helpsystems

User Guide
Powertech Exit Point Manager
7.23

Copyright Terms and Conditions

201910100316

Welcome to Powertech Exit Point Manager for IBM i **1**

What is Powertech Exit Point Manager? 2

Powertech Exit Point Manager Architecture 3

Network Access to IBM i Servers 3

Exit Point Manager Auditing & Reporting vs. Access Control 4

Getting Started with Exit Point Manager . **4**

Installation and Activation Introduction . 5

Adding and Configuring Managed Systems 5

Exit Point Manager System Values 10

Activating Powertech Exit Point Manager 10

Insite Web Browser Help 14

Dashboards 18

Exit Program Activation Considerations18

Powertech Work Management 19

Implementing Exit Point Manager **20**

Securing your Servers 21

Discovery, Data Collection, and Analysis 21

Adding the Initial Rule Set 30

Recursive Data Collection, Review, and Analysis 33

Adding, Changing, and Deleting User Rules 34

Copying Rules across Systems 35

Public Lockdown 37

Oversight Review 38

Granulating Rules for Specific Needs ...41

Ongoing Auditing 42

Keeping Exit Point Manager Up-to-Date 42

More on Access Control Rules - Insite web UI 42

More on Access Control Rules - green screen 60

Transaction Security 92

Reports 118

Utilities 147

Reference **155**

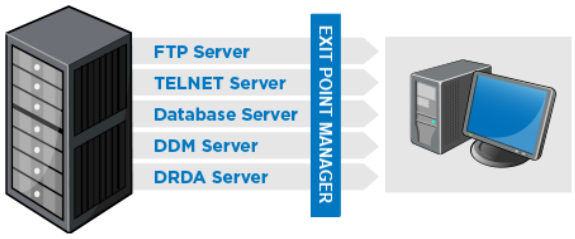
Browser Interface Reference 155

Green Screen Panel Reference 249

Appendix 511

Welcome to Powertech Exit Point Manager for IBM i

WARNING: Prior to version 7.22, Powertech Exit Point Manager was named *Powertech Network Security*. HelpSystems Insite 3.0, the current version of HelpSystems Insite as of the date of this publication, still refers to this product as *Powertech Network Security*.



NOTE: If you are using Exit Point Manager 7 version 7.07 or earlier, refer to the Exit Point Manager 7.07 Administrator's Guide. If you have just updated from version 7.07 or earlier, see Appendix M: Interface Changes in Exit Point Manager 7.08 for a list of green screen interface changes.

Powertech Exit Point Manager for IBM i™ (also referred to as *Exit Point Manager*) is a comprehensive software solution designed to help you understand and control network access to your Power Systems™ running IBM i data and services. Today, your network can include IBM i servers, PCs, mainframes, and multiple UNIX and Linux systems. In this networked environment, tools like FTP, Client Access Express Data Transfer, Remote SQL, DDM, and others allow easy access to your IBM i data and services. These alternative access methods bypass the traditional menu-based security used by many IBM i installations. In today's networked environment, even attaching one PC to your IBM i introduces a new set of security challenges that you need to consider and deal with effectively.

The IBM i security architecture is very robust, and has received the Department of Defense C2 security rating for "Trusted Systems"-*when it is properly configured*. The security exposures introduced by network data access tools like FTP and ODBC do not indicate a failure on the part of IBM i security. Instead, the data access level you provide to a user using IBM i security for green screen access through menus and screens is not the same level of access you want to allow using network tools like ODBC.

For example, the IBM i authority that allows a user to view the contents of a Payroll file is the same authority needed to download the file to a PC and post it on the Internet. IBM recognized the potential issues and introduced additional security features to manage the problem. Powertech Exit Point Manager leverages these additional features to provide a separately controlled level of network data access and service access.

The following table provides an overview of the IBM i authorities and the capabilities of users to access and manipulate data and other objects using three different access methods.

Authority	IBM i Green Screen User	PC User without Exit Point Manager	PC User with Exit Point Manager
*USE	Restricted by menu security	View, download file	Controlled by Exit Point Manager
*CHANGE		Add, change, delete records	
*OBJMGT		Clear or replace file	
*ALL		View, add, change, or delete file	

For example, consider payroll supervisor Bob:

- Bob has *ALL authority to the payroll master file so he can make changes to pay rates and add new employees through green screen menus.
- However, Bob is also familiar with programs like Microsoft Excel and Microsoft Access. Using these PC-based programs, Bob's *ALL authority allows him to add, change, and delete records from the payroll master. In fact, he could delete all the records from the file, or even delete the file altogether. Even a simple typing error on Bob's part could wipe out the entire payroll file.
- By configuring Powertech Exit Point Manager to control Bob's network access authorities, you can easily prevent any of these scenarios.

What is Powertech Exit Point Manager?

Powertech Exit Point Manager interfaces directly with IBM i network access points to control and audit network access requests. The ability to audit and control network access allows Exit Point Manager to provide Intrusion Detection, and to alert the system administrator when someone attempts unauthorized access through the network.

Exit Point Manager lets the system administrator easily configure all network access rules, including what users can perform what functions. For example, "Can Joan in Accounting download the Payroll Master file?," or more generically, "Can Joan use the file download function at all?"

Exit Point Manager also allows you to easily manage remote access by specifying which SNA device or IP address, or range of IP addresses, can perform critical functions, such as FTP. Its Switch Profile feature allows system administrators to customize levels of network access control for a user or a group of users. Using native IBM i security, Exit Point Manager Switch Profiles lets the administrator decrease, or even increase, a user's authority to data or services.

Increasing a user's authority is critical when IBM i is configured to allow "Application Only" access in which all data files are restricted from view by all users. Exit Point Manager does all this without the need to change your existing IBM i security scheme, saving valuable time and effort.

Exit Point Manager uses a secure audit journal to log all unauthorized attempts to gain access to IBM i data and services. This allows system administrators to receive alerts in real time when any unauthorized access is attempted.

When Exit Point Manager is installed on multiple systems in a network, the system administrator can use Powertech Central Administration to manage all Endpoints from a central Management System.

Rules can easily be copied from one system to another, improving management efficiency. Security policy changes, for example, can be implemented across large networks with speed and precision. Furthermore, audits can ensure Exit Point Manager's Rules and configuration on Endpoints matches that of the Management System, and Remedies can be used to manage any discrepancy.

See Central Administration Administrator's Guide for more information on Central Administration.

Rule configuration can be managed using the classic green screen interface familiar to IBM i users, or using HelpSystem's Insite web browser interface, which grants access to most of Exit Point Manager's functions in a format compatible with both desktop and mobile devices. Insite's Dashboards offer a visual representation of network activity, as well as easy access to view and edit rules for multiple systems across your network when used in conjunction with Central Administration. See HelpSystem's Insite Help for more details.

Powertech Exit Point Manager Architecture

IBM i provides full support to many TCP/IP applications including FTP, TELNET, DDM, ODBC, database serving, print serving, and many others.

Network Access to TCP/IP Applications without Powertech Exit Point Manager

Under this scenario, IBM i object-level authorities are in force. However, there are two main problems with this approach:

1. There is no record of who did what! The IBM i server programs do not record who is accessing your system, nor do they record the activity that is performed. For example, a user might use FTP to download the payroll file to their PC, but you have no way of knowing that this has occurred.
2. You are relying solely on your IBM i object authorization scheme to control access to sensitive data files and other objects. If your authorization schemes are too liberal, you are allowing access to restricted data. If your authorization schemes are too rigid, you close off access to the data that users need to perform their jobs.

Network Access to IBM i Servers

Exit Point Manager acts as your software firewall between networked clients and your IBM i servers. Exit Point Manager eliminates the problems you would see in the previous scenario:

Network Access controlled by Powertech Exit Point Manager

1. Exit Point Manager provides a secured audit and reporting capability so you can easily see who is doing what. It also provides real-time alerts when a user tries to circumvent the access rules you've specified.
2. Exit Point Manager allows you to configure network access rules to control who can do what. For example, using Exit Point Manager you can enforce network rules that say "Bob is allowed to download the payroll file, but cannot upload the file, or modify it in any way."

Exit Point Manager integrates with the IBM i network server programs at the exit point level. When you activate Exit Point Manager, several exit point programs are installed in the IBM i registration facility. You can view the names of these exit-point programs using the IBM i WRKREGINF (Work with Registration Information) command.

The Powertech Exit Point Manager exit point programs are called when someone makes a network request to the associated server. For example, when a user requests an FTP logon, the IBM i FTP server passes control to the Exit Point Manager exit point program to allow Exit Point Manager to validate the request. Exit Point Manager may tell the FTP server to accept or reject the FTP logon request, or to perform some other action, such as sending an alert message that an intruder has tried to penetrate the system.

For a complete overview of the IBM i servers and their functions, see Appendix B: Servers and Functions. You'll find useful information to help you define your Exit Point Manager access rules.

Exit Point Manager Auditing & Reporting vs. Access Control

Powertech Exit Point Manager is actually two different products in one package. In addition to controlling network access, it also includes powerful auditing and reporting features.

Auditing and Reporting

Exit Point Manager's auditing and reporting options allow you to collect audit information and to print reports about who is doing what on your system through the network interfaces. Exit Point Manager can report on all network accesses, so you can easily see potential security exposures initiated by tools such as FTP, ODBC, data transfer, and so on. This information can be used to implement Access Control Rules.

Controlling Network Access

Access Control Rules can be used to allow or reject specific Users, Locations (e.g ip addresses) , or transactions. The information you acquire from reports can be used to define a robust security policy based on the nuances of your network activity. For example, using the report information, Rules can be configured to allow authorized activity, then Exit Point Manager's default public rule (*PUBLIC) can be set to *REJECT in order to refuse all other access attempts.

Getting Started with Exit Point Manager

Before installing Exit Point Manager, refer to the Exit Point Manager Release Notes to learn about the latest updates.

> **NOTE:** The Powertech installation procedure creates libraries, profiles, authorization lists, commands, objects, and, in some cases, exit points on your system. Changing the configuration of any of these installed application components may result in product failure.

Installation and Activation Introduction

Installation and activation are two separate processes. First, the installation process installs Exit Point Manager on your IBM i system. The second process, activation, activates the Exit Point Manager exit programs. If you install the software, but do not complete the activation process, Exit Point Manager protection and auditing are not active. However, after you have completed both processes, Exit Point Manager can actively audit and secure your network traffic. You can install Exit Point Manager at any time, but activation requires planning and scheduling.

See Installing or Updating Exit Point Manager 7 (v7.04 and higher) on the HelpSystems website for installation and update instructions.

> **NOTE:** Powertech Exit Point Manager makes two changes to your network attributes during exit program activation. These modifications are necessary so the operating system is aware of the exit programs that have been assigned to the IBM exit points.

Parameter	Description	Before	After
DDMACC	DDM request access	*OBJAUT	PTNS0107
PCSACC	Client request access	*OBJAUT	*REGFAC

Adding and Configuring Managed Systems

You can start Exit Point Manager from the IBM i Main Menu.

To Start Exit Point Manager

1. From the IBM i Main Menu, enter **POWERTECH**.
2. Enter **2** to view the Powertech Exit Point Manager Main Menu.

To start Exit Point Manager from the Command Line

- Type **PTNSLIB07/WRKPTNS** or **PTNSLIB/WRKPTNS** depending on your product library.

Adding Managed Systems (Endpoints)

The following instructions explain how to add systems for management by Exit Point Manager either from the green screen or the HelpSystems Insite web browser interface. Once managed systems have been configured in Exit Point Manager, they can be connected to Insite in order to be managed from a web browser. For details on adding systems to HelpSystems Insite, see IBM i Connections in the Insite Server Settings Help.

Each system to be managed requires a licensed Exit Point Manager installation. Once an Endpoint to be managed has been installed, it can be licensed from within the Management System. After adding systems, assign them to System Groups in order to manage them together.

If you intend to use Exit Point Manager on the Management System only, you can skip the instructions in this section.

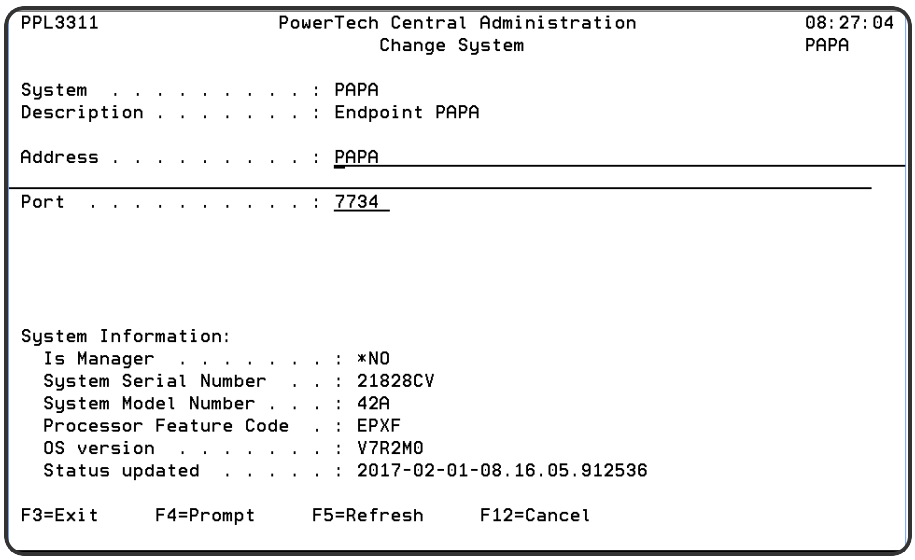
Defining Systems

NOTE: When a system is defined as an Endpoint and connected to the Management System, Exit Point Manager is also accessible by an administrator by logging in to the Endpoint directly. Changes made to an Endpoint directly are not reflected in Exit Point Manager's configuration on the Management System. Use Audits to identify discrepancies between the Management System and Endpoints (see Auditing Exit Point Manager Rules).

Before you begin, select the system you would like to use as the *Management System*. This is the system that will be used to manage Exit Point Manager across your network. Then, identify the systems to be managed, or *Endpoints*. Then, proceed with the following instructions:

On Each Endpoint

1. Install Exit Point Manager on each system for which you want to manage user rules. At installation, each system is a Management System for itself.
2. To allow one system to be the Management System, sign on to each Endpoint system and do the following: Type **POWERTECH** on a command line and then take menu option **80**, Central Administration.
3. On the Central Administration Main Menu, select option **3**, Network Configuration Menu.
4. On the Network Configuration Menu, select option **1**, Work with Systems.
5. Enter option **2**, Change, next to the endpoint system.



6. Pick a port number to use on both the Endpoint and Management System.
    - Each Endpoint can use the same port number (recommended).
    - Each Endpoint can have a different port.
    - On the Change System panel, enter a description, the IP address or the name by which the system is known, and the port number that will be used to communicate with the Central Administration Management System. You will use this port number when you

add the system to the network from the Management System. It is recommended that you set all the ports to the same number so that it is easily remembered, but this is not required. The same port number is required for the Management System and the Endpoint. If you change to a different port number, you will need to do so for the Management System and the Endpoint.

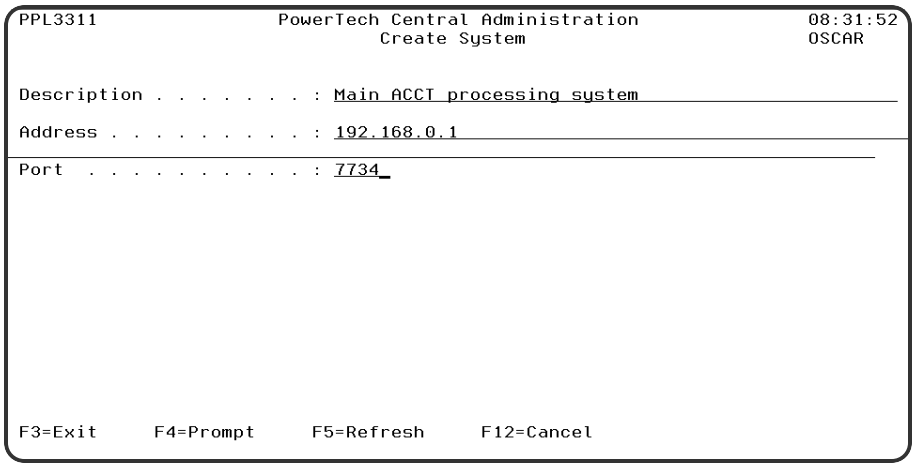
7. Start the Central Administration monitor jobs using the command **PPLSTRMON**. This starts four monitor jobs in the PTWRKMGT subsystem: PPLCMNMON, PPLCMNSVR, PPLEVTMON, and PNSEVTMON.

> **NOTE:** PNSEVTMON must be running in order to add user profile rules in Exit Point Manager. If for some reason PNSEVTMON gets shut down, you can issue PTNSLIB07/PNSSTRMON (or PTNSLIB/PNSSTRMON, depending on your product library) to restart the monitors, restoring the ability to add user profile rules.

On the Management System

1. Sign on to the system designated as the Management System and do the following: Type **POWERTECH** on a command line and then take menu option **80**, Central Administration.
2. On the Central Administration Main Menu, select option **3**, Network Configuration Menu.
3. Start the monitor jobs: **PPLSTRMON**
4. On the Network Configuration Menu, select option **1**, Work with Systems. The Work with Systems panel lists all systems that have been defined in Central Administration.
5. Press `F6` to add a new system. Enter a brief description of the system on the Create System panel. Specify the address (either the IP address or the name by which the system is known) and the port number you entered on the endpoint system that is used to communicate with the system.
6. Press Enter to include the Endpoint as a managed system. The system name and system information (serial number, model number, and whether the system is the Central Administration Management System) display on the panel.

   > **NOTE:** The monitor jobs must be running on the Endpoint in order for it to be included as a managed system.



7. You also can enter product license information for an Endpoint. Enter option **7**, Licenses next to the system name to display the Work with Licenses for System panel. Select the product for

which you want to enter the license code with option **2**. Use the License Entry panel to enter the license code.

Configuring Exit Point Manager Product Security Roles

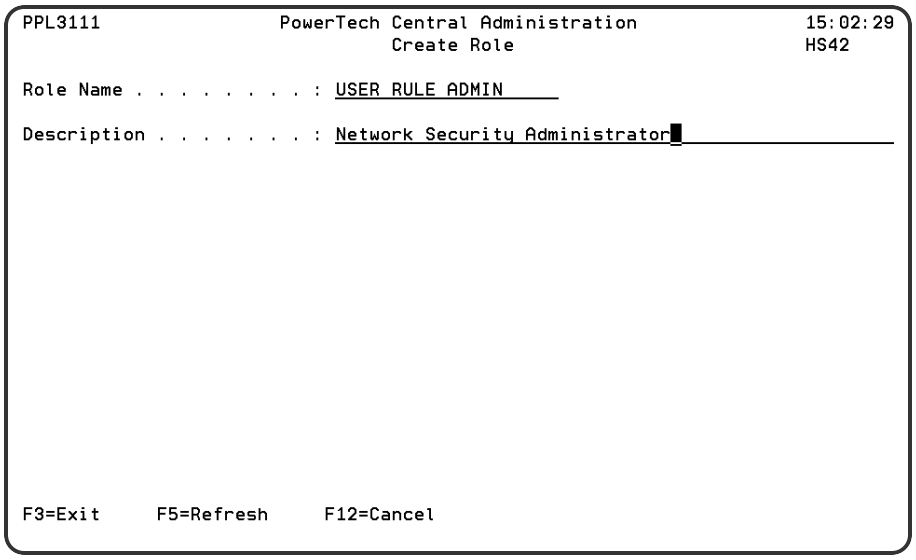
A Product administrator on the PTADMIN Authorization list has unencumbered access to all aspects of both Exit Point Manager and Central Administration. This high level of authority may be excessive if a Powertech user does not require access to every function in order to perform their required administrative tasks. To delegate access to the required subset of product functions, define Product Security *Roles*. A Role overrides the global authorities provided by the PTADMIN authorization list and defines the user's authority over the managed systems. For example, if a user is Report Personnel, and does not require access to non-report-related functions, you can define a "Report" Role, then assign this Role to the individual responsible for running reports in order to issue them access to *only* report-related functions.

To turn on Role Based Security

1. From the Powertech Main Menu, enter **80**, Central Administration.
2. Enter **2**, Product Security Menu, then **2**, Product Security Controls.
3. Set Role-Based Security to **1**.

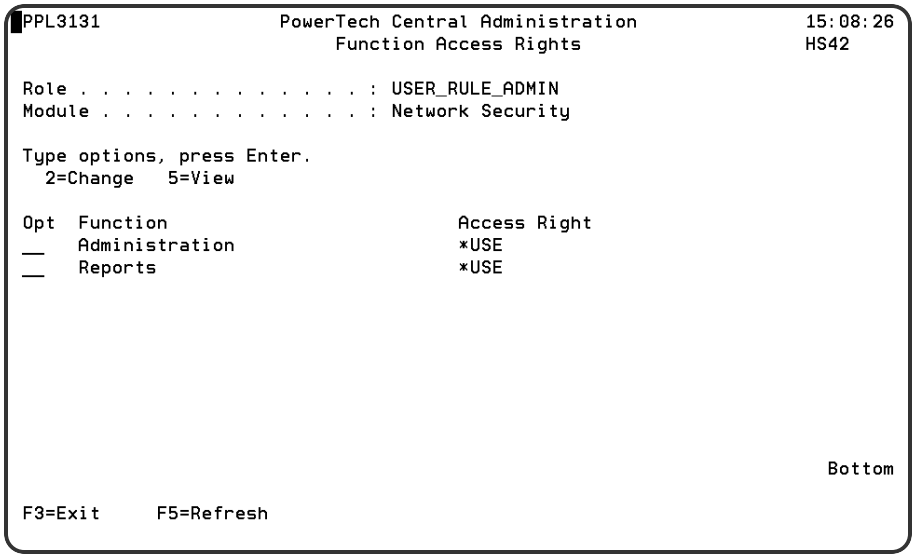
To Create a Role

1. From the Powertech Main Menu, enter **80**, Central Administration.
2. Enter **2**, Product Security Menu, then **1**, Work with Roles.
3. Press `F6` to create a new Role, then enter a Role name and brief description on the Create Role panel.



4. Press `Enter`.
5. Enter **7**, Function Access Rights, for the Role you created.
6. Enter **2**, Change, for the Exit Point Manager Module.

7. Select each function on the Function Access Rights panel with option **2** and specify the access right you want to assign to the function. See the panel help for a description of the possible values.



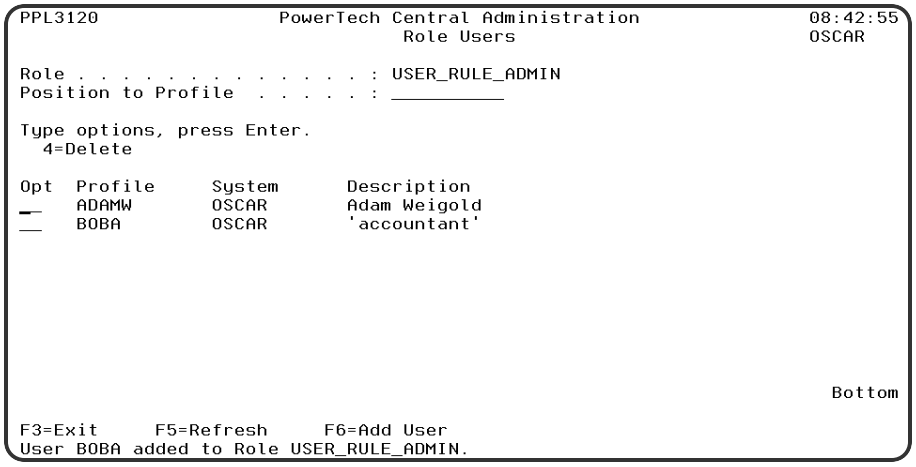
8. After you have defined the access rights, press `F3` twice to return to the Work with Roles panel.

> **NOTE:** When you create a new role, all access rights are automatically set to *EXCLUDE.

9. Now that you've defined a Role and its access rights, you can add users to the Role. Enter option **6** (Role Users), next to the Role.
10. On the Role Users panel, press `F6`, Add User, to display the Select User Profile panel. Enter a **1** next to each user profile you want to add to the Role; you can add multiple users at the same time. Press `Enter` to add the users.

> **NOTE:** A user can be assigned to only one role at a time. If a user already is assigned to a different role, you'll be asked if you want to transfer the user to the new role.

For more information, see "Product Security - Creating Roles" in the Central Administration Administrator's Guide.

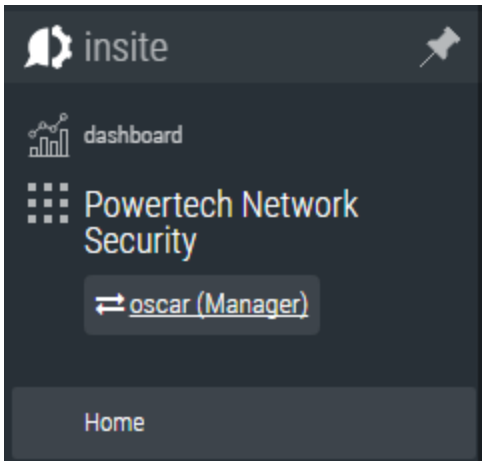


Switching Systems

After you have installed and licensed Exit Point Manager on one or more Endpoints, you can log in to the Management System to manage any of these systems.

Press `F7` in the green screen (in any panel that includes this option) to open the Select Systems panel, which allows you to choose a new system to work with.

In HelpSystems Insite, click the name of the system in the Navigation Pane.



Exit Point Manager System Values

After you've installed Exit Point Manager, use the Work with System Values screen to set the initial system values for Exit Point Manager.

1. From the Exit Point Manager Main Menu, select option **81**, Configuration Menu.
2. Select option **1**, Work with System Values, to display the Work with System Values screen. The Work with System Values screen allows you to set and maintain your Exit Point Manager system values.
3. To change default system values, enter your changes and press `Enter` to save them. A confirmation message, Exit Point Manager System values successfully updated, displays at the bottom of the screen.

> **NOTE:** You cannot change the Product Owner, Product Library, and Product Administrator system values. However, you can modify the system values for Log Journal Name, Log Journal Library, Log Message Queue Name, and Log Message Queue Library at any time.

Activating Powertech Exit Point Manager

Exit Point Manager uses several exit programs that interact with the various servers on IBM i. For the servers to use the exit programs, the exit programs must be registered. The Exit Point Manager activation process uses the Add Exit Program (ADDEXITPGM) command to add the exit programs to

the system registration. (You can use the Work with Registration Info [WRKREGINF] command to see a list of registered exit programs.)

You can select from either of two methods to register the exit programs:

- The Silent method (performed during an IPL)
- The Interactive method

Activation requires the following special authorities:

- *ALLOBJ
- *IOSYSCFG
- *JOBCTL
- *SECADM

Exit Point Manager provides several activation/deactivation options and information on your activation/deactivation setup.

Compliance Monitor Users: Interactive Activation of Exit Point Manager will stop Compliance Monitor. End Compliance Monitor prior to interactive activation, and then restart it after activation.

To activate Powertech Exit Point Manager

1. From the Exit Point Manager Main Menu, select option **81**, Configuration Menu.
2. On the Configuration Menu, select option **2**, Work with Activation, to display the Work with Exit Point Manager Activation panel.

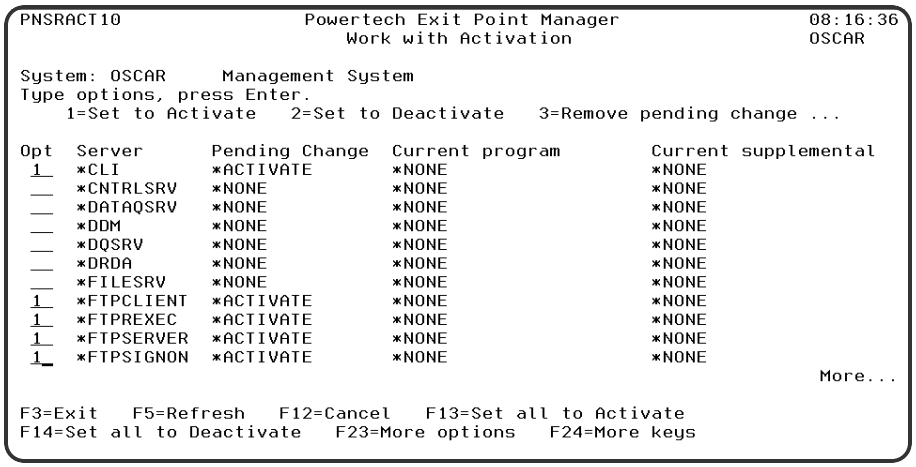
> **NOTE:** The Interactive method stops and starts QCMN and QSERVER. Other jobs are also restarted, like QZDASOINIT if *SQLSRV is activated. If you want to use the interactive method on a production system, you should perform it at a time when it will not interfere with your critical business processes. Due to time-sensitive interactions with IBM i system processes, there is a small possibility that the IBM i NetServer will not be running after activation. Also, if IBM Tivoli Directory Server is active before the activation, it will need to be restarted after activation.
> Use the following table to check if either server is active before the activation:

Server	Function	How to check if active
IBM i NetServer	File server (for example, for access to the IFS from Windows Explorer)	`WRKACTJOB JOB (QZLSSERVER)` If a job is displayed, the server is active.
IBM Tivoli Directory Server	LDAP	`WRKACTJOB JOB(QUSRDIR)` If a job is displayed, the server is active.

> See also Manual Restart After Activation.

3. Enter a **1** next to a server to mark it for activation.

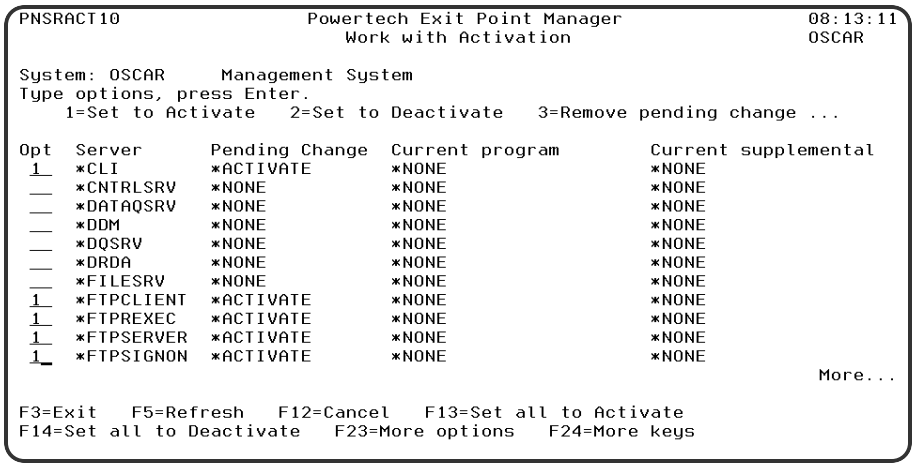
   WARNING: Registering any exit program over the *SQLSRV server can impact system performance since this server is called for each SQL request. High SQL traffic environments, or systems known to be underpowered, can experience significant delays when processing these requests. Consider object level security before Activating *SQLSRV in Exit Point Manager.



   Alternatively, you can choose F13 to activate all servers. If you do this, all servers are selected except the sockets-related servers. These can potentially render your system unreachable via TCP and need to be treated with the utmost caution. They can still be activated by selecting them with a 1.

4. When you press `Enter`, *ACTIVATE displays in the Pending Change column on the Work with Activation panel.

   Pending Activate request



5. After you set the Pending Change field to *ACTIVATE, you must run the activation request to apply the Exit Point Manager exit program to each selected exit point. You can select to run an Interactive activation request (`F20`, Run activation) or a Silent activation request (`F18`, Add silent activation).

   NOTE: To activate all exit points, press `F13` (Set all to Activate).

To activate all exit points, press F13 (Set all to Activate). The *DDM and *DRDA servers, as well as the four ShowCase servers (see Servers and Functions), are physically the same server and are activated (or deactivated) together. If you choose to activate one, both/all are activated. They appear as separate servers in the list so that you can define different rules for each, and are interpreted as different servers at run time.

Using Silent Activation (F18)

For Exit Point Manager to activate itself at the next IPL, it changes the QSTRUPPGM system value to LNUR004, which is a Exit Point Manager-supplied program. Among the actions taken during the Silent Activation process, the program does the following at IPL (or when the controlling subsystem next starts):

If not a conversion from NS6, or conversion but no product library rename is to occur:

1. Registers all Exit Point Manager exit programs to the associated exit point.
2. Restores the QSTRUPPGM system value to the name of your original startup program.
3. Calls your startup program.

If a conversion from NS6 and the product library is to be changed to PTNSLIB:

1. Before powering down, all exit programs are deregistered and the TCP attribute STRTCP is set to *NO.

   WARNING: PWRDWNSYS **must** be used to IPL. Bringing the system into and out of restricted state is not enough, nor is ENDSYS or ENDSBS(*ALL).

2. After powering up, when the IPL has completed and QCTL is started:

   a. Sets the IPL attribute STRTCP to *YES if it was *YES before.
   b. Swaps the library PTNSLIB07 name to PTNSLIB and puts NS6 in PTNSLIB06.
   c. Registers all Exit Point Manager exit programs to the associated exit point.
   d. Restores the QSTRUPPGM system value to the name of your original startup program.
   e. Calls your startup program.

If you decide you don't want to use Silent Activation, display the Work with Activation panel and press F19, Remove silent activation.

Do not delete the Exit Point Manager product library after selecting Silent Activation without canceling the activation.

- Exit Point Manager activation recognizes the presence of an existing exit program and gives you the option to register it as a supplemental exit program. You do not need to do this, but you should be aware of the consequences if the current exit programs are being used for other processes on your system.
- A Powertech Exit Point Manager exit program cannot be made supplemental to itself.

Manual Restart After Activation

After an interactive activation, restart the following (if they were running prior to activation):

Server	Commands to Restart
IBM i NetServer	If server was active prior to activation: 1. Check if active now using: **`WRKACTJOB SBS(QSERVER) JOB (QZLSSERVER)`** 2. If not active, restart: **`STRTCPSVR *NETSVR`**
IBM Tivoli Directory Server for IBM i*	If server was active prior to activation and if *RMTSVR, *RQSVR, or both servers were included in the activation. **`ENDTCPSVR *DIRSRV`** **`STRTCPSVR *DIRSRV`**

Insite Web Browser Help

WARNING: Prior to version 7.22, Powertech Exit Point Manager was named *Powertech Network Security*. HelpSystems Insite 2.7, the current version of Insite as of the date of this publication, still refers to this product as *Powertech Network Security*.

The HelpSystems Insite browser interface provides an efficient, interactive method of managing Exit Point Manager across all managed systems on your network. All the core functions of Exit Point Manager are available from Insite, including access to Rules, IP Address Groups, Pre-Filters, Product Defaults, Captured Transactions, Memorized Transactions, Object Rules, and Reports. Similar procedures are used for searching, filtering, adding, editing, deleting, and otherwise managing all of these items from your browser. The following instructions explain these common procedures.

IMPORTANT: To users planning to use the HelpSystems Insite web browser interface with Exit Point Manager

If *PUBLIC is locked down in your current Exit Point Manager configuration, you need to create rules that allow some of Exit Point Manager's profiles to access to the following server functions.

Server	Function(s)
*SIGNON	RETRIEVE
*RMTSRV	RMTCMD, DSTPGMCALL
*SQL	INIT
*SQLSRV	OPENFETCH, PRPDESCRB
*QNPSERVR	INIT

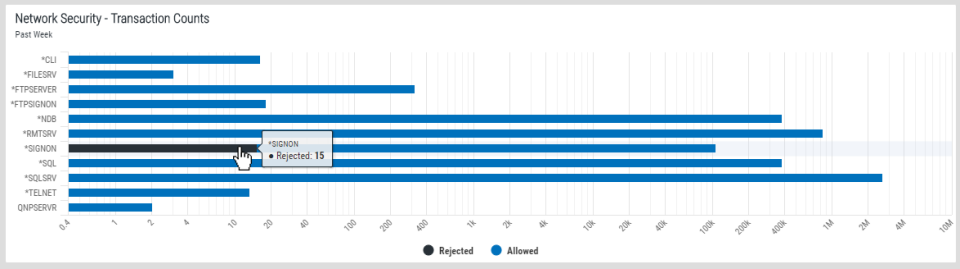
See Creating a Service Profile User Rule - green screen for information on how to allow these profiles to access these functions.

Using Insite with Exit Point Manager

The following instructions provide an overview for how to manage Exit Point Manager using your web browser. For more details, see the HelpSystems Insite help.

Dashboard

The Dashboard allows you to see a snapshot of all network activity that has passed through (or been blocked by) Exit Point Manager.



Use the Dashboard to see an overview of your Network Activity.

To start the Dashboard Data Collector, which records the transactions shown in the Dashboard charts, in the green screen, run the command **PNSSTRDASH**. Or press `F22` to activate the Dashboard Data Collector using the Operational Status screen.

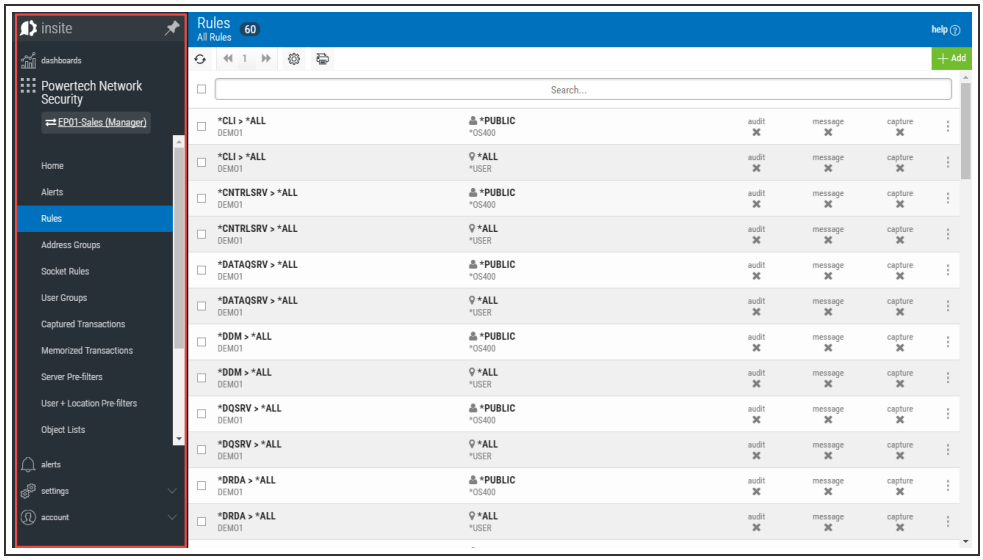
See Dashboards Overview for more details.

Navigation Pane and Select Products Pane

The Navigation Pane includes the general directory of management tools for Exit Point Manager, and, when open, is located on the left side of your browser window.

Click  to allow the Navigation Pane to minimize. Click  to pin the Navigation Pane open, so its contents remain visible.

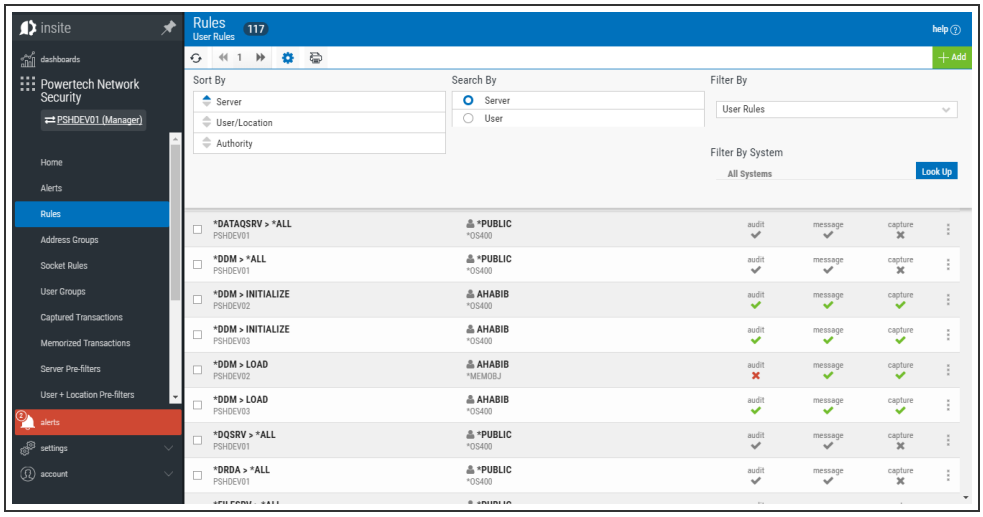
Click  to open or close the Select Product Pane.



The Navigation Pane includes a directory of Exit Point Manager's main management tools.

Sort, Search, and Filter settings

Each of the main pages include settings that allow you to choose how to sort the existing list items, what type of data will be searched when you do a search, and how to filter the list.



- Click the Settings button  to open the sort, search, and filter settings.
- Select how you want the status list sorted (Sort By). Click your selection again to change the sort order to ascending or descending  .

> **NOTE:** Sorting information, including the column the list is currently sorted by and the sorting direction, is available in your browser's address bar. For example, a URL that includes "sort/**server**/dir/**1**" indicates the list is sorted by *server*, *low to high*. A URL that includes "sort/**server**/dir/**0**" indicates the list is sorted by *server*, *high to low*.

- Select the list category that will be used for searching (Search By). For example, for Rules, you can choose to search by Server, User, or Location.
- Select the filtering you want used (Filter By). You can choose to see all the list items, or you can select a specific type.
- Click Close to close the settings.

Searching

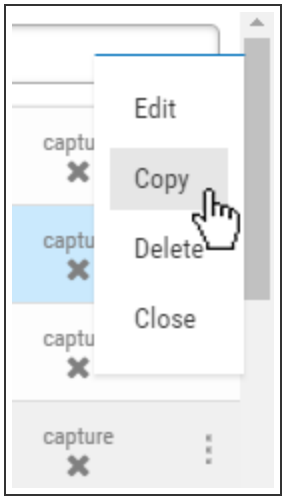
Type into Insite's Search box to find all items that include the specified text. Be sure the text you are searching for is in the same category selected for "Search By" in the Sort, Search, and Filter settings (see above). A text search queries all items in the category selected for all servers shown.

A search box appears near the top of your browser window.

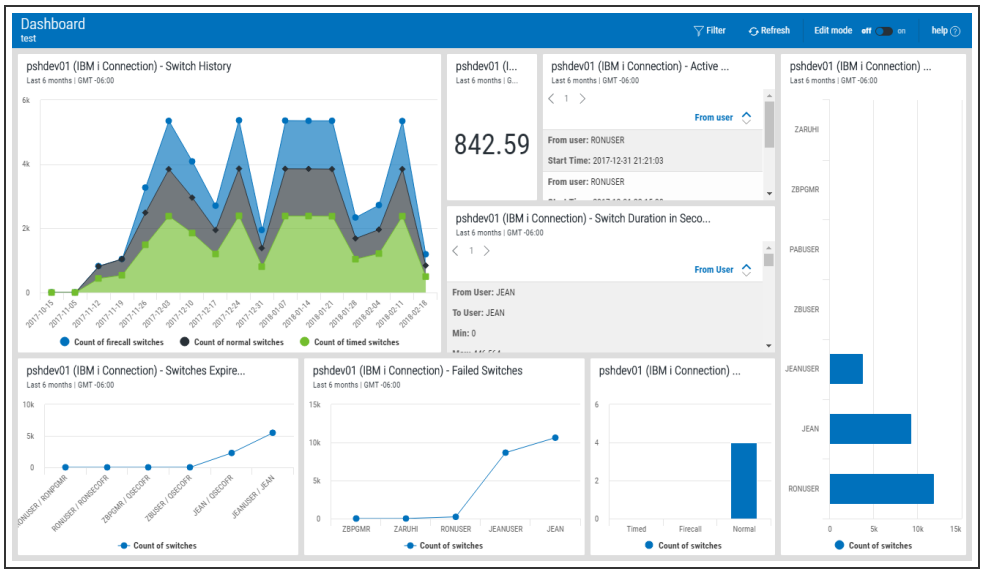
NOTE: All search results are accompanied by a unique URL. To save search results, simply bookmark or otherwise record the URL located in your browser's address bar. This URL can then be used to reference the results later. The results will appear in the same sort order.

Action Menu

Roll your cursor over the right side of the list of Rules, Object Lists, and Pre-filters to display three dots . Click these dots to display a context menu you can use to Edit, Copy, or Delete the item.



Dashboards



The HelpSystems Insite Dashboard can be used to display a visual representation of Exit Point Manager product activity. See *HelpSystems Insite Dashboard Overview* in the Insite User Guide for details.

A Dashboard can include any combination of *Widgets*, which are the individual visual displays of product data (e.g. charts, graphs, and so forth). See *Dashboard Widgets* in the Insite help for details on creating and editing Widgets. The type of Exit Point Manager data to include in a widget, such as the number of profile switches over a given time frame, is specified using Assets. See Dashboard Assets for a description of the types of Exit Point Manager data that can be added to an Insite Dashboard.

You can mix widgets from different products and Data Sources (servers) on the same Dashboard. You can create as many Dashboards as you like.

Dashboards are specific to the profile you used to log on. However, you can share them with everyone or keep them private, as needed. Users logging on with the guest profile can view only those dashboards marked as Guest. For more on the guest profile, see *Authentication* in the Insite help.

Exit Program Activation Considerations

If exit programs have already been assigned to the exit points Exit Point Manager secures, you can retain them as supplemental exit programs by selecting the server for activation using option **11**, Set to Activate/Retain supplemental. When you run the activation process, the operating system registration facility is updated to reflect that Exit Point Manager is the new exit program, and the Exit Point Manager internal tables are updated to show that your exit program is now a supplemental exit program.

Supplemental exit programs are called from the Exit Point Manager exit program after the Exit Point Manager exit program runs successfully. If you choose not to have Exit Point Manager make your existing exit programs supplemental exit programs, they no longer are called. You should consider the

implications if existing exit programs are being used for other processes on your system. However, Exit Point Manager creates a file named LNSSEP in QGPL and stores the names of your original exit programs.

Activation of Exit Point Manager exit programs requires that the subsystems QCMN and QSERVER, as well as server jobs, are ended and restarted. If you select to perform an interactive activation, current user sessions may be terminated.

The QCMN subsystem is typically used to support SNA communications traffic. If you have an alternate subsystem that supports SNA traffic, you must manually end and restart that subsystem to activate the exit program that handles SNA traffic.

Most IBM i installations use the QCTL controlling subsystem. However, if you use QBASE as your controlling subsystem, then SNA traffic typically runs under QBASE. In this case, you need to end and restart QBASE to install Exit Point Manager support for SNA traffic. Ending QBASE brings your system into restricted state. If you use QBASE, you should not perform an Interactive activation, but instead select Silent activation to activate Exit Point Manager at the next IPL.

Powertech Work Management

Powertech installs a work management subsystem called PTWRKMGT with Exit Point Manager. This allows Powertech products to submit long-running batch jobs without interfering with customer job queues. The PTWRKMGT library installed with Exit Point Manager consists of a subsystem description and a class description. PTWRKMGT is first activated when a product needs to use it, for example, when the summary job for captured transactions starts. The work management subsystem also is used by other Powertech products. If you already have another Powertech product installed on your system, PTWRKMGT will not be installed again.

There are three jobs in PTWRKMGT that are exclusive to Exit Point Manager: SUMCAPTRAN, PTNSGMSTR, and PNSEVTMON. SUMCAPTRAN summarizes captured transactions for further display. PTNSGMSTR collects transaction statistics for Insite's Dashboard. PNSEVTMON is a monitor job required for user profile rules.

The three other jobs that run in the PTWRKMGT subsystem are PPLCMNMON, PPLCMNSVR and PPLEVTMON. These are used by Central Administration to communicate between the systems. For example, these jobs are responsible for handling product license key distribution, auditing, and sending rules from the Manager to the Endpoint systems.

> **NOTE:** Auto-start entries exist for Central Administration's Event Monitor job, which in-turn starts all other Powertech products' event monitor jobs. All other jobs currently intended for PTWRKMGT are submitted jobs.

Changing the default wait time for PTWRKMGT class

Each monitor has a 30-second delay allowed (by default) for reporting back that it is ending. You can raise the delay time if any of the following conditions apply to your system(s):

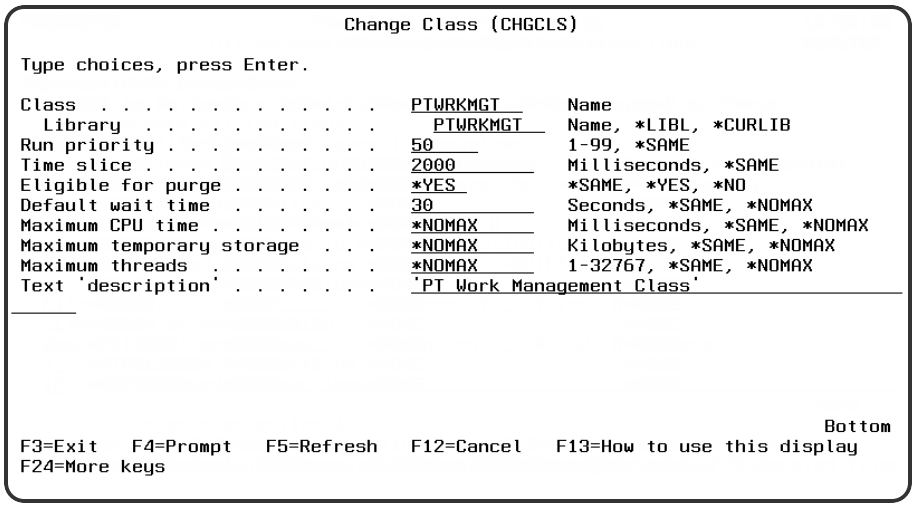
- The system is slow
- The system has a large number of entries
- The system leaves monitors running for an extended period or has environments that generate excessive job logs

To change the default wait time, enter the following command and press **F4**:

CHGCLS PTWRKMGT/PTWRKMGT

When the Change Class screen displays, you can customize the default wait time. (You also can access this screen by using the WRKCLS PTWRKMGTIPTWRKMGT command.)

> **NOTE:** Changes to attributes of the work management class will be reflected the next time a job starts in PTWRKMGT.



Implementing Exit Point Manager

Once Exit Point Manager has been installed and activated, you may be asking “what’s next? How do I use this product to meet and enforce my company’s compliance requirements?”

These instructions offer a method for how to proceed using the four essential components of *discovery*, *analysis*, *securing servers*, and *ongoing review*. The first three are performed in recursive iterations, first by taking a general, high-level look at server activity, and then again at a deeper level for each pass, with increasing granularity, until compliance is met. The fourth component is performed to respond to ongoing changes in server activity.

While the following recommendations are based on years of experience by Powertech experts, final security procedures are ultimately the decision of the administrators, your company auditor, or as outlined in your security policy.

NOTE: The following steps offer a typical approach to securing your servers by user profile. Other approaches are available (both general and highly specific), designed to accommodate diverse security needs. Contact Support for more information on the various forms if you feel they could be better suited to your needs.

In addition to user profiles, rules can apply to:

- **Group Profiles**
- **Locations (IP Addresses)**
- **IP Address Ranges**
- **Server Functions**
- **Transactions**
- **Objects**
- **Server Pre-filters**

Securing your Servers

Powertech Exit Point Manager uses exit point technology to intercept traffic passing through the IBM exit points for 30 servers. It provides two essential functions: auditing and access control.

The procedure for securing your servers, and keeping them secure, has been subdivided into the following general steps:

- Discovery, Data Collection, and Analysis
- Adding the Initial Rule Set
- Recursive Data Collection, Review, and Analysis
- Adding, Changing, and Deleting User Rules
- Public Lockdown
- Oversight Review
- Granulating Rules for Specific Needs
- Ongoing Auditing
- Keeping Exit Point Manager Up-to-Date

Discovery, Data Collection, and Analysis

In this section you will learn how to perform basic discovery in order to identify existing authorized network activity, and how to analyze this data in preparation for configuring your security implementation.

Discovery

After you have activated Exit Point Manager it's time to monitor your system in order to identify the servers that are reporting current network traffic and then identify the specific transactions on those servers.

Identifying Network Activity

> **NOTE:** If you are not using the Insite web UI, you do not have access to the Dashboard, and will need to identify network traffic by auditing your servers. Skip ahead to "Auditing Servers."

To identify network activity, you can first refer to the Exit Point Manager *Dashboard*. The Dashboard reveals all transactions that have passed through Exit Point Manager's active servers (see Activating Powertech Exit Point Manager). The activity reported on the Dashboard reveals which servers you may want to begin auditing.

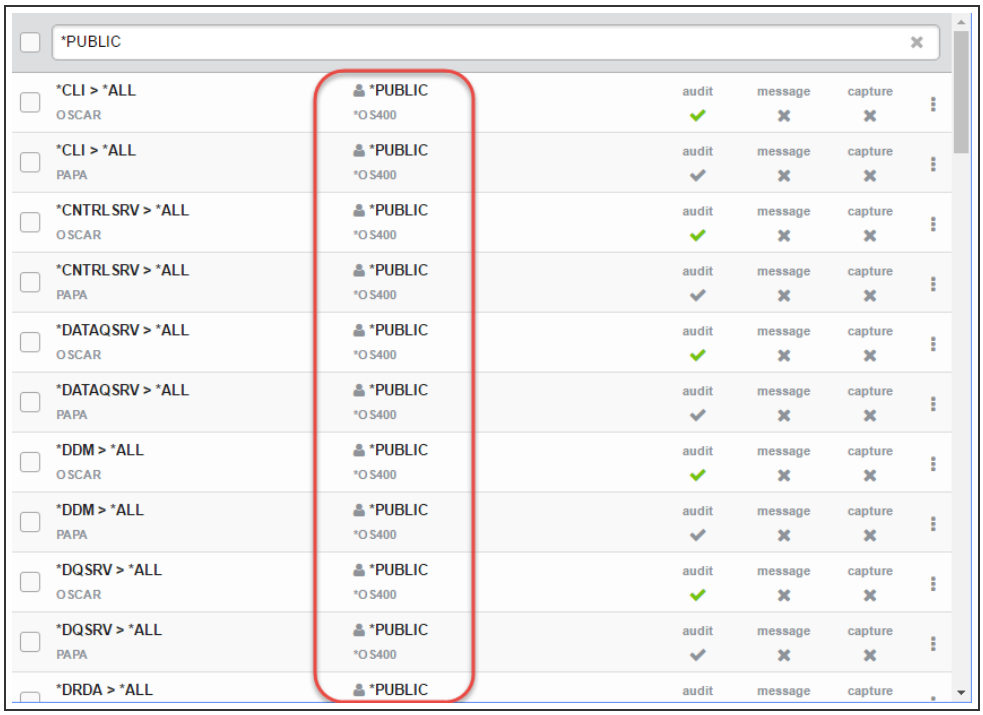
Auditing Servers

To identify specific transactions you must configure *Audit Flags* to instruct Exit Point Manager to retain access information. After the access information has been collected, Exit Point Manager's Reports can be used to identify the origin and other information about each transaction. This is the information that will be used to define access control rules.

Exit Point Manager's default (*PUBLIC) User Rules apply to all (*ALL) Functions on all servers that permit remote access. Each is defined to inherit (*) the Audit (Aud) value from the product's global system values.

Viewing *PUBLIC User Rules - web browser

1. On the Powertech Exit Point Manager portion of the Insite Navigation Pane, select Rules to open the Rules screen.
2. Click  and select the following filter options:
    - Sort By: **User/Location**
    - Filter By: **Server**
3. Click  to dismiss the sort/search/filter options.
4. Scroll down, if necessary, to view the rules marked *PUBLIC.



Viewing *PUBLIC User Rules - green screen

On the Main Menu choose **2** to view the Work with Security by User screen that displays the Aud value for each default rule.

```
LNSR090                  PowerTech Network Security                 13:58:28
                         Work with Security by User                 HAN

Subset by User : __________

                                        Filter Rule Properties
User         Server ID   Function    Authority   Aud  Msg  Cap  Switch Profile
*PUBLIC      *CLI        *ALL        *OS400      *    *    *    *NONE
*PUBLIC      *CNTRLSRV   *ALL        *OS400      *    *    *    *NONE
*PUBLIC      *DATAQSRV   *ALL        *OS400      *    *    *    *NONE
*PUBLIC      *DDM        *ALL        *OS400      *    *    *    *NONE
*PUBLIC      *DQSRV      *ALL        *OS400      *    *    *    *NONE
*PUBLIC      *DRDA       *ALL        *OS400      *    *    *    *NONE
*PUBLIC      *FILESRV    *ALL        *OS400      *    *    *    *NONE
*PUBLIC      *FTPCLIENT  *ALL        *OS400      *    *    *    *NONE
*PUBLIC      *FTPREXEC   *ALL        *OS400      *    *    *    *NONE
*PUBLIC      *FTPSERVER  *ALL        *OS400      *    *    *    *NONE
*PUBLIC      *FTPSIGNON  *ALL        *OS400      *    *    *    *NONE
*PUBLIC      *LMSRV      *ALL        *OS400      *    *    *    *NONE
                                                                   More...
F3=Exit   F4=Prompt   F5=Refresh   F10=Copy User   F12=Cancel   F24=More Keys

                                                                    9/2
```

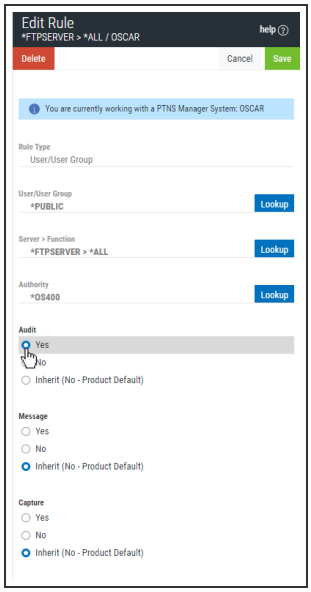
All default rules are configured to inherit the Aud value from the global System Values.

By default, Exit Point Manager's global Audit Flag is set to **Yes** (retain) for all servers. This global setting can be configured in the Edit Product Defaults screen using the web browser interface (or the Work with System Values panel using the green screen). This means that immediately after activation, Exit Point Manager is configured to audit all transactions on all servers.

Auditing all server requests can produce an overwhelming amount of data to evaluate, especially if you are unfamiliar with the amount of data your system generates. There can also be performance considerations, such as an increased frequency of journal receiver generation, and some CPU impact. To address these issues, you may decide to selectively audit a smaller number of servers (by setting some servers to **No** and others to **Yes**), complete the process of adding rules to secure those servers (as described later under "Adding the Initial Rule Set"), and then set Audit to **Yes** for a different selection of servers, and repeat the process. For example, if on the Dashboard you noticed a high number of FTP transactions, you may want to focus on just those servers first. While this approach extends the overall amount of time required for a complete analysis, it also reduces the amount of data that is collected in a given period to a more manageable level.

Selecting servers to audit - web browser

1. On the Navigation Pane, select **Product Configuration**. To save time, we'll set the Product Default for Audit to No, then specify the individual servers you want to audit.
2. Select **System Values (Product Defaults)** (the top option).
3. Set **Audit** to **No** and click **Save**. All the *PUBLIC rules now inherit this setting.
4. On the Navigation Pane, click **Rules**.
5. On the Rules screen, identify the *PUBLIC user rules (see previous steps).
6. Choose the *PUBLIC user rule for a server you would like to Audit. Under Audit, select **Yes**.



7. Choose **Save**. Repeat for the remaining *PUBLIC servers you would like to audit.

Selecting servers to audit - green screen

1. From the Main Menu, choose **2** to show the Work with Security by User panel.
2. Enter **2** for the *PUBLIC rule of a server you would like to audit.
3. For Audit, change * to **Y** if you would like to audit the server. Change Audit to **N** to specify you would not like to audit the server. (Note that alternatively you could change the global Audit setting to **N** and leave the Audit value on the servers you do not want to audit to *, but specifying this value at the server level makes it easier to reference later.)

NOTE: Without the collected audit information you will not be able to create audit reports for data traffic analysis.

After setting the Audit value to Yes for select servers, the next step is to allow your system time to accumulate data.

Data Collection

A common question is: “How long should I let data collection run, and how much is enough?” While auditing is never ‘complete,’ there does come a point when enough data has been collected in order to facilitate sound decisions. Because the stream of data collection may ebb and flow over time, determining the correct point in time is essential. The correct point for your organization will depend on your assessment of critical events that must be considered before audit rules can be put in place. Consider auditing over ranges of time that would show typical daily or weekly traffic patterns for your environment. It is also preferable to include periods of time with anomalies that may occur only, for example, on weekends or during month-end processing.

Audited Traffic Data for Reporting

Audit traffic is retained in Journal receivers. The default journal upon installation is the IBM-supplied journal QAUDJRN. However, you are not limited to using QAUDJRN.

Review your journal receiver retention policy. Removing the journal receivers will remove the ability to run audit reports for the date ranges the receivers cover. If the receivers are removed from the system, restoration from backups will be necessary to report over date range.

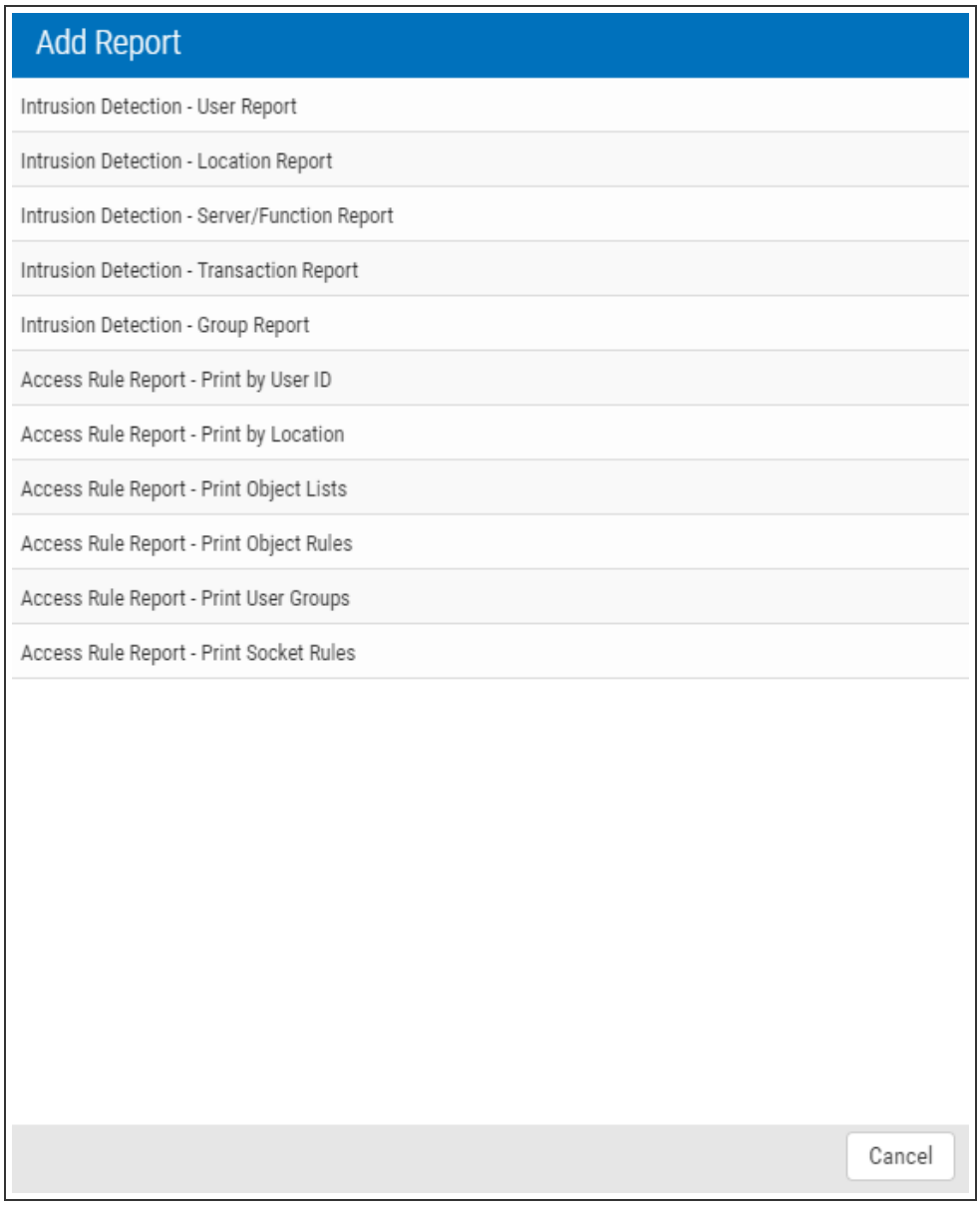
Recommendation – Use an alternate journal if QAUDJRN is not your preference. See IBM documentation for details.

Initial Data Review and Analysis

Reviewing the server transaction summary - web browser

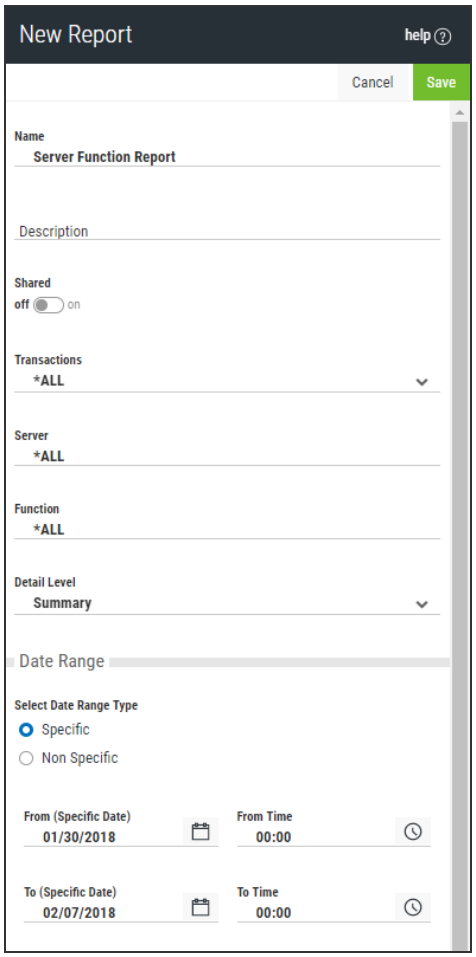
If there is a very large volume of traffic, there may be service profiles generating automated transactions that can be ignored in order to isolate the relevant activity.

1. On the Navigation Pane, select **Reports**.
2. Click **Add** and choose **Intrusion Detection - Server/Function Report**.



3. Create the report using the following settings:
    - Name: "Server Function Report"
    - Transactions: *ALL
    - Server *ALL
    - Function: *ALL
    - For Date Range, specify the number of days you would like the report to include. For the first report, a week is usually a reasonable duration. For Date Range, choose Specific to indicate the report should include a specific start and end date. Choose Non Specific to include a period of time previous to the time the report is run.
    - For Detail Level, choose Summary.

4. Click **Save** to save the report. You return to the Reports screen.
5. Click  to the right of Server Function Report and choose **Submit**. A message should appear in the lower left indicating the report has been submitted successfully.
6. Click **Spooled Files** in the Navigation Pane.
7. The report you just submitted will be at the top of the list. Click it to view.



The summary of transactions on audited servers is a starting point for planning your security configuration.

Your audit results may not show traffic on each of the audited servers. A typical system will show activity on 12-15 servers with the heaviest activity on 6-8 servers. Some may not be used at all in your environment. (If you don't see traffic, remember it is also possible your system did not generate activity during the captured time range). If a server is not being used, it can be blocked to prevent all access, accidental or malicious.

For your initial review, you can identify the servers with and without activity in a general transaction summary. To do this, run a report that displays all transactions on all the servers you are auditing.

Reviewing the server transaction summary - green screen

If there is a very large volume of traffic, there may be service profiles generating automated transactions that can be ignored in order to isolate the relevant activity.

1. From the Exit Point Manager Main Menu (green screen), choose option **80**, then **3** to view the Server Function Reports menu.
2. Choose **1**, (All Servers All Functions) All Transactions.
3. In the **From date/time** and **To date/time** fields, enter the time range. For the first report, a week is usually a reasonable duration.
4. For Detail, transaction, or summary (D/T/S), enter **S** to generate a summary by server only.

```
LNSD087SV                                                        09:44:12
              Selected Server All Functions - All Transactions   TATOOSH


 Server.......... *DATAQSRV


 From date/time.. 11/07/13   08:44:12
 To date/time.... 11/07/13   09:44:12

 Detail, transaction, or summary (D/T/S)? S

 Output type..... *PRINT      *PRINT, *OUTFILE, *IFS

  File........... __________  Create? _  Y=Yes, N=No
   Library....... __________
  Member......... __________  Option  _  A=Add, R=Replace

  IFS report name ____________________________________________________________
_____________________________________________________________


F3=Exit  F4=Prompt  F12=Cancel  F13=Msgs  F14=Submitted jobs  F15=Spooled files

                                                                      5/29
```

5. Press **Enter** to run the report.
6. Press **F14** to view Submitted Jobs, then move your cursor to the bottom (most recent) AUDIT job and type **8**, Work with Spooled Files, then press **Enter**. (The amount of time it takes for the spooled file to appear will depend on the number of transactions).
7. Choose option **5** to display the report.

```
                            Display Spooled File
File  . . . . . :   LNSP087                        Page/Line   3/23
Control . . . . .   ________                       Columns     79 - 156
Find  . . . . . .   ____________________________
.8....+....9....+....0....+....1....+....2....+....3....+....4....+....5....+.
                          0  ( *DRDA      *ALL      )
                          0  ( *FILESRV   *ALL      )
                          0  ( *FTPCLIENT *ALL      )
                          0  ( *FTPREXEC  *ALL      )
ow                       14  ( *FTPSERVER *ALL      )
ect                       1  ( *FTPSERVER *ALL      )
or                        0  ( *FTPSERVER *ALL      )
ow                        5  ( *FTPSERVER CHGCURLIB )
ect                       0  ( *FTPSERVER CHGCURLIB )
or                        0  ( *FTPSERVER CHGCURLIB )
                          0  ( *FTPSERVER CREATELIB )
                          0  ( *FTPSERVER DELETEFILE)
                          0  ( *FTPSERVER DELETELIB )
ow                        6  ( *FTPSERVER INIT      )
ect                       0  ( *FTPSERVER INIT      )
or                        0  ( *FTPSERVER INIT      )
                                                                    More...
F3=Exit   F12=Cancel   F19=Left   F20=Right   F24=More keys
Overprinting not displayed.

                                                                     3/22
```

The summary of transactions on audited servers is a starting point for planning your security configuration.

Your audit results may not show traffic on each of the audited servers. A typical system will show activity on 12-15 servers with the heaviest activity on 6-8 servers. Some may not be used at all in your environment. (If you don't see traffic, remember it is also possible your system did not generate activity during the captured time range). If a server is not being used, it can be blocked to prevent all access, accidental or malicious.

For your initial review, you can identify the servers with and without activity in a general transaction summary. To do this, run a report that displays all transactions on all the servers you are auditing.

Reviewing Server Transactions

Now that your server summary has revealed the servers that are being used, you can review the transaction history on those servers to identify unauthorized activity or automated service profiles that do not require auditing.

> **NOTE:** User profiles used for automated tasks can contribute to heavy volumes of traffic that do not represent human action or a security threat. Once identified, auditing for these profiles (or more efficiently, groups that include several or all of these profiles) can be turned off to reduce the 'noise' of automated activity, so that effort can be concentrated on dealing with activity from real users. The IBM-supplied user profiles beginning in "Q" (QSECOFR, QTCP) are usually service accounts (but not always). On reports, service accounts can often be identified by repetitive activity, or activity at regular intervals.

Reviewing server activity

If there is a very large volume of traffic, there may be service profiles generating automated transactions that can be ignored in order to isolate the relevant activity.

1. On the Navigation Pane, select **Reports**.
2. Click **Add** and choose **Intrusion Detection - Server/Function Report**.
3. Your settings should include the server that yielded a large amount of transactions from your initial data review, and specify a time range. The best time range will be long enough to acquire a representative sample of transactions, but short enough to avoid excessive transactions in the tens of thousands or more. Use the following settings:
    - Name: "Server Function Report [server name]"
    - Transactions: *ALL
    - Server [server name] (e.g. *DATAQSRV)
    - Function: *ALL
    - For Date Range, specify the number of days you would like the report to include. For the first report, a week is usually a reasonable duration. For Date Range, choose Specific to indicate the report should include a specific start and end date. Choose Non Specific to include a period of time previous to the time the report is run.
    - For Detail Level, choose Transaction.
4. Click **Save** to save the report. You return to the Reports screen.
5. Click  to the right of Server Function Report and choose **Submit**. A message should appear in the lower left indicating the report has been submitted successfully.
6. Click **Spooled Files** in the Navigation Pane.
7. The report you just submitted will be at the top of the list. Click it to view. The summary of transactions on audited servers is a starting point for planning your security configuration.

Your audit results may not show traffic on each of the audited servers. A typical system will show activity on 12-15 servers with the heaviest activity on 6-8 servers. Some may not be used at all in your environment. (If you don't see traffic, remember it is also possible your system did not generate activity during the captured time range). If a server is not being used, it can be blocked to prevent all access, accidental or malicious.

For your initial review, you can identify the servers with and without activity in a general transaction summary. To do this, run a report that displays all transactions on all the servers you are auditing.

Reviewing server activity

1. From the Main Menu, choose option **80**, then **3** to view the Server Function Reports menu.
2. Choose **4**, (Selected Server, All Functions) All Transactions.
3. Next to Server, enter the server that yielded a large amount of transactions from your initial data review, and specify a time range. The best time range will be long enough to acquire a representative sample of transactions, but short enough to avoid excessive transactions in the tens of thousands or more.
4. Press `Enter` to run the report.
5. Press `F14` to work with submitted jobs.
6. Enter **8** for the job and press `Enter`. Scroll to identify profiles that submit repetitive transactions. Notice in the example below, the PLCM2ADM profile submits a transaction every 5 seconds.

```
                          Display Spooled File
File . . . . . :   LNSP087                        Page/Line   116/15
Control . . . . .  _______                        Columns     1 - 78
Find . . . . . .   ____________________________
*...+....1....+....2....+....3....+....4....+....5....+....6....+....7....+...
Allow  127.000.000.001 *DATAQSRV  RCVDTQMSG  10/31/13 07:38:01 PLCM2ADM  44490
Allow  127.000.000.001 *DATAQSRV  RCVDTQMSG  10/31/13 07:38:06 PLCM2ADM  44490
Allow  127.000.000.001 *DATAQSRV  RCVDTQMSG  10/31/13 07:38:11 PLCM2ADM  44490
Allow  127.000.000.001 *DATAQSRV  RCVDTQMSG  10/31/13 07:38:16 PLCM2ADM  44490
Allow  127.000.000.001 *DATAQSRV  RCVDTQMSG  10/31/13 07:38:21 PLCM2ADM  44490
Allow  127.000.000.001 *DATAQSRV  RCVDTQMSG  10/31/13 07:38:26 PLCM2ADM  44490
Allow  127.000.000.001 *DATAQSRV  RCVDTQMSG  10/31/13 07:38:31 PLCM2ADM  44490
Allow  127.000.000.001 *DATAQSRV  RCVDTQMSG  10/31/13 07:38:36 PLCM2ADM  44490
Allow  127.000.000.001 *DATAQSRV  RCVDTQMSG  10/31/13 07:38:41 PLCM2ADM  44490
Allow  127.000.000.001 *DATAQSRV  RCVDTQMSG  10/31/13 07:38:46 PLCM2ADM  44490
Allow  127.000.000.001 *DATAQSRV  RCVDTQMSG  10/31/13 07:38:51 PLCM2ADM  44490
Allow  127.000.000.001 *DATAQSRV  RCVDTQMSG  10/31/13 07:38:56 PLCM2ADM  44490
Allow  127.000.000.001 *DATAQSRV  RCVDTQMSG  10/31/13 07:39:01 PLCM2ADM  44490
Allow  127.000.000.001 *DATAQSRV  RCVDTQMSG  10/31/13 07:39:06 PLCM2ADM  44490
Allow  127.000.000.001 *DATAQSRV  RCVDTQMSG  10/31/13 07:39:11 PLCM2ADM  44490
Allow  127.000.000.001 *DATAQSRV  RCVDTQMSG  10/31/13 07:39:16 PLCM2ADM  44490
                                                                    More...
F3=Exit    F12=Cancel    F19=Left    F20=Right    F24=More keys

                                                                    3/22
```

Service accounts usually exhibit repetitive activity at regular intervals.

Now that you have discovered the servers with activity, and identified the users and transactions on those servers, you can begin implementing your security configuration by defining your own custom access control rules.

Adding the Initial Rule Set

In this section you will learn how to add user rules that tell Exit Point Manager to reject access to a server for a specific user, or for all users. You will also learn how to manage service profiles that require access, but do not need to be audited.

Blocking Unused Servers

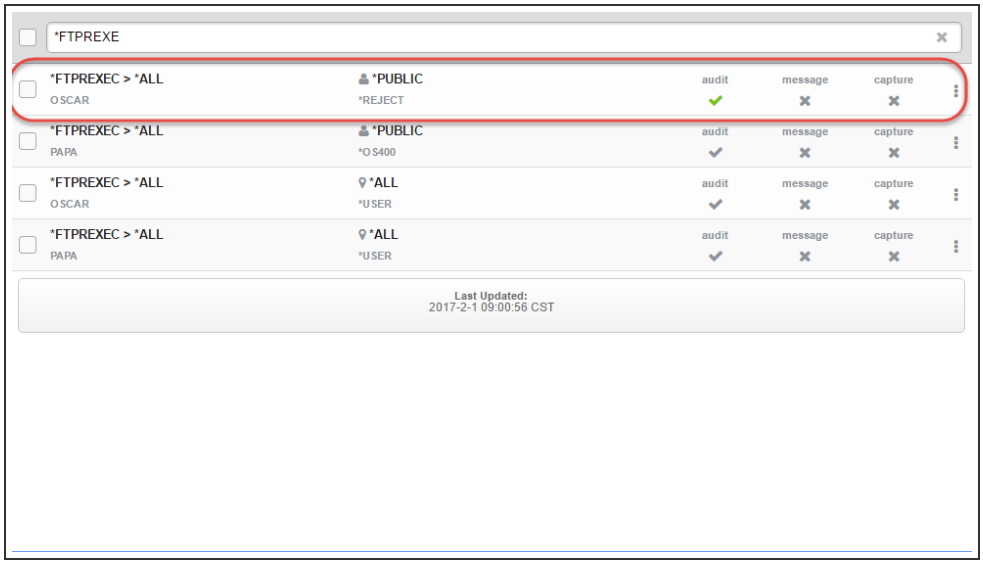
When you are confident that a server is not being used, you can create a rule to block any possible access. For the following example, we will assume the *FTPREXEC server is not being used and should be blocked.

Blocking a server for all users or for a specific user - web browser

1. On the Rules screen, click the *PUBLIC rule for the *FTPREXEC server.
2. Choose **Lookup** to the right of the Authority field.
3. Choose ***REJECT**.
4. Ensure Audit is set to Yes.

> **NOTE:** Whenever a reject rule is put in place it is highly recommended the Audit flag remains set to Yes. In the future, it may be useful to run an audit report showing any rejected access attempts against servers you have blocked. (If you are creating a new rule, set Messages to "Yes" in order to immediately submit a message upon any access attempts that are rejected.)

5. Choose **Save**. The *FTPREXEC server has been blocked for all users.
   This rule blocks access to all functions of the *FTPREXEC server for all users.



Blocking a server for all users or for a specific user - green screen

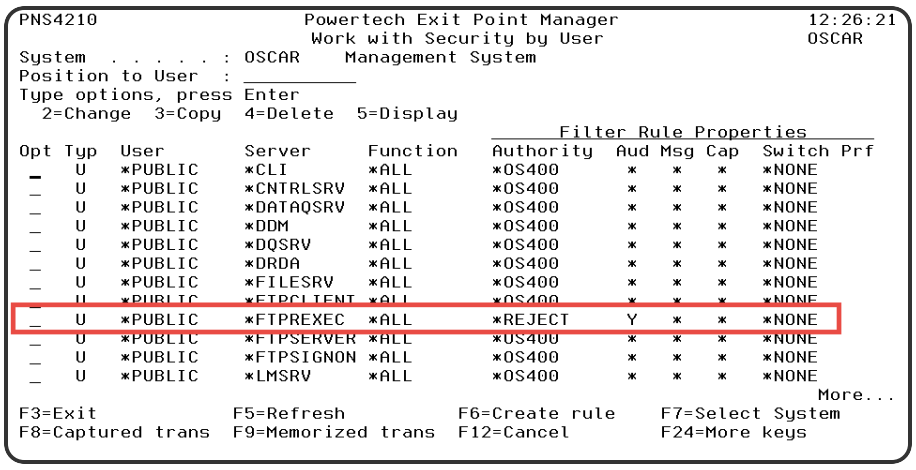
1. From the Main Menu, choose option **2**, Work with Security by User.
2. Next to the *FTPREXEC server *PUBLIC (default) user rule, enter **2**.
3. Change the Authority column from *OS400 to ***REJECT**. (Alternatively, to block a server for a particular user, you would create a new rule, indicating ***ALL** for Function, the user's ID for **User**, and ***REJECT** for Authority.)

> **NOTE:** Consider using a message management tool to help alert you of any reject messages.

4. Ensure Audit is set to **Y**.

> **NOTE:** Whenever a reject rule is put in place it is highly recommended the Audit flag remains set to Y. In the future, it may be useful to run an audit report showing any rejected access attempts against servers you have blocked. (If you are creating a new rule, set Msg to "Y" in order to immediately submit a message upon any access attempts that are rejected. Set Switch Profile to *NONE).

5. Press `Enter`. The *FTPREXEC server has been blocked for all users.



```
PNS4210                  Powertech Exit Point Manager                  12:26:21
                          Work with Security by User                    OSCAR
System  . . . . . : OSCAR    Management System
Position to User  : __________
Type options, press Enter
  2=Change  3=Copy  4=Delete  5=Display
                                          Filter Rule Properties
Opt Typ  User       Server     Function   Authority  Aud Msg Cap  Switch Prf
 _   U   *PUBLIC    *CLI       *ALL       *OS400      *   *   *   *NONE
 _   U   *PUBLIC    *CNTRLSRV  *ALL       *OS400      *   *   *   *NONE
 _   U   *PUBLIC    *DATAQSRV  *ALL       *OS400      *   *   *   *NONE
 _   U   *PUBLIC    *DDM       *ALL       *OS400      *   *   *   *NONE
 _   U   *PUBLIC    *DQSRV     *ALL       *OS400      *   *   *   *NONE
 _   U   *PUBLIC    *DRDA      *ALL       *OS400      *   *   *   *NONE
 _   U   *PUBLIC    *FILESRV   *ALL       *OS400      *   *   *   *NONE
 _   U   *PUBLIC    *FTPCLIENT *ALL       *OS400      *   *   *   *NONE
 _   U   *PUBLIC    *FTPREXEC  *ALL       *REJECT     Y   *   *   *NONE
 _   U   *PUBLIC    *FTPSERVER *ALL       *OS400      *   *   *   *NONE
 _   U   *PUBLIC    *FTPSIGNON *ALL       *OS400      *   *   *   *NONE
 _   U   *PUBLIC    *LMSRV     *ALL       *OS400      *   *   *   *NONE
                                                                    More...
F3=Exit            F5=Refresh          F6=Create rule    F7=Select System
F8=Captured trans  F9=Memorized trans  F12=Cancel        F24=More keys
```

6. When the server cache is cleared this rule will take effect. For the rule to be effective immediately, clear the server cache manually. To do so, turn rule enforcement off an on again as follows:

    a. In Work with Security by Server, enter **SP** for the server (in this case, *FTPEXEC).
    b. Change Exit Point Manager Rules Enforced to **N** and press `Enter`.

Managing Service Profile Activity

In the previous section (Discovery, Data Collection, and Analysis) we learned that PLCM2ADM is an automated service profile that requires access to the system, but does not need to be audited. Its transaction history produces unnecessary data that can be inconvenient to sift through while analyzing reports. Therefore, we can add a rule that grants it access to the server it requires (*DATAQSRV), with auditing turned off.

Creating a service profile user rule - web browser

1. On the Rules screen, choose **Add**.

Select the following values:

a. Rule Type = **User/User Group**
b. User=**PLCM2ADM** (the service profile account ID)
c. Server > Function=***DATAQSRV** and ***ALL** (this rule applies to all server functions)
d. Authority=***OS400** (uses the authorities granted by the system)
e. Audit=**X** (do not audit)

f. Message=**Inherit** (inherit global system value)
g. Capture=**Inherit** (inherit global system value)
h. Choose **Save** to create the rule.

Creating a service profile user rule - green screen

1. From the Main Menu, choose **1**, Work with Security by Server.
2. Type **UA** next to the server used by the service profile (in this case *DATAQSRV) and press `Enter`.
3. Enter **2** for the *PUBLIC rule.
4. Enter the following values:
    a. User Rule Type=**U** for an individual user (you would choose **G** for an User Group).
    b. User=**PLCM2ADM** (the service profile account ID)
    c. Server=***DATAQSRV** (the chosen server)
    d. Function=***ALL** (this rule applies to all server functions - alternatively, you could enter a specific function)
    e. Authority=***OS400** (uses the authorities granted by the system)
    f. Audit=**N** (do not audit)
    g. Message=* (inherit global system value (default=N))
    h. Capture=* (inherit global system value (default=N))
    i. Switch Profile=***NONE** (do not switch user profiles)
5. Press `Enter` to create the rule.

If the *PUBLIC rule for this server is set to *REJECT, all access attempts will be rejected. But, since this new rule is more specific, it is evaluated first, allowing PLCM2ADM access while restricting all other users. With this configuration, all access requests will be rejected, except for those originating from the user PLCM2ADM. See Active Rule and Rule Derivation for an explanation of Exit Point Manager's rule hierarchy.

Recursive Data Collection, Review, and Analysis

The general procedure explained so far in this guide of discovering, analyzing, and addressing security vulnerabilities with rules, is a process that must be repeated regularly to both respond to network security risks, and to ensure reports yield the most valuable data.

The following actions will help improve your Exit Point Manager implementation:

- Run reports in regular intervals. Rechecking report data regularly, and for select intervals, will help you validate your initial rule set and identify previously missed data points. See Reports.
- Confirm the users accessing the system are the ones expected. After auditing for all service profiles has been disabled, you will see only activity for real users.
- Confirm system accesses by users are correct for their needs. A user accessing the system should be doing so in a prescribed manner pertaining to their jobs description. For example, if the application they use daily is an SQL or ODBC based application, and you discover access by

that user over the FTP server, additional research may be warranted. Also consider the time of day and the point or origin of the access - identify events that occur at unusual or unexpected times and from unexpected locations (IP addresses).

- Watch for new service accounts used by new applications and user profiles added for new hires.

Adding, Changing, and Deleting User Rules

As you study the historical data, add, change, and delete user rules to respond to the access requirements of your organization. Continue to monitor reports and become more familiar with the authorized activity.

At this point it is time to add rules to allow *authorized user(s)* access at the SERVER level (setting the Audit value to **Yes** or **No** based on your auditing requirements). This is done in preparation for public lockdown, where the default (*PUBLIC) rules are set to reject (*REJECT), and all users who are not specifically granted access to them will be locked out. Earlier, under Adding the Initial Rule Set, we already blocked access to the FTPREXEC server for all users. Now, we can create a rule that grants access to that server for specific users only, while all other requests will continue to be rejected.

> **NOTE:** The following steps focus on FTPSERVER, which is a common server to lock down.

Granting authorized access at the SERVER level

> **NOTE:** When creating rules to grant authorized users access to a server, you may decide to add rules using their individual profile, or a group profile they are a member of. Choosing to audit or not audit will depend on whether the accesses or the user activity is required to visible. (Remember that activity is not retained for any user whose Audit flag setting is **No**.)

Authorizing a user access at the SERVER level - web browser

1. On the Rules Screen, click **Add**.
2. Select the following values:
    a. Rule Type=**User/User Groups**
    b. User=**MARKJ** (the user who requires access)
    c. Server > Function=***FTPSERVER** > ***ALL** (this rule applies to all server functions)
    d. Authority=***OS400** (uses the authorities granted by the system)
    e. Audit=**Yes** (audit (this value will depend on your requirements))
    f. Message=**Inherit** (inherit global system value (default=NO))
    g. Capture=**Inherit** (inherit global system value (default=NO))
3. Choose **Save**. The rule has been added. Rules for specific user profiles (or group profiles) are processed before *PUBLIC in the hierarchy, and allow you to grant access to specific users while blocking all others.
4. Repeat this procedure for all other servers the authorized user requires. Then, repeat the process for all other authorized users, until all users have access to the servers they require.

Authorizing a user access at the SERVER level - green screen

1. From the Main Menu, choose **1**, Work with Security by Server.
2. Type **UA** next to the server you would like to grant access to. The existing rules for that server appear. For this example, we will be granting MARKJ access to the FTP server (*FTPSERVER).
3. Press `F6` to create a new rule.
4. Enter the following values:
    a. User Rule Type=**U** for an individual user (you would choose **G** for an User Group).
    b. User=**MARKJ** (the user who requires access)
    c. Server=***FTPSERVER**
    d. Function=***ALL** (this rule applies to all server functions)
    e. Authority=***OS400** (uses the authorities granted by the system)
    f. Aud=**Y** (audit (this value will depend on your requirements))
    g. Msg=* (inherit global system value (default=N))
    h. Cap=* (inherit global system value (default=N))
    i. Switch Profile=***NONE** (do not switch user profiles)

    Rules for specific user profiles (or group profiles) are processed before *PUBLIC in the hierarchy, and allow you to grant access to specific users while blocking all others.
5. Press `Enter`. The rule has been added. (Remember, the rule will take effect once the server cache is cleared).
6. Repeat this procedure for all other servers the authorized user requires. Then, repeat the process for all other authorized users, until all users have access to the servers they require.

Changing and Deleting Profile Rules

As employees depart the company, or move to other roles, it is helpful to develop internal procedures to notify the Exit Point Manager product administrator a user has left, or has changed roles. If individual profile rules are used, their profile should be changed from *OS400 to *REJECT. At some point the profile should be deleted from the product. (If group profiles are used, you would not need to make rule changes in the product, assuming the profile is removed from the system or group.)

Deleting a Rule

- See Insite Web Browser Help for information on deleting rules using Insite.
- To delete a rule on the green screen, use **4** (Delete) on the Work with Security by User panel or Work with Security by Location panel.

Copying Rules across Systems

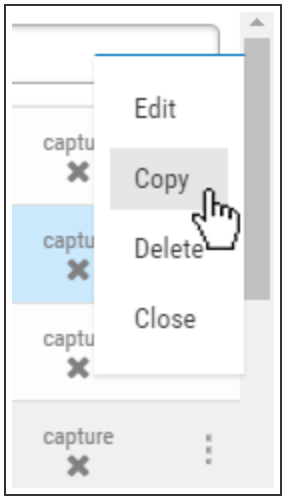
Once you have configured Rules on the Management System, you can copy them to other Endpoints in order to quickly propagate your security policy across your network.

> **NOTE:** Copying across systems is a feature of the Insite web UI and is not available from the green screen.

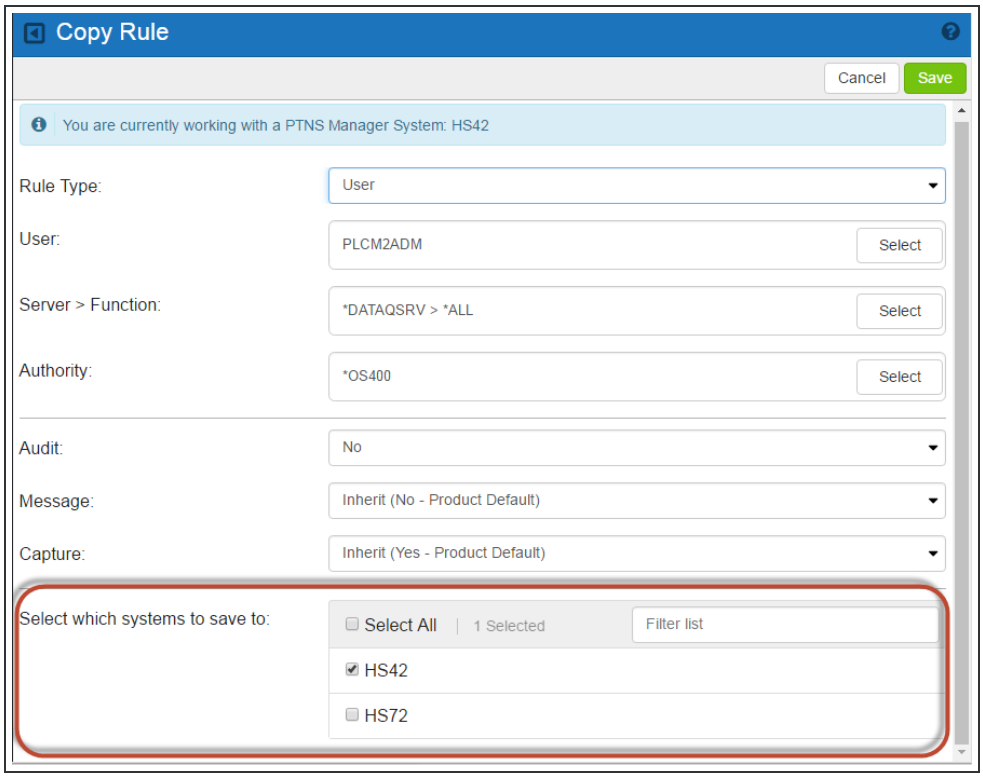
For the following instructions, we will copy a User Rule. Before copying a User Rule, you must ensure a user profile with a matching name exists on all target Endpoints.

To Copy a Rule

1. On the Rules screen, click  on the right side of the Rule listing and select **Copy**.



2. In the Copy Rule screen, at the bottom, choose which systems to save to. If the rule already exists on the system you are using (the Manager system), uncheck the checkbox for that system. Otherwise you will get an error stating that the rule already exists on that system.



3. Click **Save**. You are notified of the results. Note that duplicate rules on a system are not allowed.

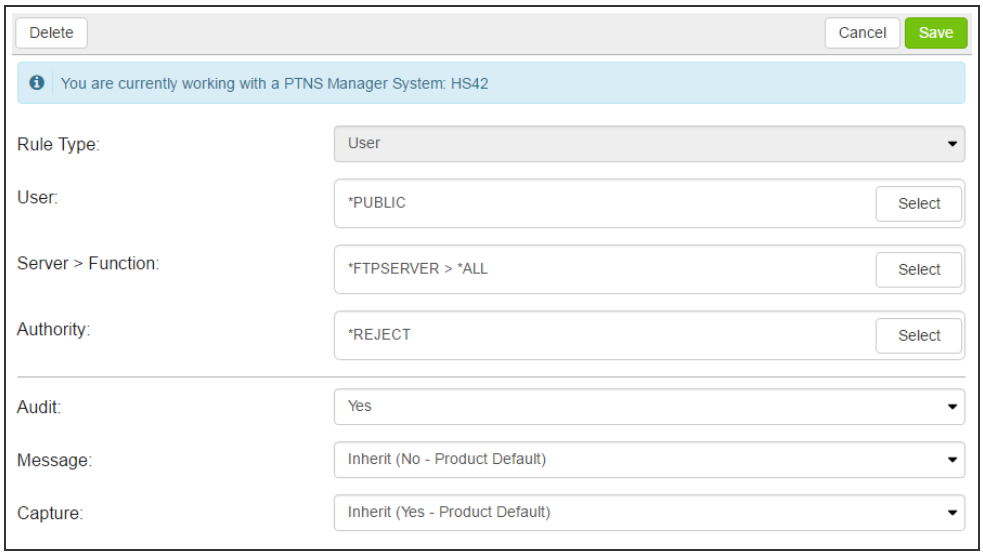
Public Lockdown

Once you are confident you have spent enough time and study looking at the historical data, and have the allowed SERVER user rules in place, it is time to block the potential for all other unauthorized access. This process is known as *public lockdown*. In addition to rejecting public access, during this process, you will instruct Exit Point Manager to trigger an immediate alert for all rejected transactions so they can be promptly addressed.

If you are using Central Administration to manage multiple systems, note that the default *PUBLIC rules cannot be copied to Endpoints. Each default *PUBLIC Rule will need to be changed to *REJECT manually for all Endpoints individually.

Locking down your servers - web browser

1. On the Rules screen, click one of the *PUBLIC user rules.
2. Choose **Lookup** to the right of the Authority field and choose *REJECT.
3. Under Audit, select **Yes**.



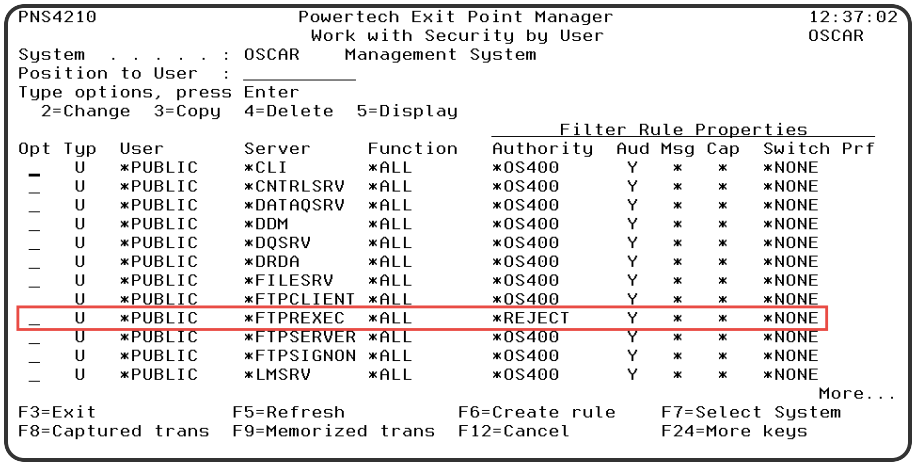
4. Click **Save**.
5. Repeat these steps for the next server, until all servers have been locked down.

NOTE: Reject rules may have an immediate impact once added. You may get calls from users who think they should have access to a service no longer permitted, or users whose job description has changed, requiring different accesses. On implementation of public lockdown, plan to run regular rejected transaction reports. See Transaction Report Menu.

Locking down your servers - green screen

1. From the Main Menu, choose option **2**, Work with Security by User.
2. Choose **2** to change one of the *PUBLIC rules.

3. Change Audit to **Y**. Repeat for all the *PUBLIC rules so they will all be audited.
4. Choose **2** on the *PUBLIC rule for a server you want to lock down.
5. Set Authority to ***REJECT**. Change one server to *REJECT (with Aud=Y) at a time, then monitor and respond to any subsequent access requirements.



6. Repeat these steps for the next server, until all servers have been locked down.

NOTE: Reject rules may have an immediate impact once added. You may get calls from users who think they should have access to a service no longer permitted, or users whose job description has changed, requiring different accesses. On implementation of public lockdown, plan to run regular rejected transaction reports. See Transaction Report Menu.

Recommendation – Use a message management process such as Powertech Interact to be notified of reject messages (with Msg set to Y) in real time.

Oversight Review

After all of your servers have been locked down, continue monitoring for rejected transactions. Add user rules as necessary to amend any access oversights. In urgent situations you have the option of changing the *PUBLIC *REJECT value back to *OS400 while research of the prior rules are reviewed.

Use reports to look at the rejected and allowed transactions. Reports are available by Server, User profile, and Location (IP address). See Reports.

Auditing Exit Point Manager Rules

While the majority of oversight and Rule management will take place from the Management System, Exit Point Manager also allows Rules to be managed directly from an Endpoint. This might be necessary, for example, if access to the Management System is unavailable, but critical business processes require a Rule to be changed on an Endpoint. To verify the integrity of Exit Point Manager

throughout your network, and ensure adherence to your organization's security policy, you can run an audit to identify and manage Rules that have been changed on Endpoints directly.

> **NOTE:** Audits only apply to Endpoints. The Management System is always skipped during an audit.

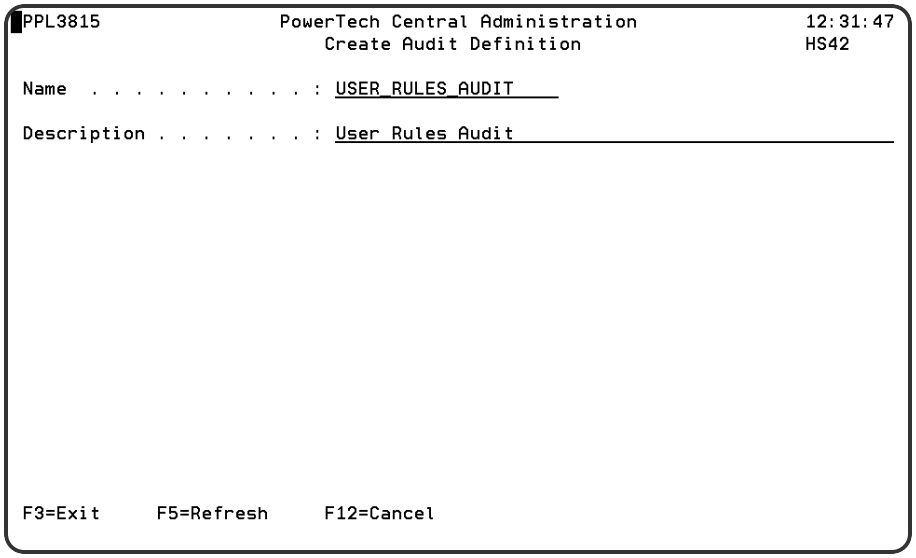
To conduct an audit, you must first define a System Group that includes the systems you would like to audit, then use Central Administration's Audit Menu to complete the audit, applying remedies as necessary.

To add a system group

1. From the Powertech Main Menu, choose option **80**, Central Administration, then choose option **5**, Auditing Menu.
2. Choose option **80**, Work with System Groups.
3. Type `F6` to create a System Group.
4. Name the Group and add a description, then use **1** to specify the systems you will be auditing.
5. Press `Enter` twice to add the System Group, then press `F3` until you return to the Auditing Menu.

To run a user rules audit

1. On the Auditing Menu, choose option **1**, Audit Definitions.
2. Type `F6` to create a new Audit Definition.
3. Name the definition (e.g. "USER_RULES_AUDIT"), add a description, and press `Enter`.

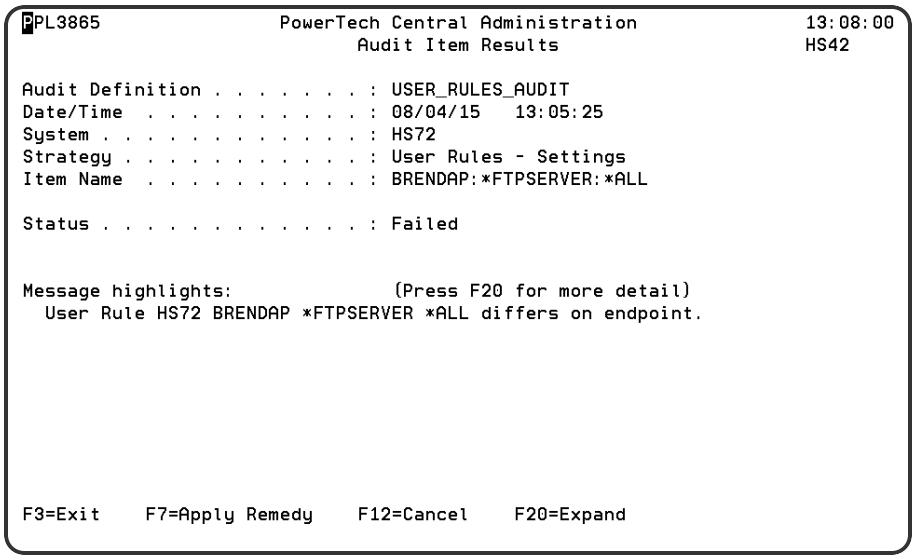


4. Enter option **7** (Strategies) for the Audit Definition you just created.
5. Place a **1** next to the strategies you would like to use (e.g. the User Rules strategies), and press `Enter`, then press `F3` to return to Audit Definitions.
6. Enter **6** (Start) for the Audit Definition and press `Enter`. Then, choose the System Group you defined earlier.
7. Enter **9** for the Audit Definition. When the audit is finished, enter **7** (Strategy Results) for the audit you just ran.

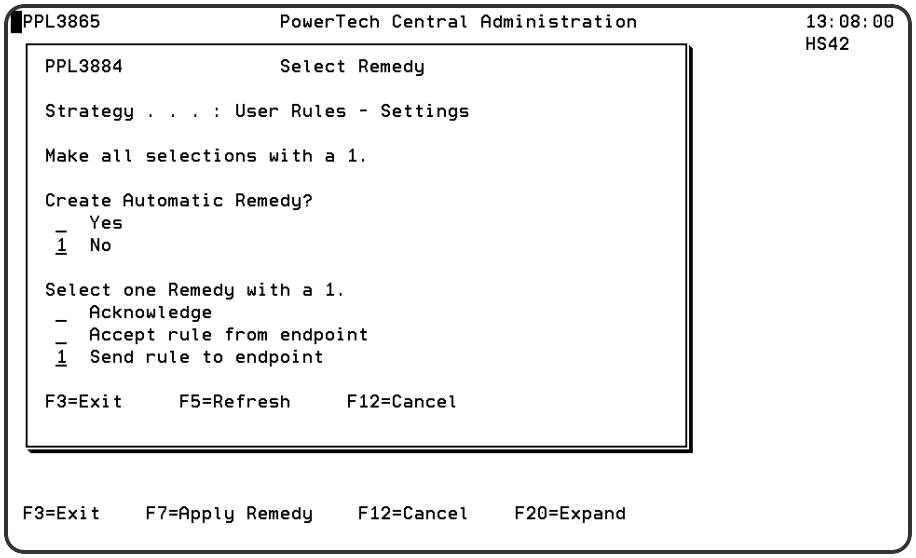
8. Enter **6** (System Results) for User Profile Settings. ("Failed" means there is at least one User Rule that doesn't match the Management System.)
9. Enter **5** (Item Results) for a system marked "Failed."

> **NOTE:** Any discrepancy to a Rule between systems, including differences to the audit, message, and capture flags, will cause an Endpoint to fail the audit.

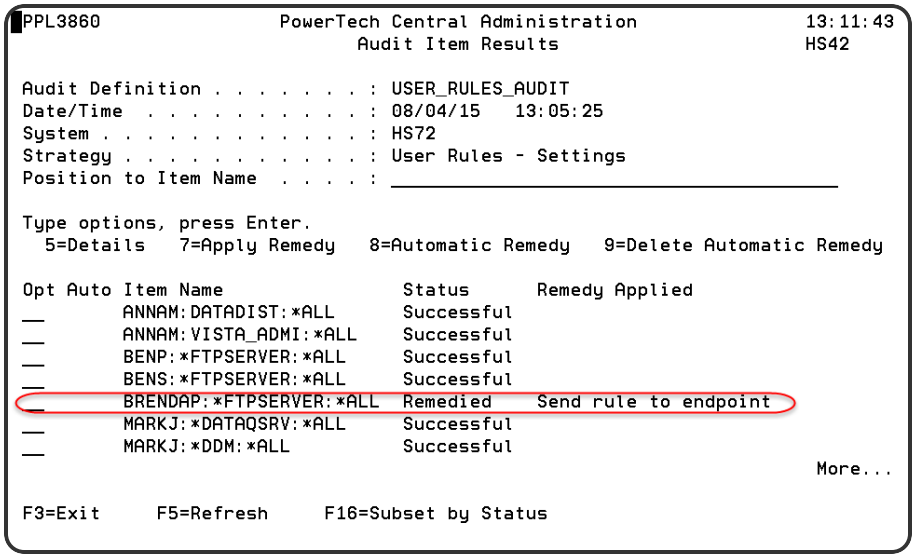
10. Find the Rule whose Status is Failed and enter **5** (Details) to review the inconsistent setting(s).



11. Press **F7** (Apply Remedy).
12. Enter **1** for "Accept rule from endpoint" to update Exit Point Manager's Rule Configuration to match that of the Endpoint for this Rule. Choose "Send rule to endpoint" to reset the Rule to match Exit Point Manager's configuration. If you would like the Rule to continue to differ on the endpoint, choose "Acknowledge."



13. Press `Enter`. You return to the Audit Item Results, where the Status and Remedy Applied are listed.



14. Press `F3` and repeat for other Profiles on the system. Then, repeat this process for Failed Profiles on other systems.

Granulating Rules for Specific Needs

Granular rule forms may be preferable in some instances. They can be used to target specific users, objects, and transactions. They are highly desirable for targeting specific objects or transactions. While they offer precision security, they may add administrative and system overhead.

Web browser users, for more information, see

- User Rules to learn more about copying, deleting, and adding multiple user rules at once, and adding rules for specific server functions.
- Object Rules to learn more about defining authority rules to control access at the object level.
- Transaction Security to learn more about controlling which transactions are allowed to flow in and out of your system.

Green screen users, for more information, see:

- User Rules to learn more about copying, deleting, and adding multiple user rules at once, and adding rules for specific server functions.
- Object Rules to learn more about defining authority rules to control access at the object level.
- Transaction Security to learn more about controlling which transactions are allowed to flow in and out of your system.

Recommendation – Consider contacting Powertech Support for guidance on making the optimal choice to fit your specific need.

Ongoing Auditing

Review and modify user auditing controls for long term appropriateness.

- Repeat general recursive data review and analysis, responding with new or updated user rules to accommodate the current access requirements.
- Continue oversight of rejected transactions at chosen intervals, responding with user, object, or transaction rules to ensure up-to-date, precision compliance.

Recommendation – You can use Powertech Compliance Monitor or Robot Schedule to automate reporting. See www.helpsystems.com for more details.

Keeping Exit Point Manager Up-to-Date

- Updates to new product versions can be performed at any time, but it is highly recommended you contact Powertech Support for considerations on system impact.
- Visit https://community.helpsystems.com/products-and-downloads/ to acquire the latest product versions.
- Visit the Help Systems Monthly product update pages to see all the new updates and fixes.

Recommendation – Develop a plan to update Exit Point Manager on a regular basis and apply software updates 2-3 times per year.

More on Access Control Rules - Insite web UI

The power of Exit Point Manager resides in its ability to control network access to IBM i network servers and server functions according to the rules you specify.

As discussed earlier (see Getting Started with Exit Point Manager, you can set rules for a User (user profile), Group profile, or Supplemental Group profile. For example, you can create a rule by user ID that directs the FTP server to reject any upload attempt from users who are members of a particular group profile. For more information on user rules, see User Rules.

Another method of defining an access rule is by *location*. A Location is Exit Point Manager's definition of the origin of an access request. A location can be a specific IP, group IP, generic IP, range of IP addresses, or SNA device. (For example, a group of IP addresses may correspond to a corporate office's physical location, e.g. *DENVER.) Location security rules allow you to grant access to, and define the authorities for, all approved dial-in and Internet origins, while restricting access to unapproved origins according to the rules you define. For example, you can create a location rule to direct the IBM i FTP server to reject any FTP request coming from outside your local network. See Location Rules.

Exit Point Manager also lets you set object rules that are configured at the object level, for a specific user or location, for a specific object, and for a specific type of access. Creating an object rule allows you to, for example, specify who can access your IBM i payroll database. See Object Rules.

Authorities

Access Control Rules establish the action to be taken when a particular server or server function is accessed. You can specify the following actions:

- ***OS400** - Allow the request using the user's normal IBM i authorities as if Exit Point Manager were not installed.
- ***REJECT** - Reject the request.
- ***SWITCH** - Allow the request after switching the request to run under the authority of a different user profile—the switch profile. See Switch Profiles.
- ***MEMOS400/*MEMREJECT/*MEMSWITCH** - Use the rules specified in a previously memorized transaction. See Memorizing Transactions.
- ***MEMOBJ** - Check Object List. (Refer to rules defined for specific objects.) See Object Rules.

> NOTE: **Note:** Many of the examples shown throughout this section use *FTPSERVER. The process of setting up other servers is similar, although you will see different functions. In addition, some types of rules may not apply to all servers.

Flags

Access Control Rules also include *flags*. The three flags are Aud (Audit), Msg (Message), and Cap (Capture).

- **Audit**
  - ✔ = Record this request to the Audit Journal
  - ✘ = Do not record the request (unless request fails)
- **Message**
  - ✔ = Send a message when the request is received
  - ✘ = Do not send a message
- **Capture**
  - ✔ = Capture transactions for this request
  - ✘ = Do not capture transactions

> NOTE: If Authority is *USER, Audit, Message, Capture, and Switch Profile are deferred. If Authority is not *USER, Audit, Message, Capture, and Switch are enforced.

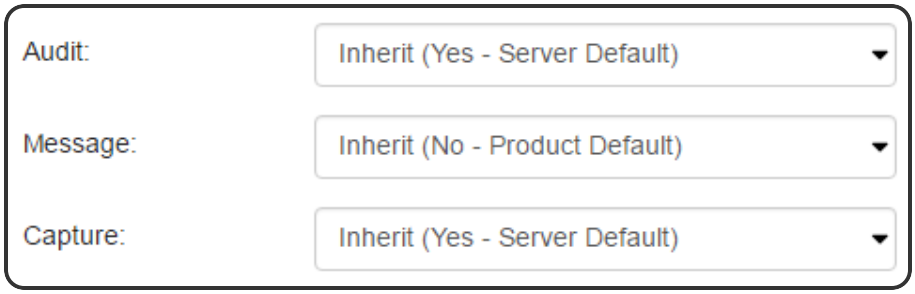
Active Rule and Rule Derivation

A hierarchy of settings dictate the Audit/Message/Capture Flag status for any given rule. The hierarchy, from most general to most specific, is composed of settings from the following screens:

Rule derivation on Insite

- System level details can be changed in the Edit System Values screen.
- Server level details can be changed in the Edit Server Function Rule screen (*ALL).
- Function level details can be changed in the Edit Server Function Rule screen (*[server] > [function]).
- User/Location-level details can be changed in the Edit Rule screen.

A setting of *Yes* or *No* on a more specific level of the hierarchy always overrides a *Yes* or *No* setting on a more general level. When a Flag is set to *Inherit*, its setting is derived from the next-highest level in the hierarchy. You can instantly see the status of all Flags, including the setting from which the status derives, by referring to the text adjacent to the Flag's setting in the rule's drop-down menu.



Identify the status of Flags using the static text.

For example, suppose there is a rule for user MARKJ and the audit and capture values are both set to Inherit. If that rule is invoked, those Inherit values each resolve to either Yes or No based on the hierarchy. If all properties are set as shown in the following table, then the Active Rule for user MARKJ is Audit = Yes, Message = No, and Capture = Yes.

IF	Audit	Msg	Cap
Edit System Values (Product Defaults)	yes	yes	No
Edit Server Defaults	Inherit	No	Inherit
Edit Server Function Rule	Inherit	No	Inherit
MARKJ (rule)	Inherit	Inherit	Yes
Then, the Active Rule is	**Yes**	**No**	**Yes**

NOTE: For Location Rules with authority set to *USER, the transaction is evaluated by the incoming user profile. See Authorities Selection window.

Switch Profiles

The switch profile action is the key to providing flexible security for your network users. This action lets you specify an alternate user profile, called a *switch profile*, that network access requests run under. This allows you to use standard IBM i security commands to establish the authorities to objects on your system for a user when they access the system through the network servers.

To define a Switch Profile as part of a rule:

1. Set the Authority to *SWITCH. When you do, the Users selection window appears.
2. Specify the target user.

A typical requirement for *SWITCH profile:

- User belongs to a group profile that owns objects.
- Network access gives the user *ALL authority to the entire application.
- Use Exit Point Manager to allow selective access.
- Dynamically change user authority “on the fly.”
    - Give more or less authority than normal.
- *SWITCH profile does not affect green screen operations.
    - Can configure authority independently.

For details, see Switch Profiles.

Exit Point Manager always searches for location access rules first

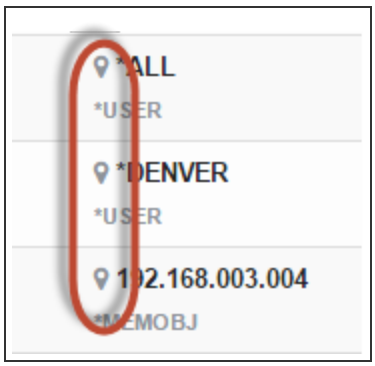
User access rules are considered only if a location access rule is found with an action that indicates that user access rules should be used.

Location Rules

A Location rule can be used to control access to the IBM i servers capable of accepting remote transactions. (Exit Point Manager includes one default location rule for each server). Location rules can be used to define actions for access to a server, or for access to a specific function of a server (e.g. DELETEFILE).

All default location rules include the same parameters and are set with the same default values. See Parameters and Default Values.

All functions related to adding, editing, and deleting rules are available using either the web browser interface or the green screen, although the procedures for accomplishing these tasks differ considerably. While the green screen interface offers many different screens that display the existing location rules in different formats, the browser interface offers a single screen (the Rules screen), with robust search and filtering capabilities that allow *all* rules (user and location) to be accessed immediately, for multiple systems, and with the ability to copy rules between systems. See Using the Web Browser Interface for details.



On the Rules screen, location rules can be identified by the icon next to the user profile or group name.

Adding and changing location rules using the web browser interface

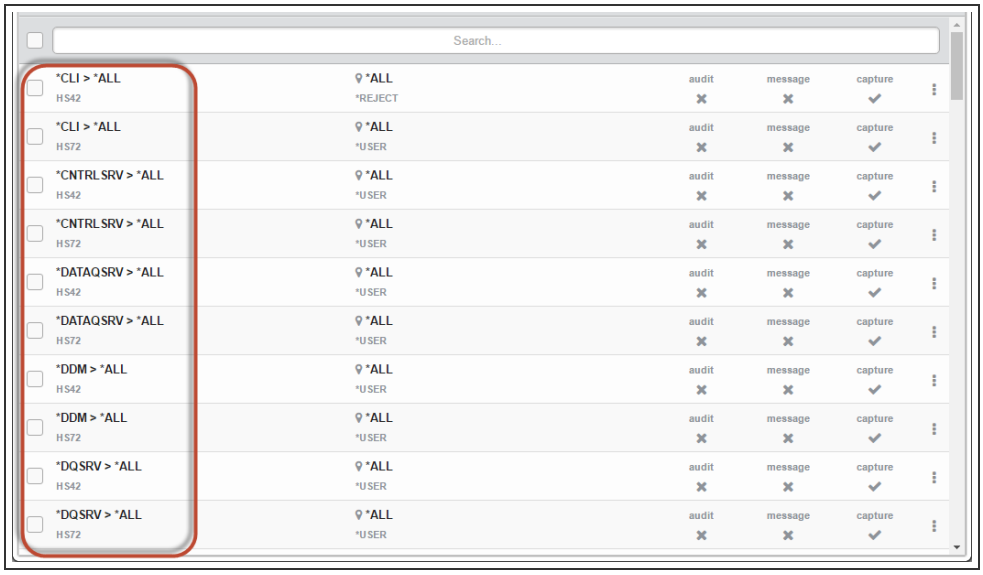
1. To add a location rule, from the Rules screen, choose **Add** or, select an existing rule to change it.
2. For Rule Type, choose **Location/Group**.
3. Choose the **Lookup** button next to Location/Group to select a location or IP address group. For information on creating an IP address group, see IP Address Groups. Or, enter an IP address, or range of IP addresses in this field. (See New/Edit Rule screen for the list of syntax criteria for valid IP address values and other devices.)
4. Choose the **Lookup** button next to Server > Function to select the desired server and function. For Functions, choose ***ALL** if you would like the rule to apply to all server functions.
5. Choose the **Lookup** button next to Authority to choose an authority for the location rule. See Authorities selection window for a list of the available authorities.
6. Use the Audit/Message/Capture drop-down lists to turn on auditing, messaging, and capturing. See New/Edit Rule screen for more details.
7. Choose **Save** to add the new location rule.

Viewing default location rules using the web browser interface

Exit Point Manager ships with default location authority rules for each server. You can view these rules from the Rules screen.

To display the Locations Rules:

1. Click **Rules** on the Navigation Pane.
2. Click and select Filter By > **Location Rules**. (Click to dismiss the Filter).



User Rules

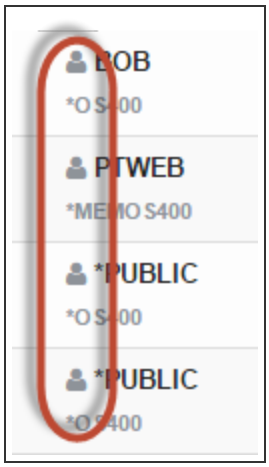
User authority rules are useful to control access to servers and functions for particular *users*. User security rules are evaluated only if a location rule specifies to use *USER security rules. (Exit Point

Manager includes one default user rule for each server. See Default User Rules). Like Location rules, User rules can be used to define actions for access to a server, or for access to a specific function of a server (e.g. DELETEFILE).

> **NOTE:** In order to add User Rules on an endpoint, the PNSEVTMON monitor job must be running. This job starts automatically during Exit Point Manager installation. If, for some reason, this job has been stopped, you can issue the PTNSLIB07/PNSSTRMON (or PTNSLIB/PNSSTRMON, depending on your product library) command to restart it.

To apply the same rule to multiple profiles, create an *User Group*, then choose the group when you create the User Rule. See Creating a User Group.

All default location rules include the same parameters and are set with the same default values. See Parameters and Default Values.



On the Rules screen, user rules can be identified by the icon to the left of the user profile or group name.

Adding user rules

1. To add a user rule, from the Rules screen, choose **Add**.
2. For Rule Type, choose **User/User Group**.
3. Choose **Lookup** next to User/User Group to select a user profile or User Group. See Users selection window.
4. Choose **Lookup** next to the Server > Function field to select the desired server and function. For Functions, choose *ALL if you would like the rule to apply to all server functions. See Server selection window.
5. Choose **Lookup** next to the Authority field to choose an authority for the location rule. See Authorities selection window for a list of the available authorities.
6. Use the drop-down lists below to turn on auditing, messaging, and capturing. See New/Edit Rule screen for more details.
7. Click **Save** to add the new user rule.

Creating a User Group

1. On the Navigation Pane, choose **User Groups**.
2. Click **Add**. The New User Group screen appears.

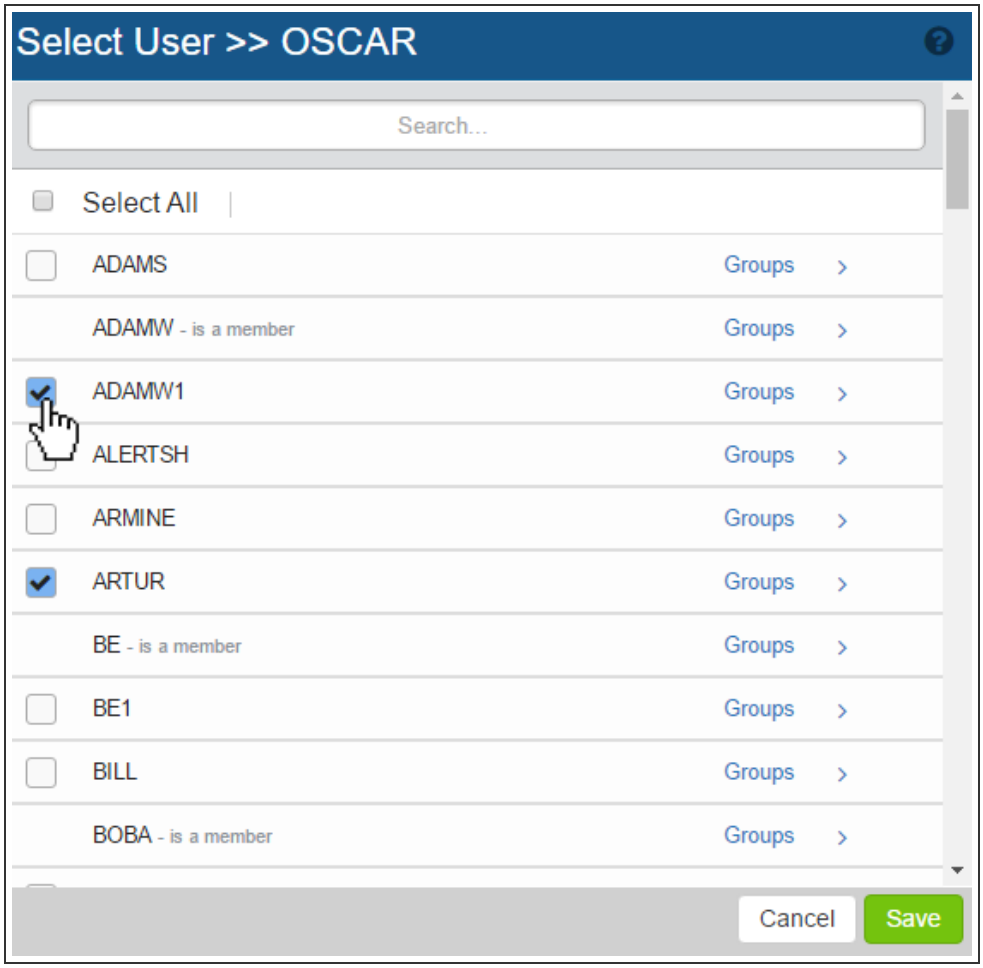
3. Name the User Group and add a Description.
4. In the "Sequence" section, indicate the order in which this User Group will be evaluated by the exit point programs. For more details, see User Groups.
5. In the "Members" section, specify the profiles you would like to include as members of the User Group. Click **Add Member** to open the Select User screen where you can select one or more users.

> **NOTE:** Adding OS User Groups to a Exit Point Manager Group is not recommended.

6. Click **Save** to save the User Group. This User Group will now be available in the list of profiles while creating or editing user rules.

Adding Members to a User Group

1. On the Navigation Pane, choose **User Groups**.
2. Select a User Group to open the Edit User Group screen.
3. Under Members, choose **Add Member**.
4. Check the users you would like to add.

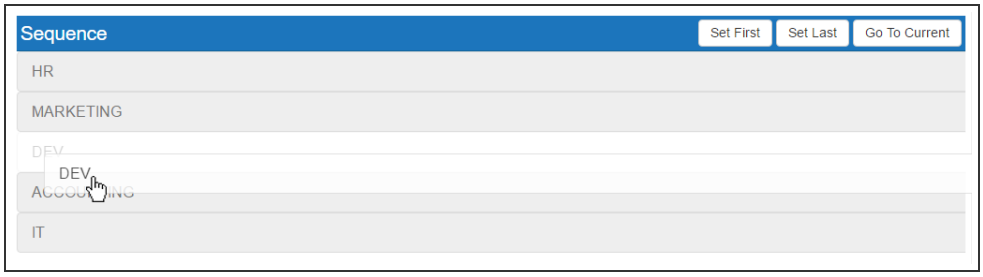


> **NOTE:** Adding OS User Groups to a Exit Point Manager Group is not recommended.

5. Click **Save**.

Changing the Sequence of User Groups

1. On the Navigation Pane, choose **User Groups**.
2. Select the User Group whose sequence you want to change. The Edit User Group screen appears.
3. Click and drag the User Group to the desired order in the sequence.

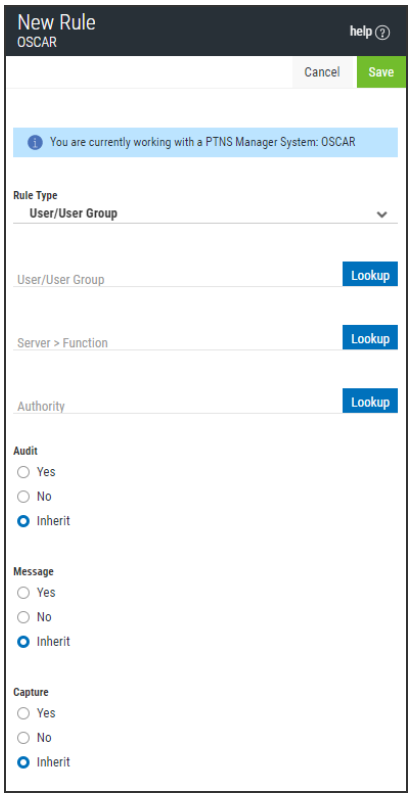


4. Click **Save**.

Restricting access to a server function for all users but one

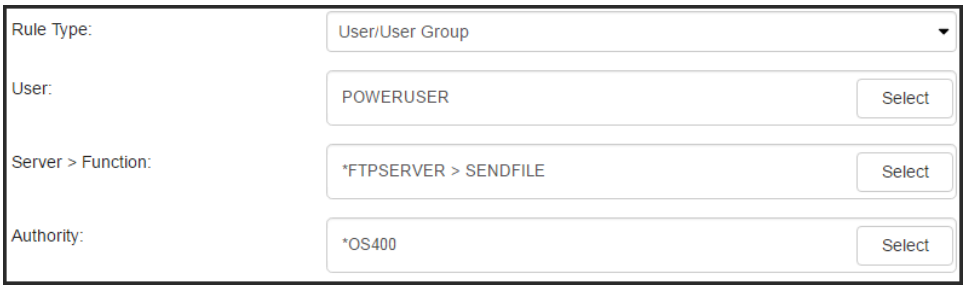
1. First, create a new user rule that sets the SENDFILE function of the FTP server to reject for all users (*PUBLIC). To do so, from the Navigation Pane, click **Rules**, then choose **Add**.
2. For Rule Type, choose **User/User Group**.
3. Select the following values in New User Rule screen:

- User = ***PUBLIC**. The rule will be in effect for all users.
- Server > Function = **SENDFILE**. This is the function used by the FTP server to download files from IBM i.
- Authority = ***REJECT**. Exit Point Manager will reject any FTP SENDFILE transactions.



4. Click **Save**. Now, create a rule to allow POWERUSER to use the SENDFILE function.
5. Choose **Add** and select the following values:

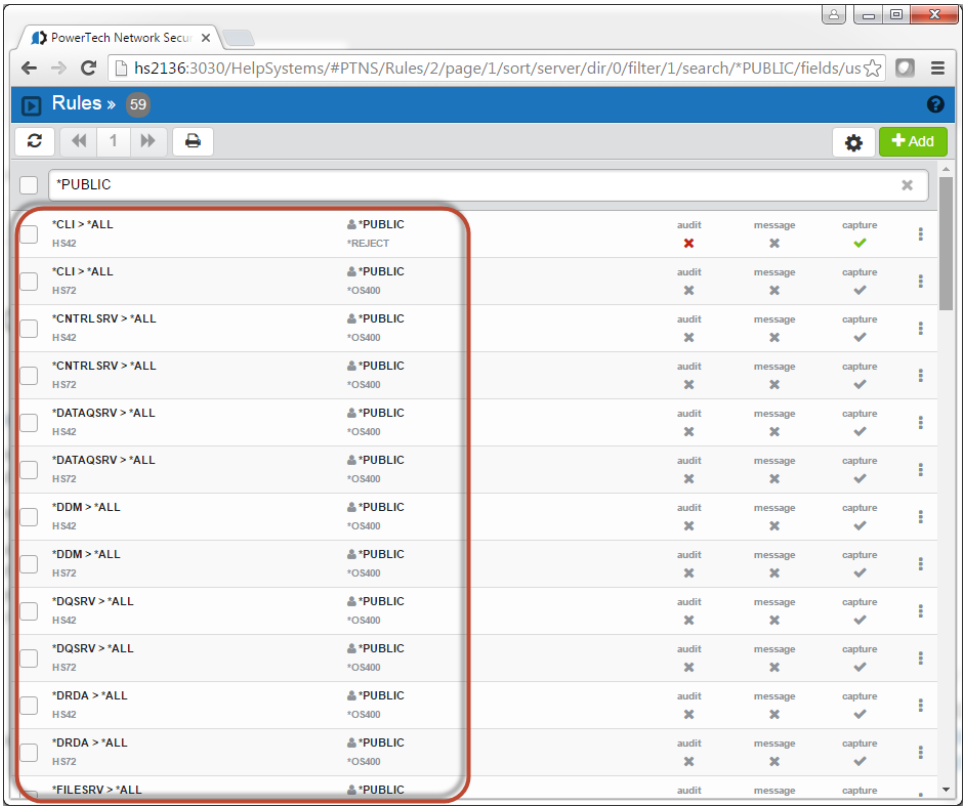
- For Rule Type, choose **User/User Group**.
- User = **POWERUSER**. The rule will be in effect for all users.
- Server > Function = **SENDFILE**. This is the function used by the FTP server to download files from IBM i.
- Authority = ***OS400**. Exit Point Manager will *allow* any FTP SENDFILE transaction for POWERUSER.



6. Click **Save**. Since this new rule is more specific than the other rules in effect, it is evaluated first, allowing POWERUSER to download files, but restricting all other users from the SENDFILE function.

Default User Rules

Exit Point Manager ships with default user authority rules for all supported IBM i servers. View these rules by referring to the *PUBLIC rules on the Rules screen.



Server IDs

Exit Point Manager supports the following servers and provides one default user rule for each server.

Exit Point Server	Description
*CLI	Call Level Interface
*DDM	*Distributed Data Management Server
*DRDA	Distributed Relational Database
*DQSRV	Data Queue Server
*FILESRV	File Server
*FTPCLIENT	IBM i FTP Client
*FTPSERVER	IBM i FTP Server
*NDB	Native Database Request

Exit Point Server	Description
*RMTSRV	Remote Command and Distributed Program Call Server
*RTVOBJINF	SQL Retrieve Object Information
*SQL	Database Server Initialization
*SQLSRV	SQL Server
*TELNET	Telnet Device Initiation/Termination
*DATAQSRV	Optimized Data Queue Server
*FTPREXEC	FTP Execute Remote Command (REXEC)
*REXEC_SO	Remote Execute Command Signon Server
*TFRFCL	File Transfer Server
*TFTP	Trivial FTP Server
*CNTRLSRV	License Management Central Server
*FTPSIGNON	FTP Logon Server
*LMSRV	License Management Server
*MSGFCL	Message Function Server
*RQSRV	Remote SQL Server
*SIGNON	Signon Server
*VPRT	Virtual Print Server
QNPSERV	Network Print Server

Servers and Functions

ShowCase Exit Points

Exit Point Manager provides access control and monitoring for exit points that are specific to the ShowCase software suite:

Exit Point Server	Description
*VISTA A Showcase corporation server. (*VISTA)	ShowCase *VISTA Clients
*VISTAPRO A Showcase corporation server. (*VISTAPRO)	ShowCase *VISTAPRO Clients

Exit Point Server	Description
DATADIST A Showcase corporation server. (DATADIST)	ShowCase DATADIST Clients
VISTA_ADMI A Showcase corporation server. (VISTA_ADMI)	ShowCase VISTA_ADMI Clients

Pre-filters

Pre-filters allow you to establish a one-to-one relationship between a specific IP address (location) and a user in order to screen transactions before they are evaluated in full by Exit Point Manager, or restrict access to a server altogether. For example, by configuring a Location + User Pre-filter, you can specify whether to allow or not allow a transaction from a specific IP address and user — allowing it causes the transaction to be further evaluated by Exit Point Manager rules; not allowing it is equivalent to a Exit Point Manager reject. A Server Pre-filter can perform the same action for all transactions to, for example, the FTP server. The other actions that you can specify are to audit the transaction, send an immediate message, and capture the transaction.

These actions work exactly like their equivalents within the Exit Point Manager rules processing scheme.

To configure Pre-filters, see Server Pre-filters panel and Location + User Pre-filters panel.

Object Rules

IBM defines an object as a named storage space that consists of a set of characteristics that describe it and its data. Thus, an object is anything that occupies space in storage, and on which you can perform operations. Examples of objects include programs, files, libraries, folders, and IFS directories and files. Exit Point Manager allows you to define authority rules to control access at the object level.

You can set rules for libraries and the objects in them, or an IFS path. These rules can be specific to a user (or *PUBLIC) or location and contain the object library, name, and type. Using an object rule, you can define access to both the object and the data contained within the object.

Object rules allow you to specify the operation that the rule allows (*ALL, *CREATE, *READ, *UPDATE, or *DELETE), and the action to take (*REJECT, *OS400, *SWITCH) for data access and object access. Thus, you can define an object rule for a specific user or location, for a specific object, and for a specific type of access. In addition, you can specify values for auditing, capturing transactions, and messaging in your object rules.

Setting rules at the object level provides a different measure of control than setting rules at the user or location levels. For example, you can set one object rule to restrict all users and locations from accessing a specific file (such as payroll) instead of setting multiple rules at the user or location levels to control access.

Object Rules and Exit Point Manager

There is a close relationship between rules in Exit Point Manager. Object rules need *MEMOBJ filter rules to trigger them. When you define an object rule, you select the servers and functions that will enforce the rule. This creates the *MEMOBJ Authority filter rules for the user or location object rule. The *MEMOBJ Authority filter rule tells Exit Point Manager to check memorized transactions (MTR) for authority. If no MTR authority is found, it then checks the transaction against the object rules.

Whenever any rule changes, Exit Point Manager manages the relationships between the filter rules, object rules, and memorized transactions.

If there are no filter rules with *MEMOBJ authority that refer to a particular active object rule, that object rule is set to *INACTIVE by the system.

> **NOTE:** When there are no more active object rules for a given user or location, you should remove or modify the filter rules for that user or location. When you select to deactivate (for example, by changing or deleting) the last active object rule for a user or location, Exit Point Manager asks you to select how to handle the filter rules that are in place. If you use a command (such as CHGOBJRUL or DLTOBJRUL), you must specify command parameters that define how to handle the filter rules in case they are needed at run time during command processing.

Object Rules and the Remote Command Server

The Remote Command server has some unusual properties. The server only recognizes and reports on object type *CMD, and does not supply any other object type to the server. This means Exit Point Manager cannot identify any other object type to apply to the object rule. Remote Command server Object Rules will not work unless they are for the command itself.

Example:

The following remote command issued from a DOS prompt:

```
RMTCMD CRTLIB TESTLIB //mysystem
```

will work if the object rule is for CRTLIB (type *CMD). It will not work for TESTLIB (type *LIB).

Managing object lists

To create an object list

1. From the Navigation Pane, click **Object Lists**.
2. Choose **Add**. The New Object List screen appears.
3. Enter the Name and Description, then, for Select Object Type, select whether you want to create a list of IFS objects (ISF Path) or native objects (Native Objects).
4. Enter the IFS Path or Native Object Library, Name, and Type (see New Object List screen for more details).
5. If you would like to add an additional IFS Path or Native Object to the list, click **Add IFS Path** or **Add Native Object**, respectively, and enter the object's path or library/name/type. Repeat for additional objects.
6. Choose **Save** to create the Object List. You can now specify this Object List in an Object Rule.

To rename an object List

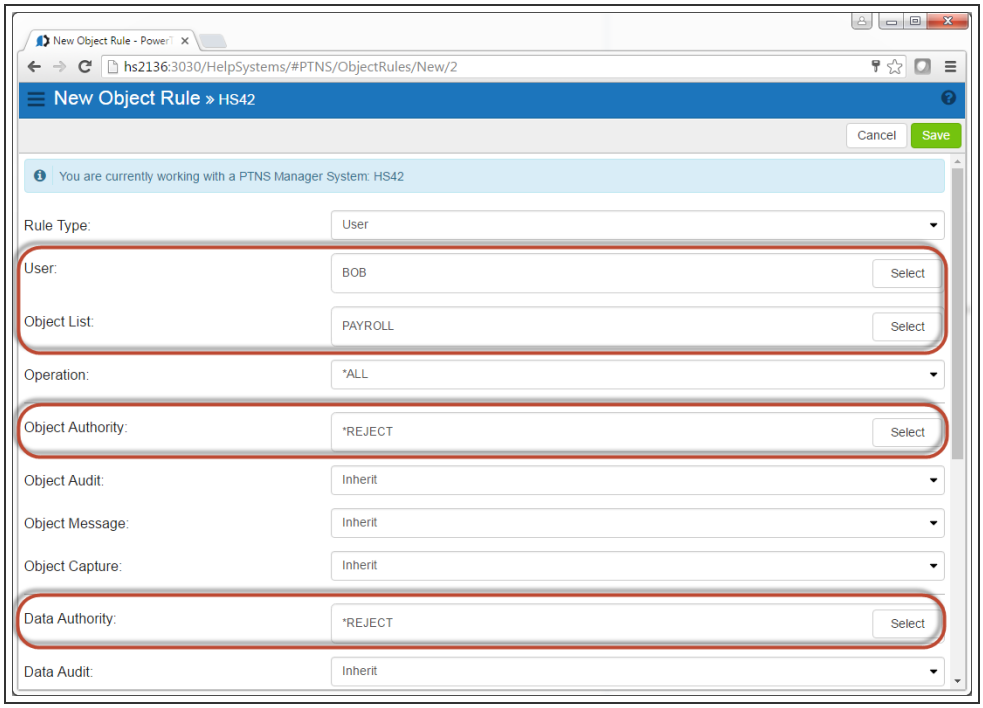
1. On the Object Lists screen, select an Object List.
2. Change the Name and Description as desired and clicktap**Save**.

Creating Rules for Object Lists

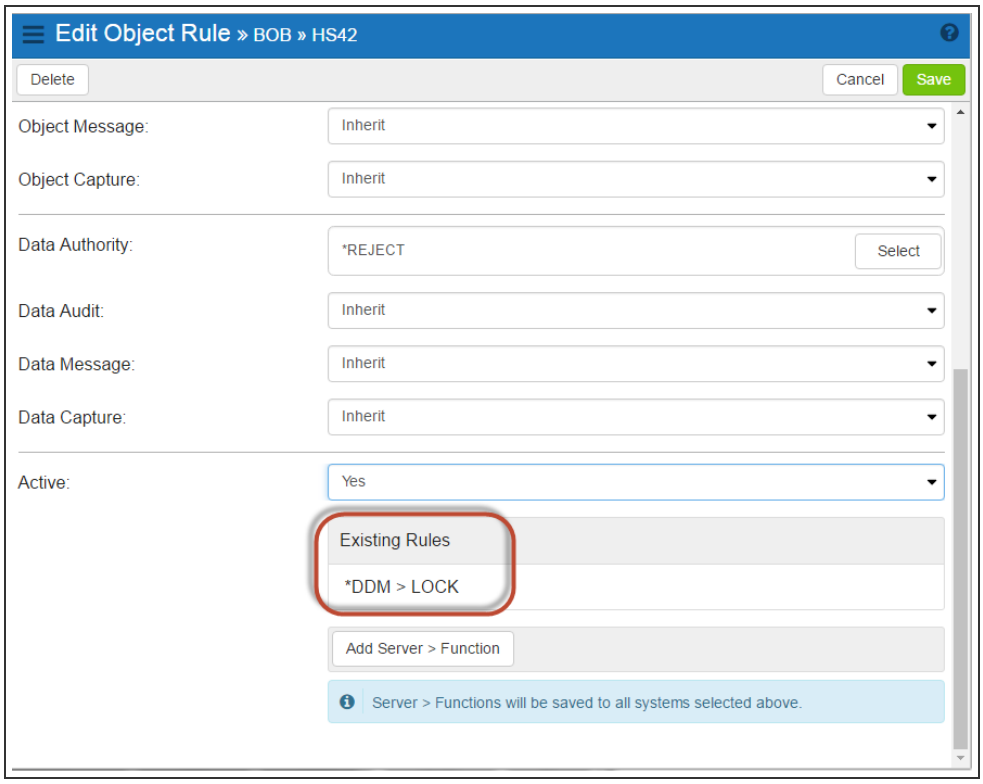
You can create rules to control access to the objects listed in an object list from the Object Rules screen. Creating a rule adds filter rules for the user or location specified for the rule.

