

# iSecurity Queries and Reporting

User Guide  
Version 6.04

[www.razlee.com](http://www.razlee.com)



# Contents

---

Contents .....	3
Introduction .....	5
Real Time Monitoring .....	7
Query Generator Characteristics .....	8
Log of queries that were run .....	10
Report Scheduler .....	11
LOGS Additional benefits .....	13
Query Generator Capabilities .....	14
Information Types .....	17
Setup of Alert for Ransomware detection .....	28
Alert of Ransomware by email .....	29
IFS format of Antivirus scan (Beginning) .....	30
IFS format of Antivirus scan (Ending) .....	31
Antivirus / Anti-Ransomware log (Tabular format) .....	32
	33
Antivirus / Anti-Ransomware log (Message format) .....	34
Details of single line (Tabular format) from a Log .....	35
Details of single line (Message format) From a Log – A virus detection ....	36
Query Creation and Modification .....	37
Data Filtering .....	38
Selecting and Ordering Output Fields .....	39
Selecting and Ordering Output Fields .....	40
Specifying Sort .....	41
Specifying Sort .....	42
Adding Explanation .....	43
Running the Query – Output Format .....	44
Adding Explanation .....	45
Scheduling the Query .....	46

---

Running the Query .....	47
Dates as Figurative Constants (Week-Start, Month-Start...) .....	48
Dates as Figurative Constants (Week-Start, Month-Start...) .....	49
Scheduling the Query .....	50
Selecting LPARS to run for (LPAR Name, Group of LPARS, All LPARS)51	
Scheduling the Query .....	52
Selecting LPARS to run for (LPAR Name, Group of LPARS, All LPARS)53	
Selecting LPARS to run for (LPAR Name, Group of LPARS, All LPARS)54	
All Run Capabilities from the GUI in a Command Prompter .....	55
<b>Query Creation and Modification .....</b>	<b>56</b>
General details .....	57
Data Filtering .....	58
Final Screen - Adding Summary Report, Explanation, Scheduling .....	59
Scheduling the Query .....	60
Selecting LPARS to run for (LPAR Name, Group of LPARS, All LPARS)61	
System Name is automatically added for Multi-LPAR queries .....	62
<b>Business Intelligence over Firewall Data .....</b>	<b>63</b>
Activity by Date .....	64
Activity on September 2022 by User .....	65
Activities by Functions .....	66
Activity by Files .....	67
Activities by Commands .....	68
Activities by IP .....	69

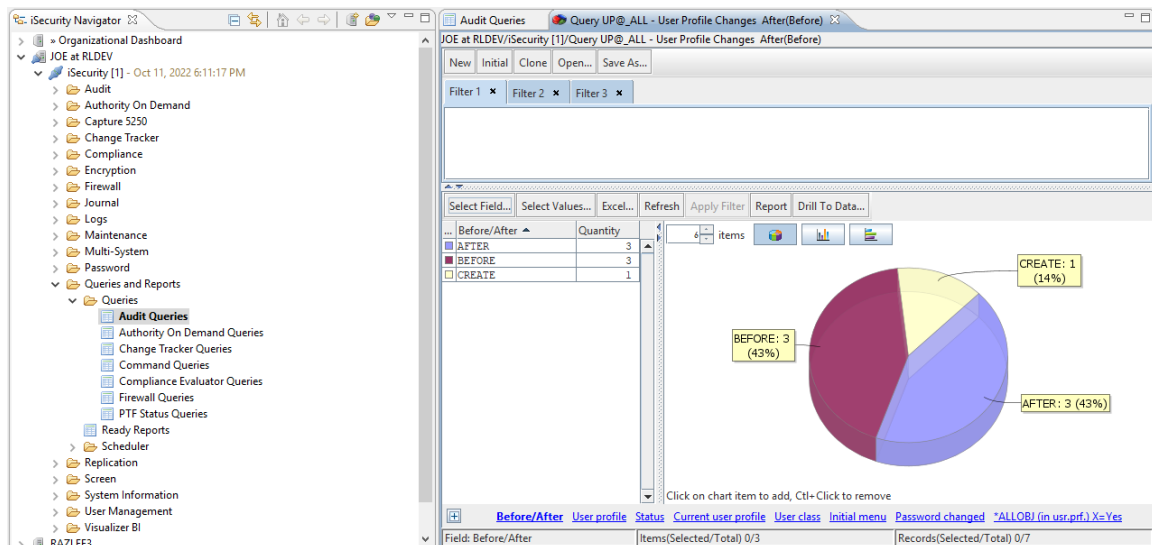
# Introduction

---

This document was prepared in order to illustrate some of the reporting capabilities of Firewall, Antivirus and Anti-Ransomware.

iSecurity includes powerful tools for creating and viewing queries, reports, and logs.

These tools exist on both the GUI version and the Native one.



The reporting features are:

- Display of log – showing the collected information of logs in either a message format which looks similar to a job log, or in a tabular view
- Query generator – a comprehensive report generator which has tremendous filtering capabilities and can create reports for one or more systems without copying the report definition
- Report Scheduler - enabling automatic run of groups of reports and logs.

- Ready Report Storage – Reports can be automatically stored in a data warehouse, making it possible to keep information for long periods.
- Visualizer – BI (Business Intelligence) for activity logs. It uses a data warehouse with compressed information, making it possible to keep information for long periods. This is available in the GUI interface only.
- Compliance Evaluator – score cards type reports to verify compliance with predefined targets

# Real Time Monitoring

---

Products react in real time to detected threats:

Anti-Ransomware will stop an attack and Alert

Antivirus will mark the object as unusable and/or quarantine it, and Alert.

Firewall will reject the transaction

Additional Real-time monitoring is available via iSecurity Action which can:

- SIEM messages, log to QSYSOPR, send SMS, Send EMAIL
- Run CL Scripts with parameters that are fields of the event
- Run User Programs

See <https://www.razlee.com/isecurity-action/> .

# Query Generator Characteristics

---

The Query Generator is extremely flexible and provides comprehensive data filtering, selection of fields and field order, and sorting data.

iSecurity provides numerous example queries.

Creating a query takes just few minutes and requires no programming skills.

Same query can be run for:

- Single LPAR – The current one, or another one
- Multiple LPARs, noting the LPAR originating the transaction on each line and/or sorted by LPAR.
- Groups of LPARs or All LPARs

Each query can be run for by the scheduler for:

- Predefined periods such as Day, Week, Month
- Selected time ranges such as From Date/Time - To Date/Time
- Last x minutes

Each query can produce for the same information in addition to the regular report three summary reports.

Each query can include an explanatory “handover” document along with the reports.

The query output can be displayed on the Green or GUI screen, or output as HTML, PDF, CSV (Excel), and OUTFILE (Output file). When using the GUI, the results of a query can also be directed to the Visualizer so BI methods can deal with the results.

The output can be sent by email, either one report at a time or as a group of reports together. Optional zip and password are available.

Alternatively, the query's output can be kept on the IBM i for future observation.

Customers can set the product to either send or eliminate empty reports.

The subject of the email will say If it only contains empty reports. (Some auditors prefer to keep all reports, even if they are empty, to ensure that the definition of the report did not change.)

## Log of queries that were run

---

The product collects information about each query that is run, including

- the full command used to run the report
- the time that it ran
- how long it took to run it, and
- the name of the output that it produced.

# Report Scheduler

---

The iSecurity Report Scheduler can run queries or groups of queries automatically.

It can run a Report Group for:

- Single LPAR
- Multiple LPARs, noting the LPAR originating the transaction on each line and/or sorted by LPAR.
- Groups of LPARs or All LPARs

Each Report Group can be run for by the scheduler for:

- Predefined periods such as Day, Week, Month
- Selected time ranges such as From Date/Time - To Date/Time

The Report Group output can be sent by email with or without Zip or Password protection.

Alternatively, the query's output can be kept on the IBM i for future observation.

## User Profile Changes After(Before)

\*GROUP\*

[Report Summaries](#) [Filter Conditions](#)

Query: UP@\_ALL User Profile Changes After(Before)

Printed: 11/10/22 18:36:13 On: RLDEV

Data Source: C@ User profile changed (After & Previous images)

For: 11/10/22-11/10/22

Before/	User	Status	Current	User	Initial	Password	*ALL	*JOB	*SAV	*SEC	*SPL	*SER	*AU	*IOSY
After	Profile		User	Class	Menu	Changed	OBJ	CTL	SYS	ADM	CTL	VICE	DIT	SCFG
			Profile											

BEFORE	VV2	*DISABLED	VICTOR	*USER	MAIN	N	N	N	N	N	N	N	N	N
AFTER	VV2	##ENABLED	VICTOR	*USER	MAIN	N	N	N	N	N	N	N	N	N
BEFORE	VV2	*DISABLED	VICTOR	*USER	MAIN	Y	N	N	N	N	N	N	N	N
AFTER	VV2	*DISABLED	VICTOR	*USER	MAIN	N	N	N	N	N	N	N	N	N
BEFORE	VV1	*DISABLED	VICTOR	*USER	MAIN	N	N	N	N	N	N	N	N	N
AFTER	VV1	##ENABLED	VICTOR	*USER	MAIN	N	N	N	N	N	N	N	N	N
CREATE	VV2	*DISABLED	VICTOR	*USER	MAIN	Y	N	N	N	N	N	N	N	N

4 records in the report.

Query: 000002UP @\_ALL User Profile Changes After(Before)

Printed: 11/10/22 18:36:13 On:

---\*\*\* Start Summary Report \*\*\*---

Count of User Profiles by Group Profile

Count	Group Profile
-------	---------------

4	*NONE
---	-------

=====

4 in total, 1 unique values, 4 records in the report.

---\*\*\* End Summary Report \*\*\*---

Query: UP@\_ALL User Profile Changes After(Before)  
Filter\_Conditions

11/10/22 18:36:13

Entry . . . . . C@ User profile changed (After & Previous images)

\*\* No Filters Found \*\*

[Back to Top](#)

## LOGS Additional benefits

---

Logs provide also the abilities to access, modify or create rules for similar situations. For example, the Firewall log can create or modify allow/reject rules.

# Query Generator Capabilities

---

## Output

Screen, GUI, \*PRINT, \*PRINT1-9 (special user settings for print), PDF, HTML, CSV, OUTFILE (output file by fields)

## Select (Filter)

The following TEST operations are supported:

- **EQ, NE, LE, GE, LT, GT**
- **LIST, NLIST** (Not LIST),
- **LIKE, NLIKE** (Not LIKE),
- **START, NSTART** (Not START),
- **ITEM, NITEM** (Not ITEM), where a value is checked to see if it is in a group. Supported groups include:
  - **\*GRPPRF** User is included in Group/Supplemental profile
  - **\*LMTCPB** User Limit Capabilities
  - **\*SPCAUT** User has a specified or any Special Authority
  - **\*TIMEGRP** Time group – a weekly time table (e.g. after hours and weekends)
  - **\*USRGRP** User is included in iSecurity/Firewall Group
  - **General group** Multiple groups ordered in classes such as Users, IPs, Libraries, and Objects. To simplify the setting of a rule, enter **ITEM** or **NITEM** as the TEST and press **F4**
- **PGM, NPGM** (Not Program), a provided or user written program that return True or False. For example, whether the command in CD audit type was entered during elevated authority by Authority On Demand

- To simplify the setting of rules, enter **PGM**, **NPGM**, **ITEM**, or **NITEM** as the test and press **F4**.

General groups can include generic names. **\*GENERIC** should follow the named group.

You can combine tests with **And** or **Or**. **And** is the default. You can include the same field multiple times.

## Sort

The following characteristics are available:

- Multiple Fields
- Ascending or Descending order
- Break after change of a number of sort fields. A title is created containing the specified sort fields. All lines exclude these fields.
- Report can include either all records or one record per key

## Summary Sub Reports

While running the main report, data can be grouped in addition sub-reports. For example, when running on objects in a group of libraries, you can create counts of objects by owner or counts of objects by type, or sum objects sizes per library).

Up to 3 Summary Sub Reports can be processed simultaneously.

Data is Counted or a value of a field is Summarized.

Each such report classifies the data based on 1 to 3 fields.

Condition to print lines in a Summary Sub Reports.

The total number of records is always printed.

