SafeNet/i

IBM QRadar® SIEM and QRadar Log Manager

MP Associates of Westchester, Inc.

08/20/2020
PTF 11.10

Table of Contents

Function Overview

SafeNet/i is introducing new features in this product update.

1. Integration with ***IBM*** QRadar SIEM and QRadar Log Manager

   Administrators can now configure SafeNet/i to integrate with IBM's QRADAR family of products.

   SafeNet/i can send alerts via the required LEFF compliant log file format and store that log file in the system IFS for FTP pickup and processing by the QRADAR Network Anomaly Detection Monitor software.

   New for SafeNet/i V11: A full payload output file can now be created. You can now configure SafeNet/i to send ALL the collected transactions to QRADAR. See command STRSNRADAR.

Prerequisites

1. IBM i OS V7R2 or later is required.
2. SafeNet/i minimum of V11.10 must be installed. See our support website for PTF level required. (PTF11.10)
3. Alert Notifications must be configured and active in SafeNet/i. (In V11 this is NOT required for ALL transactions in the payload file build)
4. IBM's QRADAR software must be installed on a separate system.

Integration Process Overview

Listed below are the general setup steps for integration with QRadar.

You must have a SafeNet/i minimum PTF Version 11.10 for this function to operate.

1. On IBM i, create an IFS Directory to hold the SafeNet/i QRadar alert files.
   Example: /SafeNet/QRadar

2. Setup an IBM i User Profile that QRadar will use to pick up the alert files by FTP or SFTP.
   Example: QRADARUSER

3. Setup the same user in SafeNet/i, allowing FTP access to the directory created above.

    a. User must have authority to the FTPLogon and FTPServer points.
    b. User must have authority to LIST and GET FTP Sub commands.
    c. User must have READ authority to the IFS Path created for the QRADAR alert files.

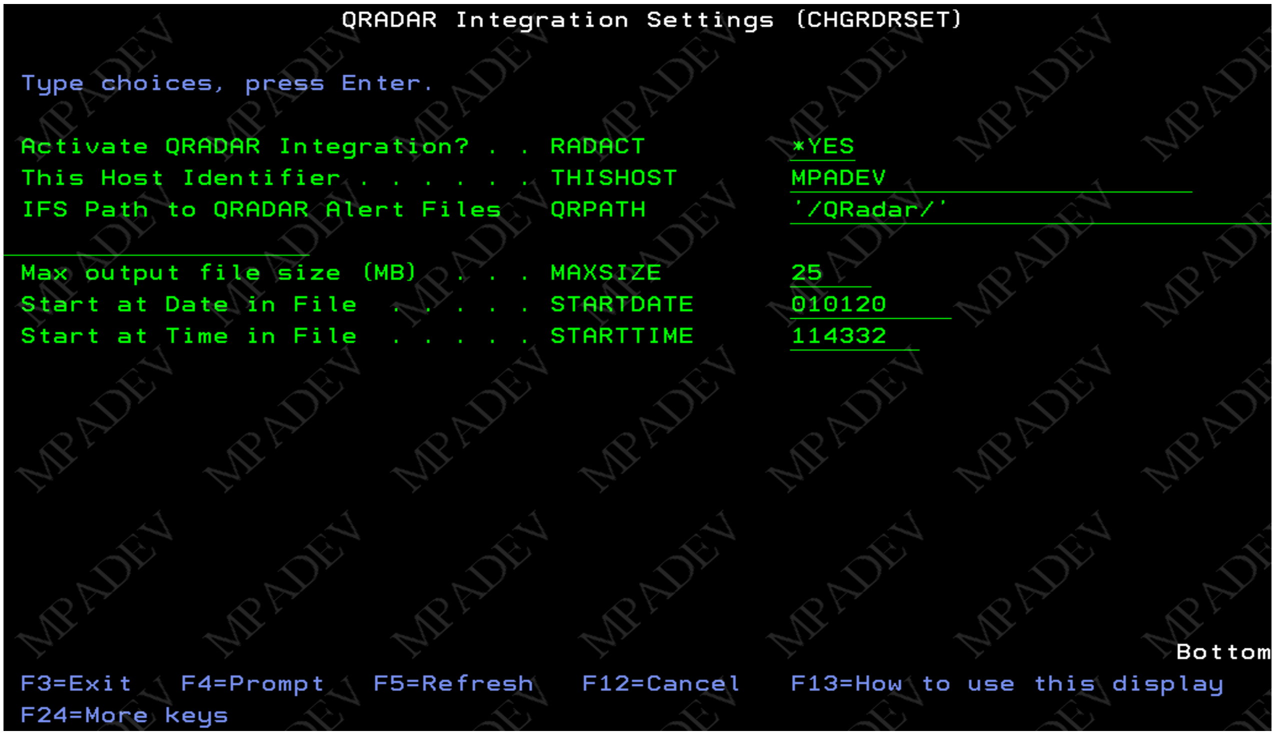
4. Using the SafeNet/i CHGRDRSET command, verify or enter the following:
    a. THISHOST: Enter a Host name or identifier for this IBM i. This is for QRadar identification.
    b. QRPATH: Path to directory created above used for output file creation. Must be in the format of '/path1/path2/'
    c. MAXSIZE: If you intend to send ALL transactions, set the Maximum Output file size. 25MB = approximately 100,000 transactions to a file.
    d. STARTDATE/STARTTIME: If this is the first time you are using this function, set a starting date and starting time. These values are used to determine where in your transaction file (TRAPOD) you want to start the full payload build point. These values will update as the files are output. It represents the "last" record processed and is a starting point for new payload file builds.

