Powershell – Caintech.co.uk

Archived: 2026-04-05 16:12:07 UTC

Many companies spend a fortune on Next Generation anti-virus and Machine Learning “AI” tools to halt the spread of ransomware and although I strongly believe that user education and training plays a key part in this Windows does can help in a massive way. Windows File Services Resource Manager (FSRM) a resource already built into Windows can halt the spread and quarantine accounts that are affected.

This solution utilises PowerShell and Windows File Services Resource Manager to automatically lockout a user account when ransomware activities are detected.

Installing FSRM

First and foremost, you will need to set up FSRM on your file servers. This feature is part of the File Services Role and can be installed with the following PowerShell command (all one line).

Install-WindowsFeature –Name FS-Resource-Manager
–IncludeManagementTool

```
PS C:\Users\Administrator> Install-WindowsFeature -Name FS-Resource-Manager -IncludeManagementTools

Success Restart Needed Exit Code      Feature Result
------- -------------- ---------      --------------
True    No             Success        {File and iSCSI Services, File Server, Fil...
```

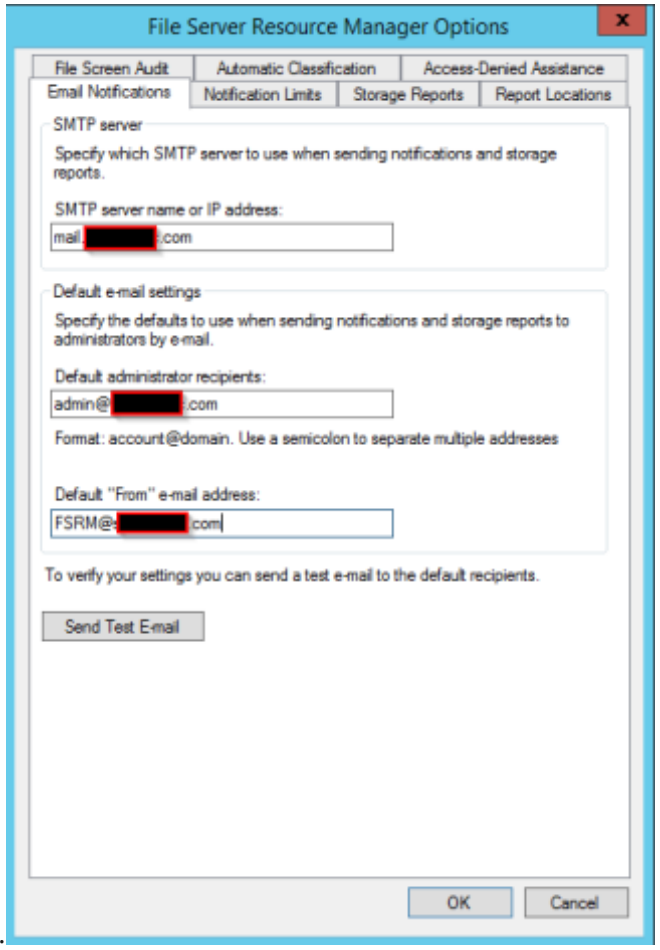
Take note, FSRM is only available on Windows *Server*. If you’re interested in workstation mitigation, comment below and I’ll get to writing!

Get Email Alerts

In order to be emailed of the action our killswitch takes, we will need to set up the SMTP Server settings within FSRM. We don’t necessarily have to do this right now, but it saves us from seeing annoying prompts in the future steps.

