) The CryptoStopper Installation is complete.

After the installation, CryptoStopper will sync settings with the portal and run its first integrity check. During the integrity check, CryptoStopper syncs the agent settings and begins the automated deployment and protection process.

Automating the CryptoStopper Installation

The CryptoStopper install can be automated in several ways. We recommend utilizing an RMM for automated installations; however, if an RMM isn't available you can still automate the install using Windows GPO on a domain controller, a powershell script, or third-party installers.

RMM Installation

CryptoStopper supports an install via a number of different RMM products. Please consult your RMM documentation, check the resources tab for further info about RMM installations or reach out to support@getcryptostopper.com and set up a meeting to discuss your RMM deployment.

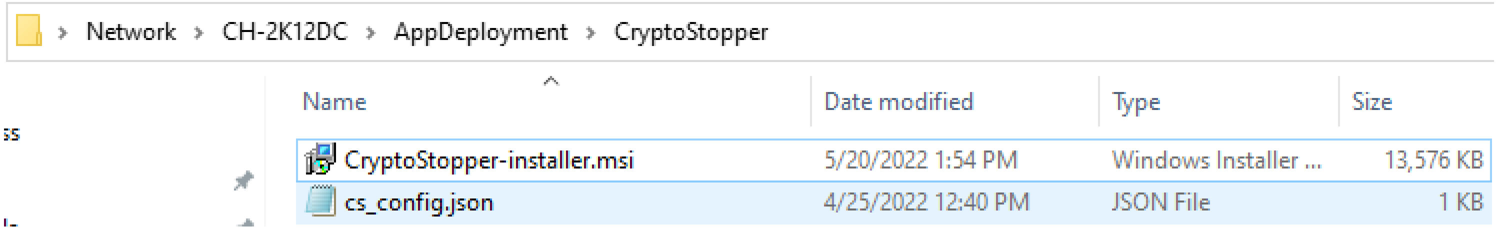
N-ABLE
CONNECTWISE
datto
Kaseya
ninjaOne
Syncro
ATERA

GPO Deployment

CryptoStopper can be pushed out using Windows Group Policy. To push CryptoStopper via GPO, you need the CryptoStopper installer and a JSON config file. The json config file needs to be named "cs_config.json" and must contain the serial key. You can copy the following json configuration template and replace the X's with your customer key.

{"Serialkey": "XXXX-XXXX-XXXX-XXXX"}

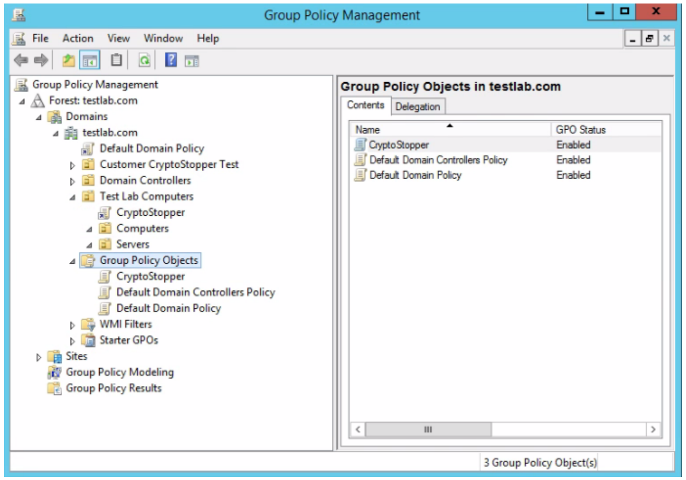
Once the json has been created, copy the JSON and CryptoStopper installer to a shared folder on your domain controller and then create the GPO object to perform the software installation.



Network › CH-2K12DC › AppDeployment › CryptoStopper

Name	Date modified	Type	Size
CryptoStopper-installer.msi	5/20/2022 1:54 PM	Windows Installer ...	13,576 KB
cs_config.json	4/25/2022 12:40 PM	JSON File	1 KB

How to use Group Policy to remotely install software in Windows Server 2003 and Windows Server 2008.
These instructions apply to all versions of Windows Server.
https://support.microsoft.com/en-us/help/816102/how-to-use-group-policy-to-remotely-install-software-in-windows-server



