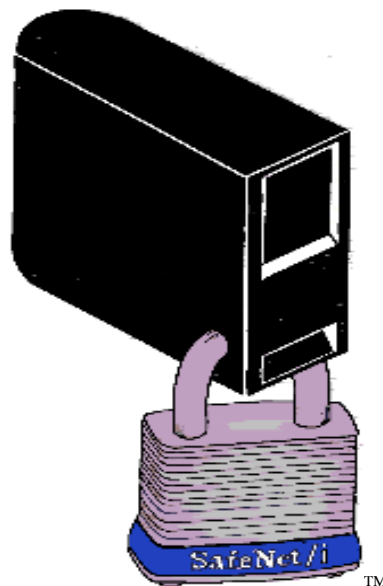


SafeNet/i

FOR IBM i

**RANSOMWARE DETECTION
AND
CONTROL**

SafeNet Version 12



How to contact us

Direct all inquiries to:

Kisco Systems LLC
54 Danbury Road
Suite 439
Ridgefield, CT 06877

Phone: (518) 897-5002

Email: support@kisco.com

SafeNet/i Website: <http://www.safeneti.com/>

SafeNet/i Support Website: <https://www.kisco.com/safenet/support/index.html>

Kisco Website: <https://www.kisco.com/>

Table of Contents

CHAPTER 1 – OVERVIEW	1-1
<i>What is Ransomware</i>	<i>1-1</i>
<i>Ransomware Detection.....</i>	<i>1-1</i>
CHAPTER 2 - SAFENET RANSOMWARE SETUP	2-1
<i>Licensing.....</i>	<i>2-1</i>
<i>Prerequisites:</i>	<i>2-1</i>
<i>How SafeNet/i Ransomware Detection works</i>	<i>2-2</i>
CHAPTER 3 - SAFENET RANSOMWARE DETECTION CONFIGURATION	3-4
<i>Initial Setup.....</i>	<i>3-5</i>
<i>Configurable Event Actions</i>	<i>3-7</i>
<i>Special Setup Considerations</i>	<i>3-9</i>
CHAPTER 4 – VIEWING AND WORKING WITH RANSOMWARE EVENTS.....	4-17
CHAPTER 5 – ROLLING BACK EVENT ACTIONS.....	5-21
CHAPTER 6 – FINDING THE TRANSACTIONS.....	6-23
<i>Commands available with the SafeNet/i Ransomware Detection module</i>	<i>6-28</i>
<i>Ransomware Detection Job Problem Determination</i>	<i>6-29</i>

SafeNet/i Ransomware Detection and Control Guide

Chapter 1 – OVERVIEW

What is Ransomware

Ransomware is a type of malicious software – or malware – that prevents you from accessing your computer files, systems or networks, and demands you pay a ransom for their return. Ransomware attacks can cause costly disruptions to operations and the loss of critical information and data.

You can unknowingly download ransomware onto a computer by opening an email attachment, clicking an ad, following a link, or even visiting a website that's embedded with malware.

Once the code is loaded on a computer, it will lock access to the computer itself or data and files stored there. More aggressive versions can encrypt files and folders on local drives, attached drives, and even networked computers.

Most of the time, you don't know your computer has been infected. You usually discover it when you can no longer access your data or you see computer messages letting you know about the attack and demanding ransom payments.

Ransomware Detection

Ransomware detection is a critical part of overall network security.

It is vital to the security of corporate infrastructure because it enables early intervention to minimize the massive financial, operational, and reputational damage that modern ransomware attacks cause. Advanced detection methods, such as behavioral and traffic analysis, are needed to spot sophisticated ransomware in the early stages, before it can fully encrypt files or exfiltrate sensitive data.

Early detection:

- **Avoids costly downtime:** By catching ransomware early, a company can isolate the threat before it spreads and encrypts critical systems across the network. This prevents catastrophic, company-wide downtime that could otherwise last for weeks and result in immense revenue loss.
- **Prevents data theft:** The majority of modern ransomware operations involve double extortion, where attackers steal sensitive data before encrypting it. Early detection is the only way to block data exfiltration attempts and prevent the irreversible damage of a public data leak.
- **Reduces recovery costs:** Detecting and containing an attack early can make remediation faster and more cost-effective. Organizations can restore systems from clean backups and avoid paying expensive ransom fees, which offer no guarantee of file recovery.

Enhanced security and resilience:

- **Helps maintain business continuity:** Incorporating robust ransomware detection into a broader cybersecurity strategy strengthens your overall resilience. This enables your organization to recover faster and minimize business disruption.
- **Ensures regulatory compliance:** Early detection is critical for companies in regulated industries, such as healthcare and finance. By limiting data exposure, it helps organizations avoid regulatory penalties for non-compliance with data protection laws.
- **Empowers rapid incident response:** An early detection system provides security teams with vital alerts and forensic information. This allows them to quickly identify the scope of the attack, pinpoint the root cause, and execute a response plan before extensive damage occurs.

Chapter 2 - SafeNet/i Ransomware Setup

Licensing

The **SafeNet/i Ransomware Detection and Control Module** is an optional feature available with SafeNet/i Version 12.

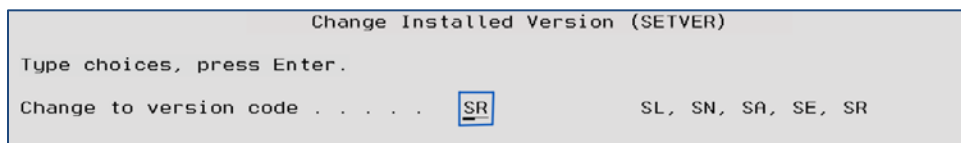
A separate license is required to use this feature.

30-day Trial License

To activate a 30-day trial, set your existing SafeNet/i license to include Ransomware detection.

Use the **SETVER** command to activate the Ransomware Detection Module.

Prompt **SETVER > F4** to set *Change to version code* to **SR**.



This begins your 30-day TRIAL license.

Please contact Kisco Systems for more information regarding the additional license requirements.

Prerequisites:

- The base SafeNet/i Version 12 **MUST** already be installed and configured on your system.
- Use the **WRKSRV** command to verify:
 - ***FILESRV PWFS0200** format **MUST** be activated on your system
 - ***FILESRV** exit point **MUST** be set to Security Level 3 or 4 to be able to use the SafeNet functions to block or disable use access to the ***FILESRV**. Level 1 can be used for Ransomware detection **alerts only**.
- Use the **CHGNOTIFY** command to make sure *Alert Notifications* for SafeNet/i are already configured and active.

How SafeNet/i Ransomware Detection works

SafeNet/i Ransomware Detection consists of several specialized processes which will analyze network transactions processed by the IBM i operating system. These transactions are held in the regular SafeNet log file and are collected using the base SafeNet/i exit point software. SafeNet/i Ransomware Detection uses a behavioral analysis algorithm to determine if possible ransomware activity is occurring on the system.

If potential ransomware activity is found, the SafeNet/i Ransomware module can immediately notify personnel and perform several user configurable ransomware counter Event Actions.

What does SafeNet/i Ransomware software look for?

The SafeNet/i Ransomware Detection module looks for repetitive actions during a pre-defined length of time. These would be actions that access the IBM i IFS via the File Server (i.e. IBM i NetServer), Java processes, and most other programs that can access the IBM i IFS objects. These actions could be file Reads, Copies, Moves, Renames and Rewrites (encrypting a file) or when a user tries to access a predefined “trigger” file.

