
Security and Compliance Tools for IBM i

IBM i Exit Point Tool

User's Guide

Terry Ford

IBM Technology Expert Labs

IBM i Exit Point Tool

Overview/Disclaimer	4
Download and Install the Exit Point Tool from IBM	5
Launching the Tool	19
Authorities required to run the IBM i Exit Point Tool	19
The IBM i Exit Point Tool Menu (Go XPT)	20
Option 1 - Work with Exit Point User Access	22
Creating an Exit Point User Access Record	23
Changing an Exit Point User Access Record	24
Copying an Exit Point User Access Record	25
Deleting an Exit Point User Access Record	26
Displaying an Exit Point User Access Record	27
Option 2 - Work with Exit Point Definitions	28
Changing an Exit Point Action	31
Displaying an Exit Point Definition	32
Option 3 - Work with Restricted Commands	33
Creating a Restricted Command	34
Changing a Restricted Command	34
Copy a Restricted Command	35
Display a Restricted Command	35
Adding a Command Restriction to the QIBM_QCA_CHG_COMMAND Exit Point	35
Removing a Command Restriction from the QIBM_QCA_CHG_COMMAND Exit Point	35
Viewing the QIBM_QCA_CHG_COMMAND Exit Point	36
Option 4 - Work with Exit Point Journal Entries	38
Option 5 - Exit Point Reports	39
Option 11 – Start TCP Server	40
Option 12 – End TCP Server	41
Option 21 – Start Host Server	42
Option 22 – Start Prestart Jobs	43
Option 23 – End Host Server Jobs	44
Option 24 – End Prestart Jobs	45
Option 25 – Work with ODBC Related Jobs	46
Option 50 - Display Status of XPT Application (DSPXPTINFO)	47
Option 61 – Set Exit Point Tool Options	48
Option 62 – Retrieve Exit Point Tool Options	48
Option 63 – Send/Install XPT to another System	48

File Server Convenience Options	49
Option 71 – Start QSERVER Subsystem	49
Option 72 – Start NetServer	49
Option 73 – Start File Server	49
Option 81 – End NetServer	49
Option 82 – End QSERVER Subsystem	49
Option 83 – End File Server	49
XPT Menu Convenience Function Keys	50
F2 – View Messages in the QXPTMSQ Message Queue	50
F6 – View Messages in the QXPTMSQ Message Queue	50
F7 - Work with QSYSWRK Subsystem Jobs	50
F8 - Work with QUSRWRK Subsystem Jobs	50
F10 – Work with Registration Information	51
Exit Point Considerations	52
Data Base Server SQL Access (QIBM_QZDA_SQLx)	52
Distributed Program Calls (DPC) and Remote Command (RMTCMD)	55
File Server (QIBM_QPWFS_FILE_SERV)	55
File Transfer Protocol (FTP)	56
Remote Execution (REXEC)	56
TELNET	57
Restricted Commands (QIBM_QCA_CHG_COMMAND)	58
Alternate Audit Journal	59
*ALLOBJ, *NOIPCTL, and IP Filtering	60
Save / Restore of Network Interface Firewall Configuration	62
Report of Users Defined to Exit Points	63
Scheduling Reports	64
View Exit Point Journal Entries (VUXPTJREP)	66
View Exit Point Reports (VUXPTRPTP)	67
Exit Point Job Schedule Example Program 1 (SCDXPTO)	69
Exit Point Job Schedule Example Program 2 (SCDXPT2)	70
Compliance Automation Reporting Tool (CART) Integration	72
Activity Logging of Exit Point Tool Usage	75
Record Layout of Journal Entries created through Exit Point Use	76
Record Layouts of Files used by the Exit Point Tool	78
Restricted Commands Record Layouts	79
Removing the IBM i Exit Point Tool	80
Additional Resources	81
IBM Systems Technology Expert Labs Security	84

Overview/Disclaimer

The IBM i Exit Point Tool (XPT) is a utility to assist those who have the responsibility for maintaining and implementing the security features of the IBM i operating system.

The primary purpose of this tool is to register Exit Points and administer the Users allowed to use them. It should be noted that Object security is the best mechanism for securing your information assets. Object security will protect your applications/files regardless of the interface being used. Customers mistakenly think that Object security is difficult or too time consuming to take on or that Object security requires a thorough data processing analysis to properly classify data and define the roles and responsibilities of the users who use that data. Rather than take a methodical approach beginning with a security policy, many customers have opted to implement Exit points for securing its information assets. In so many ways this is an incorrect approach and further discussion is beyond the scope of this tool or overview. Exit Points, however, do have a place. They are not a complete security solution, but they are a complementary solution along with Object security as part of the overall security architecture of an enterprise.

The current Exits Points administered through the Exit Point Tool are CLI, DDM, Distributed Program Call, DRDA, Client Access Data Queue Server, Client Access File Server, Client Access Print Server File Transfer, FTP inbound, FTP outbound, ODBC/JDBC, REXEC, RMTCMD, Signon Server, TELNET, and TFTP. The following table documents the exit point coverage:

IBM i Exit Point Tool	Exit Point / Network Attribute
CLI DB Connection	QIBM_QSQ_CLI_CONNECT
DDM / DRDA	CHGNETA
Distributed Program Call	QIBM_QZRC_RMT *
FTP Client Request Validation	QIBM_QTMF_CLIENT_REQ
FTP Server Logon	QIBM_QTMF_SVR_LOGON
FTP Request Validation	QIBM_QTMF_SERVER_REQ
Host Servers Data Queue Server	QIBM_QZHQ_DATA_QUEUE
Host Servers File Server	QIBM_QPWFS_FILE_SERV
Host Servers Network Print Server	QIBM_QNPS_ENTRY
ODBC / JDBC / File Transfer	QIBM_QZDA_INIT
Database Server SQL Access	QIBM_QZDA_SQLx
Remote Execution (REXEC) Request Validation	QIBM_QTMX_SERVER_REQ
Remote Command (RMTCMD)	QIBM_QZRC_RMT *
Remote Execution (REXEC) Server Logon	QIBM_QTMX_SVR_LOGON
Host Servers Signon Server	QIBM_QZSO_SIGNONSRV
TELNET Initialization	QIBM_QTG_DEVINIT
TFTP Request Validation	QIBM_QTOD_SERVER_REQ
Command Restrictions	QIBM_QCA_CHG_COMMAND

* Distributed Program Calls and Remote Commands are designed by IBM to share and utilize the same Exit Point interface. Be careful not to deregister the Exit Point when turning on/off either of them so as to not disable the other. Further information in this regard is provided later in this document.

It is worth noting again that there are limitations with this tool and perhaps Exit point programs in general – regardless of who writes them. Exit point programs cannot provide 100% protection for the interfaces they are associated with. To minimize the risk that having these interfaces and host servers active provides, we have implemented a deny-by-default policy. That is, unless a user has been given access to an Exit point through this tool, they will be denied access to the interface. This should be a good first line of defense for potential inappropriate use.

The authors of the contents of this tool have done extensive testing to ensure a safe implementation of its contents. However not every customer environment can be anticipated. This tool is provided AS IS. Neither IBM, IBM Technology Expert Labs, nor its employees or its representatives are responsible for the contents of this tool or the operations of its contents.

Download and Install the Exit Point Tool from IBM

1. Create the XPTTOOL library on target system if it does not exist.

At the command line type **CRTLIB XPTTOOL** then press the **Enter** key.

```
Selection or command  
==> CRTLIB XPTTOOL
```

```
F3=Exit   F4=Prompt   F9=Retrieve   F12=Cancel   F13=Information Assistant  
F23=Set initial menu
```

When completed, you should see confirmation at the bottom of the screen. If the library already exists simply continue.

```
Selection or command  
==>
```

```
F3=Exit   F4=Prompt   F9=Retrieve   F12=Cancel   F13=Information Assistant  
F23=Set initial menu  
Library XPTTOOL created. ←
```

2. Create the XPTBASE Save File in the XPTTOOL Library on the target system.

At the command line type **CRTSAVF XPTTOOL/XPTBASE** then press the **Enter** key.

```
Selection or command  
==> CRTSAVF XPTTOOL/XPTBASE
```

```
F3=Exit   F4=Prompt   F9=Retrieve   F12=Cancel   F13=Information Assistant  
F23=Set initial menu
```

When completed, you should see confirmation at the bottom of the screen

```
selection or command
===>

F3=Exit  F4=Prompt  F9=Retrieve  F12=Cancel  F13=Information Assistant
F23=Set initial menu
File XPTBASE created in library XPTTOOL. ←
```

If the SAVF already exists, you may see the following message at the bottom of the screen.

```
File XPTBASE in library XPTTOOL already exists. +
```

If it does exist, simply clear the contents using the following command

CLRSVF XPTTOOL/XPTBASE then press the **Enter** key.

When completed, you should see confirmation at the bottom of the screen.

```
selection or command
===>

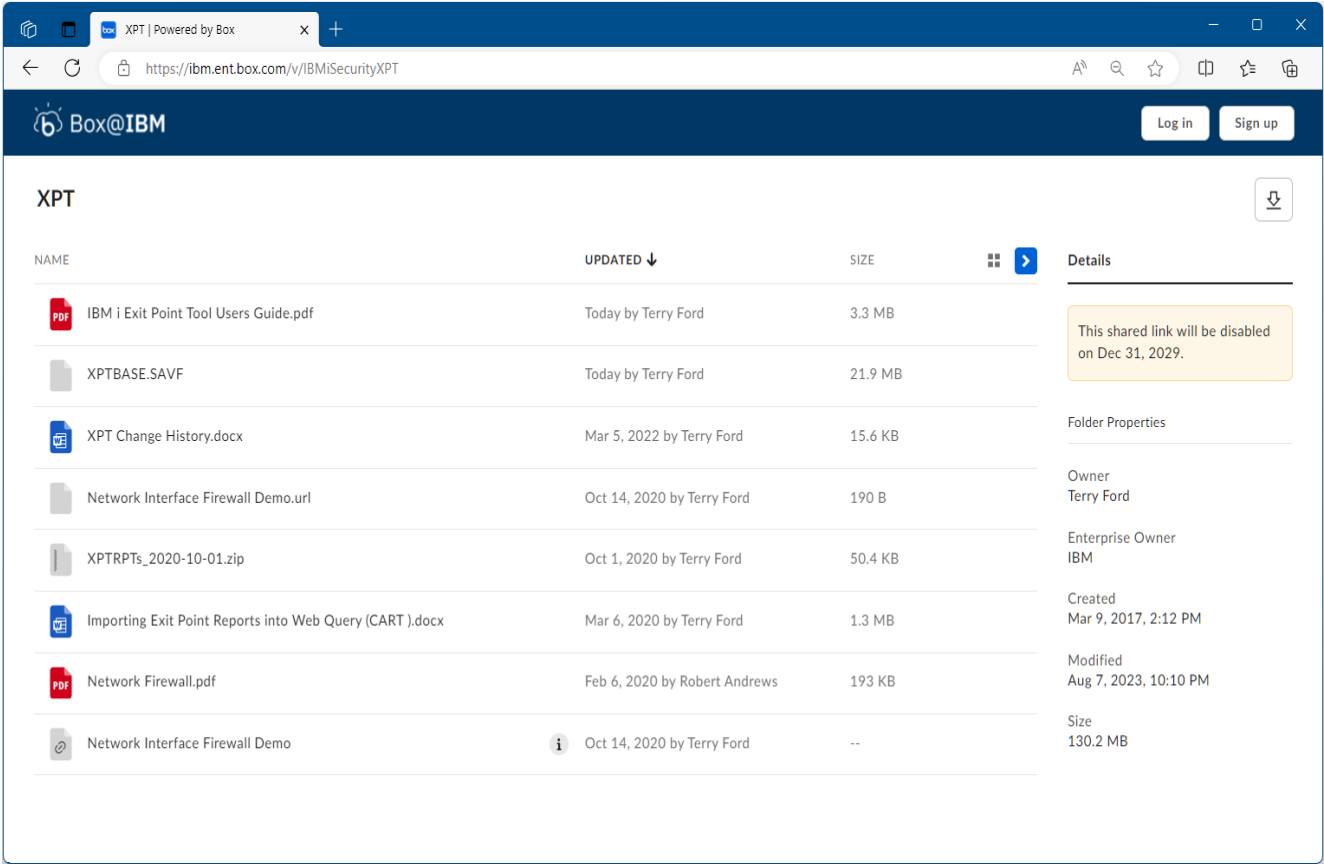
F3=Exit  F4=Prompt  F9=Retrieve  F12=Cancel  F13=Information Assistant
F23=Set initial menu
Save file XPTBASE in library XPTTOOL cleared.
```

3. Download the Exit Point Tool Save File (XPTBASE) from BOX

From your PC’s Internet browser, go to

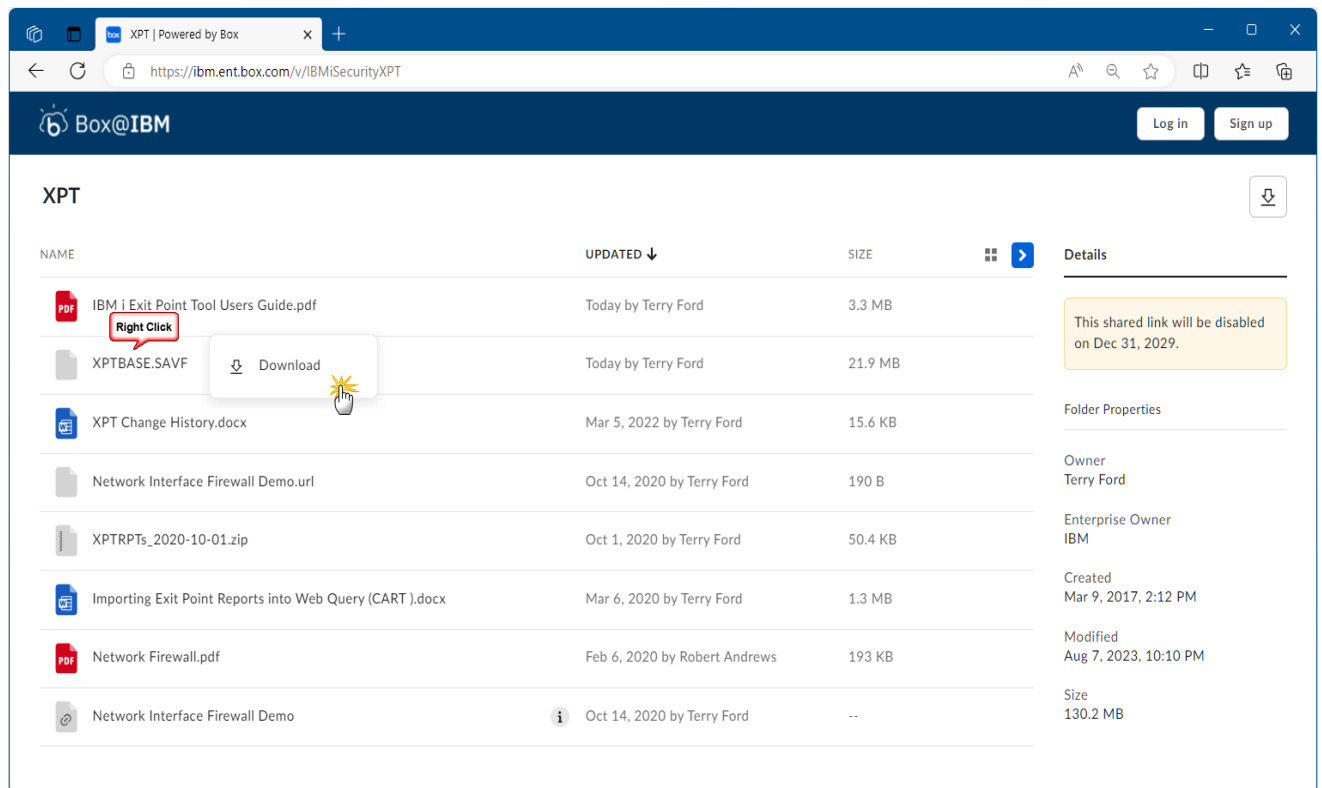
<https://ibm.box.com/v/IBMiSecurityXPT>

Depending on your browser, BOX membership, etc. you might see a browser window similar to the following example:

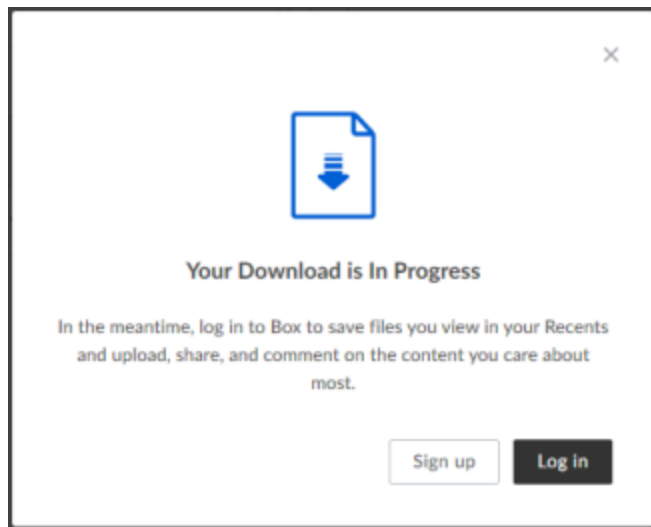


NOTE: It is not necessary to log in or Sign up in order to download these files.

Right click on the **XPTBASE.SAVF** file to save it to your desktop.



A pop up confirmation should appear...



NOTE: It is not necessary to log in or Sign up in order to download these files.

When prompted, choose **Save** when the popup window appears (your popup – if it shows – may appear different than the following). Select a location on your PC where you can easily navigate to in DOS.

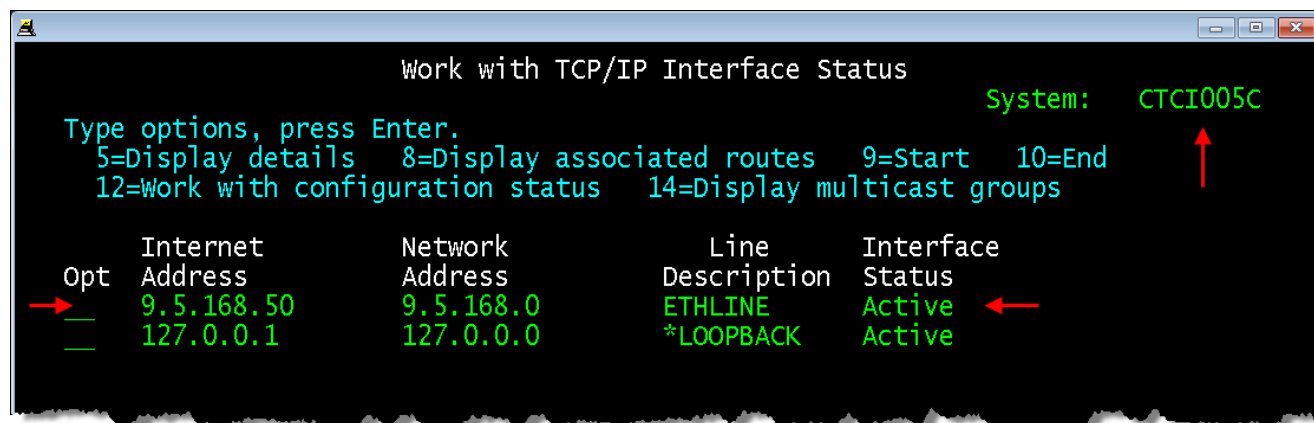
You might find the other files in the BOX Folder of interest as well. Download these as you did the Save File.

4. Transfer the Save File (SAVF), **XPTBASE** to the XPTTOOL library

If you are not sure what your system name or TCPIP Address is, use the following commands from the 5250 session that you are logged on to as an aid:

At the command line type

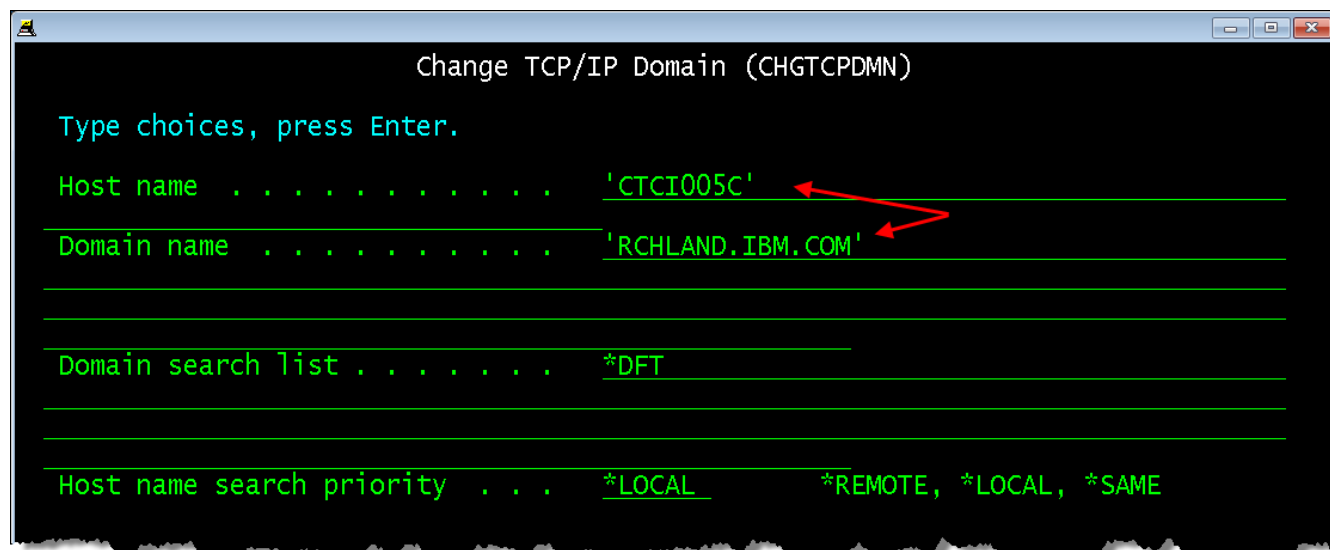
NETSTAT OPTION(*IFC) then press the **Enter** key. You should see a screen similar to the following.



A couple things to notice... On many of the IBM i Menu screens, and on this screen in the upper right hand corner is the **System Name**. Also, You may see multiple adapter interfaces on this screen. Start with the first **non *LOOPBACK TCPIP Address** that is **Active** when performing your File Transfer.

If the TCPIP Address does not work, you can try the domain address of the system. This can be found using the following at the command line:

CHGTCPDMN then press the **F4** key to prompt. You should see a screen similar to the following.



The fully qualified domain name would be the concatenation of the Host Name and the Domain Name. In the above example that would be:

CTCI005C.RCHLAND.IBM.COM

Another suggestion. To be sure that the FTP server is Active use the following at the command line:

NETSTAT OPTION(*CNN) then press the **Enter** key.

You should see a screen similar to the following. This will show you the status of the various network interfaces. For FTP in particular, look for the local port value **ftp-con** and that it is in a **Listen** State. You may have to scroll down several pages.

Work with IPv4 Connection Status

System: CTCV71

Type options, press Enter.
 3=Enable debug 4=End 5=Display details 6=Disable debug
 8=Display jobs

Opt	Remote Address	Remote Port	Local Port	Idle Time	State
—	*	*	ftp-con >	003:12:02	Listen
—	*	*	ssh	060:04:22	Listen
—	*	*	telnet	004:04:41	Listen
—	*	*	smtp	060:04:23	Listen
—	*	*	ntp	000:03:05	*UDP
—	*	*	netbios >	060:04:25	Listen
—	*	*	netbios >	000:00:32	*UDP
—	*	*	netbios >	000:00:32	*UDP


If you do not find it, it may mean that the FTP server is not started. To start FTP, use the following at the command line:

STRTCPSVR SERVER(*FTP) and then press the **Enter** key. Wait a few seconds, and then use the

NETSTAT OPTION(*CNN) command again to see if the FTP Server becomes active.

Now, you will use File Transfer Protocol (FTP) of Windows to transfer the SAVF to the IBM i. On your PC, open up a command prompt and navigate to the directory where you previously saved the **XPTBASE** save file.

```
cd downloads
```



The screenshot shows a Windows Command Prompt window. The title bar at the top reads "C:\WINDOWS\system32\cmd.exe". The window contains the following text:

```
Microsoft Windows [Version 10.0.19043.1466]  
(c) Microsoft Corporation. All rights reserved.  
  
C:\Users\TerryFord>cd downloads  
  
C:\Users\TerryFord\Downloads>
```

Next, use FTP to log into the IBM i using the same user profile and password that you used previously. See the previous paragraphs for finding the target system name.

```
ftp yoursystemname
```

you will then be prompted for your User Id and Password - [use the ID/password supplied to you to log into the system](#) (the password will not be shown as you type it).



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 10.0.19043.1466]
(c) Microsoft Corporation. All rights reserved.