5. Setup Alert Notifications in SafeNet/i with the CHGNOTIFY command. You must use Summarized Alerts. (Not required if doing a full payload file builds only)

6. Configure the QRadar software for your SafeNet/i system as a Log Source:
    a. Define a log source for this IBM i (see details below)
    b. Test alert generation and file pickup by QRadar

7. The alert files created in the IFS directory will be named "SN_QRAD_xxxx.txt" where xxxx = a number

CHGRDRSET Command Example

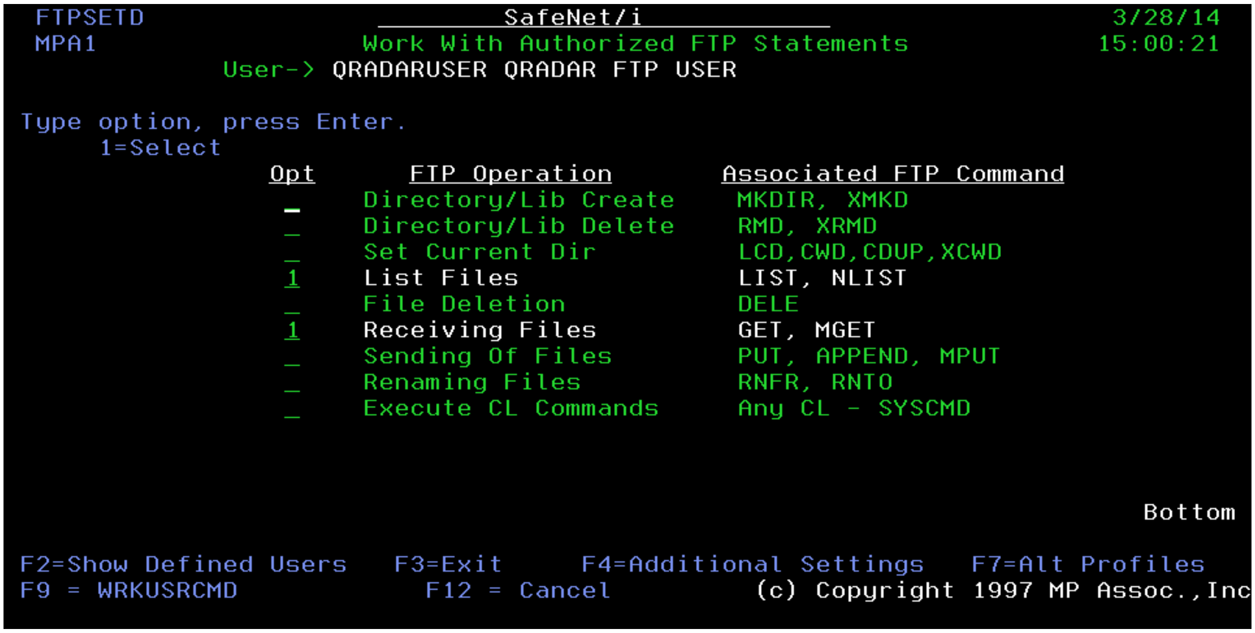


```
                     QRADAR Integration Settings (CHGRDRSET)

 Type choices, press Enter.

 Activate QRADAR Integration? . . RADACT         *YES
 This Host Identifier . . . . . . THISHOST       MPADEV
 IFS Path to QRADAR Alert Files   QRPATH         '/QRadar/'

 Max output file size (MB) . . .  MAXSIZE        25
 Start at Date in File  . . . . . STARTDATE      010120
 Start at Time in File  . . . . . STARTTIME      114332




                                                                         Bottom
 F3=Exit   F4=Prompt   F5=Refresh   F12=Cancel   F13=How to use this display
 F24=More keys
```