When ransomware attacks your system, the typical behavior is to re-write a file using encryption, then rename the file and possibly move the file. All these types of “attack actions”, if done repeatedly will cause a **Ransomware Event** in SafeNet.

What are Trigger Files?

A Trigger File in SafeNet is a file that you specify to be used as a “lure” to “trigger” a ransomware event. This file or files can be placed in any system IFS directory and IF any user opens, copies or touches the file, a ransomware alert and event will be “triggered”. You can choose to just send an alert in the case of a file tampering or perform any of the other optional event control actions.

What are the Ransomware Event Control Actions that can be performed?

In the case of an actual Ransomware Event, SafeNet can perform several configurable Event Actions that include:

- Immediately terminating any File Server jobs associated with the offending user
- Disabling the user profile in the SafeNet/i base product. This will prevent future connections to the server from that user.

- Disabling the User Profile in the IBM i OS. This will prevent all types of access to the system for the offending user.
- Completely disable and turn off access to the *File server exit point for ALL Users. This would in effect be a complete shutdown of the IBM i NetServer.

What are the five main types of ransomware behavior being tracked?

- **File Read.** A file read action can be anything from browsing a directory using the Windows File Explorer or opening a file using a text editor. Most of the time, a read will not be an indicator of a ransomware attack. However, an excessive amount of reads or a change in pattern can indicate possible ransomware behavior.
- **File Rewrites.** A file rewrite action could be a user simply opening a file using the Windows File Explorer and a text editor. Or it could be a program that is actually encrypting one of your files. If a user is opening many files for update in a short period of time, that could be a real indication of a ransomware attack.
- **File Renames.** A typical behavior of ransomware is to rename a file after doing a rewrite to encrypt it. Renaming the file immediately hides its original purpose.
- **File Moves.** Also a typical ransomware behavior in some infections, ransomware may move files to different locations on the system after renaming them.
- **File Copies.** Sometimes Ransomware will copy a file before encrypting or renaming a file. Many file copies in a short period of time could also indicate a ransomware event is occurring.
- **OPTIONAL - TRIGGER FILES.** You can place a file anywhere in the IFS and if any user opens, copies, moves or tries to rename the file a Ransomware event will be generated.

Chapter 3 - SafeNet/i Ransomware Detection Configuration

Important: You must be signed on as a SafeNet/i Administrator prior to accessing the SafeNet/i Ransomware Detection functions.

1. Make sure your currently installed base SafeNet/i version is at V12.0 or above. You can check your current version by going to the SafeNet install menu and taking **Option 5**.

GO PCSECLIB/INSTALL

If you are not at V12 or above, you will need to upgrade to V12 before you can access the SafeNet/i Ransomware Detection Module.

2. Access the SafeNet/i Ransomware Main Menu

From the SafeNet/i Main Menu (SN1) use **Option 29 – Ransomware Detection**

or use command **GO PCSECLIB/SNRWD**

The *Ransomware Detection Menu* will be displayed:

SNRWD	SafeNet/i Version 12	10/06/25
MPADDEV	Ransomware Detection Menu	12:48:46
Select one of the following:		<u>Fast Path</u>
1. Work with Ransomware Detection Status		WRKSNRWD
2. Work with Ransomware Events		WRKRWEVT
3. View Historical Network Transactions		PCREVIEW
4.		
5.		
6. Work with TRIGGER File Definitions		WRKRWPTH
7. Work with Path Exclusions		WRKRWPTH
8.		
9.		
10. WRKACTJOB SBS(SAFELOGING)		
21. SafeNet Main Menu(SN1)		
Selection or command		(c) Copyright 1997-2025 MP Assoc., Inc.
==>		
F3=Exit F4=Prompt F9=Retrieve F12=Cancel		
F13=Information Assistant F16=System main menu		

Continue with the initial setup of Ransomware Detection and Controls.

Initial Setup

Prerequisites:

Make sure *Alert Notification Status* in the base SafeNet/i product is set to ***ON** and configured properly to be able to send Ransomware alerts.

Before you turn on Ransomware Controls, you will want to let it run without taking any actions. This will give you the opportunity to analyze your network traffic prior to allowing Ransomware to change or terminate user activity.

Review Default Configuration:

From the Ransomware Detection Menu (SNRWD) use **Option 1-Work with Ransomware Detection Status**.

This will display the current status of the *Ransomware Detection Jobs*.

Initially the *Detection Job Status* should be *Inactive* and *AutoStart Detection Job* set to *No*.

```
RwSTAT10
MPADDEV
SafeNet/i vi2
SafeNet/i Ransomware Status
10/06/25
13:53:05
Options:
1=StartJob 2=Change 7=WorkJob
Last Event Date
2025-10-03-20.08.44
Enter option, press enter:
Detection Job Function. . . Reads Renames Rewrites Moves Copies Triggers
Detection Job Name. . . . RWREADS RWRENAMES RWREWRITES RWMOVES RWCOPIES RWTRIGGERS
Detection Job Status. . . Inactive Inactive Inactive Inactive Inactive Inactive
AutoStart Detection Job. . No No No No No No
Event Threshold Count . . 25 3 20 3 3 1
Recheck Delay in Seconds. 30 30 30 30 30 30
Lookback Time in Minutes. 10 10 10 10 10 30
-----Event Actions-----
Disable User in SafeNet?. . No No No No No No
End User *FILESRV Jobs? . . No No No No No No
Disable IBMi User Profile?. No No No No No No
Block ALL *FILESRV Access?. No No No No No No
F1=Help F3=Exit F10=View RW Events (c)1997-2025 MP Associates, Inc
```

The six RW Detection Jobs are listed across the top of the screen, and their descriptions are as follows:

- **Reads:** Any IFS operation that reads an IFS object.
- **Renames:** Any IFS operation that renames an IFS object.
- **Rewrites:** Any IFS operation that simply opens a file for Update.
- **Moves:** Any IFS operation that moves a file from one directory to another.
- **Copies:** Any IFS operation that copies a file to the same or other location.
- **Triggers:** You can set any file name to be used as bait or a trigger file. Any attempt to open, move, copy, rename or access the file will “trigger” a ransomware event in SafeNet.

Configurable Ransomware Detection Job Settings

Ransomware Detection Job Settings are configured using *Option 2 (Change)* on the *Work with Ransomware Detection Status* screen.

The screenshot shows the 'SafeNet/i v12' interface with the title 'SafeNet/i Ransomware Status'. The date and time are 10/06/25, 13:56:36. The 'Options:' section shows '1=StartJob', '2=Change' (highlighted), and '7=WorkJob'. The 'Last Event Date' is 2025-10-03-20.08.44. Below this is a table of settings for six detection jobs: Reads, Renames, Rewrites, Moves, Copies, and Triggers. Each job has a status (Inactive) and a list of actions (RUREADS, RURENAMES, RUREWRITES, RUMOVES, RUMCOPIES, RUMTRIGGERS) with their respective counts (25, 30, 10, 3, 3, 1). At the bottom, there are keyboard shortcuts: F1=Help, F3=Exit, and F10=View RU Events. The copyright notice '(c)1997-2025 MP Associates, Inc.' is at the bottom right.