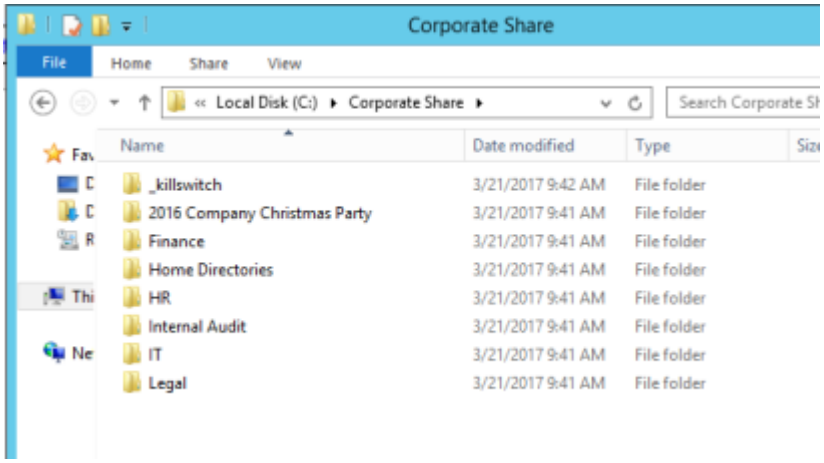
Open up Server Manager > File and Storage Services > Right-click on your server > File Server Resource Manager (this can also be accessed through Administrative Tools). Once opened, right-click “File Server Resource

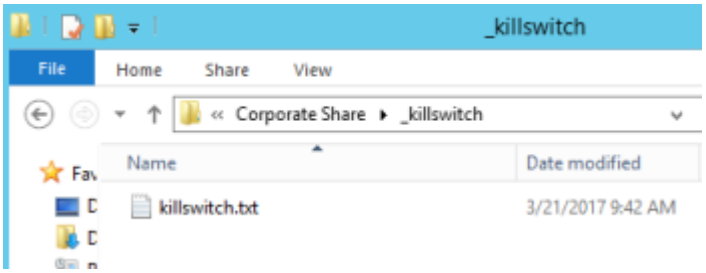
Manager (Local)" in the left pane and select "Configure Options…" Go ahead and set up all your email settings, similar to below.



Set up Killswitch Directory

In your corporate file share(s), set up a directory that begins with an underscore. If the ransomware is encrypting alphabetically, this will ensure that it is tripped as soon as possible. Within that directory, we will place a text file called killswitch.txt.