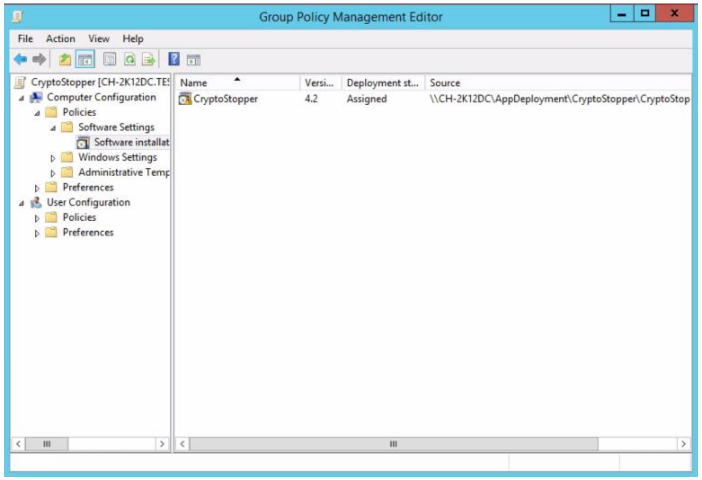
```
Group Policy Management
  Forest: testlab.com
    Domains
      testlab.com
        Default Domain Policy
        Customer CryptoStopper Test
        Domain Controllers
        Test Lab Computers
          CryptoStopper
          Computers
          Servers
        Group Policy Objects
          CryptoStopper
          Default Domain Controllers Policy
          Default Domain Policy
        WMI Filters
        Starter GPOs
    Sites
    Group Policy Modeling
    Group Policy Results
```

Group Policy Objects in testlab.com

Contents | Delegation

Name	GPO Status
CryptoStopper	Enabled
Default Domain Controllers Policy	Enabled
Default Domain Policy	Enabled

3 Group Policy Object(s)



```
CryptoStopper [CH-2K12DC.TE
  Computer Configuration
    Policies
      Software Settings
        Software installat
      Windows Settings
      Administrative Temp
    Preferences
  User Configuration
    Policies
    Preferences
```

Name	Versi...	Deployment st...	Source
CryptoStopper	4.2	Assigned	\\CH-2K12DC\AppDeployment\CryptoStopper\CryptoStop

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.

Powershell Script

The powershell script can be run independently or inside an RMM. This makes using the script very versatile in any network situation. The powershell script sets three variables: the web path for download, the local path to copy files to and the path to the shared network folder that contains the json config file.

Step1. Create the json file and enter the correct license key for the customer install.

JSON Configuration Template

{"Serialkey": "XXXX-XXXX-XXXX-XXXX"}

Step 2. Create a powershell script with the following information and then you can run this script from your RMM or on the customer network.

```
#Before runnning this script, update the variable $cs_config_json with the location of the customer json file.
#Ensure you have updated the json with the correct customer license key and it is named cs_config.json

#variables
$cs_web_path = 'https://go.watchpointdata.com/hubfs/CryptoStopper/CryptoStopper-installer.msi'
$cs_local_path = 'C:\Temp\CryptoStopper_Install'
$cs_config_json = '\\CH-2K12DC\AppDeployment\4.2.2\cs_config.json'


#Check if temp directory exists
if(Get-Item -Path $cs_local_path -ErrorAction Ignore)
{
Write-Host "Folder Exists"
}
else
{
#PowerShell Create directory if not exists
New-Item $cs_local_path -ItemType Directory
}
#Download latest version of CryptoStopper and save to temp
Invoke-WebRequest -uri $cs_web_path -OutFile $cs_local_path\CryptoStopper-installer.msi

#Copy json config file to temp
Copy-Item $cs_config_json -Destination $cs_local_path

#Install CryptoStopper
msiexec /qn /i $cs_local_path\CryptoStopper-installer.msi CONFIGFILE=$cs_local_path\cs_config.json
```

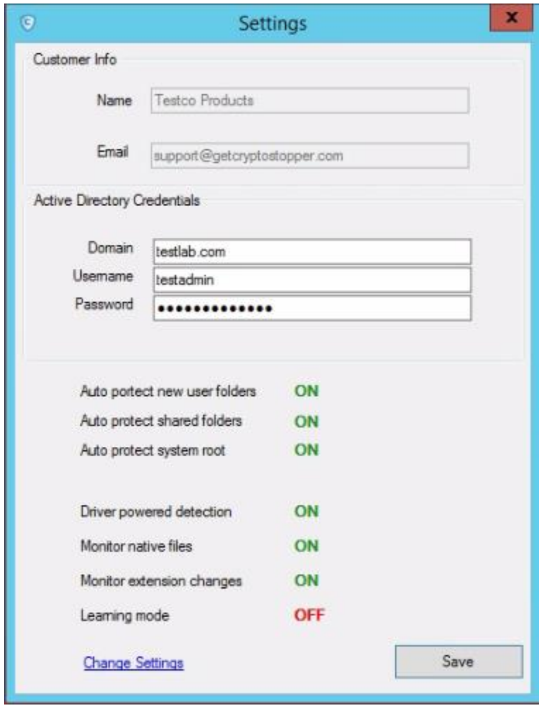
Third-Party Application

It is possible to install CryptoStopper via a third party installer. We do not provide support for third-party installers but they follow the same principal as the other methods of install. You simply create an install job, point to the installer and json files, then push to a target list of endpoints.