To create rules for an object list

1. From the Navigation Pane, click **Object Rules**.
2. Choose **Add**. The New Object Rule screen appears.
3. Specify the User/Location, Object List, Operation, and Data/Object authority. See New Object Rule screen for details.



   In this example of a User Object Rule, Bob is restricted from performing all operations on objects in the PAYROLL object list.
4. For Active, choose **Yes** to activate the Object Rule.
5. Next, specify which systems should enforce this rule. After "Select which systems to save to", check the desired systems. Or, choose **Select All** to enforce the Object Rule on all managed systems.
6. Click **Add Server > Function** if you would like the Object Rule to apply to specific functions. Choose the server and function, then repeat for any additional server functions.
7. Choose **Save** to create the object rule. *MEMOBJ rules are generated based on your selections. Existing *MEMOBJ are listed at the bottom of the Edit Object Rules screen.



On the Rules Screen, object rules are indicated with the authority *MEMOBJ.

Example: Blocking access to a library while allowing a specific user to access a specific file within that library

In this example, we will block access to all files in the library PAYROLL but still allow user SHAASE to access the EMPLOYEE file within that library.

To block access using this method, you must change the *PUBLIC rule for *SQLSRV to *MEMOBJ. This instructs Exit Point Manager to consult Object Lists to determine access control. Additional Object Lists will need to be created to authorize access to other objects and libraries using *SQLSVR.

To change the *PUBLIC rule for *SQLSRV to *MEMOBJ:

1. Select **Rules** on the Navigation Pane.
2. Click  and select the following filter options:
   - Sort By: **User/Location**
   - Filter By: **User Rules**
3. Click  to dismiss the sort/search/filter options.
4. In the search box, type "*SQLSRV" and open the existing *SQLSRV > *ALL *PUBLIC rule.
5. Click **Lookup** for Authority and choose *MEMOBJ.
6. Select **Save**.

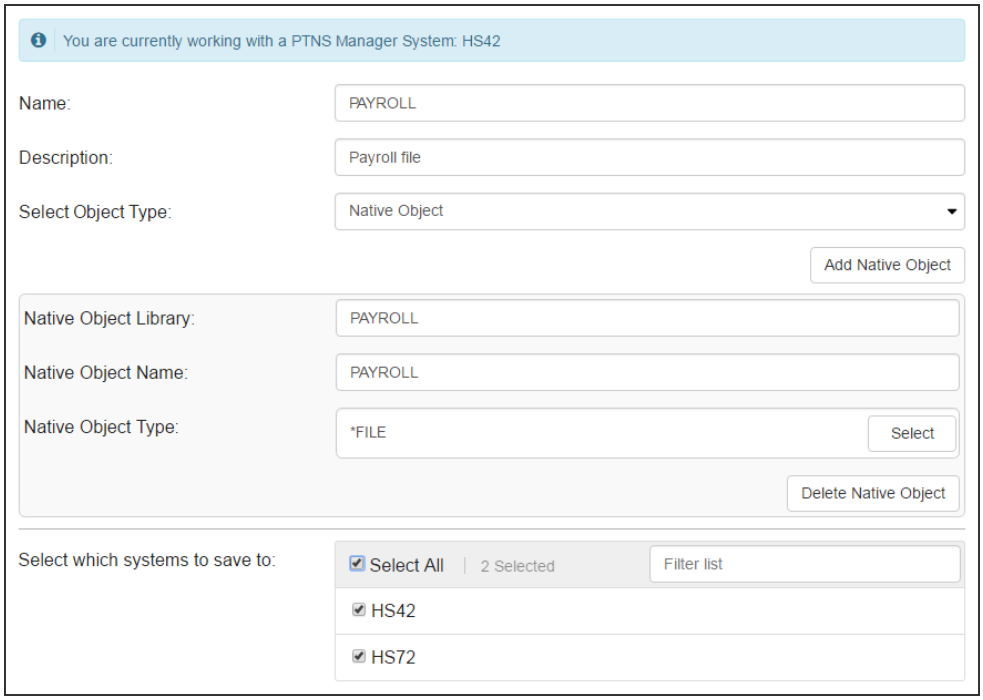
Create an Object List to block access to all files in the library.

1. Select **Object Lists** on the Navigation Pane.

2. Choose **Add**.
3. Create the Object List PAYROLL that includes the object PAYROLL using the following values:

   - Name = PAYROLL
   - Description = [*Enter description here*]
   - Select Object Type = Native Object

     Objects
   - Native Object Library = PAYROLL
   - Native Object Name = PAYROLL
   - Native Object Type = *FILE



4. Choose the systems this Object List should be added to.
5. Click **Save** to return to the Object List page.

Create another Object List to allow user access to the file EMPLOYEE.

1. Choose **Add**.
2. Create the Object List EMPLOYEE that includes the object EMPLOYEE using the following values:

   - Name = EMPLOYEE
   - Description = [*Enter description here*]
   - Select Object Type = Native Object

     Objects
   - Native Object Library = PAYROLL
   - Native Object Name = EMPLOYEE
   - Native Object Type = *FILE

3. Click **Save** to return to the Object List page.

Give user SHAASE access to the EMPLOYEE Object List.

1. Select **Object Rules** on the Navigation Pane.
2. Choose **Add**.
3. Create a new User Object Rule using the following values:
   - Rule Type: User
   - User = SHAASE
   - Object List = EMPLOYEE
   - Operation = *ALL
   - Object Authority = *OS400
   - Data Authority = *OS400

   NOTE: Make sure Active is set to **Yes** checked before saving.
4. Specify which systems you would like this rule enforced.
5. Choose **Add Server > Function** and select ***SQLSRV**, then ***ALL**.
6. Click **Save** to return to the Object Rules page.

Block user *PUBLIC access to the PAYROLL Object List.

1. Click **Add > New User Object Rule**.
2. Create a new User Object Rule using the following values:
   - User = *PUBLIC
   - Object List Name = PAYROLL
   - Operation = *ALL
   - Object Authority = *OS400
   - Data Authority = *REJECT

   NOTE: Make sure **Active** is checked before saving.
3. Choose **Continue**.
4. Select ***SQLSRV**, then ***ALL**.

5. Click **Save** to return to the Object Rules page.

Now, only the user SHAASE will have access to the EMPLOYEE file in the library PAYROLL. Access to all other files in PAYROLL will be blocked.

IP Address Groups

IP address groups allow you to set rules when a number of locations need the same location filter rules applied to them. Use the IP Address Groups screen to create, change, and delete groups, as well as define IP address groupings.

Exit Point Manager IP address groupings allow you to associate IP addresses with an IP address group name. Once you've associated a set of IP addresses with a group name, you can specify the group name as a location when entering location rules. Exit programs check to see if an IP address is part of a group. If the address is part of a group and no specific rule for it exists, the group name is used to determine if a specific rule exists.

Entering IP address groups

1. In the Navigation Pane, choose **IP Address Groups**.
2. Choose **Add** to open the New IP Address screen.
3. Enter the desired name for the new group, then add a description in the Description field.
4. Under IP Address Range, specify the IP Address or IP address range.
   Examples:
   Single: 192.168.0.1
   Range 192.168.0.1-192.168.0.255 or 192.168.0.1:192.168.0.255
5. Select which systems you would like to save the IP address group to and click **Save** to create the new group.

Switch Profiles

Exit Point Manager's *Switch Profiles* function allows you to customize Exit Point Manager authorizations for network access requests.

For example, you might use switch profiles in the following situation:

User POWERUSER initiates an incoming FTP request. The POWERUSER profile normally has IBM i authority to change or delete almost any file on the system, and to run most commands using the FTP RMTCMD facility. Because you want to limit the ability of POWERUSER to run FTP requests, you tell Exit Point Manager to switch to another user ID, called READONLY, whenever POWERUSER runs FTP. The READONLY user ID has *USE authority to IBM i files, allowing read-only access to the files, preventing POWERUSER from making any file modifications.

Specifying a Switch Profile

1. Switch profiles are specified when adding or editing rules. From the Rules screen, choose **Add** or click an existing rule.
2. Choose the **Lookup** button next to the Authority field.
3. Select ***SWITCH**, the select the user profile you would like to switch to.
4. Configure the server, function, location/user, and flags as you would normally and click **Save**.

If you want to switch to a different user profile only for a particular server function, such as SENDFILE (PUT), you can specify the switch profile for just that function.

Setting a Switch Profile for a Function

1. Switch profiles are specified when adding or editing rules. From the Rules screen, choose **Add**, or click an exisitng user rule.

2. Choose the **Lookup** button next to the Server > Function field and choose ***FTPSERVER > SENDFILE**.
3. For Authority, select ***SWITCH**, and then the select the user profile you would like to switch to (in this case, READONLY).
4. Choose **Save**.

Note: When you specify a switch profile, all subsequent actions performed in that FTP session are performed using the switch profile until the user performs another FTP function. Then, Exit Point Manager switches back and performs the next function as the original user.

For example:

- User Bill makes a request to PUT (perform a SENDFILE) a file to the IBM i. Since a rule exists to switch profiles whenever a SENDFILE function is performed, the FTP PUT is switched to run under the user profile POWERUSER.
- All subsequent commands run during Bill's FTP session run under the profile POWERUSER, not Bill.
- As soon Bill performs another FTP function (such as CHGCURLIB or GET), Exit Point Manager changes the job to run as Bill.

More on Access Control Rules - green screen

The power of Exit Point Manager resides in its ability to control network access to IBM i network servers and server functions according to the rules you specify.

> NOTE: All functions related to adding, editing, and deleting rules are available using either the web browser interface or the green screen, although the procedures for accomplishing these tasks differ considerably. While the green screen interface offers many different screens that display the existing user rules in different formats, the browser interface offers a single screen (the Rules screen), with robust search and filtering capabilities that allow *all* rules (user and location) to be accessed immediately. See Using the Web Browser Interface for details.

As discussed in Getting Started with Exit Point Manager, you can set rules for a User (user profile), Group profile, or Supplemental Group profile. For example, you can create a rule by user ID that directs the FTP server to reject any upload attempt from users who are members of a particular group profile. For more information on user rules, see User Rules.

Another method of defining an access rule is by *location*. A location is Exit Point Manager's definition of the origin of an access request. A location can be a specific IP, group IP, generic IP, range of IP addresses, or SNA device. (For example, a group of IP addresses may correspond to a corporate office's physical location, e.g. *DENVER). Location security rules allow you to grant access to, and define the authorities for, all approved dial-in and Internet origins, while restricting access to unapproved origins according to the rules you define. For example, you can create a location rule to direct the IBM i FTP server to reject any FTP request coming from outside your local network. See Location Rules.

Exit Point Manager also lets you set object rules that are configured at the object level, for a specific user or location, for a specific object, and for a specific type of access. Creating an object rule allows you to, for example, specify who can access your IBM i payroll database. See Object Rules.

Authorities

Access Control Rules establish the action to be taken when a particular server or server function is accessed. You can specify the following actions:

> **NOTE:** Many of the examples shown throughout this section use *FTPSERVER. The process of setting up other servers is similar, although you will see different functions. In addition, some types of rules may not apply to all servers.

- ***OS400** - Allow the request using the user's normal IBM i authorities as if Exit Point Manager were not installed.
- ***REJECT** - Reject the request.
- ***SWITCH** - Allow the request after switching the request to run under the authority of a different user profile—the switch profile. See Switch Profiles).
- ***MEMOS400/*MEMREJECT/*MEMSWITCH** - Use the rules specified in a previously memorized transaction. (See Memorizing Transactions).
- ***MEMOBJ** - Check Object List. (Refer to rules defined for specific objects. See Object Rules.)

Flags

Access Control Rules also include *flags*. The three flags are Aud (Audit), Msg (Message), and Cap (Capture).

> **NOTE:** If Authority is *USER, Audit, Message, Capture and Switch Profile are deferred. If Authority is not *USER, Audit, Message, Capture and Switch are enforced.

- **Audit**
  - Yes= Record this request to the Audit Journal
  - No= Do not record the request (unless request fails)
- **Message**
  - Yes= Send a message when the request is received
  - No= Do not send a message
- **Capture**
  - Yes= Capture transactions for this request
  - No= Do not capture transactions

* = Inherited from a higher level (such as Change Server Function Rule). When using the browser interface, the "Inherit" check box indicates the value is inherited from a higher level, and the origin of the inherited value is indicated adjacent to the check box. See Active Rule and Rule Derivation.

Switch Profiles

The switch profile action is the key to providing flexible security for your network users. This action lets you specify an alternate user profile, called a *switch profile*, that network access requests run under. This allows you to use standard IBM i security commands to establish the authorities to objects on your system for a user when they access the system through the network servers.

To define a Switch Profile as part of a rule:

- Set the Authority to *SWITCH.
- Specify the target user.

A typical requirement for *SWITCH profile:

- User belongs to a group profile that owns objects.
- Network access gives the user *ALL authority to the entire application.
- Use Exit Point Manager to allow selective access.
- Dynamically change user authority “on the fly”.
    - Give more or less authority than normal.
- *SWITCH profile does not affect green screen operations.
    - Can configure authority independently.

For details, see Switch Profiles.

Exit Point Manager always searches for location access rules first

User access rules are considered only if a location access rule is found with an action that indicates that user access rules should be used.

Active Rule and Rule Derivation

When working with User and Location rules, you can use **5**, Display, to see the Rule Derivation panel, which provide Active Rule and Rule Derivation information. A value of ‘*’ indicates that Exit Point Manager is inheriting the actual value from another location (much like *SYSVAL in the OS).

> **NOTE:** When using the web user interface, the source of the inherited value is listed next to the respective check box when adding or editing rules.

Identifying Rule Derivation on the Green Screen

Exit Point Manager has a hierarchy of rules that, when displayed, shows what the current active rule is. For most rules, you can set the values that determine what the rule does to * (or *DEFAULT).

The Rule Derivation screen lets you see the following: 1) For a given rule, which values are set to the default and 2) from which setting did that value come.

For example, suppose there is a rule for user MARKJ and the audit and capture values are all set to *. If that rule is invoked, those asterisks each resolve to either Y or N based on the hierarchy. If all properties are set as shown in the following table, then the Active Rule for user MARKJ is Audit = Y, Message = N, and Capture = Y.

F	Audit	Msg	Cap
Work with System Values	y	y	N
Change Server Function Rule	*	N	*
MARKJ (rule)	*	*	Y
Then, the Active Rule is	**Y**	**N**	**Y**

The following screen shows the rule derivation. The asterisks in the Audit and Msg fields in the Rule Derivation section for MARKJ take the values from the levels above. The Active Rule is the rule that results from the Rule Derivation values.

```
PNS4215                    Powertech Exit Point Manager                  14:33:12
                              User Rule Derivation                       OSCAR
System: OSCAR     Management System
Server . . . . : *FTPSERVER  iSeries FTP Server
Function . . . : DELETEFILE  Delete file(s) (DELE)

                                  Active Rule

Type Level      Authority  Audit Msg Cap Switch     Supplemental Exit
 U   MARKJ      *OS400       Y    N   Y  *NONE      *NONE

                              User Rule Derivation

Type Level      Authority  Audit Msg Cap Switch     Supplemental Exit
 _   System     *OS400       Y    N   N  *NONE
     Server     *SYSTEM      *    N   *  *NONE      *NONE
     Function   *SERVER      *    N   *  *NONE
 U   MARKJ      *OS400       *    *   Y  *NONE



F3=Exit     F12=Cancel
```

User Rule Detail showing Active Rule and Rule Derivation

- System level details can be changed in the Work with System Values panel.
- Server and server function level details can be changed in the Change Server Function Rule panel.
- User level details can be changed in the Work with Security by User panel.

Location Rules

The green screen is the traditional Exit Point Manager interface. All functions related to adding, editing, and deleting rules are available using either the web browser interface or the green screen, although the procedures for accomplishing these tasks differ considerably.

You can use the Work with Security by Location panel to maintain a location's server and server function filter rules. After entering a valid location, you can add, change, or delete the location's individual server and server function filter rules. You also can copy a location's filter rules to another location, or delete all the location's filter rules. To change a rule, simply type over the existing values, and press `Enter`.

Adding location rules

1. Select option **3** on the Exit Point Manager Main Menu to open the Work with Security by Location panel. (Or, from the Main Menu, select option **1** to display the Work with Security by

Server panel and Enter option **LA** (Edit Location Authority) in the Opt column next to a server you would like to display.)

```
PNS4110                  Powertech Exit Point Manager                  14:15:09
                         Work with Security by Server                  OSCAR
System  . . . . . : OSCAR
Position to Server: __________
Type options, press Enter
  FN=Work with Functions      SP=Server Properties    CT=Captured trans
  LA=Edit Location Authority  UA=Edit User Authority  MT=Memorized trans
                                                    Rules      Exit Point
Opt  Server      Description                       Enforced    Activated
 __  *CLI        CLI Connection Server               Y            N
 __  *CNTRLSRV   License Management Central Server   Y            N
 __  *DATAQSRV   Optimized Data Queue Server         Y            N
 __  *DDM        DDM Server                          Y            N
 __  *DQSRV      Data Queue Server                   Y            N
 __  *DRDA       Distributed Relational Database     Y            N
 __  *FILESRV    File Server                         Y            N
 __  *FTPCLIENT  iSeries FTP Client                  Y            Y
 __  *FTPREXEC   FTP Execute Remote Command (REXEC)  Y            Y
 LA  *FTPSERVER  iSeries FTP Server                  Y            Y
 __  *FTPSIGNON  FTP Signon Server                   Y            N
 __  *LMSRV      License Management Server           Y            N
                                                                  More...
F3=Exit   F5=Refresh   F7=Select System   F12=Cancel   F24=More keys
```

2. The Work with Security by Location panel displays. Initially, this screen lists the default rules. You can add and maintain additional server function filter rules for locations using this panel.

```
PNS4310                  Powertech Exit Point Manager                  13:00:24
                         Work with Security by Location                OSCAR
System  . . . . . : OSCAR    Management System
Position to Location: __________
Type options, press Enter
  2=Change  3=Copy  4=Delete  5=Display
                                          Filter Rule Properties
Opt Location        Server     Function   Authority  Aud Msg Cap  Switch Prf
 _  *ALL            *CLI       *ALL       *USER       *   *   *   *NONE
 _  *ALL            *CNTRLSRV  *ALL       *USER       *   *   *   *NONE
 _  *ALL            *DATAQSRV  *ALL       *USER       *   *   *   *NONE
 _  *ALL            *DDM       *ALL       *USER       *   *   *   *NONE
 _  *ALL            *DQSRV     *ALL       *USER       *   *   *   *NONE
 _  *ALL            *DRDA      *ALL       *USER       *   *   *   *NONE
 _  *ALL            *FILESRV   *ALL       *USER       *   *   *   *NONE
 _  *ALL            *FTPCLIENT *ALL       *USER       *   *   *   *NONE
 _  *ALL            *FTPREXEC  *ALL       *USER       *   *   *   *NONE
 _  *ALL            *FTPSERVER *ALL       *USER       *   *   *   *NONE
 _  *ALL            *FTPSIGNON *ALL       *USER       *   *   *   *NONE
 _  *ALL            *LMSRV     *ALL       *USER       *   *   *   *NONE
                                                                  More...
F3=Exit            F5=Refresh          F6=Create rule     F7=Select System
F8=Captured trans  F9=Memorized trans  F12=Cancel         F24=More keys
```

3. To add a new rule, press `F6`. The Create Location Rule panel appears. (To change the filter rule properties of an existing rule, simply choose **2** for the existing rule.)
4. Enter the function, location, and filter rule properties. To see a list of available functions, authorities, or switch profiles for the selected server, you can press `F4` (Prompt) to display a prompt screen.

   For example, press `F4` in the Function field to display the Prompt Server Functions panel. Enter a **1** next to the function for which you want to define a rule.

   - To apply the rule to all locations, enter ***ALL** in the Location field. To restrict the rule to one IP address, enter the IP address (for example, 10.123.144.213). To restrict the rule to a range of IP addresses, you can enter a generic IP address (for example, 10.123.*).
   - To select from a list of valid authorities, press `F4` to display the Valid Authorities panel. If you set the Authority to *REJECT, Exit Point Manager rejects the specified transaction. Whenever Exit Point Manager rejects a request for any reason, the transaction is recorded in the audit journal and the Aud column is not considered. The rejected request is audited regardless of the value in the Aud column.

5. Specify if you want Exit Point Manager to send a message (Msg = Y) and capture transactions for memorization (Cap = N). If you do not specify a Switch Profile, it defaults to *NONE. Press `Enter` to add the rule.

Copying rules from one location to another

1. Enter **3** for the location rule you would like to copy. The Copy Location Rule panel appears.
2. Specify the new location and press `Enter`.

```
PNS4311                  Powertech Exit Point Manager                  09:23:58
                              Copy Location Rule                       OSCAR
System: OSCAR     Management System



Location  . . . : 192.168.001.001
Server  . . . . : *FTPSERVER
Function  . . . : *ALL
Authority . . . : *OS400
Switch Profile  : *NONE
Audit . . . . . : *
Message . . . . : *
Capture . . . . : *




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

NOTE:

- When you copy a location's rules, it does not copy all sublocation rules; only the rules for the selected location, for example, 192.*, are copied.
- All existing authorities for the location you are copying to are deleted.

Displaying Properties Detail

On the Work with Security by Location panel, choose **5** for a location rule to display the Location Rule Derivation panel. This panel provides location rule detail information, including parameter settings and Active Rule and Rule Derivation information.

```
PNS4315                  Powertech Exit Point Manager                  10:05:42
                           Location Rule Derivation                    OSCAR
System: OSCAR     Management System
Server . . . . : DATADIST    Showcase Warehouse Builder Server
Function . . . : *ALL

                                 Active Rule

Level           Authority  Audit Msg Cap Switch    Supplemental Exit
*ALL            *USER        Y    N   N  *NONE      *NONE

                            Location Rule Derivation

Level           Authority  Audit Msg Cap Switch    Supplemental Exit
System          *OS400       Y    N   N  *NONE
Server          *SYSTEM      *    *   *  *NONE      *NONE
*ALL            *USER        *    *   *  *NONE




F3=Exit     F12=Cancel
```

Deleting an Authority Rule for a Location

On the Work with Security by Location panel, choose **4** for a location rule to delete it.

NOTE: Rules can also be deleted using Insite. See Deleting under "Using the Web Browser Interface."

Working with global location rules

You also have the option to set rules across multiple servers at one time from the Work with Security by Location panel.

1. On the Work with Security by Location panel, press `F2` to display the Add Location Rules panel.
2. Specify the desired Location, Authority, Switch Profile, and Audit/Message/Capture flags for the rule.
3. For Replace, choose **Y** to set the new rule across only those servers where a rule already exists for the specified location. This option updates existing rules with the specified rule filters and changes all existing rules for the location to those you entered.
4. Press Enter to set a new rule across all Exit Point Manager servers, including servers that don't already have a rule for the specified location. This option adds *ALL functions for any missing servers and updates any existing rules.

NOTE: If an Authority setting is set to *SAME, Exit Point Manager does not change the existing settings and does not create new rules when you select Add and Change records (All Servers).

Viewing Default Location Rules

Exit Point Manager ships with 30 default location authority rules. You can view these rules from the Work with Security by Location panel. To display the Work with Security by User panel, select option **2** from the Main Menu.

Use **F16** to Sort and Subset by Server, Function, or Location.

```
PNS4310                  Powertech Exit Point Manager                  13:00:24
                        Work with Security by Location                 OSCAR
System  . . . . . : OSCAR    Management System
Position to Location: _________
Type options, press Enter
  2=Change  3=Copy  4=Delete  5=Display
                                          Filter Rule Properties
Opt Location        Server     Function   Authority  Aud Msg Cap  Switch Prf
 _  *ALL            *CLI       *ALL       *USER       *   *   *   *NONE
 _  *ALL            *CNTRLSRV  *ALL       *USER       *   *   *   *NONE
 _  *ALL            *DATAQSRV  *ALL       *USER       *   *   *   *NONE
 _  *ALL            *DDM       *ALL       *USER       *   *   *   *NONE
 _  *ALL            *DQSRV     *ALL       *USER       *   *   *   *NONE
 _  *ALL            *DRDA      *ALL       *USER       *   *   *   *NONE
 _  *ALL            *FILESRV   *ALL       *USER       *   *   *   *NONE
 _  *ALL            *FTPCLIENT *ALL       *USER       *   *   *   *NONE
 _  *ALL            *FTPREXEC  *ALL       *USER       *   *   *   *NONE
 _  *ALL            *FTPSERVER *ALL       *USER       *   *   *   *NONE
 _  *ALL            *FTPSIGNON *ALL       *USER       *   *   *   *NONE
 _  *ALL            *LMSRV     *ALL       *USER       *   *   *   *NONE
                                                                    More...
F3=Exit            F5=Refresh          F6=Create rule    F7=Select System
F8=Captured trans  F9=Memorized trans  F12=Cancel        F24=More keys
```

User Rules

User authority rules are useful to control access to servers and functions for particular *users* or groups of users (*User Groups*). User security rules are evaluated only if a location rule specifies to use *USER security rules. (Exit Point Manager includes one default user rule for each server; see Default User

Rules). Like Location rules, User rules can be used to define actions for access to a server, or for access to a specific function of a server (e.g. DELETEFILE).

> **NOTE:** In order to add User Rules on an endpoint, the PNSEVTMON monitor job must be running. This job starts automatically during Exit Point Manager installation. If, for some reason, this job has been stopped, you can issue the PTNSLIB07/PNSSTRMON (or PTNSLIB/PNSSTRMON, depending on your product library) command to restart it.

All default location rules include the same parameters and are set with the same default values. See Parameters and Default Values.

Adding user rules

The Work with Security by User panel lets you select the servers to which you want to add or maintain user authority rules.

1. From the Main Menu, select option **2** to display the Work with Security by User panel.

```
PNS4215                  Powertech Exit Point Manager                 14:33:12
                             User Rule Derivation                     OSCAR
System: OSCAR     Management System
Server . . . . : *FTPSERVER  iSeries FTP Server
Function . . . : DELETEFILE  Delete file(s) (DELE)

                                  Active Rule

Type Level      Authority  Audit Msg Cap Switch     Supplemental Exit
 U   MARKJ      *OS400       Y    N   Y  *NONE      *NONE

                              User Rule Derivation

Type Level      Authority  Audit Msg Cap Switch     Supplemental Exit
 _   System     *OS400       Y    N   N  *NONE
     Server     *SYSTEM      *    N   *  *NONE      *NONE
     Function   *SERVER      *    N   *  *NONE
 U   MARKJ      *OS400       *    *   Y  *NONE



F3=Exit     F12=Cancel
```

2. Press `F6` to create a new rule. The Create User Rule panel appears.
3. Enter the following details:
    a. **User Rule Type: U** for user or **G** for User Group.
    b. **User:** The user profile or User Group (press `F4` to prompt).
    c. **Server:** The IBM i server (press `F4` to prompt).
    d. **Function:** The IBM i server function (press `F4` to prompt).
    e. **Authority:** The authority assigned to the user for this server/function (press `F4` to prompt).
    f. **Switch Profile:** The name of a user profile whose authority is used to process the transaction instead of the authority of the User initiating the transaction (press `F4` to prompt).
    g. **Audit • Message • Capture:** Whether or not to audit, message, or capture these transactions. See Create User Rule panel for details.
4. Press `Enter` to create the User Rule.

Creating User Groups

1. On the Exit Point Manager Main Menu, choose **7**, Work with User Groups.
2. Press **F6** to create a new User Group.

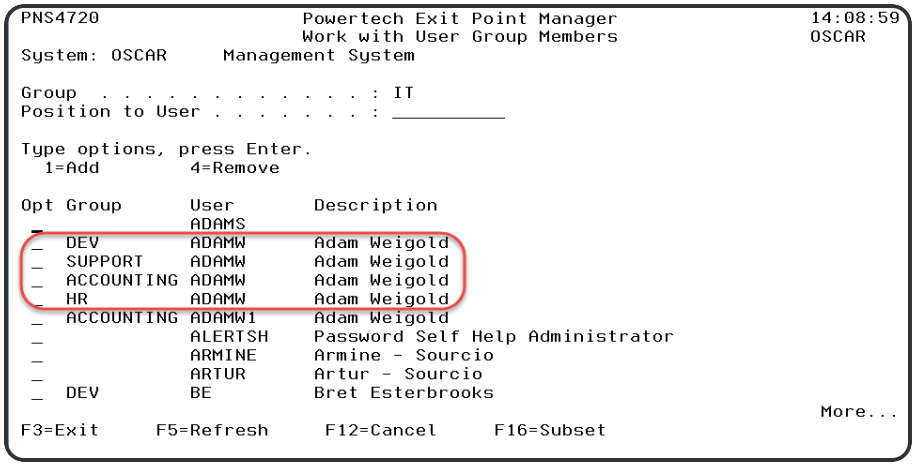
3. Specify the Sequence Number, User Group (name), and Description. The **Sequence Number** indicates the order in which this User Group will be evaluated by the exit point programs. For more details, see Work With User Groups.
4. Press `Enter` to create the User Group. You return to the Work with User Groups panel.
5. Choose **8**, Work with Members, for the User Group you just created. The Work with User Group Members panel appears.

> **NOTE:** Adding OS User Groups to a Exit Point Manager Group is not recommended.

6. Enter **1** for the profiles you would like to add as members to the User Group and press `Enter`. The User Group name appears under the Group column for the profile and a message indicates the profiles that have been added. Repeat for any additional profiles. Or, use **4** to remove members from a User Group.
7. Press `F3` to return to the Work with User Groups panel. Now, when you create or edit a user rule, choose User Rule Type **G** to select the User Group (instead of a profile).

Adding Members to a User Group

1. On the Exit Point Manager Main Menu, choose **7**, Work with User Groups.
2. Choose **8** for a User Group. The Work with User Group Members panel appears. Here, an entry appears for every user and group combination. For example, if ADAMW is in multiple User Groups, user ADAMW will be listed multiple times - once for each User Group in which he is a member.



3. Choose **1** for the user(s) you want to add to the currently selected User Group. (If multiple entries exist for a user, choose any one.)

```
PNS4720                  Powertech Exit Point Manager                  14:08:59
                         Work with User Group Members                  OSCAR
System: OSCAR     Management System

Group  . . . . . . . . . . . . : IT
Position to User . . . . . . . : __________

Type options, press Enter.
  1=Add        4=Remove

Opt Group      User       Description
 _             ADAMS
 1  DEV        ADAMW      Adam Weigold
 _  SUPPORT    ADAMW      Adam Weigold
 _  ACCOUNTING ADAMW      Adam Weigold
 _  HR         ADAMW      Adam Weigold
 _  ACCOUNTING ADAMW1     Adam Weigold
 _             ALERTSH    Password Self Help Administrator
 _             ARMINE     Armine - Sourcio
 _             ARTUR      Artur - Sourcio
 _  DEV        BE         Bret Esterbrooks
                                                                    More...
F3=Exit     F5=Refresh     F12=Cancel     F16=Subset
```

> **NOTE:** Adding OS User Groups to a Exit Point Manager Group is not recommended.

4. Press `Enter` to add the chosen user(s) to the User Group. In the above example, profile ADAMW will be added to the IT User Group.

Removing Members from a User Group

1. On the Exit Point Manager Main Menu, choose **7**, Work with User Groups.
2. Choose **8** for a User Group. The Work with User Group Members panel appears. Here, an entry appears for every user and group combination. For example, if ADAMW is in multiple User Groups, user ADAMW will be listed multiple times - once for each User Group in which he is a member.
3. Choose **4** for the user entries that should be removed from their corresponding group.

```
PNS4720                  Powertech Exit Point Manager                  14:08:59
                         Work with User Group Members                  OSCAR
System: OSCAR     Management System

Group  . . . . . . . . . . . . : IT
Position to User . . . . . . . : __________

Type options, press Enter.
  1=Add        4=Remove

Opt Group      User       Description
 _             ADAMS
 4  DEV        ADAMW      Adam Weigold
 _  SUPPORT    ADAMW      Adam Weigold
 4  ACCOUNTING ADAMW      Adam Weigold
 _  HR         ADAMW      Adam Weigold
 _  ACCOUNTING ADAMW1     Adam Weigold
 _             ALERTSH    Password Self Help Administrator
 _             ARMINE     Armine - Sourcio
 _             ARTUR      Artur - Sourcio
 _  DEV        BE         Bret Esterbrooks
                                                                    More...
F3=Exit     F5=Refresh     F12=Cancel     F16=Subset
```

4. Press `Enter` to remove the user(s) from the corresponding group(s). In the above example, profile ADAMW will be removed from the DEV and ACCOUNTING User Groups.

Changing the User Group Sequence

1. On the Exit Point Manager Main Menu, choose **7**, Work with User Groups.
2. Press **F10** to open the Work with User Group Sequence panel.

```
PNS4712                  Powertech Exit Point Manager                  08:08:23
                        Work with User Group Sequence                  OSCAR
System: OSCAR     Management System


Type Sequence numbers, press Enter

  Seq     Name           Seq     Name           Seq     Name
  _ 1     HR
    1     MARKETING
    1     ACCOUNTING
    1     IT
    1     DEV

                                                                      Bottom
F3=Exit   F5=Refresh   F7=Select System   F10=View 3   F12=Cancel
```

3. Use the entry fields to order the User Groups in the sequence in which Exit Point Manager will evaluate the User Groups. For example, if there are three User Rules with User Groups for a specific Server/Function, and all three have ADAMW as a member, the User Rule for the User Group with the lowest sequence number will be used by the exit programs first.

```
PNS4712                                                               13:12:53
                        Work with User Group Sequence                  OSCAR
System: OSCAR     Management System


Type Sequence numbers, press Enter

  Seq     Name           Seq     Name           Seq     Name
   50     HR
   40     MARKETING
   10     ACCOUNTING
   20     IT
   30     DEV

                                                                      Bottom
F3=Exit   F5=Refresh   F7=Select System   F10=View 3   F12=Cancel
```

4. Press `Enter`. The above configuration will change the order to Accounting, IT, Dev, HR, Marketing.

Restricting access to a server function for all users but one

This example shows how you might use server user rules to allow the POWERUSER user profile to download files from IBM i using FTP, while preventing other users from performing that function.

This requires the addition of two rules. The first rule rejects attempts to download a file by all users, while the second rule specifically allows the user POWERUSER to download a file. Since the rule to allow POWERUSER to download a file is more specific than the rule to prevent downloading, it takes precedence.

1. First, create a new user rule that sets the SENDFILE function of the FTP server to reject for all users (*PUBLIC).

2. Enter the following values in the Create User Rule panel.
    - User = ***PUBLIC**. The rule will be in effect for all users.
    - Function = **SENDFILE**. This is the function used by the FTP server to download files from IBM i.
    - Authority = ***REJECT**. Exit Point Manager will reject any FTP SENDFILE transactions.
3. Now, create another rule to allow POWERUSER to use the SENDFILE function.
    - User = **POWERUSER**. The rule will be in effect for all users.
    - Function = **SENDFILE**. This is the function used by the FTP server to download files from IBM i.
    - Authority = ***OS400**. Exit Point Manager will reject any FTP SENDFILE transactions.

Since this second rule is more specific than the other rules in effect, it is evaluated first, allowing POWERUSER to download files, but restricting all other users from the SENDFILE function.

To copy rules from one user to another

1. In the Work with Security by User panel, choose **3** for the rule you want to copy. The Copy User Rule panel appears.
2. Make the desired changes and press `Enter` to create the new rule.

Displaying Rule Derivation

Choose **5** (Display) on the Work with Security by User panel to display the User Rule Derivation panel. The User Rule Derivation panel provides user rule detail information, including parameter settings, Active Rule and Rule Derivation information.

Deleting Rules for specific Users

1. If you want to delete all Exit Point Manager authority rules for a specified user, in the Work with Security by User panel, press **F16** to open the User Rules Subset panel.
2. For Select User, enter the user profile associated with the rules you want to delete and press `Enter`.
3. Use **4** for all the rules in the list to delete them.

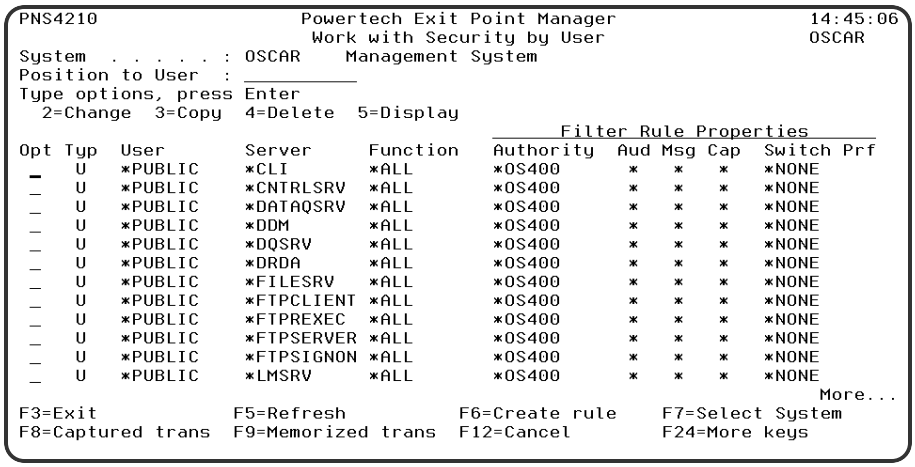
Adding Global User Rules

You also have the option to set rules across multiple servers at one time from the Work with Security by User panel. Press `F2` to display the Add User Rules panel. This panel allows you to create user rules for all Servers.

See Add User Rules panel.

Default User Rules

Exit Point Manager ships with default user authority rules for all supported IBM i servers. View these rules by referring to the *PUBLIC rules on the Work with Security by User panel.



Server IDs

Exit Point Manager supports the following servers and provides one default user rule for each server.

Exit Point Server	Description
*CLI	Call Level Interface
*DDM	*Distributed Data Management Server
*DRDA	Distributed Relational Database
*DQSRV	Data Queue Server
*FILESRV	File Server
*FTPCLIENT	IBM i FTP Client
*FTPSERVER	IBM i FTP Server
*NDB	Native Database Request
*RMTSRV	Remote Command and Distributed Program Call Server
*RTVOBJINF	SQL Retrieve Object Information
*SQL	Database Server Initialization
*SQLSRV	SQL Server
*TELNET	Telnet Device Initiation/Termination
*DATAQSRV	Optimized Data Queue Server
*FTPREXEC	FTP Execute Remote Command (REXEC)
*REXEC_SO	Remote Execute Command Signon Server
*TFRFCL	File Transfer Server
*TFTP	Trivial FTP Server

Exit Point Server	Description
*CNTRLSRV	License Management Central Server
*FTPSIGNON	FTP Logon Server
*LMSRV	License Management Server
*MSGFCL	Message Function Server
*RQSRV	Remote SQL Server
*SIGNON	Signon Server
*VPRT	Virtual Print Server
QNPSERV	Network Print Server

Servers and Functions

ShowCase Exit Points

Exit Point Manager provides access control and monitoring for exit points that are specific to the ShowCase software suite:

Exit Point Server	Description
*VISTA A Showcase corporation server. (*VISTA)	ShowCase *VISTA Clients
*VISTAPRO A Showcase corporation server. (*VISTAPRO)	ShowCase *VISTAPRO Clients
DATADIST A Showcase corporation server. (DATADIST)	ShowCase DATADIST Clients
VISTA_ADMI A Showcase corporation server. (VISTA_ADMI)	ShowCase VISTA_ADMI Clients

Pre-filters

Pre-filters allow you to establish a one-to-one relationship between a specific IP address (location) and a user or user group in order to screen transactions before they are evaluated in full by Exit Point Manager, or restrict access to a server altogether. For example, by configuring a Location + User Pre-filter, you can specify whether to allow or not allow a transaction from a specific IP address and user (or user group) — allowing it causes the transaction to be further evaluated by Exit Point Manager rules; not allowing it is equivalent to a Exit Point Manager reject. A Server Pre-filter can perform the same action for all transactions to, for example, the FTP server. The other actions that you can specify are to audit the transaction, send an immediate message, and capture the transaction.

These actions work exactly like their equivalents within the Exit Point Manager rules processing scheme.

To configure Pre-filters, see Pre-filters panel, User+Location Pre-filter panel, User+Location Pre-filter panel, and User+Location Pre-filter test panel.

Object Rules

IBM defines an object as a named storage space that consists of a set of characteristics that describe it and its data. Thus, an object is anything that occupies space in storage, and on which you can perform operations. Examples of objects include programs, files, libraries, folders, and IFS directories and files. Exit Point Manager allows you to define authority rules to control access at the object level.

You can set rules for libraries and the objects in them, or an IFS path. These rules can be specific to a user (or *PUBLIC) or location and contain the object library, name, and type. Using an object rule, you can define access to both the object and the data contained within the object.

> **NOTE:**
> Path strings must begin with a slash (/) and must not begin with any of "QSYS.LIB", "QFileSvr.400", "QOpenSys", "QOPT" or "QNTC". These values are not case sensitive, thus QOPENSYS and qopensys are similarly invalid. Also, the virtual directory names "." and ".." are not allowed in the path. Additionally, there must be at least one character between each slash in the path.

Object rules allow you to specify the operation that the rule allows (*ALL, *CREATE, *READ, *UPDATE, or *DELETE), and the action to take (*REJECT, *OS400, *SWITCH) for data access and object access. Thus, you can define an object rule for a specific user or location, for a specific object, and for a specific type of access. In addition, you can specify values for auditing, capturing transactions, and messaging in your object rules.

Setting rules at the object level provides a different measure of control than setting rules at the user or location levels. For example, you can set one object rule to restrict all users and locations from accessing a specific file (such as payroll) instead of setting multiple rules at the user or location levels to control access.

Object Rules and Exit Point Manager

There is a close relationship between rules in Exit Point Manager. Object rules need *MEMOBJ filter rules to trigger them. When you define an object rule, you select the servers and functions that will enforce the rule. This creates the *MEMOBJ Authority filter rules for the user or location object rule. The *MEMOBJ Authority filter rule tells Exit Point Manager to check memorized transactions (MTR) for authority. If no MTR authority is found, it then checks the transaction against the object rules.

Whenever any rule changes, Exit Point Manager manages the relationships between the filter rules, object rules, and memorized transactions.

If there are no filter rules with *MEMOBJ authority that refer to a particular active object rule, that object rule is set to *INACTIVE by the system.

NOTE:
When there are no more active object rules for a given user or location, you should remove or modify the filter rules for that user or location. When you select to deactivate (for example, by changing or deleting) the last active object rule for a user or location, Exit Point Manager asks you to select how to handle the filter rules that are in place. If you use a command (such as CHGOBJRUL or DLTOBJRUL), you must specify command parameters that define how to handle the filter rules in case they are needed at run time during command processing.

Object Rules and the Remote Command Server

The Remote Command server has some unusual properties. The server only recognizes and reports on object type *CMD, and does not supply any other object type to the server. This means Network Security cannot identify any other object type to apply to the object rule. Remote Command server Object Rules will not work unless they are for the command itself.

Example:

The following remote command issued from a DOS prompt:

```
RMTCMD CRTLIB TESTLIB //mysystem
```

will work if the object rule is for CRTLIB (type *CMD). It will not work for TESTLIB (type *LIB).

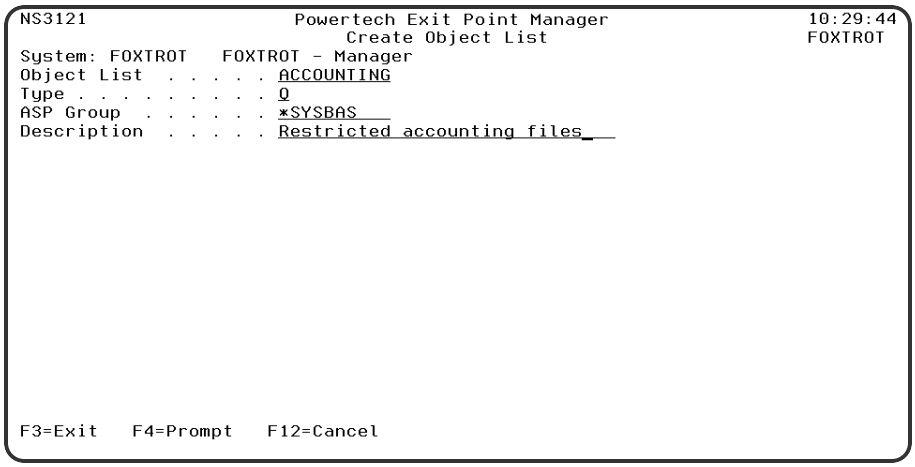
Managing Object Lists

To create an object list

1. From the Exit Point Manager Main Menu, select option **4** to display the Work with Security by Object screen.
2. To work with the object lists you want to secure, select option **1** to display the Work with Object Lists screen. It displays all object lists that have been defined.

```
NS3120                  Powertech Exit Point Manager                 10:25:59
                          Work with Object Lists                     FOXTROT
System: FOXTROT   FOXTROT - Manager
Position to Object List: __________

Type options, press Enter.
  1=Create   2=Change   3=Copy   4=Delete   7=Rename
  8=Work with Entries   9=Object Rules using Object List

Opt  Object List  Type   ASP Group   Description
 _   __________    _     __________  ______________________________
 _   ASID          Q     *SYSBAS     SID / bigkeypf & filetest
 _   NEWIASP       Q     IASP01      New IASP List
 _   SIDLIST       Q     IASP01      sid1 bigkeypf & filetestxx

                                                                  Bottom
F3=Exit   F4=Prompt   F5=Refresh   F7=Select System   F12=Cancel
F16=Sort/Subset       F17=Print     F19=Top            F20=Bottom
```

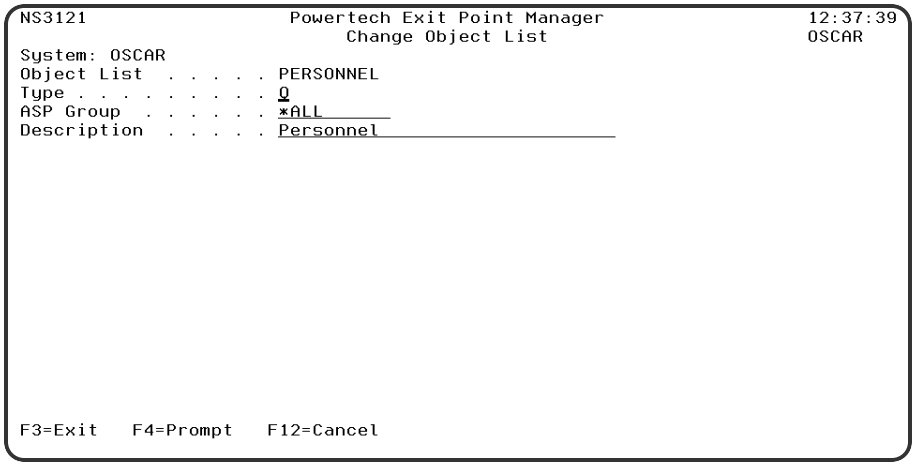
3. Here, you can add new lists and copy, change, delete, or work with existing lists. See Work with Object Lists screen for details.
4. **Adding an Object List.** Enter a **1** in the Opt column on the first line of the Work with Object Lists screen. You can enter the object list name, type, and description in the blank lines or press `Enter` to display the Create Object List screen.



See Create Object List screen for more details.

To change the Type and Description of an existing object list

1. Enter a **2** next to an object list name on the Work with Object Lists screen to display the Change Object List screen.
2. Enter the new type and/ or description and press `Enter` to save the change.

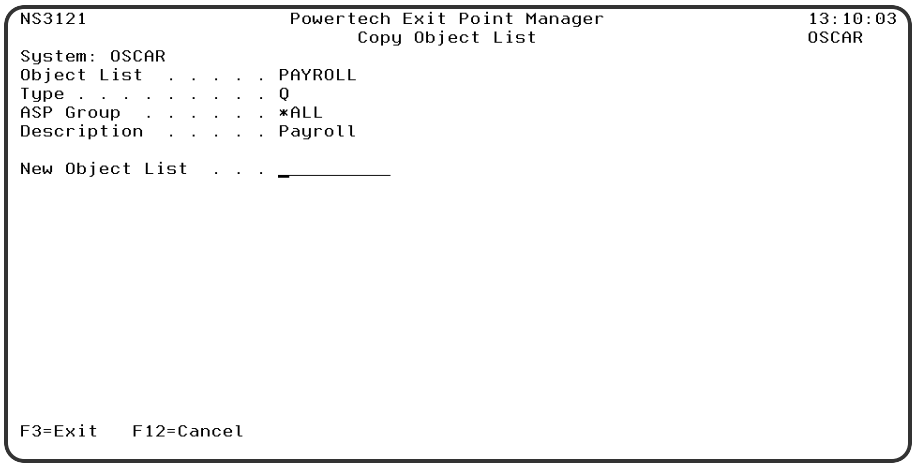


See Change Object List screen.

To copy an existing object list to create a new list with the same object list entries

1. Enter a **3** next to an object list name on the Work with Object Lists screen to display the Copy Object List screen.

2. Enter a name for the new object list press `Enter`.

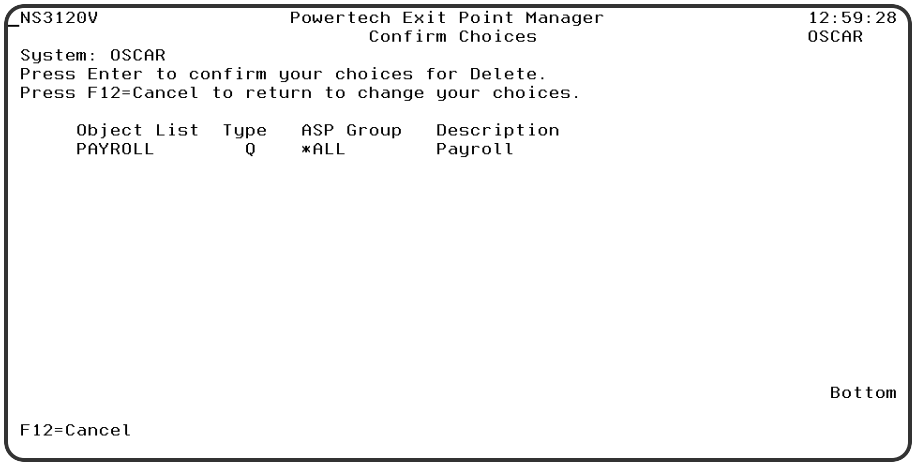


See Copy Object List screen.

To delete an object list

Enter a **4** next to one or more object list names on the Work with Object Lists screen. The Confirm Choices screen displays asking you to confirm that you want to delete the selected object list(s).

> **NOTE:** To delete object lists using the web browser interface, see Using the Web Browser Interface.



See Conform Choices screen.

To rename an object list

1. Enter a **7** next to an object list name on the Work with Object Lists screen to display the Rename Object List screen.
2. Enter a new name for the object list and press `Enter`.

Working with Object List Entries

The purpose of an object list is to group the objects in a library that you want to secure in one object list to which you then can apply Exit Point Manager Object Rules. The object list entries specify the

objects that you are securing.

To add entries to an object list

1. Enter a **1** in the Opt column on the first line of the Work with Object List Entries screen and enter your values in the blank lines or press `Enter` to display the Add Object List Entry screen.
2. Enter the following information to define the object list entry.

```
NS3221                  Powertech Exit Point Manager                  08:09:25
                            Add Object List Entry                     OSCAR
System: OSCAR
Object List  . . . : PERSONNEL   Personnel

Library  . . . . . : ACCTPAY     name, *generic*, <UNKNOWN>
Object . . . . . . : PAYLIST     name, *generic*
Type . . . . . . . : *FILE_


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

See Add Object List Entry screen for more details.

To add entries to an IFS-type object list

1. Enter a **1** in the Opt column of the Work with Object List Entries screen and press `Enter` to display the Add Object List Entry screen.

   > **NOTE:** To add entries to an IFS-type object list using the web browser interface, see To add entries to an object list (web browser) above.

2. Enter the path name for the directory you want to secure. Press `F4` (Prompt) in the Path field to display the Select Path screen, which allows you to select a path in your IFS. The path name can contain either generic or wildcard characters.

3. If the IFS path name is too long to display on the Work with Object List Entries screen, press `F22` (Full Name) to display the full path name in a window.

Sorting object lists and object list entries

You can subset and sort object lists or object list entries so that you see only the lists or objects that meet the criteria you specify. To display the sort screens, press `F16` (Sort/Subset) on the Work with Object Lists or Work with Object List Entries screens. See Sort and Subset Object Lists screen and Sort and Subset Object List Entries screen.

Creating rules for an object list using the green screen

You can create rules to control access to the objects listed in an object list from the Work with Object Lists screen. Creating a rule adds filter rules for the user or location specified for the rule.

To create rules for object lists

1. Enter a **9** in the Opt column next to the object list you want to work with to display the Object Rules using Object List screen.

```
NS3130                                                          14:09:09
                      Object Rules using Object List            HS42
System: HS42      HS42 - MANAGER
Object List  . . . . . : PERSONNEL   Type: Q  Personnel files
Position to Location . : _____________

Type options, press Enter.
  1=Create   2=Change   3=Copy   4=Delete   5=Display   8=Activate Rule ...
                                          Data Accesses
Opt Location        User          Operation  Authority  Aud Msg Cap Switch
 __ _______________ __________    _________  _________  _   _   _  _________



       (No records to be displayed)




F3=Exit   F4=Prompt   F5=Refresh   F7=Select System   F11=Object View
F12=Cancel  F16=Sort/Subset F17=Print  F19=Top  F20=Bottom F23=More Options
```

2. On the Object Rules using Object List screen, enter a **1** in the Opt column and a Location or User name. Press `Enter` to display the Create Object Rule by Location or User screen.

> **NOTE:** Although you can enter your rule directly on the Object Rules using Object Lists screen, the Create Object Rule by Location or User screen makes it easier to see all the fields you need to complete. This example shows how to create a rule by User; creating a rule by location follows the same process.

```
NS3331                 Powertech Exit Point Manager                 13:33:38
                _       Create Object Rule by User                   OSCAR
System: OSCAR
User . . . . . . . . . . . ADAMW_____      User profile, *PUBLIC
Object List  . . . . . . . PAYROLL___      F4 for list
Operation  . . . . . . . . *ALL______      F4 for list
Status . . . . . . . . . . *ACTIVE___      *ACTIVE, *INACTIVE

Data Accesses:
  Authority  . . . . . . . *OS400____      *OS400, *REJECT, *SWITCH
  Audit Transactions . . . *               Y=Yes, N=No, *=Default
  Send Messages  . . . . . *               Y=Yes, N=No, *=Default
  Capture Transactions . . *               Y=Yes, N=No, *=Default
  Switch Profile . . . . . *NONE_____      User profile, *NONE

Object Accesses:
  Authority  . . . . . . . *OS400____      *OS400, *REJECT, *SWITCH
  Audit Transactions . . . *               Y=Yes, N=No, *=Default
  Send Messages  . . . . . *               Y=Yes, N=No, *=Default
  Capture Transactions . . *               Y=Yes, N=No, *=Default
  Switch Profile . . . . . *NONE_____      User profile, *NONE

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

See Create Object Rule by User screen.

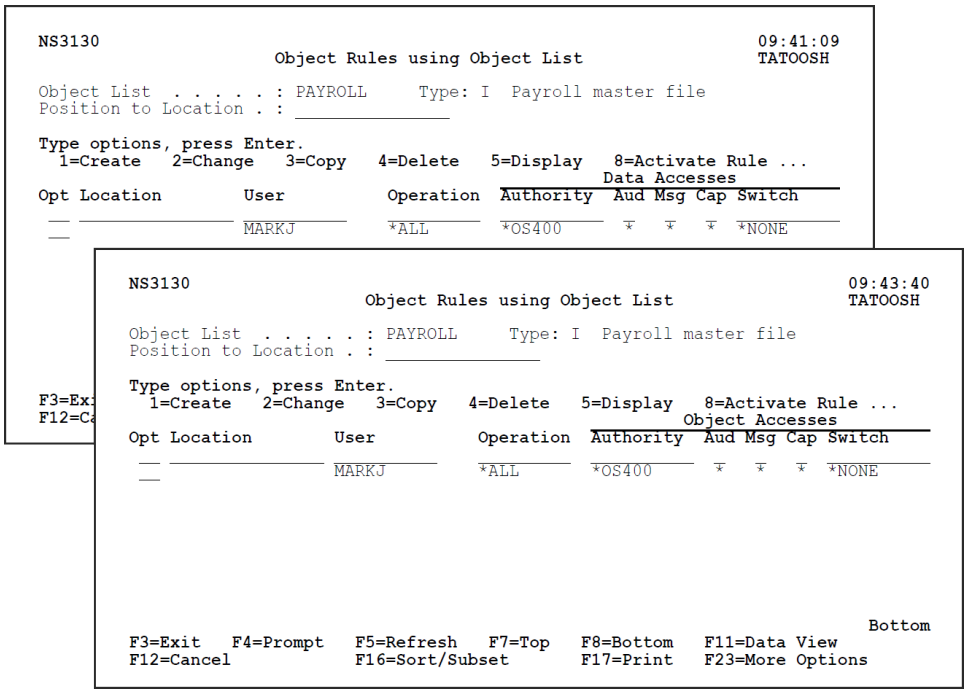
Specifying the Server/Functions for an Object Rule

When you've defined your rule, press `Enter` to display the Select Target Server Functions for Object Rule screen, which allows you to select the servers and functions that will enforce the new user or location filter rule with *MEMOBJ authority you are creating.

1. Enter a **1** next to a server to select server function *ALL, which tells Exit Point Manager to enforce the rule for all functions of the selected server. To select the function *ALL for all servers, press `F10`. If you have previously selected individual functions for a server, pressing `F10` deselects those functions and selects function *ALL for the server.
2. To select individual server functions, enter a **2** next to the server to display the second Select Target Server Functions for Object rule screen, which displays a list of functions for the selected server.
3. Enter a **1** next to each function that should enforce the object rule. To deselect a function, enter a **4** next to the function. To select all individual server functions, except *ALL, press `F10`.

NOTE: If you've previously set filter rules with *MEMOBJ authority for the user or location and don't want to create a new filter rule, you can press `Enter` without making any selections on the Select Target Server Function for Object Rule screens.

4. When you've completed defining your rules, they display on the Object Rules using Object List screen. To switch between the Data Access and Object Access rights, press `F11` (Object View/Data View).



Example: Blocking access to a library while allowing a specific user to access a specific file within that library

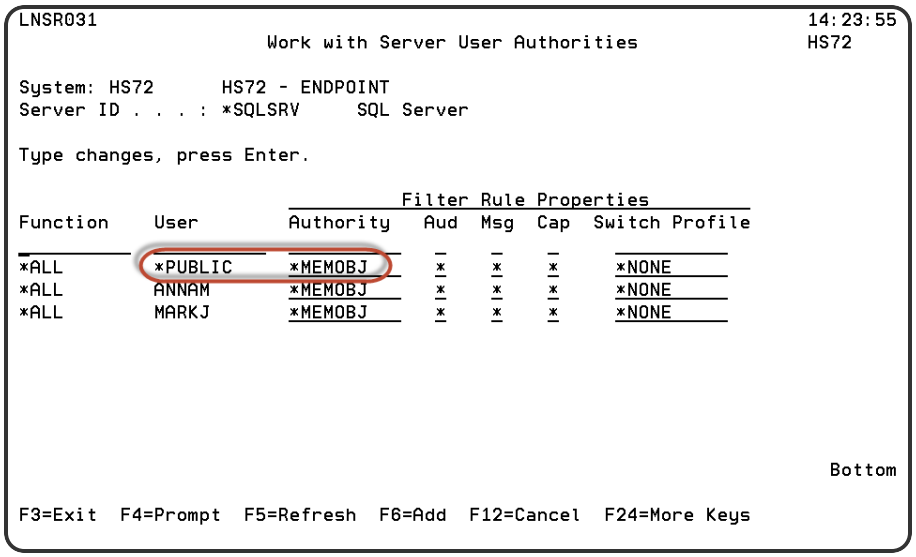
In this example, we will block access to all files in the library PAYROLL but still allow user SHAASE to access the EMPLOYEE file within that library.

To block access using this method, you must change the *PUBLIC rule for *SQLSRV to *MEMOBJ. This instructs Exit Point Manager to consult Object Lists to determine access control. Additional Object Lists will need to be created to authorize access to other objects and libraries using *SQLSVR.

Change the *PUBLIC rule for *SQLSRV to *MEMOBJ:

1. Choose **1** (Work with Security by Server) from the Exit Point Manager Main Menu.

2. Enter **UA** for *SQLSRV.

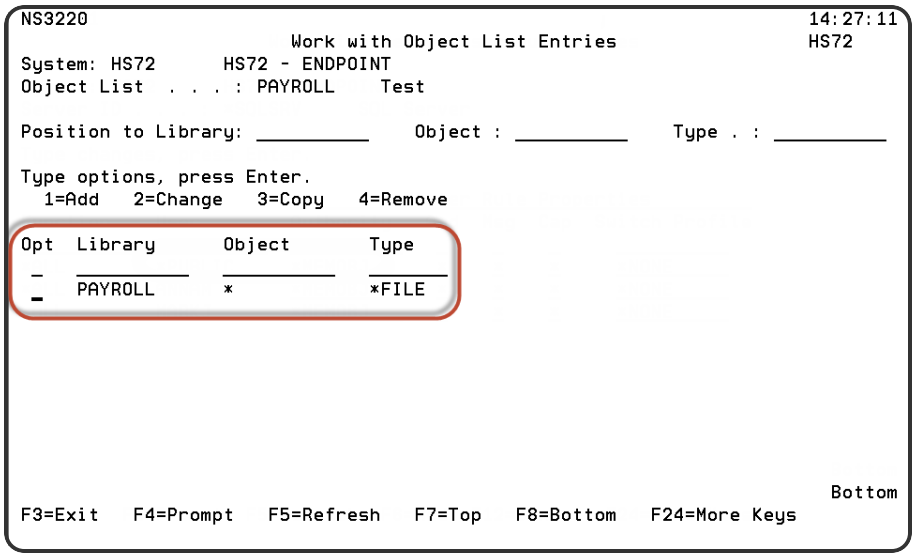


3. Change the Authority for User *PUBLIC to *MEMOBJ and press `Enter`.
4. Press `F3` twice to return to the Main Menu.

2. Create an Object List to block access to all files in the library.

1. Select **4** (Work with Security by Object).
2. Select **1** (Work with Object Lists).
3. Create the Object List PAYROLL using the following values:
    - Opt = 1 (Create)
    - Object List = PAYROLL
    - Type = Q
    - Description = [***Enter description here***]
4. Press `Enter` twice to create the PAYROLL Object List.
5. Enter Opt **8** (Work with Entries) for the PAYROLL Object List.
6. Add an entry for all files using the following values:
    - Opt = 1 (Add)
    - Library = PAYROLL
    - Object = * (* indicates ALL objects)

- Type = *FILE



7. Press `Enter` twice to add the Object List Entry to the PAYROLL Object List.
8. Press `F3` to return to Work with Object Lists.

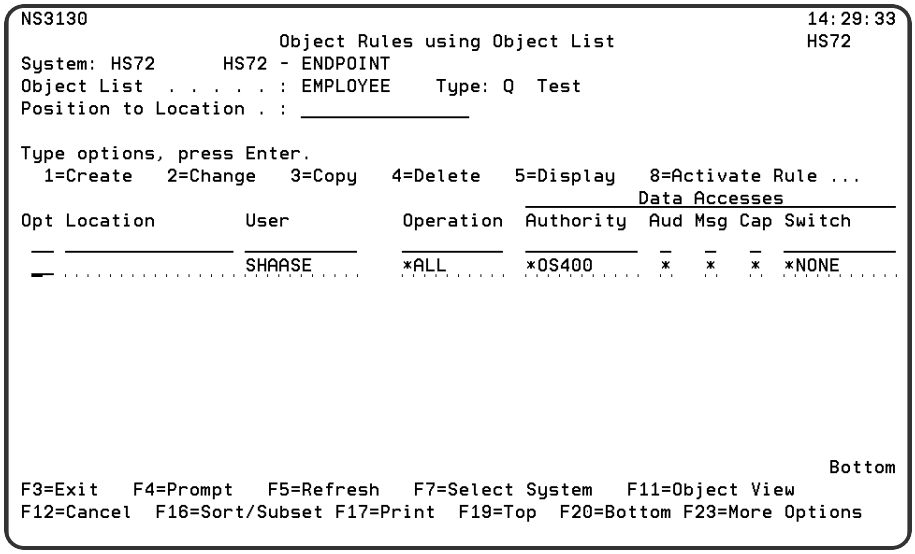
3. Now that the PAYROLL Object List has been successfully added and configured, create another Object List to allow user access to the file EMPLOYEE.

1. Create the Object List EMPLOYEE using the following values:
   - Opt = 1 (Create)
   - Object List = EMPLOYEE
   - Type = Q
   - Description = [*Enter description here*]
2. Press `Enter` twice to create the EMPLOYEE Object List.
3. Enter Opt **8** (Work with Entries) for the EMPLOYEE Object List.
4. Add an entry using the following values:
   - Opt = 1 (Add)
   - Library = PAYROLL
   - Object = EMPLOYEE
   - Type = *FILE
5. Press `Enter` twice to add the Object List Entry to the EMPLOYEE Object List.
6. Press `F3` to return to Work with Object Lists.

4. Give user SHAASE access to the EMPLOYEE Object List.

1. Enter Opt **9** (Object Rules using Object List) next to the object list EMPLOYEE.

- Opt = 1 (Create)
- User = SHAASE
- Operation = *ALL



- Authority = *OS400

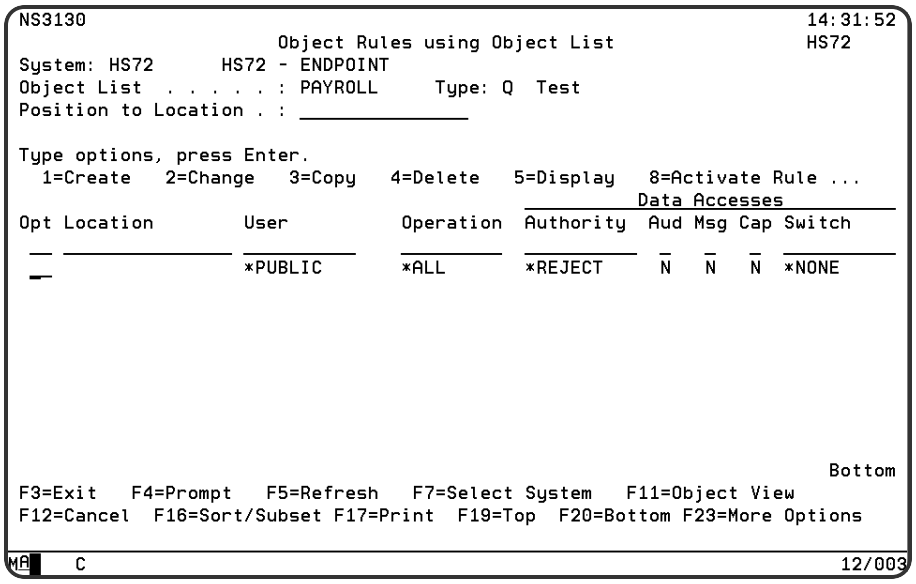
2. Create a new record using the following values:
3. Press `Enter` to review the information on the Create Object Rule by User screen.
4. Press `Enter` again. The Select Target Server Functions for Object Rule screen appears.
5. Enter Opt **1** (Select Server Function *ALL) next to the server *SQLSRV and press `Enter` twice.
6. Press `F3` to return to the Work with Object Lists.

5. Block user *PUBLIC access to the PAYROLL Object List.

1. Enter Opt **9** (Object Rules using Object List) next to the Object List PAYROLL.
2. Create a new record using the following values:

- Opt = 1 (Create)
- User = *PUBLIC
- Operation = *ALL

- Authority = *REJECT

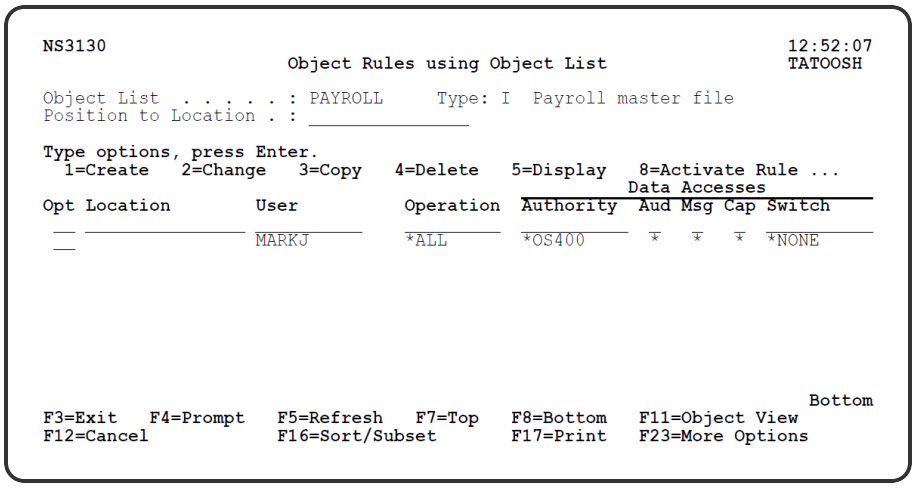


3. Create a new record using the following values:
4. Press `Enter` to review the information on the Create Object Rule by User screen.
5. Press `Enter` again. The Select Target Server Functions for Object Rule screen appears.
6. Enter Opt **1** (Select Server Function *ALL) next to the server *SQLSRV and press `Enter` twice.
7. Press `F3` to return to the Work with Object Lists.

Now, only the user SHAASE will have access to the EMPLOYEE file in the library PAYROLL. Access to all other files in PAYROLL will be blocked.

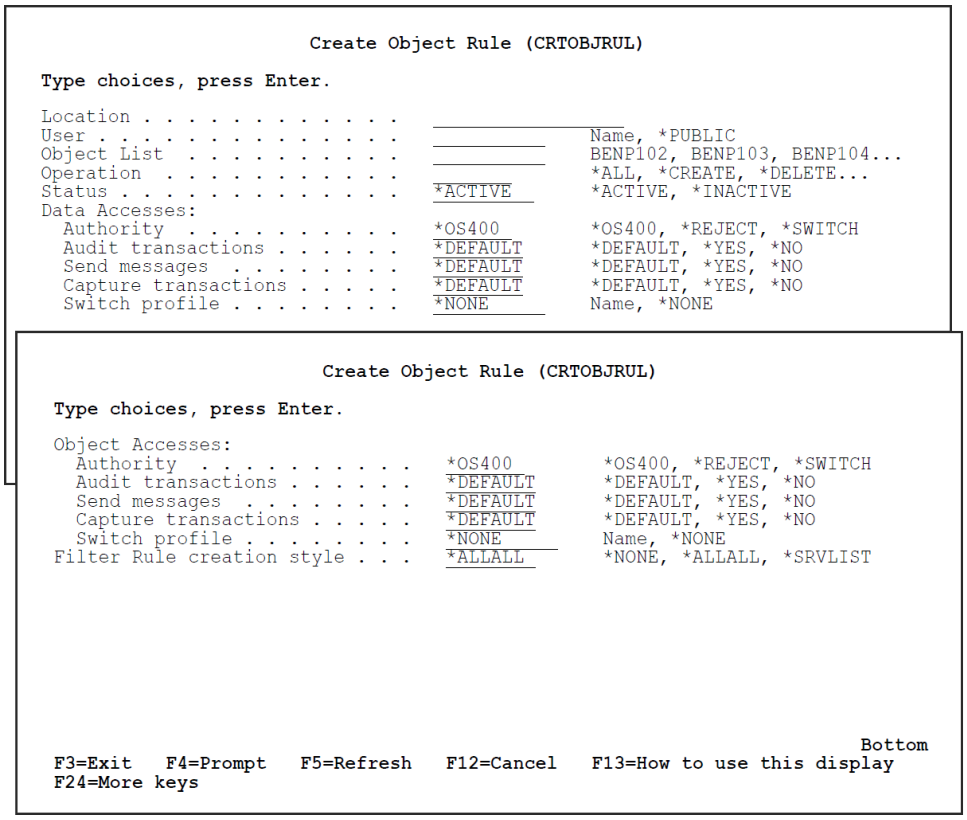
6. Working with Object Rules

To work with the object rules you've created, you can select from the following options. Press `F23` (More Options) to see additional options.



Using the CRTOBJRUL and CHGOBJRUL Commands

The Create Object Rule (CRTOBJRUL) and Change Object Rule (CHGOBJRUL) commands also allow you to create or change an object rule.



```
                    Create Object Rule (CRTOBJRUL)

Type choices, press Enter.

Location . . . . . .
User . . . . . .          Name, *PUBLIC
Object List . . . . . .   BENP102, BENP103, BENP104...
Operation . . . . . .     *ALL, *CREATE, *DELETE...
Status . . . . . .  *ACTIVE  *ACTIVE, *INACTIVE
Data Accesses:
  Authority . . . . . .  *OS400  *OS400, *REJECT, *SWITCH
  Audit transactions . . . . .  *DEFAULT  *DEFAULT, *YES, *NO
  Send messages . . . . . .  *DEFAULT  *DEFAULT, *YES, *NO
  Capture transactions . . . . .  *DEFAULT  *DEFAULT, *YES, *NO
  Switch profile . . . . . .  *NONE  Name, *NONE
```

```
                    Create Object Rule (CRTOBJRUL)

Type choices, press Enter.

Object Accesses:
  Authority . . . . . .  *OS400  *OS400, *REJECT, *SWITCH
  Audit transactions . . . . .  *DEFAULT  *DEFAULT, *YES, *NO
  Send messages . . . . . .  *DEFAULT  *DEFAULT, *YES, *NO
  Capture transactions . . . . .  *DEFAULT  *DEFAULT, *YES, *NO
  Switch profile . . . . . .  *NONE  Name, *NONE
Filter Rule creation style . . .  *ALLALL  *NONE, *ALLALL, *SRVLIST

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

The commands allow you to specify the location or user, the object list, the operation to which the rule applies, and whether it should be active or inactive. The data access and object access options are the same as on the Create or Change Object Rule by User/Location screens.

The Filter Rule creation style parameter allows you to specify how the *MEMOBJ filter rules will be created:

*ALLALL

Selects the *ALL function for all servers.

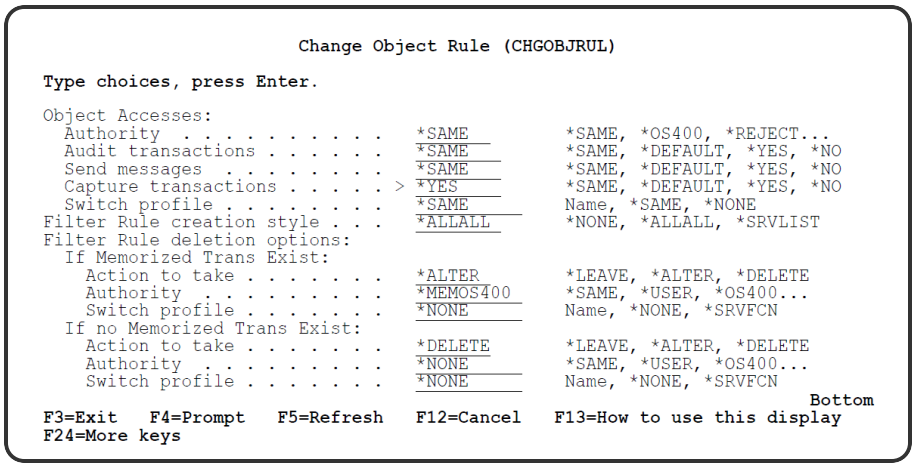
*SRVLIST

Allows you to specify which servers and functions are populated with *MEMOBJ filter rules. Use the Server List parameter to specify the servers and functions.

*NONE

If you don't specify any servers/functions and no *MEMOBJ filter rules already exist when the command is run, no *MEMOBJ filter rules are created and the object rule is placed in *INACTIVE status.

If you use the CHGOBJRUL command to inactivate the last active user or location rule, an additional set of parameters displays allowing you to specify how to handle any *MEMOBJ filter rules that exist at run time.



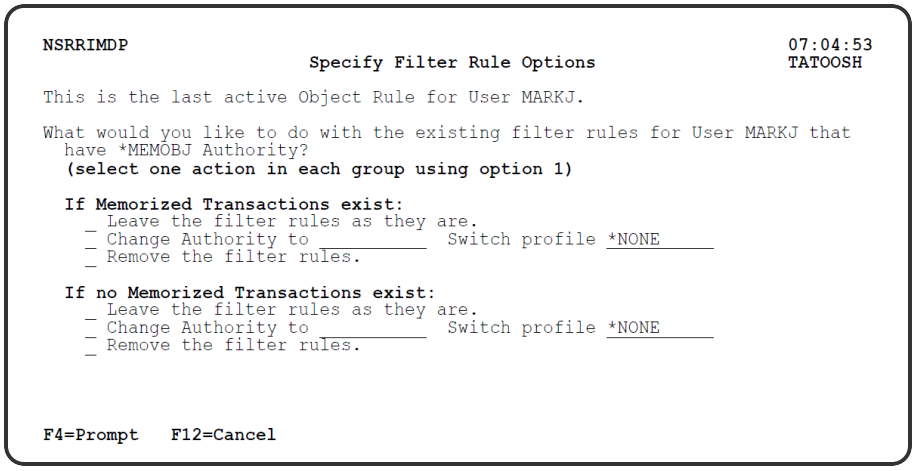
Use the Filter Rule deletion options to specify how you want Exit Point Manager to handle the filter rules.

Deleting an Object Rule

When you create an object rule, it creates filter rules with *MEMOBJ authority for the user or location. When you select to delete or deactivate the last active object rule for a user or location, you should review these filter rules to determine if they are still necessary.

> **NOTE:** Rules can also be deleted using the Insite web UI. See Deleting under "Using the Web Browser Interface."

When you select to delete the last active object rule, the Confirm Choices screen first asks you to confirm the deletion. If you confirm that you want to delete the rule, the Specify Filter Rule Options screen displays so you can specify how you want Exit Point Manager to handle any *MEMOBJ filter rules that exist for the object rule.



You can specify the following for the filter rules depending on whether or not any memorized transactions exist for the same server, function, and user or location as the object rule you are deleting.

If Memorized Transactions exist:

This section controls what happens to the User or Location rules when memorized transactions exist.

Leave the filter rules as they are

The *MEMOBJ User or Location filter rules are not altered or removed.

Change Authority to_____Switch profile_____

Changes the Authority on the filter rules to the value you specify. You must specify a valid Authority value. If you specify *SWITCH or *MEMSWITCH, you also must enter a switch profile name.

Remove the filter rules

Deletes the *MEMOBJ User or Location filter rules.

If no Memorized Transactions exist:

This section controls what happens to the user or location rules when no memorized transactions exist.

Leave the filter rules as they are

The *MEMOBJ User or Location filter rules are not altered or removed.

Change Authority to_____ Switch profile_____

Changes the Authority on the filter rules to the value you specify. You must specify a valid Authority value. If you specify *SWITCH or *MEMSWITCH, you also must enter a switch profile name.

Remove the filter rules

Deletes the *MEMOBJ user or location filter rules.

9. Using the DLTOBJRUL Command

You also can use the Delete Object Rule (DLTOBJRUL) command to delete an object rule.

```
                    Delete Object Rule (DLTOBJRUL)

Type choices, press Enter.

Location . . . . . .   _________________
User . . . . . .   __________    Name, *PUBLIC
Object List  . . . . . .   __________    ACCOUNTING, FTPFILES...
Operation  . . . . . .   _______    *ALL, *CREATE, *DELETE...
Filter Rule deletion options:
  If Memorized Trans Exist:
    Action to take . . . . . .   *ALTER       *LEAVE, *ALTER, *DELETE
    Authority  . . . . . .   *MEMOS400    *USER, *OS400, *REJECT...
    Switch profile . . . . . .   *NONE       Name, *NONE, *SRVFCN
  If no Memorized Trans Exist:
    Action to take . . . . . .   *DELETE      *LEAVE, *ALTER, *DELETE
    Authority  . . . . . .   *NONE       *USER, *OS400, *REJECT...
    Switch profile . . . . . .   *NONE       Name, *NONE, *SRVFCN



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

The command allows you to specify the location or user, the object list, and the operation for which you are deleting an object rule. You also must specify how to handle any *MEMOBJ filter rules currently in existence at run time if the rule being deleted is the last active object rule for the user or location.

The Filter Rule deletion options, for both If Memorized Trans Exist and If no Memorized Trans Exist are:

Action to take

Specify the action to take when *MEMOBJ filter rules exist for the user or location. Valid values are:

***LEAVE** Leaves the existing filter rules as they are.
***ALTER** Changes the authority on existing filter rules to the value you specify in the Authority field.
***DELETE** Deletes the *MEMOBJ user or location filter rules.

Authority

If you specified *ALTER in the Action to take field, enter the Authority value to apply to the user or location rule. Press `F4` to select from a list of possible Authority values.

Switch profile

If you entered *SWITCH or *MEMSWITCH in the Authority field, enter the name of the switch profile. If you entered any other value in the Authority field, Switch profile must be *NONE.

IP Address Groups

IP address groups allow you to set rules when a number of locations need the same location filter rules applied to them. Use the Work with IP Address Groups panel to create, change, and delete groups, as well as define IP address groupings.

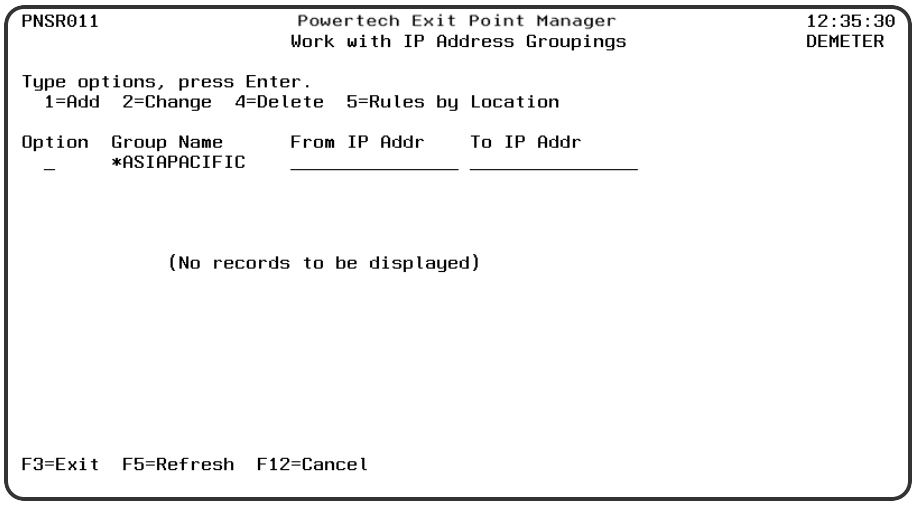
Exit Point Manager IP address groupings allow you to associate IP addresses with an IP address group name. Once you've associated a set of IP addresses with a group name, you can specify the group name as a location when entering location rules. Exit programs check to see if an IP address is part of a group. If the address is part of a group and no specific rule for it exists, the group name is used to determine if a specific rule exists.

Entering IP address groups

1. To specify an IP address grouping, select the IP address group to which you want to assign addresses.
2. On the Work with IP Address Groups panel, enter option **5** next to the group name.

```
PNSR010                  Powertech Exit Point Manager                10:38:10
                          Work with IP Address Groups                DEMETER

Type options, press Enter.
  1=Add  2=Change  4=Delete  5=Work with IP Address Groupings
       (Group Name must start with *)
Opt     Group Name      Description
 _      ______________  ____________________________________________
 5      *ASIAPACIFIC    Asia-Pacific sales region
 _      *EUROPEGRP      European sales region

                                                                  Bottom
F3=Exit  F5=Refresh  F12=Cancel
```

3. The Work with IP Address Groupings panel displays allowing you to add a range of IP addresses to the specified address group.



Switch Profiles

Exit Point Manager's *Switch Profiles* function allows you to customize Exit Point Manager authorizations for network access requests.

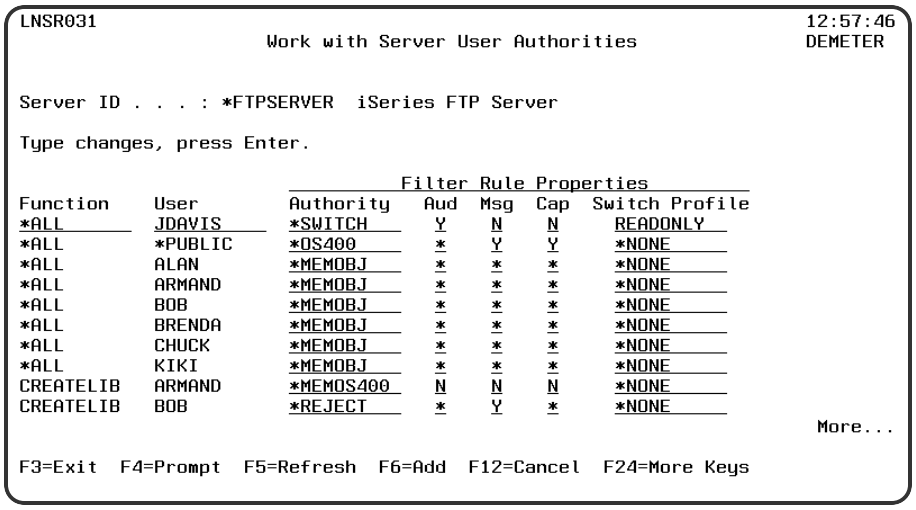
For example, you might use switch profiles in the following situation:

User POWERUSER initiates an incoming FTP request. The POWERUSER profile normally has IBM i authority to change or delete almost any file on the system, and to run most commands using the FTP RMTCMD facility. Because you want to limit the ability of POWERUSER to run FTP requests, you tell Exit Point Manager to switch to another user ID, called READONLY, whenever POWERUSER runs FTP. The READONLY user ID has *USE authority to IBM i files, allowing read-only access to the files, preventing POWERUSER from making any file modifications.

Specifying a Switch Profile

1. On the Exit Point Manager Main Menu, select option **1** to display the Work with Security by Server panel.
2. On the Work with Security by Server panel, enter **UA** (Edit User Authority) to display the Work with Security by User panel. (You also can enter **FN**, Work with Functions, or **LA**, Edit Location Authority, to work with server functions or locations.)
3. On the Work with Security by User panel, specify a Switch Profile to use for a User rule. To create a new user rule, complete the first blank line. The switch profile you enter must be an active profile residing on the system.

> **NOTE:** The administrator specifying the switch profile must have at least *USE authority to the profile.

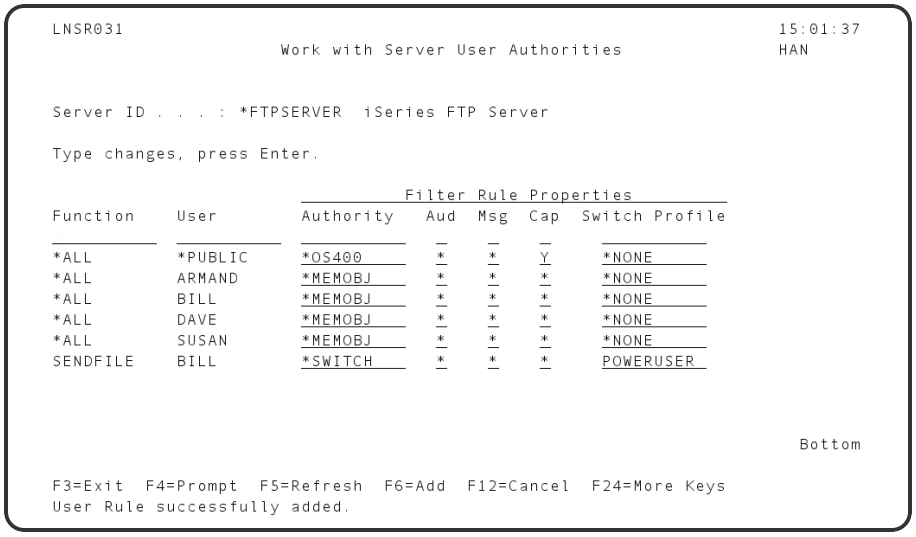


For *FTPSERVER *ALL functions run by user JDAVIS, Exit Point Manager will switch the request to run under the READONLY user profile

If you want to switch to a different user profile only for a particular server function, such as SENDFILE (PUT), you can specify the switch profile for just that function.

Setting a Switch Profile for a Function

1. On the Work with Security by Server panel, enter **FN** next to the server to display the Work with Security by Server/Function panel.
2. On the Work with Security by Server/Function panel, enter **UA** next to the function you want to work with.
3. When the Work with User Authorities panel display, you can specify the switch profile for the function.



For *FTPSERVER SENDFILE functions run by the specified user, Exit Point Manager will switch the request to run under the POWERUSER user profile.

> **NOTE:** When you specify a switch profile, all subsequent actions performed in that FTP session are performed using the switch profile until the user performs another FTP function. Then, Exit Point Manager switches back and performs the next function as the original user.

For example:

- User Bill makes a request to PUT (perform a SENDFILE) a file to the IBM i. Since a rule exists to switch profiles whenever a SENDFILE function is performed, the FTP PUT is switched to run under the user profile POWERUSER.
- All subsequent commands run during Bill's FTP session run under the profile POWERUSER, not Bill.
- As soon Bill performs another FTP function (such as CHGCURLIB or GET), Exit Point Manager changes the job to run as Bill.

Creating a Switch Profile

You probably have user profiles on your system that you can use as a switch profile. However, if you decide to create new user profiles to be used as Exit Point Manager Switch Profiles, use the following guidelines.

> **NOTE:** The switch profile function is not allowed on the file server. If the file server exit program swaps to another user and does not swap back to the original user, the file server session continues to operate with the user that originally connected to the session. This is because the host file server and IBM i NetServer get credential information for the user who did the initial connection to the session and uses this credential information when doing client requests. With the host file server and IBM i NetServer using the credential information, any swapping of the user profile in the file server exit program is not used by the file server for file system operations.

Creating a Switch Profile to limit user authorities:

1. Create a switch user profile using the following command:
   CRTUSRPRF USRPRF(*profile-name*) PASSWORD(*NONE) LMTCPB(*YES) SPCAUT(*NONE)
2. Restrict the switch profile from sensitive libraries by assigning *EXCLUDE authority for the library to be restricted:
   GRTOBJAUT OBJ(*library-name*) OBJTYPE(*LIB) USER(*profile-name*) AUT(*EXCLUDE)
   If you want to allow access to some files in a library, but not others, the switch profile must have at least *USE authority to the library, or the library must have the *PUBLIC authority set to AUT(*USE). If you want read-only access to a file, the switch profile must have at least *USE authority to the file or the file must have the authority set to AUT(*USE). If the switch profile will perform record update operations, the profile must have at least *CHANGE rights, or the file must have the *PUBLIC authority set to AUT(*CHANGE).
   If you want to restrict any files, they must have *PUBLIC authority set to AUT(*EXCLUDE) or you must assign *EXCLUDE authority for the switch profile with the following command:
   GRTOBJAUT OBJ(*library/file*) OBJTVPE(*FILE) USER(*profile-name*) AUT(*EXCLUDE)

NOTE:

- If you don't want to set new user authorities, you can use Exit Point Manager memorized transactions to control network requests for file access.
- To create a switch profile to increase user authorities, you should grant the special authorities needed, and set LMTCPB(*NO) if, for example, you want the user to be able to run commands through network interfaces like FTP's RMTCMD.

To restrict the use of RMTCMD, create a Exit Point Manager authority rule that rejects the FTP RMTCMD function.

```
LNSR031                                                          14:32:25
                      Work with Server User Authorities          DEMETER


Server ID . . . : *FTPSERVER  iSeries FTP Server

Type changes, press Enter.

                                 Filter Rule Properties
Function    User        Authority    Aud  Msg  Cap  Switch Profile
RMTCMD      *PUBLIC     *REJECT      Y    Y    N    *NONE
*ALL        *PUBLIC     *OS400       *    Y    Y    *NONE
*ALL        ALAN        *MEMOBJ      *    *    *    *NONE
*ALL        ARMAND      *MEMOBJ      *    *    *    *NONE
*ALL        BOB         *MEMOBJ      *    *    *    *NONE
*ALL        BRENDA      *MEMOBJ      *    *    *    *NONE
*ALL        CHUCK       *MEMOBJ      *    *    *    *NONE
*ALL        JDAVIS      *SWITCH      Y    N    N    READONLY
*ALL        KIKI        *MEMOBJ      *    *    *    *NONE
CREATELIB   ARMAND      *MEMOS400    N    N    N    *NONE
                                                              More...

F3=Exit  F4=Prompt  F5=Refresh  F6=Add  F12=Cancel  F24=More Keys
```

Transaction Security

What is Transaction Security?

You know that Exit Point Manager helps you monitor and secure your network traffic based on the user making the request or their location. But, what do you do if you need to control network traffic at a more precise level? For example, you might want to reject all FTP requests except when the accounting manager uses FTP to download the accounts receivable file. Or, you want to allow SQL queries against all files on your system except the payroll file.

These are typical scenarios that many companies encounter every day. They illustrate that what you need is transaction security—the ability to control which transactions are allowed to flow into, or out of, your system.

Enabling Transaction Security

Enabling transaction security requires two steps:

Step 1: Capture Transactions

Enable the Capture Transactions process. This tells Exit Point Manager to keep a file of the network transactions that occur on your system.

Step 2: Memorize Transactions

Tell Exit Point Manager to memorize transactions from the captured transactions. By memorizing a transaction, Exit Point Manager can recognize the transaction when it sees it again, and then allow this particular transaction but reject all others.

Transaction Security (Insite web UI)

The following instructions demonstrate how to configure transaction security using HelpSystems Insite.

For more information on HelpSystems Insite, see the HelpSystems Insite User Guide.

Capturing Transactions

When a transaction occurs that fits the criteria of a rule that is flagged to capture, a *captured transaction* is created. The captured transaction can be viewed and edited using the Captured Transactions screen. Subsequent identical transactions are recorded in the incremental count within the captured transaction record. Captured transactions can be memorized and associated with rules specific to that transaction. (See Memorizing Transactions.)

Prerequisites to Capturing Transactions

You must do the following before you can begin capturing transactions:

- Activate exit programs. See Activating Powertech Exit Point Manager, earlier in this User Guide for complete information on activation.
- The job SUMCAPTRAN, in the PTWRKMGT subsystem, must be running before you can display captured transactions. The SUMCAPTRAN job starts automatically when you select option **10**, Work with Captured Transactions, from the Exit Point Manager Main Menu. If it doesn't start automatically, which can occur if it previously ended abnormally, enter the command LENDCAPSUM to reset the job.

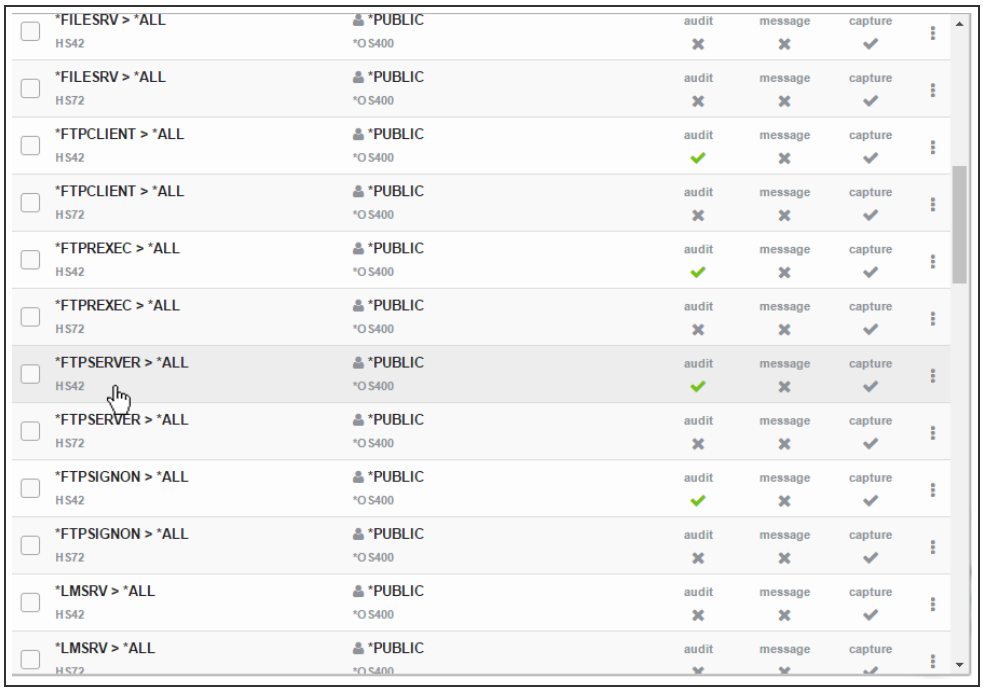
Capturing transactions

1. To start capturing transactions, click **Rules** in the Navigation Pane to open the Rules screen.
2. To capture *user authorities*:

   - Click  .
   - Under Filter By, choose **User Rules**.
   - For Search By, choose **User** (then click  to close the Filter).
   - Check the box to the left of the Search box to select all rules.
   - In the search box, type *PUBLIC from the drop-down menu to display the default user rules for each server.

     > **NOTE:** To capture *location authorities*, in the Filter, select **Filter By > Location Rules** and **Search By > Location**. Then, type *ALL in the search box.

3. Select the rule listing the Server for which you would like to capture transactions.



4. In the Edit Rule screen, for Capture, choose **Yes**.
5. Choose **Save**. Now, when any transactions occur using the selected server/function, Exit Point Manager will capture them.
6. Choose **Captured Transactions** in the Navigation Pane to view all captured transactions. See Captured Transactions screen.

NOTE: To memorize a captured transaction, see Memorizing Transactions.

About SUMCAPTRAN

- You can verify that the SUMCAPTRAN job is running by issuing the WRKACTJOB command. SUMCAPTRAN should appear in the Subsystem/Job column on the Work with Active Jobs screen. The SUMCAPTRAN job runs in the PTWRKMGT subsystem.
- If necessary, you can start the captured transaction subsystem manually by entering the LSTRCAPSUM command on a command line.
- The default SUMCAPTRAN delay time is 120 seconds. You can use the LCHGCAPSUM command to reset the delay time, journal receiver delete handling, and change the last captured date/time.
- When you display the Work with Captured Transactions panel, the summarization process starts automatically and runs every 5 minutes to check if there are new transactions to consolidate. It can take up to 5 minutes before a new captured transaction displays on the screen.
- To end the summarization process, use the LENDCAPSUM command.

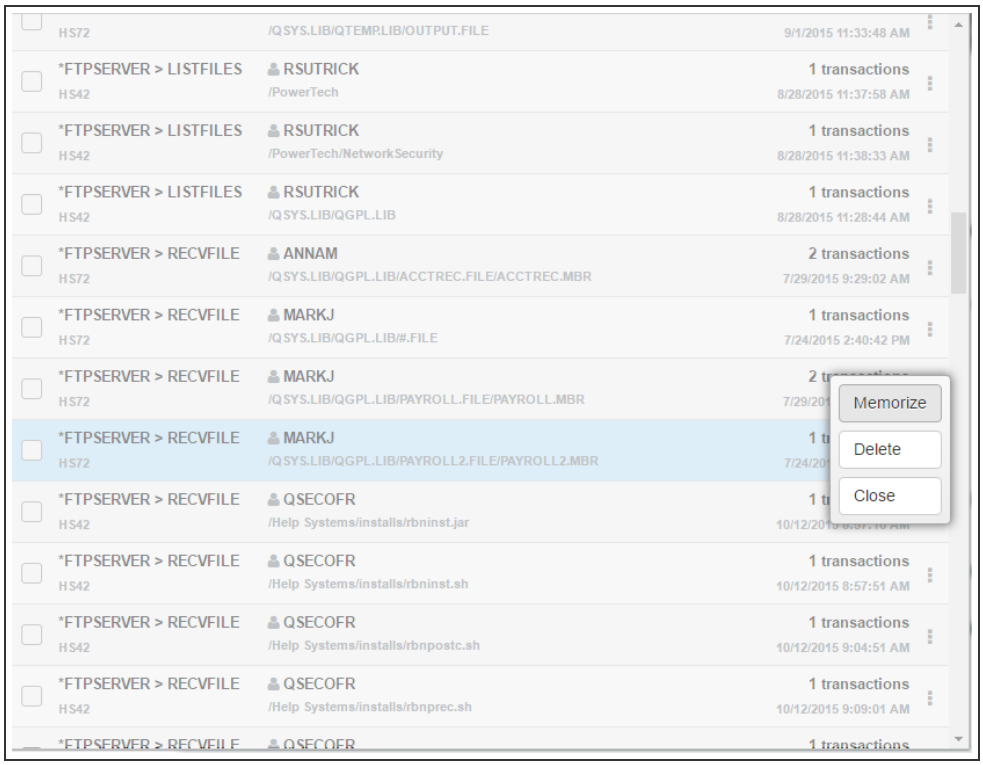
Memorizing Transactions

Exit Point Manager memorized transactions allow you to fine-tune the rules for any captured transaction.

NOTE: When choosing to memorize a transaction, the user still must have authority to any objects (libraries, files, folders, and so on) that are named in the transaction.

Memorizing a transaction

1. Choose **Captured Transactions** in the Navigation Pane to open the Captured Transactions screen.
2. Click ⋮ on the right side of the transaction entry and choose **Memorize**.



3. Configure settings in the New Memorized Transaction screen.
4. Ensure the Status is set to **Active**.
5. Choose **Save** to create the Memorized Transaction.

Working with Memorized Transactions - Insite web UI

After you've memorized your transactions, you should review them periodically to see whether they are still required or need modification.

Working with memorized transactions

1. On the Navigation Pane, click **Memorized Transactions** to display the list of memorized transactions. You can use this screen to view and delete your memorized transactions. To

delete a memorized transaction, select the box to the left of the transaction(s) you would like to delete and choose **Delete**. See also Using the Web Browser Interface.

2. Select a memorized transaction to display the Edit Memorize Transaction screen where you can change a memorized transaction.

Filter Rules Added with Memorized Transactions

Memorized Transactions are processed by Exit Point Manager only when a Filter Rule's Authority setting instructs Exit Point Manager to check them, and they have an *ACTIVE status. When the Filter Rule's Authority setting does not begin with *MEM, Memorized Transactions will not be processed even though some may exist and have an *ACTIVE status. When a Filter Rule's Authority setting begins with *MEM, the active Memorized Transactions that have the same Server, Function, and User or Location values will be processed before the Filter Rules. The portion of the Authority setting that follows *MEM indicates what action to take if no active Memorized Transaction matches the incoming transaction data: REJECT means to reject the transaction, OS400 means to allow it to fall through to the operating system, and SWITCH means to run using the authority of another user profile and fall through to the operating system.

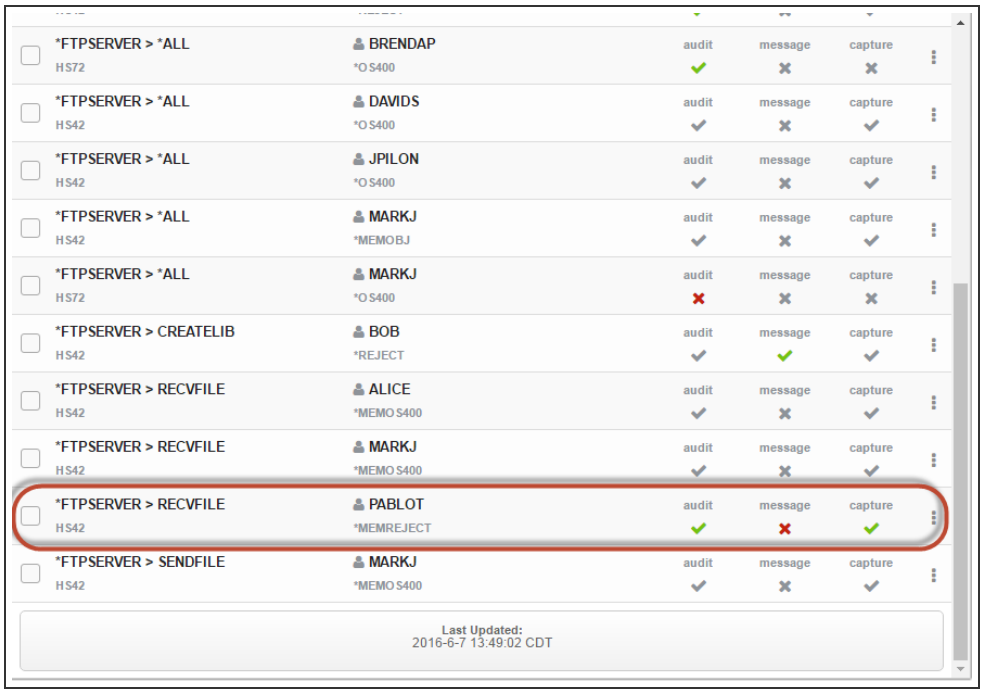
Think of a given combination of Server, Function, and User or Location as the identifier of a "pool" of transactions. There may be a mix of active and inactive transactions in the pool, but only active transactions are matched to incoming transactions.

When a pool of transactions gains its first active transaction, a Filter Rule with matching Server, Function, and User or Location values will be created with *MEMOS400 authority (if one does not exist), or an existing Filter Rule will have its Authority setting modified to begin with *MEM. This is done to initially allow processing of Memorized Transactions for the Server, Function, and User or Location. You may subsequently "turn off" processing of Memorized Transactions by removing the "MEM" from the Authority setting on the associated Filter Rule. The "MEM" portion of the Authority settings will be automatically removed when the pool loses its last active transaction (there are no more active transactions to process). Between the time the first active transaction enters the pool and the last active transaction leaves the pool, the Authority setting on the associated Filter Rule will not be altered by Exit Point Manager.

Authority Filter Properties Example

For example, any attempt by the general public to use the FTP server is allowed (to the extent that the user's authority allows the transaction to occur). However, if user PABLOT attempts to use the RECFILE function of the FTP server, Exit Point Manager looks at the transactions that have been memorized for the FTP server and rejects the attempt—the *MEM portion of the Authority value of *MEMREJECT.) The REJECT portion of *MEMREJECT says that if a memorized transaction is not found for user PABLOT that exactly matches the incoming transaction, the incoming transaction is rejected.

If Exit Point Manager finds a memorized transaction that exactly matches the incoming transaction for the specified user, it takes the action defined by the Authority property in the memorized transaction.



Exit Point Manager provides the following Authority values for a memorized transaction:

*MEMOS400

If the transaction does not match any memorized transactions, the transaction is allowed to the extent that OS/400 security allows the transaction.

*MEMSWITCH

If the transaction does not match any memorized transactions, the job is switched to the specified user profile before allowing the transaction. A switch profile entry is required.

*MEMUSR

If the transaction does not match any memorized transactions, Exit Point Manager looks for a user rule to determine whether the transaction is allowed. *MEMUSR is valid only when working with location authorities.

*SRVFCN

The value used is stored in the Server Function File (select SP on the Server Properties screen).

> **NOTE:** You can see more information about any of the filter rules shown on the Rules Screen by referencing the Captured Transactions screen and Memorized Transactions screen (using the Navigation Pane).

*MEMOBJ

If the transaction does not match any memorized transactions, Exit Point Manager looks for an object rule for a user or location.

How Exit Point Manager Derives Authority Values for Rules

The action that Exit Point Manager takes when an incoming transaction matches a memorized transaction is determined by the Authority property value of the transaction itself. The action Exit Point Manager takes when the incoming transaction does not match a memorized transaction is determined by the Filter Rule that caused the Memorized Transactions to be interrogated.

“Matching transactions” means that the Server, Function, and User or Location on a Memorized Transaction all match exactly with the incoming transaction, and that the transaction data either matches the Memorized Transaction data exactly, or matches a generic portion of the transaction data.

When a transaction MATCHES a memorized transaction

The value you specify for the Memorized Transaction’s Authority, *OS/400, *REJECT or *SWITCH, becomes the action taken by Exit Point Manager when an incoming transaction matches the memorized transaction.

When a transaction does NOT MATCH a memorized transaction

The Authority setting on the Filter Rule that caused the Memorized Transactions to be checked will be used.

*MEMREJECT will reject the non-matching transaction.

*MEMOS400 will allow the transaction to fall through to the operating system.

*MEMSWITCH will let the transaction fall through to the operating system on behalf of a different user profile.

*MEMOBJ will check Object Rules.

*MEMUSR will check User Rules (this value is valid only for Location Rules).

Considerations When Using Memorized Transactions

Keep the following basic considerations in mind when using memorized transactions.

Keep the following basic considerations in mind when using memorized transactions.

- **Captured transactions are always for a specific user.** You can change the server properties to capture transactions for the server. However, the user recorded in the captured transaction is the user who attempted the transaction, not *PUBLIC.
- **Captured transactions are always specific for a server function.** Many of the servers that Exit Point Manager protects have more than one function. For example, the FTP server has several functions including SENDFILE and RECVFILE. You can change the server properties of the FTP server to capture transactions, but when the transaction occurs, the captured transaction specifies the exact function that was requested.
- Exit Point Manager recognizes a transaction as matching a memorized transaction only if the transaction data strings match exactly (except for generic strings specified using the % character).

    - For example, although the following SQL statements produce the same query, the requested transaction does not match the memorized transaction because the fields are specified in a different order.
    - Requested transaction: SELECT custno, name, payrate from Production/PAYROLL01
    - Memorized transaction: SELECT custno, payrate, name from Production/PAYROLL01
- **You can enter memorized transactions manually.** In addition to capturing and memorizing transactions, you can enter transactions by typing the transaction string using the green screen. However, because you are entering the entire transaction string, it is important that you double-check the string contents and spelling to make sure it is accurate. Exit Point Manager memorized transactions perform an exact string match, and thus rely on the quality of the memorized transaction string.
- **Memorized transactions are case-sensitive.** Because the comparison to a memorized transaction string must match exactly, it is case sensitive. If you are modifying a transaction string or entering a string manually, be aware of the case of the string contents. If the match isn't exact, the rule is ineffective.
- **Capturing transactions for some servers doesn't make sense.** Capturing and memorizing transactions for some servers doesn't provide any additional security than does a user, location, or object rule. In general, you don't need to capture transactions for servers that don't provide any user transaction data. For example, when a transaction occurs through the Signon Server, no transaction data is provided. All you can do is control whether a user or group is allowed to use the Signon Server. Thus, you do not need to use a captured/memorized transaction to control the Signon Server. You can control the following servers and functions effectively with a user or location rule instead of using a memorized transaction.

Server	Function
*SQL	All
*SIGNON	All
*FTPSIGNON	All
*REXEC_SO	All
QNPSERVR	INIT
*FTPCLIENT	INIT
*FTPSERVER	INIT

Performance Considerations

Using memorized transactions may add some overhead to the authority checking routine performed by Exit Point Manager. However, performance is affected only while executing the specific function for the particular user or location. The extent to which performance is affected depends on a number of variables, including CPU utilization.

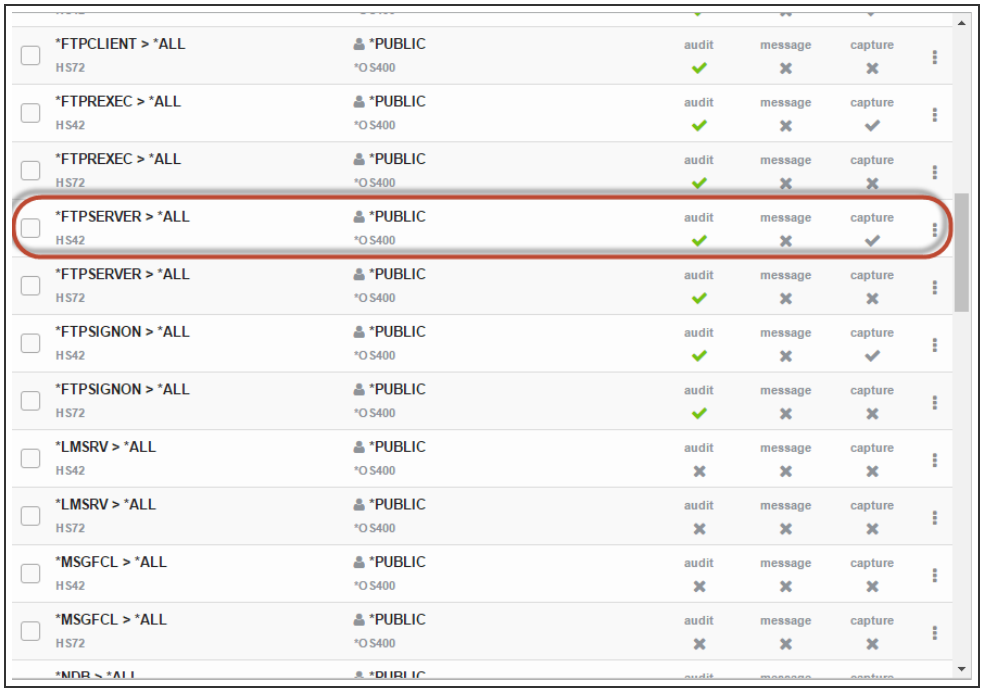
Example: Rejecting All Transactions Except a Specific Transaction

Suppose your company security policy prohibits the use of FTP. However, your accounting associate needs to download the accounts receivable file into an MS Excel spreadsheet. To accommodate this transaction, but prohibit all others, you can capture and memorize the individual transaction, and configure a rule that permits it alone while rejecting all others.

NOTE: In order for these steps to work, the server being used for the transaction (in this case *FTPSERVER) must be active and enabled. See Activating Exit Point Manager.

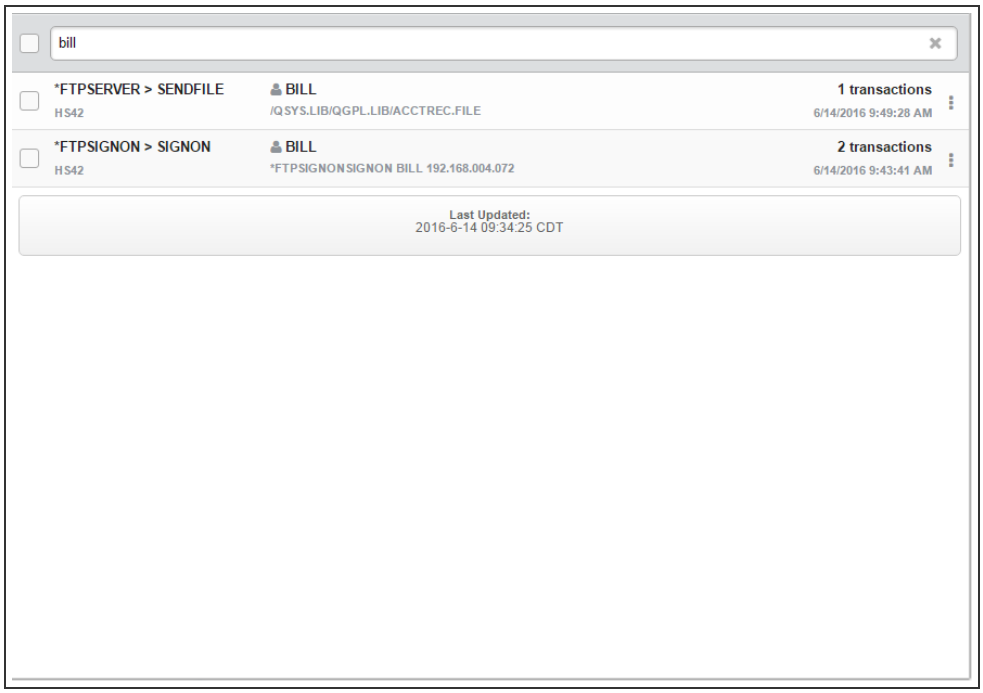
Rejecting all transactions except a specific transaction

1. In the Navigation Pane, select **Rules**, then click and set Search By to **User**. Click to dismiss the search/filter menu. Enter ***PUBLIC** into the search field and press `Enter`. Then, select the *FTPSERVER > *ALL,*PUBLIC rule for a system. This is one of Exit Point Manager's default user rules.



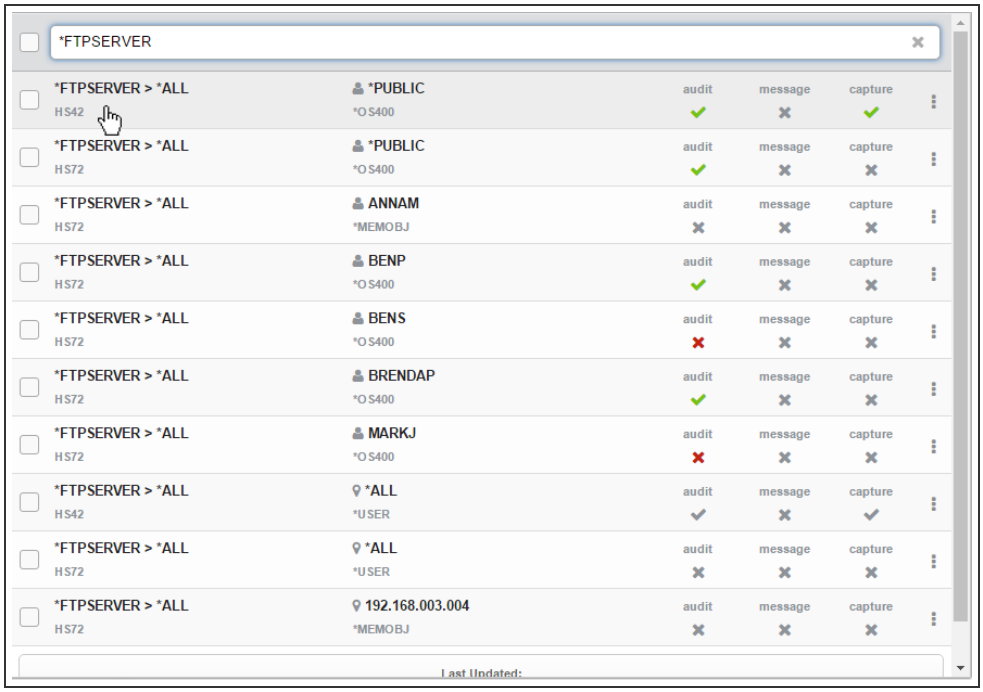
2. For Capture, select **Yes**.
3. Choose **Save**. You have just told Exit Point Manager to capture a record of all transactions coming through your IBM i system's FTP server.
4. Have the accounting associate, (in this example, Bill), download the accounts receivable file. Based on the rule you've set up, Exit Point Manager will allow and capture the transaction. For this example, we'll assume Bill has downloaded the file "ACCTREC" using the FTP server's SENDFILE (get) function.
5. In the Navigation Pane, select **Captured Transactions**.
6. Click and set Search By to **User**. Click to dismiss the search/filter menu.

7. In the search box, for this example, we will type "bill" to show only the transactions by user BILL.



8. Select the SENDFILE transaction. In the View Captured Transaction panel, verify the details of the transaction are accurate and choose **Memorize** .
9. In the New Memorized Transaction screen, next the Authority field, click **Lookup** and choose ***OS400**. This instructs Exit Point Manager to allow the transaction (deferring to the IBM i security settings). (If you have chosen to memorize this transaction for a specific location, specify both the location and the authority. See New Location Memorized Transaction.)
10. Set the Status to **Active** to activate the rule.
11. Choose **Save**.
12. You've now created a rule that allows Bill to download the accounts receivable file. However, Bill, or any other user, still has access to all the FTP server functions. Next we will configure Exit Point Manager to reject all other transactions coming through the FTP server.

13. Click to open the Navigation Pane , select **Rules**, then select the ***FTPSERFVER > *ALL *PUBLIC** user rule.



14. In the Edit Rule screen, click **Lookup** for Authority and choose ***REJECT**. This indicates you want to reject all attempts to use the FTP server. Because of the hierarchy of Exit Point Manager's rule evaluation procedure, this rule will not apply to the transactions you just captured and memorized. On the Rules screen, you may have noticed the new rules with the authority *MEMOS400 (see above). These rules were created when we memorized the captured transactions. *MEMx rules are evaluated after the *PUBLIC rule, and in this example allow these specific transactions to proceed).
15. Set Capture back to **Inherit**.
16. Choose **Save**. Now, only the two transactions specified will be allowed on the FTP server. All others will be rejected.

Transaction Security (green screen)

The following instructions demonstrate how to configure transaction security using the green screen.

Capturing Transactions

When a transaction occurs that fits the criteria of a rule that is flagged to capture, a *captured transaction* is created. The captured transaction can be viewed and edited using the Work With Captured Transactions panel. Subsequent identical transactions are recorded in the incremental count within the captured transaction record. Captured transactions can be memorized and associated with rules specific to that transaction. (See Memorizing Transactions.)

Prerequisites to Capturing Transactions

You must do the following before you can begin capturing transactions:

- Activate exit programs. See Activating Powertech Exit Point Manager, earlier in this User Guide for complete information on activation.
- The job SUMCAPTRAN, in the PTWRKMGT subsystem, must be running before you can display captured transactions. The SUMCAPTRAN job starts automatically when you select option 10, Work with Captured Transactions, from the Exit Point Manager Main Menu. If it doesn't start automatically, which can occur if it previously ended abnormally, enter the command LENDCAPSUM to reset the job.

Capturing transactions

> **NOTE:** We recommend that you capture the transactions at either the Server or Function level, rather than capturing all transactions for all servers. Capturing all transactions, for all servers, could produce a very large log file in a very short period of time. In addition, you should capture transactions only for the servers, server functions, or the particular user for which you want to enable transaction security.

1. To start capturing transactions, select option **1** from the Exit Point Manager Main Menu to display the Work with Security by Server panel.
2. On the Work with Security by Server panel, select the server for which you want to capture transactions. You can select to capture either user authorities by entering **UA**, Edit User Authority, or **LA**, Edit Location Authority, for the server.

```
PNS4110                  Powertech Exit Point Manager                  11:12:16
                         Work with Security by Server                  OSCAR
System  . . . . . : OSCAR    Management System
Position to Server: _________
Type options, press Enter
  FN=Work with Functions      SP=Server Properties
  LA=Edit Location Authority  UA=Edit User Authority
                                                      Rules      Exit Point
Opt  Server      Description                         Enforced    Activated
 __  *CLI        CLI Connection Server                  Y            Y
 __  *CNTRLSRV   License Management Central Server     Y            N
 __  *DATAQSRV   Optimized Data Queue Server           N            N
 __  *DDM        DDM Server                            N            N
 __  *DQSRV      Data Queue Server                     N            N
 __  *DRDA       Distributed Relational Database       N            N
 __  *FILESRV    File Server                           Y            N
 __  *FTPCLIENT  iSeries FTP Client                    Y            Y
 __  *FTPREXEC   FTP Execute Remote Command (REXEC)    Y            Y
 UA  *FTPSERVER  iSeries FTP Server                    Y            Y
 __  *FTPSIGNON  FTP Signon Server                     N            Y
 __  *LMSRV      License Management Server             Y            N
                                                                   More...
F3=Exit   F5=Refresh   F7=Select System   F12=Cancel   F24=More keys
```

3. When the Work with Security by User (or Location) panel displays, choose **2** for the *PUBLIC rule, set the Capture flag to **Y** (Yes), and press `Enter`. The confirmation message User Rule(s) successfully updated displays at the bottom of the panel.

When any transactions occur using the selected server/function, Exit Point Manager will capture them.

To memorize a captured transaction, see Memorizing Transactions.

About SUMCAPTRAN

- You can verify that the SUMCAPTRAN job is running by issuing the WRKACTJOB command. SUMCAPTRAN should appear in the Subsystem/Job column on the Work with Active Jobs panel. The SUMCAPTRAN job runs in the PTWRKMGT subsystem.

- If necessary, you can start the captured transaction subsystem manually by entering the LSTRCAPSUM command on a command line.
- The default SUMCAPTRAN delay time is 120 seconds. You can use the LCHGCAPSUM command to reset the delay time, journal receiver delete handling, and change the last captured date/time.
- When you display the Work with Captured Transactions panel, the summarization process starts automatically and runs every 5 minutes to check if there are new transactions to consolidate. It can take up to 5 minutes before a new captured transaction displays on the panel.
- To end the summarization process, use the LENDCAPSUM command.

Working with Captured Transactions

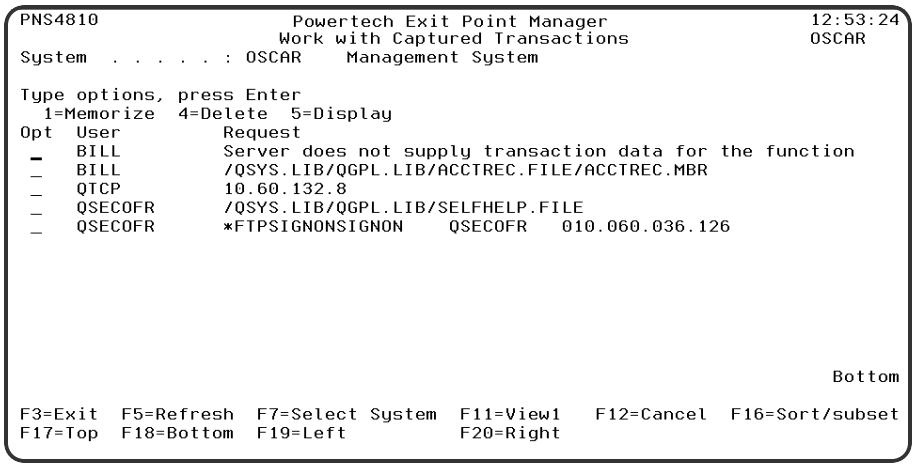
Once you've captured transactions, you can memorize, delete, display, filter, and sort them.

1. From the Exit Point Manager Main Menu, select option **10** to display the Work with Captured Transactions panel.

```
PNS4810                  Powertech Exit Point Manager                  12:12:32
                       Work with Captured Transactions                 OSCAR
System  . . . . . : OSCAR    Management System

Type options, press Enter
  1=Memorize  4=Delete  5=Display
Opt  Server      Function    User       Count Request
 -   *FTPCLIENT  INIT        MARKJ          1 Server does not supply transactio
 _   *FTPCLIENT  SENDFILE    MARKJ          1 /QSYS.LIB/QGPL.LIB/PAYROLL.FILE

                                                                       Bottom
F3=Exit  F5=Refresh  F7=Select System  F11=View2   F12=Cancel  F16=Sort/subset
F17=Top  F18=Bottom
```

2. The Work with Captured Transactions panel provides three views of the transaction data. Each view displays additional parameters and information. Press `F11` to switch to the next view.

```
PNS4810                  Powertech Exit Point Manager                  12:52:22
                       Work with Captured Transactions                 OSCAR
System  . . . . . : OSCAR    Management System

Type options, press Enter
  1=Memorize  4=Delete  5=Display
Opt  Server      Function    User       Count Request
 -   *FTPCLIENT  INIT        BILL           1 Server does not supply transactio
 _   *FTPCLIENT  RECVFILE    BILL           2 /QSYS.LIB/QGPL.LIB/ACCTREC.FILE/A
 _   *FTPSERVER  INIT        QTCP           1 10.60.132.8
 _   *FTPSERVER  RECVFILE    QSECOFR        1 /QSYS.LIB/QGPL.LIB/SELFHELP.FILE
 _   *FTPSIGNON  SIGNON      QSECOFR        1 *FTPSIGNONSIGNON    QSECOFR   010

                                                                       Bottom
F3=Exit  F5=Refresh  F7=Select System  F11=View2   F12=Cancel  F16=Sort/subset
F17=Top  F18=Bottom
```



Work with Captured Transactions, Views 1 and 3

> **NOTE:** Press `F19` (Left) and `F20` (Right) to scroll through the Transaction text to the left or right.

Sorting Captured Transactions

Function key `F16` allows you to filter and sort the captured transactions data that displays on the Work with Captured Transactions panel. This lets you see only the data you want to view.

Use the Select by section to filter the view. See Memorized Transactions Subset. See Memorized Transactions Subset panel.

Deleting Captured Transactions

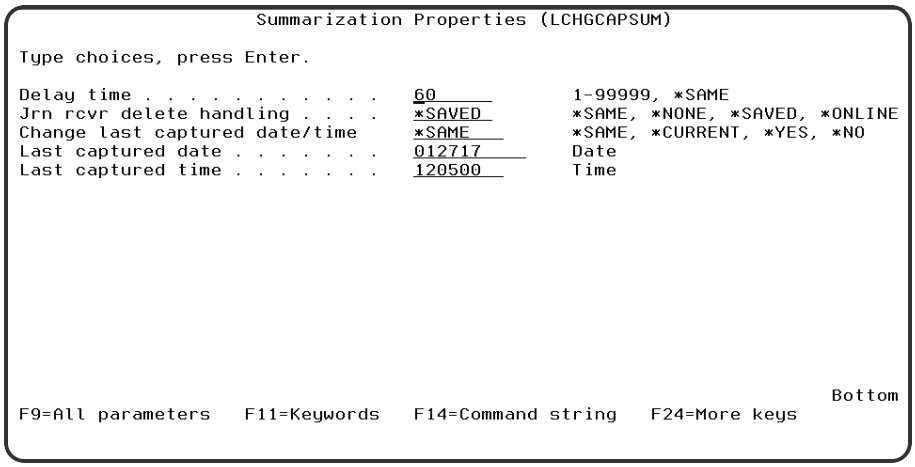
> **NOTE:** Captured Transactions can also be deleted using Insite. See Deleting under "Using the Web Browser Interface."

Earlier versions of Exit Point Manager required the captured transaction file to be purged on a regular basis to prevent the file from growing too large. You could use the LPWRPURGE command in a scheduled job (PowerPurge) to perform the purge.

Starting with Exit Point Manager 6.0, the LPWRPURGE process is no longer available or necessary. Instead, the Capture (transaction) Summarization process cleans up the journal receivers. (Journal PTCAPJRN in the product library stores transactions before summarization.) The DELETE parameter of the command LCHGCAPSUM determines how (and if) the journal receivers are deleted.

Enter the following command and press `F4` to display the Summarization Properties panel.

```
LCHGCAPSUM
```



The Summarization Properties panel allows you to specify how long the Capture Summarization process waits between runs, how the process handles the journal receivers that have been examined, and the date/time in the journal entries the process starts looking for more information the next time it runs.

Summarization Properties Fields

Delay time

Specify the time (in seconds) between summarizations. The summarization, once started, begins summarizing all new captured information. After completing, it waits the number of seconds you've specified and then summarizes any new captured information. This cycle continues until you end the process.

Possible values are:

***SAME** Do not change the delay time currently in effect.
1-99999 Enter the delay time you want to use.

Jrn rcvr delete handling

Determines which, if any, fully processed journal receivers should be deleted. The capture summarization process uses a product-specific journal receiver to store captured information that is waiting for summarization. This parameter specifies what the process does with the receivers that have had all of the information summarized.

Possible values are:

***SAME** Do not change the delete handling.
***NONE** Do not delete any captured transaction summarization journal receivers.
***SAVED** Delete any captured transaction summarization journal receivers that have had their information summarized and are in a *SAVED status.
***ONLINE** Delete any captured transaction summarization journal receivers that have had their information summarized and are in a *SAVED or *ONLINE status.

Change last captured date/time

Allows you to change the date and time of the last processed captured information. You might use this value to skip over (and ignore) captured information that has not already been summarized.

Possible values are:

***SAME** Do not change the last transaction date/time.
***NO** Do not change the last transaction date/time.
***YES** Change the last transaction date/time. If you enter *YES, additional parameters for these two fields display.
***CURRENT** Change the last transaction date/time to the current date and time.

Last captured date

The date the last transaction (of the journal entry in which it was captured) was summarized. Enter the date in the current date format for your job.

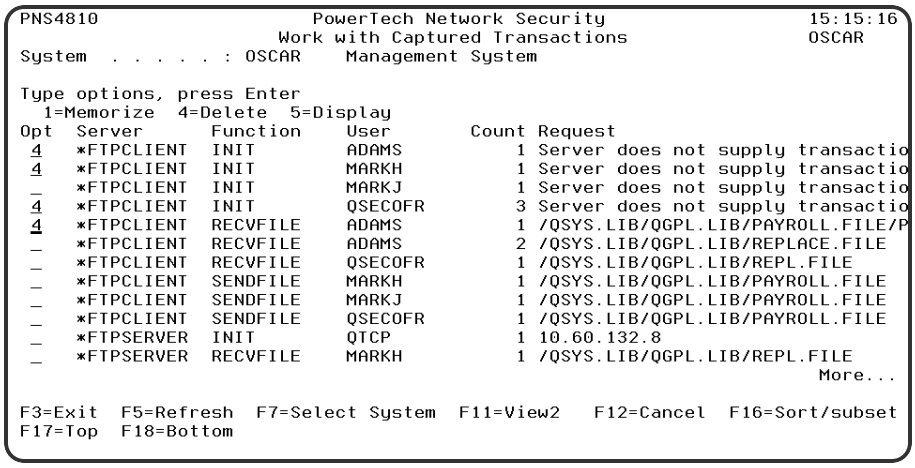
Last captured time

The time the last transaction (of the journal entry in which it was captured) was summarized. Enter this time in the current time format for your job.

Deleting Captured Transactions Manually

You also can delete captured transaction manually directly from the Work with Captured Transactions panel. Typically, you'd delete a captured transaction after you have memorized all the transactions you want to capture.

From the Exit Point Manager Main Menu, select option 10 to display the Work with Captured Transactions panel. Enter option **4**, Delete, next to each captured transaction you want to delete and press `Enter`. You can select to delete one or more captured transactions.



```
PNS4810                  PowerTech Network Security                  15:15:16
                      Work with Captured Transactions                OSCAR
System  . . . . . : OSCAR    Management System

Type options, press Enter
  1=Memorize  4=Delete  5=Display
Opt  Server      Function    User       Count Request
 4   *FTPCLIENT  INIT        ADAMS          1 Server does not supply transactio
 4   *FTPCLIENT  INIT        MARKH          1 Server does not supply transactio
 _   *FTPCLIENT  INIT        MARKJ          1 Server does not supply transactio
 4   *FTPCLIENT  INIT        QSECOFR        3 Server does not supply transactio
 4   *FTPCLIENT  RECVFILE    ADAMS          1 /QSYS.LIB/QGPL.LIB/PAYROLL.FILE/P
 _   *FTPCLIENT  RECVFILE    ADAMS          2 /QSYS.LIB/QGPL.LIB/REPLACE.FILE
 _   *FTPCLIENT  RECVFILE    QSECOFR        1 /QSYS.LIB/QGPL.LIB/REPL.FILE
 _   *FTPCLIENT  SENDFILE    MARKH          1 /QSYS.LIB/QGPL.LIB/PAYROLL.FILE
 _   *FTPCLIENT  SENDFILE    MARKJ          1 /QSYS.LIB/QGPL.LIB/PAYROLL.FILE
 _   *FTPCLIENT  SENDFILE    QSECOFR        1 /QSYS.LIB/QGPL.LIB/PAYROLL.FILE
 _   *FTPSERVER  INIT        QTCP           1 10.60.132.8
 _   *FTPSERVER  RECVFILE    MARKH          1 /QSYS.LIB/QGPL.LIB/REPL.FILE
                                                                    More...

F3=Exit  F5=Refresh  F7=Select System  F11=View2   F12=Cancel  F16=Sort/subset
F17=Top  F18=Bottom
```

Memorizing Transactions - green screen

Exit Point Manager memorized transactions allow you to fine-tune the rules for any captured transaction.

> **NOTE:** When choosing to memorize a transaction, the user still must have authority to any objects (libraries, files, folders, and so on) that are named in the transaction.

Memorizing a transaction

1. On the Main Menu, select option **10** to display the Work with Captured Transactions panel.
2. Enter a **1** in the Opt column next to the transaction you want to memorize and press `Enter`.

```
PNS4810                  Powertech Exit Point Manager                  10:20:12
                       Work with Captured Transactions                 OSCAR
System  . . . . . : OSCAR    Management System

Type options, press Enter
  1=Memorize  4=Delete  5=Display
Opt  Server      Function    User       Count Request
     *FTPCLIENT  INIT        MARKJ          1 Server does not supply transactio
 1   *FTPCLIENT  SENDFILE    MARKJ          1 /QSYS.LIB/QGPL.LIB/PAYROLL.FILE
                                                                        Bottom
F3=Exit  F5=Refresh  F7=Select System  F11=View2   F12=Cancel  F16=Sort/subset
F17=Top  F18=Bottom
```

3. The Memorize Captured Transaction panel displays, allowing you to specify the values for the memorized transaction.

```
PNS4811                  Powertech Exit Point Manager                  10:23:24
                                                                        OSCAR
System: OSCAR     Management System

Server  . . . . : *FTPCLIENT                  iSeries FTP Client
Function  . . . : SENDFILE                    Send file (APPEND, PUT, MPUT)
Type  . . . . . : U                           User is a profile name
User  . . . . . : MARKJ
Location  . . . :
Authority . . . : *OS400                      OS/400 authority
Audit . . . . . : *                           Determined when evaluated
Message . . . . : *                           Determined when evaluated
Capture . . . . : *                           Determined when evaluated
Switch Profile  : *NONE                       No switch profile is used

Request (at 1 of 31):
/QSYS.LIB/QGPL.LIB/PAYROLL.FILE
F3=Exit   F4=Prompt   F12=Cancel
```

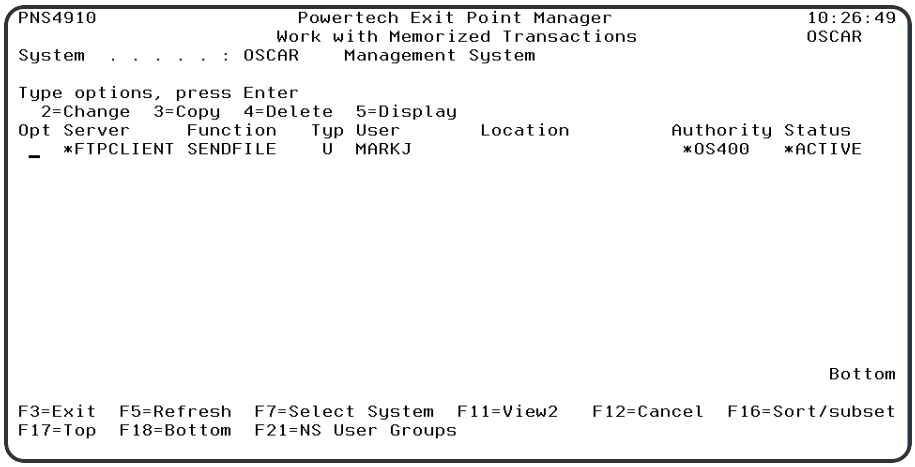
See Work with Captured Transactions panel.

Working with Memorized Transactions

After you've memorized your transactions, you should review them periodically to see whether they are still required or need modification.

Working with memorized transactions

1. On the Main Menu, select option **11** to display the Work with Memorized Transactions panel. You can use this panel to change, copy, delete, and display your memorized transactions.



2. The Work with Memorized Transactions panel provides three views of the transaction data. Each view displays additional parameters and information.
3. Press **F11** to switch to the next view.

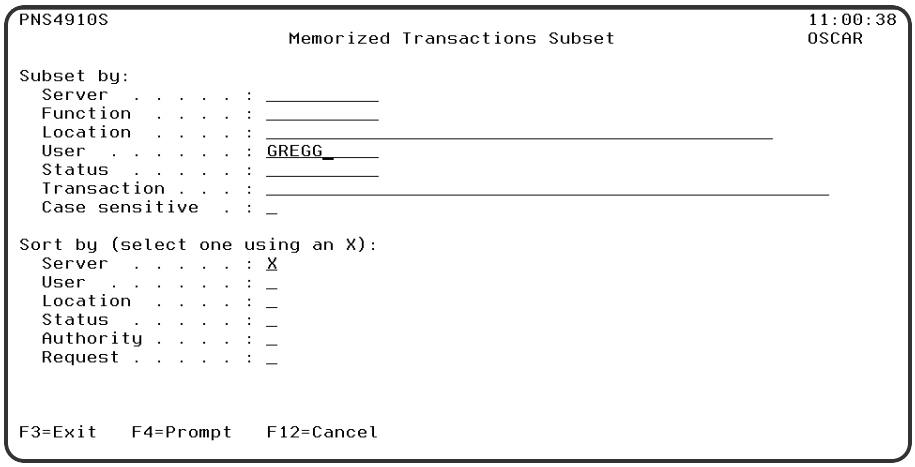
See Work with Memorized Transactions panel.

NOTE: Press **F19** (Left) and **F20** (Right) to scroll through the Transaction text to the left or right.

Sorting Memorized Transactions

F16 allows you to filter and sort the memorized transactions data that displays on the Work with Memorized Transactions panel. This lets you see only the data you want to view.

NOTE: See Sorting to learn how to sort records using Exit Point Manager's web browser interface.



Use the Select by section to filter the view. See Memorized Transactions Subset panel.

Filter Rules Added with Memorized Transactions

Memorized Transactions are processed by Exit Point Manager only when a Filter Rule's Authority setting instructs Exit Point Manager to check them, and they have an *ACTIVE status. When the Filter

Rule's Authority setting does not begin with *MEM, Memorized Transactions will not be processed even though some may exist and have an *ACTIVE status. When a Filter Rule's Authority setting begins with *MEM, the active Memorized Transactions that have the same Server, Function, and User or Location values will be processed before the Filter Rules. The portion of the Authority setting that follows *MEM indicates what action to take if no active Memorized Transaction matches the incoming transaction data: REJECT means to reject the transaction, OS400 means to allow it to fall through to the operating system, and SWITCH means to run using the authority of another user profile and fall through to the operating system.

Think of a given combination of Server, Function, and User or Location as the identifier of a "pool" of transactions. There may be a mix of active and inactive transactions in the pool, but only active transactions are matched to incoming transactions.

When a pool of transactions gains its first active transaction, a Filter Rule with matching Server, Function, and User or Location values will be created with *MEMOS400 authority (if one does not exist), or an existing Filter Rule will have its Authority setting modified to begin with *MEM. This is done to initially allow processing of Memorized Transactions for the Server, Function, and User or Location. You may subsequently "turn off" processing of Memorized Transactions by removing the "MEM" from the Authority setting on the associated Filter Rule. The "MEM" portion of the Authority settings will be automatically removed when the pool loses its last active transaction (there are no more active transactions to process). Between the time the first active transaction enters the pool and the last active transaction leaves the pool, the Authority setting on the associated Filter Rule will not be altered by Exit Point Manager.

Authority Filter Properties Example

By referring to the panel below, you can see that any attempt by the general public to use the FTPCLIENT server is to be rejected. However, if user MARKJ attempts to use the SENDFILE function of the FTPCLIENT server, Exit Point Manager looks at the transactions that have been memorized for the FTPCLIENT server first due to the *MEM portion of the Authority value of *MEMREJECT. The REJECT portion of *MEMREJECT instructs Exit Point Manager to reject the incoming transaction if a memorized transaction is not found for user MARKJ that exactly matches the incoming transaction.

If Exit Point Manager finds a memorized transaction that exactly matches the incoming transaction for the specified user (or user group), it takes the action defined by the Authority property in the memorized transaction.