Enter option, press enter:	Reads	Renames	Rewrites	Moves	Copies	Triggers
Detection Job Function. . .	RUREADS	RURENAMES	RUREWRITES	RUMOVES	RUMCOPIES	RUMTRIGGERS
Detection Job Name.	Inactive	Inactive	Inactive	Inactive	Inactive	Inactive
Detection Job Status. . . .	Yes	Yes	Yes	Yes	Yes	No
AutoStart Detection Job. . .	25	3	20	3	3	1
Event Threshold Count. . . .	30	30	30	30	30	30
Recheck Delay in Seconds. .	10	10	10	10	10	30
Lookback Time in Minutes. .	----Event Actions----					
Disable User in SafeNet?. . .	No	No	No	No	No	No
End User *FILESRV Jobs?. . .	No	No	No	No	No	No
Disable IBMi User Profile?. .	No	No	No	No	No	No
Block ALL *FILESRV Access?. .	No	No	No	No	No	No

These are the configurable settings for each of the six Ransomware Detection Jobs

AutoStart Detection Job:

If this value is set to YES, the job will start and end automatically with the regular SafeNet logging job in the SAFELOGING subsystem. See the STRTRP and ENDTRP commands for the logging job instructions.

If this parameter is set to NO, then you must manually start the detection Jobs by using the STRSNRWD command or the WRKSNRWD command.

Default setting is **NO**.

Event Threshold Count:

This is the number of repetitive operations from a single user in the Look Back Time frame that would be considered a potential ransomware event. If this count value is exceeded in the given look back time a ransomware event will be triggered.

Decreasing this value may lead to a higher false positive rate.

Increasing this value may allow a ransomware attack to progress farther before detection.

Default setting is a count of **3** for all the detection jobs **except for READS**.

For READS the default value is **25**. However, you may need to raise this value considerably based on your system usage.

Recheck Delay in Seconds:

This is the time in seconds the detection process will sleep before rechecking transactions for ransomware events.

Decreasing this value could have a potential performance impact on high transaction volume systems.

Increasing this value could potentially allow a ransomware attack to progress farther before detection.

Default setting is **30 seconds**.

Lookback Time in Minutes:

This value is the amount of time the detection job will “look back” at transactions to determine if the threshold count has been met or exceeded.

Decreasing this value could potentially allow a ransomware attack to progress without being detected or it could potentially allow the infection to progress farther before detection.

Increasing this value could have a potential performance impact on high transaction volume systems.

Default Value is **10 minutes**.

Configurable Event Actions

If Ransomware Events are discovered, you have options to counter those attacks. The following Event Actions can be used to stop or thwart an attack once detected.

Disable User in SafeNet:

If this is set to **YES**, a Ransomware Event will cause SafeNet to put a specific rejection entry into the User-To-Server control file that will REJECT all further NetServer/*FILESRV connections from the offending user. Use WRKUSRSRV to review user authorities to the server.

This function is only available if the *FILESRV exit point security is set to level 3 or 4 within SafeNet.

Recommended value: **YES**

End User *FILESRV Jobs:

If this is set to **YES**, all current NetServer Jobs for the user will be terminated immediately. When used with the above “*Disable User in SafeNet*”, this parameter will ensure all active connections are terminated and the individual user will no longer be able to access the IBM i NetServer.

Recommended Value: **YES**

Disable IBM i User Profile:

If this value is set to YES, a Ransomware Event will cause SafeNet to disable the IBM i user profile.

SafeNet will issue the command: CHGUSRPRF USRPRF(*userprofile*) STATUS(*DISABLED)

This will completely disable the user on the system. The user will no longer be able to access any interface on the system including native 5250 sessions.

Recommended Setting: **NO**

Block ALL *FILESRV Access:

If this value is set to **YES**, SafeNet will block ALL access by ALL users to the NetServer/*FILESRV. This will change the value in the SafeNet Server Settings for the *FILESRV exit point to a Security Level 2, meaning **NO ACCESS** for all users. This is considered an extreme measure.

Recommended Setting: **NO**

Important Note: If all the configurable **Event Actions** are set to **NO**, Ransomware Alerts ONLY will be sent to the administrators.

When initially starting to use Ransomware Detection you should leave ALL these Event Actions to **NO** until you are sure your normal daily processing does not generate false positives.

Special Setup Considerations

It is important to decide if you need to “exclude” certain users or IFS paths from being included in the ransomware scans. If you have heavy users of the IBM i NetServer or if you have specific IFS directories that need to be excluded from the ransomware detection scanning, then you need to do some additional setup. It’s possible that some jobs or users that interact with the IFS content could trigger a ransomware event as a false positive.

Excluding Directory Paths from Ransomware scanning

If you have a directory path that should be excluded, use **Option 6 - Work with Path Exclusions** and enter the Exclusion path into the control file. This is a global system setting.

```
SNRWD                      SafeNet/i Version 12                      10/06/25
MPADEV                      Ransomware Detection Menu                 12:48:46

Select one of the following:
  1. Work with Ransomware Detection Status
  2. Work with Ransomware Events
  3. View Historical Network Transactions
  4.
  5.
  6. Work with TRIGGER File Definitions
  → 7. Work with Path Exclusions
  8.
  9.
 10. WRKACTJOB SBS(SAFELOGING)

21. SafeNet Main Menu(SN1)

Fast Path
WRKSNRWD
WRKRWEVT
PCREVIEW
WRKRWPTH
WRKRWPTH

Selection or command
====>

F3=Exit  F4=Prompt  F9=Retrieve  F12=Cancel
F13=Information Assistant  F16=System main menu
```

```
WRKRWPTHR                  SafeNet/i  v12
MPADEV                      Maintain IFS Ransomware Path Names

Options:      2=Edit Long IFS Path      4=Delete IFS Path
Add records, press enter. Maximum: 10 records
Opt  Ransomware Exclusion Path Names

_ /PackingLists/
_ /anonftp/
```

Excluding Users from Ransomware scanning:

If you need to exclude certain users from a detection job, access the detection job's settings, and include those users on the *Users to Omit* parameter.

You may use the individual detection job settings commands (CHGSNRW1, CHGSNRW2, etc.), or you may use *Option 2* (Change) from the *Ransomware Detection Status* screen to change the job settings. This is a detection job-based setting.

```

RwSTAT10                               SafeNet/i v12                               10/06/25
MPADeV                                SafeNet/i Ransomware Status                               13:26:18

Options:                                Last Event Date                               2025-10-03-20,08.44
1=StartJob 2=Change 7=WorkJob

Enter option, press enter:
Detection Job Function. . . . . 2
Detection Job Name. . . . .
Detection Job Status. . . . . Inactive
AutoStart Detection Job. . . . . Yes
Event Threshold Count. . . . . 5
Recheck Delay in Seconds. . . . . 30
Lookback Time in Minutes. . . . . 10
----- Event Actions -----
Disable User in SafeNet? . . . . . No
End User *FILESRV Jobs? . . . . . No
Disable IBMi User Profile? . . . . . No
Block ALL *FILESRV Access? . . . . . No

F1=Help      F3=Exit                               F10=View RM Events (c)1997-2025 MP Associates, Inc

```

Each of the detection jobs allows for omitting certain users from triggering a Ransomware Event. You can enter up to 10 users to omit.

```

Ransomware Detection Settings (CHGSNRW1)

Type choices, press Enter.

AutoStart *RENAME Pattern Job?      *YES      *YES, *NO
Look Back Time in Minutes . . . . . 10        # of Minutes
Event Threshold Count . . . . . 3        Number
Pattern Recheck Delay . . . . . 30        # of Seconds
Disable User in SafeNet? . . . . . *YES      *YES, *NO
End User *FILESRV Jobs? . . . . . *YES      *YES, *NO
Disable IBMi User Profile? . . . . . *YES      *YES, *NO
Block ALL *FILESRV Access? . . . . . *NO       *YES, *NO
Users to Omit . . . . . *NONE      Name, *NONE
+ for more values

