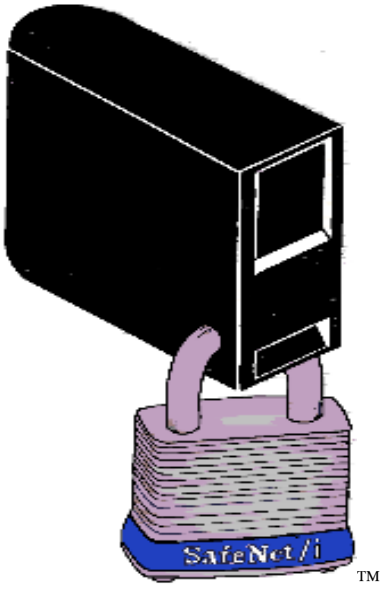
SafeNet/i

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

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.

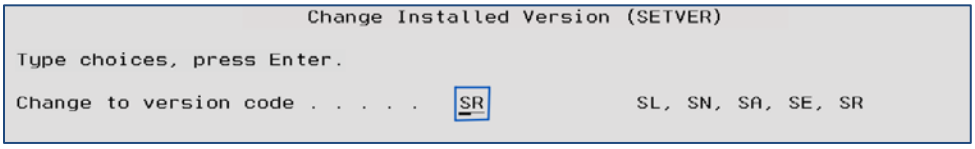
A separate license is required to use this feature.

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 O**ption 5**.

   GO PCSECLIB/INSTALL

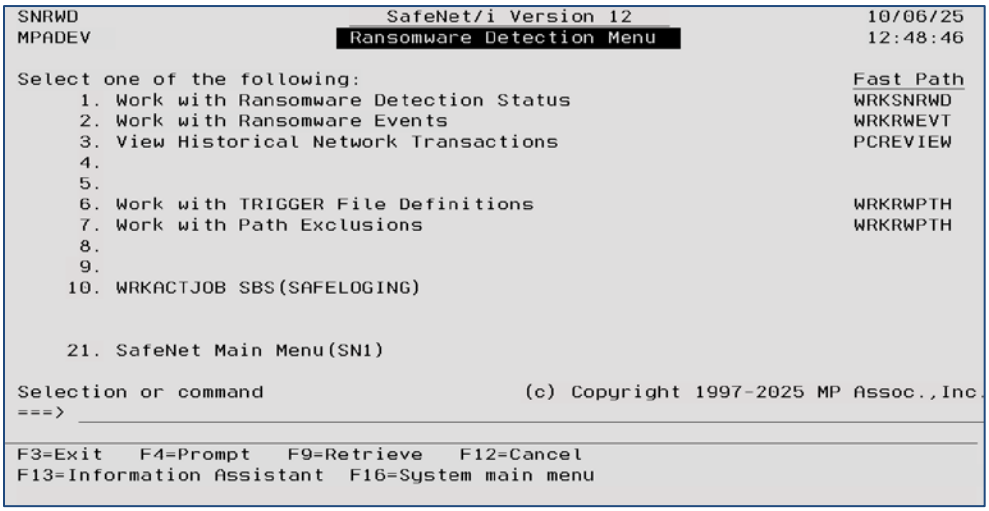
   If you are not at V12 or above, you will need to upgrade to V12 before you can access the SafeNet/i Ransomware Detection Module.

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:



   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.

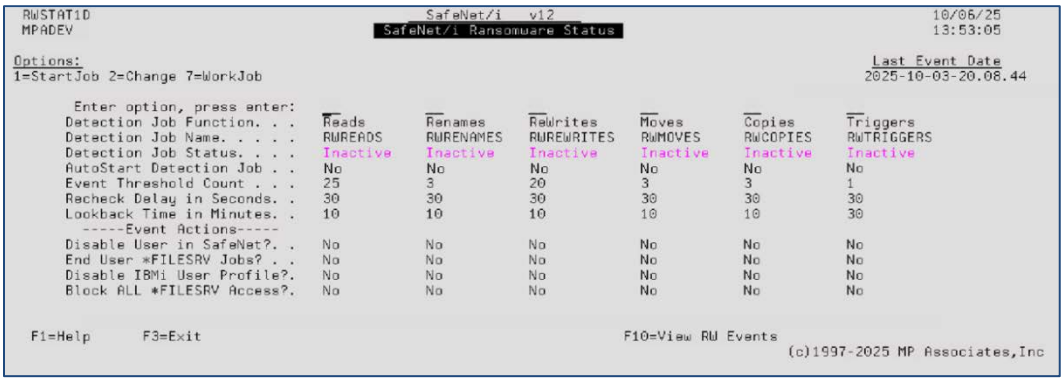
Before you turn on Ransomware Controls, you will want to let it run without taking any actions. This will give you the opportunity to analyze your network traffic prior to allowing Ransomware to change or terminate user activity.

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*.

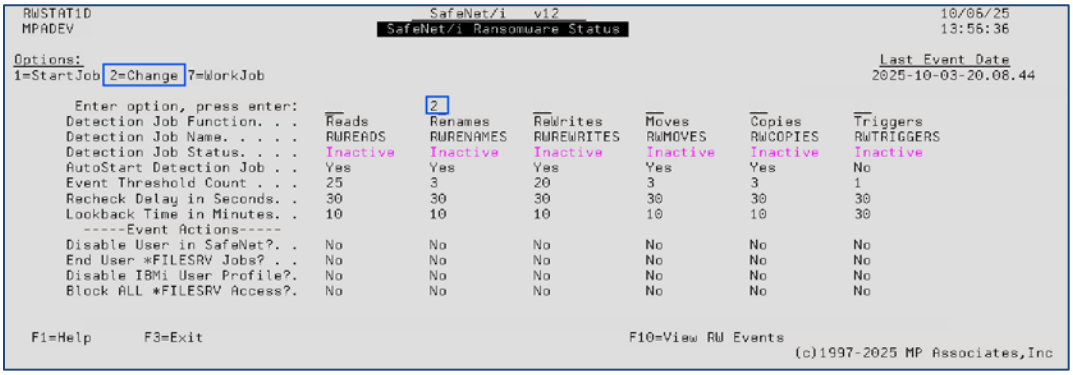


The six RW Detection Jobs are listed across the top of the screen, and their descriptions are as follows:

- **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.



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.