```
PNS4210                  Powertech Exit Point Manager                  14:57:41
                          Work with Security by User                   OSCAR
System  . . . . . : OSCAR    Management System
Position to User  : __________
Type options, press Enter
  2=Change  3=Copy  4=Delete  5=Display
                                          Filter Rule Properties
Opt Typ  User       Server     Function   Authority  Aud Msg Cap  Switch Prf
 _   U   *PUBLIC    *FTPCLIENT *ALL       *REJECT     Y   *   *   *NONE
 _   U   ADAMS      *FTPCLIENT RECVFILE   *MEMOS400   *   *   *   *NONE
 _   U   BILL       *FTPCLIENT RECVFILE   *MEMOS400   *   *   *   *NONE
 _   U   MARKH      *FTPCLIENT SENDFILE   *MEMOS400   *   *   *   *NONE
 _   U   MARKJ      *FTPCLIENT SENDFILE   *MEMREJECT  *   *   *   *NONE
                                                                      Bottom
F3=Exit            F5=Refresh          F6=Create rule    F7=Select System
F8=Captured trans  F9=Memorized trans  F12=Cancel        F24=More keys
The list is subsetted.
```

Exit Point Manager provides the following Authority values that enable processing of Memorized Transactions:

*MEMOS400

If the transaction does not match any memorized transactions, the transaction is allowed to the extent that OS/400 security allows the transaction.

*MEMSWITCH

If the transaction does not match any memorized transactions, the job is switched to the specified user profile before allowing the transaction. A switch profile entry is required.

*MEMUSR

If the transaction does not match any memorized transactions, Exit Point Manager looks for a user rule to determine whether the transaction is allowed. *MEMUSR is valid only when working with location authorities.

*MEMOBJ

If the transaction does not match any memorized transactions, Exit Point Manager looks for an object rule for a user or location.

NOTE: You can see more information about any of the filter rules shown on the Work with Security by User and Work with Security by Location panels by pressing **F8** and **F9**.

- F8, Captured transactions, displays the Work with Captured Transactions panel where you can view details of a captured transaction, including the authority value, the function, or the exact file specified by the transaction.
- F9, Memorized transactions, displays the Work with Memorized Transactions panel where you can view details of a memorized transaction, including the authority value, the function, or the exact file specified by the transaction.

How Exit Point Manager Derives Authority Values for Rules

The action that Exit Point Manager takes when an incoming transaction matches a memorized transaction is determined by the Authority property value of the transaction itself. The action Exit Point Manager takes when the incoming transaction does not match a memorized transaction is determined by the Filter Rule that caused the Memomrized Transactions to be interrogated.

“Matching transactions” means that the Server, Function, and User or Location on a Memorized Transaction all match exactly with the incoming transaction, and that the transaction data either matches the Memorized Transaction data exactly, or matches a generic portion of the transaction data.

When a transaction MATCHES a memorized transaction

The value you specify for the Memorized Transaction’s Authority, *OS/400, *REJECT or *SWITCH, becomes the action taken by Exit Point Manager when an incoming transaction matches the memorized transaction.

When a transaction does NOT MATCH a memorized transaction

The Authority setting on the Filter Rule that caused the Memorized Transactions to be checked will be used.

*MEMREJECT will reject the non-matching transaction.

*MEMOS400 will allow the transaction to fall through to the operating system.

*MEMSWITCH will let the transaction fall through to the operating system on behalf of a different user profile.

*MEMOBJ will check Object Rules.

*MEMUSR will check User Rules (this value is valid only for Location Rules).

Considerations When Using Memorized Transactions

Keep the following basic considerations in mind when using memorized transactions.

- **Captured transactions are always for a specific user.** You can change the server properties to capture transactions for the server. However, the user recorded in the captured transaction is the user who attempted the transaction, not *PUBLIC.
- **Captured transactions are always specific for a server function.** Many of the servers that Exit Point Manager protects have more than one function. For example, the FTP server has several functions including SENDFILE and RECVFILE. You can change the server properties of the FTP server to capture transactions, but when the transaction occurs, the captured transaction specifies the exact function that was requested.
- Exit Point Manager recognizes a transaction as matching a memorized transaction only if the transaction data strings match exactly (except for generic strings specified using the % character).
    - For example, although the following SQL statements produce the same query, the requested transaction does not match the memorized transaction because the fields are specified in a different order.
    - Requested transaction: SELECT custno, name, payrate from Production/PAYROLL01
    - Memorized transaction: SELECT custno, payrate, name from Production/PAYROLL01
- **You can enter memorized transactions manually.** In addition to capturing and memorizing transactions, you can enter transactions by typing the transaction string using the green screen. However, because you are entering the entire transaction string, it is important that you double-check the string contents and spelling to make sure it is accurate. Exit Point Manager memorized transactions perform an exact string match, and thus rely on the quality of the memorized transaction string.
- **Memorized transactions are case-sensitive.** Because the comparison to a memorized transaction string must match exactly, it is case sensitive. If you are modifying a transaction string or entering a string manually, be aware of the case of the string contents. If the match isn't exact, the rule is ineffective.
- **Capturing transactions for some servers doesn't make sense.** Capturing and memorizing transactions for some servers doesn't provide any additional security than does a user, location, or object rule. In general, you don't need to capture transactions for servers that don't provide any user transaction data. For example, when a transaction occurs through the Signon Server, no transaction data is provided. All you can do is control whether a user or group is allowed to use the Signon Server. Thus, you do not need to use a captured/memorized transaction to control the Signon Server. You can control the following servers and functions effectively with a user or location rule instead of using a memorized transaction.

Server	Function
*SQL	All

Server	Function
*SIGNON	All
*FTPSIGNON	All
*REXEC_SO	All
QNPSERVR	INIT
*FTPCLIENT	INIT
*FTPSERVER	INIT

Performance Considerations

Using memorized transactions may add some overhead to the authority checking routine performed by Exit Point Manager. However, performance is affected only while executing the specific function for the particular user or location. The extent to which performance is affected depends on a number of variables, including CPU utilization.

Example 1: Rejecting All Transactions Except a Specific Transaction

Suppose your company security policy prohibits the use of FTP. However, your accounting associate needs to download the accounts receivable file into an MS Excel spreadsheet. To accommodate this transaction, but prohibit all others, you can capture and memorize the individual transaction, and configure a rule that permits it alone while rejecting all others.

> **NOTE:** In order for these steps to work, the server being used for the transaction (in this case *FTPCLIENT) must be active and enabled. See Activating Exit Point Manager.

Rejecting all transactions except a specific transaction

1. Select option **1** from the Exit Point Manager Main Menu to display the Work with Security by Server panel. Enter **SP** next to *FTPCLIENT to display the Change Server Function Rule panel. Enter a **Y** next to Capture to turn on the Capture Transactions filter rule property for the FTP client server.

```
PNS4111                  Powertech Exit Point Manager                  08:37:30
                          Change Server Function Rule                  OSCAR
System: OSCAR     Management System

Server  . . . . : *FTPCLIENT  iSeries FTP Client
Function  . . . : *ALL

Enforce Server rules  . . . . : Y

Server filter rule properties:
 Authority  . . . . . . . . . : *SYSTEM
 Audit  . . . . . . . . . . . : *
 Message  . . . . . . . . . . : *
 Capture  . . . . . . . . . . : Y
 Switch Profile . . . . . . . : *NONE
 Supplemental Exit Program  . : *NONE
   Library  . . . . . . . . . : __________




F3=Exit  F4=Prompt  F5=Refresh  F12=Cancel
```

2. Have the accounting associate download the accounts receivable file. Based on the current configuration, Exit Point Manager will allow the transaction and capture it. For this example, we'll assume Bill has downloaded the file "ACCTREC" using the FTP client server's RECVFILE (get) function.
3. Press **F3** until you return the Main Menu.
4. Choose option **10** to open the Work with Captured Transactions panel.
5. press **F16** to display the Subset panel. Filter the captured transactions by the server name *FTPCLIENT.

```
PNS4810S                 Powertech Exit Point Manager                  08:42:42
                        Memorized Transactions Subset                  OSCAR

Subset by:
  User  . . . . . . . : _________
  Server  . . . . . . : *FTPCLIENT
  Function  . . . . . : _________
  Type  . . . . . . . : _________
  Transaction . . . . : ____________________________________________________
  Case sensitive  . . : _


Sort by (select one using an X):
  Server  . . . . . . : X
  User  . . . . . . . : _
  Status  . . . . . . : _
  Authority . . . . . : _
  Request . . . . . . : _




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

6. Press Enter to view the transactions. In this case, two FTP transactions were required in order for Bill to download the ACCTREC file: the INIT function required to initialize the FTP session, and the RECVFILE function called to download the file. In order to permit Bill to download the file in the future, both of these transactions must be memorized and allowed. Then, to prevent all other users from downloading the file, the *PUBLIC rule for the FTP Client server must be set to *REJECT.

```
PNS4810                  Powertech Exit Point Manager                  08:57:56
                       Work with Captured Transactions                 OSCAR
System  . . . . . : OSCAR    Management System

Type options, press Enter
  1=Memorize  4=Delete  5=Display
Opt  Server      Function    User       Count Request
 _   *FTPCLIENT  INIT        BILL           1 Server does not supply transactio
 _   *FTPCLIENT  RECVFILE    BILL           2 /QSYS.LIB/QGPL.LIB/ACCTREC.FILE/A

                                                                        Bottom
F3=Exit  F5=Refresh  F7=Select System  F11=View2   F12=Cancel  F16=Sort/subset
F17=Top  F18=Bottom
The list is subsetted.
```

7. Enter **1** next to the RECVFILE transaction and press `Enter`.

```
PNS4811                  Powertech Exit Point Manager                  09:02:57
                                                                        OSCAR
System: OSCAR     Management System

Server  . . . . : *FTPCLIENT                  iSeries FTP Client
Function  . . . : RECVFILE                    Receive file (GET, MGET)
Type  . . . . . : U                           User is a profile name
User  . . . . . : BILL
Location  . . . :
Authority . . . : *OS400                      OS/400 authority
Audit . . . . . : *                           Determined when evaluated
Message . . . . : *                           Determined when evaluated
Capture . . . . : *                           Determined when evaluated
Switch Profile  : *NONE                       No switch profile is used

Request (at 1 of 43):
/QSYS.LIB/QGPL.LIB/ACCTREC.FILE/ACCTREC.MBR

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

8. Ensure the Authority is set to *OS400, in order to allow the transaction, and press `Enter` to save your changes.
9. Repeat steps 7-8 for the INIT transaction. You've now created rules that allow Bill to download the accounts receivable file. However, Bill, or any other user, still has access to all the FTPCLIENT server functions. Next we will configure Exit Point Manager to reject all other transactions coming through the FTPCLIENT server by setting the *PUBLIC user rule to *REJECT.
10. Press `F3` to return to the Main Menu and select option **1**, Work with Security by Server.
11. Type **UA** next to *FTPCLIENT and press `Enter` to open the Work with Security by User panel.
12. Enter **2** to change the *PUBLIC rule.
13. Change the Authority for *PUBLIC to ***REJECT** and set Capture to * (to stop capturing transactions).
14. Press `Enter`. Now, only the two transactions specified will be allowed on the FTP server. All others will be rejected.

Example 2: Editing Transactions to Make Them Generic

You can make a memorized transaction generic by editing the transaction data string (on the green screen) so that it ends with the % wildcard character. You might decide to make a transaction generic

if, for example, you want the transaction security to apply to all the objects in a particular library. Making the transaction generic saves you from adding a transaction for each object in the library.

1. From the Exit Point Manager Main Menu, select option **11** to display the Work with Memorized Transactions panel.

   Press **F16** to display the Memorized Transactions Subset panel. Filter the memorized transactions by server *FTPCLIENT.

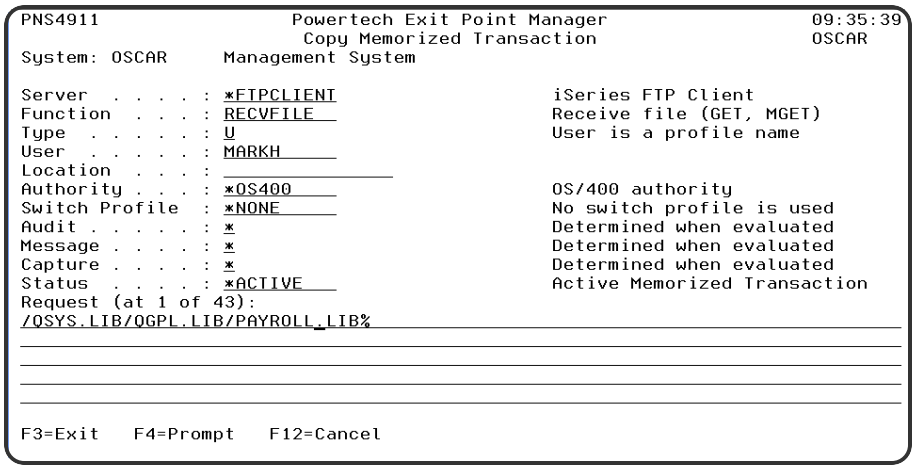
```
PNS4910S                 Powertech Exit Point Manager                 09:29:35
                        Memorized Transactions Subset                 OSCAR

Subset by:
  Server  . . . . . : *FTPCLIENT
  Function  . . . . : _________
  Location  . . . . : ____________________________________________________
  User  . . . . . . : __________
  Status  . . . . . : __________
  Transaction . . . : ____________________________________________________
  Case sensitive  . : _

Sort by (select one using an X):
  Server  . . . . . : X
  User  . . . . . . : _
  Location  . . . . : _
  Status  . . . . . : _
  Authority . . . . : _
  Request . . . . . : _



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

2. On the Work with Memorized Transactions panel, locate the transaction as close as possible to the kind of transaction you want to prohibit. Enter a **3** in the Opt column and press **Enter** to copy the transaction.

```
PNS4910                  Powertech Exit Point Manager                 09:33:39
                       Work with Memorized Transactions               OSCAR
System  . . . . . : OSCAR    Management System

Type options, press Enter
  2=Change  3=Copy  4=Delete  5=Display
Opt Server     Function   Typ User       Location         Authority Status
 _  *FTPCLIENT RECVFILE    U  ADAMS                        *REJECT  *ACTIVE
 3  *FTPCLIENT RECVFILE    U  BILL                         *OS400   *ACTIVE
 _  *FTPCLIENT SENDFILE    U  MARKH                        *REJECT  *ACTIVE
 _  *FTPCLIENT SENDFILE    U  MARKJ                        *OS400   *ACTIVE

                                                                      Bottom

F3=Exit  F5=Refresh  F7=Select System  F11=View2   F12=Cancel  F16=Sort/subset
F17=Top  F18=Bottom  F21=NS User Groups
The list is subsetted.
```

3. On the Copy Memorized Transaction panel, edit the transaction string to end with the % wildcard character, making the transaction generic. Then, edit the contents of the rule accordingly. For example, this new rule rejects user MARKH if he attempts to download any

object in the PAYROLL library.



Example 3: Add a Memorized Transaction for a Profile Group

> **NOTE:** In addition to using IBM i's group profiles as described here, Exit Point Manager also offers its own *NS Group Profiles*, which can be used to assign a rule to multiple user profiles at once. See Creating a User Group.

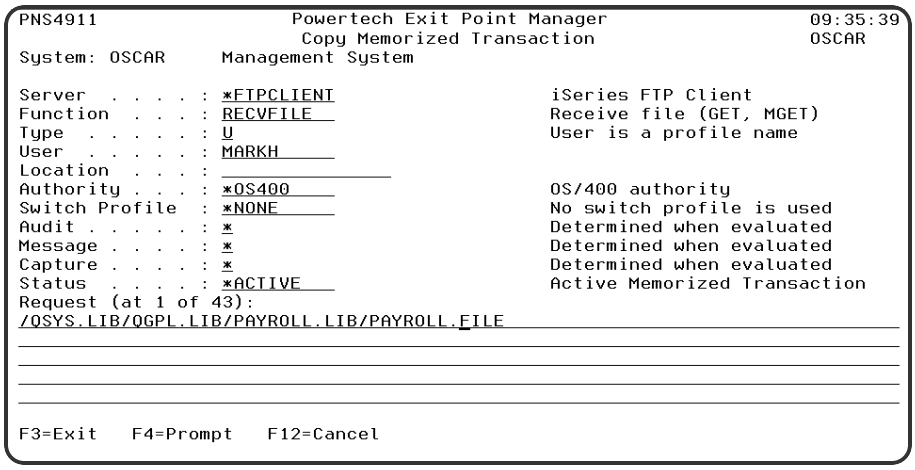
You can use Exit Point Manager memorized transactions for users and groups. Suppose you've secured access to the *FTPCLIENT function RECVFILE by setting authority for *PUBLIC to *REJECT. You can allow a single user or a group to GET information (use the RECVFILE function) by memorizing transactions.

> **NOTE:** To memorize a transaction for a user using the web browser interface, in the View Transaction screen, choose **Memorize > For User**, then choose the desired user in the User field of the New User Memorized Transaction dialog box.

Memorized transaction for a user

1. Copy the memorized transaction and modify it to allow the user to GET information (use RECVFILE) from the PAYROLL library. Although user MARKH is allowed to download the

payroll file using FTPCLIENT's GET subcommand, no one else is.

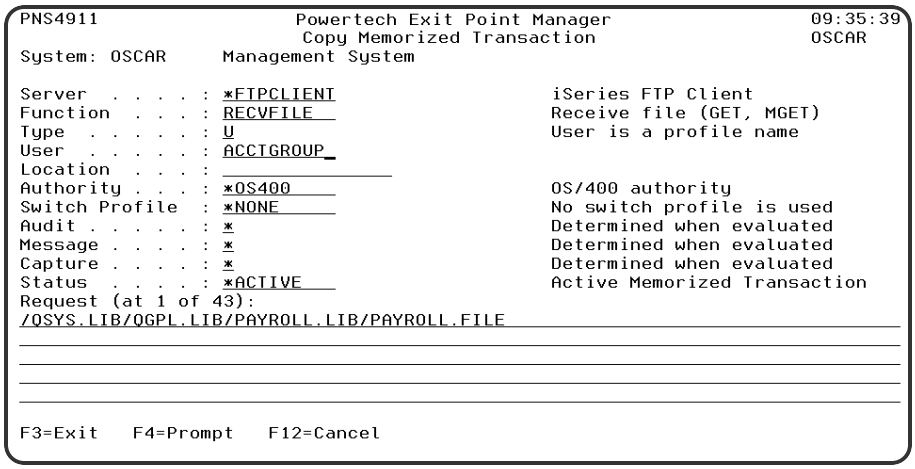


NOTE: To memorize a transaction for a group using the web browser interface, in the View Transaction screen, choose **Memorize > For Location**, then choose the desired IP Address Group in the Location field of the New Location Memorized Transaction dialog box.

Memorized transaction for a group

In the previous step, you secured the PAYROLL file from the FTPCLIENT GET command by everyone but MARKH. What if others also need to access the file? By creating a memorized transaction for a group, you authorize the members of that group to use the FTPCLIENT GET command against library PAYROLL.

2. To create a memorized transaction for a group, copy the memorized transaction. On the Copy Memorized Transaction panel, enter the name of the group, ACCTGROUP, in the User field and save the new memorized transaction.



Reports

Exit Point Manager provides a number of reports to help you document your exit point security and activity. These reports show the actions monitored by Exit Point Manager. Using the green screen, you can view spooled reports using the WRKSPLF (Work with Spooled Files) command, or press `F15`

on many Exit Point Manager screens. The Insite Web UI allows you to define, submit, and view reports all from your web browser.

> **NOTE:** Exit Point Manager submits most reporting jobs to the QBATCH job queue in library QGPL. To submit reports to a different job queue, use the following command:

CHGJOBD JOBD(POWERLOCK) JOBQ(*your-jobq-name*)

To display the Reports screen in the Insite web UI, click Reports in the Navigation Pane. The Reports screen allows you to define, edit, and submit reports.

To display the Reports Menu on the green screen, select option **80** on the Exit Point Manager Main Menu. The Reports Menu allows you to select from the following reports.

Granting Reporting Authority

The PTNSRPT authorization list grants authority to run Exit Point Manager reports. You can use the authorization list to authorize a programmer or other technical user to access report information without providing them with full configuration access.

To add profiles to the authorization list, enter the following command:

ADDAUTLE AUTL(PTNSRPT) USER(*myuser*) AUT(*USE)

Once users are added to the report authorization list, they have all the authorities needed to create Exit Point Manager reports. Users can display the Reports Menu with the following command:

PTNSLIB07/PLNSREPORT or **PTNSLIB/PLNSREPORT** (depending on your product library)

Working with Reports in Insite

The following topics describe how to create, edit, submit, and view reports using the HelpSystems Insite web browser interface.

Viewing, Sorting, and Filtering Reports

Viewing the Reports Page

To view the Reports page, click **Reports** under the Exit Point Manager menu. If the menu on the left is hidden, clicktap  in the upper left corner.

Things to know and do:

- The total number of saved reports in the list and the server they're on is displayed at the top of the page.
- Click the Refresh button  to refresh the information in the display.
- Click the page number and select the page you want to view. Or, click the previous and next arrows.
- Start typing in the Search field to find a specific report. It will find everything that contains what you're typing. See Sorting and filtering below to learn how to filter your search.

- "Shared" indicates whether or not others are allowed to see the report. You can change this preference in the report's settings. For instructions, see Adding or Editing Reports.
- Click **Add** to set up a new report for printing.

Actions you can take:

Click the Show Actions button by any report to display the following actions that you can take:

- Select **Preview** to build and open a report to preview its progress. The preview will open a new browser tab.
- Select **Schedule** to open the page where you can schedule the report for printing.
- Select **Submit** to immediately submit the report for printing.
- Select **Edit** to open the page where you can edit the report.

Sorting and Filtering the Display

There are settings for the Reports page that allow you to choose how to sort the list, and what types of data will be searched when you do a search.

Follow these steps:

1. Click the Settings button  .
2. Select how you want the list sorted (**Sort By**). Click your selection again to change the sort order to ascending or descending  .
3. Select one or more options under **Search By** to narrow the list of items displayed.
4. Click the Close button  to close the settings.

Adding or Editing a Saved Report

You can set up a Exit Point Manager report and save the setup so you can print it whenever you need to. For most reports, you can specify selection criteria, such as a date range. The criteria that's available varies depending on the report you choose.

> **NOTE:** Some of the following steps may not apply to the specific report you want to set up.

To add or edit a report:

1. Click **Reports** under the Exit Point Manager menu. If the menu on the left is hidden, clicktap  in the upper left corner.
2. To edit an existing report, find it and click its row.
3. To add a new report, click **Add**. Then, select the report you want to set up.
4. Enter a **Name** for the report.
5. Slide **Shared** to "On" if you want others to be able to work with and use this report.
6. Select the Transaction Type, User, or other report options. The values available here will depend on the report chosen. For more details on the various reports, see New/Edit Report screen.

- **Specific** - Choose this option if you want to specify a specific To and From date for the range of the report.
- **Non-specific** - Choose this option if you want to specify a relative To and From date for the range of the report (for example, transactions for the last two days).

7. For Date Range, choose from the following:
8. Click **Save**.

You can now preview the report, schedule the report for printing, or print the report immediately.

Deleting Reports

To delete a saved report:

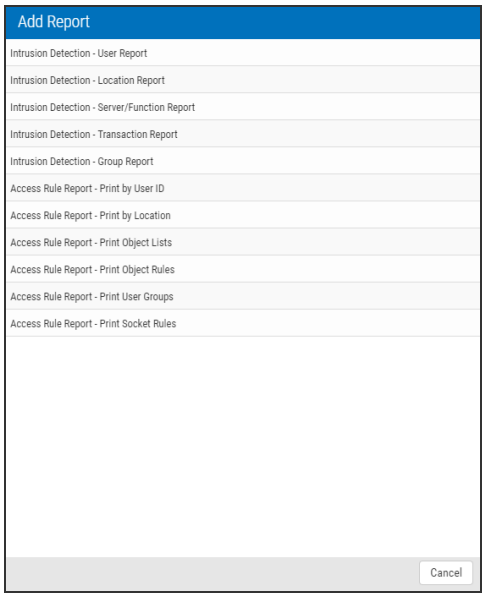
1. Click **Reports** under the Exit Point Manager menu. If the menu on the left is hidden, clicktap  in the upper left corner.
2. Select the reports you need to delete.
3. Click **Delete**.
4. Click **Delete** again when asked to confirm the deletion.

Reporting Access Attempts by User ID

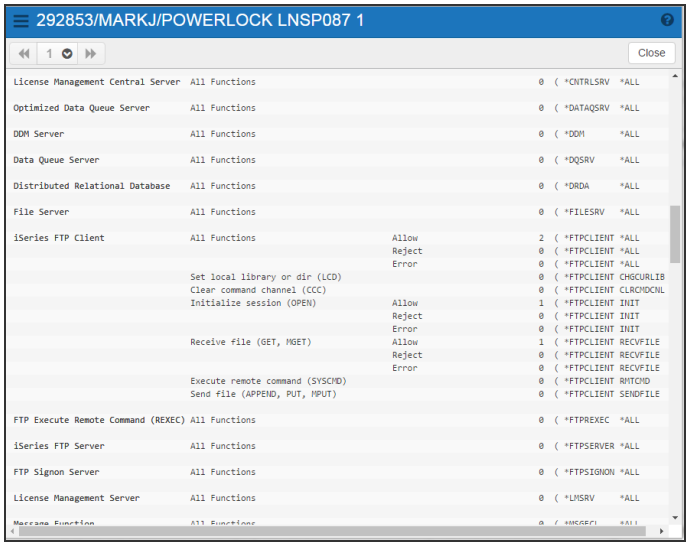
You can generate reports based on access attempts by user ID.

To create a report based on user access attempts

1. On the Navigation Pane, select **Reports**.
2. Click **Add** and choose **Intrusion Detection - Server/Function Report**.



3. Create the report using the following settings:
    - Name: "Server Function Report"
    - Transactions: *ALL
    - Server *ALL
    - Function: *ALL
    - For Date Range, specify the number of days you would like the report to include. For the first report, a week is usually a reasonable duration. For Date Range, choose Specific to indicate the report should include a specific start and end date. Choose Non Specific to include a period of time previous to the time the report is run.
    - For Detail Level, choose Summary.
4. Click **Save** to save the report. You return to the Reports screen.
5. Click  to the right of Server Function Report and choose **Submit**. A message should appear in the lower left indicating the report has been submitted successfully.
6. Click **Spooled Files** in the Navigation Pane.
7. The report you just submitted will be at the top of the list. Click it to view.



Working with Reports in the green screen

The following topics describe how to create, edit, submit, and view reports using the IBM i green screen.

Report Output Options

Each Exit Point Manager report allows you to specify an output type for the report. You can select from the following:

*PRINT (Insite web UI or green screen)

Creates a spooled file and sends the report to a print queue. You can view the report using the WRKSPLF command.

*OUTFILE (green screen only)

Directs the report output to an IBM i data file using the filename and library you specify when you submit the report.

*IFS (green screen only)

The report is output to a Comma Separated Value (.csv) file on the IBM i Integrated File System (IFS). The name of the directory is controlled by the Report Output Control file (PNSGRO in the product library). The default location for the IFS output is "ihome" followed by the name of the user running the report. You must specify the report name when you submit the report.

> **NOTE:** Exit Point Manager treats IFS output as a file name, not a path name. You cannot use path delimiters (i) to direct the output to another directory. If you include path delimiters (i) in your report name, they are converted to underscore characters.

Exit Point Manager uses the following sequence when adding a file to the IFS:

- The IFS Output File Name (report name) is appended to the path defined in the PNSGRO file. If the directory does not exist, it is created by Exit Point Manager.

  /home

- The user profile is appended to the path name:

  /home/USERID

- Appends a date and time stamp (CCYY-MM-DD-HH.MM.SS.mmm) to the file name to make it unique. You cannot specify Replace, Append or Cancel.

  If there is no path entry in PNSGRO, the reporting process creates a directory with the name of the user (in all caps), if one does not already exist:
  /USERID

Examples:

With PNSGRO set to the default value, the directory is:

/home/USERID/IFSOutputFileName_2010-06-14-12.42.09.987

Without PNSGRO, the directory is:

/USERID/IFSOutputFileName_2010-06-14-12.42.09.987

Exit Point Manager creates both a .csv and a .rpt file. The .rpt corresponds to a printed report's summary page.

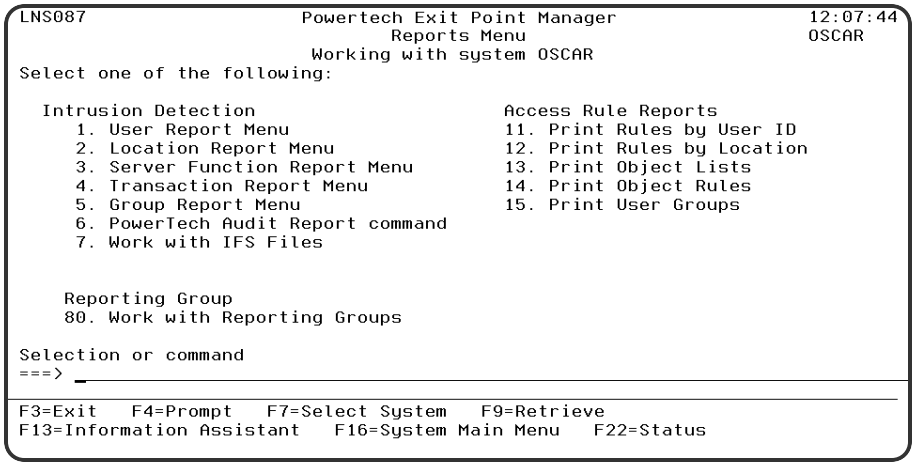
> **NOTE:** Selecting output types *OUTFILE or *IFS prints reports by Transaction only, regardless of the Detail, Transaction, or Summary setting (DITIS) you selected.

Reporting Access Attempts by User ID

You can generate reports based on access attempts by user ID.

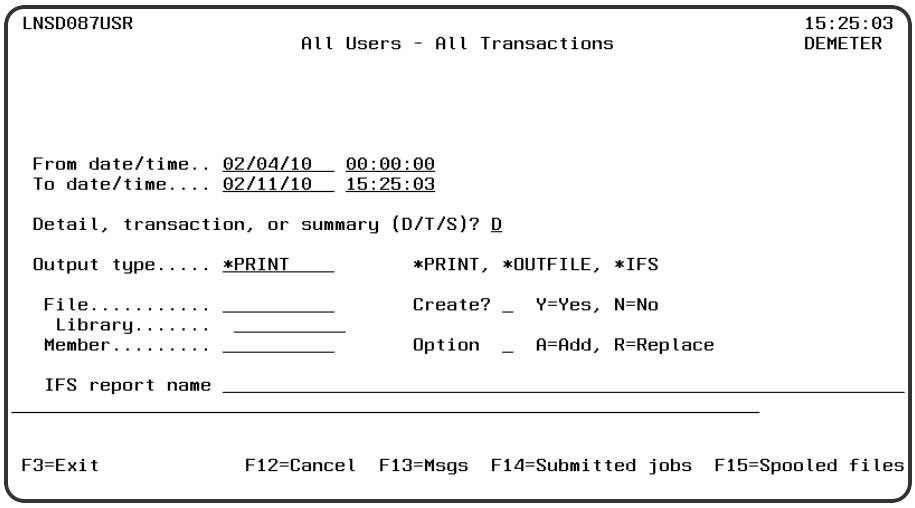
To create a report based on user access attempts - green screen

1. Select option **1** on the Reports Menu to display the User Report Menu where you can select the type of report to run.



   You can select to run a report for all users (options 1-3), or for a specific user (options 4-6). You also can select the types of transactions to include in the report: all transactions, allowed transactions only, or rejected transactions only.

2. To run a report, select an option to display the entry screen for the report type.



You can enter your selection criteria for the report, including:

From date/time • To date/time

The date range you want to include in the report.

Detail, transaction, or summary (D/T/S)

The level of detail to include in the report, from most detailed (transaction) to least detailed (summary).

Output type

The output type of the report. Possible values are:

***PRINT** The report is sent to the specified print queue.
***OUTFILE** The report is sent to a file. You must specify the file name and library for the report.

***IFS** The report is placed in the IFS. You must specify the report name.

File/Library/Member

The file name for the report, and the library for the file. Enter Y to create the report or N to not create a report. You also can specify if you want to add (A) to the file member, or replace (R) the existing member.

IFS report name

If you specified *IFS as the output type, enter a name for the report.

> **NOTE:** If you selected to create a report for a specific user (options 4-6), you're also asked to enter the user name.

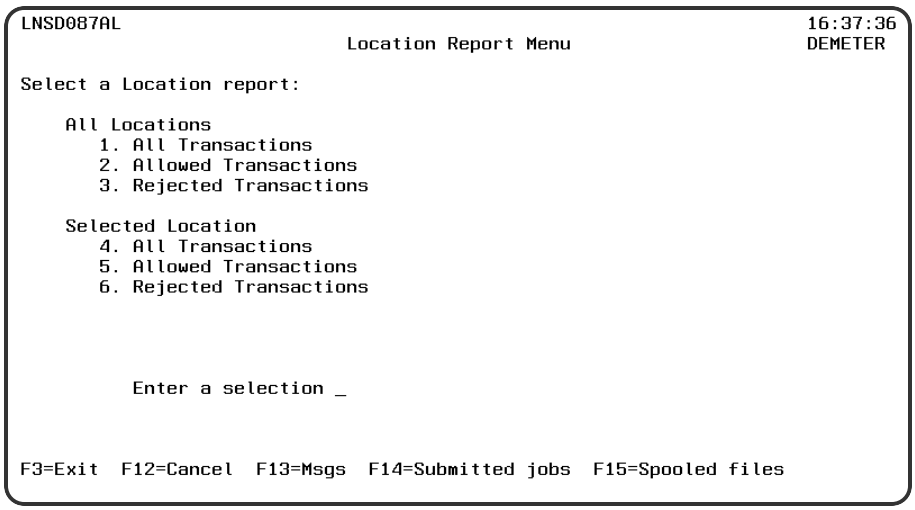
Reporting Access Attempts by Location

You can generate reports based on access attempts by location. Exit Point Manager refers to IP addresses and SNA device names as *locations*. Some servers, like FTP, send client IP address information to Exit Point Manager. Others can send IP address or SNA name information.

However, not all server programs communicate location information. The location reports allow you to see information on your servers that do provide location information.

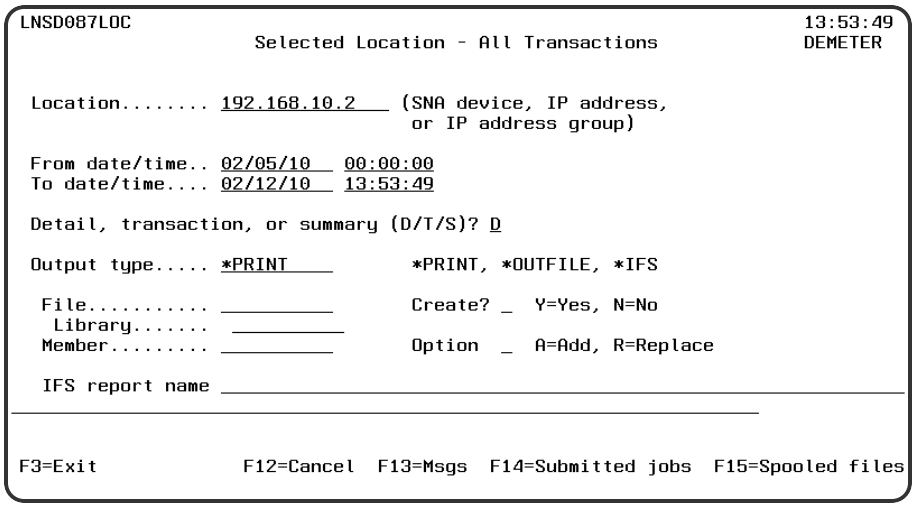
To create a report based on user access attempts

1. On the Reports menu, select option **2** to display the Location Report Menu where you can select the type of report to run.



2. You can select to run a report for all locations (options 1-3), or for a specific location (options 4-6). You also can select the types of transactions to include in the report: all transactions, allowed transactions only, or rejected transactions only.

3. To run a report, select an option to display the entry screen for the report type.



You can enter your selection criteria for the report, including:

From date/time • To date/time

The date range you want to include in the report.

Detail, transaction, or summary (D/T/S)

The level of detail to include in the report, from most detailed (transaction) to least detailed (summary).

Output type

The output type of the report. Possible values are:

***PRINT** The report is sent to the specified print queue.
***OUTFILE** The report is sent to a file. You must specify the file name and library for the report.
***IFS** The report is placed in the IFS. You must specify the report name.

File/Library/Member

The file name for the report, and the library for the file. Enter Y to create the report or N to not create a report. You also can specify if you want to add (A) to the file member, or replace (R) the existing member.

IFS report name

> **NOTE:** If you selected to create a report for a specific location (options 4-6), you're also asked to enter the location, which can be an SNA device name, an IP address, or an IP address group. Generic IP addresses (for example, 192.168.1*.*) also are supported. When you enter a generic IP address, Exit Point Manager reports transactions for any IP address that starts with the characters before the asterisk (*).

If you specified *IFS as the output type, enter a name for the report.

Reporting Access Attempts by Server / Function

Some of the network servers (such as FTP and Telnet) audited and controlled by Exit Point Manager have several functions that you can perform. For example, when you request the FTP GET subcommand, the FTP server runs the SENDFILE internal function. (See Appendix A for a list of all servers and functions that Exit Point Manager can audit and control.)

To create reports based on attempts to access an individual server, or server/function combination

1. Select option **3** on the Reports Menu to display the Server Function Report Menu.

```
LNSD087AS                                                        14:15:25
                        Server Function Report Menu              DEMETER

Select a SERVER report:

    All Servers All Functions
       1. All Transactions
       2. Allowed Transactions
       3. Rejected Transactions

    Selected Server All Functions
       4. All Transactions
       5. Allowed Transactions
       6. Rejected Transactions

    Selected Server Function
       7. All Transactions
       8. Allowed Transactions
       9. Rejected Transactions

          Enter a selection _

F3=Exit  F12=Cancel  F13=Msgs  F14=Submitted jobs  F15=Spooled files
```

   The Server Function reporting option in Exit Point Manager sorts the Journal by Server/Function and allows you to select a Specific Server and a Specific Function. Date range and type of transactions to be viewed can also be specified to narrow or expand the report to your specific requirements.

   You can select to run a report for all servers and all functions (options 1-3), for all functions on a specific server (options 4-6), or for a specified function on a server (options 7-9). You also can select the types of transactions to include in the report: all transactions, allowed transactions only, or rejected transactions only.

2. To run a report, select an option to display the entry screen for the report type.

```
LNSD087SVF                                                       14:29:08
              Selected Server Function - All Transactions        DEMETER


 Server.......... *FTPSERVER
  Function....... SENDFILE

 From date/time.. 02/05/10   00:00:00
 To date/time.... 02/12/10   14:29:08

 Detail, transaction, or summary (D/T/S)? D

 Output type..... *PRINT      *PRINT, *OUTFILE, *IFS

  File........... __________  Create? _  Y=Yes, N=No
   Library.......  __________
  Member......... __________  Option  _  A=Add, R=Replace

  IFS report name _____________________________________________________
_____________________________


F3=Exit  F4=Prompt  F12=Cancel  F13=Msgs  F14=Submitted jobs  F15=Spooled files
```

You can enter your selection criteria for the report, including:

From date/time • To date/time
The date range you want to include in the report.

Detail, transaction, or summary (D/T/S)
The level of detail to include in the report, from most detailed (transaction) to least detailed (summary).

Output type
The output type of the report. Possible values are:

***PRINT** The report is sent to the specified print queue.
***OUTFILE** The report is sent to a file. You must specify the file name and library for the report.
***IFS** The report is placed in the IFS. You must specify the report name.

File/Library/Member
The file name for the report, and the library for the file. Enter Y to create the report or N to not create a report. You also can specify if you want to add (A) to the file member, or replace (R) the existing member.

IFS report name

> **NOTE:** If you selected to create a report for a specific server (options 4-6) or a specific function on a server (options 7-9), you're also asked to enter the server/function names.

If you specified *IFS as the output type, enter a name for the report.

Reporting Transactions

Network tools like FTP, ODBC, DDM, and Remote SQL pose serious security risks to your IBM i system. For example, each of these network tools can access and change database files, run programs and commands, and even modify objects. Exit Point Manager is designed to audit and report on access attempts by these tools, and to control access according to the rules you've specified.

To create reports based on attempts to run commands and programs, to access or manipulate data, or to modify objects

1. Select option **4** on the Reports Menu to display the Transaction Report Menu.

```
LNSD087AC                                                       14:39:22
                          Transaction Report Menu               DEMETER

Select a transaction type report:


    Network Transactions that:
       1. Run commands and programs
       2. Update data
       3. Read data
       4. Modify objects



           Enter a selection  _



F3=Exit  F12=Cancel  F13=Msgs  F14=Submitted jobs  F15=Spooled files
```

2. Select the desired option on the Transaction Report Menu. Each of the four options displays a report entry screen where you can enter the selection criteria for the report.

```
LNSD087TR                                                       15:04:44
                    Network Transactions that Run Programs      DEMETER




 From date/time.. 02/05/10   00:00:00
 To date/time.... 02/12/10   15:04:44

 Detail, transaction, or summary (D/T/S)? D

 Output type..... *PRINT      *PRINT, *OUTFILE, *IFS

  File.......... __________   Create? _  Y=Yes, N=No
   Library.......  __________
  Member......... __________   Option  _  A=Add, R=Replace

  IFS report name _____________________________________________________
_____________________________________________


F3=Exit            F12=Cancel  F13=Msgs  F14=Submitted jobs  F15=Spooled files
```

The transaction report entry screens ask for the following information:

From date/time • To date/time

The date range you want to include in the report.

Detail, transaction, or summary (D/T/S)

The level of detail to include in the report, from most detailed (transaction) to least detailed (summary).

Output type

The output type of the report. Possible values are:

***PRINT** The report is sent to the specified print queue.
***OUTFILE** The report is sent to a file. You must specify the file name and library for the report.
***IFS** The report is placed in the IFS. You must specify the report name.

File/Library/Member
The file name for the report, and the library for the file. Enter Y to create the report or N to not create a report. You also can specify if you want to add (A) to the file member, or replace (R) the existing member.

IFS report name
If you specified *IFS as the output type, enter a name for the report.

Reporting Access Attempts by Groups of Users

The Group Report Menu allows you to create reports by accounting code, operating system group profile, or Powertech group.

To create reports based on groups of users.

1. Select option **5** on the Reports Menu to display the Group Report Menu.

```
LNSD087AG                                                        15:13:30
                            Group Report Menu                    DEMETER

Select a GROUP report:

    All Groups
       1. All Transactions
       2. Allowed Transactions
       3. Rejected Transactions

    Selected Group
       4. All Transactions
       5. Allowed Transactions
       6. Rejected Transactions



          Enter a selection _


F3=Exit  F12=Cancel  F13=Msgs  F14=Submitted jobs  F15=Spooled files
```

   You can select to run a report for all groups of a specified type (options 1-3), or for a specific group (options 4-6). You also can select the types of transactions to include in the report: all transactions, allowed transactions only, or rejected transactions only.

2. To run a report, select an option to display the entry screen for the report type.

```
LNSD087GS                                                        15:18:10
                     Selected Group - All Transactions           DEMETER


 Group........... MARKETING_____  Group Name/*NOGRP
 Group Type...... P (P/A/O)  PowerTech Group/Account Code/OS400 Group Profile

 From date/time.. 02/05/10__ 00:00:00
 To date/time.... 02/12/10__ 15:18:10

 Detail, transaction, or summary (D/T/S)? D

 Output type..... *PRINT____       *PRINT, *OUTFILE, *IFS

  File........... __________       Create? _  Y=Yes, N=No
   Library.......  __________
  Member......... __________       Option  _  A=Add, R=Replace

  IFS report name ____________________________________________________________
_____


F3=Exit            F12=Cancel  F13=Msgs  F14=Submitted jobs  F15=Spooled files
```

You can enter your selection criteria for the report, including:

From date/time • To date/time
The date range you want to include in the report.

Detail, transaction, or summary (D/T/S)
The level of detail to include in the report, from most detailed (transaction) to least detailed (summary).

Output type
The output type of the report. Possible values are:

***PRINT** The report is sent to the specified print queue.
***OUTFILE** The report is sent to a file. You must specify the file name and library for the report.
***IFS** The report is placed in the IFS. You must specify the report name.

> **NOTE:** If you selected to create a report for All Groups (options 1-3), you're asked to enter the group type. If you selected to create a report for a specific group (options 4-6), you're also asked to enter the group name or accounting code.

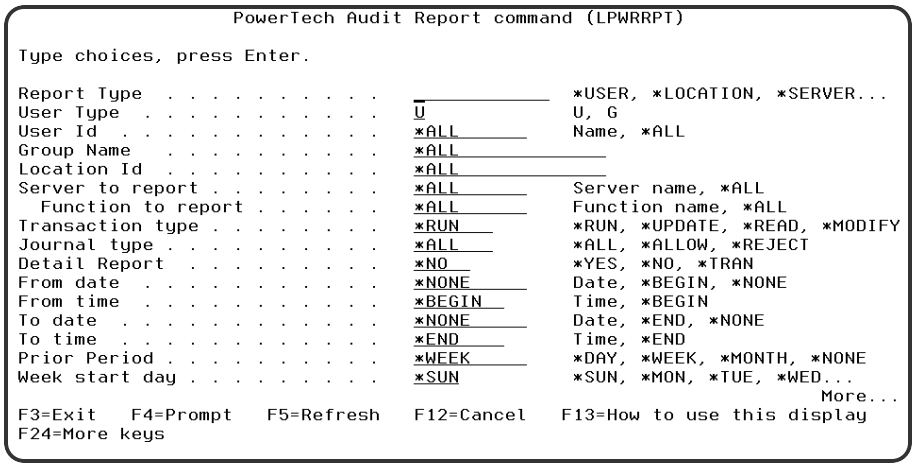
File/Library/Member
The file name for the report, and the library for the file. Enter Y to create the report or N to not create a report. You also can specify if you want to add (A) to the file member, or replace (R) the existing member.

IFS report name
If you specified *IFS as the output type, enter a name for the report.

Using the Audit Report Command (LPWRRPT)

In addition to running reports from the Reports Menu, you also can use the LPWRRPT command to run reports from your own programs, or to include Exit Point Manager reporting in your job scheduler.

To display the LPWRRPT command prompt panel, enter the command on a command line and press **F4**, or select option **7**, Powertech Audit Report command, on the Reports Menu.



Specify the report type you want to run and press `Enter`. The parameters for that report type display, allowing you to specify your selection criteria.

See Powertech Audit Report Command panel for a complete description of all the command parameters.

Command Keys

F3 (Exit): Exit the panel without processing any pending changes.

F4 (Prompt): Displays a list of possible values from which you may select one.

F5 (Refresh): Refreshes the panel and resets all available text fields.

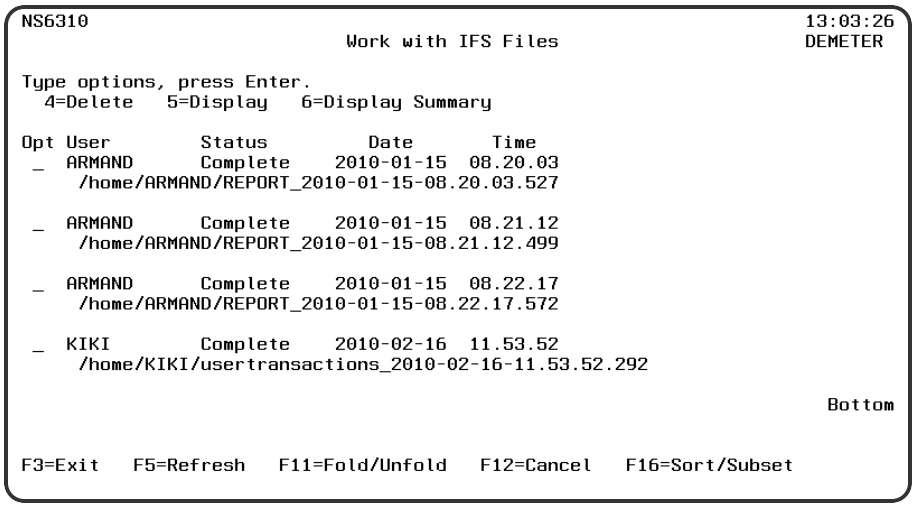
F12 (Cancel): Exit the panel without processing any pending changes.

F13 (How to use this display): Shows help for the prompt display or associated display you are currently using.

F24 (More keys): Shows additional function keys that can be used for this display.

Work with IFS Files

When you specify an output type of *IFS on any of the report selection entry panels, you must specify an IFS file name. The Work with IFS Files panel allows you to work with the IFS files produced when you run the reports. To display the Work with IFS Files panel, select option **10** on the Reports Menu.



The Work with IFS Files panel displays the name of the user who ran the report, the report status, the date and time the report was run, and the name of the IFS file produced. Press `F11` to display or hide the file name information. Press `F16` to sort the IFS files listed on the panel.

You can select from the following options for an IFS file:

4=Delete

Deletes the file from the IFS directory.

5=Display

Displays the Display Object Links panel, from which you can display the .csv file.

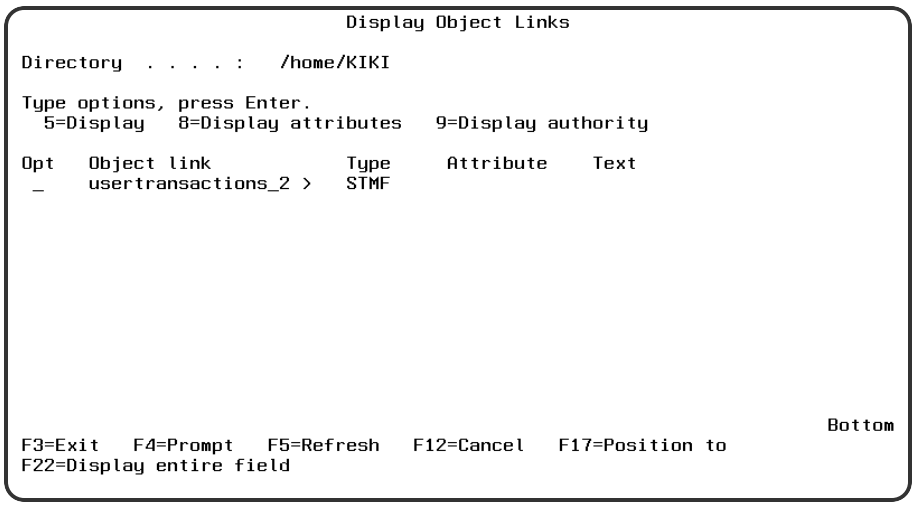
6=Display Summary

Displays the Display Object Links panel, from which you can display the .rpt file.

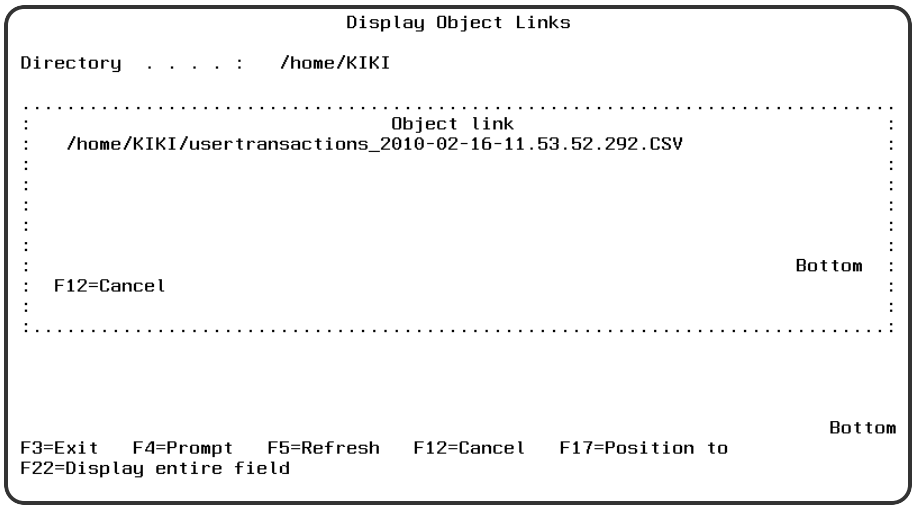
Displaying an IFS File

When you select option **5**, Display, or option **6**, Display Summary, on the Work with IFS Reports panel, the Display Object Links panel displays.

The Display Object Links panel lists the names of objects in a directory and allows you to see additional information about those objects.



Press **F22**, Display entire field, to display a window that contains the full path IFS file name of the file produced when you ran the report.



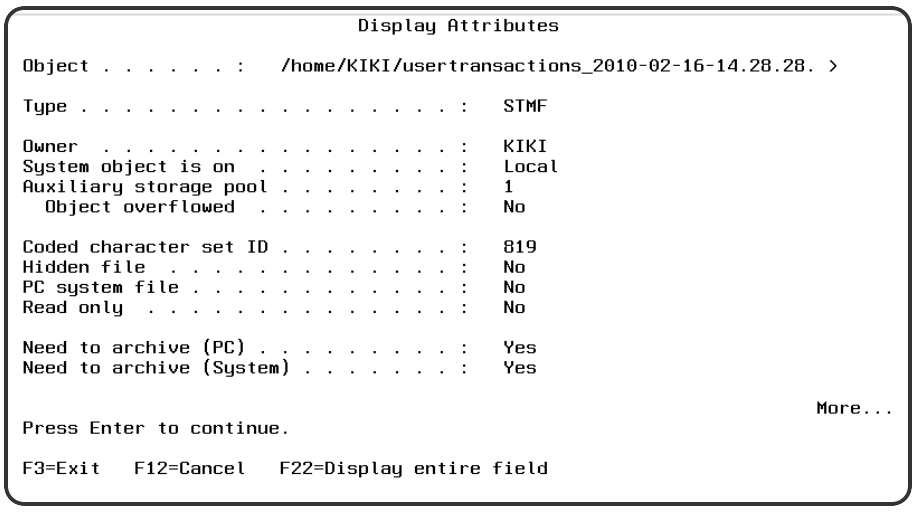
You can select from the following options on the Display Object Links panel:

Option 5 = Display

Displays your report data.

Option 8 = Display attributes

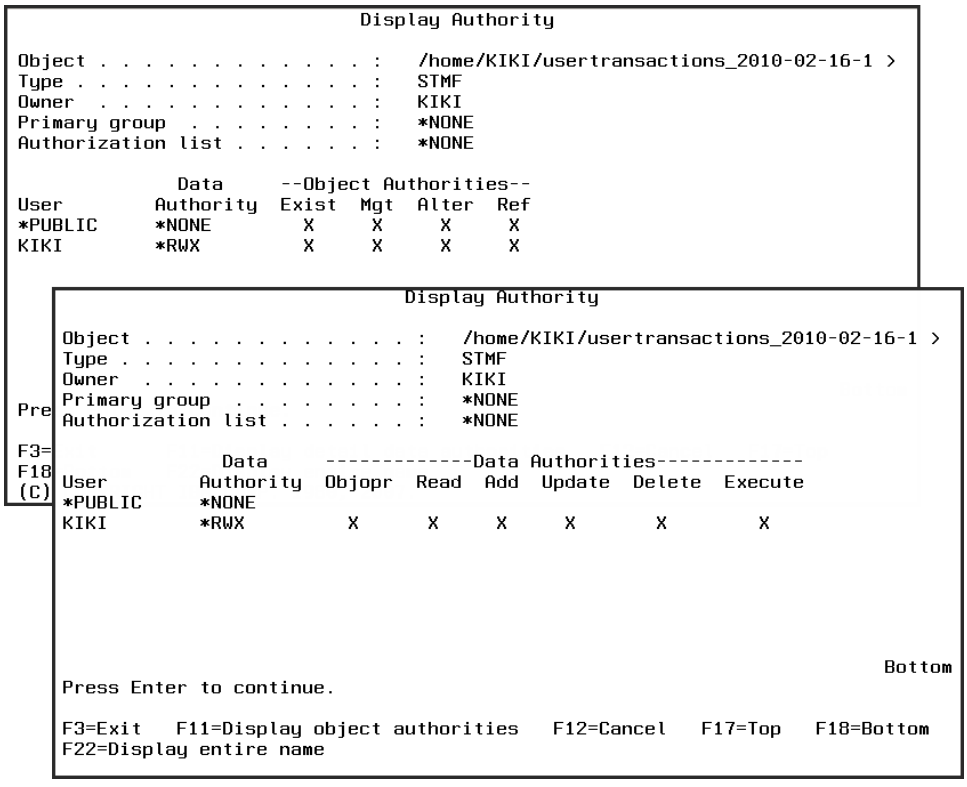
Displays the Display Attributes panel, which shows the attributes of an object. Page down to see all the attributes for the selected file.



```
                          Display Attributes

Object . . . . . :   /home/KIKI/usertransactions_2010-02-16-14.28.28. >

Type . . . . . :   STMF

Owner  . . . . . :   KIKI
System object is on  . . . . . :   Local
Auxiliary storage pool . . . . . :   1
  Object overflowed  . . . . . :   No

Coded character set ID . . . . . :   819
Hidden file  . . . . . :   No
PC system file . . . . . :   No
Read only  . . . . . :   No

Need to archive (PC) . . . . . :   Yes
Need to archive (System) . . . . . :   Yes

                                                                      More...
Press Enter to continue.

F3=Exit   F12=Cancel   F22=Display entire field
```

Option 9 = Display Authority

Displays the Display Authority panel, which shows a list of users that have authority to the requested object and the users' authorities. It also shows the public authority, owner authority, and primary group authority. Press `F11` to switch between system-defined object authorities and data authorities.

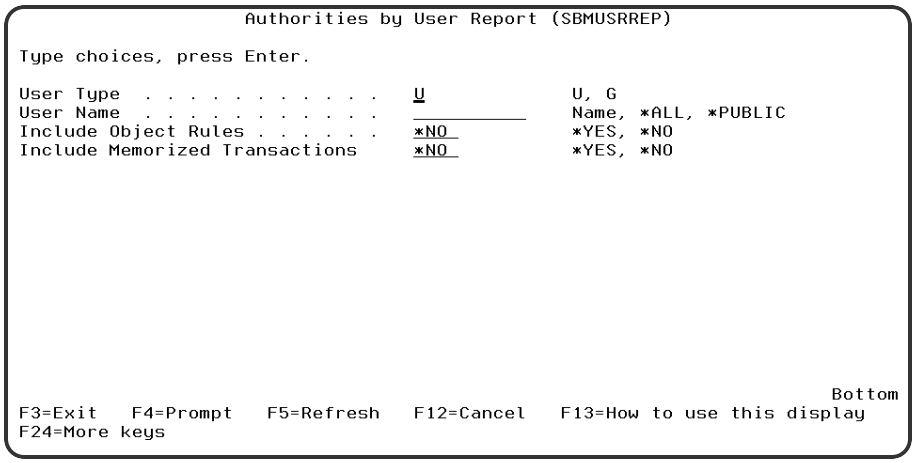


```
                          Display Authority

Object . . . . . :   /home/KIKI/usertransactions_2010-02-16-1 >
Type . . . . . :   STMF
Owner  . . . . . :   KIKI
Primary group  . . . . . :   *NONE
Authorization list . . . . . :   *NONE

             Data     --Object Authorities--
User        Authority  Exist  Mgt  Alter  Ref
*PUBLIC     *NONE        X     X     X     X
KIKI        *RWX         X     X     X     X
```

```
                          Display Authority

Object . . . . . :   /home/KIKI/usertransactions_2010-02-16-1 >
Type . . . . . :   STMF
Owner  . . . . . :   KIKI
Primary group  . . . . . :   *NONE
Authorization list . . . . . :   *NONE

             Data     -------------Data Authorities-------------
User        Authority  Objopr  Read  Add  Update  Delete  Execute
*PUBLIC     *NONE
KIKI        *RWX         X      X     X     X       X        X

                                                                      Bottom
Press Enter to continue.

F3=Exit   F11=Display object authorities   F12=Cancel   F17=Top   F18=Bottom
F22=Display entire name
```

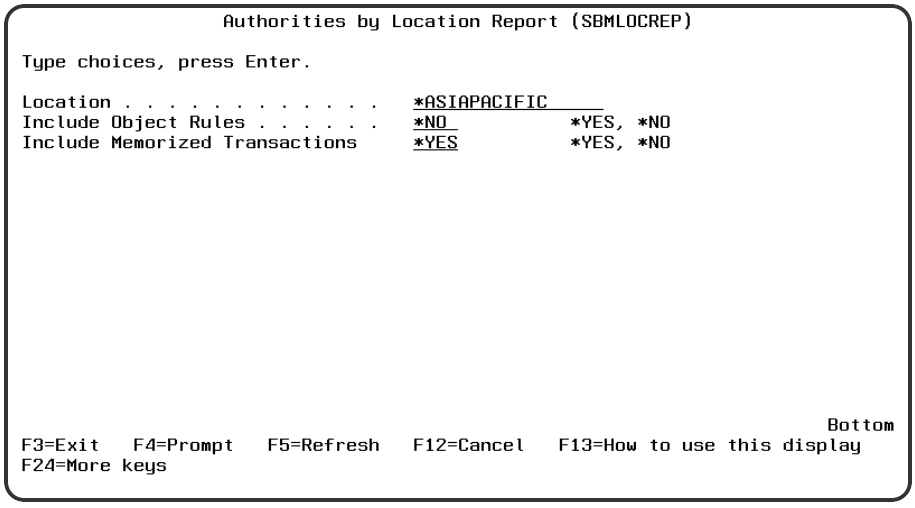
Printing Rules by User ID

You can use the Reports menu to print access rules by the location to which they apply. A location can be an IP address, an IP address group, or an SNA device name. To create a report by location, select option **12**, Print Rules by Location, on the Reports Menu to display the Authorities by Location Report (SBMLOCREP) prompt screen. You also can enter the SBMLOCREP command on a command line and press **F4** to display the prompt screen.



Printing Rules by Location

You can use the Reports menu to print access rules by the location to which they apply. A location can be an IP address, an IP address group, or an SNA device name. To create a report by location, select option **12**, Print Rules by Location, on the Reports Menu to display the Authorities by Location Report (SBMLOCREP) prompt screen. You also can enter the SBMLOCREP command on a command line and press **F4** to display the prompt screen.



Print Object List

The Print Object List (PRTOBJL) command allows you to print a listing of the Object Lists you have configured. The Object List Entries can be printed, as well as the Object Rules that protect a given Object List.

```
                        Print Object List (PRTOBJL)

Type choices, press Enter.

Subset by:
  Object List  . . . . . .   ACCOUNTING    ASID, NEWIASP, SIDLIST
  Type . . . . . .           Q             Q, I
  ASP Group  . . . . . .     *SYSBAS       Character value
  Description  . . . . . .   Restricted accounting files
Sort by:
  Object List  . . . . . > 1               1-3, *NO
  ASP Group  . . . . . > 2                 1-3, *NO
  Description  . . . . . > 3               1-3, *NO
Include Entries  . . . . .   *YES          *YES, *NO
Include Usage  . . . . . .   *YES          *YES, *NO




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

Options

Subset by (SUBSET):

This is a multi-part parameter consisting of three elements. If you leave any of the elements blank, the report will not be subset using that element. The elements are:

Object List

Specify criteria to subset by Object List name. You can use the Generic Character to indicate that a partial value is to be used for selection. In some circumstances you may also use the Wildcard Character to indicate that a partial value is to be used for selection.

Type

Specify criteria to subset by Object List Type.

ASP Group

Specify criteria to subset by ASP.

Description

Specify criteria to subset by Object List Description. You can use the Generic Character to indicate that a partial value is to be used for selection. In some circumstances you may also use the Wildcard Character to indicate that a partial value is to be used for selection.

Sort by (SORTBY)

This is a multi-part parameter consisting of three elements. Indicate the order in which you would like the Object Lists to be listed on the report. To omit an element from the sort, specify *NO for that element.

The elements are:

Object List

Specify the sort order for Object List name.

Type

Specify the sort order for Object List Description.

iASP

Specify criteria to subset by iASP.

Description

Specify the sort order for the Object List description.

Include Entries (INCLENT)

Specify if you want to include Object List entries for each Object List in the report. The default value is *YES.

Include Usage (INCLUSG)

> **NOTE:** If you specify *YES for Include Entries and Include Usage, additional fields display allowing you to further sort and subset the information to appear in the report.

Indicate whether you would like the Object List Usage information for each Object list to be printed on the report. If you specify *NO, do not enter any subset or sorting criteria for Object List Usage information.

The valid values are:

***YES** The Object List Usage information is printed on the report.
***NO** The Object List Usage information is not printed on the report.

Object List Entries (ENTRIES)

This is a multi-part parameter consisting of two groups of elements, one for subsetting the report and one for sorting it. This parameter is valid only when INCLENT(*YES) is specified on the command.

The elements are:

Subset by

This is a multi-part parameter consisting of four elements. If you leave any of the elements blank, the report will not be subset using that element.

The elements are:

Library

Specify criteria to subset by Library name. You can use the generic character to indicate that a partial value is to be used for selection. In some circumstances you may also use the wildcard character to indicate that a partial value is to be used for selection. You may specify <UNKNOWN> to select Object List Entries that pertain only to unqualified objects whose library cannot be determined.

Object

Specify criteria to subset by Object name. You can use the generic character to indicate that a partial value is to be used for selection. In some circumstances you may also use the wildcard character to indicate that a partial value is to be used for selection.

Type

Specify criteria to subset by Object Type.

Path

Specify criteria to subset by Path. You can use the generic character to indicate that a partial value is to be used for selection. In some circumstances you may also use the wildcard character to indicate that a partial value is to be used for selection.

Sort by

This is a multi-part parameter consisting of four elements. Indicate the order in which you would like the Object List Entries to be listed on the report. To omit an element from the sort, specify *NO for that element.

The elements are:

Library

Specify the sort order for Library name.

Object

Specify the sort order for Object name.

Type

Specify the sort order for Object Type.

Path

Specify the sort order for Path.

Object List Usage (USAGE)

This is a multi-part parameter consisting of three groups of elements, one for subsetting the report, one for broadly selecting User or Location rules, and one for sorting the report. This parameter is valid only when INCLUSG(*YES) is specified on the command.

The elements are:

Subset by

This is a multi-part parameter consisting of five elements. If you leave any of the elements blank, the report will not be subset using that element.

The elements are:

Location

Specify criteria to subset by Location. Location represents the source of a transaction. Location can hold an IP Address, an IP Address Group or the name of an SNA Communications Device. The special value *ALL, when used on a rule, means that the rule applies to any rule means that the rule applies to any Location lacking a specific rule. when used as a subset or selection parameter, *ALL generally means to select all such rules for display or printing. You can use the Generic Character to indicate that a partial value is to be used for selection. In some circumstances you may also use the wildcard character to indicate that a partial value is to be used for selection.

Style of Location value

When the value you key begins with an asterisk, this element allows you to format your request to find a single IP Address Group or any Location value that ends with the value you keyed (after the asterisk).

Valid values are:

***GROUP** List only rules that have the specified IP Address Group on them.
***ENDSWITH** List rules with any value that ends with the value you keyed.

Operation

Specify criteria to subset by operation.

Show rules for

This is a multi-part parameter consisting of two elements. This parameter allows you to show Object List Usage information listing only Location-based or User-based Object Rules. At least one of these elements must be *YES when you have specified INCLUSG(*YES).

The elements are:

Location

Indicate whether you want Location—based Object Rules to appear in the Usage section of the report. If you have specified subset criteria for Location, this value must be *YES. The valid values are:

***YES** Location—based Object Rules will be included.
***NO** Location—based Object Rules will not be included.

User

Indicate whether you want User—based Object Rules to appear in the Usage section of the report. If you have specified subset criteria for User, this value must be *YES. The valid values are:

***YES** User—based Object Rules will be included.
***NO** User—based Object Rules will not be included.

Sort by

This is a multi-part parameter consisting of three elements. Indicate the order in which you would like the Object List Usage information to be listed on the report. To omit an element from the sort, specify *NO for that element.

The elements are:

Location

Specify the sort order for Location. If you specified *NO for Show rules for Locations then this value must be *NO.

User

Specify the sort order for User. If you specified *NO for Show rules for Users then this value must be *NO.

Operation

Specify the sort order for Operation.

Command Keys

F3 (Exit): Exit the screen without processing any pending changes.

F4 (Prompt): Displays a list of possible values from which you may select one.

F5 (Refresh): Refreshes the screen and resets all available text fields.

F12 (Cancel): Exit the screen without processing any pending changes.

F13 (How to use this display): Shows help for the prompt display or associated display you are currently using.

F24 (More keys): Shows additional function keys that can be used for this display.

Print Object Rules

The Print Object Rule (PRTOBJRUL) command allows you to print a listing of the Object Rules you have configured. The Object List Entries contained in the Object List named on the rule can also be listed.

```
                      Print Object Rule (PRTOBJRUL)

Type choices, press Enter.

Subset by:
  Location . . . . . .  _________________
  Style of Location value  . . .  *ENDSWITH     *GROUP, *ENDSWITH
  User . . . . . .  __________     Character value
  Style of User value  . . . . .  *ENDSWITH     *PUBLIC, *ENDSWITH
  Object List  . . . . . .  __________     ACCOUNTING, FTPFILES...
  Operation  . . . . . .  _______     *ALL, *CREATE, *READ...
Show rules for:
  Locations  . . . . . .  *YES          *YES, *NO
  Users  . . . . . .  *YES          *YES, *NO
Sort by:
  Location . . . . . .  1_____         1-4, *NO
  User . . . . . .  2_____         1-4, *NO
  Object List  . . . . . .  3_____         1-4, *NO
  Operation  . . . . . .  4_____         1-4, *NO
Include Entries  . . . . . .  *NO_          *YES, *NO
                                                                    Bottom
F3=Exit   F4=Prompt   F5=Refresh   F12=Cancel   F13=How to use this display
F24=More keys
```

Options

Subset by (SUBSET):

Use this parameter to subset the Object Rules printed on the report. This is a multi-part parameter consisting of six elements. If you leave any of the elements blank, the report will not be subset using that element. The elements are:

Location

Specify criteria to subset by Location. Location represents the source of a transaction. Location can hold an IP Address, an IP Address Group or the name of an SNA Communications Device. The special value *ALL, when used on a rule, means that the rule applies to any rule means that the rule applies to any Location lacking a specific rule. when used as a subset or selection parameter, *ALL generally means to select all such rules for display or printing. You can use the generic character to indicate that a partial value is to be used for selection. In some circumstances you may also use the wildcard character to indicate that a partial value is to be used for selection.

Style of Location value

When the value you key begins with an asterisk, this element allows you to format your request to find a single IP Address Group or any Location value that ends with the value you keyed (after the asterisk).

Valid values are:

***GROUP** List only rules that have the specified IP Address Group on them.
***ENDSWITH** List rules with any value that ends with the value you keyed.

User

Specify criteria to subset by User. User represents the identity of the person initiating a transaction as a user profile. The special value *PUBLIC, when used on a rule, means that the rule applies to any User lacking a specific rule. when used as a subset or selection parameter, *PUBLIC means to select all such rules for display or printing.

You can use the generic character to indicate that a partial value is to be used for selection. In some circumstances you may also use the wildcard character to indicate that a partial value is to be used for selection.

Style of User value

When the value you key is *PUBLIC, this element allows you to format your request to find only rules for *PUBLIC or any User value that ends with PUBLIC (like JIMPUBLIC, XPUBLIC, etc).

Valid values are:

***PUBLIC** List only rules that have *PUBLIC as the User value.
***ENDSWITH** List rules with any value that ends with PUBLIC.

Object List

Specify criteria to subset by Object list name. You can use the generic character to indicate that a partial value is to be used for selection. In some circumstances you may also use the wildcard character to indicate that a partial value is to be used for selection.

Operation

Specify criteria to subset by Operation.

Show rules for (SHOWFOR)

Use this parameter to include only Location—based rules or User—based rules in the report. You must select at least one by specifying *YES. This is a multi-part parameter consisting of two elements.

The elements are:

Locations

Indicate whether you want Location—based Object Rules to appear in the report. The valid values are:

***YES** Location—based Object Rules will be included.
***NO** Location—based Object Rules will not be included.

User

Indicate whether you want User—based Object Rules to appear in the report.

The valid values are:

***YES** User—based Object Rules will be included.
***NO** User—based Object Rules will not be included.

Sort by (SORTBY)

Use this parameter to sort the Object Rules printed on the report. Indicate the order in which you would like the Object Rules listed on the report. To omit an element from the sort, specify *NO for that element. Duplicate values are not allowed; you cannot sort more than one field at any given position. This is a multi-part parameter consisting of four elements.

The elements are:

Location

Specify the sort order for Location.

User

Specify the sort order for User.

Object List

Specify the sort order for Object List name.

Operation

Specify the sort order for Operation.

> NOTE: If you specify *YES for Include Entries and Include Usage, additional fields display allowing you to further sort and subset the information to appear in the report.

Include Entries (INCLENT)

Indicate whether you would like the Object List Entries for each Object list to be printed on the report. The valid values are:

***YES** The Object List Entries are printed on the report.
***NO** The Object List Entries are not printed on the report.

Object List Entries (ENTRIES)

This is a multi-part parameter consisting of two groups of elements, one for subsetting the report and one for sorting it. This parameter is valid only when INCLENT(*YES) is specified on the command.

The elements are:

Subset by

This is a multi-part parameter consisting of four elements. If you leave any of the elements blank, the report will not be subset using that element.

The elements are:

Library

Specify criteria to subset by Library name. You can use the generic character to indicate that a partial value is to be used for selection. In some circumstances you may also use the wildcard character to indicate that a partial value is to be used for selection. You may specify <UNKNOWN> to select Object List Entries that pertain only to unqualified objects whose library cannot be determined.

Object

Specify criteria to subset by Object name. You can use the generic character to indicate that a partial value is to be used for selection. In some circumstances you may also use the wildcard character to indicate that a partial value is to be used for selection.

Type

Specify criteria to subset by Object Type.

Path

Specify criteria to subset by Path. You can use the generic character to indicate that a partial value is to be used for selection. In some circumstances you may also use the wildcard character to indicate that a partial value is to be used for selection.

Sort by

This is a multi-part parameter consisting of four elements. Indicate the order in which you would like the Object List Entries to be listed on the report. To omit an element from the sort, specify *NO for that element.

The elements are:

Library

Specify the sort order for Library name.

Object

Specify the sort order for Object name.

Type

Specify the sort order for Object Type.

Path

Specify the sort order for Path.

Command Keys

F3 (Exit): Exit the screen without processing any pending changes.

F4 (Prompt): Displays a list of possible values from which you may select one.

F5 (Refresh): Refreshes the screen and resets all available text fields.

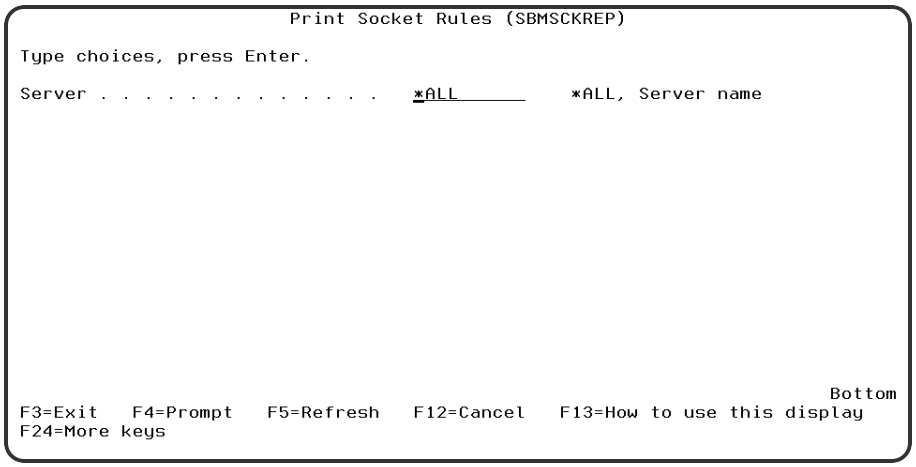
F12 (Cancel): Exit the screen without processing any pending changes.

F13 (How to use this display): Shows help for the prompt display or associated display you are currently using.

F24 (More keys): Shows additional function keys that can be used for this display.

Print Socket Rules

The Socket Rules Report (SBMSCKREP) command produces the "Socket Rules" report. This report lists Socket Rules and their Conditions.



Options

Server (SERVER)

Selects the server for which the rules are to print.

Allowed values are:

QSOLISTEN The report prints rules for the QSOLISTEN server.
QSOCONNECT The report prints rules for the QSOCONNECT server.
QSOACCEPT The report prints rules for the QSOACCEPT server.
***ALL** The report prints rules for the all servers.

Command Keys

F3 (Exit): Exit the screen without processing any pending changes.

F4 (Prompt): Displays a list of possible values from which you may select one.

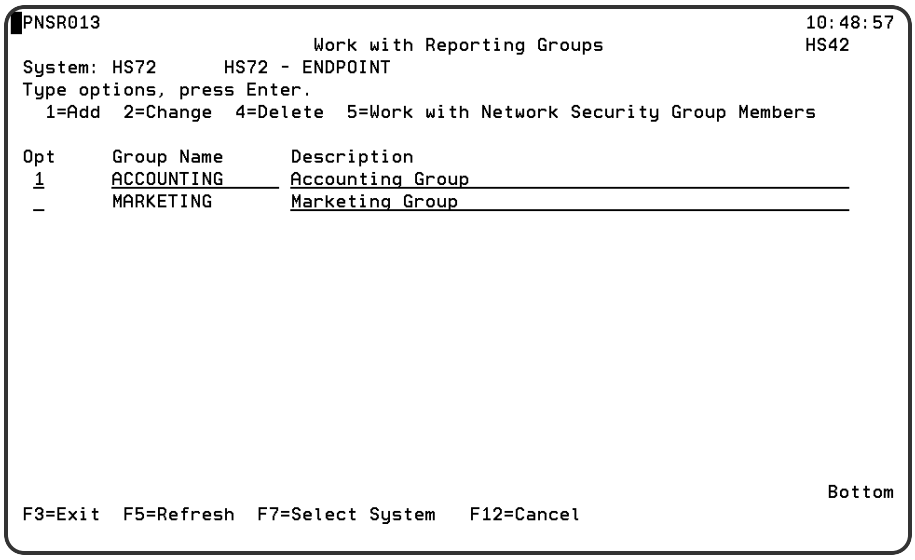
F5 (Refresh): Refreshes the screen and resets all available text fields.

F12 (Cancel): Exit the screen without processing any pending changes.

F13 (How to use this display): Shows help for the prompt display or associated display you are currently using.

F24 (More keys): Shows additional function keys that can be used for this display.

Work with Reporting Groups



What it Does

Exit Point Manager's Work with Reporting Groups is used when a number of Profiles are required to be reported on together. To add a new Network Reporting Group, enter the information on the blank line below the column headings. Once a Network Reporting Group is created a list of Profiles may be associated to it. Option **5** displays a list of profiles associated to the group. Type an option next to a specific group and press `Enter`. You can type option numbers next to more than one group at a time. This allows you to run more than one task at a time. If you see 'More...' in the lower right corner of your display, there is more information to be listed. Press the Page Down (Roll Up) key to move toward the end of the Network Reporting Groups. Press the Page Up (Roll Down) key to move toward the beginning of the Network Reporting Groups.

Options

Type the option number you want and press `Enter`.

1=Add

Add a Exit Point Manager Group. Valid for line 1 only.

2=Change

Change a Exit Point Manager Group.

> **NOTE:** You cannot use option **2** to change the reporting group name.

4=Delete

Use option 4 to delete a reporting group.

> **NOTE:** If the reporting group has user profiles assigned to it, you must remove the user profiles before you can delete the group.

5=Work with Exit Point Manager Group Members

Work with the Profiles associated with the group.

Field Descriptions

Group Name

The name of a group of Profiles.

Group Description

The description of a Reporting Group. It is a required entry.

Command Keys

F3 (Exit): Exit the current panel without processing any pending changes.

F5 (Refresh): Refreshes the panel and resets all available text fields.

F7 (Select system): Use this command to work with data from a different System.

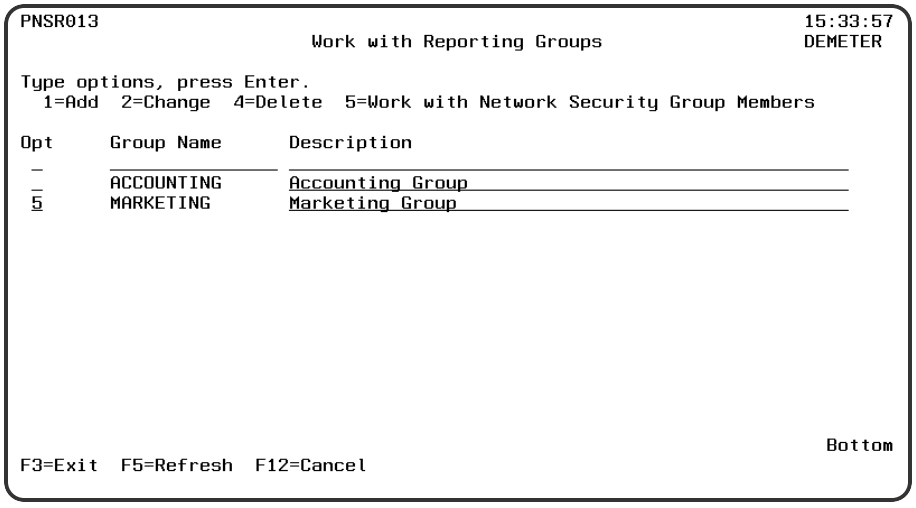
F12 (Cancel): Exit the current panel without processing any pending changes.

Working with Report Group Members

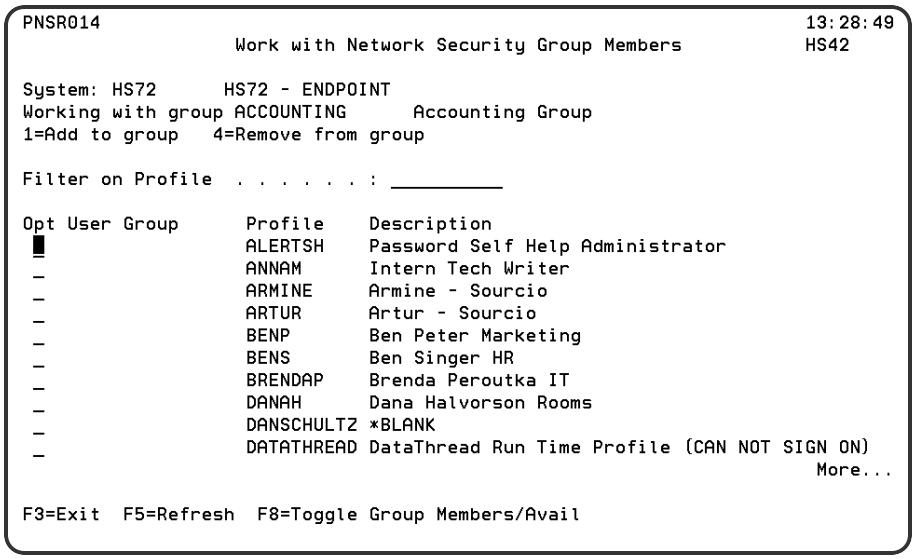
A Exit Point Manager reporting group allows you to assign users (user profiles) to the reporting groups you have created. Once you've associated user profiles with the group, you can run a report on the entire group.

Entering Reporting Group Members

1. To add members to a reporting group, select the group to which you want to add.
2. On the Work with Reporting Groups panel, enter option **5** next to the group name.



The Work with Exit Point Manager Group Members panel displays allowing you to add user profiles to a specified reporting group.



Work with Exit Point Manager Group Members Fields

Group Name
The name of the reporting group you selected.

User Profile
The user profiles that are members of the reporting group.

Work with Exit Point Manager Group Members Options
You can select from the following options to work with the reporting group members.

1=Add to group
Enter a **1** in the Opt column and enter the user profile you want to add to the reporting group. You can select the users you want to add by pressing `F8`, which switches views between group members and available users. In the Available Users view, you can enter a **1** next to multiple user profiles and add them to the group at one time.

4=Remove from group
Enter option **4** to remove a user from the reporting group.

Command Keys
F3 (Exit): Exit the current panel without processing any pending changes.

F5 (Refresh): Refreshes the panel and resets all available text fields.

F12 (Cancel): Exit the current panel without processing any pending changes.

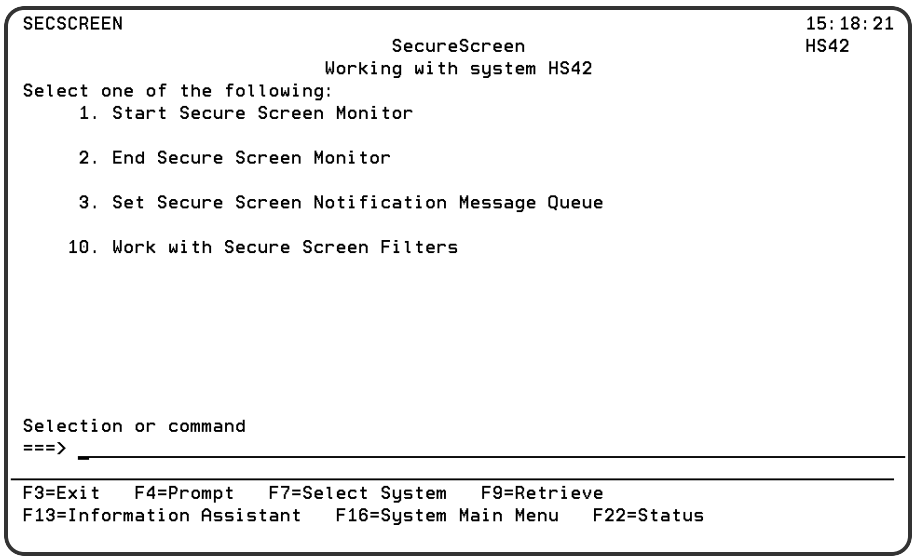
Utilities

The topics in this section describe utilities included with Powertech Exit Point Manager.

Working with Powertech SecureScreen

The Powertech Secure Screen Main Menu allows you to start and end the Secure Screen monitor, set the notification message queue, and work with Secure Screen filters.

Select option **1** on the Work with Utilities menu to display the Secure Screen main menu. You also can enter the WRKSECSCR command to display the main menu.



You can select from the following options on the Secure Screen Main Menu:

1. **Start Secure Screen Monitor.** Starts the session inactivity monitor job. The job runs in the PWRWRKMGT subsystem; the subsystem starts if it is not currently active.

The monitor receives messages from the message queue specified in the QINACTMSGQ system value. The messages describe jobs that have been inactive the interval specified in the QINACTITV system value. Information from the message is used to retrieve attributes of the inactive job, and compare them against the Secure Screen filters to determine the action to take.

Notes:

- You must configure the QINACTMSGQ and QINACTITV system values before starting the Secure Screen monitor. Use the WRKSYSVAL QINA* command to locate the system values.
- You should not define QSYSOPR as the message queue in QINACTMSGQ. Secure Screen monitors for inactivity messages and sees other messages as garbage. The QSYSOPR message queue will be locked any time QSYSOPR signs on.

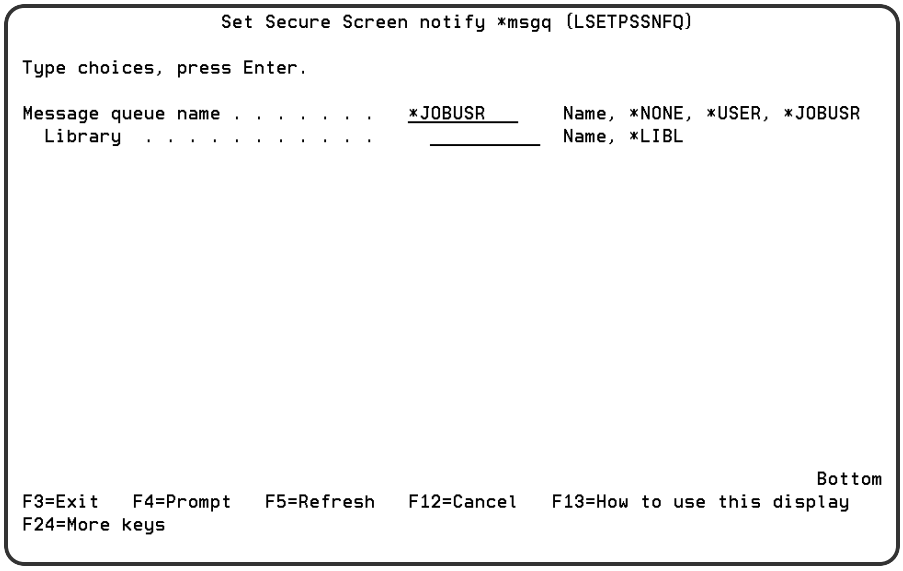
You also can use the STRPLSSMON command to start the Secure Screen monitor job.

2. **End Secure Screen Monitor.** Ends the session inactivity monitor job. When the monitor ends, inactive sessions are no longer processed against the Secure Screen filters, and sessions are not disconnected or ended.

> **NOTE:** You can end the monitor job using the ENDJOB command or ENDSBS for the PWRWRKMGT subsystem. If you specify *CNTRLD, the monitor detects the request and ends normally.

You also can use the ENDPLSSMON command to end the monitor job.

3. **Set Secure Screen Notification Message Queue.** Allows the administrator to set the name of the message queue to receive Secure Screen notifications when selected sessions time out. The monitor sends notification messages when a session times out and matches a filter that has the Notify Administrator value set to *MSG. You also can use the LSETPSSNFQ command to set a notification message queue.



Enter the following message queue information:

Message queue name

Enter the name of the message queue to use. Possible values are:

***JOBUSER** Use the message queue of the user running the job.
***USER** Use the message queue of the user associated with monitor job.
***NONE** No messages are sent.
Name Enter a message queue name to use.

Command Keys

F3 (Exit): Exit the menu.

F4 (Prompt): Provides assistance in entering or selecting a command.

F7 (Select System): Use this command key to work with data from a different System.

F9 (Retrieve): Displays the last command you entered on the command line and any parameters you included. Pressing this key once shows the last command you ran. Pressing this key twice shows the command you ran before that, and so on.

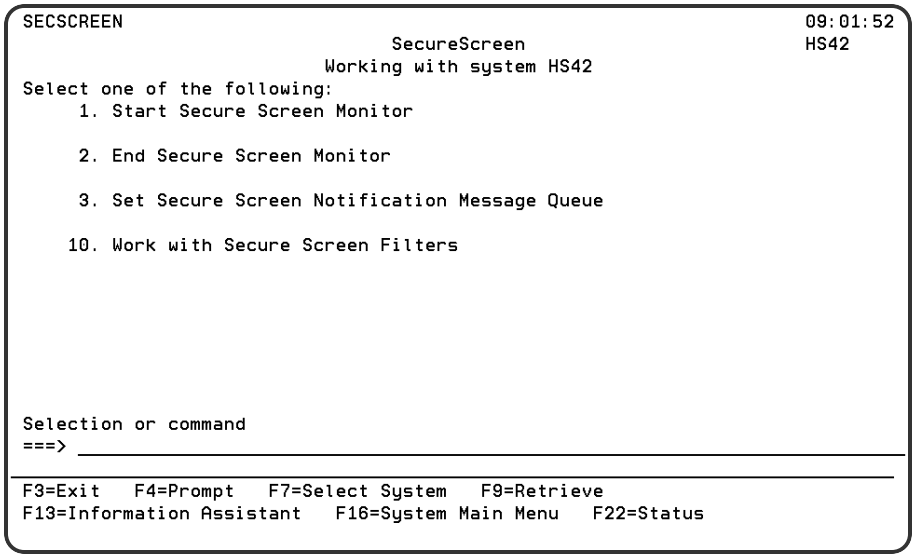
F13 (Information Assistant): Displays the Information Assistant menu with several types of assistance available. Press this key to access more information about the IMB i system.

F16 (System Main Menu): Displays the IBM i Main Menu (MAIN).

F22 (Status): Displays the Operational Resources pop-up window containing the status of several operation aspects of Powertech products.

Working with Powertech SecureScreen

The Powertech Secure Screen Main Menu allows you to start and end the Secure Screen monitor, set the notification message queue, and work with Secure Screen filters. Select option 1 on the Work with Utilities menu to display the Secure Screen main menu. You also can enter the WRKSECSCR command to display the main menu.



You can select from the following options on the Secure Screen Main Menu:

1. **Start Secure Screen Monitor.** Starts the session inactivity monitor job. The job runs in the PWRWRKMGT subsystem; the subsystem starts if it is not currently active.

The monitor receives messages from the message queue specified in the QINACTMSGQ system value. The messages describe jobs that have been inactive the interval specified in the QINACTITV system value. Information from the message is used to retrieve attributes of the inactive job, and compare them against the Secure Screen filters to determine the action to take.

NOTE:

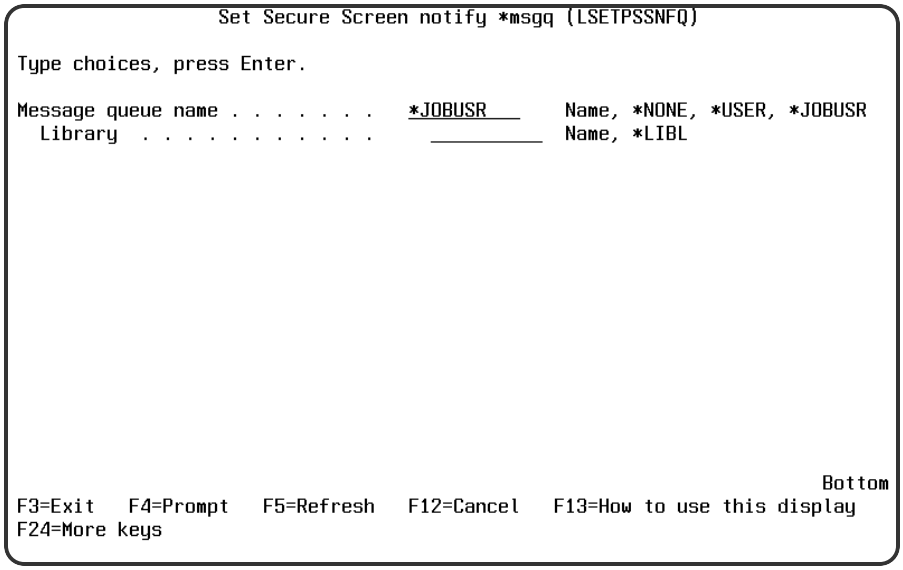
- You must configure the QINACTMSGQ and QINACTITV system values before starting the Secure Screen monitor. Use the WRKSYSVAL QINA* command to locate the system values.
- You should not define QSYSOPR as the message queue in QINACTMSGQ. Secure Screen monitors for inactivity messages and sees other messages as garbage. The QSYSOPR message queue will be locked any time QSYSOPR signs on.

You also can use the STRPLSSMON command to start the Secure Screen monitor job.

2. **End Secure Screen Monitor.** Ends the session inactivity monitor job. When the monitor ends, inactive sessions are no longer processed against the Secure Screen filters, and sessions are not disconnected or ended. You also can use the ENDPLSSMON command to end the monitor job.

> **NOTE:** You can end the monitor job using the ENDJOB command or ENDSBS for the PWRWRKMGT subsystem. If you specify *CNTRLD, the monitor detects the request and ends normally.

3. **Set Secure Screen Notification Message Queue.** Allows the administrator to set the name of the message queue to receive Secure Screen notifications when selected sessions time out. The monitor sends notification messages when a session times out and matches a filter that has the Notify Administrator value set to *MSG. You also can use the LSETPSSNFQ command to set a notification message queue.



Enter the following message queue information:

Message queue name

Enter the name of the message queue to use. Possible values are:

***JOBUSER** Use the message queue of the user running the job.

***USER** Use the message queue of the user associated with monitor job.

***NONE** No messages are sent.

Name Enter a message queue name to use.

Library

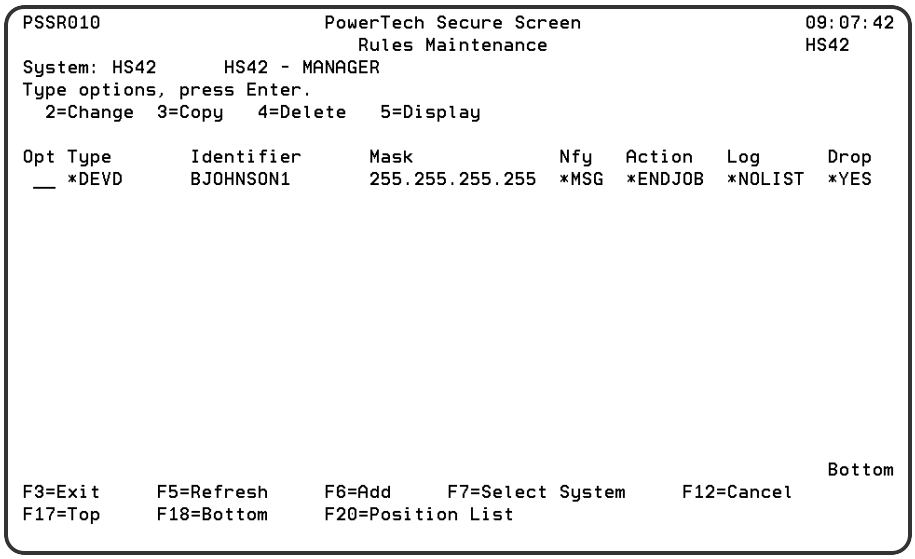
Enter a library name. Possible values are:

***LIBL** No messages are sent.

library-name Enter the name of the library where the message queue exists.

Working with Secure Screen Filters

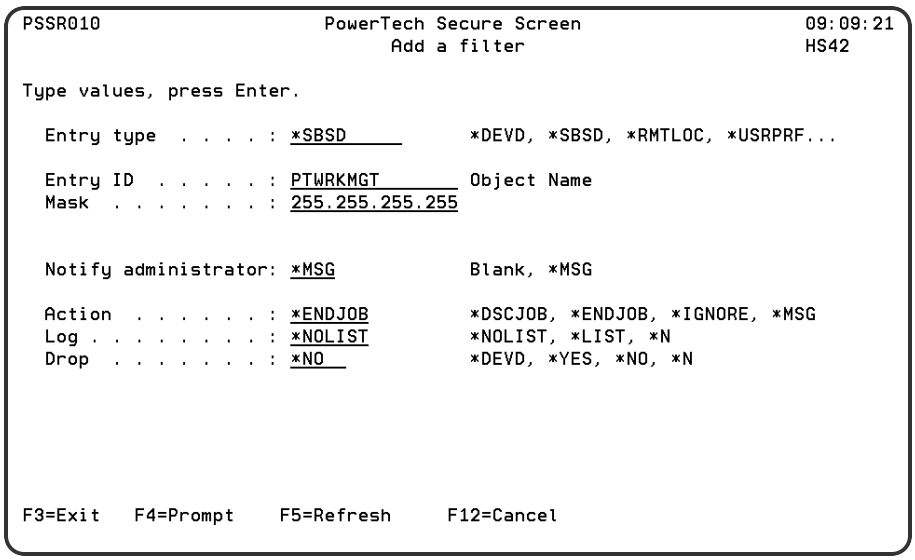
You can set up rules for using Secure Screen by defining filters. Select option **10**, Work with Secure Screen Filters, on the Secure Screen Main Menu to display the Rules Maintenance screen. You also can enter the command, LEDTPSSFTR, to display the Rules Maintenance screen.



The Rules Maintenance screen lists all filters you currently have in place, and their values. From the screen you can add, change, copy, delete, and display filters.

Adding A Filter

To add a new filter, press **F6**. The Add a filter screen displays, allowing you to specify the filter rules.



Enter the following information for the filter:

Entry Type

The type of filter. There are six types of filters; possible values are:

*__DEVD__ Device Description

*__SBSD__ Subsystem Description

*__RMTLOC__ Remote Location

*__USRPRF__ User Profile

***GRPPRF** Group User Profile

***ACGCDE** Accounting Code

Entry ID
Enter the name of the device, subsystem, user profile, remote location, group profile, or accounting code. Press F4 to select from a list of values. For a remote location, enter the IP address of the location.

Mask
The subnet mask to be combined with an IP address. The value in this field is used only when you entered an IP address for *RMTLOC. An IP address from a Telnet device is masked to compare with the IP address entered for a filter. This allows the filtering of a range of IP addresses.

Notify Administrator
Tells Secure Screen whether to send a message to the administrator's message queue. Enter *MSG to send a message when a timeout occurs; leave this field blank if you do not want a notification message sent.

Action
Specify what will happen when a timeout occurs for a session. Possible values are:

***DSCJOB** Device Description

***ENDJOB** Subsystem Description

***MSG** Remote Location

***IGNORE** User Profile

Log
When the Action is *DSCJOB, this specifies whether or not to print the job log. Possible values are:

***LIST** Print the job log

***NOLIST** Do not print the job log

***N** Use the default from the *DSCJOB command on your system

Drop
When the Action is *DSCJOB, this specifies whether the connection should be dropped if the session time out. Possible values are:

***DEVD** Handle the connection as it's specified on the session device

***YES** Force the connection to drop

***NO** Leave the connection available

***N** Use the default from the *DSCJOB command on your system

Changing A Filter

To change an existing filter, enter option 2 next to the filter on the Rules Maintenance screen. This displays the Change a filter screen.

Use the Change a filter screen to change the filter settings. You cannot change the filter Type or Entry ID.

```
PSSR010                    PowerTech Secure Screen                    12:31:22
                               Change a filter                        DEMETER

Type values, press Enter.

  Entry type  . . . . : *RMTLOC         *DEVD, *SBSD, *RMTLOC, *USRPRF...

  Entry ID  . . . . . : 198.196.5.0     Object Name
  Mask  . . . . . . . : 255.255.255.0

  Notify administrator: *MSG            Blank, *MSG

  Action  . . . . . . : *IGNORE         *DSCJOB, *ENDJOB, *IGNORE, *MSG
  Log . . . . . . . . : *NOLIST         *NOLIST, *LIST, *N
  Drop  . . . . . . . : *YES            *DEVD, *YES, *NO, *N

F3=Exit   F4=Prompt    F5=Refresh     F12=Cancel
```

Copying A Filter

You can copy an existing filter to copy the filter's settings and modify them to define a new filter. To copy a filter, enter option **3** next to the filter you want to copy.

Deleting a Filter

To delete a filter, enter option **4** next to the filter you want to delete.

Displaying a Filter

You can display the settings for a filter. Enter option **5** next to a filter to display the Display a filter screen.

```
PSSR010                    PowerTech Secure Screen                    12:59:28
                               Display a filter                       DEMETER

Press enter to continue.

  Entry type  . . . . : *RMTLOC
  Entry ID  . . . . . : 192.192.1.0
  Mask  . . . . . . . : 255.255.255.0

  Notify administrator: *MSG

  Action  . . . . . . : *DSCJOB
  Log . . . . . . . . : *LIST
  Drop  . . . . . . . : *YES