## Explanation

Each report may carry a free format text that explains its contents. This reduces the effort of explaining the intention of the report and saves as its documentation.

## Print of Filter

The filter used for the report can be printed.

### Print of Header

A place for signing the report after inspecting it can be printed.

# Information Types

---

An effective security policy relies on queries and reports to provide traceability for system activity. Audit queries and reports contain information from an extremely wide range of sources.

Information code ID	Description	Where used (products)
\$@	History Log	Audit
\$A	User profile information	Audit,UserProfile
\$B	Objects that are owned by a user	Audit
\$C	Objects that a user is their primary group	Audit
\$D	Objects for which a user has specific authority	Audit
\$E	Job schedule entries	Audit
\$F	Command attributes	Audit
\$G	Group profile and their users	Audit,UserProfile
\$H	File members	Audit
\$I	Object description	Audit
\$J	Object authority	Audit
\$K	Job descriptions with user profile & *PUBLIC=*USE	Audit
\$L	Libraries description	Audit
\$M	User profile activation schedule	Audit,UserProfile
\$N	User profile expiration schedule	Audit,UserProfile
\$O	Program/Service-Program information	Audit
\$P	Users with default password (Repair by ANZDFTPWD)	Audit,UserProfile
\$Q	Programs that adopt authorities	Audit
\$R	IFS Objects	Audit
\$S	System values	Audit
\$T	Network attributes	Audit
\$U	Authorization Lists	Audit
\$V	Native objects secured by authorization list	Audit
\$W	DLO objects secured by authorization list	Audit
\$X	Library information [run RTVDSKINF	Audit

	first]	
\$Y	Modules of Program/Service-Program	Audit
\$0	Audit Statistics processing	Audit
\$1	Firewall Statistics processing	Audit
\$3	Compliance report	Audit
\$8	Query log report	Audit
\$9	Interface to any spool file query	All products
#A	System limits trending	Audit,KPI
#C	PTF Groups Installed vs. Available	Audit,ChgTracker,KPI
#G	Group PTF Info	Audit,ChgTracker,KPI
#H	PTF Info	Audit,ChgTracker,KPI
#K	Netstat information	Audit,KPI
#L	NETSTAT interface information	Audit,KPI
#M	NETSTAT routing information	Audit,KPI
#N	NetStat job info	Audit,KPI
#Q	AU TCP/IP information	Audit
#R	Current server information	Audit,KPI
#S	List of Servers-Share info	Audit
#U	System status	Audit,KPI
#V	System memory pool information	Audit,KPI
#W	AU Active jobs	Audit
#X	Disk status	Audit,KPI
#Y	Output queue information (summary)	Audit,KPI
#Z	License Information	Audit
@J	Active job information	Audit
@K	Job NOT active	Audit
@P	Pool NOT active	Audit
@Q	Active JobQ/OutQ information	Audit
@S	System status and pool information	Audit
@0	Message queue (Group Id 0)	Audit
@1	Message queue (Group Id 1)	Audit

@2	Message queue (Group Id 2)	Audit
@3	Message queue (Group Id 3)	Audit
@4	Message queue (Group Id 4)	Audit
@5	Message queue (Group Id 5)	Audit
@6	Message queue (Group Id 6)	Audit
@7	Message queue (Group Id 7)	Audit
@8	Message queue (Group Id 8)	Audit
@9	QHST messages	Audit
A\$	All types of QAUDJRN containing Library & Object	Audit
A#	All types of QAUDJRN	Audit
AD	Auditing changes	Audit
AF	Authority failure	Audit
AP	Obtaining adopted authority	Audit
AU	Attribute change	Audit
AX	Row and Column Access Control (RCAC)	Audit
C@	User profile changed (After & Previous images)	Audit,UserProfile
CA	Authority changes	Audit
CD	Command string audit	Audit,AOD
CF	Mail configuration info (QZMF)	Audit
CO	Create object	Audit
CP	User profile changed, created, or restored	Audit,UserProfile
CQ	Change of *CRQD object	Audit
CU	Cluster operations	Audit
CV	Connection verification	Audit
CY	Cryptographic configuration	Audit
D@	Command checked	Command
DI	Directory services	Audit
DO	Delete object	Audit
DP	Direct print info (QACGJRN)	Audit

DS	DST security password reset	Audit
ER	Mail error info (QZMF)	Audit
EV	System environment variables	Audit
GR	Generic record	Audit
GS	Socket description was given to another job	Audit
IM	Intrusion monitor	Audit
IP	Interprocess communication	Audit
IR	IP rules actions	Audit
IS	Internet security management	Audit
JB	Job resource info (QACGJRN)	Audit
JD	Change to user parameter of a job description	Audit
JS	Actions that affect jobs	Audit
KF	Key ring file	Audit
LD	Link, unlink, or look up directory entry	Audit
LG	Mail logging table info (QZMF)	Audit
ML	Office services mail actions	Audit
MP	QoS policies Modification (QQOS)	Audit
NA	Network attribute changed	Audit
ND	APPN directory search filter violation	Audit
NE	APPN end point filter violation	Audit
OM	Object move or rename	Audit
OR	Object restore	Audit
OW	Object ownership changed	Audit
O1	Optical access: Single file or directory	Audit
O2	Optical access: Dual file or directory	Audit
O3	Optical access: Volume	Audit
P@	Password Reset	P-R
PA	Program changed to adopt	Audit

	authority	
PF	PTF Operations	Audit
PG	Change of an object's primary group	Audit
PO	Printed output	Audit
PS	Profile swap	Audit
PU	PTF Object Change	Audit
PW	Invalid password	Audit
RA	Authority change during restore	Audit
RJ	Restoring job description with profile specific	Audit
RO	Change of object owner during restore	Audit
RP	Restoring adopted authority program	Audit
RQ	Restoring a *CRQD object	Audit
RU	Restoring user profile authority	Audit
RZ	Changing a primary group during restore	Audit
SD	Changes to system distribution directory	Audit
SE	Subsystem routing entry changed	Audit
SF	Actions to spooled files	Audit
SG	Asynchronous Signals	Audit
SK	Sockets Connections (IP/Port)	Audit
SM	System management changes	Audit
SN	Simple Network Management Protocol (SNMP) informat	Audit
SO	Server security user information actions	Audit
SP	Spooled print info (QACGJRN)	Audit
ST	Use of service tools	Audit
SV	System value changed	Audit
SY	Mail system info (QZMF)	Audit

TF	IP filter rules actions (QIPFILTER)	Audit
TN	IP NAT rules actions (QIPNAT)	Audit
TS	VPN information (QVPN)	Audit
VA	*REMOVED BY IBM* Changing an access control list	Audit
VC	*REMOVED BY IBM* Starting or ending a connection	Audit
VF	*REMOVED BY IBM* Closing server files	Audit
VL	*REMOVED BY IBM* Account limit exceeded	Audit
VN	*REMOVED BY IBM* Logging on and off the network	Audit
VO	Validation list actions	Audit
VP	Network password error	Audit
VR	*REMOVED BY IBM* Network resource access	Audit
VS	*REMOVED BY IBM* Starting/ending a server session	Audit
VU	*REMOVED BY IBM* Changing a network profile	Audit
VV	*REMOVED BY IBM* Changing service status	Audit
XD	Directory server extension	Audit
XE	DSNX error entry (QDSNX)	Audit
XL	DSNX logging entry (QDSNX)	Audit
X0	Network Authentication	Audit
X1	Identity token	Audit
X2	Query Manager profile values.	Audit
YC	DLO object accessed (change)	Audit
YR	DLO object accessed (read)	Audit
ZC	Object accessed (change)	Audit
ZM	SOM method access (no longer used by IBM)	Audit

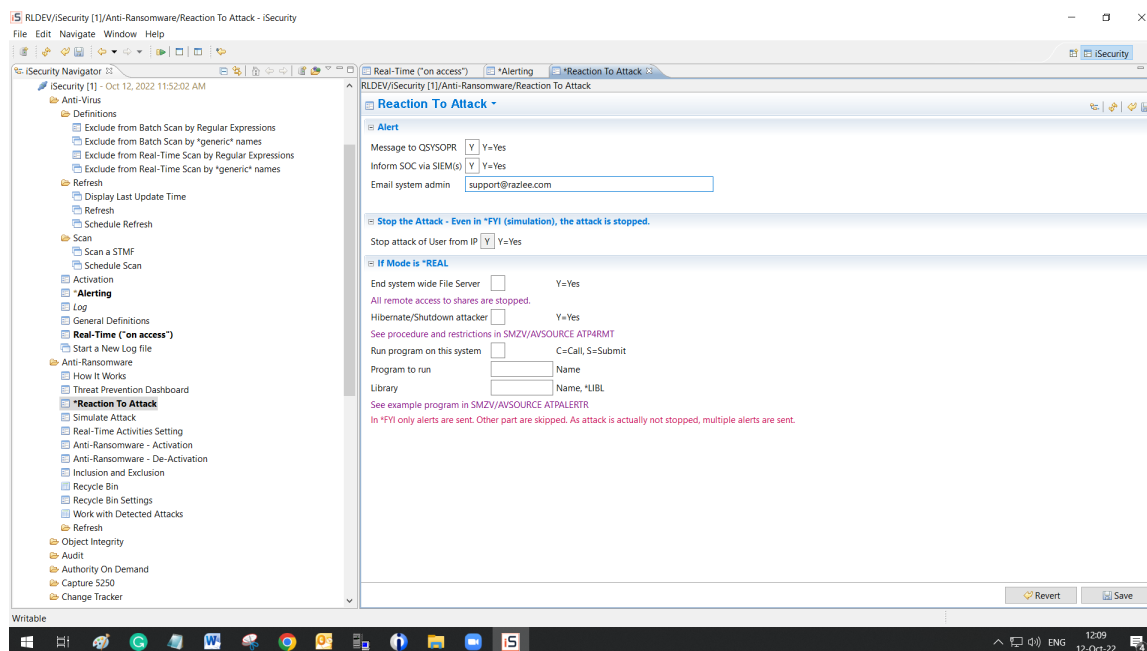
ZR	Object accessed (read)	Audit
00	Generic entry type (00-99 for reporting only)	Firewall
01	*FILTFR Original File Transfer Function	Firewall
02	*FTPLOG FTP Server Logon	Firewall
03	*FTPSRV FTP Server-Incoming Rqst Validation	Firewall
04	*SQL Database Server - SQL access	Firewall
05	*RMTSRV Remote Command/Program Call	Firewall
06	*FILSRV File Server	Firewall
07	*DDM DDM request access	Firewall
08	*TELNET Telnet Device Initialization	Firewall
09	*TFTP TFTP Server Request Validation	Firewall
1K	*FW-DFN Native Object Security	Firewall (dfn)
1L	*FW-DFN IFS object security	Firewall (dfn)
1M	*FW-DFN Command Exceptions	Firewall (dfn)
1N	*FW-DFN Users & Groups	Firewall (dfn)
1Y	iSecurity groups members	Audit
10	*REXLOG REXEC Server Logon	Firewall
11	*REXEC REXEC Server Request Validation	Firewall
12	*RMTSQL Original Remote SQL Server	Firewall
13	*NDB Database Server - data base access	Firewall
14	*WSG WSG Server Sign-On Validation	Firewall
15	*ORDTAQ Original Data Queue Server	Firewall
16	*DTAQ Data Queue Server	Firewall
17	*MSGSRV Original Message Server	Firewall

18	*SQLENT Database Server - entry	Firewall
19	*OBJINF Database Server - object information	Firewall
20	*VPRT Original Virtual Print Server	Firewall
21	*NPARENT Network Print Server - entry	Firewall
22	*NPRSPL Network Print Server - spool file	Firewall
23	*CHGUP Change User Profile	Firewall
24	*CRTUP Create User Profile	Firewall
25	*DLTUPA Delete User Profile - after delete	Firewall
26	*DLTUPB Delete User Profile	Firewall
27	*RSTUP Restore User Profile	Firewall
28	*ORLICM Original License Mgmt Server	Firewall
29	*CSLICM Central Server - license mgmt	Firewall
30	*CSCNVM Central Server - conversion map	Firewall
31	*CSCLNM Central Server - client mgmt	Firewall
32	*TCPSGN TCP Signon Server	Firewall
33	*PWRDWN Prepower Down System	Firewall
34	*RMTSGN Remote sign-on (Passthrough)	Firewall
35	*PWDVLD Password Dictionary Check / Validation	Firewall
36	*DRDA DRDA Distributed Relational DB access	Firewall
37	*FTPCLN FTP Client-Outgoing Rqst Validation	Firewall
38	*TELOFF Telnet Device Termination	Firewall
39	*DHCPAB DHCP Address Binding	Firewall