Notes:

1. The IFS Path must exist prior to entering it in this command.
2. The Host Name entered here is only for documentation/identification of this host to the QRadar log activity.
3. You must have Alert Notification active in SafeNet/i for rejected transaction QRadar alerts to be generated. This is not required when you want ALL transactions included in the build of the payload file. If you want rejections to IMMEDIATELY be available to QRadar, set this function to RADACT(*YES). Any Batch files built will also include rejected transactions.
4. You can still use the batch full payload build (STRSNRADAR) function even if this is RADACT(*NO)

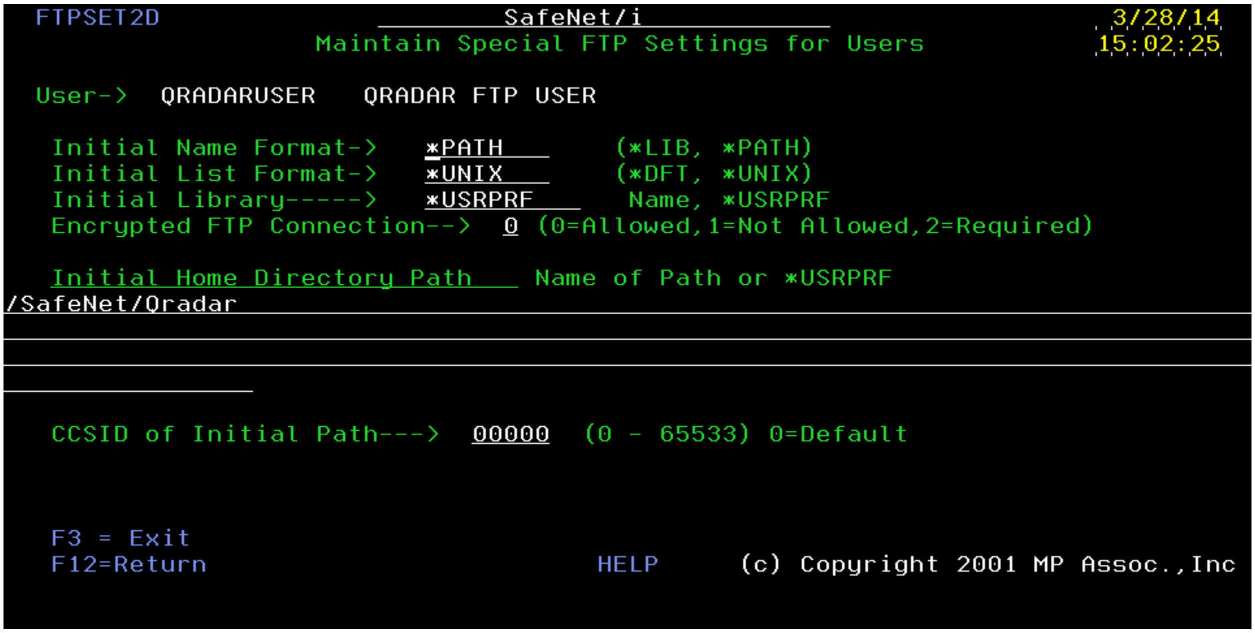
The FTP User from QRadar must have at a minimum LIST and GET authority.



```
 FTPSETD                    SafeNet/i                          3/28/14
 MPA1               Work With Authorized FTP Statements        15:00:21
              User-> QRADARUSER QRADAR FTP USER

Type option, press Enter.
     1=Select
                 Opt     FTP Operation          Associated FTP Command
                  _    Directory/Lib Create      MKDIR, XMKD
                  _    Directory/Lib Delete      RMD, XRMD
                  _    Set Current Dir           LCD,CWD,CDUP,XCWD
                  1    List Files                LIST, NLIST
                  _    File Deletion             DELE
                  1    Receiving Files           GET, MGET
                  _    Sending Of Files          PUT, APPEND, MPUT
                  _    Renaming Files            RNFR, RNTO
                  _    Execute CL Commands       Any CL - SYSCMD



                                                                  Bottom

F2=Show Defined Users   F3=Exit     F4=Additional Settings   F7=Alt Profiles
F9 = WRKUSRCMD            F12 = Cancel         (c) Copyright 1997 MP Assoc.,Inc
```