```

Configuring a Trigger file

To add a trigger file, use **Option 6 – Work with TRIGGER File Definitions** on the Ransomware Detection Menu (SNRWD) or use the **WRKRWPTH** command

```
SNRWD                      SafeNet/i Version 12                      10/06/25
MPADEV                     Ransomware Detection Menu                 12:48:46

Select one of the following:
  1. Work with Ransomware Detection Status
  2. Work with Ransomware Events
  3. View Historical Network Transactions
  4.
  5.
  → 6. Work with TRIGGER File Definitions
  7. Work with Path Exclusions
  8.
  9.
 10. WRKACTJOB SBS(SAFELOGING)

                                Fast Path
                                WRKSNRWD
                                WRKRWEVT
                                PCREVIEW
                                WRKRWPTH
                                WRKRWPTH

 21. SafeNet Main Menu(SN1)

Selection or command          (c) Copyright 1997-2025 MP Assoc., Inc.
===>

F3=Exit  F4=Prompt  F9=Retrieve  F12=Cancel
F13=Information Assistant  F16=System main menu
```

You may add one or more file names that you wish to use as triggers (decoys). The file(s) can exist on any IFS directory and can be in multiple directories if needed. Once active, ANY operation on the file(s) in any directory will trigger a Ransomware Event in SafeNet.

```
WRKRWPTH                    SafeNet/i    v12
MPADEV                     Maintain IFS Ransomware Path Names

Options:      2=Edit Long IFS Path      4=Delete IFS Path
Add records, press enter. Maximum: 10 records
Opt  Ransomware Trigger Path Names

_ /anyfile.txt
_ /mikesfile.xlsx
```

Starting Ransomware Jobs

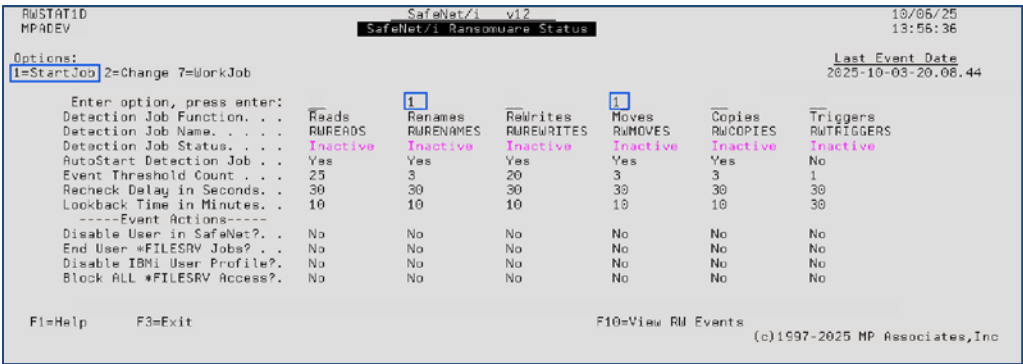
After making the following changes to *AutoStart* values, remember to use the normal SafeNet/i **STRTRP** and **ENDTRP** commands to start and stop the jobs along with the regular SafeNet Logging job in subsystem *SAFELOGING*.

You can start the Ransomware jobs **Manually** or **Automatically**

1. Manually

From the Ransomware Detection Menu use **Option 1 – Work with Ransomware Detection Status**

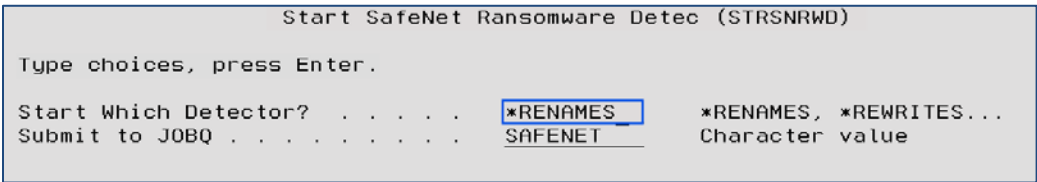
On the Ransomware Status screen type a **1** (*StartJob*) above each job to start



OR

On a command line, enter the command **STRSNRWD** and **press F4**.

Enter the name of the job you want to start and press enter.



2. Automatically

Set Autostart Detection Job to **Yes** for each job you want to start automatically

Type a **2** (Change) above the job

```

RwSTAT10                               SafeNet/i v12                10/05/25
MPADeV                                SafeNet/i Ransomware Status    13:56:36

Options:
1=StartJob 2=Change 7=WorkJob          Last Event Date
                                       2025-10-03-20:08:44

Enter option, press enter:
Detection Job Function. . . . . 1 Reads      Renames      Rewrites      Moves      Copies      Triggers
Detection Job Name. . . . .      RUREADS     RURENAMES     RUREWRITES     RUMOVES     RUCOPIES     RUTRIGGERS
Detection Job Status. . . . .      Inactive    Inactive      Inactive      Inactive    Inactive      Inactive
AutoStart Detection Job. . . . .      Yes        Yes          Yes          Yes        Yes          Yes
Event Threshold Count. . . . .      25         3           20          3          3           1
Recheck Delay in Secnds. . . . .      30         30          30          30         30          30
Lookback Time in Minutes. . . . .      10         10          10          10         10          30

-----Event Actions-----
Disable User in SafeNet?. . . . .      No         No           No           No          No          No
End User *FILESRV Jobs?. . . . .      No         No           No           No          No          No
Disable IBMi User Profile?. . . . .      No         No           No           No          No          No
Block ALL *FILESRV Access?. . . . .      No         No           No           No          No          No

F1=Help      F3=Exit                                F10=View RM Events    (c)1997-2025 MP Associates, Inc
  
```

Change *AutoStart xxx Job* to ***YES**

```

Change Ransomware *COPIES Job (CHGSNRW4)

Type choices, press Enter.

AutoStart *COPIES Pattern Job?      *YES          *YES, *NO
Look Back Time in Minutes . . . . . 10            # of Minutes
Event Threshold Count . . . . .      3            Number
Pattern Recheck Delay . . . . .      30           # of Seconds
Disable User in SafeNet? . . . . .  *NO           *YES, *NO
End User *FILESRV Jobs? . . . . .  *NO           *YES, *NO
Disable IBMi User Profile? . . . . .  *NO           *YES, *NO
Block ALL *FILESRV Access? . . . . .  *NO           *YES, *NO
Users to Omit . . . . .              *NONE         Name, *NONE
+ for more values                    _____
  
```

OR

On a command line, enter the command **CHGSNRWx AUTOSTR(*YES)**

Where **x** is:

1 = Renames	4 = Moves
2 = Rewrites	5 = Triggers
3 = Copies	6 = Reads

Ending Ransomware Jobs

Under normal circumstances, you would not be ending the Ransomware Detection jobs. However, if you need to end the jobs individually, you can use *Ransomware Detection Status* to do this.

From the Ransomware Detection Menu (SNRWD) use **Option 1 – Work with Ransomware Detection Status**

Option 7 (WorkJob) allows you to work with each job individually.