F3=Exit   F12=Cancel
```

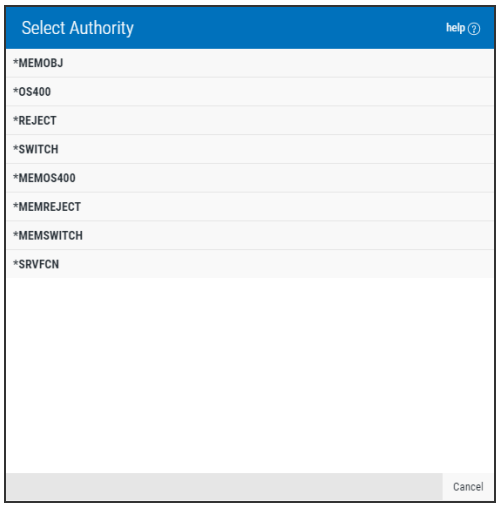
Reference

The topics in this section include descriptions of Exit Point Manager's options and controls.

Browser Interface Reference

The following topics list descriptions for all fields and options on Exit Point Manager's screens when using the web browser interface. To view green screen panels, see Green Screen Panel Descriptions.

Authorities selection window



How to Get There

Choose **Lookup** next to the Authorities field when adding or changing a rule.

What it Does

This window allows you to specify an authority when adding or changing a rule.

Options

This list may include all or some of the following authorities, depending on the rule being defined.

***OS400**Exit Point Manager will use normal IBM i authority for the location. This is valid for both location and user.

***REJECT**Exit Point Manager will reject requests for the specified location. This is valid for both location and user.

***SWITCH**Exit Point Manager will use the authority of the switch profile for the specified location. A switch profile entry is required. This is valid for both location and user. To view the profile to be switched to view the expanded rule properties.

***MEMREJECT** Check Memorized Transactions (MTR) for authority. If no MTR authority is encountered, Exit Point Manager will reject requests for the specified location. This is valid for both location and user.

***MEMOS4OO** Check Memorized Transactions (MTR) for authority. If no MTR authority is encountered, Exit Point Manager will use normal OS/400 authority for the location. This is valid for both location and user.

***MEMUSR** Check Memorized Transactions (MTR) for authority. If no MTR authority is encountered, Exit Point Manager will check server user authority. This is only valid for location.

***USER**Exit Point Manager will check server user authority.

> **NOTE:** When *USER is selected for a Location rule, the Audit, Message, and Capture flags are always set to Inherit (green screen = *). Flags defer to the User Rule that applies to the transaction's incoming user profile.

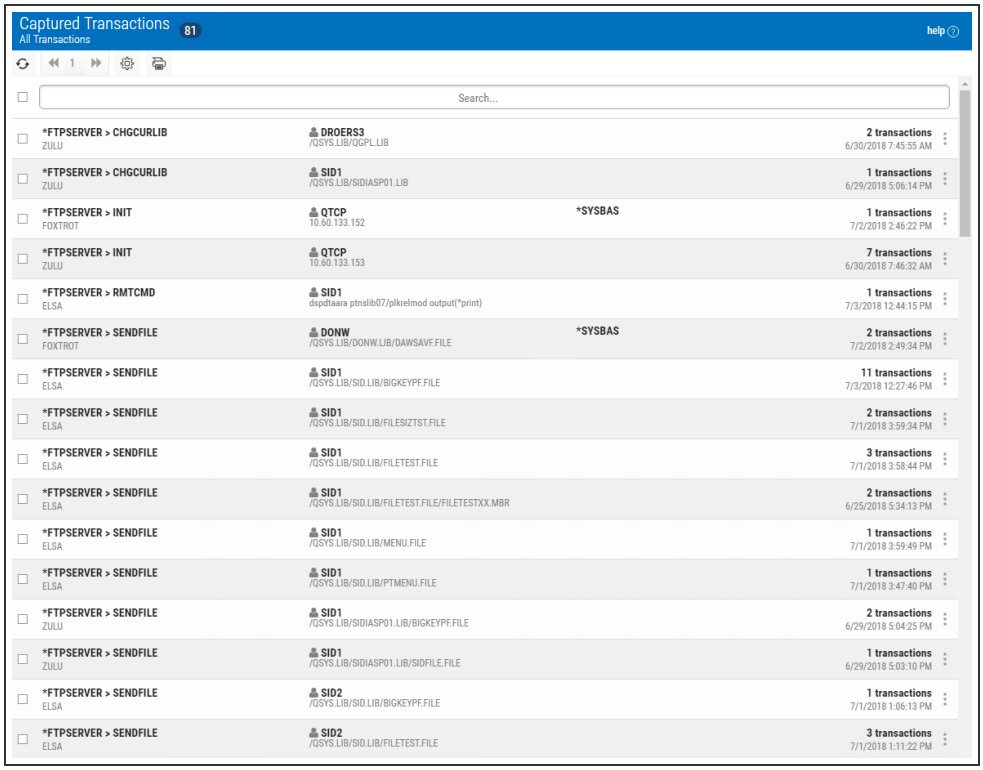
***MEMSWITCH** Check Memorized Transactions (MTR) for authority. If no MTR authority is encountered, Exit Point Manager will use the authority of the switch profile for the specified location. A switch profile entry is required. This is valid for both location and user.

***MEMOBJ** Memorized Transactions (MTR) are checked for authority first. If no MTR authority is encountered, Exit Point Manager will check any objects used in the transactions for authorities defined by Object Rules.

***SRVFCN**Exit Point Manager will use the authority defined for the server/function. This is valid for both location and user.

***SAME**Exit Point Manager will not change the existing settings and will not create new rules when the All Servers option is taken. This is valid for both location and user.

Captured Transactions screen



How to Get There

Click the **Captured Transactions** tab on the navigation pane on the left side of the Insite window.

What it Does

The Captured Transactions screen allows you to view, sort, and delete Captured Transactions. The list is ordered chronologically by time stamp with the most recent transaction at the top of the list. Captured transactions are displayed in pages with 200 records to a page (or 100 when viewing with a mobile device).

Exit Point Manager caches captured transactions on the web server to facilitate speedy page viewing and navigation. The cache is created upon the initial page load, on refresh, or when a filter search is submitted (even if the search query is the same). The cache is used only for navigating through pages (i.e. when using the previous button, next button, or page select drop-down menu). The cache expires 10 minutes from creation. After cache expiration, a message appears indicating the cache has expired, after which the cache is recreated with the same page displayed (or the closest possible page).

See Capturing Transactions for details on how to capture a transaction.

Options

Choose a transaction record to open the View Transaction screen where you can view and memorize a captured transaction.

Selection, sorting, filtering, deleting, and navigation features on this screen are described in Using the Web Browser Interface.

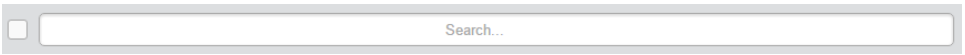
Refresh

Choose this button to refresh from the server to display the latest captured transactions.

Page Scroll

Select the left and right arrows to move forward and backward through pages.

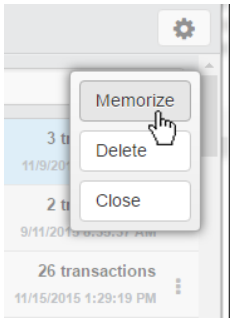
Search and filter box



Select the records you want to filter (choose the check box next to the Search field to Select All), then enter text in the Search box and press `Enter` to query captured transactions. Use the  button to identify other Search Filter and Sorting criteria.

Memorize

Click  next to a record and select **Memorize**.

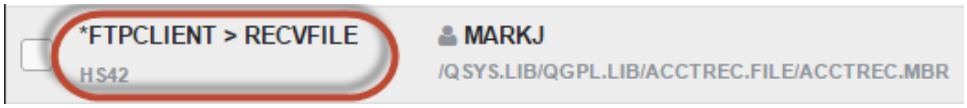


This opens the New Memorized Transaction screen, which allows you to memorize the transaction for a user or location. See also Memorizing a Transaction.

Field Descriptions

The Captured Transaction screen allows you to change some of the values for the captured transaction to fine tune it to your specification before you memorize it.

Server > Function



A Server in Exit Point Manager is a controlled entry point into your system. These entry points are determined and defined by IBM. Exit Point Manager has assigned easy-to-remember names to these controlled entry points.

A Function, or Server Function, in Exit Point Manager represents a class of operations that a given Server may perform. For example, the *SIGNON Server classifies its operations as those pertaining to changing passwords, generating authentication tokens, and retrieving sign-on information. Exit Point Manager has assigned easy-to-remember names to these Functions, such as CHGPWD, GENAUTTKN and RETRIEVE.

User/Location

User represents the identity of the person initiating a transaction as a user profile. The special value *PUBLIC, when used on a rule, means that the rule applies to any User lacking a specific rule. when used as a subset or selection parameter, *PUBLIC means to select all such rules for display or printing. This is the User that initiated the transaction.

> **NOTE:** The count includes only transactions that you've specified should be captured by Exit Point Manager. It does not reflect all network traffic and cannot be used for a general statistical analysis of network traffic.

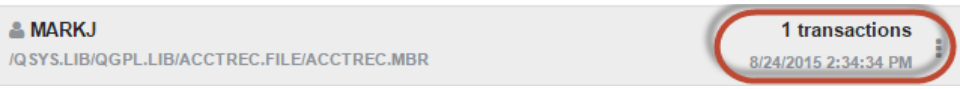
ASP Group

This is the name of an ASP Group. It is used in rule evaluation to determine if an object referenced in a transaction is the one specified on the object entries for this list.

Possible values are:

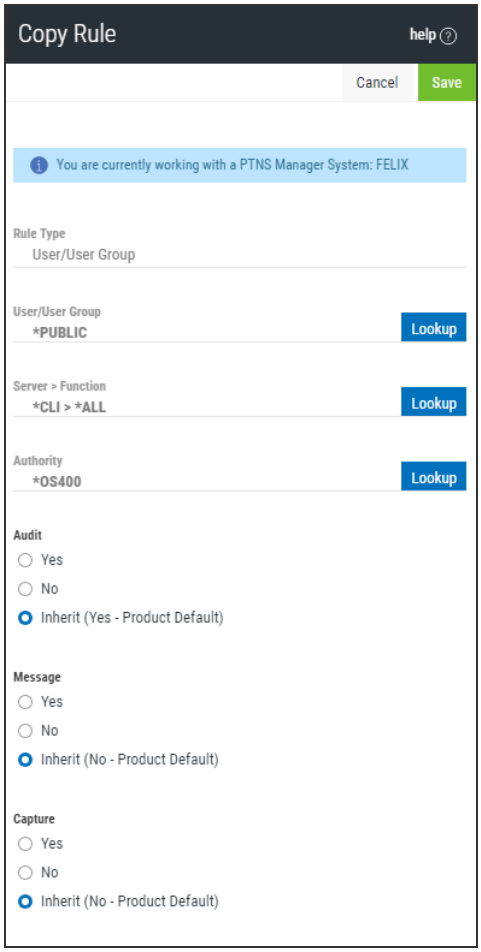
- ***SYSBAS** The Object List entries refer to those objects in *SYSBAS.
- ***ALL** The Object List entries refer to those objects in any namespace.

Count



The number of times this exact transaction has been captured.

Copy Rules screen



How to Get There

1. On the Navigation Pane, choose **Rules**.
2. Click the  icon adjacent to the Rules you would like to copy and choose **Copy**.

What it Does

Use the Copy Rules screen to copy Rules to one or more managed systems.

To add Endpoints to your Exit Point Manager configuration, see Adding and Configuring Managed Systems.

Options

Rule Type

Specifies whether this is a User or Location rule.

User/User Group; Select

Choose this **Lookup** button to open the Users selection window where you can choose from a list of user profiles.

Server > Function; Lookup

Choose this **Lookup** button to open the Servers selection window where you can choose from a list of servers and server functions. For a description of servers and functions, see Appendix B: Servers and Functions.

Authority; Lookup

Choose this **Lookup** button to open the Authorities selection window where you can choose from a list of Authorities.

Audit

The audit property controls the type of requests Exit Point Manager will log.

Possible values are:

Yes Log all requests by the location/server/function.
No Only log authority failures for the location/server/function.
Inherit Inherit the value.

Message

The message property entry will determine if Exit Point Manager sends a message to the Exit Point Manager message queue.

Possible values are:

Yes A message is sent to the Exit Point Manager message queue.
No No message is sent.
Inherit Inherit the value.

Capture

Capture transactions for Memorized Transaction Request.

Possible values are:

Yes Capture transactions.
No Do not capture transactions.
Inherit Inherit the value.

Select which systems to save to

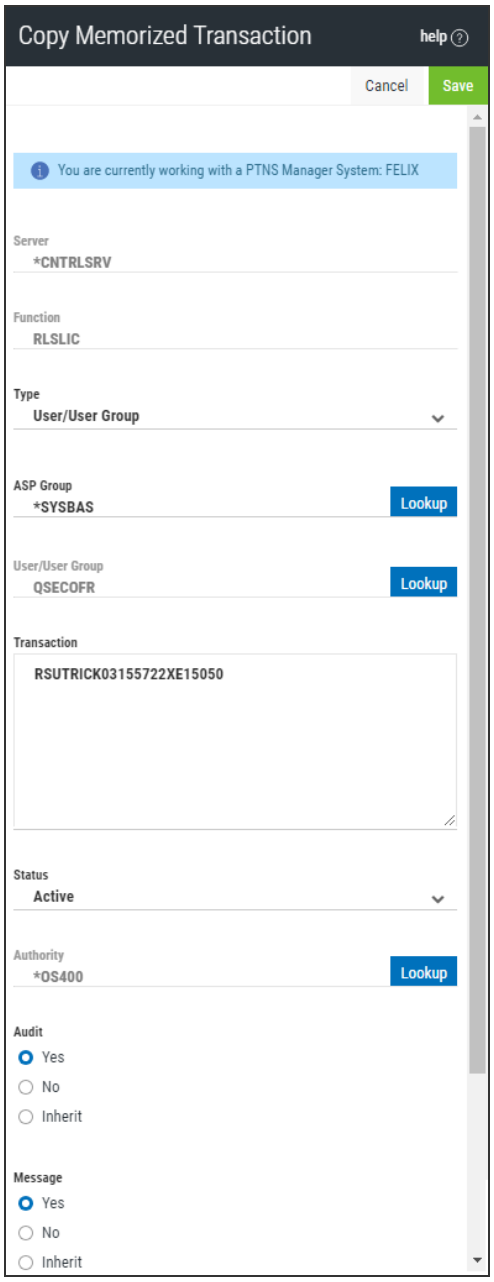
All managed systems are listed here. Check the systems you would like to save the Rule to. Or, check Select All to copy the Rule to all managed systems.

If the rule already exists on the system you are using (the Manager system), uncheck the checkbox for that system. Otherwise you will get an error stating that the rule already exists on that system.

Save • Cancel

Click **Save** to copy the Rule to the selected system(s). Choose **Cancel** to dismiss the screen without making changes.

Copy Memorized Transaction screen



A screen similar to the one shown above is used to copy Rules, Object Lists, Memorized Transactions, and Pre-filters.

How to Get There

1. On the Navigation Pane, choose **Memorized Transactions**.
2. Click the  icon adjacent to the IP Address Group you would like to copy and choose **Copy**.

What it Does

Use the Copy screen to copy Rules (User/Location/Object), Object Lists, Memorized Transactions, and Pre-filters to one or more Endpoints.

> **NOTE:** To add Endpoints to your Exit Point Manager configuration, see Adding and Configuring Managed Systems.

Options

Server

A Server in Exit Point Manager is a controlled entry point into your system. These entry points are determined and defined by IBM. Exit Point Manager has assigned easy-to-remember names to these controlled entry points.

Function

A Function, or Server Function, in Exit Point Manager represents a class of operations that a given Server may perform. For example, the *SIGNON Server classifies its operations as those pertaining to changing passwords, generating authentication tokens, and retrieving sign-on information. Exit Point Manager has assigned easy-to-remember names to these Functions, such as CHGPWD, GENAUTTKN and RETRIEVE.

Type

Specifies whether this is a User or Location rule.

User
User represents the identity of the person initiating a transaction as a user profile. The special value *PUBLIC, when used on a rule, means that the rule applies to any User lacking a specific rule. When used as a subset or selection parameter, *PUBLIC means to select all such rules for display or printing. Specify the name of the User for the memorized transaction. You can create a memorized transaction that applies to all Users by specifying the special value *PUBLIC.

Location
Location represents the source of a transaction. Location can hold an IP Address, an IP Address Group or the name of an SNA Communications Device. The special value *ALL, when used on a rule, means that the rule applies to any rule means that the rule applies to any Location lacking a specific rule. when used as a subset or selection parameter, *ALL generally means to select all such rules for display or printing. Specify the Location for the memorized transaction. You can create a memorized transaction that applies to all Locations by specifying the special value *ALL.

ASP Group; Lookup

This is the name of an ASP Group. It is used in rule evaluation to determine if an object referenced in a transaction is the one specified on the object entries for this list.

Click **Lookup** to open the Select ASP Group screen where you can choose from the following ASP Groups:

***SYSBAS** The Object List entries refer to those objects in *SYSBAS.

***ALL** The Object List entries refer to those objects in any namespace.

User/User Group; Select

Choose this **Lookup** button to open the Users selection window where you can choose from a list of user profiles.

Transaction

The transaction data.

Status

This is the status of the Memorized Transaction.

Possible values are:

***ACTIVE**
Exit Point Manager will attempt to match this transaction during rule enforcement. Memorized Transactions that are changed to *ACTIVE will have a matching User or Location rule changed to the corresponding action; *ALLOW to *MEMOS400, *REJECT to *MEMREJECT, or *SWITCH to *MEMSWITCH.
***INACTIVE**
Exit Point Manager will not attempt to match this transaction during rule enforcement. Memorized Transactions that are changed to *INACTIVE will have the matching User or Location rule changed (if there are no other Memorized Transactions for that rule) to the corresponding action; *MEMOS400 to *ALLOW, *MEMREJECT to *REJECT, or *MEMSWITCH to *SWITCH.

Authority

Authority represents the action to be taken when a rule is found that matches the data present on a transaction.

Specify the Authority value for the new memorized transaction.

The list of valid values may include one or more of these values:

***USER** Current user authority is used.
***0S400** Exit Point Manager will use normal operating system authority for the user.
***REJECT** Exit Point Manager will reject requests.
***SWITCH** Exit Point Manager will use the authority of the switch profile for the transaction. A switch profile entry is required.
***MEMUSR** Memorized Transactions (MTR) are checked for authority first. If no MTR authority is encountered, Exit Point Manager will use the authority of the current user.
***MEMOS400** Memorized Transactions (MTR) are checked for authority first. If no MTR authority is encountered, Exit Point Manager will use normal operating system authority for the user.
***MEMREJECT** Memorized Transactions (MTR) are checked for authority first. If no MTR authority is encountered, Exit Point Manager will reject requests for the specified user.
***MEMSWITCH** Memorized Transactions (MTR) are checked for authority first. If no MTR authority is encountered, Exit Point Manager will use the authority of the switch profile for the specified user. A switch profile entry is required.
***MEMOBJ** Memorized Transactions (MTR) are checked for authority first. If no MTR authority is encountered, Exit Point Manager will check any objects used in the transactions for authorities defined by Object Rules.
***SERVER** Exit Point Manager will use the authority defined for the Server.
***SRVFCN** Exit Point Manager will use the authority defined for the Server Function.

Audit

The Audit flag controls the logging of transactions to the Log Journal set up on the work with Exit Point Manager System Values panel.

Specify one of these values for Audit:

*__INHERIT__ Uses the value found in the rule above this one in the rule hierarchy.
*__YES__ Logs all requests when this rule is enforced.
*__NO__ Logs only access failures (rejects) for this rule.

Message

The Send messages flag controls the sending of messages to the Log Message Queue set up on the work with Exit Point Manager System Values panel.

Specify one of these values for Send messages:

*__INHERIT__ Uses the value found in the rule above this one in the rule hierarchy.
*__YES__ Sends a message when this rule is enforced.
*__NO__ Does not send a message when this rule is enforced.

Capture

The Capture transactions flag controls whether transactions are remembered in Exit Point Manager for later memorization. Once captured, transactions can become Memorized Transactions which can act as rules.

Specify one of these values for Capture transactions:

*__INHERIT__ Uses the value found in the rule above this one in the rule hierarchy.
*__YES__ Captures the transaction when this rule is enforced.
*__NO__ Does not capture the transaction when this rule is enforced.

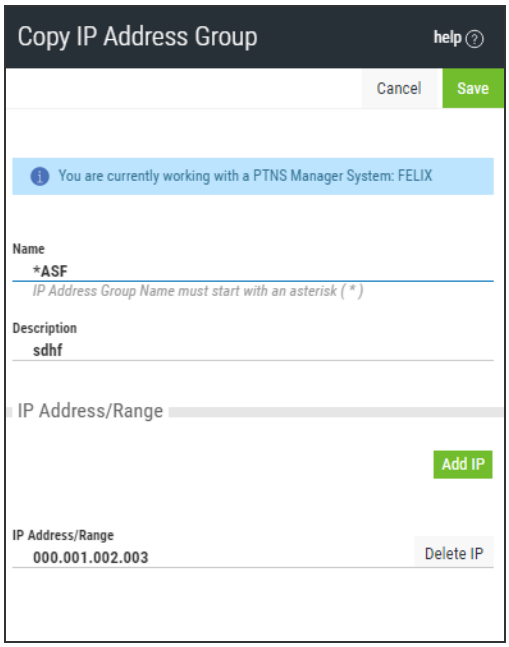
Select which systems to save to

All managed systems are listed here. Check the systems you would like to save the IP Address group to. Or, check Select All to copy the IP Address Group to all managed systems.

Save • Cancel

Click **Save** to copy the IP Address Group to the selected system(s). Choose **Cancel** to dismiss the screen without making changes.

Copy IP Address Group screen



How to Get There

1. On the Navigation Pane, choose **IP Address Groups**.
2. Click the  icon adjacent to the IP Address Group you would like to copy and choose **Copy**.

What it Does

Use the Copy IP Address Group screen to copy an IP Address Group to one or more managed systems.

> **NOTE:** To add Endpoints to your Exit Point Manager configuration, see Adding and Configuring Managed Systems.

Options

Name

The name of the IP Address Group.

Description

The IP Address Group's description.

IP Address Group Range

The range of IP addresses included in the group. Click **Add** IP to add an IP Address or IP Address range to the group. Click Delete to delete an existing IP address or IP address range.

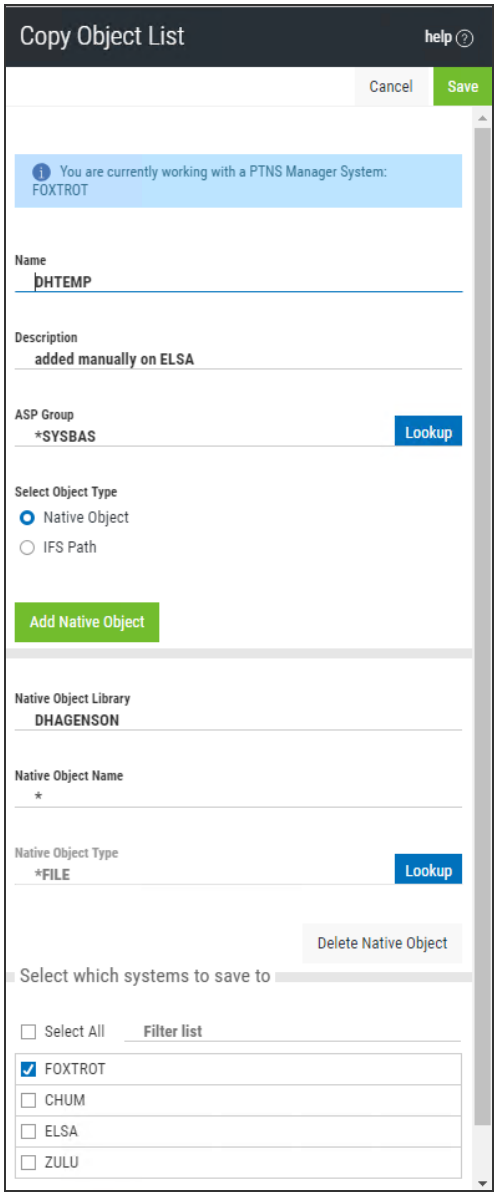
Select which systems to save to

All managed systems are listed here. Check the systems you would like to save the IP Address group to. Or, check Select All to copy the IP Address Group to all managed systems.

Save • Cancel

Click **Save** to copy the IP Address Group to the selected system(s). Choose **Cancel** to dismiss the screen without making changes.

Copy Object List screen



How to Get There

1. On the Navigation Pane, choose **Object Lists**.
2. Click the  icon adjacent to the Object List you would like to copy and choose **Copy**.

What it Does

Use the Copy Object List screen to copy an Object List to one or more managed systems.

> **NOTE:** To add Endpoints to your Exit Point Manager configuration, see Adding and Configuring Managed Systems.

Options

Name

The name of the Object List.

Description

The Object List's description.

ASP Group; Lookup

This is the name of an ASP group. It is used in rule evaluation to determine if an object referenced in a transaction is the one specified on the object entries for this list.

Click **Lookup** to open the Select ASP Group screen where you can choose from the following ASP Groups:

***SYSBAS** The Object List entries refer to those objects in *SYSBAS.

***ALL** The Object List entries refer to those objects in any namespace.

Select Object Type

This is the type of Object List; Native Object, or IFS Path. The Object List type determines what type of entries can be added to an Object List. Object lists can hold native object specifications (library, object and type) or paths to IFS objects.

Native Object Library, Name, and Type (for Native Object Lists only)

In the first two fields, enter the Library and Name of the object. Choose **Lookup** to open the Types of Object Entries selection window where you can select the Object type.

IFS Path (for IFS Object Lists only)

Each slot includes the path of an IFS object in the Object List. This name is required to be a valid OS name.

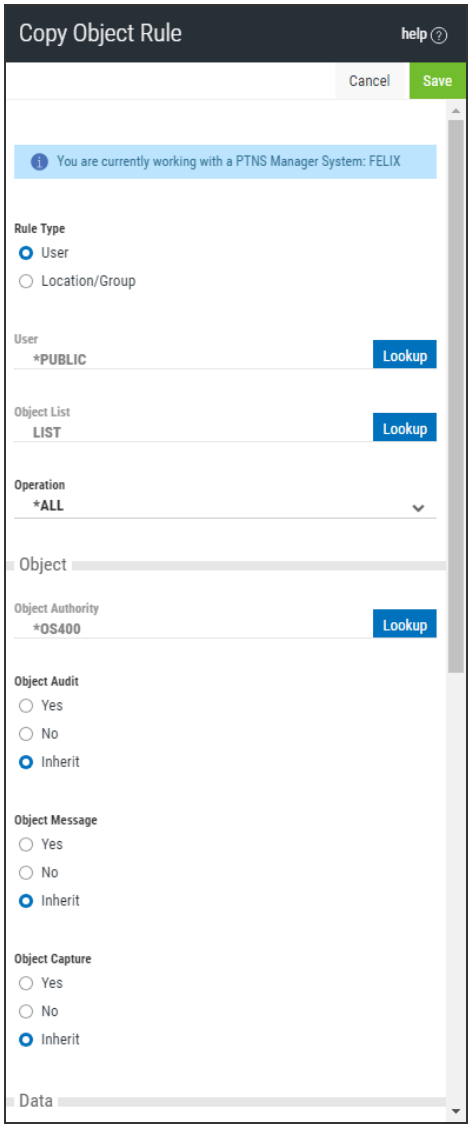
Select which systems to save to

All managed systems are listed here. Check the systems you would like to save the IP Address group to. Or, check Select All to copy the IP Address Group to all managed systems.

Save • Cancel

Click **Save** to copy the IP Address Group to the selected system(s). Choose **Cancel** to dismiss the screen without making changes.

Copy Object Rule screen



How to Get There

1. On the Navigation Pane, choose **Object Rules**.
2. Click the  icon adjacent to the Object Rule you would like to copy and choose **Copy**.

What it Does

Use the Copy Object Rules screen to copy Object Rules to one or more managed systems.

NOTE: To add Endpoints to your Exit Point Manager configuration, see Adding and Configuring Managed Systems.

Options

Cancel
Choose **Cancel** to return to the Object Rules screen without making changes.

Save
Choose **Save** to save the Rule and return to the Object Rules screen.

Rule Type
Specifies whether this is a User or Location Object rule.

User; Lookup
This field is available when creating a new Object Rule. Choose this **Lookup** button to open the Users selection window where you can choose from a list of user profiles.

Object List; Lookup
This field is available when creating a new Object Rule. Choose this **Lookup** button to open the Object Lists selection window where you can choose from a list of Object Lists. Object Lists can be added and changed using the Object Lists screen.

Operation
*__ALL__ Applies to all of the above types of operations.
*__CREATE__ Applies to objects when they are being created or to their data when they are being added to an object; for example, when writing records to a database.
*__READ__ Applies to non—modifying accesses of objects or the reading of an object's data.
*__UPDATE__ Applies to changes to objects or changes to their data.
*__DELETE__ Applies to deletion of objects or deletion of their data; for example, deleting records from a database file.

Object Authority; Lookup
Choose this **Lookup** button to open the Authorities selection window where you can choose from a list of Authorities.

Object Audit
This audit property controls the type of requests Exit Point Manager will log. This Audit Transaction flag pertains to Object Accesses.

Possible values are:

Yes - Log all requests by the location/server/function.
No - Only log authority failures for the location/server/function.
Inherit - Inherit the value.

Object Message
The message property entry will determine if Exit Point Manager sends a message to the Exit Point Manager message queue.

This Send Messages flag pertains to Object Accesses.

Yes - A message is sent to the Exit Point Manager message queue.
No - No message is sent.
Inherit - Inherit the value.

Object Capture
Capture transactions for Memorized Transaction Request.

This Capture Transactions flag pertains to Data Accesses.

Yes - Capture transactions.
No - Do not capture transactions.
Inherit - Inherit the value.

Data Audit
This audit property controls the type of requests Exit Point Manager will log. This Audit Transaction flag pertains to Data Accesses.

Possible values are:

Yes - Log all requests by the location/server/function.
No - Only log authority failures for the location/server/function.
Inherit - Inherit the value.

Data Message
The message property entry will determine if Exit Point Manager sends a message to the Exit Point Manager message queue.

This Send Messages flag pertains to Data Accesses.

Yes - A message is sent to the Exit Point Manager message queue.
No - No message is sent.
Inherit - Inherit the value.

Data Capture
Capture transactions for Memorized Transaction Request.

This Capture Transactions flag pertains to Data Accesses

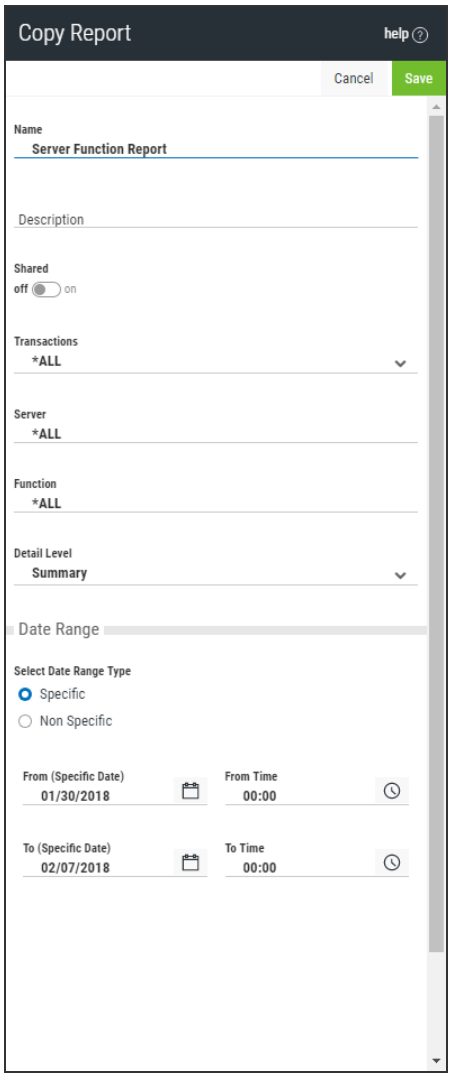
Yes - Capture transactions.
No - Do not capture transactions.
Inherit - Inherit the value.

Active
Choose **Yes** to activate the rule. Choose **No** to make the rule inactive.

Add Server > Function
Click this button to open the Select Server/Function screen, where you can choose additional Servers/Functions.

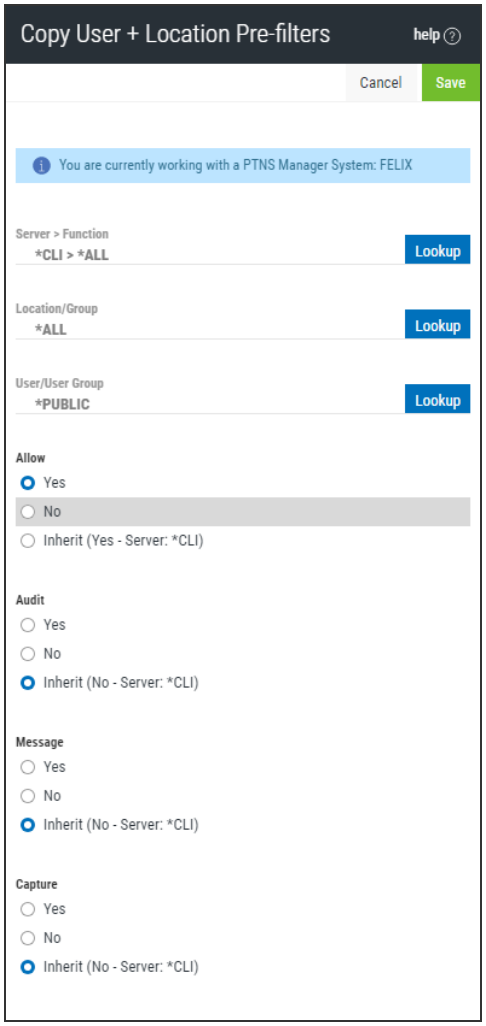
Copy Report screen

Use this screen to confirm the settings of the report you want to copy.



For a description of the Report options, see the New/Edit Report screen.

Copy User+Location Pre-filter screen



How to Get There

1. On the Navigation Pane, choose **User+Location Pre-filters**.
2. Click the  icon adjacent to the Pre-filter you would like to copy and choose **Copy**.

What it Does

Use the Copy User+Location Pre-filter screen to copy User+Location Pre-filters to one or more managed systems.

Options

Server > Function

A Server in Exit Point Manager is a controlled entry point into your system. These entry points are determined and defined by IBM. Exit Point Manager has assigned easy-to-remember names to these

controlled entry points.

A Function, or Server Function, in Exit Point Manager represents a class of operations that a given Server may perform. For example, the *SIGNON Server classifies its operations as those pertaining to changing passwords, generating authentication tokens, and retrieving sign-on information. Exit Point Manager has assigned easy-to-remember names to these Functions, such as CHGPWD, GENAUTTKN and RETRIEVE.

Location/Group

Select the location of the Pre-filter. The location is the name of the location for which authority is being specified. IP Address Groups must be established prior to their entry on this screen (see IP Address Groups).

User

Select the User. User represents the identity of the person initiating a transaction as a user profile. The special value *PUBLIC, when used on a Pre-filter, means that the Pre-filter applies to any User lacking a specific Pre-filter.

Allow

The setting for whether transactions matching this record should be allowed to continue to be processed by Exit Point Manager. Select Yes to indicate that Exit Point Manager rules should evaluate this transaction, which may or may not cause it to be rejected. Select No to reject the transaction. Select Inherit to inherit the value from the System (*ALL) Pre-filter.

Audit

The Audit flag controls the logging of transactions to the Log Journal set up on the work with Exit Point Manager System Values panel. Specify one of these values for Audit:

***INHERIT** Uses the value found in the rule above this one in the rule hierarchy.
***YES** Logs all requests when this rule is enforced.
***NO** Logs only access failures (rejects) for this rule.

Message

The Send messages flag controls the sending of messages to the Log Message Queue set up on the work with Exit Point Manager System Values panel.

Specify one of these values for Send messages:

***INHERIT** Uses the value found in the rule above this one in the rule hierarchy.
***YES** Sends a message when this rule is enforced.
***NO** Does not send a message when this rule is enforced.

Capture

The Capture transactions flag controls whether transactions are remembered in Exit Point Manager for later memorization. Once captured, transactions can become Memorized Transactions which can act as rules. Specify one of these values for Capture transactions:

***INHERIT** Uses the value found in the rule above this one in the rule hierarchy.
***YES** Captures the transaction when this rule is enforced.
***NO** Does not capture the transaction when this rule is enforced.

Select which systems to save to

All managed systems are listed here. Check the systems you would like to save the Pre-filter to. Or, check Select All to copy the Pre-filter to all managed systems.

Save • Cancel

Click **Save** to copy the Pre-filter to the selected system(s). Choose **Cancel** to dismiss the screen without making changes.

Appendix N: Exit Point Manager Dashboard Asset Descriptions

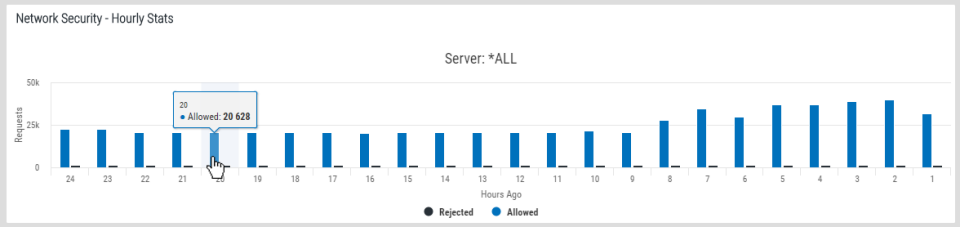
Assets represent the type of Exit Point Manager data for which you can generate a visual representation within an Insite Dashboard, via a widget.

While defining Dashboard Widgets in Insite, once a Data Source has been selected, you can then select the asset that the widget will represent. Only the assets from the selected Data Source are available. If the required asset is not displayed, it must first be created in the Data Source before it is available within Insite. See Assets in the Insite help for more details.

Exit Point Manager Assets

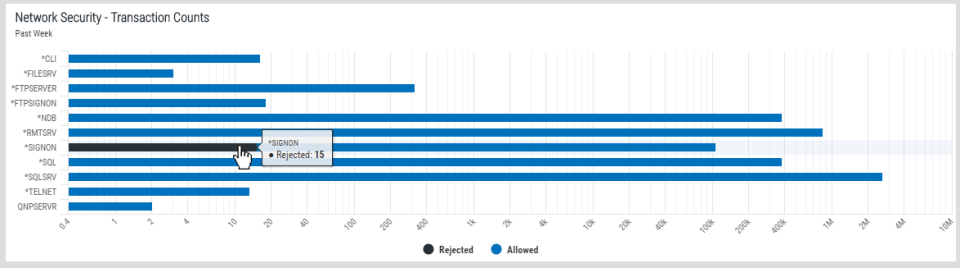
Hourly Stats

This widget displays a timeline of recent activity can be displayed for any number of servers and shows all activity that has occurred on active servers in the past 24-hours.

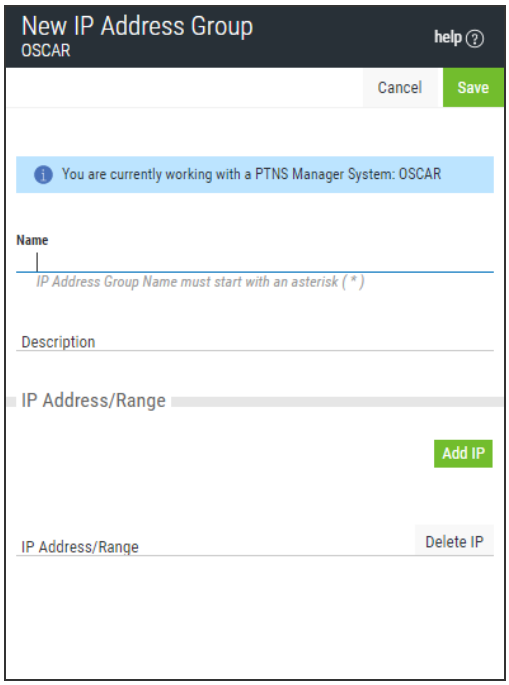


Transaction Counts

The Transaction Count asset lists the number of accepted and rejected transactions for each server over a specified time range.



New/Edit IP Address screen



How to Get There

Choose the **IP Address Groups** tab on the navigation pane on the left side of the Insite window, then clicktap **Add**. Or, click an existing IP Address Group to edit it.

What it Does

The New IP Address screen is used to associate multiple locations to one (group) identifier. The Edit IP Address screen is used to edit an existing (group) identifier.

Options

Delete (edit only)

When editing an existing IP Address Group, choose **Delete** to delete the Group.

Save

Choose **Save** to save the IP Address Group and return to the IP Address Groups screen.

Cancel

Choose **Cancel** to return to the IP Address Groups screen without making changes.

Field descriptions

Name

This is the short name of the IP Address Group (max 14 characters).

Description

The description of the Address Group. It is a required entry.

IP Address/Range

An IP Address Group can include one IP address or a range of IP addresses. To delete values, click the 'X' icon to the right of each input. IP Address ranges can be separated by a dash or a colon.

Examples:

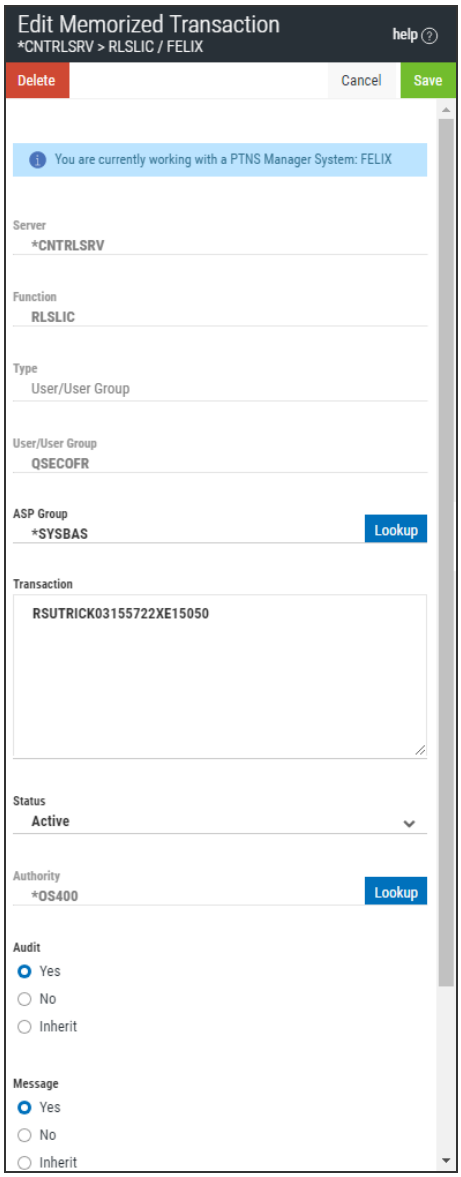
Single: 192.168.0.1
Range 192.168.0.1-192.168.0.255 or 192.168.0.1:192.168.0.255

> **NOTE:** If the IP address group has IP address groupings and has been applied to a location rule, you must delete all rules and groupings before you can delete the address group.

Add values

Choose **Add IP** to display a text field where additional IP addresses or IP address ranges can be added to the group.

New/Edit Memorized Transaction screen



How to Get There

Click the **Memorized Transactions** tab on the navigation pane on the left side of the Exit Point Manager window. In the Memorized Transaction screen, click a memorized transaction.

What it Does

The Edit Memorized Transaction screen allows you to make changes to some of the attributes of a Memorized Transaction. Those attributes that are input capable can be changed.

Options

Save

Choose **Save** to save the Memorized Transaction and return to the Memorized Transactions screen.

Cancel

Choose **Cancel** to return to the Memorized Transactions screen without making changes.

Field Descriptions

Server

A Server in Exit Point Manager is a controlled entry point into your system. These entry points are determined and defined by IBM. Exit Point Manager has assigned easy-to-remember names to these controlled entry points. This field cannot be changed.

Function

A Function, or Server Function, in Exit Point Manager represents a class of operations that a given Server may perform. For example, the *SIGNON Server classifies its operations as those pertaining to changing passwords, generating authentication tokens, and retrieving sign-on information. Exit Point Manager has assigned easy-to-remember names to these Functions, such as CHGPWD, GENAUTTKN and RETRIEVE. This field cannot be changed.

Type

Specifies whether this is a User or Location rule.

User/Location

User represents the identity of the person initiating a transaction as a user profile. The special value *PUBLIC, when used on a rule, means that the rule applies to any User lacking a specific rule. When used as a subset or selection parameter, *PUBLIC means to select all such rules for display or printing. This displays the User to which this Memorized Transaction applies. If blank, then this is for a specific Location. If the value is *PUBLIC, the transaction applies to all users. This field cannot be changed.

Location represents the source of a transaction. Location can hold an IP Address, an IP Address Group or the name of an SNA Communications Device. The special value *ALL, when used on a rule, means that the rule applies to any rule means that the rule applies to any Location lacking a specific rule. when used as a subset or selection parameter, *ALL generally means to select all such rules for display or printing. This displays the Location to which this Memorized Transaction applies. If blank, then this is for a specific User. If the value is *ALL, the transaction applies to all locations. This field cannot be changed.

ASP Group; Lookup

This is the name of an ASP Group. It is used in rule evaluation to determine if an object referenced in a transaction is the one specified on the object entries for this list.

Click **Lookup** to open the Select ASP Group screen where you can choose from the following ASP Groups:

***SYSBAS** The Object List entries refer to those objects in *SYSBAS.

***ALL** The Object List entries refer to those objects in any namespace.

Transaction

The Memorized Transaction against which incoming transactions are tested. If a match is found, then this rule will be invoked. Undisplayable characters in the transaction data are replaced by the mid—dot character (-).

You can use the Transaction wildcard character (%) to make a Transaction generic. The wildcard character is valid only at the end of a Transaction string. When you are memorizing or changing a Memorized Transaction, the first occurrence of the wildcard character that was NOT present in the string before you changed it will make the string generic and all data after that wildcard character will be discarded.

Status

This is the status of the Memorized Transaction.

If this box is checked, the memorized transaction is "Active," and Exit Point Manager will attempt to match this transaction during rule enforcement. Memorized Transactions that are changed to *ACTIVE will have a matching User or Location rule changed to the corresponding action; *ALLOW to *MEMOS400, *REJECT to *MEMREJECT, or *SWITCH to *MEMSWITCH.

If this box is not checked, the memorized transaction is "Inactive," and Exit Point Manager will not attempt to match this transaction during rule enforcement. Memorized Transactions that are changed to *INACTIVE will have the matching User or Location rule changed (if there are no other Memorized Transactions for that rule) to the corresponding action; *MEMOS400 to *ALLOW, *MEMREJECT to *REJECT, or *MEMSWITCH to *SWITCH.

Authority

Authority represents the action to be taken when a rule is found that matches the data present on a transaction.

Choose **Lookup** to specify the new Authority value for the rule. The list of valid values may include one or more of these values:

***OS400** Exit Point Manager will use normal operating system authority for the user.

***REJECT** Exit Point Manager will reject requests.

***SWITCH** Exit Point Manager will use the authority of the switch profile for the transaction. A switch profile entry is required.

Audit

The Audit transactions flag controls the logging of transactions to the Log Journal set up on the work with Exit Point Manager System Values panel. Specify one of these values for Audit transactions:

Yes Logs all requests when this rule is enforced.
No Logs only access failures (rejects) for this rule.
Inherit Uses the value found in the rule above this one in the rule hierarchy.

Message

The Send messages flag controls the sending of messages to the Log Message Queue set up on the work with Exit Point Manager System Values panel.

Specify one of these values for Send messages:

Yes Sends a message when this rule is enforced.
No Does not send a message when this rule is enforced.
Inherit Uses the value found in the rule above this one in the rule hierarchy.

Capture

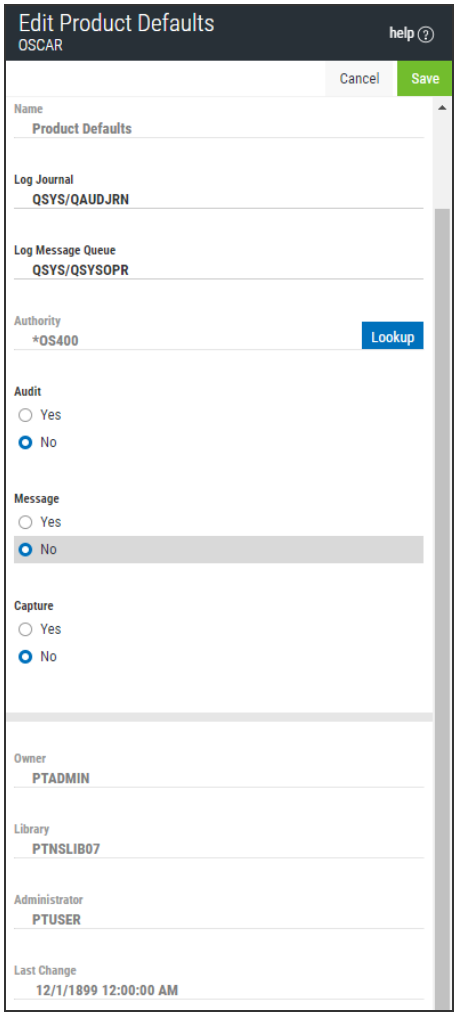
The Capture transactions flag controls whether transactions are remembered in Exit Point Manager for later memorization. Once captured, transactions can become Memorized Transactions which can act as rules. Specify one of these values for Captured transactions:

Yes Captures the transaction when this rule is enforced.
No Does not capture the transaction when this rule is enforced.
Inherit Uses the value found in the rule above this one in the rule hierarchy.

Select which systems to save to

All managed systems are listed here. Check the systems you would like to save the memorized transaction to. Or, check Select All to copy the memorized transaction to all managed systems.

Edit Product Defaults screen



How to Get There

Click the **Product Configuration** tab on the navigation pane on the left side of the Insite window. On the Product Configuration screen, select **System Values (Product Defaults)**.

What it Does

The Edit System Values screen allows you to maintain product defaults for Powertech Exit Point Manager. The system values for Log Journal and Log Message Queue can be maintained any time.

On the green screen interface, these values can be found at Work with System Values.

Field Descriptions

The following describes the parameters and allowable values for each field on the Work with System Values screen.

Name

Indicates you are viewing Product Defaults.

Log Journal

This is the library/name of the journal that Powertech Exit Point Manager will log information. You can control the level of detail with the audit flag when you specify location and user authorities. Most installations will specify QSYS/QUADJRN.

The Log Journal Library specifies the library where the log journal is located.

Notes:

1. You also can specify *NONE in the Log Journal Name field. However, if a journal name of *NONE is found in the Exit Point Manager system values, network transactions are not journaled.
2. Some versions of Powertech Compliance Monitor expect Exit Point Manager audit entries to be written to QSYS/QAUDJRN. Contact Powertech technical support if you need further information concerning log journal entries.

Log Message Queue

This is the library/name of the message queue, where Powertech Exit Point Manager sends messages. Messages are sent to this queue when specified on location and user authority records. Most installations specify QSYS/QSYSOPR.

The log message queue library is the library where the log message queue is located.

Authority

The authority assigned if no other authority is found for a server or function. Possible values are:

***OS400** Exit Point Manager allows the transaction without taking any action
***REJECT** Exit Point Manager rejects requests for the transaction
***SWITCH** Exit Point Manager switches the job to run as the user profile specified in the Switch field.

Audit

Controls the type of requests Exit Point Manager will log. Exit Point Manager uses this value if no other value is entered for a server or function. Possible values are:

Yes Log All requests
No Only log authority failures

Message

Determines if Exit Point Manager sends a message to the log message queue. Exit Point Manager uses this value if no other value is entered for a server or function. Possible values are:

Yes A message is sent to the specified queue
No No message is sent

Capture

Capture transactions for Memorized Transaction Request (MTR). Exit Point Manager uses this value if no other value is entered for a server or function. Possible values are:

Yes Capture transactions
No Do not capture transactions

Owner

The product owner is the name of the user profile that owns all data objects and exit programs in the Powertech Exit Point Manager product.

Library

The product library is the library that contains all of the Powertech Exit Point Manager objects.

Administrator

The product administrator is the name of the user profile that owns administrative program objects in the Powertech Exit Point Manager product. We recommend granting administrators *USE authority to the PTADMIN authorization list using the following command, where myuser is the administrator profile to add.

ADDAUTLE AUTL(PTADMIN) USER(myuser) AUT(*USE)

> **NOTE:** To access reporting functions, administrators must be authorized to the PTNSRPT authorization list.

For more information, see Granting Reporting Authority.

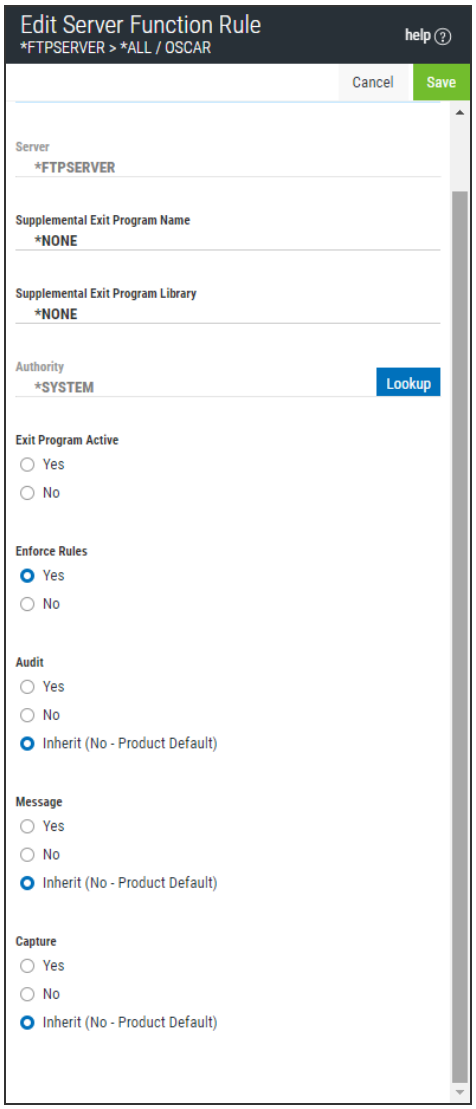
Once authorized to the PTADMIN and PTNSRPT authorization lists, the administrator has all the authorities needed to administer Powertech Exit Point Manager. Product administrators have *CHANGE authority to Exit Point Manager data and *USE authority to Exit Point Manager programs.

> **NOTE:** Users set to the *SECOFR User Class do not need to be members of the PTADMIN or PTNSRPT authorizations lists to use Exit Point Manager or Exit Point Manager Reports.

Last Change User/Date/Time

The user profile that changed the Exit Point Manager system values and the date and time the changes were made.

Edit Server Function Rule screen



How to Get There

Click the **Product Configuration** tab on the navigation pane on the left side of the Insite window. In the Product Configuration window, click a server. This screen opens with *ALL appended to the title, indicating the settings apply to all server functions.

Alternatively, in the Product Configuration screen, click to display a server's functions, then click a function to display settings specific to that function.

What it Does

The Edit Server Function Rule screen is used to maintain the server function's properties. Server function options provide processing control to Powertech's exit programs. They also act as defaults for location, user, and memorized transaction request level values.

Field Descriptions

Server
The server ID is the name of the server that options are being specified for.

Function
The function is the name of the function for a server that options are being specified for.

Function Description
The description of the server function whose options are being displayed.

Options

Supplemental Exit Program Name and Library
The name and library of the supplemental exit program for the selected server. Supplemental exit programs are executed after Exit Point Manager has processed the server transaction.

The default value for both the Supplemental Exit Program Name and the Supplemental Exit Program Library field is *NONE.

Authority
The authority assigned to the server function. The value entered here is used when *SRVFCN authority is placed on a location, user, or memorized transaction request.

Possible values are:

***SERVER** Use the authority defined for the function's server, which you can display and change by displaying this screen for *ALL functions of the selected server. This value can only be selected when the screen is displayed for a specific function of the selected server.
***SYSTEM** Use the authority defined in Exit Point Manager Product Defaults. This value can only be selected when displaying the settings for *ALL functions of the selected server.
***OS400** Use normal IBM i authority for the server.
***REJECT** Reject all requests to the server.
***SWITCH** Use the authority of the switch profile for the server. A switch profile entry is required.
***MEMOS400** Check Memorized Transactions (MTR) for authority. If no MTR authority is encountered, Exit Point Manager will use normal IBM i authority for the server.
***MEMREJECT** Check Memorized Transactions (MTR) for authority. If no MTR authority is encountered, Exit Point Manager will reject requests for the server.
***MEMSWITCH** Check Memorized Transactions (MTR) for authority. If no MTR authority is encountered, Exit Point Manager will use the authority of the switch profile for the server. A switch profile entry is required.
***MEMOBJ** Check Memorized Transactions (MTR) for authority. If no MTR authority is encountered, Exit Point Manager will check the transaction against the Object Rules.

> **NOTE:** If the server has not been activated, you will not be able to save with Enforce Rules checked. See Activating Powertech Exit Point Manager.

Exit Program Active
Indicates whether the Powertech Exit Point Manager exit program is activated for this server. This is a display-only setting. If you wish to deactivate the exit program for a server, refer to the help on

Activating Powertech Exit Point Manager.

This option is only displayed if the screen is displayed for *ALL functions of the selected server. If a specific function is selected, this option is not displayed.

Enforce Rules

Check this box to enforce Exit Point Manager rules defined for this server. This option is only displayed if the screen is displayed for *ALL functions of the selected server. If a specific function is selected, this option is not displayed.

Audit

Controls the type of requests Exit Point Manager will log to the server/for the function. Possible values are:

- Log all requests to the server for the server/function.
- Log only authority failures for the server/function.
- or (inherit) Product defaults.

Message

Specifies if Exit Point Manager sends a message to the message queue specified in Powertech's System Values. Possible values are:

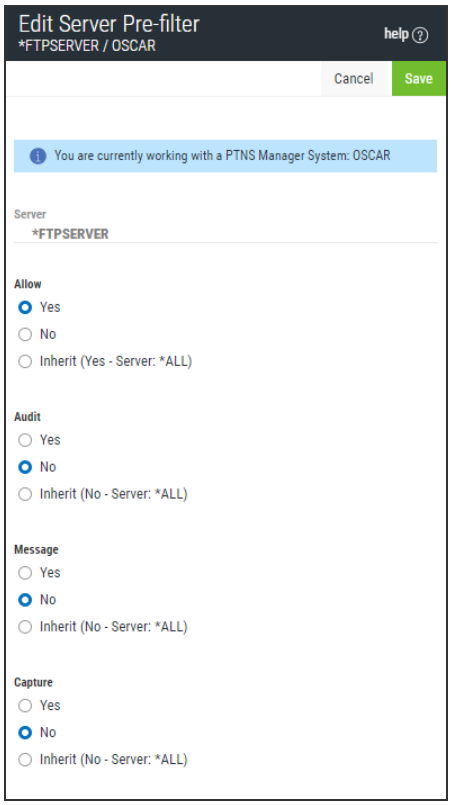
- A message is sent to the specified queue.
- No message is sent.
- or (inherit) Product defaults.

Capture Transactions

Capture transactions for Memorized Transaction Requests (MTRs). Possible values are:

- Capture transactions.
- Do not capture transactions.
- or (inherit) Product Defaults.

Edit Server Pre-filter



How to Get There

Click the **Server Pre-filters** tab on the navigation pane on the left side of the Exit Point Manager window. Click a Server Pre-filter.

What it Does

Use this screen to edit a Server Pre-filter.

Options

Allow

The setting for whether transactions matching this record should be allowed to continue to be processed by Exit Point Manager. Valid settings are

Yes Exit Point Manager rules should evaluate this transaction, which may or may not cause it to be rejected,
No Reject the transaction, and Inherit — inherit the value from the System (*ALL) Pre-filter.

Audit

The audit property controls the type of requests Exit Point Manager will log. Possible values are:

✔ Log all requests by the location/server/function.
✘ Only log authority failures for the location/server/function.
✔ or ✘ (inherit) Uses the value found in the rule above this one in the rule hierarchy.

Message

The message property entry will determine if Exit Point Manager sends a message to the Exit Point Manager message queue.

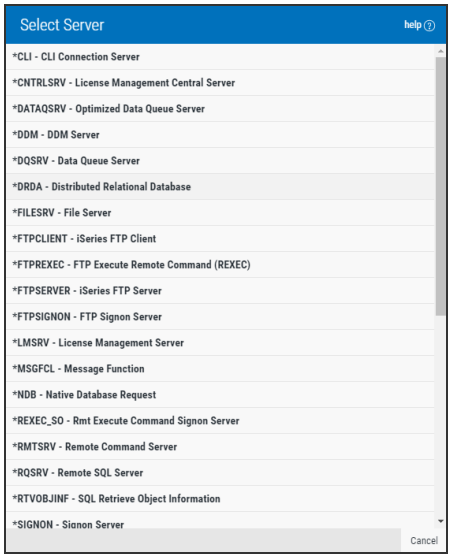
- A message is sent to the Exit Point Manager message queue.
- No message is sent.
- or (inherit) Uses the value found in the rule above this one in the rule hierarchy.

Capture

Capture transactions for Memorized Transaction Request (MTR).

- Capture transactions.
- Do not capture transactions.
- or (inherit) Uses the value found in the rule above this one in the rule hierarchy.

Functions Selection window



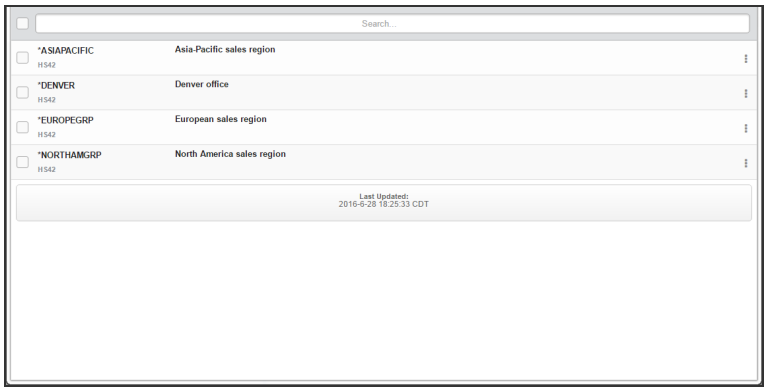
How to Get There

This window is available by choosing a server in the Servers selection window.

What it Does

This window allows you to select a server function when adding or changing a Rule or User+Location Pre-filter.

IP Address Groups screen



How to Get There

Click the **IP Address Groups** tab on the navigation pane on the left side of the Exit Point Manager window.

What it Does

The IP Address Groups panel is used when a number of IP addresses need the same group filter rules applied. You can use this panel to add or change IP Address groups.

Options

Selection, sorting, filtering, deleting, and navigation features on this panel are described in Using the Web Browser Interface.

Add

Choose **Add** to open the New IP Address panel where you can add a new IP Address Group. See New IP Address panel.

Column Descriptions

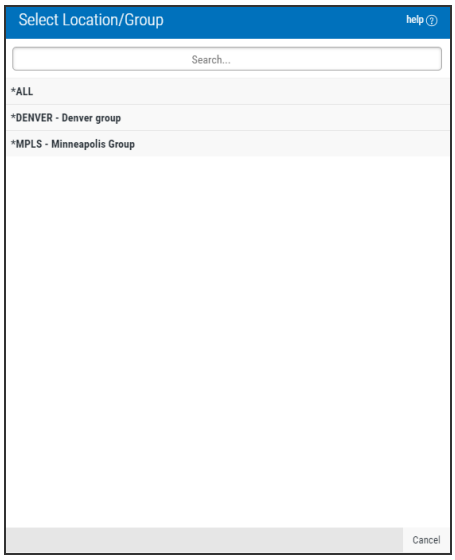
Group Name

The name of an IP Address Group. It must begin with special character "*".

Description

The description of the Address Group as defined in the New/Edit IP Address panel.

Location/Group Selection window



How to Get There

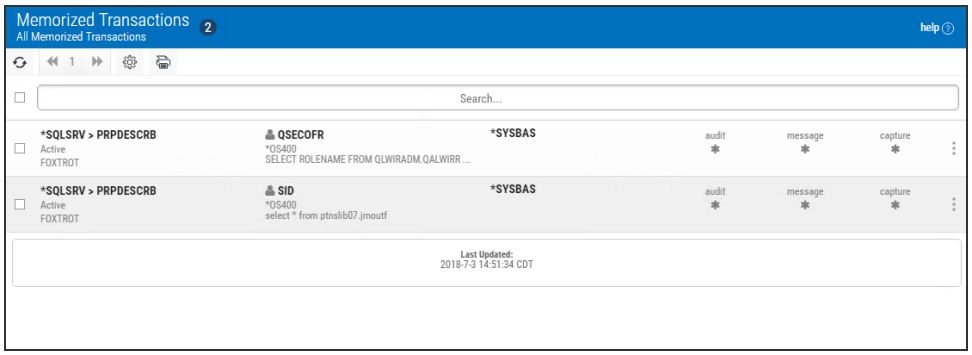
Choose **Lookup** next to the Location/Group field when adding or changing location rules.

What it Does

This window allows you to select an IP address group.

This list includes all existing IP Address Groups. IP Address Groups are defined in the IP Address Groups screen.

Memorized Transactions screen



How to Get There

Click the **Memorized Transactions** tab on the navigation pane on the left side of the Insite window.

What it Does

The Memorized Transactions screen enables you to maintain memorized transactions. To create a Memorized Transaction, you can select the **Memorize** button on the View Transaction screen.

Options

Selection, sorting, filtering, deleting, and navigation features on this screen are described in Using the Web Browser Interface.

Click a memorized transaction to open the Edit Memorized Transaction screen where you can view and edit a memorized transaction.

Field Descriptions

Server > Function

A Server in Exit Point Manager is a controlled entry point into your system. These entry points are determined and defined by IBM. Exit Point Manager has assigned easy-to-remember names to these controlled entry points.

A Function, or Server Function, in Exit Point Manager represents a class of operations that a given Server may perform. For example, the *SIGNON Server classifies its operations as those pertaining to changing passwords, generating authentication tokens, and retrieving sign-on information. Exit Point Manager has assigned easy-to-remember names to these Functions, such as CHGPWD, GENAUTTKN and RETRIEVE.

Status

This is the status of the Memorized Transaction, listed directly under the Server and Function. Possible values are:

*ACTIVE Exit Point Manager will attempt to match this transaction during rule enforcement. Memorized Transactions that are changed to *ACTIVE will have a matching User or Location rule changed to the corresponding action; *ALLOW to *MEMOS400, *REJECT to *MEMREJECT, or *SWITCH to *MEMSWITCH.

*INACTIVE Exit Point Manager will not attempt to match this transaction during rule enforcement. Memorized Transactions that are changed to *INACTIVE will have the matching User or Location rule changed (if there are no other Memorized Transactions for that rule) to the corresponding action; *MEMOS400 to *ALLOW, *MEMREJECT to *REJECT, or *MEMSWITCH to *SWITCH.

User /Location

User represents the identity of the person initiating a transaction as a user profile. The special value *PUBLIC, when used on a rule, means that the rule applies to any User lacking a specific rule. when used as a subset or selection parameter, *PUBLIC means to select all such rules for display or printing. This displays the User to which this Memorized Transaction applies. If blank, then this is for a specific Location. If the value is *PUBLIC, the transaction applies to all users.

Location represents the source of a transaction. Location can hold an IP Address, an IP Address Group or the name of an SNA Communications Device. The special value *ALL, when used on a rule, means that the rule applies to any rule means that the rule applies to any Location lacking a specific rule. when used as a subset or selection parameter, *ALL generally means to select all such rules for display or printing. This displays the Location to which this Memorized Transaction applies. If blank, then this is for a specific User. If the value is *ALL, the transaction applies to all Users.

ASP Group

This is the name of an ASP Group. It is used in rule evaluation to determine if an object referenced in a transaction is the one specified on the object entries for this list.

Possible values are:

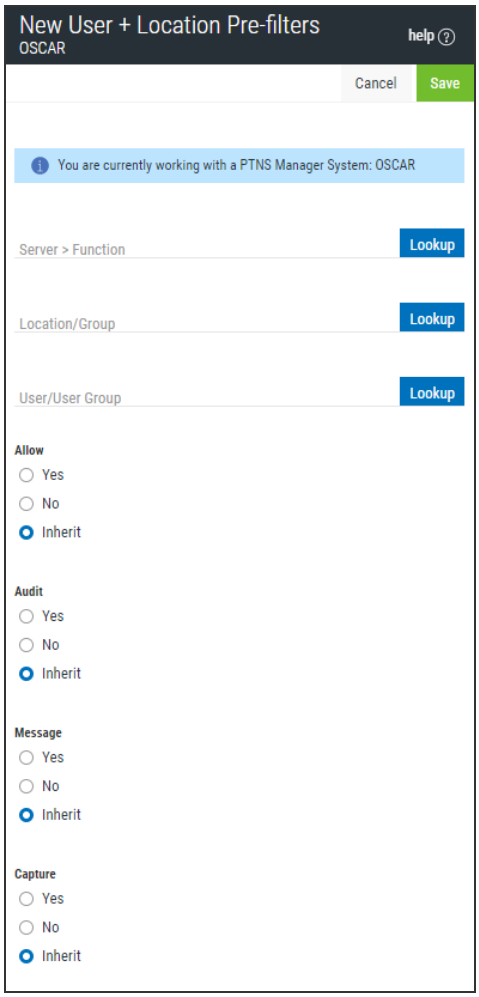
- ***SYSBAS** The Object List entries refer to those objects in *SYSBAS.
- ***ALL** The Object List entries refer to those objects in any namespace.

Authority

Authority represents the action to be taken when a rule is found that matches the data present on a transaction. This field may hold one of these values:

***USER** Current user authority is used.
***OS40O** Exit Point Manager will use normal operating system authority for the user.
***REJECT** Exit Point Manager will reject requests.
***SWITCH**Exit Point Manager will use the authority of the switch profile for the transaction. A switch profile entry is required.
***MEMUSR** Memorized Transactions (MTR) are checked for authority first. If no MTR authority is encountered, Exit Point Manager will use the authority of the current user.
***MEMOS400** Memorized Transactions (MTR) are checked for authority first. If no MTR authority is encountered, Exit Point Manager will use normal operating system authority for the user.
***MEMREJECT** Memorized Transactions (MTR) are checked for authority first. If no MTR authority is encountered, Exit Point Manager will reject requests for the specified user.
***MEMSWITCH** Memorized Transactions (MTR) are checked for authority first. If no MTR authority is encountered, Exit Point Manager will use the authority of the switch profile for the specified user. A switch profile entry is required.
***MEMOBJ** Memorized Transactions (MTR) are checked for authority first. If no MTR authority is encountered, Exit Point Manager will check any objects used in the transactions for authorities defined by Object Rules.
***SERVER** Exit Point Manager will use the authority defined for the Server.
***SRVFCN** Exit Point Manager will use the authority defined for the Server Function.

New/Edit User+Location Pre-filter screen



How to Get There

Choose the **User+Location Pre-filters** on the navigation pane on the left side of the Insite window. Choose **Add** to add a new Pre-filter. Or, click an existing Pre-filter to edit it.

What it Does

The New User+Location Pre-filter screen is used to add new User+Location Pre-filters. The Edit User+Location Pre-filter screen includes identical options and is used to edit an existing User+Location Pre-filter.

Options

Delete (edit only)

Choose **Delete** to delete the Pre-filter.

Server > Function; Lookup

Choose this **Lookup** button to open the Servers selection window where you can choose from a list of servers and server functions. For a description of servers and functions, see Appendix B: Servers

and Functions.

Location/Group; Lookup

Choose this **Lookup** button to open the Location/Group selection window where you can choose from a list of IP Address Groups.

Unlike most fields in Exit Point Manager, the Location field can be populated by manually typing into the field. You type an IP address, SNA device, or IP Address group manually. The following lists the syntax criteria for valid IP address values and other devices:

- Must have 4 nodes separated by periods.
- Each node can have a value between 0 and 255.
- No Alpha characters allowed in the IP address other than "." And "*"
- Therefore The IP address cannot be more than 15 chars long including the three "."
- The wild card character "*" is allowed as the last character of an address, in which case the IP address can have fewer than 4 nodes. If using the "*" wild card then the node cannot have more than 3 characters.
    - Valid IP addresses have to follow the following format where n=number: n.n.n.n n can be 1 digit, 2 digit or 3 digit numbers.
        - 192.168.1.1
        - 192.168.001.001
        - 192.000.000.000
    - Invalid IP addresses
        - 923.4.1.1 (1923 > 255)
        - 192.0000.1.1 (0000 is a 4 digit number)
        - 192.168.R.3 (R is an invalid character for an IP address.)
    - Valid IP addresses with wildcard
        - 192.*
        - 19*
        - 192.168.*
        - 192.168.1.*
        - 192.168.1.00*
    - Invalid IP addresses with wildcard
        - 192* (too many characters in the first node.
        - 192.*.0.0 (No characters allowed after the "*".
        - 192.*.* (No characters allowed after the first "*".
    - Others
        - *192.168.1.1 (Would be validated server side as a IP Address group name because the first character is a "*")
        - Nameofdevice (Would be validated server side as a SNA device name because first character is alpha)

User/User Group; Lookup

Choose this **Lookup** button to open the Users selection window where you can choose from a list of Users.

Allow

The setting for whether transactions matching this record should be allowed to continue to be processed by Exit Point Manager. Valid settings are Yes — Exit Point Manager rules should evaluate this transaction, which may or may not cause it to be rejected, No — reject the transaction, and Inherit — inherit the value from the System (*ALL) Pre-filter.

Audit

The audit property controls the type of requests Exit Point Manager will log. Possible values are:

Yes Log all requests by the location/server/function.
No Only log authority failures for the location/server/function.
Inherit Inherit the value.

Message

The message property entry will determine if Exit Point Manager sends a message to the Exit Point Manager message queue.

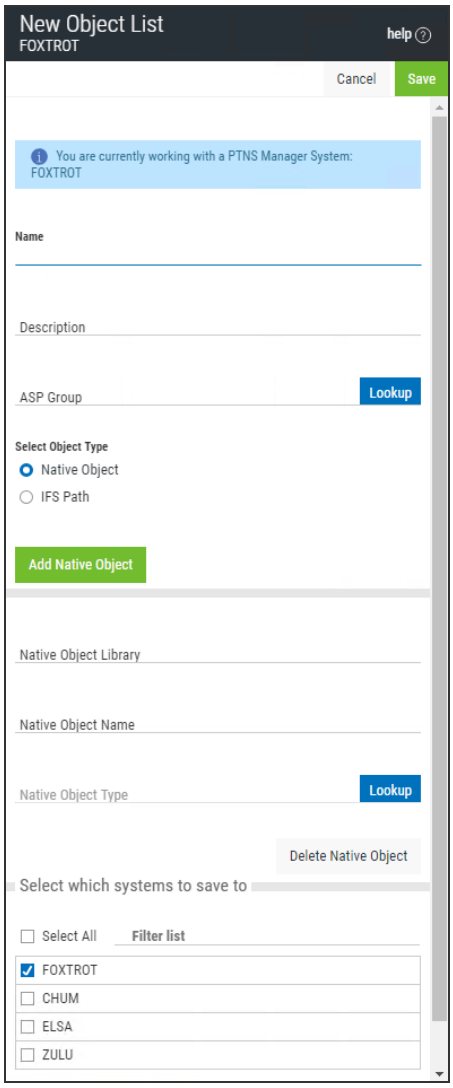
Yes A message is sent to the Exit Point Manager message queue.
No No message is sent.
Inherit Inherit the value.

Capture

Capture transactions for Memorized Transaction Request (MTR).

Yes Capture transactions.
No Do not capture transactions.
Inherit Inherit the value.

New/Edit Object List



How to Get There

Choose the **Object Lists** tab on the navigation pane on the left side of the Exit Point Manager window, then choose **Add**.

What it Does

The New Native Object List screen is used to define a new Native Object List. The Edit Native Object List screen is used to edit an existing Native Object List.

Options

Cancel

Choose **Cancel** to return to the Object Lists screen without making changes.

Save

Choose **Save** to save the Object list

Field Descriptions

Name
The name of the Object List.

Description
The Object List's description.

ASP Group; Lookup
This is the name of an ASP Group. It is used in rule evaluation to determine if an object referenced in a transaction is the one specified on the object entries for this list.

Click **Lookup** to open the Select ASP Group screen where you can choose from the following ASP Groups:

***SYSBAS** The Object List entries refer to those objects in *SYSBAS.

***ALL** The Object List entries refer to those objects in any namespace.

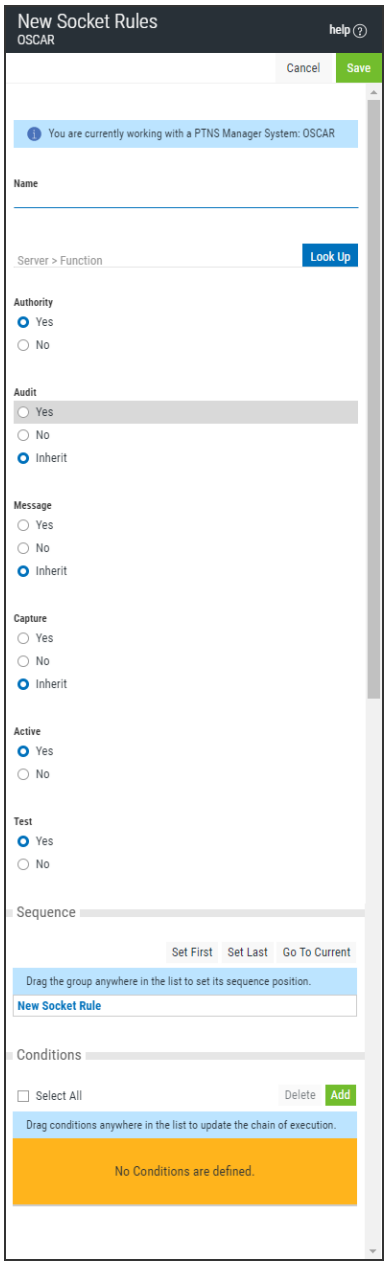
Select Object Type
This is the type of Object List; Native Object, or IFS Path. The Object List type determines what type of entries can be added to an Object List. Object lists can hold native object specifications (library, object and type) or paths to IFS objects.

Native Object Library, Name, and Type (for Native Object Lists only)
In the first two fields, enter the Library and Name of the object. Choose **Lookup** to open the Types of Object Entries selection window where you can select the Object type.

IFS Path (for IFS Object Lists only)
Each slot includes the path of an IFS object in the Object List. This name is required to be a valid OS name.

Select which systems to save to
All managed systems are listed here. Check the systems you would like to save the Object List to. Or, check Select All to copy the Object List to all managed systems.

New/Edit Socket Rule screen



How to Get There

1. On the Navigation Pane, choose **Socket Rules**.
2. Click **Add**. Or, to edit an existing Socket Rule, click the ⋮ icon adjacent to the Socket Rule you would like to change and choose **Edit**.

What it Does

The New Socket Rule screen is used to add new Socket Rules. The Edit Socket Rule screen is used to edit Socket Rules.

Options

Name
The name of the Socket Rule.

Server > Function; Lookup
Choose **Lookup** for a new rule to open the Servers selection window where you can choose from the socket Accept (QSOACCEPT), Connect (QSOCONNECT), and Listen (QSOLISTEN) servers. For a description of servers and functions, see Appendix B: Servers and Functions.

Authority; Lookup

Y Exit Point Manager will allow requests when this rule is enforced.
N Exit Point Manager will reject requests when this rule is enforced.

Audit
The audit property controls the type of requests Exit Point Manager will log.

Possible values are:

Yes Log all requests by the location/server/function.
No Only log authority failures for the location/server/function.
Inherit Inherit the value.

Message
The message property entry will determine if Exit Point Manager sends a message to the Exit Point Manager message queue.

Possible values are:

Yes A message is sent to the Exit Point Manager message queue.
No No message is sent.
Inherit Inherit the value.

Capture
Capture transactions for Memorized Transaction Request.

Possible values are:

Yes Capture transactions.
No Do not capture transactions.
Inherit Inherit the value.

Active
The Socket Rule Active flag determines whether the rule will be evaluated by the exit point program.

It can be useful to initially set a Socket Rule as not active in order to test it without enforcing it.

The valid values are:

Yes Exit Point Manager will evaluate the rule.
No Exit Point Manager will not evaluate the rule.

The value N is not allowed for the default Socket Rule (sequence number 99999).

Test

The Socket Rule Test flag determines whether the rule will be evaluated by the Socket Rule test facility.

It can be useful to flag a rule to not be tested in order to verify the effects of removing that rule.

The value N is not allowed for the default Socket Rule (sequence number 99999).

The valid values are:

Yes The Socket Rule test facility will evaluate the rule.
No The Socket Rule test facility will not evaluate the rule.

Sequence

Set First • Set Last • Go To Current

This list shows the sequence used to determine the order in which this Socket Rule will be evaluated.

For example, if there are three Socket Rules for a specific Server/Function (e.g. QSOACCEPT), then the Socket Rule at the top of this list will be used.

Click **Set First** to move the current Socket Rule to the top of the list.
Click **Set Last** to move the current Socket Rule to the bottom of the list.
Click **Go To Current** to automatically scroll the list so that the currently selected Socket Rule is visible.

Conditions

Use this section to view or change Socket Rule conditions.

[Conditions list]

The sequence number of a Socket Condition determines the order in which it is combined with other Socket Conditions for a Socket Rule.

Connector

The connector determines how a Socket Condition relates to other Socket Conditions for a Socket Rule.

Socket Conditions with a higher order of precedence are evaluated before ones with a lower order of precedence.

The connector for the Socket Condition with the lowest sequence number is ignored.

The valid values are:

OR This Socket Condition is OR'ed with others. An OR has the lowest order of precedence (evaluated last).
AND This Socket Condition is AND'ed with others. An AND has a higher order of precedence than an OR, but lower than an ORAND.
ORAND This Socket Condition is OR'ed with others. An ORAND has the highest order of precedence (evaluated first).

[Field]

This is the name of the field to be evaluated at run time.

The valid values are dependent on the Socket Rule.

Valid values for the QSOLISTEN server are:

LCL_PORT The local port number; an integer between 1 and 65535.
LCL_USR The user profile associated with the job issuing the listen.
LCL_USR_GRP A User Group containing the user profile associated with the job issuing the listen.

Valid values for the QSOCONNECT server are:

LCL_PORT The local port number; an integer between 1 and 65535.
RMT_PORT The remote port number; an integer between 1 and 65535.
RMT_ADDR The remote address. Valid formats are IPv4, IPv6, and Powertech Exit Point Manager IP address groups.
LCL_USR The user profile associated with the job issuing the connect.
LCL_USR_GRP A User Group containing the user profile associated with the job issuing the connect.

Valid values for the QSOACCEPT server are:

LCL_IN_PORT The local incoming port number; an integer between 1 and 65535.
LCL_BND_PORT The local bound port number; an integer between 1 and 65535.
RMT_PORT The remote port number; an integer between 1 and 65535.
RMT_ADDR The remote address. Valid formats are IPv4, IPv6, and Powertech Exit Point Manager IP address groups.
LCL_USR The user profile associated with the job issuing the accept.
LCL_USR_GRP A User Group containing the user profile associated with the job issuing the accept.

[Operator]

The test used for the value of the field and the criteria to evaluate this Socket Condition.

= The value of the field is equal to the criteria, or, if the criteria can be a list, the value of the field is found in that list.
<> The value of the field is not equal to the criteria, or, if the criteria can be a list, the value of the field is not found in that list.
> The value of the field is greater than the criteria.
< The value of the field is less than the criteria.
>= The value of the field is greater than or equal to the criteria.
<= The value of the field is less than or equal to the criteria.
ALWAYS This will cause the condition to always match. It is used on the Socket Condition of the default Socket Rule, and may be used on non-default Socket Rules. If present, it must be the only Socket Condition for a Socket Rule.

[Criteria]

This is the value against which the value of the selected field will be compared at run time.

The valid values are dependent on the selected Field.

Delete • Add •Edit • OK

Select a condition and press **Delete** to remove the condition.

Select **Add** to add a new condition.

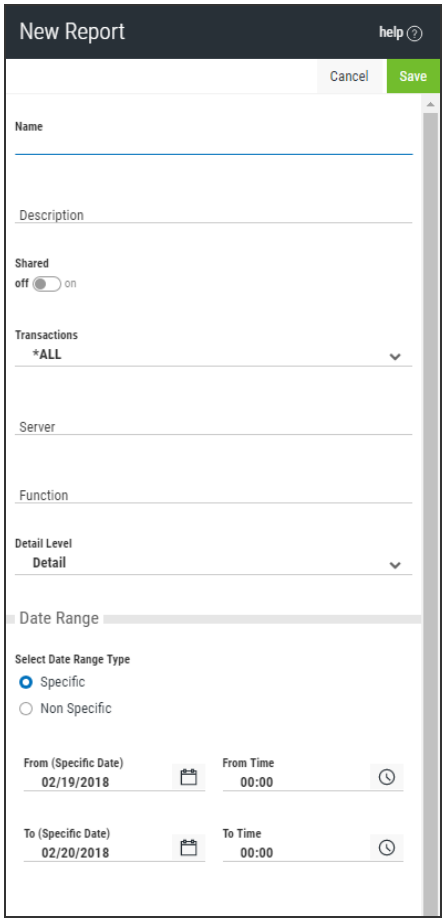
Select **Edit** to change a condition.

Select **OK** to confirm a condition.

Save • Cancel

Click **Save** to save the Socket Rule to the database. Choose **Cancel** to dismiss the screen without making changes.

New/Edit Report screen



How to Get There

In the Navigation Pane, click **Reports**, then click **Add**. The Add Report screen appears. Select the kind of report you would like to create.

Or, to edit an existing report, on the Reports screen, click the report you would like to edit.

What it Does

Use the New Report screen to define a new report. Use the Edit Report screen to edit an existing report.

Options

Intrusion Detection - User Report

Name

The name of the report.

Description
The description of the report.

Shared: On/Off
This allows you to choose whether or not you want to share the report.

Transactions

- ***ALL** This option produces a report of all current transactions for the User.
- ***ALLOW** This option produces a report of all current allowed transactions for the User.
- ***REJECT** This option produces a report of all current rejected transactions for the User.

User
User represents the identity of the person initiating a transaction as a user profile. The special value *PUBLIC, when used on a rule, means that the rule applies to any User lacking a specific rule. When used as a subset or selection parameter, *PUBLIC means to select all such rules for display or printing.

Date Range

- **Specific** - Choose this option if you want to specify a specific To and From date for the range of the report.
- **Non-specific** - Choose this option if you want to specify a relative To and From date for the range of the report (for example, transactions for the last two days).

From (Specific Date/Days Ago)
If Date Range is set to Specific, this field is the oldest specific transaction date you wish to see. If Date Range is set to Non-specific, this value represents the number of days previous to the current date. A value of 0 is the current date.

From Time
This field is the oldest transaction time you wish to see on the chosen From Date.

To Date (Specific Date/Days Ago)
If Date Range is set to Specific, this field is the most recent specific transaction date you wish to see. If Date Range is set to Non-specific, this value represents the number of days previous to the current date. A value of 0 is the current date.

To Time
This field is the most recent transaction time you wish to see on the chosen To Date.

Detail Level
This field controls the amount of information shown on the report. Select one of the following values:

Detail Detail information.

Summary Summary information (least amount of detail)

Transaction Transaction information (greatest amount of detail).

Intrusion Detection - Location Report

Name
The name of the report.

Description
The description of the report.

Shared: On/Off
This allows you to choose whether or not you want to share the report.

Transactions

- ***ALL** This option produces a report of all current transactions for the Location.
- ***ALLOW** This option produces a report of all current allowed transactions for the Location.
- ***REJECT** This option produces a report of all current rejected transactions for the Location.

Location
Location represents the source of a transaction. Location can hold an IP Address, an IP Address Group or the name of an SNA Communications Device. The special value *ALL, when used on a rule, means that the rule applies to any Location lacking a specific rule. When used as a subset or selection parameter, *ALL generally means to select all such rules for display or printing.

Date Range

- **Specific** - Choose this option if you want to specify a specific To and From date for the range of the report.
- **Non-specific** - Choose this option if you want to specify a relative To and From date for the range of the report (for example, transactions for the last two days).

From (Specific Date/Days Ago)
If Date Range is set to Specific, this field is the oldest specific transaction date you wish to see. If Date Range is set to Non-specific, this value represents the number of days previous to the current date. A value of 0 is the current date.

From Time
This field is the oldest transaction time you wish to see on the chosen From Date.

To Date (Specific Date/Days Ago)
If Date Range is set to Specific, this field is the most recent specific transaction date you wish to see. If Date Range is set to Non-specific, this value represents the number of days previous to the current date. A value of 0 is the current date.

To Time
This field is the most recent transaction time you wish to see on the chosen To Date.

Detail Level
This field controls the amount of information shown on the report. Select one of the following values:

Detail Detail information.

Summary Summary information (least amount of detail)

Transaction Transaction information (greatest amount of detail).

Intrusion Detection - Server/Function Report

Name
The name of the report.

Description
The description of the report.

Shared: On/Off
This allows you to choose whether or not you want to share the report.

Transactions

- ***ALL** This option produces a report of all current transactions for the server and function.
- ***ALLOW** This option produces a report of all current allowed transactions for the server and function.
- ***REJECT** This option produces a report of all current rejected transactions for the server and function.

Server
A Server in Exit Point Manager is a controlled entry point into your system. These entry points are determined and defined by IBM. Exit Point Manager has assigned easy-to-remember names to these controlled entry points.

Specify the name of the Server to include in the report. Leave this field blank to select all Servers.

Function
A Function, or Server Function, in Exit Point Manager represents a class of operations that a given Server may perform. For example, the *SIGNON Server classifies its operations as those pertaining to changing passwords, generating authentication tokens, and retrieving signon information. Exit Point Manager has assigned easy-to-remember names to these Functions, such as CHGPWD, GENAUTTKN and RETRIEVE.

Date Range

- **Specific** - Choose this option if you want to specify a specific To and From date for the range of the report.
- **Non-specific** - Choose this option if you want to specify a relative To and From date for the range of the report (for example, transactions for the last two days).

From (Specific Date/Days Ago)
If Date Range is set to Specific, this field is the oldest specific transaction date you wish to see. If Date Range is set to Non-specific, this value represents the number of days previous to the current date. A value of 0 is the current date.

From Time
This field is the oldest transaction time you wish to see on the chosen From Date.

To Date (Specific Date/Days Ago)

If Date Range is set to Specific, this field is the most recent specific transaction date you wish to see. If Date Range is set to Non-specific, this value represents the number of days previous to the current date. A value of 0 is the current date.

To Time

This field is the most recent transaction time you wish to see on the chosen To Date.

Detail Level

This field controls the amount of information shown on the report. Select one of the following values:

Detail Detail information.

Summary Summary information (least amount of detail)

Transaction Transaction information (greatest amount of detail).

Intrusion Detection - Transaction Report

Name

The name of the report.

Description

The description of the report.

Shared: On/Off

This allows you to choose whether or not you want to share the report.

Transaction Type

- ***RUN** - Network Transactions that Run commands and programs. This option produces a report of transactions that resulted in a command or program being executed and sorts by Server/Function/Date/Time. You will be prompted for Type and Date/Time range on a later screen.
- ***UPDATE** - Network Transactions that Update data. This option produces a report of transactions that resulted in data being updated and sorts by Server/Function/Date/Time. You will be prompted for Type and Date/Time range on a later screen.
- ***READ** - Network Transactions that Read data. This option produces a report of transactions that resulted in data being read and sorts by Server/Function/Date/Time. You will be prompted for Type and Date/Time range on a later screen.
- ***MODIFY** - Network Transactions that Modify objects. This option produces a report of transactions that resulted in objects being modified and sorts by Server/Function/Date/Time. You will be prompted for Type and Date/Time range on a later screen.

Date Range

- **Specific** - Choose this option if you want to specify a specific To and From date for the range of the report.
- **Non-specific** - Choose this option if you want to specify a relative To and From date for the range of the report (for example, transactions for the last two days).

From (Specific Date/Days Ago)
If Date Range is set to Specific, this field is the oldest specific transaction date you wish to see. If Date Range is set to Non-specific, this value represents the number of days previous to the current date. A value of 0 is the current date.

From Time
This field is the oldest transaction time you wish to see on the chosen From Date.

To Date (Specific Date/Days Ago)
If Date Range is set to Specific, this field is the most recent specific transaction date you wish to see. If Date Range is set to Non-specific, this value represents the number of days previous to the current date. A value of 0 is the current date.

To Time
This field is the most recent transaction time you wish to see on the chosen To Date.

Detail Level
This field controls the amount of information shown on the report. Select one of the following values:

Detail Detail information.
Summary Summary information (least amount of detail)
Transaction Transaction information (greatest amount of detail).

Intrusion Detection - Group Report

Name
The name of the report.

Description
The description of the report.

Shared: On/Off
This allows you to choose whether or not you want to share the report.

Transactions
- ***ALL** This option produces a report of all the transactions for the Group.
- ***ALLOW** This option produces a report of all the allowed transactions for the Group.
- ***REJECT** This option produces a report of all the rejected transactions for the Group.

Group
Specify the name of the group of users you would like listed in your report. This value can be a Powertech Group, accounting code or group profile. Indicate the type of name in the following field, Group Type.

> **NOTE:** You can specify *NOGRP to list only those users that are NOT part of a group.

Group Type
Specify the type of user group you would like listed in your report using one of these values:

- **Powertech Group** - The name is a Powertech Group name.
- **Account Code** - The name is an accounting code.
- **OS/400 Group Profile** - The name is an operating system group profile.

Date Range

- **Specific** - Choose this option if you want to specify a specific To and From date for the range of the report.
- **Non-specific** - Choose this option if you want to specify a relative To and From date for the range of the report (for example, transactions for the last two days).

From (Specific Date/Days Ago)

If Date Range is set to Specific, this field is the oldest specific transaction date you wish to see. If Date Range is set to Non-specific, this value represents the number of days previous to the current date. A value of 0 is the current date.

From Time

This field is the oldest transaction time you wish to see on the chosen From Date.

To Date (Specific Date/Days Ago)

If Date Range is set to Specific, this field is the most recent specific transaction date you wish to see. If Date Range is set to Non-specific, this value represents the number of days previous to the current date. A value of 0 is the current date.

To Time

This field is the most recent transaction time you wish to see on the chosen To Date.

Detail Level

This field controls the amount of information shown on the report. Select one of the following values:

Detail Detail information.
Summary Summary information (least amount of detail)
Transaction Transaction information (greatest amount of detail).

Access Rule Report - Print by User ID

Name

The name of the report.

Description

The description of the report.

Shared: On/Off

This allows you to choose whether or not you want to share the report.

User

Specify the name of a user whose rules are to be listed.

The valid values are:

Name A specific user profile.
***ALL** All users.

***PUBLIC** The user level for non-specific users.

Object Rules
Indicate whether you would like the Object Rules printed on the report for each User Rule printed.

The valid values are:

***YES** Object Rules are printed on the report.
***NO** Object Rules are not printed on the report.

Memorized Transactions
Indicate whether you would like the Memorized Transactions printed on the report for each User Rule printed.

The valid values are:

***YES** Memorized Transactions are printed on the report.
***NO** Memorized Transactions are not printed on the report.

Access Rule Report - Print by Location

Name
The name of the report.

Description
The description of the report.

Shared: On/Off
This allows you to choose whether or not you want to share the report.

Location
Specifies the location or locations whose rules will be included in the report. Specifying *ALL for this parameter will include rules for all locations.

The valid values are:

Location Specify a Location (an IP address, IP Address Group name, SNA device).
***ALL** Includes rules for all locations.

Object Rules
Indicate whether you would like the Object Rules printed on the report for each Location Rule printed.

The valid values are:

***YES** Object Rules are printed on the report.
***NO** Object Rules are not printed on the report.

Memorized Transactions
Indicate whether you would like the Memorized Transactions printed on the report for each Location Rule printed.

The valid values are:

***YES** Memorized Transactions are printed on the report.

***NO** Memorized Transactions are not printed on the report.

Access Rule Report - Print Object Lists

The Print Object Lists report allows you to print a listing of the Object Lists you have configured.

Name

The name of the report.

Description

The description of the report.

Shared: On/Off

This allows you to choose whether or not you want to share the report.

Sort By:

Specify how you want to sort the Object Lists. Click and drag the  icon to change the sort order. Uncheck an item to omit it.

Object List

Check this box to sort by Object List name.

Description

Check this box to sort by Object List description.

ASP Group

Check this box to sort by ASP Group.

Include Entries

Specify if you want to include Object List entries for each Object List in the report. The default value is *YES.

Include Usage

> **NOTE:** If you specify *YES for Include Entries and Include Usage, additional fields display allowing you to further sort and subset the information to appear in the report.

Indicate whether you would like the Object List Usage information for each Object list to be printed on the report. If you specify *NO, do not enter any subset or sorting criteria for Object List Usage information.

The valid values are:

***YES** The Object List Usage information is printed on the report.
***NO** The Object List Usage information is not printed on the report.

Object List Entries - Sort By

Specify how you want to sort Object List Entries. Click and drag the  icon to change the sort order. Uncheck an item to omit it.

The elements are:

Library

Check to sort by Library name.

Object

Check to sort by Object name.

Type

Check to sort by Object Type.

Path

Check to sort by Path.

Object List Usage - Subset By Location Style

When the value you key begins with an asterisk, this element allows you to format your request to find a single IP Address Group or any Location value that ends with the value you keyed (after the asterisk).

Valid values are:

***GROUP** List only rules that have the specified IP Address Group on them.
***ENDSWITH** List rules with any value that ends with the value you keyed.

Object List Usage - Subset By User Style

When the value you key is *PUBLIC, this element allows you to format your request to find only rules for *PUBLIC or any User value that ends with PUBLIC (like JIMPUBLIC, XPUBLIC, etc).

Valid values are:

***PUBLIC** List only rules that have *PUBLIC as the User value.
***ENDSWITH** List rules with any value that ends with PUBLIC.

Object List Usage - Show Location Rules

Indicate whether you want Location-based Object Rules to appear in the Usage section of the report. If you have specified subset criteria for Location, this value must be *YES. The valid values are:

***YES** Location-based Object Rules will be included.
***NO** Location-based Object Rules will not be included.

Object List Usage - Show User Rules

Indicate whether you want User-based Object Rules to appear in the Usage section of the report. If you have specified subset criteria for User, this value must be *YES. The valid values are:

***YES** User-based Object Rules will be included.
***NO** User-based Object Rules will not be included.

Object List Usage - Sort By

Click and drag the  icon to change the sort order. Uncheck an item to omit it.

Location

Check to specify the sort order for Location.

User

Check to specify the sort order for User.

Operation

Check to specify the sort order for Operation.

Optional Fields

Toggle this switch to On in order to access the following additional, optional fields.

Subset By Object List

Specify criteria to subset by Object list name. You can use the generic character to indicate that a partial value is to be used for selection. In some circumstances you may also use the wildcard character to indicate that a partial value is to be used for selection.

Subset By Object Type

Choose to subset by Native Object or IFS Path.

Subset By Description

Choose to subset by the description.

Object List Entries - Subset By Library

Specify criteria to subset by Library name. You can use the generic character to indicate that a partial value is to be used for selection. In some circumstances you may also use the wildcard character to indicate that a partial value is to be used for selection. You may specify <UNKNOWN> to select Object List Entries that pertain only to unqualified objects whose library cannot be determined.

Object List Entries - Subset by Object

Specify criteria to subset by Object name. You can use the generic character to indicate that a partial value is to be used for selection. In some circumstances you may also use the wildcard character to indicate that a partial value is to be used for selection.

Object List Entries - Subset By Type

Specify criteria to subset by Object Type.

Object List Entries - Subset By Path

Specify criteria to subset by Path. You can use the generic character to indicate that a partial value is to be used for selection. In some circumstances you may also use the wildcard character to indicate that a partial value is to be used for selection.

Object List Usage - Subset By Location

Specify criteria to subset by Location. Location represents the source of a transaction. Location can hold an IP Address, an IP Address Group or the name of an SNA Communications Device. The special value *ALL, when used on a rule, means that the rule applies to any rule means that the rule applies to any Location lacking a specific rule. when used as a subset or selection parameter, *ALL generally means to select all such rules for display or printing. You can use the Generic Character to indicate that a partial value is to be used for selection. In some circumstances you may also use the wildcard character to indicate that a partial value is to be used for selection.

Object List Usage - Subset By User

Specify criteria to subset by User.

Object List Usage - Subset By Operation

*__ALL__ Subset by all types of operations.
*__CREATE__ Subset by operations that apply to objects when they are being created or to their data when they are being added to an object; for example, when writing records to a database.
*__READ__ Subset by operations that apply to non-modifying accesses of objects or the reading of an object's data.
*__UPDATE__ Subset by operations that apply to changes to objects or changes to their data.
*__DELETE__ Subset by operations that apply to deletion of objects or deletion of their data; for example, deleting records from a database file.

Access Rule Report - Print Object Rules

The Print Object Rule report allows you to print a listing of the Object Rules you have configured.

Subset By Location Style

When the value you key begins with an asterisk, this element allows you to format your request to find a single IP Address Group or any Location value that ends with the value you keyed (after the asterisk).

Valid values are:

*__GROUP__ List only rules that have the specified IP Address Group on them.
*__ENDSWITH__ List rules with any value that ends with the value you keyed.

Subset by User Style

When the value you key is *PUBLIC, this element allows you to format your request to find only rules for *PUBLIC or any User value that ends with PUBLIC (like JIMPUBLIC, XPUBLIC, etc).

Valid values are:

*__PUBLIC__ List only rules that have *PUBLIC as the User value.
*__ENDSWITH__ List rules with any value that ends with PUBLIC.

Show Location Rules

Indicate whether you want Location-based Object Rules to appear in the report. The valid values are:

*__YES__ Location-based Object Rules will be included.
*__NO__ Location-based Object Rules will not be included.

Show User Rules

Indicate whether you want User-based Object Rules to appear in the report.

The valid values are:

*__YES__ User-based Object Rules will be included.
*__NO__ User-based Object Rules will not be included.

Sort By

Use these check boxes to sort the Object Rules printed on the report. Click and drag the  icon up or down to change the sort order. To omit an element from the sort, uncheck that element. Duplicate

values are not allowed; you cannot sort more than one field at any given position. This is a multi-part parameter consisting of four elements.

The elements are:

Location

Specify the sort order for Location.

User

Specify the sort order for User.

Object List

Specify the sort order for Object List name.

Operation

Specify the sort order for Operation.

Include Entries

Indicate whether you would like the Object List Entries for each Object list to be printed on the report.

The valid values are:

***YES** The Object List Entries are printed on the report.
***NO** The Object List Entries are not printed on the report.

Object List Entries - Sort By

Specify how you want to sort Object List Entries. Click and drag the  icon to change the sort order. Uncheck an item to omit it.

The elements are:

Library

Check to sort by Library name.

Object

Check to sort by Object name.

Type

Check to sort by Object Type.

Path

Check to sort by Path.

Optional Fields

Toggle this switch to On in order to access the following additional, optional fields.

Subset by Location

Specify criteria to subset by Location. Location represents the source of a transaction. Location can hold an IP Address, an IP Address Group or the name of an SNA Communications Device. The special

value *ALL, when used on a rule, means that the rule applies to any rule means that the rule applies to any Location lacking a specific rule. when used as a subset or selection parameter, *ALL generally means to select all such rules for display or printing. You can use the generic character to indicate that a partial value is to be used for selection. In some circumstances you may also use the wildcard character to indicate that a partial value is to be used for selection.

Subset By User

Specify criteria to subset by User. User represents the identity of the person initiating a transaction as a user profile. The special value *PUBLIC, when used on a rule, means that the rule applies to any User lacking a specific rule. when used as a subset or selection parameter, *PUBLIC means to select all such rules for display or printing.

You can use the generic character to indicate that a partial value is to be used for selection. In some circumstances you may also use the wildcard character to indicate that a partial value is to be used for selection.

Subset By Object List

Specify criteria to subset by Object list name. You can use the generic character to indicate that a partial value is to be used for selection. In some circumstances you may also use the wildcard character to indicate that a partial value is to be used for selection.

Subset By Operation

Specify criteria to subset by Operation.

Object List Entries - Subset By Library

Specify criteria to subset by Library name. You can use the generic character to indicate that a partial value is to be used for selection. In some circumstances you may also use the wildcard character to indicate that a partial value is to be used for selection. You may specify <UNKNOWN> to select Object List Entries that pertain only to unqualified objects whose library cannot be determined.

Object List Entries - Subset by Object

Specify criteria to subset by Object name. You can use the generic character to indicate that a partial value is to be used for selection. In some circumstances you may also use the wildcard character to indicate that a partial value is to be used for selection.

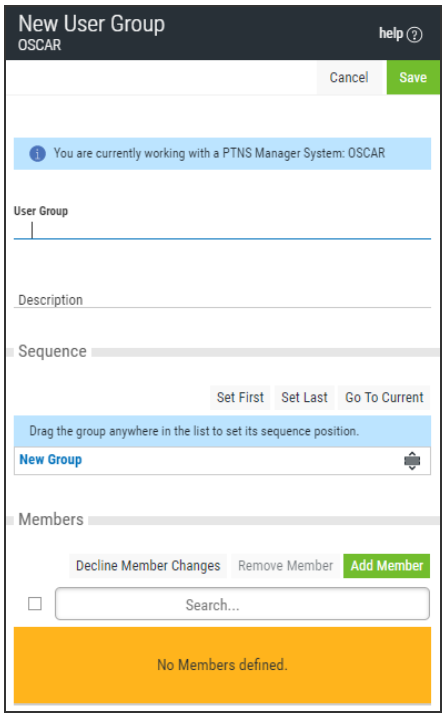
Object List Entries - Subset By Type

Specify criteria to subset by Object Type.

Object List Entries - Subset By Path

Specify criteria to subset by Path. You can use the generic character to indicate that a partial value is to be used for selection. In some circumstances you may also use the wildcard character to indicate that a partial value is to be used for selection.

New/Edit User Group screen



How to Get There

Choose the **User Groups** tab on the navigation pane on the left side of the Insite window to open the User Groups screen, then click **Add**. Or, click an existing User Group to edit it.

What it Does

Use this screen to create or edit an User Group.

Field descriptions

User Group

The User Group name is a short name you assign to a group of user profiles to help you identify the group. This name is required to be a valid OS name.

Description

The User Group description is a short textual description of the User Group. It is typically used to indicate the purpose or contents of the User Group.

Options

Delete (edit only)

When editing an existing User Group, choose **Delete** to delete the Group.

Save

Choose **Save** to save the User Group and return to the User Groups screen.

Cancel

Choose **Cancel** to return to the User Groups screen without making changes.

Sequence: Set First • Set Last • Go To Current

This list shows the sequence used to determine the order in which this User Group will be evaluated by the exit point programs.

For example, if there are three User Rules with User Groups for a specific Server/Function, and all three have USER1 as a member, then the User Rule at the top of this list will be used by the exit programs (if a User Rule with the specific user name of 'USER1' is not found).

Click **Set First** to move the current User Group to the top of the list.

Click **Set Last** to move the current User Group to the bottom of the list.

Click **Go To Current** to automatically scroll the list so that the currently selected group is visible.

TIP: Click and drag the User Group to quickly change its position in the list.

Members: Remove Member • Add Member • Decline Member Changes • Search

This section lists the members of the User Group, and allows you to add and remove profiles to the User Group.

Select one or more members and choose **Remove Member** to remove the profile from the User Group.

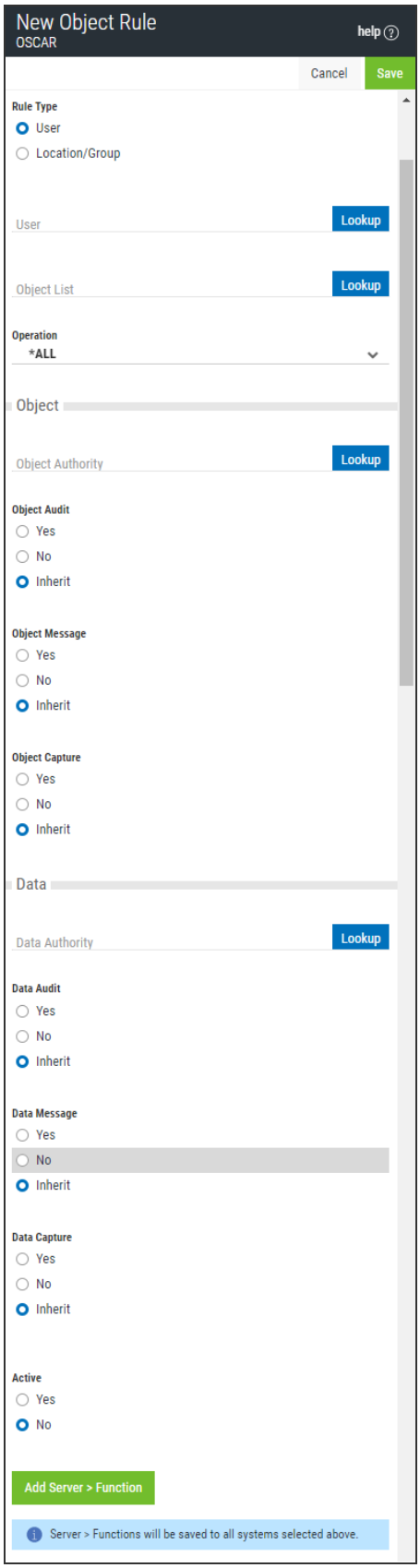
Click **Add Member** to open the Select User screen where you can select one or more profiles to add to the User Group.

Click **Decline Member Changes** to remove all profiles added to the membership list during this session (i.e. that have not been applied to the database).

Type a profile name, or a portion of a profile name, into the **Search** field to subset the list of available profiles.

[Member List]: Click **Groups** adjacent to a member profile to display all other groups that include the profile.

New/Edit Object Rule screen


New Object Rule
OSCAR
help
Cancel
Save
Rule Type
User
Location/Group
User
Lookup
Object List
Lookup
Operation
*ALL
Object
Object Authority
Lookup
Object Audit
Yes
No
Inherit
Object Message
Yes
No
Inherit
Object Capture
Yes
No
Inherit
Data
Data Authority
Lookup
Data Audit
Yes
No
Inherit
Data Message
Yes
No
Inherit
Data Capture
Yes
No
Inherit
Active
Yes
No
Add Server > Function
Server > Functions will be saved to all systems selected above.

How to Get There

Choose the **Object Rules** tab on the navigation pane on the left side of the Exit Point Manager window, then choose **Add**. Or, select an existing User Object Rule to edit it.

What it Does

The New User Object Rule screen is used to add new User Object Rules. The Edit User Object Rule screen includes identical options and is used to edit an existing User Object rule. Object rules are used to control access to Object Lists. See Object Rules.

Options

Delete (Edit User Object Rule screen only)

Choose **Delete** to delete the User Object Rule. When asked to confirm, Choose **Delete** again. If the Object Rule is Active, you will be prompted with the Object Rules Delete screen, where you can select how to handle associated *MEMOBJ rules and other Rules that constitute the Object Rule.

Cancel

Choose **Cancel** to return to the Object Rules screen without making changes.

Save

Choose **Save** to save the Rule and return to the Object Rules screen.

Rule Type

Specifies whether this is a User or Location Object rule.

User; Lookup

This field is available when creating a new Object Rule. Choose this **Lookup** button to open the Users selection window where you can choose from a list of user profiles.

Object List; Lookup

This field is available when creating a new Object Rule. Choose this **Lookup** button to open the Object Lists selection window where you can choose from a list of Object Lists. Object Lists can be added and changed using the Object Lists screen.

Operation

***ALL** Applies to all of the above types of operations.
***CREATE** Applies to objects when they are being created or to their data when they are being added to an object; for example, when writing records to a database.
***READ** Applies to non-modifying accesses of objects or the reading of an object's data.
***UPDATE** Applies to changes to objects or changes to their data.
***DELETE** Applies to deletion of objects or deletion of their data, for example, deleting records from a database file.

Object Authority; Lookup

Choose this **Lookup** button to open the Authorities selection window where you can choose from a list of Authorities.

Object Audit

This audit property controls the type of requests Exit Point Manager will log. This Audit Transaction flag pertains to Object Accesses. Possible values are:

Yes - Log all requests by the location/server/function.
No - Only log authority failures for the location/server/function.
Inherit - Inherit the value.

Object Message

The message property entry will determine if Exit Point Manager sends a message to the Exit Point Manager message queue. This Send Messages flag pertains to Object Accesses.

Yes - A message is sent to the Exit Point Manager message queue.
No - No message is sent.
Inherit - Inherit the value.

Capture Transactions

Capture transactions for Memorized Transaction Request. This Capture Transactions flag pertains to Data Accesses.

Yes - Capture transactions.
No - Do not capture transactions.
Inherit - Inherit the value.

Data Audit

This audit property controls the type of requests Exit Point Manager will log. This Audit Transaction flag pertains to Data Accesses. Possible values are:

Yes - Log all requests by the location/server/function.
No - Only log authority failures for the location/server/function.
Inherit - Inherit the value.

Data Message

The message property entry will determine if Exit Point Manager sends a message to the Exit Point Manager message queue. This Send Messages flag pertains to Data Accesses.

Yes - A message is sent to the Exit Point Manager message queue.
No - No message is sent.
Inherit - Inherit the value.

Data Capture

Capture transactions for Memorized Transaction Request. This Capture Transactions flag pertains to Data Accesses

Yes - Capture transactions.
No - Do not capture transactions.
Inherit - Inherit the value.

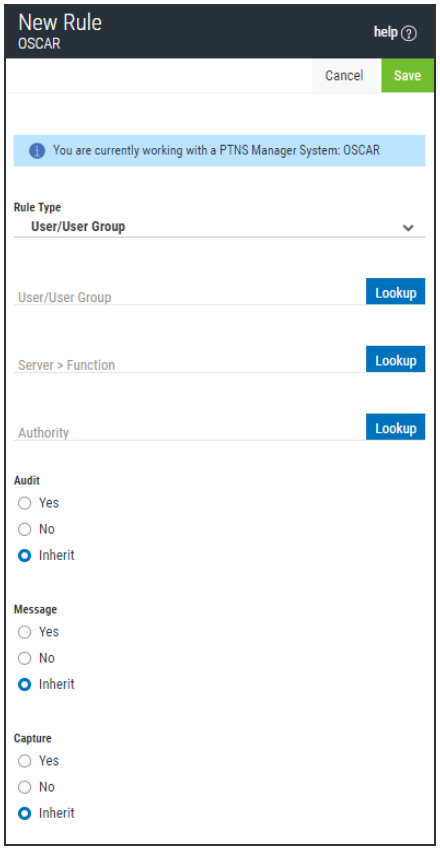
Active

Choose **Yes** to activate the rule. Choose **No** to make the rule inactive.

Select which systems to save to

All managed systems are listed here. Check the systems you would like to save the Object Rule to. Or, check Select All to copy the Object Rule to all managed systems.

New/Edit Rule screen



How to Get There

Choose the **Rules** tab on the navigation pane on the left side of the Exit Point Manager window. Choose **Add** to add a new Rule. Or, click an existing user rule to edit it.

What it Does

The New Rule screen is used to add new server/function filter rules for a user or location.

Options

Delete

When editing an existing User Rule, choose **Delete** to delete the Rule.

Cancel

Choose **Cancel** to return to the Rules screen without making changes.

Save

Choose **Save** to save the User Rule and return to the Rules screen.

Rule Type
Specifies whether this is a User or Location rule.

User/User Group; Lookup
Choose this **Lookup** button to open the Users selection window where you can choose from a list of user profiles.

Server > Function; Lookup
Choose this **Lookup** button to open the Servers selection window where you can choose from a list of servers and server functions. For a description of servers and functions, see Appendix B: Servers and Functions.

Authority; Lookup
Choose this **Lookup** button to open the Authorities selection window where you can choose from a list of Authorities.

Audit
The audit property controls the type of requests Exit Point Manager will log. Possible values are:

Yes Log all requests by the location/server/function.

No Only log authority failures for the location/server/function.

Inherit Inherit the value.

Message
The message property entry will determine if Exit Point Manager sends a message to the Exit Point Manager message queue.

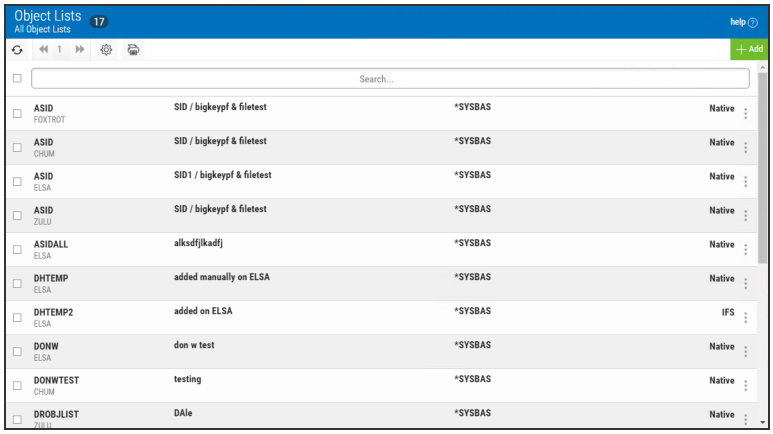
Yes A message is sent to the Exit Point Manager message queue.
No No message is sent.
Inherit Inherit the value.

Capture
Capture transactions for Memorized Transaction Request.

Yes Capture transactions.
No Do not capture transactions.
Inherit Inherit the value.

Select which systems to save to
All managed systems are listed here. Check the systems you would like to save the Rule to. Or, check Select All to copy the Rule to all managed systems.

Object List screen



How to Get There

Click the **Object Lists** tab on the navigation pane on the left side of the Insite window.

What it Does

The Object List screen enables you to add and edit Object Lists.

Options

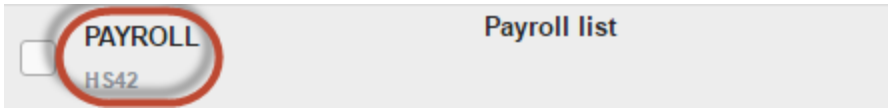
Selection, sorting, filtering, deleting, and navigation features on this screen are described in Using the Web Browser Interface. Click an Object List to open the Edit IFS Object List screen or Edit Native Object List screen where you can edit the Object List.

Add

Choose **Add** to open the New Object List screen where you can define a new Object List.

Column Descriptions

Name/System



The Object List name as defined in the New/Edit IFS Object List screen or New/Edit Native Object List screen. The system of the Object List is indicated beneath its name.

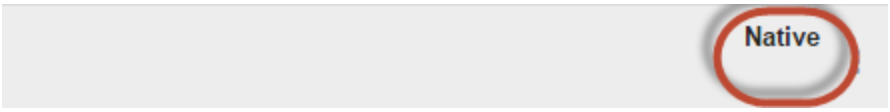
Description

The Object List description as defined in the New/Edit IFS Object List screen or New/Edit Native Object List screen.

ASP Group

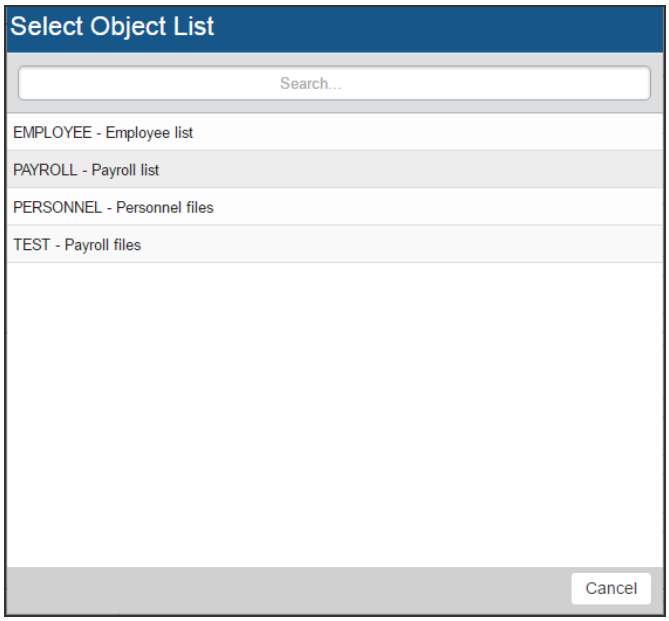
This is the name of an ASP Group. It is used in rule evaluation to determine if an object referenced in a transaction is the one specified on the object entries for this list.

Type (Native or IFS)



The Object List type determines what type of entries can be added to an Object List. Object lists can hold native object specifications (library, object and type) or paths to IFS objects.

Object Lists Selection Window



How to Get There

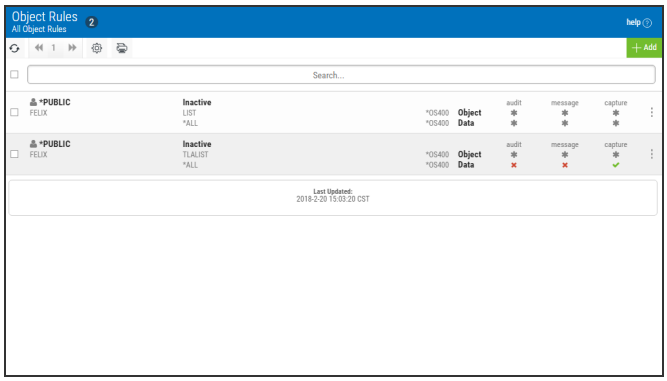
Choose **Lookup** next to the Object List Name field when adding or changing an Object Rule rule in the New/Edit Object Rule screen.

What it Does

This window allows you to specify an Object List when adding or changing an object rule.

This list includes all existing Object Lists. Object Lists can be added and changed using the Object Lists screen.

Object Rules screen



How to Get There

Click the **Object Rules** tab on the Navigation Pane on the left side of the browser window.

What it Does

The Object Rules screen allows you to create, modify, and delete Object Rules that pertain to Users or Locations. Object Rules can be active or inactive.

Options

Selection, sorting, filtering, deleting, and navigation features on this screen are described in Using the Web Browser Interface. Click an Object Rule to open the Edit Object Rules screen where you can edit the Object Rule.

Add

Choose **Add** to open the New Object Rule screen where you can define a new user rule.

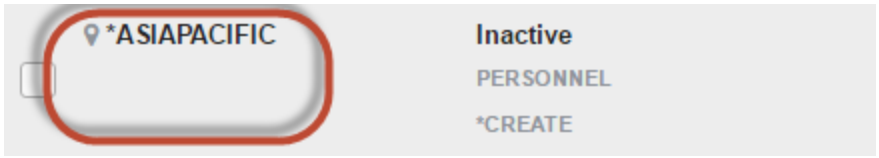
[Actions]

Click  next to an Object Rule to show Actions.

- **Edit.** Choose **Edit** to open the Edit Object Rule screen where you can edit the Object Rule.
- **Copy.** Choose **Copy** to open the Copy Object Rule screen, where you can select the system(s) you would like to copy the Object Rule to.
- **Delete.** Choose **Delete** to delete the Object Rule.
- **Close.** Choose **Close** to dismiss the Action Pane.

Column Descriptions

User/Location column

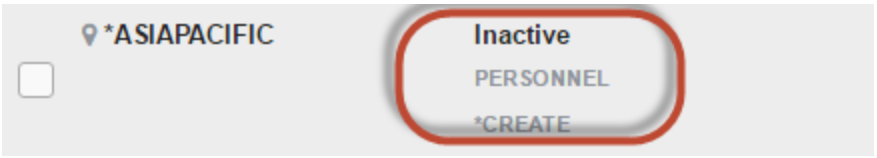


This column lists the user or location of the rule.

A icon indicates a User rule. User represents the identity of the person initiating a transaction as a user profile. The special value *PUBLIC, when used on a rule, means that the rule applies to any User lacking a specific rule. When used as a subset or selection parameter, *PUBLIC means to select all such rules for display or printing.

An icon indicates a Location Rule. The location is the name of the location for which authority is being specified. The location can be an SNA device, an IP address, an IP Address Group, or the special value '*ALL'. If specifying an IP address, enter either the full IP address or a generic IP address using an asterisk as the final character. IP Address Groups must be established prior to their entry on this screen (see IP Address Groups).

Status/Object List Name/Operation

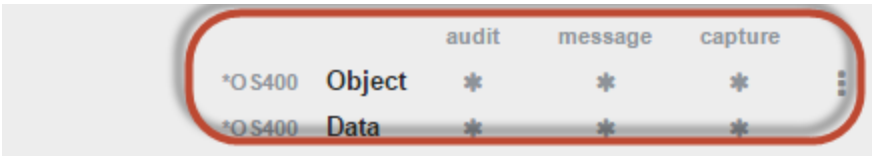


The name of the Object List assigned to the object rule. See Object Lists screen.

The operation to which the rule applies.

***ALL** The rule applies to all operations.
***CREATE** The rule applies to attempts to create an object matching an entry defined in the Object List.
***READ** The rule applies to attempts to read an object matching an entry defined in the Object List.
***UPDATE** The rule applies to attempts to update an object matching an entry defined in the Object List.
***DELETE** The rule applies to attempts to delete an object matching an entry defined in the Object List.

Authority



Authority represents the action to be taken when a rule is found that matches the data present on a transaction. Two values are listed for each Object Rule, one for Object Accesses and one for Data Accesses.

The valid values are:

***OS400** The transaction will be allowed and object authority will be determined by the operating system.
***REJECT** The transaction will not be allowed.
***SWITCH** The transaction will be allowed and the transaction will occur as if the user profile named as the Swap Profile had initiated the transaction. After switching to the Swap Profile, the authority used during the transaction will be determined by the operating system.

Audit

The Audit flag controls the logging of transactions to the Log Journal set up on the work with Exit Point Manager System Values panel. Two values are listed for each Object Rule, one for Object Accesses and one for Data Accesses.

The valid values are:

- The transaction will be logged to the Log Journal.
- The transaction will not be logged to the Log Journal.
- The default value from a prior rule will control the logging.

Message

The Send messages flag controls the sending of messages to the Log Message Queue set up on the Work with Exit Point Manager System Values panel. Two values are listed for each Object Rule, one for Object Accesses and one for Data Accesses.

The valid values are:

- A log message will be sent to the Log Message Queue.
- A log message will not be sent to the Log Message Queue.
- The default value from a prior rule will control the logging.

Capture

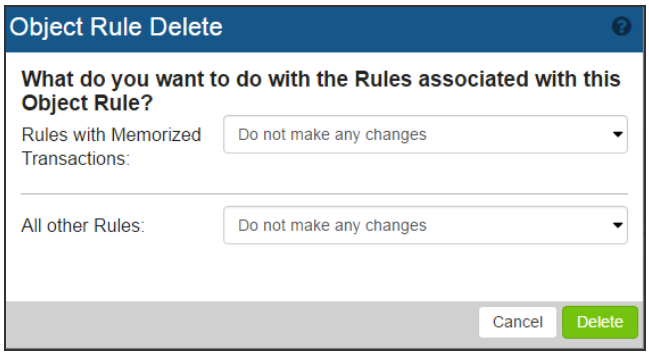
Capture transactions flag controls whether transactions are remembered in Exit Point Manager for later memorization. Once captured, transactions can become Memorized Transactions which can act as rules. Two values are listed for each Object Rule: one for Object Accesses and one for Data Accesses.

The valid values are:

- A log message will be sent to the Log Message Queue.
- A log message will not be sent to the Log Message Queue.
- The default value from a prior rule will control the logging.

Object Rule Delete screen

This screen appears after choosing to delete an active object Rule on the Object Rules screen.



Options

Rules with Memorized Transactions

From this drop-down list, choose how you want to handle *MEMOBJ rules associated with this Object Rule.

- Choose 'Do not make any changes' to leave other *MEMOBJ Rules as-is.
- Choose 'Switch to a different authority' to update existing *MEMOBJ rules so that they have a different authority setting.
- Choose 'Delete rules associated with this Object Rule' to delete the associated *MEMOBJ rules.

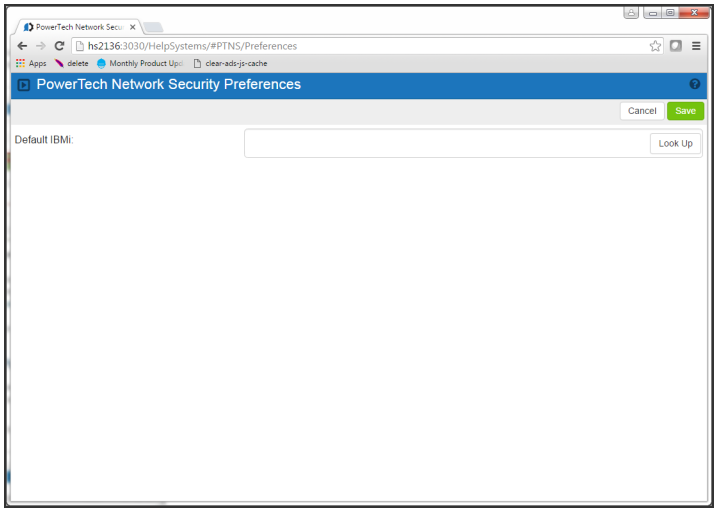
All other Rules

From this drop-down list, choose how you want to handle other Rules associated with this Object Rule.

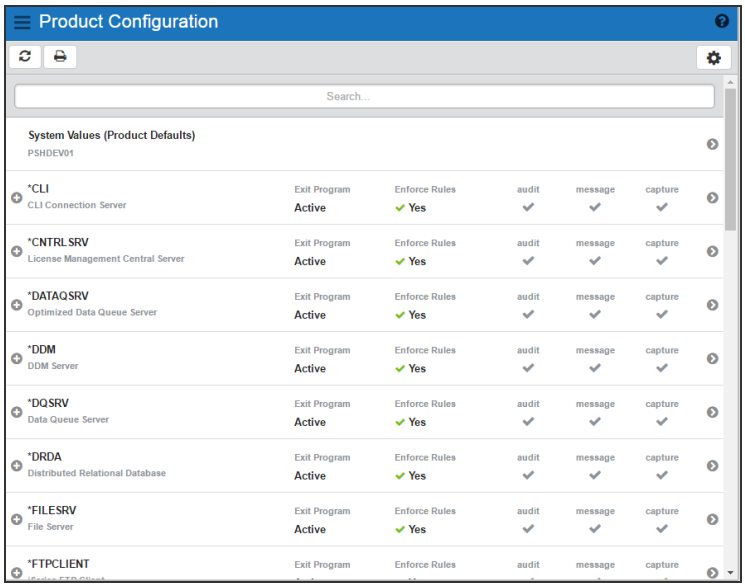
- Choose 'Do not make any changes' to leave other *Rules as-is.
- Choose 'Switch to a different authority' to update existing rules so that they have a different authority setting.
- Choose 'Delete rules associated with this Object Rule' to delete the associated rules.

Preferences screen

Use this screen to define the default IBM i system. Click **Look Up** to select the system you want to assign as the default system.



Product Configuration screen



How to Get There

Click the **Product Configuration** tab on the navigation pane on the left side of the Insite window.

What it Does

The Product Configuration window allows you to view each servers' default properties.

> **NOTE:** This screen is equivalent to using the **SP** (Server Properties) option for servers in the Work with Security by Server screen when using the green screen.

Options

Sorting, filtering, and navigation features on this screen are described in Using the Web Browser Interface.

Click to display a server's functions. Click a function to open the Edit Server Function Rule screen where you can edit the server function's properties.

Field Descriptions

Server

The server ID is the name of the IBM server that authority is being specified.

Server Description

The description of the IBM server.

Active

Indicates that Powertech Exit Point Manager will enforce rules for this server. See also Exit Pgm Enrolled.

Yes Exit Point Manager will enforce rules for this server.

No Exit Point Manager will not enforce rules for this server.

Audit

Controls the type of requests Exit Point Manager will log. Possible values are:

- Log all requests to the server.
- Log only authority failures for the server.
- or Product defaults.

Message

Specifies if Exit Point Manager sends a message to the message queue specified in Powertech's System Values. Possible values are:

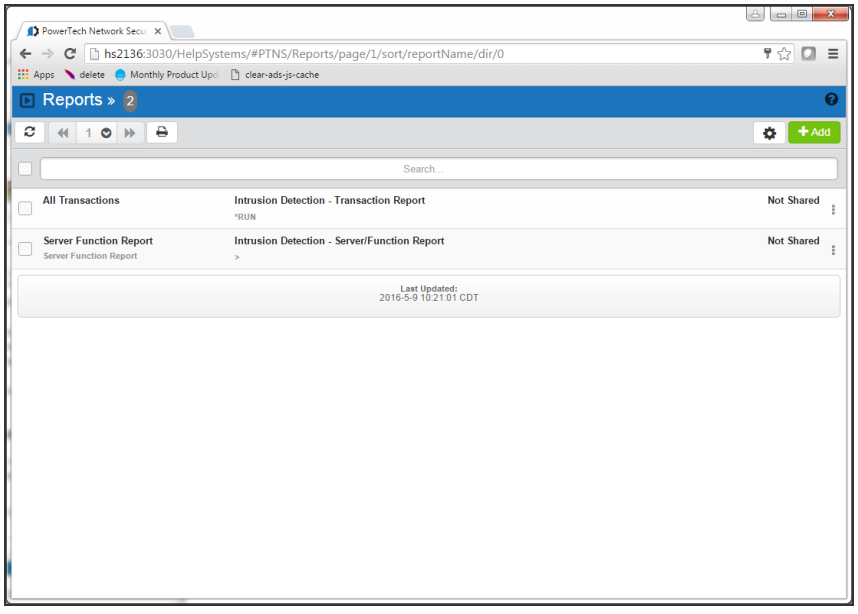
- A message is sent to the specified queue.
- No message is sent.
- or Product defaults.

Capture Transactions

Capture transactions for Memorized Transaction Request (MTR). Possible values are:

- Capture transactions.
- Do not capture transactions.
- or Product defaults.

Reports screen



How to Get There

Choose **Reports** in the Insite Navigation Pane.

Options

Selection, sorting, filtering, deleting, and navigation features on this screen are described in Using the Insite Web Browser Interface.

Click an existing report to open the Edit Report screen, where you can edit the report.

Add

Choose **Add** to open the Add Report screen where you can choose the type of report you would like to add.

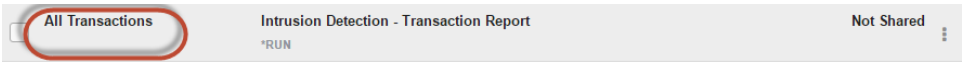
[Actions]

Click  next to a report to show Actions.

- **Submit.** Choose **Submit** to run the report. After the report has been run, it is available in the list of Spooled Files. See Spooled Files screen.
- **Edit.** Choose **Edit** to open the Edit Report screen where you can edit the report.
- **Copy.** Choose **Copy** to open the Copy Report screen, where you can select the system(s) you would like to copy the report to.
- **Delete.** Choose **Delete** to delete the report.
- **Close.** Choose **Close** to dismiss the Action Pane.

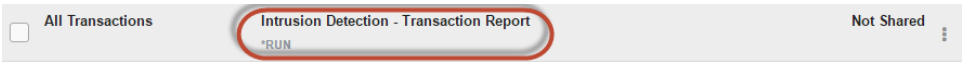
Column Descriptions

Name/Description



This column lists the name and description of the report.

Transaction Type



This is the Type of the transaction.

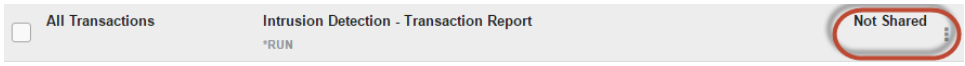
***RUN** - Network Transactions that Run commands and programs. This option produces a report of transactions that resulted in a command or program being executed and sorts by Server/Function/Date/Time. You will be prompted for Type and Date/Time range on a later screen.

***UPDATE** - Network Transactions that Update data. This option produces a report of transactions that resulted in data being updated and sorts by Server/Function/Date/Time. You will be prompted for Type and Date/Time range on a later screen.

***READ** - Network Transactions that Read data. This option produces a report of transactions that resulted in data being read and sorts by Server/Function/Date/Time. You will be prompted for Type and Date/Time range on a later screen.

***MODIFY** - Network Transactions that Modify objects. This option produces a report of transactions that resulted in objects being modified and sorts by Server/Function/Date/Time. You will be prompted for Type and Date/Time range on a later screen.

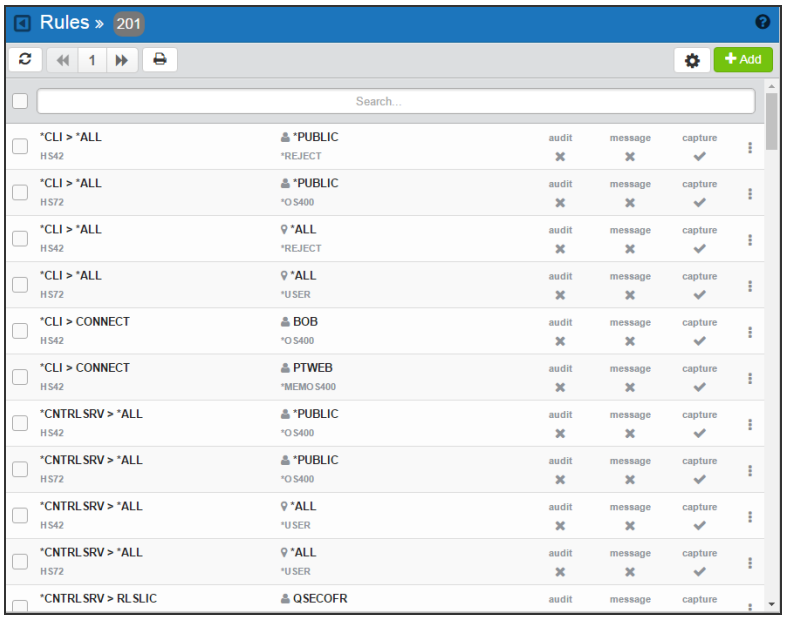
Shared/Not Shared



This column indicates whether the report is shared or not.

Rules screen

The Rules screen lists all the rules defined by Exit Point Manager, including the server and function, user or location, and properties for each. From this screen, you can easily identify specific rules, and edit, add, or delete them.



How to Get There

Click the **Rules** tab on the navigation pane on the left side of the Exit Point Manager window.

Options

Selection, sorting, filtering, deleting, and navigation features on this screen are described in Using the Web Browser Interface.

Click a User or Location rule to open the Edit Rule screen, where you can edit the rule.

Add

Choose **Add** to open the New Rule screen where you can define a new user rule.

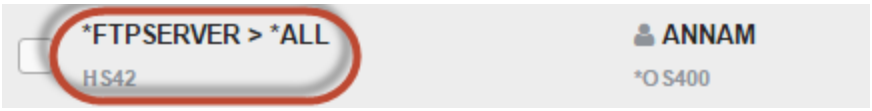
Show Actions

Click  next to a rule to show Actions.

- **Edit.** Choose **Edit** to open the Edit Rule screen where you can edit the rule.
- **Copy.** Choose **Copy** to open the Copy Rule screen, where you can select the system(s) you would like to copy the rule to.
- **Delete.** Choose **Delete** to delete the rule.
- **Close.** Choose **Close** to dismiss the Action Pane.

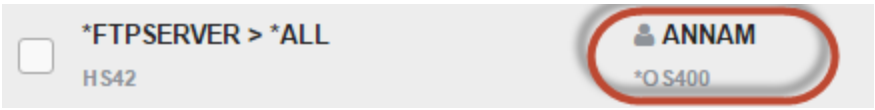
Column Descriptions

Server/Function column



This column lists the server ID for each rule. The server ID is the name of the IBM server for which authority is being specified. For a description of servers and functions, see Appendix B: Servers and Functions.

User/Location/Authority column



This column lists the user or location of the rule.

A icon indicates a User rule. User represents the identity of the person initiating a transaction as a user profile. The special value *PUBLIC, when used on a rule, means that the rule applies to any User lacking a specific rule. When used as a subset or selection parameter, *PUBLIC means to select all such rules for display or printing.

An icon indicates a Location Rule. The location is the name of the location for which authority is being specified. The location can be an SNA device, an IP address, an IP Address Group, or the special value '*ALL'. If specifying an IP address, enter either the full IP address or a generic IP address using an asterisk as the final character. IP Address Groups must be established prior to their entry on this screen (see IP Address Groups).

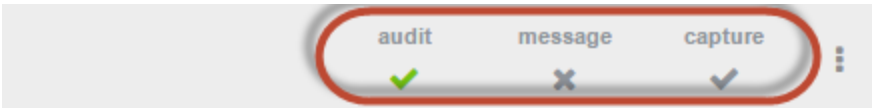
The authority assigned for servers and their functions.

Possible values are:

***OS400**Exit Point Manager will use normal OS/400 authority for the location. This is valid for both location and user.
***REJECT**Exit Point Manager will reject requests for the specified location. This is valid for both location and user.
***SWITCH**Exit Point Manager will use the authority of the switch profile for the specified location. A switch profile entry is required. This is valid for both location and user. To view the profile to be switched to view the expanded rule properties.
***MEMREJECT** Check Memorized Transactions (MTR) for authority. If no MTR authority is encountered, Exit Point Manager will reject requests for the specified location. This is valid for both location and user.
***MEMOS4OO** Check Memorized Transactions (MTR) for authority. If no MTR authority is encountered, Exit Point Manager will use normal OS/400 authority for the location. This is valid for both location and user.

***MEMUSR** Check Memorized Transactions (MTR) for authority. If no MTR authority is encountered, Exit Point Manager will check server user authority. This is only valid for location.
***USER**Exit Point Manager will check server user authority. This is only valid for location.
***MEMSWITCH** Check Memorized Transactions (MTR) for authority. If no MTR authority is encountered, Exit Point Manager will use the authority of the switch profile for the specified location. A switch profile entry is required. This is valid for both location and user.
***SRVFCN**Exit Point Manager will use the authority defined for the server/function. This is valid for both location and user.
***SAME**Exit Point Manager will not change the existing settings and will not create new rules when the All Servers option is taken. This is valid for both location and user.

Aud/Msg/Cap columns



A ✔ or ✖ in one of these columns indicates the value is explicitly defined in the rule. A [gray] ✔ or ✖ indicates the value is not defined in the rule itself, but is inheriting the actual value from another location (much like *SYSVAL in the OS). See Active Rule and Rule derivation.

Audit

The audit property controls the type of requests Exit Point Manager will log. Possible values are:

✔ Log all requests by the location/server/function.
✖ Only log authority failures for the location/server/function.

Message

The message property entry will determine if Exit Point Manager sends a message to the Exit Point Manager message queue.

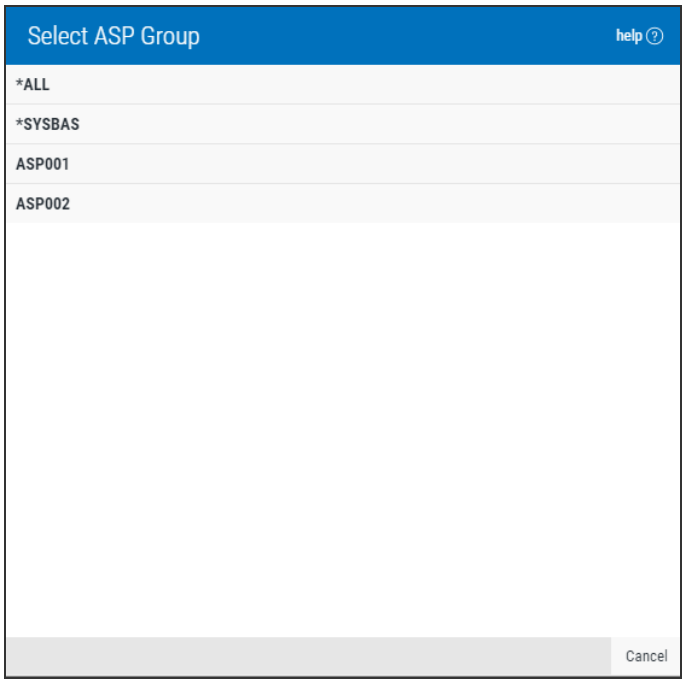
✖ No message is sent.
✔ A message is sent to the Exit Point Manager message queue.

Capture

Capture transactions for Memorized Transaction Request (MTR).

✖ Do not capture transactions.
✔ Capture transactions.

Select ASP Group



How to Get There

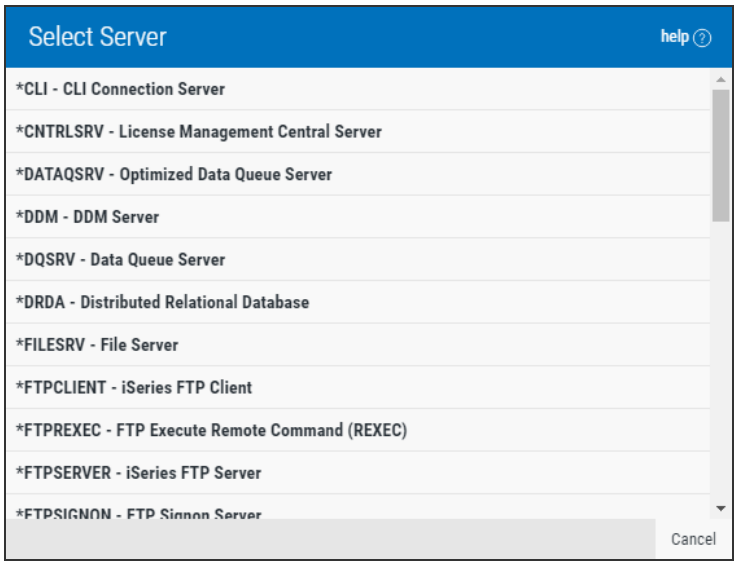
Click **Lookup** next to ASP Group when, for example, adding or changing an Object List on the New/Edit Object List screen.

What it Does

This screen allows you to choose from a list of ASP Groups.

> **NOTE:** The ability to choose an ASP Group is not available for endpoints with versions of Network Security that do not include ASP support (v7.19 or earlier).

Servers Selection window



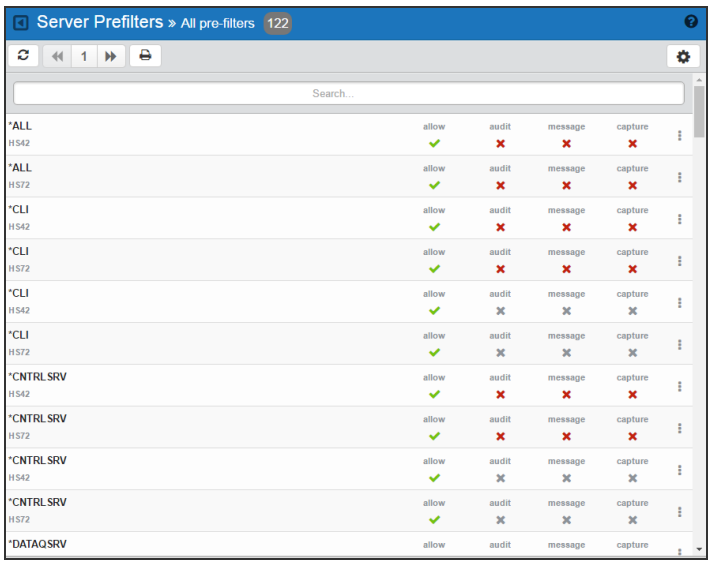
How to Get There

Click **Lookup** next to the Server > Function field when adding or changing rules.

What it Does

This window allows you to select a server. By selecting a server, you are directed to the Function selection window where you can select a specific function of that server.

Server Pre-filters screen



How to Get There

Click the **Server Pre-filters** tab on the navigation pane on the left side of the Insite window.

What it Does

The Server Pre-filters screen allows you to specify certain actions for transactions before they are evaluated by the regular Powertech Exit Point Manager rules. The primary action is to allow or not allow a transaction — allowing it causes it to be further evaluated by Exit Point Manager rules; not allowing it is equivalent to a Exit Point Manager reject. The other actions that you can specify are to audit the transaction, send an immediate message, and capture the transaction. These actions work exactly like their equivalents within Exit Point Manager rules processing. The Server Pre-filter function allows you to specify settings by server. The default system Pre-filter record has a Server of *ALL. These records can be changed but not deleted. The system (*ALL) record must have either a 'Y' or an 'N' for each of the settings (allow, audit, message, and capture). The subsequent individual server Pre-filters can inherit from this system value.

The Pre-filter function attempts to match the most specific record to the transaction. Once a match is found, the Pre-filter function processes the transaction based on those settings.

Options

Sorting, filtering, and navigation features on this screen are described in Using the Web Browser Interface.

Click a Pre-filter to open the Edit Server Pre-filter screen where you can edit a Server Pre-filter.

Column Descriptions

Allow

The setting for whether transactions matching this record should be allowed to continue to be processed by Exit Point Manager. Valid settings are 'Y' (Yes — Exit Point Manager rules should evaluate this transaction, which may or may not cause it to be rejected, 'N' (No — reject the transaction), and a gray Y or N (inherit the value from the System (*ALL) Pre-filter).

Aud/Msg/Cap columns

A ✔ or ✘ in one of these columns indicates the value is explicitly defined in the rule. A gray ✔ or ✘ indicates the value is not defined in the Pre-filter itself, but is inheriting the actual value from the default System Pre-filter (*ALL). See Active Rule and Rule derivation.

Audit

The audit property controls the type of requests Exit Point Manager will log. Possible values are:

- ✔ Log all requests by the location/server/function.
- ✘ Only log authority failures for the location/server/function.

Message

The message property entry will determine if Exit Point Manager sends a message to the Exit Point Manager message queue.

- ✘ No message is sent.
- ✔ A message is sent to the Exit Point Manager message queue.

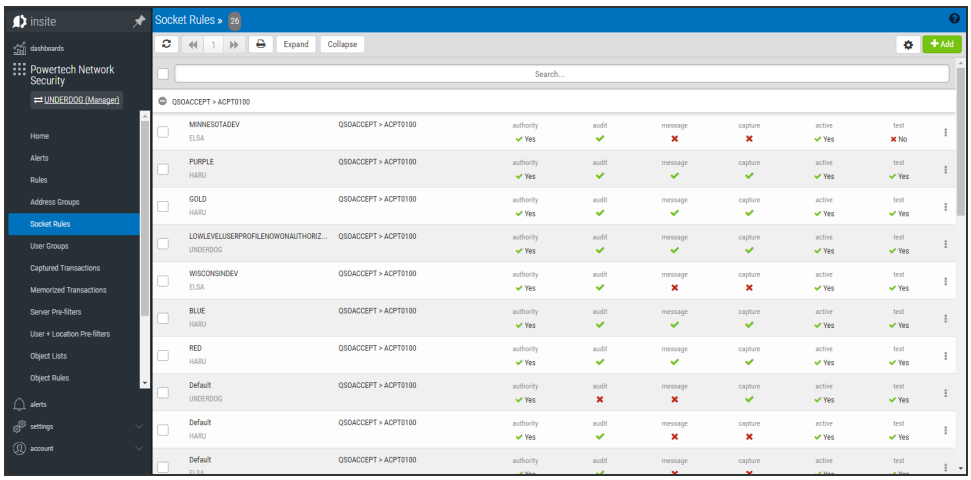
Capture

Capture transactions for Memorized Transaction Request (MTR).

- ✘ Do not capture transactions.

✔ Capture transactions.

Socket Rules screen



How to Get There

Click the **Socket Rules** tab on the Navigation Pane on the left side of the browser window.

What it Does

The Socket Rules screen allows you to create, modify, and delete Socket Rules.

Options

Selection, sorting, filtering, deleting, and navigation features on this screen are described in Using the Web Browser Interface. Click a Socket Rule to open the Socket Rules screen where you can edit the Socket Rule.

Add

Choose **Add** to open the New Socket Rule screen where you can define a new socket rule.

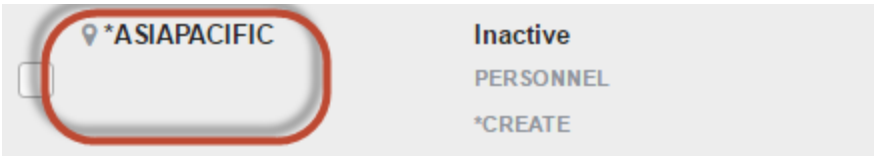
[Actions]

Click ⋮ next to an Object Rule to show Actions.

- **Edit.** Choose **Edit** to open the Edit Socket Rule screen where you can edit the Socket Rule.
- **Copy.** Choose **Copy** to open the Copy Object Rule screen, where you can select the system(s) you would like to copy the Object Rule to.
- **Delete.** Choose **Delete** to delete the Object Rule.
- **Close.** Choose **Close** to dismiss the Action Pane.

Column Descriptions

User/Location column

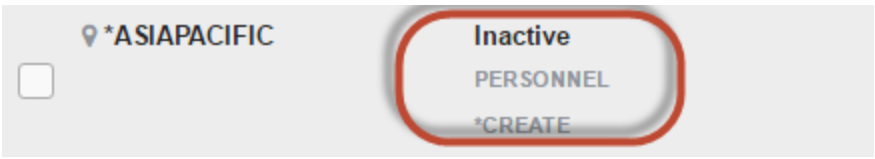


This column lists the user or location of the rule.

A icon indicates a User rule. User represents the identity of the person initiating a transaction as a user profile. The special value *PUBLIC, when used on a rule, means that the rule applies to any User lacking a specific rule. When used as a subset or selection parameter, *PUBLIC means to select all such rules for display or printing.

An icon indicates a Location Rule. The location is the name of the location for which authority is being specified. The location can be an SNA device, an IP address, an IP Address Group, or the special value '*ALL'. If specifying an IP address, enter either the full IP address or a generic IP address using an asterisk as the final character. IP Address Groups must be established prior to their entry on this screen (see IP Address Groups).

Status/Object List Name/Operation

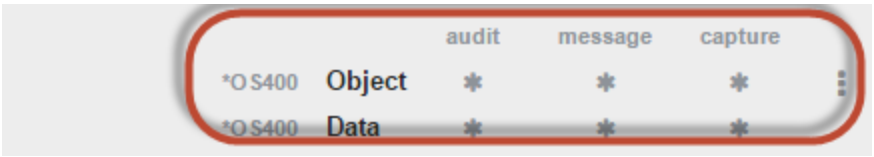


The name of the Object List assigned to the object rule. See Object Lists screen.

The operation to which the rule applies.

***ALL** The rule applies to all operations.
***CREATE** The rule applies to attempts to create an object matching an entry defined in the Object List.
***READ** The rule applies to attempts to read an object matching an entry defined in the Object List.
***UPDATE** The rule applies to attempts to update an object matching an entry defined in the Object List.
***DELETE** The rule applies to attempts to delete an object matching an entry defined in the Object List.

Authority



Authority represents the action to be taken when a rule is found that matches the data present on a transaction. Two values are listed for each Object Rule, one for Object Accesses and one for Data Accesses.

The valid values are:

*__OS400__ The transaction will be allowed and object authority will be determined by the operating system.
*__REJECT__ The transaction will not be allowed.
*__SWITCH__ The transaction will be allowed and the transaction will occur as if the user profile named as the Swap Profile had initiated the transaction. After switching to the Swap Profile, the authority used during the transaction will be determined by the operating system.

Audit

The Audit flag controls the logging of transactions to the Log Journal set up on the work with Exit Point Manager System Values panel. Two values are listed for each Object Rule, one for Object Accesses and one for Data Accesses.

The valid values are:

 The transaction will be logged to the Log Journal.
 The transaction will not be logged to the Log Journal.
 The default value from a prior rule will control the logging.

Message

The Send messages flag controls the sending of messages to the Log Message Queue set up on the Work with Exit Point Manager System Values panel. Two values are listed for each Object Rule, one for Object Accesses and one for Data Accesses.

The valid values are:

 A log message will be sent to the Log Message Queue.
 A log message will not be sent to the Log Message Queue.
 The default value from a prior rule will control the logging.

Capture

Capture transactions flag controls whether transactions are remembered in Exit Point Manager for later memorization. Once captured, transactions can become Memorized Transactions which can act as rules. Two values are listed for each Object Rule: one for Object Accesses and one for Data Accesses.

The valid values are:

 A log message will be sent to the Log Message Queue.
 A log message will not be sent to the Log Message Queue.
 The default value from a prior rule will control the logging.

Spooled Files

This panel displays spooled files the current user has created by submitting reports on the Reports panel. You can use the Spooled Files page to view, print, and delete these spooled files on your system.

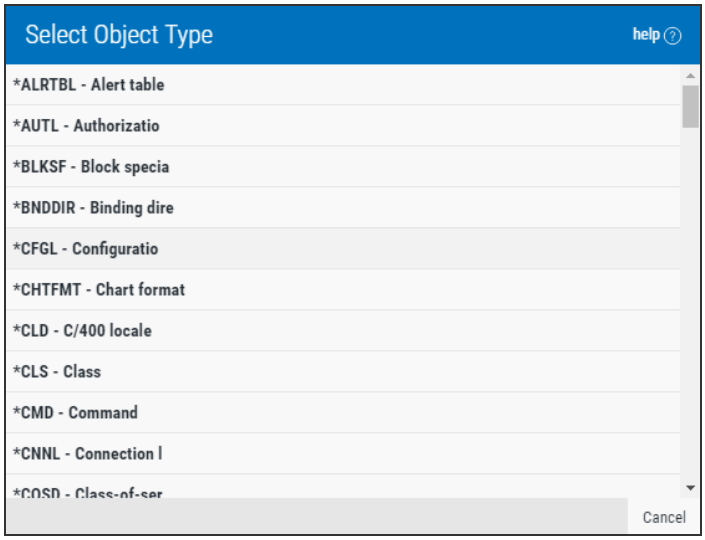
View Spooled File

This panel displays the report chosen on the Spooled Files panel. The report must have first been submitted. See Reports panel. Use the View Spooled File page to view the contents of a spooled file and search the text in it.

Spooled Files Properties

Use the Spooled Files Properties page to display and edit the properties of a spooled file.

Types of Object Entries selection window



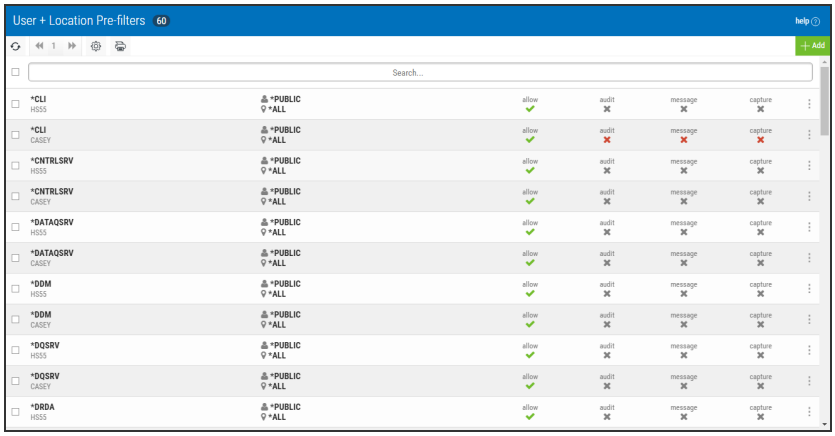
How to Get There

Click **Lookup** next to the Native Object Type field when adding or changing an Object List rule in the New/Edit Native Object List screen.

What it Does

This window allows you to specify the object type when defining an object in a Native Object List.

User+Location Pre-filters screen



How to Get There

Click the **User+Location** tab on the navigation pane on the left side of the Exit Point Manager window.

What it Does

The User+Location Pre-filters screen allows you to specify certain actions for transactions before they are evaluated by the regular Powertech Exit Point Manager rules. The primary action is to allow or not allow a transaction — allowing it causes it to be further evaluated by Exit Point Manager rules; not allowing it is equivalent to a Exit Point Manager reject. The other actions that you can specify are to audit the transaction, send an immediate message, and capture the transaction. These actions work exactly like their equivalents within Exit Point Manager rules processing. The Location + User Pre-filter function allows you to specify settings by function, location, and user. These records can be changed but not deleted. System record must have either a 'Y' or an 'N' for each of the settings (allow, audit, message, and capture).

The Pre-filter function attempts to match the most specific record to the transaction. Once a match is found, the Pre-filter function processes the transaction based on those settings.

Options

Selection, sorting, filtering, deleting, and navigation features on this screen are described in Using the Web Browser Interface. Click a Pre-filter to open the Edit Location + User Pre-filter screen where you can edit the Pre-filter.

Add

Choose **Add** to open the New Location + User Pre-filters screen where you can define a new User+Location Pre-filter.

Field Descriptions

Server > Function column

This column lists the server and function IDs for each Pre-filter. For a description of servers and functions, see Appendix B: Servers and Functions.

Location/User/User Group Column

This column lists the location of the Pre-filter. The location is the name of the location for which authority is being specified. The location can be an SNA device, an IP address, an IP Address Group, or the special value '*ALL'. If specifging an IP address, enter either the full IP address or a generic IP address using an asterisk as the final character. IP Address Groups must be established prior to their entry on this screen (see IP Address Groups).

User represents the identity of the person initiating a transaction as a user profile. The special value *PUBLIC, when used on a Pre-filter, means that the Pre-filter applies to any User lacking a specific Pre-filter.

Allow

The setting for whether transactions matching this record should be allowed to continue to be processed by Exit Point Manager. Valid settings are 'Y' (Yes — Exit Point Manager rules should evaluate this transaction, which may or may not cause it to be rejected, 'N' (No — reject the transaction), and a gray Y or N (inherit the value from the System (*ALL) Pre-filter).

Aud/Msg/Cap columns

A ✔ or ✖ in one of these columns indicates the value is explicitly defined in the rule. A gray ✔ or ✖ indicates the value is not defined in the Pre-filter itself, but is inheriting the actual value from the default System Pre-filter (*ALL). See Active Rule and Rule derivation.

Audit

The audit property controls the type of requests Exit Point Manager will log. Possible values are:

Yes Log all requests by the location/server/function.
No Only log authority failures for the location/server/function.
Inherit Inherit the value.

Message

The message property entry will determine if Exit Point Manager sends a message to the Exit Point Manager message queue.

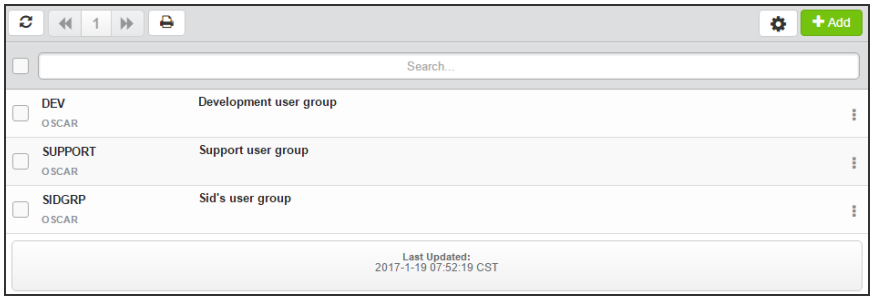
Yes A message is sent to the Exit Point Manager message queue.
No No message is sent.
Inherit Inherit the value.

Capture

Capture transactions for Memorized Transaction Request (MTR).

Yes Capture transactions.
No Do not capture transactions.
Inherit Inherit the value.

User Groups



How to Get There

Click the **User Groups** tab on the navigation pane on the left side of the Exit Point Manager window.

What it Does

The User Group screen allows you to maintain User Groups.

An User Group is simply a container for a group of user profile names. An User Group can be used in place of a user profile name in user rules.

The *sequence number* of a User Group determines the order in which it will be used by the exit point programs.

For example, if there are three User Rules with User Groups for a specific Server/Function, and all three have USER1 as a member, then the User Rule for the User Group with the lowest sequence number will be used by the exit programs (if a User Rule with the specific user name of 'USER1' is not found).

> **NOTE:** Adding OS User Groups to a Exit Point Manager Group is not recommended.

Options

Selection, sorting, filtering, deleting, and navigation features on this screen are described in Using the Web Browser Interface.

Add

Choose **Add** to open the New User Groups screen where you can add a new User Group. See New User Groups screen.

See also Creating User Groups.

Column Descriptions

Group Name

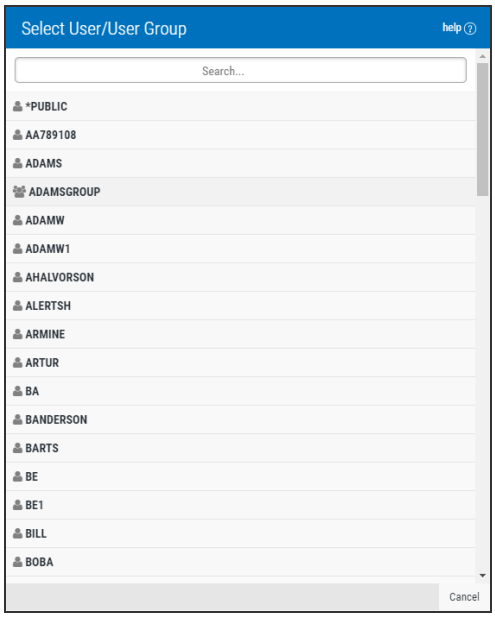
The name of the User Group.

Description

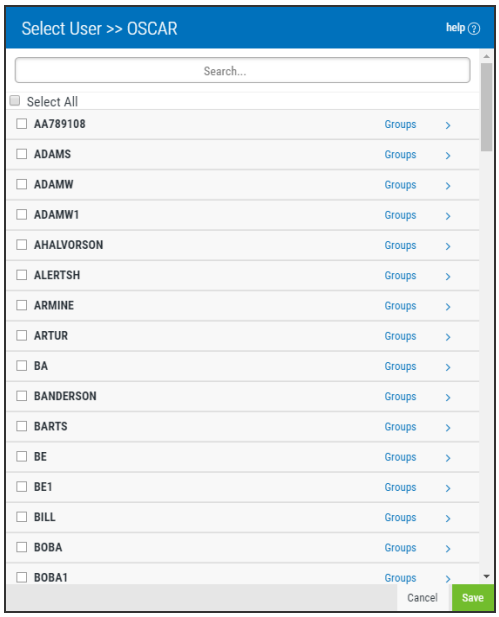
The description of the User Group.

Select User/User Group window

Rule Select User/User Group Window



Select User



How to Get There

Click **Lookup** next to the User field in the New/Edit Rule screen when adding or changing a rule.

Or, in the New/Edit User Groups screen, click **Add Member**.

What it Does

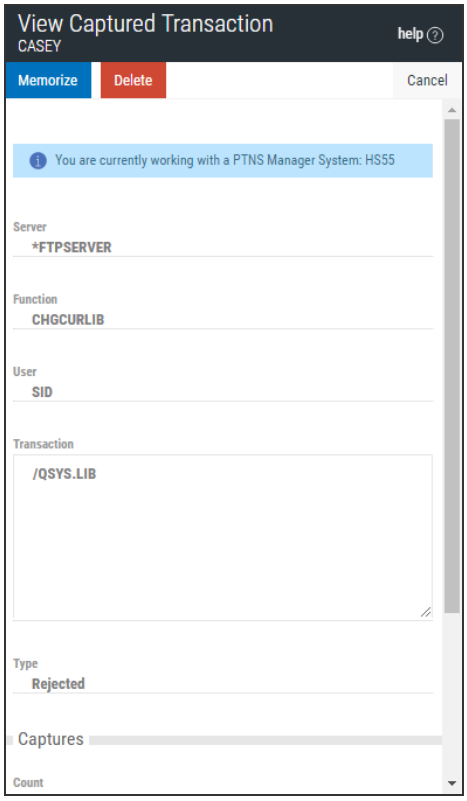
This window allows you to select a user or User Group when adding or changing rules. When accessed while creating or editing a User Group, it allows you to select the profiles you would like to add to the User Group and display all other groups that include each profile.

Options

[User/Group List]: When creating or editing a user rule, choose the user or User Group in the list that you would like the rule to apply to. When creating or editing an User Group, check the user or users you would like to add as members to the User Group.

Save: Click **save** to add the user or User Group to the rule, or, if creating or editing an User Group, add the profile(s) as members to the User Group.

View Captured Transaction



How to Get There

Click the **Captured Transactions** tab on the navigation pane on the left side of the Exit Point Manager window and click a captured transaction.

What it Does

The View Captured Transaction screen allows you to view the details of a memorized transaction.

Options

Memorize
Select **Memorize** to save this captured transaction as a Memorized Transaction for the user. See Memorized Transactions screen.

Delete
Choose **Delete** to delete the Memorized Transaction.

Cancel
Click **Cancel** to dismiss the View Transaction screen and return to the Captured Transactions screen.

Field Descriptions

Server
A Server in Exit Point Manager is a controlled entry point into your system. These entry points are determined and defined by IBM. Exit Point Manager has assigned easy-to-remember names to these controlled entry points.

Function
A Function, or Server Function, in Exit Point Manager represents a class of operations that a given Server may perform. For example, the *SIGNON Server classifies its operations as those pertaining to changing passwords, generating authentication tokens, and retrieving sign-on information. Exit Point Manager has assigned easy-to-remember names to these Functions, such as CHGPWD, GENAUTTKN and RETRIEVE.

User /Location
User represents the identity of the person initiating a transaction as a user profile. The special value *PUBLIC, when used on a rule, means that the rule applies to any User lacking a specific rule. when used as a subset or selection parameter, *PUBLIC means to select all such rules for display or printing. This displays the User to which this Memorized Transaction applies. If blank, then this is for a specific Location. If the value is *PUBLIC, the transaction applies to all users.

Location represents the source of a transaction. Location can hold an IP Address, an IP Address Group or the name of an SNA Communications Device. The special value *ALL, when used on a rule, means that the rule applies to any rule means that the rule applies to any Location lacking a specific rule. when used as a subset or selection parameter, *ALL generally means to select all such rules for display or printing. This displays the Location to which this Memorized Transaction applies. If blank, then this is for a specific User. If the value is *ALL, the transaction applies to all Users.

Transaction
The data portion of the transactions that were summarized into this record.

Type
The type of action performed by Exit Point Manager for the transactions summarized into this record.

Type values:

- NA Accepted
- NR Rejected
- NF Network Failure

Captures

Count
The number of times this transaction was recorded.

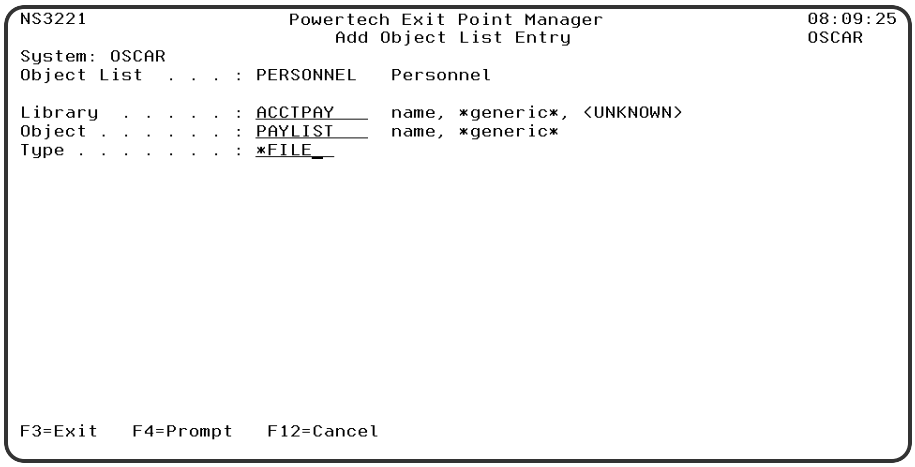
First Collected
The date and time when a transaction was first summarized into this record.

Last Collected
The date and time when a transaction was last summarized into this record.

Green Screen Panel Reference

The following topics list descriptions for all fields and options on Exit Point Manager's green screen panels. To view screens for the browser interface, see Browser Interface Screen Descriptions.

Add Object List Entry panel



How to Get There
From the Exit Point Manager Main Menu, select option **4** to display the Work with Security by Object panel. Select option **1** to display the Work with Object Lists panel, then enter a **8** in the Opt column on one of the Object Lists, then enter a **1** in the top slot under the Opt column and press `Enter`.

What it Does
The Add Object List Entry panel allows you to add an entry to an Object List.

Options

Library
The Library is the name of the library in which an object exists. This name is required to be a valid OS name. You can use the Generic Character to indicate that a partial value is to be used for selection. In some circumstances you may also use the Wildcard Character to indicate that a partial value is to be used for selection. You may specify <UNKNOWN> to indicate that the Object List Entry pertains only to unqualified objects whose library cannot be determined.

Object
Object is the name of an object in a library. This name is required to be a valid OS name. You can use the Generic Character to indicate that a partial value is to be used for selection. In some circumstances you may also use the wildcard Character to indicate that a partial value is to be used for selection.

Type
Object Type is the type of an object in a library.

Command Keys
F3 (Exit): Exit the panel without processing any pending changes.

F4 (Prompt): Displays a list of possible values from which you may select one.

F12 (Cancel) Exit the panel without processing any pending changes.

Add/Change User Rules

```
PNS4211                  Powertech Exit Point Manager              14:34:43
                            Add/Change User Rules                  OSCAR
System: OSCAR     Management System


User Rule Type  : _
User  . . . . . : __________


Authority . . . : __________
Switch Profile  : __________
Audit . . . . . : _
Message . . . . : _
Capture . . . . : _

Replace . . . . : _
Change only . . : _




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

How to Get There
Enter option **2** on the Exit Point Manager Main Menu to display the Work with Security by User panel. Press `F2` to display the Add User Rules panel.

What it Does
The Global Rule Facility panel allows you to create user rules for all Servers.

These rules will have a Function of *ALL.

Options

System
System indicates the target of any operations you perform. When you add rules, for example, those rules will be sent to, and will affect processing on, the System named.

User Type
This field is used to indicate whether the associated User field refers to an O/S user profile or a Exit Point Manager User Group.

Valid values are:

U The associated User field refers to an O/S user profile.
G The associated User field refers to a Exit Point Manager user group.

User
User represents the identity of the person initiating a transaction as a user profile.

The special value *PUBLIC, when used on a rule, means that the rule applies to any User lacking a specific rule. when used as a subset or selection parameter, *PUBLIC means to select all such rules for display or printing.

If the associated User Type is a 'G', User represents a Exit Point Manager User Group.

Server
A Server in Exit Point Manager is a controlled entry point into your system. These entry points are determined and defined by IBM. Exit Point Manager has assigned easy-to-remember names to these controlled entry points.

Function
A Function, or Server Function, in Exit Point Manager represents a class of operations that a given Server may perform. For example, the *SIGNON Server classifies its operations as those pertaining to changing passwords, generating authentication tokens, and retrieving signon information. Exit Point Manager has assigned easy-to-remember names to these Functions, such as CHGPWD, GENAUTTKN and RETRIEVE.

Authority Property
The authority assigned for servers and their functions.

Possible values are:

***OS400**Exit Point Manager will use normal OS/400 authority for the location. This is valid for both location and user.
***REJECT**Exit Point Manager will reject requests for the specified location. This is valid for both location and user.
***SWITCH**Exit Point Manager will use the authority of the switch profile for the specified location. A switch profile entry is required. This is valid for both location and user.
***MEMREJECT** Check Memorized Transactions (MTR) for authority. If no MTR authority is encountered, Exit Point Manager will reject requests for the specified location. This is valid for both location and user.

***MEMOS4OO** Check Memorized Transactions (MTR) for authority. If no MTR authority is encountered, Exit Point Manager will use normal OS/400 authority for the location. This is valid for both location and user.
***MEMSWITCH** Check Memorized Transactions (MTR) for authority. If no MTR authority is encountered, Exit Point Manager will use the authority of the switch profile for the specified location. A switch profile entry is required. This is valid for both location and user.
***SRVFCN**Exit Point Manager will use the authority defined for the server/function. This is valid for both location and user.

Switch

The Switch profile holds the name of a user profile whose authority is used to process the transaction instead of the authority of the User initiating the transaction. The transaction is executed as, and uses the authority of, this Switch profile.

Switch profile is allowed only when Authority contains *SWITCH or *MEMSWITCH, if *MEMSWITCH is allowed. Otherwise it must contain *NONE.

Audit Property

The audit property controls the type of requests Exit Point Manager will log.

Possible values are:

* Use the audit value for the server/function.
Y Log all requests by the location/server/function.
N Only log authority failures for the location/server/function.

Exit Point Manager will not change the existing settings and will not create new rules when the All Servers option is taken. This is valid for both location and user.

Message

The message property entry will determine if Exit Point Manager sends a message to the Exit Point Manager message queue.

Possible values are:

* Use the audit value for the server/function.
Y A message is sent to the Exit Point Manager message queue.
N No message is sent.

Capture

Capture transactions for Memorized Transaction Request (MTR).

Possible values are:

* Use the audit value for the server/function.
Y Capture transactions.
N Do not capture transactions.

Change existing

The Change existing option controls whether any existing rules are updated or not updated.

The valid values are Y and N.

Change only
If this is set to 'N' then new rules are added and (depending on the setting for Replace) existing rules are changed.

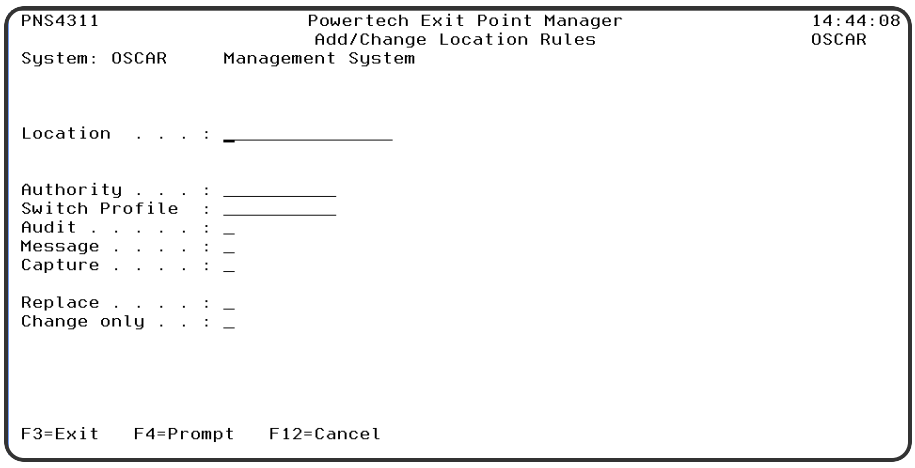
If this is set to 'Y' then only existing rules are changed.

The valid values are Y and N.

Command Keys
F3 (Exit): Exit the panel without processing any pending changes.

F12 (Cancel) Exit the panel without processing any pending changes.

Add Location Rules



How to Get There
Enter option **3** on the Exit Point Manager Main Menu to display the Work with Security by Location panel. Press `F2` to display the Add Location Rules panel.

What it Does
The Global Rule Facility panel allows you to create location rules for all Servers.

Options
These rules will have a Function of *ALL.

System
System indicates the target of any operations you perform. When you add rules, for example, those rules will be sent to, and will affect processing on, the System named.

Location
Location represents the source of a transaction. Location can hold an IP Address, an IP Address Group or the name of an SNA Communications Device.

The special value *ALL, when used on a rule, means that the rule applies to any Location lacking a specific rule. When used as a subset or selection parameter, *ALL generally means to select all such rules for display or printing.

Server

A Server in Exit Point Manager is a controlled entry point into your system. These entry points are determined and defined by IBM. Exit Point Manager has assigned easy-to-remember names to these controlled entry points.

Function

A Function, or Server Function, in Exit Point Manager represents a class of operations that a given Server may perform. For example, the *SIGNON Server classifies its operations as those pertaining to changing passwords, generating authentication tokens, and retrieving signon information. Exit Point Manager has assigned easy-to-remember names to these Functions, such as CHGPWD, GENAUTTKN and RETRIEVE.

Authority Property

The authority assigned for servers and their functions.

Possible values are:

***OS400**Exit Point Manager will use normal OS/400 authority for the location. This is valid for both location and user.
***REJECT**Exit Point Manager will reject requests for the specified location. This is valid for both location and user.
***SWITCH**Exit Point Manager will use the authority of the switch profile for the specified location. A switch profile entry is required. This is valid for both location and user.
***MEMREJECT** Check Memorized Transactions (MTR) for authority. If no MTR authority is encountered, Exit Point Manager will reject requests for the specified location. This is valid for both location and user.
***MEMOS4OO** Check Memorized Transactions (MTR) for authority. If no MTR authority is encountered, Exit Point Manager will use normal OS/400 authority for the location. This is valid for both location and user.
***MEMUSR** Check Memorized Transactions (MTR) for authority. If no MTR authority is encountered, Exit Point Manager will check server user authority. This is only valid for location.
***USER**Exit Point Manager will check server user authority. This is only valid for location.
***MEMSWITCH** Check Memorized Transactions (MTR) for authority. If no MTR authority is encountered, Exit Point Manager will use the authority of the switch profile for the specified location. A switch profile entry is required. This is valid for both location and user.
***SRVFCN**Exit Point Manager will use the authority defined for the server/function. This is valid for both location and user.
***SAME**Exit Point Manager will not change the existing settings and will not create new rules when the All Servers option is taken. This is valid for both location and user.

Switch Profile Property

The name of a switch profile for this location/server/function. If a profile name is supplied, processing is swapped to run under this profile's authority. This is only valid for authorities *SWITCH and *MEMSWITCH.

Possible values are:

***NONE** No switch profile is being used.
switch-profile The switch profile to process under. It must be an active profile residing on the AS/400.
***SRVFCN**Exit Point Manager will use the switch profile defined for the server/function. Exit Point Manager will use the switch profile defined for the server/function.

***SAME**Exit Point Manager will not change the existing settings and will not create new rules when the All Servers option is taken. This is valid for both location and user.

Audit Property

The audit property controls the type of requests Exit Point Manager will log.

Possible values are:

Y Log all requests by the location/server/function.
N Only log authority failures for the location/server/function.
* Use the audit value for the server/function.

Exit Point Manager will not change the existing settings and will not create new rules when the All Servers option is taken. This is valid for both location and user.

Message

The message property entry will determine if Exit Point Manager sends a message to the Exit Point Manager message queue.

Possible values are:

N No message is sent.
Y A message is sent to the Exit Point Manager message queue.
* Use the audit value for the server/function.
S Exit Point Manager will not change the existing settings and will not create new rules when the All Servers option is taken. This is valid for both location and user.

Capture

Capture transactions for Memorized Transaction Request (MTR).

Possible values are:

N Do not capture transactions.
Y Capture transactions.
* Use the audit value for the server/function.
S Exit Point Manager will not change the existing settings and will not create new rules when the All Servers option is taken. This is valid for both location and user.

Change existing

The Change existing option controls whether any existing rules are updated or not updated.