C:\Users\TerryFord>cd downloads

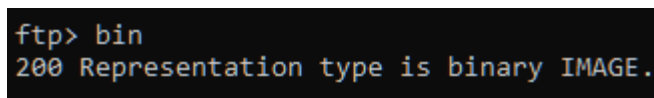
C:\Users\TerryFord\Downloads>

C:\Users\TerryFord\Downloads>ftp ctci005c.rchland.ibm.com
Connected to ctci005c.rchland.ibm.com.
220-QTCP at CTCI005C.RCHLAND.IBM.COM.
220 Connection will close if idle more than 5 minutes.
501 OPTS unsuccessful; specified subcommand not recognized.
User (ctci005c.rchland.ibm.com:(none)): taford
331 Enter password.
Password:
230 TAFORD logged on.
```

After entering the password and pressing **Enter** you should see a visual confirmation that you are logged on.

Next put your FTP session in binary transfer mode with the **bin** command

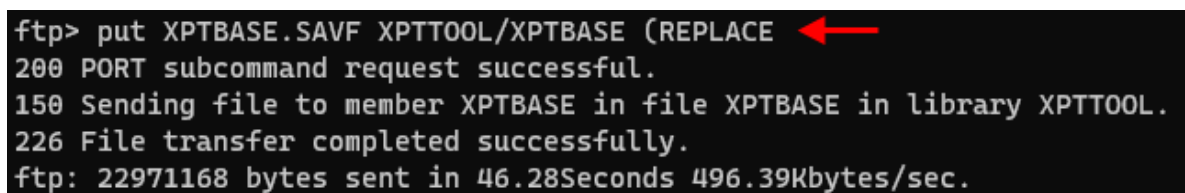
```
bin
```



```
ftp> bin
200 Representation type is binary IMAGE.
```

Then, to transfer the SAVF use the put command

```
put XPTBASE.SAVF XPTTOOL/XPTBASE (REPLACE
```



```
ftp> put XPTBASE.SAVF XPTTOOL/XPTBASE (REPLACE
200 PORT subcommand request successful.
150 Sending file to member XPTBASE in file XPTBASE in library XPTTOOL.
226 File transfer completed successfully.
ftp: 22971168 bytes sent in 46.28Seconds 496.39Kbytes/sec.
```

Wait for the completion message. Depending on your connection speed, the transfer could be a few seconds to a few minutes.

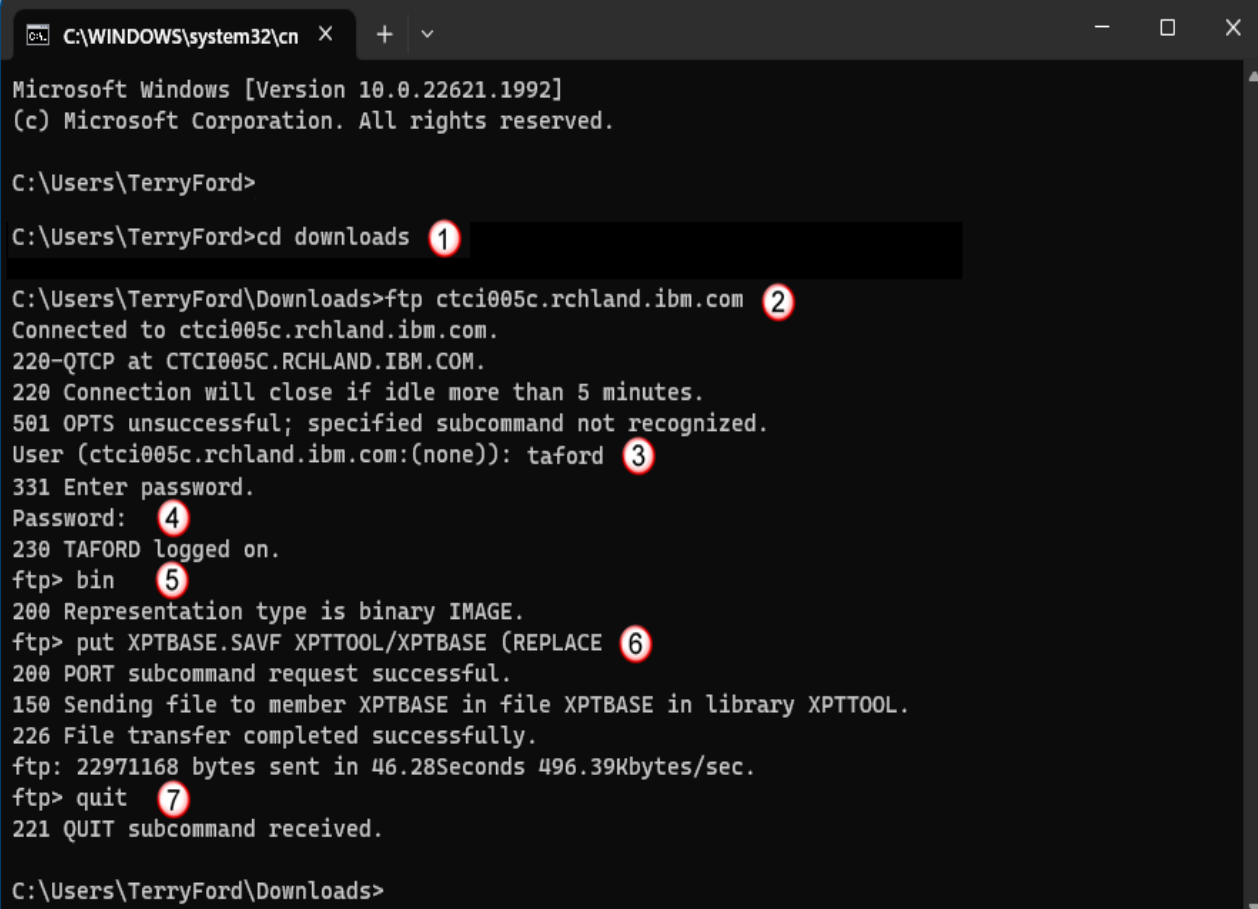
Last, use the quit command to exit FTP and return to the command prompts

Quit

```
ftp> quit
221 QUIT subcommand received.

C:\Users\TerryFord\Downloads>
```

A completed FTP session at the windows command line should look similar to the following:



```
C:\WINDOWS\system32\cmd X + v
Microsoft Windows [Version 10.0.22621.1992]
(c) Microsoft Corporation. All rights reserved.

C:\Users\TerryFord>
C:\Users\TerryFord>cd downloads ①

C:\Users\TerryFord\Downloads>ftp ctci005c.rchland.ibm.com ②
Connected to ctci005c.rchland.ibm.com.
220-QTCP at CTCI005C.RCHLAND.IBM.COM.
220 Connection will close if idle more than 5 minutes.
501 OPTS unsuccessful; specified subcommand not recognized.
User (ctci005c.rchland.ibm.com:(none)): taford ③
331 Enter password.
Password: ④
230 TAFORD logged on.
ftp> bin ⑤
200 Representation type is binary IMAGE.
ftp> put XPTBASE.SAVF XPTTOOL/XPTBASE (REPLACE ⑥
200 PORT subcommand request successful.
150 Sending file to member XPTBASE in file XPTBASE in library XPTTOOL.
226 File transfer completed successfully.
ftp: 22971168 bytes sent in 46.28Seconds 496.39Kbytes/sec.
ftp> quit ⑦
221 QUIT subcommand received.

C:\Users\TerryFord\Downloads>
```

5. Verify the SAVF transferred successfully to the target system ([return to the 5250 emulator session](#)).

At the command line type **DSPSAVF XPTT00L/XPTBASE** then press the **Enter** key.

```
selection or command
==> DSPSAVF XPTT00L/XPTBASE

F3=Exit  F4=Prompt  F9=Retrieve  F12=Cancel  F13=Information Assistant
F23=Set initial menu
```

you should see a screen similar to the following showing the contents of the XPTBASE Save File

```
Display Saved Objects

Library saved . . . . . : QTEMP

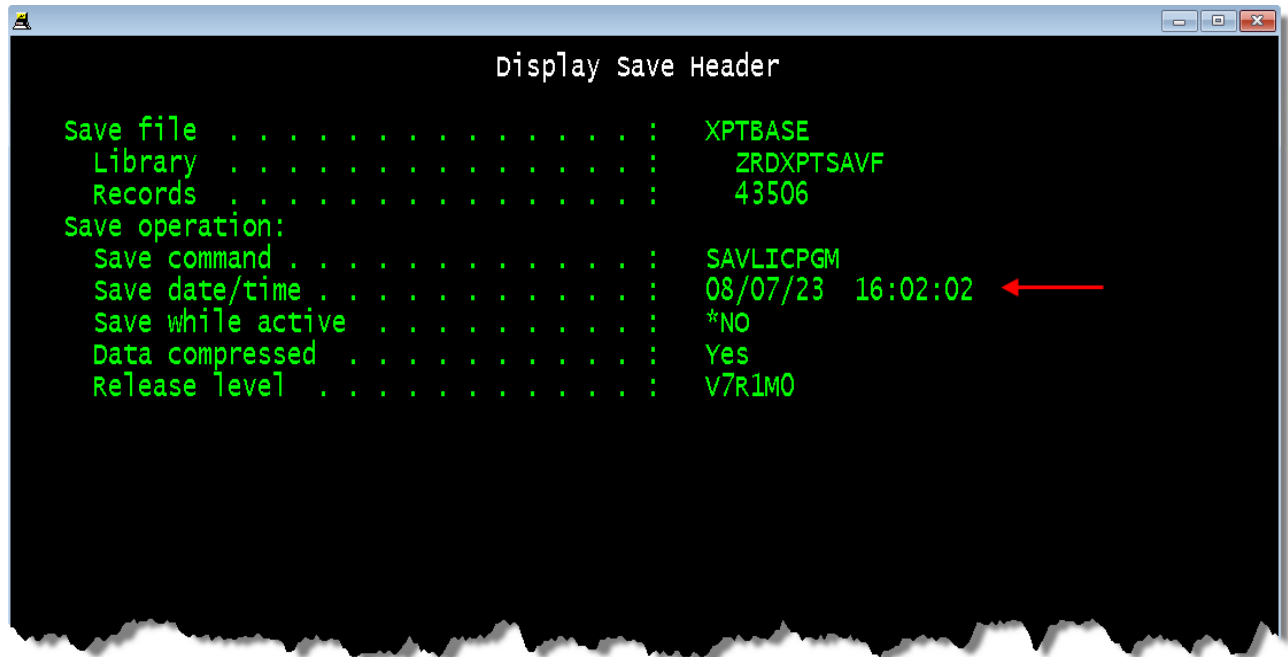
Type Options, press Enter.
5=Display

Opt  Object      Type      Attribute  Owner      Size (K)  Data
--  -
  -  QM.0000      *FILE     SAVF       QSYS        52      YES
  -  QM.0001      *FILE     SAVF       QSYS       348      YES
  -  QM.0002      *FILE     SAVF       QSYS     21536      YES
  -  QLPSVPRDDA  *DTAARA   QSYS         8      YES

F3=Exit  F11=Alternate view  F12=Cancel  F16=Display header

Bottom
```

Use the **F16** key (that is, shift + **F4**) to display the save file header which should look like the following:



The **Save date/time** should be on or after August 7th, 20231 (**08/07/23**)

6. Restore the Licensed Program.

```
RSTLICPGM LICPGM(5ZRDXPT) DEV(*SAVF) SAVF(XPTTOOL/XPTBASE)
```

Read and Accept (F14) the license when prompted...

```
Software Agreement

System: CTCI005c

Licensed program . . . . . : 5ZRDXT
Licensed program option . . . . . : *BASE
Release . . . . . : V2R1M0

IMPORTANT: READ CAREFULLY BEFORE USING THIS PROGRAM

Two agreements are included by reference that must be
accepted with the use of this program.

- When used for Evaluation Purposes

IBM International License Agreement for Evaluation of
Programs

See the following URL for the Terms and Conditions of

F3=Exit  F6=Print  F12=Cancel  F13=select available language  F14=Accept
F16=Decline  F17=Top  F18=Bottom
```

NOTE: This solution requires the Operating System to be at V7R1 or above

This command could take up to 15 minutes to complete - please be patient and note that the system will not accept keyboard input while the RSTLICPGM command is running. Wait until this process has completed and you see the following message at the bottom of the screen.

```
selection or command
===>

F3=Exit  F4=Prompt  F9=Retrieve  F12=Cancel  F13=Information Assistant
F23=Set initial menu

*PGM objects for product 5ZRDXT option *BASE release *FIRST restored. +
```

7. Obtain a license key for the Exit Point Tool and apply the key to the system.

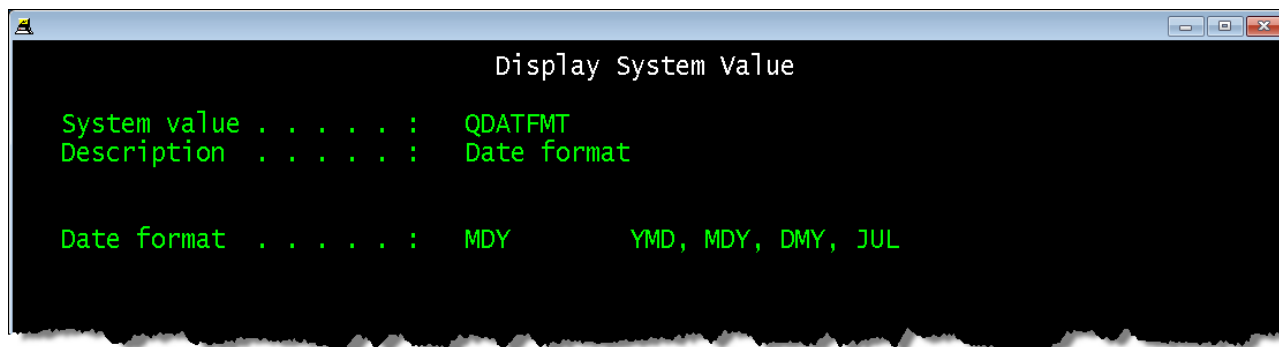
If you haven't done it already, contact one of the following IBM Lab Services representatives to obtain a license key for the trial. [The system serial number will be required to generate the license key.](#)

- Robert Andrews, robert.andrews@us.ibm.com, 507-253-4205
 - Thomas Barlen (Europe), barlen@de.ibm.com, +49-6701-205084
 - Terry Ford, taford@us.ibm.com, 507-253-7241
- Before proceeding, there are two pieces of system information you need to know. The system date format and the system date separator character. Use DSPSYSVAL at the command line to retrieve these settings.

First, the system date format is found in system value **QDATFMT**. At the command line type

DSPSYSVAL SYSVAL(QDATFMT)

then press the **Enter** key. You should see a screen similar to the following.

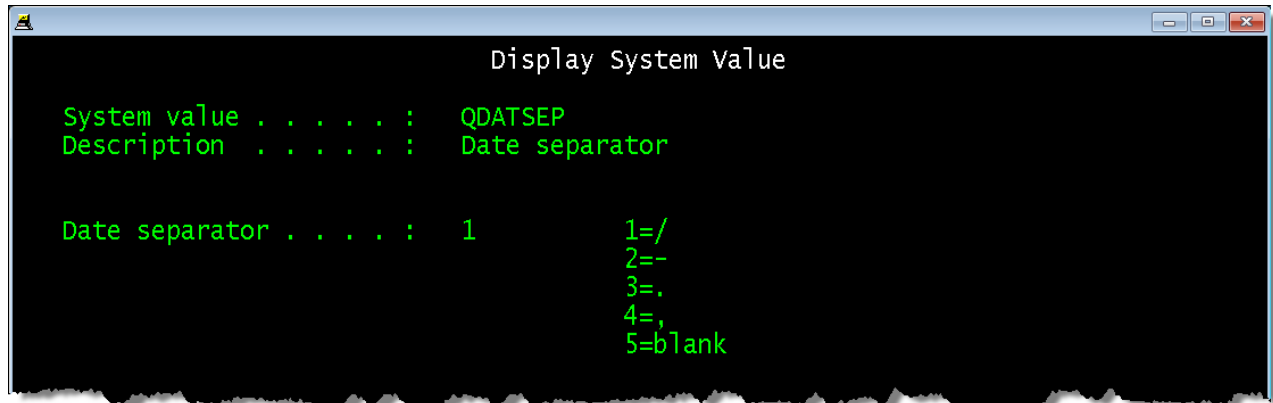


Take note, in the above example, the date format is Month-Date-Year which means a date of March 5th, 2022 is represented by the values 03 (the month of March), 05 (the 5th day), and 2022 for the year – so **03052022**. Some interfaces allow to use only the last two digits of the year.

Second, the system date separator is found in system value **QDATSEP**. At the command line type

```
DSPPSYVAL SYSVAL(QDATSEP)
```

then press the **Enter** key. You should see a screen similar to the following.



In the above example the **1** represents the date separator **/**. So when entering the date on certain system prompts (using the March 5th, 2022 example) you would use **03/05/2022**. If the date separator value is **5** you would use **03052022**.

The following is an example of license information that might be provided (note that the date format is NOT necessarily in the format that the system value is set as described in the previous steps):

Product ID	Serial#	Key Expiry	License Key
5ZRDXT-V2-5050	1012345	2024-12-25	05EA8E 1F235A 4F6C01

Once you have a key, use the following IBM i command to register the key:

```
ADDLICENSE LICKEYINP(*PROMPT) PRDID(5ZRDXT) LICTRM(V2) FEATURE(5050)
SERIAL(your_systems_serial_number) LICKEY(IBM_provided_license_key)
USGLMT(*NOMAX) EXPDTE(expiration_date_provided_by_IBM)
```

For example...

```
ADDLICENSE LICKEYINP(*PROMPT) PRDID(5ZRDXT) LICTRM(V2) FEATURE(5050)
SERIAL(1012345) LICKEY(05EA8E 1F235A 4F6C01) USGLMT(*NOMAX)
EXPDATE('12/25/2024')
```

Add License Key Information (ADDLICENSE)

Type choices, press Enter.

License key input	LICKEYINP	> *PROMPT
Product identifier	PRDID	> 5ZRDXT
License term	LICTRM	> V2
Feature	FEATURE	> 5050
System serial number	SERIAL	> 1012345
Processor group	PRGRP	> *ANY
License key:	LICKEY	
Characters 1 - 6		> 05EA8E
Characters 7 - 12		> 1F235A
Characters 13 - 18		> 4F6C01
Usage limit	USGLMT	> *NOMAX
Expiration date	EXPDATE	> '12/25/2024'
Vendor data	VNDATA	> *NONE

Bottom

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

NOTE: The expiration date must be entered in the format of the system value QDATEFMT (YMD, MDY, DMY, JUL) AND must include the appropriate separator from QDATESEP.

After you press Enter, you will see confirmation that the license key was added

selection or command

===>

F3=Exit F4=Prompt F9=Retrieve F12=Cancel F13=Information Assistant
F23=Set initial menu

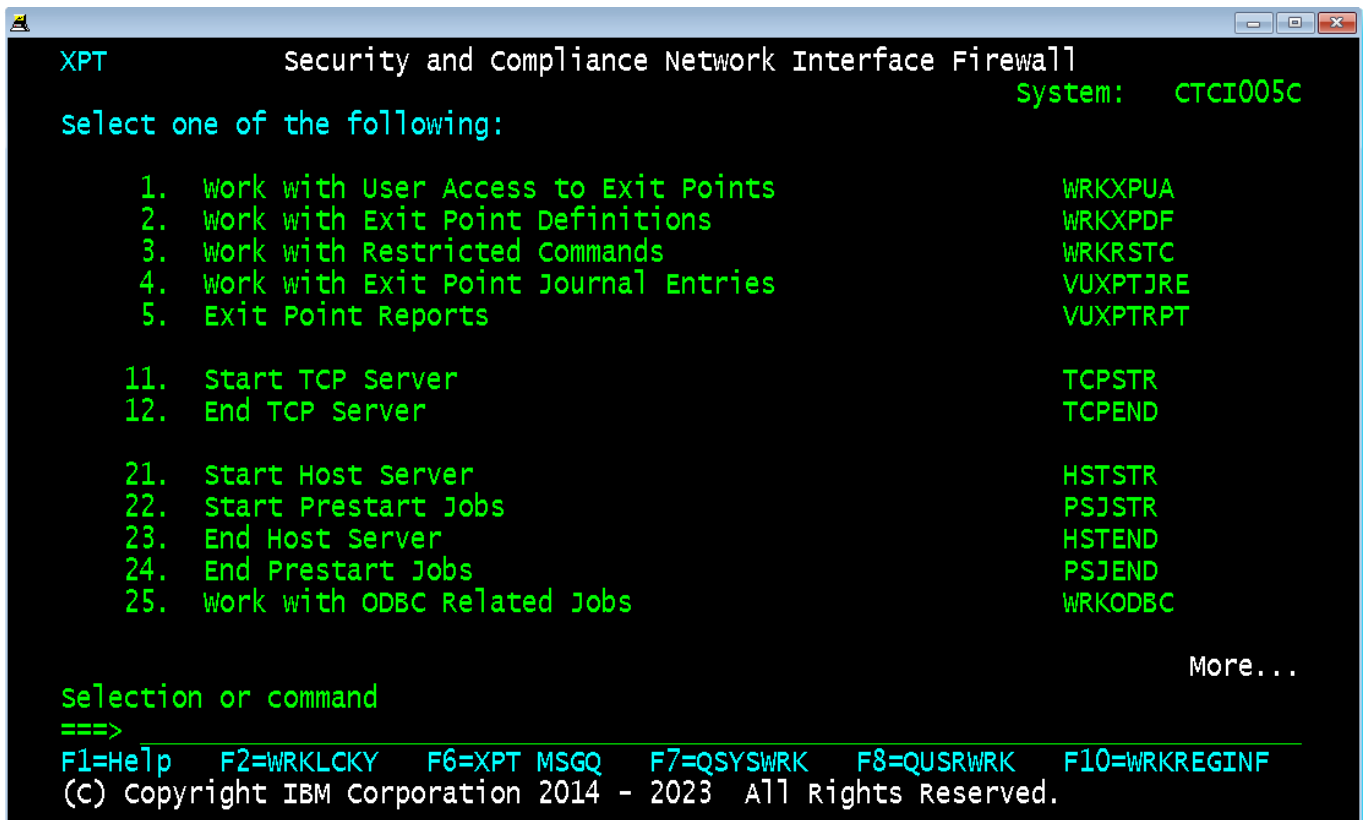
License key information added for 5ZRDXT.

Launching the Tool

To Launch the tool, at the command line type

- CHGCURLIB QZRDSECXPT <ENTER>
- GO XPT <ENTER> A screen similar to the following should appear

NOTE: During installation, the shortcut **XP** was placed in library QSYS. You can also navigate to the XPT Menu from any other IBM i menu. This command will also change your current library to QZRDSECXPT.



```
XPT                      Security and Compliance Network Interface Firewall
                                                                    System:  CTCI005c
select one of the following:

    1.  Work with User Access to Exit Points          WRKXPUA
    2.  Work with Exit Point Definitions             WRKXPDF
    3.  Work with Restricted Commands                WRKRSTC
    4.  Work with Exit Point Journal Entries         VUXPTJRE
    5.  Exit Point Reports                          VUXPTRPT

    11. Start TCP Server                             TCPSTR
    12. End TCP Server                               TCPEND

    21. Start Host Server                           HSTSTR
    22. Start Prestart Jobs                         PSJSTR
    23. End Host Server                             HSTEND
    24. End Prestart Jobs                           PSJEND
    25. Work with ODBC Related Jobs                  WRKODBC

More...

selection or command
==>
F1=Help  F2=WRKLCKY  F6=XPT MSGQ  F7=QSYSWRK  F8=QUSRWRK  F10=WRKREGINF
(C) Copyright IBM Corporation 2014 - 2023 All Rights Reserved.
```

Before you use the Exit Point Tool for the first time you will need to enable the application with the license key that was previously sent to you in an email.

Authorities required to run the IBM i Exit Point Tool



The user running this tool must have *ALLOBJ, *AUDIT, *IOSYSCFG and *SECADM special authorities or must be QSECOFR or an equivalent profile.

The IBM i Exit Point Tool Menu (Go XPT)

The first page of the Exit Point Tool menu is where most work in defining the exit points of interest is found. The first few options help you manage and control the Exit Point interfaces. The next few help you report on usage of the Exit Points. The remainder of the options on the page utilities with small modifications of the standard IBM commands for administrating the network interfaces. The modifications were made to minimize the complexity of the commands that may intimidate new users who wish to perform these tasks for their company. Generally, once the Exit Point programs have been registered you will not need to re-register them again.

```
XPT Security and Compliance Network Interface Firewall
System: CTCI005c

select one of the following:

1. Work with User Access to Exit Points      WRKXPUA
2. Work with Exit Point Definitions          WRKXPDF
3. Work with Restricted Commands            WRKRSTC
4. Work with Exit Point Journal Entries     VUXPTJRE
5. Exit Point Reports                      VUXPTRPT

2 11. Start TCP Server                      TCPSTR
   12. End TCP Server                      TCPEND

   21. Start Host Server                   HSTSTR
   22. Start Prestart Jobs                PSJSTR
   23. End Host Server                   HSTEND
   24. End Prestart Jobs                PSJEND
   25. Work with ODBC Related Jobs        WRKODBC

More...

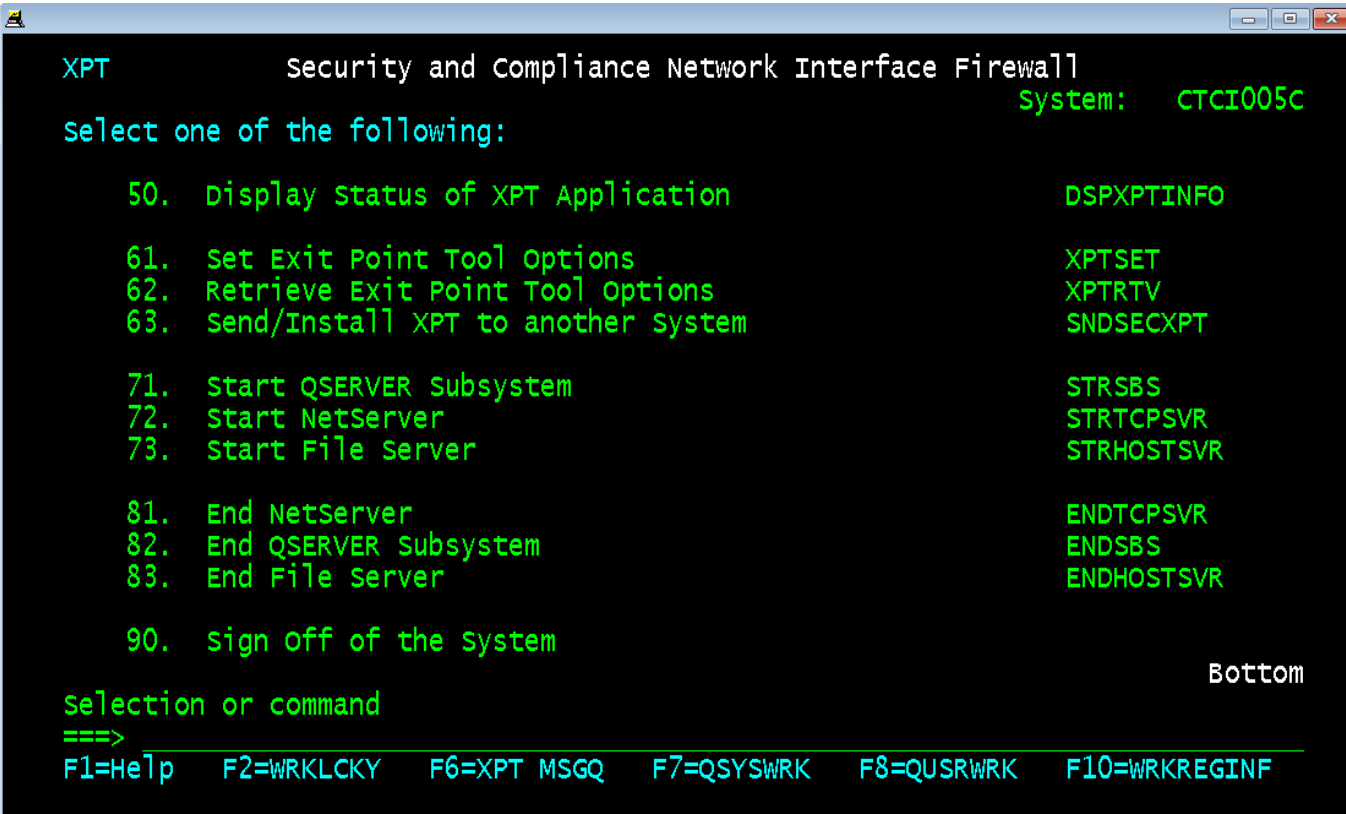
selection or command
===>
F1=Help  F2=WRKLCKY  F6=XPT MSGQ  F7=QSYSWRK  F8=QUSRWRK  F10=WRKREGINF
(c) copyright IBM Corporation 2014 - 2023 All Rights Reserved.
```

Both pages of the IBM i Exit Point Tool menu can be broken down as follows.

- 1 The items to the left side of the menu define the menu options to choose from.
- 2 To the far right of each of the menu options is a column that shows the commands that are used to run the menu options. As long as the QZRDSECXPT library is in the library list you could run these commands.
- 3 At the bottom of the menu are some convenience functions created to simplify troubleshooting. See the section on [XPT Menu Convenience](#) options.

NOTE: If you type the command, it may appear differently than when selecting the option.

The second page of the Exit Point Tool menu is where the configuration options are set, as well as some convenience option options for working with the File Server Exit Point.