Configure CryptoStopper Server Settings

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.

Server Settings



Settings

Customer Info

Name: Testco Products

Email: support@getcryptostopper.com

Active Directory Credentials

Domain: testlab.com

Username: testadmin

Password: ••••••••••••••

Auto portect new user folders: ON

Auto protect shared folders: ON

Auto protect system root: ON

Driver powered detection: ON

Monitor native files: ON

Monitor extension changes: ON

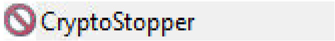
Learning mode: OFF

Log in to the server and open CryptoStopper from the deskop or tray icon. Enter the Active Directory Credentials. 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.

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.

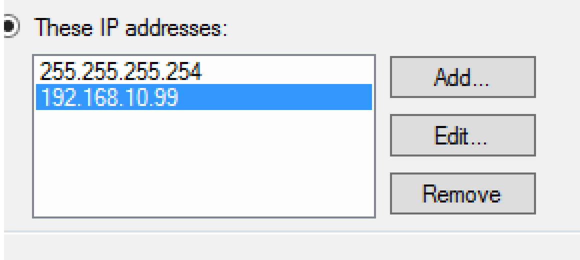
The firewall rule will not be visible until ransomware activity is identified for the first time. After the first attack or attack test, you will see this listed as an inbound firewall rule.



🚫 CryptoStopper

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."



● These IP addresses:

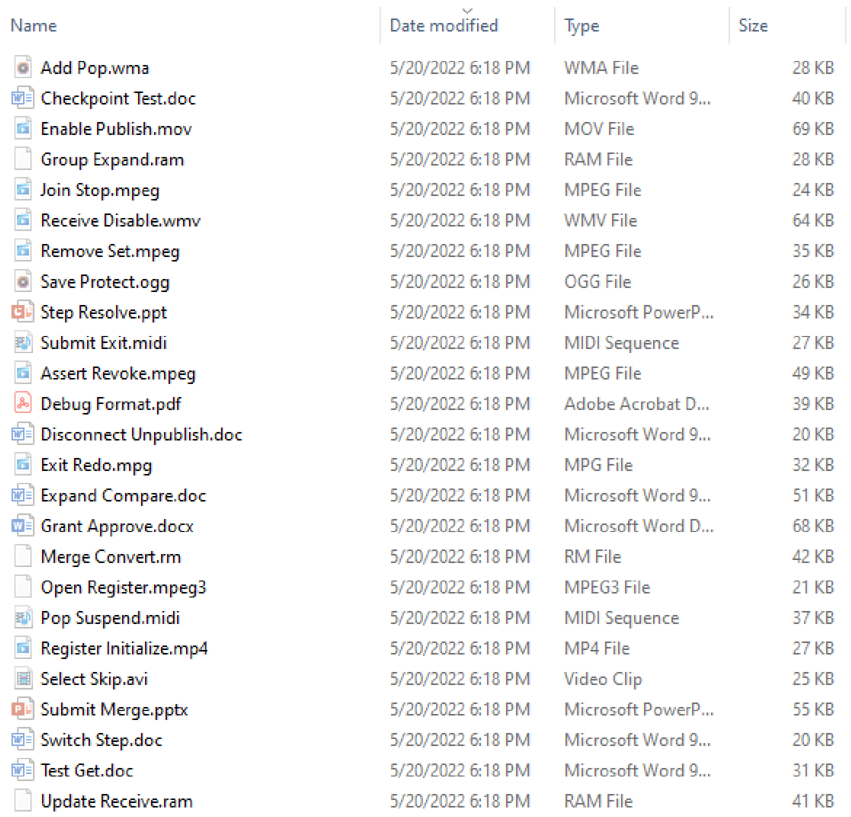
255.255.255.254
192.168.10.99

Honeypot Files

CryptoStopper creates ‘Honeypot files’ within the directories selected for protection. The honeypot files are used as bait by CryptoStopper as it continuously monitors the files for signs of ransomware activity. The screenshot to the right is an example of the honeypot files created by CryptoStopper.

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

The hidden attribute hides the honeypot 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 honeypot 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.