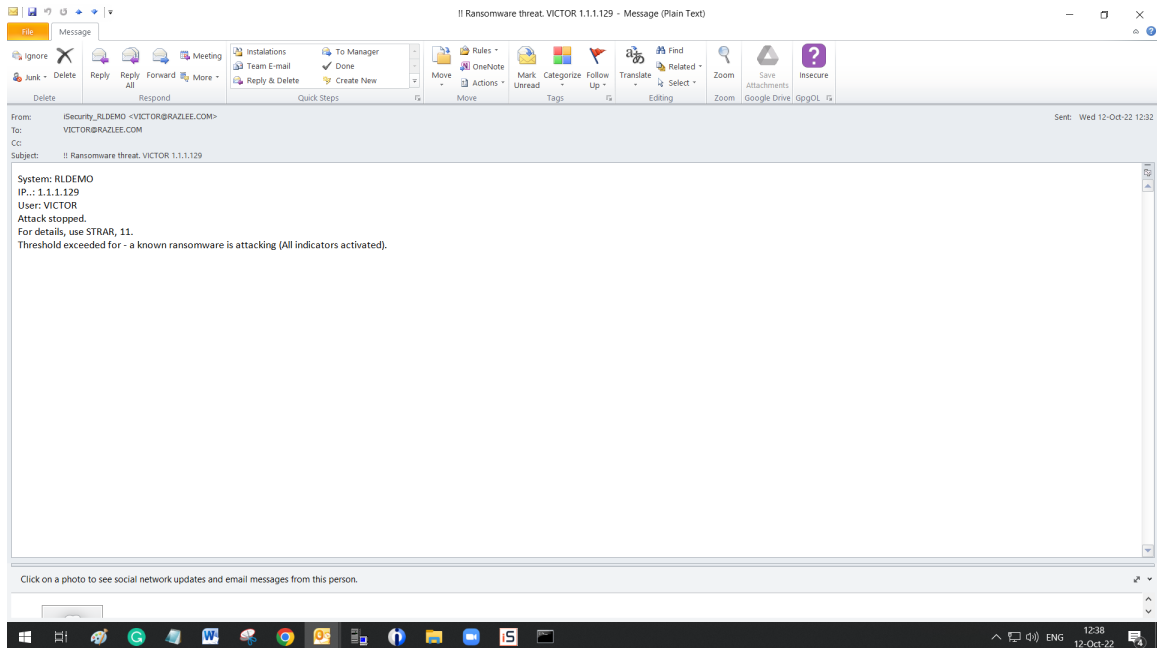
	Notify	
40	*DHCPAR DHCP Address Release Notify	Firewall
41	*DHCPRP DHCP Request Packet Validation	Firewall
42	*SIGNON Sign-On completed	Firewall
43	*PWDCHK Password Dictionary Check / Check	Firewall
44	*SSHD SSH Daemon	Firewall
45	*DBOPEN Open Database	Firewall
46	*PWDVL2 Password Dictionary Check /Validation fmt2	Firewall
47	*SKTACP Socket Accept	Firewall
48	*SKTCNT Socket Connect	Firewall
49	*SKTLSN Socket Listen	Firewall
5A	Tracking Data (Native/IFS/PTF/Source)	ChgTracker
5B	ILE Modules Inventory	ChgTracker
5D	Definition of IFS Directories	ChgTracker
5F	PTF Status	ChgTracker
5G	PTF Advanced status (Rel 7.2)	ChgTracker
5I	Definition of Activity to Disregard	ChgTracker
5J	Definition of Environments	ChgTracker
5L	Definition of Libraries to Trace	ChgTracker
5M	Definition of Projects	ChgTracker
5N	Definition of Tasks	ChgTracker
5R	Definition of IFS Directories to Disregard	ChgTracker
5W	Tracking Data (Native Objects)	ChgTracker
5X	Tracking Data (Source Members)	ChgTracker
5Y	Tracking Data (IFS Objects)	ChgTracker
5Z	Tracking Data (PTF Objects)	ChgTracker
50	*DBSTT Database statistics	Firewall

6A	Object Journaling Plan	AP-Journal
6B	Object check Journaling Plan	AP-Journal
6C	Confirmation tickets	AP-Journal
6I	AOD History	AOD
6V	Virus, Worm, Trojan, Ransomware detected	Antivirus, Anti-Ransomware
	Ransomware Detections	
6X	Person - Attributes	P-R
6Y	Users of a Person	P-R
6Z	Log of who changed questions	P-R
7E	User Compliance Check	Action
7F	User Compliance Plan	Action
7I	Native Object Compliance Check	Action
7J	Native Object Compliance Plan	Action
7M	IFS Object Compliance Check	Action
7N	IFS Object Compliance Plan	Action
97	*SCRLCK Screen locked due to timeout	Firewall
98	*SCRRLS Screen released	Firewall
99	*SCREND Screen jobs ended as timeout passed	Firewall

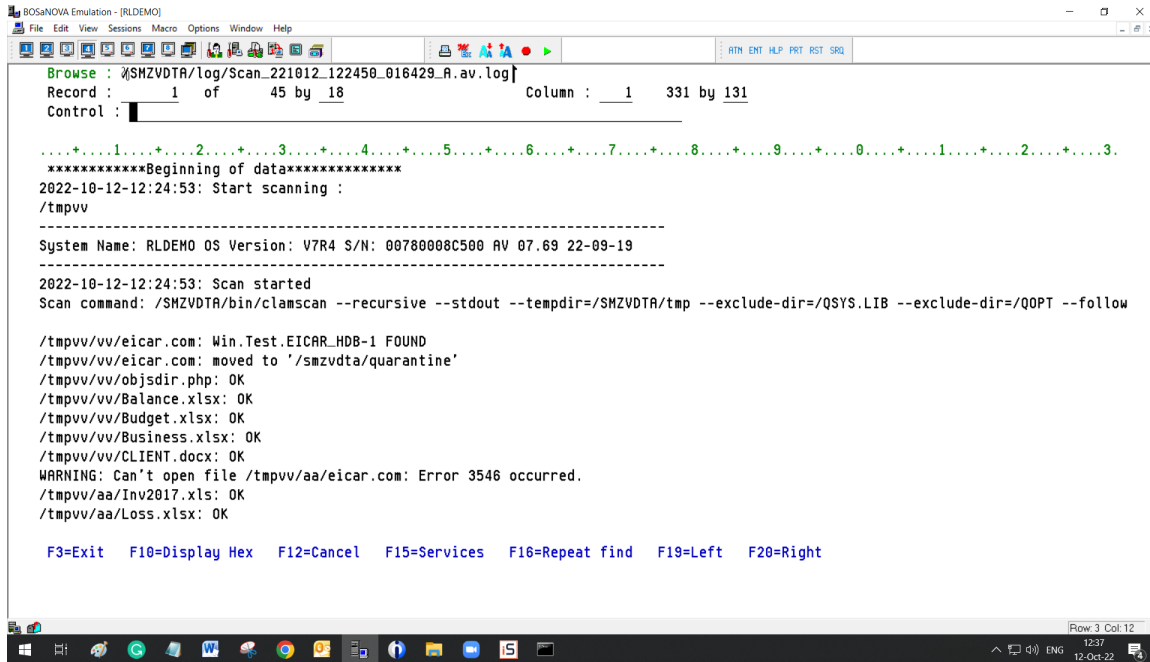
# Setup of Alert for Ransomware detection



# Alert of Ransomware by email



# IFS format of Antivirus scan (Beginning)



The screenshot shows a BOSaNOVA Emulation window titled "[RLDEMO]". The window contains a terminal-like interface with a menu bar (File, Edit, View, Sessions, Macro, Options, Window, Help) and a toolbar. The main display area shows the following text:

```
Browse : %SMZVDTA/log/Scan_221012_122450_016429_A.av.log
Record : 1 of 45 by 18 Column : 1 331 by 131
Control :

.....1.....2.....3.....4.....5.....6.....7.....8.....9.....0.....1.....2.....3
*****Beginning of data*****
2022-10-12-12:24:53: Start scanning :
/tmpvv

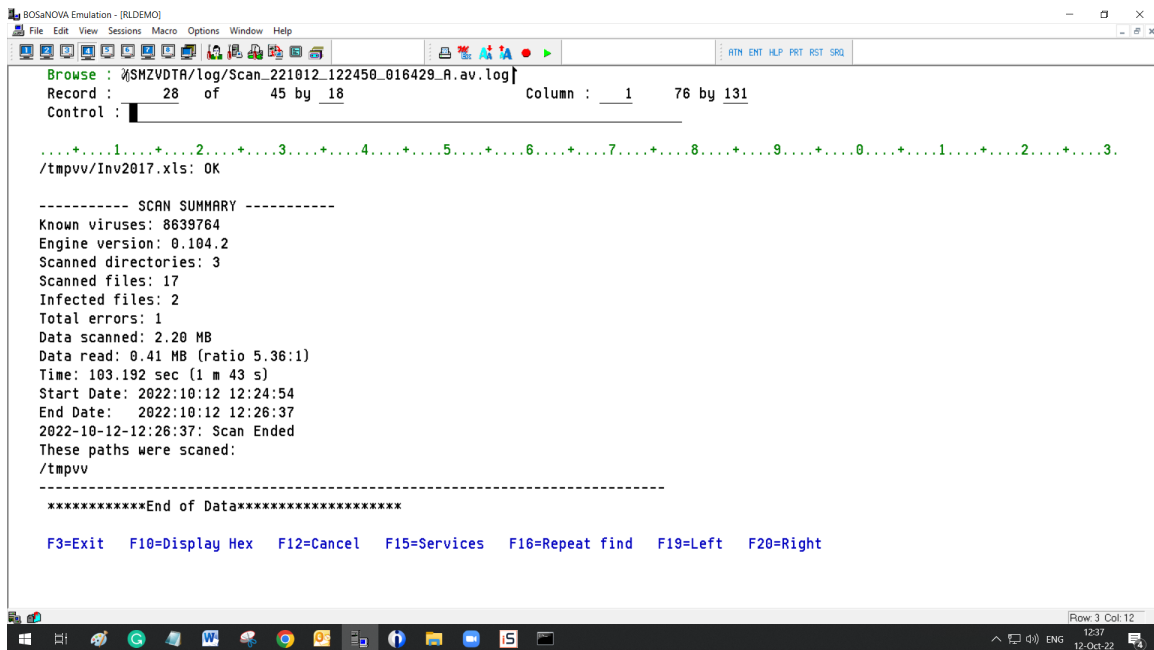
-----
System Name: RLDEMO OS Version: V7R4 S/N: 00780008C500 AV 07.69 22-09-19
-----
2022-10-12-12:24:53: Scan started
Scan command: /SMZVDTA/bin/clamscan --recursive --stdout --tempdir=/SMZVDTA/tmp --exclude-dir=/QSYS.LIB --exclude-dir=/QOPT --follow

/tmpvv/vv/eicar.com: Win.Test.EICAR_HDB-1 FOUND
/tmpvv/vv/eicar.com: moved to '/smzvdt/quarantine'
/tmpvv/vv/objdir.php: OK
/tmpvv/vv/Balance.xlsx: OK
/tmpvv/vv/Budget.xlsx: OK
/tmpvv/vv/Business.xlsx: OK
/tmpvv/vv/CLIENT.docx: OK
WARNING: Can't open file /tmpvv/aa/eicar.com: Error 3546 occurred.
/tmpvv/aa/Inv2017.xls: OK
/tmpvv/aa/Loss.xlsx: OK

F3=Exit F10=Display Hex F12=Cancel F15=Services F16=Repeat find F19=Left F20=Right
```

The bottom of the window shows a Windows taskbar with various application icons and a system tray on the right displaying the time as 12:37 on 12-Oct-22.