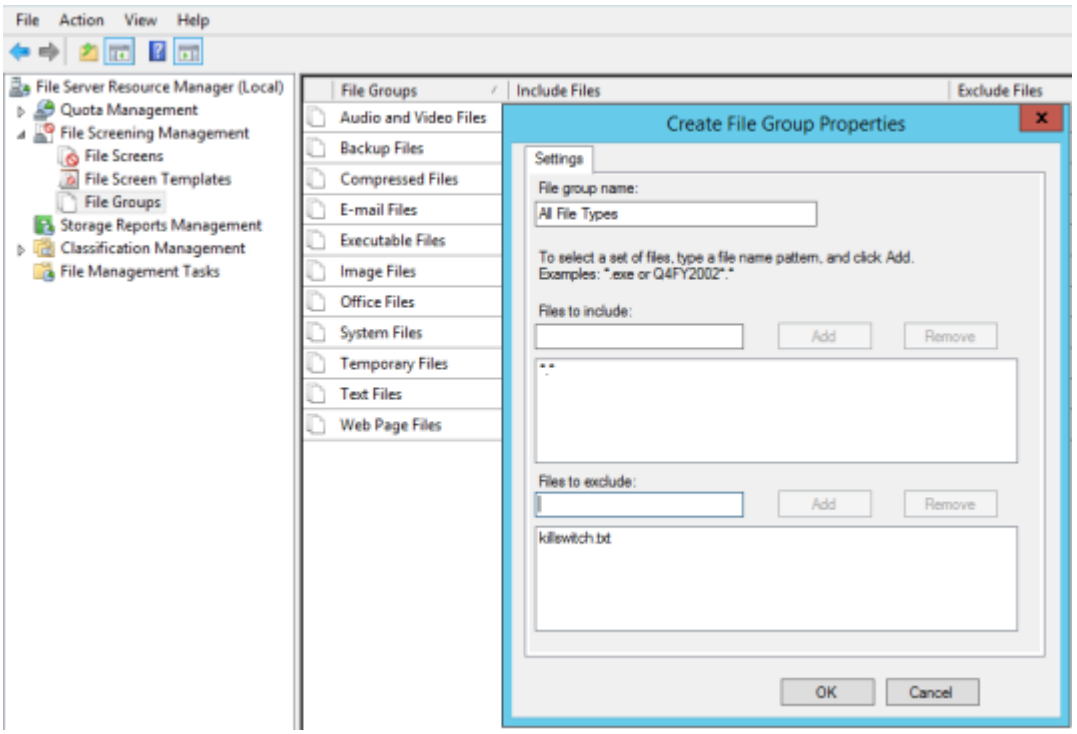




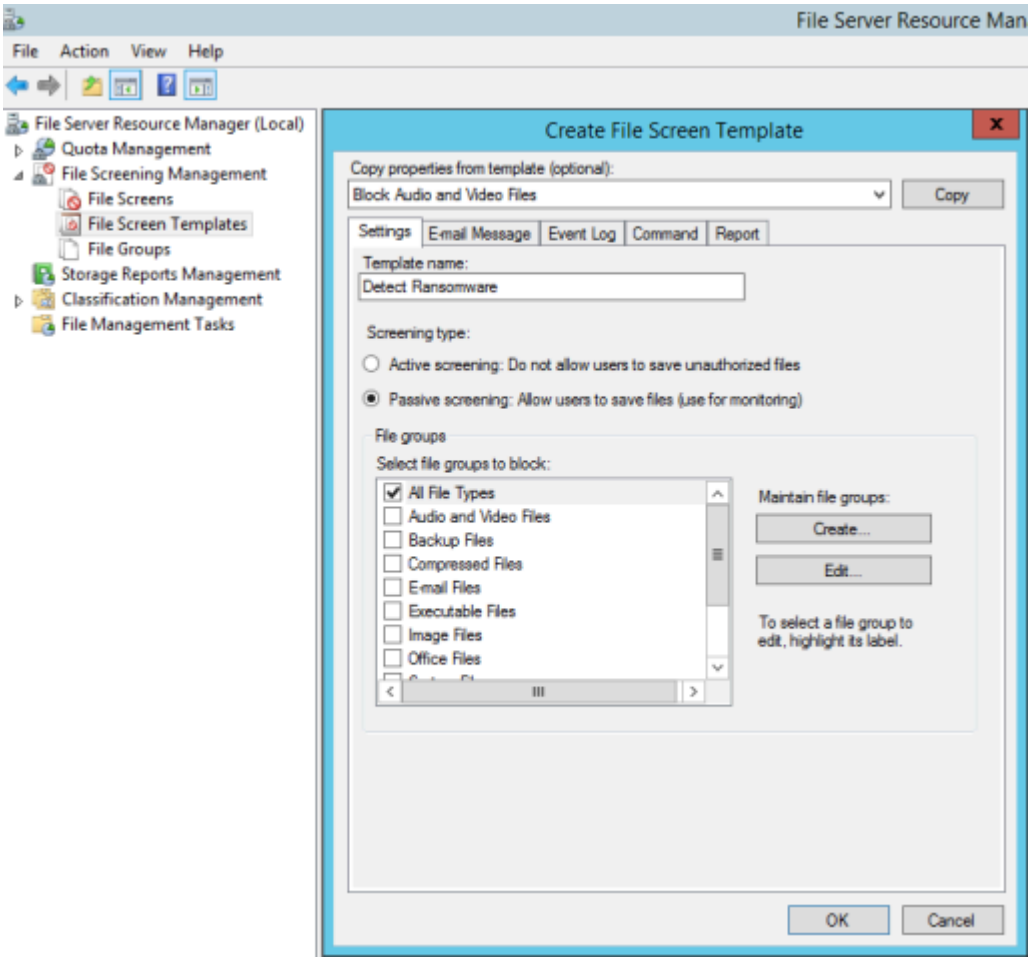
Set Up the Killswitch

Many variants of ransomware look to find mapped drives and will begin encrypting data in **alphabetical** order. Because of this, our killswitch is going to be a directory placed in the file shares that begins with an underscore.