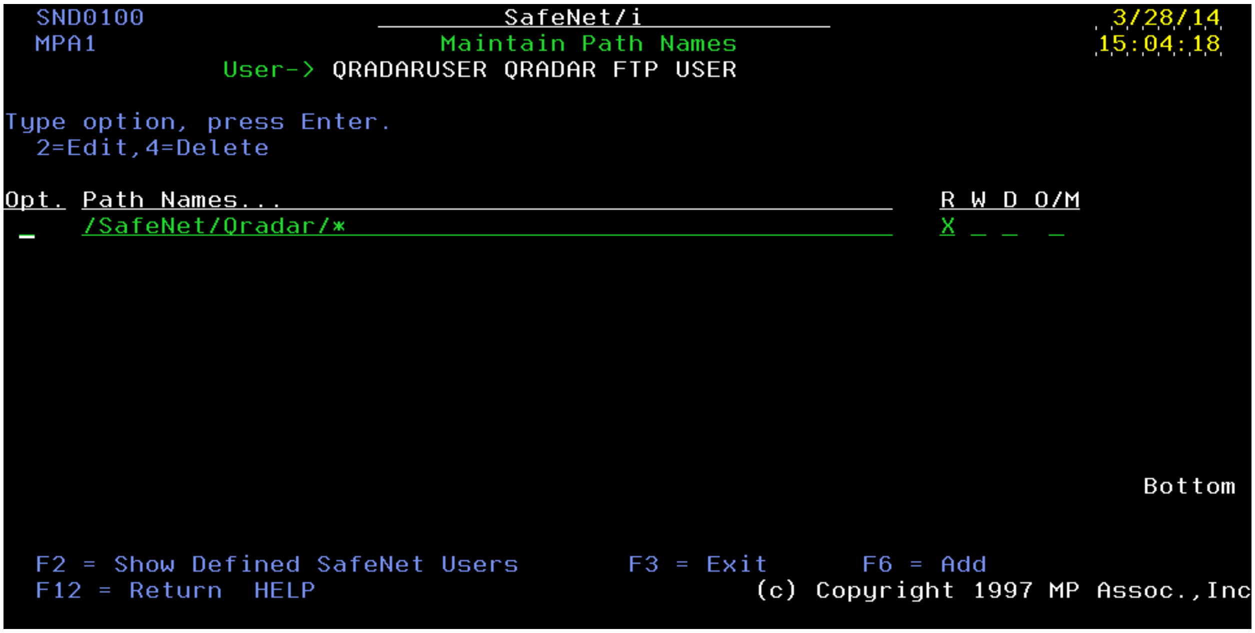
Then, Press F4 for Additional Parameters

Note the Initial Name Format and Home Directory settings:



```
  FTPSET2D                        SafeNet/i                             3/28/14
                       Maintain Special FTP Settings for Users         15:02:25

  User->  QRADARUSER   QRADAR FTP USER

   Initial Name Format->   *PATH       (*LIB, *PATH)
   Initial List Format->   *UNIX       (*DFT, *UNIX)
   Initial Library----->   *USRPRF      Name, *USRPRF
   Encrypted FTP Connection--> 0 (0=Allowed,1=Not Allowed,2=Required)

   Initial Home Directory Path    Name of Path or *USRPRF
/SafeNet/Qradar



   CCSID of Initial Path---> 00000  (0 - 65533) 0=Default



   F3 = Exit
   F12=Return                         HELP     (c) Copyright 2001 MP Assoc.,Inc
```

Finally, Use the WRKUSRPTH command and give the FTP user authority to the IFS path where the QRADAR alerts files will be placed.



```
  SND0100                         SafeNet/i                             3/28/14
  MPA1                        Maintain Path Names                      15:04:18
              User-> QRADARUSER QRADAR FTP USER

Type option, press Enter.
  2=Edit,4=Delete

Opt. Path Names...                                         R W D O/M
 _   /SafeNet/Qradar/*                                     X _ _  _









                                                                           Bottom


  F2 = Show Defined SafeNet Users      F3 = Exit      F6 = Add
  F12 = Return  HELP                             (c) Copyright 1997 MP Assoc.,Inc
```