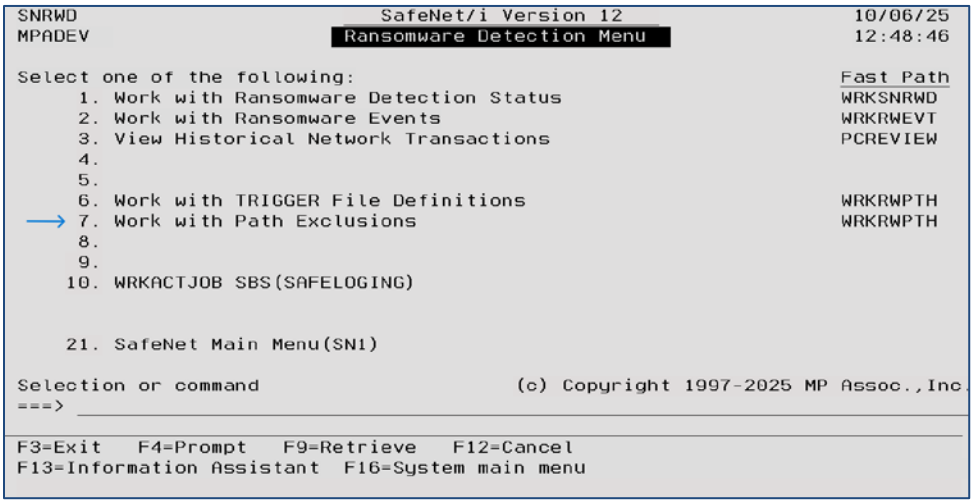
When initially starting to use Ransomware Detection you should leave ALL these Event Actions to **NO** until you are sure your normal daily processing does not generate false positives.

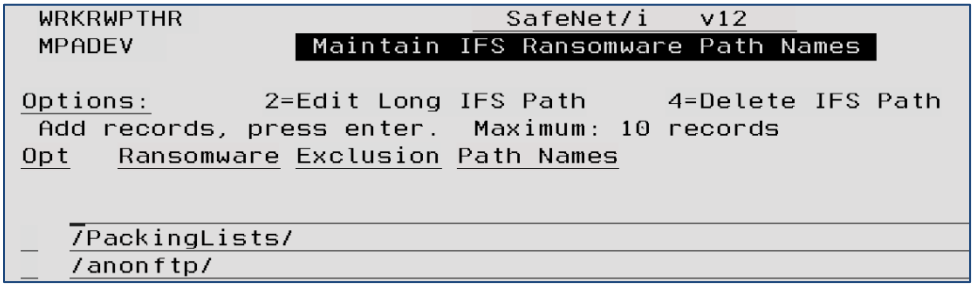
Special Setup Considerations

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.

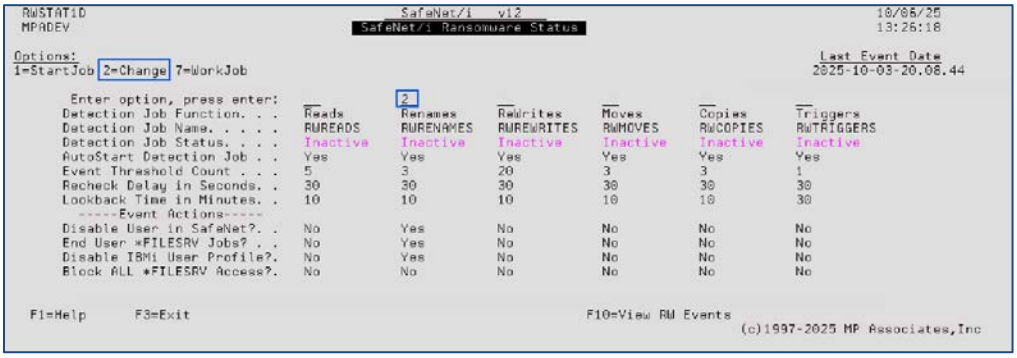




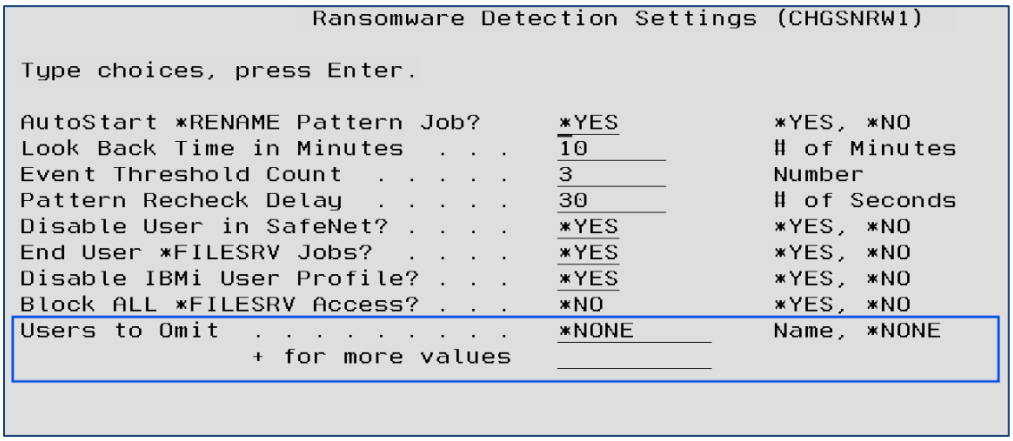
Excluding Users from Ransomware scanning:

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.

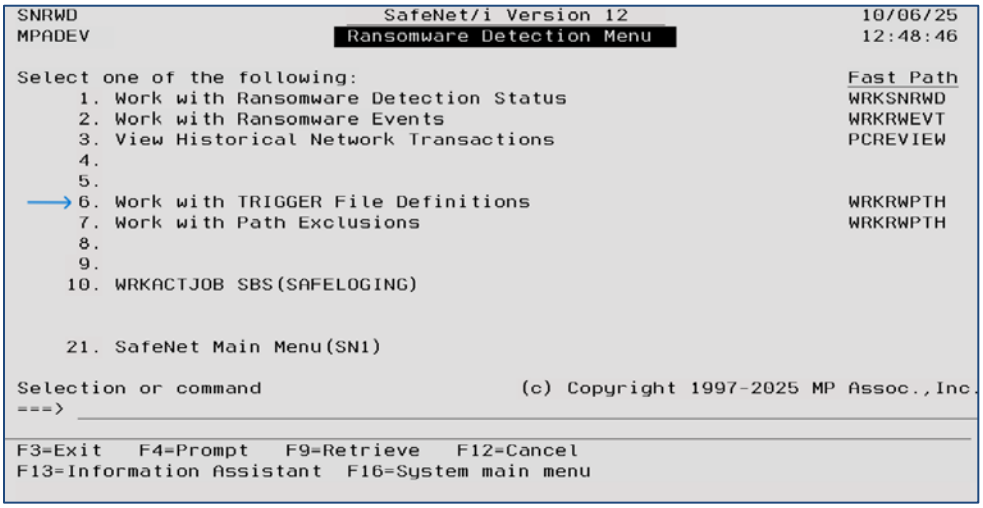


Each of the detection jobs allows for omitting certain users from triggering a Ransomware Event. You can enter up to 10 users to omit.