Type **7** on each job to be ended and **ENTER**.

```
RwSTAT10                               SafeNet/i v12                               10/05/25
MPADEV                                SafeNet/i Ransomware Status                               14:50:14

Options:
1=StartJob 2=Change 7=WorkJob                               Last Event Date
                                                            2025-10-03-20:08:44

Enter option, press enter:
Detection Job Function... Reads      Renames    Rewrites   Moves     Copies    Triggers
Detection Job Name...    RMREADS   RMRENAMES  RMREWRITES RMMOVES   RMCOPIES  RWTRIGGERS
Detection Job Status...  Active    Active     Active     Active    Active    Active
AutoStart Detection Job... Yes       Yes        Yes        Yes       Yes       No
Event Threshold Count... 25        3          20         3         3         1
Recheck Delay in Seconds... 30       30         30         30        30        30
Lockback Time in Minutes... 10       10         10         10        10        30
-----Event Actions-----
Disable User in SafeNet?... No        No         No         No        No        No
End User *FILESRV Jobs?... No        No         No         No        No        No
Disable IBMi User Profile?... No        No         No         No        No        No
Block ALL *FILESRV Access?... No        No         No         No        No        No

F1=Help      F3=Exit                               F10=View RM Events   (c)1997-2025 MP Associates, Inc
```

After using *Option 7* you will be presented with one of two screens.

If there is only one job running on your system, you will see the IBM i OS *Work with Job* display.

```
Work with Job                               System:  MPADEV
Job:  RWTRIGGERS   User:  SAFENET   Number:  608878

Select one of the following:

  1. Display job status attributes
  2. Display job definition attributes
  3. Display job run attributes, if active
  4. Work with spooled files

 10. Display job log, if active, on job queue, or pending
 11. Display call stack, if active
 12. Work with locks, if active
 13. Display library list, if active
 14. Display open files, if active
 15. Display file overrides, if active
 16. Display commitment control status, if active

Selection or command
====> 41

F3=Exit  F4=Prompt  F9=Retrieve  F12=Cancel
```

Use **Option 41** and select **IMMED* to end the job immediately

If there are multiple jobs running on your system, either active or inactive, you will see the *Select Job* display.

Type **1** under *Option* to select the active job and **ENTER**.

Select Job						MPADEV
Type option, press Enter.						10/06/25 14:54:16 EDT
1=Select						
Option	Job	User	Number	Type	-----Status-----	Entered System
1	RWTRIGGERS	SAFENET	608878	BATCH	ACTIVE	10/06/25
—	RWTRIGGERS	SAFENET	608806	BATCH	OUTQ	10/06/25
—	RWTRIGGERS	SAFENET	608753	BATCH	OUTQ	10/06/25
—	RWTRIGGERS	SAFENET	608248	BATCH	OUTQ	10/03/25
—	RWTRIGGERS	SAFENET	608237	BATCH	OUTQ	10/03/25
—	RWTRIGGERS	SAFENET	608225	BATCH	OUTQ	10/03/25
—	RWTRIGGERS	SAFENET	608204	BATCH	OUTQ	10/03/25
—	RWTRIGGERS	SAFENET	608192	BATCH	OUTQ	10/03/25
—	RWTRIGGERS	SAFENET	608144	BATCH	OUTQ	10/03/25
—	RWTRIGGERS	SAFENET	606377	BATCH	OUTQ	09/25/25
F3=Exit F12=Cancel						Bottom
Duplicate jobs found.						

This will bring you to the IBM i OS *Work with Job* display.

Use **Option 41** and select **IMMED* to end the job immediately

Return to the *Ransomware Dection Status* display and repeat this process for each job you want to end.

Important - Ending Ransomware Detection jobs and SafeNet Logging

If you use the SafeNet/i ENDTRP command, then ALL the Ransomware Detection jobs will end, along with normal SafeNet/i logging.

If you use the ENDTRP command and DO NOT want the Detection jobs to restart automatically with the logging job restart, then you must change each of the Ransomware Detection job settings to *AUTOSTART(*NO)*.

Viewing the Current Active Jobs for SafeNet Logging and Ransomware Detection

From the Ransomware Detection Menu (SNRWD) use **Option 10 – WRKACTJOB**
SBS(SAFELOGING)

This displays both the *SAFELOGING* job as active along with the *ALERTWATCH* process (required for Ransomware Alerts) and the various jobs for Ransomware Detection.

Work with Active Jobs						MPADEV
CPU %:		Elapsed time:		10/06/25 14:13:27 EDT		
1.3		00:49:24		Active jobs:		230
Type options, press Enter.						
2=Change		3=Hold	4=End	5=Work with	6=Release	7=Display message
8=Work with spooled files		13=Disconnect ...				
Current						
Opt	Subsystem/Job	User	Type	CPU %	Function	Status
—	SAFELOGING	QSYS	SBS	.0		DEQW
—	ALERTWATCH	SAFENET	PJ	.0	DLY-120	DLYW
—	RWCOPIES	SAFENET	BCH	.0	PGM-SNRW004CL	SIGW
—	RWMOVES	SAFENET	BCH	.0	PGM-SNRW003CL	SIGW
—	RWREADS	SAFENET	BCH	.0	PGM-SNRW006CL	SIGW
—	RWRENAMES	SAFENET	BCH	.0	PGM-SNRW001CL	SIGW
—	RWREWRITES	SAFENET	BCH	.0	PGM-SNRW002CL	SIGW
—	RWTRIGGERS	SAFENET	BCH	.0	PGM-SNRW005CL	SIGW
—	SAFELOGING	SAFENET	BCH	.0	PGM-WRITETCL	DEQW
						Bottom
Parameters or command						
==>						
F3=Exit	F5=Refresh	F7=Find	F10=Restart statistics			
F11=Display elapsed data	F12=Cancel	F23=More options	F24=More keys			

Chapter 4 – Viewing and Working with Ransomware Events

If a Ransomware Event is detected on the system, there are several things that will happen based on your *Event Action* settings for each Detection job.

1. An Alert notification will be sent to all the users defined in the CHGNOTIFY command. This is the list of users that get the normal alerts from SafeNet. The Alert will contain information about the Ransomware Event and what actions were taken.

Alert email sample:

ALERT: SafeNet Has Rejected 3 Requests on System: MPADEV Since 10/09/25 At 16:10:12

Details:

User:	Server:	Reason:	TimeStamp:	Client IP:
CLEWIST	*SPECIAL	Possible Ransomware Event Detected	2025-10-09-16.10.53.691073	127.0.0.1
CLEWIST	*SPECIAL	Ransomware Event! SN User Disabled	2025-10-09-16.10.53.810877	127.0.0.1
CLEWIST	*SPECIAL	Ransomware Event! User Jobs Ended	2025-10-09-16.10.53.917245	127.0.0.1

2. To view the details of the events, select **Option 2** on the Ransomware Detection Menu

```
SNRWD                      SafeNet/i Version 12                      10/09/25
MPADEV                     Ransomware Detection Menu                 16:12:05

Select one of the following:
  1. Work with Ransomware Detection Status
  2. Work with Ransomware Events
  3. View Historical Network Transactions
  4.
  5.
  6. Work with TRIGGER File Definitions
  7. Work with Path Exclusions
  8.
  9.
 10. WRKACTJOB SBS(SAFELOGING)

21. SafeNet Main Menu(SN1)

Fast Path
WRKSNRWD
WRKRWEVT
PCREVIEW
WRKRWPTH
WRKRWPTH

Selection or command
==> 2
```

Or use the command **WRKRWEVT** to display the most recent events.