# IFS format of Antivirus scan (Ending)



The screenshot shows a terminal window titled "BOSaNOVA Emulation - [RLDEMO]". The window displays the ending of an Antivirus scan. The scan summary includes the following information:

```
----- SCAN SUMMARY -----
Known viruses: 8639764
Engine version: 0.104.2
Scanned directories: 3
Scanned files: 17
Infected files: 2
Total errors: 1
Data scanned: 2.20 MB
Data read: 0.41 MB (ratio 5.36:1)
Time: 103.192 sec (1 m 43 s)
Start Date: 2022:10:12 12:24:54
End Date: 2022:10:12 12:26:37
2022-10-12-12:26:37: Scan Ended
These paths were scanned:
/tmpuv
*****End of Data*****

F3=Exit F10=Display Hex F12=Cancel F15=Services F16=Repeat find F19=Left F20=Right
```

The window also shows a file path: `\\SMZVDTA\log\Scan_221012_122450_016429_A.av.log`. The record number is 28 of 45 by 18. The column is 1, 76 by 131. The control is set to 1. The window title bar includes "File Edit View Sessions Macro Options Window Help". The bottom status bar shows "Row 3 Col:12", "12:37", and "12-Oct-22".

# Antivirus / Anti-Ransomware log (Tabular format)

Top=Newest

Date	Time	Job	IP	Type	Display Audit Log	User	Object
10/12	12:31	QZLSFILE		6V/1	Known ransomware is	VICTOR	*STMF /atptest/Business.xlsx.WNCRY
10/12	12:26	QP0ZSPWT		6V/V	Antivirus	VICTOR	*STMF /tmpvv/eicar.com
10/12	12:26	QP0ZSPWT		6V/V	Antivirus	VICTOR	*STMF /tmpvv/eicar.com
10/12	12:26	QP0ZSPWT		6V/V	Antivirus	VICTOR	*STMF /tmpvv/vv/eicar.com
10/12	12:26	QP0ZSPWT		6V/V	Antivirus	VICTOR	*STMF /tmpvv/vv/eicar.com

Bottom

F3=Exit F5=Screen F6=Add rule F7=Subset F10=Message F11=Details F13=By message F17=Top F18=Bottom

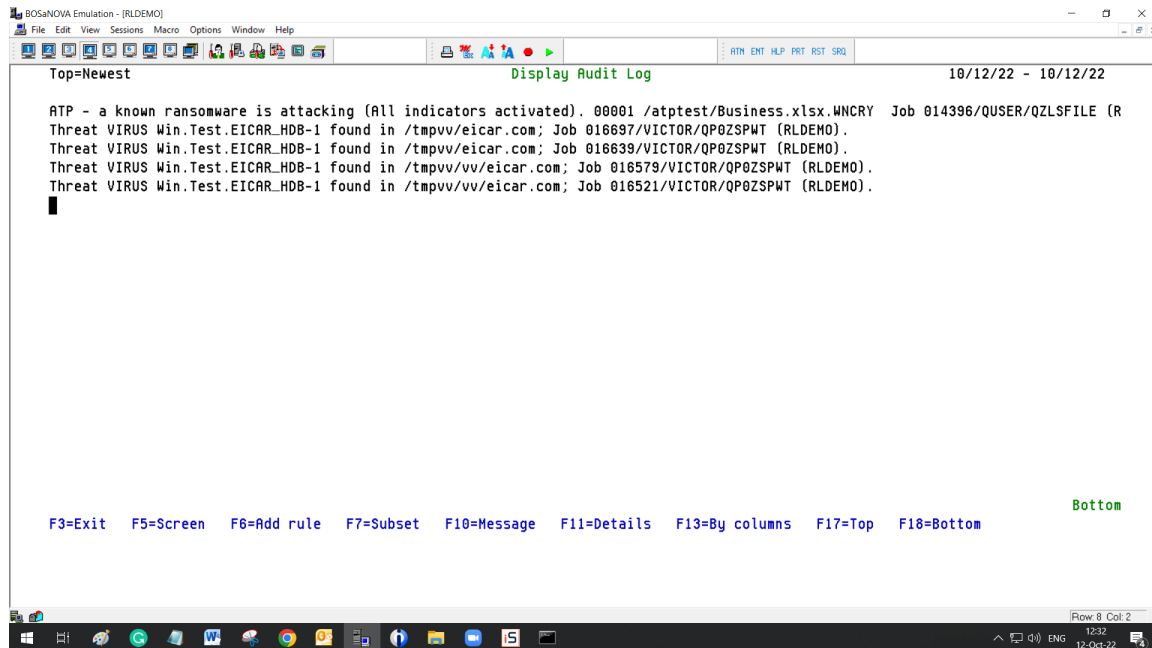
Row: 3 Col: 2

1231  
12-Oct-22

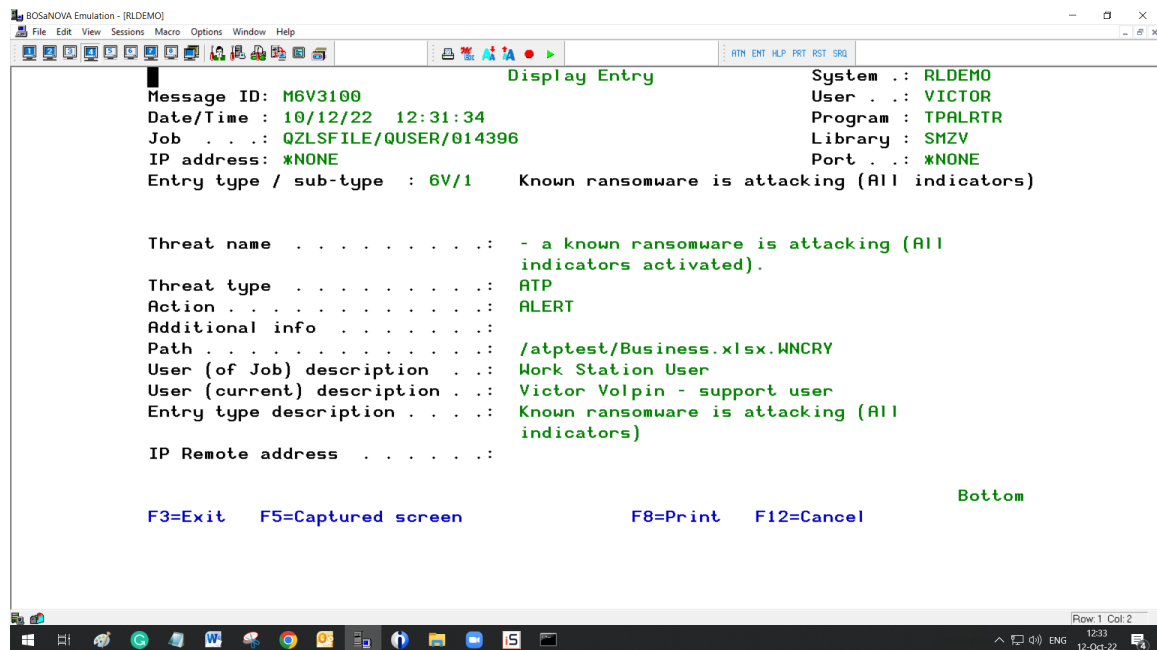


# Antivirus / Anti-Ransomware log (Message format)

---

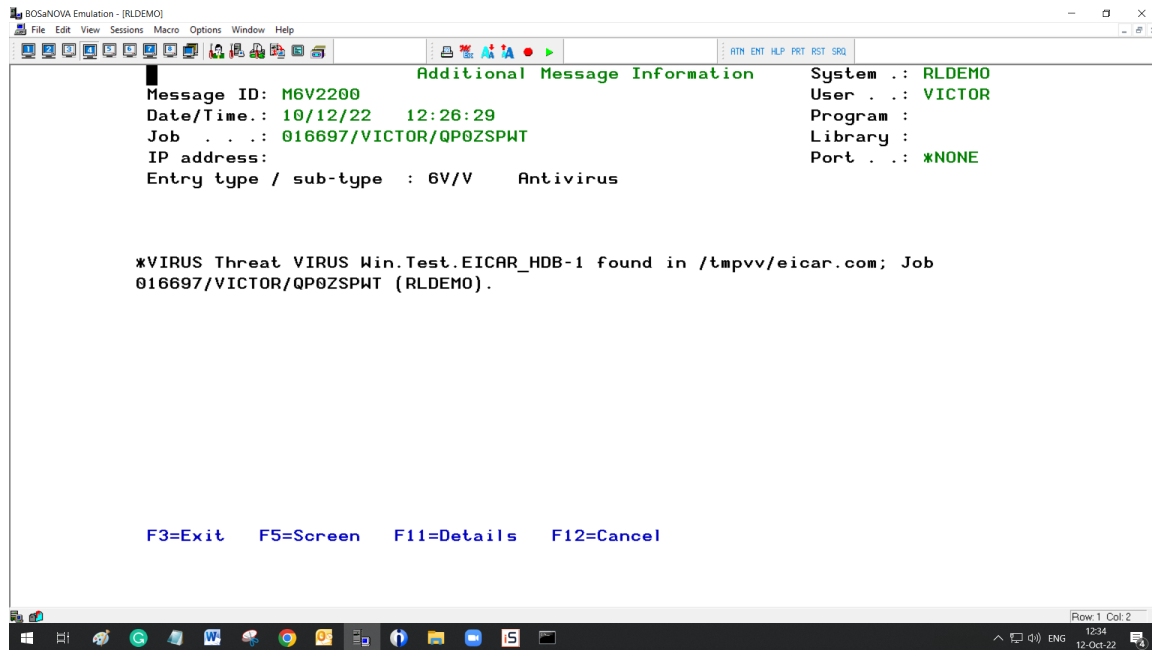


# Details of single line (Tabular format) from a Log



# Details of single line (Message format) From a Log – A virus detection

---



# Query Creation and Modification

---

# Data Filtering

RLDEV/Security [2]/Queries and Reports/Queries/Firewall Queries - (Security)

File Edit Navigate Window Help

Security Navigator

- Activation
- Alerting
- Log
- General Definitions
- Real-Time ("on access")
- Start a New Log file
- Anti-Ransomware
- Object Integrity
- Audit
- Authority On Demand
- Capture 5250
- Change Tracker
- Compliance
- Encryption
- Firewall
- Journal
- Logs
- Maintenance
- MFA
- Multi-System
- Password
- PGP Encryption
- Queries and Reports
  - Queries
    - Audit Queries
    - Authority On Demand Queries
    - Change Tracker Queries
    - Command Queries
    - Compliance Evaluator Queries
    - Firewall Queries**
    - PTT Status Queries
  - Ready Reports
- Scheduler
- Replication
- Screen
- System Information
- User Management
- Visualizer BI

Firewall Queries

RLDEV/Security [2]/Queries and Reports/Queries/Firewall Queries [64 min idle]

Firewall Queries

Edit Query - Z6SIGNON1

General Filter Output Fields Sort Fields Compliance and Explanation

Checked/Unchecked Checked/Unchecked Browse...