The valid values are Y and N.

Change only

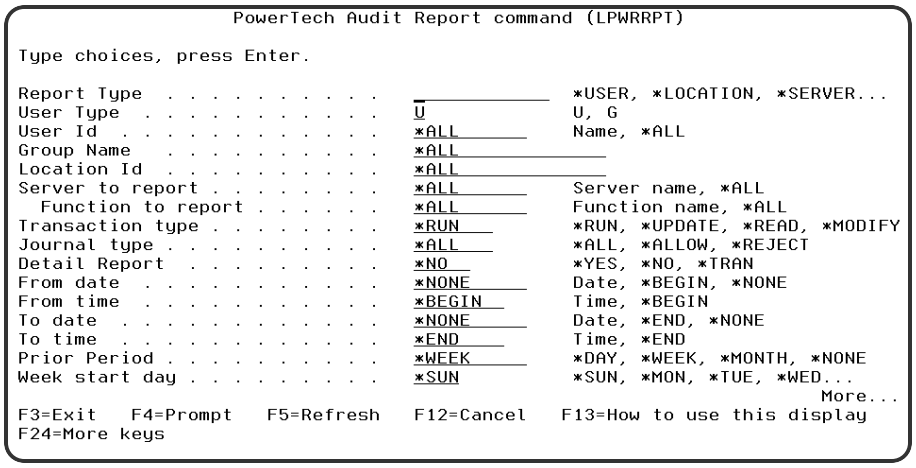
If this is set to 'N' then new rules are added and (depending on the setting for Replace) existing rules are changed.

If this is set to 'Y' then only existing rules are changed.

The valid values are Y and N.

Powertech Audit Report Command

The LPWRRPT command provides a command-line interface to Exit Point Manager audit reports. This allows scheduling reports through the job scheduler or other scheduling function.



Field Descriptions

Report type (RPTTYP)

Specifies the name of the basic report type. This requests a report selecting by user, location, server/function, user group or transaction. This is a required parameter.

The possible values are:

***USER** A report by user should be run.
***LOCATION** A report by location should be run.
***SERVER** A report by server/function should be run.
***TRANSACTION** A report by network transaction type should be run.
***GRPPRF** A report by iSeries Group Profile should be run.
***ACCNTCDE** A report by iSeries Recount Code should be run.
***PWRLCKGRP** A report by Exit Point Manager Group should be run.

User Type (USERTYPE)

Specifies whether the user field is a user profile or a User Group.

Allowed values are:

U The user field is a user profile.
G The user field is a User Group

User ID (USER)

Specifies the user profile to run the report over.

This is an optional parameter.

Allowed values are:

***ALL** Print the report including all user profiles.
user ID Enter a valid user profile identifier. Or, if the User Type is G, enter the User Group name.

Group Name (GROUP)

Specifies group (Account Code, Exit Point Manager, Grp Profile) for the report.

This is an optional parameter.

Allowed values are:

***ALL** Print the report including all Groups of selected type.
Group ID Enter a valid user Group identifier for selected group type.
***NOGRP** Print the report and do not include records associated with groups.

Location ID (LOCATION)

Specifies the SNA or TCP/IP location to run the report over.

This is an optional parameter.

Allowed values are:

*ALL Print the report including all locations.

location Enter a valid SNA or TCP/IP location. This can be a location name or a TCP/IP address.

Server to Report (SVR)

Specifies the server to run the report over.

This is an optional parameter.

Allowed values for server are:

***ALL** Print the report including all servers.
server-name Enter a valid server name.

Function to Report (FNC)

Specifies the function to run the report over. This is an optional parameter.

Allowed values for function are:

***ALL** Print the report including all functions.
function-name Enter a valid function name.

Transaction type (TRNTYP)

Specifies the network transaction type to run the report over. This is an optional parameter.

Allowed values are:

***RUN** The report shows requests to run commands and/or programs.
***UPDATE** The report shows requests to update data.
***READ** The report shows requests to read data.
***MODIFY** The report shows requests to modify data.

Journal type (JRNTYP)

Specifies the type of journal entry to include in the report.

This is an optional parameter.

Allowed values are:

***ALL** The report includes all Exit Point Manager journal entries.

***ALLOW** The report shows only Exit Point Manager allowed entries.
***REJECT** The report shows only Exit Point Manager rejected entries.

Detail report (DTLREPORT)

Specifies whether a detail-level report is generated. This is an optional parameter.

Allowed values are:

***NO** A detail-level report will not be generated.
***YES** A detail-level report will be generated.
***TRAN** A detail-level report will be generated and the transaction will be printed.

From date (FRMDAT)

Specifies the beginning date to include in the report when a date range is requested. This is an optional parameter. This parameter is mutually exclusive with PERIOD.

Allowed values are:

***BEGIN** The report will begin with the oldest transactions in the journal.
***NONE** The from-date is not specified. Note: This is only meaningful when a PERIOD report is requested.
date The report will begin with transactions from [including] this date. Note: If old journal receivers have been deleted, they must be restored if entries are to be included from their dates.

From time (FRMTIM)

Specifies the beginning time to include in the report when a date range is requested. This is an optional parameter. This parameter is mutually exclusive with PERIOD.

Allowed values are:

***BEGIN** The report will begin with transactions in the journal with no time limit.
time The report will begin with transactions from (including) this time.

To date (TODAT)

Specifies the ending date to include in the report when a date range is requested. This is an optional parameter. This parameter is mutually exclusive with PERIOD.

Allowed values are:

***END** The report will end with the newest transactions in the journal.
***NONE** The to-date is not specified. Note: This is only meaningful when a PERIOD report is requested.
date The report will end with transactions from (including) this date.

To time [TOTIM]

Specifies the ending time to include in the report when a date range is requested. This is an optional parameter. This parameter is mutually exclusive with PERIOD.

Allowed values are:

***END** The report will end with transactions in the journal with no time limit.
time The report will end with transactions up to (including) this time.

Prior Period [PERIOD]

Specifies the period type when a period report is requested. Period reports are intended to be run at regularly scheduled intervals. The available periods are day, week and month. Periods are considered as "prior day", "prior week" and "prior month" and are used to avoid specifying dates for every scheduled run. Use the COUNT parameter to request multiple periods. This is an optional parameter. This parameter is mutually exclusive with FRMDAT and TODAT.

Allowed values are:

***DAY** The report includes entries for the dag prior to the run-date of this command.
***WEEK** The report includes entries for the week period prior to the run-date of this command.
***MONTH** The report includes entries for the month period prior to the run-date of this command.

week start day (STRDAY)

Specifies the starting dag for a weekly period report.

When a period report is requested and the period type is *WEEK, this specifies the first day of each weekly period. The default is set for Sunday, but any day can be chosen. This allows weekly reports based on the customer definition of a "week". This is an optional parameter. This parameter is meaningful only when period is *WEEK.

Allowed values are:

***SUN** The report includes entries for a week period beginning on Sunday and ending on Saturday.
***MON** The *WEEK report begins on a Monday.
***TUE** The *WEEK report begins on a Tuesday.
***WED** The *WEEK report begins on a Wednesday.
***THU** The *WEEK report begins on a Thursday.
***FRI** The *WEEK report begins on a Friday.
***SAT** The *WEEK report begins on a Saturday.

Period count [COUNT]

Specifies the number of prior periods to include when a period report is requested. This is an optional parameter.

Allowed values are:

1 The report will include a single period.
count The report will include as many periods as are given here. Note: If old journal receivers have been deleted, they must be restored if entries are to be included from their dates.

Output type [OUTPUT] Specifies the form of output.

This requests the output in either printed or database form or in a .CSV streamfile.

This is a required parameter.

The possible values are:

***PRINT** The output should be a printed report.
***OUTFILE** The output should be directed to a database file.
***IFS** The output should be directed to a .CSV streamfile in the IFS. The streamfile will be created in the location identified in the GNUI Report Output control file (PNSGRO).

Create file [CRTFILE]

Specifies whether the output file should be created if it does not exist. This is an optional parameter.

Allowed values are:

***NO** The output file should not be created. The command will fail if the file does not exist.
***YES** The file will be created if it does not exist when the command executes.

IFS report name (RPTNAM)

Specifies the report name of the IFS streamfile. This name is used to log the creation and location of any IFS streamfiles that are created.

The possible values are:

report-name Enter the name of IFS report. This is a report name, not a streamfile name. IFS output is created in the users home directory. This report name identifies report requests.

Output file (OUTFILE)

Specifies the name of the database file that will contain the selected output.

The possible values are:

database-file-name Enter the name of the database file that will contain the selected output.

The possible library values are:

***CURLIB** The current library will be used. If you have not assigned a library as the current library, QGPL will be used.
library-name Enter the name of the library where the database file is located.

Output member options (OUTMBR)

Specifies the member name and option when output is directed to a database file. This is an optional parameter. This is only meaningful when OUTPUT[*OUTFILE] is selected.

Allowed values for member are:

***FIRST** The first [or only] member receives the output.
member-name Enter a valid member name.

Allowed values for option are:

***REPLACE** The member data is replaced by this output.
***ADD** The existing member data is kept and this output is added to the end of the member.

Command Keys

F3 (Exit): Exit the panel without processing any pending changes.

F4 (Prompt): Displays a list of possible values from which you may select one.

F5 (Refresh): Refreshes the panel and resets all available text fields.

F9 (All Parameters): Shows all available parameters.

F11 (Keywords): Displays command keywords on the entry fields.

F12 (Cancel): Exit the panel without processing any pending changes.

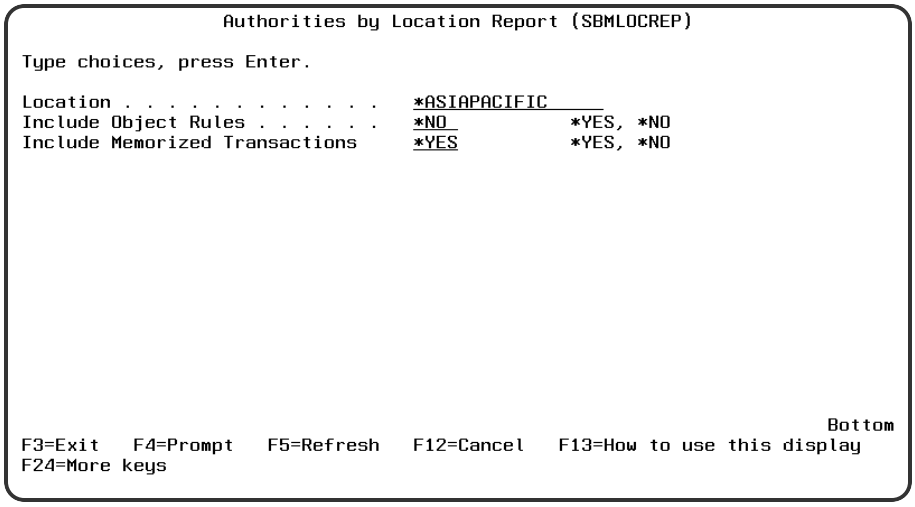
F13 (How to use this display): Shows help for the prompt display or associated display you are currently using.

F14 (Command string): Displays the command string based on the panel configuration.

F24 (More keys): Shows additional function keys that can be used for this display.

Authorities by Location Report (SBMLOCREP)

The Authorities by Location Report (SBMLOCREP) command produces the "Location/IP Address Rules Listing" report. The report can optionally list the Object Rules and Memorized Transaction associated with the Locations printed on the report.



Options

Location (LOC)

Specifies the location or locations whose rules will be included in the report. Specifying *ALL for this parameter will include rules for all locations.

The valid values are:

Location Specify a Location (an IP address, IP Address Group name, SNA device).
***ALL** Includes rules for all locations.

Include Object Rules (INCLOBJRUL)

Indicate whether you would like the Object Rules printed on the report for each Location Rule printed.

The valid values are:

***YES** Object Rules are printed on the report.
***NO** Object Rules are not printed on the report.

Include Memorized Transactions (INCLMEMTRN)

Indicate whether you would like the Memorized Transactions printed on the report for each Location Rule printed.

The valid values are:

***YES** Memorized Transactions are printed on the report.
***NO** Memorized Transactions are not printed on the report.

Command Keys

F3 (Exit): Exit the panel without processing any pending changes.

F4 (Prompt): Displays a list of possible values from which you may select one.

F5 (Refresh): Refreshes the panel and resets all available text fields.

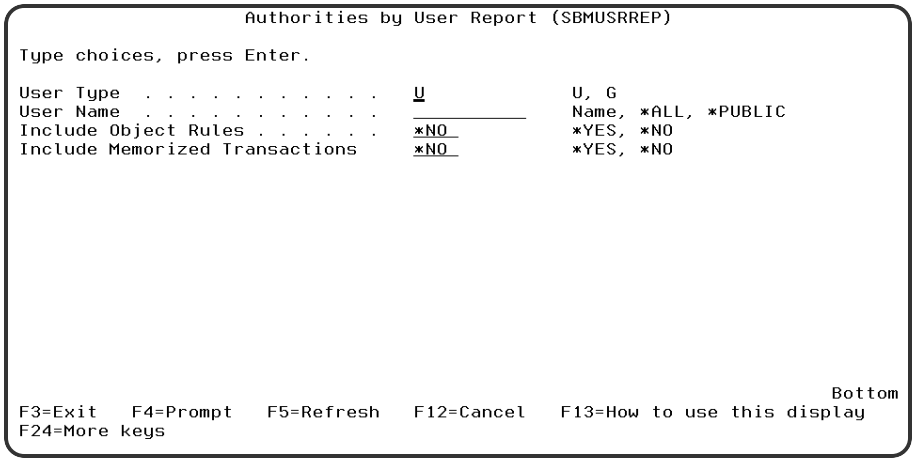
F12 (Cancel): Exit the panel without processing any pending changes.

F13 (How to use this display): Shows help for the prompt display or associated display you are currently using.

F24 (More keys): Shows additional function keys that can be used for this display.

Authorities by User Report (SBMUSRREP)

The Authorities by User Report (SBMUSRREP) command produces the "User Rules Listing" report. The report can optionally list the Object Rules and Memorized Transaction associated with the users printed on the report.



Options

User Type

This field is used to indicate whether the associated User field refers to an O/S user profile or a Exit Point Manager User Group.

Valid values are:

U The associated User field refers to an O/S user profile.
G The associated User field refers to a Exit Point Manager user group.

User Name (USR)

Specify the name of a user whose rules are to be listed.

The valid values are:

Name A specific user profile.
***ALL** All users.
***PUBLIC** The user level for non-specific users.

Include Object Rules (INCLOBJRUL)

Indicate whether you would like the Object Rules printed on the report for each User Rule printed.

The valid values are:

***YES** Object Rules are printed on the report.
***NO** Object Rules are not printed on the report.

Include Memorized Transactions (INCLMEMTRN)

Indicate whether you would like the Memorized Transactions printed on the report for each User Rule printed.

The valid values are:

***YES** Memorized Transactions are printed on the report.
***NO** Memorized Transactions are not printed on the report.

Command Keys

F3 (Exit): Exit the panel without processing any pending changes.

F4 (Prompt): Displays a list of possible values from which you may select one.

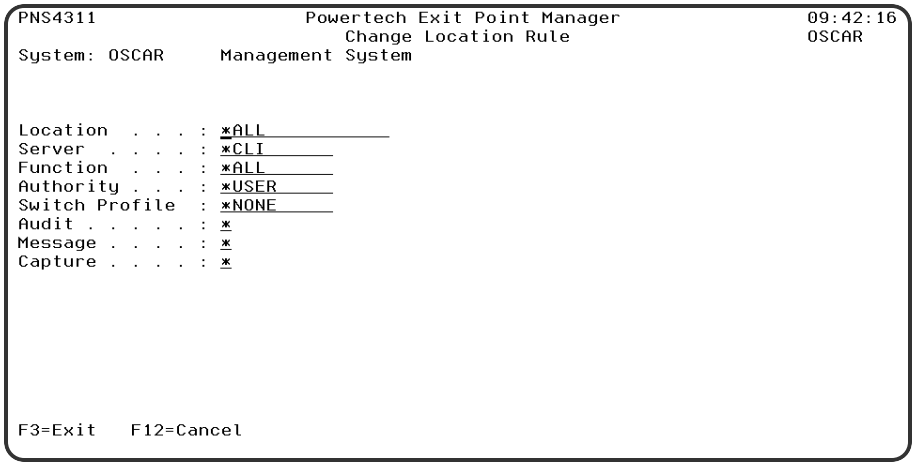
F5 (Refresh): Refreshes the panel and resets all available text fields.

F12 (Cancel): Exit the panel without processing any pending changes.

F13 (How to use this display): Shows help for the prompt display or associated display you are currently using.

F23 (More keys): Shows additional function keys that can be used for this display.

Change Location Rule panel



How to Get There

On the Work with Security by Location panel, choose **2** for a Location Rule.

What it Does

The Change Location Rule panel allows you to modify a Location Rule's attributes.

Field Descriptions

System

System indicates the target of any operations you perform. When you add rules, for example, those rules will be sent to, and will affect processing on, the System named.

Location

Location represents the source of a transaction. Location can hold an IP Address, an IP Address Group or the name of an SNA Communications Device.

The special value *ALL, when used on a rule, means that the rule applies to any Location lacking a specific rule. When used as a subset or selection parameter, *ALL generally means to select all such rules for display or printing.

Server

A Server in Exit Point Manager is a controlled entry point into your system. These entry points are determined and defined by IBM. Exit Point Manager has assigned easy-to-remember names to these controlled entry points.

Function

A Function, or Server Function, in Exit Point Manager represents a class of operations that a given Server may perform. For example, the *SIGNON Server classifies its operations as those pertaining to changing passwords, generating authentication tokens, and retrieving signon information. Exit Point Manager has assigned easy-to-remember names to these Functions, such as CHGPWD, GENAUTTKN and RETRIEVE.

Authority Property

The authority assigned to the location for this server/function. If authority is left blank, Exit Point Manager will remove the location's entry.

Possible values are:

***OS400** Exit Point Manager will use normal OS/400 authority for the location.
***REJECT** Exit Point Manager will reject requests for the specified location.
***SWITCH** Exit Point Manager will use the authority of the switch profile for the specified location. A switch profile entry is required.
***MEMREJECT** Check Memorized Transactions (MTR) for authority. If no MTR authority is encountered, Exit Point Manager will reject requests for the specified location.
***MEMOS4OO** Check Memorized Transactions (MTR) for authority. If no MTR authority is encountered, Exit Point Manager will use normal OS/400 authority for the location. This is valid for both location and user.
***MEMSWITCH** Check Memorized Transactions (MTR) for authority. If no MTR authority is encountered, Exit Point Manager will use the authority of the switch profile for the specified location. A switch profile entry is required.
***SRVFCN** Exit Point Manager will use the authority defined for the server/function.

Switch The Switch profile holds the name of a user profile whose authority is used to process the transaction instead of the authority of the User initiating the transaction. The transaction is executed as, and uses the authority of, this Switch profile.

Switch profile is allowed only when Authority contains *SWITCH or *MEMSWITCH, if *MEMSWITCH is allowed. Otherwise it must contain *NONE.

Aud

The Audit transactions flag controls the logging of transactions to the Log Journal set up on the Work with Exit Point Manager System Values panel.

The valid values are:

* Uses the value found in the rule above this one in the rule hierarchy.
Y Logs all requests when this rule is enforced.
N Logs only access failures (rejects) for this rule.

Msg

The Send messages flag controls the sending of messages to the Log Message Queue set up on the Work with Exit Point Manager System Values panel.

The valid values are:

* Uses the value found in the rule above this one in the rule hierarchy.
Y Sends a message when this rule is enforced.
N Does not send a message when this rule is enforced.

Capture

The Capture transactions flag controls whether transactions are remembered in Exit Point Manager for later memorization. Once captured, transactions can become Memorized Transactions which can act as rules.

The valid values are:

* Uses the value found in the rule above this one in the rule hierarchy.
Y Captures the transaction when this rule is enforced.
N Does not capture the transaction when this rule is enforced.

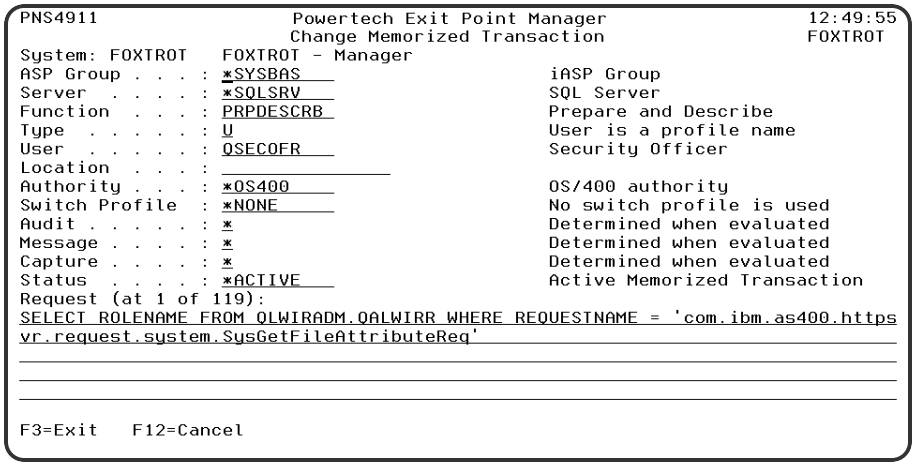
Command Keys

F3 (Exit): Exit the panel without processing any pending changes.

F4 (Prompt): Displays a list of possible values from which you may select one.

F12 (Cancel): Exit the panel without processing any pending changes.

Change Memorized Transaction



How to Get There

From the Exit Point Manager Main Menu, select option **11**. On the Work with Memorized Transactions panel, choose option **2** for a Memorized Transaction and press `Enter`.

What it Does

The Change a Memorized Transaction panel allows you to make changes to some of the attributes of a Memorized Transaction. Those attributes that are input capable can be changed.

Options

System

System indicates the target of any operations you perform. When you add rules, for example, those rules will be sent to, and will affect processing on, the System named.

ASP Group

When a memorized transaction is evaluated, this ASP Group name will be compared to the current ASP Group name of the job issuing the transaction. These need to be the same (or this must be set to the special value *ALL) for this memorized transaction to be considered a match.

Server

A Server in Exit Point Manager is a controlled entry point into your system. These entry points are determined and defined by IBM. Exit Point Manager has assigned easy-to-remember names to these controlled entry points. This field cannot be changed.

Function

A Function, or Server Function, in Exit Point Manager represents a class of operations that a given Server may perform. For example, the *SIGNON Server classifies its operations as those pertaining to changing passwords, generating authentication tokens, and retrieving sign-on information. Exit Point Manager has assigned easy-to-remember names to these Functions, such as CHGPWD, GENAUTTKN and RETRIEVE. This field cannot be changed.

Type

This field is used to indicate whether the associated User field refers to an O/S user profile or a Exit Point Manager User Group.

Valid values are:

U The associated User field refers to an O/S user profile.
G The associated User field refers to a Exit Point Manager user group.

User

User represents the identity of the person initiating a transaction as a user profile. The special value *PUBLIC, when used on a rule, means that the rule applies to any User lacking a specific rule. When used as a subset or selection parameter, *PUBLIC means to select all such rules for display or printing. This displays the User to which this Memorized Transaction applies. If blank, then this is for a specific Location. If the value is *PUBLIC, the transaction applies to all users. This field cannot be changed.

Location

Location represents the source of a transaction. Location can hold an IP Address, an IP Address Group or the name of an SNA Communications Device. The special value *ALL, when used on a rule, means that the rule applies to any rule means that the rule applies to any Location lacking a specific rule. when used as a subset or selection parameter, *ALL generally means to select all such rules for display or printing. This displays the Location to which this Memorized Transaction applies. If blank, then this is for a specific User. If the value is *ALL, the transaction applies to all locations. This field cannot be changed.

Authority

Authority represents the action to be taken when a rule is found that matches the data present on a transaction.

Specify the new Authority value for the rule. You can press `F4` to see a list of valid values that can be specified. The list of valid values may include one or more of these values:

***USER** Current user authority is used.
***0S400** Exit Point Manager will use normal operating system authority for the user.
***REJECT** Exit Point Manager will reject requests.
***SWITCH** Exit Point Manager will use the authority of the switch profile for the transaction. A switch profile entry is required.
***MEMUSR** Memorized Transactions (MTR) are checked for authority first. If no MTR authority is encountered, Exit Point Manager will use the authority of the current user.
***MEMOS400** Memorized Transactions (MTR) are checked for authority first. If no MTR authority is encountered, Exit Point Manager will use normal operating system authority for the user.
***MEMREJECT** Memorized Transactions (MTR) are checked for authority first. If no MTR authority is encountered, Exit Point Manager will reject requests for the specified user.
***MEMSWITCH** Memorized Transactions (MTR) are checked for authority first. If no MTR authority is encountered, Exit Point Manager will use the authority of the switch profile for the specified user. A switch profile entry is required.
***MEMOBJ** Memorized Transactions (MTR) are checked for authority first. If no MTR authority is encountered, Exit Point Manager will check any objects used in the transactions for authorities defined by Object Rules.
***SERVER** Exit Point Manager will use the authority defined for the Server.
***SRVFCN** Exit Point Manager will use the authority defined for the Server Function.

Audit transactions

The Audit transactions flag controls the logging of transactions to the Log Journal set up on the work with Exit Point Manager System Values panel. Specify one of these values for Audit transactions:

***DEFAULT** Uses the value found in the rule above this one in the rule hierarchy.
***YES** Logs all requests when this rule is enforced.
***NO** Logs only access failures (rejects) for this rule.

Send messages

The Send messages flag controls the sending of messages to the Log Message Queue set up on the work with Exit Point Manager System Values panel.

Specify one of these values for Send messages:

***DEFAULT** Uses the value found in the rule above this one in the rule hierarchy.
***YES** Sends a message when this rule is enforced.
***NO** Does not send a message when this rule is enforced.

Capture transactions

The Capture transactions flag controls whether transactions are remembered in Exit Point Manager for later memorization. Once captured, transactions can become Memorized Transactions which can act as rules. Specify one of these values for Capture transactions:

***DEFAULT** Uses the value found in the rule above this one in the rule hierarchy.
***YES** Captures the transaction when this rule is enforced.
***NO** Does not capture the transaction when this rule is enforced.

Switch profile

The Switch profile holds the name of a user profile whose authority is used to process the transaction instead of the authority of the User initiating the transaction. The transaction is executed as, and uses the authority of, this Switch profile. Switch profile is allowed only when Authority contains *SWITCH or *MEMSWITCH, if *MEMSWITCH is allowed. Otherwise it must contain *NONE. Specify the new Switch profile value or one of these special values:

***NONE** No Switch profile is to be used. This is the only value allowed unless you have specified *SWITCH or *MEMSWITCH for Authority.
***SRVFCN** Use the Switch profile specified for the Server Function.

Status

This is the status of the Memorized Transaction.

Possible values are:

***ACTIVE** Exit Point Manager will attempt to match this transaction during rule enforcement. Memorized Transactions that are changed to *ACTIVE will have a matching User or Location rule changed to the corresponding action; *ALLOW to *MEMOS400, *REJECT to *MEMREJECT, or *SWITCH to *MEMSWITCH.
***INACTIVE**Exit Point Manager will not attempt to match this transaction during rule enforcement. Memorized Transactions that are changed to *INACTIVE will have the matching User or Location rule changed (if there are no other Memorized Transactions for that rule) to the corresponding action; *MEMOS400 to *ALLOW, *MEMREJECT to *REJECT, or *MEMSWITCH to *SWITCH.

Transaction

The Memorized Transaction against which incoming transactions are tested. If a match is found, then this rule will be invoked. Undisplayable characters in the transaction data are replaced by the mid—dot character (-).

You can use the Transaction wildcard character (%) to make a Transaction generic. The wildcard character is valid only at the end of a Transaction string. when you are memorizing or changing a Memorized Transaction, the first occurrence of the wildcard character that was NOT present in the string before you changed it will make the string generic and all data after that wildcard character will be discarded.

Command Keys

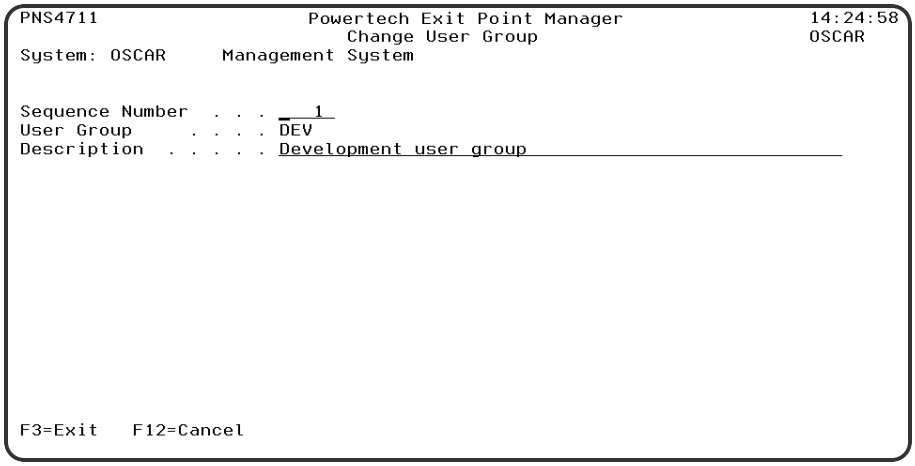
F3 (Exit): Exit the panel without processing any pending changes.

F4 (Prompt): Displays a list of possible values from which you may select one.

F12 (Cancel): Exit the panel without processing any pending changes.

Page Up/Page down: Rolls the transaction data up and down.

Change User Group



How to Get There

From the Exit Point Manager Main Menu, select option **7**, Work with User Groups, then choose **2** for a Group.

What it Does

The Change User Group panel allows you to modify a User Group's attributes.

Field Descriptions

System

System indicates the target of any operations you perform. When you add rules, for example, those rules will be sent to, and will affect processing on, the System named.

Seq
Enter the sequence number used that will be used to determine the order in which this User Group will be evaluated by the exit point programs.

For example, if there are three User Rules with User Groups for a specific Server/Function, and all three have USER1 as a member, then the User Rule for the User Group with the lowest sequence number will be used by the exit programs (if a User Rule with the specific user name of 'USER1' is not found).

Name
The User Group name is a short name you assign to a group of user profiles to help you identify the group.

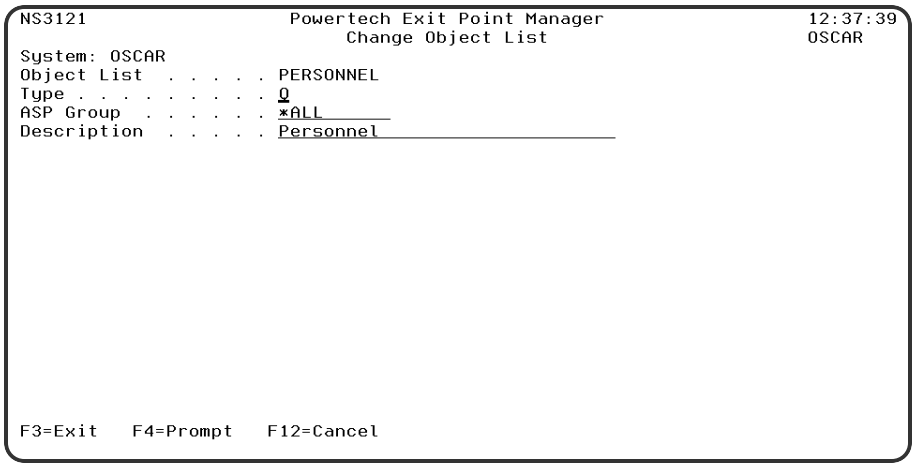
This name is required to be a valid OS name.

Description
The User Group description is a short textual description of the User Group. It is typically used to indicate the purpose or contents of the User Group.

Command Keys
F3=Exit: Exit the current panel without processing any pending changes.

F12=Cancel: Exit the current panel without processing any pending changes.

Change Object List



How to Get There
To view these options, from the Exit Point Manager Main Menu, select option **4** to display the Work with Security by Object panel. Select option **1** to display the Work with Object Lists panel, then enter a **2** in the Opt column on one of the Object Lists.

What it Does
The Change Object List panel allows you to modify an Object List's attributes.

Field Descriptions

Object List
The Object List name is a short name you assign to a list of objects to help you identify the list. This name is required to be a valid OS name.

Type
The Object List type determines what type of entries can be added to an Object List. Object lists can hold native object specifications (library, object and type) or paths to IFS objects.

Valid values are:

Q The Object List entries are native object specifiers.
I The Object List entries are paths to IFS objects.

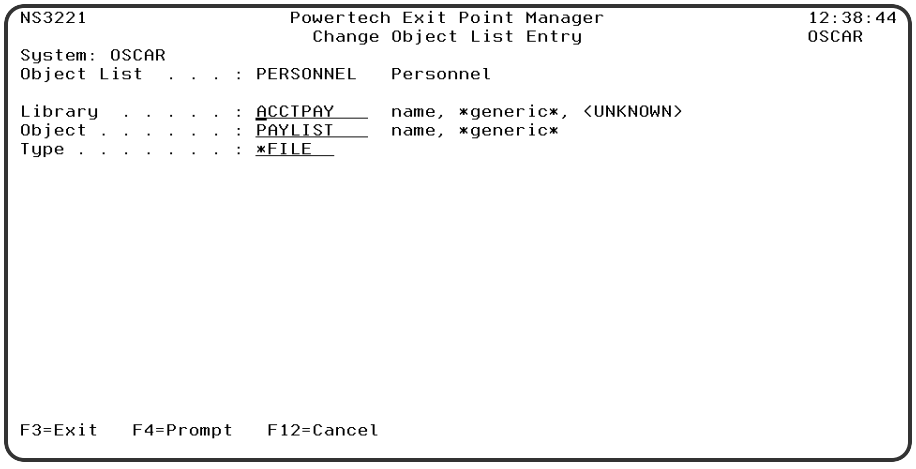
Description
The Object List description is a short textual description of the Object List. It is typically used to indicate the purpose or contents of the Object List.

Command Keys
F3 (Exit): Exit the panel without processing any pending changes.

F4 (Prompt): Displays a list of possible values from which you may select one.

F12 (Cancel): Exit the panel without processing any pending changes.

Change Object List Entry



How to Get There
From the Exit Point Manager Main Menu, select option **4** to display the Work with Security by Object panel. Select option **1** to display the Work with Object Lists panel, then enter an **8** in the Opt column on one of the Object Lists. In the Work with Object List Entries panel, enter **2** in the Opt column for one of the libraries.

What it Does
The Change Object List Entry panel allows you to modify an Object List Entry's attributes.

Options

Library
The Library is the name of the library in which an object exists. This name is required to be a valid OS name. You can use the Generic Character (*) to indicate that a partial value is to be used for selection. In some circumstances you may also use the Wildcard Character (?) to indicate that a partial value is to be used for selection. You may specify <UNKNOWN> to indicate that the Object List Entry pertains only to unqualified objects whose library cannot be determined.

Object
Object is the name of an object in a library. This name is required to be a valid OS name. You can use the Generic Character (*) to indicate that a partial value is to be used for selection. In some circumstances you may also use the wildcard Character (?) to indicate that a partial value is to be used for selection.

Type
Object Type is the type of an object in a library.

Command Keys
F3 (Exit): Exit the panel without processing any pending changes.

F4 (Prompt): Displays a list of possible values from which you may select one.

F12 (Cancel): Exit the panel without processing any pending changes.

Change Object Rule by User

```
NS3331                  Powertech Exit Point Manager                  12:51:20
                         Change Object Rule by User                   OSCAR
System: OSCAR     _
User . . . . . . . . . . . MARKJ
Object List  . . . . . . . PERSONNEL        Personnel
Operation  . . . . . . . . *ALL             F4 for list
Status . . . . . . . . . . *ACTIVE          *ACTIVE, *INACTIVE

Data Accesses:
  Authority  . . . . . . . *OS400           *OS400, *REJECT, *SWITCH
  Audit Transactions . . . N                Y=Yes, N=No, *=Default
  Send Messages  . . . . . N                Y=Yes, N=No, *=Default
  Capture Transactions . . N                Y=Yes, N=No, *=Default
  Switch Profile . . . . . *NONE            User profile, *NONE

Object Accesses:
  Authority  . . . . . . . *OS400           *OS400, *REJECT, *SWITCH
  Audit Transactions . . . *                Y=Yes, N=No, *=Default
  Send Messages  . . . . . *                Y=Yes, N=No, *=Default
  Capture Transactions . . *                Y=Yes, N=No, *=Default
  Switch Profile . . . . . *NONE            User profile, *NONE

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

How to Get There
From the Exit Point Manager Main Menu, select option **4** to display the Work with Security by Object panel. Select option **1** to display the Work with Object Lists panel, then enter an **9** in the Opt

column on one of the Object Lists. On the Object Rules using Object List panel, enter a **2** in the Opt column and a User. Press `Enter` to display the Change Object Rule by User panel.

What it Does

The Change Object Rule by User panel allows you to modify an Object Rule's attributes.

Options

User

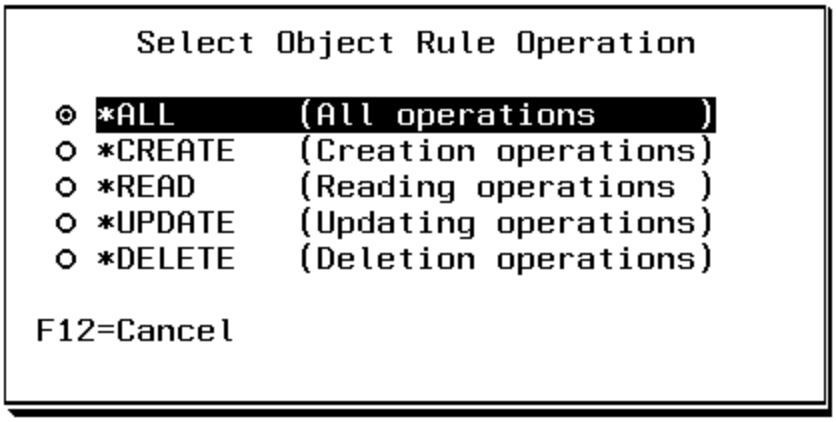
User represents the identity of the person initiating a transaction as a user profile. The special value *PUBLIC, when used on a rule, means that the rule applies to any User lacking a specific rule. when used as a subset or selection parameter, *PUBLIC means to select all such rules for display or printing.

Object List

The Object List name is a short name you assign to a list of objects to help you identify the list. This name is required to be a valid OS name.

Operation

Operation represents the type of action being performed upon an object or upon the data in an object.



Valid values and their meanings are:

*__ALL__ Applies to all of the above types of operations.
*__CREATE__ Applies to objects when they are being created or to their data when they are being added to an object; for example, when writing records to a database.
*__READ__ Applies to non—modifying accesses of objects or the reading of an object's data.
*__UPDATE__ Applies to changes to objects or changes to their data.
*__DELETE__ Applies to deletion of objects or deletion of their data; for example, deleting records from a database file.

Status

Status indicates that an Object Rule is active (being enforced) or inactive (not being enforced).

Data Accesses

Use the data access rights to specify user rights to the data in the objects contained in the Object List.

Authority

Authority represents the action to be taken when a rule is found that matches the data present on a transaction. This Authority value pertains to Data Accesses.

The valid values are:

***OS400** The transaction will be allowed and object authority will be determined by the operating system.
***REJECT** The transaction will not be allowed.
***SWITCH** The transaction will be allowed and the transaction will occur as if the user profile named as the Swap Profile had initiated the transaction. After switching to the Swap Profile, the authority used during the transaction will be determined by the operating system.

Audit Transactions

The Audit transactions flag controls the logging of transactions to the Log Journal set up on the work with Exit Point Manager System Values panel. This Audit Transaction flag pertains to Data Accesses.

The valid values are:

Y The transaction will be logged to the Log Journal.
N The transaction will not be logged to the Log Journal.
* The default value from a prior rule will control the logging.

Send Messages

The Send messages flag controls the sending of messages to the Log Message Queue set up on the Work with Exit Point Manager System Values panel. This Send Messages flag pertains to Data Accesses.

The valid values are:

Y A log message will be sent to the Log Message Queue.
N A log message will not be sent to the Log Message Queue.
* The default value from a prior rule will control the logging.

Capture Transactions

The Capture transactions flag controls whether transactions are remembered in Exit Point Manager for later memorization. Once captured, transactions can become Memorized Transactions which can act as rules. This Capture Transactions flag pertains to Data Accesses.

The valid values are:

Y A log message will be sent to the Log Message Queue.
N A log message will not be sent to the Log Message Queue.
* The default value from a prior rule will control the logging.

Switch Profile

The Switch profile holds the name of a user profile whose authority is used to process the transaction instead of the authority of the User initiating the transaction. The transaction is executed as, and uses the authority of, this Switch profile. Switch profile is allowed only when Authority contains *SWITCH or *MEMSWITCH, if *MEMSWITCH is allowed. Otherwise it must contain *NONE.

This Switch Profile pertains to Data Accesses.

Object Access Rights

Use the object access rights to specify user rights to the objects in the Object List.

Authority

Authority represents the action to be taken when a rule is found that matches the data present on a transaction. This Authority value pertains to Object Accesses.

The valid values are:

***OS400** The transaction will be allowed and object authority will be determined by the operating system.
***REJECT** The transaction will not be allowed.
***SWITCH** The transaction will be allowed and the transaction will occur as if the user profile named as the Swap Profile had initiated the transaction. After switching to the Swap Profile, the authority used during the transaction will be determined by the operating system.

Audit Transactions

The Audit transactions flag controls the logging of transactions to the Log Journal set up on the work with Exit Point Manager System Values panel. This Audit Transaction flag pertains to Object Accesses.

The valid values are:

Y The transaction will be logged to the Log Journal.
N The transaction will not be logged to the Log Journal.
* The default value from a prior rule will control the logging.

Send Messages

The Send messages flag controls the sending of messages to the Log Message Queue set up on the work with Exit Point Manager System Values panel.

This Send Messages flag pertains to Object Accesses.

The valid values are:

Y A log message will be sent to the Log Message Queue.
N A log message will not be sent to the Log Message Queue.
* The default value from a prior rule will control the logging.

Capture Transactions

The Capture transactions flag controls whether transactions are remembered in Exit Point Manager for later memorization. Once captured, transactions can become Memorized Transactions which can act as rules. This Send Messages flag pertains to Object Accesses.

The valid values are:

Y A log message will be sent to the Log Message Queue.
N A log message will not be sent to the Log Message Queue.
* The default value from a prior rule will control the logging.

Switch Profile

The Switch profile holds the name of a user profile whose authority is used to process the transaction instead of the authority of the User initiating the transaction. The transaction is executed as, and uses the authority of, this Switch profile. Switch profile is allowed only when Authority contains *SWITCH or *MEMSWITCH, if *MEMSWITCH is allowed. Otherwise it must contain *NONE. This Switch Profile pertains to Object Accesses.

See Specifying the Server/Functions for an Object Rule.

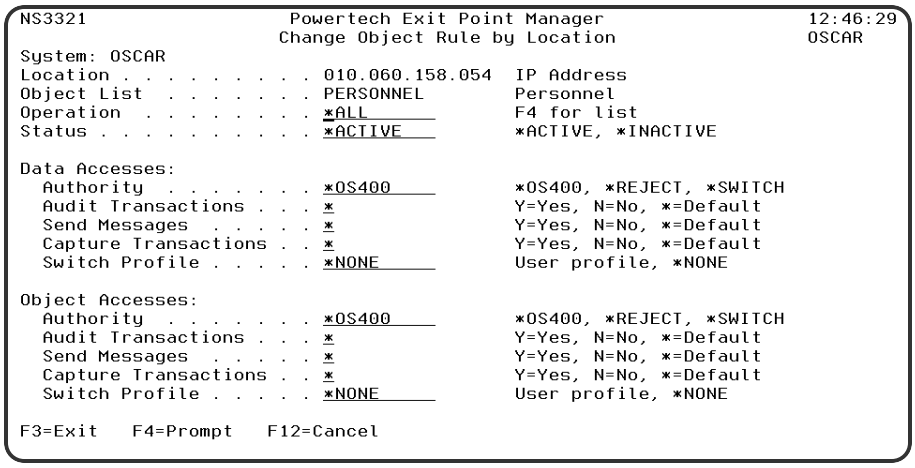
Command Keys

F3 (Exit): Exit the panel without processing any pending changes.

F4 (Prompt): Displays a list of possible values from which you may select one.

F12 (Cancel): Exit the panel without processing any pending changes.

Change Object Rule by Location



How to Get There

From the Exit Point Manager Main Menu, select option **4** to display the Work with Security by Object panel. Select option **1** to display the Work with Object Lists panel, then enter an **9** in the Opt column on one of the Object Lists. On the Object Rules using Object List panel, enter a **2** in the Opt column and a Location. Press `Enter` to display the Change Object Rule by Location panel.

What it Does

The Change Object Rule by Location panel allows you to modify an Object Rule's attributes.

Options

Location

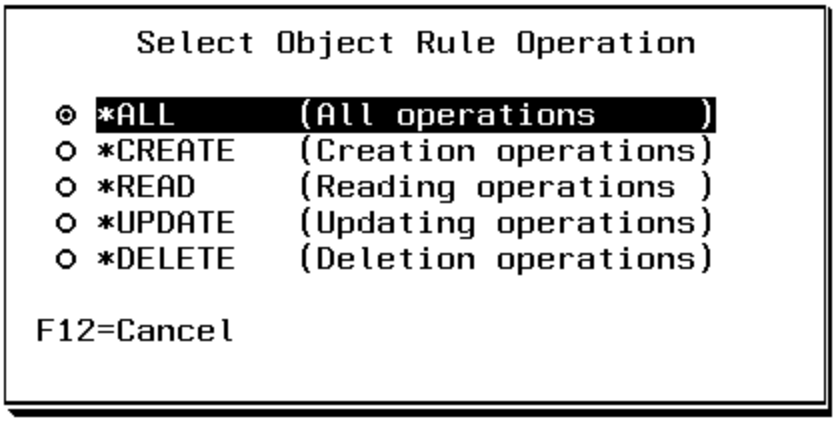
Location represents the source of a transaction. Location can hold an IP Address, an IP Address Group or the name of an SNA Communications Device. The special value *ALL, when used on a rule, means that the rule applies to any rule means that the rule applies to any Location lacking a specific rule. when used as a subset or selection parameter, *ALL generally means to select all such rules for display or printing.

Object List

The Object List name is a short name you assign to a list of objects to help you identify the list. This name is required to be a valid OS name.

Operation

Operation represents the type of action being performed upon an object or upon the data in an object.



Valid values and their meanings are:

*__ALL__ Applies to all of the above types of operations.
*__CREATE__ Applies to objects when they are being created or to their data when they are being added to an object; for example, when writing records to a database.
*__READ__ Applies to non—modifying accesses of objects or the reading of an object's data.
*__UPDATE__ Applies to changes to objects or changes to their data.
*__DELETE__ Applies to deletion of objects or deletion of their data; for example, deleting records from a database file.

Status

Status indicates that an Object Rule is active (being enforced) or inactive (not being enforced).

Data Accesses

Use the data access rights to specify user rights to the data in the objects contained in the Object List.

Authority

Authority represents the action to be taken when a rule is found that matches the data present on a transaction. This Authority value pertains to Data Accesses.

The valid values are:

*__OS400__ The transaction will be allowed and object authority will be determined by the operating system.
*__REJECT__ The transaction will not be allowed.
*__SWITCH__ The transaction will be allowed and the transaction will occur as if the user profile named as the Swap Profile had initiated the transaction. After switching to the Swap Profile, the authority used during the transaction will be determined by the operating system.

Audit Transactions

The Audit transactions flag controls the logging of transactions to the Log Journal set up on the work with Exit Point Manager System Values panel. This Audit Transaction flag pertains to Data Accesses.

The valid values are:

__Y__ The transaction will be logged to the Log Journal.
__N__ The transaction will not be logged to the Log Journal.
* The default value from a prior rule will control the logging.

Send Messages

The Send messages flag controls the sending of messages to the Log Message Queue set up on the Work with Exit Point Manager System Values panel. This Send Messages flag pertains to Data Accesses.

The valid values are:

Y A log message will be sent to the Log Message Queue.
N A log message will not be sent to the Log Message Queue.
* The default value from a prior rule will control the logging.

Capture Transactions

The Capture transactions flag controls whether transactions are remembered in Exit Point Manager for later memorization. Once captured, transactions can become Memorized Transactions which can act as rules. This Capture Transactions flag pertains to Data Accesses.

The valid values are:

Y A log message will be sent to the Log Message Queue.
N A log message will not be sent to the Log Message Queue.
* The default value from a prior rule will control the logging.

Switch Profile

The Switch profile holds the name of a user profile whose authority is used to process the transaction instead of the authority of the User initiating the transaction. The transaction is executed as, and uses the authority of, this Switch profile. Switch profile is allowed only when Authority contains *SWITCH or *MEMSWITCH, if *MEMSWITCH is allowed. Otherwise it must contain *NONE.

This Switch Profile pertains to Data Accesses.

Object Access Rights

Use the object access rights to specify user rights to the objects in the Object List.

Authority

Authority represents the action to be taken when a rule is found that matches the data present on a transaction. This Authority value pertains to Object Accesses.

The valid values are:

***OS400** The transaction will be allowed and object authority will be determined by the operating system.
***REJECT** The transaction will not be allowed.
***SWITCH** The transaction will be allowed and the transaction will occur as if the user profile named as the Swap Profile had initiated the transaction. After switching to the Swap Profile, the authority used during the transaction will be determined by the operating system.

Audit Transactions

The Audit transactions flag controls the logging of transactions to the Log Journal set up on the work with Exit Point Manager System Values panel. This Audit Transaction flag pertains to Object Accesses.

The valid values are:

Y The transaction will be logged to the Log Journal.

N The transaction will not be logged to the Log Journal.
* The default value from a prior rule will control the logging.

Send Messages

The Send messages flag controls the sending of messages to the Log Message Queue set up on the work with Exit Point Manager System Values panel.

This Send Messages flag pertains to Object Accesses.

The valid values are:

Y A log message will be sent to the Log Message Queue.
N A log message will not be sent to the Log Message Queue.
* The default value from a prior rule will control the logging.

Capture Transactions

The Capture transactions flag controls whether transactions are remembered in Exit Point Manager for later memorization. Once captured, transactions can become Memorized Transactions which can act as rules. This Send Messages flag pertains to Object Accesses.

The valid values are:

Y A log message will be sent to the Log Message Queue.
N A log message will not be sent to the Log Message Queue.
* The default value from a prior rule will control the logging.

Switch Profile

The Switch profile holds the name of a user profile whose authority is used to process the transaction instead of the authority of the User initiating the transaction. The transaction is executed as, and uses the authority of, this Switch profile. Switch profile is allowed only when Authority contains *SWITCH or *MEMSWITCH, if *MEMSWITCH is allowed. Otherwise it must contain *NONE. This Switch Profile pertains to Object Accesses.

See Specifying the Server/Functions for an Object Rule.

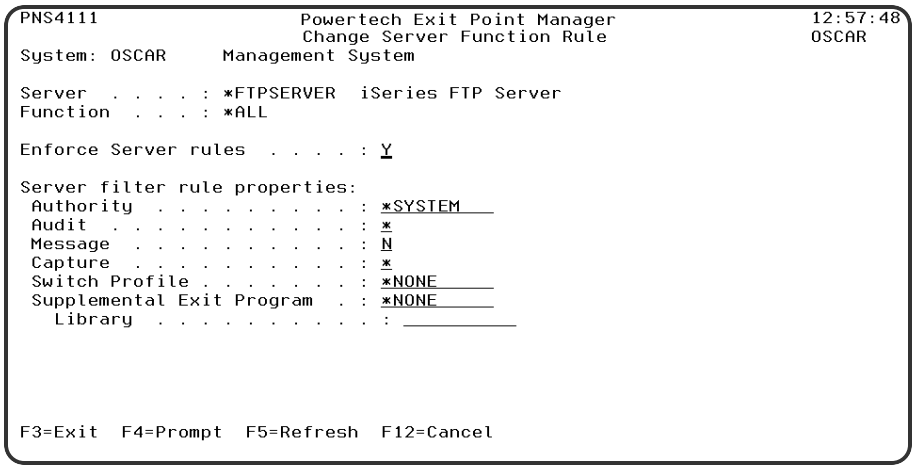
Command Keys

F3 (Exit): Exit the panel without processing any pending changes.

F4 (Prompt): Displays a list of possible values from which you may select one.

F12 (Cancel): Exit the panel without processing any pending changes.

Change Server Function Rule panel



How to Get There

From the Exit Point Manager Main Menu, select option **1**, Work with Security by Server. Under the Options column, type **SP** for a server and press `Enter` to access the Change Server Function Rule panel.

What it Does

The Change Server Function Rule panel allows you to change one or more of the properties for a selected server. To change a server property, type over the existing value and press `Enter`. Server Function Rules provide processing control to Powertech's exit programs and also act as defaults for server function values.

Options

You can enter the following values in the Change Server Function Rule panel. The server name and description display at the top of the window and cannot be changed.

Exit Point Manager rules enforced?

The Powertech rules defined for this server are enforced. (This value is referenced under the "Rules Active" column in the Work with Security by Server panel. This value is referenced under the "Rules Active" column of the Product Configuration panel in the Insite web UI.)

Possible values are:

Y Enter Y to activate the Powertech rules defined for this server.
N Enter N if you don't want to activate the Powertech rules for this server.

Authority

The authority assigned to the server. The value you enter is used when *SERVER authority is placed on a server function.

Possible values are:

***SYSTEM** Use the authority defined for the system.
***OS400** Allow the transaction without taking any action.
***REJECT** Reject all requests for the transaction.

***SWITCH** Switch the job to run as the user profile specified in the switch profile field. A switch profile entry is required.
***MEMOS400** Check Memorized Transactions (MTR) for authority. If no MTR authority is found, allow the transaction.
***MEMREJECT** Check Memorized Transactions (MTR) for authority. If no MTR authority is found, reject requests for the server.
***MEMSWITCH** Check Memorized Transactions (MTR) for authority. If no MTR authority is found, use the authority of the switch profile for the server. A switch profile entry is required.
***MEMOBJ** Check Memorized Transactions (MTR) for authority. If no MTR authority is found, check the transaction against the object rules.

Audit

Controls the type of requests Exit Point Manager will log.

Possible values are:

Y Log all requests to the server.
N Log only authority failures for the server.
* Use the default system value for the system.

Send message on rejected request

Specifies if Exit Point Manager sends a message to the message queue specified in Powertech's System Values.

Possible values are:

Y A message is sent to the specified queue.
N No message is sent.
* Use the default system value for the system.

Capture Transactions

Capture transactions for Memorized Transaction Request (MTR).

Possible values are:

Y Capture transactions.
N Do not capture transactions.
* Use the default system value for the system.

Switch Profile

The name of a switch profile for this server. If you enter a profile name, processing is swapped to run under this profile's authority. This is only valid for authorities *SWITCH and *MEMSWITCH.

Possible values are:

***NONE** No switch profile is being used.

switch-profile The switch profile to process under. It must be an active profile on the IBM i system.

***SYSTEM** Use the switch profile defined for the system.

Supplemental Exit Program

The exit program to run after Powertech's exit program has processed a request successfully. The supplemental exit program is called only for authorities *OS400, *MEMOS400, *SWITCH, and

*MEMSWITCH if the transaction has not been rejected by Exit Point Manager rules. Exit Point Manager's rules must be enforced for a supplemental exit program to run.

Possible values are:

***NONE** No supplemental exit program is to run.

exit-program-name The name of the supplemental exit program to run after Powertech's exit program completes normally. It must be a valid object name and exist on the IBM i system.

Library

Enter the name of the library where the supplemental exit program is found. It must be a valid object name and exist on the IBM i system.

Command Keys

F3 (Exit): Exit the program without processing any pending changes.

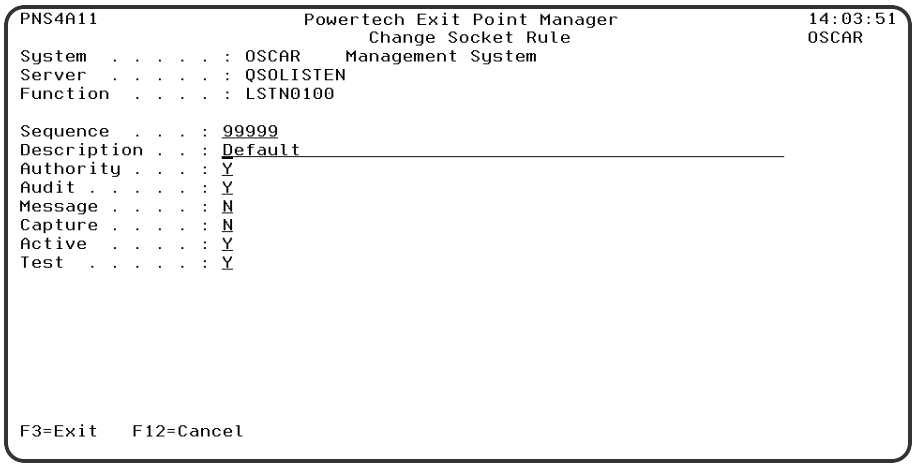
F4 (Prompt): Displays a list of values from which you may select one.

F5 (Refresh): Refreshes the panel and resets all available text fields.

F12 (Cancel): Exit the panel without processing any pending changes.

Change Socket Rule panel

WARNING: Misuse of Socket Rules can render your system unreachable via TCP. Exercise extreme caution when using this feature. Consider adding Socket Rules as not active and testing them using the Socket Rule test feature, and setting them to be not used by that feature and testing the rule set before removing them. If you render your system unreachable via TCP, you will need to access the system via the console in order to fix the rules (or to deactivate the Socket Rule servers).



How to Get There

On the Work with Socket Rules panel, choose option **1**, **2**, or **3**. Then choose option **2**.

What it Does

The Change Socket Rule panel allows you to modify a Socket Rule's attributes.

Field Descriptions

System
System indicates the target of any operations you perform. When you add rules, for example, those rules will be sent to, and will affect processing on, the System named.

Server
A Server in Exit Point Manager is a controlled entry point into your system. These entry points are determined and defined by IBM. Exit Point Manager has assigned easy-to-remember names to these controlled entry points.

Function
A Function, or Server Function, in Exit Point Manager represents a class of operations that a given Server may perform. For example, the *SIGNON Server classifies its operations as those pertaining to changing passwords, generating authentication tokens, and retrieving signon information. Exit Point Manager has assigned easy-to-remember names to these Functions, such as CHGPWD, GENAUTTKN and RETRIEVE.

Sequence
The sequence number of a Socket Rule determines the order in which it will be evaluated by the exit program, with the lowest sequence number being evaluated first. Socket Rules are evaluated until a match is found.

Description
The Socket Rule description is a short textual description of the Socket Rule. It is typically used to indicate the purpose of the Socket Rule.

Authority
Authority represents the action to be taken when a rule is found that matches the data present on a transaction.

The valid values are:

Y Exit Point Manager will allow requests when this rule is enforced.
N Exit Point Manager will reject requests when this rule is enforced.
* Uses the value found in the rule above this one in the rule hierarchy when this rule is enforced.

The value * will cause the rule to inherit the value from the default Socket Rule (sequence number 99999). This default rule may not be set to the value *.

Audit
The Audit transactions flag controls the logging of transactions to the Log Journal set up on the Work with Exit Point Manager System Values panel.

The valid values are:

* Uses the value found in the rule above this one in the rule hierarchy.
Y Logs all requests when this rule is enforced.
N Logs only access failures (rejects) for this rule.

The value * will cause the rule to inherit the value from the default Socket Rule (sequence number 99999). This default rule may not be set to the value *.

Message

The Send messages flag controls the sending of messages to the Log Message Queue set up on the Work with Exit Point Manager System Values panel.

The valid values are:

* Uses the value found in the rule above this one in the rule hierarchy.
Y Sends a message when this rule is enforced.
N Does not send a message when this rule is enforced.

The value * will cause the rule to inherit the value from the default Socket Rule (sequence number 99999). This default rule may not be set to the value *.

Capture

The Capture transactions flag controls whether transactions are remembered in Exit Point Manager. Unlike some other rule types, a captured Socket Rule cannot be memorized.

The valid values are:

* Uses the value found in the rule above this one in the rule hierarchy.
Y Captures the transaction when this rule is enforced.
N Does not capture the transaction when this rule is enforced.

The value * will cause the rule to inherit the value from the default Socket Rule (sequence number 99999). This default rule may not be set to the value *.

Active

The Socket Rule Active flag determines whether the rule will be evaluated by the exit point program.

It can be useful to initially set a Socket Rule as not active in order to test it without enforcing it.

The valid values are:

Y Exit Point Manager will evaluate the rule.
N Exit Point Manager will not evaluate the rule.

The value N is not allowed for the default Socket Rule (sequence number 99999).

Test

The Socket Rule Test flag determines whether the rule will be evaluated by the Socket Rule test facility.

It can be useful to flag a rule to not be tested in order to verify the effects of removing that rule.

The value N is not allowed for the default Socket Rule (sequence number 99999).

The valid values are:

Y The Socket Rule test facility will evaluate the rule.
N The Socket Rule test facility will not evaluate the rule.

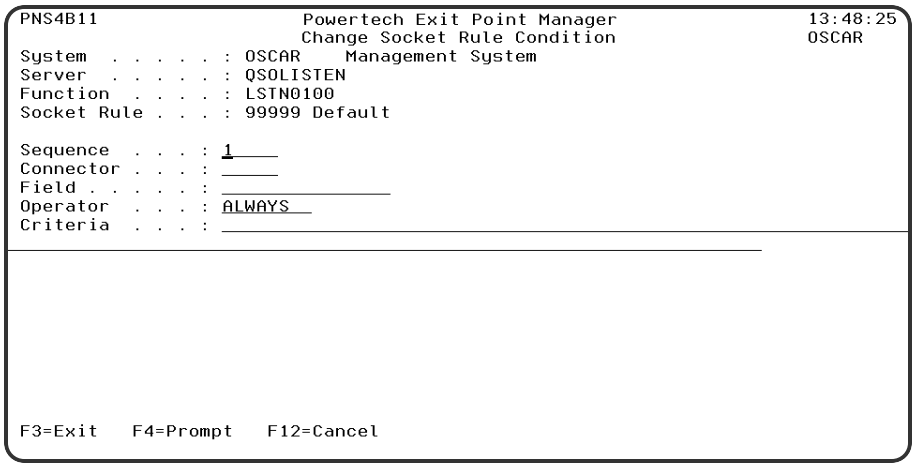
Command Keys

F3 (Exit): Exit the panel without processing any pending changes.

F12 (Cancel): Exit the panel without processing any pending changes.

Change Socket Rule Condition panel

WARNING: Misuse of Socket Rules can render your system unreachable via TCP. Exercise extreme caution when using this feature. Consider adding Socket Rules as not active and testing them using the Socket Rule test feature, and setting them to be not used by that feature and testing the rule set before removing them. If you render your system unreachable via TCP, you will need to access the system via the console in order to fix the rules (or to deactivate the Socket Rule servers).



How to Get There

On the Work with Socket Conditions panel, choose **2** for a condition.

What it Does

The Change Socket Condition panel allows you to modify the attributes of a Socket Condition.

Field Descriptions

System

System indicates the target of any operations you perform. When you add rules, for example, those rules will be sent to, and will affect processing on, the System named.

Server

A Server in Exit Point Manager is a controlled entry point into your system. These entry points are determined and defined by IBM. Exit Point Manager has assigned easy-to-remember names to these controlled entry points.

Function

A Function, or Server Function, in Exit Point Manager represents a class of operations that a given Server may perform. For example, the *SIGNON Server classifies its operations as those pertaining to changing passwords, generating authentication tokens, and retrieving signon information. Exit Point Manager has assigned easy-to-remember names to these Functions, such as CHGPWD, GENAUTTKN and RETRIEVE.

Socket Rule

The Socket Rule to which this Socket Condition belongs. A Socket Rule without a Socket Condition, or with an invalid Socket Condition, will not be enforced.

Sequence

The sequence number of a Socket Condition determines the order in which it is combined with other Socket Conditions for a Socket Rule.

Connector

The connector determines how a Socket Condition relates to other Socket Conditions for a Socket Rule.

Socket Conditions with a higher order of precedence are evaluated before ones with a lower order of precedence.

The connector for the Socket Condition with the lowest sequence number is ignored.

> **EXAMPLE:**
> Given three Socket Conditions:
>
> ```
> Seq = 10 Connector = <ignored> evaluates to False
> Seq = 20 Connector = AND evaluates to True
> Seq = 30 Connector = OR evaluates to True
> ```
>
> This will return True as it is equivalent to:
> (False AND True) OR True
> If the OR were evaluated first then it would return False as it would be equivalent to:
> False AND (True OR True)

The valid values are:

OR This Socket Condition is OR'ed with others. An OR has the lowest order of precedence (evaluated last).

AND This Socket Condition is AND'ed with others. An AND has a higher order of precedence than an OR, but lower than an ORAND.

ORAND This Socket Condition is OR'ed with others. An ORAND has the highest order of precedence (evaluated first).

Field

This is the name of the field to be evaluated at run time.

The valid values are dependent on the Socket Rule.

Valid values for the QSOLISTEN server are:

LCL_PORT The local port number; an integer between 1 and 65535.
LCL_USR The user profile associated with the job issuing the listen.
LCL_USR_GRP A User Group containing the user profile associated with the job issuing the listen.

Valid values for the QSOCONNECT server are:

LCL_PORT The local port number; an integer between 1 and 65535.

RMT_PORT The remote port number; an integer between 1 and 65535.
RMT_ADDR The remote address. Valid formats are IPv4, IPv6, and Powertech Exit Point Manager ip address groups.
LCL_USR The user profile associated with the job issuing the connect.
LCL_USR_GRP A User Group containing the user profile associated with the job issuing the connect.

Valid values for the QSOACCEPT server are:

LCL_IN_PORT The local incoming port number; an integer between 1 and 65535.
LCL_BND_PORT The local bound port number; an integer between 1 and 65535.
RMT_PORT The remote port number; an integer between 1 and 65535.
RMT_ADDR The remote address. Valid formats are IPv4, IPv6, and Powertech Exit Point Manager ip address groups.
LCL_USR The user profile associated with the job issuing the accept.
LCL_USR_GRP A User Group containing the user profile associated with the job issuing the accept.

Operator

The test used for the value of the field and the criteria to evaluate this Socket Condition.

= The value of the field is equal to the criteria, or, if the criteria can be a list, the value of the field is found in that list.
<> The value of the field is not equal to the criteria, or, if the criteria can be a list, the value of the field is not found in that list.
> The value of the field is greater than the criteria.
< The value of the field is less than the criteria.
>= The value of the field is greater than or equal to the criteria.
<= The value of the field is less than or equal to the criteria.

ALWAYS

This will cause the condition to always match. It is used on the Socket Condition of the default Socket Rule, and may be used on non-default Socket Rules.

If present, it must be the only Socket Condition for a Socket Rule.

Criteria

This is the value against which the value of the selected field will be compared at run time.

The valid values are dependent on the selected Field.

Command Keys

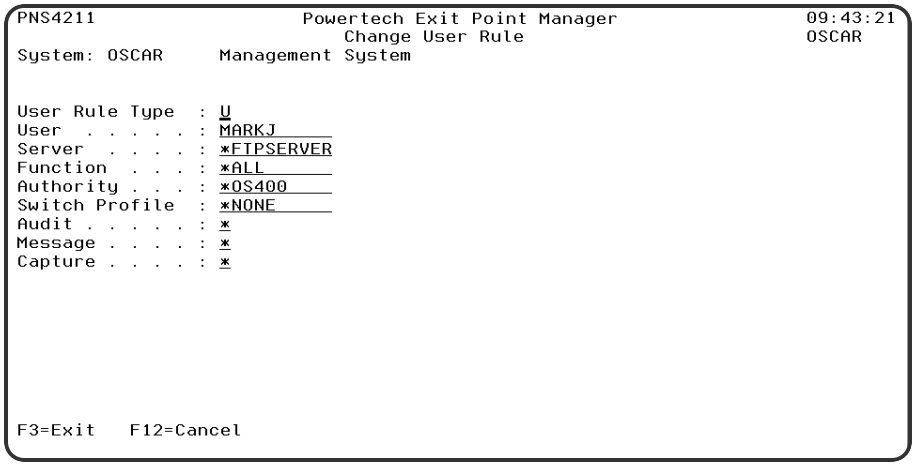
F3 (Exit): Exit the panel without processing any pending changes.

F4 (Prompt): Displays a list of items from which one or more may be selected.

F5 (Refresh): Refreshes the panel with the most current data.

F12 (Cancel): Exit the panel without processing any pending changes.

Change User Rule panel



How to Get There

On the Work with Security by User panel, choose **2** for a User Rule.

What it Does

The Change User Rule panel allows you to modify a User Rule's attributes.

Field Descriptions

System

System indicates the target of any operations you perform. When you add rules, for example, those rules will be sent to, and will affect processing on, the System named.

User Type

This field is used to indicate whether the associated User field refers to an O/S user profile or a Exit Point Manager User Group.

Valid values are:

U The associated User field refers to an O/S user profile.
G The associated User field refers to a Exit Point Manager user group.

User

If the associated User Type is a 'U', User represents the identity of the person initiating a transaction as a user profile.

The special value *PUBLIC, when used on a rule, means that the rule applies to any User lacking a specific rule. When used as a subset or selection parameter, *PUBLIC means to select all such rules for display or printing.

If the associated User Type is a 'G', User represents a Exit Point Manager User Group.

Server

A Server in Exit Point Manager is a controlled entry point into your system. These entry points are determined and defined by IBM. Exit Point Manager has assigned easy-to-remember names to these

controlled entry points.

Function

A Function, or Server Function, in Exit Point Manager represents a class of operations that a given Server may perform. For example, the *SIGNON Server classifies its operations as those pertaining to changing passwords, generating authentication tokens, and retrieving signon information. Exit Point Manager has assigned easy-to-remember names to these Functions, such as CHGPWD, GENAUTTKN and RETRIEVE.

Authority Property

The authority assigned to the user for this server/function. If authority is left blank, Exit Point Manager will remove the user's entry.

Possible values are:

***OS400** Exit Point Manager will use normal OS/400 authority for the user.
***REJECT** Exit Point Manager will reject requests for the specified user.
***SWITCH** Exit Point Manager will use the authority of the switch profile for the specified user. A switch profile entry is required.
***MEMREJECT** Check Memorized Transactions (MTR) for authority. If no MTR authority is encountered, Exit Point Manager will reject requests for the specified user.
***MEMOS4OO** Check Memorized Transactions (MTR) for authority. If no MTR authority is encountered, Exit Point Manager will use normal OS/400 authority for the location. This is valid for both location and user.
***MEMSWITCH** Check Memorized Transactions (MTR) for authority. If no MTR authority is encountered, Exit Point Manager will use the authority of the switch profile for the specified user. A switch profile entry is required.
***SRVFCN** Exit Point Manager will use the authority defined for the server/function.
Switch The Switch profile holds the name of a user profile whose authority is used to process the transaction instead of the authority of the User initiating the transaction. The transaction is executed as, and uses the authority of, this Switch profile.

Switch profile is allowed only when Authority contains *SWITCH or *MEMSWITCH, if *MEMSWITCH is allowed. Otherwise it must contain *NONE.

Aud

The Audit transactions flag controls the logging of transactions to the Log Journal set up on the Work with Exit Point Manager System Values panel.

The valid values are:

* Uses the value found in the rule above this one in the rule hierarchy.
Y Logs all requests when this rule is enforced.
N Logs only access failures (rejects) for this rule.

Msg

The Send messages flag controls the sending of messages to the Log Message Queue set up on the Work with Exit Point Manager System Values panel.

The valid values are:

* Uses the value found in the rule above this one in the rule hierarchy.
Y Sends a message when this rule is enforced.
N Does not send a message when this rule is enforced.

Capture

The Capture transactions flag controls whether transactions are remembered in Exit Point Manager for later memorization. Once captured, transactions can become Memorized Transactions which can act as rules.

The valid values are:

* Uses the value found in the rule above this one in the rule hierarchy.
Y Captures the transaction when this rule is enforced.
N Does not capture the transaction when this rule is enforced.

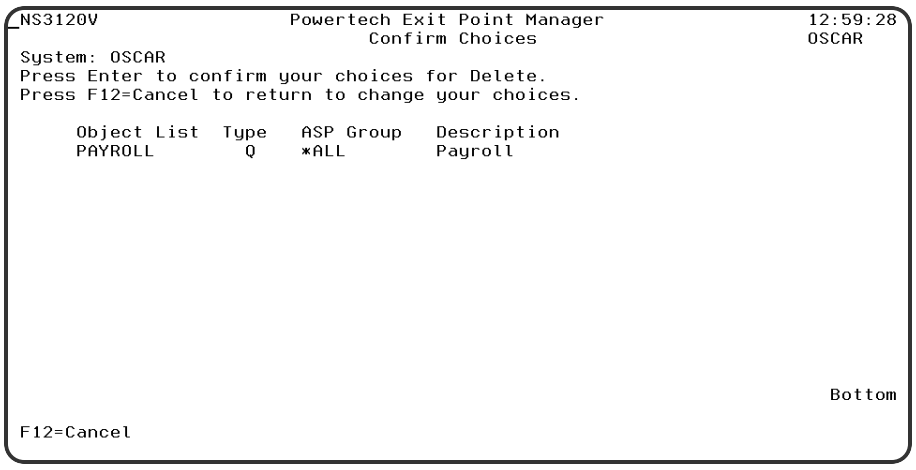
Command Keys

F3 (Exit): Exit the panel without processing any pending changes.

F4 (Prompt): Displays a list of possible values from which you may select one.

F12 (Cancel): Exit the panel without processing any pending changes.

Confirm Choices



How to Get There

Variations of this panel appear, depending on the option chosen, whenever Exit Point Manager prompts you to confirm your choice.

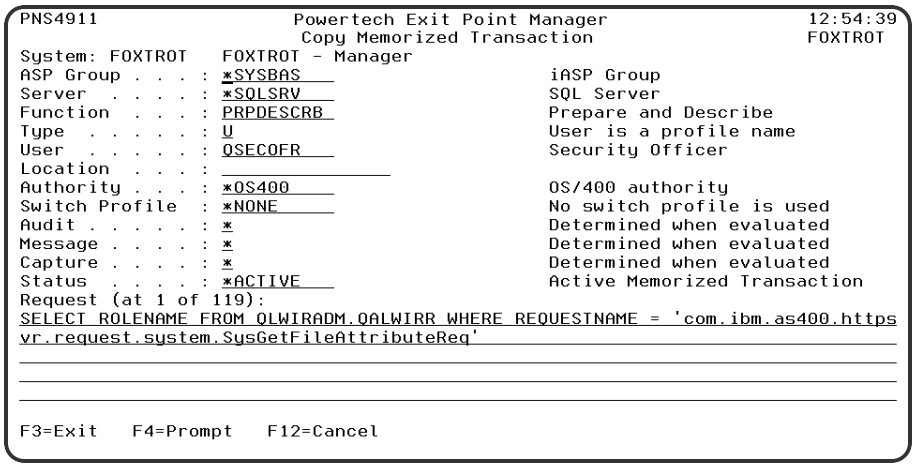
What it Does

The Confirm Choices panel asks you to confirm that you intend to delete the listed items. Press `Enter` to confirm your choices for Delete, or press `F12` to return to change your choices.

Command Keys

F12 (Cancel): Exit the panel without processing any pending changes.

Copy Memorized Transaction



How to Get There

From the Exit Point Manager Main Menu, select option **11**. On the Work with Memorized Transactions panel, choose option **3** for a Memorized Transaction and press `Enter`.

What it Does

The Copy a Memorized Transaction enables you to copy a memorized transaction.

Options

Server

A Server in Exit Point Manager is a controlled entry point into your system. These entry points are determined and defined by IBM. Exit Point Manager has assigned easy-to-remember names to these controlled entry points.

Function

A Function, or Server Function, in Exit Point Manager represents a class of operations that a given Server may perform. For example, the *SIGNON Server classifies its operations as those pertaining to changing passwords, generating authentication tokens, and retrieving sign-on information. Exit Point Manager has assigned easy-to-remember names to these Functions, such as CHGPWD, GENAUTTKN and RETRIEVE.

Type

This field is used to indicate whether the associated User field refers to an O/S user profile or a Exit Point Manager User Group.

Valid values are:

U The associated User field refers to an O/S user profile.
G The associated User field refers to a Exit Point Manager user group.

User

User represents the identity of the person initiating a transaction as a user profile. The special value *PUBLIC, when used on a rule, means that the rule applies to any User lacking a specific rule. When

used as a subset or selection parameter, *PUBLIC means to select all such rules for display or printing. Specify the name of the User for the memorized transaction. You can create a memorized transaction that applies to all Users by specifying the special value *PUBLIC. You can press F4 to see a list of valid values that can be specified.

Location

Location represents the source of a transaction. Location can hold an IP Address, an IP Address Group or the name of an SNA Communications Device. The special value *ALL, when used on a rule, means that the rule applies to any rule means that the rule applies to any Location lacking a specific rule. when used as a subset or selection parameter, *ALL generally means to select all such rules for display or printing. Specify the Location for the memorized transaction. You can create a memorized transaction that applies to all Locations by specifying the special value *ALL.

Authority

Authority represents the action to be taken when a rule is found that matches the data present on a transaction.

Specify the Authority value for the new memorized transaction. You can press F4 to see a list of valid values that can be specified.

The list of valid values may include one or more of these values:

*__USER__ Current user authority is used.
*__0S400__ Exit Point Manager will use normal operating system authority for the user.
*__REJECT__ Exit Point Manager will reject requests.
*__SWITCH__ Exit Point Manager will use the authority of the switch profile for the transaction. A switch profile entry is required.
*__MEMUSR__ Memorized Transactions (MTR) are checked for authority first. If no MTR authority is encountered, Exit Point Manager will use the authority of the current user.
*__MEMOS400__ Memorized Transactions (MTR) are checked for authority first. If no MTR authority is encountered, Exit Point Manager will use normal operating system authority for the user.
*__MEMREJECT__ Memorized Transactions (MTR) are checked for authority first. If no MTR authority is encountered, Exit Point Manager will reject requests for the specified user.
*__MEMSWITCH__ Memorized Transactions (MTR) are checked for authority first. If no MTR authority is encountered, Exit Point Manager will use the authority of the switch profile for the specified user. A switch profile entry is required.
*__MEMOBJ__ Memorized Transactions (MTR) are checked for authority first. If no MTR authority is encountered, Exit Point Manager will check any objects used in the transactions for authorities defined by Object Rules.
*__SERVER__ Exit Point Manager will use the authority defined for the Server.
*__SRVFCN__ Exit Point Manager will use the authority defined for the Server Function.

Audit transactions

The Audit transactions flag controls the logging of transactions to the Log Journal set up on the work with Exit Point Manager System Values panel.

Specify one of these values for Audit transactions:

*__DEFAULT__ Uses the value found in the rule above this one in the rule hierarchy.
*__YES__ Logs all requests when this rule is enforced.
*__NO__ Logs only access failures (rejects) for this rule.

Send messages

The Send messages flag controls the sending of messages to the Log Message Queue set up on the work with Exit Point Manager System Values panel.

Specify one of these values for Send messages:

***DEFAULT** Uses the value found in the rule above this one in the rule hierarchy.
***YES** Sends a message when this rule is enforced.
***NO** Does not send a message when this rule is enforced.

Capture transactions

The Capture transactions flag controls whether transactions are remembered in Exit Point Manager for later memorization. Once captured, transactions can become Memorized Transactions which can act as rules.

Specify one of these values for Capture transactions:

***DEFAULT** Uses the value found in the rule above this one in the rule hierarchy.
***YES** Captures the transaction when this rule is enforced.
***NO** Does not capture the transaction when this rule is enforced.

Switch profile

The Switch profile holds the name of a user profile whose authority is used to process the transaction instead of the authority of the User initiating the transaction. The transaction is executed as, and uses the authority of, this Switch profile. Switch profile is allowed only when Authority contains *SWITCH or *MEMSWITCH, if *MEMSWITCH is allowed. Otherwise it must contain *NONE.

Specify the new Switch profile value or one of these special values:

***NONE** No Switch profile is to be used. This is the only value allowed unless you have specified *SWITCH or *MEMSWITCH for Authority.
***SRVFCN** Use the Switch profile specified for the Server Function.

Status

This is the status of the Memorized Transaction.

Possible values are:

***ACTIVE** Exit Point Manager will attempt to match this transaction during rule enforcement. Memorized Transactions that are changed to *ACTIVE will have a matching User or Location rule changed to the corresponding action; *ALLOW to *MEMOS400, *REJECT to *MEMREJECT, or *SWITCH to *MEMSWITCH.
***INACTIVE**Exit Point Manager will not attempt to match this transaction during rule enforcement. Memorized Transactions that are changed to *INACTIVE will have the matching User or Location rule changed (if there are no other Memorized Transactions for that rule) to the corresponding action; *MEMOS400 to *ALLOW, *MEMREJECT to *REJECT, or *MEMSWITCH to *SWITCH.

Transaction

The Memorized Transaction against which incoming transactions are tested. If a match is found, then this rule will be invoked. Undisplayable characters in the transaction data are replaced by the mid—dot character (-).

You can use the Transaction wildcard character (%) to make a Transaction generic. The wildcard character is valid only at the end of a Transaction string. when you are memorizing or changing a Memorized Transaction, the first occurrence of the wildcard character that was NOT present in the string before you changed it will make the string generic and all data after that wildcard character will be discarded.

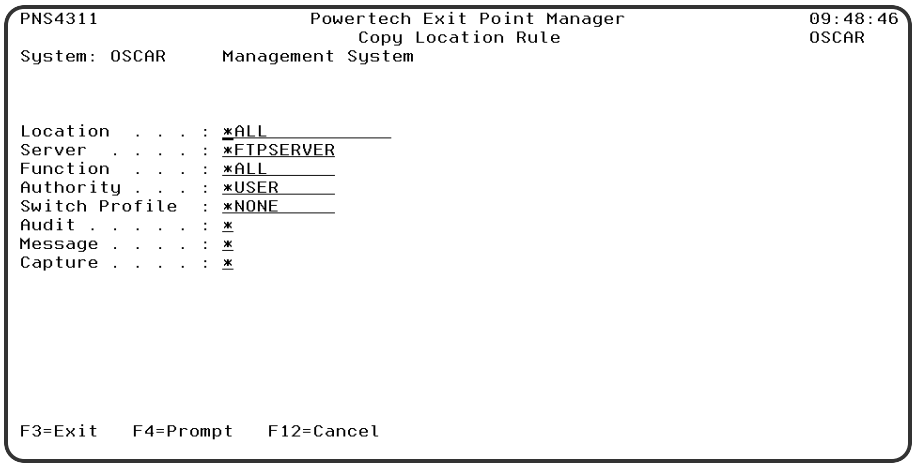
Command Keys

F3 (Exit): Exit the panel without processing any pending changes.

F4 (Prompt): Displays a list of possible values from which you may select one.

F12 (Cancel): Exit the panel without processing any pending changes.

Copy Location Rule panel



How to Get There

On the Work with Security by Location panel, choose **3** for a Location Rule.

What it Does

The Copy Location Rule panel allows you to copy a Location Rule to a new Location.

Field Descriptions

System

System indicates the target of any operations you perform. When you add rules, for example, those rules will be sent to, and will affect processing on, the System named.

Location

Location represents the source of a transaction. Location can hold an IP Address, an IP Address Group or the name of an SNA Communications Device.

The special value *ALL, when used on a rule, means that the rule applies to any Location lacking a specific rule. When used as a subset or selection parameter, *ALL generally means to select all such rules for display or printing.

Server

A Server in Exit Point Manager is a controlled entry point into your system. These entry points are determined and defined by IBM. Exit Point Manager has assigned easy-to-remember names to these controlled entry points.

Function

A Function, or Server Function, in Exit Point Manager represents a class of operations that a given Server may perform. For example, the *SIGNON Server classifies its operations as those pertaining to changing passwords, generating authentication tokens, and retrieving signon information. Exit Point Manager has assigned easy-to-remember names to these Functions, such as CHGPWD, GENAUTTKN and RETRIEVE.

Authority Property

The authority assigned to the user for this server/function. If authority is left blank, Exit Point Manager will remove the user's entry.

Possible values are:

***OS400** Exit Point Manager will use normal OS/400 authority for the user.
***REJECT** Exit Point Manager will reject requests for the specified user.
***SWITCH** Exit Point Manager will use the authority of the switch profile for the specified user. A switch profile entry is required.
***MEMREJECT** Check Memorized Transactions (MTR) for authority. If no MTR authority is encountered, Exit Point Manager will reject requests for the specified user.
***MEMOS4OO** Check Memorized Transactions (MTR) for authority. If no MTR authority is encountered, Exit Point Manager will use normal OS/400 authority for the location. This is valid for both location and user.
***MEMSWITCH** Check Memorized Transactions (MTR) for authority. If no MTR authority is encountered, Exit Point Manager will use the authority of the switch profile for the specified user. A switch profile entry is required.
***SRVFCN** Exit Point Manager will use the authority defined for the server/function.
Switch The Switch profile holds the name of a user profile whose authority is used to process the transaction instead of the authority of the User initiating the transaction. The transaction is executed as, and uses the authority of, this Switch profile.

Switch profile is allowed only when Authority contains *SWITCH or *MEMSWITCH, if *MEMSWITCH is allowed. Otherwise it must contain *NONE.

Aud

The Audit transactions flag controls the logging of transactions to the Log Journal set up on the Work with Exit Point Manager System Values panel.

The valid values are:

* Uses the value found in the rule above this one in the rule hierarchy.
Y Logs all requests when this rule is enforced.
N Logs only access failures (rejects) for this rule.

Msg

The Send messages flag controls the sending of messages to the Log Message Queue set up on the Work with Exit Point Manager System Values panel.

The valid values are:

* Uses the value found in the rule above this one in the rule hierarchy.
Y Sends a message when this rule is enforced.
N Does not send a message when this rule is enforced.

Capture

The Capture transactions flag controls whether transactions are remembered in Exit Point Manager for later memorization. Once captured, transactions can become Memorized Transactions which can act as rules.

The valid values are:

* Uses the value found in the rule above this one in the rule hierarchy.
Y Captures the transaction when this rule is enforced.
N Does not capture the transaction when this rule is enforced.

Command Keys

F3 (Exit): Exit the panel without processing any pending changes.

F4 (Prompt): Displays a list of possible values from which you may select one.

F12 (Cancel): Exit the panel without processing any pending changes.

Copy User Group

```
PNS4711                    Powertech Exit Point Manager                  14:56:13
                                Copy User Group                          OSCAR
System: OSCAR     Management System


Sequence Number  . . .    2
User Group     . . . . SUPPORT
Description  . . . . . Support user group

New Sequence Number  . _____
New User Group     . . __________
New Description  . . . ________________________________________________________




F3=Exit   F12=Cancel
```

How to Get There

From the Exit Point Manager Main Menu, select option **7**, Work with User Groups, then choose **3** for a Group.

What it Does

The Copy User Group panel allows you to copy a User Group to a new name. No entries currently in the User Group being copied will be copied to the new User Group as a user profile can only be in one User Group.

Field Descriptions

System
System indicates the target of any operations you perform. When you add rules, for example, those rules will be sent to, and will affect processing on, the System named.

Sequence Number
The sequence number that determines the order in which User Groups are evaluated by the exit point programs.

User Group
The User Group name is a short name you assign to a group of user profiles to help you identify the group.

This name is required to be a valid OS name.

Description
The User Group description is a short textual description of the User Group. It is typically used to indicate the purpose or contents of the User Group.

New Sequence Number
The sequence number that determines the order in which User Groups are evaluated by the exit point programs.

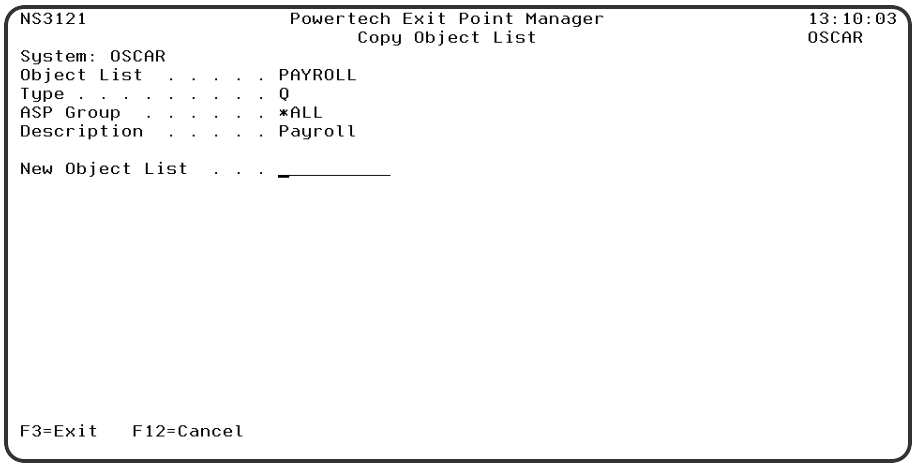
New User Group
The new name for the User Group.

New User Group Description
The new description for the User Group.

Command Keys
F3=Exit: Exit the current panel without processing any pending changes.

F12=Cancel: Exit the current panel without processing any pending changes.

Copy Object List



How to Get There

From the Exit Point Manager Main Menu, select option **4** to display the Work with Security by Object panel. Select option **1** to display the Work with Object Lists panel, then enter a **3** in the Opt column on one of the Object Lists.

What it Does

The Copy Object List panel allows you to copy an Object List to a new name. All entries currently in the Object List being copied will be copied to the new Object List.

Field Descriptions

Object List

The Object List name is a short name you assign to a list of objects to help you identify the list. This name is required to be a valid OS name.

Type

The Object List type determines what type of entries can be added to an Object List. Object lists can hold native object specifications (library, object and type) or paths to IFS objects.

Valid values are:

Q The Object List entries are native object specifiers.
I The Object List entries are paths to IFS objects.

Description

The Object List description is a short textual description of the Object List. It is typically used to indicate the purpose or contents of the Object List.

New Object List

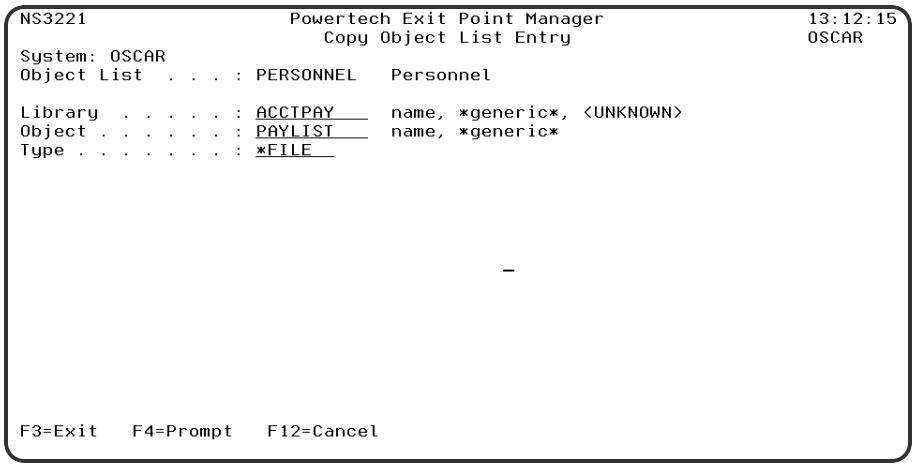
Specify the new name for the Object List.

Command Keys

F3 (Exit): Exit the panel without processing any pending changes.

F12 (Cancel): Exit the panel without processing any pending changes.

Copy Object List Entry



How to Get There

From the Exit Point Manager Main Menu, select option **4** to display the Work with Security by Object panel. Select option **1** to display the Work with Object Lists panel, then enter an **8** in the Opt column on one of the Object Lists. In the Work with Object List Entries panel, enter **3** in the Opt column for one of the libraries.

What it Does

The Copy Object List Entry panel allows you to copy an Object List Entry to a new entry.

Options

Library

The Library is the name of the library in which an object exists. This name is required to be a valid OS name. You can use the Generic Character (*) to indicate that a partial value is to be used for selection. In some circumstances you may also use the wildcard Character (?) to indicate that a partial value is to be used for selection. You may specify <UNKNOWN> to indicate that the Object List Entry library name. Circumstances arise when an unqualified object reference cannot be resolved to the actual object on the system, so the library name cannot be determined. Exit Point Manager allows you to make Object Rules to cover these circumstances by specifying the <UNKNOWN> special value for the library portion of an Object List Entry.

Object

Object is the name of an object in a library. This name is required to be a valid OS name.

Type

Object Type is the type of an object in a library.

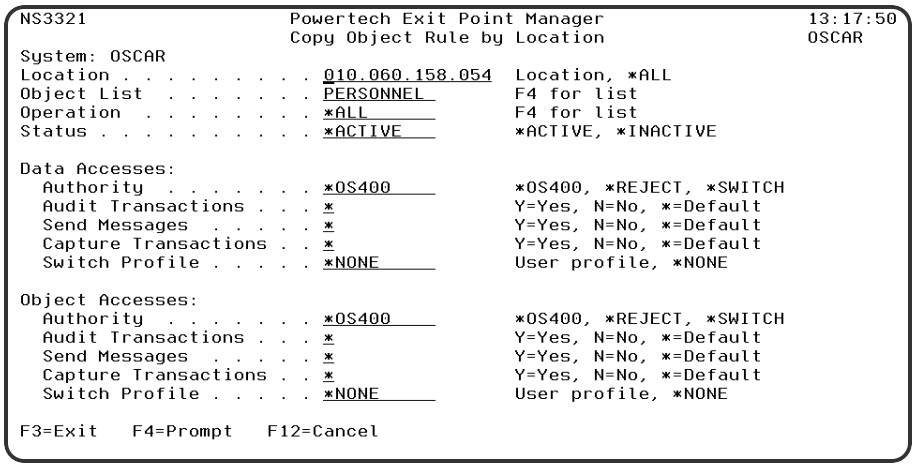
Command Keys

F3 (Exit): Exit the panel without processing any pending changes.

F4 (Prompt): Displays a list of possible values from which you may select one.

F12 (Cancel): Exit the panel without processing any pending changes.

Copy Object Rule by Location



How to Get There

From the Exit Point Manager Main Menu, select option **4** to display the Work with Security by Object panel. Select option **1** to display the Work with Object Lists panel, then enter an **9** in the Opt column on one of the Object Lists. On the Object Rules using Object List panel, enter a **3** in the Opt column and a Location. Press `Enter` to display the Copy Object Rule by Location panel.

What it Does

The Copy Object Rule by Location panel allows you to create a new Object Rule using an existing rule as the basis for the new rule.

Options

Location

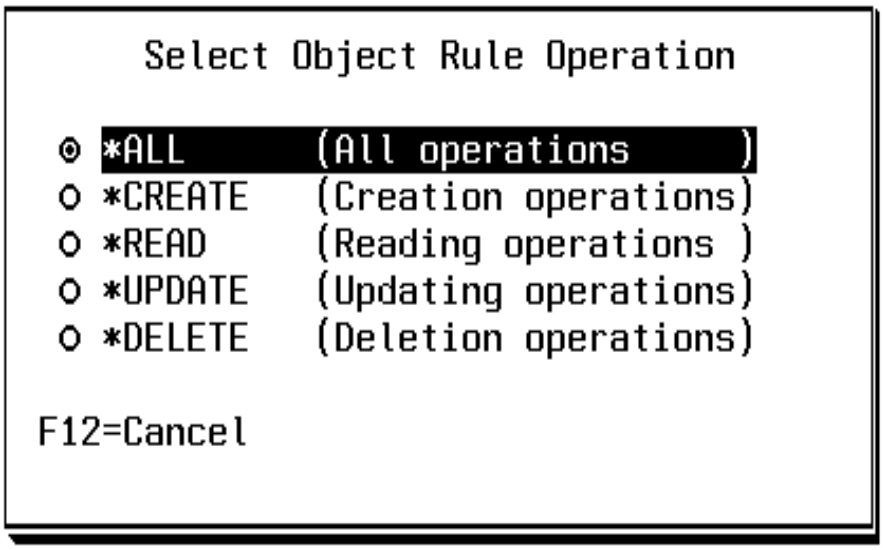
Location represents the source of a transaction. Location can hold an IP Address, an IP Address Group or the name of an SNA Communications Device. The special value *ALL, when used on a rule, means that the rule applies to any rule means that the rule applies to any Location lacking a specific rule. when used as a subset or selection parameter, *ALL generally means to select all such rules for display or printing.

Object List

The Object List name is a short name you assign to a list of objects to help you identify the list. This name is required to be a valid OS name.

Operation

Operation represents the type of action being performed upon an object or upon the data in an object.



Valid values and their meanings are:

*__ALL__ Applies to all of the above types of operations.
*__CREATE__ Applies to objects when they are being created or to their data when they are being added to an object; for example, when writing records to a database.
*__READ__ Applies to non—modifying accesses of objects or the reading of an object's data.
*__UPDATE__ Applies to changes to objects or changes to their data.
*__DELETE__ Applies to deletion of objects or deletion of their data; for example, deleting records from a database file.

Status

Status indicates that an Object Rule is active (being enforced) or inactive (not being enforced).

Data Accesses

Use the data access rights to specify user rights to the data in the objects contained in the Object List.

Authority

Authority represents the action to be taken when a rule is found that matches the data present on a transaction. This Authority value pertains to Data Accesses.

The valid values are:

*__OS400__ The transaction will be allowed and object authority will be determined by the operating system.
*__REJECT__ The transaction will not be allowed.
*__SWITCH__ The transaction will be allowed and the transaction will occur as if the user profile named as the Swap Profile had initiated the transaction. After switching to the Swap Profile, the authority used during the transaction will be determined by the operating system.

Audit Transactions

The Audit transactions flag controls the logging of transactions to the Log Journal set up on the work with Exit Point Manager System Values panel. This Audit Transaction flag pertains to Data Accesses.

The valid values are:

Y The transaction will be logged to the Log Journal.
N The transaction will not be logged to the Log Journal.
* The default value from a prior rule will control the logging.

Send Messages

The Send messages flag controls the sending of messages to the Log Message Queue set up on the Work with Exit Point Manager System Values panel. This Send Messages flag pertains to Data Accesses.

The valid values are:

Y A log message will be sent to the Log Message Queue.
N A log message will not be sent to the Log Message Queue.
* The default value from a prior rule will control the logging.

Capture Transactions

The Capture transactions flag controls whether transactions are remembered in Exit Point Manager for later memorization. Once captured, transactions can become Memorized Transactions which can act as rules. This Capture Transactions flag pertains to Data Accesses.

The valid values are:

Y A log message will be sent to the Log Message Queue.
N A log message will not be sent to the Log Message Queue.
* The default value from a prior rule will control the logging.

Switch Profile

The Switch profile holds the name of a user profile whose authority is used to process the transaction instead of the authority of the User initiating the transaction. The transaction is executed as, and uses the authority of, this Switch profile. Switch profile is allowed only when Authority contains *SWITCH or *MEMSWITCH, if *MEMSWITCH is allowed. Otherwise it must contain *NONE.

This Switch Profile pertains to Data Accesses.

Object Access Rights

Use the object access rights to specify user rights to the objects in the Object List.

Authority

Authority represents the action to be taken when a rule is found that matches the data present on a transaction. This Authority value pertains to Object Accesses.

The valid values are:

***OS400** The transaction will be allowed and object authority will be determined by the operating system.
***REJECT** The transaction will not be allowed.
***SWITCH** The transaction will be allowed and the transaction will occur as if the user profile named as the Swap Profile had initiated the transaction. After switching to the Swap Profile, the authority used during the transaction will be determined by the operating system.

Audit Transactions

The Audit transactions flag controls the logging of transactions to the Log Journal set up on the work with Exit Point Manager System Values panel. This Audit Transaction flag pertains to Object Accesses.

The valid values are:

Y The transaction will be logged to the Log Journal.
N The transaction will not be logged to the Log Journal.
* The default value from a prior rule will control the logging.

Send Messages

The Send messages flag controls the sending of messages to the Log Message Queue set up on the work with Exit Point Manager System Values panel.

This Send Messages flag pertains to Object Accesses.

The valid values are:

Y A log message will be sent to the Log Message Queue.
N A log message will not be sent to the Log Message Queue.
* The default value from a prior rule will control the logging.

Capture Transactions

The Capture transactions flag controls whether transactions are remembered in Exit Point Manager for later memorization. Once captured, transactions can become Memorized Transactions which can act as rules. This Send Messages flag pertains to Object Accesses.

The valid values are:

Y A log message will be sent to the Log Message Queue.
N A log message will not be sent to the Log Message Queue.
* The default value from a prior rule will control the logging.

Switch Profile

The Switch profile holds the name of a user profile whose authority is used to process the transaction instead of the authority of the User initiating the transaction. The transaction is executed as, and uses the authority of, this Switch profile. Switch profile is allowed only when Authority contains *SWITCH or *MEMSWITCH, if *MEMSWITCH is allowed. Otherwise it must contain *NONE. This Switch Profile pertains to Object Accesses.

See Specifying the Server/Functions for an Object Rule.

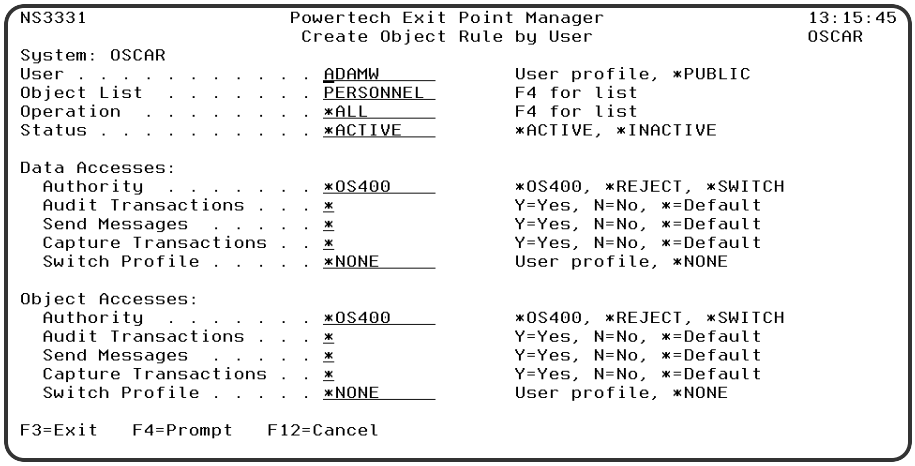
Command Keys

F3 (Exit): Exit the panel without processing any pending changes.

F4 (Prompt): Displays a list of possible values from which you may select one.

F12 (Cancel): Exit the panel without processing any pending changes.

Copy Object Rule by User



How to Get There

From the Exit Point Manager Main Menu, select option **4** to display the Work with Security by Object panel. Select option **1** to display the Work with Object Lists panel, then enter an **9** in the Opt column on one of the Object Lists. On the Object Rules using Object List panel, enter a **3** in the Opt column and a User. Press `Enter` to display the Copy Object Rule by User panel.

What it Does

The Copy Object Rule by User panel allows you to create a new Object Rule using an existing rule as the basis for the new rule.

Options

User

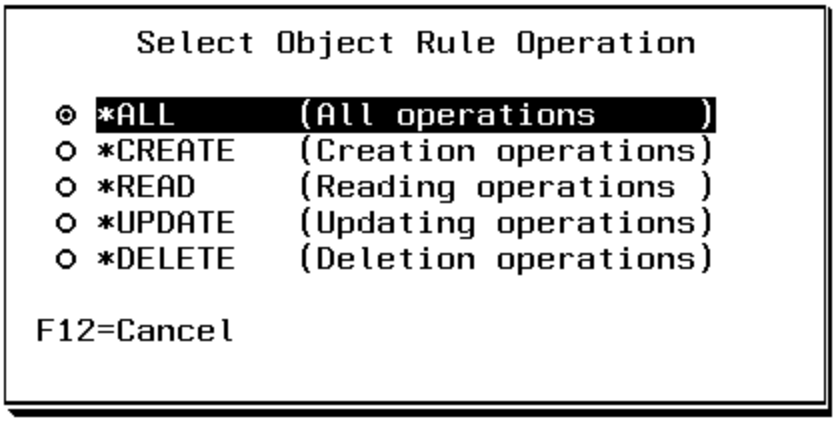
User represents the identity of the person initiating a transaction as a user profile. The special value *PUBLIC, when used on a rule, means that the rule applies to any User lacking a specific rule. when used as a subset or selection parameter, *PUBLIC means to select all such rules for display or printing.

Object List

The Object List name is a short name you assign to a list of objects to help you identify the list. This name is required to be a valid OS name.

Operation

Operation represents the type of action being performed upon an object or upon the data in an object.



Valid values and their meanings are:

*__ALL__ Applies to all of the above types of operations.
*__CREATE__ Applies to objects when they are being created or to their data when they are being added to an object; for example, when writing records to a database.
*__READ__ Applies to non—modifying accesses of objects or the reading of an object's data.
*__UPDATE__ Applies to changes to objects or changes to their data.
*__DELETE__ Applies to deletion of objects or deletion of their data; for example, deleting records from a database file.

Status

Status indicates that an Object Rule is active (being enforced) or inactive (not being enforced).

Data Accesses

Use the data access rights to specify user rights to the data in the objects contained in the Object List.

Authority

Authority represents the action to be taken when a rule is found that matches the data present on a transaction. This Authority value pertains to Data Accesses.

The valid values are:

*__OS400__ The transaction will be allowed and object authority will be determined by the operating system.
*__REJECT__ The transaction will not be allowed.
*__SWITCH__ The transaction will be allowed and the transaction will occur as if the user profile named as the Swap Profile had initiated the transaction. After switching to the Swap Profile, the authority used during the transaction will be determined by the operating system.

Audit Transactions

The Audit transactions flag controls the logging of transactions to the Log Journal set up on the work with Exit Point Manager System Values panel. This Audit Transaction flag pertains to Data Accesses.

The valid values are:

__Y__ The transaction will be logged to the Log Journal.
__N__ The transaction will not be logged to the Log Journal.
* The default value from a prior rule will control the logging.

Send Messages

The Send messages flag controls the sending of messages to the Log Message Queue set up on the Work with Exit Point Manager System Values panel. This Send Messages flag pertains to Data Accesses.

The valid values are:

Y A log message will be sent to the Log Message Queue.
N A log message will not be sent to the Log Message Queue.
* The default value from a prior rule will control the logging.

Capture Transactions

The Capture transactions flag controls whether transactions are remembered in Exit Point Manager for later memorization. Once captured, transactions can become Memorized Transactions which can act as rules. This Capture Transactions flag pertains to Data Accesses.

The valid values are:

Y A log message will be sent to the Log Message Queue.
N A log message will not be sent to the Log Message Queue.
* The default value from a prior rule will control the logging.

Switch Profile

The Switch profile holds the name of a user profile whose authority is used to process the transaction instead of the authority of the User initiating the transaction. The transaction is executed as, and uses the authority of, this Switch profile. Switch profile is allowed only when Authority contains *SWITCH or *MEMSWITCH, if *MEMSWITCH is allowed. Otherwise it must contain *NONE.

This Switch Profile pertains to Data Accesses.

Object Access Rights

Use the object access rights to specify user rights to the objects in the Object List.

Authority

Authority represents the action to be taken when a rule is found that matches the data present on a transaction. This Authority value pertains to Object Accesses.

The valid values are:

***OS400** The transaction will be allowed and object authority will be determined by the operating system.
***REJECT** The transaction will not be allowed.
***SWITCH** The transaction will be allowed and the transaction will occur as if the user profile named as the Swap Profile had initiated the transaction. After switching to the Swap Profile, the authority used during the transaction will be determined by the operating system.

Audit Transactions

The Audit transactions flag controls the logging of transactions to the Log Journal set up on the work with Exit Point Manager System Values panel. This Audit Transaction flag pertains to Object Accesses.

The valid values are:

Y The transaction will be logged to the Log Journal.

N The transaction will not be logged to the Log Journal.
* The default value from a prior rule will control the logging.

Send Messages

The Send messages flag controls the sending of messages to the Log Message Queue set up on the work with Exit Point Manager System Values panel.

This Send Messages flag pertains to Object Accesses.

The valid values are:

Y A log message will be sent to the Log Message Queue.
N A log message will not be sent to the Log Message Queue.
* The default value from a prior rule will control the logging.

Capture Transactions

The Capture transactions flag controls whether transactions are remembered in Exit Point Manager for later memorization. Once captured, transactions can become Memorized Transactions which can act as rules. This Send Messages flag pertains to Object Accesses.

The valid values are:

Y A log message will be sent to the Log Message Queue.
N A log message will not be sent to the Log Message Queue.
* The default value from a prior rule will control the logging.

Switch Profile

The Switch profile holds the name of a user profile whose authority is used to process the transaction instead of the authority of the User initiating the transaction. The transaction is executed as, and uses the authority of, this Switch profile. Switch profile is allowed only when Authority contains *SWITCH or *MEMSWITCH, if *MEMSWITCH is allowed. Otherwise it must contain *NONE. This Switch Profile pertains to Object Accesses.

See Specifying the Server/Functions for an Object Rule.

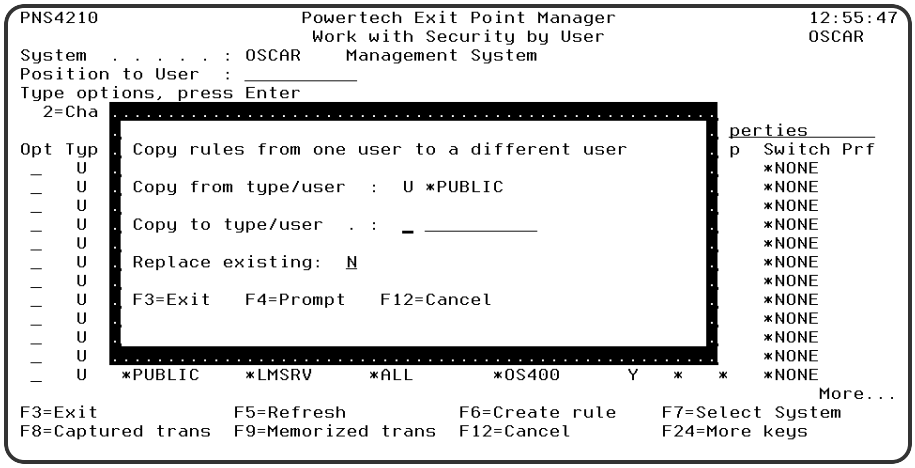
Command Keys

F3 (Exit): Exit the panel without processing any pending changes.

F4 (Prompt): Displays a list of possible values from which you may select one.

F12 (Cancel): Exit the panel without processing any pending changes.

Copy Rules from One User to a Different User window



How to Get There

On the Work with Security by User panel, choose `F10`.

What it Does

This window supports copying user rules from one user to another.

Field Descriptions

Copy from type/user

This field lists the user or User Group being copied from.

Copy to type/user • Replace Existing

If the target user is a user profile, enter a 'U' in the type field. If the target user is a User Group, enter an 'G' in the type field. The target user profile, or User Group, must exist for the rules to be copied.

Any existing rules for the target user, specified in the 'Copy to' field, may be replaced by selecting 'Y' for 'Replace existing'.

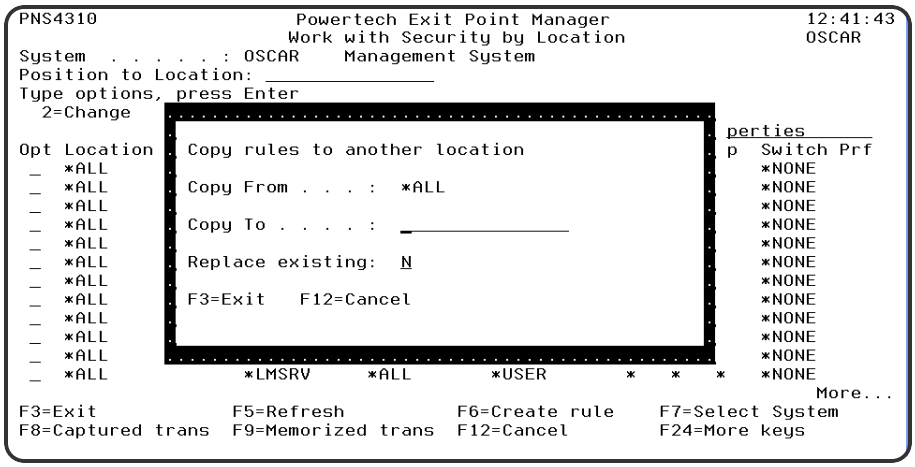
Command Keys

F3 (Exit): Exit the window without processing any pending changes.

F4 (Prompt): Will prompt for user profiles unless a 'G' is entered in the type field, in which case it will prompt for User Groups.

F12 (Cancel): Exit the window without processing any pending changes.

Copy Rules to Another Location window



How to Get There

On the Work with Security by Location panel, choose `F10`.

What it Does

This window supports copying location rules from one location to another.

Field Descriptions

Copy From

This field lists the location being copied from.

Copy To • Replace Existing

Any existing rules for the target location, specified in the 'Copy to' field, may be replaced by selecting 'Y' for 'Replace existing'.

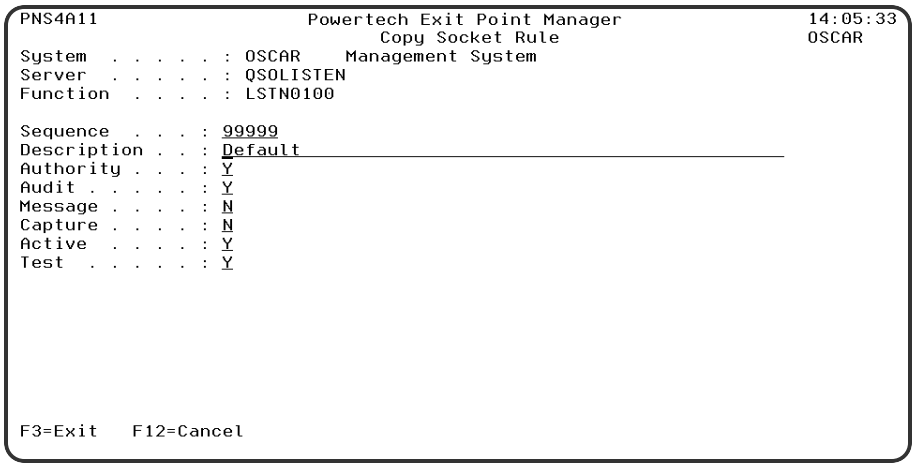
Command Keys

F3 (Exit): Exit the window without processing any pending changes.

F12 (Cancel): Exit the window without processing any pending changes.

Copy Socket Rule panel

WARNING: Misuse of Socket Rules can render your system unreachable via TCP. Exercise extreme caution when using this feature. Consider adding Socket Rules as not active and testing them using the Socket Rule test feature, and setting them to be not used by that feature and testing the rule set before removing them. If you render your system unreachable via TCP, you will need to access the system via the console in order to fix the rules (or to deactivate the Socket Rule servers).



How to Get There

On the Work with Socket Rules panel, choose option **1**, **2**, or **3**. Then choose option **3**.

What it Does

The Copy Socket Rule panel allows you to copy a Socket Rule.

Field Descriptions

System

System indicates the target of any operations you perform. When you add rules, for example, those rules will be sent to, and will affect processing on, the System named.

Server

A Server in Exit Point Manager is a controlled entry point into your system. These entry points are determined and defined by IBM. Exit Point Manager has assigned easy-to-remember names to these controlled entry points.

Function

A Function, or Server Function, in Exit Point Manager represents a class of operations that a given Server may perform. For example, the *SIGNON Server classifies its operations as those pertaining to changing passwords, generating authentication tokens, and retrieving signon information. Exit Point Manager has assigned easy-to-remember names to these Functions, such as CHGPWD, GENAUTTKN and RETRIEVE.

Sequence

The sequence number of a Socket Rule determines the order in which it will be evaluated by the exit program, with the lowest sequence number being evaluated first. Socket Rules are evaluated until a match is found.

Description

The Socket Rule description is a short textual description of the Socket Rule. It is typically used to indicate the purpose of the Socket Rule.

Authority

Authority represents the action to be taken when a rule is found that matches the data present on a transaction.

The valid values are:

Y Exit Point Manager will allow requests when this rule is enforced.
N Exit Point Manager will reject requests when this rule is enforced.
* Uses the value found in the rule above this one in the rule hierarchy when this rule is enforced.

The value * will cause the rule to inherit the value from the default Socket Rule (sequence number 99999). This default rule may not be set to the value *.

Audit

The Audit transactions flag controls the logging of transactions to the Log Journal set up on the Work with Exit Point Manager System Values panel.

The valid values are:

* Uses the value found in the rule above this one in the rule hierarchy.
Y Logs all requests when this rule is enforced.
N Logs only access failures (rejects) for this rule.

The value * will cause the rule to inherit the value from the default Socket Rule (sequence number 99999). This default rule may not be set to the value *.

Message

The Send messages flag controls the sending of messages to the Log Message Queue set up on the Work with Exit Point Manager System Values panel.

The valid values are:

* Uses the value found in the rule above this one in the rule hierarchy.
Y Sends a message when this rule is enforced.
N Does not send a message when this rule is enforced.

The value * will cause the rule to inherit the value from the default Socket Rule (sequence number 99999). This default rule may not be set to the value *.

Capture

The Capture transactions flag controls whether transactions are remembered in Exit Point Manager. Unlike some other rule types, a captured Socket Rule cannot be memorized.

The valid values are:

* Uses the value found in the rule above this one in the rule hierarchy.
Y Captures the transaction when this rule is enforced.
N Does not capture the transaction when this rule is enforced.

The value * will cause the rule to inherit the value from the default Socket Rule (sequence number 99999). This default rule may not be set to the value *.

Active

The Socket Rule Active flag determines whether the rule will be evaluated by the exit point program.

It can be useful to initially set a Socket Rule as not active in order to test it without enforcing it.

The valid values are:

Y Exit Point Manager will evaluate the rule.
N Exit Point Manager will not evaluate the rule.

The value N is not allowed for the default Socket Rule (sequence number 99999).

Test

The Socket Rule Test flag determines whether the rule will be evaluated by the Socket Rule test facility.

It can be useful to flag a rule to not be tested in order to verify the effects of removing that rule.

The value N is not allowed for the default Socket Rule (sequence number 99999).

The valid values are:

Y The Socket Rule test facility will evaluate the rule.
N The Socket Rule test facility will not evaluate the rule.

Command Keys

F3 (Exit): Exit the panel without processing any pending changes.

F12 (Cancel): Exit the panel without processing any pending changes.

Copy User Rule panel

```
PNS4211                  Powertech Exit Point Manager                16:35:07
                               Copy User Rule                        OSCAR
System: OSCAR     Management System


User Rule Type  : U
User  . . . . . : MARKJ
Server  . . . . : *FIPSERVER
Function  . . . : DELETEFILE
Authority . . . : *OS400
Switch Profile  : *NONE
Audit . . . . . : *
Message . . . . : *
Capture . . . . : Y









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

How to Get There

On the Work with Security by User panel, choose **3** for a User Rule.

What it Does

The Copy User Rule panel allows you to copy a User Rule to a new User.

Field Descriptions

System
System indicates the target of any operations you perform. When you add rules, for example, those rules will be sent to, and will affect processing on, the System named.

User Type
This field is used to indicate whether the associated User field refers to an O/S user profile or a Exit Point Manager User Group.

Valid values are:

U The associated User field refers to an O/S user profile.
G The associated User field refers to a Exit Point Manager user group.

User
If the associated User Type is a 'U', User represents the identity of the person initiating a transaction as a user profile.

The special value *PUBLIC, when used on a rule, means that the rule applies to any User lacking a specific rule. When used as a subset or selection parameter, *PUBLIC means to select all such rules for display or printing.

If the associated User Type is a 'G', User represents a Exit Point Manager User Group.

Server
A Server in Exit Point Manager is a controlled entry point into your system. These entry points are determined and defined by IBM. Exit Point Manager has assigned easy-to-remember names to these controlled entry points.

Function
A Function, or Server Function, in Exit Point Manager represents a class of operations that a given Server may perform. For example, the *SIGNON Server classifies its operations as those pertaining to changing passwords, generating authentication tokens, and retrieving signon information. Exit Point Manager has assigned easy-to-remember names to these Functions, such as CHGPWD, GENAUTTKN and RETRIEVE.

Authority Property
The authority assigned to the user for this server/function. If authority is left blank, Exit Point Manager will remove the user's entry.

Possible values are:

***OS400** Exit Point Manager will use normal OS/400 authority for the user.
***REJECT** Exit Point Manager will reject requests for the specified user.
***SWITCH** Exit Point Manager will use the authority of the switch profile for the specified user. A switch profile entry is required.
***MEMREJECT** Check Memorized Transactions (MTR) for authority. If no MTR authority is encountered, Exit Point Manager will reject requests for the specified user.
***MEMOS4OO** Check Memorized Transactions (MTR) for authority. If no MTR authority is encountered, Exit Point Manager will use normal OS/400 authority for the location. This is valid for both location and user.

***MEMSWITCH** Check Memorized Transactions (MTR) for authority. If no MTR authority is encountered, Exit Point Manager will use the authority of the switch profile for the specified user. A switch profile entry is required.
***SRVFCN** Exit Point Manager will use the authority defined for the server/function.
Switch The Switch profile holds the name of a user profile whose authority is used to process the transaction instead of the authority of the User initiating the transaction. The transaction is executed as, and uses the authority of, this Switch profile.

Switch profile is allowed only when Authority contains *SWITCH or *MEMSWITCH, if *MEMSWITCH is allowed. Otherwise it must contain *NONE.

Aud

The Audit transactions flag controls the logging of transactions to the Log Journal set up on the Work with Exit Point Manager System Values panel.

The valid values are:

* Uses the value found in the rule above this one in the rule hierarchy.
Y Logs all requests when this rule is enforced.
N Logs only access failures (rejects) for this rule.

Msg

The Send messages flag controls the sending of messages to the Log Message Queue set up on the Work with Exit Point Manager System Values panel.

The valid values are:

* Uses the value found in the rule above this one in the rule hierarchy.
Y Sends a message when this rule is enforced.
N Does not send a message when this rule is enforced.

Capture

The Capture transactions flag controls whether transactions are remembered in Exit Point Manager for later memorization. Once captured, transactions can become Memorized Transactions which can act as rules.

The valid values are:

* Uses the value found in the rule above this one in the rule hierarchy.
Y Captures the transaction when this rule is enforced.
N Does not capture the transaction when this rule is enforced.

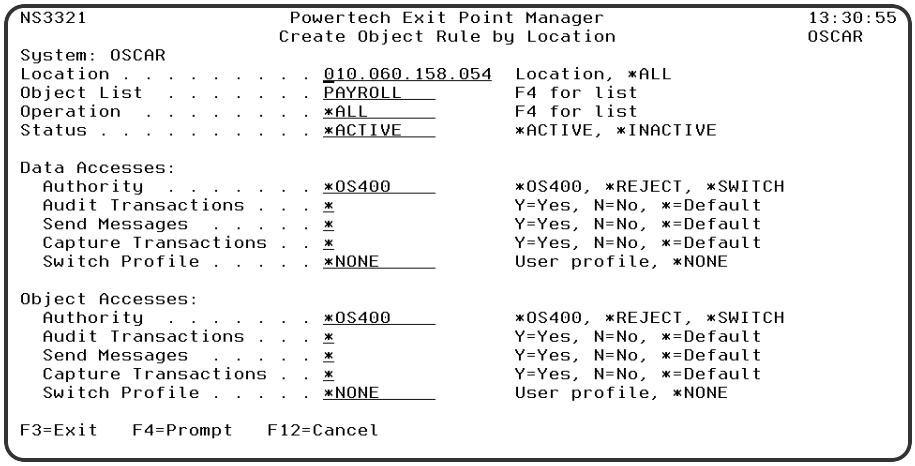
Command Keys

F3 (Exit): Exit the panel without processing any pending changes.

F4 (Prompt): Displays a list of possible values from which you may select one.

F12 (Cancel): Exit the panel without processing any pending changes.

Create Object Rule by Location



How to Get There

From the Exit Point Manager Main Menu, select option **4** to display the Work with Security by Object panel. Select option **1** to display the Work with Object Lists panel, then enter an **9** in the Opt column on one of the Object Lists. On the Object Rules using Object List panel, enter a **1** in the Opt column and a Location. Press `Enter` to display the Create Object Rule by Location panel.

What it Does

The Create Object Rule by Location panel allows you to create an Object Rule linking a Location to an Object List.

Options

Location

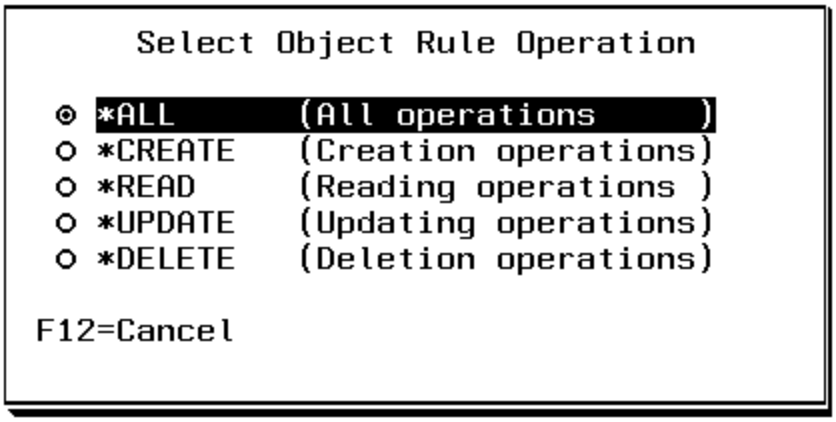
Location represents the source of a transaction. Location can hold an IP Address, an IP Address Group or the name of an SNA Communications Device. The special value *ALL, when used on a rule, means that the rule applies to any rule means that the rule applies to any Location lacking a specific rule. when used as a subset or selection parameter, *ALL generally means to select all such rules for display or printing.

Object List

The Object List name is a short name you assign to a list of objects to help you identify the list. This name is required to be a valid OS name.

Operation

Operation represents the type of action being performed upon an object or upon the data in an object.



Valid values and their meanings are:

*__ALL__ Applies to all of the above types of operations.
*__CREATE__ Applies to objects when they are being created or to their data when they are being added to an object; for example, when writing records to a database.
*__READ__ Applies to non—modifying accesses of objects or the reading of an object's data.
*__UPDATE__ Applies to changes to objects or changes to their data.
*__DELETE__ Applies to deletion of objects or deletion of their data; for example, deleting records from a database file.

Status

Status indicates that an Object Rule is active (being enforced) or inactive (not being enforced).

Data Accesses

Use the data access rights to specify user rights to the data in the objects contained in the Object List.

Authority

Authority represents the action to be taken when a rule is found that matches the data present on a transaction. This Authority value pertains to Data Accesses.

The valid values are:

*__OS400__ The transaction will be allowed and object authority will be determined by the operating system.
*__REJECT__ The transaction will not be allowed.
*__SWITCH__ The transaction will be allowed and the transaction will occur as if the user profile named as the Swap Profile had initiated the transaction. After switching to the Swap Profile, the authority used during the transaction will be determined by the operating system.

Audit Transactions

The Audit transactions flag controls the logging of transactions to the Log Journal set up on the work with Exit Point Manager System Values panel. This Audit Transaction flag pertains to Data Accesses.

The valid values are:

__Y__ The transaction will be logged to the Log Journal.
__N__ The transaction will not be logged to the Log Journal.
* The default value from a prior rule will control the logging.

Send Messages

The Send messages flag controls the sending of messages to the Log Message Queue set up on the Work with Exit Point Manager System Values panel. This Send Messages flag pertains to Data Accesses.

The valid values are:

Y A log message will be sent to the Log Message Queue.
N A log message will not be sent to the Log Message Queue.
* The default value from a prior rule will control the logging.

Capture Transactions

The Capture transactions flag controls whether transactions are remembered in Exit Point Manager for later memorization. Once captured, transactions can become Memorized Transactions which can act as rules. This Capture Transactions flag pertains to Data Accesses.

The valid values are:

Y A log message will be sent to the Log Message Queue.
N A log message will not be sent to the Log Message Queue.
* The default value from a prior rule will control the logging.

Switch Profile

The Switch profile holds the name of a user profile whose authority is used to process the transaction instead of the authority of the User initiating the transaction. The transaction is executed as, and uses the authority of, this Switch profile. Switch profile is allowed only when Authority contains *SWITCH or *MEMSWITCH, if *MEMSWITCH is allowed. Otherwise it must contain *NONE.

This Switch Profile pertains to Data Accesses.

Object Access Rights

Use the object access rights to specify user rights to the objects in the Object List.

Authority

Authority represents the action to be taken when a rule is found that matches the data present on a transaction. This Authority value pertains to Object Accesses.

The valid values are:

***OS400** The transaction will be allowed and object authority will be determined by the operating system.
***REJECT** The transaction will not be allowed.
***SWITCH** The transaction will be allowed and the transaction will occur as if the user profile named as the Swap Profile had initiated the transaction. After switching to the Swap Profile, the authority used during the transaction will be determined by the operating system.

Audit Transactions

The Audit transactions flag controls the logging of transactions to the Log Journal set up on the work with Exit Point Manager System Values panel. This Audit Transaction flag pertains to Object Accesses.

The valid values are:

Y The transaction will be logged to the Log Journal.

N The transaction will not be logged to the Log Journal.
* The default value from a prior rule will control the logging.

Send Messages

The Send messages flag controls the sending of messages to the Log Message Queue set up on the work with Exit Point Manager System Values panel.

This Send Messages flag pertains to Object Accesses.

The valid values are:

Y A log message will be sent to the Log Message Queue.
N A log message will not be sent to the Log Message Queue.
* The default value from a prior rule will control the logging.

Capture Transactions

The Capture transactions flag controls whether transactions are remembered in Exit Point Manager for later memorization. Once captured, transactions can become Memorized Transactions which can act as rules. This Send Messages flag pertains to Object Accesses.

The valid values are:

Y A log message will be sent to the Log Message Queue.
N A log message will not be sent to the Log Message Queue.
* The default value from a prior rule will control the logging.

Switch Profile

The Switch profile holds the name of a user profile whose authority is used to process the transaction instead of the authority of the User initiating the transaction. The transaction is executed as, and uses the authority of, this Switch profile. Switch profile is allowed only when Authority contains *SWITCH or *MEMSWITCH, if *MEMSWITCH is allowed. Otherwise it must contain *NONE. This Switch Profile pertains to Object Accesses.

See Specifying the Server/Functions for an Object Rule.

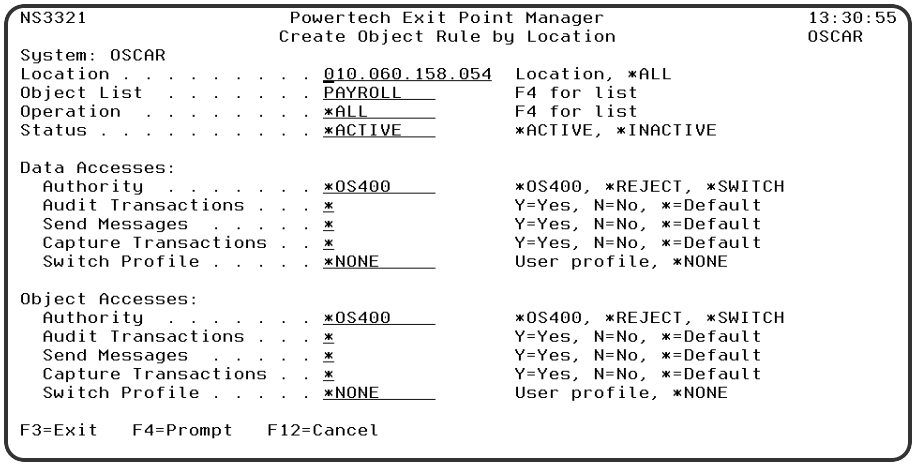
Command Keys

F3 (Exit): Exit the panel without processing any pending changes.

F4 (Prompt): Displays a list of possible values from which you may select one.

F12 (Cancel): Exit the panel without processing any pending changes.

Create Object Rule by Location



How to Get There

From the Exit Point Manager Main Menu, select option **4** to display the Work with Security by Object panel. Select option **1** to display the Work with Object Lists panel, then enter an **9** in the Opt column on one of the Object Lists. On the Object Rules using Object List panel, enter a **1** in the Opt column and a Location. Press `Enter` to display the Create Object Rule by Location panel.

What it Does

The Create Object Rule by Location panel allows you to create an Object Rule linking a Location to an Object List.

Options

Location

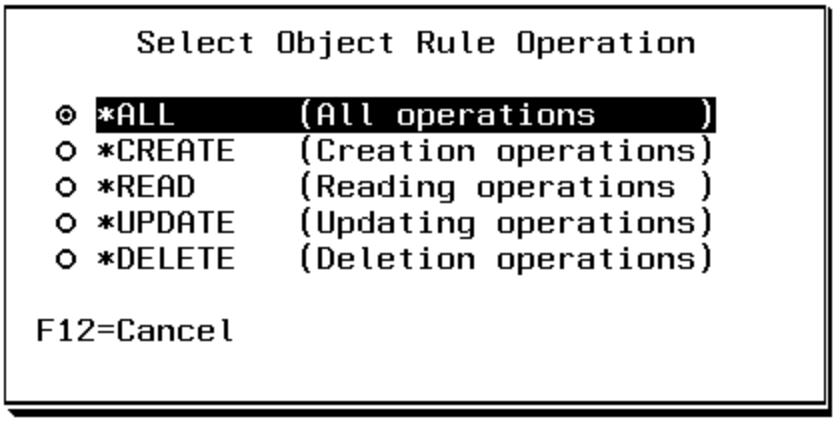
Location represents the source of a transaction. Location can hold an IP Address, an IP Address Group or the name of an SNA Communications Device. The special value *ALL, when used on a rule, means that the rule applies to any rule means that the rule applies to any Location lacking a specific rule. when used as a subset or selection parameter, *ALL generally means to select all such rules for display or printing.

Object List

The Object List name is a short name you assign to a list of objects to help you identify the list. This name is required to be a valid OS name.

Operation

Operation represents the type of action being performed upon an object or upon the data in an object.



Valid values and their meanings are:

*__ALL__ Applies to all of the above types of operations.
*__CREATE__ Applies to objects when they are being created or to their data when they are being added to an object; for example, when writing records to a database.
*__READ__ Applies to non—modifying accesses of objects or the reading of an object's data.
*__UPDATE__ Applies to changes to objects or changes to their data.
*__DELETE__ Applies to deletion of objects or deletion of their data; for example, deleting records from a database file.

Status

Status indicates that an Object Rule is active (being enforced) or inactive (not being enforced).

Data Accesses

Use the data access rights to specify user rights to the data in the objects contained in the Object List.

Authority

Authority represents the action to be taken when a rule is found that matches the data present on a transaction. This Authority value pertains to Data Accesses.

The valid values are:

*__OS400__ The transaction will be allowed and object authority will be determined by the operating system.
*__REJECT__ The transaction will not be allowed.
*__SWITCH__ The transaction will be allowed and the transaction will occur as if the user profile named as the Swap Profile had initiated the transaction. After switching to the Swap Profile, the authority used during the transaction will be determined by the operating system.

Audit Transactions

The Audit transactions flag controls the logging of transactions to the Log Journal set up on the work with Exit Point Manager System Values panel. This Audit Transaction flag pertains to Data Accesses.

The valid values are:

__Y__ The transaction will be logged to the Log Journal.
__N__ The transaction will not be logged to the Log Journal.
* The default value from a prior rule will control the logging.

Send Messages

The Send messages flag controls the sending of messages to the Log Message Queue set up on the Work with Exit Point Manager System Values panel. This Send Messages flag pertains to Data Accesses.

The valid values are:

Y A log message will be sent to the Log Message Queue.
N A log message will not be sent to the Log Message Queue.
* The default value from a prior rule will control the logging.

Capture Transactions

The Capture transactions flag controls whether transactions are remembered in Exit Point Manager for later memorization. Once captured, transactions can become Memorized Transactions which can act as rules. This Capture Transactions flag pertains to Data Accesses.

The valid values are:

Y A log message will be sent to the Log Message Queue.
N A log message will not be sent to the Log Message Queue.
* The default value from a prior rule will control the logging.

Switch Profile

The Switch profile holds the name of a user profile whose authority is used to process the transaction instead of the authority of the User initiating the transaction. The transaction is executed as, and uses the authority of, this Switch profile. Switch profile is allowed only when Authority contains *SWITCH or *MEMSWITCH, if *MEMSWITCH is allowed. Otherwise it must contain *NONE.

This Switch Profile pertains to Data Accesses.

Object Access Rights

Use the object access rights to specify user rights to the objects in the Object List.

Authority

Authority represents the action to be taken when a rule is found that matches the data present on a transaction. This Authority value pertains to Object Accesses.

The valid values are:

***OS400** The transaction will be allowed and object authority will be determined by the operating system.
***REJECT** The transaction will not be allowed.
***SWITCH** The transaction will be allowed and the transaction will occur as if the user profile named as the Swap Profile had initiated the transaction. After switching to the Swap Profile, the authority used during the transaction will be determined by the operating system.

Audit Transactions

The Audit transactions flag controls the logging of transactions to the Log Journal set up on the work with Exit Point Manager System Values panel. This Audit Transaction flag pertains to Object Accesses.

The valid values are:

Y The transaction will be logged to the Log Journal.

N The transaction will not be logged to the Log Journal.
* The default value from a prior rule will control the logging.

Send Messages

The Send messages flag controls the sending of messages to the Log Message Queue set up on the work with Exit Point Manager System Values panel.

This Send Messages flag pertains to Object Accesses.

The valid values are:

Y A log message will be sent to the Log Message Queue.
N A log message will not be sent to the Log Message Queue.
* The default value from a prior rule will control the logging.

Capture Transactions

The Capture transactions flag controls whether transactions are remembered in Exit Point Manager for later memorization. Once captured, transactions can become Memorized Transactions which can act as rules. This Send Messages flag pertains to Object Accesses.

The valid values are:

Y A log message will be sent to the Log Message Queue.
N A log message will not be sent to the Log Message Queue.
* The default value from a prior rule will control the logging.

Switch Profile

The Switch profile holds the name of a user profile whose authority is used to process the transaction instead of the authority of the User initiating the transaction. The transaction is executed as, and uses the authority of, this Switch profile. Switch profile is allowed only when Authority contains *SWITCH or *MEMSWITCH, if *MEMSWITCH is allowed. Otherwise it must contain *NONE. This Switch Profile pertains to Object Accesses.

See Specifying the Server/Functions for an Object Rule.

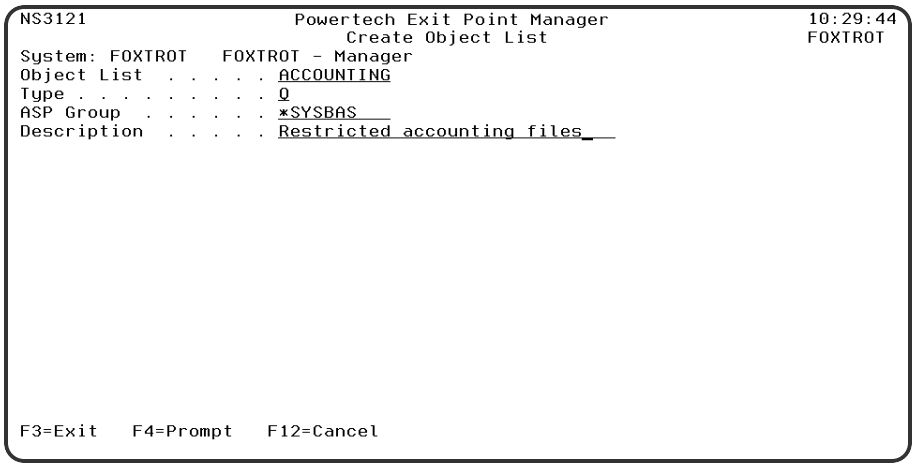
Command Keys

F3 (Exit): Exit the panel without processing any pending changes.

F4 (Prompt): Displays a list of possible values from which you may select one.

F12 (Cancel): Exit the panel without processing any pending changes.

Create Object List



How to Get There

From the Exit Point Manager Main Menu, select option **4** to display the Work with Security by Object panel. Select option **1** to display the Work with Object Lists panel, then enter a **1** in the Opt column on the first line of the Work with Object Lists panel. You can enter the Object List name, type, and description in the blank lines or press `Enter` to display the Create Object List panel.

What it Does

The Create Object List panel allows you to create an Object List. An Object list is simply a list of names of objects. These lists of objects are attached to Users or Locations on Object Rules. These rules help protect objects from outside access.

Field Descriptions

Object List

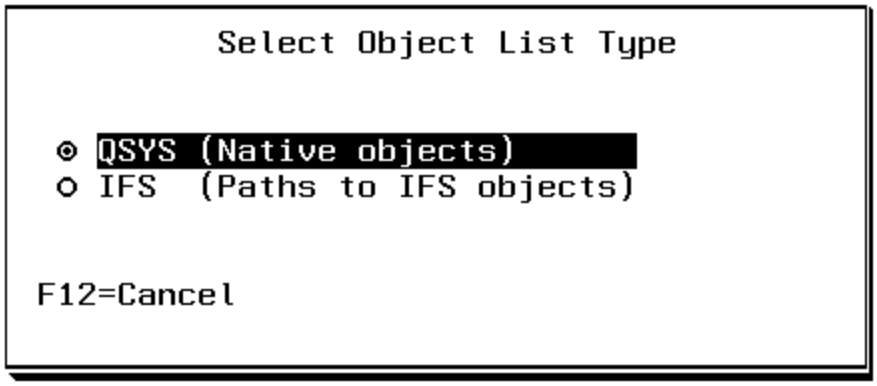
Enter a name for the Object List.

Type

Specify the type of the Object List. An Object List can be one of the following types:

QSYS	The list contains objects in an IBM i library.
IFS	The Object List contains objects from the IFS.

To select an Object List type, press `F4` to display the Select Object List Type window. Highlight a list type and press `Enter` to save your selection.



ASP Group

This is the name of an ASP Group. It is used in rule evaluation to determine if an object referenced in a transaction is the one specified on the object entries for this list.

Valid values:

***SYSBAS** The Object List entries refer to those objects in *SYSBAS.

***ALL** The Object List entries refer to those objects in any namespace.

Description

Enter a brief description of the Object List.

When you press enter to add the Object List, the message Object List successfully created displays at the bottom of the Work with Object Lists panel.

Command Keys

F3 (Exit): Exit the screen without processing any pending changes.

F4 (Prompt): Displays a list of possible values from which you may select one.

F12 (Cancel): Exit the screen without processing any pending changes.