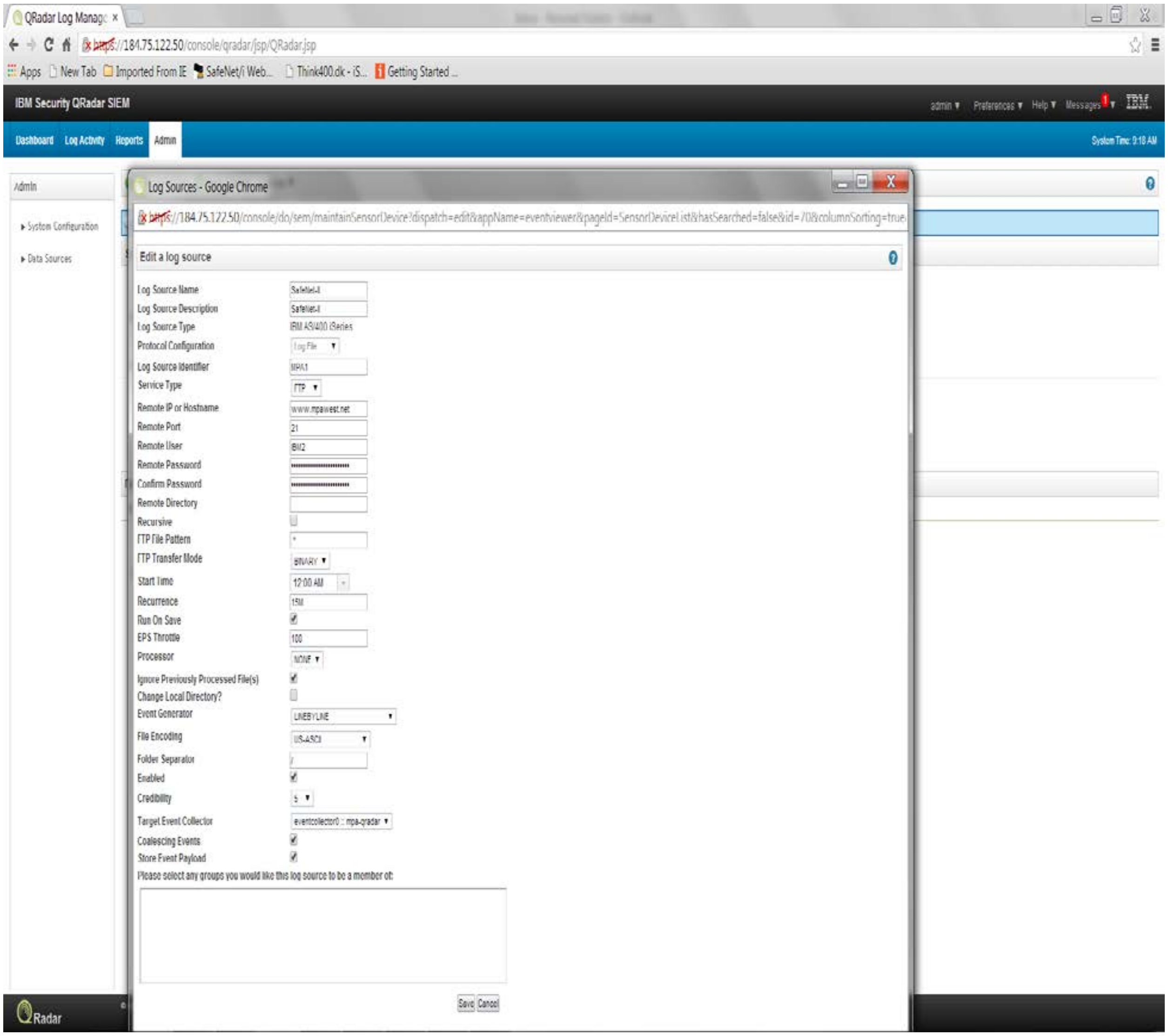
Setting Up a Log Source in QRadar®.

1. From the main menu of QRadar, select ADMIN, then LOG SOURCES
2. Click on “Add” top add a new log source.
3. Define the IBM i as a log source in Qradar as follows

Log Source Parameter Values:

Log Source Type	IBM AS/400 iSeries ←Must Be Selected
Protocol Configuration	LOG FILE ←Must Be Selected
Service Type	FTP ←Must Select FTP or SFTP
Remote IP or Hostname	IBMiHostIP ←Enter the ACTUAL IP or Host name of IBM i
Remote Port	21 ←For FTP use 21.
Remote User	IBMiUser ←Use the ID you created on the IBMi
Remote Directory	(leaveblank) ←No need to enter if setup in SafeNet/i correctly.
FTP File Pattern	.* ← Use .* for all files to be picked up (a dot and asterisk)
FTP Transfer Mode	Binary ←Must Be BINARY
Recurrence	15M ←15 minutes minimum allowed (customer choice)
Processor	NONE ←Must be NONE
Event Generator	LINEBYLINE ←Must be LINEBYLINE
File Encoding	US-ASCII ←Must be US-ASCII

See Screenshots on Next Page.