RUEVENTR	SafeNet Ransomware							11/13/25
MPADEV	Ransomware Event Actions							11:06:53
Options:		Position to Date: 251106 YYMMDD						
1=Display, R=Rollback								
Event								Rollback
Opt	No.	Action Taken	Operation	On User	Status	Server	Date of Action	Back
-	111	Possible Ransomware Event Detected	*RWALERT	CLEWIS	*ALERT	*FILESRV	2025-11-06 10:38	
-	111	Ransomware Event! SN User Disabled	ADDUSRSRV	CLEWIS	*DISABLED	*FILESRV	2025-11-06 10:38	Yes
-	111	Ransomware Event! User Jobs Ended	ENDJOB	CLEWIS	*IMMED	*FILESRV	2025-11-06 10:38	

Shown above is a list of Event Actions

1. The first line shows that a Ransomware Event was detected and that an Alert was sent.
2. The second line shows a specific single Event Action that was performed. In this case, the event action indicates the User in SafeNet was Disabled.
3. The third line indicates another Event Action that was performed. In this case, the action performed was to END all the user's current IBM i NetServer/*FILESRV jobs. Line 3 is also a type of Event Action that can be *Rolledback*. (See Chapter 5 in this guide for more information on events that can be rolled back.)
4. Any additional actions performed would also be listed if applicable.

Viewing the Event Action Details:

From the above Ransomware Event Actions display, choose *Option 1* and press **ENTER** to display the details of a selected Event Action.

In this example, the details for the first Event Action have been selected. The upper part of the detail screen shows the event details and any actions that were taken. The lower part of the screen shows the reason for the Event Detection.

Event		
Opt	No.	Action Taken
1	109	Possible Ransomware Event Detected
-	109	Ransomware Event! SN User Disabled
-	109	Ransomware Event! User Jobs Ended

RwEVENTR	SafeNet Ransomware	10/14/25
	Ransomware Event Actions	12:36:51
Event--> Possible Ransomware Event Detected Event#--> 109		
Date---> 2025-10-09-16.10.53.704040		
Action-> *RWALERT CLEWIST *ALERT		
Server-> *FILESRV		
Threshold Exceeded for *FILESRV *RENAMES		
The event count was 3 during the time range of 2025-10-09-16.00.53.350382 -thru- 2025-10-09-16.10.53.397821		
The events were performed by user CLEWIST		
F1=Help	F3=Exit	F10=View Event Transactions F12=Return

Shown are the details of the first event

1. A possible Ransomware Event was detected and the event ID number assigned.
2. The Date and Time of the event.
3. The Action was that an Alert was sent, and it lists the user profile that caused the Event.
4. The *FILESRV exit point was where the event was detected.
5. The Event Count and the time frame that the operations occurred in. You can use these date/time values to find the transaction details for the user in *PCREVIEW*.
6. The user profile who performed the operations that triggered the Event Alert.

In this next example, the details for the second Event Action have been selected.

Event		Action Taken
Opt	No.	
—	109	Possible Ransomware Event Detected
<u>1</u>	109	Ransomware Event! SN User Disabled
—	109	Ransomware Event! User Jobs Ended

```
SafeNet: Ransomware
Ransomware Event Actions
10/14/25
12:47:07

Event--> Ransomware Event! SN User Disabled   Event#--> 109           Rolledback to Previous?--> No
* The User was Disabled in SafeNet.

Date--> 2025-10-09-16.10.53.811418
Action-> ADDUSRSRV CLEMIST *DISABLED
Server-> *FILESRV

New Security Setting-> *Reject
New Logging Level----> *All

Threshold Exceeded for *FILESRV *RENAMES
The event count was 3 during the time range of 2025-10-09-16.00.53.350382 -thru- 2025-10-09-16.10.53.397821
The events were performed by user CLEMIST

F1=Help      F3=Exit      F10=View Event Transactions  F12=Return    F24 to Rollback Change
```

Shown are the details of the second Event and Action:

1. The SafeNet User was Disabled.
2. The Date and Time of the Event Action.
3. The Action taken was (ADDUSRSRV) and the user was Disabled.
4. The New Security Setting and logging level for the user in SafeNet.
Note: If the user had previous security settings, those settings have been recorded for rollback if necessary.
5. The bottom of the screen explains all the reasons WHY the Action was taken.
6. On the upper right of the screen you can see the Rolledback status. If this is displayed and the value is NO, then you can use the F24 function key to reverse or RollBack the changes made automatically due to the event. A value of YES indicates the Event Action has already been Rolledback or reversed.

In this next example, the details for the third Event Action have been selected.

Event		
Opt	No.	Action Taken
—	109	Possible Ransomware Event Detected
—	109	Ransomware Event! SN User Disabled
<u>1</u>	109	Ransomware Event! User Jobs Ended

```

RWEVENTR                                     SafeNet Ransomware                               10/14/25
                                           Ransomware Event Actions                               13:12:52

Event--> Ransomware Event! User Jobs Ended   Event#--> 109
          * The Users Active *FILESRV Jobs were Ended.

Date---> 2025-10-09-15.10.53.917784
Action-> ENDJOB      CLEWIST      *IMMED
Server-> *FILESRV

Threshold Exceeded for *FILESRV *RENAMES
The event count was 3 during the time range of 2025-10-09-15.00.53.350382 -thru- 2025-10-09-15.10.53.397821
The events were performed by user CLEWIST

F1=Help      F3=Exit      F10=View Event Transactions      F12=Return

```

Shown are the details of the third Event and Action:

1. The User's **FILESRV* NetServer Jobs were terminated. This is the users connection to the **FILESRV* exit point/IBM i NetServer.
2. The Date and Time of the Event Action.
3. The Action taken was ENDJOB *IMMED.
4. The bottom of the screen explains all the reasons WHY the Action was taken.
5. On the upper right of the screen you can see there is no Rolledback status since there is no Rollback option available for this action.

The above only shows a sampling of the possible event actions that could have been taken. See the previous section describing the Configurable Event Actions that are available.

Chapter 5 – Rolling Back Event Actions

What is a RollBack for an Event Action?

Certain Event Actions that were performed can be rolled back to the original values if needed or in the case of false positive results.

Event Actions that can be Rolledback

1. User was disabled in SafeNet
This indicates a REJECT entry added to the Server Control file for the user in SafeNet for the *FILESRV exit point. Use command WRKUSRSRV.
2. User Profile was Disabled in IBM i
This indicates the offending users native profile was set to *DISABLED status in IBM i OS.
3. All Access to IBM i NetServer/*FILESRV was Blocked
This indicates that the *FILESRV exit point security setting has been changed to Level 2 meaning NO ACCESS for all users in SafeNet Security Settings. Use command WRKSRV.

How to Rollback an Event Action

When viewing an Event from the Event Log display and you see a *NO* value in the right column under Rolledback then it is possible to reverse or rollback the changes made due to the event.

Event	Action Taken	Operation	On User	Status	Server	Date of Action	Rolled Back?
Opt No.							
[R] 109	Possible Ransomware Event Detected	*RMLERT	CLEWIST	*ALERT	*FILESRV	2025-10-09 16:10	No
109	Ransomware Event! SN User Disabled	ADDUSASRV	CLEWIST	*DISABLED	*FILESRV	2025-10-09 16:10	No
- 109	Ransomware Event! User Jobs Ended	ENDJOB	CLEWIST	*IMMED	*FILESRV	2025-10-09 16:10	No

To rollback event actions, use *Option R* (Rollback) or enter a *1* to display the Event Details and then **press F24**.

If the value you see is *YES* under *Rolledback* then the changes that were made during the event were previously reversed to their original values.