```
XPT Security and Compliance Network Interface Firewall
System: CTCI005c
select one of the following:

50. Display Status of XPT Application          DSPXPTINFO
61. Set Exit Point Tool Options              XPTSET
62. Retrieve Exit Point Tool Options          XPTRTV
63. Send/Install XPT to another System        SNDSECXPT

71. Start QSERVER Subsystem                  STRSBS
72. Start NetServer                          STRTCPSVR
73. Start File Server                        STRHOSTSVR

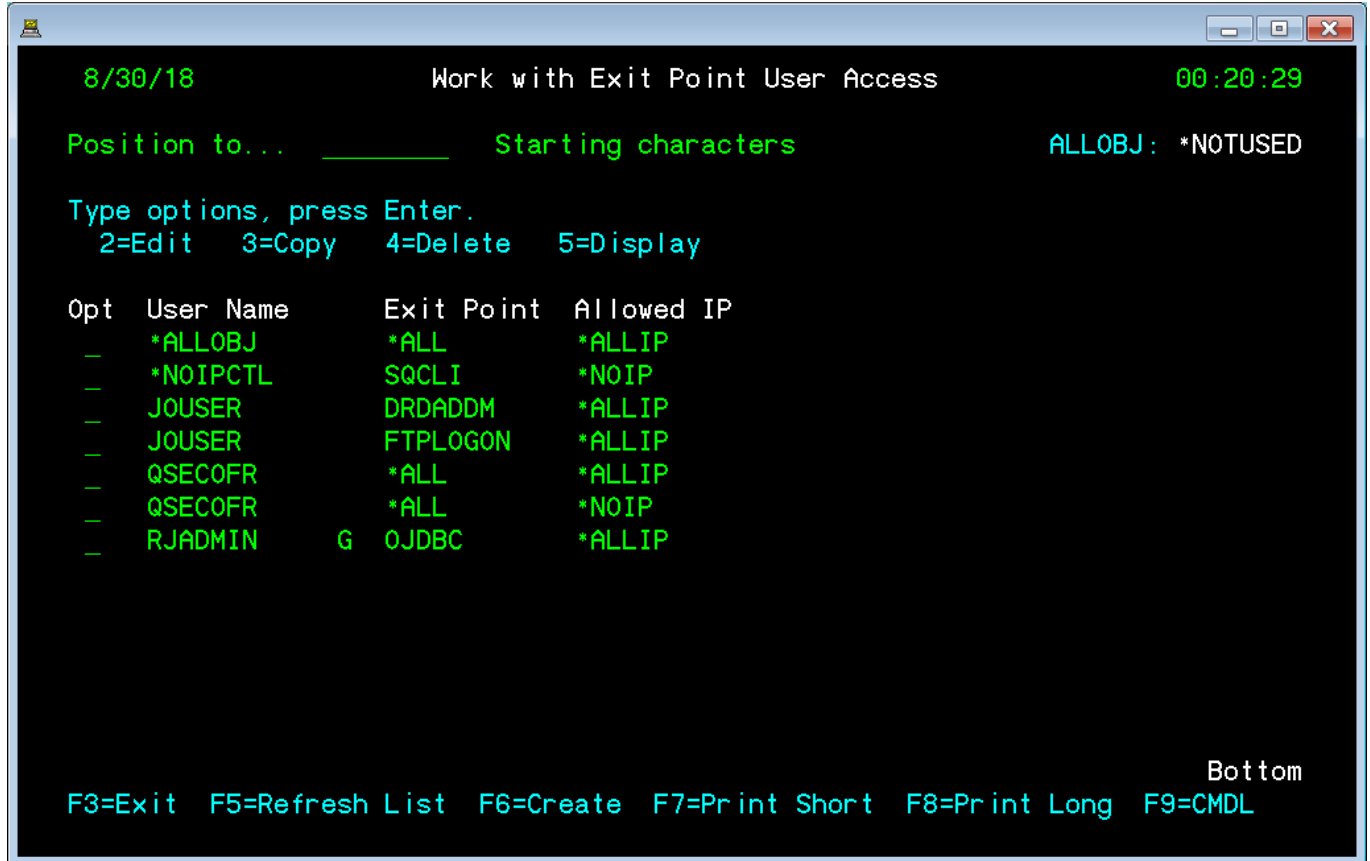
81. End NetServer                            ENDTCPVR
82. End QSERVER Subsystem                    ENDSBS
83. End File Server                          ENDHOSTSVR

90. Sign Off of the System

Bottom
Selection or command
===>
F1=Help  F2=WRKLCKY  F6=XPT MSGQ  F7=QSYSWRK  F8=QUSRWRK  F10=WRKREGINF
```

Option 1 - Work with Exit Point User Access

Once the license key has been registered you are ready to start working with User access to Exit points. By default, once the Exit point interfaces have been activated, all Users will be denied access to the Exit Point. Only those Users that are defined by the Exit Point Tool will be allowed to transfer files through the Exit point. After selecting this menu option you should see a screen similar to the following but with different or no data:



```
8/30/18                      Work with Exit Point User Access                      00:20:29
Position to... _____ Starting characters                      ALLOBJ: *NOTUSED

Type options, press Enter.
  2=Edit  3=Copy  4=Delete  5=Display

Opt  User Name      Exit Point  Allowed IP
--  -
  *ALLOBJ          *ALL          *ALLIP
  *NOIPCTL         SQCLI          *NOIP
  JOUSER          DRDADDM        *ALLIP
  JOUSER          FTPLOGON       *ALLIP
  QSECOFR          *ALL          *ALLIP
  QSECOFR          *ALL          *NOIP
  RJADMIN          G 0JDBC        *ALLIP

Bottom
F3=Exit  F5=Refresh List  F6=Create  F7=Print Short  F8=Print Long  F9=CMDL
```

The screen is relatively easy to work with. There are 4 key areas to note on the screen.

- 1 This area displays the Exit points that a User has access to and any IP Address restrictions they may have. Note the **G** next to **RJADMIN** in the above example. This indicates that the User is a Group Profile.
- 2 In this area are typical commands you might see on any IBM i application screen. **F3** exits this screen, **F5** refreshes or resets the list, and **F9** presents a command line. Unique to this application is **F6** which will allow you to create an Exit Point user access record, **F7** / **F8** prints reports of the Exit Point Users.
- 3 This area provides four ways to work with the users defined to Exit points. You can Edit a record, Copy a record as a model for a different user, copy as a base record for the same user with different parameters, Delete a record or Display a record.
- 4 If the number of Exit Point users grows beyond what can be displayed on this screen the additional pages can be viewed by scrolling thru the pages using the **PAGE UP** or **PAGE DOWN** keys. You can also use the Position To field to reset the screen to the user of your choice by keying in that USERID and pressing the **Enter** key.

Creating an Exit Point User Access Record

To create a User Access record, press **F6** from the Work with Exit Point User Access screen. You will see a screen similar to the following but with different or no data:

```

Create Exit Point User Access (CRTXPUA)

Type choices, press Enter.

Select User Name . . . . . BRUCE          User Name, *ALLOBJ, *NOIPCTL
Select Exit Point Definition . . DSTPGMC   *ALL, DRDADDM, DSTPGMC, DTA...
Allowed IPv4 Address . . . . . 9.5.157.158

-

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

MA  A  13/037
```

The screen is quite simple to use. Add the following information:

1. The User profile name. The user must be defined on the system and could be a user or a group profile.
2. The Exit point you wish to allow the User to access. This can be either one Exit Point or *ALL of them. Use F4 in the Exit Point Definition field to display all Exit Points available.
3. The IP Address that a User is allowed to access the Exit Point from. The default value is *ALLIP which allows the user to access the specified exit point from any IP Address.

For IP address masking, the mask should be able to handle the following per octet

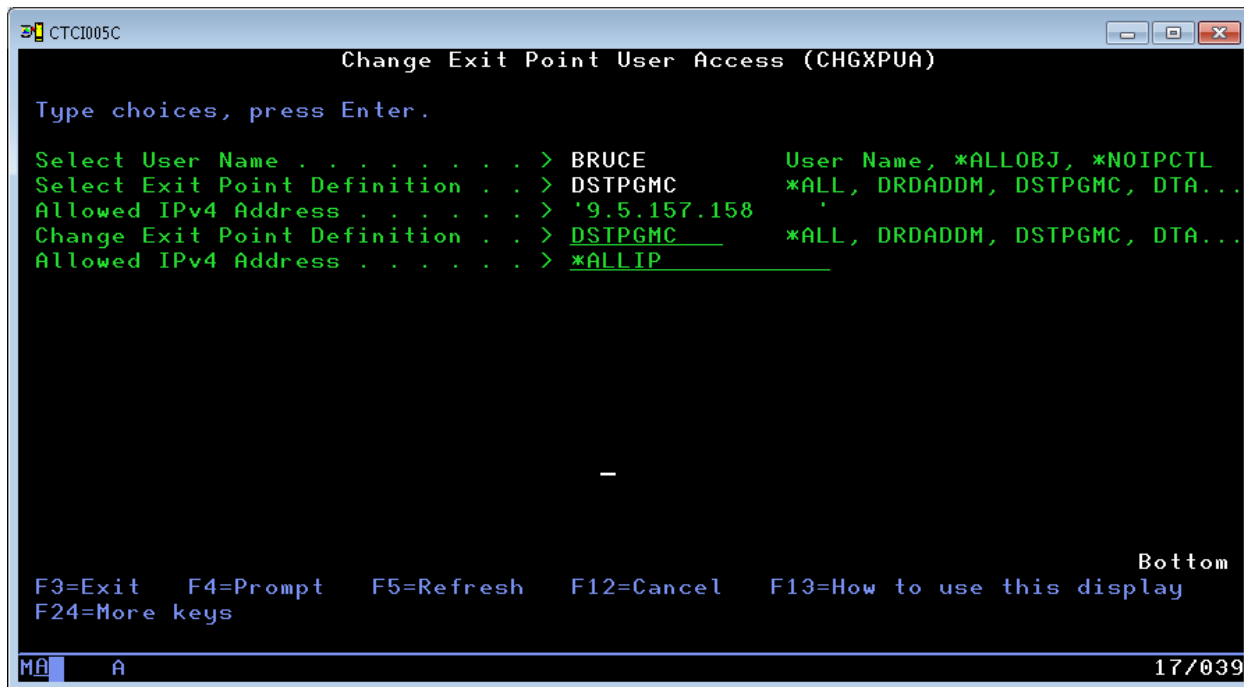
*nn	---	>	*10	=	10, 110, 210
*n	---	>	*5	=	5, and any valid address ending in 5, ie., 15, 25, 35 ... 125, 135 ... 205, 215 ...
n*	---	>	1*	=	1, 10 thru 19, 100 thru 199
nn*	---	>	12*	=	12, 120 thru 129
n	---	>	1*5	=	105, 115, 125, 135 ... 195
*	---	>		=	any valid address 0 thru 255

4. To create the User Access record, press **Enter**. Otherwise, press **F3** or **F12** to cancel.

NOTE: A user can have multiple access records for different Exit points. Each record must be unique for a user.

Changing an Exit Point User Access Record

To change a User Access record, select option 2 for the User from the Work with Exit Point User Access screen. You will see a screen similar to the following but with different data:



```
CTCI005C
Change Exit Point User Access (CHGXPUA)

Type choices, press Enter.

Select User Name . . . . . > BRUCE      User Name, *ALLOBJ, *NOIPCTL
Select Exit Point Definition . . > DSTPGMC  *ALL, DRDADD, DSTPGMC, DTA...
Allowed IPv4 Address . . . . . > '9.5.157.158  '
Change Exit Point Definition . . > DSTPGMC  *ALL, DRDADD, DSTPGMC, DTA...
Allowed IPv4 Address . . . . . > *ALLIP

-

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

MA A 17/039
```

This screen is quite simple to use. On this screen the original User Access record is displayed for reference. To change a User Access record, provide the following information:

1. The Exit point you wish to allow the User to access. This can be either one Exit Point or *ALL of them. Use F4 in the Exit Point Definition field to display all Exit Points available.
2. The IP Address that a User is allowed to access the Exit Point from. This can be a specific IP Address or *ALLIP which allows the user to access the specified exit point from any IP Address.

For IP address masking, the mask should be able to handle the following per octet

```
*nn      --->  *10  = 10, 110, 210
*n       --->  *5   = 5, and any valid address ending in 5,
              ie., 15, 25, 35 ... 125, 135 ... 205, 215 ...
n*       --->  1*   = 1, 10 thru 19, 100 thru 199
nn*      --->  12*  = 12, 120 thru 129
*n*      --->  1*5  = 105, 115, 125, 135 ... 195
*        --->      = any valid address 0 thru 255
```

3. To change the User Access record, press **Enter**. Otherwise, press **F3** or **F12** to cancel.

NOTE: A user can have multiple access records for different Exit points. Each record must be unique for a user.

Copying an Exit Point User Access Record

To copy a User Access record, select option 2 for the User from the Work with Exit Point User Access screen. You will see a screen like the following but with different data:

```
Copy Exit Point User Access (CPYXPUA)

Type choices, press Enter.

Select User Name . . . . . > BRUCE           User Name, *ALLOBJ, *NOIPCTL
Select Exit Point Definition . . > DSTPGMC      *ALL, DRDADD, DSTPGMC, DTA...
Allowed IPv4 Address . . . . . > '9.5.157.158'
Copy to User Name . . . . . > IAFORD          User Name, *ALLOBJ, *NOIPCTL
Select Exit Point Definition . . > DSTPGMC      *ALL, DRDADD, DSTPGMC, DTA...
Allowed IPv4 Address . . . . . > '9.5.157.158'

-

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

Bottom

MA  A  17/035
```

This screen is also simple to use. On this screen the original User Access record is displayed for reference. To copy a User Access record, provide the following information:

1. The User profile name. This can be the same user or a different user.
2. The Exit point you wish to allow the User to access. This can be either one Exit Point or *ALL of them. Use F4 in the Exit Point Definition field to display all Exit Points available.
3. The IP Address that a User is allowed to access the Exit Point from. This can be a specific IP Address or *ALLIP which allows the user to access the specified exit point from any IP Address.

For IP address masking, the mask should be able to handle the following per octet

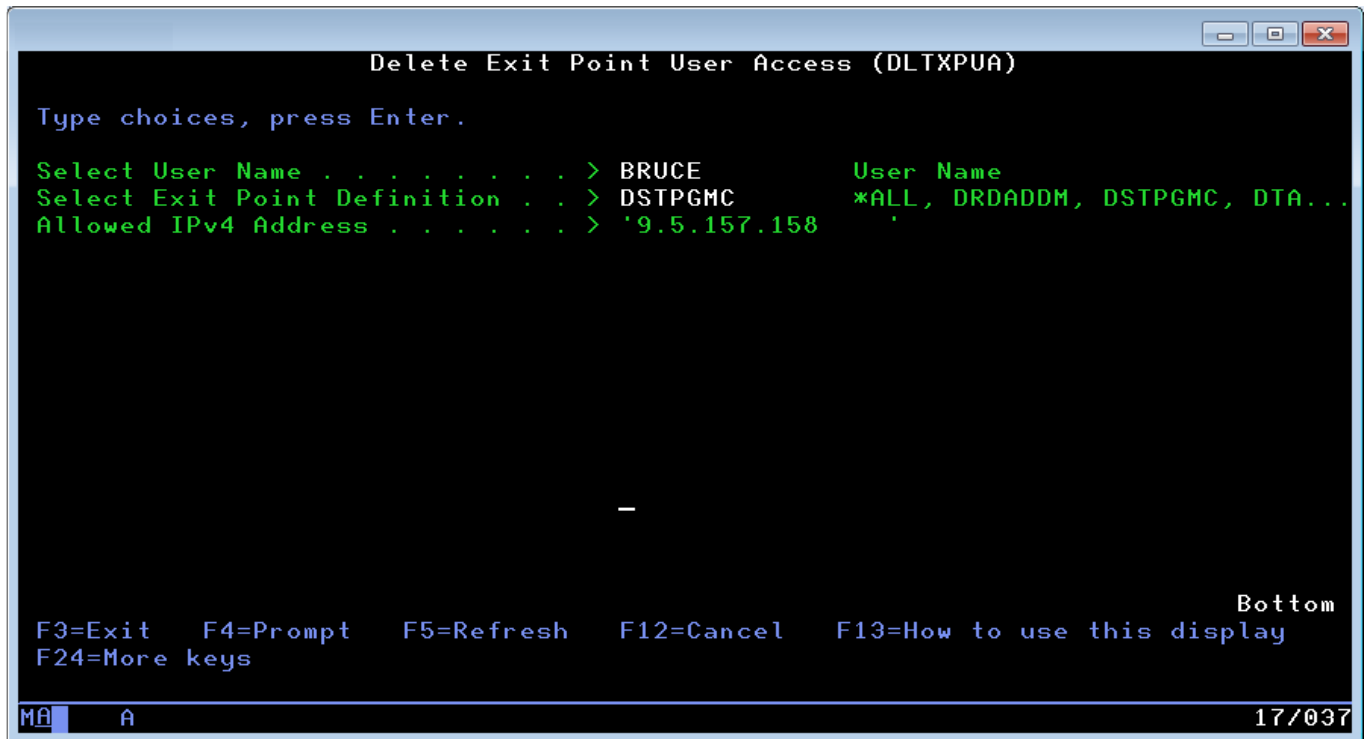
```
*nn      --->  *10  = 10, 110, 210
*n       --->  *5   = 5, and any valid address ending in 5,
                ie., 15, 25, 35 ... 125, 135 ... 205, 215 ...
n*       --->  1*   = 1, 10 thru 19, 100 thru 199
nn*      --->  12*  = 12, 120 thru 129
*n*      --->  1*5  = 105, 115, 125, 135 ... 195
*        --->      = any valid address 0 thru 255
```

4. To copy the User Access record, press **Enter**. Otherwise, press **F3** or **F12** to cancel.

NOTE: A user can have multiple access records for different Exit points. Each record must be unique for a user.

Deleting an Exit Point User Access Record

To delete a User Access record, select option 4 for the User from the Work with Exit Point User Access screen. You will see a screen similar to the following but with different data:



This screen is also simple to use. On this screen the original User Access record is displayed for reference.

To delete the User Access record, press **Enter**. Otherwise, press **F3** or **F12** to cancel.

Displaying an Exit Point User Access Record

To display a User Access record, select option 5 for the User from the Work with Exit Point User Access screen. You will see a screen similar to the following but with different data:

```
Display Exit Point User Access (DSPXPUA)

Type choices, press Enter.

Select User Name . . . . . > BRUCE      User Name
Select Exit Point Definition . . > DSTPGMC *ALL, DRDADDM, DSTPGMC, DTA...
Allowed IPv4 Address . . . . . > '9.5.157.158'

-

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

Bottom

MA  A  16/033
```

This screen is also simple to use. On this screen the original User Access record is displayed for reference.

To exit the display of the User Access record, press **Enter**, **F3** or **F12**.

Option 2 - Work with Exit Point Definitions

Generally, once the Exit points have been registered you will not need to use this screen. When you select this menu option you will be presented with a screen similar to the following

8/10/23 Work with Exit Point Definitions 10:09:41

Position to: 5 Filter Definitions: 5 ALLOBJ: *NOTUSED

Type options, press Enter.

5=Display 8=Add Exit 9=Remove Exit N=*ON F=*OFF L=*LOGONLY W=WRKREGINF 3

Opt	Definition	Exit Point Name	Exit Point Description	Status
—	DRDADDM	CHGNETA	DRDA/DDM Logon	*ADDED2NAT
—	DSTPGMC	QIBM_QZRC_RMT	Distributed Program Call	2
1	DTAQRVR	QIBM_QZHQ_DATA_QUEUE	Host Servers DATAQ Server	2
—	FILESVR	QIBM_QPWFS_FILE_SERV	Host Servers File Server	
—	FTPCLNRQ	QIBM_QTMF_CLIENT_REQ	FTP Client Request Validation	
—	FTPLOGON	QIBM_QTMF_SVR_LOGON	FTP Server Logon	*ADDED2XPT
—	FTPSVRQ	QIBM_QTMF_SERVER_REQ	FTP Request Validation	
—	HSTPRT	QIBM_QNPS_ENTRY	Host Server Net Print Server	
—	OJDBC	QIBM_QZDA_INIT	DB Logon - ODBC/JDBC/File XFR	*ADDED2XPT
—	ONDB1	QIBM_QZDA_NDB1	Native DB Ops via ODBC/JDBC	
—	OROI1	QIBM_QZDA_ROI1	Object INFO REQs via ODBC/JDBC	
—	OSQL1	QIBM_QZDA_SQL1	DB Server SQL Access	*ADDED2XPT
—	OSQL2	QIBM_QZDA_SQL2	DB Server SQL Access	

F3=Exit F5=Refresh F6=Create Definition U=View Exit Users 6 Q=SQL2 Access 7 More... 4

The screen is relatively easy to work with. There are several key areas to note on the screen.

1 This area displays the Exit points that are available to work with. The key area to note in the list is to the far right column, called Status. If you see ***ADDED2XPT** that means the Exit point program is attached to the Exit point and ready to use. If the status is missing the Exit point program is not ready for use. A key point is that the Exit point program could be ready to use, but not necessarily activated. **Generally, in order for an Exit point program to work the associated TCP or Host Server must be stopped and restarted. Also, in the case of Host Servers, the Prestart Jobs for QZDASOINIT in subsystem QUSRWRK may also need to be stopped and restarted. However, this is not a hard and fast rule. TELNET for example when added will take affect immediately upon the next user signing on. Because of this inconsistency, the default "Action" for an Exit Point is *LOGONLY.** This ensures that a restriction isn't put in place without your proper preparation.

NOTE: Whatever the Status of an Exit point program at the time the TCP or Host Server is stopped and restarted is what will be in effect. For example, if the Exit point status is *ADDED2XPT and the TCP or HOST server is stopped and restarted, then the Exit point program will be active, logging and/or restricting user access. If for example, the Exit point status is blanks and the TCP or HOST server is stopped and restarted, then the Exit point program will **not** be active.

The Exit point program can be removed or added back any number of times without restarting the TCP or Host Server. However, the adding or removing of the Exit point program does not necessarily take effect until the TCP or Host Server is stopped and restarted.

2 This area is for reference only to indicate the “Action” status for an Exit Point Definition. The “Action” is seen as a color in the “Definition” column of the Exit Point list. When an Exit Point program is added to an Exit Point (Option 8), as previously mentioned it is placed in ***LOGONLY** mode by default. You will notice that the color of the Exit Point turns to **Blue** on the screen. Entries that are in **Green** indicate that the entry is active and restricting users according to User Access records (if *ADDED2XPT is present in the Status column). If an entry in the **Definition** column is **Red**, it means the entry is registered to the Exit Point, but that User Access restrictions are being bypassed. The following illustration should provide clarity to the colors and their meanings:

Opt	Definition	Exit Point Description	Status	
—	FTPCLNRQ	FTP Client Request Validation	*ADDED2XPT	← registered and actively restricting
—	FTPLOGON	FTP Server Logon	*ADDED2XPT	← registered but only logging
—	FTPSVRRQ	FTP Request Validation	*ADDED2XPT	← registered but turned off - no logging
—	FILESVR	Host Servers File Server		← not registered, not active, no logging

3 Generally, it is not recommended to Change or Delete any of the Exit point definitions defined on this screen unless changing the Exit Point Action or **directed by an IBM Technology Service representative**. See “[Changing the Exit Point Action](#)” section. The other three options you will use are the options to Add/Remove Exit Programs and to display the Exit Point status via WRKREGINF (except DRDADDMM which uses DSPNETA)

To add the Exit program simply select the Exit point definition you wish to add the Exit point program to and select it using option 8. When finished you should notice the Status of the Exit point definition change from blanks to ***ADDED2XPT** and the color of the Exit Point definition in the **Definition** column change to **Blue**.

To remove the Exit program simply select the Exit point definition you wish to remove the Exit point program from and select it using option 9. When finished you should notice the Status of the Exit point definition change from ***ADDED2XPT** to blanks and the color of the Exit Point definition in the **Definition** column change to **Green**.

4 Additional Exit Point Definitions can be accessed by pressing the **PAGE DOWN** key.

5 As mentioned, additional Exit Point Definitions can be accessed by pressing the **PAGE DOWN** key or positioning the list to the desired Exit Point Definition. Key in the desired Exit Point Definition and press **Enter**. The list will be position so the desired Exit Point Definition is listed first on the display. Additionally, you can use the **Filter Definitions:** field to type the Exit Point definition or the first few characters of a definition or definition(s) to subset the listed Exit Definitions to only those Exit Point definitions that begin with those characters. For example, typing FTP in the **Filter Definitions:** field will only show:

Position to: _____ Filter Definitions: FTP ALLOBJ: *NOTUSED

Type options, press Enter.

5=Display 8=Add Exit 9=Remove Exit N=*ON F=*OFF L=*LOGONLY W=WRKREGINF

Opt	Definition	Exit Point Name	Exit Point Description	Status
—	FTPCLNRQ	QIBM_QTMF_CLIENT_REQ	FTP Client Request Validation	
—	FTPLOGON	QIBM_QTMF_SVR_LOGON	FTP Server Logon	*ADDED2XPT
—	FTPSVRRQ	QIBM_QTMF_SERVER_REQ	FTP Request Validation	

6 In this area are typical commands you might see on any IBM i application screen. **F3** exits this screen, and **F5** refreshes or resets the list. Unique to this application is **F6** which will allow you to create an Exit point definition. **Only use if directed by an IBM STG Lab Service representative.** **U** presents a list of the users with access to the Exit Point as defined in the User Access File.

For more information on the ***ALLOBJ: *NOTUSED** referenced in the upper right of the screen read the section in the Additional Considerations titled, [**ALLOBJ, *NOIPCTL, and IP Filtering*](#)

7 **Q** is an option specifically for **SQL2** that presents a panel to define users who can use SQL through ODBC/JDBC activity. The interface limits what SQL statements can be run by these users. Users not defined to this interface can only run a SELECT statement. For additional information see, [*Data Base Server SQL Access \(QIBM_QZDA_SQLx\)*](#).

8/10/23 Work with ODBC SQL Verb Permissions 10:41:39

Position to... starting characters

Type op 2=Edi

opt Us

ODBC SQL VERB PERMISSIONS

Enter the User and the SQL Verbs they are allowed to run.

Add User

Allowed verbs (Y or N):

Alter.: <input type="checkbox"/>	Grant...: <input type="checkbox"/>	Update: <input type="checkbox"/>
Call...: <input type="checkbox"/>	Insert...: <input type="checkbox"/>	
Create: <input type="checkbox"/>	Merge...: <input type="checkbox"/>	
Delete: <input type="checkbox"/>	QCMDEXC: <input type="checkbox"/>	
Drop...: <input type="checkbox"/>	Revoke...: <input type="checkbox"/>	

Date: 2023-08-10 Time: 10.41.47

F3/F12=CANCEL ENTER=Set ODBC User

F1=Verb Legend F3=Exit F5=Refresh List F6=Add User

G QCMD RVK UPD Last changed

Changing an Exit Point Action

To change the Exit Point Action for an Exit Point Definition, select option 2 for the Exit Point Definition from the *Work with Exit Point Definitions* screen. You will see a screen similar to the following but with different data:

```

8/10/23                               Work with Exit Point Definitions                               10:09:41

Position to: _____ Filter Definitions: _____ ALLOBJ: *NOTUSED

Type options, press Enter.
5=Display 8=Add Exit 9=Remove Exit N=*ON F=*OFF L=*LOGONLY W=WRKREGINF

Opt Definition  Exit Point Name      Exit Point Description      Status
--
DRDADDM        CHGNETA              DRDA/DDM Logon              *ADDED2NAT
DSTPGMC        QIBM_QZRC_RMT        Distributed Program Call
DTAQSRVR       QIBM_QZHQ_DATA_QUEUE Host Servers DATAQ Server
FILESVR       QIBM_QPWFS_FILE_SERV Host Servers File Server
FTPCLNRQ       QIBM_QTMF_CLIENT_REQ FTP Client Request Validation
FTPLOGON       QIBM_QTMF_SVR_LOGON  FTP Server Logon            *ADDED2XPT
FTPSVRQ       QIBM_QTMF_SERVER_REQ FTP Request Validation
HSTPRT        QIBM_QNPS_ENTRY      Host Server Net Print Server
OJDBC         QIBM_QZDA_INIT       DB Logon - ODBC/JDBC/File XFR *ADDED2XPT
ONDB1         QIBM_QZDA_NDB1       Native DB OPs via ODBC/JDBC
OROI1         QIBM_QZDA_ROI1       Object INFO REQS via ODBC/JDBC
OSQL1         QIBM_QZDA_SQL1       DB Server SQL Access        *ADDED2XPT
OSQL2         QIBM_QZDA_SQL2       DB Server SQL Access

More...