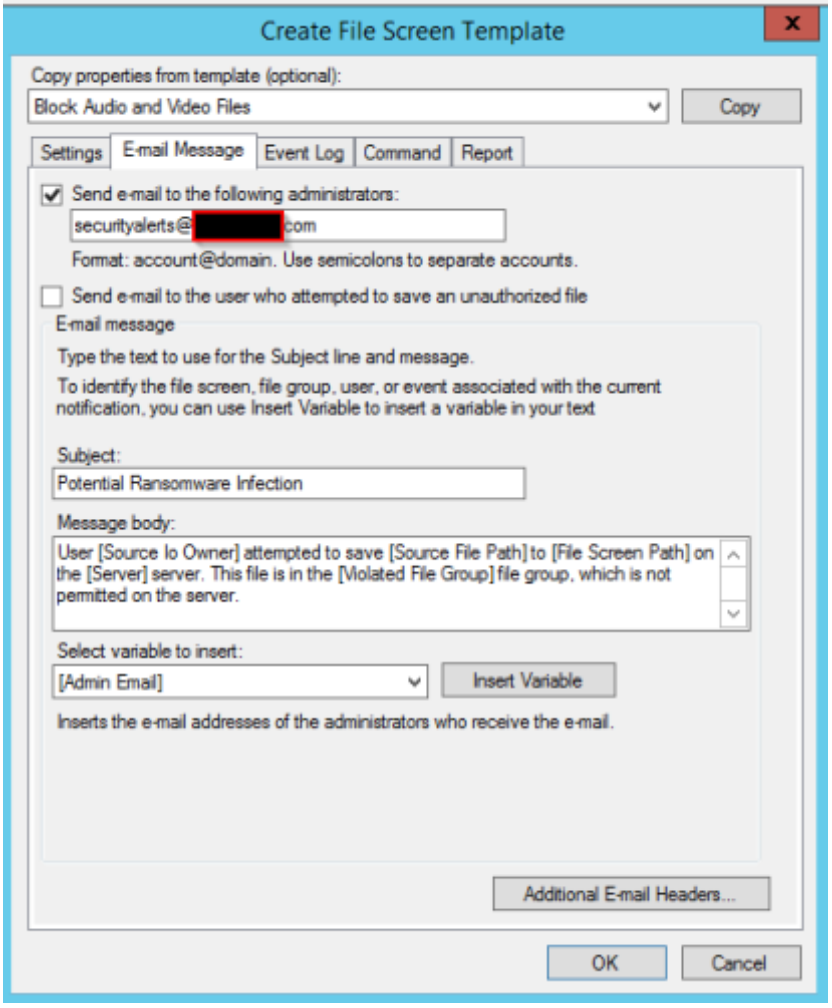
Create a new File Group under File Screening Management that will look at all files except our killswitch.txt.



Next, we will create a File Screen Template utilizing the File Group we created called “All File Types”.



We will want to configure email alerts, so on the E-Mail Message tab, fill out the pertinent information.



We also want to automate the removal of the offending user in order to stop the ransomware from encrypting our entire file server. We will do this with some PowerShell. Copy the following and save it to your preferred location. In this example, I'm just saving it to C:\kickuser.ps1.

param([string]$username = "") Get-SmbShare -Special $false | ForEach-Object { Block-SmbShareAccess -Name $_.Name -AccountName "$username" -Force }