Once an event has been Rolledback, the event details will show the *Rolledback* status as *YES* and the *Rollback* action as **ENABLED*.

```
RmEVENTR                                     SafeNet Ransomware                               10/14/25
                                     Ransomware Event Actions                          14:12:21

Event--> Ransomware Event! SN User Disabled   Event#--> 109
          * The User was Disabled in SafeNet.

Date--> 2025-10-09-15.10.53.811418
Action-> ADDUSASRV CLEWIST *DISABLED
Server-> *FILESRV

Rolledback to Previous?--> Yes
Rolledback By--> SAFENET

Rollback Date--> 2025-10-14-14.12.18.025055
Rollback Action--> *ENABLED

Threshold Exceeded for *FILESRV *RENAMES
The event count was 3 during the time range of 2025-10-09-15.00.53.350382 -thru- 2025-10-09-15.10.53.397821
The events were performed by user CLEWIST

F1=Help      F3=Exit      F10=View Event Transactions      F12=Return
```

Chapter 6 – Finding the Transactions

When a Ransomware Event is detected, you may want to review all the transactions that caused the event. You can view the events using the SafeNet *On-Line Transaction Review* screen (*PCREVIEW*) or by running a SafeNet security report.

Viewing the transactions that caused the event detection:

1. The easiest way to view the transactions that caused an event detection is from the *Ransomware Event Action Details* screen. Here, you can **press F10** to view the transactions for the user and the time range of the displayed Alert Event.

```
RwEVENTR                                     SafeNet Ransomware                               10/09/25
                                     Ransomware Event Actions                               16:28:32

Event--> Possible Ransomware Event Detected   Event#--> 109

Date--> 2025-10-09-16.10.53.704040
Action-> *RWALERT  CLEWIST  *ALERT
Server-> *FILESRV

Threshold Exceeded for *FILESRV *RENAMES
The event count was 3 during the time range of 2025-10-09-16.00.53.350382 -thru- 2025-10-09-16.10.53.397821
The events were performed by user CLEWIST

F1=Help      F3=Exit      F10=View Event Transactions      F12=Return
```

Press F10 to display all of the transactions leading up to the Event Alert.

```
MPADEV    PCTRAND    SafeNet/i    v12    10/09/25    16:28:32
                                     Network On-Line Transaction Review

User..: CLEWIST                                     From Date.: 10/09/2025 (MMDDYYYY)
Server: *FILESRV                                     To Date...: 10/09/2025 (MMDDYYYY)
Status: _ (A=Accepted, R=Rejected, Blank=All) Start Time: 160053 (HHMMSS)
Order..: A (A=Ascending, D=Descending)
Type option, press Enter.
1-Details
Sel Stat User      Format      Server      Date      Time      IP Address
- Accept CLEWIST    PWFS0200    *FILESRV    10/09/25  16.10.19.032  10.242.2.2
- Accept CLEWIST    PWFS0200    *FILESRV    10/09/25  16.10.21.111  10.242.2.2
- Accept CLEWIST    PWFS0200    *FILESRV    10/09/25  16.10.30.315  10.242.2.2
- Accept CLEWIST    PWFS0200    *FILESRV    10/09/25  16.10.30.863  10.242.2.2
- Accept CLEWIST    PWFS0200    *FILESRV    10/09/25  16.10.31.204  10.242.2.2
- Accept CLEWIST    PWFS0200    *FILESRV    10/09/25  16.10.32.401  10.242.2.2
- Accept CLEWIST    PWFS0200    *FILESRV    10/09/25  16.10.42.286  10.242.2.2
- Accept CLEWIST    PWFS0200    *FILESRV    10/09/25  16.10.42.981  10.242.2.2
- Accept CLEWIST    PWFS0200    *FILESRV    10/09/25  16.10.44.642  10.242.2.2
- Accept CLEWIST    PWFS0200    *FILESRV    10/09/25  16.10.51.808  10.242.2.2
- Accept CLEWIST    PWFS0200    *FILESRV    10/09/25  16.10.52.421  10.242.2.2  +

F1=Help  F3=Exit  F5=Refresh  F12=Cancel  F17=Top  F18=Toggle (Ascend/Descend)
(c) 1997, 2025 MP Assoc., Inc
```

2. Alternatively, from the SafeNet Special Jobs Menu (SN2) use **Option 2 - On-Line Transaction Review** or type the command **PCREVIEW**.

On the *On-Line Transaction Review* screen

- a. Enter the User name
- b. Enter the Server name **FILESRV*
- c. Enter the starting date and time range of the detailed Alert Event.

You then will be shown all the transactions for the user beginning from the date/time entered.

```

MPADEV      PCTRAND      SafeNet/i      v12      10/09/25      16:28:32
Network On-Line Transaction Review
User...: CLEWIST
Server: *FILESRV
Status: _ (A=Accepted, R=Rejected, Blank=All)
Order..: A (A=Ascending, D=Descending)
Type option, press Enter.
1=Details
Sel Stat User      Format      Server      Date      Time      IP Address
- Accept CLEWIST    PWFS0200    *FILESRV    10/09/25    16.10.19.032 10.242.2.2
- Accept CLEWIST    PWFS0200    *FILESRV    10/09/25    16.10.21.111 10.242.2.2
- Accept CLEWIST    PWFS0200    *FILESRV    10/09/25    16.10.30.315 10.242.2.2
  
```

Use *Option 1* to see the details of the transactions

```

PCTESTR      SafeNet/i      v12      10/09/25
MPADEV      On-Line Transaction Review Mode      16:28:32
      Actual Status At Time Of Request

Requested Security Level to Check --> H Historical Review
Current Server Security Setting-----> 1 No Checking Performed
Max. Security Level For this Server-> 4 Object Level Checking
Return Information:
Status ---> Accepted
User--> CLEWIST
Job-> QZLSFILE      Date/Time--> 10/09/25 16.10.31.204
Source IP Address--> 10.242.2.2
Server--> *FILESRV Integrated File/Folder Server-200 Long Path
Format--> PWFS0200 File or Folder system request-200
Details-----: /home/clewis/attr.txt
File Server Request-> 06 Rename Request -Obj Mngmt

Renamed: /home/clewis/attr1.txt

F3=Exit      Pageup/Pagedown
F12=Return
(c)1997,2025 MP Assoc., Inc
  
```

The transaction shown is a sample of a RENAME operation. There were several RENAME operations performed that caused the Event Detection. You can continue through the list of transactions as needed.

Printing the transactions that caused the event detection:

You can also print the SafeNet Security Report to get the details of the transactions leading up to the Ransomware Detection Event.