0/3

Select All Deselect All Add Delete

OK Cancel

Classification	Last Change Date	Last Change By User
	Apr 18, 2017	GS
	Jul 24, 2019	ALEX3
	Apr 18, 2017	GS
	Apr 18, 2017	GS
	Apr 18, 2017	GS
	Apr 18, 2017	GS
	Jul 2, 2020	OD
	Oct 12, 2022	AU
	Apr 18, 2017	GS
	Apr 18, 2017	GS
	Mar 17, 2020	GS
	Jan 18, 2022	OD
	Apr 18, 2017	GS
	Aug 9, 2020	OD
	Apr 18, 2017	GS
	Feb 9, 2021	GS
	Sep 27, 2017	GS
	Nov 22, 2018	GS
	Apr 19, 2017	GS

1/93

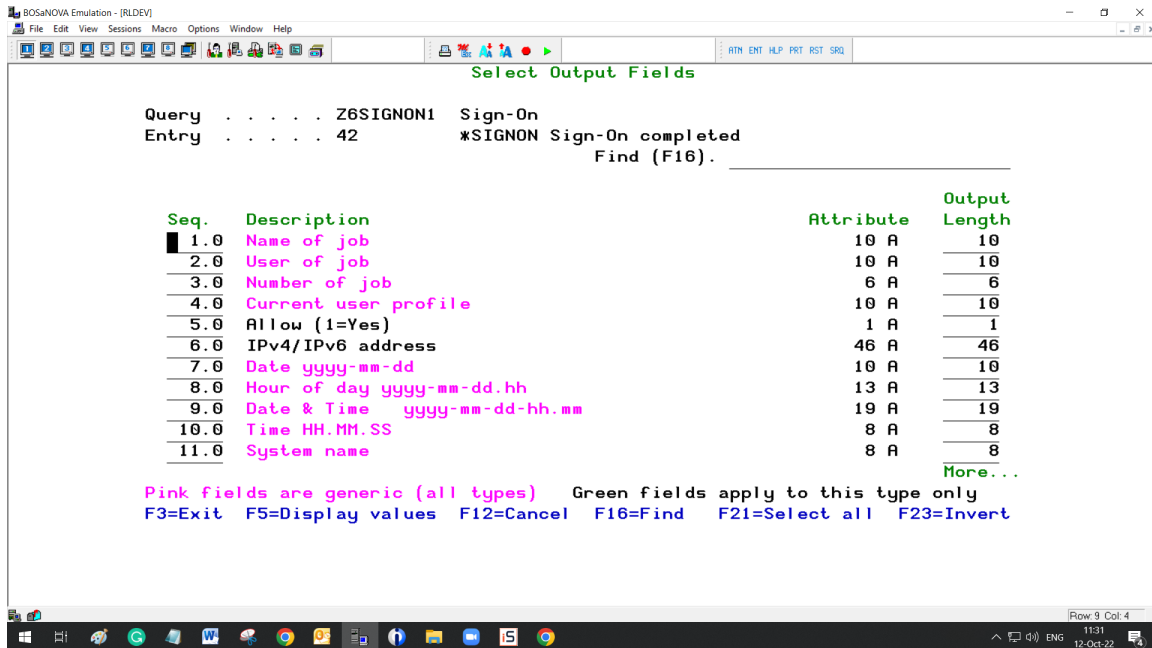
Run... Schedule...

Copy... Add... Delete Open...

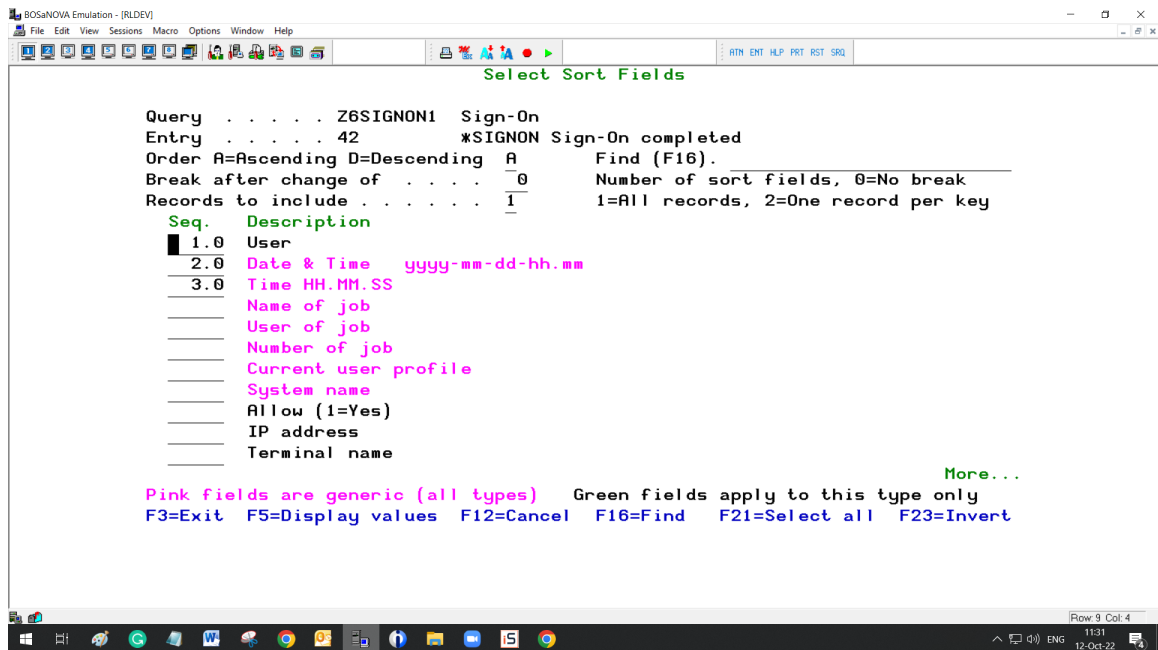
13:51 12-Oct-22



# Selecting and Ordering Output Fields



# Specifying Sort



# Specifying Sort

RLDEV/Security [2]/Queries and Reports/Queries/Firewall Queries - iSecurity

File Edit Navigate Window Help

iSecurity Navigator

- Activation
  - Alerting
  - Log
  - General Definitions
  - Real-Time ("on access")
  - Start a New Log file
- Anti-Ransomware
- Object Integrity
- Audit
  - Authority On Demand
- Capture 5250
- Change Tracker
- Compliance
- Encryption
- Journal
- Logs
- Maintenance
- MFA
- Multi-System
- Password
- PGP Encryption
- Queries and Reports
  - Queries
    - Audit Queries
    - Authority On Demand Queries
    - Change Tracker Queries
    - Command Queries
    - Compliance Evaluator Queries
    - Firewall Queries**
    - PTT Status Queries
  - Ready Reports
- Scheduler
- Replication
- Screen
- System Information
- User Management
- Visualizer BI

Firewall Queries

RLDEV/Security [2]/Queries and Reports/Queries/Firewall Queries [65 min idle]

Firewall Queries

Edit Query - Z6SIGNON1

General Filter Output Fields Sort Fields Compliance and Explanation

☐ Include one record per key

☒ Checked/Unchecked  Browse... Up Down Top Bottom Compact

Field
<input checked="" type="checkbox"/> User
<input checked="" type="checkbox"/> Date & Time yyyy-mm-dd-hh:mm (generic header)
<input checked="" type="checkbox"/> Time HH:MM:SS (generic header)
<input type="checkbox"/> Terminal name
<input type="checkbox"/> IP-v4/IPv6 address
<input type="checkbox"/> Name of job (generic header)
<input type="checkbox"/> Number of job (generic header)
<input type="checkbox"/> IP address
<input type="checkbox"/> Allow (1=Yes)
<input type="checkbox"/> System name (generic header)
<input type="checkbox"/> User of job (generic header)
<input type="checkbox"/> Current user profile (generic header)
<input type="checkbox"/> Date yyyy-mm-dd (generic header)
<input type="checkbox"/> Hour of day yyyy-mm-dd:hh (generic header)

1/14 Select All Deselect All

OK Cancel

Classification	Last Change Date	Last Change By User
	Apr 18, 2017	GS
	Jul 24, 2019	ALEX3
	Apr 18, 2017	GS
	Apr 18, 2017	GS
	Apr 18, 2017	GS
	Apr 18, 2017	GS
	Jul 2, 2020	OD
	Oct 12, 2022	AU
	Apr 18, 2017	GS
	Apr 18, 2017	GS
	Mar 17, 2020	GS
	Jan 18, 2022	OD
	Apr 18, 2017	GS
	Aug 9, 2020	OD
	Apr 18, 2017	GS
	Feb 9, 2021	GS
	Sep 27, 2017	GS
	Nov 22, 2018	GS
	Apr 19, 2017	GS

1/93 Run... Schedule... Copy... Add... Delete Open...

13:52 12-Oct-22

# Adding Explanation

The screenshot shows the iSecurity application interface. The 'Firewall Queries' window is open, displaying a list of queries. The 'Edit Query - Z6SIGNON1' dialog box is open, showing the 'Explanation' tab. The dialog box contains a 'Classification List' and an 'Explanation' text area. The background window shows a table of query details.

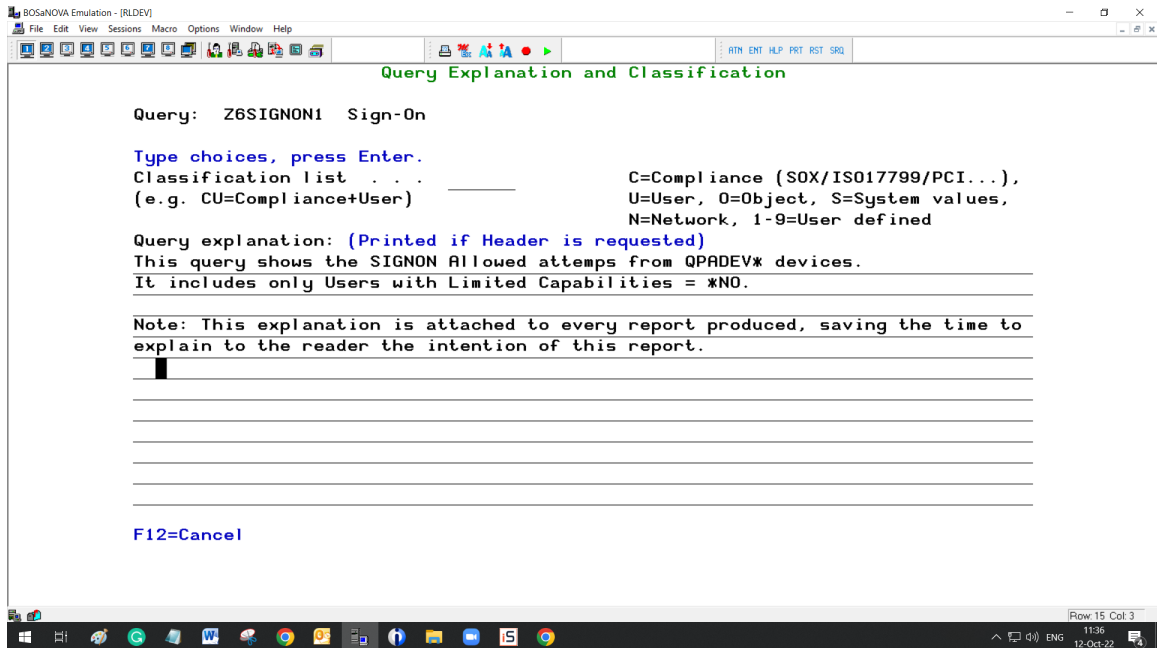
Classification	Last Change Date	Last Change By User
	Apr 18, 2017	GS
	Jul 24, 2019	ALEX3
	Apr 18, 2017	GS
	Apr 18, 2017	GS
	Apr 18, 2017	GS
	Jul 2, 2020	OD
	Oct 12, 2022	AU
	Apr 18, 2017	GS
	Apr 18, 2017	GS
	Mar 17, 2020	GS
	Jan 18, 2022	OD
	Apr 18, 2017	GS
	Aug 9, 2020	OD
	Apr 18, 2017	GS
	Feb 9, 2021	GS
	Sep 27, 2017	GS
	Nov 22, 2018	GS
	Apr 19, 2017	GS

# Running the Query – Output Format

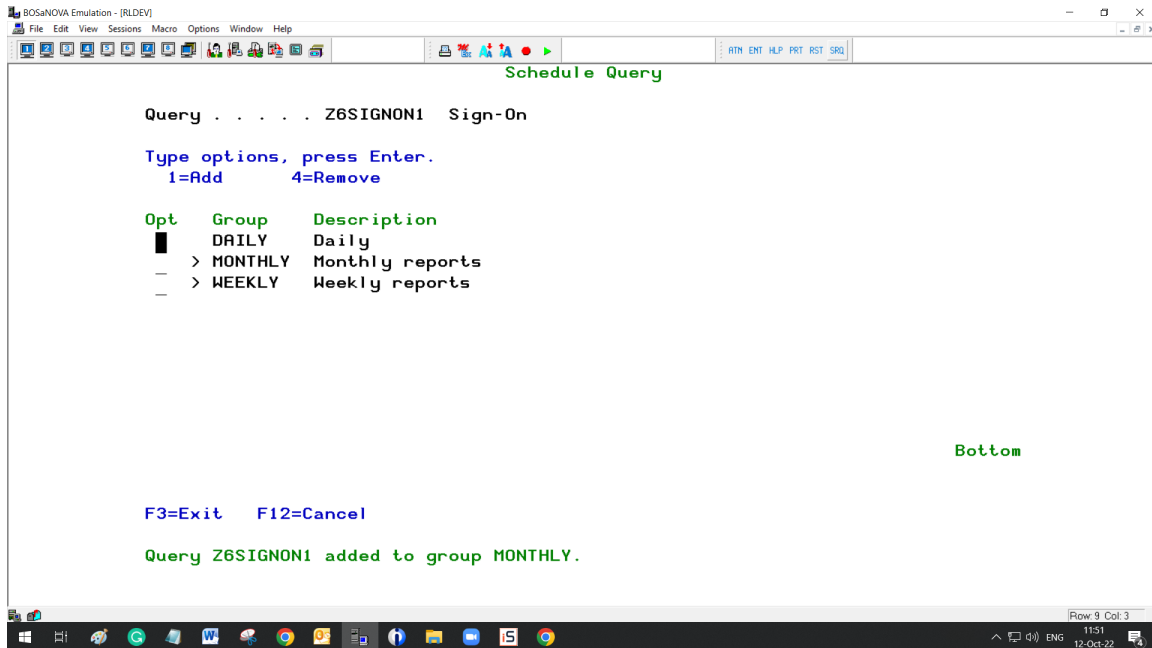
The screenshot displays the iSecurity Navigator interface. A dialog box titled "Run Firewall Query - Sign-On" is open, showing the "Output Format" configuration. The "HTML" option is selected under "Select output format". There are checkboxes for "Keep file" next to "CSV" and "PDF". A "PRINT" button is visible. Below, the "Mail to:" field is set to "victor@razlee.com" with a dropdown menu showing "mail1,mail2,mail3...". The background shows a list of queries in the "Firewall Queries" section, including Z6SQL, Z6TRSQL, Z6TPSGN, Z6TELNET, Z6TELOFF, Z6TFTP, Z6USER, Z6USRCT, Z6VPRT, and Z6WSG, each with a description and a "Last Change Date".