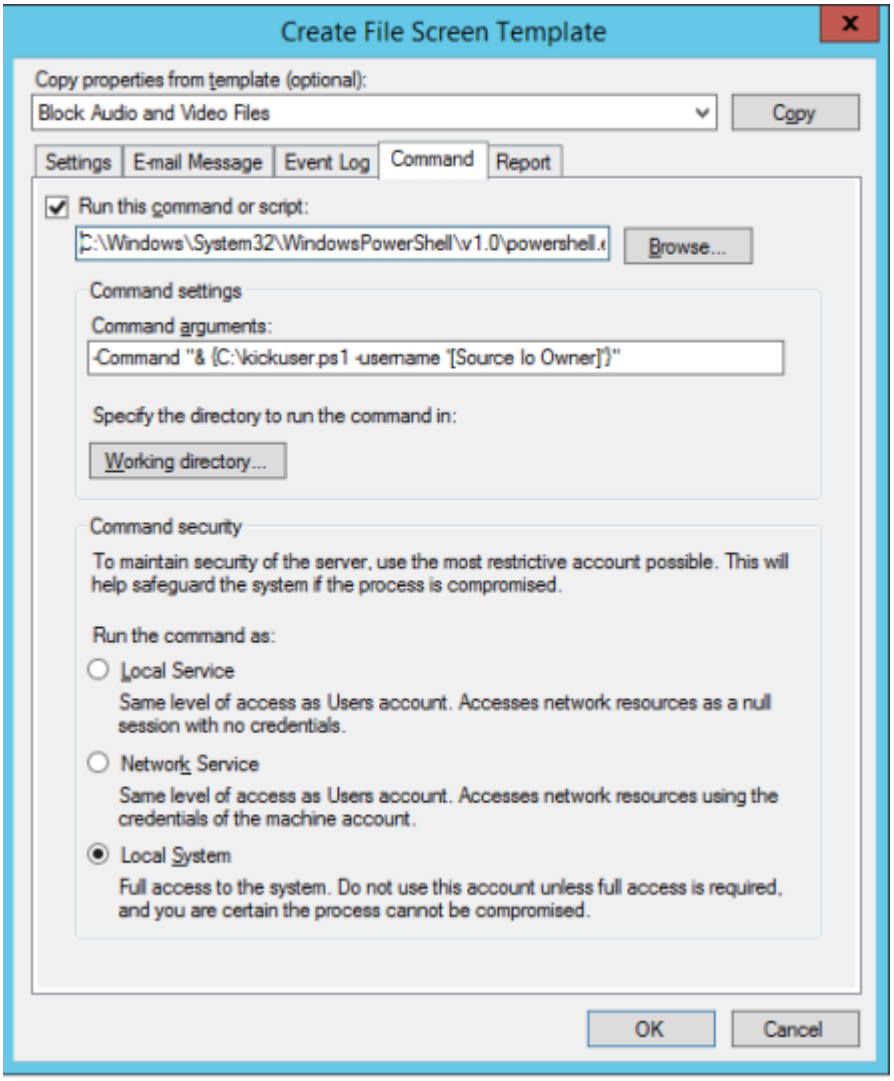
On the Command-Tab, check "Run this command or script:" and the following:

C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe

For the command arguments, insert the following:

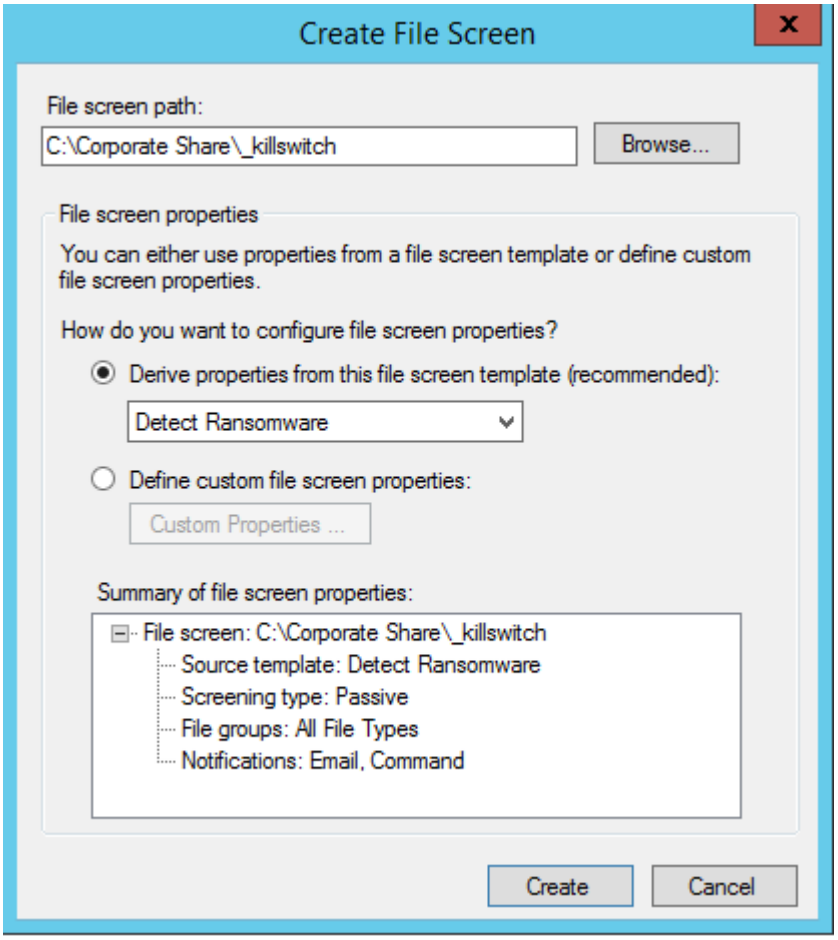
-Command "& {C:\smbblock.ps1 -username '[Source Io Owner]'}"

Set it to run as Local System.