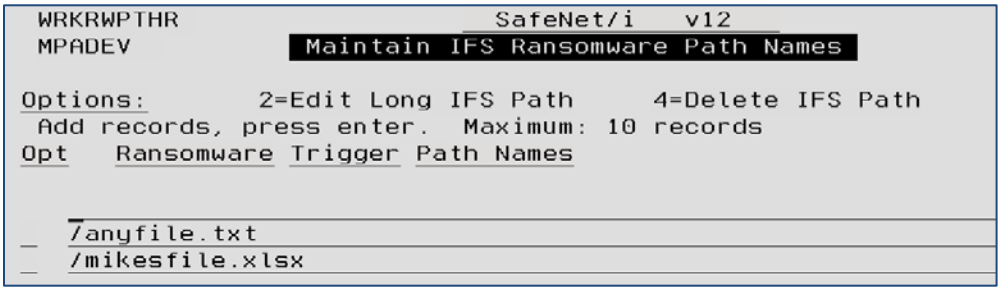


Configuring a Trigger file

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



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.



Starting Ransomware Jobs

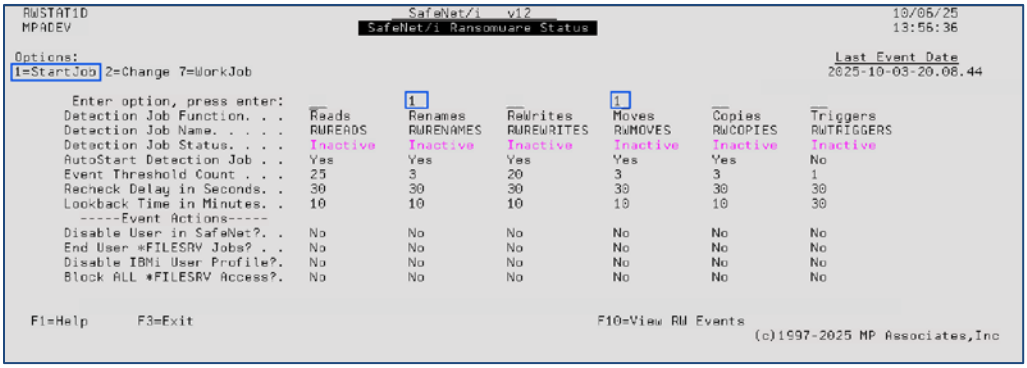
After making the following changes to *AutoStart* values, remember to use the normal SafeNet/i **STRTRP** and **ENDTRP** commands to start and stop the jobs along with the regular SafeNet Logging job in subsystem *SAFELOGING*.

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

1. Manually

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

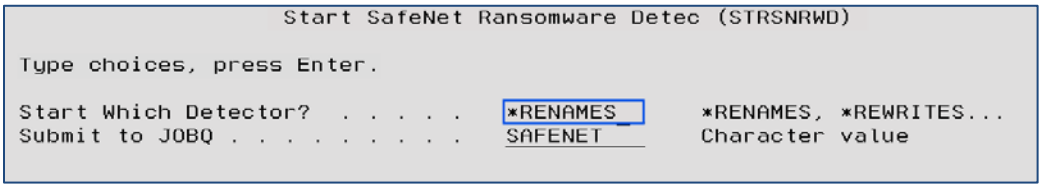
On the Ransomware Status screen type a **1** (*StartJob*) above each job to start



OR

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

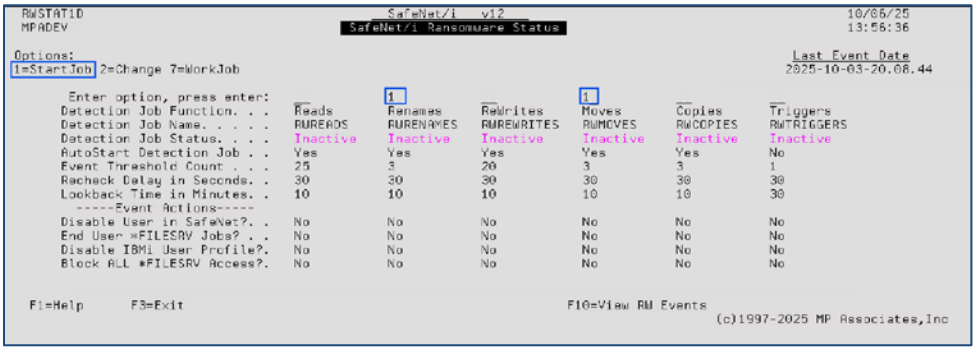
Enter the name of the job you want to start and press enter.