F3=Exit  F5=Refresh  F6=Create Definition  U=View Exit Users  Q=SQL2 Access
  
```

This screen is quite simple to use. On this screen the original Exit Point Definition record is displayed for reference. To change the Exit Point Action of an Exit Point Definition record, cursor down to the input capable field titled, "Exit Point Action" and change the Exit Point Action as required:

- *ON** When the Exit Point Definition status has been set to ***ADDED2XPT**, ***ON** indicates to the Exit Program to restrict access to the users defined in the Exit Point User Access file. When ***ON**, every access through the Exit Point is classified as ***PASS** or ***FAIL** and logged into the security audit journal QAUDJRN. Additional information is provided in the journal entry noting the IP Address the attempt originated from, the USERID, and miscellaneous information to the specific Exit Point that may be useful for further analysis. If the Exit Point Definition status is blanks this value has no effect.
- *OFF** When the Exit Point Definition status has been set to ***ADDED2XPT**, ***OFF** indicates to the Exit Program **not** to restrict access to the users defined in the Exit Point User Access file. When ***OFF**, no restriction of access through the Exit Point occurs, no logging occurs, and no entries are logged into the security audit journal QAUDJRN. Effectively, this is the same as the Exit Point Definition not being registered to the Exit Point. If the Exit Point Definition status is blanks this value has no effect.
- *LOGONLY** When the Exit Point Definition status has been set to ***ADDED2XPT**, ***LOGONLY** indicates to the Exit Program **not** to restrict access to the users defined in the Exit Point User Access file. When set to ***LOGONLY**, every access through the Exit Point is classified as ***LOGONLY** and logged into the security audit journal QAUDJRN. Additional information is provided in the journal entry noting the IP Address the attempt originated from, the USERID, and miscellaneous information to the specific Exit Point that may be useful for further analysis. If the Exit Point Definition status is blanks this value has no effect.

Displaying an Exit Point Definition

To display the Exit Point Action for an Exit Point Definition, select option 5 for the Exit Point Definition from the *Work with Exit Point Definitions* screen. You will see a screen similar to the following but with different data:

```
Display Exit Point Definition (DSPXPDF)

Type choices, press Enter.

Exit Point Definition . . . . . > FTPCLNRQ      Name
Exit Point Name . . . . . > QIBM_QTMF_CLIENT_REQ
Exit Point Format . . . . . > VLRQ0100     Name
Exit Point Program . . . . . > QTMFXCSREQ    Name
  Library . . . . . > QZRDSECXPT    Name
Exit Point User Prompt . . . . . > Y           Y=Yes, N=No
Exit Point Action . . . . . > *ON          *ON *OFF *LOGONLY
Exit Point Description . . . . . > 'FTP Client Request Validation '

-

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

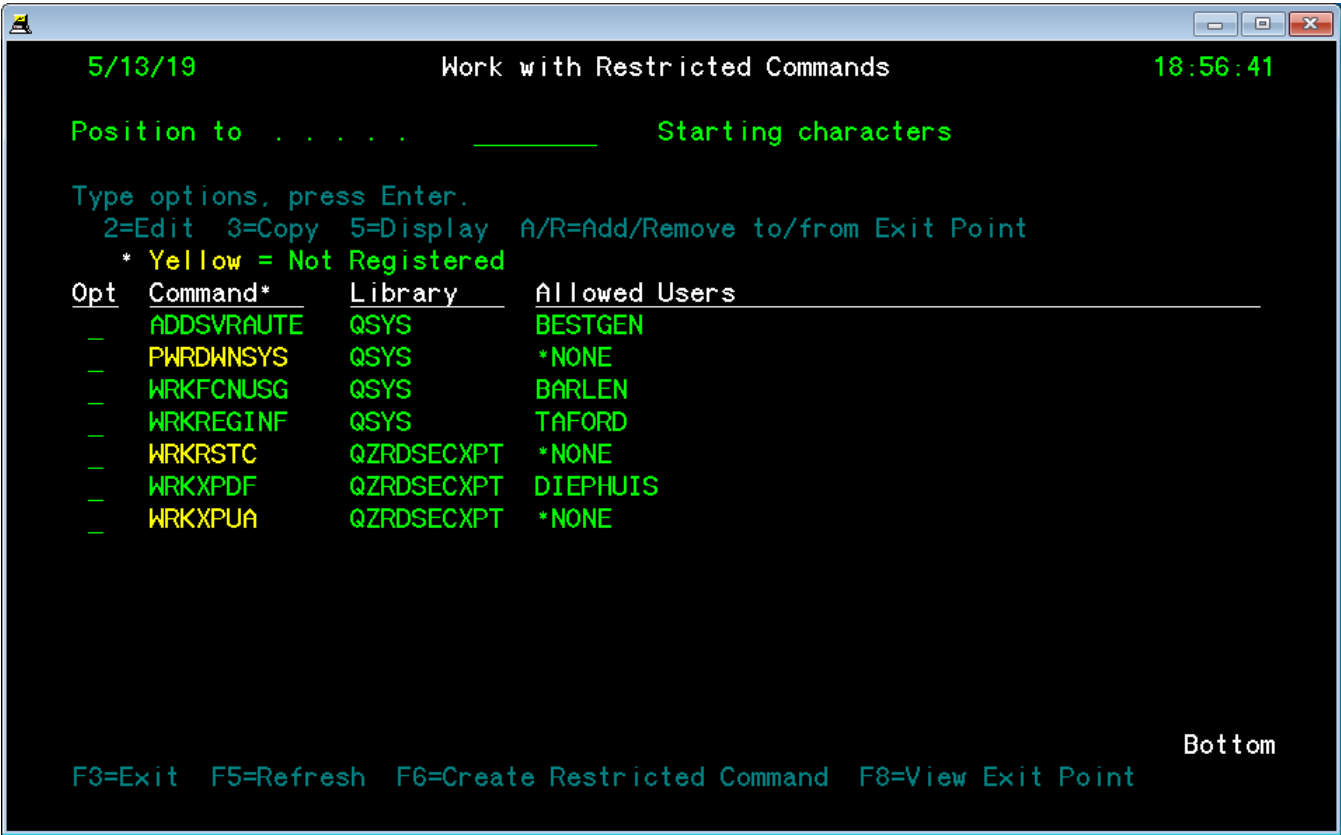
Bottom
17/027
```

This screen is also simple to use. On this screen the Exit Point Definition record is displayed for reference.

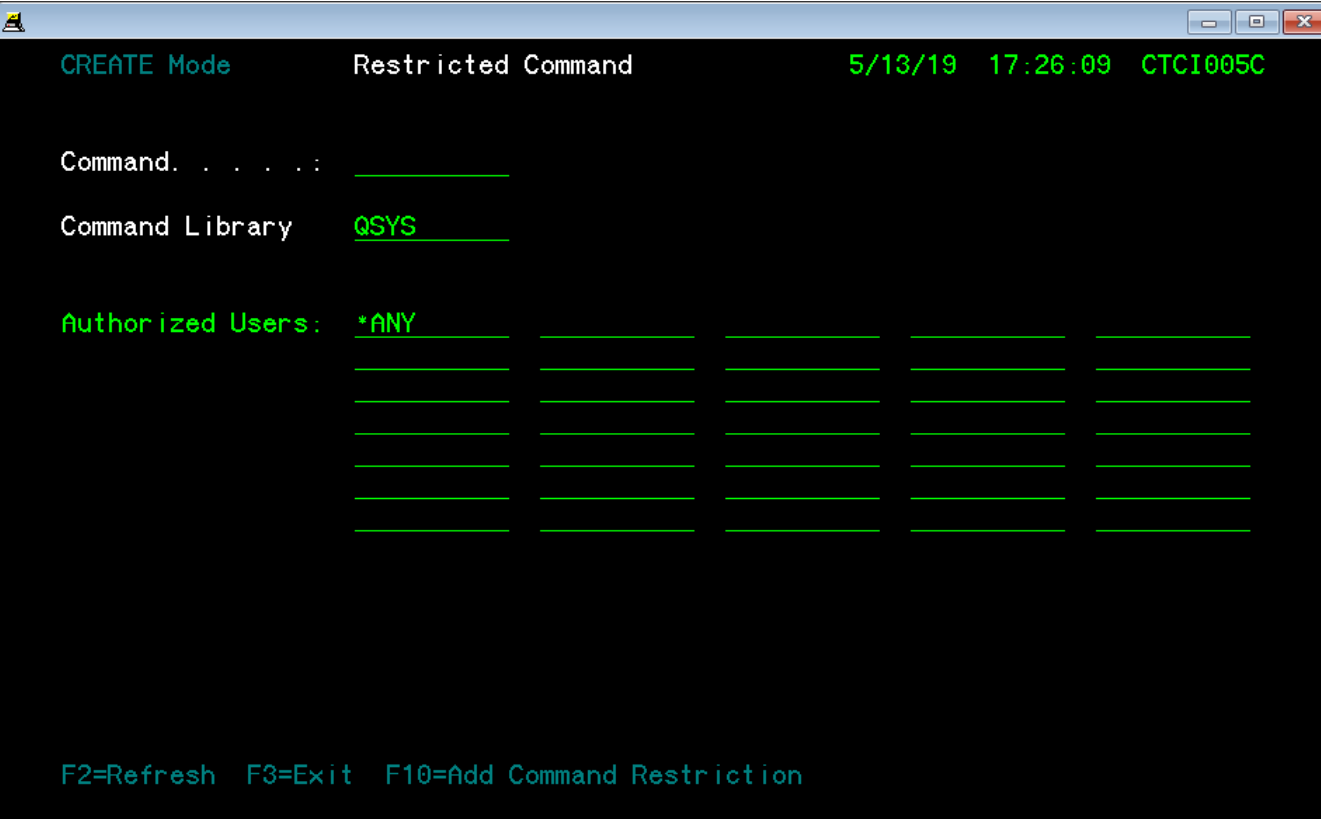
To exit the display of the Exit Point Definition record, press **Enter**, **F3** or **F12**.

Option 3 - Work with Restricted Commands

Besides Network Interfaces, the Exit Point Tool provides the capability to restrict sensitive commands to specific users or groups. When you select this menu option you will be presented with a screen similar to the following:



Creating a Restricted Command



CREATE Mode

Restricted Command

5/13/19 17:26:09 CTCI005C

Command. : _____

Command Library QSYS

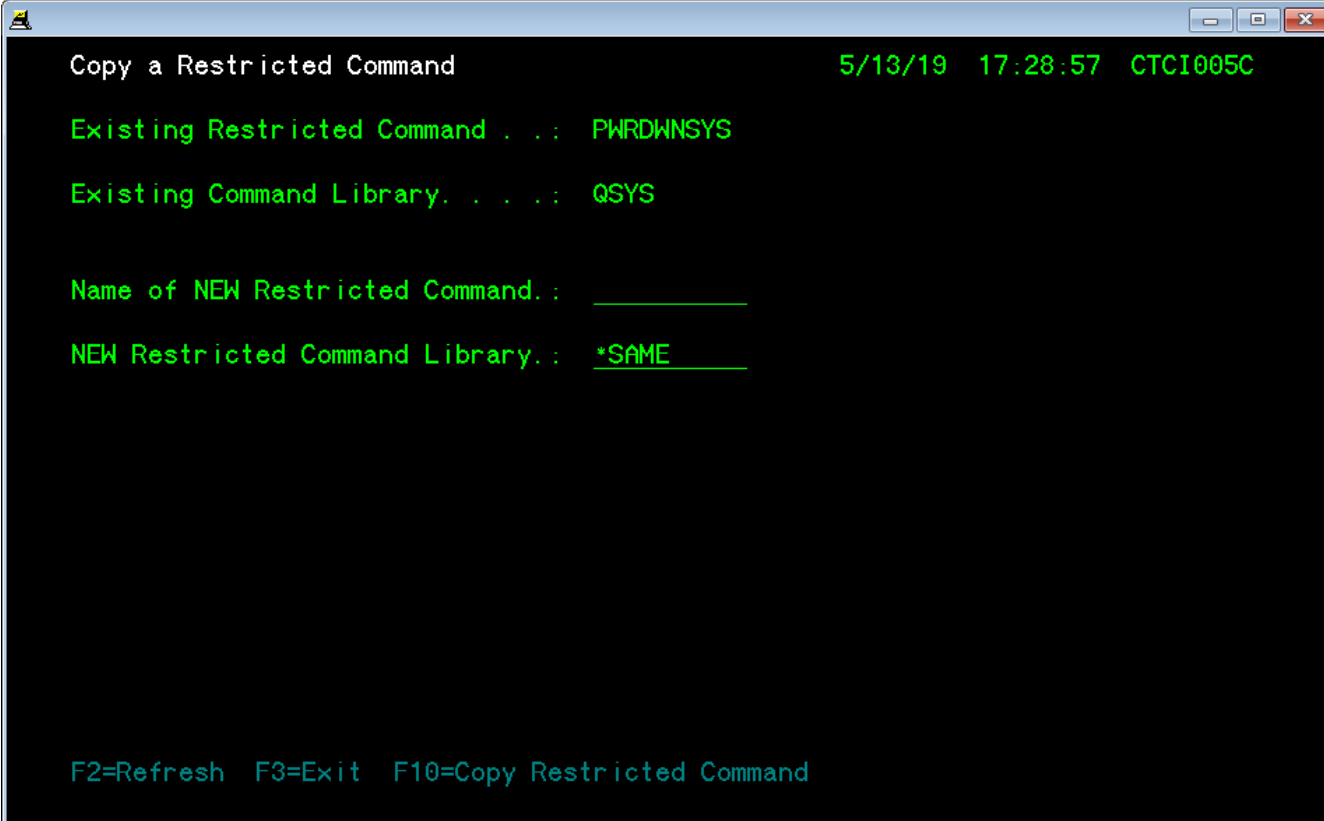
Authorized Users:

*ANY					

F2=Refresh F3=Exit F10=Add Command Restriction

Changing a Restricted Command

Copy a Restricted Command



The screenshot shows a terminal window with a title bar containing a small icon and standard window controls (minimize, maximize, close). The terminal content is as follows:

```
Copy a Restricted Command                                5/13/19  17:28:57  CTCI005C

Existing Restricted Command . . : PWRDWN SYS
Existing Command Library. . . : QSYS

Name of NEW Restricted Command.: _____
NEW Restricted Command Library.: *SAME_____

F2=Refresh  F3=Exit  F10=Copy Restricted Command
```

Display a Restricted Command

Adding a Command Restriction to the QIBM_QCA_CHG_COMMAND Exit Point

Removing a Command Restriction from the QIBM_QCA_CHG_COMMAND Exit Point

Viewing the QIBM_QCA_CHG_COMMAND Exit Point

Work with Registration Information

Type options, press Enter.
5=Display exit point 8=Work with exit programs

Opt	Exit Point	Exit Point Format	Registered	Text
_	QIBM_QCA_CHG_COMMAND	CHGC0100	*YES	Change command exit programs

Bottom

Command
===> _____

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

Select Option 8 to Work with exit programs

Work with Exit Programs

Exit point: QIBM_QCA_CHG_COMMAND Format: CHGC0100

Type options, press Enter.
1=Add 4=Remove 5=Display 10=Replace

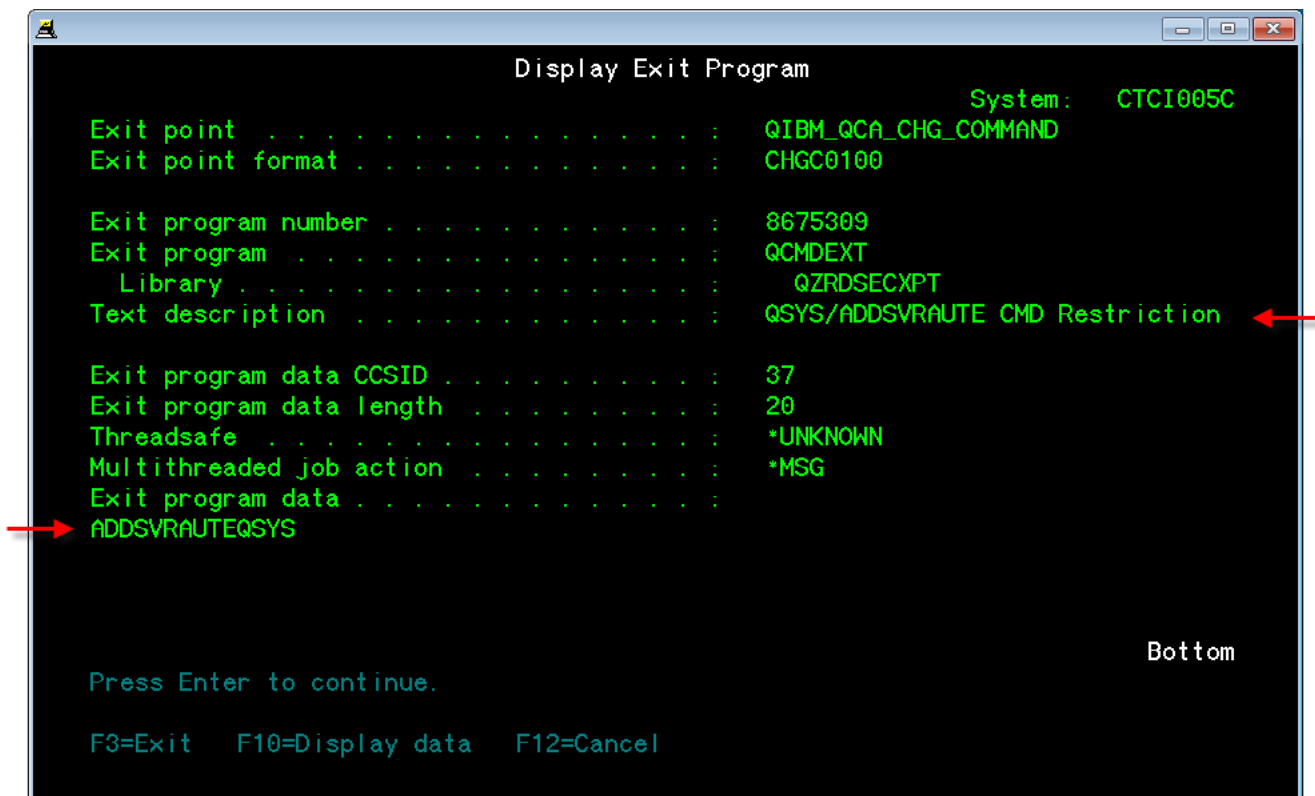
Opt	Exit Program Number	Exit Program	Library
__	8675309	QCMDEXT	QZRDSEXP

Bottom

Command
===> _____

F3=Exit F4=Prompt F5=Refresh F9=Retrieve F12=Cancel

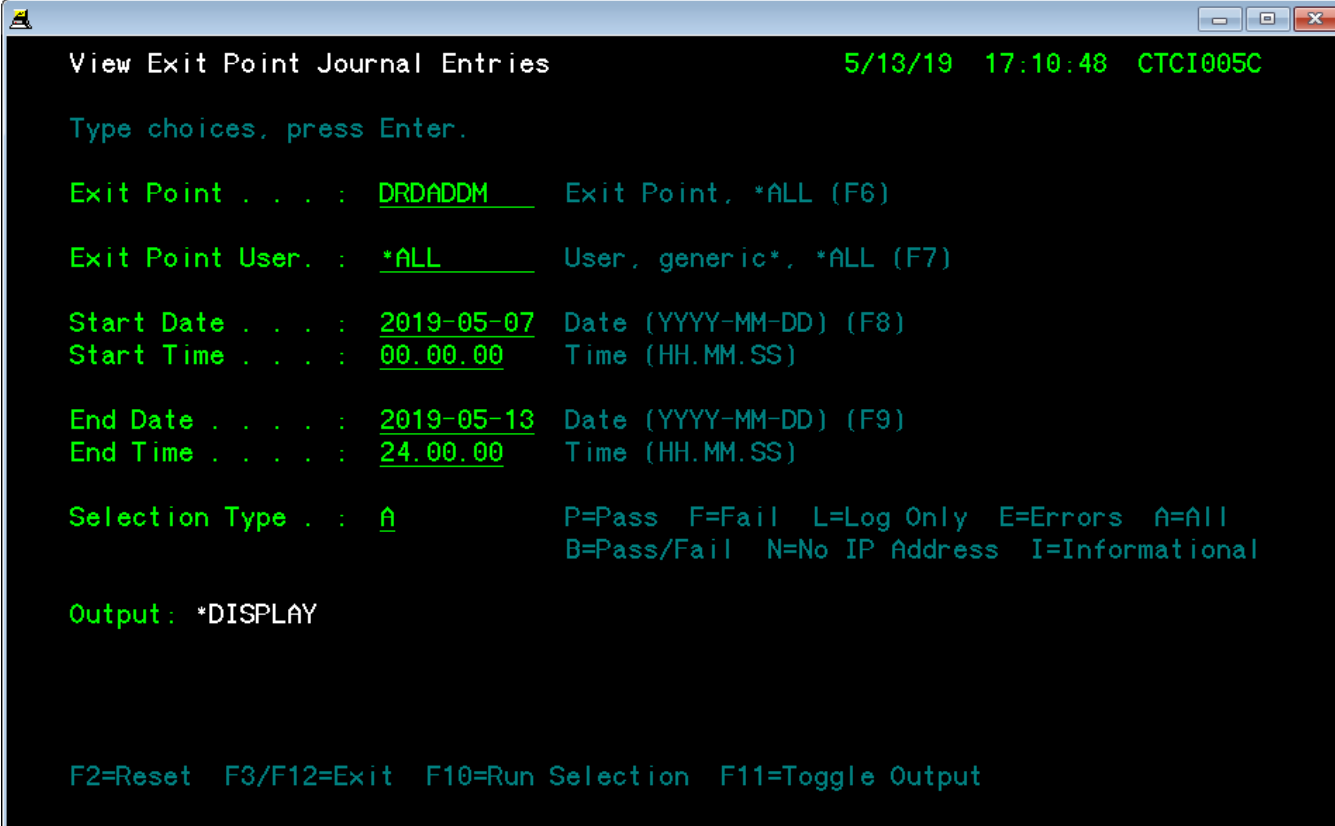
Select Option 5 to display the details of the Exit Point



Option 4 - Work with Exit Point Journal Entries

This option provides several options for viewing the Exit Point Journal Entries.

NOTE: Restricted Commands are not included in this option.



The screenshot shows a command window titled "View Exit Point Journal Entries" with a green title bar. The window contains the following text:

```
View Exit Point Journal Entries          5/13/19  17:10:48  CTCI005C

Type choices, press Enter.

Exit Point . . . . : DRDADDM      Exit Point, *ALL (F6)
Exit Point User. . : *ALL          User, generic*, *ALL (F7)
Start Date . . . . : 2019-05-07   Date (YYYY-MM-DD) (F8)
Start Time . . . . : 00.00.00     Time (HH.MM.SS)
End Date . . . . . : 2019-05-13   Date (YYYY-MM-DD) (F9)
End Time . . . . . : 24.00.00     Time (HH.MM.SS)
Selection Type . . : A           P=Pass  F=Fail  L=Log Only  E=Errors  A=All
                                   B=Pass/Fail N=No IP Address I=Informational

Output: *DISPLAY

F2=Reset  F3/F12=Exit  F10=Run Selection  F11=Toggle Output
```

Option 5 - Exit Point Reports

This option provides several options for reporting the Exit Point Journal Entries.

```
View Exit Point Reports                    5/13/19  17:07:23  CTCI005C

Type choices, press Enter.