~~https~~://184.75.122.50/console/do/sem/maintainSensorDevice?dispatch=edit&appName=eventviewer&pageId=SensorDeviceList&hasSearched=false&id=/0&columnSorting=true

Edit a log source

Log Source Name	SafeNet-I
Log Source Description	SafeNet-I
Log Source Type	IBM AS/400 iSeries
Protocol Configuration	Log File ▾
Log Source Identifier	MPA1
Service Type	FTP ▾
Remote IP or Hostname	www.mpawest.net
Remote Port	21
Remote User	IBM2
Remote Password	••••••••••••••••••••
Confirm Password	••••••••••••••••••••
Remote Directory	
Recursive	□
FTP File Pattern	*
FTP Transfer Mode	BINARY ▾
Start Time	12:00 AM
Recurrence	15M
Run On Save	☑
EPS Throttle	100
Processor	NONE ▾
Ignore Previously Processed File(s)	☑
Change Local Directory?	□
Event Generator	LINEBYLINE ▾
File Encoding	US-ASCII ▾
Folder Separator	/
Enabled	☑
Credibility	5 ▾
Target Event Collector	eventcollector0 :: mpa-qradar ▾
Coalescing Events	☑
Store Event Payload	☑

Please select any groups you would like this log source to be a member of:

Testing the Initial Configuration

SafeNet/i Verification:

After the initial setup in SafeNet/i, perform the following to verify proper setup.

1. Make sure the FTP user can connect and logon, then is able to LIST and GET files from the directory.

2. Make sure Alert Notifications are active in SafeNet/i (See CHGNOTIFY) (Not required if doing a full payload build using STRSNRADAR command)

Do one of the following:

If using RADACT(*YES) for just rejections:

1. Manually cause an alert to be generated by SafeNet/i.

   Using FTP, connect to the IBM i and enter an invalid user id. That will cause a rejection.

2. After the normal Alert wait interval (see CHGNOTIFY), check for the SN_QRAD_xxxx.txt file in the IFS directory.

OR

If using STRSNRADAR for a Full Payload of normal transactions:

1. Set your start date and time using the CHGRDRSET command

2. Issue the STRSNRADAR command.

   This will initiate the batch job in SAFELOGING subsystem that builds the output file for QRADAR. This is a never ending job that will output all the records in the TRAPOD file. It may build multiple files of output until the EOF is reached.

   For the initial test, set your MAXSIZE value in command CHGRDRSET to 1 megabyte. Remember to set it back once you testing is complete (25MB is recommended file size)

3. This job will sleep for ten minutes once EOF occurs before building again. You can manually cancel this job at anytime if required.

Once a file is output, check the directory you entered in the CHGRDRSET command parameters (/QRADAR is default)

If the file is NOT found, re-check the configuration and the joblog for the ALERTWATCH job and/or the SN_QRADAR job in subsystem SAFELOGING

This finishes the verification of SafeNet/i alert processing.

QRADAR should be verified next:

1. Define the Log source in the QRadar application.
2. Activate the Log Source.
3. Check Status of Log Source in QRadar.
4. Check the SafeNet/i transaction file for FTP entries from the QRADAR system. You can select records based on the User ID assigned to the QRadar install. This will allow you to verify if QRadar successfully retrieved the alert files from the IBM i IFS.

STRSNRADAR and System Start-up

If you want to use the full payload output to build QRadar log files continuously as transactions occur on your system, you must either issue the STRSNRADAR command manually or add it to your system start up program. The command has no parameters.

STRSNRADAR submits a job called SN_RADAR to the SafeLoging subsystem. The batch job will read all the transactions from a starting timestamp in file TRAPOD until the Max File size is reached, or EOF occurs. Once either condition happens, a file will be created in the IFS path for pickup by QRADAR. This process does us the “/tmp” directory as a working directory during file build.

ENDSNRADAR

Additional References

See the SafeNet/i Reference guide at www.safeneti.com

See QRADAR software guides at www.ibm.com