Classification	Last Change Date	Last Change By User
	Apr 18, 2017	GS
	Jul 24, 2019	ALEX3
	Apr 18, 2017	GS
	Apr 18, 2017	GS
	Apr 18, 2017	GS
	Apr 18, 2017	GS
	Apr 18, 2017	GS
	Jul 2, 2020	OD
	Oct 12, 2022	AU
	Apr 18, 2017	GS
	Aug 9, 2020	OD
	Apr 18, 2017	GS
	Feb 9, 2021	GS
	Jan 18, 2022	OD
	Apr 18, 2017	GS
	Sep 27, 2017	GS
	Nov 22, 2018	GS
	Apr 19, 2017	GS

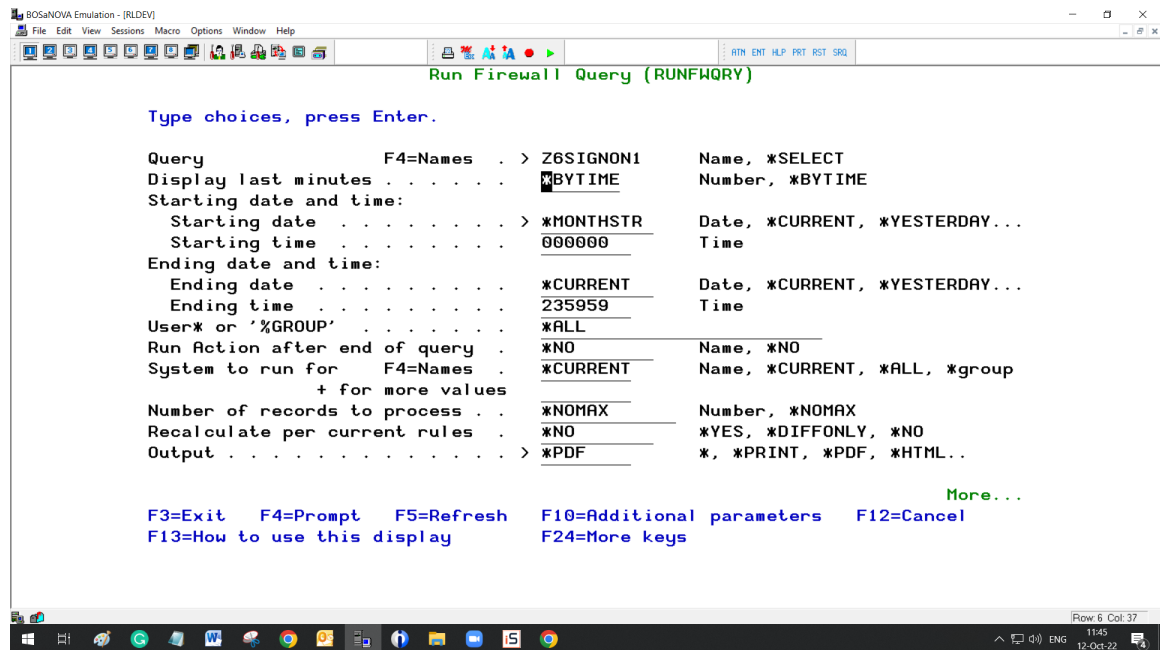
# Adding Explanation



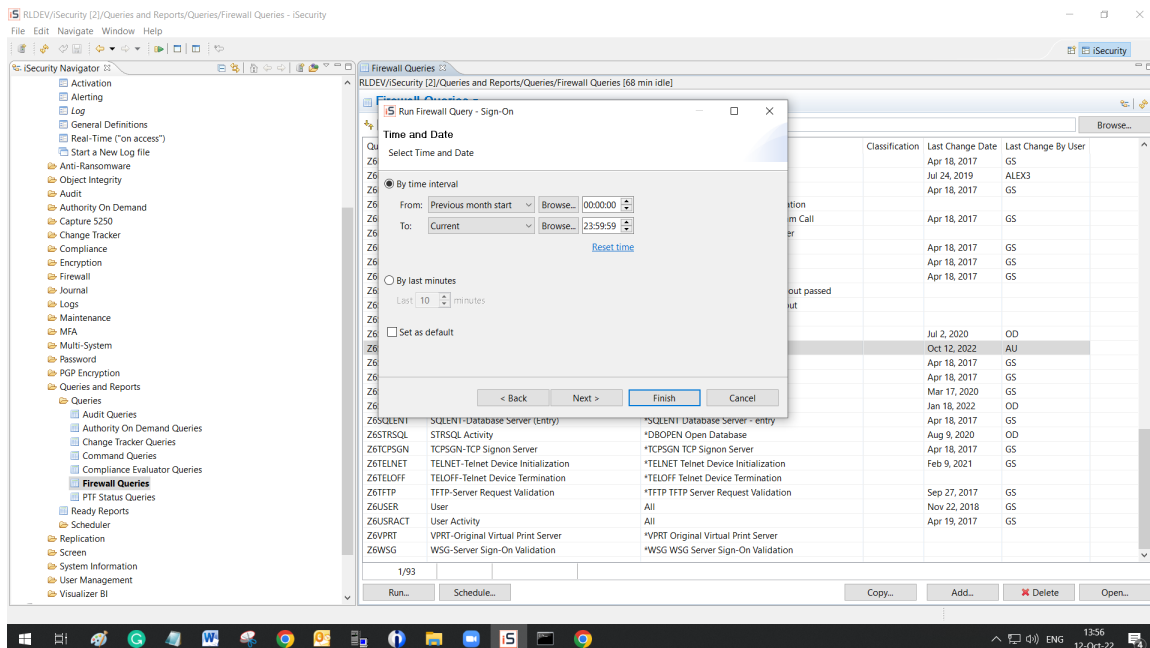
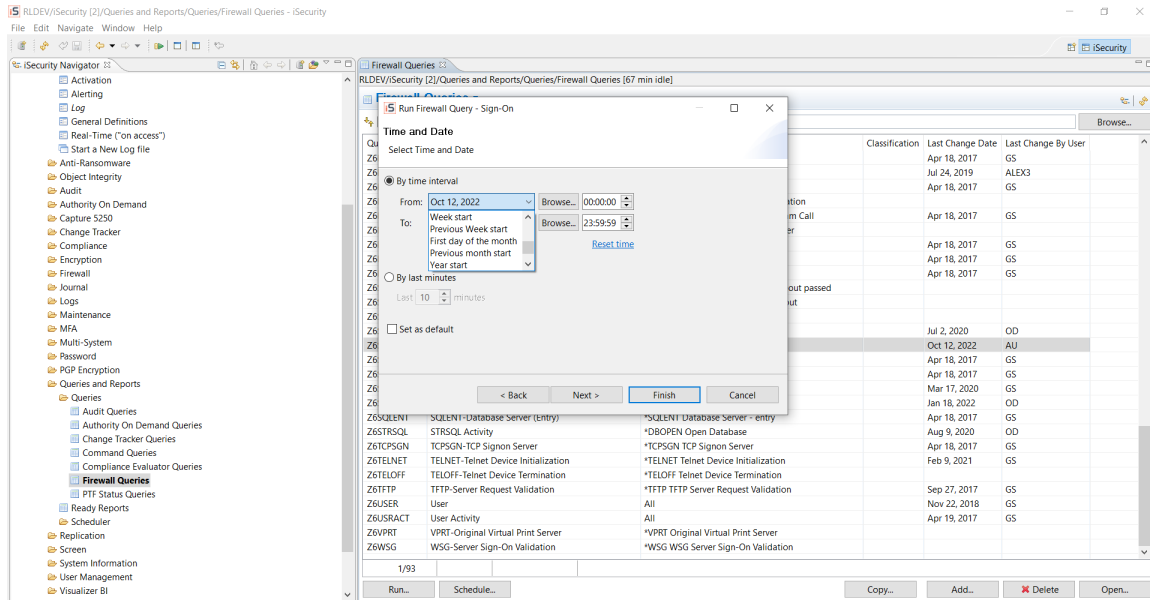
# Scheduling the Query