User by Exit Point . . . . . : Y  Y=Yes, N=No
Exit Point by User . . . . . : N  Y=Yes, N=No
Exit Point by Status . . . . . : N  Y=Yes, N=No
User by Status . . . . . : N  Y=Yes, N=No
IP Address by Status. . . . . : N  Y=Yes, N=No
Exit Point by IP Address and User . . . . . : N  Y=Yes, N=No
IP Address by Exit Point by User . . . . . : N  Y=Yes, N=No
Exit Point accesses through Group . . . . . : N  Y=Yes, N=No
Exit Point accesses by non Exit Point User(s) : N  Y=Yes, N=No
Exit Point by IP Address . . . . . : N  Y=Yes, N=No
Restricted Command Usage . . . . . : N  Y=Yes, N=No

User ID . : *ALL -----> User, Group, *ALL (F7)
Start Date: 2019-05-13 > 00.00.00 Date (YYYY-MM-DD) (F8) > Time (HH.MM.SS)
End Date  : 2019-05-13 > 24.00.00 Date (YYYY-MM-DD) (F9) > Time (HH.MM.SS)

Output: *DISPLAY

F2=Reset  F3/F12=Exit  F10=Run Selection  F11=Toggle Output
```

```
End Date  : 2019-05-13 > 24.00.00 Date (YYYY-MM-DD) (F9) > Time (HH.MM.SS)

Output: *DISPLAY

F2=Reset  F3/F12=Exit  F10=Run Selection  F11=Toggle Output
Data area LSTXPTRPT created in library QZRDSEXP. +
```

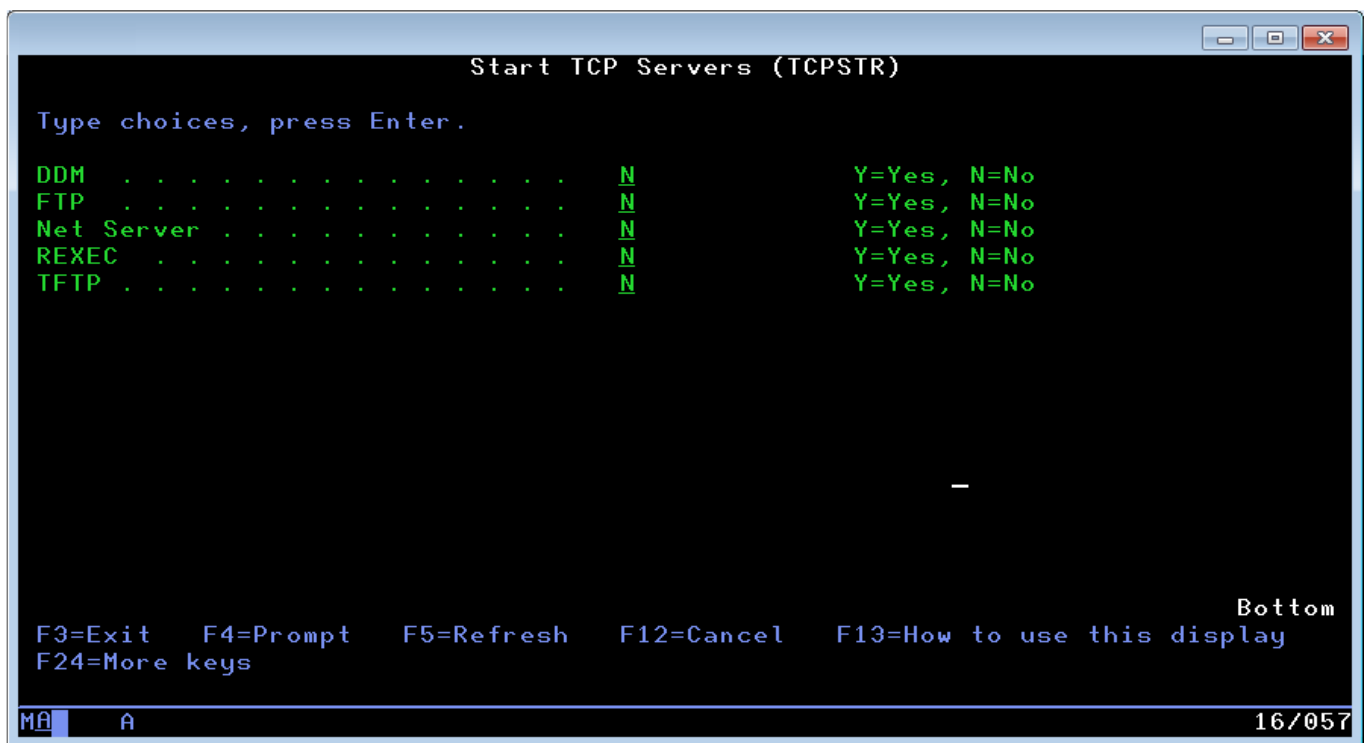
Option 11 – Start TCP Server

This option is the standard IBM system command to start a TCP/IP Server, ENDTCPSPVR. The Start TCP/IP Server (STRTCPSVR) command is used to start the TCP/IP application server jobs. The number of server jobs started by this command is specified, where appropriate, in the configuration for each TCP/IP application. The Start TCP/IP Server command can only be used when TCP/IP is fully operational and the interface server job QTCPIP is available. This command is not allowed when the IBM i is in a restricted state. Subsequent use of the STRTCPSVR command specifying SERVER(*FTP) will start one additional FTP server.

NOTE: Having more than one FTP server job running can improve the performance of initiating a session when multiple users attempt to connect to the server in a short period of time.

Be sure you understand the impact to client applications before running this command.

The screen has been configured so that it is easier to work with so that the options that often confuse users are hidden. You can cause them to re-appear by pressing the **F9** key.



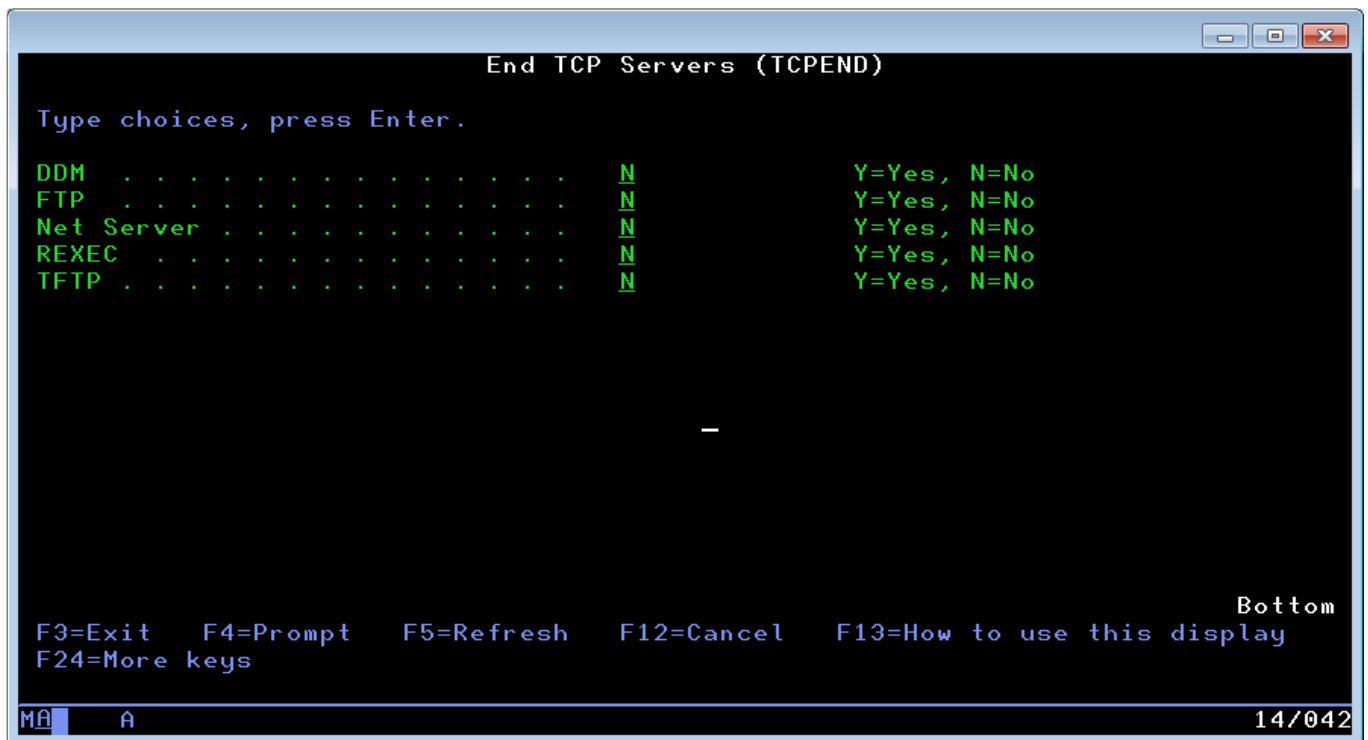
NOTE: Before the FTP Exit point definitions can be activated the Exit point definition for FTP Status must have its status set to ***ADDED2XPT** (option 8) on the Work with Exit Point Definitions screen and the ***FTP** TCP Server must be stopped and then restarted.

Option 12 – End TCP Server

This option is the standard IBM system command to end a TCP/IP Server, ENDTCPSVR. The End TCP/IP Server (ENDTCPSVR) command is used to end the TCP/IP application server jobs. If the jobs have any current active connections, these connections are ended immediately. If the ENDTCPSVR command is used to end a server that is not active, an error message may appear. The End TCP/IP Server command can only be used when TCP/IP is fully operational and the interface server job QTCPIP is available. This command is not allowed when the IBM i is in a restricted state.

Be sure you understand the impact to client applications before running this command.

The screen has been configured so that it is easier to work with so that the options that often confuse users are hidden. You can cause them to re-appear by pressing the **F9** key.



NOTE: Before the FTP Exit point definitions can be de-activated the FTP Exit point definition must have its status cleared (option 9) on the Work with Exit Point Definitions screen and the *FTP TCP Server must be stopped and then restarted.

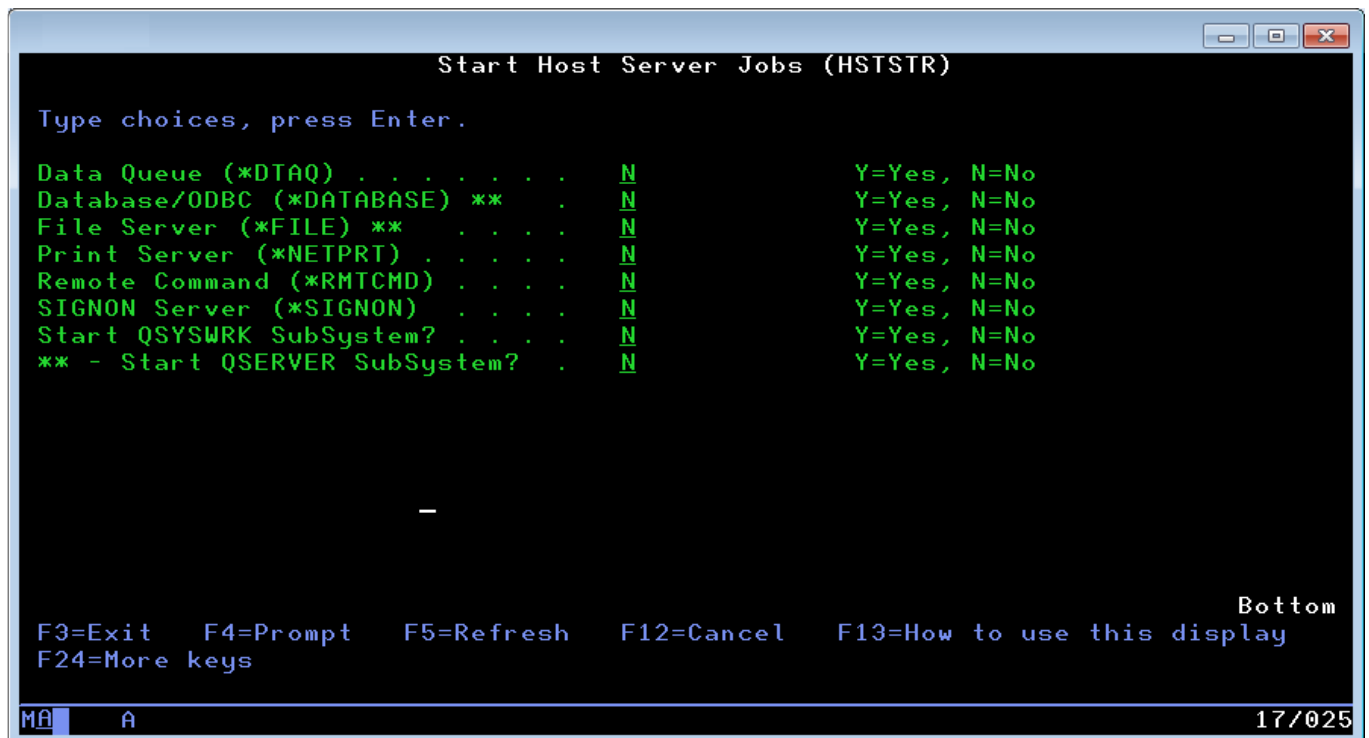
Option 21 – Start Host Server

This option is the standard IBM system command to start a Host Server, STRHOSTSVR. The Start Host Server (STRHOSTSVR) command is used to start a Host Server. One or more Host Servers can be started.

In order for the Host Server to start successfully, the QSYSWRK and QSERVER subsystems must be active. If they are not active the Host Servers will not start. Additionally, the QUSRWRK subsystem or the user-defined subsystem must be active in order to start associated server jobs. Also, TCP/IP must be active at the time the STRHOSTSVR command is issued. If TCP/IP is not active the Host Server will not be started

Be sure you understand the impact to client applications before running this command.

The screen has been configured so that it is easier to work with so that the options that often confuse users are hidden. You can cause them to re-appear by pressing the **F9** key.



NOTE: Before the Database Exit point definition (OJDBC) can be activated the Exit point definition for Database status must be set to ***ADDED2XPT** (option 8) on the Work with Exit Point Definitions screen and the ***DATABASE** Host Server must be stopped and then restarted.

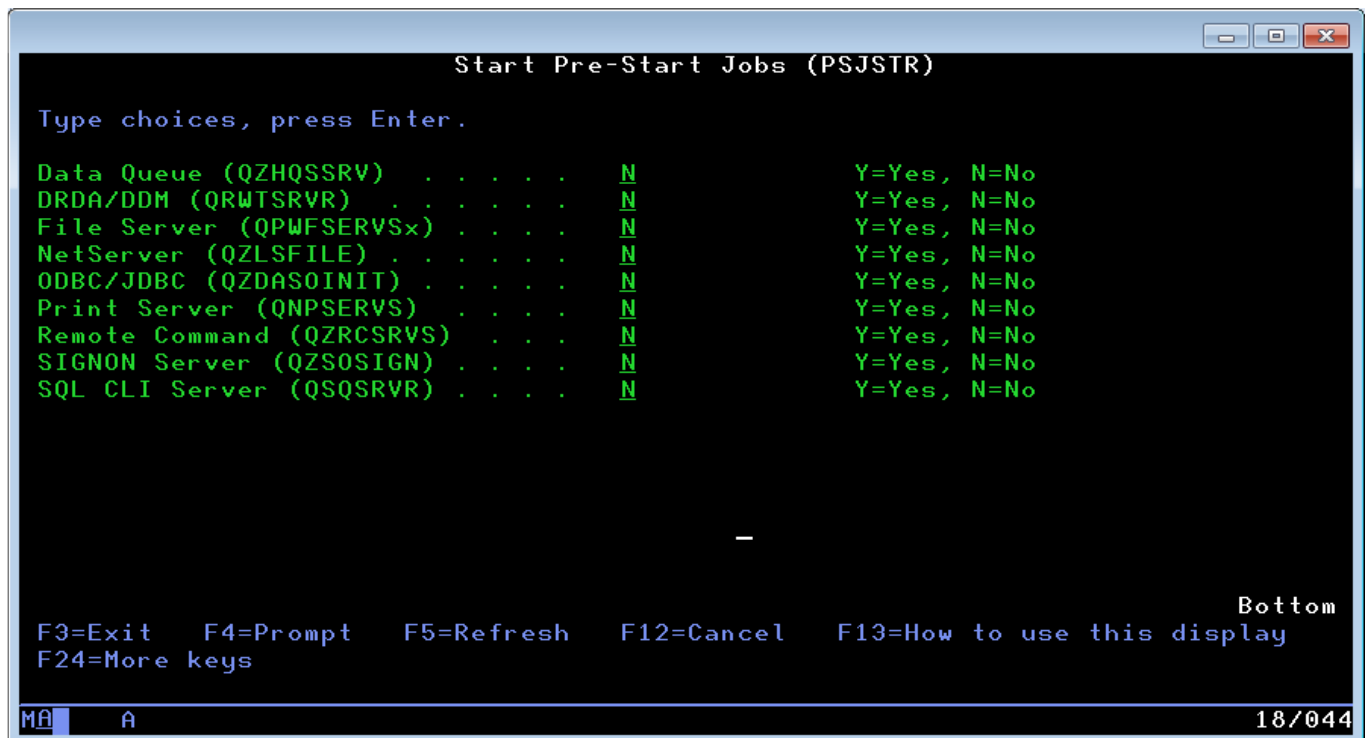
Option 22 – Start Prestart Jobs

This option is the standard IBM system command to start Prestart Jobs, STRPJ. The Start Prestart Jobs (STRPJ) command starts jobs for a prestart job entry in an active subsystem when there are no currently active prestart jobs for the prestart job entry.

This command is valid after an ENDPJ command is complete, or when all prestart jobs have been ended by the system due to an error or were never started during subsystem start up due to STRJOBS (*NO) on the ADDPJE command. The number of jobs started is determined by the INLJOBS value on the prestart job entry.

Be sure you understand the impact to client applications before running this command.

The screen has been configured so that it is easier to work with so that the options that often confuse users are hidden. You can cause them to re-appear by pressing the **F9** key.



Option 23 – End Host Server Jobs

This option is the standard IBM system command to end a Host Server, ENHHOSTSVR. The End Host Server (ENDHOSTSVR) command is used to end a Host Server. One or more Host Servers can be ended. Optionally, active connections to the *DATABASE and *FILE servers can be ended with this command. By default, when a Host Server is ended, and there are active connections to client applications, the Host Server jobs will remain active until communication with the client application is ended, unless the optional ENDACTCNN parameter is specified. However subsequent connection requests from the client application to that Host Server will fail until the Host Server is started again.

Be sure you understand the impact to client applications before running this command and/or change the ENDACTCNN parameter.

```
End Host Server Jobs (HSTEND)

Type choices, press Enter.

Data Queue (*DTAQ) . . . . . N      Y=Yes, N=No
Database/ODBC (*DATABASE) . . . . N  Y=Yes, N=No
File Server (*FILE) . . . . . N     Y=Yes, N=No
Print Server (*NETPRT) . . . . . N   Y=Yes, N=No
Remote Command (*RMTCMD) . . . . . N Y=Yes, N=No
SIGNON Server (*SIGNON) . . . . . N  Y=Yes, N=No
End QSYSWRK SubSystem? . . . . . N   Y=Yes, N=No
End QSERVER SubSystem? . . . . . N   Y=Yes, N=No

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

MA A 05/037
```

NOTE: Before the Database Exit point definition (OJDBC) can be de-activated you must remove the Exit Program (option 9) on the Work with Exit Point Definitions screen and the *DATABASE Host Server must be stopped and then restarted.

Option 24 – End Prestart Jobs

This option is the standard IBM system command to end Prestart Jobs, ENDPJ. The End Prestart Jobs (ENDPJ) command ends all jobs and any associated inline data files for a prestart job entry in an active subsystem.

Jobs can be waiting for a request or can already be associated with a request. Spooled output files associated with the jobs being ended can also be ended or allowed to remain on the output queue. The limit on the number of messages being written to each of the joblogs can also be changed.

Be sure you understand the impact to client applications before running this command.

The screen has been configured so that it is easier to work with so that the options that often confuse users are hidden. You can cause them to re-appear by pressing the **F9** key.



Option 25 – Work with ODBC Related Jobs

This option is a useful utility for managing the ODBC related jobs on the system. You will find this useful when determining whether ODBC related work is still active when attempting to recycle the database server.

```
CTCI005C - TAFORD          Work with ODBC Related Jobs          3/21/12  15:03:43

Press F4 for Available Options          Number of jobs listed ---> 2

Opt  Subsystem  Job Name  Curr User  Number Job User  IP Address  Files
---  ---
    QUSRWRK    QZDASOINIT  QUSER      058217  QUSER
    QUSRWRK    QZDASOINIT  QUSER      058218  QUSER

Bottom

F3=Exit  F4=Options Window  F5=Refresh  F9=Command Line  F12=Cancel

06/003
```



```
RUN OPTION CHOICES WINDOW

Opt  Description
  1  Display Job Status
  2  Display Job Definition
  3  Display Job Run Attributes
  4  Work with Spooled Files
 10  Display Job Log
 11  Display Call Stack
 12  Work with Job Locks
 13  Display Library List
 14  Display Open Files
 15  Display File Overrides
 16  Display Commitment Control
 99  End Selected Job

ENTER=Exit Window
```

Option 50 - Display Status of XPT Application (DSPXPTINFO)

Use this option to display configuration status of the Network Interface Firewall Library. This may be requested by your Lab Services representative to validate the application is setup properly. Output of running this will be to the display, a spool file, and to the output file QZRDSECXPT/XPTINFO. The Option 50 screen should look similar to the following:

```

Display Report
Report width . . . . . : 72
Shift to column . . . . .
Position to line . . . . .
Line ....+....1....+....2....+....3....+....4....+....5....+....6....+....7..

Item to Check      Value Retrieved      Item KEY
000001 Exit Point Tool Library      QZRDSECXPT - SZRDXPT V2      MSXPT000
000002 Information Timestamp      2023-08-07 12:29:12      MSXPT001
000003 Exit Point Tool Version      Version v8.00 Level 002.0010      MSXPT002
000004 QZRDSECXPT Library Owner      QTCP      MSXPT003
000005 Object Auditing Value      *NONE      MSXPT004
000006 *PUBLIC Authority      *USE      MSXPT005
000007 Object Create Authority      *EXCLUDE      MSXPT006
000008 Object Auditing on CREATE      *CHANGE      MSXPT007
000009 Library Size      30 MB      MSXPT008
000010 Number of Objects in Library      169      MSXPT009
000011 Number of XPT License Keys      1      MSXPT010
000012 Exit Point Tool License Key      203D01 06FD4B 16F101      MSXPT011
000013 License Expiration      *NONE      MSXPT012
000014 License Usage Limit      *NOMAX      MSXPT013
000015 License Key Serial Association      *LOCAL - 1014C6P      MSXPT014
000016 Alternate Exit Point Journal      QSYS/QAUDJRN      MSXPT015
000017 Exit Point Message Queue      QSYS/QXPTMSQ      MSXPT016
000018 *ALLOBJ Special Authority      *USED      MSXPT017

F3=Exit      F12=Cancel      F19=Left      F20=Right      F21=Split      F22=width 80
More...
```

Option 61 – Set Exit Point Tool Options

This option is used to set the configuration options for the Exit Point Tool.

Option 62 – Retrieve Exit Point Tool Options

This option is used to retrieve the configuration options for the Exit Point Tool.

Option 63 –Send/Install XPT to another System

This option is used send and/or install the Exit Point Tool to another system.

File Server Convenience Options

When working with the File Server Exit Point the order in which servers and subsystems are started/ended is important for properly registering and deregistering the exit program.

Before registering (or de-registering) Exit Programs start by using (in order) options 81 through 83 to end servers and subsystems related to the File Server Exit Point.

After registering (or de-registering) Exit Programs start by using (in order) options 71 through 73 to start or restart servers and subsystems related to the File Server Exit Point.

Option 71 – Start QSERVER Subsystem

This option is the standard IBM system command (STRSBS) for starting the subsystem QSERVER.

```
STRSBS SBSD(QSYS/QSERVER)
```

Option 72 – Start NetServer

This option is the standard IBM system command (STRTCPSVR) for starting all instances of the TCP/IP Server *NETSVR.

```
STRTCPSVR SERVER(*NETSVR) INSTANCE(*ALL)
```

Option 73 – Start File Server

This option is the standard IBM system command (STRHOSTSVR) for starting the *TCP protocol of the *FILE Host Server.

```
STRHOSTSVR SERVER(*FILE) RQDPCL(*TCP)
```

Option 81 – End NetServer

This option is the standard IBM system command (ENDTCPSVR) for ending the default (*DFT) instance of the TCP/IP Server *NETSVR.

```
ENDTCPSVR SERVER(*NETSVR)
```

Option 82 – End QSERVER Subsystem

This option is the standard IBM system command (ENDSBS) for ending the subsystem QSERVER immediately.

```
ENDSBS SBS(QSERVER) OPTION(*IMMED)
```

Option 83 – End File Server

This option is the standard IBM system command (ENDHOSTSVR) for ending the *FILE Host Server.