1. Using the Ransomware Event Action log, display the Event Action details and record the beginning date and time of the Alert Event and the user name that is shown.

```
SafeNet Ransomware
Ransomware Event Actions
10/14/25
15:14:36

Event--> Possible Ransomware Event Detected  Events--> 109

Date--> 2025-10-09-16.10.53.704040
Action--> *RMALERT CLEWIST *ALERT
Server--> *FILESRV

Threshold Exceeded for *FILESRV *RENAMES
The event count was 3 during the time range of 2025-10-09-16.00.53.350382 -thru- 2025-10-09-16.10.53.397821
The events were performed by user CLEWIST

F1=Help      F3=Exit      F10=View Event Transactions      F12=Return
```

2. On a command line, enter the command **PRTSECRPT** and press **F4**, or type **GO SN2** and select menu **Option 2 to Print Transaction Security Report**. You will be presented a list of options for the report.

```
Print Security Report (PRTSECRPT)

Type choices, press Enter.

Only print rejections . . . . . N          Y, N
Select Servers . . . . . *SELECT          *ALL, *DEFAULT, *SELECT
Sort Type . . . . . *USRDAT              *USRDAT, *USRSRV, *SRVUSR
Security Level Check . . . . . H          H, C, F
Selection From Date . . . . . 10092025     Date, *BEGIN,
      From Time . . . . . 160053          Time, *BEGIN,
Selection To Date . . . . . *END           Date, *END,
      To Time . . . . . *END             Time, *END,
User(s) or Group to Select . . . CLEWIST   Name
      + for more values
```

Fill in the paramters as follows:

- Only Print Rejections - **N**
- Select Servers - ***SELECT**
- Enter start date and time you recorded from the Alert Event details screen
- Enter an ending date and time you recorded
- Enter the user profile you recorded

ENTER

On the next screen use *Option 1* to select *File Server* and **ENTER**

```

TRAP04R                               SafeNet/i   v12                               10/14/25
MPADEV                                Select Servers for Security Report          15:22:29

Type choice, press Enter
1=Select

Opt.      Server Text Description                               Server ID   Format
-          *SPECIAL Safenet Audit Transactions                  *DDM        COMMAND
-          Distributed Data Management                          *DDM        *DDM
-          DRDA DB2 Database Access Rqst                        *DRDA       *DRDA
-          Original Data Queue Server                           *DQSRV      DTAQ0100
-          Original License Mgmt Server                         *LMSRV      LICM0100
-          Original Message Server                             *MSGFCL     MESS0100
-          Network Print Server - entry                         QNPSEVR    ENTR0100
-          Network Print Server - spool file                    QNPSEVR    SPLF0100
1        File Server                                           *FILESRV    PWFS0200
-          Original Remote SQL Server                           *RQSRV      RSQL0100
-          Exit point for APIs that accept socket connections  *TCPACCEPT  ACPT0100
-          Spooled file security exit point                     *SPLAUT     SPSY0200
                                                More...

                                Add/Remove The 1 To Select/Deselect
F1=Help                                F12=Cancel          (c)1997,2025 MP Assoc., Inc

```

Press **F10** to submit the Security Report to batch

```

TRAP04R                               SafeNet/i   v12                               10/14/25
MPADEV                                Select Servers for Security Report          15:25:01

Type choice, press Enter
1=Select

Opt.      Server Text Description                               Server ID   Format
-          *SPECIAL Safenet Audit Transactions                  *DDM        COMMAND
-          Distributed Data Management                          *DDM        *DDM
-          DRDA DB2 Database Access Rqst                        *DRDA       *DRDA
-          Original Data Queue Server                           *DQSRV      DTAQ0100
-          Original License Mgmt Server                         *LMSRV      LICM0100
-          Original Message Server                             *MSGFCL     MESS0100
-          Network Print Server - entry                         QNPSEVR    ENTR0100
-          Network Print Server - spool file                    QNPSEVR    SPLF0100
1        File Server                                           *FILESRV    PWFS0200
-          Original Remote SQL Server                           *RQSRV      RSQL0100
-          Exit point for APIs that accept socket connections  *TCPACCEPT  ACPT0100
-          Spooled file security exit point                     *SPLAUT     SPSY0200
                                                More...

                                Add/Remove The 1 To Select/Deselect
F1=Help                                F10=Process          F12=Cancel          (c)1997,2025 MP Assoc., Inc

```

The Security Report will be spooled to your output queue. It will produce a detailed report of all the transactions for the user during the event timeframe.

Below, you can see the first of the RENAME requests. The additional pages will show the remaining RENAME requests.

Display Spooled File									
File	TRAP05RL							Page/Line	1/2
Control								Columns	1 - 130
Find									
*...+...1...+...2...+...3...+...4...+...5...+...6...+...7...+...8...+...9...+...0...+...1...+...2...+...3									
Start Time	Start Date	Ending Date	System	Historical Transaction Review Report	User ID	Report	RUN DATE	PAGE	
16:00:53	10/09/2025	10/14/2025	MPADEV	*** Security Report by User ***	CLEWIST	TRAP05RS	10/14/25	1	
USER - CLEWIST Cheryl Lewis - Kisco Support - Testing									
File Server	Server		Srv Tst	Request	Function	Request		Reques	Status
	Description		Sts Lvl	Date	Time	ID			
File Server	IP Address: 10.242.2.2	200	1 -	10/09/2025	16:10:19	*FILESRV	/home		Accept
File Server		200	1 -	10/09/2025	16:10:21	*FILESRV	/home/clewis	For READ	Accept
File Server		200	1 -	10/09/2025	16:10:30	*FILESRV	/	For READ	Accept
File Server		200	1 -	10/09/2025	16:10:30	*FILESRV	/home	For READ	Accept
File Server		200	1 -	10/09/2025	16:10:31	*FILESRV	/home/clewis/attr.txt	For READ	Accept
File Server		200	1 -	10/09/2025	16:10:32	*FILESRV	RENAME REQUEST	-Obj Mgmt	Accept
File Server		200	1 -	10/09/2025	16:10:42	*FILESRV	/home/clewis	For READ	Accept
File Server		200	1 -	10/09/2025	16:10:42	*FILESRV	/	For READ	Accept
F3=Exit F12=Cancel F19=Left F20=Right F24=More keys									

Commands available with the SafeNet/i Ransomware Detection module

CHGSNRW1	CHG Settings for *RENAMES
CHGSNRW2	CHG Settings for *REWRITES
CHGSNRW3	CHG Settings for *MOVES
CHGSNRW4	CHG Settings for *COPIES
CHGSNRW5	CHG Settings for TRIGGERS
CHGSNRW6	CHG Settings for *READS
STRSNRWD	Starts RW Detector Jobs
WRKRWEVT	Work with Event Log Actions
WRKRWPTH	Work with RW Exclusion & Trigger paths
WRKSNRWD	Work with Ransomware Status

Ransomware Detection Job Problem Determination

SafeNet/i Detector Jobs are not starting

- You might not have the correct license type for the product. You must have an **SR license type** to run SafeNet/i Ransomware Detection. Contact Kisco Systems for licensing information.
- You are not a SafeNet Administrator. You must be an administrator for the product to operate correctly.
- Do you have the Detector Job *AutoStart* parameter set to **YES*? See the chapter on setting the Detector Job parameters.
- Did you try reissuing the ENDTRP and STRTRP commands to restart logging and the Detector Jobs?

SafeNet/i Detector Jobs are not reacting to Possible Events

- Check to make sure the SafeNet Logging job is active in the SAFELOGING subsystem. Use the STRTRP command if the job has not been started.
- Lower the *Event Threshold Count*. You might have too high an event count value for the *Look Back Time* value on the detector job setting.
- Increase the *Look Back Time* value. This will pick up more transactions during scanning. However, if the value is too high performance may be affected.

SafeNet/i Detector Jobs are using a lot of system resources

- Increase the *Pattern Recheck Delay* time value. The longer this delay the less system resources are utilized. However, the longer the delay the longer an infection could run before being detected.
- Decrease the *Look Back Time* value. A shorter look back time value will reduce the processing overhead. However, a shorter look back time period will also reduce the number of potential ransomware actions that are counted towards the threshold count.

I am not receiving the Ransomware Alerts

- The alerts are dependent on the *Alert Notification* setup in SafeNet/i. Check **Alert Notification Settings** on the SafeNet Main Menu and make sure the ALERTWATCH job is running in the SAFELOGING subsystem.