# Running the Query

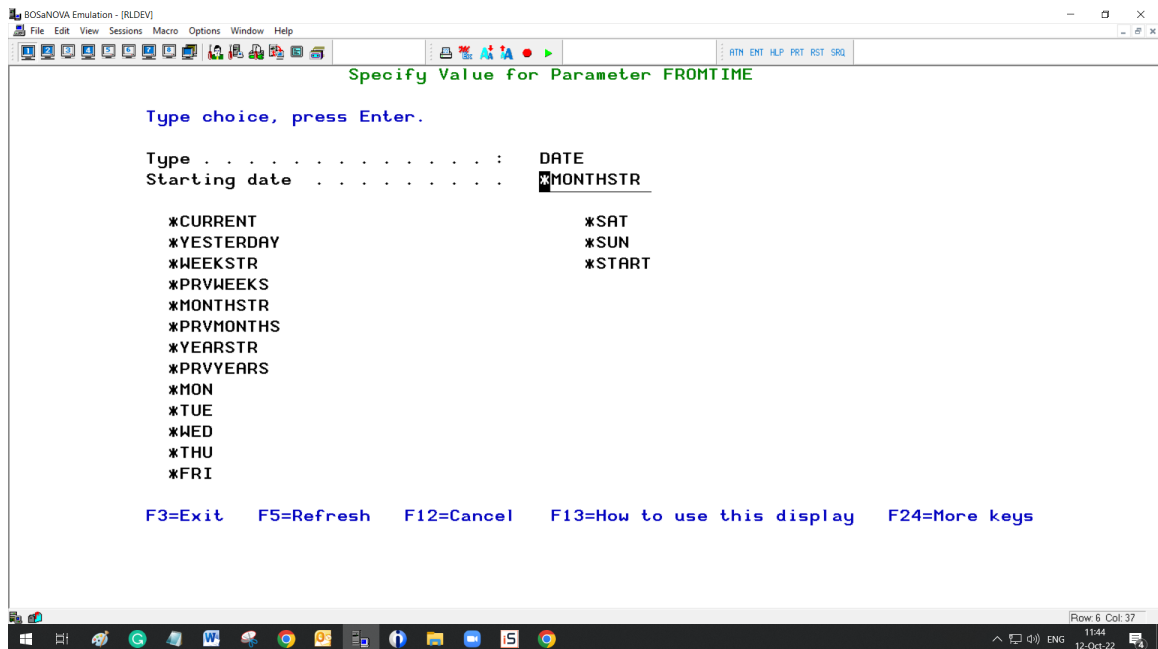


# Dates as Figurative Constants (Week-Start, Month-Start...)

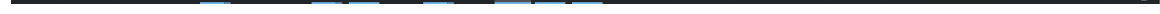


## Dates as Figurative Constants (Week-Start, Month-Start...)

---

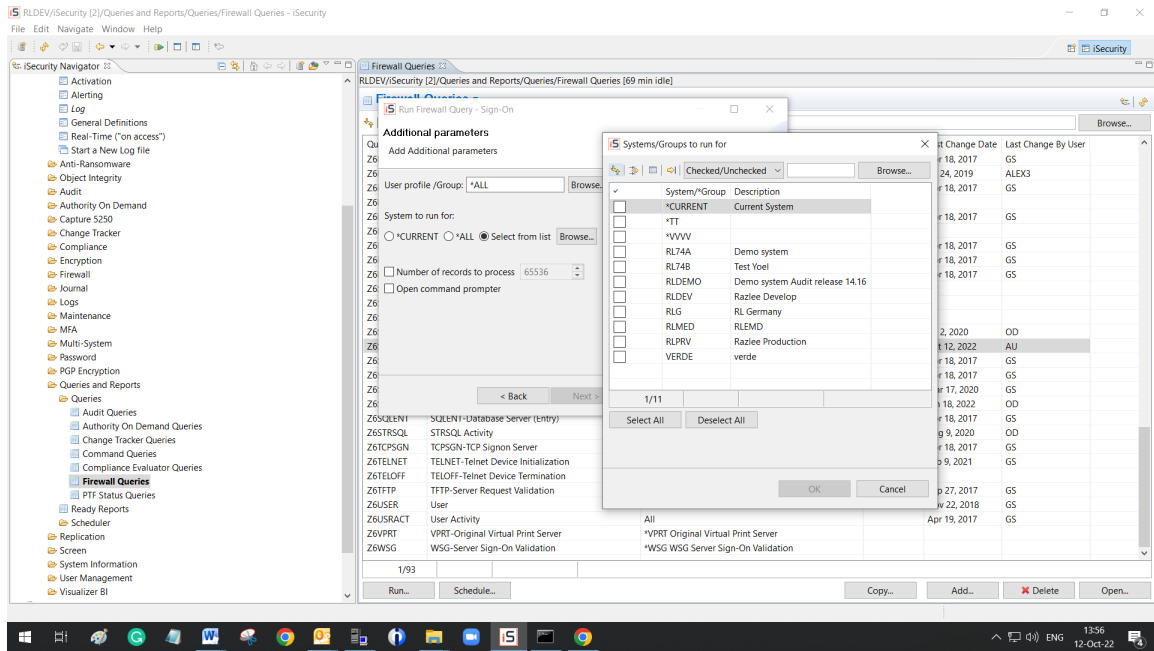






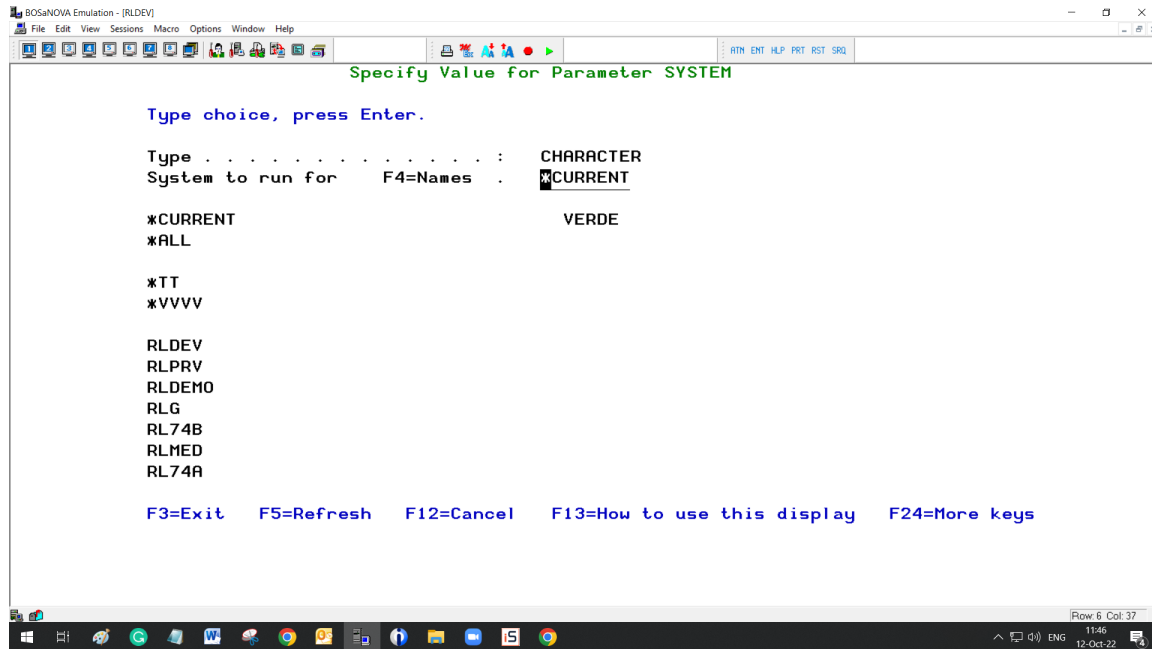


# Selecting LPARS to run for (LPAR Name, Group of LPARS, All LPARS)

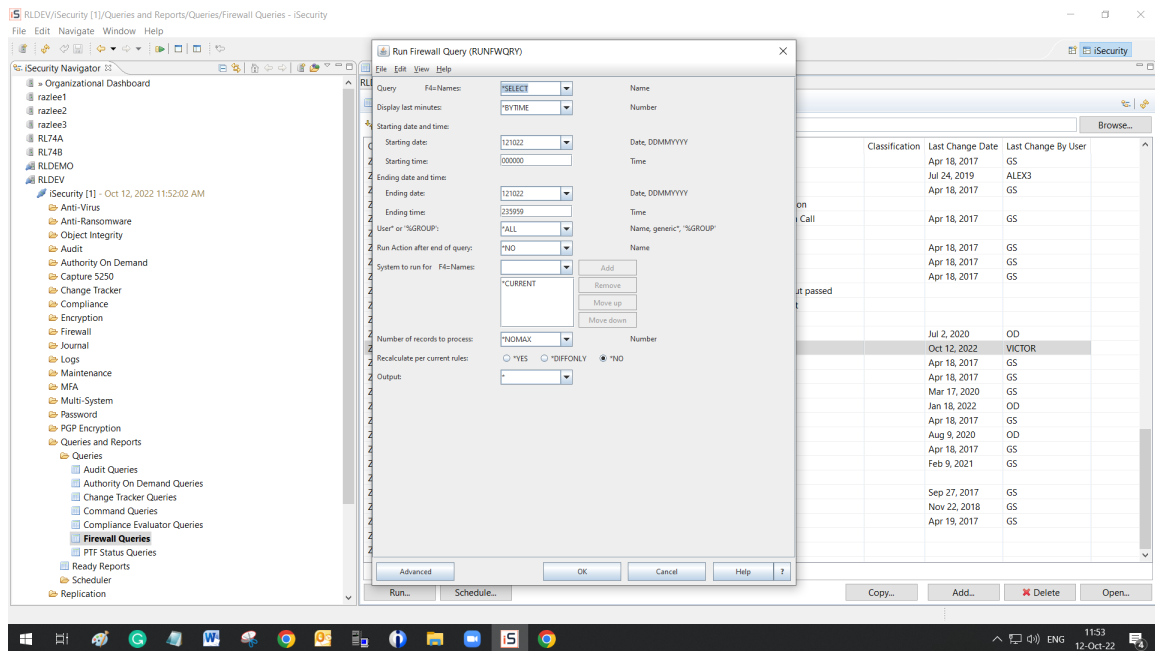


## Selecting LPARS to run for (LPAR Name, Group of LPARS, All LPARS)

---



# All Run Capabilities from the GUI in a Command Prompter



# Query Creation and Modification

---

# General details

BOSaNOVA Emulation - [RLDEV]

File Edit View Sessions Macro Options Window Help

Modify Query Last change date 12/10/22 by user AU

Type choices, press Enter.

Query name . . . . . Z6SIGNON1  
Description . . . . . Sign-On

Type (00=All) . . . . . 42 \*SIGNON Sign-On completed

Time group . . . . . Not Name N=Not in time group

Output format . . . . . 2 1=Tabular and wrap, 2=One line, 9=Log  
If Output=1, Wrap on. 0 Field number, 0=\*AUTO

Add Header / Total . 1 1=Both, 2=Header, 3=Total, 4=Total only,  
9=None

Add Filter / Desc. . 1 1=Filter and description, 2=Filter,  
3=Description, 9=None

Password . . . . .

F3=Exit F4=Prompt F8=Print F12=Cancel

Row: 6 Col: 25

14:17  
12-Oct-22

# Data Filtering

BOSaNOVA Emulation - [RLDEV]

File Edit View Sessions Macro Options Window Help

Filter Conditions

Entry . . . . . 42 \*SIGNON Sign-On completed

Sequence . . . . . 1.0

Subset by text . . . . .

Type conditions, press Enter. Specify OR to start each new group.

Test: EQ, NE, LE, GE, LT, GT, N/LIST, N/LIKE, N/ITEM, N/START, N/PGM

And For N/LIKE: % is "any string"; Case is ignored

Or

Field	Test	Value (If Test=ITEM use F4)
Terminal name	START	QPADEV
User	ITEM	*LMTCPB/*NO
Allow (1=Yes)	EQ	1
Date & Time		yyyy-mm-dd-hh.mm
Name of job		
User of job		
Number of job		
Current user profile		
System name		
User		
Allow (1=Yes)		

More...

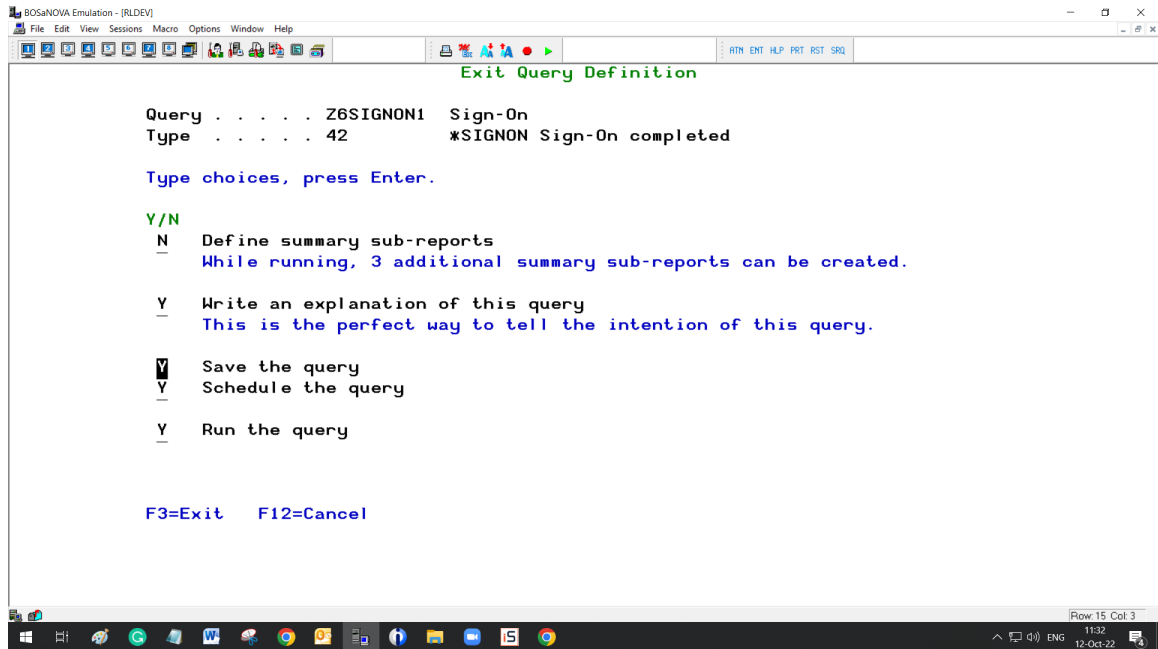
Pink fields are from the generic header. Green fields apply to this type only.