```
ENDHOSTSVR SERVER(*FILE) ENDACTCNN(*FILE)
```

XPT Menu Convenience Function Keys

When working with the XPT Menu several Function keys have been defined to simplify problem determination when troubleshooting Exit Point related issues.

F2 – View Messages in the QXPTMSQ Message Queue

Use this to set the License Key for this system or for use in exporting to other systems.

F6 – View Messages in the QXPTMSQ Message Queue

This option is the standard IBM system command for displaying the messages in the QXPTMSQ message queue.

F7 - Work with QSYSWRK Subsystem Jobs

Use this option to navigate to the Work with Subsystem Jobs (WRKSBSJOB) command panel for jobs in the QSYSWRK Subsystem.

F8 - Work with QUSRWRK Subsystem Jobs

Use this option to navigate to the Work with Subsystem Jobs (WRKSBSJOB) command panel for jobs in the QUSRWRK Subsystem.

F10 – Work with Registration Information

This option is the standard IBM system command for Work with Registration Information (WRKREGINF). The Work with Registration Information display shows a list of exit points. You can use this list to display information about an exit point or to work with exit programs associated with an exit point. Many customers find this command intimidating. With the Exit Point Tool, we have attempted to remove the necessity for using this interface. Occasionally, however, there may be a need to look more closely at a specific exit point and have included it for your convenience.

Opt	Exit Point	Exit Point Format	Registered	Text
—	QIBM_QTF_TRANSFER	TRAN0100	*YES	Original File Transfer Functi
—	QIBM_QTG_DEVINIT	INIT0100	*YES	Telnet Device Initialization
—	QIBM_QTG_DEVTERM	TERM0100	*YES	Telnet Device Termination
—	QIBM_QTMF_CLIENT_REQ	VLRQ0100	*YES	FTP Client Request Validation
—	QIBM_QTMF_SERVER_REQ	VLRQ0100	*YES	FTP Server Request Validation
—	QIBM_QTMF_SVR_LOGON	TCPL0100	*YES	FTP Server Logon
—	QIBM_QTMF_SVR_LOGON	TCPL0200	*YES	FTP Server Logon
—	QIBM_QTMF_SVR_LOGON	TCPL0300	*YES	FTP Server Logon
—	QIBM_QTMX_SERVER_REQ	VLRQ0100	*YES	REXEC Server Request Validati
—	QIBM_QTMX_SVR_LOGON	TCPL0100	*YES	REXEC Server Logon
—	QIBM_QTMX_SVR_LOGON	TCPL0300	*YES	REXEC Server Logon

More...

Command
==>

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

24/034

Exit Point Considerations

When first using Exit Points it would be wise to first understand how the interfaces they protect are being used. Turning on an Exit Point without this understanding could cause a disruption in business processes. For example, turning on the TELNET Exit Point could prevent anyone from signing on to the system! So, tread carefully. One strategy would be to analyze the security journal entries (JS) for Exit Point interfaces from QAUDJRN for a period of 90 days and create user groups according to the interface category being used, ie., FTPGROUP for users who will have access to the File Transfer Protocol (FTP). Another strategy would be to turn on the Exit Points in *LOGONLY mode and observe usage for 90 days. After 90 days, as you would have with QAUDJRN analysis, create user groups according to the Exit Points being used. Whichever method is used, proper security protocol should be followed, and access granted only to those individuals with a business need. Verify that those individuals who are currently accessing the system from Exit Point interfaces have the proper business approval. Quite possibly, your analysis may reveal access that has already taken place without proper authorization.

Data Base Server SQL Access (QIBM_QZDA_SQLx)

Generally, this Exit Point should only be registered in *LOGONLY mode. When registering both QIBM_QZDA_SQL1 and QIBM_QZDA_SQL2 take note that the QIBM_QZDA_SQL2 exit point takes precedence over the QIBM_QZDA_SQL1 exit point. If a program is registered for the QIBM_QZDA_SQL2 exit point it will be called and the program for the QIBM_QZDA_SQL1 exit point will not be called.

Other notes and considerations...

... users are denied by default to any of the interfaces where an exit program has been registered and turned ON.

... users defined to *ALL exits are always granted access

... OJDBC is a separate exit that controls who can use ODBC in general. If you only use this Exit it protects from general use of ODBC so that only those with a business need are granted access.

... if OJDBC is NOT registered then OSQL2 governs access as described below.

... if the OSQL2 Exit Program is not registered, there is no restriction of what can be done using ODBC.

... if registered, the OSQL2 exit is called after the OJDBC exit completes, which asserts

... basic access to use ODBC has been determined by the OJDBC exit and what follows, is a subsequent grant of access

... if the OJDBC Exit is NOT registered anyone can use ODBC at a minimum to select information

... if a user/group is not defined to the SQL2 exit that the following statements are restricted for use:

ALTER, CALL, CREATE, DELETE, DROP,
GRANT, MERGE, INSERT, QCMDXEC, REVOKE, UPDATE

... restricted verbs are monitored and reported for usage in the audit journal

SQL2 Processing Flow:

Assumes either OJDBC is NOT registered or assumes user or group is registered to OJDBC

In the following,

- **OPT1-OSQL2** refers to XPT Menu Option 1 user/group registration to OSQL2
 - **OPT2-Q** refers to XPT Menu Option 2 - selection Q registration to OSQL2
1. if non-restricted verbs only, no need to register a user or group to OPT1-OSQL2 or OPT2-Q
 2. if restricting verbs then register allowed users or group as follows:
 - a. to use the exit in restriction mode a user or group must be registered to OPT1-OSQL2
 - consistent with other interfaces for allowing access to the interface
 - maintains single location to monitor users of all exit points
 - ensures user/group restrictions by IP address are continued for the interface
 - honors *ALLOBJ and other "special" features
 - Non-restricted verbs are always allowed regardless of whether the user or group is registered to OPT2-Q
 - b. consequently, after registering a user in OPT1-OSQL2 then also register the user in OPT2-Q
 - note: if the user is not registered in OPT2-Q, the group(s) of users registered in OPT1-OSQL2 are not considered if specified in OPT2-Q unless one of the groups is also specified in OPT1-OSQL2
 - a user defined in OPT1-OSQL2 that is a member of a group also specified in OPT1-OSQL2 will be evaluated with precedence over a group they may be a member of if it is also specified in OPT2-Q
- and
- c. if registering a group in OPT1-OSQL2 then
 - register the group in OPT2-Q
 - or
 - register individual group members in OPT2-Q
 - but
 - not both as the group permissions will take precedence over the user (since the user is not registered in OPT1-OSQL2)
 - group and user permissions are not OR'd together
3. High-level summary
 - add users to OPT1-OSQL2 and OPT2-Q
 - or
 - add groups to OPT1-OSQL2 and either the group defined in OPT1-OSQL2 or group members to OPT2-Q

Additional Notes:

- Users not defined to the EXTPUAP table are only allowed use of the SELECT verb (just as before)
- If SQL2 is set to LOGONLY it logs **ALL**, if set to ON then the exit will only log **FAILs** for performance purposes.
- A **FAIL** is defined as:
 - non authorized use of a restricted verb
 - IP address not valid for exit
 - user not passed to exit program
 - user not found on the system
 - license key failure
 - file open errors

Fastpaths:

- No entries are written to journal that begin **SET_MONITOR_OPTION(** - could be hundreds / thousands of them
- No entries are written to journal that begin **CALL SYSIBM** for the following related items- could be hundreds / thousands of entries:

SQLCOLPRIVILEGES
SQLCOLUMNS
SQLFOREIGNKEYS
SQLFUNCTIONCOLS
SQLFUNCTIONS
SQLGETTYPEINFO
SQLPRIMARYKEYS
SQLPROCEDURECOLS
SQLPROCEDURES
SQLPSEUDOCOLUMNS
SQLSPECIALCOLUMNS
SQLSTATISTICS
SQLTABLEPRIVILEGES
SQLTABLES
SQLUDTS

- No restricted verbs used - normal exit checking - generally a **PASS** unless failure due to other causes such as an incorrect IP Address
- No restricted verb used and user in EXTPUAP with NNNNNNNNNNN - **PASS**
- Restricted verb used and user not in EXTPUAP - no further checking of anything – **FAIL**
- Restricted verb used and user in EXTPUAP with YYYYYYYYYYY – **PASS**

NOTE: If the data area **QZRDSECTXPT/XPTLOGALL2** exists, then even **PASS** entries will be logged. Keep in mind, this could impact performance.

CRTDTAARA (QZRDSECTXPT/XPTLOGALL2) TYPE(*CHAR) LEN(1)

Distributed Program Calls (DPC) and Remote Command (RMTCMD)

The QIBM_QZRC_RMT Exit Point is used for both Remote Command (RMTCMD) and Distributed Program Calls (DPC). For customers using Client Access 5250 emulator the DPC is used for Application Administration and Navigator. To prevent the Client Access emulator from failing when using RMTCMD the DPCs must be allowed through by a simple check of the incoming DPC programs QSYS/QSYRTUFI and GY/QGYSETG. If these are present in the incoming request then DPC checking is bypassed.

IMPORTANT: At least one of the QIBM_QZRC_RMT Exit Point Definitions must have a status of ***ADDED2XPT** to restrict access.

Associated with incoming remote command access is the system command called Run Remote Command (RUNRMTCMD), also known as AREXEC. On the IBM i RUNRMTCMD is mostly thought of as a mechanism to communicate with PCs and UNIX servers. It also has the ability to remote command (RMTCMD) to another IBM i. Neither the RMTCMD exit or REXEC exit control the command. It is generally found *PUBLIC *USE. To secure use of the command set the *PUBLIC authority to *EXCLUDE and attach an authorization list (*AUTL) to it. Additionally, consider changing the *PUBLIC authority of the program REXEC in library QSHELL. Be sure to locate and secure all occurrences of these objects. A side note to this command, if someone wanted to be a destructive, they could use this command to harm client PC's or worse other UNIX servers that are not properly secured. Be advised and be aware of this commands potential.

NOTE: If limited capabilities is correctly specified for users the risk for RUNRMTCMD is further reduced.

NOTE: No command entries are written to the audit log for **CHGJOB**.

File Server (QIBM_QPWFS_FILE_SERV)

If the data area **QZRDSEXP/XPTNOFSLAT** exists, then entries related to listing of file/folder attributes will **not** be logged. This occurs for every object in the path a user might navigate representing a significant volume of entries.

CRTDTAARA (QZRDSEXP/XPTNOFSLAT) TYPE(*CHAR) LEN(1)

File Transfer Protocol (FTP)

File Transfer Protocol (FTP) is a very useful utility for the administration and operations of the IBM i, however, it does pose a risk if not used by those with a proper business need. Additionally, the security administrator should realize that the FTP risk is more than inbound requests from PC's and other Servers. FTP can also be used by a user signed in to a 5250 session and connect to other systems for both sending and receiving information. This fact is often missed by security administrators. Also often missed is that Remote Command (RMTCMD) is used within FTP. Understand, when granting a user the ability to use FTP you are providing them the capability to perform remote commands.

So two important facts are to be noted here:

- FTP transmissions can be both inbound and outbound
- RMTCMD operations can be run within FTP

The following exit point definitions help you administer FTP:

FTPCLNRQ - restricts a user signed on to 5250 session from using FTP. At this time the restriction for use is limited to the ability to use FTP as a client to other systems. In future versions of this tool, the ability to limit what operations a user can perform may be added.

FTPSVRRQ - restricts FTP operations from PC's or other servers and assumes an FTP logon has taken place. . At this time the restriction for use is limited to the ability to use FTP to access the system. In future versions of this tool, the ability to limit what operations a user can perform once logged in may be added.

FTPLOGON - restricts FTP transmissions from entering the system by PC's or other servers - at logon. Once logged in, all operations are accessible to the user unless the FTPSVRRQ exit point definition is defined for the user to further restrict their usage.

The difference between the FTPLOGON and FTPSVRRQ exit points is that FTPSVRRQ allows a logon to take place. Using, FTPLOGON restricts without regard to what operations a user wants to perform. At this time, either one can be used to restrict use of inbound FTP.

NOTE: If limited capabilities is correctly specified for users the risk for outbound FTP is reduced.

Remote Execution (REXEC)

Similar to FTP, Remote Execution (REXEC) is a very useful utility for the administration and operations of the IBM i, however, it does pose a risk if not used by those with a proper business need. Additionally, the security administrator should realize that the REXEC risk is more than inbound requests from PC's and other Servers. REXEC can also be used by a user signed in to a 5250 session and connect to other systems for both sending and receiving information. This fact is often missed by security administrators.

The following exit point definitions help you administer REXEC:

REXECREQ - restricts REXEC operations from PC's or other servers and assumes an REXEC logon has taken place. . At this time the restriction for use is limited to the ability to use REXEC to access the system. In future versions of this tool, the ability to limit what operations a user can perform once logged in will be added.

RXCLOGON - restricts REXEC transmissions from entering the system by PC's or other servers - at logon. Once logged in, all operations are accessible to the user unless the FTPSVRRQ exit point definition is defined for the user to further restrict their usage.

Associated with incoming REXEC access is the system command called Run Remote Command (RUNRMTCMD), also known as AREXEC. On the IBM i RUNRMTCMD is mostly thought of as a mechanism to communicate with PCs and UNIX servers. It also has the ability to remote command (RMTCMD) to another IBM i. Neither the RMTCMD exit or REXEC exit control the command. It is generally found *PUBLIC *USE. To secure use of both commands set the *PUBLIC authority to *EXCLUDE and attach an authorization list (*AUTL) to it. Additionally, consider changing the *PUBLIC authority of the program REXEC in library QSHELL. Be sure to locate and secure all occurrences of these objects. A side note to this command, if someone wanted to be a destructive, they could use this command to harm client PC's or worse other UNIX servers that are not properly secured. Be advised and be aware of this commands potential.

Additionally, if REXEC capability is not desired be sure that the server is not started:

```
CHGRXCA AUTOSTART(*NO)
```

Also consider the use of Port Restrictions to prevent a socket application, for example, from using REXEC.

NOTE: If limited capabilities is correctly specified for users the risk for outbound REXEC is reduced.

TELNET

Using this exit point may have minimal value for restricting users. Primarily because the user would have to be known at connect time. This exit is called before the green screen ever appears. Generally, this is only known if authenticating thru Client Access first or if it were passed as part of the connection, for example:

```
telnet -l TAFORD
```

or

```
TN5250.exe user=TAFORD" or "STRTCPTELN RMTUSER(TAFORD)
```

It could have value by checking Device Name (Session ID), Port, SSL. or IP Address, etc.,

For restricting users it will have little value unless you insure that the USERID is passed. **If a USERID is not passed, the connection will be rejected.**

Restricted Commands (QIBM_QCA_CHG_COMMAND)

The Exit Point for restricting commands has limitations with displaying information to end users due to the ability of the Exit Point registered to alter the command string run by the end user. While the implementation of the Exit Point Tool for restricting commands does not currently provide the ability to alter the command, the fact that it could prevents the program from communicating informational messages to the end user in the following situations:

- When a command is library qualified
- When a command has a parameter defined with RTNVAL(*YES), ie., all CL retrieve (RTVxxxx) commands
- When a command has parameters defined with DSPINPUT(*NO) or DSPINPUT(*PROMPT)
- When a command is running in a System State program

In these scenarios the failure message might look similar to the following:



Note: In this scenario the user will be sent back to the previous call level. To see the failure check the Audit Journal (QAUDJRN) or view the Restricted Commands Usage report through the [Exit Point Reports](#) menu option.

Alternate Audit Journal

If desired, you may change the output of the audit journal entries from QSYS/QAUDJRN to one of your own choosing. There are a number of reasons you may want to do this, but note that the integrity and security of alternate journals is not guaranteed. If you make this change, it is your responsibility to secure and protect these journals. **IBM will not be held liable for lost entries or journals as a result of using this option.**

Setting the Alternate Journal:

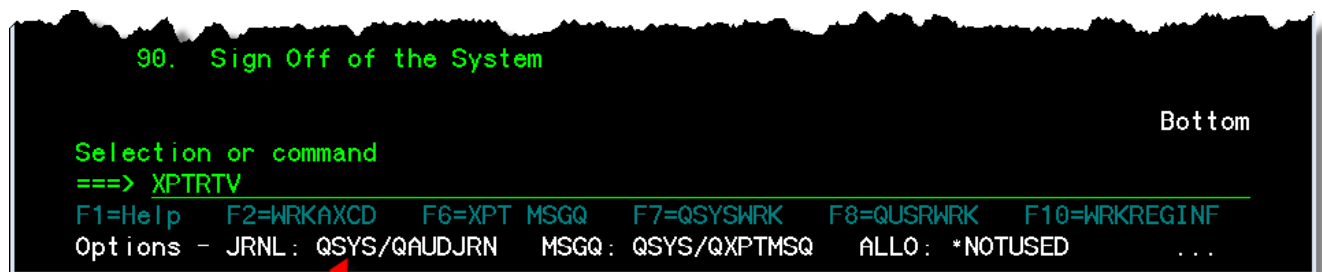
Use the command [QZRDSECXPT/XPTSET](#) to set the alternate Journal (or option 61 from the XPT menu).




Considerations:

- If you do not use the command to set an alternate journal the default will always be QSYS/QAUDJRN
- The Journal must exist, you cannot set an entry for a journal that does not exist
- Blank entries are not allowed
- After setting the Journal a User-Defined (U) Audit Journal entry (QZ) will be created in QSYS/QAUDJRN
- Using a journal other than QAUDJRN may require additional security administration on your part to insure its integrity. The operating system insures the security of QAUDJRN. Other Journals are not secured to the same degree.

Use the command [QZRDSECXPT/XPTRTV](#) to retrieve the alternate Journal (or option 62 from the XPT menu).



Considerations:

- No parameters are required, simply type XPTRTV and press 
- If the retrieval is successful the alternate journal will be shown at the bottom of the screen
- If parameters are passed they are ignored and the currently defined alternate Journal is displayed
- If no entry is found for the alternate Journal the command will default to QSYS/QAUDJRN.
- If when retrieving the entry and the alternate journal it specifies is not found it will also default to QSYS/QAUDJRN

****ALLOBJ, *NOIPCTL, and IP Filtering***

For *ALLOBJ users, there is a master switch and individual switches for each Network Interface Exit thru use of the special user registration name ***ALLOBJ**. This acts as a pseudo group that allows any user with *ALLOBJ special authority access to the network interface.

The master switch is set with the same menu option as the alternate journal and message queue and its status is displayed in the upper right corner of the User and Exit Definition panels...

```
cess                21:19:03

ALLOBJ: *USED
```

As mentioned, the individual exits require the use of the user entry ***ALLOBJ**. The exit definition for ***ALLOBJ** could be *ALL or specified individually like DRDADD, FTPLOGON... through multiple entries ...

Opt	User Name	Exit Point	Allowed IP
—	*ALLOBJ	*ALL	9.*.*.*

Use of ***ALLOBJ** is checked at both the user and group level and depending on how the access is obtained will be shown in the log like the following...

XPT User	XPT Type	XPT Name	Logon By XPT Group	XPT Status	XPT IP Address	XPT Other Data
TAFTST	*SIGNON	SIGNONSRV	*GRPALL	*PASS	9.10.86.65	Function = Retrie
TAFTST	RNTCMD	QZRC_RNT	*GRPALL	*PASS	9.10.86.65	RNTCMD Command = 0
TAFTST4	*SIGNON	SIGNONSRV		*FAIL	9.10.86.65	Function = Retrie
TAFTST	RNTCMD	QZRC_RNT	*USRALL	*PASS	9.10.86.65	RNTCMD Command = 0
QWKUSER	*DRDA	NETW_ATTR		*PASS	9.5.168.75	Request = SQLCNN
QWKUSER	*DRDA	NETW_ATTR		*PASS	9.5.168.75	Request = SQLCNN
QWKUSER	*DRDA	NETW_ATTR		*PASS	9.5.168.75	Request = SQLCNN

NOTE: When setting the ***ALLOBJ** special value you will be prompted to enter the installation license key provided to you by your Technology Expert Labs representative to prevent unauthorized setting of this value.

Related to IP Address filtering...

Several of the network related exit point interfaces (NetServer, iNav, Remote Command/Program, ODBC, Signon Server, etc...) do not always return an IP Address to the Exit Point when the Exit Program is run. In various situations, work is actually done via local Unix sockets, via Java Toolbox code, and other internal calls. If that code needs to access a server, it does so via those mechanisms. As a result, there is no IPv4 address that can be stored. Often if there even is an IP Address the local loopback 127.0.0.1 is presented.

For other server jobs, they connect to a port and accept requests coming in on any TCP/IP interface. For example, the TELNET server listens for requests coming in on port 23. If you look at NETSTAT option 3 and display the connection details for the telnet server connection (Port 23), you'll see that the server is not listening on any specific local IP address. Most server jobs are going to behave in a similar way, they'll bind to a port and listen for any requests coming in on that port just like the TELNET server does with port 23.

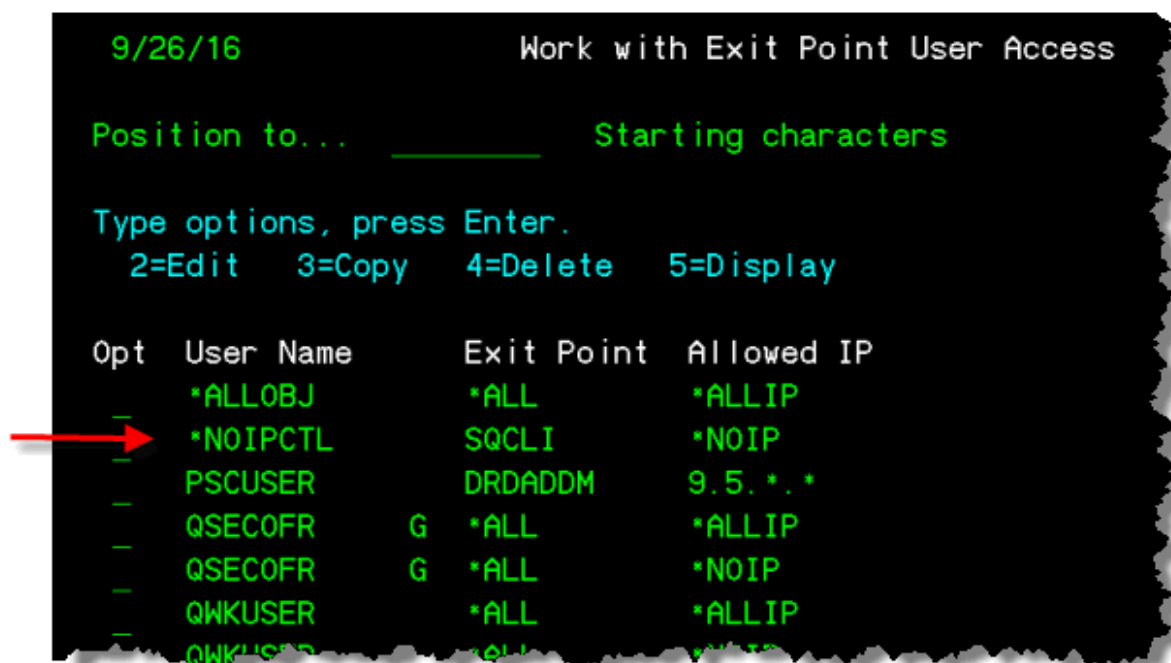
Some jobs such as pre-start jobs like QZRCRSVS may be started before a TCP/IP connection has even been established. So, it wouldn't have an IP address associated with it until a client connection gets established.

The IP address resolved is always for the most recently used socket in the thread. When the most recently used socket is closed, the remote address is zeroed out (if the remote address matches the value for the socket being closed). So you will see a blank IP address if the last sockets operation was a `close()`.

So the IP address returned (if it is returned) all depends on the point at which the remote address is retrieved for the thread and it is based on the last sockets operation done in that thread.

What this means is that operationally, the system doesn't always return IP addresses and blocking on interfaces with no IP address could cause an application to fail. So, by default, the Exit Point tool will allow network traffic that has no IP address.

To help secure the network interfaces with no ip address, the special user ***NOIPCTL** can be used to prevent transactions from the network server interface (Exit Point) from entering the system. Further, transactions by user or network interface (Exit Point) with no IP address can be blocked. For those users that do need to get thru the interface with no address there is the special keyword ***NOIP** that can be used for all interfaces or a single interface.



```
9/26/16                                Work with Exit Point User Access

Position to...      Starting characters

Type options, press Enter.
  2=Edit  3=Copy  4=Delete  5=Display

Opt  User Name      Exit Point  Allowed IP
--  -
-    *ALLOBJ        *ALL      *ALLIP
-    *NOIPCTL       SQCLI     *NOIP
-    PSCUSER        DRDADDM   9.5.*.*
-    QSECOFR        G        *ALL      *ALLIP
-    QSECOFR        G        *ALL      *NOIP
-    QWKUSER        *ALL      *ALLIP
-    QWKUSER        *ALL      *ALLIP
```

Save / Restore of Network Interface Firewall Configuration

Occasionally, it might be wise to save the configuration elements of the Exit Point Tool. To facilitate the Save and Restore of the configuration elements, a couple of new programs have been added to assist in these tasks.

To save your existing configuration:

```
CHGCURLIB QZRDSECXPT
```

```
CALL QZRDSECXPT/XPCFGSAV
```

The program will create the library XPTTOOL if it is not found and save the configuration elements into the save file (SAVF) **XPCFGBAK** in XPTTOOL.

To restore the configuration:

```
CHGCURLIB QZRDSECXPT
```

```
CALL QZRDSECXPT/XPCFGRST PARM(XPTTOOL XPCFGBAK)
```

Report of Users Defined to Exit Points

To print a report of Users defined to the Exit Points, press **F7** or **F8** from the Work with Exit Point User Access screen. Two reports are possible, a short report that prints the contents as displayed on the screen and a long report that explodes the group members so that a clear picture of all Users defined to use Exit Points is possible. The reports should print within moments (depending on the number of users on the system and the number of users defined to the Exit Points) and a confirmation displayed at the bottom of the screen...

F3=Exit F5=Refresh List F6=Create F7=Print F9=Comm
The User Access audit report has been printed

To view the report, use WRKSPLF or IBM i Navigator or your favorite spool file viewer (or printed output) to review the contents. For Users that are Group profiles (look for the "G" indicator in the report) be sure to review the members of the Group to understand the full extent of the users who have access to an Exit Point. In the long report, an "M" indicates the user is a member of a group defined to an Exit Point. The following are examples of the two reports:

EXIT POINT TOOL (XPT) - USER ACCESS AUDIT REPORT

5:02pm 08/17/2012

User Name	Exit Point	Internet Address
TAFORD	*ALL	*ALLIP
SHARONSU	DSTPGMC	9.5.157.158
SHARONSU	FTPLOGON	9.5.157.158
ERNEST	OJDBC	*ALLIP
BADINGB	*ALL	*ALLIP
BARLEN	*ALL	*ALLIP
QSECOFR	*ALL	*ALLIP
QEJBSVR G	*ALL	*ALLIP

----- End of Report -----

EXIT POINT TOOL (XPT) - USER ACCESS AUDIT REPORT

10:59pm 08/17/2012

User Name	Exit Point	Internet Address	Group Association
BADINGB	*ALL	*ALLIP	
BARLEN	*ALL	*ALLIP	
ERNEST	OJDBC	*ALLIP	
QEJBSVR G	*ALL	*ALLIP	
ORDARS400 G	OJDBC	*ALLIP	
QSECOFR	*ALL	*ALLIP	
SHARONSU	DSTPGMC	9.5.157.158	
SHARONSU	FTPLOGON	9.5.157.158	
TAFORD	*ALL	*ALLIP	
OPYMWEB M	*ALL	*ALLIP	QEJBSVR
ORDARS4001 M	OJDBC	*ALLIP	ORDARS400
ORDARS4002 M	OJDBC	*ALLIP	ORDARS400
ORDARS4003 M	OJDBC	*ALLIP	ORDARS400
ORDARS4004 M	OJDBC	*ALLIP	ORDARS400
ORDARS4005 M	OJDBC	*ALLIP	ORDARS400

----- End of Report -----

Scheduling Reports

Two example programs exist for reporting exit point entries for the last 24 hours:

SCDXPT0 Outputs to a specified file for a specified Exit Point (or *ALL). Existing data if any is overwritten.
SCDXPT2 Outputs to a predefined set of files for several Exit Points. Existing data if any is overwritten.

SCDXPT2 creates a set of daily files in library (a passed_variable of CHAR(10) to the program) for the two XPT reporting options on the XPT Menu:

XPDRDDM	DDM/DRDA Journal Entries
XPFILSV	File Server (IFS) Journal Entries
XPFTPLO	FTP Logon Journal Entries
XPFTPCL	FTP Client Requests Journal Entries
XPFTPSV	FTP Server Requests Journal Entries
XPOJDBC	ODBC/JDBC Journal Entries
XPRMTCM	Remote Comand Journal Entries
XPSIGNO	SIGNON Server Journal Entries
XPTELNT	TELNET - 5250 - Journal Entries
XPUBYXP	Users by Exit Point
XPXBYXP	Exit Point by Users
XPXBYST	Exit Point by Status
XPUBYST	User by Status
XPIBYST	IP Address by Status
XPXBYIP	Exit Point by IP Address and User
XPIBYXU	IP Address by Exit Point by User
XPBYGRP	Exit Point accesses through Group
XPXBYNN	Exit Point accesses by non Exit Point User(s)
XPBYIPA	Exit Point by IP Address
XPCMDRS	Restricted Commands

Add (or change) to the job scheduler on the systems you wish to track exit point use for daily processing as follows:

```
ADDJOBSCDE JOB(XPJRNE24)
            CMD(CALL PGM(QZRDSEXP/SCDXPT0) PARM(*ALL XPTRCKNG QGPL))
            FRQ(*WEEKLY)
            SCDDATE(*NONE)
            SCDDAY(*ALL)
            SCDTIME('23:55:00')
            RCYACN(*SBMRLS)
            USER(QSECOFR)
            TEXT('Exit Point Journal Entry Reports in the Last 24 Hours')
```

```
ADDJOBSCDE JOB(XPRPTS24)
            CMD(CALL PGM(QZRDSEXP/SCDXPT2) PARM(QGPL))
            FRQ(*WEEKLY)
            SCDDATE(*NONE)
            SCDDAY(*ALL)
            SCDTIME('23:55:00')
            RCYACN(*SBMRLS)
            USER(QSECOFR)
            TEXT('Exit Point Reports for the Last 24 Hours')
```

NOTE the following in the above two examples:

- The schedules are set to run daily at 11:55 PM
- The Job Names (XPJRNE24 and XPRPTS24) could have been anything
- The name of the Library (QGPL) could have been anything
- The name of the File (XPTRCKNG) could have been anything

The key part of these job schedule examples is the CALL component. In the first example, note the following:

```
CALL PGM(QZRDSECXPT/SCDXPT0) PARM( exit_definition output_file output_library )
```

where

- the first parameter defines either *ALL or an Exit Point Definition of interest (see option 2 on the XPT Menu)
- the 2nd parameter defines the output file name.
- the 3rd parameter defines the output library.

In the second example, note the following:

```
CALL PGM(QZRDSECXPT/SCDXPT2) PARM( output_library )
```

where

the only parameter defines the output library.

Fundamentally, the above two SCDXPTx programs use one or both programs...

QZRDSECXPT/VUXPTJREP	View Exit Point Journal Entries
QZRDSECXPT/VUXPTRPTP	View Exit Point Reports

View Exit Point Journal Entries (VUXPTJREP)

Exit Point Journal Entries can be viewed through XPTMENU option 4. Additionally, they can be sent to a printer or file through a program call or through a scheduled job as described above. The CALL structure is as follows:

```
CALL PGM(QZRDSEXP/VUXPTJREP)
      PARM(  exit_defn
            exit_user
            start_date
            start_time
            end_date
            end_time
            selection_type
            output_type
            output_file
            output_library
            file_option      )
```

Where:

- exit_defn	---> Exit Point:	The Exit Point Definition defined to option 2 of the XPT Menu CHAR(10)
- exit_user	---> Exit Point User:	The Exit Point User causing the entry CHAR(10)
- start_date	---> Start Date:	Date in YYYY-MM-DD ISO format CHAR(10)
- start_time	---> Start Time:	Time in HH.MM.SS ISO format CHAR(8)
- end_date	---> End Date:	Date in YYYY-MM-DD ISO format CHAR(10)
- end_time	---> End Time:	Time in HH.MM.SS ISO format CHAR(8)
- selection_type	---> Selection Type:	The category of data to view CHAR(1) P=Pass F=Fail L=Log Only E=Errors A=All B=Pass/Fail N=No IP Address I=Informational
- output_type	---> Output Type:	*DISPLAY, *PRINT, *FILE CHAR(8)
- output_file	---> File Name:	If Output Type is *FILE the target file (a name must always be present regardless of Output Type) CHAR(10)
- output_library	---> Library:	If Output Type is *FILE the library of target file (a name must always be present regardless of Output Type) CHAR(10)
- file_option	---> File Option:	A(Add) or R(Replace) If Output Type is *FILE whether to Add/Replace contents of the target file (a name must always be present regardless of Output Type) CHAR(1)

Example:

```
CALL PGM(QZRDSEXP/VUXPTJREP)
      PARM(FILESRVR BADINGB '2018-11-25' '00.00.00' '2018-11-25' '23.59.59' A *FILE XPJRN RPT QGPL R)
```

View Exit Point Reports (VUXPTRPTP)

Exit Point Reportstries can be viewed through XPTMENU option 5. Additionally, they can be sent to a printer or file through a program call or through a scheduled job as described above. The CALL structure is as follows:

```
CALL PGM(QZRDSEXP/VUXPTRPTP)
  PARM(   USR_by_XP
         XP_by_USR
         XP_by_STS
         USR_by_STS
         IP_by_STS
         XP_by_IP_US
         IP_by_XP_US
         XP_thru_GRP
         XP_by_NX_US
         XP_by_IP
         RST_CMDS
         exit_user
         start_date
         start_time
         end_date
         end_time
         output_type
         output_file
         output_library
         file_option      )
```

Where:

- USR_by_XP	---> User by Exits	Report Selector - must be Y or N CHAR(1)
- XP_by_USR	---> Exits by User	Report Selector - must be Y or N CHAR(1)
- XP_by_STS	---> Exits by Status	Report Selector - must be Y or N CHAR(1)
- USR_by_STS	---> User by Status	Report Selector - must be Y or N CHAR(1)
- IP_by_STS	---> IP by Status	Report Selector - must be Y or N CHAR(1)
- XP_by_IP_US	---> Exit by IP/User	Report Selector - must be Y or N CHAR(1)
- IP_by_XP_US	---> IP by Exit/User	Report Selector - must be Y or N CHAR(1)
- XP_thru_GRP	---> Exit by Groups	Report Selector - must be Y or N CHAR(1)
- XP_by_NX_US	---> Exit by non User	Report Selector - must be Y or N CHAR(1)
- XP_by_IP	---> Exit by IP	Report Selector - must be Y or N CHAR(1)
- RST_CMDS	---> Restricted CMDs	Report Selector - must be Y or N CHAR(1)
- exit_user	---> Exit Point User:	The Exit Point User causing the entry CHAR(10)
- start_date	---> Start Date:	Date in YYYY-MM-DD ISO format CHAR(10)
- start_time	---> Start Time:	Time in HH.MM.SS ISO format CHAR(8)
- end_date	---> End Date:	Date in YYYY-MM-DD ISO format CHAR(10)
- end_time	---> End Time:	Time in HH.MM.SS ISO format CHAR(8)
- output_type	---> Output Type:	*DISPLAY, *PRINT, *FILE CHAR(8)
- output_file	---> File Name:	If Output Type is *FILE the target file (a name must always be present regardless of Output Type) CHAR(10)
- output_library	---> Library:	If Output Type is *FILE the library of target file (a name must always be present regardless of Output Type) CHAR(10)
- file_option	---> File Option:	A(Add) or R(Replace) If Output Type is *FILE whether to Add/Replace contents of the target file (a name must always be present regardless of Output Type) CHAR(1)

Example:

```
CALL PGM(QZRDSECXPT/VUXPTRPTP)
  PARM(Y N Y N N N N N N N *ALL '2018-11-25' '00.00.00' '2018-11-25' '23.59.59' *FILE CARTOUT QGPL R)
```

TIP: When using the VUxxxxx programs the general difficulty is with dates

In a CL Program define some fields as follows:

```
DCL      &CURDAT   *CHAR      10
DCL      &CURRYR   *CHAR       2
DCL      &CURRMO   *CHAR       2
DCL      &CURRDY   *CHAR       2
```

Then retrieve the date related system values:

```
RTVSYSVAL SYSVAL(QYEAR  ) RTNVAR(&CURRYR)
RTVSYSVAL SYSVAL(QMONTH ) RTNVAR(&CURRMO)
RTVSYSVAL SYSVAL(QDAY   ) RTNVAR(&CURRDY)
```

Then change the data parameter to use as follows:

```
CHGVAR      &CURDAT ('20' *CAT &CURRYR *TCAT '-' *CAT &CURRMO *TCAT '-' *CAT &CURRDY )
```

(of course, there are many ways to resolve dates. This is just a simple example).

Then use in the call to the program:

```
CALL PGM(QZRDSECXPT/VUXPTJREP)
  PARM(QJDBC *ALL &CURDAT '00.00.00' &CURDAT '23.59.59' A *FILE XPTODBC YOURLIB R)
```

Exit Point Job Schedule Example Program 1 (SCDXPT0)

```

/* ***** */
/* (C) COPYRIGHT IBM CORP. 2012, 2013, 2019 */
/* The source code for this program is not published or otherwise divested of its trade secrets, */
/* irrespective of what has been deposited with the U.S. Copyright Office. */
/* Author(s): Terry Ford Date: 15-MAY-2019 */
/* ***** */

PGM      PARM(&XPTDEF &XPTFIL &XPTLIB)

DCL      &XPTDEF  *CHAR    10
DCL      &XPTFIL  *CHAR    10
DCL      &XPTLIB  *CHAR    10
DCL      &FOUND   *CHAR     1  'N'
DCL      &CURDAT  *CHAR    10
DCL      &CURRYR  *CHAR     2
DCL      &CURRMO  *CHAR     2
DCL      &CURRDY  *CHAR     2
DCL      &STR     *CHAR     8  '00.00.00'
DCL      &END     *CHAR     8  '23.59.59'

DCLF     FILE(QZRDSEXP/EXTPDF)

IF       ((&XPTDEF *EQ ' ') *OR +
          (&XPTFIL *EQ ' ') *OR +
          (&XPTLIB *EQ ' ')) DO
          SNDPGMMSG MSG('A required input parameter is missing')
          GOTO  EXIT
          ENDDO

CHKOBJ   OBJ(QSYS/&XPTLIB) OBJTYPE(*LIB)
MONMSG   (CPF9801 CPF9810) EXEC(DO)
          SNDPGMMSG MSG('Invalid Output Library specified')
          GOTO  EXIT
          ENDDO

ADDLIB   QZRDSEXP
MONMSG   MSGID(CPF2103)
IF       (&XPTDEF *EQ '*ALL') DO
          CHGVAR &FOUND 'Y'
          GOTO  ENDREED
          ENDDO

REED:    RCVF
          MONMSG  MSGID(CPF0864) EXEC(GOTO ENDREED)
IF       (&XPDEFN *NE &XPTDEF) GOTO REED
CHGVAR   &FOUND 'Y'
GOTO     REED
ENDREED:

IF       (&FOUND = 'N') DO
          SNDPGMMSG MSG('Invalid Exit Point specified')
          GOTO  EXIT
          ENDDO

RTVSYSVAL SYSVAL(QYEAR ) RTNVAR(&CURRYR)
RTVSYSVAL SYSVAL(QMONTH ) RTNVAR(&CURRMO)
RTVSYSVAL SYSVAL(QDAY  ) RTNVAR(&CURRDY)
CHGVAR   &CURDAT ('20' *CAT &CURRYR *TCAT '-' *CAT &CURRMO *TCAT '-' *CAT &CURRDY )
CALL     PGM(QZRDSEXP/VUXPTJREP) +
          PARM(&XPTDEF *ALL &CURDAT &STR &CURDAT &END A *FILE &XPTFIL &XPTLIB R)

EXIT:    ENDPGM

```

Exit Point Job Schedule Example Program 2 (SCDXPT2)

```

/* ***** */
/* (C) COPYRIGHT IBM CORP. 2012, 2013, 2019 */
/* The source code for this program is not published or otherwise divested of its trade secrets, */
/* irrespective of what has been deposited with the U.S. Copyright Office. */
/* Author(s): Terry Ford Date: 15-MAY-2019 */
/* ***** */

PGM          PARM(&XPTLIB)

DCL          &XPTDEF  *CHAR      10
DCL          &XPTFIL  *CHAR      10
DCL          &XPTLIB  *CHAR      10

DCL          &CURDAT  *CHAR      10
DCL          &CURRYR  *CHAR      2
DCL          &CURRMO  *CHAR      2
DCL          &CURRDY  *CHAR      2

DCL          &STR      *CHAR      8  '00.00.00'
DCL          &END      *CHAR      8  '23.59.59'

MONMSG      MSGID(CPF2105 CPF2110)

IF          (&XPTLIB *EQ ' ') DO
                SNDPGMMSG MSG('A required input parameter is missing')
                GOTO      EXIT
            ENDDO

CHKOBJ      OBJ(QSYS/&XPTLIB) OBJTYPE(*LIB)
MONMSG      (CPF9801 CPF9810) EXEC(DO)
                SNDPGMMSG MSG('Invalid Output Library specified')
                GOTO      EXIT
            ENDDO

ADDLIB     QZRDSEXP
MONMSG      MSGID(CPF2103)

RTVSYSVAL   SYSVAL(QYEAR ) RTNVAR(&CURRYR)
RTVSYSVAL   SYSVAL(QMONTH ) RTNVAR(&CURRMO)
RTVSYSVAL   SYSVAL(QDAY ) RTNVAR(&CURRDY)

CHGVAR      &CURDAT ('20' *CAT &CURRYR *TCAT '-' *CAT &CURRMO *TCAT '-' *CAT &CURRDY )

CALL        PGM(QZRDSEXP/VUXPTJREP) PARM(DRDADD *ALL &CURDAT &STR &CURDAT &END A *FILE XPDRDDM &XPTLIB R)
CHGOBJD     &XPTLIB/XPDRDDM *FILE TEXT('DDM/DRDA Journal Entries ')
CALL        PGM(QZRDSEXP/VUXPTJREP) PARM(FILESRV *ALL &CURDAT &STR &CURDAT &END A *FILE XPFILSV &XPTLIB R)
CHGOBJD     &XPTLIB/XPFILSV *FILE TEXT('File Server (IFS) Journal Entries ')
CALL        PGM(QZRDSEXP/VUXPTJREP) PARM(FTPLOGON *ALL &CURDAT &STR &CURDAT &END A *FILE XPFTPLO &XPTLIB R)
CHGOBJD     &XPTLIB/XPFTPLO *FILE TEXT('FTP Logon Journal Entries ')
CALL        PGM(QZRDSEXP/VUXPTJREP) PARM(FTPCLN *ALL &CURDAT &STR &CURDAT &END A *FILE XPFTPCL &XPTLIB R)
CHGOBJD     &XPTLIB/XPFTPCL *FILE TEXT('FTP Client Requests Journal Entries ')
CALL        PGM(QZRDSEXP/VUXPTJREP) PARM(FTPSVR *ALL &CURDAT &STR &CURDAT &END A *FILE XPFTPSV &XPTLIB R)
CHGOBJD     &XPTLIB/XPFTPSV *FILE TEXT('FTP Server Requests Journal Entries ')
CALL        PGM(QZRDSEXP/VUXPTJREP) PARM(OJDBC *ALL &CURDAT &STR &CURDAT &END A *FILE XPOJDBC &XPTLIB R)
CHGOBJD     &XPTLIB/XPOJDBC *FILE TEXT('ODBC/JDBC Journal Entries ')
CALL        PGM(QZRDSEXP/VUXPTJREP) PARM(RMTCMD *ALL &CURDAT &STR &CURDAT &END A *FILE XPRMTCM &XPTLIB R)
CHGOBJD     &XPTLIB/XPRMTCM *FILE TEXT('Remote Command Journal Entries ')
CALL        PGM(QZRDSEXP/VUXPTJREP) PARM(SIGNON *ALL &CURDAT &STR &CURDAT &END A *FILE XPSIGNO &XPTLIB R)
CHGOBJD     &XPTLIB/XPSIGNO *FILE TEXT('SIGNON Server Journal Entries ')
CALL        PGM(QZRDSEXP/VUXPTJREP) PARM(TELNET *ALL &CURDAT &STR &CURDAT &END A *FILE XPTELNT &XPTLIB R)
CHGOBJD     &XPTLIB/XPTELNT *FILE TEXT('TELNET - 5250 - Journal Entries ')

```