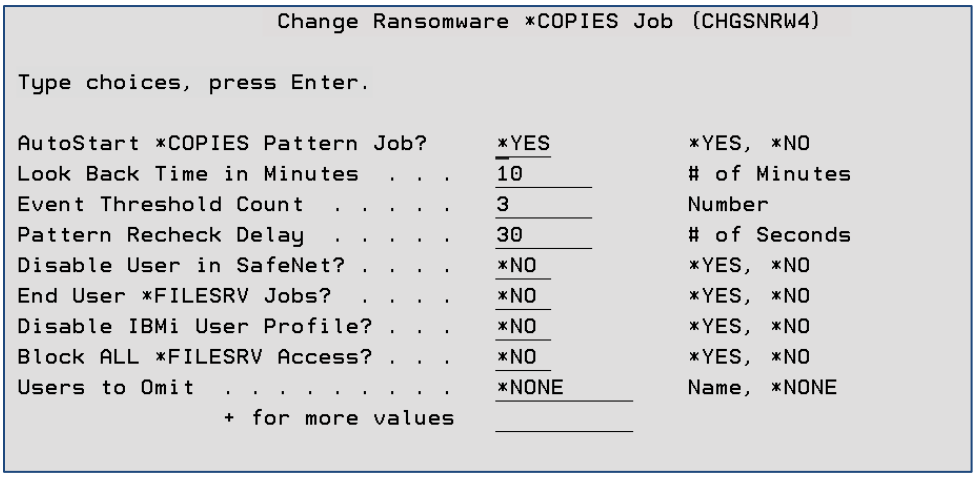
2. Automatically

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

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



Change *AutoStart xxx Job* to **YES*



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

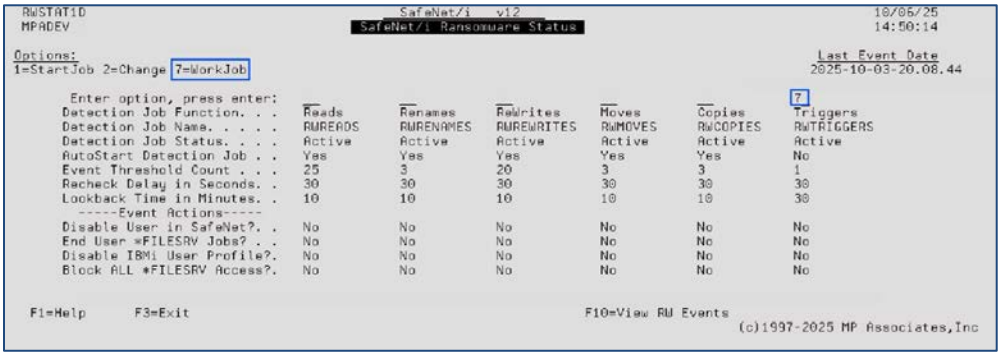
Ending Ransomware Jobs

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**

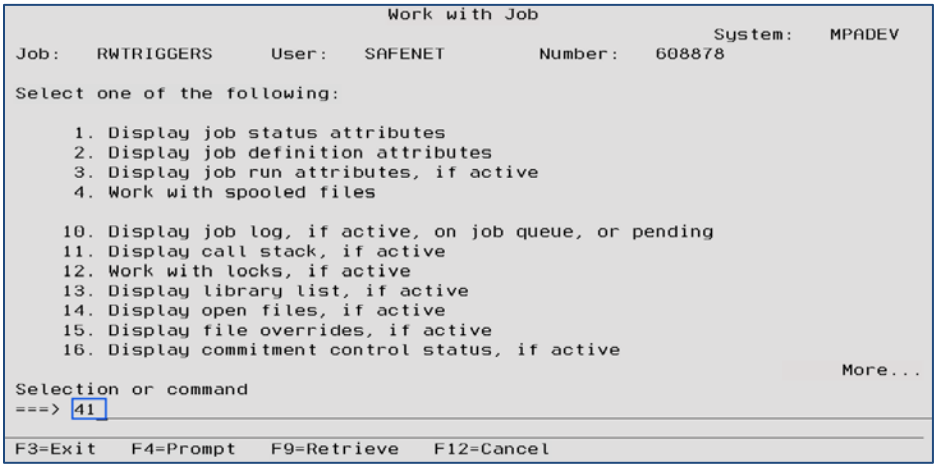
Option 7 (WorkJob) allows you to work with each job individually.

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



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

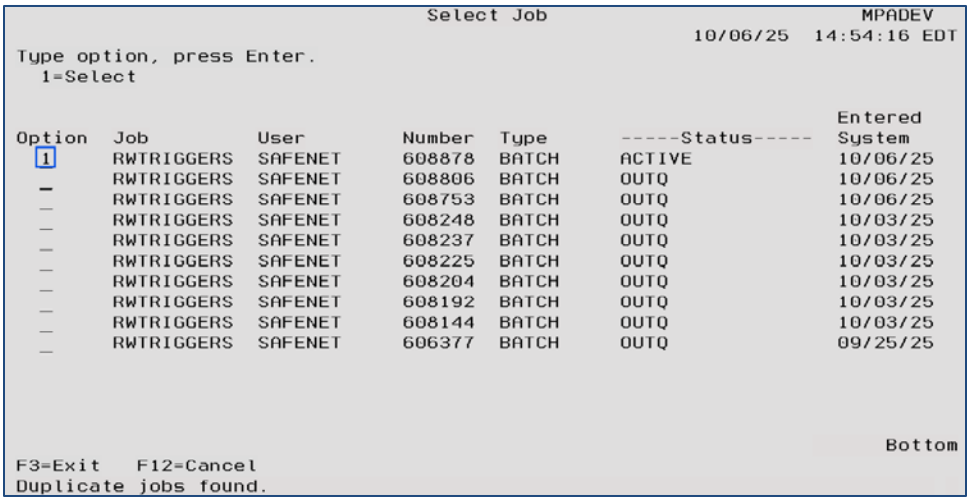
If there is only one job running on your system, you will see the IBM i OS *Work with Job* display.



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.

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



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

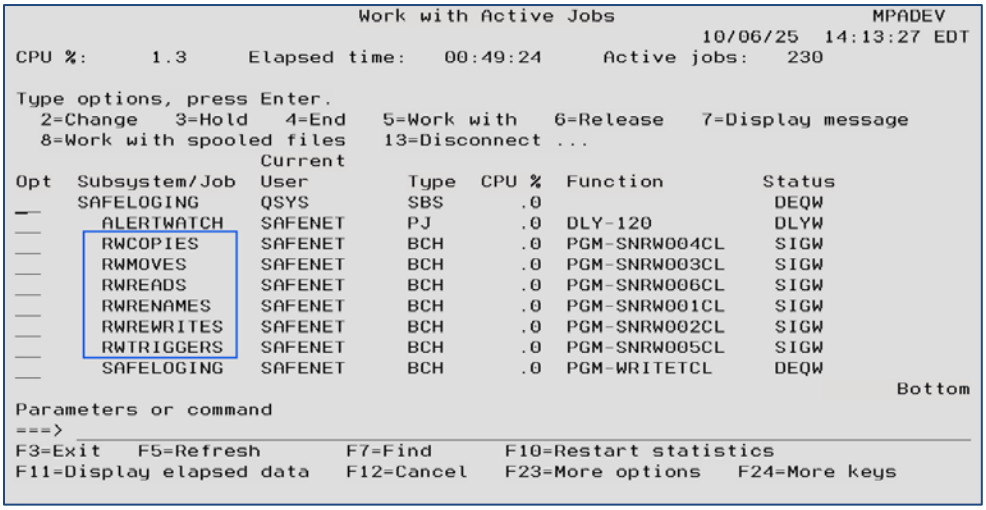
If you use the SafeNet/i ENDTRP command, then ALL the Ransomware Detection jobs will end, along with normal SafeNet/i logging.

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.



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.