F3=Exit F4=Prompt F6=Insert F8=UC/LC F12=Cancel

Row 9 Col 38

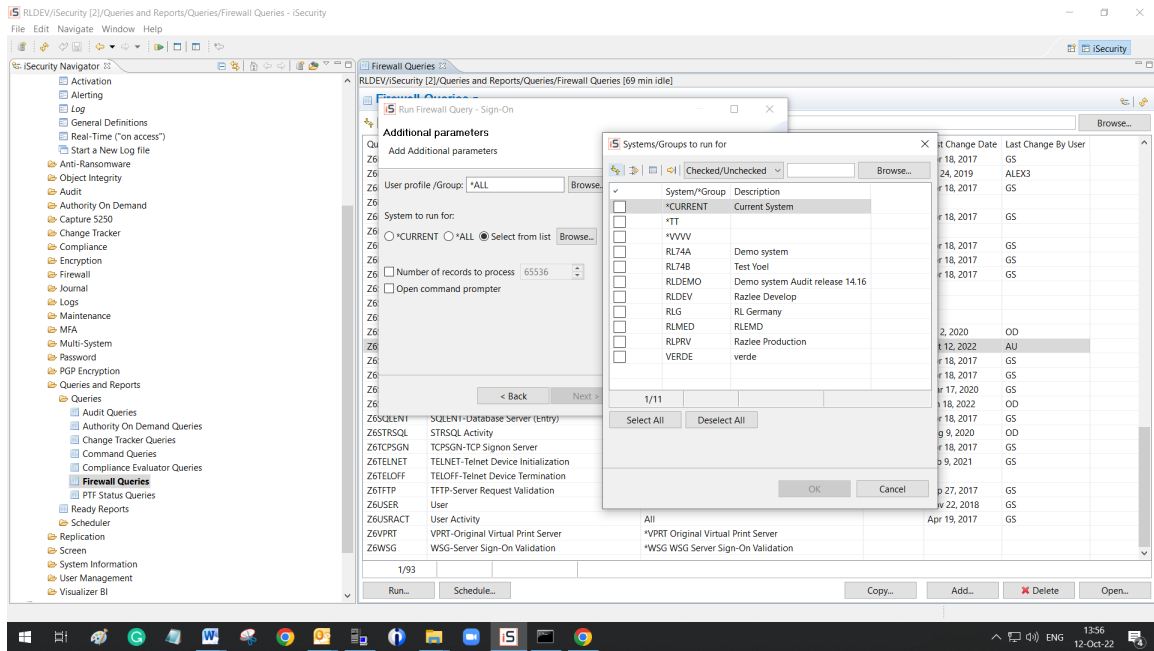
11:30  
12-Oct-22

## Final Screen - Adding Summary Report, Explanation, Scheduling





# Selecting LPARS to run for (LPAR Name, Group of LPARS, All LPARS)



# System Name is automatically added for Multi-LPAR queries

ROSaNOVA Emulation - [RLDEMO]

File Edit View Sessions Macro Options Window Help

RTM ENT HLP PRT RST SRQ

Z6SIGNON1 Sign-On

42 \*SIGNON Sign-On completed

Control: T, B, +/-nnn, Wnnn, F4=Position to field W: 1

RLDEMO 4/10/22 - 10/12/22

System Name	Date & Time	Allow 1=Yes	User	Job Name	IP address
RLDEMO	2022-10-04-10.23.13	1	ADAM	QPADEV000F	1.1.1.129
RLDEMO	2022-10-04-10.43.36	1	ADAM	QPADEV000F	1.1.1.129
RLDEMO	2022-10-04-10.56.15	1	ADAM	QPADEV000F	1.1.1.129
RLDEMO	2022-10-04-10.59.31	1	ADAM	QPADEV000F	1.1.1.129
RLDEMO	2022-10-04-11.00.15	1	ADAM	QPADEV000F	1.1.1.129
RLDEMO	2022-10-04-14.05.32	1	ADAM	QPADEV000F	1.1.1.129
RLDEMO	2022-10-04-09.35.17	1	VICTOR	QPADEV0006	1.1.1.129
RLDEMO	2022-10-06-10.23.04	1	VICTOR	QPADEV0006	1.1.1.129
RLDEMO	2022-10-06-18.19.14	1	VICTOR	QPADEV0009	1.1.1.129
RLDEMO	2022-10-09-13.06.04	1	VICTOR	QPADEV0009	1.1.1.129
RLDEMO	2022-10-12-11.00.16	1	VICTOR	QPADEV0006	1.1.1.129

Bottom

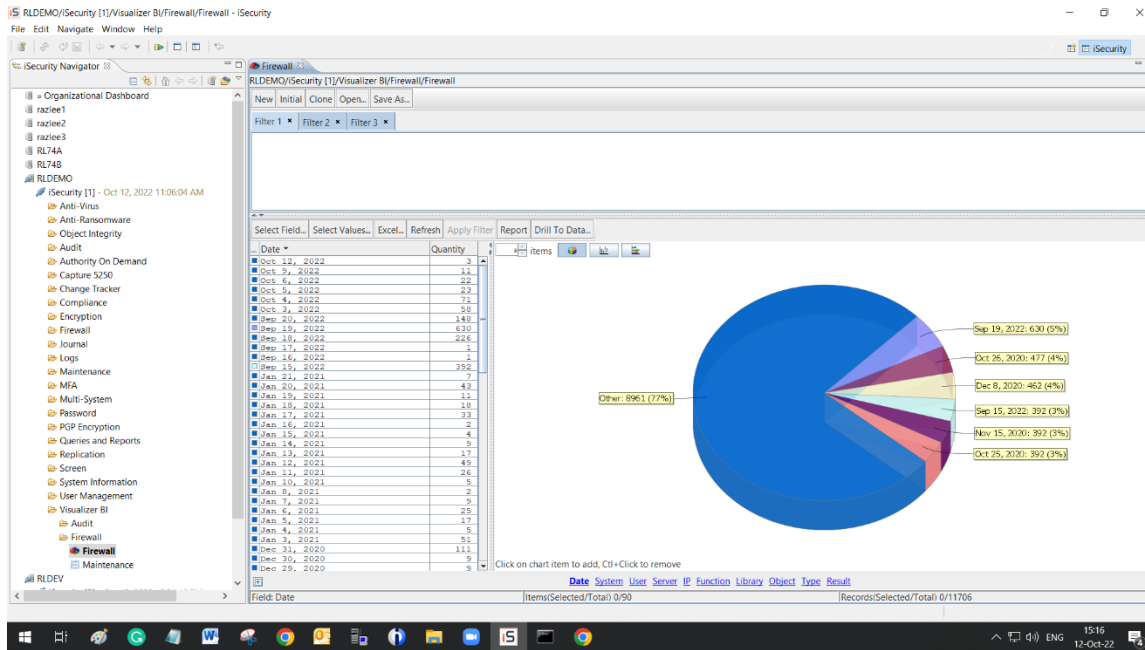
F3=Exit F7=Subset F8=Print F9=Email F10=Entire message F11=Single entry F14=Reorder  
F16=Scan F17=Top F18=Bottom F19=Left F20=Right

Row 3 Col:12 11:20 12-Oct-22

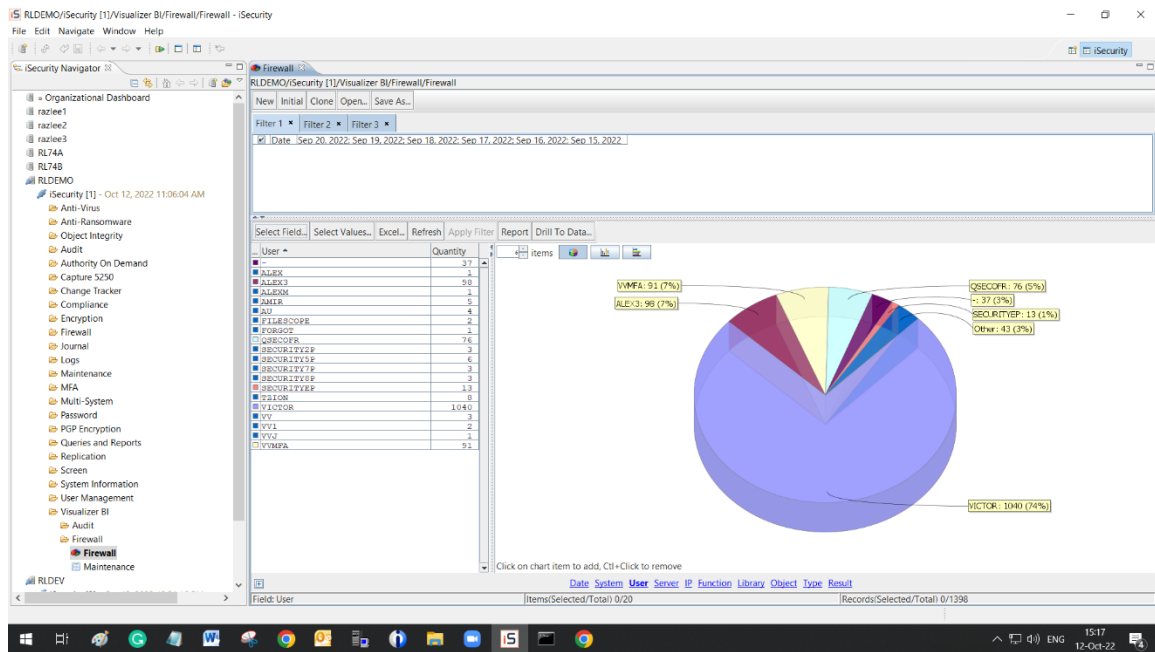
# Business Intelligence over Firewall Data

---

# Activity by Date

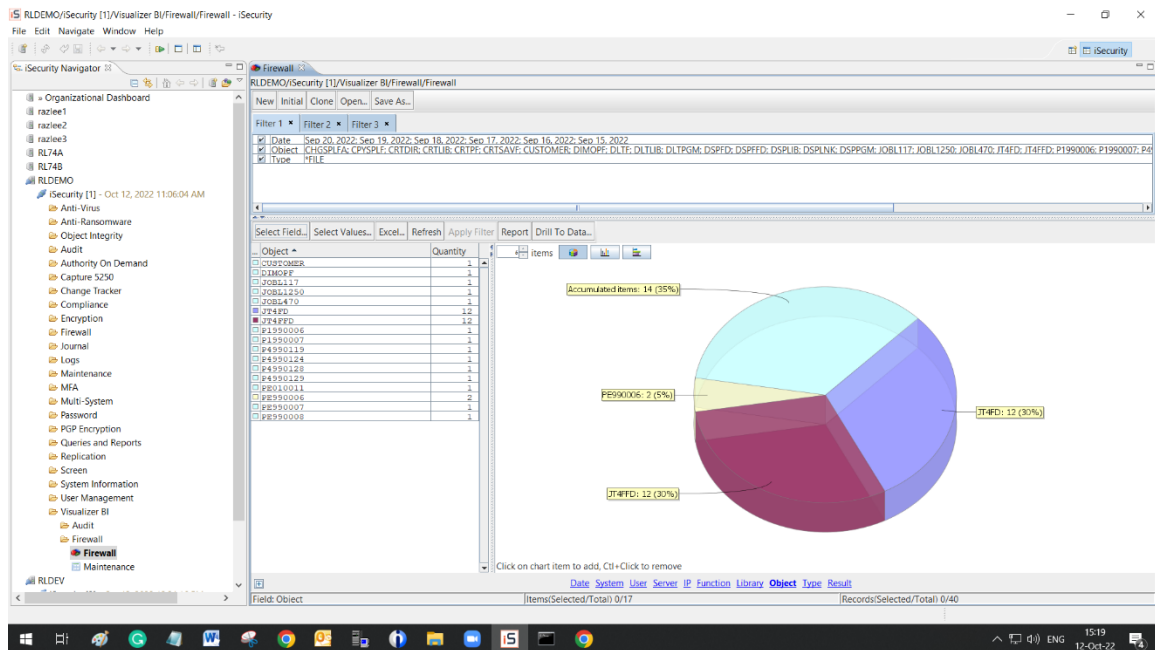


# Activity on September 2022 by User





# Activity by Files



# Activities by Commands