Apply the File Screen

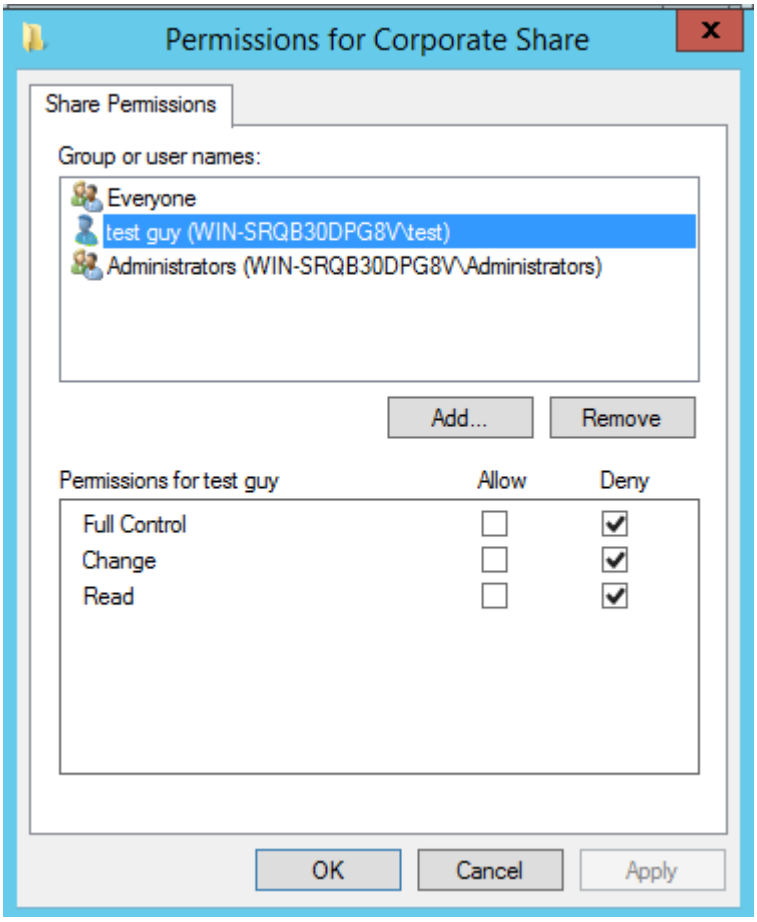
From within FSRM, Select File Screening Management > File Screens and create a new File Screen. Set the path to your underscore directory and use the “Detect Ransomware” File Screen template that we created earlier.



Testing

To test, I created a test account (test guy) and modified the file. I was instantly locked out of the share. The output of our PowerShell script, as well as the share permissions, show this:

```
Name                 ScopeName  AccountName                AccessControlType  AccessRight
----                 ---------  -----------                -----------------  -----------
Corporate Share      *          WIN-SRQB3ODPG8V\test       Deny               Full
Corporate Share      *          BUILTIN\Administrators     Allow              Full
Corporate Share      *          Everyone                   Allow              Full
```



Wrapping Up

This methodology should help mitigate some risk around ransomware attacks. In the future, it may also be beneficial to make the following changes:

1. Create a secondary killswitch in a ZZZ_Killswitch directory in case a ransomware-variant starts in reverse-alphabetical order.
2. Extend the PowerShell script to also lock out their AD account.
3. Create more killswitch files and file screens due to newer ransomware variants focusing on document and image files (.doc, .docx, .pdf, .jpg, .png, etc.)

I believe in using the resources we already have available to us in helping secure our organisations, and hopefully, this helps. Feel free to comment with any questions or suggestions.

Source: https://caintechnews.wordpress.com/category/windows/powershell/