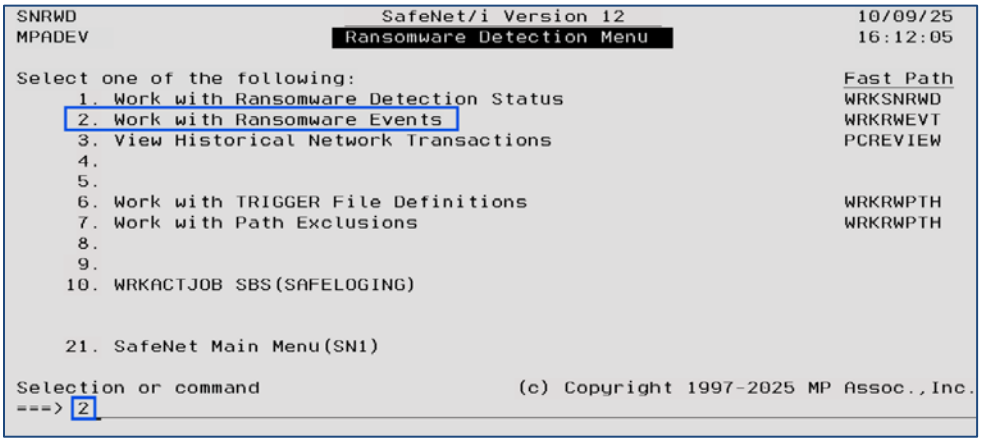
   Alert email sample:

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

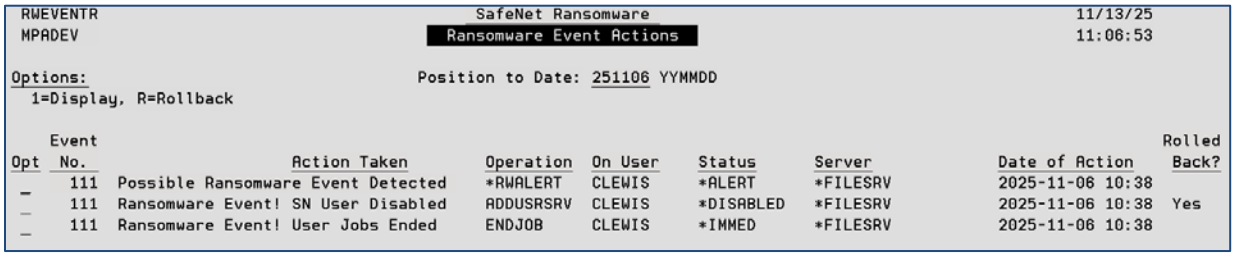
   Details:

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



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

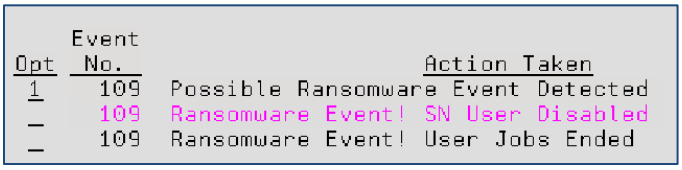


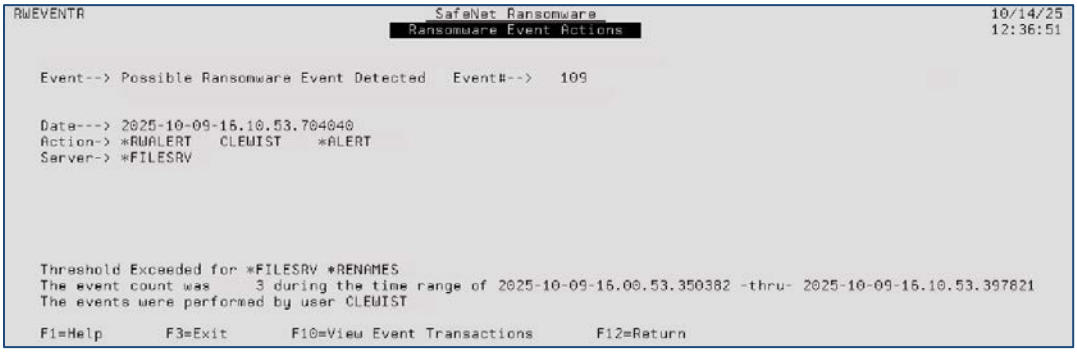
Shown above is a list of Event Actions

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.

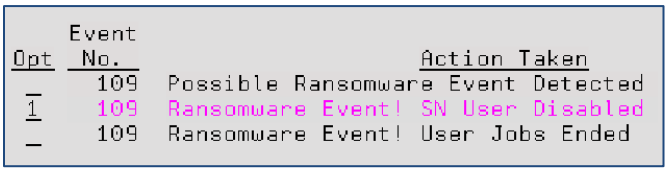


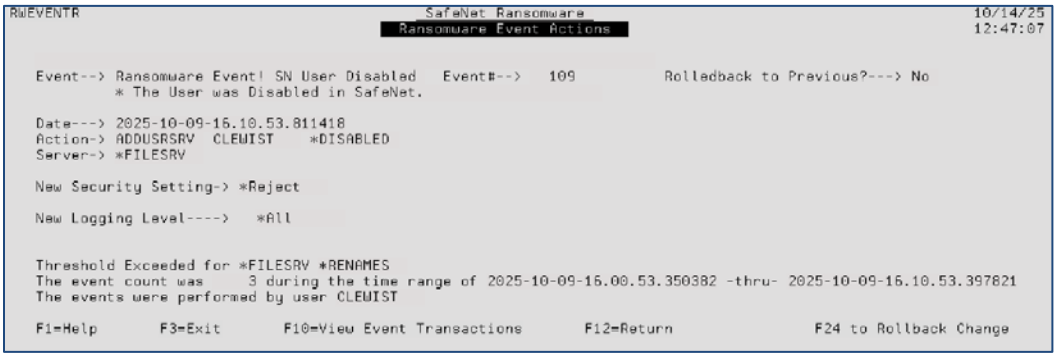


Shown are the details of the first event

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.

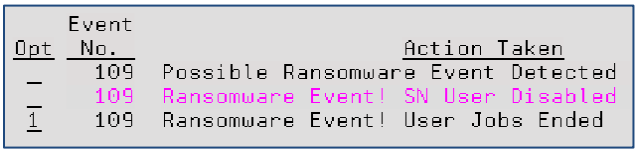


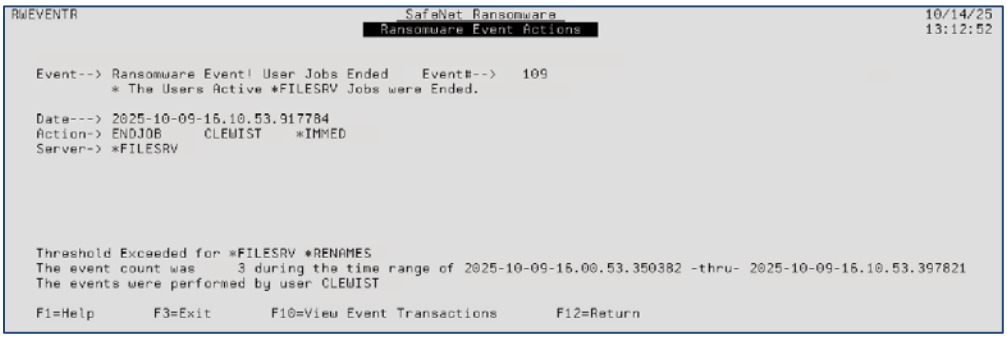


Shown are the details of the second Event and Action:

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.