```

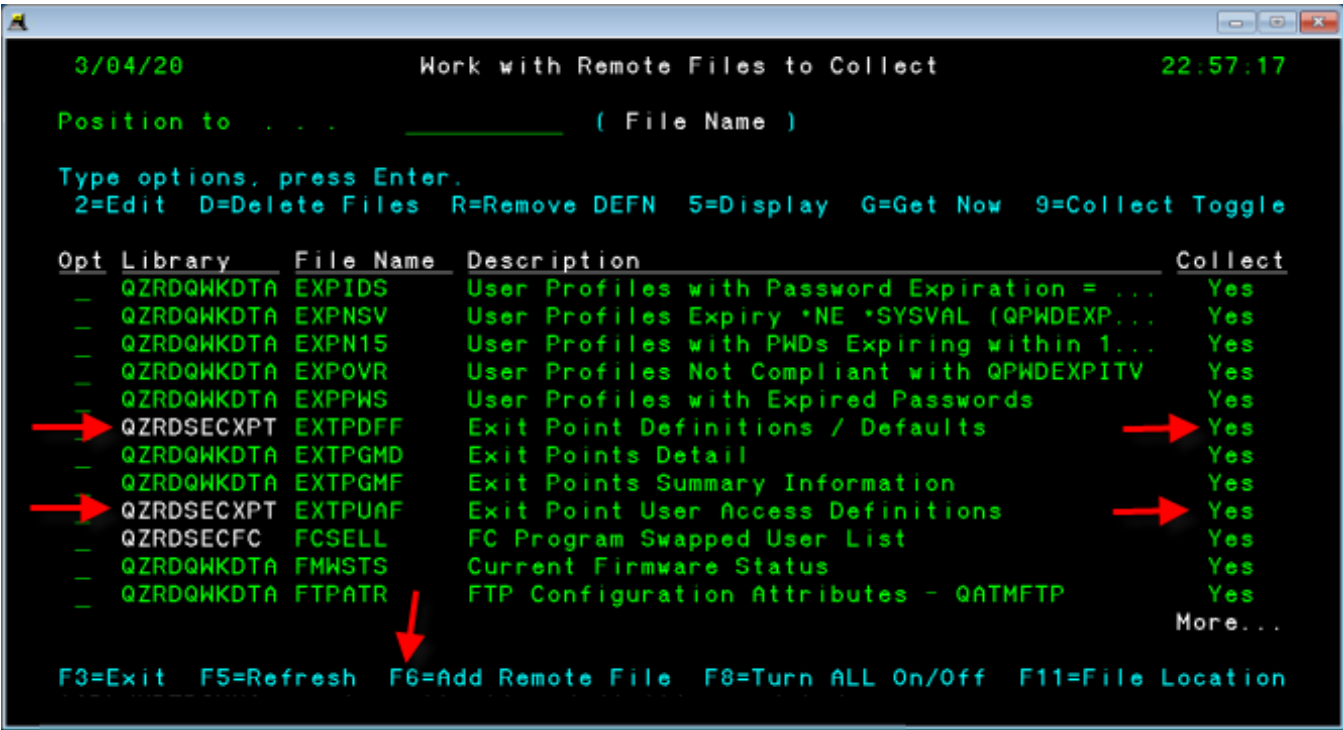
CALL      PGM(QZRDSECP/VPTRPT) PARM(Y N N N N N N N N N N *ALL &CURDAT &STR &CURDAT &END *FILE XPBYXP &XPTLIB R)
CHGOBJD  &XPTLIB/XPBYXP *FILE TEXT('Users by Exit Point
CALL      PGM(QZRDSECP/VPTRPT) PARM(N Y N N N N N N N N N N *ALL &CURDAT &STR &CURDAT &END *FILE XPBYXP &XPTLIB R)
CHGOBJD  &XPTLIB/XPBYXP *FILE TEXT('Exit Point by Users
CALL      PGM(QZRDSECP/VPTRPT) PARM(N N Y N N N N N N N N N *ALL &CURDAT &STR &CURDAT &END *FILE XPBYST &XPTLIB R)
CHGOBJD  &XPTLIB/XPBYST *FILE TEXT('Exit Point by Status
CALL      PGM(QZRDSECP/VPTRPT) PARM(N N N Y N N N N N N N N *ALL &CURDAT &STR &CURDAT &END *FILE XPBYST &XPTLIB R)
CHGOBJD  &XPTLIB/XPBYST *FILE TEXT('User by Status
CALL      PGM(QZRDSECP/VPTRPT) PARM(N N N N Y N N N N N N N *ALL &CURDAT &STR &CURDAT &END *FILE XPBYST &XPTLIB R)
CHGOBJD  &XPTLIB/XPBYST *FILE TEXT('IP Address by Status
CALL      PGM(QZRDSECP/VPTRPT) PARM(N N N N N Y N N N N N N *ALL &CURDAT &STR &CURDAT &END *FILE XPBYIP &XPTLIB R)
CHGOBJD  &XPTLIB/XPBYIP *FILE TEXT('Exit Point by IP Address and User
CALL      PGM(QZRDSECP/VPTRPT) PARM(N N N N N N Y N N N N N *ALL &CURDAT &STR &CURDAT &END *FILE XPBYXU &XPTLIB R)
CHGOBJD  &XPTLIB/XPBYXU *FILE TEXT('IP Address by Exit Point by User
CALL      PGM(QZRDSECP/VPTRPT) PARM(N N N N N N N Y N N N N *ALL &CURDAT &STR &CURDAT &END *FILE XPBYGRP &XPTLIB R)
CHGOBJD  &XPTLIB/XPBYGRP *FILE TEXT('Exit Point accesses through Group
CALL      PGM(QZRDSECP/VPTRPT) PARM(N N N N N N N N Y N N N *ALL &CURDAT &STR &CURDAT &END *FILE XPBYNN &XPTLIB R)
CHGOBJD  &XPTLIB/XPBYNN *FILE TEXT('Exit Point accesses by non Exit Point User(s)')
CALL      PGM(QZRDSECP/VPTRPT) PARM(N N N N N N N N N Y N N *ALL &CURDAT &STR &CURDAT &END *FILE XPBYIPA &XPTLIB R)
CHGOBJD  &XPTLIB/XPBYNN *FILE TEXT('Exit Point by IP Address
CALL      PGM(QZRDSECP/VPTRPT) PARM(N N N N N N N N N N Y *ALL &CURDAT &STR &CURDAT &END *FILE XPCMDRS &XPTLIB R)
CHGOBJD  &XPTLIB/XPBYNN *FILE TEXT('Restricted Command Usage

```

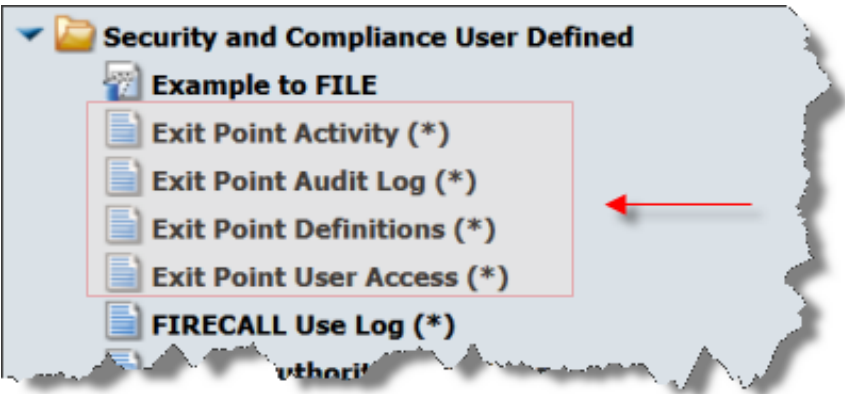
EXIT: [ENDPGM](#)

Compliance Automation Reporting Tool (CART) Integration

Using the Compliance Automation Reporting Tool (CART) you can centralize reporting of Exit Point settings and activity. From the Central Server of CART navigate to the ENTMENU and run option 56 to Work with Remote Files to Collect. Press F6 to add the Exit Point files EXTPDFF, EXTPUAF, and XPTLOG to the collector. If you have scheduled the SCDXPT0 and/or SCDXPT2 programs to extract activity, you should also consider adding the file QGPL/XPTRCKNG (or the named defined) to the collector.



Within the CART Web Query Portal there are 3 reports already defined in the User Defined section to report on the Exit Point Files.



See the document [Importing Exit Point Reports into Web Query \(CART \).docx](#) for information on importing these reports into DB2 Web Query.

Exit Point Activity Report

Provides parameters to prefilter Exit Point activity with the ability to export to other formats

Exit Point Activity																
System(s):																
Exit Point User(s):																
Exit Point(s):																
Status(s):																
Enterprise System Name	Journal Date	Journal Time	Journal Type	Current User	Job Name	Job User	Job Number	Program Library	Program Name	Remote Port	Remote IP Address	XPT User	XPT Type	XPT Name	Logon By	XPT Status
CTCI005C	2020/03/03	00:05:22	LA	QWKUSER	QWTSRVR	QUSER	460598	QZRDSECP	QDRDADM	45048	9.5.168.75	QWKUSER	*DRDA	NETW_ATTR		*LOGMODE
		00:08:24	LA	QWKUSER	QWTSRVR	QUSER	460598	QZRDSECP	QDRDADM	58496	9.5.168.75	QWKUSER	*DRDA	NETW_ATTR		*LOGMODE
		00:11:25	LA	QWKUSER	QWTSRVR	QUSER	460598	QZRDSECP	QDRDADM	47472	9.5.168.75	QWKUSER	*DRDA	NETW_ATTR		*LOGMODE
		00:14:27	LA	QWKUSER	QWTSRVR	QUSER	460598	QZRDSECP	QDRDADM	37160	9.5.168.75	QWKUSER	*DRDA	NETW_ATTR		*LOGMODE
		00:17:28	LA	QWKUSER	QWTSRVR	QUSER	460598	QZRDSECP	QDRDADM	28985	9.5.168.75	QWKUSER	*DRDA	NETW_ATTR		*LOGMODE
		00:20:30	LA	QWKUSER	QWTSRVR	QUSER	460598	QZRDSECP	QDRDADM	60225	9.5.168.75	QWKUSER	*DRDA	NETW_ATTR		*LOGMODE
		00:23:32	LA	QWKUSER	QWTSRVR	QUSER	460598	QZRDSECP	QDRDADM	28984	9.5.168.75	QWKUSER	*DRDA	NETW_ATTR		*LOGMODE
		00:26:33	LA	QWKUSER	QWTSRVR	QUSER	460598	QZRDSECP	QDRDADM	37187	9.5.168.75	QWKUSER	*DRDA	NETW_ATTR		*LOGMODE
		00:29:35	LA	QWKUSER	QWTSRVR	QUSER	460598	QZRDSECP	QDRDADM	37184	9.5.168.75	QWKUSER	*DRDA	NETW_ATTR		*LOGMODE
		00:32:36	LA	QWKUSER	QWTSRVR	QUSER	460598	QZRDSECP	QDRDADM	37440	9.5.168.75	QWKUSER	*DRDA	NETW_ATTR		*LOGMODE
		00:35:38	LA	QWKUSER	QWTSRVR	QUSER	460598	QZRDSECP	QDRDADM	42944	9.5.168.75	QWKUSER	*DRDA	NETW_ATTR		*LOGMODE
		00:38:39	LA	QWKUSER	QWTSRVR	QUSER	460598	QZRDSECP	QDRDADM	50753	9.5.168.75	QWKUSER	*DRDA	NETW_ATTR		*LOGMODE
		00:41:41	LA	QWKUSER	QWTSRVR	QUSER	460598	QZRDSECP	QDRDADM	37465	9.5.168.75	QWKUSER	*DRDA	NETW_ATTR		*LOGMODE
		00:44:43	LA	QWKUSER	QWTSRVR	QUSER	460598	QZRDSECP	QDRDADM	58664	9.5.168.75	QWKUSER	*DRDA	NETW_ATTR		*LOGMODE
		00:47:44	LA	QWKUSER	QWTSRVR	QUSER	460598	QZRDSECP	QDRDADM	60153	9.5.168.75	QWKUSER	*DRDA	NETW_ATTR		*LOGMODE
		00:50:46	LA	QWKUSER	QWTSRVR	QUSER	460598	QZRDSECP	QDRDADM	37514	9.5.168.75	QWKUSER	*DRDA	NETW_ATTR		*LOGMODE
		00:53:47	LA	QWKUSER	QWTSRVR	QUSER	460598	QZRDSECP	QDRDADM	37523	9.5.168.75	QWKUSER	*DRDA	NETW_ATTR		*LOGMODE
		00:56:49	LA	QWKUSER	QWTSRVR	QUSER	460598	QZRDSECP	QDRDADM	37585	9.5.168.75	QWKUSER	*DRDA	NETW_ATTR		*LOGMODE
		00:59:50	LA	QWKUSER	QWTSRVR	QUSER	460598	QZRDSECP	QDRDADM	37684	9.5.168.75	QWKUSER	*DRDA	NETW_ATTR		*LOGMODE

Exit Point Audit Log Report

Provides parameters to prefilter Exit Point audit log with the ability to export to other formats. Only reports the last 72 hours.

Exit Point Audit Log (last 72 hours)									
Data Center(s):									
System Purpose:									
System(s):									
Exit Point Name(s):									
System Name	Date	Time	Reporting Program	Entry Created By	File Modified	File Action	Scope of Action	User Impacted	Exit Point
CTCI005C	20/03/05	17:32:48	DLTXPUAP	TAFORD	EXTPUAF	DELETE	*ALLIP	FCEMRGRP	DRDADM
		17:32:17	WRKXPUAP	TAFORD	EXTPUAF	VIEW			
		15:35:05	WRKRSTCP	TAFORD	EXTPCMF	UPDATE	WRKREGINF	UNKNOWN	CMDEXIT
		15:35:00	WRKRSTCP	TAFORD	EXTPCMF	VIEW			
		15:34:57	WRKXPDFP	TAFORD	EXTPDFP	VIEW			
		15:02:30	WRKRSTCP	TAFORD	EXTPCMF	UPDATE	ADDSVRAUTE	UNKNOWN	CMDEXIT
		15:02:26	WRKRSTCP	TAFORD	EXTPCMF	VIEW			
		14:20:02	WRKRSTCP	TAFORD	EXTPCMF	UPDATE	WRKFCNUSG	UNKNOWN	CMDEXIT
		14:19:53	WRKRSTCP	TAFORD	EXTPCMF	VIEW			
		14:12:53	WRKRSTCP	TAFORD	EXTPCMF	UPDATE	PWRDWNYS	ALL	CMDEXIT
		14:12:43	WRKRSTCP	TAFORD	EXTPCMF	VIEW			
		14:12:11	WRKRSTCP	TAFORD	EXTPCMF	VIEW			
		20/03/04 22:32:52	CRTXPUAP	TAFORD	EXTPUAF	CREATE	*ALLIP	FCEMRGRP	DRDADM
		22:32:38	WRKXPUAP	TAFORD	EXTPUAF	VIEW			
		22:31:49	WRKXPUAP	TAFORD	EXTPUAF	VIEW			
		21:23:31	WRKXPDFP	TAFORD	EXTPDFP	VIEW			
		20:58:45	WRKXPDFP	TAFORD	EXTPDFP	VIEW			

Exit Point Definitions Report

Provides parameters to prefilter Exit Point definitions with the ability to export to other formats

Exit Point Definitions

Data Center(s):

System Purpose:

System(s):

Exit Point Name(s):

System Name	Remote Date	Exit Point Definition	Exit Point Name	Exit Point Format	Exit Point Program	Exit Point Program Library	Status	Exit Point Description	Command Prompt	On Sw
CTCI005C	2020/03/04	DRDADDMM	CHGNETA	DDMACC	QDRDADDMM	QZRDSECXPT	*ADDED2NAT	DRDA/DDM Logon	Y	*L
		DSTPGMC	QIBM_QZRC_RMT	CZRC0100	QRMTCMD	QZRDSECXPT		Distributed Program Call	Y	*L
		DTAQSRVR	QIBM_QZHQ_DATA_QUEUE	ZHQ00100	QDQSRVR	QZRDSECXPT		Host Servers DATAQ Server	Y	*L
		FILESVR	QIBM_QPWFS_FILE_SERV	PWFS0100	QFLSRVR	QZRDSECXPT		Host Servers File Server	Y	*L
		FTPCLNRQ	QIBM_QTMF_CLIENT_REQ	VLRQ0100	QTMFXCSREQ	QZRDSECXPT		FTP Client Request Validation	Y	
		FTPLOGON	QIBM_QTMF_SVR_LOGON	TCPL0100	QTMFSVRLOG	QZRDSECXPT	*ADDED2XPT	FTP Server Logon	Y	*L
		FTPSVRREQ	QIBM_QTMF_SERVER_REQ	VLRQ0100	QTMFXCSREQ	QZRDSECXPT		FTP Request Validation	Y	
		HSTPRT	QIBM_QNPS_ENTRY	ENTRO100	QNPSEV	QZRDSECXPT		Host Server Net Print Server	Y	*L
		OJDBC	QIBM_QZDA_INIT	ZDAI0100	QZDAINIT	QZRDSECXPT		DB Logon - ODBC/JDBC/File XFR	Y	
		ONDB1	QIBM_QZDA_NDB1	ZDAD0100	QZDANDB1	QZRDSECXPT		Native DB OPs via ODBC/JDBC	Y	*L
		OROI1	QIBM_QZDA_ROI1	ZDAR0100	QZDAROI1	QZRDSECXPT		Object INFO REQs via ODBC/JDBC	Y	*L
		OSQL1	QIBM_QZDA_SQL1	ZDAQ0100	QZDASQL1	QZRDSECXPT		DB Server SQL Access	Y	*L
		OSQL2	QIBM_QZDA_SQL2	ZDAQ0200	QZDASQL2	QZRDSECXPT		DB Server SQL Access	Y	
		REXECREQ	QIBM_QTMX_SERVER_REQ	VLRQ0100	QTMFXCSREQ	QZRDSECXPT		REXEC Request Validation	Y	*L
		RMTCMD	QIBM_QZRC_RMT	CZRC0100	QRMTCMD	QZRDSECXPT		RMTCMD Logon	Y	
		RMTLOGON	QIBM_QTMX_SVR_LOGON	TCPL0100	QTMFSVRLOG	QZRDSECXPT		REXEC Server Logon	Y	

Exit Point User Access Report

Provides parameters to prefilter Exit Point User Access definitions with the ability to export to other formats

Exit Point User Access

System Purpose:

System(s):

Exit Point Name(s):

Exit Point User(s):

System Name	Remote Date	User Name	User Type	Exit Point	Allowed IP Address
CTCI005C	2020/03/04	*ALLOBJ	User	*ALL	*ALLIP
		*NOIPCTL	User	SQCLI	*NOIP
		QSECOFR	User	*ALL	*ALLIP
					*NOIP
		QWKUSER	User	DRDADDMM	*ALLIP
		TAFORD	User	FTPLOGON	*ALLIP
CTCV71	2020/03/04	*ALLOBJ	User	*ALL	*ALLIP
		*NOIPCTL	User	SQCLI	*NOIP
		BADINGB	User	*ALL	*ALLIP
		BRUCE	User	SIGNON	*ALLIP
		QSECOFR	User	*ALL	*ALLIP
					*NOIP
		QWKUSER	User	DRDADDMM	*ALLIP
		QWQADMIN	GROUP	*ALL	*ALLIP
		RDABRB	User	*ALL	*ALLIP
		TAFORD	User	*ALL	*ALLIP

Report generated by Security and Compliance Tools for IBM i on: March 04, 2020 at 23:11:02

Activity Logging of Exit Point Tool Usage

An important aspect of security is security monitoring. Exit Points are generally used to restrict access to user interfaces. A nefarious user may attempt to hide his actions or gain access by turning “*OFF” or de-registering the Exit Program. For this reason, regular security monitoring should take place that includes the tools used to secure the system. The Exit Point Tool includes a log of all accesses and changes that occur thru the Exit Point Tool interfaces and can be found in the file XPTLOG in library QZRDSEXP. An example of the contents of this file is provided below. Validate that those making accessing the Exit Point Tool are authorized to do so.

In addition to the Exit Point Tool Log, a regular check of the security audit journal QAUDJRN should be done to ensure that tampering of the Exit Point Tool library, files, and programs are not occurring. **This should be done for all security related tools used on the system.** A regular inspection of the following journal entry types should be done:

- AD** – check for changes to auditing for the library or objects in QZRDSEXP
- AF** – check for invalid attempts to access the library or objects in QZRDSEXP
- CA** – check for changes to authority for the library or objects in QZRDSEXP
- GR** – check for Exit Point access/registration/deregistration by users outside of the Exit Point Tool
- ZC** – check for changes to the library or objects in QZRDSEXP

Exit Point Audit Log Example

Reporting Program	Date YY/MM/DD	Time HH:MM:SS	Entry Created By	File Modified	File Action	Scope of Action	User Impacted	Exit Point	Miscellaneous Information
WRKXPDFP	08/16/12	16:47:26	TAFORD	EXTPDFP	VIEW	-	-	-	-
CRTXPUAP	08/16/12	17:18:45	TAFORD	EXTPUAF	CREATE	*ALLIP	SHARONSU	DRDADD	-
WRKXPUAP	08/16/12	17:18:05	TAFORD	EXTPUAF	VIEW	-	-	-	-
CHGXPUAP	08/16/12	17:36:56	TAFORD	EXTPUAF	CHANGE	*ALL	SHARONSU	DRDADD	PREV PNT=DRDADD PREV NET=*ALLIP
CHGXPUAP	08/16/12	17:38:04	TAFORD	EXTPUAF	CHANGE	9.5.157.158	SHARONSU	DSTPGMC	PREV PNT=DRDADD PREV NET=*ALL
CPYXPUAP	08/16/12	17:53:06	TAFORD	EXTPUAF	CREATE	*ALLIP	TAFORD	DSTPGMC	COPY USR=SHARONSU COPY PNT=DSTPGMC COPY NET=9.5.157.158
WRKXPUAP	08/16/12	17:36:23	TAFORD	EXTPUAF	VIEW	-	-	-	-
WRKXPUAP	08/16/12	18:45:11	TAFORD	EXTPUAF	VIEW	-	-	-	-
WRKXPUAP	08/16/12	18:45:15	TAFORD	EXTPUAF	PRINT	-	-	-	-

Record Layout of Journal Entries created through Exit Point Use

One important aspect of using Exit Points is monitoring their use. When active or in log mode, every Exit Point transaction produces a User Defined (JRNCDE = "U") audit record in the security journal QAUDJRN. The QAUDJRN Journal Entry Types used by the Exit Point Tool are as follows:

Exit Point	WRKREGINF	Application Type	*LOGONLY	*PASS	*FAIL
CLI DB Connection	QSQ_CLI	DB	LL	DC	DL
Distributed Program Call (DPC)	QZRC_RMT	DSTPGMC	LC	DP	DF
Host Server Data Queue Server	QZHQ_DATA	*DATAQSRV	LQ	VB	VQ
FTP HOST Request Validation	QTMF_CLIEN	FTPCLNT	LH	VG	VW
FTP Request Validation	QTMF_SERVE	FTPSRV	LV	VM	VX
REXEC Request Validation	QTMX_SERVE	REXEC	LY	VJ	VY
TFTP Request Validation	QTOD_SERVE	TFTPSRV	LZ	VT	VZ
Host Server Print server	QNPS_ENTRY	QNPSERV	LP	XB	XN
Remote Execution (REXEC)	SVR_LOGON	REXEC	LX	XC	XQ
Host Server File server (IFS)	FILE_SERV	*FILESRV	LI	XI	XY
DRDA / DDM	NETW_ATTR	*DRDA / *DDM	LA	XM	XK
Host Server Signon server	SIGNONSRV	*SIGNON	LS	XO	XV
ODBC / JDBC / File Transfer	QDZA_INIT	OJDBC	LO	XP	XJ
SQL Server Access	QDZA_SQL1	OSQL1	L1	P1	F1
SQL Server Access	QDZA_SQL2	OSQL2	L2	P2	F2
Remote Command (RMTCMD)	QZRC_RMT	RMTCMD	LR	XR	XW
FTP Server LOGON	SVR_LOGON	FTP	LF	XS	XF
TELNET Initialization	QTG_DEVINT	TELNET	LT	XT	XZ
COMMAND Restrictions	IBM_CHGCMD	CMD_ACCESS	--	PE	FE
Additional Entries: II - Informational AX - Add Registered Exit Program RX - Remove Registered Exit Program QZ - Change or setting the alternate audit journal XX - User not Allowed / Exit Point License Key Error / Internal Error					

As a User Defined Journal Entry, the information placed in the journal record is located in the Entry Specific Data (ESD) of the journal record as follows:

Offset					
J2	J4	J5	Format	Position in ESD	Description
1	1	1			Headings common to all entry types *
156	224	610	A (10)	1	User Causing Entry
166	234	620	A (10)	11	Application Type
176	244	630	A (10)	21	WRKREGINF Exit Point Short Name
186	254	640	A (10)	31	Group Name (if accessed thru the group)
196	264	650	A (10)	41	*PASS, *FAIL, or *LOGONLY
206	274	660	A (15)	51	User IP Address
221	289	675	A (256)	66	Additional Information specific to each Exit Point The QIBM_QZDA_SQLx Exit Points provide an additional 512 bytes of information.

* Details of the common headings can be found in Appendix F of the [Security Reference Manual SC-5302](#)

Record Layouts of Files used by the Exit Point Tool

There are three primary files used by the Exit Point Tool. They are located in library QZRDSECXPT. A fourth, EXTPUAE is created when the long report (F8) of Users defined to the Exit Points is submitted on the Work with Exit Point User Access screen.

Exit Point User Access Definitions (EXTPUAF)

File Name	Record Format	Unique Keys	K=Key Field	Key No.	Field Name	Field Type	Field Length	Start	End	Field Text Description
EXTPUAF	EXTPUAR	Y	K	1	UATYPE	A	10	1	10	User Profile Name
		Y	K	2	UAXPNT	A	10	11	20	Exit Point
					UAGRPI	A	1	21	21	User is a Group
		Y	K	3	UAIPA4	A	15	22	36	Allowed IPv4 Address
					UAIPA6	A	39	37	75	Allowed IPv6 Address (Future)

Exit Point Definitions / Defaults (EXTPDFF)

File Name	Record Format	Unique Keys	K=Key Field	Key No.	Field Name	Field Type	Field Length	Start	End	Field Text Description
EXTPDFF	EXTPDFR	Y	K	1	XPDEFN	A	10	1	10	Exit Point Definition
					XPNAME	A	20	11	30	Exit Point Name
					XPFRMT	A	8	31	38	Exit Point Format
					XPPROG	A	10	39	48	Exit Point Program
					XPLIBR	A	10	49	58	Exit Point Program Library
					XPSTAT	A	10	59	68	Exit Point Status
					XPDESC	A	30	69	98	Exit Point Description
					XPCMDP	A	1	99	99	Add to Command Prompt
					XPONOF	A	8	100	107	Exit Point ON/OFF/LOGONLY Switch

Exit Point Audit Log (XPTLOG)

File Name	Record Format	Unique Keys	K=Key Field	Key No.	Field Name	Field Type	Field Length	Start	End	Field Text Description
XPTLOG	XPTLOGR				PROGRM	A	10	1	10	Program Reporting the Entry
					ENTDAT	A	8	11	18	Entry Date - YY/MM/DD
					RSRVED	A	1	19	19	Reserved Space
					ENTTIM	A	8	20	27	Entry Time - HH:MM:SS
					ENTUSR	A	10	28	37	User Creating Entry
					FILMOD	A	10	38	47	File that was Modified
					FILACT	A	10	48	57	Action Occurring on the File
					ACTSCP	A	15	58	72	Scope of Action
					USRACT	A	10	73	82	User Impacted by Action
					EXITPT	A	10	83	92	Exit Point Definition
					MSCTXT	A	256	93	348	Miscellaneous Information

Exit Point User Access Expansion (EXTPUAE)

File Name	Record Format	Unique Keys	K=Key Field	Key No.	Field Name	Field Type	Field Length	Start	End	Field Text Description
EXTPUAE	EXTPUAE				UATYPE	A	10	1	10	User Profile
					UAXPNT	A	10	11	20	Exit Point
					UAGRPI	A	1	21	21	Group / Member Indicator
					UAIPA4	A	15	22	36	Allowed IPv4 Address
					UAGRPN	A	10	37	46	Group Association (If Member)

Restricted Commands Record Layouts

The files used for Command Restrictions are also located in library QZRDSECXPT.

Exit Point Command Line Restrictions (EXTPCMF)

File Name	Record Format	Unique Keys	K=Key Field	Key No.	Field Name	Field Type	Field Length	Start	End	Field Text Description
EXTPCMF	EXTPCMR				XPRCMN	A	10	1	10	Restricted Command
					XPRCML	A	10	11	20	Restricted Command Library
					XPRCM#	P	7	21	24	Exit Point Number on WRKREGINF
					XPRALU	A	350	25	374	Users Allowed to use Command
					XPRHSH	A	32	375	406	Authentication Hash

Removing the IBM i Exit Point Tool

To remove the IBM i Exit Point Tool from your system, enter the following command.

QZRDSECXPT/RMVSECXPT <ENTER>

PLEASE NOTE!

The Exit Point Program removal will not be complete until the associated TCP Servers and Host Servers have been stopped and restarted. Only then will the removal process be complete.

Additional Resources

This section lists some additional sources of information pertaining IBM i security and common security guidelines and standards that may prove useful to you.

IBM i Information

System i Security reference Version 6 Release 1 SC41-5302-10

<http://publib.boulder.ibm.com/infocenter/iseries/v6r1m0/topic/rzarl/sc415302.pdf>

System i Security reference Version 7 Release 1 SC41-5302-11

http://www.ibm.com/support/knowledgecenter/api/content/nl/en-us/ssw_ibm_i_71/rzarl/sc415302.pdf

System i Security reference Version 7 Release 2 SC41-5302-12

http://www.ibm.com/support/knowledgecenter/api/content/nl/en-us/ssw_ibm_i_72/rzarl/sc415302.pdf

System i Security reference Version 7 Release 3 SC41-5302-13

http://www.ibm.com/support/knowledgecenter/api/content/nl/en-us/ssw_ibm_i_73/rzarl/sc415302.pdf

IBM Redbook:

Implementation and Practical Use of LDAP on the IBM eServer iSeries Server, SG24-6193

<http://www.redbooks.ibm.com/abstracts/sg246193.html?Open>

IBM Redbook:

IBM eServer iSeries Wired Network Security: OS/400 V5R1 DCM and Cryptographic Enhancements, SG24-6168

<http://www.redbooks.ibm.com/abstracts/sg246168.html?Open>

IBM Redbook:

Securing Communications with OpenSSH on IBM i5/OS, REDP-4163

<http://www.redbooks.ibm.com/abstracts/redp4163.html?Open>

IBM Redbook:

IBM i5/OS Network Security Scenarios A Practical Approach, SG24-7374

<http://www.redbooks.ibm.com/abstracts/sg247374.html?Open>

IBM Redbook:

IBM System i Security Guide for IBM i5/OS Version 5 Release 4, SG24-6668-01

<http://www.redbooks.ibm.com/abstracts/sg246668.html?Open>

IBM Redbook:

Security Guide for IBM i V6.1, SG24-7680

<http://www.redbooks.ibm.com/abstracts/sg247680.html?Open>

IBM Redbook:

Windows-based Single Signon and the EIM Framework on the IBM eServer iSeries Server, SG24-6975

<http://www.redbooks.ibm.com/abstracts/sg246975.html?Open>

IBM Redbook (HTTP server security):

IBM HTTP Server (powered by Apache): An Integrated Solution for IBM eServer iSeries Servers, SG24-6716-02

<http://www.redbooks.ibm.com/abstracts/sg246716.html?Open>

IBM Redbook Power System Security (HMC)

IBM Power Systems HMC Implementation and Usage Guide

<http://www.redbooks.ibm.com/abstracts/sg247491.html?Open>

WebSphere MQ Security

As a general recommendation regarding WebSphere MQ Security, always encrypt your messages with SSL. This ensures authentication of the data origin, the confidentiality, and the integrity of messages.

IBM Redbook:

WebSphere MQ Security in an Enterprise Environment, SG24-6814

<http://www.redbooks.ibm.com/abstracts/sg246814.html?Open>

WebSphere MQ Information Center → Security

http://publib.boulder.ibm.com/infocenter/wmqv6/v6r0/index.jsp?topic=/com.ibm.mq.csqzas.doc/sy10120_.htm

Internet Security Standards and Organizations

The standards contain valuable information regarding writing security policies and implementing best practices.

Common Criteria

Security Product Certification and Standards

<http://www.commoncriteriaportal.org/>

Security Standards download page (i.e. ISO27001, ISO27002)

<http://www.standards-online.net/InformationSecurityStandard.htm>

Control Objectives for Information and related Technology (COBIT)

ISACA Site

<https://www.isaca.org/search/Pages/ResultsAjax.aspx#cobit>

SANS Institute

Information about standards, security vulnerabilities, and policies

Policies:

<http://www.sans.org/security-resources/policies/>

Best Practices in Mitigation and Control:

<http://www.sans.org/top-cyber-security-risks/best-practices.php>

CERT

Information about vulnerabilities and fixes

<http://www.cert.org/>

Common Vulnerabilities and Exposures

<http://cve.mitre.org/>

BSI Security Standards and Best Practices

Contains very good information that can be reused to implement proper security policies

https://www.bsi.bund.de/cln_174/EN/Topics/ITGrundschutz/itgrundschutz_node.html

International Information Systems Security Certification Consortium, Inc., (ISC)²

Maintains a critical body of knowledge (CBK) with regard to information security topics. The CBK defines global industry standards, serving as a common framework of terms and principles that the CISSP security certification is based upon.

<https://www.isc2.org/>

Center for Internet Security (CIS)

The CIS Controls® and CIS Benchmarks™ are the global standard and recognized best practices for securing IT systems and data.

<https://www.cisecurity.org/cis-benchmarks/>

IBM Systems Technology Expert Labs Security

Privacy and data protection are the responsibility of all. In a world where data is easily acquired, shared and stored (and potential data misuse is a concern) everyone must do their part to handle information in compliance with their company's requirements and values. IBM research indicates security expenses are growing three times faster than IT budgets. Mounting regulatory and compliance mandates carry stiff government penalties and fines if ignored; every-growing volumes of data tax infrastructures and control capabilities; customer records disappear with alarming frequency; and security breaches cost an average of \$6.6 million per incident.

With the added pressure of a challenging economy, to compete effectively a business cannot tolerate any security exposures. From a minor breach like exposing one's password to a peer or major failure like the disclosure of client data, neither are unacceptable and can result in new administrative procedures, a failed audit or lost business. Some circumstances could even lead to a lawsuit.

Engage with IBM Technology Expert Labs to help uphold your company's commitment to privacy and data security. Our team has developed a multitude of offerings to address your specific security concerns. From help implementing a security feature to additional resources to supplement your staff, our Consulting and Implementation Services provide general and custom consulting. Services include password elimination and single sign-on, data and tape encryption, system auditing setup and analysis, security assessments, breach analysis and IBM i penetration testing.

Security and Compliance Tools for IBM i

Complementing our security offerings are a number of tools that we have developed over the years to assist us in the delivery of our services. These tools have been written with customers in mind to aid them in the tasks of administrating security and in response to requirements to fill product gaps. They range from easy-to-install tools and utilities to more complex solutions; the latter often includes a services component intended to provide technical training and implementation services so clients and business partners can acquire and maintain mission critical skills. The tools listed below are our most requested. Others exist as well. Perhaps we can build something for you?

Compliance Automation Reporting Tool (CART)

The Compliance Automation Reporting Tool is a security and systems information Data Mart with "Real Time" event monitoring capabilities. The tool utilizes DB2 Web Query to provide a low-cost web-based interface for business analytics that can easily monitor the compliance on any or all systems in an enterprise.

- ✓ A centralized view of Security and Compliance across an enterprise providing the ability to quantify and act upon several aspects of security as statistical and measurable components as well as to corporate defined objectives for configuration consistency
- ✓ A federated repository of IBM i user profiles that provide cross system observability of profile administration.
- ✓ Security Event Monitoring - monitor and act on events as they happen - providing near "real time" monitoring of more than 180 of the most common security events. Additional events can be monitored through a customization utility.
- ✓ A customizable scoring mechanism for prioritization of policy by customer objectives which highlights deviations from policy, unexpected differences of policy settings between systems, and security attributes that do not adhere to corporate security objectives.
- ✓ A utility to add user-defined items for monitoring security inventory, auditing, status, events, etc. that integrates with scoring mechanisms provided by the tool.
- ✓ A utility for deploying tool fixes or enhancements that can be leveraged for deploying customer defined fixes
- ✓ A central repository of summarized and detailed security and security related information!

Certificate Expiration Manager

Certificate Expiration Manager is a java-based tool for simplifying the management of certificate expiration (cross-platform). CEM maintains a log of all expiration activities and can send notifications via eMail. An easy to use configuration GUI is included for managing the XML settings. The tool only runs on platforms that support Java.

IBM i SYSLOG Reporting Manager

The IBM i SYSLOG Reporting Manager (SRM) is a utility for administrators to simplify the setup for monitoring of audit journal events (QAUDJRN), history log events (QHST), as well as Integrated File System (IFS) stream files change events. An administrator can select the events that should be monitored and specify the remote syslog server or Security Information and Event Management (SIEM) server that should receive the monitored events. SRM formats events to Common Event Format (CEF) and reports events in syslog message format to the remote syslog server or SIEM system. SRM assists the client with satisfying compliance requirements for centralized logging of security-related events.

Security Exit Points

This tool simplifies managing the addition and removal of exit point definitions for users on IBM i. Exit points are a provision of the IBM i operating system that allows certain system functions to perform additional checking and validation through user-created programs. Currently the tool includes programs for managing the exit points such as FTP, TFTP, ODBC, JDBC, File Transfer, Host Servers Data Queue-Print-Signon, DRDA/DDM, REXEC, and RMTCMD. TELNET is also available but additional customization is needed to be effective. Additional exit point programs will be added in the future. The tool provides the security administrator with an easy to use interface to define which users are allowed through the defined exit point. An audit journal record is created whenever a user accesses the exit point.

Privilege Elevation Tool (FIRECALL)

The most common problem (all platforms) with security administration is too many people with privileged access to business-critical data. Often this is granted by a perceived need for the privileges in the course of their daily job. In fact, these privileges are only needed on an occasional basis - for example when troubleshooting (sometimes referred to as firefighting - thus **FIRECALL**) a problem at 3AM. The tool allows the administrator to reduce the risk of too many privileged accounts by giving the approved access to individuals as needed instead of all the time. The Privilege Elevation Tool provides a full audit trail of activities performed when elevated.

IBM i Password Synchronization and Validation Tool

The IBM i Password Synchronization Tool is a utility to assist those who have the responsibility for maintaining and implementing security features to synchronize passwords across multiple partitions in a customer's environment. A number of studies show that corporate users tend to repeat passwords on the various systems they use. The Password synchronization tool makes it easier for end users to remember these passwords and simplify their access to multiple partitions. This is accomplished by reducing the number of passwords that an end user needs to remember, making it less likely for them to write them down, resulting in fewer calls to the corporate Help Desk and less opportunity for others to gain improper access.

In addition to password synchronization, this tool supplements the IBM i Operating System supplied password rules with password validation to strengthen your security posture. It ships with 10,000 of the most commonly used passwords in technology today. More than 90% of all commonly used are found in this file, which can help strengthen your stance against dictionary-style attacks. By not using one of these passwords you will greatly reduce the risk of an intrusion due to a weak password. You can also add and remove entries to this list; as most organizations develop exposures internally with their own set of commonly used and known passwords.

Security Diagnostics Tool (aka iSAT)

The IBM i Security Assessment Tool (iSAT) is an exhaustive security collection tool that is often used during a security assessment to help discover and document security vulnerabilities. More than statistical information found in the Quick Security Check Tool, the iSAT tool drills deep to analyze object authorities, elevated privileges, etc. to enable a holistic methodical approach towards security hardening. It can also be purchased separately for customers wishing to enhance their security reporting capability.

Advanced Authentication

Passwords are no longer strong enough to provide adequate security. Cyber attackers have the power to test billions of passwords combinations in less than a second on an unprotected or weakly configured system. The Security and Compliance Tools for IBM i Advanced Authentication Tool provides an extra layer of security to authenticate a user via two different factors (or steps) before an operation takes place. This operation could be something such as signing on to a Telnet session or something more administrative such as issuing a Power Down System command or running other administrative tools.

Single Sign On (SSO) / Enterprise Identity Mapping (EIM) Populator Tool

The need for multiple user registries, an issue most enterprises face, creates a large administrative challenge. EIM for the IBM i platform offers administrators and application developers an inexpensive solution for easier management of multiple user registries and user identities. EIM creates a system of identity mappings, called associations, between various user identities in various user registries. It provides a common interface across platforms to look up relationships between user identities.

One of the most time-consuming tasks in implementing a single sign-on solution is registering users to the EIM repository. The EPT is a Java-based desktop GUI application that allows an administrator to easily import information from a comma-separated value text file. With EPT, take a spreadsheet of known user IDs and/or names and create identifiers and mappings for each user. Java 1.4 or higher is required.

Password Validation Tool

Despite warnings, one-in-five users choose a non-compliant password to protect their identity. We've developed a program that validates and ensures passwords meets company and industry recommended rules and guidelines. The tool also allows the security administrator to establish a dictionary of excluded terms, to further tighten password security.

[For more information about IBM Technology Expert Labs or our Security Offerings...](#)

Terry Ford, Team Leader
Senior Managing Consultant
Security Services Delivery
507-253-7241
taford@us.ibm.com

Robert Andrews,
Senior Managing Consultant
Security Services Delivery
507-253-4205
robert.andrews@us.ibm.com

Thomas Barlen,
Senior Managing Consultant
Security Services Delivery
+49-6701-205084
barlen@de.ibm.com

Ron Bibby, Opportunity Manager
281-455-6573
ronbibby@us.ibm.com

Or visit our website at:

www.ibm.com/services/infrastructure

Or visit our team wiki pages at:

<http://ibm.biz/IBMiSecurity>