Create Object Rule by User

```
NS3331                  Powertech Exit Point Manager                  13:33:38
                         Create Object Rule by User                   OSCAR
System: OSCAR
User . . . . . . . . . . . ADAMW      User profile, *PUBLIC
Object List  . . . . . . . PAYROLL    F4 for list
Operation  . . . . . . . . *ALL       F4 for list
Status . . . . . . . . . . *ACTIVE    *ACTIVE, *INACTIVE

Data Accesses:
  Authority  . . . . . . . *OS400     *OS400, *REJECT, *SWITCH
  Audit Transactions . . . *          Y=Yes, N=No, *=Default
  Send Messages  . . . . . *          Y=Yes, N=No, *=Default
  Capture Transactions . . *          Y=Yes, N=No, *=Default
  Switch Profile . . . . . *NONE      User profile, *NONE

Object Accesses:
  Authority  . . . . . . . *OS400     *OS400, *REJECT, *SWITCH
  Audit Transactions . . . *          Y=Yes, N=No, *=Default
  Send Messages  . . . . . *          Y=Yes, N=No, *=Default
  Capture Transactions . . *          Y=Yes, N=No, *=Default
  Switch Profile . . . . . *NONE      User profile, *NONE

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

How to Get There

From the Exit Point Manager Main Menu, select option **4** to display the Work with Security by Object panel. Select option **1** to display the Work with Object Lists panel, then enter an **9** in the Opt column on one of the Object Lists. On the Object Rules using Object List panel, enter a **1** in the Opt column and a User name. Press `Enter` to display the Create Object Rule by User panel.

What it Does

The Create Object Rule by User panel allows you to create an Object Rule linking a User to an Object List. The Copy Object List Entry panel allows you to copy an Object List Entry to a new entry.

Options

User

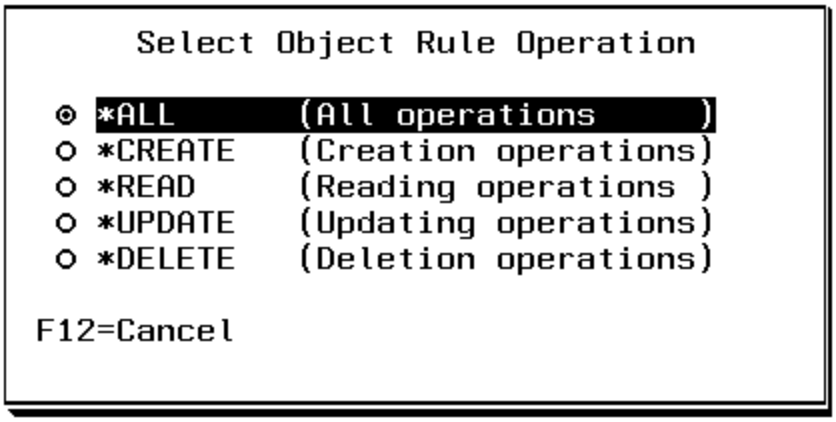
User represents the identity of the person initiating a transaction as a user profile. The special value *PUBLIC, when used on a rule, means that the rule applies to any User lacking a specific rule. when used as a subset or selection parameter, *PUBLIC means to select all such rules for display or printing.

Object List

The Object List name is a short name you assign to a list of objects to help you identify the list. This name is required to be a valid OS name.

Operation

Operation represents the type of action being performed upon an object or upon the data in an object.



Valid values and their meanings are:

*__ALL__ Applies to all of the above types of operations.
*__CREATE__ Applies to objects when they are being created or to their data when they are being added to an object; for example, when writing records to a database.
*__READ__ Applies to non—modifying accesses of objects or the reading of an object's data.
*__UPDATE__ Applies to changes to objects or changes to their data.
*__DELETE__ Applies to deletion of objects or deletion of their data; for example, deleting records from a database file.

Status

Status indicates that an Object Rule is active (being enforced) or inactive (not being enforced).

Data Access Rights

Use the data access rights to specify user rights to the data in the objects contained in the Object List.

Authority

Authority represents the action to be taken when a rule is found that matches the data present on a transaction. This Authority value pertains to Data Accesses.

The valid values are:

***OS400** The transaction will be allowed and object authority will be determined by the operating system.
***REJECT** The transaction will not be allowed.
***SWITCH** The transaction will be allowed and the transaction will occur as if the user profile named as the Swap Profile had initiated the transaction. After switching to the Swap Profile, the authority used during the transaction will be determined by the operating system.

Audit Transactions

The Audit transactions flag controls the logging of transactions to the Log Journal set up on the work with Exit Point Manager System Values panel. This Audit Transaction flag pertains to Data Accesses.

The valid values are:

Y The transaction will be logged to the Log Journal.
N The transaction will not be logged to the Log Journal.
* The default value from a prior rule will control the logging.

Send Messages

The Send messages flag controls the sending of messages to the Log Message Queue set up on the Work with Exit Point Manager System Values panel. This Send Messages flag pertains to Data Accesses.

The valid values are:

Y A log message will be sent to the Log Message Queue.
N A log message will not be sent to the Log Message Queue.
* The default value from a prior rule will control the logging.

Capture Transactions

The Capture transactions flag controls whether transactions are remembered in Exit Point Manager for later memorization. Once captured, transactions can become Memorized Transactions which can act as rules. This Capture Transactions flag pertains to Data Accesses.

The valid values are:

Y A log message will be sent to the Log Message Queue.
N A log message will not be sent to the Log Message Queue.
* The default value from a prior rule will control the logging.

Switch Profile

The Switch profile holds the name of a user profile whose authority is used to process the transaction instead of the authority of the User initiating the transaction. The transaction is executed as, and uses

the authority of, this Switch profile. Switch profile is allowed only when Authority contains *SWITCH or *MEMSWITCH, if *MEMSWITCH is allowed. Otherwise it must contain *NONE.

This Switch Profile pertains to Data Accesses.

Object Access Rights

Use the object access rights to specify user rights to the objects in the Object List.

Authority

Authority represents the action to be taken when a rule is found that matches the data present on a transaction. This Authority value pertains to Object Accesses.

The valid values are:

***OS400** The transaction will be allowed and object authority will be determined by the operating system.
***REJECT** The transaction will not be allowed.
***SWITCH** The transaction will be allowed and the transaction will occur as if the user profile named as the Swap Profile had initiated the transaction. After switching to the Swap Profile, the authority used during the transaction will be determined by the operating system.

Audit Transactions

The Audit transactions flag controls the logging of transactions to the Log Journal set up on the work with Exit Point Manager System Values panel. This Audit Transaction flag pertains to Object Accesses.

The valid values are:

Y The transaction will be logged to the Log Journal.
N The transaction will not be logged to the Log Journal.
* The default value from a prior rule will control the logging.

Send Messages

The Send messages flag controls the sending of messages to the Log Message Queue set up on the work with Exit Point Manager System Values panel.

This Send Messages flag pertains to Object Accesses.

The valid values are:

Y A log message will be sent to the Log Message Queue.
N A log message will not be sent to the Log Message Queue.
* The default value from a prior rule will control the logging.

Capture Transactions

The Capture transactions flag controls whether transactions are remembered in Exit Point Manager for later memorization. Once captured, transactions can become Memorized Transactions which can act as rules. This Send Messages flag pertains to Object Accesses.

The valid values are:

Y A log message will be sent to the Log Message Queue.
N A log message will not be sent to the Log Message Queue.
* The default value from a prior rule will control the logging.

Switch Profile
The Switch profile holds the name of a user profile whose authority is used to process the transaction instead of the authority of the User initiating the transaction. The transaction is executed as, and uses the authority of, this Switch profile. Switch profile is allowed only when Authority contains *SWITCH or *MEMSWITCH, if *MEMSWITCH is allowed. Otherwise it must contain *NONE. This Switch Profile pertains to Object Accesses.

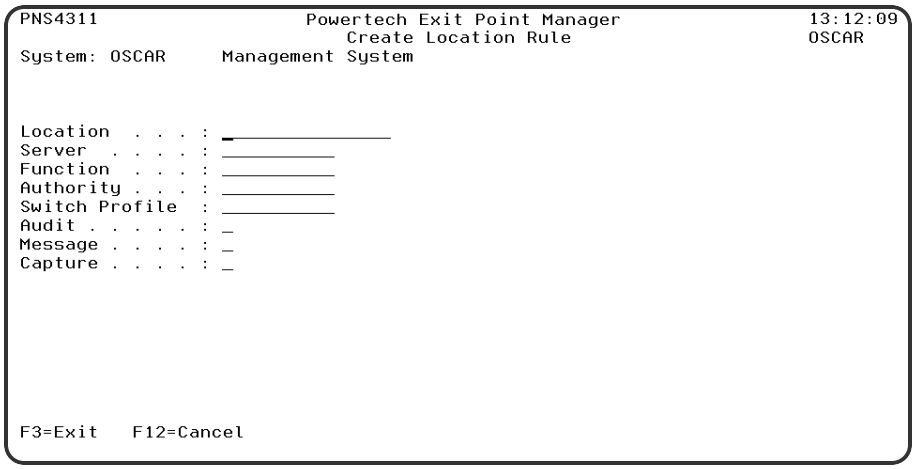
See Specifying the Server/Functions for an Object Rule.

Command Keys
F3 (Exit): Exit the panel without processing any pending changes.

F4 (Prompt): Displays a list of possible values from which you may select one.

F12 (Cancel): Exit the panel without processing any pending changes.

Create Location Rule panel



How to Get There
From the Exit Point Manager Main Menu, select option **3** to display the Work with Security by Location panel. Press `F6` to create a new Location rule.

What it Does
The Create Location Rule panel allows you to create a Location Rule.

Field Descriptions

System
System indicates the target of any operations you perform. When you add rules, for example, those rules will be sent to, and will affect processing on, the System named.

Location
Location represents the source of a transaction. Location can hold an IP Address, an IP Address Group or the name of an SNA Communications Device.

The special value *ALL, when used on a rule, means that the rule applies to any Location lacking a specific rule. When used as a subset or selection parameter, *ALL generally means to select all such rules for display or printing.

Server

A Server in Exit Point Manager is a controlled entry point into your system. These entry points are determined and defined by IBM. Exit Point Manager has assigned easy-to-remember names to these controlled entry points.

Function

A Function, or Server Function, in Exit Point Manager represents a class of operations that a given Server may perform. For example, the *SIGNON Server classifies its operations as those pertaining to changing passwords, generating authentication tokens, and retrieving signon information. Exit Point Manager has assigned easy-to-remember names to these Functions, such as CHGPWD, GENAUTTKN and RETRIEVE.

Authority Property

The authority assigned to the location for this server/function. If authority is left blank, Exit Point Manager will remove the location's entry.

Possible values are:

***OS400** Exit Point Manager will use normal OS/400 authority for the location.
***REJECT** Exit Point Manager will reject requests for the specified location.
***SWITCH** Exit Point Manager will use the authority of the switch profile for the specified location. A switch profile entry is required.
***MEMREJECT** Check Memorized Transactions (MTR) for authority. If no MTR authority is encountered, Exit Point Manager will reject requests for the specified location.
***MEMOS4OO** Check Memorized Transactions (MTR) for authority. If no MTR authority is encountered, Exit Point Manager will use normal OS/400 authority for the location. This is valid for both location and user.
***MEMSWITCH** Check Memorized Transactions (MTR) for authority. If no MTR authority is encountered, Exit Point Manager will use the authority of the switch profile for the specified location. A switch profile entry is required.
***SRVFCN** Exit Point Manager will use the authority defined for the server/function.
Switch The Switch profile holds the name of a user profile whose authority is used to process the transaction instead of the authority of the User initiating the transaction. The transaction is executed as, and uses the authority of, this Switch profile.

Switch profile is allowed only when Authority contains *SWITCH or *MEMSWITCH, if *MEMSWITCH is allowed. Otherwise it must contain *NONE.

Aud

The Audit transactions flag controls the logging of transactions to the Log Journal set up on the Work with Exit Point Manager System Values panel.

The valid values are:

* Uses the value found in the rule above this one in the rule hierarchy.
Y Logs all requests when this rule is enforced.
N Logs only access failures (rejects) for this rule.

Msg

The Send messages flag controls the sending of messages to the Log Message Queue set up on the Work with Exit Point Manager System Values panel.

The valid values are:

* Uses the value found in the rule above this one in the rule hierarchy.
Y Sends a message when this rule is enforced.
N Does not send a message when this rule is enforced.

Capture

The Capture transactions flag controls whether transactions are remembered in Exit Point Manager for later memorization. Once captured, transactions can become Memorized Transactions which can act as rules.

The valid values are:

* Uses the value found in the rule above this one in the rule hierarchy.
Y Captures the transaction when this rule is enforced.
N Does not capture the transaction when this rule is enforced.

Command Keys

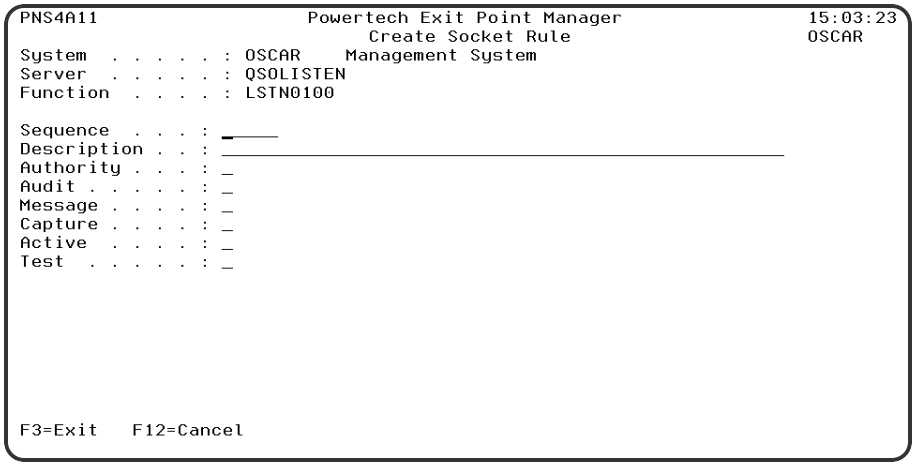
F3 (Exit): Exit the panel without processing any pending changes.

F4 (Prompt): Displays a list of possible values from which you may select one.

F12 (Cancel): Exit the panel without processing any pending changes.

Create Socket Rule panel

WARNING: Misuse of Socket Rules can render your system unreachable via TCP. Exercise extreme caution when using this feature. Consider adding Socket Rules as not active and testing them using the Socket Rule test feature, and setting them to be not used by that feature and testing the rule set before removing them. If you render your system unreachable via TCP, you will need to access the system via the console in order to fix the rules (or to deactivate the Socket Rule servers).



How to Get There

On the Work with Socket Rules panel, choose option **1**, **2**, or **3**. Then press **F6**.

What it Does

The Create Socket Rule panel allows you to create a new Socket Rule.

Field Descriptions

System

System indicates the target of any operations you perform. When you add rules, for example, those rules will be sent to, and will affect processing on, the System named.

Server

A Server in Exit Point Manager is a controlled entry point into your system. These entry points are determined and defined by IBM. Exit Point Manager has assigned easy-to-remember names to these controlled entry points.

Function

A Function, or Server Function, in Exit Point Manager represents a class of operations that a given Server may perform. For example, the *SIGNON Server classifies its operations as those pertaining to changing passwords, generating authentication tokens, and retrieving signon information. Exit Point Manager has assigned easy-to-remember names to these Functions, such as CHGPWD, GENAUTTKN and RETRIEVE.

Sequence

The sequence number of a Socket Rule determines the order in which it will be evaluated by the exit program, with the lowest sequence number being evaluated first. Socket Rules are evaluated until a match is found.

Description

The Socket Rule description is a short textual description of the Socket Rule. It is typically used to indicate the purpose of the Socket Rule.

Authority

Authority represents the action to be taken when a rule is found that matches the data present on a transaction.

The valid values are:

Y Exit Point Manager will allow requests when this rule is enforced.
N Exit Point Manager will reject requests when this rule is enforced.
* Uses the value found in the rule above this one in the rule hierarchy when this rule is enforced.

The value * will cause the rule to inherit the value from the default Socket Rule (sequence number 99999). This default rule may not be set to the value *.

Audit

The Audit transactions flag controls the logging of transactions to the Log Journal set up on the Work with Exit Point Manager System Values panel.

The valid values are:

* Uses the value found in the rule above this one in the rule hierarchy.
Y Logs all requests when this rule is enforced.
N Logs only access failures (rejects) for this rule.

The value * will cause the rule to inherit the value from the default Socket Rule (sequence number 99999). This default rule may not be set to the value *.

Message

The Send messages flag controls the sending of messages to the Log Message Queue set up on the Work with Exit Point Manager System Values panel.

The valid values are:

* Uses the value found in the rule above this one in the rule hierarchy.
Y Sends a message when this rule is enforced.
N Does not send a message when this rule is enforced.

The value * will cause the rule to inherit the value from the default Socket Rule (sequence number 99999). This default rule may not be set to the value *.

Capture

The Capture transactions flag controls whether transactions are remembered in Exit Point Manager. Unlike some other rule types, a captured Socket Rule cannot be memorized.

The valid values are:

* Uses the value found in the rule above this one in the rule hierarchy.
Y Captures the transaction when this rule is enforced.
N Does not capture the transaction when this rule is enforced.

The value * will cause the rule to inherit the value from the default Socket Rule (sequence number 99999). This default rule may not be set to the value *.

Active

The Socket Rule Active flag determines whether the rule will be evaluated by the exit point program.

It can be useful to initially set a Socket Rule as not active in order to test it without enforcing it.

The valid values are:

Y Exit Point Manager will evaluate the rule.
N Exit Point Manager will not evaluate the rule.

The value N is not allowed for the default Socket Rule (sequence number 99999).

Test

The Socket Rule Test flag determines whether the rule will be evaluated by the Socket Rule test facility.

It can be useful to flag a rule to not be tested in order to verify the effects of removing that rule.

The value N is not allowed for the default Socket Rule (sequence number 99999).

The valid values are:

Y The Socket Rule test facility will evaluate the rule.
N The Socket Rule test facility will not evaluate the rule.

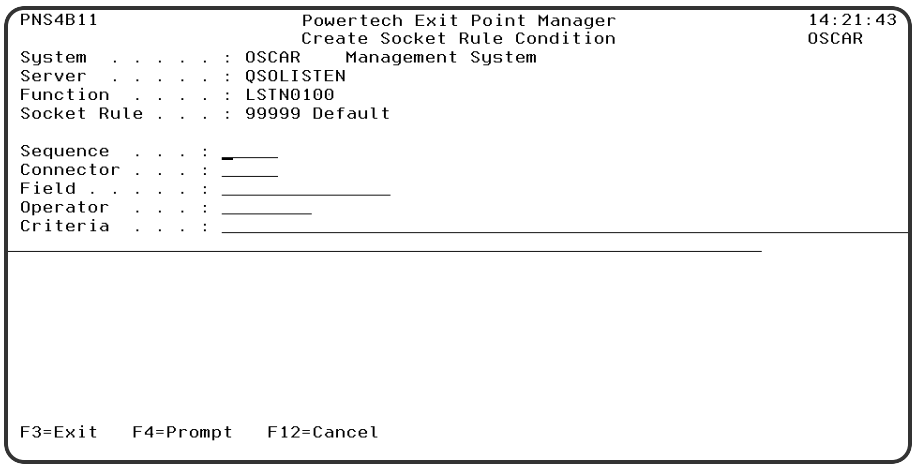
Command Keys

F3 (Exit): Exit the panel without processing any pending changes.

F12 (Cancel): Exit the panel without processing any pending changes.

Create Socket Rule Condition panel

WARNING: Misuse of Socket Rules can render your system unreachable via TCP. Exercise extreme caution when using this feature. Consider adding Socket Rules as not active and testing them using the Socket Rule test feature, and setting them to be not used by that feature and testing the rule set before removing them. If you render your system unreachable via TCP, you will need to access the system via the console in order to fix the rules (or to deactivate the Socket Rule servers).



How to Get There

On the Work with Socket Conditions panel, press **F6**.

What it Does

The Create Socket Condition panel allows you to create a Socket Condition.

Field Descriptions

System

System indicates the target of any operations you perform. When you add rules, for example, those rules will be sent to, and will affect processing on, the System named.

Server

A Server in Exit Point Manager is a controlled entry point into your system. These entry points are determined and defined by IBM. Exit Point Manager has assigned easy-to-remember names to these controlled entry points.

Function

A Function, or Server Function, in Exit Point Manager represents a class of operations that a given Server may perform. For example, the *SIGNON Server classifies its operations as those pertaining to

changing passwords, generating authentication tokens, and retrieving signon information. Exit Point Manager has assigned easy-to-remember names to these Functions, such as CHGPWD, GENAUTTKN and RETRIEVE.

Socket Rule

The Socket Rule to which this Socket Condition belongs. A Socket Rule without a Socket Condition, or with an invalid Socket Condition, will not be enforced.

Sequence

The sequence number of a Socket Condition determines the order in which it is combined with other Socket Conditions for a Socket Rule.

Connector

The connector determines how a Socket Condition relates to other Socket Conditions for a Socket Rule.

Socket Conditions with a higher order of precedence are evaluated before ones with a lower order of precedence.

The connector for the Socket Condition with the lowest sequence number is ignored.

> **EXAMPLE:**
> Given three Socket Conditions:
>
> ```
> Seq = 10 Connector = <ignored> evaluates to False
> Seq = 20 Connector = AND evaluates to True
> Seq = 30 Connector = OR evaluates to True
> ```
>
> This will return True as it is equivalent to:
> (False AND True) OR True
> If the OR were evaluated first then it would return False as it would be equivalent to:
> False AND (True OR True)

The valid values are:

OR This Socket Condition is OR'ed with others. An OR has the lowest order of precedence (evaluated last).

AND This Socket Condition is AND'ed with others. An AND has a higher order of precedence than an OR, but lower than an ORAND.

ORAND This Socket Condition is OR'ed with others. An ORAND has the highest order of precedence (evaluated first).

Field

This is the name of the field to be evaluated at run time.

The valid values are dependent on the Socket Rule.

Valid values for the QSOLISTEN server are:

LCL_PORT The local port number; an integer between 1 and 65535.
LCL_USR The user profile associated with the job issuing the listen.

LCL_USR_GRP A User Group containing the user profile associated with the job issuing the listen.

Valid values for the QSOCONNECT server are:

LCL_PORT The local port number; an integer between 1 and 65535.
RMT_PORT The remote port number; an integer between 1 and 65535.
RMT_ADDR The remote address. Valid formats are IPv4, IPv6, and Powertech Exit Point Manager IP address groups.
LCL_USR The user profile associated with the job issuing the connect.
LCL_USR_GRP A User Group containing the user profile associated with the job issuing the connect.

Valid values for the QSOACCEPT server are:

LCL_IN_PORT The local incoming port number; an integer between 1 and 65535.
LCL_BND_PORT The local bound port number; an integer between 1 and 65535.
RMT_PORT The remote port number; an integer between 1 and 65535.
RMT_ADDR The remote address. Valid formats are IPv4, IPv6, and Powertech Exit Point Manager IP address groups.
LCL_USR The user profile associated with the job issuing the accept.
LCL_USR_GRP A User Group containing the user profile associated with the job issuing the accept.

Operator

The test used for the value of the field and the criteria to evaluate this Socket Condition.

= The value of the field is equal to the criteria, or, if the criteria can be a list, the value of the field is found in that list.
<> The value of the field is not equal to the criteria, or, if the criteria can be a list, the value of the field is not found in that list.
> The value of the field is greater than the criteria.
< The value of the field is less than the criteria.
>= The value of the field is greater than or equal to the criteria.
<= The value of the field is less than or equal to the criteria.

ALWAYS

This will cause the condition to always match. It is used on the Socket Condition of the default Socket Rule, and may be used on non-default Socket Rules.

If present, it must be the only Socket Condition for a Socket Rule.

Criteria

This is the value against which the value of the selected field will be compared at run time.

The valid values are dependent on the selected Field.

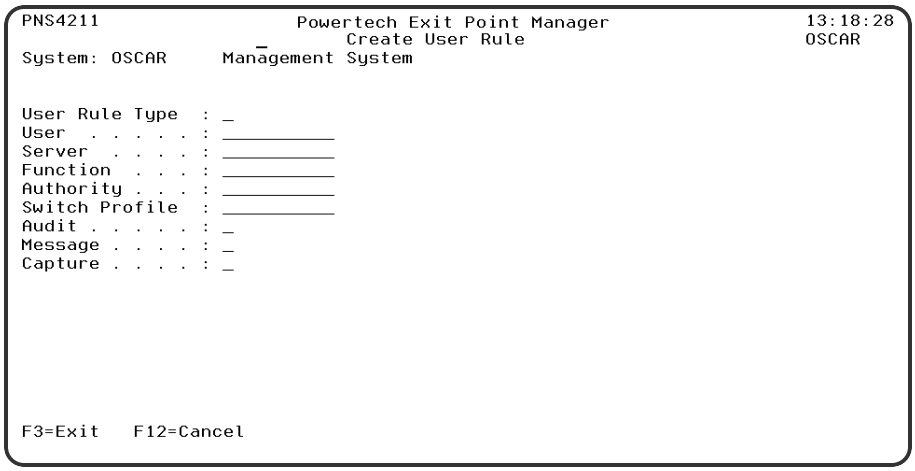
Command Keys

F3 (Exit): Exit the panel without processing any pending changes.

F4 (Prompt): Displays a list of items from which one or more may be selected.

F12 (Cancel): Exit the panel without processing any pending changes.

Create User Rule panel



How to Get There

From the Exit Point Manager Main Menu, select option **2** to display the Work with Security by User panel. Press `F6` to create a new user rule.

What it Does

The Create User Rule panel allows you to create a User Rule.

Field Descriptions

System

System indicates the target of any operations you perform. When you add rules, for example, those rules will be sent to, and will affect processing on, the System named.

User Type

This field is used to indicate whether the associated User field refers to an O/S user profile or a Exit Point Manager User Group.

Valid values are:

U The associated User field refers to an O/S user profile.
G The associated User field refers to a Exit Point Manager user group.

User

If the associated User Type is a 'U', User represents the identity of the person initiating a transaction as a user profile.

The special value *PUBLIC, when used on a rule, means that the rule applies to any User lacking a specific rule. When used as a subset or selection parameter, *PUBLIC means to select all such rules for display or printing.

If the associated User Type is a 'G', User represents a Exit Point Manager User Group.

Server

A Server in Exit Point Manager is a controlled entry point into your system. These entry points are determined and defined by IBM. Exit Point Manager has assigned easy-to-remember names to these controlled entry points.

Function

A Function, or Server Function, in Exit Point Manager represents a class of operations that a given Server may perform. For example, the *SIGNON Server classifies its operations as those pertaining to changing passwords, generating authentication tokens, and retrieving signon information. Exit Point Manager has assigned easy-to-remember names to these Functions, such as CHGPWD, GENAUTTKN and RETRIEVE.

Authority Property

The authority assigned to the user for this server/function. If authority is left blank, Exit Point Manager will remove the user's entry.

Possible values are:

***OS400** Exit Point Manager will use normal OS/400 authority for the user.
***REJECT** Exit Point Manager will reject requests for the specified user.
***SWITCH** Exit Point Manager will use the authority of the switch profile for the specified user. A switch profile entry is required.
***MEMREJECT** Check Memorized Transactions (MTR) for authority. If no MTR authority is encountered, Exit Point Manager will reject requests for the specified user.
***MEMOS4OO** Check Memorized Transactions (MTR) for authority. If no MTR authority is encountered, Exit Point Manager will use normal OS/400 authority for the location. This is valid for both location and user.
***MEMSWITCH** Check Memorized Transactions (MTR) for authority. If no MTR authority is encountered, Exit Point Manager will use the authority of the switch profile for the specified user. A switch profile entry is required.
***SRVFCN** Exit Point Manager will use the authority defined for the server/function.
Switch The Switch profile holds the name of a user profile whose authority is used to process the transaction instead of the authority of the User initiating the transaction. The transaction is executed as, and uses the authority of, this Switch profile.

Switch profile is allowed only when Authority contains *SWITCH or *MEMSWITCH, if *MEMSWITCH is allowed. Otherwise it must contain *NONE.

Aud

The Audit transactions flag controls the logging of transactions to the Log Journal set up on the Work with Exit Point Manager System Values panel.

The valid values are:

* Uses the value found in the rule above this one in the rule hierarchy.
Y Logs all requests when this rule is enforced.
N Logs only access failures (rejects) for this rule.

Msg

The Send messages flag controls the sending of messages to the Log Message Queue set up on the Work with Exit Point Manager System Values panel.

The valid values are:

* Uses the value found in the rule above this one in the rule hierarchy.
Y Sends a message when this rule is enforced.
N Does not send a message when this rule is enforced.

Capture

The Capture transactions flag controls whether transactions are remembered in Exit Point Manager for later memorization. Once captured, transactions can become Memorized Transactions which can act as rules.

The valid values are:

* Uses the value found in the rule above this one in the rule hierarchy.
Y Captures the transaction when this rule is enforced.
N Does not capture the transaction when this rule is enforced.

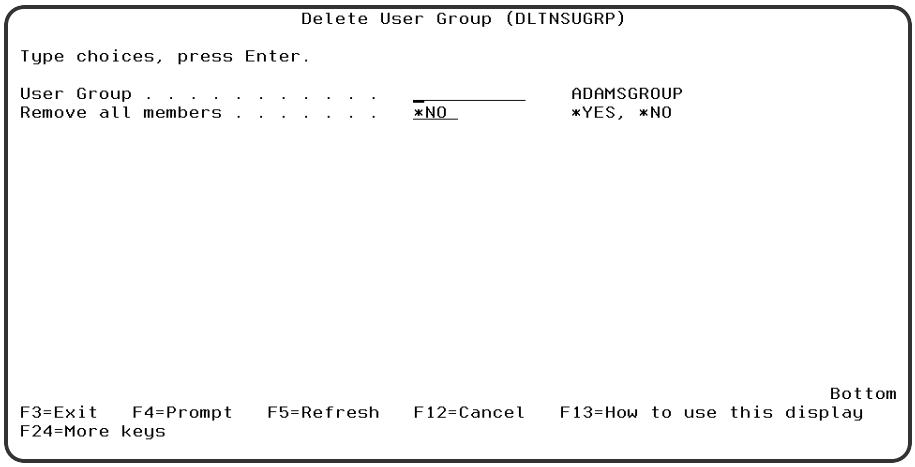
Command Keys

F3 (Exit): Exit the screen without processing any pending changes.

F4 (Prompt): Displays a list of possible values from which you may select one.

F12 (Cancel): Exit the screen without processing any pending changes.

Delete User Group (DLTNSUGRP)



What it Does

The Delete User Group command allows you to delete a User Group. Optionally you can also remove each User Group Member from the group prior to attempting to delete it.

Options

User Group (NAME)

Specify the name of the User Group to be deleted. The User Group must be empty unless you specify RMVMBRS(*YES) on the command.

The User Group name is a short name you assign to a group of user profiles to help you identify the group.

This name is required to be a valid OS name.

Remove all members (RMVMBRS)

This parameter allows you to remove each User Group Member from the group prior to attempting to delete it. Normally you must manually remove each User Group Member from the User Group prior to attempting to delete it. Specify one of the following values:

***YES**

Deletes each User Group Member from the User Group, then attempts to delete the User Group

***NO**

Attempts to delete the User Group as it exists when the command is executed. The command may fail if the User Group contains even a single User Group Member.

Command Keys

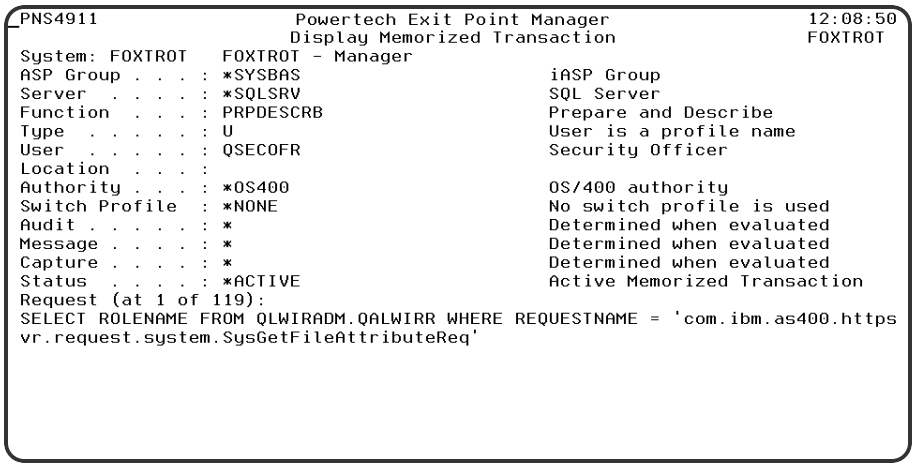
F3 (Exit): Exit the current panel without processing any pending changes.

F4 (Prompt): Displays a list of possible values from which you may select one.

F5 (Refresh): Refreshes the panel and resets all available text fields.

F12 (Cancel): Exit the current panel without processing any pending changes.

Display Memorized Transaction panel



How to Get There

From the Exit Point Manager Main Menu, select option **11**. On the Work with Memorized Transactions panel, choose option **5** for a Memorized Transaction and press `Enter`.

What it Does

The Display Memorized Transaction panel enables you to display a memorized transaction.

Options

System
System indicates the target of any operations you perform. When you add rules, for example, those rules will be sent to, and will affect processing on, the System named.

ASP Group
When a memorized transaction is evaluated, this ASP Group name will be compared to the current ASP Group name of the job issuing the transaction. These need to be the same (or this must be set to the special value *ALL) for this memorized transaction to be considered a match.

Server
A Server in Exit Point Manager is a controlled entry point into your system. These entry points are determined and defined by IBM. Exit Point Manager has assigned easy-to-remember names to these controlled entry points.

Function
A Function, or Server Function, in Exit Point Manager represents a class of operations that a given Server may perform. For example, the *SIGNON Server classifies its operations as those pertaining to changing passwords, generating authentication tokens, and retrieving sign-on information. Exit Point Manager has assigned easy-to-remember names to these Functions, such as CHGPWD, GENAUTTKN and RETRIEVE. This field cannot be changed.

Special values are:

***ALL** The rule will apply to all Functions of the specified Server.

User Type
This field is used to indicate whether the associated User field refers to an O/S user profile or a Exit Point Manager User Group.

Valid values are:

U The associated User field refers to an O/S user profile.
G The associated User field refers to a Exit Point Manager user group.

User
User represents the identity of the person initiating a transaction as a user profile. The special value *PUBLIC, when used on a rule, means that the rule applies to any User lacking a specific rule. When used as a subset or selection parameter, *PUBLIC means to select all such rules for display or printing.

Special values are:

***PUBLIC** The rule will apply to all Users.

Location
Location represents the source of a transaction. Location can hold an IP Address, an IP Address Group or the name of an SNA Communications Device. The special value *ALL, when used on a rule, means that the rule applies to any rule means that the rule applies to any Location lacking a specific rule. when used as a subset or selection parameter, *ALL generally means to select all such rules for display or printing.

Special values are:

*__ALL__ The rule will apply to all Locations.

Authority

Authority represents the action to be taken when a rule is found that matches the data present on a transaction.

The list of valid values may include one or more of these values:

*__USER__ Current user authority is used.
*__0S400__ Exit Point Manager will use normal operating system authority for the user.
*__REJECT__ Exit Point Manager will reject requests.
*__SWITCH__ Exit Point Manager will use the authority of the switch profile for the transaction. A switch profile entry is required.
*__MEMUSR__ Memorized Transactions (MTR) are checked for authority first. If no MTR authority is encountered, Exit Point Manager will use the authority of the current user.
*__MEMOS400__ Memorized Transactions (MTR) are checked for authority first. If no MTR authority is encountered, Exit Point Manager will use normal operating system authority for the user.
*__MEMREJECT__ Memorized Transactions (MTR) are checked for authority first. If no MTR authority is encountered, Exit Point Manager will reject requests for the specified user.
*__MEMSWITCH__ Memorized Transactions (MTR) are checked for authority first. If no MTR authority is encountered, Exit Point Manager will use the authority of the switch profile for the specified user. A switch profile entry is required.
*__MEMOBJ__ Memorized Transactions (MTR) are checked for authority first. If no MTR authority is encountered, Exit Point Manager will check any objects used in the transactions for authorities defined by Object Rules.
*__SERVER__ Exit Point Manager will use the authority defined for the Server.
*__SRVFCN__ Exit Point Manager will use the authority defined for the Server Function.

Audit transactions

The Audit transactions flag controls the logging of transactions to the Log Journal set up on the work with Exit Point Manager System Values panel. Specify one of these values for Audit transactions:

*__DEFAULT__ Uses the value found in the rule above this one in the rule hierarchy.
*__YES__ Logs all requests when this rule is enforced.
*__NO__ Logs only access failures (rejects) for this rule.

Send messages

The Send messages flag controls the sending of messages to the Log Message Queue set up on the work with Exit Point Manager System Values panel.

Specify one of these values for Send messages:

*__DEFAULT__ Uses the value found in the rule above this one in the rule hierarchy.
*__YES__ Sends a message when this rule is enforced.
*__NO__ Does not send a message when this rule is enforced.

Capture transactions

The Capture transactions flag controls whether transactions are remembered in Exit Point Manager for later memorization. Once captured, transactions can become Memorized Transactions which can act as rules. Specify one of these values for Capture transactions:

*__DEFAULT__ Uses the value found in the rule above this one in the rule hierarchy.
*__YES__ Captures the transaction when this rule is enforced.

***NO** Does not capture the transaction when this rule is enforced.

Switch profile

The Switch profile holds the name of a user profile whose authority is used to process the transaction instead of the authority of the User initiating the transaction. The transaction is executed as, and uses the authority of, this Switch profile.

Switch profile is allowed only when Authority contains *SWITCH or *MEMSWITCH, if *MEMSWITCH is allowed. Otherwise it must contain *NONE. This field may hold the special value *NONE in which case no Switch profile will be used.

Status

This is the status of the Memorized Transaction.

Possible values are:

***ACTIVE** Exit Point Manager will attempt to match this transaction during rule enforcement. Memorized Transactions that are changed to *ACTIVE will have a matching User or Location rule changed to the corresponding action; *ALLOW to *MEMOS400, *REJECT to *MEMREJECT, or *SWITCH to *MEMSWITCH.
***INACTIVE**Exit Point Manager will not attempt to match this transaction during rule enforcement. Memorized Transactions that are changed to *INACTIVE will have the matching User or Location rule changed (if there are no other Memorized Transactions for that rule) to the corresponding action; *MEMOS400 to *ALLOW, *MEMREJECT to *REJECT, or *MEMSWITCH to *SWITCH.

Transaction

The Memorized Transaction against which incoming transactions are tested. If a match is found, then this rule will be invoked. Undisplayable characters in the transaction data are replaced by the mid—dot character (-).

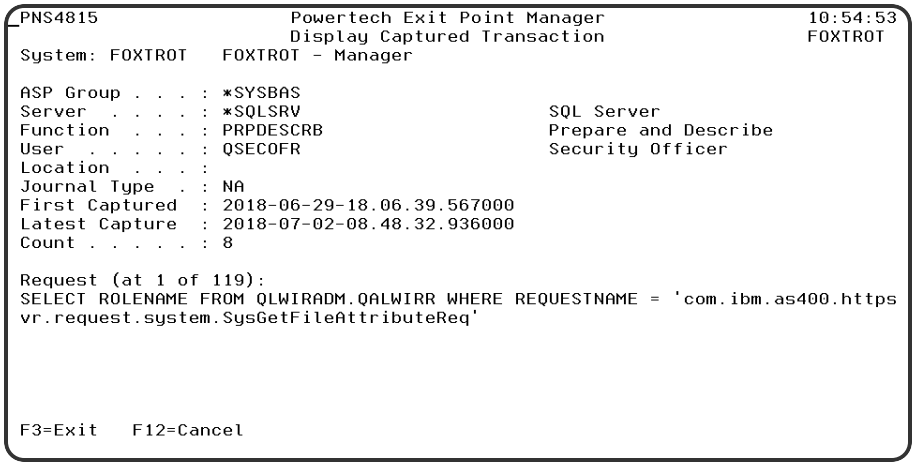
You can use the Transaction wildcard character (%) to make a Transaction generic. The wildcard character is valid only at the end of a Transaction string. when you are memorizing or changing a Memorized Transaction, the first occurrence of the wildcard character that was NOT present in the string before you changed it will make the string generic and all data after that wildcard character will be discarded.

Command Keys

F3 (Exit): Exit the panel without processing any pending changes.

F12 (Cancel): Exit the panel without processing any pending changes.

Display Captured Transaction panel



How to Get There

On the Work with Captured Transactions screen, choose **5** for a transaction.

What it Does

The Display Captured Transaction panel shows the properties for the captured transaction, including the Server, Function, User name, Location, Count (how many times this transaction has occurred), First Collected (the date and time when a transaction was first summarized into this record), Last Collected (the date and time when a transaction was last summarized into this record), and the type of action performed by Exit Point Manager for the transactions summarized into this record. The actual transaction string also displays.

Field Descriptions

The Display Captured Transaction panel allows you to change some of the values for the captured transaction to fine tune it to your specification before you memorize it.

System

System indicates the target of any operations you perform. When you add rules, for example, those rules will be sent to, and will affect processing on, the System named.

ASP Group

This is the name of the ASP Group to which the job was set when the transaction was captured.

Server

A Server in Exit Point Manager is a controlled entry point into your system. These entry points are determined and defined by IBM. Exit Point Manager has assigned easy-to-remember names to these controlled entry points.

Function

A Function, or Server Function, in Exit Point Manager represents a class of operations that a given Server may perform. For example, the *SIGNON Server classifies its operations as those pertaining to changing passwords, generating authentication tokens, and retrieving sign-on information. Exit Point

Manager has assigned easy-to-remember names to these Functions, such as CHGPWD, GENAUTTKN and RETRIEVE.

User

User represents the identity of the person initiating a transaction as a user profile. The special value *PUBLIC, when used on a rule, means that the rule applies to any User lacking a specific rule. when used as a subset or selection parameter, *PUBLIC means to select all such rules for display or printing. This is the User that initiated the transaction.

> **NOTE:** The count includes only transactions that you've specified should be captured by Exit Point Manager. It does not reflect all network traffic and cannot be used for a general statistical analysis of network traffic.

Count

The number of times this exact transaction has been captured.

Transaction

This is the data handed to Exit Point Manager by the operating system. Much of this transaction data is binary in nature and may not be human-readable. Undisplayable characters in the transaction data are replaced by the mid—dot character (-).

Command Keys

F3 (Exit): Exit the current panel without processing any pending changes.

F5 (Refresh): Refreshes the panel and resets all available text fields.

F7 (Select System): Use this command key to work with data from a different System.

F11 (View): Switches views of the list so that you can see other data.

F12 (Cancel): Exit the current panel without processing any pending changes.

F16 (Sort/Subset): Allows you to sort and subset information by user, server, type, and/or transaction.

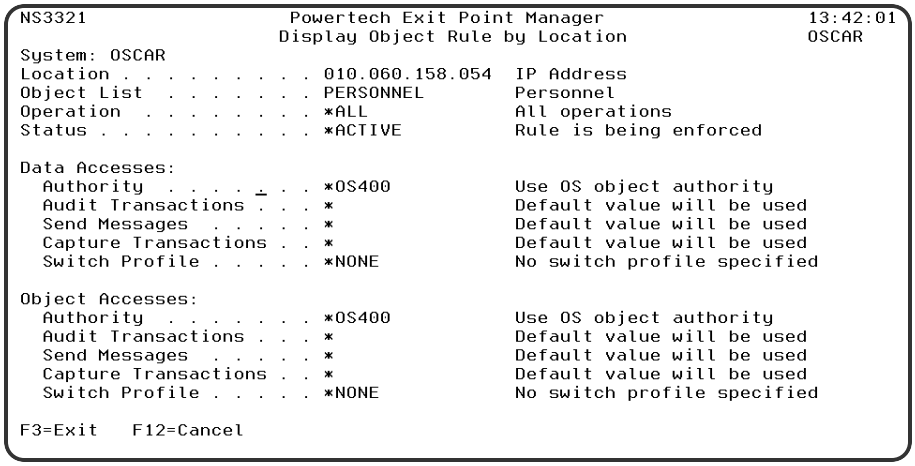
F17 (Top): Positions the list panel to the first record.

F18 (Bottom): Positions the list panel to the last record.

F19 (Left): Shifts the transaction data to the left.

F20 (Right): Shifts the transaction date to the right.

Display Object Rule by Location



How to Get There

From the Exit Point Manager Main Menu, select option **4** to display the Work with Security by Object panel. Select option **1** to display the Work with Object Lists panel, then enter an **9** in the Opt column on one of the Object Lists. On the Object Rules using Object List panel, enter a **5** in the Opt column. Press `Enter` to display the Display Object Rule by Location panel.

What it Does

The Display Object Rule by Location panel shows you the detailed attributes of an Object Rule.

Column Descriptions

Location

Location represents the source of a transaction. Location can hold an IP Address, an IP Address Group or the name of an SNA Communications Device. The special value *ALL, when used on a rule, means that the rule applies to any rule means that the rule applies to any Location lacking a specific rule. when used as a subset or selection parameter, *ALL generally means to select all such rules for display or printing.

Object List

The Object List name is a short name you assign to a list of objects to help you identify the list.

Operation

Operation represents the type of action being performed upon an object or upon the data in an object.

Status

Status indicates that an Object Rule is active (being enforced) or inactive (not being enforced).

Data Accesses

Use the data access rights to specify user rights to the data in the objects contained in the Object List.

Authority

Authority represents the action to be taken when a rule is found that matches the data present on a transaction. This Authority value pertains to Data Accesses.

The valid values are:

***OS400** The transaction will be allowed and object authority will be determined by the operating system.
***REJECT** The transaction will not be allowed.
***SWITCH** The transaction will be allowed and the transaction will occur as if the user profile named as the Swap Profile had initiated the transaction. After switching to the Swap Profile, the authority used during the transaction will be determined by the operating system.

Audit Transactions

The Audit transactions flag controls the logging of transactions to the Log Journal set up on the work with Exit Point Manager System Values panel. This Audit Transaction flag pertains to Data Accesses.

The valid values are:

Y The transaction will be logged to the Log Journal.
N The transaction will not be logged to the Log Journal.
* The default value from a prior rule will control the logging.

Send Messages

The Send messages flag controls the sending of messages to the Log Message Queue set up on the Work with Exit Point Manager System Values panel. This Send Messages flag pertains to Data Accesses.

The valid values are:

Y A log message will be sent to the Log Message Queue.
N A log message will not be sent to the Log Message Queue.
* The default value from a prior rule will control the logging.

Capture Transactions

The Capture transactions flag controls whether transactions are remembered in Exit Point Manager for later memorization. Once captured, transactions can become Memorized Transactions which can act as rules. This Capture Transactions flag pertains to Data Accesses.

The valid values are:

Y A log message will be sent to the Log Message Queue.
N A log message will not be sent to the Log Message Queue.
* The default value from a prior rule will control the logging.

Switch Profile

The Switch profile holds the name of a user profile whose authority is used to process the transaction instead of the authority of the User initiating the transaction. The transaction is executed as, and uses the authority of, this Switch profile. Switch profile is allowed only when Authority contains *SWITCH or *MEMSWITCH, if *MEMSWITCH is allowed. Otherwise it must contain *NONE.

This Switch Profile pertains to Data Accesses.

Object Access Rights

Use the object access rights to specify user rights to the objects in the Object List.

Authority

Authority represents the action to be taken when a rule is found that matches the data present on a transaction. This Authority value pertains to Object Accesses.

The valid values are:

***OS400** The transaction will be allowed and object authority will be determined by the operating system.
***REJECT** The transaction will not be allowed.
***SWITCH** The transaction will be allowed and the transaction will occur as if the user profile named as the Swap Profile had initiated the transaction. After switching to the Swap Profile, the authority used during the transaction will be determined by the operating system.

Audit Transactions

The Audit transactions flag controls the logging of transactions to the Log Journal set up on the work with Exit Point Manager System Values panel. This Audit Transaction flag pertains to Object Accesses.

The valid values are:

Y The transaction will be logged to the Log Journal.
N The transaction will not be logged to the Log Journal.
* The default value from a prior rule will control the logging.

Send Messages

The Send messages flag controls the sending of messages to the Log Message Queue set up on the work with Exit Point Manager System Values panel.

This Send Messages flag pertains to Object Accesses.

The valid values are:

Y A log message will be sent to the Log Message Queue.
N A log message will not be sent to the Log Message Queue.
* The default value from a prior rule will control the logging.

Capture Transactions

The Capture transactions flag controls whether transactions are remembered in Exit Point Manager for later memorization. Once captured, transactions can become Memorized Transactions which can act as rules. This Send Messages flag pertains to Object Accesses.

The valid values are:

Y A log message will be sent to the Log Message Queue.
N A log message will not be sent to the Log Message Queue.
* The default value from a prior rule will control the logging.

Switch Profile

The Switch profile holds the name of a user profile whose authority is used to process the transaction instead of the authority of the User initiating the transaction. The transaction is executed as, and uses the authority of, this Switch profile. Switch profile is allowed only when Authority contains *SWITCH or *MEMSWITCH, if *MEMSWITCH is allowed. Otherwise it must contain *NONE. This Switch Profile pertains to Object Accesses.

See Specifying the Server/Functions for an Object Rule.

Command Keys

F3 (Exit): Exit the panel without processing any pending changes.

F12 (Cancel): Exit the panel without processing any pending changes.

Display Object Rule by User

```
NS3331                  Powertech Exit Point Manager                  13:43:15
                         Display Object Rule by User                  OSCAR
System: OSCAR
User . . . . . . . . . . . MARKJ
Object List  . . . . . . . PERSONNEL        Personnel
Operation  . . . . . . . . *ALL             All operations
Status . . . . . . . . . . *ACTIVE          Rule is being enforced

Data Accesses:
  Authority  . . . . . . . *OS400           Use OS object authority
  Audit Transactions . . . N                Transactions will not be audited
  Send Messages  . . . . . N                Messages will not be sent
  Capture Transactions . . N                Transactions will not be captured
  Switch Profile . . . . . *NONE            No switch profile specified

Object Accesses:
  Authority  . . . . . . . *OS400           Use OS object authority
  Audit Transactions . . . *                Default value will be used
  Send Messages  . . . . . *                Default value will be used
  Capture Transactions . . *                Default value will be used
  Switch Profile . . . . . *NONE            No switch profile specified

F3=Exit   F12=Cancel
```

How to Get There

From the Exit Point Manager Main Menu, select option **4** to display the Work with Security by Object panel. Select option **1** to display the Work with Object Lists panel, then enter an **9** in the Opt column on one of the Object Lists. On the Object Rules using Object List panel, enter a **5** in the Opt column and a User. Press `Enter` to display the Display Object Rule by User panel.

What it Does

The Display Object Rule by User panel shows you the detailed attributes of an Object Rule.

Column Descriptions

User

User represents the identity of the person initiating a transaction as a user profile. The special value *PUBLIC, when used on a rule, means that the rule applies to any User lacking a specific rule. when used as a subset or selection parameter, *PUBLIC means to select all such rules for display or printing.

Object List

The Object List name is a short name you assign to a list of objects to help you identify the list. This name is required to be a valid OS name.

Operation

Operation represents the type of action being performed upon an object or upon the data in an object.

Status

Status indicates that an Object Rule is active (being enforced) or inactive (not being enforced).

Data Accesses

Use the data access rights to specify user rights to the data in the objects contained in the Object List.

Authority

Authority represents the action to be taken when a rule is found that matches the data present on a transaction. This Authority value pertains to Data Accesses.

The valid values are:

*__OS400__ The transaction will be allowed and object authority will be determined by the operating system.
*__REJECT__ The transaction will not be allowed.
*__SWITCH__ The transaction will be allowed and the transaction will occur as if the user profile named as the Swap Profile had initiated the transaction. After switching to the Swap Profile, the authority used during the transaction will be determined by the operating system.

Audit Transactions

The Audit transactions flag controls the logging of transactions to the Log Journal set up on the work with Exit Point Manager System Values panel. This Audit Transaction flag pertains to Data Accesses.

The valid values are:

__Y__ The transaction will be logged to the Log Journal.
__N__ The transaction will not be logged to the Log Journal.
* The default value from a prior rule will control the logging.

Send Messages

The Send messages flag controls the sending of messages to the Log Message Queue set up on the Work with Exit Point Manager System Values panel. This Send Messages flag pertains to Data Accesses.

The valid values are:

__Y__ A log message will be sent to the Log Message Queue.
__N__ A log message will not be sent to the Log Message Queue.
* The default value from a prior rule will control the logging.

Capture Transactions

The Capture transactions flag controls whether transactions are remembered in Exit Point Manager for later memorization. Once captured, transactions can become Memorized Transactions which can act as rules. This Capture Transactions flag pertains to Data Accesses.

The valid values are:

__Y__ A log message will be sent to the Log Message Queue.
__N__ A log message will not be sent to the Log Message Queue.
* The default value from a prior rule will control the logging.

Switch Profile

The Switch profile holds the name of a user profile whose authority is used to process the transaction instead of the authority of the User initiating the transaction. The transaction is executed as, and uses

the authority of, this Switch profile. Switch profile is allowed only when Authority contains *SWITCH or *MEMSWITCH, if *MEMSWITCH is allowed. Otherwise it must contain *NONE.

This Switch Profile pertains to Data Accesses.

Object Access Rights

Use the object access rights to specify user rights to the objects in the Object List.

Authority

Authority represents the action to be taken when a rule is found that matches the data present on a transaction. This Authority value pertains to Object Accesses.

The valid values are:

***OS400** The transaction will be allowed and object authority will be determined by the operating system.
***REJECT** The transaction will not be allowed.
***SWITCH** The transaction will be allowed and the transaction will occur as if the user profile named as the Swap Profile had initiated the transaction. After switching to the Swap Profile, the authority used during the transaction will be determined by the operating system.

Audit Transactions

The Audit transactions flag controls the logging of transactions to the Log Journal set up on the work with Exit Point Manager System Values panel. This Audit Transaction flag pertains to Object Accesses.

The valid values are:

Y The transaction will be logged to the Log Journal.
N The transaction will not be logged to the Log Journal.
* The default value from a prior rule will control the logging.

Send Messages

The Send messages flag controls the sending of messages to the Log Message Queue set up on the work with Exit Point Manager System Values panel.

This Send Messages flag pertains to Object Accesses.

The valid values are:

Y A log message will be sent to the Log Message Queue.
N A log message will not be sent to the Log Message Queue.
* The default value from a prior rule will control the logging.

Capture Transactions

The Capture transactions flag controls whether transactions are remembered in Exit Point Manager for later memorization. Once captured, transactions can become Memorized Transactions which can act as rules. This Send Messages flag pertains to Object Accesses.

The valid values are:

Y A log message will be sent to the Log Message Queue.
N A log message will not be sent to the Log Message Queue.
* The default value from a prior rule will control the logging.

Switch Profile

The Switch profile holds the name of a user profile whose authority is used to process the transaction instead of the authority of the User initiating the transaction. The transaction is executed as, and uses the authority of, this Switch profile. Switch profile is allowed only when Authority contains *SWITCH or *MEMSWITCH, if *MEMSWITCH is allowed. Otherwise it must contain *NONE. This Switch Profile pertains to Object Accesses.

See Specifying the Server/Functions for an Object Rule.

Command Keys

F3 (Exit): Exit the panel without processing any pending changes.

F12 (Cancel): Exit the panel without processing any pending changes.

Location Rule Derivation

```
PNS4315                  Powertech Exit Point Manager                10:05:42
                           Location Rule Derivation                  OSCAR
System: OSCAR     Management System
Server . . . . : DATADIST    Showcase Warehouse Builder Server
Function . . . : *ALL

                                  Active Rule

Level            Authority  Audit Msg Cap Switch    Supplemental Exit
*ALL             *USER        Y     N   N  *NONE      *NONE

                            Location Rule Derivation

Level            Authority  Audit Msg Cap Switch    Supplemental Exit
System           *OS400       Y     N   N  *NONE
Server           *SYSTEM      *     *   *  *NONE      *NONE
*ALL             *USER        *     *   *  *NONE



F3=Exit     F12=Cancel
```

How to Get There

On the Work with Security by Location panel, choose **5** for a Location Rule.

What it Does

The Powertech Location Rule Derivation panel displays the hierarchical inheritance of the current Location rule.

Options

System

System indicates the target of any operations you perform. When you add rules, for example, those rules will be sent to, and will affect processing on, the System named.

Server

The server to which the current rule applies.

Function

The name of the IBM server function to which the current rule applies.

Level

The Level column indicates from which inheritance level the specific values listed are derived.

The last entry in the Rule Derivation section is the level from which the Location Rule Display was requested. For example, if this display were requested from "Work with Authorities by Location", the last level would represent a location.

Valid values are:

System The system values level.
Server The server level.
Function The server function level.
***ALL** The location level for all locations.

Authority
The authority assigned to the user for this rule.

Switch
The Switch profile holds the name of a user profile whose authority is used to process the transaction instead of the authority of the User initiating the transaction. The transaction is executed as, and uses the authority of, this Switch profile.

Switch profile is allowed only when Authority contains *SWITCH or *MEMSWITCH, if *MEMSWITCH is allowed. Otherwise it must contain *NONE.

Audit
The audit property controls the type of requests Exit Point Manager will log.

Possible values are:

Y Log all requests by the location/server/function.
N Only log authority failures for the location/server/function.
* Use the audit value from the prior level.

Msg
The message property entry will determine if Exit Point Manager sends a message to the specified message queue for the user/server/function. Possible values are:

* Use the audit value from the prior level.
Y A message is sent to the specified queue.
N No message is sent.

Cap
Capture transactions for Memorized Transaction Request (MTR).

Possible values are:

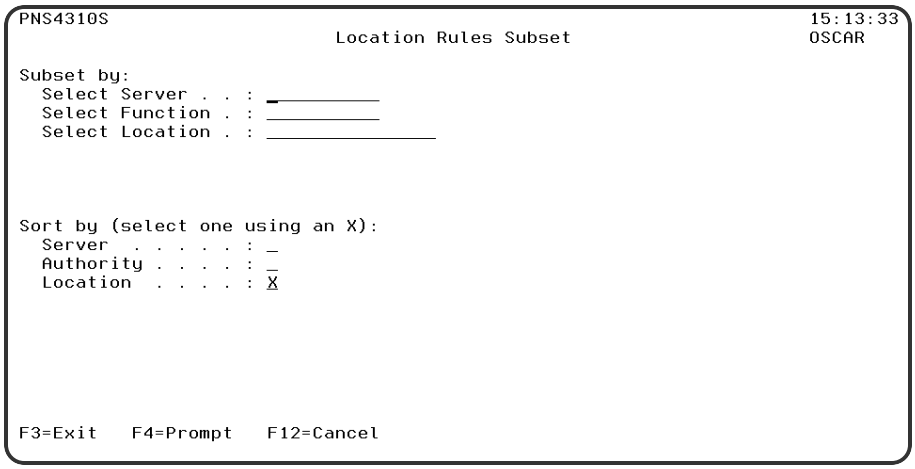
* Use the audit value from the prior level.
Y Capture transactions.
N Do not capture transactions.

Command Keys
F3 (Exit): Exit the program without processing any pending changes.

F5 (Refresh): Refreshes the screen and resets all available text fields.

F12 (Cancel): Exit the screen without processing any pending changes.

Location Rules Subset panel



How to Get There

From the Work with Security by Location panel, press `F16`, Sort/Subset.

What it Does

The Location Rules Subset panel allows you to select Location Rules for display that meet certain criteria. You can select Location Rules by Server, Function, or Location.

Options

Select Server

Specify the criteria for selection by Server name. Leaving this field blank includes all Server values.

You can use the Generic Character to indicate that a partial value is to be used for selection. In some circumstances you may also use the Wildcard Character to indicate that a partial value is to be used for selection. Generic and Wildcard characters can be used at the beginning, end, or within a value and can be freely intermixed (you can use both characters in the same value).

Select Function

Specify the criteria for selection by Function name. Leaving this field blank includes all Function values.

You can use the Generic Character to indicate that a partial value is to be used for selection. In some circumstances you may also use the Wildcard Character to indicate that a partial value is to be used for selection. Generic and Wildcard characters can be used at the beginning, end, or within a value and can be freely intermixed (you can use both characters in the same value).

Select Location

Specify the criteria for selection by Location. Leaving this field blank includes all Location values.

You can use the Generic Character to indicate that a partial value is to be used for selection. In some circumstances you may also use the Wildcard Character to indicate that a partial value is to be used for selection. Generic and Wildcard characters can be used at the beginning, end, or within a value and can be freely intermixed (you can use both characters in the same value).

Sort by (select one using an X):

The Location Rules Subset panel allows you to select Location Rules for that meet certain criteria. You can select a sort by one of the available fields.

Server • Authority • Location

Select whether you would like to sort by Server name, Authority, or Location.

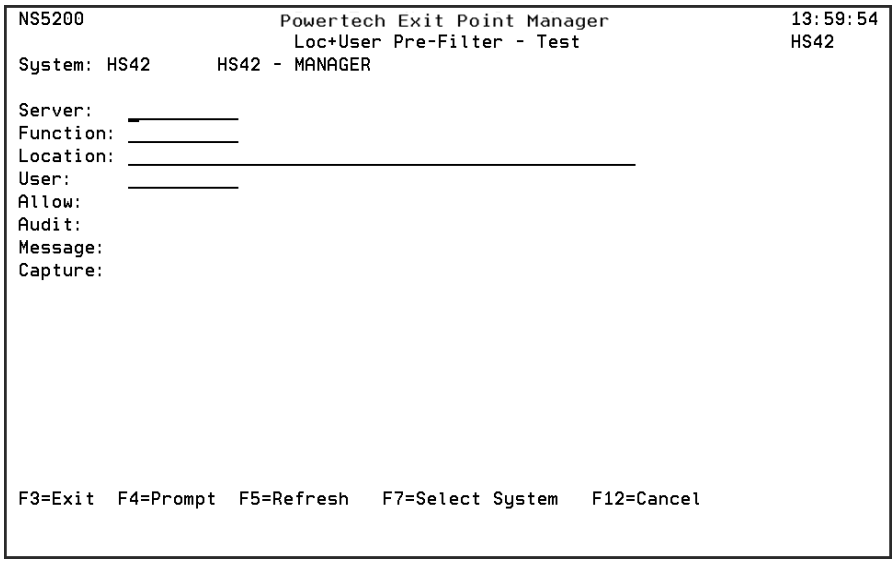
Command Keys

F3 (Exit): Exit the screen without processing any pending changes.

F4 (Prompt): Displays a list of possible values from which you may select one.

F12 (Cancel): Exit the screen without processing any pending changes.

Location + User Pre-filter test



How to Get There

From the Exit Point Manager Main Menu, choose option **6**, Work with Pre-filters. Choose option **3**.

What it Does

The Loc+User Pre-filter test panel allows you to test a server, function, location, and user. It returns the Pre-filter settings of allow, audit, message, and capture as they would be computed had a transaction come into the system with those settings. The exit point is not checked to see if Exit Point Manager is active; this allows you to test without activating a server. This Pre-filter function allows you to specify certain actions for transactions before they are evaluated by the regular Powertech Exit Point Manager rules. The primary action is to allow or not allow a transaction — allowing it causes it to be further evaluated by Exit Point Manager rules; not allowing it is equivalent to a Exit Point Manager reject. The other actions that you can specify are to audit the transaction, send an immediate message, and capture the transaction. These actions work exactly like their equivalents within Exit Point Manager rules processing. The Pre-filter function allows you to specify settings by server, function, location, and user. Records are shipped for a default system setting (this record has a server of *ALL) and for default server settings. These records can be changed but not

deleted. The system record must have either a 'Y' or an 'N' for each of the settings (allow, audit, message, and capture).

The Pre-filter function attempts to match the most specific record to the transaction. Once a match is found, the Pre-filter function processes the transaction based on those settings.

Field Descriptions

Server
The name of the Powertech Exit Point Manager server for this Pre-filter record. You can prompt this field.

Function
The name of the Powertech Exit Point Manager server function for this Pre-filter record. You can prompt this field. If the server field is not already on the screen, it would be prompted for first. A value of *ALL shows on the prompt, but cannot be used for a test transaction.

Location
The location for this Pre-filter record. Valid special values are a Exit Point Manager location group. *ALL is not allowed.

User
The user profile or Exit Point Manager User Group for this Pre-filter record. A group profile is allowed. *PUBLIC is not allowed.

Allow
The returned setting for whether transactions matching this record should be allowed to continue to be processed by Exit Point Manager.

Audit
The returned setting for whether transactions matching this record should have a journal entry written to the journal specified by the Exit Point Manager configuration.

Message
The returned setting for whether transactions matching this record should have a message sent to the message queue specified by the Exit Point Manager configuration.

Capture
The returned setting for whether transactions matching this record should be captured.

Command Keys
F3 (Exit): Exit the screen without processing any pending changes.

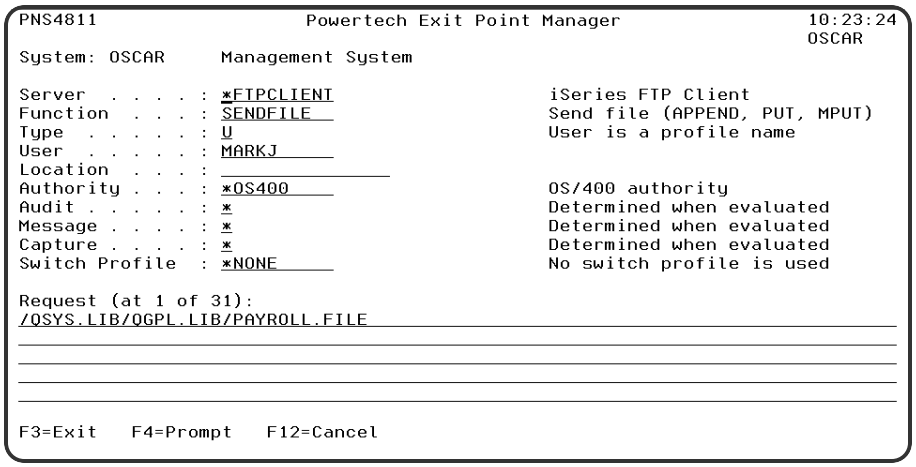
F4 (Prompt): Displays a list of possible values from which you may select one.

F5 (Refresh): Refreshes the screen and resets all available text fields.

F7 (Select System): Use this command key to work with data from a different System.

F12 (Cancel): Exit the screen without processing any pending changes.

Memorize Captured Transaction panel



How to Get There

On the Main Menu, select option **10**. Then, in the Work with Captured Transactions panel, enter a **1** in the Opt column next to the transaction you want to memorize and press `Enter`.

What it Does

The Memorize Captured Transaction panel enables you to memorize a captured transaction and specify the Authority that should be used whenever this transaction is processed in the future.

Field Descriptions

Server

A Server in Exit Point Manager is a controlled entry point into your system. These entry points are determined and defined by IBM. Exit Point Manager has assigned easy-to-remember names to these controlled entry points.

Function

A Function, or Server Function, in Exit Point Manager represents a class of operations that a given Server may perform. For example, the *SIGNON Server classifies its operations as those pertaining to changing passwords, generating authentication tokens, and retrieving sign-on information. Exit Point Manager has assigned easy-to-remember names to these Functions, such as CHGPWD, GENAUTTKN and RETRIEVE.

User Type (USERTYPE)

Specifies whether the user field is a user profile or a Exit Point Manager User Group.

Allowed values are:

U The user field is a user profile.
G The user field is a Exit Point Manager User Group

User

If the associated User Type is a 'U', User represents the identity of the person initiating a transaction as a user profile.

The special value *PUBLIC, when used on a rule, means that the rule applies to any User lacking a specific rule. When used as a subset or selection parameter, *PUBLIC means to select all such rules for display or printing.

If the associated User Type is a 'G', User represents a Exit Point Manager User Group.

Location

Location represents the source of a transaction. Location can hold an IP Address, an IP Address Group or the name of an SNA Communications Device.

The special value *ALL, when used on a rule, means that the rule applies to any Location lacking a specific rule. When used as a subset or selection parameter, *ALL generally means to select all such rules for display or printing. Specify the Location to which this rule applies. Special values are:

***ALL** The rule will apply to all Locations.

Authority

Authority represents the action to be taken when a rule is found that matches the data present on a transaction. Specify the Authority value for the rule. You can press **F4** to see a list of valid values that can be specified. The list of valid values may include one or more of these values:

***USER** Current user authority is used.
***0S400** Exit Point Manager will use normal operating system authority for the user.
***REJECT** Exit Point Manager will reject requests.
***SWITCH** Exit Point Manager will use the authority of the switch profile for the transaction. A switch profile entry is required.
***MEMUSR** Memorized Transactions (MTR) are checked for authority first. If no MTR authority is encountered, Exit Point Manager will use the authority of the current user.
***MEMOS40O** Memorized Transactions (MTR) are checked for authority first. If no MTR authority is encountered, Exit Point Manager will use normal operating system authority for the user.
***MEMREJECT** Memorized Transactions (MTR) are checked for authority first. If no MTR authority is encountered, Exit Point Manager will reject requests for the specified user.
***MEMSWITCH** Memorized Transactions (MTR) are checked for authority first. If no MTR authority is encountered, Exit Point Manager will use the authority of the switch profile for the specified user. A switch profile entry is required.
***MEMOBJ** Memorized Transactions (MTR) are checked for authority first. If no MTR authority is encountered, Exit Point Manager will check any objects used in the transactions for authorities defined by Object Rules.
***SERVER** Exit Point Manager will use the authority defined for the Server.
***SRVFCN** Exit Point Manager will use the authority defined for the Server Function.

Audit Transactions

The Audit transactions flag controls the logging of transactions to the Log Journal set up on the Work with Exit Point Manager System Values panel.

Specify one of these values for Audit transactions:

***DEFAULT** Uses the value found in the rule above this one in the rule hierarchy.
***YES** Logs all requests when this rule is enforced.
***NO** Logs only access failures (rejects) for this rule.

Send messages

The Send messages flag controls the sending of messages to the Log Message Queue set up on the work with Exit Point Manager System Values panel.

Specify one of these values for Send messages:

***DEFAULT** Uses the value found in the rule above this one in the rule hierarchy.
***YES** Sends a message when this rule is enforced.
***NO** Does not send a message when this rule is enforced. Capture transactions

Capture Transactions

The Capture transactions flag controls whether transactions are remembered in Exit Point Manager for later memorization. Once captured, transactions can become Memorized Transactions which can act as rules.

Specify one of these values for Capture transactions:

***DEFAULT** Uses the value found in the rule above this one in the rule hierarchy.
***YES** Captures the transaction when this rule is enforced.
***NO** Does not capture the transaction when this rule is enforced.

Switch profile

The Switch profile holds the name of a user profile whose authority is used to process the transaction instead of the authority of the User initiating the transaction. The transaction is executed as, and uses the authority of, this Switch profile. Switch profile is allowed only when Authority contains *SWITCH or *MEMSWITCH, if *MEMSWITCH is allowed. Otherwise it must contain *NONE.

Specify the new Switch profile value or one of these special values:

***SAME** The Switch profile value on the rule will not be changed.
***NONE** No Switch profile is to be used. This is the only value allowed unless you have specified *SWITCH or *MEMSWITCH for Authority.
***SRVFCN** Use the Switch profile specified for the Server Function.

Transaction

This is the data handed to Exit Point Manager by the operating system. Much of this transaction data is binary in nature and may not be human—readable. Undisplayable characters in the transaction data are replaced by the mid—dot character (-). You can use the Transaction wildcard character (%) to make a Transaction generic. The wildcard character is valid only at the end of a Transaction string. when you are memorizing or changing a Memorized Transaction, the first occurrence of the wildcard character that was NOT present in the string before you changed it will make the string generic and all data after that wildcard character will be discarded.

Command Keys

F3 (Exit): Exit the screen without processing any pending changes.

F4 (Prompt): Displays a list of possible values from which you may select one.

F12 (Cancel): Exit the screen without processing any pending changes.

Merge Data from Prior Version (MRGPRVNS)

```
                  Merge data from prior version (MRGPRVNS)

Type choices, press Enter.

Force run option . . . . . .   *NONE          *NONE, *FORCE
Database conversion options:
  Add missing data . . . . . .   *ADD          *ADD, *NOADD
  Update existing data . . . . .   *UPDATE     *UPDATE, *NOUPDATE
  Delete extra data  . . . . . .   *NODELETE   *DELETE, *NODELETE
Convert reporting users  . . . .   *NO          *YES, *NO

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

How to Get There

Prompt the command MRGPRVNS.

What it Does

The installation program installs Exit Point Manager 7, but does not automatically import information from a previous version. The previous version exit programs remain active, allowing you to continue to use it as you become familiar with version 7 (as long as you do not activate Exit Point Manager 7). Once you've familiarized yourself with Exit Point Manager 7, use the Merge Previous NS (MRGPRVNS) command to merge rules from your previous version to version 7. You should review these rules and make any modifications necessary before activating version 7.

Merging data from a previous version of Exit Point Manager does not automatically activate version 7. You must still run the activation process on Exit Point Manager 7 to start using it. See Reactivating Exit Point Manager After an Upgrade (below).

> **NOTE:** The files PLKCAP, PLKCAPCNT, and LNSCAP can be very large due to extensive data retention, and may extend the duration of the merge as Exit Point Manager converts data to the new data format. To expedite the merge process, we recommend clearing these files using CLRPFM. (These files include captured data that is essentially a duplicate of the Audit data for reporting. Captured transactions can go back years/decades and may not be relevant to current traffic.)

Options

Force Run option

Specifies that certain limitations in the migration are to be bypassed. This is useful if you have performed a migration once, made some changes, and need to run the migration again. Normally, the migration is allowed to be executed only once.

***NONE** This value indicates that no options are being specified. The migration performs normally.

***FORCE** This value indicates that the migration should be allowed to proceed even if it has been run already.

Database conversion options (CVTOPTS)

This parameter contains some settings you may use to limit the amount of data migrated to the new version. This is a multi-part parameter consisting of the following elements:

Add missing data: Specify *ADD to add data to the new version that is in the prior version but is missing from the new version. Specifying *NOADD will not migrate missing data from the prior version.
Update existing data: Specify *UPDATE to update data in the new version that exists in the prior version but is different to that in the prior version. Specifying *NOUPDATE will Leave the data in the new version alone.
Delete extra data Specify *DELETE to remove data from the new version that does not exist in the prior version. Specifying *NODELETE will leave the data in the new version alone.

Convert reporting users (CVTAUTH)

Reporting-only users were registered as members of a particular Authorization List in prior versions. Newer versions of Exit Point Manager employ the internal Product Security functions contained in Central Administration to control access to parts of the software.

***NO** This value indicates that no users will be transferred from the reporting Authorization List.
***YES** This value indicates that the members of the reporting Authorization List named in the CVTAUTL() parameter will be attached to the Product Security Role you name on the CVTROLE() parameter.

Authorization list (CVTAUTL)

Specifies the name of the Authorization list whose member users will be attached to the Role you name in the CVTROLE() parameter.

***VERDFT** This value indicates that the standard reporting Authorization list present in the prior version of the software will be used.
name: Specify the name of a different Authorization list to use.

"Reports-only" Role name (CVTROLE)

Specifies the name of the Product Security Role to which the members of the Authorization list will be attached. You must have already created this Role in Product Security in Central Administration; this command will not create it for you.

name Specify the name of the Product Security Role to which the members of the Authorization list will be attached.

Command Keys

F3 (Exit): Exit the screen without processing any pending changes.

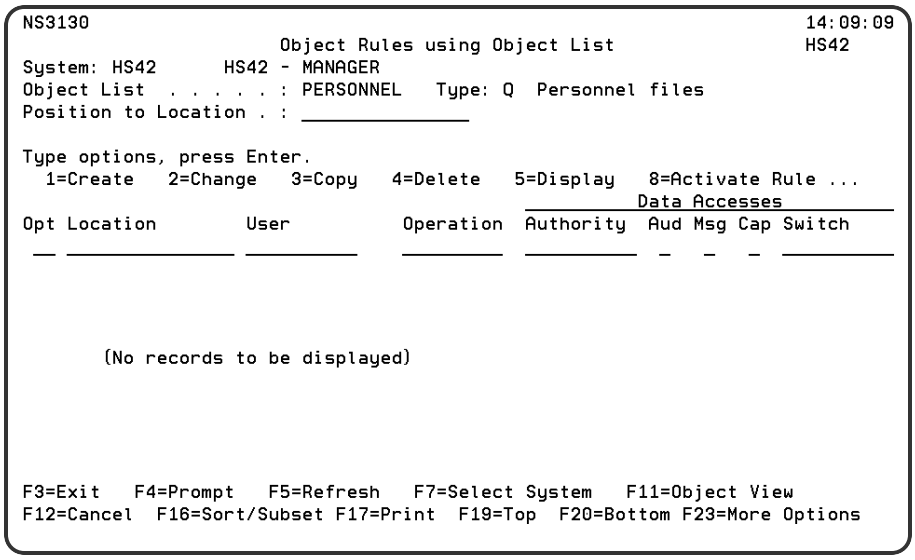
F4 (Prompt): Displays a list of possible values from which you may select one.

F5 (Refresh): Refreshes the screen and resets all available text fields.

F12 (Cancel): Exit the screen without processing any pending changes.

F24 (More keys): Exit the screen without processing any pending changes.

Object Rules using Object List



How to Get There

From the Exit Point Manager Main Menu, select option **4** to display the Work with Security by Object panel. Select option **1** to display the Work with Object Lists panel, then enter an **9** in the Opt column on one of the Object Lists.

Object List

The Object List named at the top of the screen is the Object List to which all the listed rules apply. The Object List name is followed by the Object List Type and description.

What it Does

The Object Rules using Object List panels allow you to work with Object Rules that refer to a single Object List. The Object List is named at the top of the screen. Only rules that refer to the Object List named at the top of the screen are listed. Any new rules that you add from this screen will apply to the Object List named at the top of this screen. Object Rules can be active or inactive. On this panel, the inactive rules are colored yellow and the active rules are colored green.

Options

You can select from the following options on the Work with Object List Entries panel.

1=Create

Enter a 1 next to an object rule to display the Create Object Rule by User panel, which allows you to create an Object Rule linking a User to an Object List. See Create Object Rule by User panel and Create Object Rule by Location panel.

2=Change

Enter a 2 next to an object rule to display the Change Object Rule by User or Change Object Rule by Location panels. Enter the changes you want to make and press `Enter` to display the Select Target Server Functions for Object Rule panels. Select the servers/functions to create a new filter rule. Or, press `Enter` without making a selection if you don't want to create a new filter rule. See Change Object Rule by User panel and Change Object Rule by Location panel.

NOTE: If you don't select any servers/functions, no *MEMOBJ filter rules are created. If no other *MEMOBJ filter rules already exist for the user or location, the object rule is placed in *INACTIVE status. If there are other *MEMOBJ filter rules, the rule remains active.

3=Copy

Enter a 3 next an object rule to display the Copy Object Rule by User or Location panel. You can enter a new user or location name and make other changes to the values specified in the rule. Press `Enter` to display the Select Target Server Functions for Object Rule panels. Select the servers/functions to create a new filter rule. See Copy Object Rule by User panel and Copy Object Rule by Location panel.

NOTE: If you don't select any servers/functions, no *MEMOBJ filter rules are created. If no other *MEMOBJ filter rules already exist for the user or location, the object rule is placed in *INACTIVE status. If there are existing *MEMOBJ filter rules, the rule remains active.

4=Delete

Enter a 4 next to an object rule to delete it. A confirmation screen displays asking you to confirm the deletion. See Deleting an Object Rule for more information.

5=Display

Enter a 5 next to a rule to display the Display Object Rule by User or Location panel. You cannot make any changes on this screen, it is information only. See Display Object Rule by User panel and Display Object Rule by Location panel.

8=Activate Rule

Enter an 8 next to a rule to activate it if it is inactive. A confirmation screen displays asking you to confirm the activation request. The Select Target Server Functions for Object Rule panels display allowing you to define a new filter rule. See Confirm Choices screen.

9=Deactivate Rule

Enter a 9 next to a rule to deactivate it. A confirmation screen displays asking you to confirm the deactivation request. See Confirm Choices screen. If the rule is the last active rule for the user or location, the Specify Filter Rule Options screen displays so you can specify how to handle any *MEMOBJ filter rules that exist for the object rule. See Deleting an Object Rule for more information.

LA=Location Authority

NOTE: This option is not valid for a user rule.

Enter LA next to a location rule to display the Work with Security by Location panel, which shows that the location object rule is now used for the servers/functions you selected. The Authority filter rules property is set to *MEMOBJ for each server/function. This tells Exit Point Manager to check memorized transactions (MTR) for authority. If no MTR authority is found, it then checks the transaction against the object rules.

```
LNSR091                    Powertech Exit Point Manager                  14:23:25
                          Work with Security by Location                 HS42

Subset by Location: 192.168.003.004

                                                  Filter Rule Properties
Location          Server Id  Function   Authority  Aud Msg Cap Switch Profile
_______________   _________  _________  _________  _   _   _   _____________
192.168.003.004   *DATAQSRV  *ALL       *MEMOBJ    *   *   *   *NONE
192.168.003.004   *FILESRV   *ALL       *MEMOBJ    *   *   *   *NONE
192.168.003.004   *FTPCLIENT RECVFILE   *MEMOBJ    *   *   *   *NONE
192.168.003.004   *FTPCLIENT SENDFILE   *MEMOBJ    *   *   *   *NONE
192.168.003.004   *FTPSERVER *ALL       *MEMOBJ    *   *   *   *NONE

                                                                      Bottom
F3=Exit   F4=Prompt   F5=Refresh   F7=Select System   F10=Copy Loc
F17=Top   F18=Bottom  F12=Cancel   F22=Delete User    F24=More keys
```

UA=User Authority

> **NOTE:** This option is not valid for a location rule.

Enter UA next to a user rule to display the Work with Security by User panel, which shows that the user object rule is now used for the servers/functions you selected. The Authority filter rules property is set to *MEMOBJ for each server/function. This tells Exit Point Manager to check memorized transactions (MTR) for authority. If no MTR authority is found, it then checks the transaction against the object rules.

```
LNSR090                                                              16:09:35
                          Work with Security by User                 DEMETER

Subset by User : BOB

                                                  Filter Rule Properties
User          Server ID   Function    Authority   Aud  Msg  Cap  Switch Profile
__________    _________   _________   _________   _    _    _    _____________
BOB           *DATAQSRV   *ALL        *MEMOBJ     *    *    *    *NONE
BOB           *FILESRV    *ALL        *MEMOBJ     *    *    *    *NONE
BOB           *FTPSERVER  CREATELIB   *MEMOBJ     *    *    *    *NONE
BOB           *FTPSERVER  LISTFILES   *MEMOBJ     *    *    *    *NONE
BOB           *FTPSERVER  RECVFILE    *MEMOBJ     *    *    *    *NONE
BOB           *FTPSERVER  SENDFILE    *MEMOBJ     *    *    *    *NONE
BOB           *RMTSRV     *ALL        *MEMOBJ     *    *    *    *NONE
BOB           *SQLSRV     *ALL        *MEMOBJ     *    *    *    *NONE

                                                                      Bottom
F3=Exit   F4=Prompt   F5=Refresh   F10=Copy User   F12=Cancel   F24=More Keys
```

Field Descriptions

Opt

Enter a valid option from the list of options provided on the list panel.

Location

Location represents the source of a transaction. Location can hold an IP Address, an IP Address Group or the name of an SNA Communications Device. The special value *ALL, when used on a rule, means

that the rule applies to any rule means that the rule applies to any Location lacking a specific rule. When used as a subset or selection parameter, *ALL generally means to select all such rules for display or printing.

User

User represents the identity of the person initiating a transaction as a user profile. The special value *PUBLIC, when used on a rule, means that the rule applies to any User lacking a specific rule. When used as a subset or selection parameter, *PUBLIC means to select all such rules for display or printing.

Operation

The operation to which the rule applies.

***ALL** The rule applies to all operations.
***CREATE** The rule applies to attempts to create an object matching an entry defined in the Object List.
***READ** The rule applies to attempts to read an object matching an entry defined in the Object List.
***UPDATE** The rule applies to attempts to update an object matching an entry defined in the Object List.
***DELETE** The rule applies to attempts to delete an object matching an entry defined in the Object List.

Authority

Authority represents the action to be taken when a rule is found that matches the data present on a transaction. This Authority value pertains to Data Accesses.

The valid values are:

***OS400** The transaction will be allowed and object authority will be determined by the operating system.
***REJECT** The transaction will not be allowed.
***SWITCH** The transaction will be allowed and the transaction will occur as if the user profile named as the Swap Profile had initiated the transaction. After switching to the Swap Profile, the authority used during the transaction will be determined by the operating system.

Audit

The Audit flag controls the logging of transactions to the Log Journal set up on the work with Exit Point Manager System Values panel. This Audit flag pertains to Data Accesses.

The valid values are:

Y The transaction will be logged to the Log Journal.
N The transaction will not be logged to the Log Journal.
* The default value from a prior rule will control the logging.

Msg

The Send messages flag controls the sending of messages to the Log Message Queue set up on the Work with Exit Point Manager System Values panel. This Msg flag pertains to Data Accesses.

The valid values are:

Y A log message will be sent to the Log Message Queue.
N A log message will not be sent to the Log Message Queue.
* The default value from a prior rule will control the logging.

Cap
Capture transactions flag controls whether transactions are remembered in Exit Point Manager for later memorization. Once captured, transactions can become Memorized Transactions which can act as rules. This Cap flag pertains to Data Accesses.

The valid values are:

Y A log message will be sent to the Log Message Queue.
N A log message will not be sent to the Log Message Queue.
* The default value from a prior rule will control the logging.

Switch
The Switch profile holds the name of a user profile whose authority is used to process the transaction instead of the authority of the User initiating the transaction. The transaction is executed as, and uses the authority of, this Switch profile. Switch profile is allowed only when Authority contains *SWITCH or *MEMSWITCH, if *MEMSWITCH is allowed. Otherwise it must contain *NONE. This Switch pertains to Data Accesses.

Command Keys
F3 (Exit): Exit the screen without processing any pending changes.

F4 (Prompt): Displays a list of possible values from which you may select one.

F5 (Refresh): Refreshes the screen and resets all available text fields.

F7 (Select System): Use this command key to work with data from a different System.

F11 (Object View/Data Accesses): Use this command key to switch between Object View and Data Accesses.

F12 (Cancel): Exit the screen without processing any pending changes.

F16 (Sort/Subset): Allows you to sort and subset information location, user, and/or operation.

F17 (Print): Prompts the PRTOBJL command to print the list of Object List Entries using your current sort/subset criteria.

F19 (Top): Positions the list screen to the first record.

F20 (Bottom): Positions the list screen to the last record.

F23 (More Options): Displays more options at the top of the screen.

Operational Status panel

How to Get There
Press `F22`.

What it Does
The Operational Status panel allows you to View and perform actions on the operational resources.

Column Descriptions

Opt
Enter a valid option from the list of options provided on the panel.

Module
Shows the name of the software module that published the operational resource.

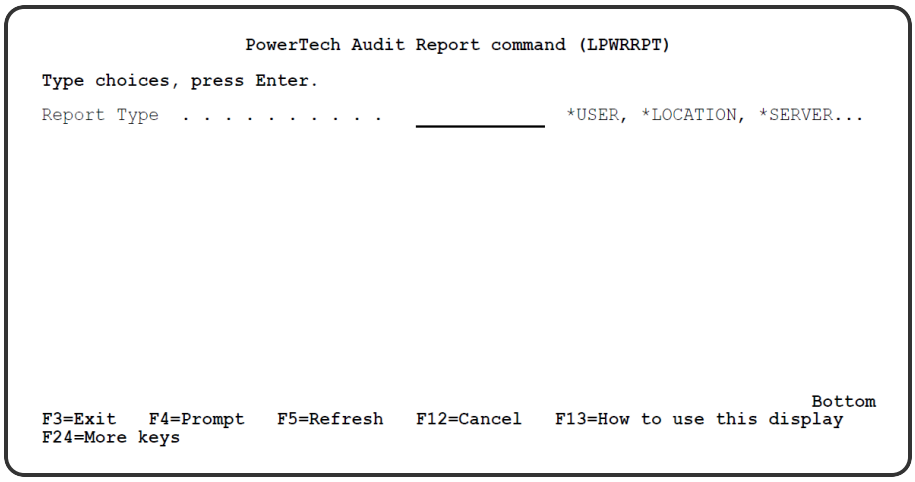
Resource
Shows the name of the operational resource.

Sts
Shows the status for the operational resource.

- **Green:** The resource is active.
- **Red:** The resource is not active.

Powertech Audit Report Command

The LPWRRPT command provides a command-line interface to Exit Point Manager audit reports. This allows scheduling reports through the job scheduler or other scheduling function.



Field Description

Report Type
Specifies the name of the basic report type. This requests a report selecting by user, location, server/function, user group or transaction. This is a required parameter.

The possible values are:

***USER** A report by user should be run.
***LOCATION** A report by location should be run.
***SERVER** A report by server/function should be run.
***GRPPRF** A report by iSeries Group Profile should be run.
***ACCNTCDE** A report by iSeries Account Code should be run.
***PWRLCKGRP** A report by Exit Point Manager Group should be run.

***TRANSACTION** A report by network transaction type should be run.

*USER

Specifies the user profile to run the report over.

This is an optional parameter.

Allowed values are:

***ALL** Print the report including all user profiles.
user ID Enter a valid user profile identifier.

Group (GROUP)

Specifies group (Account Code, Exit Point Manager, Grp Profile) for the report. This is an optional parameter.

Allowed values are:

***ALL** Print the report including all Groups of selected type.
Group ID Enter a valid user Group identifier for selected group type.
***NOGRP** Print the report and do not include records associated with groups.

Location (LOCATION)

Specifies the SNA or TCP/IP location to run the report over. This is an optional parameter.

Allowed values are:

***ALL** Print the report including all locations.
location Enter a valid SNA or TCP/IP location. This can be a location name or a TCP/IP address.

Server (SVR)

Specifies the server to run the report over. This is an optional parameter.

Allowed values for server are:

***ALL** Print the report including all servers.
server-name Enter a valid server name.

Function (FNC)

Specifies the function to run the report over.

This is an optional parameter.

Allowed values for function are:

***ALL** Print the report including all functions.
function-name Enter a valid function name.

Transaction type (TRNTYP)

Specifies the network transaction type to run the report over. This is an optional parameter.

Allowed values are:

***RUN** The report shows requests to run commands and/or programs.
***UPDATE** The report shows requests to update data.
***READ** The report shows requests to read data.
***MODIFY** The report shows requests to modify data.

Journal entry type (JRNTYP)

Specifies the type of journal entry to include in the report.

This is an optional parameter.

Allowed values are:

***ALL** The report includes all Exit Point Manager journal entries.
***ALLOW** The report shows only Exit Point Manager allowed entries.
***REJECT** The report shows only Exit Point Manager rejected entries.

Detail report (DTLREPORT)

Specifies whether a detail—level report is generated.

This is an optional parameter.

Allowed values are:

***NO** A detail—level report will not be generated.
***YES** A detail—level report will be generated.

From date (FRMDAT)

Specifies the beginning date to include in the report when a date range is requested.

This is an optional parameter. This parameter is mutually exclusive with PERIOD.

Allowed values are:

***BEGIN** The report will begin with the oldest transactions in the journal.
***NONE** The from-date is not specified.

> **NOTE:** This is only meaningful when a PERIOD report is requested.

date The report will begin with transactions from (including) this date.

> **NOTE:** If old journal receivers have been deleted, they must be restored if entries are to be included from their dates.

From time (FRMTIM)

Specifies the beginning time to include in the report when a date range is requested. This is an optional parameter. This parameter is mutually exclusive with PERIOD.

Allowed values are:

***BEGIN** The report will begin with transactions in the journal with no time limit.
time The report will begin with transactions from (including) this time.

To date (TODAT)

Specifies the ending date to include in the report when a date range is requested.

This is an optional parameter. This parameter is mutually exclusive with PERIOD.

Allowed values are:

***END** The report will end with the newest transactions in the journal.

***NONE** The to-date is not specified.

> **NOTE:** This is only meaningful when a PERIOD report is requested.

date The report will end with transactions from (including) this date.

To time (TOTIM)

Specifies the ending time to include in the report when a date range is requested. This is an optional parameter. This parameter is mutually exclusive with PERIOD.

Allowed values are:

***END** The report will end with transactions in the journal with no time limit.
time The report will end with transactions up to (including) this time.

Period (PERIOD)

Specifies the period type when a period report is requested. Period reports are intended to be run at regularly scheduled intervals. The available periods are day, week and month. Periods are considered as "prior day", "prior week" and "prior month" and are used to avoid specifying dates for every scheduled run. Use the COUNT parameter to request multiple periods. This is an optional parameter. This parameter is mutually exclusive with FRMDAT and TODAT.

Allowed values are:

***DAY** The report includes entries for the day prior to the run—date of this command.
***WEEK** The report includes entries for the week period prior to the run—date of this command.
***MONTH** The report includes entries for the month period prior to the run—date of this command.

Week start day (STRDAY)

Specifies the starting day for a weekly period report. when a period report is requested and the period type is *WEEK, this specifies the first day of each weekly period. The default is set for Sunday, but any day can be chosen. This allows weekly reports based on the customer definition of a "week". This is an optional parameter. This parameter is meaningful only when period is *WEEK.

Allowed values are:

***SUN** The report includes entries for a week period beginning on Sunday and ending on Saturday.
***MON** The *WEEK report begins on a Monday.
***TUE** The *WEEK report begins on a Tuesday.
***WED** The *WEEK report begins on a Wednesday.
***THU** The *WEEK report begins on a Thursday.
***FRI** The *WEEK report begins on a Friday.
***SAT** The *WEEK report begins on a Saturday.

Period count (COUNT)

Specifies the number of prior periods to include when a period report is requested. This is an optional parameter.

Allowed values are:

1 The report will include a single period.
count The report will include as many periods as are given here.

NOTE: If old journal receivers have been deleted, they must be restored if entries are to be included from their dates. Output type (OUTPUT) Specifies the form of output.

Output type (OUTPUT)

Specifies the form of output.

This requests the output in either printed or database form or in a .CSV streamfile.

This is a required parameter.

The possible values are:

***PRINT** The output should be a printed report.
***OUTFILE** The output should be directed to a database file.
***IFS** The output should be directed to a .CSV streamfile in the IFS. The streamfile will be created in the location identified in the GNUI Report Output control file (PNSGRO).

Create file (CRTFILE)

Specifies whether the output file should be created exist. This is Allowed an optional parameter.

Allowed values are:

***NO** The output file should not be created. The command will fail if the file does not exist.
***YES** The file will be created if it does not exist when the command executes.

IFS report name (RPTNAM)

Specifies the report name of the IFS streamfile. This name is used to log the creation and location of any IFS streamfiles that are created.

The possible values are:

report—name Enter the name of IFS report. This is a report name, not a streamfile name. IFS output is created in the users home directory. This report name identifies report requests.

Output file (OUTFILE)

Specifies the name of the database file that will contain the selected output. The possible values are: database—file—name Enter the name of the database file that will contain the selected output.

The possible library values are:

database—file—name Enter the name of the database file that will contain the selected output. The possible library values are:
***CURLIB** The current library will be used. If you have not assigned a library as the current library, QGPL will be used.
library—name Enter the name of the library where the database file is located.

Output member options (OUTMBR)

Specifies the member name and option when output is directed to a database file.

This is an optional parameter. This is only meaningful when OUTPUT(*OUTFILE) is selected.

Allowed values for member are:

***FIRST** The first (or only) member receives the output.
member-name Enter a valid member name.

Allowed values for option are:

***REPLACE** The member data is replaced by this output.
***ADD** The existing member data is kept and this output is added to the end of the member.

Command Keys

F3 (Exit): Exit the screen without processing any pending changes.

F4 (Prompt): Displays a list of possible values from which you may select one.

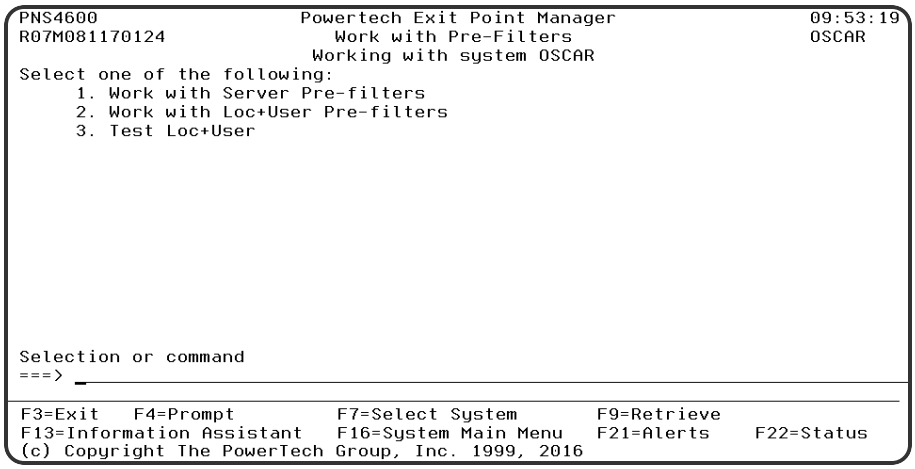
F5 (Refresh): Refreshes the screen and resets all available text fields.

F12 (Cancel): Exit the screen without processing any pending changes.

F13 (How to use this display): Shows help for the prompt display or associated display you are currently using.

F24 (More keys): Shows additional function keys that can be used for this display.

Work with Pre-filters



How to Get There

From the Exit Point Manager Main Menu, select option **6**, Work with Pre-filters.

Options

Option 1 Use this option to work with Server Pre-filters. See Location + User Pre-filter panel.

Option 2 Use this option to work with Pre-filters. See Location + User Pre-filter panel.

Option 3 Use this option to test Pre-filter setup. See Location + User Pre-filter Test panel.

What it Does

The Powertech Exit Point Manager Work with Pre-Filters offers a launchpad for maintaining Exit Point Manager settings and for reporting on Exit Point Manager activities.

The pre-filter functions allow you to specify certain actions for transactions before they are evaluated by the regular Powertech Exit Point Manager rules. The primary action is to allow or not allow a transaction - allowing it causes it to be further evaluated by Exit Point Manager rules; not allowing it is equivalent to a Exit Point Manager reject. The other actions that you can specify are to audit the transaction, send an immediate message, and capture the transaction. These actions work exactly like their equivalents within Exit Point Manager rules processing.

Command Keys

F3 (Exit): Exit the current panel without processing any pending changes.

F4 (Prompt): Provides assistance in entering or selecting a command.

F7 (Select System): Use this command key to work with data from a different System.

F9 (Retrieve): Displays the last command you entered on the command line and any parameters you included. Pressing this key once shows the last command you ran. Pressing this key twice shows the command you ran before that, and so on.

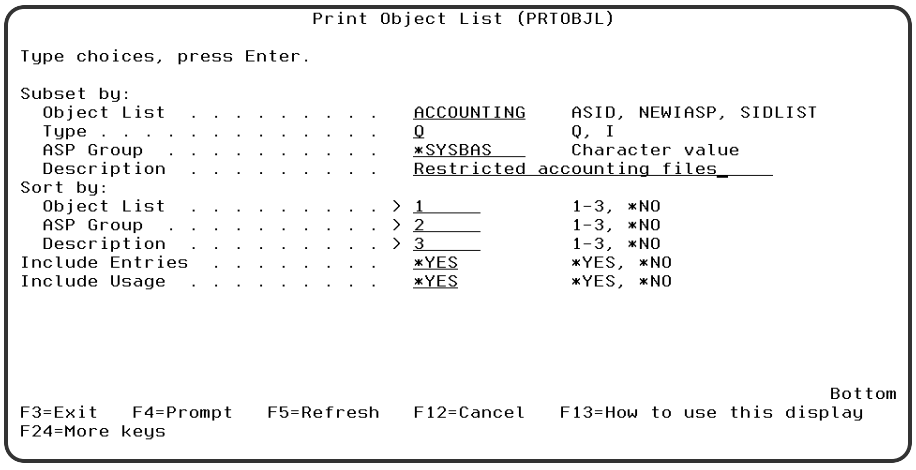
F13 (Information Assistant): Displays the Information Assistant menu with several types of assistance available. Press this key to access more information about the IBM i system.

F16 (System Main Menu): Displays the IBM i Main Menu (MAIN).

F22 (Status): Displays the Operational Resources pop-up window containing the status of several operation aspects of Powertech products.

Print Object List

The Print Object List (PRTOBJL) command allows you to print a listing of the Object Lists you have configured. The Object List Entries can be printed, as well as the Object Rules that protect a given Object List.



Options

Subset by (SUBSET):

This is a multi-part parameter consisting of three elements. If you leave any of the elements blank, the report will not be subset using that element. The elements are:

Object List

Specify criteria to subset by Object List name. You can use the Generic Character to indicate that a partial value is to be used for selection. In some circumstances you may also use the Wildcard Character to indicate that a partial value is to be used for selection.

Type

Specify criteria to subset by Object List Type.

ASP Group

Specify criteria to subset by ASP.

Description

Specify criteria to subset by Object List Description. You can use the Generic Character to indicate that a partial value is to be used for selection. In some circumstances you may also use the Wildcard Character to indicate that a partial value is to be used for selection.

Sort by (SORTBY)

This is a multi-part parameter consisting of three elements. Indicate the order in which you would like the Object Lists to be listed on the report. To omit an element from the sort, specify *NO for that element.

The elements are:

Object List

Specify the sort order for Object List name.

Type

Specify the sort order for Object List Description.

iASP

Specify criteria to subset by iASP.

Description

Specify the sort order for the Object List description.

Include Entries (INCLENT)

Specify if you want to include Object List entries for each Object List in the report. The default value is *YES.

Include Usage (INCLUSG)

> **NOTE:** If you specify *YES for Include Entries and Include Usage, additional fields display allowing you to further sort and subset the information to appear in the report.

Indicate whether you would like the Object List Usage information for each Object list to be printed on the report. If you specify *NO, do not enter any subset or sorting criteria for Object List Usage information.

The valid values are:

***YES** The Object List Usage information is printed on the report.
***NO** The Object List Usage information is not printed on the report.

Object List Entries (ENTRIES)

This is a multi-part parameter consisting of two groups of elements, one for subsetting the report and one for sorting it. This parameter is valid only when INCLENT(*YES) is specified on the command.

The elements are:

Subset by

This is a multi-part parameter consisting of four elements. If you leave any of the elements blank, the report will not be subset using that element.

The elements are:

Library

Specify criteria to subset by Library name. You can use the generic character to indicate that a partial value is to be used for selection. In some circumstances you may also use the wildcard character to indicate that a partial value is to be used for selection. You may specify <UNKNOWN> to select Object List Entries that pertain only to unqualified objects whose library cannot be determined.

Object

Specify criteria to subset by Object name. You can use the generic character to indicate that a partial value is to be used for selection. In some circumstances you may also use the wildcard character to indicate that a partial value is to be used for selection.

Type

Specify criteria to subset by Object Type.

Path

Specify criteria to subset by Path. You can use the generic character to indicate that a partial value is to be used for selection. In some circumstances you may also use the wildcard character to indicate that a partial value is to be used for selection.

Sort by

This is a multi-part parameter consisting of four elements. Indicate the order in which you would like the Object List Entries to be listed on the report. To omit an element from the sort, specify *NO for that element.

The elements are:

Library

Specify the sort order for Library name.

Object

Specify the sort order for Object name.

Type

Specify the sort order for Object Type.

Path

Specify the sort order for Path.

Object List Usage (USAGE)

This is a multi-part parameter consisting of three groups of elements, one for subsetting the report, one for broadly selecting User or Location rules, and one for sorting the report. This parameter is valid only when INCLUSG(*YES) is specified on the command.

The elements are:

Subset by

This is a multi-part parameter consisting of five elements. If you leave any of the elements blank, the report will not be subset using that element.

The elements are:

Location

Specify criteria to subset by Location. Location represents the source of a transaction. Location can hold an IP Address, an IP Address Group or the name of an SNA Communications Device. The special value *ALL, when used on a rule, means that the rule applies to any rule means that the rule applies to any Location lacking a specific rule. when used as a subset or selection parameter, *ALL generally means to select all such rules for display or printing. You can use the Generic Character to indicate that a partial value is to be used for selection. In some circumstances you may also use the wildcard character to indicate that a partial value is to be used for selection.

Style of Location value

When the value you key begins with an asterisk, this element allows you to format your request to find a single IP Address Group or any Location value that ends with the value you keyed (after the asterisk).

Valid values are:

***GROUP** List only rules that have the specified IP Address Group on them.
***ENDSWITH** List rules with any value that ends with the value you keyed.

Operation

Specify criteria to subset by operation.

Show rules for

This is a multi-part parameter consisting of two elements. This parameter allows you to show Object List Usage information listing only Location-based or User-based Object Rules. At least one of these elements must be *YES when you have specified INCLUSG(*YES).

The elements are:

Location

Indicate whether you want Location—based Object Rules to appear in the Usage section of the report. If you have specified subset criteria for Location, this value must be *YES. The valid values are:

***YES** Location—based Object Rules will be included.
***NO** Location—based Object Rules will not be included.

User

Indicate whether you want User—based Object Rules to appear in the Usage section of the report. If you have specified subset criteria for User, this value must be *YES. The valid values are:

***YES** User—based Object Rules will be included.
***NO** User—based Object Rules will not be included.

Sort by

This is a multi-part parameter consisting of three elements. Indicate the order in which you would like the Object List Usage information to be listed on the report. To omit an element from the sort, specify *NO for that element.

The elements are:

Location

Specify the sort order for Location. If you specified *NO for Show rules for Locations then this value must be *NO.

User

Specify the sort order for User. If you specified *NO for Show rules for Users then this value must be *NO.

Operation

Specify the sort order for Operation.

Command Keys

F3 (Exit): Exit the screen without processing any pending changes.

F4 (Prompt): Displays a list of possible values from which you may select one.

F5 (Refresh): Refreshes the screen and resets all available text fields.

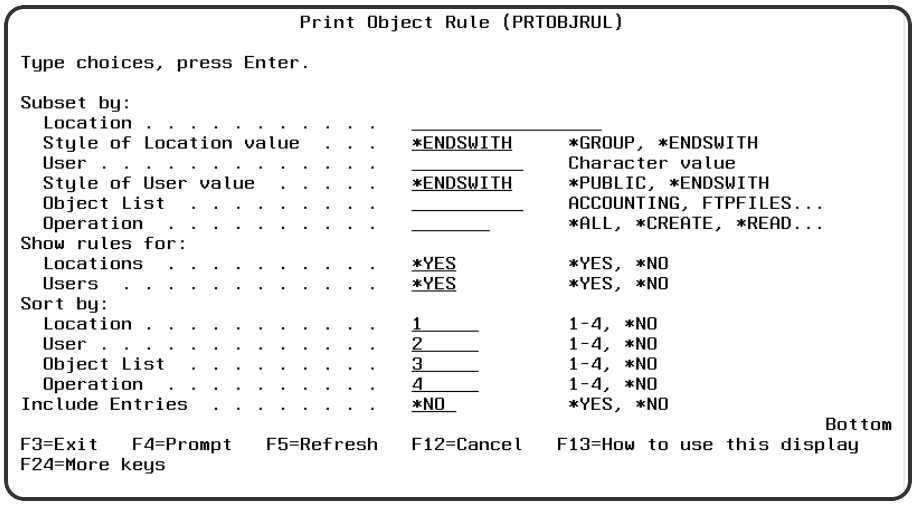
F12 (Cancel): Exit the screen without processing any pending changes.

F13 (How to use this display): Shows help for the prompt display or associated display you are currently using.

F24 (More keys): Shows additional function keys that can be used for this display.

Print Object Rules

The Print Object Rule (PRTOBJRUL) command allows you to print a listing of the Object Rules you have configured. The Object List Entries contained in the Object List named on the rule can also be listed.



Options

Subset by (SUBSET):

Use this parameter to subset the Object Rules printed on the report. This is a multi-part parameter consisting of six elements. If you leave any of the elements blank, the report will not be subset using that element. The elements are:

Location

Specify criteria to subset by Location. Location represents the source of a transaction. Location can hold an IP Address, an IP Address Group or the name of an SNA Communications Device. The special value *ALL, when used on a rule, means that the rule applies to any rule means that the rule applies to any Location lacking a specific rule. when used as a subset or selection parameter, *ALL generally means to select all such rules for display or printing. You can use the generic character to indicate that a partial value is to be used for selection. In some circumstances you may also use the wildcard character to indicate that a partial value is to be used for selection.

Style of Location value

When the value you key begins with an asterisk, this element allows you to format your request to find a single IP Address Group or any Location value that ends with the value you keyed (after the asterisk).

Valid values are:

***GROUP** List only rules that have the specified IP Address Group on them.
***ENDSWITH** List rules with any value that ends with the value you keyed.

User

Specify criteria to subset by User. User represents the identity of the person initiating a transaction as a user profile. The special value *PUBLIC, when used on a rule, means that the rule applies to any User lacking a specific rule. when used as a subset or selection parameter, *PUBLIC means to select all such rules for display or printing.

You can use the generic character to indicate that a partial value is to be used for selection. In some circumstances you may also use the wildcard character to indicate that a partial value is to be used for selection.

Style of User value

When the value you key is *PUBLIC, this element allows you to format your request to find only rules for *PUBLIC or any User value that ends with PUBLIC (like JIMPUBLIC, XPUBLIC, etc).

Valid values are:

***PUBLIC** List only rules that have *PUBLIC as the User value.
***ENDSWITH** List rules with any value that ends with PUBLIC.

Object List

Specify criteria to subset by Object list name. You can use the generic character to indicate that a partial value is to be used for selection. In some circumstances you may also use the wildcard character to indicate that a partial value is to be used for selection.

Operation

Specify criteria to subset by Operation.

Show rules for (SHOWFOR)

Use this parameter to include only Location—based rules or User—based rules in the report. You must select at least one by specifying *YES. This is a multi-part parameter consisting of two elements.

The elements are:

Locations

Indicate whether you want Location—based Object Rules to appear in the report. The valid values are:

***YES** Location—based Object Rules will be included.
***NO** Location—based Object Rules will not be included.

User

Indicate whether you want User—based Object Rules to appear in the report.

The valid values are:

***YES** User—based Object Rules will be included.
***NO** User—based Object Rules will not be included.

Sort by (SORTBY)

Use this parameter to sort the Object Rules printed on the report. Indicate the order in which you would like the Object Rules listed on the report. To omit an element from the sort, specify *NO for that element. Duplicate values are not allowed; you cannot sort more than one field at any given position. This is a multi-part parameter consisting of four elements.

The elements are:

Location

Specify the sort order for Location.

User

Specify the sort order for User.

Object List

Specify the sort order for Object List name.

Operation

Specify the sort order for Operation.

> **NOTE:** If you specify *YES for Include Entries and Include Usage, additional fields display allowing you to further sort and subset the information to appear in the report.

Include Entries (INCLENT)

Indicate whether you would like the Object List Entries for each Object list to be printed on the report. The valid values are:

***YES** The Object List Entries are printed on the report.
***NO** The Object List Entries are not printed on the report.

Object List Entries (ENTRIES)

This is a multi-part parameter consisting of two groups of elements, one for subsetting the report and one for sorting it. This parameter is valid only when INCLENT(*YES) is specified on the command.

The elements are:

Subset by

This is a multi-part parameter consisting of four elements. If you leave any of the elements blank, the report will not be subset using that element.

The elements are:

Library

Specify criteria to subset by Library name. You can use the generic character to indicate that a partial value is to be used for selection. In some circumstances you may also use the wildcard character to indicate that a partial value is to be used for selection. You may specify <UNKNOWN> to select Object List Entries that pertain only to unqualified objects whose library cannot be determined.

Object

Specify criteria to subset by Object name. You can use the generic character to indicate that a partial value is to be used for selection. In some circumstances you may also use the wildcard character to indicate that a partial value is to be used for selection.

Type

Specify criteria to subset by Object Type.

Path

Specify criteria to subset by Path. You can use the generic character to indicate that a partial value is to be used for selection. In some circumstances you may also use the wildcard character to indicate that a partial value is to be used for selection.

Sort by

This is a multi-part parameter consisting of four elements. Indicate the order in which you would like the Object List Entries to be listed on the report. To omit an element from the sort, specify *NO for that element.

The elements are:

Library

Specify the sort order for Library name.

Object

Specify the sort order for Object name.

Type

Specify the sort order for Object Type.

Path

Specify the sort order for Path.

Command Keys

F3 (Exit): Exit the screen without processing any pending changes.

F4 (Prompt): Displays a list of possible values from which you may select one.

F5 (Refresh): Refreshes the screen and resets all available text fields.

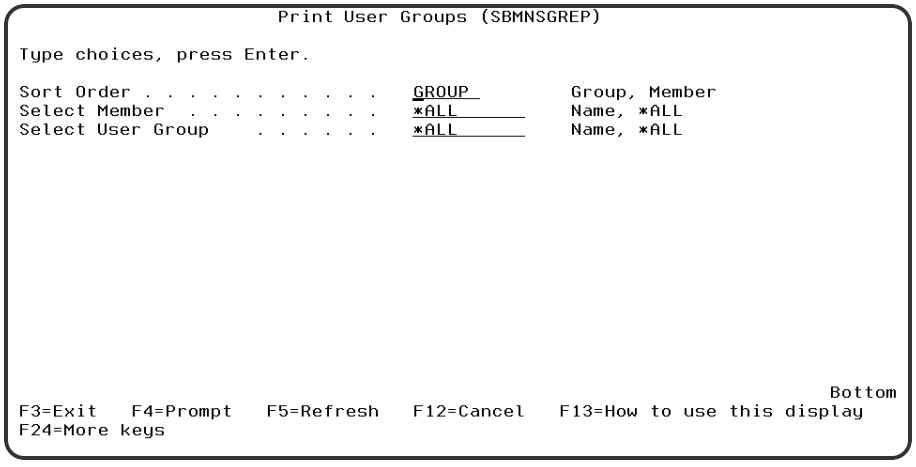
F12 (Cancel): Exit the screen without processing any pending changes.

F13 (How to use this display): Shows help for the prompt display or associated display you are currently using.

F24 (More keys): Shows additional function keys that can be used for this display.

Print User Groups

The User Group Report (SBMNSGREP) command produces the "User Group" report. This report lists User Groups and their members. User Groups Members are user profiles that have been added to User Groups.



Options

Sort Order (SORTORDER)

Specifies whether the report is to print in order of User Groups or by User Group Members.

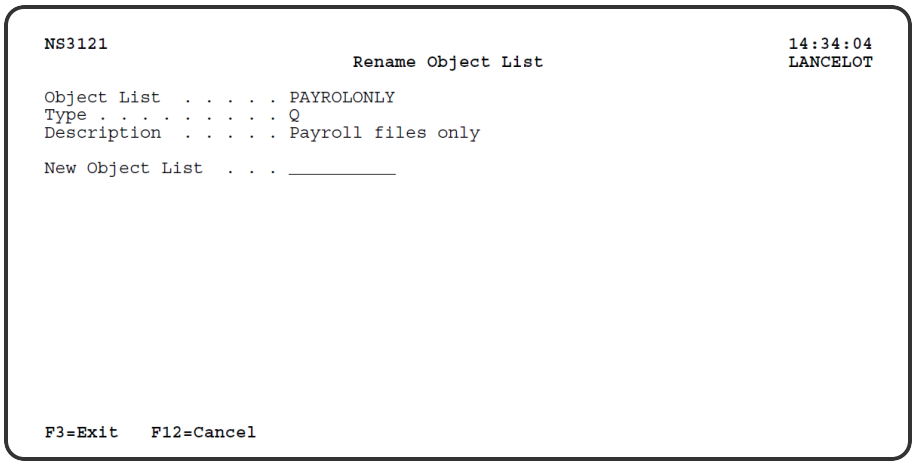
Allowed values are:

GROUP The report is sorted by User Groups
MEMBER The report is sorted by User Group Members.

Select MEMBER (MEMBER)
Allows selection by member name. Only those members that match will print. This will not affect the selection and printing of the User Groups.

Select User Group (GROUP)
Allows selection by User Group. Only those User Groups that match will print. This will not affect the selection and printing of members.

Rename Object List



How to Get There
From the Exit Point Manager Main Menu, select option **4** to display the Work with Security by Object panel. Select option **1** to display the Work with Object Lists panel, then enter an **7** in the Opt column on one of the Object Lists.

What it Does
The Rename Object List panel allows you to change the name of an existing Object List.

Field Descriptions

Object List
The Object List name is a short name you assign to a list of objects to help you identify the list. This name is required to be a valid OS name.

Type
The Object List type determines what type of entries can be added to an Object List. Object lists can hold native object specifications (library, object and type) or paths to IFS objects.

Valid values are:

Q The Object List entries are native object specifiers.

I The Object List entries are paths to IFS objects.

Description
The Object List description is a short textual description of the Object List. It is typically used to indicate the purpose or contents of the Object List.

New Object List
Specify the new name for the Object List.

Command Keys
F3 (Exit): Exit the screen without processing any pending changes.

F12 (Cancel): Exit the screen without processing any pending changes.

Rules Maintenance panel

```
PSSR010                    PowerTech Secure Screen                    09:07:42
                              Rules Maintenance                       HS42
System: HS42      HS42 - MANAGER
Type options, press Enter.
  2=Change  3=Copy   4=Delete   5=Display

Opt Type       Identifier      Mask             Nfy   Action   Log      Drop
 __ *DEVD      BJOHNSON1       255.255.255.255  *MSG  *ENDJOB  *NOLIST  *YES

                                                                        Bottom
F3=Exit     F5=Refresh     F6=Add     F7=Select System     F12=Cancel
F17=Top     F18=Bottom     F20=Position List
```

SecureScreen's Rules Maintenance panel

You can set up rules for using Secure Screen by defining filters. This function maintains the filters file PSSNAP. Filters are applied to jobs that reach an inactive timeout. The action taken depends on the filter that first matches the characteristics of the inactive job.

How to Get There
To display the Rules Maintenance panel, select option **10** from the SecureScreen menu, or enter LEDTPSSFTR in the command line.

What it Does
The Rules Maintenance panel lists all filters you currently have in place, and their values. From the panel, you can add, change, copy, delete, and display filters.

Column Descriptions

Opt
Possible values are:

2=Change The selected filter is to be changed. See the Change a Filter panel

3=Copy The selected filter is to be copied. See the Copy a Filter panel

4=Delete The selected filter is to be deleted

5=Display The selected filter is to be displayed. See the Display a Filter panel

Type

The type of filter. There are six types of filters; possible values are:

***DEVD** Device Description

***SBSD** Subsystem Description

***RMTLOC** Remote Location

***USRPRF** User Profile

***GRPPRF** Group User Profile

***ACGCDE** Accounting Code

Identifier

Specifies the name of a device, subsystem or user, a remote location or an accounting code. A user can be either an individual user profile or a group profile. A location can be either an SNA location or an IP address. An accounting code is used by system job accounting and is normally found as an attribute of a user profile or a job description. Note that accounting codes may also be set dynamically by programs when a job is running. An IP address location should have an IP mask also specified.

Mask

Specifies the subnet mask to apply against an incoming IP address. If the incoming IP address masks to the IP address of the filter, the rule is enforced.

Examples:

IP location: 10.0.1.5

Mask: 255.255.255.255

Matches: 10.0.1.5

IP location: 10.0.1.5

Mask: 255.255.255.0

Matches: 10.0.1.0 thru 10.0.1.255

IP location: 10.0.1.5

Mask: 255.255.255.254

Matches: 10.0.1.4 thru 10.0.1.5

IP location: 10.0.1.5

Mask: 255.255.255.128

Matches: 10.0.1.128 thru 10.0.1.255

> **NOTE:** The last two examples show that the subnet mask must be applied by the monitor program to the filter IP address as well as to the remote location address. Because of this, the mask is applied when the filter is entered, and the masked address is what is actually stored in the filter record.

Notify Administrator

Specifies to send a message to the administrator message queue when the job is inactive. The message queue name comes from the PSSANFYMQ data area.

The possible values are:

***MSG** The inactive message will be copied to the administrator message queue
blank The value is ignored

Action

Specifies the action to take when an identifier is matched.

The possible values are:

***DSCJOB** The job will be disconnected
***ENDJOB** The job will be ended
***MSG** A *break message is sent to the workstation message queue of the inactive job. This is used when all that is wanted is a warning
***IGNORE** No action is taken if a job matches this filter

Log

Specifies the joblog option. This is only meaningful when the action is *DSCJOB.

The possible values are:

***LIST** Print the job log
***NOLIST** Do not print the job log
***N** Use the default from the *DSCJOB command on your system

Drop

Specifies whether or not the connection is to be dropped if the job is disconnected or ended.

The possible values are:

***DEVD** The drop value is taken from the device description
***YES** The connection will be dropped
***NO** The connection will be left available
***N** The default from the *DSCJOB command on your system is used

Command Keys

F3 (Exit): Exit the screen without processing any pending changes.

F5 (Refresh): Refreshes the screen and resets all available text fields.

F6 (Add): Add a new SecureScreen filter.

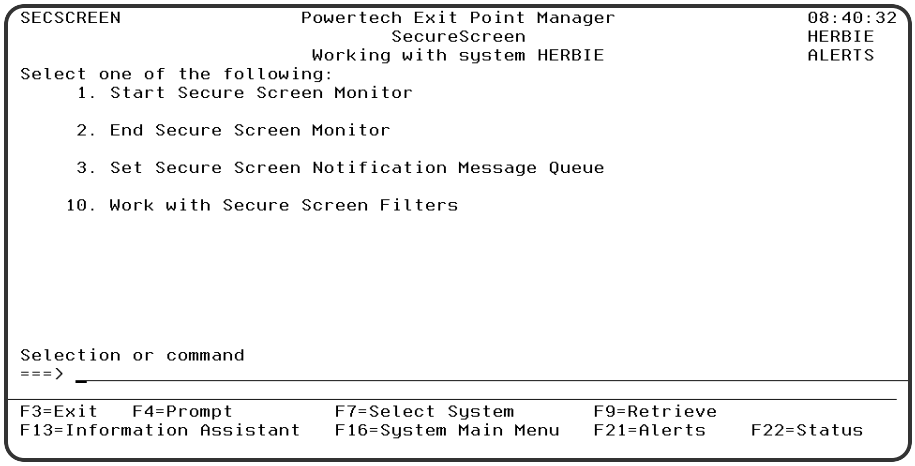
F12 (Cancel): Exit the screen without processing any pending changes.

F17 (Top): Positions the list screen to the first record.

F18 (Bottom): Positions the list screen to the last record.

F20 (Position List):

SecureScreen



How to Get There

To display the SecureScreen menu, select option **1** from the Utilities Menu.

What it Does

The Powertech Exit Point Manager SecureScreen menu offers a launchpad for SecureScreen settings.

SecureScreen Main Menu

You can select the following options from the SecureScreen panel:

1. **Start Secure Screen Monitor:** Select option **1** or use the command (STRPLSSMON) to start the Secure Screen monitor job.
2. **End Secure Screen Monitor:** Select option **2** or use the command (ENDPLSSMON) to end the SecureScreen monitor job.
3. **Set Secure Screen Notification Message Queue:** Select option **3** or use the command (LSETPSSNFQ) to open the Set Secure Screen Notification Message Queue panel. This panel allows you to set the notification message queue for SecureScreen to the message queue you specify on the MSGQ() parameter.

10. **Work with Secure Screen Filters:** Select option **10** to open the Rules Maintenance panel. The Edit Secure Screen filters function maintains the filters file PSSNAP. Filters are applied to jobs that reach an inactive timeout. The action taken depends on the filter that first matches the characteristics of the inactive job.

LCKDSP Command

The LCKDSP command can be used to lock your own screen, or it can be run with a qualified job name to lock some other screen (i.e. it can be run by a monitor program that detects screen inactivity).

It can be used instead of the IBM DSCJOB command. DSCJOB is not allowed if you are using an emulator or pass-through with an automatically assigned workstation ID. LCKDSP can be used anywhere.

To unlock, press Enter and type your password.

There are a limited number of password attempts allowed. If you make too many incorrect attempts, no further attempts will be allowed and you will either have to sign-off using sysreq-90, or you can contact your support desk to unlock you using the UNLDSP command.

You need system value QALWJOBITP = 2 to use this utility.

LCKDSP JOB Command

You can use the LCKDSP JOB(nbr/user/job) to lock some other display. To do so, you need *JOBCTL special authority unless the other job is the same job user.

When a screen is locked, a screen saver is displayed. The screen saver is comprised of a small window that moves to a random position every 5 seconds. Press Enter and enter your password to unlock. If you type the incorrect password enough times (see system value QMAXSIGN), the error "You have used the maximum allowed number of attempts to enter your password." is displayed and the password input field is no longer shown. To recover, either sign-off using Sysreq-90 or get an authorized user to unlock your display using UNLDSP command.

Once you have used up your password attempts, you must sign off and on to get more attempts.

If your display gets locked after you have already used up all your password attempts (see system value QMAXSIGN), you get the usual window and the usual Unlock Display screen when you press Enter, with the password input field showing. But, the password will be ignored even if correct, and the password field will then disappear.

While the display is locked, system request-2,4,5 and 6 are disabled, whether done via the system request menu or directly. All other system request options are allowed. Attention key is also disabled.

UNLDSP Command

You can use the UNLDSP JOB(nbr/user/job) to unlock a display that was locked by the LCKDSP command. You need *ALLOBJ special authority, or specific *USE authority on the command.

> **NOTE:** See Appendix A: Exit Point Manager Commands for additional SecureScreen Commands.

Command Keys

F3 (Exit): Exit the menu.

F4 (Prompt): Provides assistance in entering or selecting a command.

F7 (Select System): Use this command key to work with data from a different System.

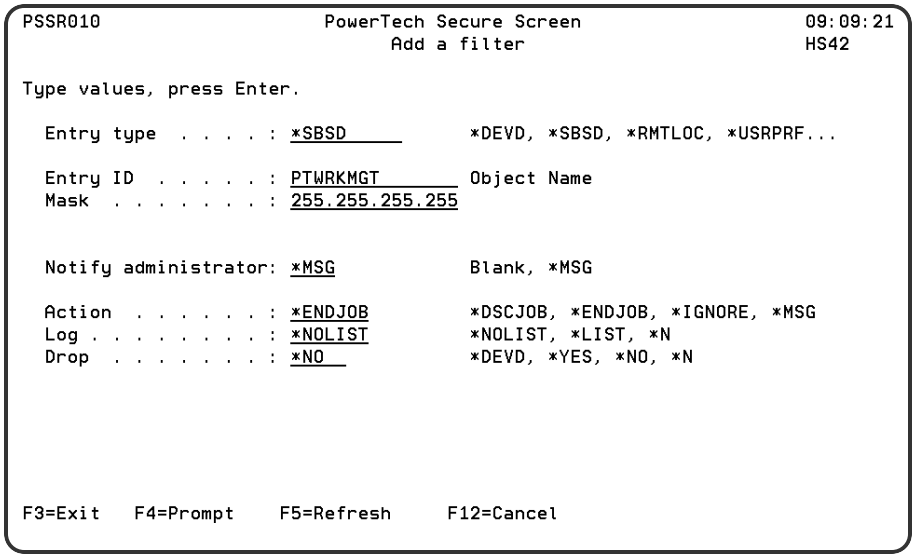
F9 (Retrieve): Displays the last command you entered on the command line and any parameters you included. Pressing this key once shows the last command you ran. Pressing this key twice shows the command you ran before that, and so on.

F13 (Information Assistant): Displays the Information Assistant menu with several types of assistance available. Press this key to access more information about the IMB i system.

F16 (System Main Menu): Displays the IBM i Main Menu (MAIN).

F22 (Status): Displays the Operational Resources pop-up window containing the status of several operation aspects of Powertech products.

SecureScreen: Add a filter



You can set up rules for using Secure Screen by defining filters. This function maintains the filters file PSSNAP. Filters are applied to jobs that reach an inactive timeout. The action taken depends on the filter that first matches the characteristics of the inactive job.

How to Get There

From the Rules Maintenance panel, select `F6`, Add.

What it Does

The Add a Filter panel allows you to create a new filter and specify the filter rules.

Column Descriptions

Enter the following information for the filter:

Entry Type

The type of filter. There are six types of filters; possible values are:

*__DEVD__ Device Description

*__SBSD__ Subsystem Description

*__RMTLOC__ Remote Location

*__USRPRF__ User Profile

*__GRPPRF__ Group User Profile

*__ACGCDE__ Accounting Code

Entry ID

Specifies the name of a device, subsystem or user, a remote location or an accounting code. Press **F4** to select from a list of values. A user can be either an individual user profile or a group profile. A location can be either an SNA location or an IP address. An accounting code is used by system job accounting and is normally found as an attribute of a user profile or a job description. Note that accounting codes mag also be set dynamically by programs when a job is running. An IP address location should have an IP mask also specified.

Mask

Specifies the subnet mask to apply against an incoming IP address. If the incoming IP address masks to the IP address of the filter, the rule is enforced.

Examples:

IP location: 10.0.1.5

Mask: 255.255.255.255

Matches: 10.0.1.5

IP location: 10.0.1.5

Mask: 255.255.255.0

Matches: 10.0.1.0 thru 10.0.1.255

IP location: 10.0.1.5

Mask: 255.255.255.254

Matches: 10.0.1.4 thru 10.0.1.5

IP location: 10.0.1.5

Mask: 255.255.255.128

Matches: 10.0.1.128 thru 10.0.1.255

> **NOTE:** The last two examples show that the subnet mask must be applied by the monitor program to the filter IP address as well as to the remote location address. Because of this, the mask is applied when the filter is entered, and the masked address is what is actually stored in the filter record.

Notify Administrator

Specifies to send a message to the administrator message queue when the job is inactive. The message queue name comes from the PSSANFYMQ data area.

The possible values are:

*__MSG__ The inactive message will be copied to the administrator message queue
blank The value is ignored

Action

Specifies the action to take when an identifier is matched.

The possible values are:

***DSCJOB** The job will be disconnected
***ENDJOB** The job will be ended
***MSG** A *break message is sent to the workstation message queue of the inactive job. This is used when all that is wanted is a warning
***IGNORE** No action is taken if a job matches this filter

Log

Specifies the joblog option. This is only meaningful when the action is *DSCJOB.

The possible values are:

***LIST** Print the job log
***NOLIST** Do not print the job log
***N** Use the default from the *DSCJOB command on your system

Drop

Specifies whether or not the connection is to be dropped if the job is disconnected or ended.

The possible values are:

***DEVD** The drop value is taken from the device description
***YES** The connection will be dropped
***NO** The connection will be left available
***N** The default from the *DSCJOB command on your system is used

Command Keys

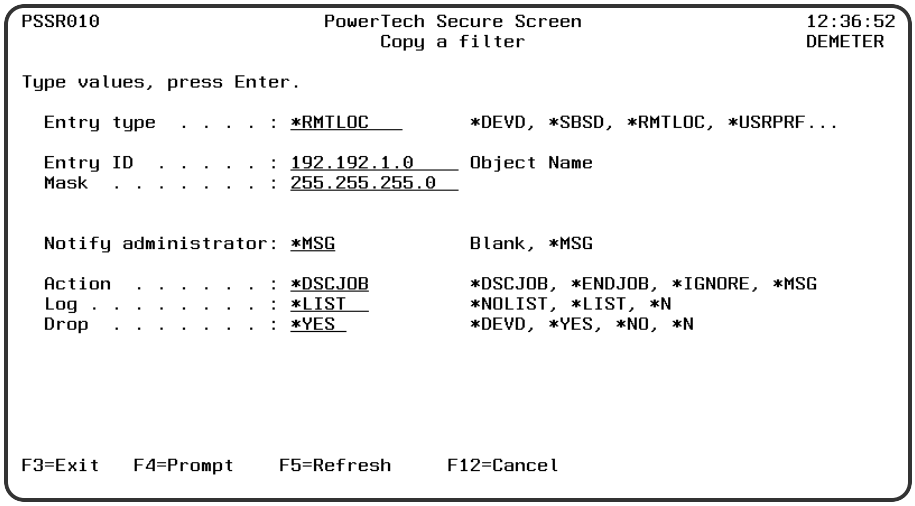
F3 (Exit): Exit the screen without processing any pending changes.

F5 (Refresh): Refreshes the screen and resets all available text fields.

F4 (Prompt): Displays a list of possible values from which you may choose one.

F12 (Cancel): Exit the screen without processing any pending changes.

SecureScreen: Change a filter



How to Get There

From the Rules Maintenance panel, enter option **2** next to a filter, then press `Enter`.

What it Does

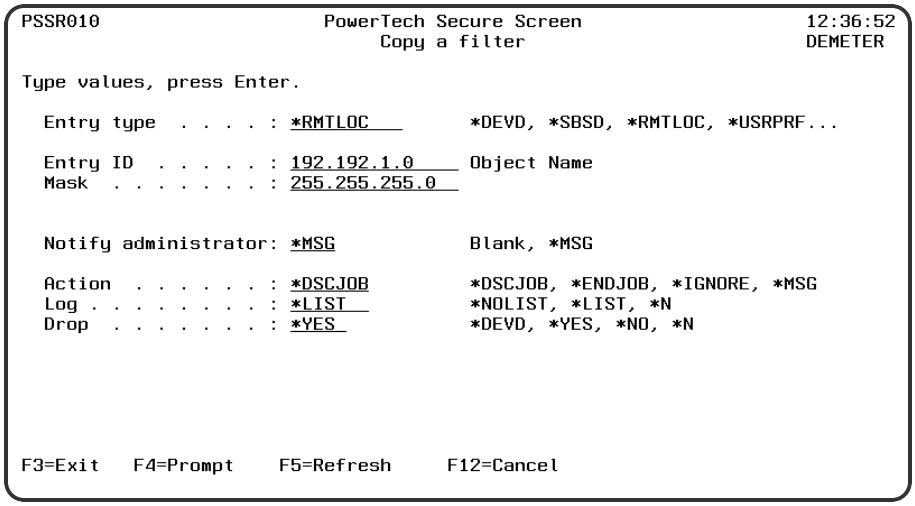
Use the Change a filter screen to change the filter settings. You cannot change the filter Type or Entry ID.

Command Keys

F3 (Exit): Exit the menu.

F12 (Cancel): Exit the screen without processing any pending changes.

SecureScreen: Copy a filter



How to Get There

From the Rules Maintenance panel, enter option **3** next to a filter, then press `Enter`.

What it Does

You can copy an existing filter to copy the filter's settings and modify them to define a new filter.

Command Keys

F3 (Exit): Exit the menu.

F12 (Cancel): Exit the screen without processing any pending changes.

SecureScreen: Display a filter

```
PSSR010                    PowerTech Secure Screen                  12:59:28
                              Display a filter                      DEMETER

Press enter to continue.

  Entry type  . . . . : *RMTLOC
  Entry ID  . . . . . : 192.192.1.0
  Mask  . . . . . . . : 255.255.255.0

  Notify administrator: *MSG

  Action  . . . . . . : *DSCJOB
  Log . . . . . . . . : *LIST
  Drop  . . . . . . . : *YES




F3=Exit   F12=Cancel
```

How to Get There

From the Rules Maintenance panel, enter option **5** next to a filter, then press `Enter`.

What it Does

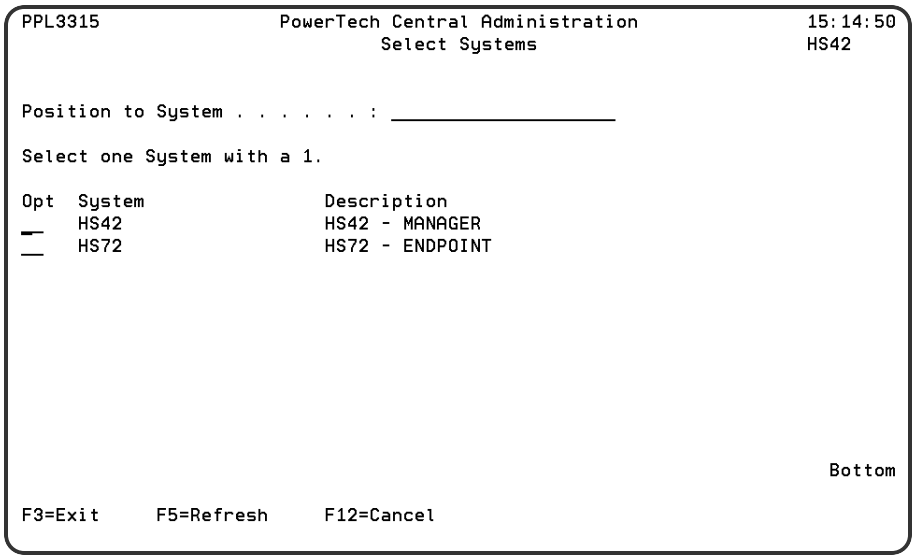
This panel displays the settings for an already-existing filter. Fields on this panel cannot be changed.

Command Keys

F3 (Exit): Exit the menu.

F12 (Cancel): Exit the screen without processing any pending changes.

Select Systems panel



How to Get There

Press F7 (Select System) on any panel that includes this command.

What it Does

The Select Systems panels allow you to select a System. A System represents an installation of an operating system on a piece of hardware.

Column Descriptions

Opt

Enter a valid option from the list of options provided on the panel.

System

System is a name you assign to a System.

Description

Description is a short description of the System.

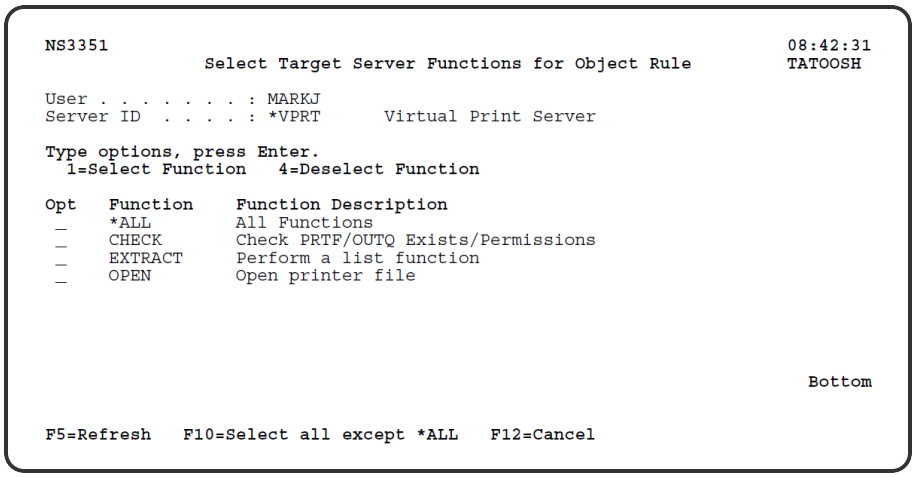
Command Keys

F3 (Exit): Exit the program.

F5 (Refresh): Refreshes the panel with the most current data.

F12 (Cancel): Discards changes and returns to the prior panel.

Select Target Functions for Object Rule



How to Get There

From the Exit Point Manager Main Menu, select option **4** to display the Work with Security by Object panel. Select option **1** to display the Work with Object Lists panel, then enter an **9** in the Opt column on one of the Object Lists. On the Object Rules using Object List panel, enter a **1** in the Opt column and a Location or User name. Press `Enter` to display the Create Object Rule by Location or User panel. Define a rule (see Object Rules) and press `Enter`. Enter option **2** for a server and press `Enter`.

What it Does

This prompt list allows you to specify the target Functions for which Location or User filter rules will be created with *MEMOBJ authority on them. Pressing `F12` discards your changes and returns to the Select Target Servers for Object Rule list.

Options

1=Select Function

Choose option 1 to select target Functions for your Object Rule.

4=Deselect Function

Choose option 4 to deselect a selected Function.

Enter

Pressing Enter without changing anything returns your selections to the Select Target Servers for Object Rule list.

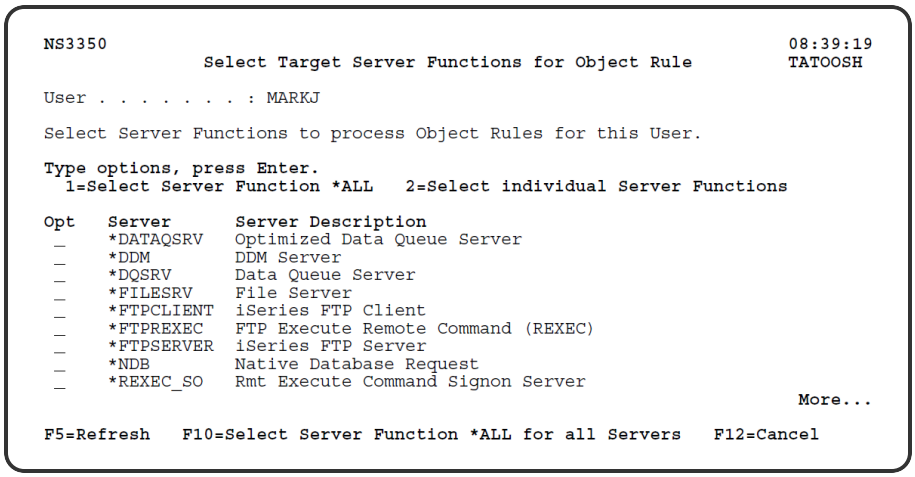
Command Keys

F5 (Refresh): Refreshes the screen and resets all available text fields.

F10 (Select all except *ALL): Selects all individual functions (excluding *ALL).

F12 (Cancel): Exit the screen without processing any pending changes.

Select Target Server Functions for Object Rule



How to Get There

From the Exit Point Manager Main Menu, select option **4** to display the Work with Security by Object panel. Select option **1** to display the Work with Object Lists panel, then enter an **9** in the Opt column on one of the Object Lists. On the Object Rules using Object List panel, enter a **1** in the Opt column and a Location or User name. Press `Enter` to display the Create Object Rule by Location or User panel. Define a rule (see Object Rules) and press `Enter`.

What it Does

This prompt list allows you to specify the target Servers and Functions for which Location or User filter rules will be created with *MEMOBJ authority on them. Select target Servers for your Object Rule from the list of selections provided.

Options

1=Select Server Function *ALL

Choose option 1 to select a Server with Function *ALL.

2=Select individual Server Functions

Choose option 2 to select individual Server Functions.

Enter

Pressing Enter without changing anything returns your selections to the Object Rule processing routine. That routine will use your selections to distribute Location or User filter rules.

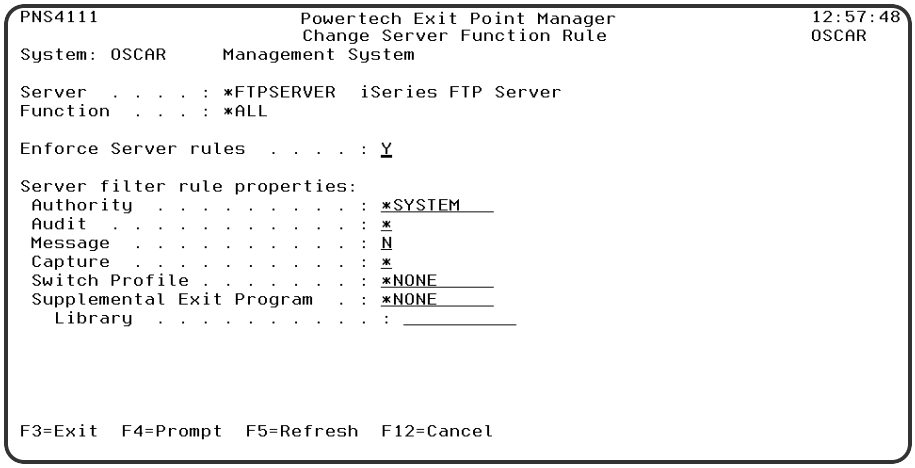
Command Keys

F5 (Refresh): Refreshes the screen and resets all available text fields.