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

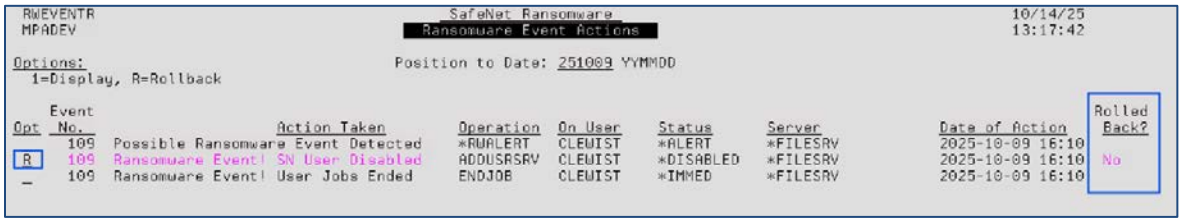
1. User was disabled in SafeNet
   This indicates a REJECT entry added to the Server Control file for the user in SafeNet for the **FILESRV* exit point. Use command WRKUSRSRV.

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

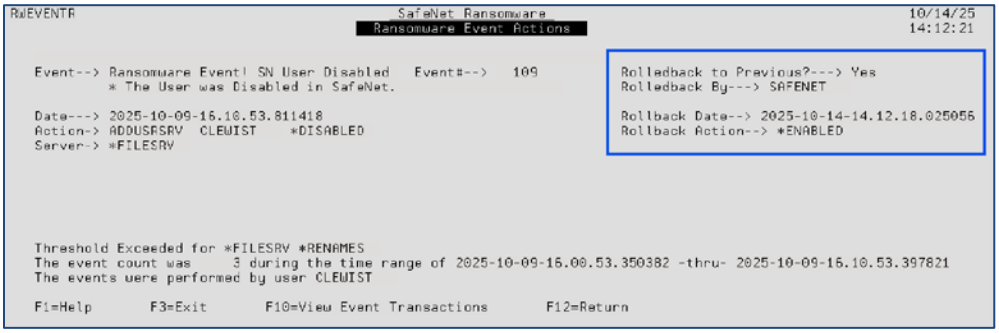
When viewing an Event from the Event Log display and you see a *NO* value in the right column under Rolledback then it is possible to reverse or rollback the changes made due to the event.



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*.

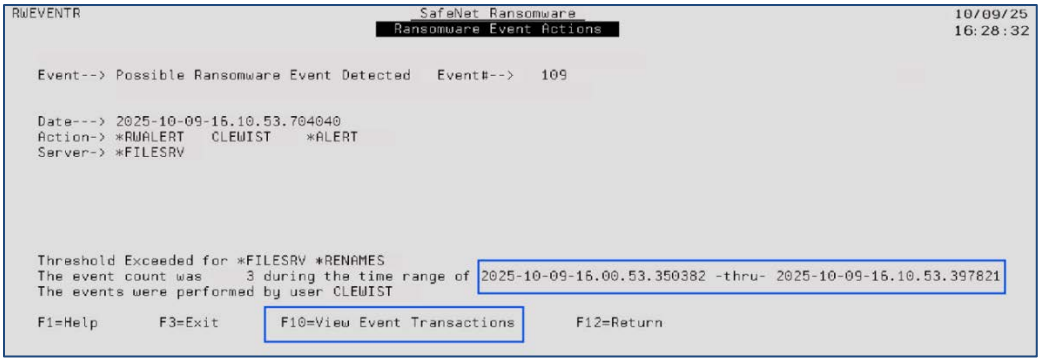


Chapter 6 – Finding the Transactions

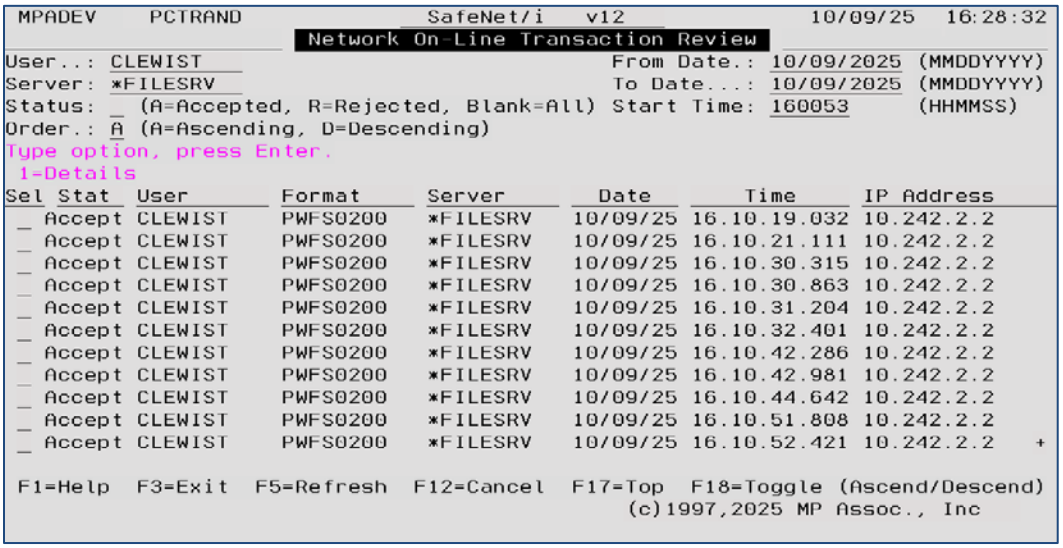
When a Ransomware Event is detected, you may want to review all the transactions that caused the event. You can view the events using the SafeNet *On-Line Transaction Review* screen (*PCREVIEW)* or by running a SafeNet security report.

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.