Name	Date modified	Type	Size
Add Pop.wma	5/20/2022 6:18 PM	WMA File	28 KB
Checkpoint Test.doc	5/20/2022 6:18 PM	Microsoft Word 9...	40 KB
Enable Publish.mov	5/20/2022 6:18 PM	MOV File	69 KB
Group Expand.ram	5/20/2022 6:18 PM	RAM File	28 KB
Join Stop.mpeg	5/20/2022 6:18 PM	MPEG File	24 KB
Receive Disable.wmv	5/20/2022 6:18 PM	WMV File	64 KB
Remove Set.mpeg	5/20/2022 6:18 PM	MPEG File	35 KB
Save Protect.ogg	5/20/2022 6:18 PM	OGG File	26 KB
Step Resolve.ppt	5/20/2022 6:18 PM	Microsoft PowerP...	34 KB
Submit Exit.midi	5/20/2022 6:18 PM	MIDI Sequence	27 KB
Assert Revoke.mpeg	5/20/2022 6:18 PM	MPEG File	49 KB
Debug Format.pdf	5/20/2022 6:18 PM	Adobe Acrobat D...	39 KB
Disconnect Unpublish.doc	5/20/2022 6:18 PM	Microsoft Word 9...	20 KB
Exit Redo.mpg	5/20/2022 6:18 PM	MPG File	32 KB
Expand Compare.doc	5/20/2022 6:18 PM	Microsoft Word 9...	51 KB
Grant Approve.docx	5/20/2022 6:18 PM	Microsoft Word D...	68 KB
Merge Convert.rm	5/20/2022 6:18 PM	RM File	42 KB
Open Register.mpeg3	5/20/2022 6:18 PM	MPEG3 File	21 KB
Pop Suspend.midi	5/20/2022 6:18 PM	MIDI Sequence	37 KB
Register Initialize.mp4	5/20/2022 6:18 PM	MP4 File	27 KB
Select Skip.avi	5/20/2022 6:18 PM	Video Clip	25 KB
Submit Merge.pptx	5/20/2022 6:18 PM	Microsoft PowerP...	55 KB
Switch Step.doc	5/20/2022 6:18 PM	Microsoft Word 9...	20 KB
Test Get.doc	5/20/2022 6:18 PM	Microsoft Word 9...	31 KB
Update Receive.ram	5/20/2022 6:18 PM	RAM File	41 KB

Responding to CryptoStopper Alerts

CryptoStopper displays a desktop alert when a ransomware attack is detected, and CryptoStopper also sends an email alert to the email address configured in settings. It is important that administrators examine these alerts immediately. This document outlines what to do when a ransomware alert message is received.

Sample Alert Message

Ransomware attack detected on Computer:SCOTT-PC User:Scott at Time:2022-06-13 15:30:49 GMT+00:00. A potentially malicious process of C:\temp\ransomware.EXE has been stopped. C:\Users\Jonathan\Desktop\Projects\CWT\Watch Confirm.mov was the last file overwritten by the potentially malicious process.Please check the host immediately.

Determine if Alert is a False Positive or a Real Ransomware Attack

If a user does not have hidden files turned off and that user trys to rename, move or delete a watcher file, the CryptoStopper alert mechanism will be activated. Ensure viewing hidden files is turned off for the user and consider configuring GPO to turn off viewing of hidden files for all users.

Ransomware Attack

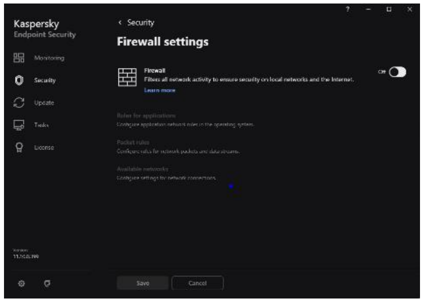
If an alert is generated and you find a few files that have been encrypted in the folder mentioned in the ransomware alert, you will know a real ransomware attack was detected and stopped. In this case, you will want to pull the infected machine off the network and remove the infection or reimage the machine before deploying it back on the network.

Frequently Asked Questions (FAQ)

Does CryptoStopper conflict with other security products?

ThreatLocker – You must put one endpoint in learning mode during install for ThreatLocker to learn that CryptoStopper is approved to run on the network. Once CryptoStopper has been installed on one endpoint in learning mode, you can apply the settings in a policy to your customers.

Kaspersky Endpoint Security – You must turn off the Firewall feature of KES on ***servers only***. CryptoStopper Server isolates infected hosts by IP address in the Windows Firewall. If KES Firewall feature is enabled, host isolation will not work.



Firewall settings

Firewall — Off
Filters all network activity to ensure security on local networks and the Internet.
Learn more

Rules for applications
Configure application network rules in the operating system.

Packet rules
Configure rules for network packets and data streams.

Available networks
Configure settings for network connections.

What port does CryptoStopper use to send alert messages?

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

Will CryptoStopper automatically protect new folders?

CryptoStopper runs an integrity check each hour and adds new folders automatically.

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 honeypot files, native files and file extension changes. 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. The single msi installer can be used for both server and desktop installations.

Does CryptoStopper automatically update?

Yes. CryptoStopper will automatically update to the latest version as it becomes available.

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 1-2 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.