F10 (Select Server Function *ALL for all Servers):Selects Function *ALL for each Server and deselects all other Functions.

F12 (Cancel): Exit the screen without processing any pending changes.

Change Server Function Rule panel



How to Get There

From the Exit Point Manager Main Menu, select option **1**, Work with Security by Server. Under the Options column, type **SP** for a server and press `Enter` to access the Change Server Function Rule panel.

What it Does

The Change Server Function Rule panel allows you to change one or more of the properties for a selected server. To change a server property, type over the existing value and press `Enter`. Server Function Rules provide processing control to Powertech's exit programs and also act as defaults for server function values.

Options

You can enter the following values in the Change Server Function Rule panel. The server name and description display at the top of the window and cannot be changed.

Exit Point Manager rules enforced?

The Powertech rules defined for this server are enforced. (This value is referenced under the "Rules Active" column in the Work with Security by Server panel. This value is referenced under the "Rules Active" column of the Product Configuration panel in the Insite web UI.)

Possible values are:

Y Enter Y to activate the Powertech rules defined for this server.
N Enter N if you don't want to activate the Powertech rules for this server.

Authority

The authority assigned to the server. The value you enter is used when *SERVER authority is placed on a server function.

Possible values are:

***SYSTEM** Use the authority defined for the system.
***OS400** Allow the transaction without taking any action.
***REJECT** Reject all requests for the transaction.

***SWITCH** Switch the job to run as the user profile specified in the switch profile field. A switch profile entry is required.
***MEMOS400** Check Memorized Transactions (MTR) for authority. If no MTR authority is found, allow the transaction.
***MEMREJECT** Check Memorized Transactions (MTR) for authority. If no MTR authority is found, reject requests for the server.
***MEMSWITCH** Check Memorized Transactions (MTR) for authority. If no MTR authority is found, use the authority of the switch profile for the server. A switch profile entry is required.
***MEMOBJ** Check Memorized Transactions (MTR) for authority. If no MTR authority is found, check the transaction against the object rules.

Audit

Controls the type of requests Exit Point Manager will log.

Possible values are:

Y Log all requests to the server.
N Log only authority failures for the server.
* Use the default system value for the system.

Send message on rejected request

Specifies if Exit Point Manager sends a message to the message queue specified in Powertech's System Values.

Possible values are:

Y A message is sent to the specified queue.
N No message is sent.
* Use the default system value for the system.

Capture Transactions

Capture transactions for Memorized Transaction Request (MTR).

Possible values are:

Y Capture transactions.
N Do not capture transactions.
* Use the default system value for the system.

Switch Profile

The name of a switch profile for this server. If you enter a profile name, processing is swapped to run under this profile's authority. This is only valid for authorities *SWITCH and *MEMSWITCH.

Possible values are:

***NONE** No switch profile is being used.

switch-profile The switch profile to process under. It must be an active profile on the IBM i system.

***SYSTEM** Use the switch profile defined for the system.

Supplemental Exit Program

The exit program to run after Powertech's exit program has processed a request successfully. The supplemental exit program is called only for authorities *OS400, *MEMOS400, *SWITCH, and

*MEMSWITCH if the transaction has not been rejected by Exit Point Manager rules. Exit Point Manager's rules must be enforced for a supplemental exit program to run.

Possible values are:

***NONE** No supplemental exit program is to run.

exit-program-name The name of the supplemental exit program to run after Powertech's exit program completes normally. It must be a valid object name and exist on the IBM i system.

Library

Enter the name of the library where the supplemental exit program is found. It must be a valid object name and exist on the IBM i system.

Command Keys

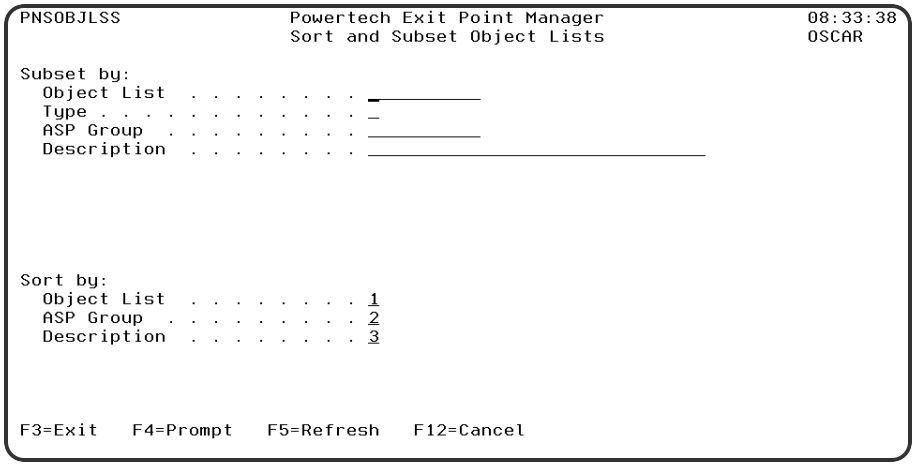
F3 (Exit): Exit the program without processing any pending changes.

F4 (Prompt): Displays a list of values from which you may select one.

F5 (Refresh): Refreshes the panel and resets all available text fields.

F12 (Cancel): Exit the panel without processing any pending changes.

Sort and Subset Object Lists panel



How to Get There

From the Work with Object Lists panel, press `F16`, Sort/Subset.

What it Does

You can subset Object Lists by name, type, or description.

Field Descriptions

Object List

Enter an Object List name. Leave the field blank to include all Object Lists. You can enter a generic name, for example, ACCT*, to include all Object Lists that start with those characters.

Type
Specify the type of Object List to display. Valid values are:

Q Display only Object Lists of type QSYS, which contain library objects.
I Display only Object Lists of type IFS, which contain IFS directory path names.

Description
Specify a description. Leave the field blank to include all descriptions. You can enter generic characters to include all descriptions that contain the specified characters.

Specify the order in which to sort the Object Lists. The default order is to sort by Object List, then description. Leave a selection blank if you don't want it to apply to the sort criteria.

The Sort and Subset selections panel allows you to change which records are displayed on the prior panel, and in which order they are displayed. Selection is performed by making entries in the "Select by" section. Sorting is accomplished by specifying a sort order in the "Order by" section.

Command Keys
F3 (Exit): Exit the panel without processing any pending changes.

F4 (Prompt): Displays a list of possible values from which you may select one.

F5 (Refresh): Refreshes the panel and resets all available text fields.

F12 (Cancel): Exit the panel without processing any pending changes.

Sort and Subset Object List Entries panel

```
NSOBJESS                                                        08:30:19
                    Sort and Subset Object List Entries         TATOOSH

Subset by:
  Library  . . . . . . . . . . . __________
  Object . . . . . . . . . . . . __________
  Type . . . . . . . . . . . . . _______




Sort by:
  Library  . . . . . . . . . . . 1
  Object . . . . . . . . . . . . 2
  Type . . . . . . . . . . . . . 3



F3=Exit    F4=Prompt    F5=Refresh    F12=Cancel
```

What it Does
You can subset Q-type Object List entries by library, object, and type.

Field Descriptions

Library
Enter a library name. Leave the field blank to include all libraries. You can enter a generic name to include all libraries that contain the specified characters.

Enter <UNKNOWN> in the library field to indicate that the Object List entry applies only to unqualified objects whose library cannot be determined by Exit Point Manager. This most commonly occurs in the SQL server when SQL statements contain unqualified references.

Object

Specify an object name. Leave the field blank to include all objects. You can enter generic characters to include all objects that contain the specified characters.

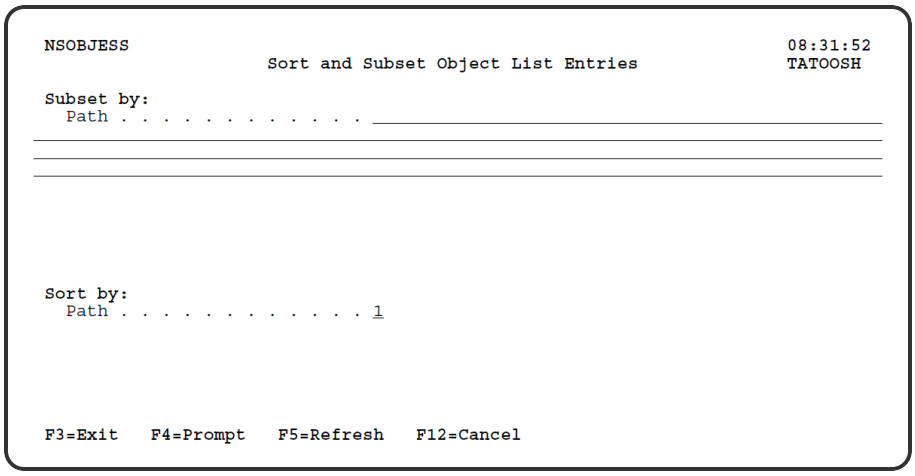
Type

Specify the type of object to display. Leave the field blank to include all object types.

Specify the order in which to sort the Object List entries. The default order is to sort by library, then object, then type. Leave a selection blank if you don't want it to apply to the sort criteria.

Sorting I-Type Object List Entries

You can also subset I-type Object List entries by path name.



Path

Enter a path name to display only the Object List entries in the specified directory path. Object list entries are sorted by path name. You can enter generic or wildcard characters for the path name.

Command Keys

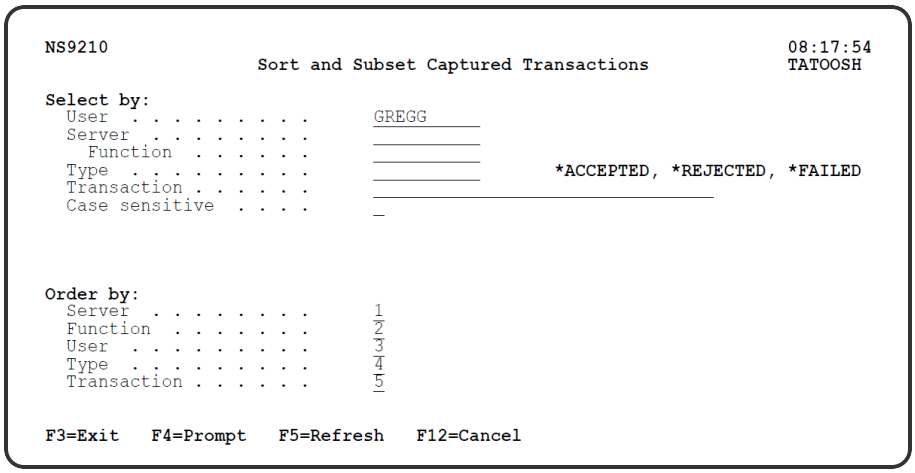
F3 (Exit): Exit the screen without processing any pending changes.

F4 (Prompt): Displays a list of possible values from which you may select one.

F5 (Refresh): Refreshes the screen and resets all available text fields.

F12 (Cancel): Exit the screen without processing any pending changes.

Captured Transactions Subset



How to Get There

On the Main Menu, select option **10**. In the Work with Captured Transactions panel, type `F16`.

What it Does

The Captured Transactions Subset screen allows you to change which records are displayed on the prior screen, and in which order they are displayed. Selection is performed by making entries in the "Select by" section. Sorting is accomplished by specifying a sort order in the "Order by" section.

Field Descriptions

Subset by:

User

User represents the identity of the person initiating a transaction as a user profile. The special value *PUBLIC, when used on a rule, means that the rule applies to any User lacking a specific rule. when used as a subset or selection parameter, *PUBLIC means to select all such rules for display or printing. Select the user profile for which you wish to see records. Leave this field blank if you wish to see all users.

Server

Select the Server for which you wish to see records. Leave this field blank if you wish to see all servers.

Function

Select the Function for which you wish to see records. Leave this field blank if you wish to see all functions.

Location

Select the Location for which you wish to see records. Leave this field blank if you wish to see all functions.

Type

If the associated User Type is a 'U', User represents the identity of the person initiating a transaction as a user profile.

The special value *PUBLIC, when used on a rule, means that the rule applies to any User lacking a specific rule. When used as a subset or selection parameter, *PUBLIC means to select all such rules for display or printing.

If the associated User Type is a 'G', User represents a Exit Point Manager User Group.

Transaction

You may select captured transactions by entering the value of the transaction in this field. Leave this field blank if you wish to see all transactions. The Memorized Transaction against which incoming transactions are tested. If a match is found, then this rule will be invoked. Undisplayable characters in the transaction data are replaced by the mid-dot character (-). You can use the Transaction wildcard character (%) to make a Transaction generic. The wildcard character is valid only at the end of a Transaction string. when you are memorizing or changing a Memorized Transaction, the first occurrence of the wildcard character that was NOT present in the string before you changed it will make the string generic and all data after that wildcard character will be discarded. F4 is not available.

Case sensitive

Selecting 'Y' for this field selects the transaction field in a case—sensitive manner. Selecting 'N' (or leaving this field blank) will select in a non—case—sensitive manner. F4 is not available.

Sort by (select one using an X):

Server
User
Location
Status
Authority
Request

Command Keys

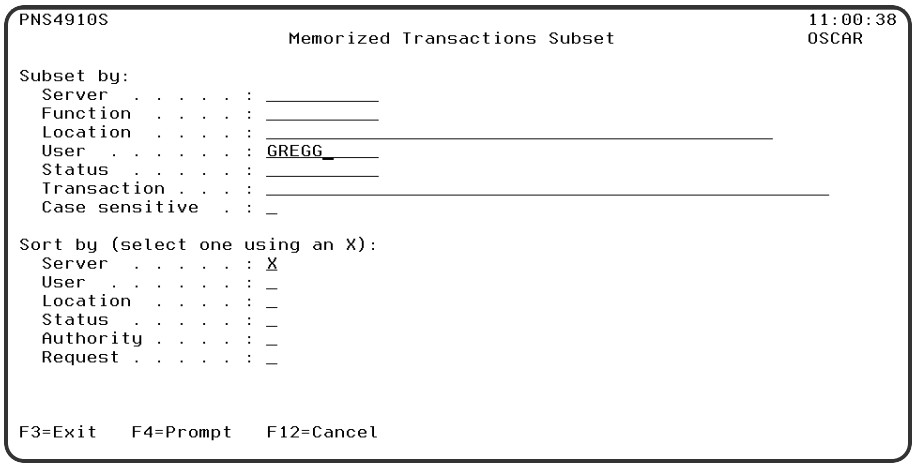
F3 (Exit): Exit the screen without processing any pending changes.

F4 (Prompt): Displays a list of possible values from which you may select one.

F5 (Refresh): Refreshes the screen and resets all available text fields.

F12 (Cancel): Exit the screen without processing any pending changes.

Memorized Transactions Subset



How to Get There

On the Main Menu, select option **11**. In the Work with Memorized Transactions panel, type `F16`.

What it Does

The Sort and Subset selections panel allows you to change which records are displayed on the prior panel, and in which order they are displayed. Selection is performed by making entries in the "Select by" section. Sorting is accomplished by specifying a sort order in the "Order by" section.

Field Descriptions

Subset by:

Server

A Server in Exit Point Manager is a controlled entry point into your system. These entry points are determined and defined by IBM. Exit Point Manager has assigned easy-to-remember names to these controlled entry points.

Function

A Function, or Server Function, in Exit Point Manager represents a class of operations that a given Server may perform. For example, the *SIGNON Server classifies its operations as those pertaining to changing passwords, generating authentication tokens, and retrieving signon information. Exit Point Manager has assigned easy-to-remember names to these Functions, such as CHGPWD, GENAUTTKN and RETRIEVE.

Location

Location represents the source of a transaction. Location can hold an IP Address, an IP Address Group or the name of an SNA Communications Device.

The special value *ALL, when used on a rule, means that the rule applies to any Location lacking a specific rule. When used as a subset or selection parameter, *ALL generally means to select all such rules for display or printing.

User

If the associated User Type is a 'U', User represents the identity of the person initiating a transaction as a user profile.

The special value *PUBLIC, when used on a rule, means that the rule applies to any User lacking a specific rule. When used as a subset or selection parameter, *PUBLIC means to select all such rules for display or printing.

If the associated User Type is a 'G', User represents a Exit Point Manager User Group.

Status

This is the status of the Memorized Transaction.

Possible values are:

***ACTIVE** Exit Point Manager will attempt to match this transaction during rule enforcement. Memorized Transactions that are changed to *ACTIVE will have a matching User or Location rule changed to the corresponding action; *ALLOW to *MEMOS400, *REJECT to *MEMREJECT, or *SWITCH to *MEMSWITCH.
***INACTIVE** Exit Point Manager will not attempt to match this transaction during rule enforcement. Memorized Transactions that are changed to *INACTIVE will have the matching User or Location rule changed (if there are no other Memorized Transactions for that rule) to the corresponding action; *MEMOS400 to *ALLOW, *MEMREJECT to *REJECT, or *MEMSWITCH to *SWITCH.

Transaction

The Memorized Transaction against which incoming transactions are tested.

Undisplayable characters in the transaction data are replaced by the mid-dot character (·).

You can use the Transaction wildcard character (%) to make a Transaction generic. The wildcard character is valid only at the end of a Transaction string. When you are memorizing or changing a Memorized Transaction, the first occurrence of the wildcard character that was NOT present in the string before you changed it will make the string generic and all data after that wildcard character will be discarded.

Case sensitive

This controls whether the selection by transactions is case-sensitive. If left blank, 'N' is assumed.

Possible values are:

Y The search will be case-sensitive.
N The search will not be case-sensitive.

Sort by (select one using an X):

Server
User
Location
Status
Authority
Request

Command Keys

F3 (Exit): Exit the screen without processing any pending changes.

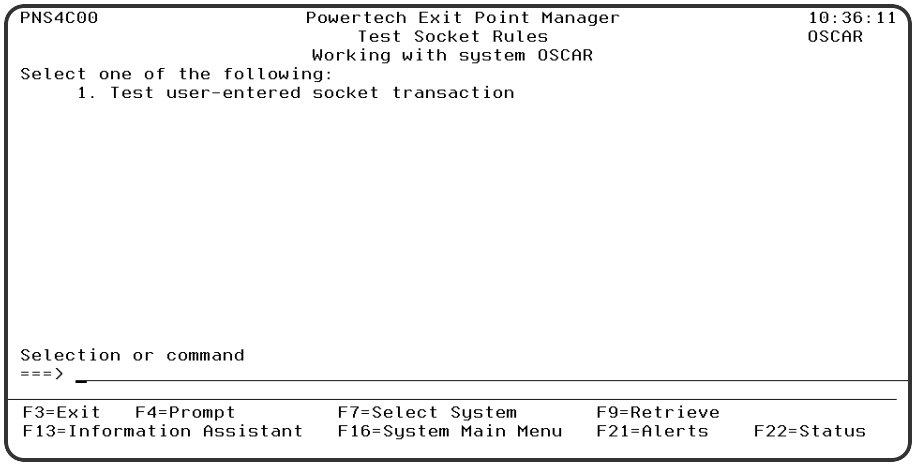
F4 (Prompt): Displays a list of possible values from which you may select one.

F5 (Refresh): Refreshes the screen and resets all available text fields.

F12 (Cancel): Exit the screen without processing any pending changes.

Test Socket Rules panel

WARNING: Misuse of Socket Rules can render your system unreachable via TCP. Exercise extreme caution when using this feature. Consider adding Socket Rules as not active and testing them using the Socket Rule test feature, and setting them to be not used by that feature and testing the rule set before removing them. If you render your system unreachable via TCP, you will need to access the system via the console in order to fix the rules (or to deactivate the Socket Rule servers).



How to Get There

On the Exit Point Manager Main Menu, choose option **20**, then choose option **4**.

What it Does

The Test Socket Rules menu offers a launchpad for testing Socket Rules.

Options

1. Test user-entered socket transaction. This option allows you to test user-entered socket transactions via the command PNSTSTQSO. See Test Socket Rules command (PNSTSTQSO).

Command Line

To run a command, type the command and press Enter. For assistance in selecting a command, press F4 (Prompt) without typing anything. For assistance in entering a command, type the command and press F4 (Prompt). To see a previous command you entered, press F9 (Retrieve).

Command Keys

F3 (Exit): Exit the current panel without processing any pending changes.

F4 (Prompt): Provides assistance in entering or selecting a command.

F7 (Select System): Use this command key to work with data from a different System.

F9 (Retrieve): Displays the last command you entered on the command line and any parameters you included. Pressing this key once shows the last command you ran. Pressing this key twice shows the command you ran before that, and so on.

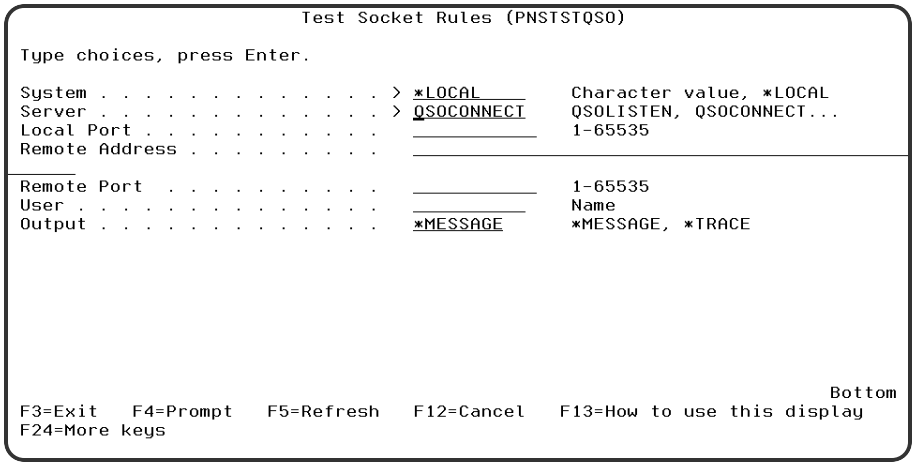
F13 (Information Assistant): Displays the Information Assistant menu with several types of assistance available. Press this key to access more information about the IBM i system.

F16 (System Main Menu): Displays the IBM i Main Menu (MAIN).

F22 (Status): Displays the Operational Resources pop-up window containing the status of several operation aspects of Powertech products.

Test Socket Rules command

WARNING: Misuse of Socket Rules can render your system unreachable via TCP. Exercise extreme caution when using this feature. Consider adding Socket Rules as not active and testing them using the Socket Rule test feature, and setting them to be not used by that feature and testing the rule set before removing them. If you render your system unreachable via TCP, you will need to access the system via the console in order to fix the rules (or to deactivate the Socket Rule servers).



How to Get There

On the Test Socket Rules panel, choose option **1**. Or, run command PNSTSTQSO.

What it Does

The Test Socket Rules (PNSTSTQSO) command allows you to see how a transaction would be evaluated by Exit Point Manager.

NOTE: Restrictions: You must have authority to process the command.

Options

System
The name of the system silo for which you want to test the rules.

You can use the special value *LOCAL for the system on which you are running this test.

Server
The name of the Server for which you wish to test rules. Valid values are:

QSOLISTEN The server that handles listen().
QSOCONNECT The server that handles connect().
QSOACCEPT The server that handles accept().

Local Port (LPORT1)
A valid local port for QSOLISTEN.

Local Port (CPORT1)
A valid local port for QSOCONNECT.

Remote Address (CADDR2)
A valid remote IP address for QSOCONNECT.

Remote Port (CPORT2)
A valid remote port for QSOCONNECT.

Local Bound Port (APORT1)
A valid bound port for QSOACCEPT.

Local Incoming Port (APORT2)
A valid incoming port for QSOACCEPT.

Remote Address (AADDR3)
A valid remote IP address for QSOACCEPT.

Remote Port (APORT3)
A valid remote port for QSOACCEPT.

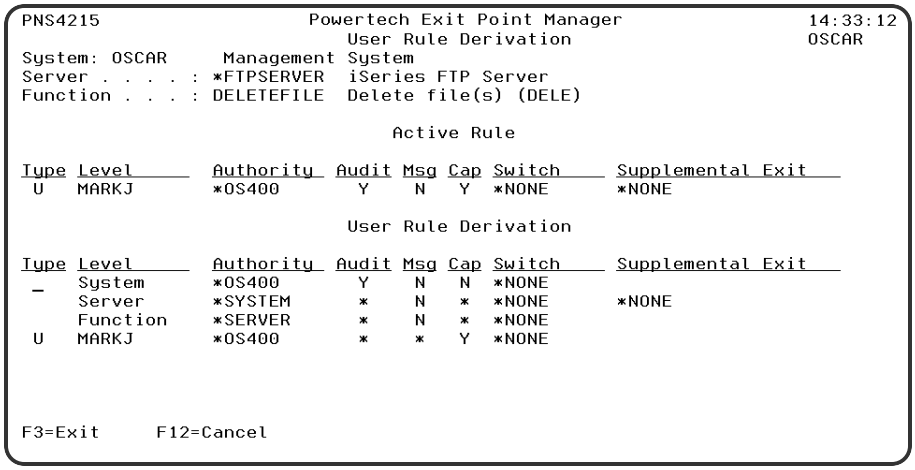
User (USER)
The user profile you want to test. This is the user profile associated with the local portion of the transaction.

A group profile is not valid for this field unless it is being used as the actual user profile.

Output (OUTPUT)
The results can be output to the following places:

***TRACE** The results are sent to the trace facility. Prior to running this, you will need to set up the trace facility via the command PNSSTRTRC and select function *TEST.
***MESSAGE** The results are sent to message queue PNSRQSO. Prior to running this, you will need to create this message queue.

User Rule Derivation



How to Get There

On the Work with Security by User panel, choose **5** for a User Rule.

What it Does

The Powertech User Rule Detail Derivation panel displays the hierarchical inheritance of the current User rule.

Options

Server

The server to which the current rule applies.

Function

The name of the IBM server function to which the current rule applies.

Type

This field is used to indicate whether the associated User field refers to an O/S user profile or a Exit Point Manager User Group.

Valid values are:

U The associated User field refers to an O/S user profile.
G The associated User field refers to a Exit Point Manager user group.

Level

The Level column indicates from which inheritance level the specific values listed are derived. The last entry in the Rule Derivation section is the level from which the Location Rule Display was requested. For example, if this display were requested from "Work with Authorities by User", the last level would represent a user and as such might be a user profile name or *PUBLIC.

Valid values are:

System The system values level.
Server The server level.
Function The server function level.

*__PUBLIC__ The user level for all users.
*__ALL__ The location level for all locations.

Authority
The authority assigned to the user for this rule.

Switch
The name of a switch profile for this rule. If a profile name is supplied, processing is swapped to run under this profile's authority. This is only valid for authorities *SWITCH and *MEMSWITCH.

Audit The audit property controls the type of requests Exit Point Manager will log.

Possible values are:

__Y__ Log all requests by the user/server/function.
__N__ Only log authority failures for the user/server/function.
* Use the audit value from the prior level.

Msg
The message property entry will determine if Exit Point Manager sends a message to the specified message queue for the user/server/function. Possible values are:

__N__ No message is sent.
__Y__ A message is sent to the specified queue.
* Use the audit value from the prior level.

Cap
Capture transactions for Memorized Transaction Request (MTR).

Possible values are:

__N__ Do not capture transactions.
__Y__ Capture transactions.
* Use the audit value from the prior level.

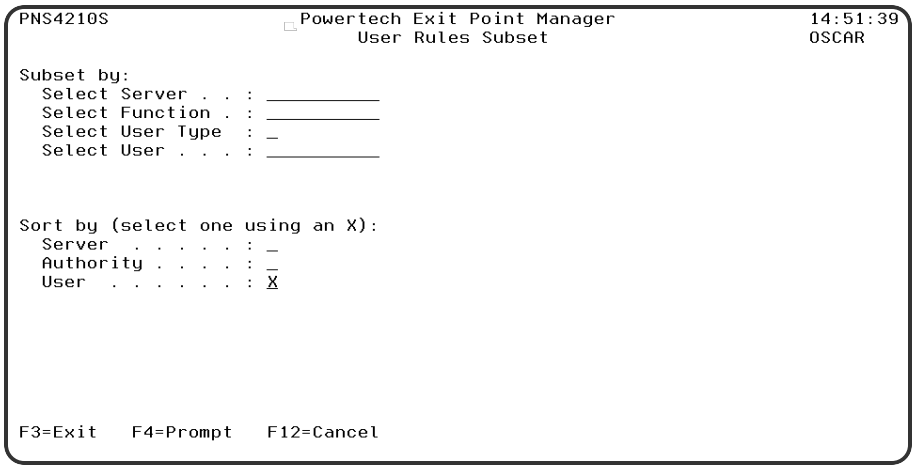
Command Keys

F3 (Exit): Exit the program without processing any pending changes.

F5 (Refresh): Refreshes the panel and resets all available text fields.

F12 (Cancel): Exit the panel without processing any pending changes.

User Rules Subset panel



How to Get There

From the Work with Security by User panel, press `F16`, Sort/Subset.

What it Does

The User Rules Subset panel allows you to select User Rules for display that meet certain criteria. You can select User Rules by Server, Function, User Type, or User.

Options

Server

Specify the criteria for selection by Server name. Leaving this field blank includes all Server values.

You can use the Generic Character to indicate that a partial value is to be used for selection. In some circumstances you may also use the Wildcard Character to indicate that a partial value is to be used for selection. Generic and Wildcard characters can be used at the beginning, end, or within a value and can be freely intermixed (you can use both characters in the same value).

Function

Specify the criteria for selection by Function name. Leaving this field blank includes all Function values.

You can use the Generic Character to indicate that a partial value is to be used for selection. In some circumstances you may also use the Wildcard Character to indicate that a partial value is to be used for selection. Generic and Wildcard characters can be used at the beginning, end, or within a value and can be freely intermixed (you can use both characters in the same value).

User Type

Specify which type of User Type you would like to have listed. Leaving this field blank includes all User Type values.

User

Specify the criteria for selection by User or User Group. Leaving this field blank includes all User or User Group values.

You can use the Generic Character to indicate that a partial value is to be used for selection. In some circumstances you may also use the Wildcard Character to indicate that a partial value is to be used for selection. Generic and Wildcard characters can be used at the beginning, end, or within a value and can be freely intermixed (you can use both characters in the same value).

Sort by (select one using an X)

The User Rules Subset panel allows you to select User Rules for display that meet certain criteria. You can select a sort by one of the available fields.

Server • Authority • User

Select whether you would like to sort by Server name, Authority, or User.

Command Keys

F3 (Exit): Exit the panel without processing any pending changes.

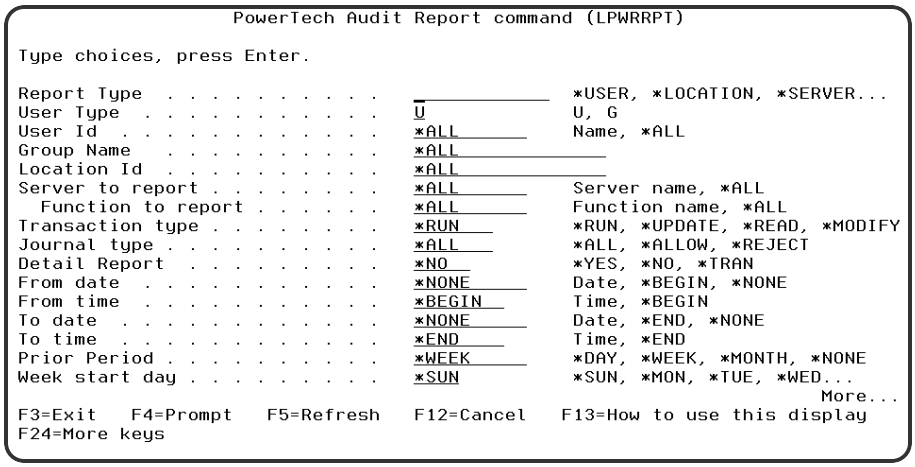
F4 (Prompt): Displays a list of possible values from which you may select one.

F12 (Cancel): Exit the panel without processing any pending changes.

Using the Audit Report Command (LPWRRPT)

In addition to running reports from the Reports Menu, you also can use the LPWRRPT command to run reports from your own programs, or to include Exit Point Manager reporting in your job scheduler.

To display the LPWRRPT command prompt panel, enter the command on a command line and press `F4`, or select option **7**, Powertech Audit Report command, on the Reports Menu.



Specify the report type you want to run and press `Enter`. The parameters for that report type display, allowing you to specify your selection criteria.

See Powertech Audit Report Command panel for a complete description of all the command parameters.

Command Keys

F3 (Exit): Exit the panel without processing any pending changes.

F4 (Prompt): Displays a list of possible values from which you may select one.

F5 (Refresh): Refreshes the panel and resets all available text fields.

F12 (Cancel): Exit the panel without processing any pending changes.

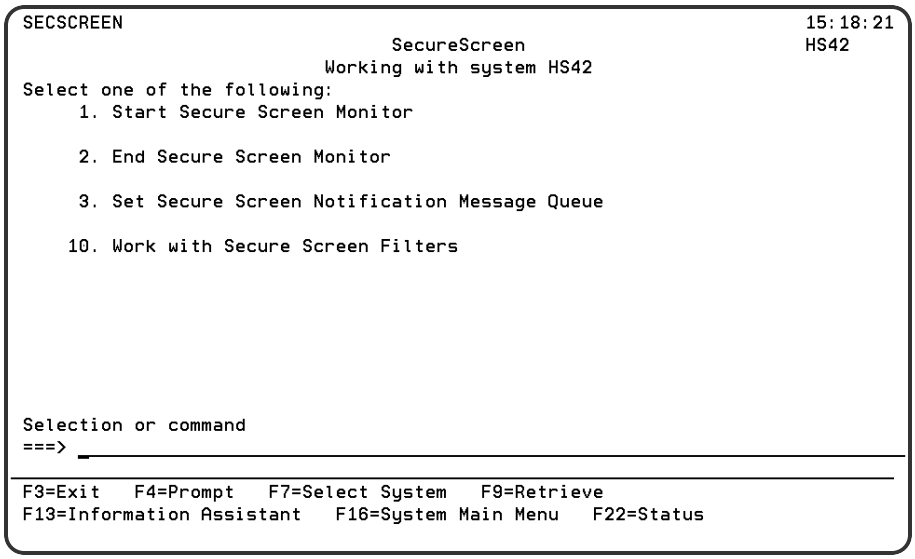
F13 (How to use this display): Shows help for the prompt display or associated display you are currently using.

F24 (More keys): Shows additional function keys that can be used for this display.

Working with Powertech SecureScreen

The Powertech Secure Screen Main Menu allows you to start and end the Secure Screen monitor, set the notification message queue, and work with Secure Screen filters.

Select option **1** on the Work with Utilities menu to display the Secure Screen main menu. You also can enter the WRKSECSCR command to display the main menu.



You can select from the following options on the Secure Screen Main Menu:

1. **Start Secure Screen Monitor.** Starts the session inactivity monitor job. The job runs in the PWRWRKMGT subsystem; the subsystem starts if it is not currently active.

The monitor receives messages from the message queue specified in the QINACTMSGQ system value. The messages describe jobs that have been inactive the interval specified in the QINACTITV system value. Information from the message is used to retrieve attributes of the inactive job, and compare them against the Secure Screen filters to determine the action to take.

Notes:

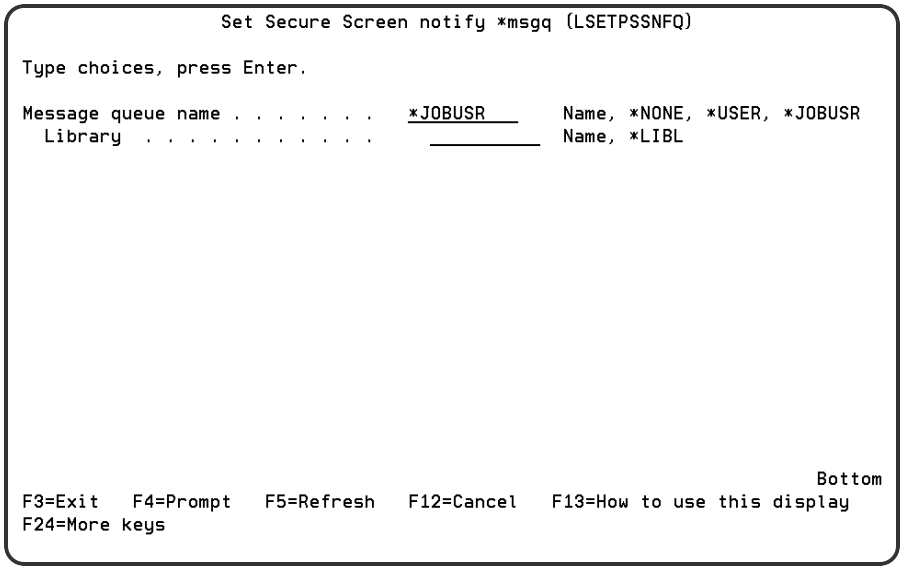
- You must configure the QINACTMSGQ and QINACTITV system values before starting the Secure Screen monitor. Use the WRKSYSVAL QINA* command to locate the system values.
- You should not define QSYSOPR as the message queue in QINACTMSGQ. Secure Screen monitors for inactivity messages and sees other messages as garbage. The QSYSOPR message queue will be locked any time QSYSOPR signs on.

You also can use the STRPLSSMON command to start the Secure Screen monitor job.

2. **End Secure Screen Monitor.** Ends the session inactivity monitor job. When the monitor ends, inactive sessions are no longer processed against the Secure Screen filters, and sessions are not disconnected or ended.

   > **NOTE:** You can end the monitor job using the ENDJOB command or ENDSBS for the PWRWRKMGT subsystem. If you specify *CNTRLD, the monitor detects the request and ends normally.

   You also can use the ENDPLSSMON command to end the monitor job.
3. **Set Secure Screen Notification Message Queue.** Allows the administrator to set the name of the message queue to receive Secure Screen notifications when selected sessions time out. The monitor sends notification messages when a session times out and matches a filter that has the Notify Administrator value set to *MSG. You also can use the LSETPSSNFQ command to set a notification message queue.



Enter the following message queue information:

Message queue name

Enter the name of the message queue to use. Possible values are:

***JOBUSER** Use the message queue of the user running the job.
***USER** Use the message queue of the user associated with monitor job.
***NONE** No messages are sent.
Name Enter a message queue name to use.

Command Keys

F3 (Exit): Exit the menu.

F4 (Prompt): Provides assistance in entering or selecting a command.

F7 (Select System): Use this command key to work with data from a different System.

F9 (Retrieve): Displays the last command you entered on the command line and any parameters you included. Pressing this key once shows the last command you ran. Pressing this key twice shows the command you ran before that, and so on.

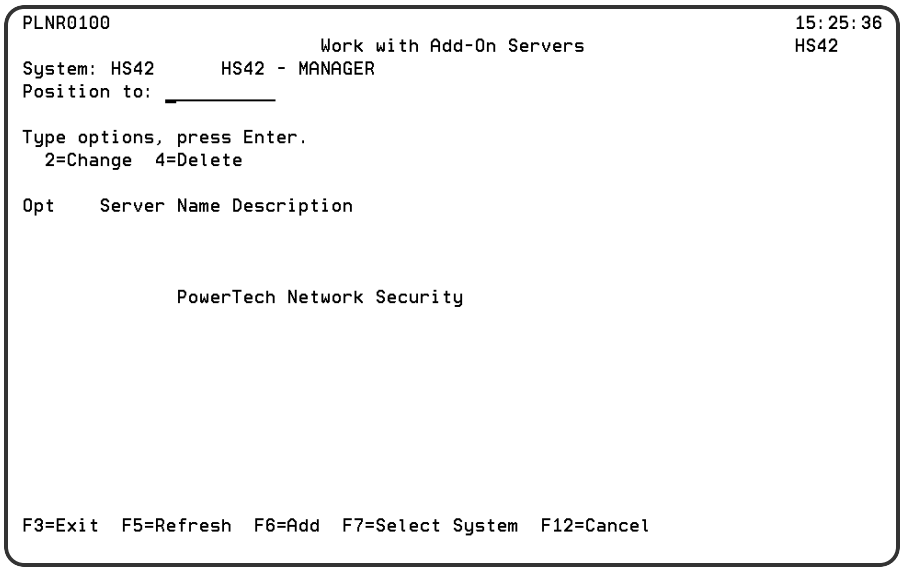
F13 (Information Assistant): Displays the Information Assistant menu with several types of assistance available. Press this key to access more information about the IMB i system.

F16 (System Main Menu): Displays the IBM i Main Menu (MAIN).

F22 (Status): Displays the Operational Resources pop-up window containing the status of several operation aspects of Powertech products.

Work with Add·On Servers (LWRKGENSRV)

Work with Add-on Servers is used to maintain customer and business partner servers and their function using Exit Point Manager's Generic Exit program. Exit Point Manager supported servers and their functions cannot be maintained with this process. Type an option next to a specific server and press `Enter`. You can type option numbers next to more than one Server at a time. This allows you to perform more than one task at a time. If you see 'More...' in the lower right corner of your display, there is more information to be listed. Press the Page Down (Roll Up) key to move toward the end of the Servers listed. Press the Page Up (Roll Down) key to move toward the beginning of the Servers listed.



Options

2=Change

Change an Add-on Server and its functions.

4=Delete

Delete an Add-on Server and its functions.

Option

This column is used to perform different operations on individual Add-on Servers and their functions. Type your option selection next to a Server Name and press `Enter`. You can type the same option next to multiple Add-on Servers. You may also type different options next to different Add-on Servers.

Available options are:

2=Change

Change an Add-on Server and its functions.

4=Delete

Delete an Add-on Server and its functions.

Server Name

The name of an Add-on Server.

Server Description

The description of the Add-on Server.

Command Keys

F3 (Exit): Exit the program without processing any pending changes.

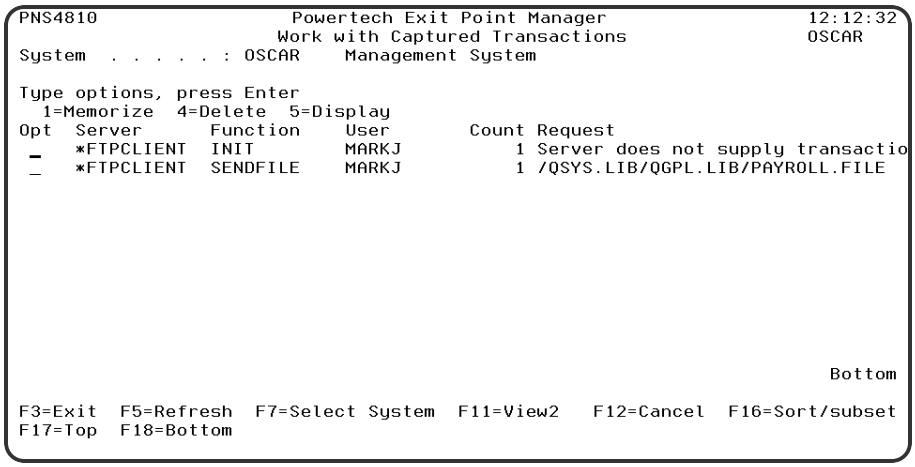
F5 (Refresh): Refresh the screen.

F6 (Add): Add a new server and its functions.

F7 (Select System): Use this command key to work with data from a different System.

F12 (Cancel): Exit the screen without processing any pending changes.

Work with Captured Transactions



How to Get There

On the Main Menu, select option **10**.

What it Does

The work with Captured Transactions panel allows you to memorize, display, or delete Captured Transactions.

Options

You can select from the following options on the Work with Captured Transactions panel.

1=Memorize

Enter a **1** in the Opt column to memorize a transaction. When you select to memorize a transaction, Network Security performs an exact string match against the incoming transaction.

When you select a transaction to memorize, the Memorize Captured Transaction panel displays allowing you to specify the parameters for the memorized transaction. See also Working with Memorizing Transactions.

4=Delete

Enter option **4** next to a transaction to delete a captured transaction.

5=Display

Enter option **5** next to a transaction to display the Display Captured Transaction panel.

Field Descriptions

Opt

Enter a valid option from the list of options provided on the list panel.

System

System indicates the target of any operations you perform. When you add rules, for example, those rules will be sent to, and will affect processing on, the System named.

> NOTE: The following fields are available in one of the three views. Press **F11** to switch between the three available views.

Server

A Server in Exit Point Manager is a controlled entry point into your system. These entry points are determined and defined by IBM. Exit Point Manager has assigned easy-to-remember names to these controlled entry points.

Function

A Function, or Server Function, in Exit Point Manager represents a class of operations that a given Server may perform. For example, the *SIGNON Server classifies its operations as those pertaining to changing passwords, generating authentication tokens, and retrieving signon information. Exit Point Manager has assigned easy-to-remember names to these Functions, such as CHGPWD, GENAUTTKN and RETRIEVE.

User

User represents the identity of the person initiating a transaction as a user profile.

The special value *PUBLIC, when used on a rule, means that the rule applies to any User lacking a specific rule. When used as a subset or selection parameter, *PUBLIC means to select all such rules for display or printing.

This is the User that initiated the transaction.

ASP Group

This is the name of the ASP Group to which the job was set when the transaction was captured.

Count
The number of times this exact transaction has been captured.

Request
This is the data handed to Exit Point Manager by the operating system. Much of this transaction data is binary in nature and may not be human-readable. Undisplayable characters in the transaction data are replaced by the mid-dot character (·). The Work with Captured Transactions panel allows you to display, delete, and memorize Captured Transactions.

Last Collected
The date and time that the most recent of these transactions was captured.

User Type
This field is used to indicate whether the associated User field refers to an O/S user profile or a Exit Point Manager User Group.

Valid values are:

U

The associated User field refers to an O/S user profile.

G

The associated User field refers to a Exit Point Manager user group.

Command Keys
F3 (Exit): Exit the current panel without processing any pending changes.

F5 (Refresh): Refreshes the panel and resets all available text fields.

F7 (Select System): Use this command key to work with data from a different System.

F11 (View): Switches views of the list so that you can see other data.

F12 (Cancel): Exit the current panel without processing any pending changes.

F16 (Sort/Subset): Allows you to sort and subset information by user, server, type, and/or transaction.

F17 (Top): Positions the list panel to the first record.

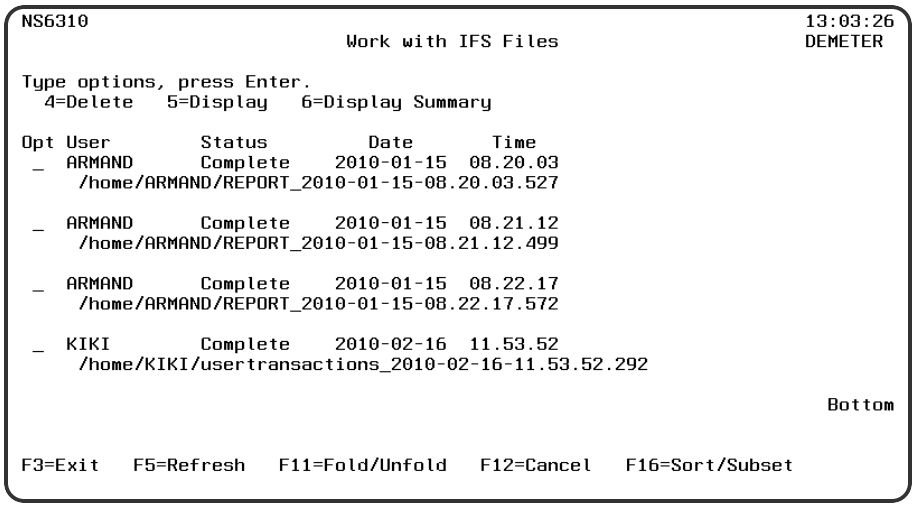
F18 (Bottom): Positions the list panel to the last record.

F19 (Left): Shifts the transaction data to the left.

F20 (Right): Shifts the transaction date to the right.

Work with IFS Files

The Work with IFS Reports enables you to work with IFS Report output.



Options
These are the options available on this panel.

4=Delete
Delete the IFS reports selected.

5=Display
Display the detailed report.

6= Display Summary
Display the summary report.

Field Descriptions

Opt
This is where you select reports with one of the above options.

User
The name of the user who created the report.

Status
Indicates the current status of the report generation. Complete Report has been generated.

Date/Time
The date and time the report was requested.

Name
Name of the report.

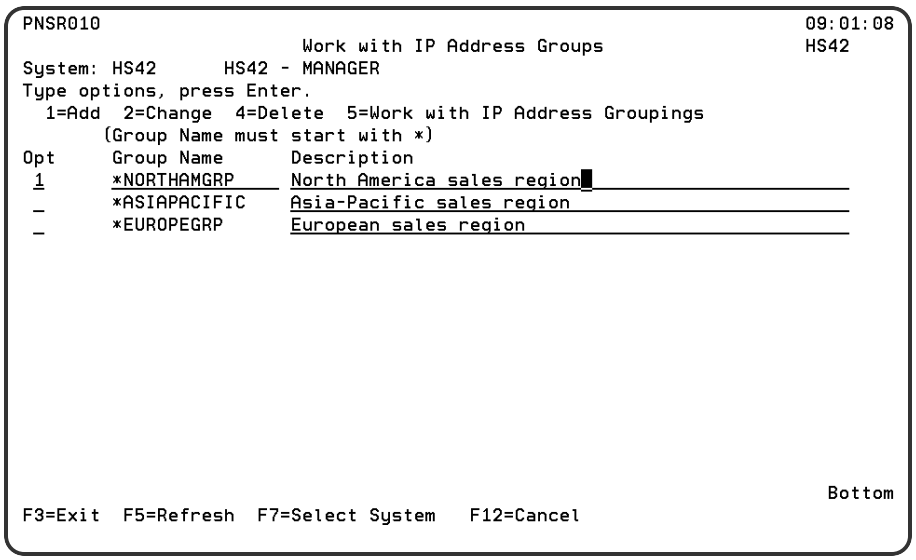
Command Keys
F3 (Exit): Exit the panel without processing any pending changes.

F5 (Refresh): Refreshes the panel and resets all available text fields.

F12 (Cancel): Exit the panel without processing any pending changes.

F16 (Sort/Subset): Allows you to sort and subset information.

Work with IP Address Groups



How to Get There

From the Exit Point Manager Main Menu, select option **5** to display the Work with IP Address Groups panel.

What it Does

The Work with IP Address Groups panel is used when a number of IP addresses need the same group filter rules applied. To add a new Address Group, enter the information on the blank line below the column headings. Once an Address Group is created a range of IP addresses may be associated to it. Option **5** displays a list of IP addresses associated to the group. Type an option next to a specific group and press `Enter`. You can type option numbers next to more than one group at a time. This allows you to do more than one task at a time. If you see 'More...' in the lower right corner of your display, there is more information to be listed.

Press the Page Down (Roll Up) key to move toward the end of the Address Groups.

Options

You can select from the following options:

1=Add

Add an Address Group. Valid for line one only.

After you create an IP address group, you can assign a range of locations to the address group using option **5**.

2=Change

Change an Address Group.

> **NOTE:** You cannot use option 2 to change the group name.

4=Delete
Delete an Address Group.

> **NOTE:** If the IP address group has IP address groupings and has been applied to a location rule, you must delete all rules and groupings before you can delete the address group.

5=Work with IP Address Groupings
Work with the IP Addresses associated with the group. See Work with IP Address Groupings panel.

Field Descriptions

Group Name
The name of a group of IP addresses. It must begin with special character "*".

Description
The description of the Address Group. It is a required entry.

Command Keys
F3 (Exit): Exit the panel without processing any pending changes.

F5 (Refresh): Refreshes the panel and resets all available text fields.

F7 (Select System): Use this command key to work with data from a different System.

F12 (Cancel): Exit the panel without processing any pending changes.

Work with IP Address Groupings

```
PNSR011                                                          09:03:49
                        Work with IP Address Groupings           HS42
System: HS42      HS42 - MANAGER
Type options, press Enter.
  1=Add  2=Change  4=Delete  5=Rules by Location

Option  Group Name      From IP Addr    To IP Addr
  _     *ASIAPACIFIC
  _     *ASIAPACIFIC    004.004.001.005 *FROMLOC
  _     *ASIAPACIFIC    192.168.001.001 192.168.062.128

                                                                 Bottom
F3=Exit  F5=Refresh  F7=Select System   F12=Cancel
```

How to Get There
From the Exit Point Manager Main Menu, select option **5** to display the Work with IP Address Groups panel. Select option **5** for a group name.

What it Does

The work with IP Address Groupings is used to associate specific locations to one identifier. To add a new IP Address Grouping, enter the information on the blank line below the column headings. Type an option next to a specific group and press `Enter`. You can type option numbers next to more than one group at a time. This allows you to do more than one task at a time. If you see 'More...' in the lower right corner of your display, there is more information to be listed. Press the Page Down (Roll Up) key to move toward the end of the IP Address Groups. Press the Page Up (Roll Down) key to move toward the beginning of the IP Address Groups.

Options

You can select from the following options to work with IP address groupings:

1=Add

Add an IP Address Grouping. Valid for line "1" only.

> **NOTE:** If you are adding only one IP address to the group, you can leave the To IP Addr field blank or you enter the same IP address in both fields. If the To IP Addr field is left blank, the default value *FROMLOC displays in the field.

2=Change

Change an IP Address Grouping.

> **NOTE:** You cannot change the group name.

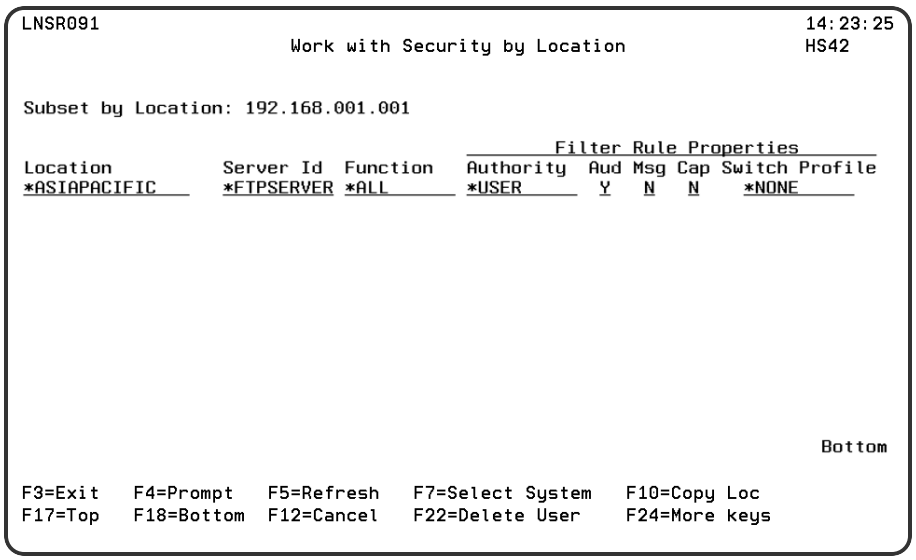
4=Delete

Delete an IP Address Grouping.

> **NOTE:** You cannot delete an IP address grouping if any location rules exist for the group. You must delete any location rules before you can delete the grouping.

5=Rules by Location

Work with Security by Location or IP Address.



To add a new location rule, enter the IP address group name in the Location field and specify the rule values. The location rule then uses the IP address groupings when evaluating the rule.

Field Descriptions

Group Name
The name of an IP Address Group. It must begin with special character "*".

From IP Address
The IP Address to begin a grouping. The location must be a valid IP address. A grouping may be a single location. when a single location is desired special value *FROMLOC is placed in the "To Location".

To IP Address
The IP Address to end a grouping. The location must be a valid IP address. This value must be greater than, or equal to, "From Location".

Command Keys
F3 (Exit): Exit the panel without processing any pending changes.

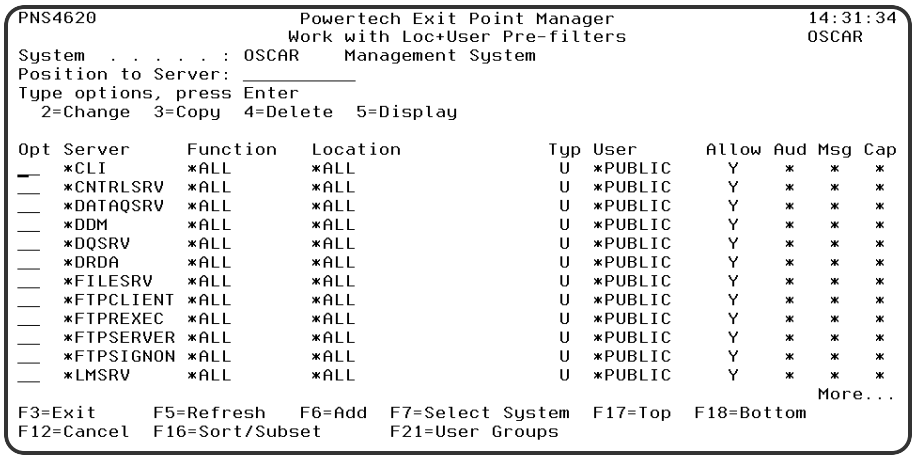
F5 (Refresh): Refreshes the panel and resets all available text fields.

F7 (Select System): Use this command key to work with data from a different System.

F12 (Cancel): Exit the panel without processing any pending changes.

Work with Location + User Pre-filter panel

```
PNS4620                  Powertech Exit Point Manager                  14:07:52
                        Work with Loc+User Pre-filters                 OSCAR
System  . . . . . : OSCAR
Position to Server: __________
Type options, press Enter
  2=Change  3=Copy  4=Delete  5=Display

Opt Server     Function   Location             Typ User      Allow Aud Msg Cap
__  *CLI       *ALL       *ALL                  U  *PUBLIC     Y    *   *   *
__  *CNTRLSRV  *ALL       *ALL                  U  *PUBLIC     Y    *   *   *
__  *DATAQSRV  *ALL       *ALL                  U  *PUBLIC     Y    *   *   *
__  *DDM       *ALL       *ALL                  U  *PUBLIC     Y    *   *   *
__  *DQSRV     *ALL       *ALL                  U  *PUBLIC     Y    *   *   *
__  *DRDA      *ALL       *ALL                  U  *PUBLIC     Y    *   *   *
__  *FILESRV   *ALL       *ALL                  U  *PUBLIC     Y    *   *   *
__  *FTPCLIENT *ALL       *ALL                  U  *PUBLIC     Y    *   *   *
__  *FTPREXEC  *ALL       *ALL                  U  *PUBLIC     Y    *   *   *
__  *FTPSERVER *ALL       *ALL                  U  *PUBLIC     Y    *   *   *
__  *FTPSIGNON *ALL       *ALL                  U  *PUBLIC     Y    *   *   *
__  *LMSRV     *ALL       *ALL                  U  *PUBLIC     Y    *   *   *
                                                                       More...
F3=Exit     F5=Refresh   F6=Add  F7=Select System  F17=Top  F18=Bottom
F12=Cancel  F16=Sort/Subset      F21=User Groups
```



How to Get There

From the Exit Point Manager Main Menu, choose option **6**, Work with Pre-filters, then enter option **1** to work with Pre-filters at a Server level, or option **2** to work with Pre-filters at the Location+User level.

What it Does

The Work with Loc+User Pre-filter panels allow you to create, modify, delete, and display the records that control the Pre-filter function. This Pre-filter function allows you to specify certain actions for transactions before they are evaluated by the regular Powertech Exit Point Manager rules. The primary action is to allow or not allow a transaction — allowing it causes it to be further evaluated by Exit Point Manager rules; not allowing it is equivalent to a Exit Point Manager reject. The other actions that you can specify are to audit the transaction, send an immediate message, and capture the transaction. These actions work exactly like their equivalents within Exit Point Manager rules processing. The Pre-filter function allows you to specify settings by server, function, location, and user. Records are shipped for a default system setting (this record has a server of *ALL) and for default server settings. These records can be changed but not deleted. System record must have either a 'Y' or an 'N' for each of the settings (allow, audit, message, and capture).

The Pre-filter function attempts to match the most specific record to the transaction. Once a match is found, the Pre-filter function processes the transaction based on those settings.

Field Descriptions

Opt

Enter a valid option from the list of options provided on the list panel. Server records can be displayed or changed. Regular records can be displayed, changed, copied, and deleted — they can also be added via `F6`.

Server

The name of the Powertech Exit Point Manager server for this Pre-filter record. On screens that allow input for this field, you can prompt this field. Allow The setting for whether transactions matching this record should be allowed to continue to be processed by Exit Point Manager. Valid settings are 'Y' (Yes - Exit Point Manager rules should evaluate this transaction, which may or may not cause it to be rejected, 'N' (No — reject the transaction), and '*' (inherit the value from a higher level record with a specific 'Y' or 'N' setting).

The system record (Server = '*ALL') can only have a ‘Y’ or an ‘N’ for this field.

Function
The name of the Powertech Exit Point Manager server function for this Pre-filter record. You can prompt this field. If the server field is not already on the screen, it would be prompted for first. A value of *ALL shows on the prompt, but cannot be used for a test transaction.

Location
The location for this Pre-filter record. Valid special values are a Exit Point Manager location group. *ALL is not allowed.

Type
Specifies whether the user field is a user profile or a Exit Point Manager User Group.

Allowed values are:

U The user field is a user profile.
G The user field is a Exit Point Manager User Group

User
If the associated User Type is a 'U', User represents the identity of the person initiating a transaction as a user profile.

The special value *PUBLIC, when used on a rule, means that the rule applies to any User lacking a specific rule. When used as a subset or selection parameter, *PUBLIC means to select all such rules for display or printing.

If the associated User Type is a 'G', User represents a Exit Point Manager User Group.

Audit
The setting for whether transactions matching this record should have a journal entry written to the journal specified by the Exit Point Manager configuration. Valid settings are 'Y' (Yes — send a journal entry), 'N' (No — do not send a journal entry), and '*' (inherit the value from a higher level record with a specific 'Y' or 'N' setting).

The system record (Server = '*ALL') can only have a 'Y' or an 'N' for this field.

Message
The setting for whether transactions matching this record should have a message sent to the message queue specified by the Network Security configuration. Valid settings are 'Y' (Yes — send a message), 'N' (No — do not send a message), and '*' (inherit the value from a higher level record with a specific 'Y' or 'N' setting).

The system record (Server = '*ALL') can only have a 'Y' or an 'N' for this field.

Capture
The setting for whether transactions matching this record should be captured. Valid settings are 'Y' (Yes — capture the transaction), 'N' (No — do not capture), and '*' (inherit the value from a higher level record with a specific 'Y' or 'N' setting). The system record (Server = '*ALL') can only have a 'Y' or an 'N' for this field.

Order
The order of checking for Pre-filter records is:

Exact server, exact function, exact location, exact user profile.

Exact server, exact function, exact location, group / supplemental profiles.

Exact server, exact function, exact location, *PUBLIC.

Exact server, exact function, location group, exact user profile.

Exact server, exact function, location group, group / supplemental profiles.

Exact server, exact function, location group, *PUBLIC.

Exact server, exact function, location *ALL, exact user profile.

Exact server, exact function, location *ALL, group / supplemental profiles.

Exact server, exact function, location *ALL, *PUBLIC.

Exact server, function *ALL, exact location, exact user profile.

Exact server, function *ALL, exact location, group / supplemental profiles.

Exact server, function *ALL, exact location, *PUBLIC.

Exact server, function *ALL, location group, exact user profile.

Exact server, function *ALL, location group, group / supplemental profiles.

Exact server, function *ALL, location group, *PUBLIC.

Exact server, function *ALL, location *ALL, exact user profile.

Exact server, function *ALL, location *ALL, group / supplemental profiles.

Exact server, function *ALL, location *ALL, *PUBLIC.

Server record (server = exact server).

System record (server = *ALL).

Once a match is found, any settings with an '*' are resolved by inheriting the value from the record with a specific ('Y' or 'N') setting. This check is done in the following order:

Exact server, exact function, location *ALL, *PUBLIC.

Exact server, function *ALL, location *ALL, *PUBLIC.

Server record (server exact server).

System record (server *ALL).

Options

2=Change

Choose **2** to open the Location + User Pre-filter Update panel where you can change the system record for each of the Pre-filter settings (allow, audit, message, and capture).

3=Copy

Choose **3** to open the Location + User Pre-filter Copy panel where you can create a copy of an already existing Pre-filter.

4=Delete
Choose **4** to delete an existing Loc+User Pre-filter. Press `Enter` to confirm or **F12** to cancel the deletion.

5=Display
Choose **5** to open the Location + User Pre-filter Display panel where you can view the system record for each of the Pre-filter settings (allow, audit, message, and capture).

Command Keys
F3 (Exit): Exit the panel without processing any pending changes.

F5 (Refresh): Refreshes the panel and resets all available text fields.

F6 (Add): Add a new location+user Pre-filter.

F7 (Select System): Use this command key to work with data from a different System.

F12 (Cancel): Exit the panel without processing any pending changes.

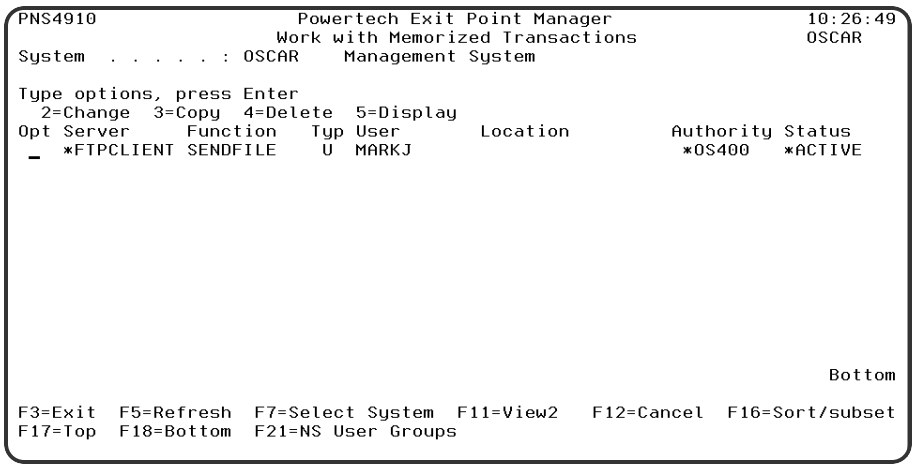
F16 (Sort/Subset): Allows you to sort and subset information by server, function, location, and/or user.

F17 (Top): Positions the list panel to the first record.

F18 (Bottom): Positions the list panel to the last record.

F21 (User Groups): Opens the Work with User Groups panel where you can create or edit a User Group.

Work with Memorized Transactions



How to Get There
On the Main Menu, select option **11**.

What it Does
The Work with Memorized Transactions panel enables you to maintain memorized transactions.

Options

2=Change

Enter option **2** next to a memorized transaction and press `Enter` to display the Change a Memorized Transaction panel. You can use the Change a Memorized Transaction panel to change the authority, auditing, message, and switch profile properties of the transaction. You also can specify that you want Exit Point Manager to capture the transaction when it occurs.

You cannot change the server/function or user of the memorized transaction. You also cannot modify the actual transaction that has been memorized.

3=Copy

Enter option **3** next to a memorized transaction and press `Enter` to display the Copy a Memorized Transaction panel. Use the panel to copy an existing transaction and edit it to filter on a different user or location than the original transaction, and change the authority, auditing, message, and switch profile filter properties. You also can enter changes to the actual transaction string before saving it as a new transaction. You cannot change the server/function.

After you have edited the transactions, press `Enter` to save it. The Work with Memorized Transactions panel displays with the confirmation message Memorized Transactions(s) successfully copied.

> **NOTE:** Transaction string entries are case sensitive. No transaction string editing or syntax checking is performed. We recommend that you terminate the memorized transaction string using the percent sign (%) wildcard character.

4=Delete

To delete a memorized transaction, enter option **4** next to a transaction on the Work with Memorized Transactions panel. When you press enter, the confirmation message Memorized Transaction(s) successfully deleted displays at the bottom of the panel. Note: Make sure you want to delete the transaction since it is deleted immediately.

5=Display

Enter option **5** next to a transaction to display the Display Memorized Transaction panel. The Display Memorized Transaction panel shows the filter properties of the memorized transaction.

Field Descriptions

Server

A Server in Exit Point Manager is a controlled entry point into your system. These entry points are determined and defined by IBM. Exit Point Manager has assigned easy-to-remember names to these controlled entry points.

Function

A Function, or Server Function, in Exit Point Manager represents a class of operations that a given Server may perform. For example, the *SIGNON Server classifies its operations as those pertaining to changing passwords, generating authentication tokens, and retrieving sign-on information. Exit Point Manager has assigned easy-to-remember names to these Functions, such as CHGPWD, GENAUTTKN and RETRIEVE.

Type

This field is used to indicate whether the associated User field refers to an O/S user profile or a Exit Point Manager User Group.

Valid values are:

U The associated User field refers to an O/S user profile.
G The associated User field refers to a Exit Point Manager user group.

User

User represents the identity of the person initiating a transaction as a user profile. The special value *PUBLIC, when used on a rule, means that the rule applies to any User lacking a specific rule. when used as a subset or selection parameter, *PUBLIC means to select all such rules for display or printing. This displays the User to which this Memorized Transaction applies. If blank, then this is for a specific Location. If the value is *PUBLIC, the transaction applies to all users.

ASP Group

When a memorized transaction is evaluated, this ASP Group name will be compared to the current ASP Group name of the job issuing the transaction. These need to be the same (or this must be set to the special value *ALL) for this memorized transaction to be considered a match.

Location

Location represents the source of a transaction. Location can hold an IP Address, an IP Address Group or the name of an SNA Communications Device. The special value *ALL, when used on a rule, means that the rule applies to any rule means that the rule applies to any Location lacking a specific rule. when used as a subset or selection parameter, *ALL generally means to select all such rules for display or printing. This displays the Location to which this Memorized Transaction applies. If blank, then this is for a specific User. If the value is *ALL, the transaction applies to all Users.

Authority

Authority represents the action to be taken when a rule is found that matches the data present on a transaction. This field may hold one of these values:

***USER** Current user authority is used.
***OS40O** Exit Point Manager will use normal operating system authority for the user.
***REJECT** Exit Point Manager will reject requests.
***SWITCH**Exit Point Manager will use the authority of the switch profile for the transaction. A switch profile entry is required.
***MEMUSR** Memorized Transactions (MTR) are checked for authority first. If no MTR authority is encountered, Exit Point Manager will use the authority of the current user.
***MEMOS400** Memorized Transactions (MTR) are checked for authority first. If no MTR authority is encountered, Exit Point Manager will use normal operating system authority for the user.
***MEMREJECT** Memorized Transactions (MTR) are checked for authority first. If no MTR authority is encountered, Exit Point Manager will reject requests for the specified user.
***MEMSWITCH** Memorized Transactions (MTR) are checked for authority first. If no MTR authority is encountered, Exit Point Manager will use the authority of the switch profile for the specified user. A switch profile entry is required.
***MEMOBJ** Memorized Transactions (MTR) are checked for authority first. If no MTR authority is encountered, Exit Point Manager will check any objects used in the transactions for authorities defined by Object Rules.
***SERVER** Exit Point Manager will use the authority defined for the Server.

***SRVFCN** Exit Point Manager will use the authority defined for the Server Function.

Status

This is the status of the Memorized Transaction. Possible values are:

***ACTIVE** Exit Point Manager will attempt to match this transaction during rule enforcement. Memorized Transactions that are changed to *ACTIVE will have a matching User or Location rule changed to the corresponding action; *ALLOW to *MEMOS400, *REJECT to *MEMREJECT, or *SWITCH to *MEMSWITCH.

***INACTIVE** Exit Point Manager will not attempt to match this transaction during rule enforcement. Memorized Transactions that are changed to *INACTIVE will have the matching User or Location rule changed (if there are no other Memorized Transactions for that rule) to the corresponding action; *MEMOS400 to *ALLOW, *MEMREJECT to *REJECT, or *MEMSWITCH to *SWITCH.

Command Keys

F3 (Exit): Exit the panel without processing any pending changes.

F5 (Refresh): Refreshes the panel and resets all available text fields.

F7 (Select System): Use this command key to work with data from a different System.

F11 (View): Changes the data presented in the list.

F12 (Cancel): Exit the panel without processing any pending changes.

F16 (Sort/Subset): Allows you to sort and subset information by user, server, status, and/or transaction.

F21 (User Groups): Allows user to go to the Work with User Groups panel.

Work with Exit Point Manager Activation

```
PNSRACT10                                                          15:34:19
                            Work with Activation                   HS42

System: HS42      HS42 - MANAGER
Type options, press Enter.
    1=Set to Activate   2=Set to Deactivate   3=Remove pending change ...

Opt  Server      Pending Change  Current program        Current supplemental
 __  *CLI        *NONE           NS R07M000000          *NONE
 __  *CNTRLSRV   *NONE           NS R07M000000          *NONE
 __  *DATAQSRV   *NONE           NS R07M000000          *NONE
 __  *DDM        *NONE           NS R07M000000          *NONE
 __  *DQSRV      *NONE           NS R07M000000          *NONE
 __  *DRDA       *NONE           NS R07M000000          *NONE
 __  *FILESRV    *NONE           NS R07M000000          *NONE
 __  *FTPCLIENT  *NONE           NS R07M000000          *NONE
 __  *FTPREXEC   *NONE           NS R07M000000          *NONE
 __  *FTPSERVER  *NONE           NS R07M000000          *NONE
 __  *FTPSIGNON  *NONE           NS R07M000000          *NONE
                                                                  More...

F3=Exit   F5=Refresh   F12=Cancel   F13=Set all to Activate
F14=Set all to Deactivate   F23=More options   F24=More keys
```

How to Get There

To display these options, from the Exit Point Manager Main Menu, select option **81**, Configuration Menu. Then select option **2**, Work with Activation.

The following describes the parameters and allowable values for each field on the Work with Activation panel.

What it Does

The work with Activation panel is used to prepare servers to be protected by Powertech's Exit Point Manager product or to remove that protection. The activation process can be run immediately or scheduled to run the next time you IPL the system. A server may be selected for activation (begin protection) or for deactivation (end protection). All pending changes take effect during the next activation operation. The process of activating protection for a server also "activates" this version of the product. This is only a concern when you have been running a prior version of Exit Point Manager and are upgrading to a new version. Part of making this version the active version involves ending the SUMCAPTRAN job running for the other version and starting it for this version. This will only happen if the SUMCAPTRAN job is running at the time you activate this version.

Field Descriptions

Opt

Select servers with one of the options listed to perform that action on the selected server. Press Help on the options line for more information on the available options.

Server

A Server in Exit Point Manager is a controlled entry point into your system. These entry points are determined and defined by IBM. Exit Point Manager has assigned easy—to—remember names to these controlled entry points.

> **NOTE:** The *DDM and *DRDA servers are activated together regardless of whether you select one of them or both.

Pending Change

The Pending Change column shows the action that Exit Point Manager will take on the server the next time the activation process is run.

The following values may appear for Pending Change:

***NONE** The server's protection status will not change.
***ACTIVATE** The server will starting being protected.
***ACT/SUPP** The server will start being protected and the program shown as the Current Supplemental will be remembered.
***DEACTIVATE** The server will stop being protected.
***DEACT/SUPP** The server will stop being protected and the program shown as the Current Supplemental will be registered on the server's exit point.

Current program

The Current program column displays the program registered to protect the server.

Current supplemental

*YES in this field indicates the exit program currently is registered to the exit point as supplemental to Exit Point Manager's exit program. However, a Powertech Exit Point Manager exit program cannot be supplemental to itself. This shows the program currently set up within Powertech Exit Point Manager as the supplemental exit program for that exit point. If an exit point is deactivated with the Reinstate supplemental option, the supplemental program will be registered as the exit program at activation time. *NONE indicates there is no supplemental exit program for the exit point.

You may see values that are not program names here. They will be formatted as follows: The first two characters are always "NS" (Exit Point Manager) and the version of the product in which that program exists follows. If you see *ERROR for the version, the library containing that version is damaged and the version is not available.

If a server is activated with the "retain supplemental" option, this exit program will, at activation time, be made supplemental to the Exit Point Manager exit program. Supplemental exit programs are executed after Exit Point Manager has processed the server transaction.

Options

You can select from the following options on the Work with Activation panel:

1=Set to Activate

Will begin protection of the server at the next activation.

2=Set to Deactivate

Will end protection of the server at the next activation.

> **NOTE:** To deactivate all exit points, press `F14` (Set all to Deactivate).

3=Remove pending change

Select option **3** to remove a pending change from a server so that no changes are made to the server when you run activation. Use this option if you've already set an exit point to activate (or deactivate), and want to remove the pending change for the exit point.

11=Set to Activate/Retain supplemental

Select option **11** to flag the exit point for activation and retain the existing exit program, making it supplemental to the Exit Point Manager exit program.

12=Set to Deactivate/Reinstate supplemental

Select option **12** to flag the exit point for deactivation (remove the Exit Point Manager exit program) and reinstate the supplemental program as the exit program. Use the following function keys to activate the selected exit points:

Command Keys

F3 (Exit):

Exit the program without processing any pending changes.

F5 (Refresh):

Refresh the panel.

F12 (Cancel):

Exit the panel without processing any pending changes.

F13 (Set all to Activate):

Select all servers to begin protection, with the exception of the sockets-related servers. These can potentially render your system unreachable via TCP and need to be treated with the utmost caution. They can still be activated by selecting them with a '1'.

F14 (Set all to Deactivate):

Press `F14` to set all servers to *DEACTIVATE.

F15 (Reset all):

Press `F15` to reset all fields to default settings of *NONE.

F18 (Add silent activation):

Press `F18` to specify a silent activation. Use this if you plan to schedule an IPL during evening hours or on a weekend. When you select silent activation, you accept the activation setup so it is ready to be applied at the next system IPL. A message displays at the bottom of the panel confirming the silent activation request. See Using Silent Activation.

F19 (Remove silent activation):

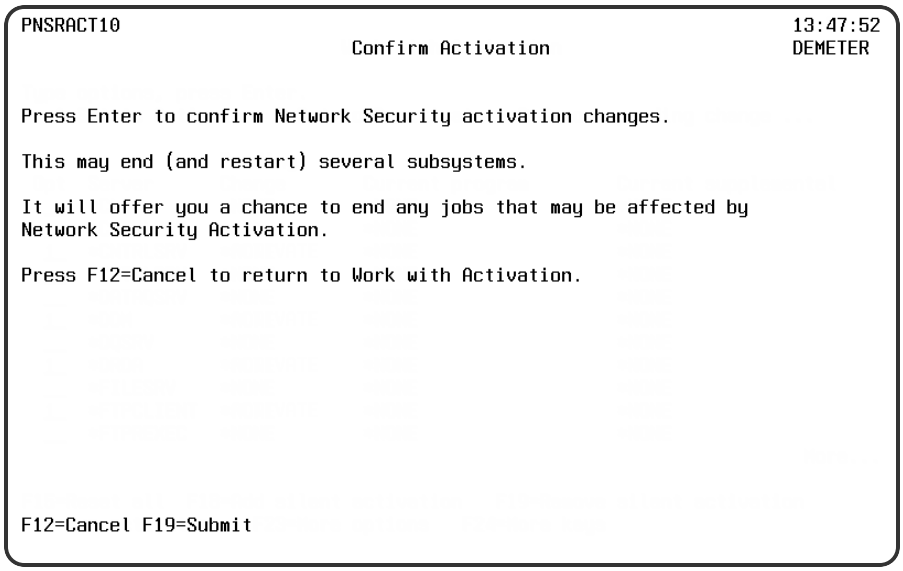
Press `F19` to remove a silent activation request. The confirmation message, Silent activation canceled, displays at the bottom of the Work with Activation panel.

> **NOTE:** If you enabled silent activation on your system, you must select this option before deleting Exit Point Manager from your system to ensure it's removed properly.

F20 (Run activation):

For an Interactive activation:

1. Press `F20` to run the activation request. You can run the activation after you've set one or more exit points to activate (by selecting option **1**, Set to Activate, `F13`, Set all to Activate, or option **11**, Set to Activate/Retain supplemental). The Confirm Activation panel displays when you press `F20`.



2. Press `Enter` to confirm the Exit Point Manager activation or press `F19` to submit the activation to batch.
3. If you don't want to accept the current activation setup, press `F12` to return to the Work with Activation panel.

If the activation request finds active server jobs, the Server Jobs to End panel displays with a list of the jobs. We recommend that you end all active server jobs to complete the activation. Follow the instructions on the panel to end the jobs.

When the activation completes, a confirmation message displays at the bottom of the Work with Activation panel.

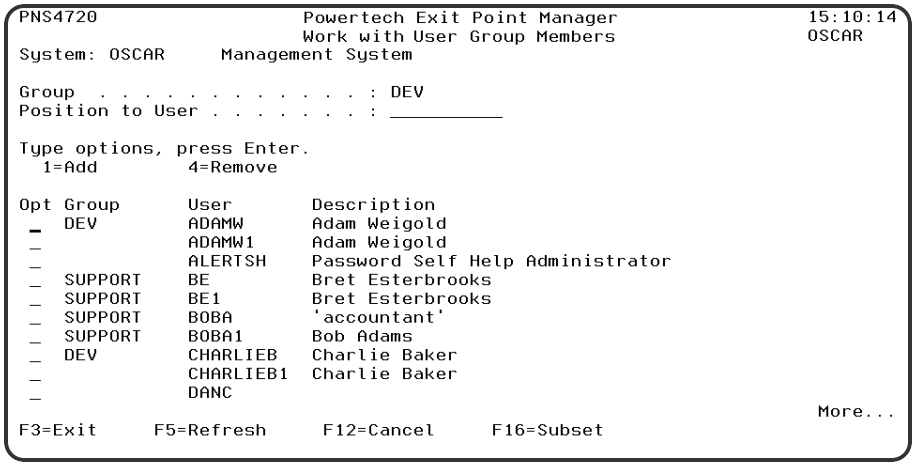
> **NOTE:** If the operating system NetServer was active prior to adding the Exit Point Manager exit programs to the IBM exit points, it should restart after activation. To check if the NetServer is active, enter the following command:

WRKACTJOB SBS(QSERVER) JOB (QZLSSERVER)

If the QZLSSERVER job is not active, you must restart the NetServer. Use the following command to start the NetServer:

STRTCPSVR *NETSVR

Work with User Group Members



How to Get There

From the Exit Point Manager Main Menu, select option **7**, Work with User Groups, then choose **3** for a Group.

What it Does

The Work with User Group Members panel allows you to add a user profile to, or remove a user profile from, a User Group.

On this panel, the selected User Group is the one used for additions. This User Group is shown near the top of the panel.

Options

1=Add

Adds the selected User to the selected User Group.

4=Remove

Removes the selected User from the corresponding User Group.

Field Descriptions

System

System indicates the target of any operations you perform. When you add rules, for example, those rules will be sent to, and will affect processing on, the System named.

Group

This is the current selected User Group. It is the group into which profiles would be added.

Position to User

This allows positioning to a starting point for the subfile.

Opt

Enter a valid option from the list of options provided on the list panel.

Group
Name of the User Group, if any, in which the User is a member.

User
Name of the User Profile.

Description
Description of the User Profile.

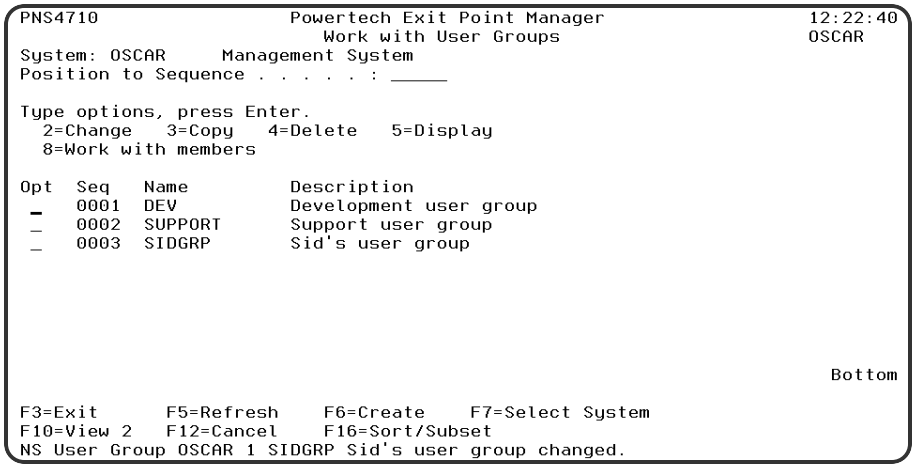
Command Keys
F3=Exit: Exit the current panel without processing any pending changes.

F5=Refresh: Refreshes the panel and resets all available text fields.

F12=Cancel: Exit the current panel without processing any pending changes.

F16=Subset: Displays parameters to subset the list to a more manageable number of items.

Work with User Groups



How to Get There
From the Exit Point Manager Main Menu, select option **7**, Work with User Groups.

What it Does
The Work with User Group panel allows you to maintain User Groups.

A User Group is simply a container for a group of user profile names. A User Group can be used in place of a user profile name in user rules.

The sequence number of a User Group determines the order in which it will be used by the exit point programs.

For example, if there are three User Rules with User Groups for a specific Server/Function, and all three have USER1 as a member, then the User Rule for the User Group with the lowest sequence number will be used by the exit programs (if a User Rule with the specific user name of 'USER1' is not found).

If a group profile is a member of a User Group, the exit programs will not test for the individual profiles that have that profile as a group (or supplemental group) profile.

Field Descriptions

System
System indicates the target of any operations you perform. When you add rules, for example, those rules will be sent to, and will affect processing on, the System named.

Position To
This allows positioning to a starting point for the subfile.

Opt
Enter a valid option from the list of options provided on the list panel.

Seq
Enter the sequence number used that will be used to determine the order in which this User Group will be evaluated by the exit point programs.

For example, if there are three User Rules with User Groups for a specific Server/Function, and all three have USER1 as a member, then the User Rule for the User Group with the lowest sequence number will be used by the exit programs (if a User Rule with the specific user name of 'USER1' is not found).

Name
The User Group name is a short name you assign to a group of user profiles to help you identify the group.

This name is required to be a valid OS name.

Description
The User Group description is a short textual description of the User Group. It is typically used to indicate the purpose or contents of the User Group.

Command Keys
F3=Exit: Exit the current panel without processing any pending changes.

F5=Refresh: Refreshes the panel and resets all available text fields.

F7=Select system: Use this command to work with data from another System.

F9=Memorized transactions: Opens the Work with Memorized Transactions panel.

F18=User Rules: Opens the Work with Security by User panel.

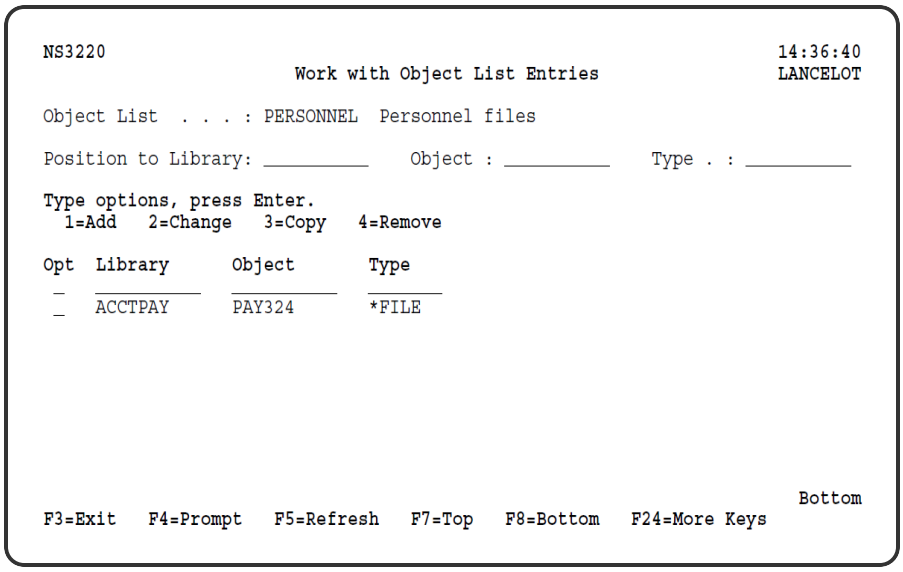
F19=Prefilters: Opens the Work with Loc+User Pre-filters panel.

F10=View2: Displays an alternate view of the panel. See Work with User Group Sequence panel.

F12=Cancel: Exit the current panel without processing any pending changes.

F16=Subset: Displays parameters to subset the list to a more manageable number of items.

Work with Object List Entries



How to Get There

From the Exit Point Manager Main Menu, select option **4** to display the Work with Security by Object panel. Select option **1** to display the Work with Object Lists panel, then enter an **8** in the Opt column on one of the Object Lists.

What it Does

The work with Object List Entries panels allow you to add, modify, or remove Object List Entries.

Options

You can select from the following options on the Work with Object List Entries panel.

1=Add

Displays the Add Object List Entry panel, which allows you to add an entry to the Object List. See Add Object List Entry panel.

2=Change

Displays the Change Object List Entry panel, which allows you to modify an existing entry. See Change Object List Entry panel.

3=Copy

Displays the Copy Object List Entry panel, which allows you to copy an entry to create a new Object List entry. See Copy Object List Entry panel.

4=Delete

Enter a 4 next to an entry to remove it from the Object List. A confirmation panel displays asking you to confirm the deletion. See Confirm Choices panel.

Field Descriptions

Opt
Enter a valid option from the list of options provided on the list panel.

Library
The Library is the name of the library in which an object exists. This name is required to be a valid OS name. The special value <UNKNOWN> represents the lack of an identifiable library name. Circumstances arise when an unqualified object reference cannot be resolved to the actual object on the system, so the library name cannot be determined. Exit Point Manager allows you to make Object Rules to cover these circumstances by specifying the <UNKNOWN> special value for the library portion of an Object List Entry.

Object
Object is the name of an object in a library. This name is required to be a > valid OS name.

Type
Object Type is the type of an object in a library.

Command Keys
F3 (Exit): Exit the panel without processing any pending changes.

F4 (Prompt): Displays a list of possible values from which you may select one.

F5 (Refresh): Refreshes the panel and resets all available text fields.

F7 (Top): Positions the list panel to the first record.

F8 (Bottom): Positions the list panel to the last record.

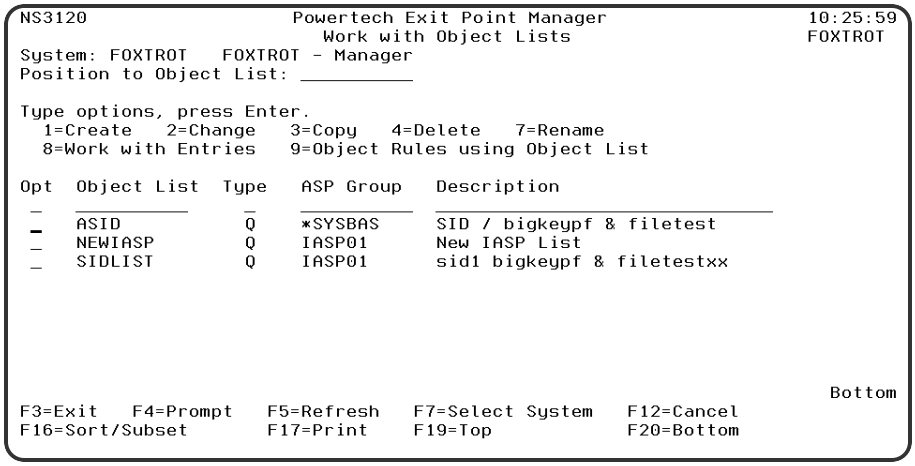
F12 (Cancel): Exit the panel without processing any pending changes.

F16 (Sort/Subset): Allows you to sort and subset information by library, object, and type.

F17 (Print): Prompts the PRTOBJL command to print the list of Object List Entries using your current sort/subset criteria.

F24 (More keys) Displays more function keys on the bottom of the panel (listed above).

Work with Object Lists



How to Get There

From the Exit Point Manager Main Menu, select option **4** to display the Work with Security by Object panel. Select option **1** to display the Work with Object Lists panel.

What it Does

The work with Object Lists panels allow you to create, modify, delete and perform other operations upon Object Lists. An Object list is simply a list of names of objects. These lists of objects are attached to Users or Locations on Object Rules. These rules help protect objects from outside access.

Options

You can select from the following options on the Work with Object Lists panel.

1=Create

Allows you to create a new Object List. See Create Object Lists panel.

2=Change

Enter a 2 next to an existing Object List to change the type or description for the list. See Change Object List panel.

3=Copy

Enter a 3 next to an Object List to copy the existing list. You must enter a name for the new Object List on the Copy Object List panel. See Copy Object List panel.

4=Delete

Enter a 4 next to an Object List to delete the list from Exit Point Manager. A confirmation panel displays asking you to confirm you want to delete the selected list(s). See Confirm Choices panel.

7=Rename

Enter a 7 next to an Object List to rename the list. See Rename Object List panel.

8=Work with Entries

Enter an 8 next to an Object List to display the Work with Object List Entries panel, which allows you to add objects to the Object List. See Work with Object List Entries panel.

9=Object Rules using Object List

Displays a list of the location or user rules that use the Object List. You can add a new rule, change or delete an existing rule, and activate or deactivate a rule. See Object Rules using Object List panel.

Field Descriptions

Opt

Enter a valid option from the list of options provided on the list panel.

Object List

The Object List name is a short name you assign to a list of objects to help you identify the list. This name is required to be a valid OS name.

Type

The Object List type determines what type of entries can be added to an Object List. Object lists can hold native object specifications (library, object and type) or paths to IFS objects.

Valid values are:

Q The Object List entries are native object specifiers.

I The Object List entries are paths to IFS objects.

ASP Group

This is the name of an ASP Group. It is used in rule evaluation to determine if an object referenced in a transaction is the one specified on the object entries for this list.

Valid values are:

***SYSBAS** The Object List entries refer to those objects in *SYSBAS.

***ALL** The Object List entries refer to those objects in any namespace.

Description

The Object List description is a short textual description of the Object List. It is typically used to indicate the purpose or contents of the Object List.

Command Keys

F3 (Exit): Exit the panel without processing any pending changes.

F4 (Prompt): Displays a list of possible values from which you may select one.

F5 (Refresh): Refreshes the panel and resets all available text fields.

F7 (Select System): Use this command key to work with data from a different System.

F11 (View): Changes the data presented in the list.

F12 (Cancel): Exit the panel without processing any pending changes.

F16 (Sort/Subset): Allows you to sort and subset information by Object List, type, and/or description.

F17 (Print): Prompts the PRTOBJL command to print the list of Object Lists using your current sort/subset criteria.

F19 (Top): Positions the panel list at the first record.

F20 (Bottom): Positions the panel list at the last record.

Work with Object Rules by User

```
NS3330                                                          09:56:49
                      Work with Object Rules by User            HS42
System: HS72      HS72 - ENDPOINT
Position to User . . . : __________

Type options, press Enter.
  1=Create   2=Change   3=Copy   4=Delete   5=Display   8=Activate Rule
  9=Deactivate Rule
                                                 Data Accesses
Opt User            Object List   Operation  Authority  Aud Msg Cap Switch
 _  _____           __________ _  _________  __________ _   _   _   __________
 _  *PUBLIC         PAYROLL    I  *READ      *OS400     *   *   *   *NONE
 _  ANNAM           PAYROLL    I  *ALL       *REJECT    *   *   *   *NONE
 _  MARKJ           PERSONNEL  Q  *ALL       *OS400     *   *   *   *NONE

                                                                      Bottom
F3=Exit   F4=Prompt   F5=Refresh   F7=Select System   F11=Object View
F12=Cancel   F16=Sort/Subset   F19=Top   F20=Bottom   F17=Print
Object Rule successfully created.
```

How to Get There

From the Exit Point Manager Main Menu, select option **4** to display the Work with Security by Object panel. Select option **2** to display the Work with Object Rules by User panel.

What it Does

The work with Object Rules by User panels allow you to create, modify, and delete Object Rules that pertain to Users. Object Rules can be active or inactive. On this panel, the inactive rules are colored yellow and the active rules are colored green.

Options

1=Create

Enter a 1 in the Opt column at the top of the list to open the Create Object Rule by User panel, where you can create an Object Rule linking a User to an Object List. When you've defined your rule, press `Enter` to display the Select Target Server Functions for Object Rule panel.

2=Change

Enter a 2 next to an object rule to display the Change Object Rule by User panel, where you can modify an Object Rule's attributes. Enter the changes you want to make and press `Enter` to display the Select Target Server Functions for Object Rule panel. See Object Rules for more information.

3=Copy

Enter a 3 next an object rule to display the Copy Object Rule by User panel where you can create a new Object Rule using an existing rule as the basis for the new rule. You can enter a new user name and make other changes to the values specified in the rule. Press `Enter` to display the Select Target Server Functions for Object Rule panel.

4=Delete

Enter a 4 next to an object rule to delete it. A confirmation panel displays asking you to confirm the deletion. See Confirm Choices panel.

5=Display

Enter a 5 next to a rule to display the Display Object Rule by User panel. You cannot make any changes on this panel, it is information only.

8=Activate Rule

Enter an 8 next to a rule to activate it if it is inactive. A confirmation panel displays asking you to confirm the activation request. See Confirm Choices panel. The Select Target Server Functions for Object Rule panels display allowing you to define a new filter rule.

9=Deactivate Rule

Enter a 9 next to a rule to deactivate it. A confirmation panel displays asking you to confirm the deactivation request. See Confirm Choices panel. If the rule is the last active rule for the user, the Specify Filter Rule Options panel displays so you can specify how you want Exit Point Manager to handle any *MEMOBJ filter rules that exist for the object rule. See Deleting an Object Rule for more information on *MEMOBJ filter rules.

Field Descriptions

Opt

Enter a valid option from the list of options provided on the list panel.

User

User represents the identity of the person initiating a transaction as a user profile. The special value *PUBLIC, when used on a rule, means that the rule applies to any User lacking a specific rule. when used as a subset or selection parameter, *PUBLIC means to select all such rules for display or printing.

Object List

The Object List name is a short name you assign to a list of objects to help you identify the list. This name is required to be a valid OS name. The Object List name is immediately followed by its type, which can be one of the following values:

Q The Object List entries are native object specifiers.
I The Object List entries are paths to IFS objects.

Operation

The operation to which the rule applies.

***ALL** The rule applies to all operations.
***CREATE** The rule applies to attempts to create an object matching an entry defined in the Object List.

***READ** The rule applies to attempts to read an object matching an entry defined in the Object List.
***UPDATE** The rule applies to attempts to update an object matching an entry defined in the Object List.
***DELETE** The rule applies to attempts to delete an object matching an entry defined in the Object List.

Data Accesses/Object Accesses

Data Accesses define user rights to the data contained in the objects in the Object List. Object Accesses define user rights to the actual objects in the Object List. Press **F11** to switch the view between the two types of access.

Authority

Authority represents the action to be taken when a rule is found that matches the data present on a transaction. This Authority value pertains to Data Accesses.

The valid values are:

***OS400** The transaction will be allowed and object authority will be determined by the operating system.
***REJECT** The transaction will not be allowed.
***SWITCH** The transaction will be allowed and the transaction will occur as if the user profile named as the Swap Profile had initiated the transaction. After switching to the Swap Profile, the authority used during the transaction will be determined by the operating system.

Aud (Audit Transactions)

The Audit transactions flag controls the logging of transactions to the Log Journal set up on the work with Exit Point Manager System Values panel. This Aud flag pertains to Data Accesses.

The valid values are:

Y The transaction will be logged to the Log Journal.
N The transaction will not be logged to the Log Journal.
* The default value from a prior rule will control the logging.

Msg (Send Messages)

The Send messages flag controls the sending of messages to the Log Message Queue set up on the work with Exit Point Manager System Values panel. This Msg flag pertains to Data Accesses.

The valid values are:

Y A log message will be sent to the Log Message Queue.
N A log message will not be sent to the Log Message Queue.
* The default value from a prior rule will control the logging.

Cap (Capture Transactions)

The Capture transactions flag controls whether transactions are remembered in Exit Point Manager for later memorization. Once captured, transactions can become Memorized Transactions which can act as rules. This Cap flag pertains to Data Accesses.

The valid values are:

Y Capture transactions.
N Do not capture transactions.
* Use the audit value for the server/function.

Switch Profile

The Switch profile holds the name of a user profile whose authority is used to process the transaction instead of the authority of the User initiating the transaction. The transaction is executed as, and uses the authority of, this Switch profile.

Switch profile is allowed only when Authority contains *SWITCH or *MEMSWITCH, if *MEMSWITCH is allowed. Otherwise it must contain *NONE. This Switch pertains to Data Accesses.

Command Keys

F3 (Exit): Exit the panel without processing any pending changes.

F4 (Prompt): Displays a list of possible values from which you may select one.

F5 (Refresh): Refreshes the panel and resets all available text fields.

F7 (Select System): Use this command key to work with data from a different System.

F11 (Object View): Changes the displayed detail columns to those that control Object Accesses.

F12 (Cancel): Exit the panel without processing any pending changes.

F16 (Sort/Subset): Allows you to sort and subset information by user, Object List, and/or operation.

F17 (Print): Prompts the PRTOBJL command to print the list of Object Lists using your current sort/subset criteria.

F19 (Top): Positions the panel list at the first record.

F20 (Bottom): Positions the panel list at the last record.

Work with Security by Object panel

Work with Object Rules by Location

```
NS3320                                                          09:59:37
                    Work with Object Rules by Location          HS42
System: HS72      HS72 - ENDPOINT
Position to Location . : _______________

Type options, press Enter.
  1=Create   2=Change   3=Copy   4=Delete   5=Display   8=Activate Rule
  9=Deactivate Rule
                                          ___________Data Accesses___________
Opt Location        Object List   Operation  Authority  Aud Msg Cap Switch
 _  _______________ ___________   _________  __________ _   _   _   _________
 _  *ALL            PAYROLL    I  *DELETE    *OS400     *   *   *   *NONE
 _  *ALL            PERSONNEL  Q  *ALL       *REJECT    *   *   *   *NONE
 _  192.168.003.004 PAYROLL    I  *ALL       *OS400     *   *   *   *NONE
                                                                    Bottom
F3=Exit   F4=Prompt   F5=Refresh   F7=Select System   F11=Object View
F12=Cancel   F16=Sort/Subset   F19=Top   F20=Bottom   F17=Print
```

How to Get There

From the Exit Point Manager Main Menu, select option **4** to display the Work with Security by Object panel. Select option **3** to display the Work with Object Rules by Location panel.

What it Does

The work with Object Rules by Location panels allow you to create, modify, and delete Object Rules. Object Rules can be active or inactive. On this panel, the inactive rules are colored yellow and the active rules are colored green.

Options

1=Create

Enter a **1** in the Opt column at the top of the list to open the Create Object Rule by Location panel where you can create an Object Rule linking a Location to an Object List. When you've defined your rule, press `Enter` to display the Select Target Server Functions for Object Rule panel.

2=Change

Enter a **2** next to an object rule to display the Change Object Rule by Location panel, where you can modify an Object Rule's attributes. Enter the changes you want to make and press `Enter` to display the Select Target Server Functions for Object Rule panel. See Object Rules for more information.

3=Copy

Enter a **3** next an object rule to display the Copy Object Rule by Location panel where you can create a new Object Rule using an existing rule as the basis for the new rule. You can enter a new user name and make other changes to the values specified in the rule. Press `Enter` to display the Select Target Server Functions for Object Rule panel. See Object Rules for more information

4=Delete

Enter a **4** next to an object rule to delete it. A confirmation panel displays asking you to confirm the deletion.

5=Display

Enter a **5** next to a rule to display the Display Object Rule by User panel. You cannot make any changes on this panel, it is information only.

8=Activate Rule

Enter an **8** next to a rule to activate it if it is inactive. A confirmation panel displays asking you to confirm the activation request. The Select Target Server Functions for Object Rule panels display allowing you to define a new filter rule.

9=Deactivate Rule

Enter a **9** next to a rule to deactivate it. A confirmation panel displays asking you to confirm the deactivation request. If the rule is the last active rule for the location, the Specify Filter Rule Options panel displays so you can so you can specify how you want Exit Point Manager to handle any *MEMOBJ filter rules that exist for the object rule. See Deleting an Object Rule for more information on *MEMOBJ filter rules.

Field Descriptions

Location

Location represents the source of a transaction. Location can hold an IP Address, an IP Address Group or the name of an SNA Communications Device. The special value *ALL, when used on a rule, means that the rule applies to any rule means that the rule applies to any Location lacking a specific rule. when used as a subset or selection parameter, *ALL generally means to select all such rules for display or printing.

Object List

The Object List name is a short name you assign to a list of objects to help you identify the list. This name is required to be a valid OS name. The Object List name is immediately followed by its type, which can be one of the following values:

Q The Object List entries are native object specifiers.
I The Object List entries are paths to IFS objects.

Operation

The operation to which the rule applies.

***ALL** The rule applies to all operations.
***CREATE** The rule applies to attempts to create an object matching an entry defined in the Object List.
***READ** The rule applies to attempts to read an object matching an entry defined in the Object List.
***UPDATE** The rule applies to attempts to update an object matching an entry defined in the Object List.
***DELETE** The rule applies to attempts to delete an object matching an entry defined in the Object List.

Data Accesses/Object Accesses

Data Accesses define access rights by location to the data contained in the objects in the Object List. Object Accesses define access rights by location to the actual objects in the Object List. Press `F11` to switch the view between the two types of access.

Authority

Authority represents the action to be taken when a rule is found that matches the data present on a transaction. This Authority value pertains to Data Accesses.

The valid values are:

***OS400** The transaction will be allowed and object authority will be determined by the operating system.
***REJECT** The transaction will not be allowed.
***SWITCH** The transaction will be allowed and the transaction will occur as if the user profile named as the Swap Profile had initiated the transaction. After switching to the Swap Profile, the authority used during the transaction will be determined by the operating system.

Aud (Audit Transactions)

The Audit transactions flag controls the logging of transactions to the Log Journal set up on the work with Exit Point Manager System Values panel. This Aud flag pertains to Data Accesses.

The valid values are:

Y The transaction will be logged to the Log Journal.
N The transaction will not be logged to the Log Journal.
* The default value from a prior rule will control the logging.

Msg (Send Messages)

The Send messages flag controls the sending of messages to the Log Message Queue set up on the work with Exit Point Manager System Values panel. This Msg flag pertains to Data Accesses.

The valid values are:

Y A log message will be sent to the Log Message Queue.
N A log message will not be sent to the Log Message Queue.
* The default value from a prior rule will control the logging.

Cap (Capture Transactions)

The Capture transactions flag controls whether transactions are remembered in Exit Point Manager for later memorization. Once captured, transactions can become Memorized Transactions which can act as rules. This Cap flag pertains to Data Accesses.

The valid values are:

Y Capture transactions.
N Do not capture transactions.
* Use the audit value for the server/function.

Switch Profile

The Switch profile holds the name of a user profile whose authority is used to process the transaction instead of the authority of the User initiating the transaction. The transaction is executed as, and uses the authority of, this Switch profile.

Switch profile is allowed only when Authority contains *SWITCH or *MEMSWITCH, if *MEMSWITCH is allowed. Otherwise it must contain *NONE. This Switch pertains to Data Accesses.

Command Keys

F3 (Exit): Exit the panel without processing any pending changes.

F4 (Prompt): Displays a list of possible values from which you may select one.

F5 (Refresh): Refreshes the panel and resets all available text fields.

F7 (Select System): Use this command key to work with data from a different System.

F11 (Object View): Changes the displayed detail columns to those that control Object Accesses.

F12 (Cancel): Exit the panel without processing any pending changes.

F16 (Sort/Subset): Allows you to sort and subset information by location, Object List, and/or operation.

F17 (Print): Prompts the PRTOBJL command to print the list of Object Lists using your current sort/subset criteria.

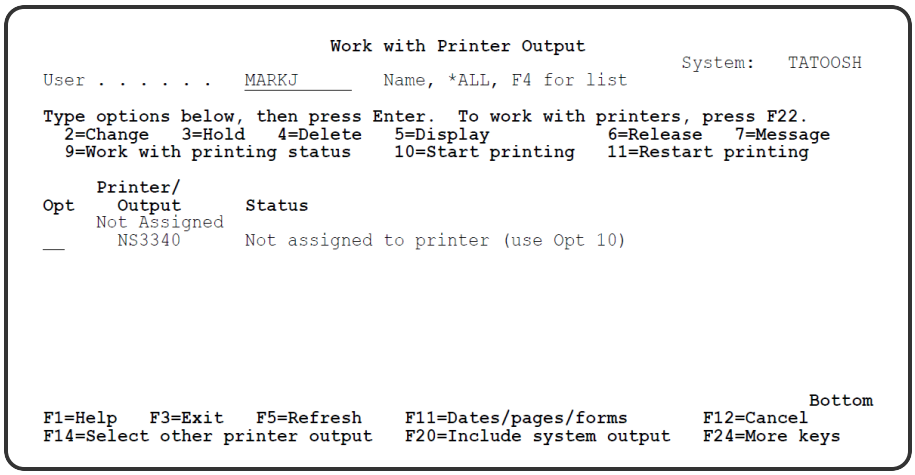
F19 (Top): Positions the panel list at the first record.

F20 (Bottom): Positions the panel list at the last record.

Work with Printer Output

NOTE: If you have *JOBCTL or *SPLCTL authority, you can use `F14` (Select other printer output) to see the printer output of one or more other users.

The Work with Printer Output display shows you the status of printer output. Use this list to do common tasks related to printer output, such as selecting a printer, changing the printer the output goes to, holding or releasing the printer output, or changing other printing options. From this display, you can use `F22`, if available, to work with printers.



Field Descriptions

User

This field shows the name of the user whose printer output is shown.

To display other users‘ printer output, specify the user's name or *ALL to display all users‘ printer output. You can press `F4` to see a list of user names to choose from when the cursor is positioned in the field.

You can use the asterisk (*) after any characters to show a list of all printer output for user names that start with the specified characters. For example, if you enter T*, you will get a list of all users that begin with T and their printer output. If you enter SMI*, you will get a list of all users that begin with SMI (Smirf, Smith, Smitty, and so on) and their printer output.

To display other user's printer output, you must have *JOBCTL or *SPLCTL authority.

Options

Type an option number in the Opt column next to a printer output name and press `Enter`. You can type option numbers next to more than one printer output to do tasks one after the other. Only the options that you have authority to do are shown. You can choose:

2=Change

Shows you a display where you can change the following information for your printer output:

- The printer to use
- The number of copies to print

- The first page of output to print
- The last page of output to print
- The type of forms to print on
- Whether to print this output next
- Whether to save the printer output

3=Hold

Holds the printer output. The output is temporarily stopped from printing and is not printed until it is released.

4=Delete

Deletes the printer output and removes it from the system.

5=Display

Displays the contents of the printer output on your display. This is what will actually print on the printer.

6=Release

If the printer output is held, it is released so that it can print.

7=Message

If the printer output status is Message Waiting or Printer Message, this option displays the message the printer output is waiting on. You can also reply to the message if you have the proper authority.

9=Work with printing status

Allows you to get more technical information about the status and gives directions on how to work with the status.

10=Start printing

If the printer is stopped, you can start the printer you want to print on. If the printer output has not been assigned to a printer you can specify and start the printer you want to print on.

11=Restart printing

Allows you to start a printer that stopped before printing all the printer output. Shows you a display with options to specify:

- The page you want to restart printing on
- If you want to print the printer output next
- A printer to use if a printer has not been specified
- If you want to save the printer output

Printer/Output

The name of a printer followed by the name of each piece of printer output waiting to print on that printer. The names of the printer output are indented 2 positions under the printer names. If the name of the printer is Not Assigned, a printer has not been specified for the printer output.

The printer output name is either a 10-character name that was used to describe the piece of printer output when it was created or if no name was specified, the printer output name is the file name used by the program that created the printer output.

Status

The status of the printer output is shown. The status can be any of the following:

- Printer stopped: Use option **10** (if available) to start printing. Otherwise, contact your system operator.
- Printer waiting: Use option **9** (if available) to print. Otherwise, contact your system operator.
- Printer message: Use option **7** (if available) to display and answer the message that is preventing the printer from printing. Otherwise, contact your system operator.
- Message waiting: Use option **7** (if available) to display and answer the message needing a reply for this printer output. Otherwise, contact your system operator.
- Waiting to print: Will print after printer output ahead of it prints.
- Still being created: A program is still creating this printer output.
- Not scheduled to print yet: A job must finish before this output prints.
- Held: Use option **6** (if available) to release.
- Printed and kept: Use option **6** to print this printer output again.
- Printing page x of y: Currently printing.
- Not assigned to printer: Use option **10** to assign the printer output to print on a specific printer.
- Printing starting or ending: Press `F5` (Refresh) to see if the status has changed.

Command Keys

F1 (Help): Provides additional information about using the display or a specific field on the display.

F3 (Exit): Exit the panel without processing any pending changes.

F4 (List): Shows a list of users on the system.

F5 (Refresh): Refreshes the panel and resets all available text fields.

F9 (Command line): Displays a command line that allows you to enter system commands. Note: This is not shown if you don't have the correct authority.

F11 (Dates/pages/forms): Changes the information displayed to show the date/time the printer output was created, the number of copies, total number of pages, and the form type that the printer output is to be printed on.

F12 (Cancel): Exit the panel without processing any pending changes.

F14 (Select other printer output): Allows you to change the contents of the printer output list. You can select the user, printer, status, and printer output.

F20 (Include system output): Displays job logs and printouts of storage (only shown if you have the correct authority).

F21 (Select assistance level): Allows you to select the level of assistance you want when interacting with the system. Possible choices (if available) are:

1=Basic assistance level

Shows the displays that provide the most assistance. Basic assistance level supports the more common user and operator tasks and does not use computer terminology.

2=Intermediate assistance level

Shows the displays that support all system tasks and uses computer terminology. Complicated tasks can be done using this level.

3=Advanced interface

Shows the displays that provide the same functions as the intermediate assistance level. However, the displays contain as much information as possible by not displaying the allowed function keys and options.

F22 (Work with printers): Displays a list of printers on the system on which the user has output printing or waiting to print and allows you to work with the printers.

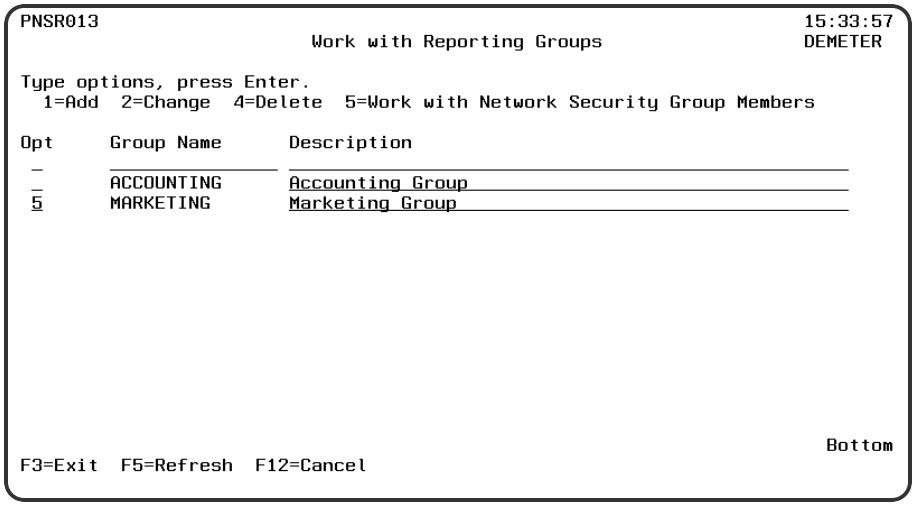
F24 (More keys): Changes the list of function keys shown at the bottom of the display (listed above).

Working with Report Group Members

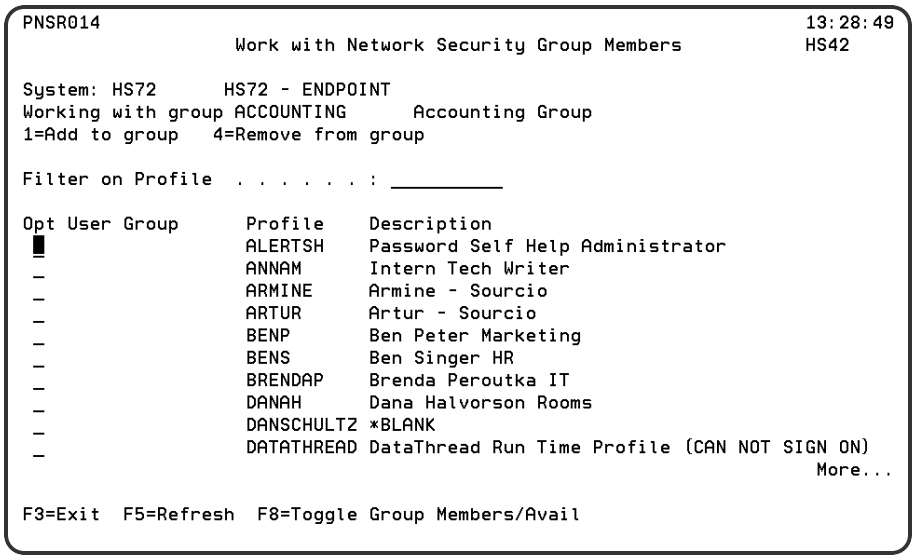
A Exit Point Manager reporting group allows you to assign users (user profiles) to the reporting groups you have created. Once you've associated user profiles with the group, you can run a report on the entire group.

Entering Reporting Group Members

1. To add members to a reporting group, select the group to which you want to add.
2. On the Work with Reporting Groups panel, enter option **5** next to the group name.



The Work with Exit Point Manager Group Members panel displays allowing you to add user profiles to a specified reporting group.



Work with Exit Point Manager Group Members Fields

Group Name

The name of the reporting group you selected.

User Profile

The user profiles that are members of the reporting group.

Work with Exit Point Manager Group Members Options

You can select from the following options to work with the reporting group members.

1=Add to group

Enter a **1** in the Opt column and enter the user profile you want to add to the reporting group. You can select the users you want to add by pressing **F8**, which switches views between group members and available users. In the Available Users view, you can enter a **1** next to multiple user profiles and add them to the group at one time.

4=Remove from group

Enter option **4** to remove a user from the reporting group.

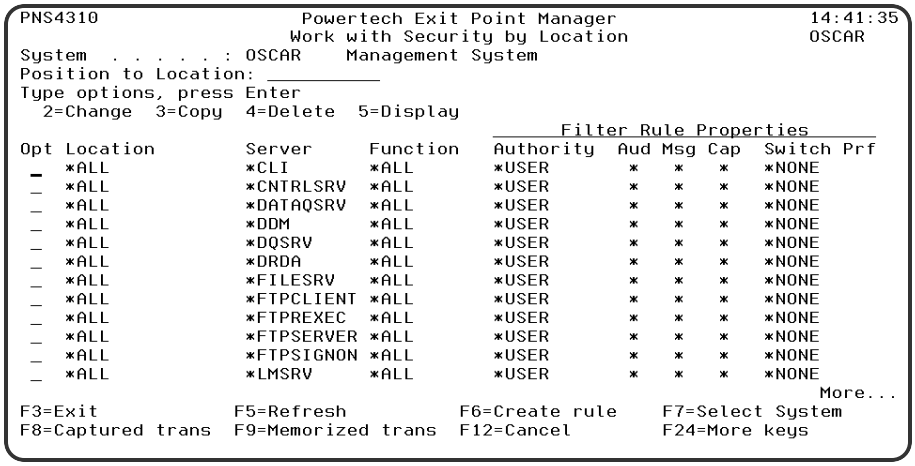
Command Keys

F3 (Exit): Exit the current panel without processing any pending changes.

F5 (Refresh): Refreshes the panel and resets all available text fields.

F12 (Cancel): Exit the current panel without processing any pending changes.

Work with Security by Location



How to Get There

From the Exit Point Manager Main Menu, select option **3**.

What it Does

The Work with Security by Location panel allows you to view or change Locations Rules.

Options

2=Change Choose this option for a rule to open the Change Location Rule panel where you can change a User Rule.

3=Copy Choose this option for a rule to open the Copy Location Rule panel where you can change a User Rule.

4=Delete Choose this option for a rule to delete it.

5=Display Choose this option to display the Location Rule Derivation panel for the rule.

Field Descriptions

The following describes the fields on the Work with Security by Location panel.

Opt

Enter a valid option from the list of options provided on the list panel.

System

System indicates the target of any operations you perform. When you add rules, for example, those rules will be sent to, and will affect processing on, the System named.

Position to Location

Used to position the list.

Location

Location represents the source of a transaction. Location can hold an IP Address, an IP Address Group or the name of an SNA Communications Device.

The special value *ALL, when used on a rule, means that the rule applies to any Location lacking a specific rule. When used as a subset or selection parameter, *ALL generally means to select all such rules for display or printing.

Function

A Function, or Server Function, in Exit Point Manager represents a class of operations that a given Server may perform. For example, the *SIGNON Server classifies its operations as those pertaining to changing passwords, generating authentication tokens, and retrieving signon information. Exit Point Manager has assigned easy-to-remember names to these Functions, such as CHGPWD, GENAUTTKN and RETRIEVE.

Authority Property

The authority assigned to the location for this server/function.

Possible values are:

***OS400** Exit Point Manager will use normal OS/400 authority for the location.
***REJECT** Exit Point Manager will reject requests for the specified location.
***SWITCH** Exit Point Manager will use the authority of the switch profile for the specified location. A switch profile entry is required.
***MEMREJECT** Check Memorized Transactions (MTR) for authority. If no MTR authority is encountered, Exit Point Manager will reject requests for the specified location.
***MEMOS400** Check Memorized Transactions (MTR) for authority. If no MTR authority is encountered, Exit Point Manager will use normal OS/400 authority for the location.
***MEMSWITCH** Check Memorized Transactions (MTR) for authority. If no MTR authority is encountered, Exit Point Manager will use the authority of the switch profile for the specified location. A switch profile entry is required.
***SRVFCN**Exit Point Manager will use the authority defined for the server/function.

Aud (Audit)

The Audit transactions flag controls the logging of transactions to the Log Journal set up on the Work with Exit Point Manager System Values panel.

Possible values are:

Y Log all requests by the location/server/function.
N Only log authority failures for the location/server/function.
* Use the audit value for the server/function.

Msg (Message)

The message property entry will determine if Exit Point Manager sends a message to the specified message queue for the location/server/function.

N No message is sent.
Y A message is sent to the Exit Point Manager message queue.
* Use the audit value for the server/function.

Cap (Capture Request)

Capture transactions for Memorized Transaction Request (MTR).

N Do not capture transactions.
Y Capture transactions.
* Use the audit value for the server/function.

Switch

The Switch profile holds the name of a user profile whose authority is used to process the transaction instead of the authority of the User initiating the transaction. The transaction is executed as, and uses the authority of, this Switch profile.

Switch profile is allowed only when Authority contains *SWITCH or *MEMSWITCH, if *MEMSWITCH is allowed. Otherwise it must contain *NONE.

Command Keys

F2 (Global Rule Facility): Maintain rules en mass.

F3 (Exit): Exit the current panel without processing any pending changes.

F5 (Refresh): Refreshes the panel and resets all available text fields.

F6 (Create rule): Creates a new location rule.

F8 (Captured trans): Goes to Work with Captured Transaction panel.

F9 (Memorized trans): Goes to Work with Memorized Transaction panel.

F10 (Copy loc): Copy all of current location authorities to another location. See Copy rules to another location window.

F12 (Cancel): Exit the current panel without processing any pending changes.

F13 (Display messages): Displays messages for user.

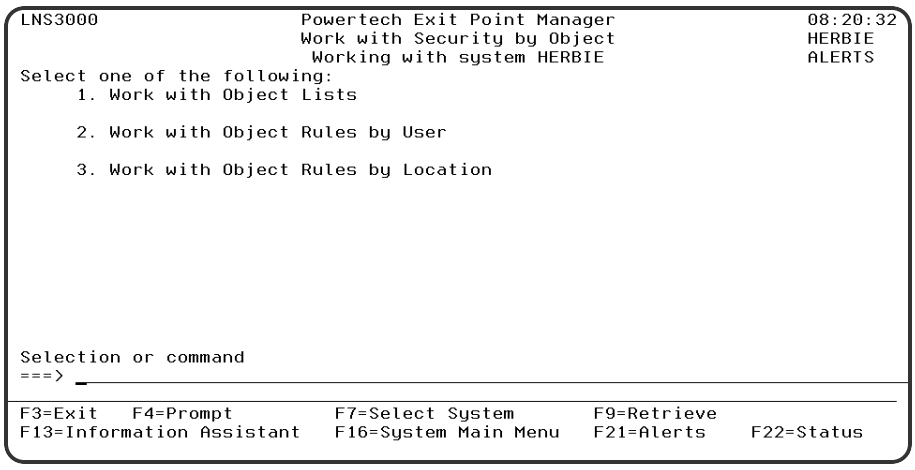
F14 (Work with submitted jobs): Displays jobs submitted from the current job.

F15 (Work with spooled files): Displays the user's print output.

F16 (Sort/subset): Opens the Location Rules Subset panel, which allows you to subset the list of User Rules by Server, Function, or Location.

F24 (More keys): Displays additional function keys (listed above).

Work with Security by Object



How to Get There

From the Exit Point Manager Main Menu, choose option **4** and press `Enter`.

What it Does

Use this panel to work with Security by Object.

Options

The following describes the fields on the Work with Security by Object panel.

Option 1 Use this option to work with Object Lists. See Work with Object Lists panel.

Option 2 Use this option to work with Object Rules concerning Users. See Work with Object Rules by User.

Option 3 Use this option to work with Object Rules concerning Locations. See Work with Object Rules by Location.

Command Keys

F3 (Exit): Exit the current panel without processing any pending changes.

F4 (Prompt): Provides assistance in entering or selecting a command.

F7 (Select System): Use this command key to work with data from a different System.

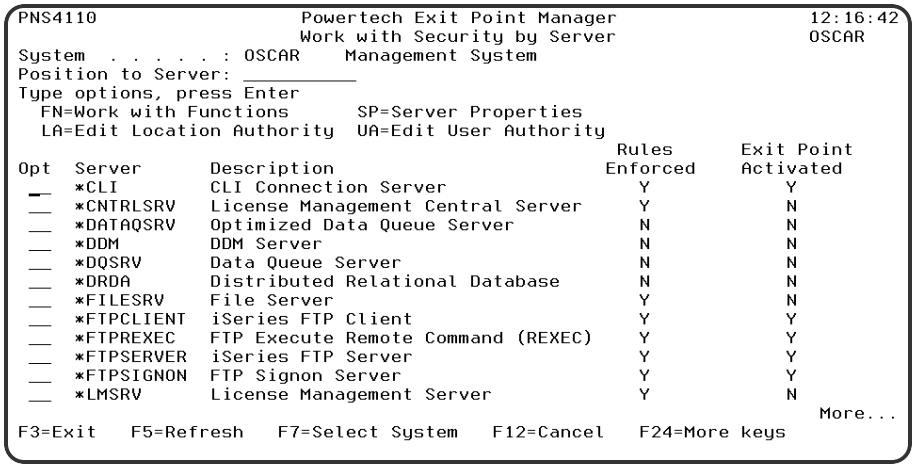
F9 (Retrieve): Displays the last command you entered on the command line and any parameters you included. Pressing this key once shows the last command you ran. Pressing this key twice shows the command you ran before that, and so on.

F13 (Information Assistant): Displays the Information Assistant menu with several types of assistance available. Press this key to access more information about the IMB i system.

F16 (System Main Menu): Displays the IBM i Main Menu (MAIN).

F22 (Status): Displays the Operational Resources pop-up window containing the status of several operation aspects of Powertech products.

Work with Security by Server



How to Get There

From the Exit Point Manager Main Menu, select option **1**.

What it Does

The work with Security by Server panel displays a list of all of the servers and whether they have location or user authorities specified for any/each server. From the work with Security by Server panel you can work with Server Functions, work with Location Authorities and Work with Server User Authorities.

Options

You can select from the following options on the Work with Security by Server panel. Press `F23` to see additional options.

> **NOTE:** You can enter an option next to more than one server at a time. This allows you to perform more than one task at a time.

FN=Work with Functions

Enter **FN** (Work with Functions) next to a server to display the Work with Security by Server/Function panel. Use the Work with Security by Server/Function panel to see a list of functions for a server, and to edit function location authorities and function user authorities. See Work with Security by Server/Function panel.

LA=Edit Location Authority and UA=Edit User Authority

To create or maintain Location and User authority rules, enter either **LA** (Edit Location Authority) or **UA** (Edit User Authority) next to a server. Option LA displays the Work with Security by Location panel; option UA displays the Work with Security by User panel. For more information on creating or maintaining rules, see Location Authority Rules and User Rules.

CT=Captured Trans and MT=Memorized Trans

To work with Captured transactions or Memorized transactions, enter either **CT** (Captured Trans)or **MT** (Memorized Trans) next to a server. Option CT displays the Work with Captured Transactions panel; option MT displays the Work with Memorized Transactions panel. For complete information on captured and memorized transactions, see Capturing Transactions and Memorizing Transactions.

SP=Server Properties

Enter SP (Server Properties) next to a server to display the Change Server Function Rule panel, which you can use to maintain and edit server function rules.

Field Descriptions

The following describes the fields on the Work with Security by Server panel.

Position To

This allows positioning to a starting point for the subfile.

Opt

Allows entry of a valid option for the function.

Server

The server ID is the name of the IBM server that authority is being specified.

Server Description

The description of the IBM server.

Rules Enforced

Indicates that Powertech Exit Point Manager will enforce rules for this server. See also Exit Pgm Active.

Y Exit Point Manager will enforce rules for this server.
N Exit Point Manager will not enforce rules for this server.

Exit Pgm Active

Indicates that a Powertech Exit Point Manager exit program is configured for this server. See also Rules Enforced.

Y Exit Point Manager exit program is active for the server.
N A Exit Point Manager exit program is not active for the server.

See also Activating Powertech Exit Point Manager.

Command Keys

F3 (Exit): Exit the current panel without processing any pending changes.

F5 (Refresh): Refreshes the panel and resets all available text fields.

F7 (Select System): Use this command key to work with data from a different System.

F12 (Cancel): Exit the current panel without processing any pending changes.

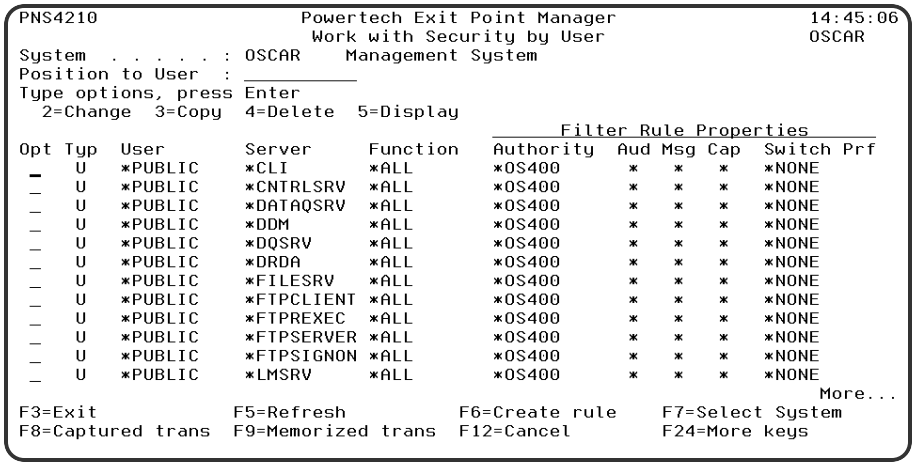
F13 (Display messages): Displays messages for user.

F14 (Work with submitted jobs): Displays jobs submitted from the current job.

F15 (Work with spooled files): Displays the user's print output.

F24 (More keys): Displays additional function keys (listed above).

Work with Security by User



How to Get There

Enter option **2** on the Exit Point Manager Main Menu.

What it Does

The work with Security by User panel allows you to maintain a user's server and server function filter rules. After entering a valid user profile, you can add, change, or delete the user's individual server and server function filter rules. You can also copy a user's filter rules to another user or delete all of the user's filter rules.

Options

2=Change Choose this option for a rule to open the Change User Rule panel where you can change a User Rule.

3=Copy Choose this option for a rule to open the Copy User Rule panel where you can change a User Rule.

4=Delete Choose this option for a rule to delete it.

5=Display Choose this option to display the User Rule Derivation panel for the rule.

Field Descriptions

System

System indicates the target of any operations you perform. When you add rules, for example, those rules will be sent to, and will affect processing on, the System named. The following describes the fields on the Work with Security by Server panel.

Position to User

Used to position the list.

Opt

Enter a valid option from the list of options provided on the list panel.

Typ

This field is used to indicate whether the associated User field refers to an O/S user profile or a Exit Point Manager User Group.

Valid values are:

U The associated User field refers to an O/S user profile.
G The associated User field refers to a Exit Point Manager user group.

User

If the associated User Type is a 'U', User represents the identity of the person initiating a transaction as a user profile.

The special value *PUBLIC, when used on a rule, means that the rule applies to any User lacking a specific rule. When used as a subset or selection parameter, *PUBLIC means to select all such rules for display or printing.

If the associated User Type is a 'G', User represents a Exit Point Manager User Group.

Server

A Server in Exit Point Manager is a controlled entry point into your system. These entry points are determined and defined by IBM. Exit Point Manager has assigned easy-to-remember names to these

controlled entry points.

Function

A Function, or Server Function, in Exit Point Manager represents a class of operations that a given Server may perform. For example, the *SIGNON Server classifies its operations as those pertaining to changing passwords, generating authentication tokens, and retrieving signon information. Exit Point Manager has assigned easy-to-remember names to these Functions, such as CHGPWD, GENAUTTKN and RETRIEVE.

Authority Property

The authority assigned to the user for this server/function. If authority is left blank, Exit Point Manager will remove the rule.

Possible values are:

***OS400** Exit Point Manager will use normal OS/400 authority for the user.
***REJECT** Exit Point Manager will reject requests for the specified user.
***SWITCH**Exit Point Manager will use the authority of the switch profile for the specified user. A switch profile entry is required.
***MEMREJECT** Check Memorized Transactions (MTR) for authority. If no MTR authority is encountered, Exit Point Manager will reject requests for the specified user.
***MEMOS400** Check Memorized Transactions (MTR) for authority. If no MTR authority is encountered, Exit Point Manager will use normal OS/400 authority for the user.
***MEMSWITCH** Check Memorized Transactions (MTR) for authority. If no MTR authority is encountered, Exit Point Manager will use the authority of the switch profile for the specified user. A switch profile entry is required.
***SRVFCN**Exit Point Manager will use the authority defined for the server/function.

Aud

The Audit transactions flag controls the logging of transactions to the Log Journal set up on the Work with Exit Point Manager System Values panel.

The valid values are:

* Uses the value found in the rule above this one in the rule hierarchy.
Y Logs all requests when this rule is enforced.
N Logs only access failures (rejects) for this rule.

Msg

The Send messages flag controls the sending of messages to the Log Message Queue set up on the Work with Exit Point Manager System Values panel.

The valid values are:

* Uses the value found in the rule above this one in the rule hierarchy.
Y Sends a message when this rule is enforced.
N Does not send a message when this rule is enforced.

Capture

The Capture transactions flag controls whether transactions are remembered in Exit Point Manager for later memorization. Once captured, transactions can become Memorized Transactions which can act as rules.

The valid values are:

* Uses the value found in the rule above this one in the rule hierarchy.
Y Captures the transaction when this rule is enforced.
N Does not capture the transaction when this rule is enforced.

Switch

The Switch profile holds the name of a user profile whose authority is used to process the transaction instead of the authority of the User initiating the transaction. The transaction is executed as, and uses the authority of, this Switch profile.

Switch profile is allowed only when Authority contains *SWITCH or *MEMSWITCH, if *MEMSWITCH is allowed. Otherwise it must contain *NONE.

The Work with Security by User panel allows you to view or change User Rules.

Command Keys

F2 (Global Rule Facility): Maintain rules en mass.

F3 (Exit): Exit the current panel without processing any pending changes.

F4 (Prompt): Display a list of valid values for field prompted.

F5 (Refresh): Refreshes the panel and resets all available text fields.

F6 (Create rule): Creates a new user rule.

F7 (Select system): Allows user to select a different silo system.

F8 (Captured trans): Allows user to go to the Work with Captured Transaction panel, which will be filtered based on the rule on which the cursor was positioned when F8 was pressed.

F9 (Memorized trans): Allows user to go to the Work with Memorized Transaction panel, which will be filtered based on the rule on which the cursor was positioned when F9 was pressed.

F10 (Copy user): Copy all of current user authorities to another user.

F12 (Cancel): Exit the current panel without processing any pending changes.

F13 (Display messages): Displays messages for user.

F14 (Work with submitted jobs): Displays jobs submitted from the current job.

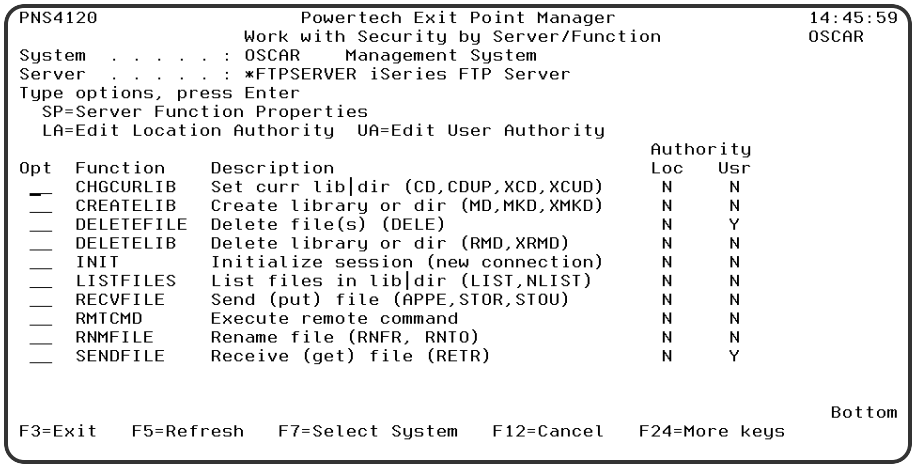
F15 (Work with spooled files): Displays the user's print output.

F16 (Sort/subset): Opens the User Rules Subset panel, which allows you to subset the list of User Rules by Server, Function, Type, or User.

F21 (User Groups): Allows user to go to the Work with User Groups panel.

F24 (More keys): Displays additional function keys (listed above).

Work with Security by Server/Function



How to Get There

From the Exit Point Manager Main Menu, select option **1**. Type **FN** for a server and press `Enter`.

What it Does

The Work with Security by Server/Function' panel displays a list of functions for a specific server and allows you to go to the Edit Location Authority and Edit User Authority.

Options

You can select from the following options on the Work with Security by Server/Function' panel:

LA=Edit Location Authority and UA=Edit User Authority

These options allow you to maintain server/function filter rules for locations or users. Enter **LA** to display the Work with Security by Location panel for the function on the server. Enter **UA** to display the Work with User Authorities panel for the function on the server. For more information on creating and maintaining rules, see Location Rules and User Rules.

CT=Captured Trans and MT=Memorized Trans

To work with Captured transactions or Memorized transactions, enter either **CT** (Captured Trans)or **MT** (Memorized Trans) next to a server. Option CT displays the Work with Captured Transactions panel; option MT displays the Work with Memorized Transactions panel. For complete information on captured and memorized transactions, see Capturing Transactions and Memorizing Transactions.

SP=Edit Server Function Properties

Enter SP to display the Change Server Function Rule panel, where you can change one or more of the properties for a selected server function.

Field Descriptions

Server ID

The server ID is the name of the IBM server that authority is being specified.

Opt

Allows entry of a valid option for the function.

Function
The function ID is the name of the IBM function that authority is being specified.

Function Description
The description of the IBM server function.

Location Authority
Indicates if there is location authority for the function for the server. 'Y' indicates a location authority record exists.

User Authority
Indicates if there is user authority for the function for the server. 'Y' indicates a user authority record exists.

Command Keys

F3 (Exit): Exit the current panel without processing any pending changes.

F5 (Refresh): Refreshes the panel and resets all available text fields.

F7 (Select system): Use this command to work with data from another System.

F8 (Captured Transactions): Displays the Work with Captured Transactions panel. See also Capturing Transactions.

F9 (Memorized Transactions): Displays the Work with Memorized Transactions panel. See also Memorizing Transactions.

F12 (Cancel): Exit the current panel without processing any pending changes.

F13 (Display messages): Displays messages for user.

F14 (Work with submitted jobs): Displays jobs submitted from the current job.

F15 (Work with spooled files): Displays the user's print output.

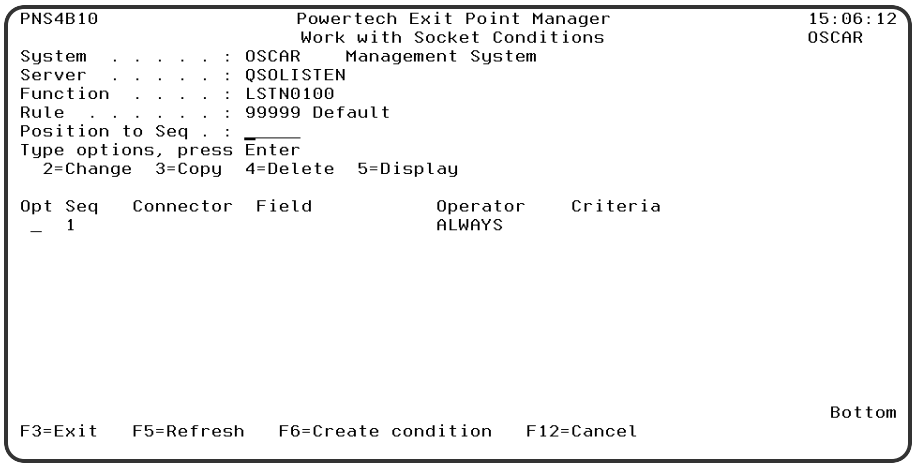
F23 (More options): Displays additional options at the top of the panel.

F24 (More keys): Displays additional function keys (listed above). The Work with Security by Server/Function' panel displays a list of functions for a specific server and allows you to go to the Edit Location Authority and Edit User Authority.

These flags do not include rules that apply to all functions. If there are rules that apply to all functions, but no rules that apply to the function specifically, the column displays an "N".

Work with Socket Conditions panel

WARNING: Misuse of Socket Rules can render your system unreachable via TCP. Exercise extreme caution when using this feature. Consider adding Socket Rules as not active and testing them using the Socket Rule test feature, and setting them to be not used by that feature and testing the rule set before removing them. If you render your system unreachable via TCP, you will need to access the system via the console in order to fix the rules (or to deactivate the Socket Rule servers).



How to Get There

On the Work with Socket Rules panel, choose option **1**, **2**, or **3**. Enter **8** for a Socket Rule.

What it Does

The Work with Socket Conditions panel allows you to view or change Socket Conditions.

Field Descriptions

System

System indicates the target of any operations you perform. When you add rules, for example, those rules will be sent to, and will affect processing on, the System named.