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

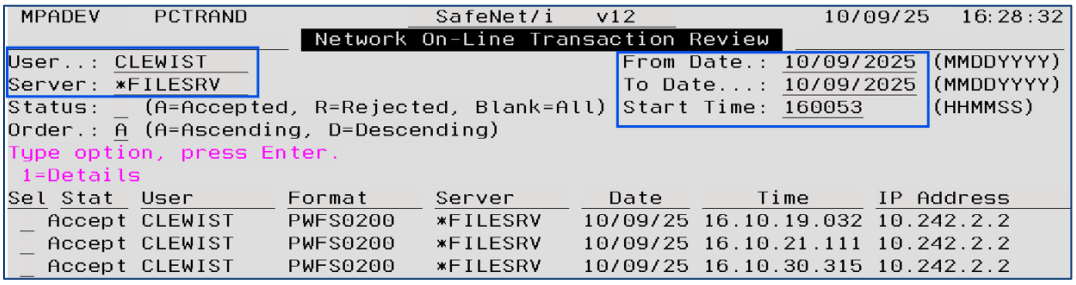


2. Alternatively, from the SafeNet Special Jobs Menu (SN2) use **Option 2 - On-Line Transaction Review** or type the command **PCREVIEW**.

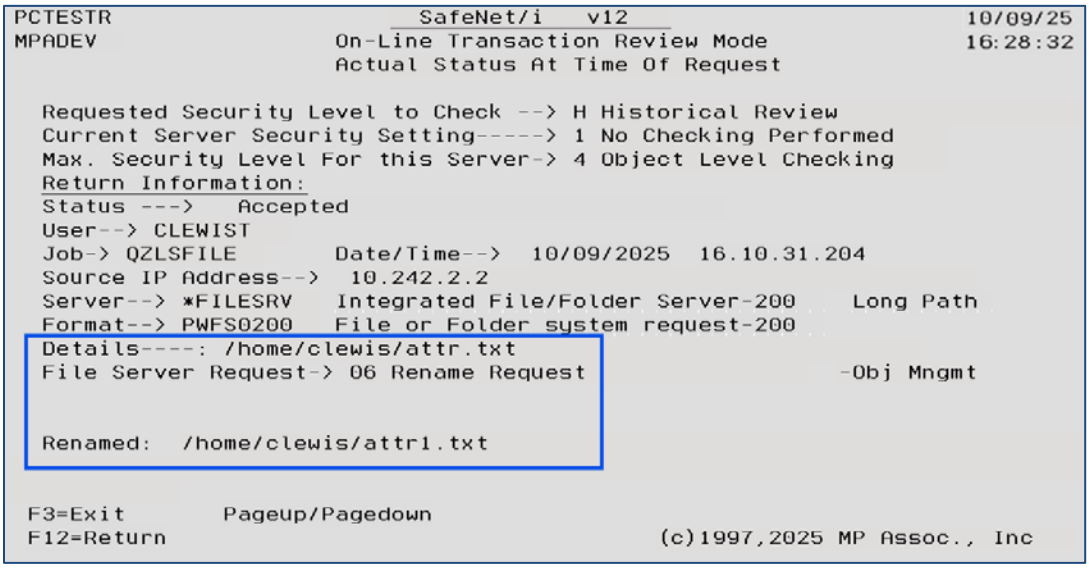
   On the *On-Line Transaction Review* screen

   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.



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

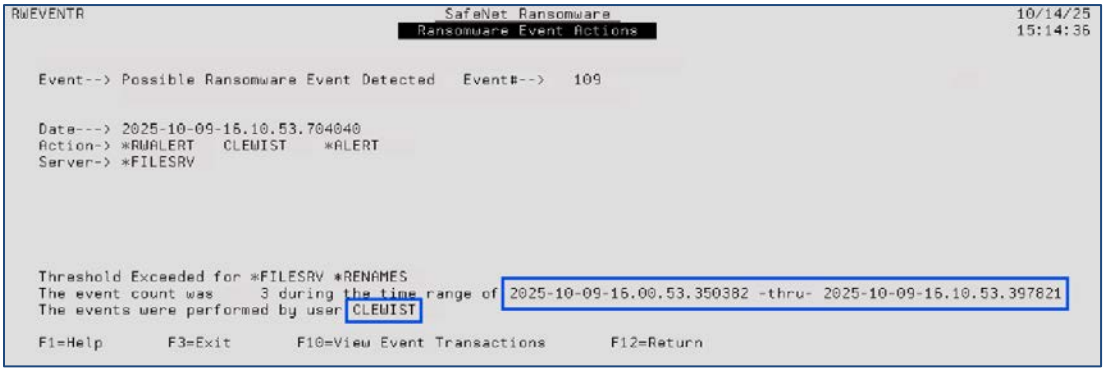


   The transaction shown is a sample of a RENAME operation. There were several RENAME operations performed that caused the Event Detection. You can continue through the list of transactions as needed.

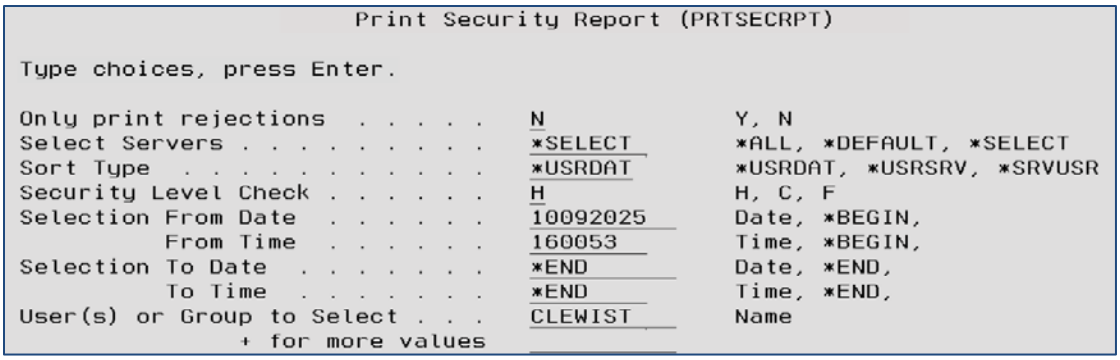
Printing the transactions that caused the event detection:

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.



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.

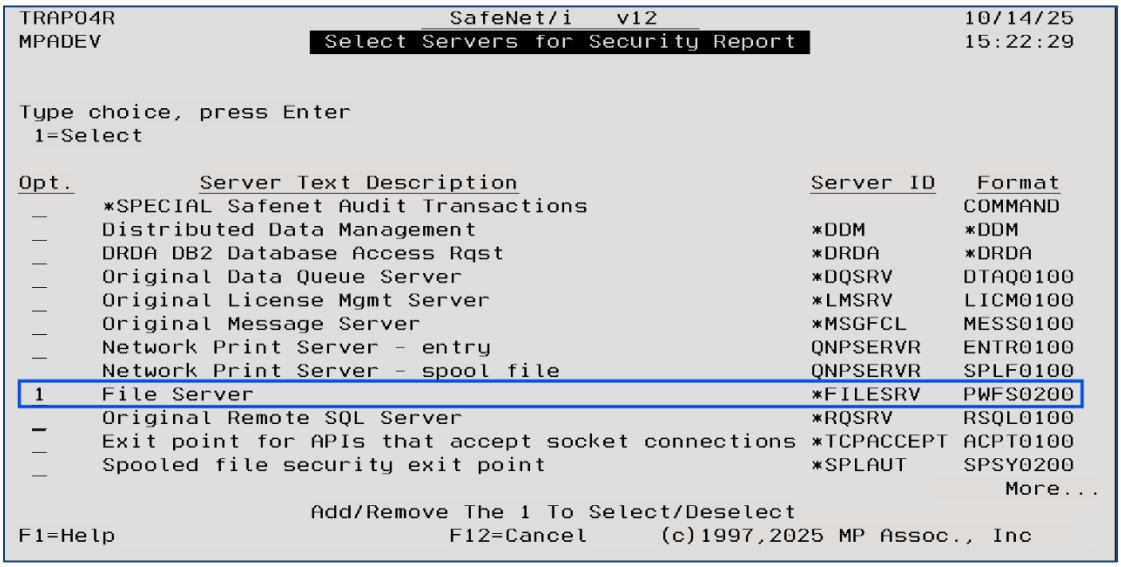


Fill in the paramters as follows:

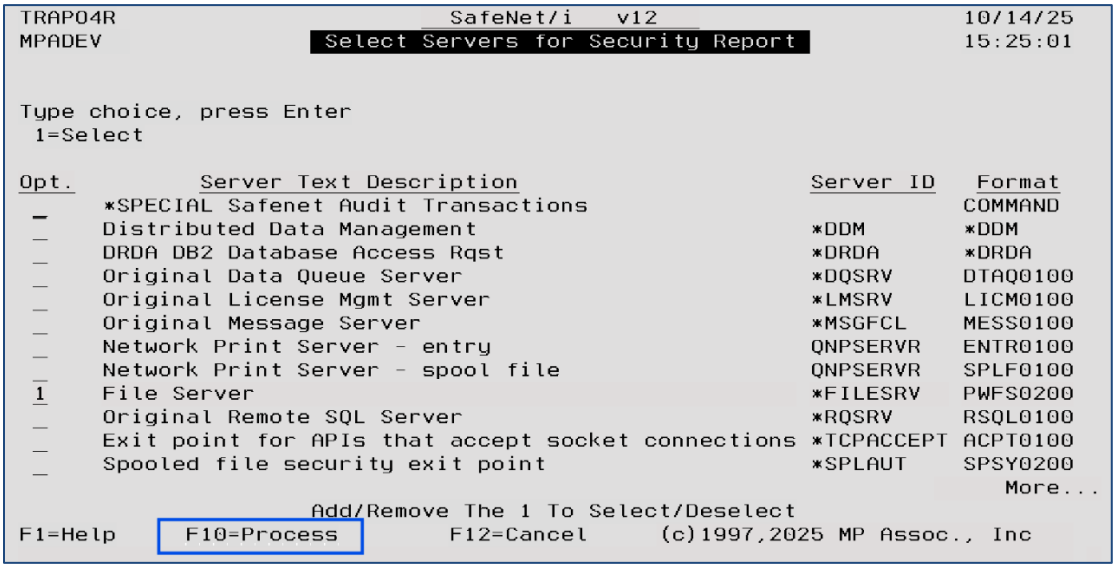
- Only Print Rejections - **N**
- Select Servers - ***SELECT**
- Enter start date and time you recorded from the Alert Event details screen
- Enter an ending date and time you recorded
- Enter the user profile you recorded

ENTER

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

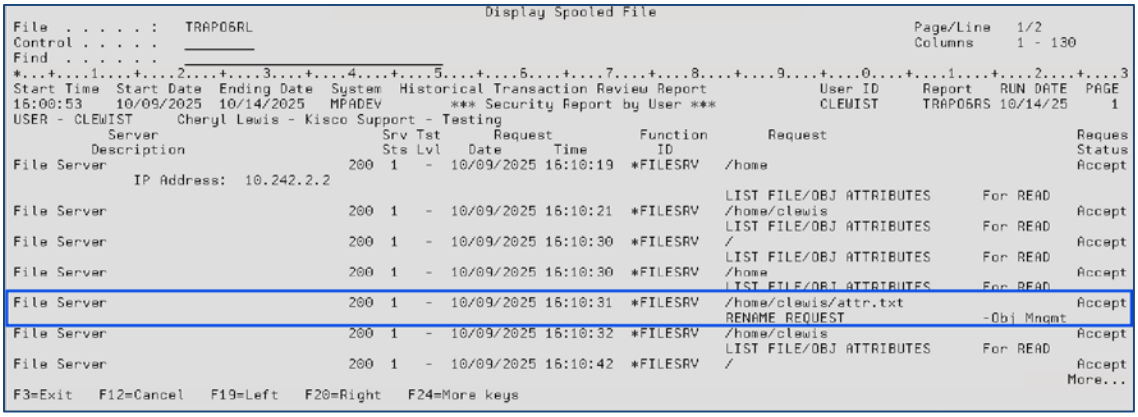


Press F10 to submit the Security Report to batch



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 . . . . . :   TRAP06RL                                                    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     TRAP06RS 10/14/25    1
USER - CLEWIST     Cheryl Lewis - Kisco Support - Testing
         Server                          Srv Tst      Request          Function      Request                                Reques
       Description                       Sts Lvl   Date      Time       ID                                                   Status
File Server                          200  1   -  10/09/2025 16:10:19  *FILESRV   /home                                      Accept
            IP Address:  10.242.2.2
                                                                       LIST FILE/OBJ ATTRIBUTES      For READ
File Server                          200  1   -  10/09/2025 16:10:21  *FILESRV   /home/clewis                               Accept
                                                                       LIST FILE/OBJ ATTRIBUTES      For READ
File Server                          200  1   -  10/09/2025 16:10:30  *FILESRV   /                                          Accept
                                                                       LIST FILE/OBJ ATTRIBUTES      For READ
File Server                          200  1   -  10/09/2025 16:10:30  *FILESRV   /home                                      Accept
                                                                       LIST FILE/OBJ ATTRIBUTES      For READ
File Server                          200  1   -  10/09/2025 16:10:31  *FILESRV   /home/clewis/attr.txt                      Accept
                                                                       RENAME REQUEST                -Obj Mngmt
File Server                          200  1   -  10/09/2025 16:10:32  *FILESRV   /home/clewis                               Accept
                                                                       LIST FILE/OBJ ATTRIBUTES      For READ
File Server                          200  1   -  10/09/2025 16:10:42  *FILESRV   /                                          Accept
                                                                                                                             More...
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.