Server

A Server in Exit Point Manager is a controlled entry point into your system. These entry points are determined and defined by IBM. Exit Point Manager has assigned easy-to-remember names to these controlled entry points.

Function

A Function, or Server Function, in Exit Point Manager represents a class of operations that a given Server may perform. For example, the *SIGNON Server classifies its operations as those pertaining to changing passwords, generating authentication tokens, and retrieving signon information. Exit Point Manager has assigned easy-to-remember names to these Functions, such as CHGPWD, GENAUTTKN and RETRIEVE.

Rule

The Socket Rule to which this Socket Condition belongs.

A Socket Rule without a Socket Condition, or with an invalid Socket Condition, will not be enforced.

Position to Sequence

Used to position the list.

Seq

The sequence number of a Socket Condition determines the order in which it is combined with other Socket Conditions for a Socket Rule.

Connector

The connector determines how a Socket Condition relates to other Socket Conditions for a Socket Rule.

Socket Conditions with a higher order of precedence are evaluated before ones with a lower order of precedence.

The connector for the Socket Condition with the lowest sequence number is ignored.

> **EXAMPLE:**
> Given three Socket Conditions:
>
> ```
> Seq = 10 Connector = <ignored> evaluates to False
> Seq = 20 Connector = AND evaluates to True
> Seq = 30 Connector = OR evaluates to True
> ```
>
> This will return True as it is equivalent to:
> (False AND True) OR True
> If the OR were evaluated first then it would return False as it would be equivalent to:
> False AND (True OR True)

The valid values are:

OR This Socket Condition is OR'ed with others. An OR has the lowest order of precedence (evaluated last).

AND This Socket Condition is AND'ed with others. An AND has a higher order of precedence than an OR, but lower than an ORAND.

ORAND This Socket Condition is OR'ed with others. An ORAND has the highest order of precedence (evaluated first).

Field

This is the name of the field to be evaluated at run time.

The valid values are dependent on the Socket Rule.

Valid values for the QSOLISTEN server are:

LCL_PORT The local port number; an integer between 1 and 65535.
LCL_USR The user profile associated with the job issuing the listen.
LCL_USR_GRP A User Group containing the user profile associated with the job issuing the listen.

Valid values for the QSOCONNECT server are:

LCL_PORT The local port number; an integer between 1 and 65535.
RMT_PORT The remote port number; an integer between 1 and 65535.
RMT_ADDR The remote address. Valid formats are IPv4, IPv6, and Powertech Exit Point Manager ip address groups.
LCL_USR The user profile associated with the job issuing the connect.
LCL_USR_GRP A User Group containing the user profile associated with the job issuing the connect.

Valid values for the QSOACCEPT server are:

LCL_IN_PORT The local incoming port number; an integer between 1 and 65535.
LCL_BND_PORT The local bound port number; an integer between 1 and 65535.
RMT_PORT The remote port number; an integer between 1 and 65535.
RMT_ADDR The remote address. Valid formats are IPv4, IPv6, and Powertech Exit Point Manager ip address groups.
LCL_USR The user profile associated with the job issuing the accept.
LCL_USR_GRP A User Group containing the user profile associated with the job issuing the accept.

Operator

The test used for the value of the field and the criteria to evaluate this Socket Condition.

= The value of the field is equal to the criteria, or, if the criteria can be a list, the value of the field is found in that list.
<> The value of the field is not equal to the criteria, or, if the criteria can be a list, the value of the field is not found in that list.
> The value of the field is greater than the criteria.
< The value of the field is less than the criteria.
>= The value of the field is greater than or equal to the criteria.
<= The value of the field is less than or equal to the criteria.

ALWAYS

This will cause the condition to always match. It is used on the Socket Condition of the default Socket Rule, and may be used on non-default Socket Rules.

If present, it must be the only Socket Condition for a Socket Rule.

Criteria

This is the value against which the value of the selected field will be compared at run time.

The valid values are dependent on the selected Field.

Opt

Enter a valid option from the list of options provided on the list panel.

2=Change

Choose 2 to open the Change Socket Rule Condition panel, where you can change a socket rule condition.

3=Copy

Choose 3 to open the Copy Socket Rule Condition panel, where you can change a socket rule condition.

4=Delete

Choose 4 to delete the Socket Rule Condition.

5=Display

Choose 5 to display the Socket Rule Condition.

Command Keys

F3 (Exit): Exit the panel without processing any pending changes.

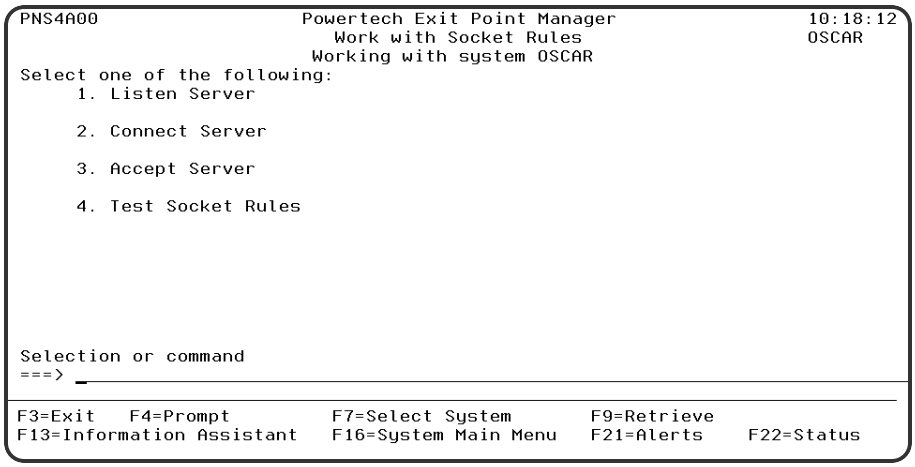
F5 (Refresh): Refreshes the panel with the most current data.

F6 (Create condition): Creates a new item. See

F12 (Cancel): Discards changes and returns to the prior panel.

Work with Socket Rules

WARNING: Misuse of Socket Rules can render your system unreachable via TCP. Exercise extreme caution when using this feature. Consider adding Socket Rules as not active and testing them using the Socket Rule test feature, and setting them to be not used by that feature and testing the rule set before removing them. If you render your system unreachable via TCP, you will need to access the system via the console in order to fix the rules (or to deactivate the Socket Rule servers).



How to Get There

On the Exit Point Manager Main Menu, choose option **20**.

What it Does

The Work with Socket Rules panel allows you to view or change Socket Rules. Socket Rules are examined by Powertech Exit Point Manager exit programs until a match is found (based on a Socket Rule's Socket Conditions).

Options

1. Listen Server

This option allows you to work with Socket Rules for the Listen Server. See Work with Socket Rules panel - Listen.

2. Connect Server

This option allows you to work with Socket Rules for the Connect Server. See Work with Socket Rules panel - Connect.

3. Accept Server

This option allows you to work with Socket Rules for the Accept Server. See Work with Socket Rules panel - Accept.

4. Test Socket Rules

This option allows you to test Socket Rules. See Test Socket Rules panel.

Command Line

To run a command, type the command and press Enter. For assistance in selecting a command, press F4 (Prompt) without typing anything. For assistance in entering a command, type the command and press F4 (Prompt). To see a previous command you entered, press F9 (Retrieve).

Command Keys

F3 (Exit): Exit the current panel without processing any pending changes.

F4 (Prompt): Provides assistance in entering or selecting a command.

F7 (Select System): Use this command key to work with data from a different System.

F9 (Retrieve): Displays the last command you entered on the command line and any parameters you included. Pressing this key once shows the last command you ran. Pressing this key twice shows the command you ran before that, and so on.

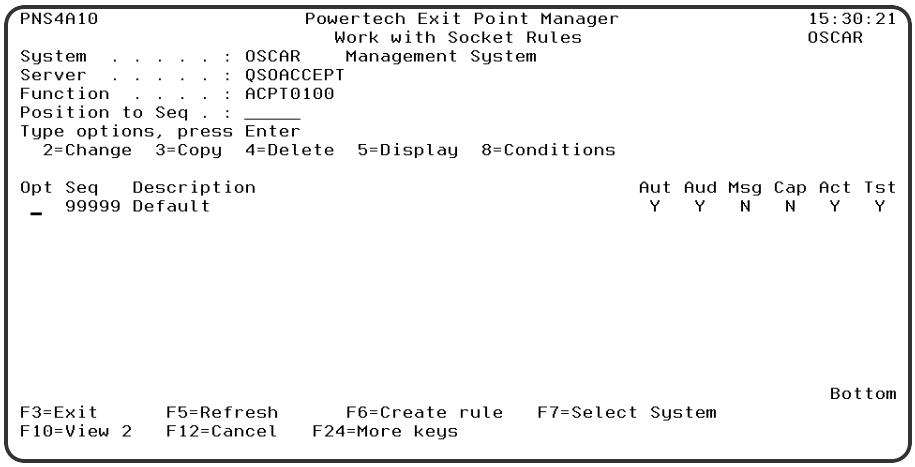
F13 (Information Assistant): Displays the Information Assistant menu with several types of assistance available. Press this key to access more information about the IBM i system.

F16 (System Main Menu): Displays the IBM i Main Menu (MAIN).

F22 (Status): Displays the Operational Resources pop-up window containing the status of several operation aspects of Powertech products.

Work with Socket Rules -Accept Server

WARNING: Misuse of Socket Rules can render your system unreachable via TCP. Exercise extreme caution when using this feature. Consider adding Socket Rules as not active and testing them using the Socket Rule test feature, and setting them to be not used by that feature and testing the rule set before removing them. If you render your system unreachable via TCP, you will need to access the system via the console in order to fix the rules (or to deactivate the Socket Rule servers).



How to Get There

On the Exit Point Manager Main Menu, choose option **20**, then choose option **3**.

What it Does

The Work with Socket Rules panel allows you to view or change Socket Rules.

Socket Rules are examined by Powertech Exit Point Manager exit programs until a match is found (based on a Socket Rule's Socket Conditions).

Field Descriptions

System

System indicates the target of any operations you perform. When you add rules, for example, those rules will be sent to, and will affect processing on, the System named.

Server

A Server in Exit Point Manager is a controlled entry point into your system. These entry points are determined and defined by IBM. Exit Point Manager has assigned easy-to-remember names to these controlled entry points.

Function

A Function, or Server Function, in Exit Point Manager represents a class of operations that a given Server may perform. For example, the *SIGNON Server classifies its operations as those pertaining to changing passwords, generating authentication tokens, and retrieving signon information. Exit Point Manager has assigned easy-to-remember names to these Functions, such as CHGPWD, GENAUTTKN and RETRIEVE.

Position to seq

Used to position the list.

Seq

The sequence number of a Socket Rule determines the order in which it will be evaluated by the exit program, with the lowest sequence number being evaluated first. Socket Rules are evaluated until a match is found.

Description

The Socket Rule description is a short textual description of the Socket Rule. It is typically used to indicate the purpose of the Socket Rule.

Aut

Authority represents the action to be taken when a rule is found that matches the data present on a transaction.

The valid values are:

Y Exit Point Manager will allow requests when this rule is enforced.
N Exit Point Manager will reject requests when this rule is enforced.
* Uses the value found in the rule above this one in the rule hierarchy when this rule is enforced.

The value * will cause the rule to inherit the value from the default Socket Rule (sequence number 99999). This default rule may not be set to the value *.

Aud

The Audit transactions flag controls the logging of transactions to the Log Journal set up on the Work with Exit Point Manager System Values panel.

The valid values are:

* Uses the value found in the rule above this one in the rule hierarchy.
Y Logs all requests when this rule is enforced.
N Logs only access failures (rejects) for this rule.

The value * will cause the rule to inherit the value from the default Socket Rule (sequence number 99999). This default rule may not be set to the value *.

Msg

The Send messages flag controls the sending of messages to the Log Message Queue set up on the Work with Exit Point Manager System Values panel.

* Uses the value found in the rule above this one in the rule hierarchy.
Y Sends a message when this rule is enforced.
N Does not send a message when this rule is enforced.

The value * will cause the rule to inherit the value from the default Socket Rule (sequence number 99999). This default rule may not be set to the value *.

Cap

The Capture transactions flag controls whether transactions are remembered in Exit Point Manager. Unlike some other rule types, a captured Socket Rule cannot be memorized.

The valid values are:

* Uses the value found in the rule above this one in the rule hierarchy.
Y Captures the transaction when this rule is enforced.
N Does not capture the transaction when this rule is enforced.

The value * will cause the rule to inherit the value from the default Socket Rule (sequence number 99999). This default rule may not be set to the value *.

Act
The Socket Rule Active flag determines whether the rule will be evaluated by the exit point program.

It can be useful to initially set a Socket Rule as not active in order to test it without enforcing it.

The valid values are:

Y Exit Point Manager will evaluate the rule.
N Exit Point Manager will not evaluate the rule.

The value N is not allowed for the default Socket Rule (sequence number 99999).

Tst
The Socket Rule Test flag determines whether the rule will be evaluated by the Socket Rule test facility.

It can be useful to flag a rule to not be tested in order to verify the effects of removing that rule.

The valid values are:

Y The Socket Rule test facility will evaluate the rule.
N The Socket Rule test facility will not evaluate the rule.

The value N is not allowed for the default Socket Rule (sequence number 99999).

Opt
Enter a valid option from the list of options provided on the list panel.

Options

2=Change
Choose this option to open the Change Socket Rule panel, where you can modify a Socket Rule's attributes.

3=Copy
Choose this option to open the Copy Socket Rule panel, where you can copy a Socket Rule.

4=Delete
Choose this option to delete the Socket Rule.

5=Display
Choose this option to display the Socket Rule.

8=Conditions
Choose this option to open the Work with Socket Conditions panel, where you can view or change Socket Conditions.

Command Keys
F3 (Exit): Exit the current screen without processing any pending changes.

F5 (Refresh): Refreshes the panel with the most current data.

F6 (Create): Creates a new item.

F7 (Select System): Use this command key to work with data from a different System.

F12 (Cancel): Discards changes and returns to the prior panel.

F13 (Display msgs): Displays messages for the current user.

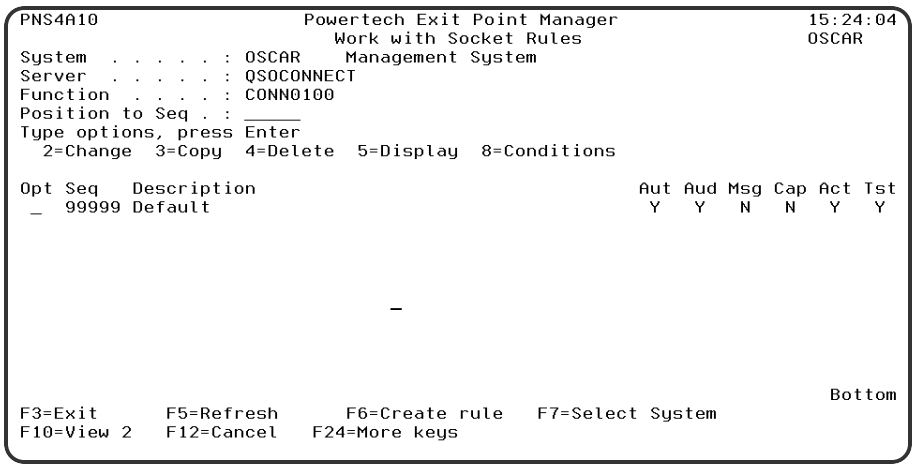
F14 (Work sbm job): Displays jobs submitted from the current user.

F15 (Work w/spooled files): Works with spooled files for the current user.

F24 (More keys): This shows additional function keys that can be used for this display.

Work with Socket Rules - Connect Server

WARNING: Misuse of Socket Rules can render your system unreachable via TCP. Exercise extreme caution when using this feature. Consider adding Socket Rules as not active and testing them using the Socket Rule test feature, and setting them to be not used by that feature and testing the rule set before removing them. If you render your system unreachable via TCP, you will need to access the system via the console in order to fix the rules (or to deactivate the Socket Rule servers).



How to Get There

On the Exit Point Manager Main Menu, choose option **20**, then choose option **2**.

What it Does

The Work with Socket Rules panel allows you to view or change Socket Rules.

Socket Rules are examined by Powertech Exit Point Manager exit programs until a match is found (based on a Socket Rule's Socket Conditions).

Field Descriptions

System

System indicates the target of any operations you perform. When you add rules, for example, those rules will be sent to, and will affect processing on, the System named.

Server

A Server in Exit Point Manager is a controlled entry point into your system. These entry points are determined and defined by IBM. Exit Point Manager has assigned easy-to-remember names to these controlled entry points.

Function

A Function, or Server Function, in Exit Point Manager represents a class of operations that a given Server may perform. For example, the *SIGNON Server classifies its operations as those pertaining to changing passwords, generating authentication tokens, and retrieving signon information. Exit Point Manager has assigned easy-to-remember names to these Functions, such as CHGPWD, GENAUTTKN and RETRIEVE.

Position to seq

Used to position the list.

Seq

The sequence number of a Socket Rule determines the order in which it will be evaluated by the exit program, with the lowest sequence number being evaluated first. Socket Rules are evaluated until a match is found.

Description

The Socket Rule description is a short textual description of the Socket Rule. It is typically used to indicate the purpose of the Socket Rule.

Aut

Authority represents the action to be taken when a rule is found that matches the data present on a transaction.

The valid values are:

Y Exit Point Manager will allow requests when this rule is enforced.
N Exit Point Manager will reject requests when this rule is enforced.
* Uses the value found in the rule above this one in the rule hierarchy when this rule is enforced.

The value * will cause the rule to inherit the value from the default Socket Rule (sequence number 99999). This default rule may not be set to the value *.

Aud

The Audit transactions flag controls the logging of transactions to the Log Journal set up on the Work with Exit Point Manager System Values panel.

The valid values are:

* Uses the value found in the rule above this one in the rule hierarchy.
Y Logs all requests when this rule is enforced.
N Logs only access failures (rejects) for this rule.

The value * will cause the rule to inherit the value from the default Socket Rule (sequence number 99999). This default rule may not be set to the value *.

Msg

The Send messages flag controls the sending of messages to the Log Message Queue set up on the Work with Exit Point Manager System Values panel.

* Uses the value found in the rule above this one in the rule hierarchy.
Y Sends a message when this rule is enforced.
N Does not send a message when this rule is enforced.

The value * will cause the rule to inherit the value from the default Socket Rule (sequence number 99999). This default rule may not be set to the value *.

Cap

The Capture transactions flag controls whether transactions are remembered in Exit Point Manager. Unlike some other rule types, a captured Socket Rule cannot be memorized.

The valid values are:

* Uses the value found in the rule above this one in the rule hierarchy.
Y Captures the transaction when this rule is enforced.
N Does not capture the transaction when this rule is enforced.

The value * will cause the rule to inherit the value from the default Socket Rule (sequence number 99999). This default rule may not be set to the value *.

Act

The Socket Rule Active flag determines whether the rule will be evaluated by the exit point program.

It can be useful to initially set a Socket Rule as not active in order to test it without enforcing it.

The valid values are:

Y Exit Point Manager will evaluate the rule.
N Exit Point Manager will not evaluate the rule.

The value N is not allowed for the default Socket Rule (sequence number 99999).

Tst

The Socket Rule Test flag determines whether the rule will be evaluated by the Socket Rule test facility.

It can be useful to flag a rule to not be tested in order to verify the effects of removing that rule.

The valid values are:

Y The Socket Rule test facility will evaluate the rule.
N The Socket Rule test facility will not evaluate the rule.

The value N is not allowed for the default Socket Rule (sequence number 99999).

Opt

Enter a valid option from the list of options provided on the list panel.

Options

2=Change
Choose this option to open the Change Socket Rule panel, where you can modify a Socket Rule's attributes.

3=Copy
Choose this option to open the Copy Socket Rule panel, where you can copy a Socket Rule.

4=Delete
Choose this option to delete the Socket Rule.

5=Display
Choose this option to display the Socket Rule.

8=Conditions
Choose this option to open the Work with Socket Conditions panel, where you can view or change Socket Conditions.

Command Keys
F3 (Exit): Exit the current panel without processing any pending changes.

F5 (Refresh): Refreshes the panel with the most current data.

F6 (Create): Creates a new item.

F7 (Select System): Use this command key to work with data from a different System.

F12 (Cancel): Discards changes and returns to the prior panel.

F13 (Display msgs): Displays messages for the current user.

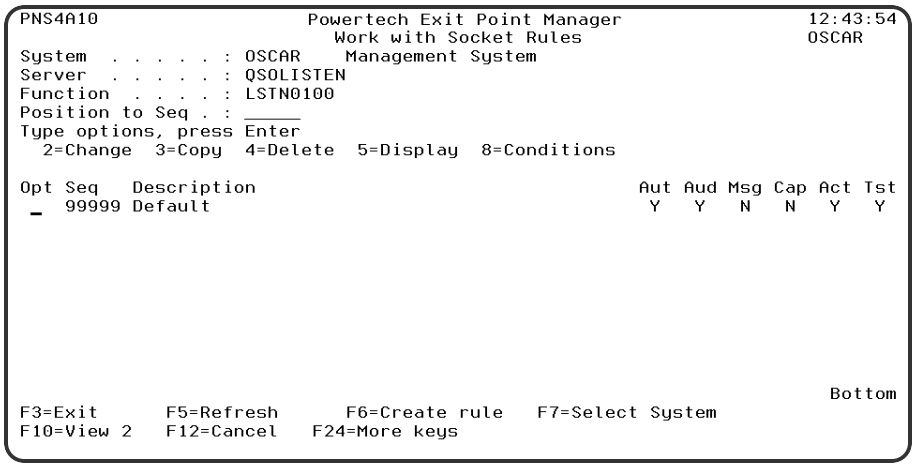
F14 (Work sbm job): Displays jobs submitted from the current user.

F15 (Work w/spooled files): Works with spooled files for the current user.

F24 (More keys): This shows additional function keys that can be used for this display.

Work with Socket Rules - Listen Server

WARNING: Misuse of Socket Rules can render your system unreachable via TCP. Exercise extreme caution when using this feature. Consider adding Socket Rules as not active and testing them using the Socket Rule test feature, and setting them to be not used by that feature and testing the rule set before removing them. If you render your system unreachable via TCP, you will need to access the system via the console in order to fix the rules (or to deactivate the Socket Rule servers).



How to Get There

On the Exit Point Manager Main Menu, choose option **20**, then choose option **1**.

What it Does

This panel allows you to work with Socket Rules for the Listen Server.

Field Descriptions

System

System indicates the target of any operations you perform. When you add rules, for example, those rules will be sent to, and will affect processing on, the System named.

Server

A Server in Exit Point Manager is a controlled entry point into your system. These entry points are determined and defined by IBM. Exit Point Manager has assigned easy-to-remember names to these controlled entry points.

Function

A Function, or Server Function, in Exit Point Manager represents a class of operations that a given Server may perform. For example, the *SIGNON Server classifies its operations as those pertaining to changing passwords, generating authentication tokens, and retrieving signon information. Exit Point Manager has assigned easy-to-remember names to these Functions, such as CHGPWD, GENAUTTKN and RETRIEVE.

Position to seq

Used to position the list.

Description

The Socket Rule description is a short textual description of the Socket Rule. It is typically used to indicate the purpose of the Socket Rule.

Aut

Authority represents the action to be taken when a rule is found that matches the data present on a transaction.

The valid values are:

Y Exit Point Manager will allow requests when this rule is enforced.
N Exit Point Manager will reject requests when this rule is enforced.
* Uses the value found in the rule above this one in the rule hierarchy when this rule is enforced.

The value * will cause the rule to inherit the value from the default Socket Rule (sequence number 99999). This default rule may not be set to the value *.

Aud

The Audit transactions flag controls the logging of transactions to the Log Journal set up on the Work with Exit Point Manager System Values panel.

The valid values are:

* Uses the value found in the rule above this one in the rule hierarchy.
Y Logs all requests when this rule is enforced.
N Logs only access failures (rejects) for this rule.

The value * will cause the rule to inherit the value from the default Socket Rule (sequence number 99999). This default rule may not be set to the value *.

Msg

The Send messages flag controls the sending of messages to the Log Message Queue set up on the Work with Exit Point Manager System Values panel.

* Uses the value found in the rule above this one in the rule hierarchy.
Y Sends a message when this rule is enforced.
N Does not send a message when this rule is enforced.

The value * will cause the rule to inherit the value from the default Socket Rule (sequence number 99999). This default rule may not be set to the value *.

Cap

The Capture transactions flag controls whether transactions are remembered in Exit Point Manager. Unlike some other rule types, a captured Socket Rule cannot be memorized.

The valid values are:

* Uses the value found in the rule above this one in the rule hierarchy.
Y Captures the transaction when this rule is enforced.
N Does not capture the transaction when this rule is enforced.

The value * will cause the rule to inherit the value from the default Socket Rule (sequence number 99999). This default rule may not be set to the value *.

Act

The Socket Rule Active flag determines whether the rule will be evaluated by the exit point program.

It can be useful to initially set a Socket Rule as not active in order to test it without enforcing it.

The valid values are:

Y Exit Point Manager will evaluate the rule.
N Exit Point Manager will not evaluate the rule.

The value N is not allowed for the default Socket Rule (sequence number 99999).

Tst
The Socket Rule Test flag determines whether the rule will be evaluated by the Socket Rule test facility.

It can be useful to flag a rule to not be tested in order to verify the effects of removing that rule.

The valid values are:

Y The Socket Rule test facility will evaluate the rule.
N The Socket Rule test facility will not evaluate the rule.

The value N is not allowed for the default Socket Rule (sequence number 99999).

Opt
Enter a valid option from the list of options provided on the list panel.

Options

2=Change
Choose this option to open the Change Socket Rule panel, where you can modify a Socket Rule's attributes.

3=Copy
Choose this option to open the Copy Socket Rule panel, where you can copy a Socket Rule.

4=Delete
Choose this option to delete the Socket Rule.

5=Display
Choose this option to display the Socket Rule.

8=Conditions
Choose this option to open the Work with Socket Conditions panel, where you can view or change Socket Conditions.

Command Keys
F3 (Exit): Exit the current panel without processing any pending changes.

F5 (Refresh): Refreshes the panel with the most current data.

F6 (Create): Creates a new item.

F7 (Select System): Use this command key to work with data from a different System.

F12 (Cancel): Discards changes and returns to the prior panel.

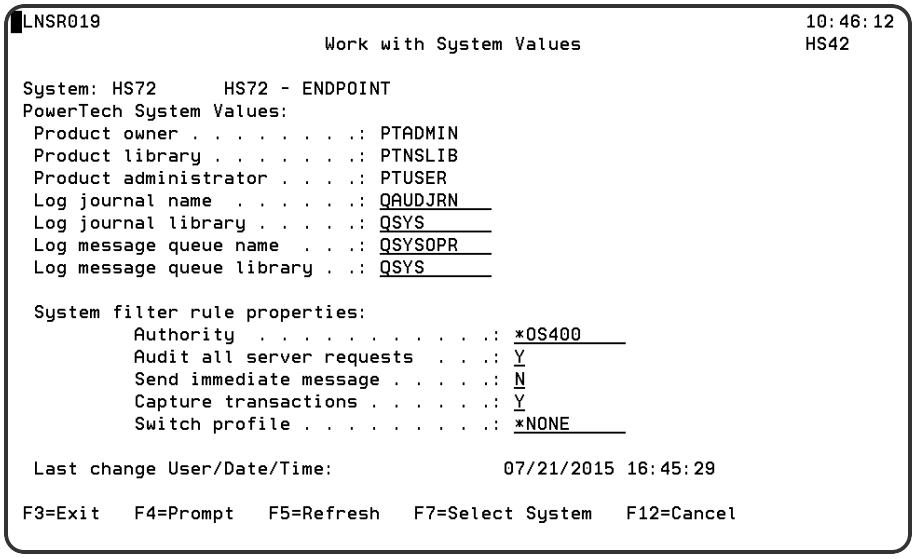
F13 (Display msgs): Displays messages for the current user.

F14 (Work sbm job): Displays jobs submitted from the current user.

F15 (Work w/spooled files): Works with spooled files for the current user.

F24 (More keys): This shows additional function keys that can be used for this display.

Work with System Values



How to Get There

To display these options, from the Exit Point Manager Main Menu, select option **81**, Configuration Menu, then option **1**, Work with System Values.

What it Does

Work with System Values allows you to maintain system values for Powertech Exit Point Manager. The system values for Log Journal Name, Log Journal Library, Log Message Queue Name, and Log Message Queue Library can be maintained anytime. Values for Product Owner, Product Library, and Product Administrator can only be maintained during installation or upgrade.

On the browser interface, these values can be found at Edit System Defaults.

Field Descriptions

The following describes the parameters and allowable values for each field on the Work with System Values panel.

Product Owner

The product owner is the name of the user profile that owns all data objects and exit programs in the Powertech Exit Point Manager product.

Product Library

The product library is the library that contains all of the Powertech Exit Point Manager objects.

Product Administrator

The product administrator is the name of the user profile that owns administrative program objects in the Powertech Exit Point Manager product. We recommend granting administrators *USE authority to the PTADMIN authorization list using the following command, where myuser is the administrator profile to add.

ADDAUTLE AUTL(PTADMIN) USER(myuser) AUT(*USE)

NOTE: To access reporting functions, administrators must be authorized to the PTNSRPT authorization list.

For more information, see Granting Reporting Authority, later in this User Guide.

Once authorized to the PTADMIN and PTNSRPT authorization lists, the administrator has all the authorities needed to administer Powertech Exit Point Manager. Product administrators have *CHANGE authority to Exit Point Manager data and *USE authority to Exit Point Manager programs.

NOTE: Users set to the *SECOFR User Class do not need to be members of the PTADMIN or PTNSRPT authorizations lists to use Exit Point Manager or Exit Point Manager Reports.

Log Journal Name and Log Journal LibraryExit Point Manager

The log journal name is the name of the journal that Powertech Exit Point Manager will log information. You can control the level of detail with the audit flag when you specify location and user authorities. Most installations will specify QUADJRN. The log journal library specifies the library where the log journal is located.

The Log Journal Library specifies the library where the log journal is located.

NOTE:

1. You also can specify *NONE in the Log Journal Name field. However, if a journal name of *NONE is found in the Exit Point Manager system values, network transactions are not journaled.
2. Some versions of Powertech Compliance Monitor expect Exit Point Manager audit entries to be written to QSYS/QAUDJRN. Contact Powertech technical support if you need further information concerning log journal entries.

Log Message Queue Name and Log Message Queue Library

The log message queue name is the name of the message queue where Powertech Exit Point Manager sends messages. Messages are sent to this queue when specified on location and user authority records. Most installations specify QSYSOPR.

The log message queue library is the library where the log message queue is located.

System Filter Rule Properties

The Work with System Values panel also allows you to specify system filter rule properties.

Authority

The authority assigned if no other authority is found for a server or function. Possible values are:

***OS400** Exit Point Manager allows the transaction without taking any action
***REJECT** Exit Point Manager rejects requests for the transaction
***SWITCH** Exit Point Manager switches the job to run as the user profile specified in the Switch Profile field.

Audit All Server Requests

Controls the type of requests Exit Point Manager will log. Exit Point Manager uses this value if no other value is entered for a server or function. Possible values are:

Y Log All requests

N Only log authority failures

Send Immediate Message

Determines if Exit Point Manager sends a message to the log message queue. Exit Point Manager uses this value if no other value is entered for a server or function. Possible values are:

Y A message is sent to the specified queue
N No message is sent

Capture Transactions

Capture transactions for Memorized Transaction Request (MTR). Exit Point Manager uses this value if no other value is entered for a server or function. Possible values are:

Y Capture transactions
N Do not capture transactions

Switch Profile

The name of a Switch Profile. If you enter a profile name, processing is switched to run as the specified profile and under this profile's authority. Exit Point Manager uses this value if no other value is entered for a server or function. Possible values are:

***NONE** No switch profile is used.
switch-profile The switch profile to process under. The profile you specify must be an active profile on IBM i.

Last Change User/Date/Time

The user profile that changed the Exit Point Manager system values and the date and time the changes were made.

Command Keys

F3 (Exit): Exit the current panel without processing any pending changes.

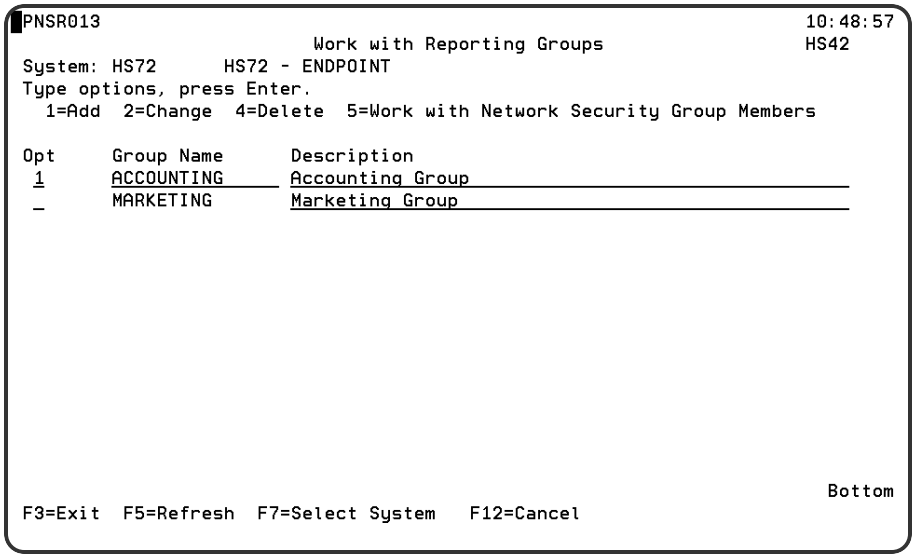
F4 (Prompt): Displays a list of possible values from which you may select one.

F5 (Refresh): Refreshes the panel and resets all available text fields.

F7 (Select system): Use this command to work with data from a different System.

F12 (Cancel): Exit the current panel without processing any pending changes.

Work with Reporting Groups



What it Does

Exit Point Manager's Work with Reporting Groups is used when a number of Profiles are required to be reported on together. To add a new Network Reporting Group, enter the information on the blank line below the column headings. Once a Network Reporting Group is created a list of Profiles may be associated to it. Option **5** displays a list of profiles associated to the group. Type an option next to a specific group and press `Enter`. You can type option numbers next to more than one group at a time. This allows you to run more than one task at a time. If you see 'More...' in the lower right corner of your display, there is more information to be listed. Press the Page Down (Roll Up) key to move toward the end of the Network Reporting Groups. Press the Page Up (Roll Down) key to move toward the beginning of the Network Reporting Groups.

Options

Type the option number you want and press `Enter`.

1=Add

Add a Exit Point Manager Group. Valid for line 1 only.

2=Change

Change a Exit Point Manager Group.

> **NOTE:** You cannot use option **2** to change the reporting group name.

4=Delete

Use option 4 to delete a reporting group.

> **NOTE:** If the reporting group has user profiles assigned to it, you must remove the user profiles before you can delete the group.

5=Work with Exit Point Manager Group Members
Work with the Profiles associated with the group.

Field Descriptions

Group Name
The name of a group of Profiles.

Group Description
The description of a Reporting Group. It is a required entry.

Command Keys
F3 (Exit): Exit the current panel without processing any pending changes.

F5 (Refresh): Refreshes the panel and resets all available text fields.

F7 (Select system): Use this command to work with data from a different System.

F12 (Cancel): Exit the current panel without processing any pending changes.

Central Administration panels

The topics in this section include descriptions for Powertech Central Administration panels used to manage Endpoints on your network with Exit Point Manager. For a complete explanation of all of Central Administration's tools and function, see the Central Administration Administrator's Guide.

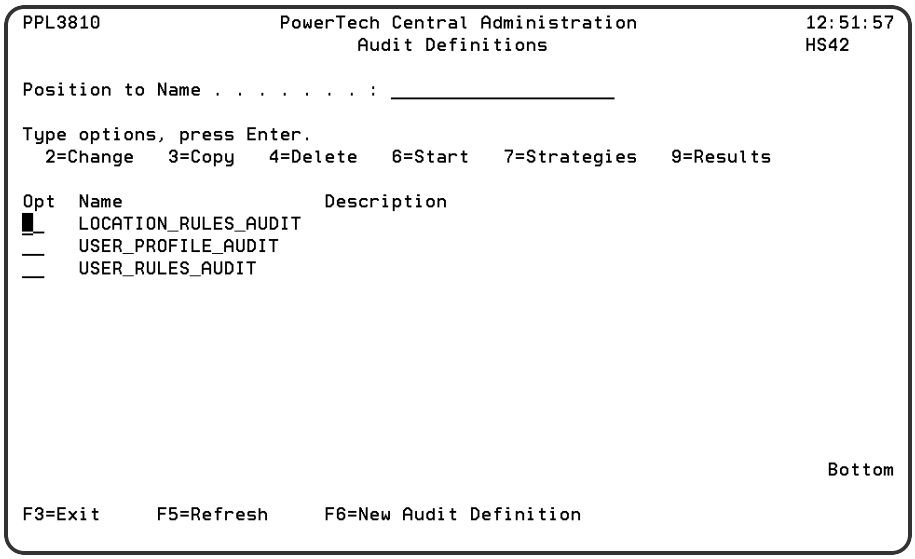
Audit Definitions Panel

Audit Results Panel

Automatic Remedies Panel

Audit Strategies Panel

Audit Definitions panel



How to Get There

From the Powertech Main Menu, choose option **80**, Central Administration, then choose option **5**, Auditing Menu. Choose option **1**, Audit Definitions.

What it Does

The Audit Definitions panel lists all the audits that have been defined in Central Administration.

Options

2=Change: Displays the Change Audit Definition panel, where you can change the name or description of an existing audit.

3=Copy: Displays the Copy Audit Definition panel, which copies an existing audit. Enter a description and name for the new audit.

4=Delete: Allows you to delete the selected audit. A confirmation panel displays asking you to confirm the deletion.

> **NOTE:** You also can schedule an audit in a job scheduling program (such as Robot SCHEDULE from HelpSystems) using the Start Audit (PPLSTRAUD) command. Specify the audit description and system on which the audit should run when scheduling the command.

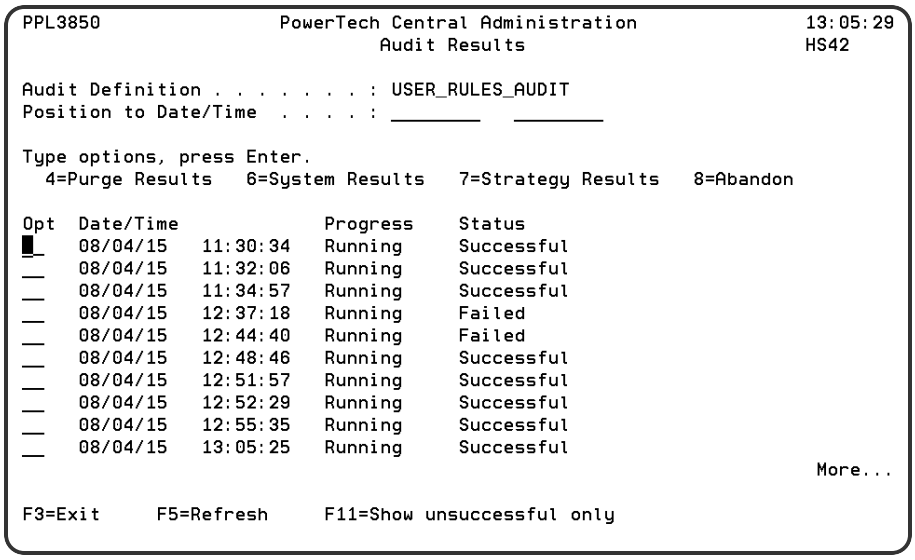
6=Start: Starts an audit. You're asked to select a system group for the audit; Central Administration then runs the audit against the systems in the group.

7=Strategies: Allows you to select an audit strategy. You must select an audit strategy before you can run an audit.

9=Results: Displays the Audit Results panel, which shows all instances of the selected audit. To position the Audit Results display to a specific date and time, enter the date and time you want to see at the top of the panel.

To define a new audit, press `F6`, New Audit Definition, and enter a name and brief description for the audit on the Create Audit Definition panel.

Audit Results panel



How to Get There

In the Audit Definitions panel, enter **9** for an Audit Definition that has been run.

What it Does

The Audit Results panel shows all instances of the selected audit that have been run and the status of each audit. To position the Audit Results display to a specific date and time, enter the date and time you want to see at the top of the panel.

Options

4=Purge: Purges all Audit Item Results for the selected execution of the Audit.

6=System Results: Displays the Audit System Results panel, which shows the status of the audit for the system on which it was run.

7=Strategy Results: Displays the Audit Strategy Results panel, which shows the status of the audit for the selected audit strategy (currently User Rules Settings).

From each System Results panel (displayed by entering option **6** next to each audit strategy), you can display the other type of audit results. Then, you can select option **5**, Item Results, to see each item that was checked during the audit and the results for each.

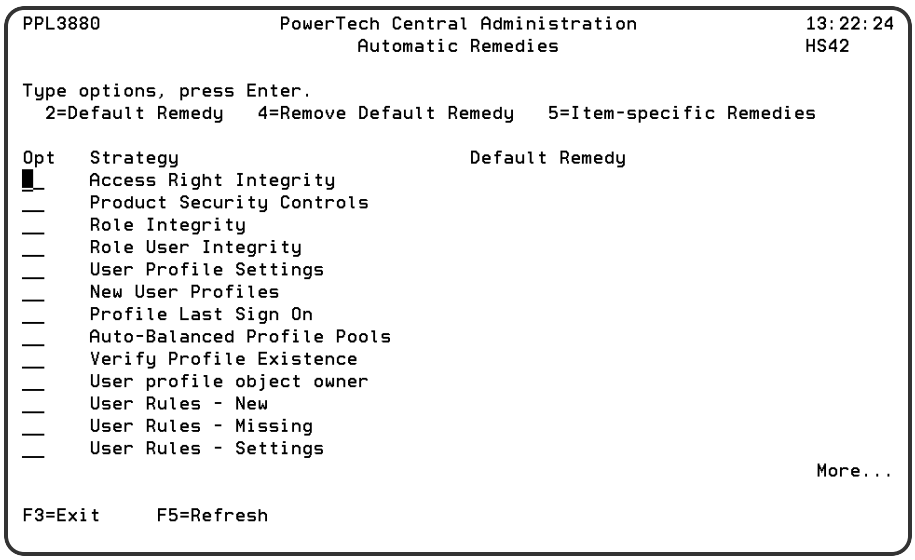
> **NOTE:** If you select option **5** (Item Results) while an audit is running, you can see the results in real time as each item is checked.

To see detailed information about an audited user rule, enter a **5** next to the Item Name to display a more complete description of why the audited item passed or failed the audit, allowing you to make adjustments, as needed. If the text of the Message is too long, press `F10` to display the complete message. Press `F20` to display further details on the audited item, including a side-by-side comparison of the Management System's values and the Endpoint's values.

The `F11` key acts as a toggle to display all audits or only those that were not successful, making it easier to identify the items you need to review.

Automatic Remedies panel

The Automatic Remedies panel lists all the Strategies and corresponding remedies, if applied. You can modify or delete Automatic Remedies.



A Strategy can have a default Automatic Remedy that will be used for any Item Result without a more specific Automatic Remedy. A greater-than symbol (">") appears to the left of the Strategy column when Item Result-specific Automatic Remedies exist for that Strategy.

How to Get There

From the Powertech Main Menu, choose option **80** (Central Administration), then press **5** (Auditing Menu), then **4** (Automatic Remedies).

Options

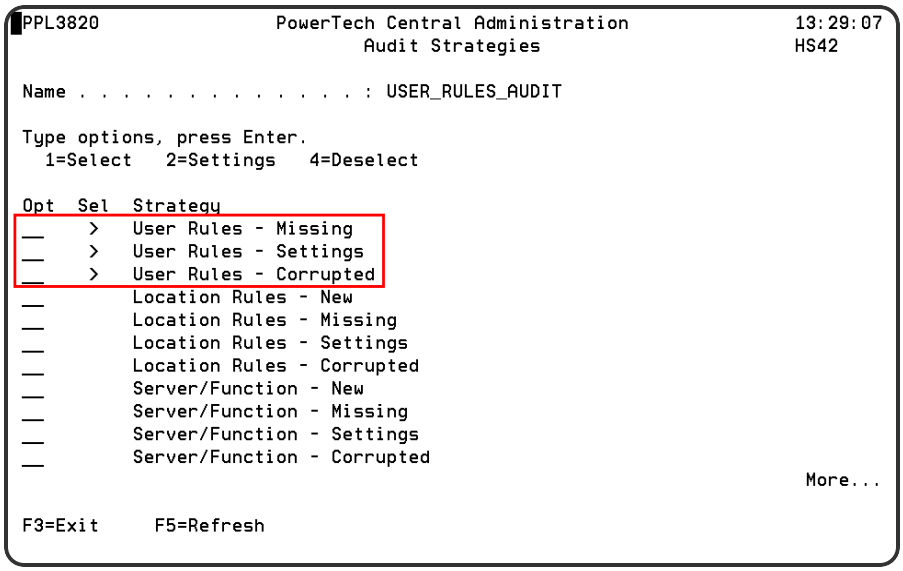
2=Default Remedy: Select option **2** in the Opt column to select a default remedy for the selected strategy.

The Select Remedy panel allows you to select a Remedy. The Remedies displayed are all valid for the Strategy named at the top of the screen; however, some Remedies may not be applicable to a particular failed Audit Item Result. Should you select a Remedy that is not valid for one or more of the Audit Item Results you selected, those Audit Item Results will not be Remedied.

4=Remove Default Remedy: Enter option **4** in the Opt column to remove the default remedy for the selected strategy. A confirmation screen displays. Press `Enter` to confirm the removal or `F12` to cancel.

5=Item-specific Remedies: Enter option **5** in the Opt column to manage the Automatic Remedies for the Strategy.

Exit Point Manager Audit Strategies panel



These are just three of several Exit Point Manager Strategies available in the Central Administration Audit Strategies panel.

How to Get There

From the Powertech Main Menu, choose option **80** (Central Administration), then **5** (Auditing Menu), **1** (Audit Definitions), then enter **7** for an Audit Definition.

> **NOTE:** If none are there, you will need to press **F6** to create a new one, then select option **7**.

What it Does

The Audit Strategies panels allow you to create, modify, delete, and perform other operations upon Audit Strategies. Audit Strategy determines how a set of items will be audited, and against what criteria they will be audited. An Audit Definition may contain more than one Audit Strategy. Each Audit Strategy may or may not have settings to control its operation.

Exit Point Manager Strategy Descriptions

- **User Rules - New** compares User Rules on the Management System with User Rules on Endpoints and identifies those that have been added to Endpoints.
- **User Rules - Missing** compares User Rules on the Management System with User Rules on Endpoints and identifies those that have been removed from Endpoints.
- **User Rules - Settings** compares User Rules on the Management System with User Rules on Endpoints and identifies those whose settings do not match.
- **User Rules - Corrupted** identifies User Rules that have been corrupted.
- **Location Rules - New** compares Location Rules on the Management System with Location Rules on Endpoints and identifies those that have been added to Endpoints.
- **Location Rules - Missing** compares Location Rules on the Management System with Location Rules on Endpoints and identifies those that have been removed from Endpoints.
- **Location Rules - Settings** compares Location Rules on the Management System with Location Rules on Endpoints and identifies those whose settings do not match.

- **Location Rules - Corrupted** identifies Location Rules that have been corrupted.
- **Server/Function - New** compares Servers and Functions on the Management System with Servers and Functions on Endpoints and identifies those that have been added to Endpoints.
- **Server/Function - Missing** compares Servers and Functions on the Management System with Servers and Functions on Endpoints and identifies those that have been removed from Endpoints.
- **Server/Function - Settings** compares the active Servers and Functions on the Management System with active Servers and Functions on Endpoints and identifies any discrepancy.
- **Server/Function - Corrupted** identifies Servers and Functions that have been corrupted.
- **Memorized Trans - New** compares Memorized Transactions on the Management System with Memorized Transactions on Endpoints and identifies those that have been added to Endpoints.
- **Memorized Trans - Missing** compares Memorized Transactions on the Management System with Memorized Transactions on Endpoints and identifies those that have been removed from Endpoints.
- **Memorized Trans - Settings** compares Memorized Transactions on the Management System with Memorized Transactions on Endpoints and identifies those that have been removed from Endpoints.
- **Memorized Trans - Corrupted** identifies Memorized Transactions that have been corrupted.
- **Pre-filters - New** compares Pre-filters on the Management System with Location+User Pre-filters on Endpoints and identifies those that have been added to Endpoints.
- **Pre-filters - Missing** compares Pre-filters on the Management System with Location+User Pre-filters on Endpoints and identifies those that have been removed from Endpoints.
- **Pre-filters - Settings** compares Pre-filters on the Management System with Location+User Pre-filters on Endpoints and identifies those whose settings do not match.
- **Pre-filters - Corrupted** identifies Pre-filters that have been corrupted.
- **SecureScreen Filters- New** compares SecureScreen Filters on the Management System with SOMETHING on Endpoints and identifies those that have been added to Endpoints.
- **SecureScreen Filters - Missing** compares SecureScreen Filters on the Management System with SOMETHING on Endpoints and identifies those that have been removed from Endpoints.
- **SecureScreen Filters - Settings** compares SecureScreen Filters on the Management System with SOMETHING on Endpoints and identifies those whose settings do not match.
- **SecureScreen Filters - Corrupted** identifies SecureScreen Filters that have been corrupted.
- **Report Groups - New** compares Report Groups on the Management System with User Groups on Endpoints and identifies those that have been added to Endpoints.
- **Report Groups - Missing** compares Report Groups on the Management System with User Groups on Endpoints and identifies those that have been removed from Endpoints.
- **Report Groups - Settings** compares Report Groups on the Management System with User Groups on Endpoints and identifies those whose settings do not match.
- **Report Groups - Corrupted** identifies Report Groups that have been corrupted.
- **Report Group Members - New** compares Report Group Members on the Management System with User Group Members on Endpoints and identifies those that have been added to Endpoints.

- **Report Group Members - Missing** compares Report Group Members on the Management System with User Group Members on Endpoints and identifies those that have been removed from Endpoints.
- **Report Group Members - Settings** compares Report Group Members on the Management System with User Group Members on Endpoints and identifies those whose settings do not match.
- **Report Group Members - Corrupted** identifies Report Group Members that have been corrupted.
- **System - New** compares System Values on the Management System with System Values on Endpoints and identifies those that have been added to Endpoints.
- **System - Missing** compares System Values on the Management System with System Values on Endpoints and identifies those that have been removed from Endpoints.
- **System - Settings** compares System Values on the Management System with System Values on Endpoints and identifies those whose settings do not match.
- **Object List - New** compares Object List on the Management System with Object Lists on Endpoints and identifies those that have been added to Endpoints.
- **Object List - Missing** compares Object Lists on the Management System with Object Lists on Endpoints and identifies those that have been removed from Endpoints.
- **Object List - Settings** compares Object Lists on the Management System with Object Lists on Endpoints and identifies those whose settings do not match.
- **Object List - Corrupted** identifies Object Lists that have been corrupted.
- **Object List Entry - New** compares Object List Entries on the Management System with Object List Entries on Endpoints and identifies those that have been added to Endpoints.
- **Object List Entry - Missing** compares Object List Entries on the Management System with Object List Entries on Endpoints and identifies those that have been removed from Endpoints.
- **Object List Entry - Settings** compares Object List Entries on the Management System with Object List Entries on Endpoints and identifies those whose settings do not match.
- **Object List Entry - Corrupted** identifies Object List Entries that have been corrupted.
- **Object Rule - New** compares Object Rules on the Management System with Object Rules on Endpoints and identifies those that have been added to Endpoints.
- **Object Rule - Missing** compares Object Rules on the Management System with Object Rules on Endpoints and identifies those that have been removed from Endpoints.
- **Object Rule - Settings** compares Object Rules on the Management System with Object Rules on Endpoints and identifies those whose settings do not match.
- **Object Rule - Corrupted** identifies Object Rules that have been corrupted.
- **Pre-filters (Server) - New** compares Server Pre-filters on the Management System with Server Pre-filters on Endpoints and identifies those that have been added to Endpoints.
- **Pre-filters (Server) - Missing** compares Server Pre-filters on the Management System with Server Pre-filters on Endpoints and identifies those that have been removed from Endpoints.
- **Pre-filters (Server) - Settings** compares Server Pre-filters on the Management System with Server Pre-filters on Endpoints and identifies those whose settings do not match.
- **User Group - New** compares User Groups on the Management System with User Groups on Endpoints and identifies those that have been added to Endpoints.

- **User Group - Missing** compares User Groups on the Management System with User Group Members on Endpoints and identifies those that have been removed from Endpoints.
- **User Group - Settings** compares User Groups on the Management System with User Group Members on Endpoints and identifies those whose settings do not match.
- **User Group - Corrupted** identifies User Groups that have been corrupted.
- **User Group Member - New** compares User Group Members on the Management System with User Group Members on Endpoints and identifies those that have been added to Endpoints.
- **User Group Member - Missing** compares User Group Members on the Management System with User Group Members on Endpoints and identifies those that have been removed from Endpoints.
- **User Group Member - Settings** compares User Group Members on the Management System with User Group Members on Endpoints and identifies those whose settings do not match.
- **User Group Member - Corrupted** identifies User Group Members that have been corrupted.
- **Socket Rule - New** compares Socket Rules on the Management System with Socket Rules on Endpoints and identifies those that have been added to Endpoints.
- **Socket Rule - Missing** compares Socket Rules on the Management System with Socket Rules on Endpoints and identifies those that have been removed from Endpoints.
- **Socket Rule - Settings** compares Socket Rules on the Management System with Socket Rules on Endpoints and identifies those whose settings do not match.
- **Socket Rule - Corrupted** identifies Socket Rules that have been corrupted.
- **Socket Condition - New** compares Socket Rule Conditions on the Management System with Socket Rules on Endpoints and identifies those that have been added to Endpoints.
- **Socket Condition - Missing** compares Socket Rule Conditions on the Management System with Socket Rules on Endpoints and identifies those that have been removed from Endpoints.
- **Socket Condition - Settings** compares Socket Rule Conditions on the Management System with Socket Rules on Endpoints and identifies those whose settings do not match.
- **Socket Condition - Corrupted** identifies Socket Rule Conditions that have been corrupted.

Options

1=Select: A selected Strategy will be processed during the next Audit run. You may select several items at once.

A greater-than symbol (>) in the Sel column indicates that the Audit Strategy is selected for use. A selected Strategy will be processed during the next Audit run.

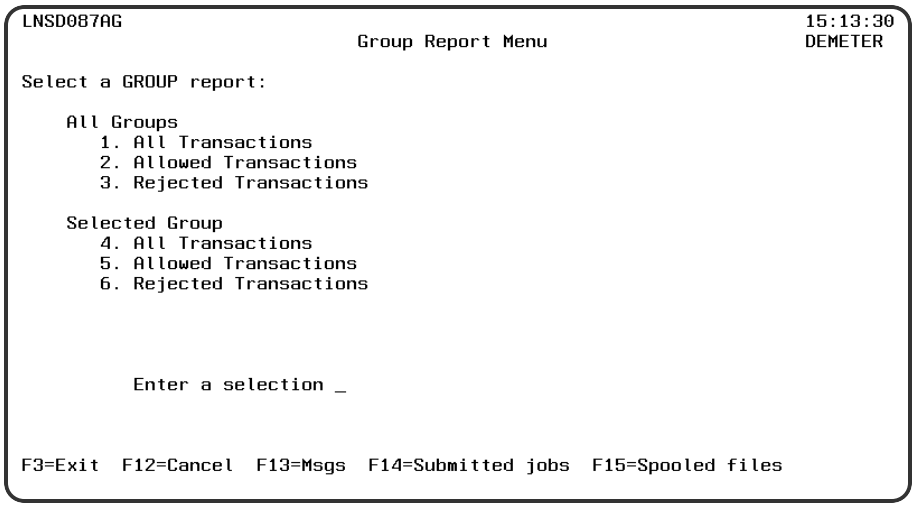
2=Settings: Allows you to maintain any settings the Strategy might support. Not every Strategy supports settings.

4=Deselect: A deselected Strategy will not be processed during the next Audit run. You may select several items at once.

Menus

The topics in this section include descriptions for Exit Point Manager's green screen menus.

Group Report Menu



How to Get There

From the Exit Point Manager Main Menu, select option **80**, Reports Menu, then option **5**.

What it Does

The Group Report Menu will sort the journal by User. You can select a group of Users by specifying a Reporting Group, accounting code or group profile name. Date range and type of transactions to be listed are also used to narrow or expand the report to your specific requirements.

User Groups are not handled on this option, only on the User Report Menu.

Options

1. All Groups All Transactions. This option produces a report of all transactions for all Users in all groups and sorts by User/Date/Time. You will be prompted for Group and Date/Time range on a later screen.

2. All Groups Allowed Transactions. This option produces a report of allowed transactions for all Users in all groups and sorts by User/Date/Time. You will be prompted for Group and Date/Time range on a later screen.

3. All Groups Rejected Transactions. This option produces a report of rejected transactions for all Users in all groups and sorts by User/Date/Time. You will be prompted for Group and Date/Time range on a later screen.

4. Selected Group All Transactions. This option produces a report of all transactions for all Users in a selected group and sorts by User/Date/Time. You will be prompted for Group and Date/Time range on a later screen.

5. Selected Group Allowed Transactions. This option produces a report of allowed transactions for all Users in a selected group and sorts by User/Date/Time. You will be prompted for Group and Date/Time range on a later screen.

6. Selected Group Rejected Transactions. This option produces a report of rejected transactions for all Users in a selected group and sorts by User/Date/Time. You will be prompted for Group and Date/Time range on a later screen.

Command Keys

F3 (Exit): Exit the screen without processing any pending changes.

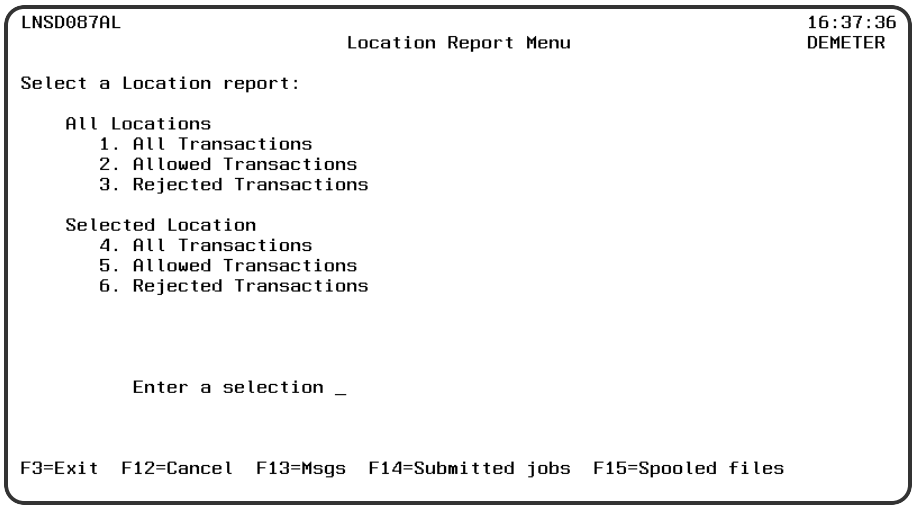
F12 (Cancel): Exit the screen without processing any pending changes.

F13 (Msgs): Displays messages for the current user.

F14 (Submitted jobs): Displays jobs submitted from the current job.

F15 (Spooled files): Displays the current user's printed output.

Location Report Menu



How to Get There

From the Exit Point Manager Main Menu, select option **80**, Reports menu, then option **2**.

What it Does

The Location Report Menu will sort the Journal by Location or allow you to select a specific Location. Date range and type of transactions to be listed are also used to narrow or expand the report to your specific requirements.

Options

1. All Locations All Transactions. This option produces a report of each Location's transactions and sorts by Location/Date/Time. You will be prompted for Date/Time range on a later screen.

2. All Locations Allowed Transactions. This option produces a report of each Location's allowed transactions and sorts by Location/Date/Time. You will be prompted for Date/Time range on a later screen.

3. All Locations Rejected Transactions. This option produces a report of each Location's rejected transactions and sorts by Location/Date/Time. You will be prompted for Date/Time range on a later screen.

4. Selected Location. All Transactions This option produces a report of a specific Location's transactions and sorts by Location/Date/Time. You will be prompted for Location and Date/Time range on a later screen.

5. Selected Location Allowed Transactions. This option produces a report of a specific Location's allowed transactions and sorts by Location/Date/Time. You will be prompted for Location and Date/Time range on a later screen.

6. Selected Location Rejected Transactions. This option produces a report of a specific Location's rejected transactions and sorts by Location/Date/Time. You will be prompted for Location and Date/Time range on a later screen.

Command Keys

F3 (Exit): Exit the screen without processing any pending changes.

F12 (Cancel): Exit the screen without processing any pending changes.

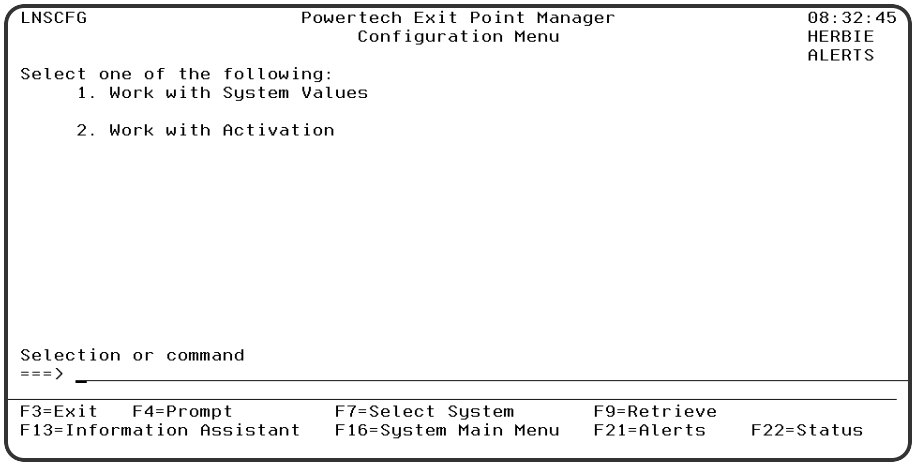
F13 (Msgs): Displays messages for the current user.

F14 (Submitted jobs): Displays jobs submitted from the current job.

F15 (Spooled files): Displays the current user's printed output.

Exit Point Manager Configuration

Use the Configuration Menu to set and maintain Exit Point Manager system values, enter your license code, and activate or deactivate Exit Point Manager exit programs.



How to Get There

To display the Configuration Menu, select option **81** from the Main Menu.

Configuration Menu Options

You can select from the following options:

1. **Work with System Values.** Select option **1** to enter your Exit Point Manager system values settings. See Exit Point Manager System Values, earlier in this User Guide, for more information.
2. **Work with Activation.** Select option **2** to work with Exit Point Manager activation and deactivation. For more information, see Activating Powertech Exit Point Manager, earlier in this User Guide.

Command Keys

F3 (Exit): Exit the menu.

F4 (Prompt): Provides assistance in entering or selecting a command.

F7 (Select System): Use this command key to work with data from a different System.

F9 (Retrieve): Displays the last command you entered on the command line and any parameters you included. Pressing this key once shows the last command you ran. Pressing this key twice shows the command you ran before that, and so on.

F13 (Information Assistant): Displays the Information Assistant menu with several types of assistance available. Press this key to access more information about the IBM i system.

F16 (System Main Menu): Displays the IBM i Main Menu (MAIN).

F22 (Status): Displays the Operational Resources pop-up window containing the status of several operation aspects of Powertech products.

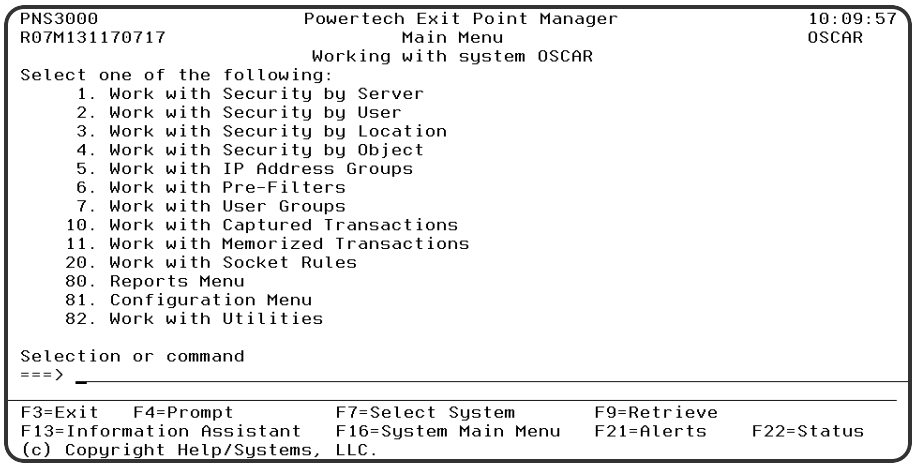
Exit Point Manager Main Menu

Use the Exit Point Manager Main Menu to work with Exit Point Manager servers, rules, reports, transactions, configuration, and utilities.

To display the Main Menu, enter the following command on an IBM i command line:

WRKPTNS

> **NOTE:** The Exit Point Manager install process places the WRKPTNS command in library PTNSLIB. Exit Point Manager activation copies the command to QGPL. If PTNSLIB or QGPL are not in your library list, enter the command as PTNSLIB/WRKPTNS or QGPL/WRKPTNS.



Main Menu Options

You can select from the following Main Menu options:

1. **Work with Security by Server.** Select option **1** to open the Work with Security by Server panel where you can you can work with server functions, work with location authorities and work with server user authorities. See Work with Servers for more information.
2. **Work with Security by User.** Select option **2** to open the Work with Security by User panel where you can work with authorities by user.

3. **Work with Security by Location.** Select option 3 to open the Work with Security by Location panel where you can work with authorities by location.
4. **Work with Security by Object.** Select option 4 to open the Work with Security by Object panel where you can work with object security. For more information, see Object Rules.
5. **Work with IP Address Groups.** Select option 5 to work with IP Address Groups. For more information, see Work with IP Address Groups.
6. **Work with Pre-filters.** Select option 6 to open the Pre-filters panel where you can establish a one-to-one relationship between a specific IP address (location) and a user.
7. **Work with User Groups.** Select option 7 to open the Work with User Groups panel where you can maintain User Groups.
10. **Work with Captured Transactions.** Select option 10 to work with captured transactions. For more information, see Working with Captured Transactions.
11. **Work with Memorized Transactions.** Select option 11 to work with memorized transactions. For more information, see Working with Memorized Transactions.
20. **Work with Socket Rules.** The Work with Socket Rules menu offers a launchpad for maintaining Socket Rules. See Work with Socket Rules panel.
80. **Reports Menu.** Select option 80 to work with Exit Point Manager reports. For more information, see Reports, later in this User Guide.
81. **Configuration Menu.** Select option 81 to work with Exit Point Manager system values, license information, and activation. For more information, see Configuration.
82. **Work with Utilities.** Select option 82 to work with Powertech Secure screen. For more information, see Utilities Menu.

Command Keys

F3 (Exit): Exit the menu.

F4 (Prompt): Provides assistance in entering or selecting a command.

F7 (Select System): Use this command key to work with data from a different System.

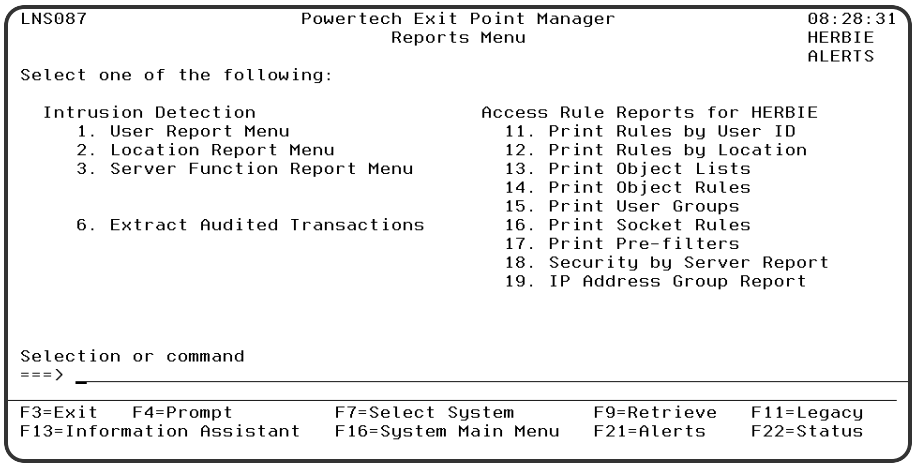
F9 (Retrieve): Displays the last command you entered on the command line and any parameters you included. Pressing this key once shows the last command you ran. Pressing this key twice shows the command you ran before that, and so on.

F13 (Information Assistant): Displays the Information Assistant menu with several types of assistance available. Press this key to access more information about the IMB i system.

F16 (System Main Menu): Displays the IBM i Main Menu (MAIN).

F22 (Status): Displays the Operational Resources pop-up window containing the status of several operation aspects of Powertech products.

Reports Menu



How to Get There

To display the Reports Menu, select option **80** on the Exit Point Manager Main Menu.

What it Does

The Powertech Reports menu is used to assist you with the reporting of status information regarding the security of your system.

> **NOTE:** This version of the Reports Menu is being deprecated. You can switch between this legacy version and the modern version by pressing function key **F11**. This legacy version uses the Powertech Audit Report command (LPWRRPT) command to produce the Intrusion Detection reports. The modern version uses the Extract Audited Transactions (PNSLOGEXT) command to produce the Intrusion Detection reports.

The options are listed for you to select. They are as follows:

Intrusion Detection

The Intrusion Detection section provides support for extracting audited transactions from any Powertech Audit Log journal that is online. Selection criteria are provided so that you can extract transactions based on attributes of the transaction such as user profile, location, server, function, date/time, etc. Most of the selection criteria support generic search terms. The extracted transactions can be printed, deposited into a database file, or streamed into a CSV-formatted file suitable for use by a spreadsheet application.

1. **User Report Menu.** Select option **1** to report on user network access attempts. See User Reports Menu.
2. **Location Report Menu.** Select option **2** to report on location network access attempts. See Location Report Menu.
3. **Server Function Report Menu.** Select option **3** to report on server/function network access attempts. See Server Function Report Menu.
4. **Transaction Report Menu.** Select option **4** to report on attempts to access data and objects, and attempts to run programs and commands. See Transaction Report Menu.
5. **Group Report Menu.** Select option **5** to report on group network access attempts. See Group Report Menu.

6. **Powertech Audit Report command.** Select option **7** to use the LPWRRPT command to create reports by user, location, server/function, user group, or transaction. See Powertech Audit Report command panel.
7. **Work with IFS Files.** Select option **10** to display reports in the IFS. See Work with IFS Files panel.

Access Rule Reports

The Access Rule Reports section provides reports listing various configuration and rule settings that you have configured. The Access Rule Reports section includes the following reporting menu options:

11. **Print Rules by User ID.** Select option **11** to print rules by user ID. See Printing Rules by User and Authorities by User Report command.
12. **Print Rules by Location.** Select option **12** to print rules by Location. See Printing Rules by Location. and Authority by Location Report panel.
13. **Print Object Lists.** Select option **13** to print a list of the Object Lists defined on your system. See Print Object Lists panel.
14. **Print Object Rules.** Select option **14** to print object rules by user or location. See Print Object Rules panel.
15. **Print User Groups.** Select option **15** to print a listing of User Groups. See Print User Groups Report.
16. **Print Socket Rules.** Select option **16** to print a listing of Socket Rules. See Print Socket Rules Report.
17. **Print Pre-Filters.** Select option **17** to print a listing of Pre-Filters. See Pre-filters Report panel.
18. **Security by Server Report.** Select option **18** to print a listing of the server and function properties you have configured. See Security by Server Report.
19. **IP Address Group Report.** Select option **19** to print a listing of the IP Address Groups you have configured. See IP Address Group Report.

Reporting Group

The Reporting Group section allows you to create and work with reporting groups.

80. **Work with Reporting Group Profiles.** Select option **80** to display the Work with Reporting Groups panel. Use this panel to create groups and assign users to them. After you associate users to a reporting group, you can report on the entire group by selecting option **5**, Group Report Menu, on the Reports Menu. See Work with Reporting Groups panel.

Command Keys

F3 (Exit): Exit the screen without processing any pending changes.

F4 (Prompt): Provides assistance in entering or selecting a command.

F7 (Select System): Use this command key to work with data from a different Silo System.

F9 (Retrieve): Displays the last command you entered on the command line and any parameters you included. Pressing this key once shows the last command you ran. Pressing this key twice shows the command you ran before that, and so on.

F11 (Legacy): Switches back to the deprecated legacy view of this menu.

F13 (Information Assistant): Displays the Information Assistant menu with several types of assistance available. Press this key to access more information about the IBM i system, such as, what's new for

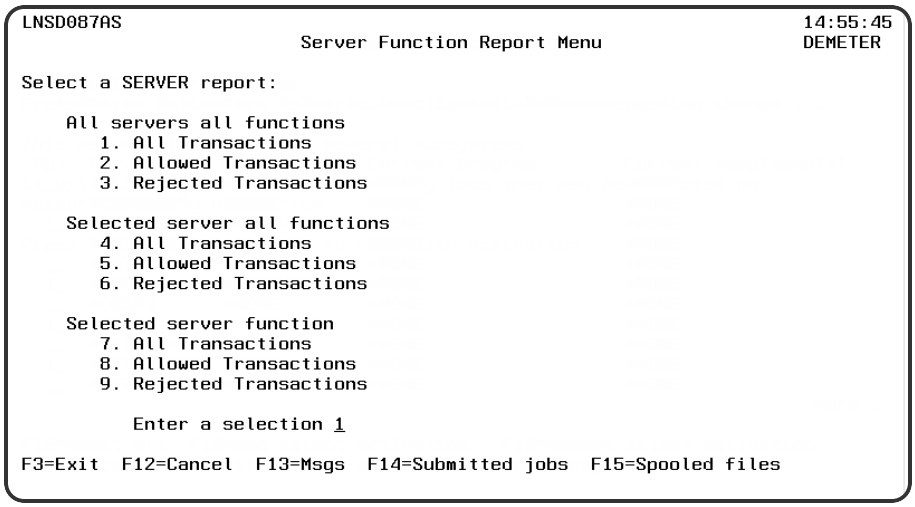
this release of the IBM i system, how to comment on information, and where to look for IBM i information in books and online.

F16 (System Main Menu): Displays the IBM i Main Menu (MAIN).

F21 (Alerts): Displays the Alerts panel where Powertech products can post errors, warnings or other general notifications to the administrator.

F22 (Status): Displays the Operational Resources pop-up window containing the status of several operation aspects of Powertech products.

Server Function Report menu



How to Get There

From the Exit Point Manager Main Menu, select option **80**, Reports Menu, then option **3**.

What it Does

The Server Function Report Menu will sort the journal by Server Function or allow you to select a specific Server with all Functions or a specific Server and a specific Function. Date range and type of transactions to be listed are also used to narrow or expand the report to your specific requirements.

Options

1. All Servers All Functions All Transactions. This option produces a report of all transactions occurring on all Servers for all Functions and sorts by Server/Function/Date/Time. You will be prompted for a Date/Time range on a later screen.

2. All Servers All Functions Allowed Transactions. This option produces a report of allowed transactions occurring on all Servers for all Functions and sorts by Server/Function/Date/Time. You will be prompted for a Date/Time range on a later screen.

3. All Servers All Functions Rejected Transactions. This option produces a report of rejected transactions occurring on all Servers for all Functions and sorts by Server/Function/Date/Time. You will be prompted for a Date/Time range on a later screen.

4. Selected Server All Functions All Transactions. This option produces a report of all transactions occurring on a selected Servers for all Functions and sorts by Server/Function/Date/Time. You will be prompted for Server and Date/Time range on a later screen.

5. Selected Server All Functions Allowed Transactions. This option produces a report of allowed transactions occurring on a selected Servers for all Functions and sorts by Server/Function/Date/Time. You will be prompted for Server and Date/Time range on a later screen.

6. Selected Server All Functions Rejected Transactions. This option produces a report of all transactions occurring on a selected Servers for all Functions and sorts by Server/Function/Date/Time. You will be prompted for Server and Date/Time range on a later screen.

7. Selected Server Function All Transactions. This option produces a report of all transactions occurring on a selected Servers for a selected Function and sorts by Date/Time. You will be prompted for Server, Function and Date/Time range on a later screen.

8. Selected Server Function Allowed Transactions. This option produces a report of allowed transactions occurring on a selected Servers for a selected Function and sorts by Date/Time. You will be prompted for Server, Function and Date/Time range on a later screen.

9. Selected Server Function Rejected Transactions. This option produces a report of rejected transactions occurring on a selected Servers for a selected Function and sorts by Date/Time. You will be prompted for Server, Function and Date/Time range on a later screen.

Command Keys

F3 (Exit): Exit the screen without processing any pending changes.

F12 (Cancel): Exit the screen without processing any pending changes.

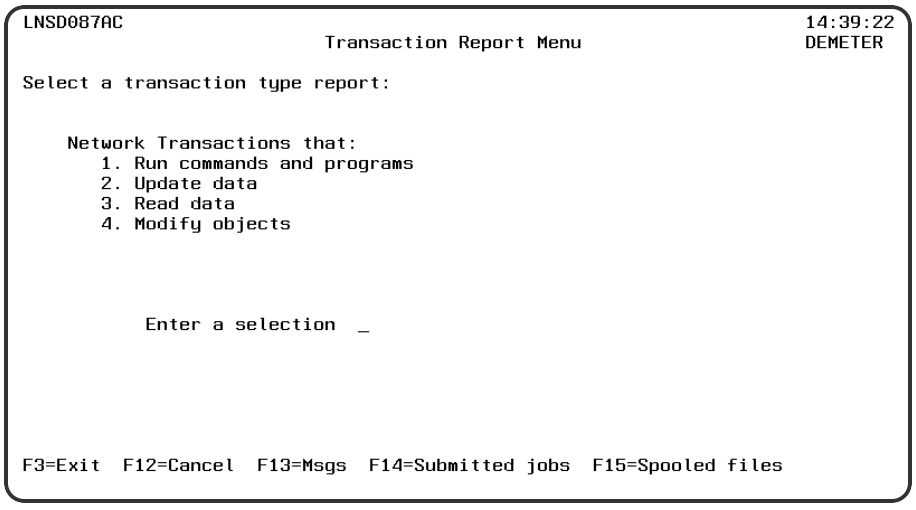
F13 (Msgs): Displays messages for the current user.

F14 (Submitted jobs): Displays jobs submitted from the current job.

F15 (Spooled files): Displays the current user's printed output.

Transaction Report menu

The Transaction Report Menu will list commands, programs, and objects that were used on your IBM i system. Date range and type of transactions to be listed are also used to narrow or expand the report to your specific requirements.



How to Get There

From the Exit Point Manager Main Menu, select option **80**, Reports Menu, then option **4**.

Options

1. Network Transactions that Run commands and programs. This option produces a report of transactions that resulted in a command or program being executed and sorts by Server/Function/Date/Time. You will be prompted for Type and Date/Time range on a later screen.

2. Network Transactions that Update data. This option produces a report of transactions that resulted in data being updated and sorts by Server/Function/Date/Time. You will be prompted for Type and Date/Time range on a later screen.

3. Network Transactions that Read data. This option produces a report of transactions that resulted in data being read and sorts by Server/Function/Date/Time. You will be prompted for Type and Date/Time range on a later screen.

4. Network Transactions that Modify objects. This option produces a report of transactions that resulted in objects being modified and sorts by Server/Function/Date/Time. You will be prompted for Type and Date/Time range on a later screen.

Command Keys

F3 (Exit): Exit the screen without processing any pending changes.

F12 (Cancel): Exit the screen without processing any pending changes.

F13 (Msgs): Displays messages for the current user.

F14 (Submitted jobs): Displays jobs submitted from the current job.

F15 (Spooled files): Displays the current user's printed output.

User Report menu

```
LNSD087AU                                                    11:00:39
                            User Report Menu                 HS42

Select a User report:

    All Users
       1. All Transactions
       2. Allowed Transactions
       3. Rejected Transactions

    Selected User
       4. All Transactions
       5. Allowed Transactions
       6. Rejected Transactions




          Enter a selection _


F3=Exit  F12=Cancel  F13=Msgs  F14=Submitted jobs  F15=Spooled files
```

How to Get There

From the Exit Point Manager Main Menu, choose option **80**, Reports Menu, then option **1**.

What it Does

The User Report Menu will sort the journal by User or allow you to select a specific User. User Groups can also be selected. Date range and type of transactions to be listed are also used to narrow or expand the report to your specific requirements.

Options

1. All Users All Transactions. This option produces a report of all current Users' transactions and sorts by User/Date/Time. User Groups can also be selected. You will be prompted for User and Date/Time range on a later panel.

2. All Users Allowed Transactions. This option produces a report of all current User's allowed transactions and sorts by User/Date/Time. User Groups can also be selected. You will be prompted for User and Date/Time range on a later panel.

3. All Users Rejected Transactions. This option produces a report of all current Users' rejected transactions and sorts by User/Date/Time. User Groups can also be selected. You will be prompted for User and Date/Time range on a later panel.

4. Selected User All Transactions. This option produces a report of a specific User's transactions and sorts by User/Date/Time. User Groups can also be selected. You will be prompted for User and Date/Time range on a later panel.

5. Selected User Allowed Transactions. This option produces a report of a specific User's allowed transactions and sorts by User/Date/Time. User Groups can also be selected. You will be prompted for User and Date/Time range on a later panel.

6. Selected User Rejected Transactions. This option produces a report of a specific User's rejected transactions and sorts by User/Date/Time. User Groups can also be selected. You will be prompted for User and Date/Time range on a later panel.

Command Keys

F3 (Exit): Exit the panel without processing any pending changes.

F12 (Cancel): Exit the panel without processing any pending changes.

F13 (Msgs): Displays messages for the current user.

F14 (Submitted jobs): Displays jobs submitted from the current job.

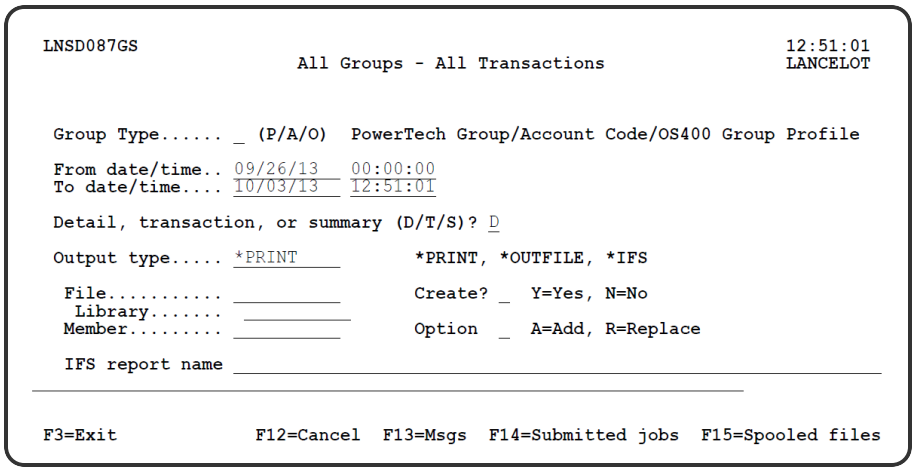
F15 (Spooled files): Displays the current user's printed output.

Prompts

The topics in this section include descriptions for Exit Point Manager's green screen prompts.

Group Report Prompt

This panel allows you to select the data that you would like in your report as well as any output options that are available.



Options

Group Type

Specify the type of user group you would like listed in your report using one of these values:

P The name is a Powertech Group name.
A The name is an accounting code.
O The name is an operating system group profile.

From Date

This field is the oldest transaction date you wish to see. Key this date in your job's current format.

From Time

This field is the oldest transaction time you wish to see. Key this time in your job's current format.

To Date

This field is the most recent transaction date you wish to see. Key this date in your job's current format.

Detail, transaction, or summary (D/T/S)?

This field controls the amount of information shown on the report.

Select one of the following values:

S Summary information (least amount of detail)
D Detail information.
T Transaction information (greatest amount of detail).

Output type

Specifies the form of output. This requests the output in either printed or database form or in a .CSV streamfile. This is a required value.

The possible values are:

***PRINT** The output should be a printed report.
***OUTFILE** The output should be directed to a database file.
***IFS** The output should be directed to a .CSV streamfile in the IFS. The streamfile will be created in the location specified in the GNUI Report Output control file (PNSGRO).

Output file

Specifies the name of the database file that will contain the selected output. The resulting output file will have the same record format as the LNSJRNQY file in the Exit Point Manager library.

The possible values are:

database—file—name Enter the name of the database file that will contain the selected output.

Output file library

Specifies the name of the library in which the output file will be created.

The possible values are:

library—name Enter the name of the library where the database file is located.

Output member

Specifies the member name when output is directed to a database file. This is an optional parameter. This is only meaningful when output type *OUTFILE is selected.

Allowed values for member are:

***FIRST** The first (or only) member receives the output. If no members exist in the file and you specify OUTMBR(*FIRST), a member will be added whose name will be the same as the output file name specified for Output File.
member—name Enter a valid member name.

Output member options

Specifies the option when output is directed to a database file.

Allowed values for option are:

A The existing member data is kept and this output end of the member.
R The member data is replaced by this output.

Create file

Specifies whether the output file should be created if it does not exist. This is an optional parameter.

Allowed values are:

N The output file should not be created. The command will fail if the file does not exist.
Y The file will be created if it does not exist when the command executes.

IFS report name

Specifies the report name of the IFS streamfile. This name is used to log the creation and location of any IFS streamfiles that are created.

The possible values are:

report—name Enter the name of IFS report. This is a report name, not a streamfile name. IFS output is created in a standard location. This report name identifies report requests.

Command Keys

F3 (Exit): Exit the panel without processing any pending changes.

F12 (Cancel): Exit the panel without processing any pending changes.

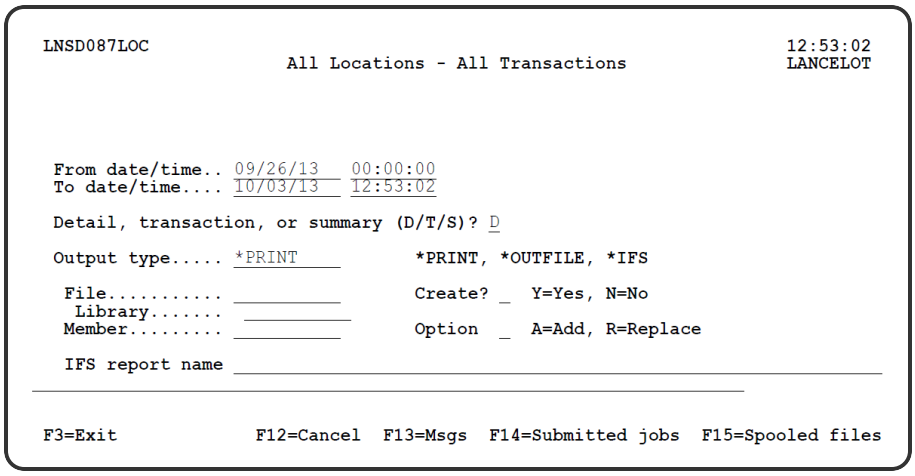
F13 (Msgs): Displays messages for the current user.

F14 (Submitted jobs): Displays jobs submitted from the current job.

F15 (Spooled files): Displays the current user's printed output.

Location Report Prompt

This screen allows you to select the data that you would like in your report as well as any output options that are available.



From Date

This field is the oldest transaction date you wish to see. Key this date in your job's current format.

From Time

This field is the oldest transaction time you wish to see. Key this time in your job's current format.

To Date

This field is the most recent transaction date you wish to see. Key this date in your job's current format.

Detail, transaction, or summary (D/T/S)?

This field controls the amount of information shown on the report.

Select one of the following values:

S Summary information (least amount of detail)
D Detail information.
T Transaction information (greatest amount of detail).

Output type

Specifies the form of output. This requests the output in either printed or database form or in a .CSV streamfile. This is a required value.

The possible values are:

***PRINT** The output should be a printed report.
***OUTFILE** The output should be directed to a database file.
***IFS** The output should be directed to a .CSV streamfile in the IFS. The streamfile will be created in the location specified in the GNUI Report Output control file (PNSGRO).

Output file

Specifies the name of the database file that will contain the selected output. The resulting output file will have the same record format as the LNSJRNQY file in the Exit Point Manager library.

The possible value is:

database—file—name Enter the name of the database file that will contain the selected output.

Output file library

Specifies the name of the library in which the output file will be created.

The possible value is:

library—name Enter the name of the library where the database file is located.

Output member

Specifies the member name when output is directed to a database file. This is an optional parameter. This is only meaningful when output type *OUTFILE is selected.

Allowed values for member are:

***FIRST** The first (or only) member receives the output. If no members exist in the file and you specify OUTMBR(*FIRST), a member will be added whose name will be the same as the output file name specified for Output File.
member—name Enter a valid member name.

Output member options

Specifies the option when output is directed to a database file.

Allowed values for option are:

A The existing member data is kept and this output end of the member.
R The member data is replaced by this output.

Create file

Specifies whether the output file should be created if it does not exist. This is an optional parameter.

Allowed values are:

N The output file should not be created. The command will fail if the file does not exist.
Y The file will be created if it does not exist when the command executes.

IFS report name

Specifies the report name of the IFS streamfile. This name is used to log the creation and location of any IFS streamfiles that are created.

The possible value is:

report—name Enter the name of IFS report. This is a report name, not a streamfile name. IFS output is created in a standard location. This report name identifies report requests.

Command Keys

F3 (Exit): Exit the screen without processing any pending changes.

F12 (Cancel): Exit the screen without processing any pending changes.

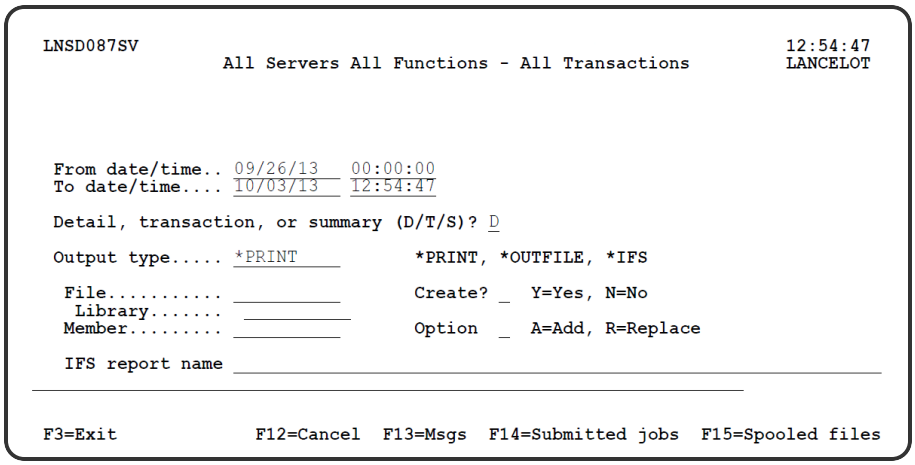
F13 (Msgs): Displays messages for the current user.

F14 (Submitted jobs): Displays jobs submitted from the current job.

F15 (Spooled files): Displays the current user's printed output.

Server Function Report prompt

This screen allows you to select the data that you would like in your report as well as any output options that are available.



Field Descriptions

From Date

This field is the oldest transaction date you wish to see. Key this date in your job's current format.

From Time

This field is the oldest transaction time you wish to see. Key this time in your job's current format.

To Date

This field is the most recent transaction date you wish to see. Key this date in your job's current format.

Detail, transaction, or summary (D/T/S)?

This field controls the amount of information shown on the report.

Select one of the following values:

S Summary information (least amount of detail)
D Detail information.
T Transaction information (greatest amount of detail).

Output type

Specifies the form of output. This requests the output in either printed or database form or in a .CSV streamfile. This is a required value.

The possible values are:

***PRINT** The output should be a printed report.
***OUTFILE** The output should be directed to a database file.
***IFS** The output should be directed to a .CSV streamfile in the IFS. The streamfile will be created in the location specified in the GNUI Report Output control file (PNSGRO).

Output file

Specifies the name of the database file that will contain the selected output. The resulting output file will have the same record format as the LNSJRNQY file in the Exit Point Manager library.

The possible value is:

database—file—name Enter the name of the database file that will contain the selected output.

Output file library

Specifies the name of the library in which the output file will be created.

The possible value is:

library—name Enter the name of the library where the database file is located.

Output member

Specifies the member name when output is directed to a database file. This is an optional parameter. This is only meaningful when output type *OUTFILE is selected.

Allowed values for member are:

***FIRST** The first (or only) member receives the output. If no members exist in the file and you specify OUTMBR(*FIRST), a member will be added whose name will be the same as the output file name specified for Output File.
member—name Enter a valid member name.

Output member options

Specifies the option when output is directed to a database file.

Allowed values for option are:

A The existing member data is kept and this output end of the member.
R The member data is replaced by this output.

Create file

Specifies whether the output file should be created if it does not exist. This is an optional parameter.

Allowed values are:

N The output file should not be created. The command will fail if the file does not exist.
Y The file will be created if it does not exist when the command executes.

IFS report name
Specifies the report name of the IFS streamfile. This name is used to log the creation and location of any IFS streamfiles that are created.

The possible values are:

> **report—name** Enter the name of IFS report. This is a report name, not a streamfile name. IFS output is created in a standard location. This report name identifies report requests.

Command Keys
F3 (Exit): Exit the screen without processing any pending changes.

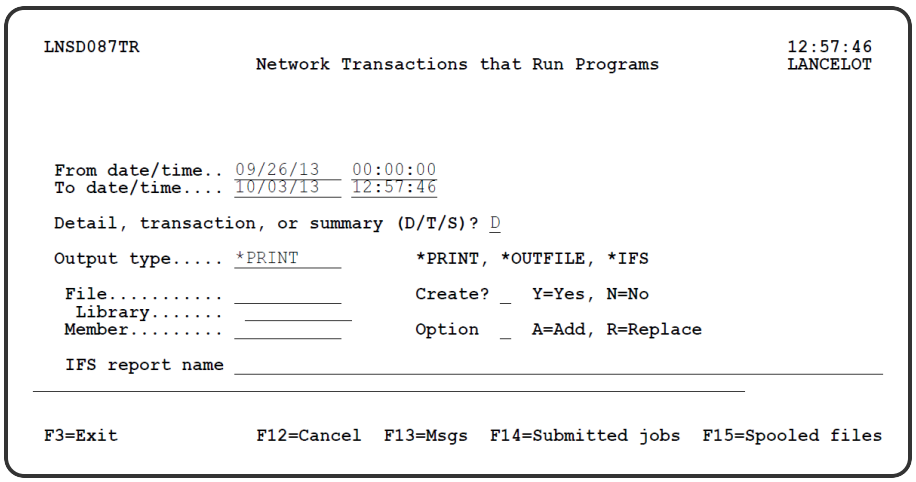
F12 (Cancel): Exit the screen without processing any pending changes.

F13 (Msgs): Displays messages for the current user.

F14 (Submitted jobs): Displays jobs submitted from the current job.

F15 (Spooled files): Displays the current user's printed output.

Transaction Report prompt
This panel allows you to select the data for your report as well as any output options that are available.



From Date
This field is the oldest transaction date you wish to see. Key this date in your job's current format.

From Time
This field is the oldest transaction time you wish to see. Key this time in your job's current format.

To Date
This field is the most recent transaction date you wish to see. Key this date in your job's current format.

Detail, transaction, or summary (D/T/S)?
This field controls the amount of information shown on the report.

Select one of the following values:

S Summary information (least amount of detail)
D Detail information.
T Transaction information (greatest amount of detail).

Output type

Specifies the form of output. This requests the output in either printed or database form or in a .CSV streamfile. This is a required value.

The possible values are:

***PRINT** The output should be a printed report.
***OUTFILE** The output should be directed to a database file.
***IFS** The output should be directed to a .CSV streamfile in the IFS. The streamfile will be created in the location specified in the GNUI Report Output control file (PNSGRO).

Output file

Specifies the name of the database file that will contain the selected output. The resulting output file will have the same record format as the LNSJRNQY file in the Exit Point Manager library.

The possible values are:

database—file—name Enter the name of the database file that will contain the selected output.

Output file library

Specifies the name of the library in which the output file will be created.

The possible values are:

library—name Enter the name of the library where the database file is located.

Output member

Specifies the member name when output is directed to a database file. This is an optional parameter. This is only meaningful when output type *OUTFILE is selected.

Allowed values for member are:

***FIRST** The first (or only) member receives the output. If no members exist in the file and you specify OUTMBR(*FIRST), a member will be added whose name will be the same as the output file name specified for Output File.
member—name Enter a valid member name.

Output member options

Specifies the option when output is directed to a database file.

Allowed values for option are:

A The existing member data is kept and this output end of the member.
R The member data is replaced by this output.

Create file

Specifies whether the output file should be created if it does not exist. This is an optional parameter.

Allowed values are:

N The output file should not be created. The command will fail if the file does not exist.
Y The file will be created if it does not exist when the command executes.

IFS report name
Specifies the report name of the IFS streamfile. This name is used to log the creation and location of any IFS streamfiles that are created.

The possible values are:

report—name Enter the name of IFS report. This is a report name, not a streamfile name. IFS output is created in a standard location. This report name identifies report requests.

Command Keys
F3 (Exit): Exit the panel without processing any pending changes.

F12 (Cancel): Exit the panel without processing any pending changes.

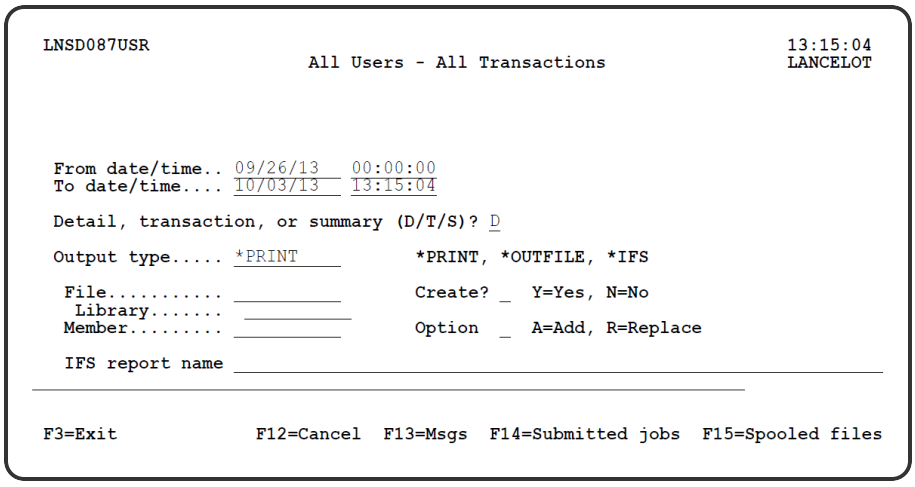
F13 (Msgs): Displays messages for the current user.

F14 (Submitted jobs): Displays jobs submitted from the current job.

F15 (Spooled files): Displays the current user's printed output.

User Report prompt

This panel allows you to select the data for your report as well as any output options that are available.



Field Descriptions

From Date
This field is the oldest transaction date you wish to see. Key this date in your job's current format.

From Time
This field is the oldest transaction time you wish to see. Key this time in your job's current format.

To Date

This field is the most recent transaction date you wish to see. Key this date in your job's current format.

Detail, transaction, or summary (D/T/S)?

This field controls the amount of information shown on the report.

Select one of the following values:

S Summary information (least amount of detail)
D Detail information.
T Transaction information (greatest amount of detail).

Output type

Specifies the form of output. This requests the output in either printed or database form or in a .CSV streamfile. This is a required value.

The possible values are:

***PRINT** The output should be a printed report.
***OUTFILE** The output should be directed to a database file.
***IFS** The output should be directed to a .CSV streamfile in the IFS. The streamfile will be created in the location specified in the GNUI Report Output control file (PNSGRO).

Output file

Specifies the name of the database file that will contain the selected output. The resulting output file will have the same record format as the LNSJRNQY file in the Exit Point Manager library.

The possible value is:

database—file—name Enter the name of the database file that will contain the selected output.

Output file library

Specifies the name of the library in which the output file will be created.

The possible value is:

library—name Enter the name of the library where the database file is located.

Output member

Specifies the member name when output is directed to a database file. This is an optional parameter. This is only meaningful when output type *OUTFILE is selected.

Allowed values for member are:

***FIRST** The first (or only) member receives the output. If no members exist in the file and you specify OUTMBR(*FIRST), a member will be added whose name will be the same as the output file name specified for Output File.
member—name Enter a valid member name.

Output member options

Specifies the option when output is directed to a database file.

Allowed values for option are:

A The existing member data is kept and this output end of the member.
R The member data is replaced by this output.

Create file

Specifies whether the output file should be created if it does not exist. This is an optional parameter.

Allowed values are:

N The output file should not be created. The command will fail if the file does not exist.
Y The file will be created if it does not exist when the command executes.

IFS report name

Specifies the report name of the IFS streamfile. This name is used to log the creation and location of any IFS streamfiles that are created.

The possible value is:

report—name Enter the name of IFS report. This is a report name, not a streamfile name. IFS output is created in a standard location. This report name identifies report requests.

Command Keys

F3 (Exit): Exit the panel without processing any pending changes.

F12 (Cancel): Exit the panel without processing any pending changes.

F13 (Msgs): Displays messages for the current user.

F14 (Submitted jobs): Displays jobs submitted from the current job.

F15 (Spooled files): Displays the current user's printed output.

Appendix

The topics in this section include additional information about Exit Point Manager.

Appendix A: Exit Point Manager Commands

Powertech Exit Point Manager offers a number of commands that provide flexibility in managing your Exit Point Manager environment. Commands range from basic filter rule maintenance to more advanced features of Exit Point Manager.

You enter the Exit Point Manager commands on a command line, or include the commands in your own programs. The following table summarizes the commands.

Command	Description
Primary Administration Commands	
DLTNSUGRP	Allows the deletion of NS User Groups and, optionally, their members
WRKPTNS	Displays the Powertech Exit Point Manager Main Menu

Command	Description
LEDTSYSVAL	Displays the Work with Exit Point Manager System Values panel
LCOPYRIGHT	Displays the Powertech Exit Point Manager End User License Agreement
MRGPRVNS	Displays the Merge previous NS panel
POWERLOCK	Powertech Exit Point Manager Main Menu (for versions prior to Exit Point Manager 6.0)
ADDNSLIC	Displays the Exit Point Manager License Setup panel
PTNSSTRWEB	Starts the server job to support the web interface
PTNSENDWEB	Ends the server job that supports the web interface
PNSHLDDASH	Sets the system in a state such that data collection to support the web interface Dashboard will not run.
PNSSTRDASH	Begins the Dashboad Data Collector.
PNSENDDASH	Ends the Dashboad Data Collector.
PNSRLSDASH	Releases the Hold Dashboard Collection command, allowing data collection to occur.
Commands that Work with Filter Rules	
LWRKSRV	Work with Servers
LWRKSRVFNC	Work with Security by Server/Function
LEDTFNCLOC	Edit Function by Location
LEDTFNCUSR	Edit Function by User
LEDTSRVLOC	Edit Server by Location
LEDTSRVUSR	Edit Server by User
LEDTUSRAUT	Edit User Authorities
Schedule Jobs Commands	
LPWRRPT	Exit Point Manager Audit Report
PNSLOGEXT	Extracts audited transaction data from the audit log, which can be printed, placed into an output database file, or placed into a CSV-formatted stream file. See Extract Audited Transactions (PNSLOGEXT) command.
SBMIPGREP	Prints a listing of the IP Address Groups that have been configured.

Command	Description
SBMSVFREP	Prints a listing of the Server and Function properties that have been configured.
LENDCAPSUM	End Captured Transaction Summarization (formerly LSENCAPSUM)
LCHGCAPSUM	Changes summarization properties for captured transactions
LSTRCAPSUM	Start Captured Transaction Summarization
LPWRCAPTRN	Work with Captured Transactions
LRSNESCMSG	Resend Escape Message
LRTNLEN	Length of the value of a string
LMOVDIAMSG	Move Diagnostic Message
SBMUSRREP	Submit Authority by User Report
SBMLOCREP	Submit Authority by Location Report
PLNSREPORT	Exit Point Manager Reports Menu
Command	Description
Customization Commands	
LPRDVRM	Product Information Display
TELNETPVL	Telnet Password Verification
LADDLNSEXT	Add Exit Point Manager Exit Programs
LRMVLNSEXT	Remove Exit Point Manager Exit Programs
LNSCCLCVT	Convert existing memorized transactions to the absolute path
NSNFREJECT	Set NF Reject Value
LWRKGENSRV	Work with Add-On Servers
Create Rules Commands	
CRTLOCRUL	Create Location Rule
CRTUSRRUL	Create User Rule
CRTOBJRUL	Create Object Rule
Change Rules Commands	
CHGLOCRUL	Change Location Rule
CHGUSRRUL	Change User Rule

Command	Description
CHGOBJRUL	Change Object Rule
Delete Rules Commands	
DLTLOCRUL	Delete Location Rule
DLTUSRRUL	Delete User Rule
DLTOBJRUL	Delete Object Rule
Display Rules Commands	
DSPLOCRUL	Display Location Rule
DSPUSRRUL	Display User Rule
DSPOBJRUL	Display Object Rule
Object List Commands	
ADDOBJLE	Add Object List Entry
CHGOBJLE	Change Object List Entry
RMVOBJLE	Remove Object List Entry
CHGOBJL	Change Object List
CPYOBJL	Copy Object List
CRTOBJL	Create Object List
DLTOBJL	Delete Object List
PRTOBJL	Print Object List
RNMOBJL	Rename Object List
WRKOBJL	Work with Object Lists
PRTOBJRUL	Print Object Rule
WRKOBJRUL	Work with Object Rules
Secure Screen commands	
ENDPLSSMON	End Secure Screen Monitors
LCKDSP	Locks your own display
LCKDSP JOB (nbr/user/job)	Locks another display. To lock another display, you need the *JOBCTL special authority unless the other job is the same job user.
LEDTPSSFTR	Secure Screen Rules Maintenance

Command	Description
LSETPSSNFQ	Set Secure Screen notify message queue
SETSECSRN	Set Secure Screen System ID
STRPLSSMON	Start Secure Screen monitor
UNLDSP JOB (nbr/user/job)	Unlocks a display that was locked by the LCKDSP command. You need *ALLOBJ special authority, or specific *USE authority on the command.
WRKSECSCR	Secure Screen Main Menu

Appendix B: Servers and Functions

Exit Point Manager supports the following servers.

Exit Point Server	Description
*CLI	Call Level Interface
*CNTRLSRV	License Management Central Server
DATADIST	ShowCase DATADIST server
*DATAQSRV	Optimized Data Queue Server
*DDM	Distributed Data Management Server
*DRDA	Distributed Relational Database
*DQSRV	Data Queue Server
*FILESRV	File Server
*FTPCLIENT	IBM i FTP Client
*FTPREXEC	FTP Execute Remote Command (REXEC)
*FTPSERVER	IBM i FTP Server
*FTPSIGNON	FTP Logon Server
*LMSRV	License Management Server
*MSGFCL	Message Function Server
*NDB	Native Database Request
QNPSERV	Network Print Server
*REXEC_SO	Remote Execute Command Signon Server
*RMTSRV	Remote Command and Distributed Program Call Server

Exit Point Server	Description
*RTVOBJINF	SQL Retrieve Object Information
*RQSRV	Remote SQL Server
*SIGNON	Signon Server
*SQL	Database Server Initialization
*SQLSRV	SQL Server
*TELNET	Telnet Device Initiation/Termination
*TFRFCL	File Transfer Server
*TFTP	Trivial FTP Server
*VISTA	ShowCase *VISTA Servers
*VISTAPRO	ShowCase *VISTAPRO Server
VISTA_ADMI	ShowCase VISTA_ADMI Servers
*VPRT	Virtual Print Server

Exit Point Manager also provides access control and monitoring for socket exit points:

Exit Point Server	Description
QSOLISTEN	Socket Listen server
QSOCONNECT	Socket Connect server
QSOACCEPT	Socket Accept server

Exit Point Manager also provides access control and monitoring for exit points that are specific to the ShowCase software suite. See the table of ShowCase Servers shown below:

Exit Point Server	Description
*VISTA A Showcase corporation server.	ShowCase *VISTA Clients
*VISTAPRO A Showcase corporation server.	ShowCase *VISTAPRO Clients
DATADIST A Showcase corporation server.	ShowCase DATADIST Clients
VISTA_ADMI A Showcase corporation server.	ShowCase VISTA_ADMI Clients

Understanding Servers

Networked clients, including Client Access, can communicate with several servers on IBM i for network access. Exit Point Manager integrates with these servers, at the exit-point level, to allow you to specify your own access rules. You should have a clear understanding of what these servers do to develop and implement an effective network security plan.

In general, each server corresponds with a client function, such as file transfer, FTP, or remote command. In some cases, IBM created two servers for some functions. It is important to secure both servers to completely secure your IBM i.

Exit Point Manager allows you to set rules for how to secure each server. The following table lists the servers used by the various client functions. Note: The mapping of client function to server is subject to change by IBM. For the latest information from IBM, go to the Information Center Web site at www.iseries.ibm.com/infocenter. Click the Client Access Express link, select Administering Client Access Express, and then select Host Server Administration.

Client Function	OS/400 Server	IBM Server ID
File Transfer	Transfer Function Server Database Server	*TFRFCL *SQL *NDB *SQLSRV *RTVOBJINF
ODBC	Remote SQL Server Database Server	*RQSRV *SQL *NDB *SQLSRV *RTVOBJINF
Shared Folders	Distributed Data Management Server File Server	*DDM *FILESRV
Virtual Print	Virtual Print Server Network Print Server	*VPRT QNPSERVR
Data Queue API	Original Data Queue Server Optimized Data Queue Server	*DQSRV *DATAQSRV
Remote Command	Distributed Data Management Server Remote Command and Distributed Program Call Server	*DDM *RMTSRV
Message Function	Message Function Server	*MSGFCL
License and Client Management	License Management Central Server	*LMSRV *CNTRLSRV

Client Function	OS/400 Server	IBM Server ID
FTP	FTP Client FTP Execute Remote Command FTP Server FTP Signon Trivial FTP	*FTPCLIENT *FTPREXEC *FTPSERVER *FTPSIGNON *TFTP
Distributed Relational Database	DRDA Server CLI Connect Server	*DRDA *CLI
Signon	Signon Server	*SIGNON
Distributed Program Call	Remote Command and Distributed Program Call Server Remote Execution Signon	*RMTSRV *REXEC_SO
Telnet	Telnet	*TELNET

When a networked client makes a request of a server, it requests the server to execute a particular function. For example, when you prompt for a list of files in the Client Access data transfer function, it sends a request to the File Transfer Server to execute the EXTRACT function. When you request to download a file to a PC, it sends a request for the SELECT function.

Exit Point Manager allows you to set security rules for the server as a whole, but also for individual functions within a server.

The Central Server

> **NOTE:** We recommend that you do not restrict the use of the Central Server as this can make it impossible for any client to connect to your IBM i system.

The Central Server is used by Client Access optimized clients to process license management and client management requests. Original clients use the License Management Server to process license management requests and do not support client management requests.

The Central Server does not implement any functions that pose security problems for most installations.

The following table lists the Central Server functions used by the different client actions.

Client Action	Server Name	Server Function
Request a license	*CNTRLSRV	RQSLIC
Release a license	*CNTRLSRV	RLSLIC
Retrieve license information	*CNTRLSRV	RTVLICINF
Set client active	*CNTRLSRV	SETACT

Client Action	Server Name	Server Function
Set client inactive	*CNTRLSRV	SETINACT
Retrieve character set conversion map	*CNTRLSRV	RTVCNVMAP

The CLI Server

Call Level Interface (*CLI) is an alternative mechanism for executing SQL statements.

From "IBM DB2 for i tips" at the IBM Knowledge Center:

For the most part, SQL CLI is syntactically and semantically equivalent to ODBC. The SQL Call Level Interface is a standard created by the X/Open standards group, and CLI was built according to the standard.

ODBC is the Microsoft implementation of the X/Open CLI standard, and has veered off from the X/Open standard in a few areas. CLI will probably never match ODBC exactly, since that is technically not the standard that CLI is built to comply with.

Client Action	Server Name	Server Function
CLI Connection	*CLI	CONNECT

The Database Server

The Database Server is used to process SQL statements received from some original and optimized clients using ODBC. In addition, the Windows 95/98/NT/2000 client UI file transfer application uses this server. It is also used by optimized clients using the Remote SQL and file transfer APIs.

The Database Server is unusual in that it looks to Exit Point Manager as if it were four different servers. Thus, when securing the Database Server you might need to enter rules for four different server names. The following table lists the Database Server functions used by the different client actions.

Client Action	Server Name	Server Function
Connect to the Database Server	*SQL	INIT
Create a database file	*NDB	CRTSRCPF CRTDBF
Add a member to a database file	*NDB	ADDDBFMBR
Add library list entry	*NDB	ADDLIBL
Delete a database file member	*NDB	DLTDBFMBR

Client Action	Server Name	Server Function
Clear a database file member	*NDB	CLRDBFMBR
Override a database file	*NDB	OVRDBF
Delete database file override	*NDB	DLTDBFOVR
Delete a database file	*NDB	DLTF
Connect to a database	*SQLSRV	CONNECT
Prepare an SQL statement	*SQLSRV	PRPDDESCRB PRPEXCOPN PREPARE
Execute an SQL statement	*SQLSRV	EXECUTE EXECUTEIMM PRPEXCOPN EXECOPEN
Prepare and execute	*SQLSRV	PRPEXECUTE
Fetch rows	*SQLSRV	FETCH
Create an SQL package	*SQLSRV	CREATEPKG
Clear an SQL package	*SQLSRV	CLEARPKG
Delete an SQL package	*SQLSRV	DELETEPKG
Open an SQL cursor	*SQLSRV	OPEN EXECOPEN OPENFETCH PRPEXCOPN
Retrieve information about libraries, databases, SQL packages, and so on	*RTVOBJINF	RTVLIBINF RTVRDBINF RTVSQLPKG RTVSQLSTMT RTVFILINF RTVMBRINF RTVFMTINF RTVFLDINF RTVIDXINF RTVFKEYINF RTVPKEYINF RTVCLMINF

The Distributed Data Management Server

The Distributed Data Management (DDM) Server is used by some clients to process Shared Folder and Remote Command requests. Older original clients used the DDM server for Shared Folders. Newer original clients and optimized clients use the File Server for Shared Folders. Original clients use the DDM Server for Remote Command support. Optimized clients use the Remote Command and Distributed Program Call Server for Remote Command support. The following table lists the DDM Server functions used by the different client actions.

Client Action	Server Name	Server Function
Initialize DDM	*DDM	INITIALIZE
Create a file	*DDM	CREATE
Delete a file	*DDM	DELETE
Rename a file	*DDM	RENAME
Change file information	*DDM	CHANGE
Lock a file	*DDM	LOCK
Copy file data from another system	*DDM	LOAD
Copy file data to another system	*DDM	UNLOAD
Copy a file on this system	*DDM	COPy
Move a file on this system	*DDM	MOVE
Retrieve file information	*DDM	EXTRACT
Open a file	*DDM	OPEN
Add a member to a file	*DDM	ADDMBR
Change a file member	*DDM	CHGMBR
Delete a file member	*DDM	RMVMBR
Rename a file member	*DDM	RNMMBR
Reorganize a file member	*DDM	RGZMBR
Clear a file member	*DDM	CLEAR
Change data area	*DDM	CHGDTAARA
Retrieve data area	*DDM	RTVDTAARA
Clear data queue	*DDM	CLRDTAQ
Receive data queue	*DDM	RCVDTAQ
Send data queue	*DDM	SNDDTAQ
Run a command on this system	*DDM	COMMAND

The Distributed Relational Database Server

The DRDA Server (*DRDA) is used by some ODBC clients to process iSeries Database requests.

Client Action	Server Name	Server Function
SQL connect	*DRDA	SQLCNN

The DRDA Server

The DRDA Server is used by some ODBC clients to process IBM i Database requests. The following table lists the DRDA Server functions used by client actions.

Client Action	Server Name	Server Function
SQL Connect	*DRDA	SQLCNN

The File Server

The File Server is used by newer Client Access original clients and optimized clients to process Shared Folder requests. Older original clients used the DDM server for Shared Folders. The following table lists the File Server functions used by the different client actions.

Client Action	Server Name	Server Function
Allocate a conversation	*FILESRV	ALCSTRMCNV
Create a file or directory	*FILESRV	CRTSTRMFIL
Delete a file or directory	*FILESRV	DLTSTRMFIL
Rename a file or directory	*FILESRV	RNMSTRMFIL
List attributes of a file or directory	*FILESRV	LSTSTRMATR
Change attributes of a file or directory	*FILESRV	CHGSTRMATR
Move a file	*FILESRV	MOVSTRMFIL
Open a file	*FILESRV	OPNSTRMFIL

The FTP Application Servers

NOTE: You might be more familiar with the *FTPREXEC server as the REXEC server.

The TCP/IP FTP Application Servers are used by various clients to send and receive files and commands via FTP. The following table lists the FTP Server functions used by different client and server actions.

Client Action	Server Name	Server Function
Initialize Session	*FTPCLIENT	INIT
Set Current Library or Directory	*FTPCLIENT	CHGCURLIB
Send Files (Put)	*FTPCLIENT	SENDFILE
Receive Files	*FTPCLIENT	RECVFILE
Execute Remote Commands	*FTPCLIENT	RMTCMD

Client Action	Server Name	Server Function
Create Library/Directory	*FTPCLIENT	CREATELIB
Delete Files	*FTPCLIENT	DELETEFILE
Delete Library/Directory	*FTPCLIENT	DELETELIB
List files in Library/Directory	*FTPCLIENT	LISTFILES
Rename File	*FTPCLIENT	RNMFILE
Remote Command Initialize Session	*FTPREXEC	INIT
Execute Remote Command	*FTPREXEC	RMTCMD
Session Initialization	*FTPSERVER	INIT
Set Current Library	*FTPSERVER	CHGCURLIB
Client Action	Server Name	Server Function
Delete Library/Directory	*FTPSERVER	DELETELIB
Create Library/Directory	*FTPSERVER	CREATELIB
List Files in Directory/Library	*FTPSERVER	LISTFILES
Delete Files	*FTPSERVER	DELETEFILE
Send Files (Put)	*FTPSERVER	SENDFILE
Receive Files (Get)	*FTPSERVER	RECVFILE
Rename Files	*FTPSERVER	RNMFILE
Execute Remote Commands	*FTPSERVER	RMTCMD
TFTP Receive File (Get)	*TFTP	RECVFILE
TFTP Send File (Put)	*TFTP	SENDFILE

The FTP Logon Server

The FTP Logon server is used to validate signon attempts to an IBM i system through FTP. The following table lists the FTP Logon Server functions used by client actions.

Client Action	Server Name	Server Function
Sign on	*FTPSIGNON	SIGNON

The License Management Server

NOTE: We recommend that you do not restrict the use of the License Management Server as this can make it impossible for any client to connect to your IBM i.

The License Management Server is used by Client Access original clients to process license management requests. Optimized clients use the Central Server to process license management requests.

The License Management Server does not implement any functions that pose security problems for most installations.

The following table lists the License Management Server functions used by the different client actions.

Client Action	Server Name	Server Function
Request a license	*LMSRV	REQUEST
Release a license	*LMSRV	RELEASE

The Message Function Server

The Message Function Server is used by Client Access to process messaging requests. The following table lists the Message Function Server functions used by the different client actions.

Client Action	Server Name	Server Function
Send a message	*MSGFCL	SEND
Receive a message	*MSGFCL	RECEIVE

The Network Print Server

The Network Print Server is used by Client Access optimized clients to process requests to print on an IBM i printer. Original clients use the Virtual Print server for requests to print on an IBM i printer. The following table lists the Network Print Server functions used by the different client actions.

Client Action	Server Name	Server Function
Initialize the Network Print Server	QNPSERVR	INIT
Process a spooled file	QNPSERVR	PROCESS

The Optimized Data Queue Server

The Optimized Data Queue Server is used by Client Access optimized clients to process requests made by client programs using the Client Access API to access IBM i data queues. Original clients use the Original Data Queue Server to process these requests. The following table lists the Optimized Data Queue Server functions used by the different client actions.

Client Action	Server Name	Server Function
Create a data queue	*DATAQSRV	CRTDTQ
Delete a data queue	*DATAQSRV	DLTDTQ
Query a data queue	*DATAQSRV	QRYDTQATR
Send a message to a data queue	*DATAQSRV	SNDDTQMSG
Receive a message from a data queue	*DATAQSRV	RCVDTQMSG RECVMSG
Clear all messages from a data queue	*DATAQSRV	CLRDTQMSG
Cancel a pending data queue request	*DATAQSRV	CNLPNDRCV

The Original Data Queue Server

The Original Data Queue Server is used by Client Access original clients to process requests by PC programs using the Client Access API to access IBM i data queues. Optimized clients use the Optimized Data Queue Server to process these requests. The following table lists the Original Data Queue Server functions used by the different client actions.

Client Action	Server Name	Server Function
Create a data queue	*DQSRV	CREATE
Delete a data queue	*DQSRV	DELETE
Query a data queue	*DQSRV	QUERY
Send a message to a data queue	*DQSRV	SEND
Receive a message from a data queue	*DQSRV	RECEIVE
Receive a message from a data queue without deleting it	*DQSRV	PEEK
Clear all messages from a data queue	*DQSRV	CLEAR

The Remote Command and Distributed Program Call Server

The Remote Command and Distributed Program Call Server (*RMTSRV) is used by clients to process Remote Command requests and PC program Distribute Program Call requests. Original clients use the Distributed Data Management Server to process Remote Command requests and do not support Distributed Program Call requests.

Client Action	Server Name	Server Function
Distributed program call	*RMTSRV	DSTPGMCALL
Remote Command	*RMTSRV	RMTCMD

The Remote SQL Server

The Remote SQL Server is used by a client to request processing of SQL statements received by PC programs using the Remote SQL API. This server is used by both the original and optimized clients when Remote SQL API requests are received. It is also used by the ODBC driver of some original clients. Other original clients and optimized clients have ODBC drivers that use the Database Server.

The following table lists the Remote SQL Server functions used by the different client actions.

Client Action	Server Name	Server Function
Connect to a database	*RQSRV	CONNECT
Execute a SELECT SQL statement	*RQSRV	SELECT SELECTPM SELECTVAL SELECTPKG
Execute a non-SELECT SQL statement	*RQSRV	EXECUTE EXECUTEPM EXECPKG
Delete the row at the cursor	*RQSRV	DELETE
Update the row at the cursor	*RQSRV	UPDATE
Call a stored procedure	*RQSRV	RMTCALL
Create an SQL package	*RQSRV	CREATEPKG PREPTOPKG

The Remote Command and Distributed Program Call Server

The Remote Command and Distributed Program Call Server (*RMTSRV) is used by clients to process Remote Command requests and PC program Distribute Program Call requests. Original clients use the Distributed Data Management Server to process Remote Command requests and do not support Distributed Program Call requests.

Client Action	Server Name	Server Function
Distributed program call	*RMTSRV	DSTPGMCALL
Remote Command	*RMTSRV	RMTCMD

The REXEC Logon Server

The REXEC Logon server is used to validate signon attempts to an IBM i system through the Remote Execution Server. The following table lists the REXEC Logon Server functions used by client actions.

Client Action	Server Name	Server Function
Sign on	*REXEC_SO	SIGNON

The Signon Server

The Signon Server is used by clients to retrieve signon information and to change passwords. The following table lists the Signon Server functions.

Client Action	Server Name	Server Function
Change password	*SIGNON	CHGPWD
Generate authentication token	*SIGNON	GENAUTTKN
Generate authentication token for other user	*SIGNON	GENAUTTKNU
Retrieve signon information	*SIGNON	RETRIEVE
Start server request	*SIGNON	STRSRVRQS

The SQL Retrieve Object Information Server

Retrieve information about libraries, databases, SQL packages, etc. It is also used for SQL catalog functions.

Client Action	Server Name	Server Function
Retrieve special column information	*RTVOBJINF	RTVCLMINF
Retrieve file information	*RTVOBJINF	RTVFILINF
Retrieve foreign key information	*RTVOBJINF	RTVFKEYINF
Retrieve field information	*RTVOBJINF	RTVFLDINF
Retrieve record format information	*RTVOBJINF	RTVFMTINF
Retrieve index information	*RTVOBJINF	RTVIDXINF
Retrieve library information	*RTVOBJINF	RTVLIBINF
Retrieve file member information	*RTVOBJINF	RTVMBRINF
Retrieve primary key information	*RTVOBJINF	RTVPKEYINF
Retrieve relational database info	*RTVOBJINF	RTVRDBINF
Retrieve SQL package information	*RTVOBJINF	RTVSQLPKG
Retrieve SQL statement information	*RTVOBJINF	RTVSQLSTMT

The TELNET Server

The TELNET Server is used by TELNET sessions to sign on to an IBM i server. The following table lists the TELNET Server functions used by client actions.

Client Action	Server Name	Server Function
Initialize session	*TELNET	INIT

The Transfer Function Server

The Transfer Function Server is used by Client Access to request uploading and downloading of database files from the IBM i system. It is also used by the original client when requests are made through the Client Access programming APIs. Client Access Programming API requests made to optimized clients do not use this server, but use the Database Server instead.

The following table lists the Transfer Function Server functions used by the different client actions. Note that uploading and downloading are separate functions. This makes it easy to prevent uploads, while still allowing downloads.

Client Action	Server Name	Server Function
Prompt for list of libraries or files	*TFRFCL	EXTRACT
Download a single file to the PC	*TFRFCL	SELECT
Download a join of 2 or more files to the PC	*TFRFCL	JOIN
Upload a file to the AS/400	*TFRFCL	REPLACE

The Trivial FTP Server

Trivial File Transfer Protocol (TFTP) is a simple protocol that provides basic file transfer function with no user authentication. Together, TFTP and Bootstrap Protocol, or BOOTP, provide support for the IBM Network Station for an IBM i system. They also provide support for other clients that use the TFTP and BOOTP protocols. The following table lists the TFTP Server functions used by client actions.

Client Action	Server Name	Server Function
Receive (get) file	*TFTP	RECVFILE
Send (put) file	*TFTP	SENDFILE

The Virtual Print Server

The Virtual Print Server is used by Client Access original clients to process Virtual Print requests for printing on an IBM i printer. Optimized clients use the Network Print server for requests to print on an IBM i printer. The following table lists the Virtual Print Server functions used by the different client actions.

Client Action	Server Name	Server Function
Get a list of IBM i printer files and output queues	*VPRT	EXTRACT

Client Action	Server Name	Server Function
Check existence and authority to a printer file or output queue	*VPRT	CHECK
Open a printer file	*VPRT	OPEN

Appendix C: Exit Point Manager Generic Exit Point

Exit Point Manager includes a Generic Exit Point for use with customer-written servers. The Generic Exit Point provides the ability to use Exit Point Manager's structure for your own applications.

The activation/deactivation process registers and de-registers exit point PTG_NS_GENERIC_ACSI format ACSOIOO with IBM's registration facility.

Required Parameter Group

All character parameters must be passed as EBCDIC. The invoking program should perform any code conversion.

The following table describes the API parameters:

Sequence	Parameter	How Used	Data Type	Required Parameter?
1	Allow operation	Output	Binary (4)	YES
2	Server name	Input	Char (10)	YES
3	Server Function name	Input	Char (10)	YES
4	OS/400 User Profile	Input	Char(10)	YES
5	Location Identifier	Input	Char(15)	YES
6	Format Name for Operation-specific information	Input	Char(10)	YES
7	Length of operation-specific information	Input	Binary (4)	YES
8	Operation-specific information	Input	Char (*)	YES
9	Profile handle	Input/Output	Char (12)	YES

Allow operation - OUTPUT; BINARY(4)

Indicates if this operation should be allowed or rejected. Valid values are:

0	Reject the operation
1	Accept the operation

Server name - INPUT; CHAR (10)

Identifies the user-written server for which the request is being made. Valid value is:

User-written server	The name of the user-written server for which the request is being made. Enter the server name in uppercase.

Server Function name - INPUT; CHAR (10)

Identifies the user-written server function for which the request is being made. Valid value is:

User-written server function	The name of the user-written server for which the request is being made. Enter the server function in uppercase.

OS/400 User Profile - INPUT; CHAR (10)

Identifies the user profile for which the request is being made. Valid values are:

OS/400 User Profile ID	A valid name assigned to an OS/400 user profile. Enter the user profile in uppercase.

Location Identifier - INPUT; CHAR (15)

Identifies the IP address or SNA device for which the request is being made. Valid values are:

IP address	A valid IP address.
SNA device name	A valid SNA device name. Enter the device name in uppercase.
***NONE**	No location identifier is provided. The job's name is used for the location identifier.
Blank	No location identifier is provided. The job's name is used for the location identifier.

Format name for operation-specific information - INPUT; CHAR(10)

Indicates the format name for provided operation-specific information. Valid values are:

Format name	The format name to be used to format the provided operation-specific information.
***NONE**	No format name is being provided.
Blank	No format name is being provided.

Length of operation-specific information - INPUT; BINARY(4)

Indicates the length (in bytes) of the operation-specific information, or 0 if no operation-specific information is provided. Valid values are 0 through 32767. A value of 0 forces memorized transaction rule verification to be ignored, regardless of rule actions.

Operation-specific information - INPUT; CHAR (*)

Information to be used when writing audit journal entries, capturing transactions, and verifying memorized transaction rules. Must not exceed 32767 bytes in length.

Profile Handle - INPUT/OUTPUT; CHAR (12)

On the first call to the generic exit point program the Profile Handle is blank. If a switch occurs within Exit Point Manager, the original user's profile handle is returned. If a profile handle is returned, the application running needs to call the generic exit point program with the profile handle to release the profile swap (a call to the Generic Exit Program is by reference).

Usage Notes

If the server name you provide is a server that is supported by Powertech, the operation is rejected. Powertech supports the following servers.

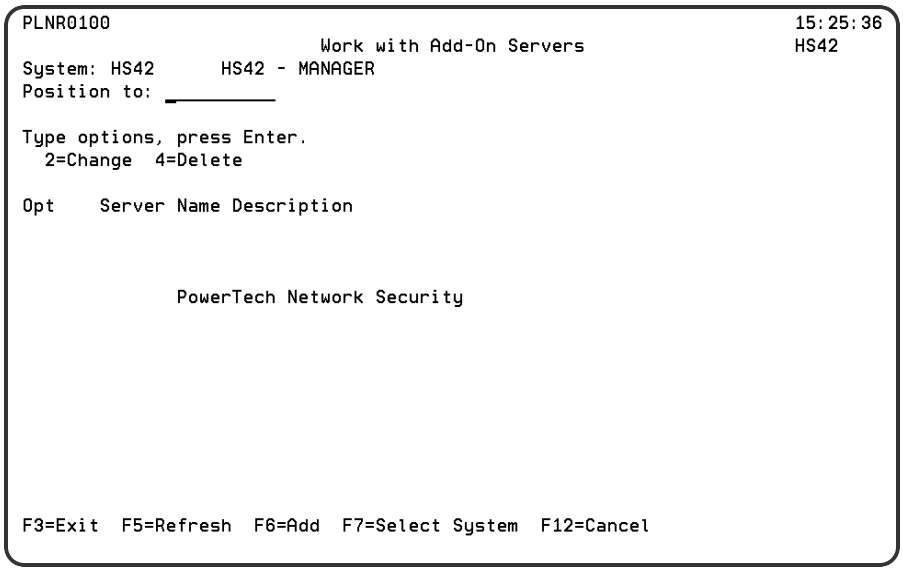
NOTE: You can use the LWRKGENSRV command to maintain any servers that are not listed.

Server	Description
*CLI	CLI Connection Server
*CNTRLSRV	License Management Central Server
*DATAQSRV	Optimized Data Queue Server
*DDM	DDM Server
*DQSRV	Data Queue Server
*DRDA	Distributed Relational Database
*FILESRV	File Server
*FTPCLIENT	FTP Client
*FTPREXEC	FTP Execute Remote Command (REXEC)
*FTPSERVER	FTP Server
*FTPSIGNON	FTP Signon Server
*LMSRV	License Management Server
*MSGFCL	Message Function
*NDB	Native Database Request
*REXEC_SO	Rmt Execute Command Signon Server
*RMTSRV	Remote Command Server

Server	Description
*RQSRV	Remote SQL Server
*RTVOBJINF	SQL Retrieve Object Information
*SIGNON	Signon Server
*SQL	Database Server Initialization
*SQLSRV	SQL Server
*TELNET	Telnet Device Init/Term
*TFRFCL	File Transfer Server
*TFTP	Trivial FTP
*VPRT	Virtual Print Server
QNPSERVR	Network Print Server

Work with Add·On Servers (LWRKGENSRV)

Work with Add-on Servers is used to maintain customer and business partner servers and their function using Exit Point Manager's Generic Exit program. Exit Point Manager supported servers and their functions cannot be maintained with this process. Type an option next to a specific server and press **Enter**. You can type option numbers next to more than one Server at a time. This allows you to perform more than one task at a time. If you see 'More...' in the lower right corner of your display, there is more information to be listed. Press the Page Down (Roll Up) key to move toward the end of the Servers listed. Press the Page Up (Roll Down) key to move toward the beginning of the Servers listed.



Options

2=Change
Change an Add-on Server and its functions.

4=Delete
Delete an Add-on Server and its functions.

Option
This column is used to perform different operations on individual Add-on Servers and their functions. Type your option selection next to a Server Name and press `Enter`. You can type the same option next to multiple Add-on Servers. You may also type different options next to different Add-on Servers.

Available options are:

2=Change

Change an Add-on Server and its functions.

4=Delete

Delete an Add-on Server and its functions.

Server Name

The name of an Add-on Server.

Server Description

The description of the Add-on Server.

Command Keys
F3 (Exit): Exit the program without processing any pending changes.

F5 (Refresh): Refresh the screen.

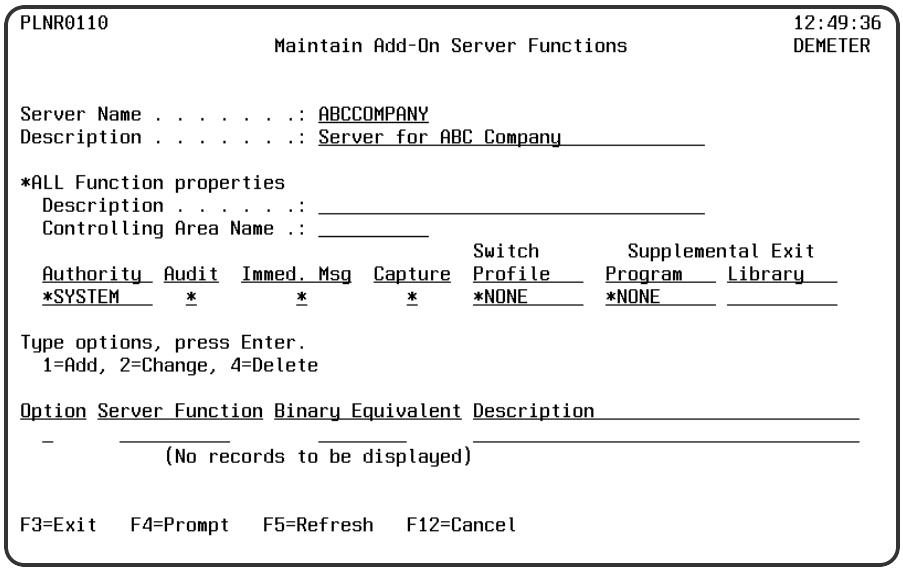
F6 (Add): Add a new server and its functions.

F7 (Select System): Use this command key to work with data from a different System.

F12 (Cancel): Exit the screen without processing any pending changes.

Adding a New Add-On Server

Enter the following information to define the add-on server:



Enter the following information to define the add-on server:

Server Name

Enter a name for the add-on server.

Server Description

Enter a brief description of the server.

*All Function Properties

These values allow you to specify the final defaults for a server's functions.

Description

Enter a description for the *ALL function. This is a required field.

Controlling Area Name

Enter the name of the control structure used by the Exit Point Manager Generic Exit Program.

Authority

The authority assigned to the server function. The value you enter is used when *SRVFCN authority is placed on a location, user, or memorized transaction request.

Audit

Controls the type of requests Exit Point Manager will log.

Immediate Message

Allows you to specify if Exit Point Manager sends a message to the message queue specified in its System Values.

Capture

Captures transactions for Memorized Transaction Request (MTR).

Switch Profile
The name of a switch profile for the server. If you enter a profile name, processing is swapped to run under this profile's authority. This is valid only for authorities *SWITCH and *MEMSWITCH.

Supplemental Exit Program
The exit program to run after Exit Point Manager's Generic Exit Program has successfully processed a request. The supplemental exit program is invoked only for authorities *OS400, *MEMOS400, *SWITCH, and *MEMSWITCH. Exit Point Manager's rules must be enforced for a supplemental exit program to execute.

Supplemental Exit Program Library
The library where the supplemental exit program resides. Special values such as *LIBL are not allowed.

Specific Functions for the Server
These values allow you to specify processing options for different operations on individual server functions.

Option
Enter one of the following options next to a specific function.

> **NOTE:** You can enter an option number next to more than one server at a time.

1	Allows you to add a new add-on server function.
2	Allows you to change an add-on server function's properties.
4	Deletes the add-on server function.

Server Function
The name of the function for an add-on server.

Binary Equivalent
The binary equivalent of the function for an add-on server. A binary equivalent is an eight digit numeric value representing the server function. A binary equivalent cannot be used more than once per server. Possible values are I through 99998887, 99998889 through 99999997, and 99999999.

Description
The description of the server function options.

Changing an Add·On Server
To change the settings for an add-on server, enter option **2** next to the server to display the Change Add-On Server panel. Enter your changes and press `Enter`. The changes take effect immediately.

Deleting an Add·On Server

> **NOTE:** You must delete all server functions before deleting the add-on server.

To delete an add-on server, enter option **4** next to the server you want to delete and press `Enter`. The server is deleted immediately.

Work with Add On Servers panel

Example of a Generic Exit Point Program

The following is an example of an RPG ILE application program that incorporates a Exit Point Manager Generic Exit Point program.

```
H Copyright ('Copyright (c)2015 The Powertech Group. +
H All Rights Reserved.')
```

This example is provided 'as is' with no warranties either expressed or implied.

```
H* * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * */
H*                                                                       */
H*            Copyright (c)2015 The Powertech Group.                     */
H*                      All Rights Reserved.                             */
H*           THE POWERTECH GROUP CONFIDENTIAL INFORMATION.               */
H*          (For the full text execute command LCOPYRIGHT).              */ H*
 */
H* * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * * */
H*
H* Program    : Use_Gexit
H* Description: Example of calling of the default exit program.
H*
H* Purpose    : This module is an example of the use of the default
H*              exit program.  It is an update engine for the file
H*              TestFile.  It checks to see if the user is allowed to
H*              update or add records to the file and checks the
H*              key to be update/added against memorized transactions.
H*
H*-------------------------------------------------------------------------
H*
H* Compile Instructions: H*
H* This module is first compiled as a  module.  It is then bound with
H* the following modules to create program Use_Gexit. H*
H* Module Name Description
H* ----------- ----------------------
H* Use_Gexit   Driving module
H*
H* Command CRTPGM is used to create executable program Use_Gexit.
H*
H* Parameter  Setting
H* ---------  ------------------------------------------------------------
H* MODULE     Use_Gexit
H* ENTMOD     Use_Gexit
H* ACTGRP     *CALLER H*
H*-------------------------------------------------------------------------
h
FTestFile  uf a e           k disk
D*-------------------------------------------------------------------------
D*
D*
D*  Procedure Definition
```

```
D*
D Use_gexit       PR                  EXTPGM('USE_GEXlT')
D  lnboundKey                   12
D  lnboundUpdate             32060
D*
D*  Procedure lnterface
D*
D Use_gexit       Pl
D  lnboundKey                   12
D  lnboundUpdate             32060
D*
D* Generic Exit Point Prototype
D*
D PLKR107GEP      PR                  ExtPgm('PLKR107GEP')
D  ReturnAllow                   9b 0
D  ServerNameln                 10
D  SrvFunctionln                10
D  UsrProfileln                10
D  Locationln                   15
D  FormatNameln                 10
D  LengthDataln                  9b 0
D  OperDataln                32767
D  ProfileHandle                12
D*
D ReturnAllow     S               9b 0
D ServerNameln    S              10
D SrvFunctionln   S              10
D UsrProfileln  s             10
D Locationln      S              15
D FormatNameln    S              10
D LengthDataln    S               9b 0
D OperDataln      S           32767
D ProfileHandle s               12
d* copy the program status data structure_d/copy @pgsds
D*-------------------------------------------------------------------
c*
c     lnboundKey    chain     testfile
c                   if        %found
c                   eval      SrvFunctionln = 'UPDATE'
c                   else
c                   eval      SrvFunctionln = 'ADD   '
c                   endif
C
c                   eval      ServerNameln = 'TESTFlLEUP'
c                   eval      UsrProfileln_= @pgusr
c                   eval      OperDataln    = %trim(lnboundKey)
c                   eval      LengthDataln  = %len(%trim(lnboundKey))
c
c                   call (E)  'PLKR107GEP'
c                   Parm                    ReturnAllow
c                   Parm                    ServerNameln
c                   Parm                    SrvFunctionln
c                   Parm                    UsrProfileln
c                   Parm                    Locationln
```

```
c                   Parm                    FormatNameln
c                   Parm                    LengthDataln
c                   Parm                    OperDataln
c                   Parm                    ProfileHandle
c*
c                   if                      ReturnAllow = 1
c                   if                      SrvFunctionln  = 'ADD    '
c                   eval                    tfkey = lnboundKey
c                   eval                    tfdata = lnboundUpdate
c                   write                   tstf
c                   else
c                   eval                    tfdata = lnboundUpdate
c                   update                  tstf
c                   endif
c                   endif
c                   return
```

Appendix D: Backing Up Exit Point Manager

When you perform a SAVLIB on a Powertech Exit Point Manager library, everything is saved except the following files:

- PLKCAP
- PLKCAPCNT

These files both are used for captured transactions and are not saved because they are open for update if summarization is active.

If you do want to perform a full backup, use the Save While Active parameter on the SAVLIB command to back up the entire library.

For example, you can enter the following command to save the entire library, plus the two captured transaction files:

If your product library is PTNSLIB07:

SAVLIB LIB(PTNSLIB07) DEV(TAP01) SAVACT(*LIB) SAVACTWAIT(30) + SAVACTMSGQ (QSYSOPR)

If your product library is PTNSLIB:

SAVLIB LIB(PTNSLIB) DEV(TAP01) SAVACT(*LIB) SAVACTWAIT(30) + SAVACTMSGQ(QSYSOPR)

Appendix E: Telnet Validation

Exit Point Manager allows you to exclude attempts to initiate Telnet sessions, based on validated password level.

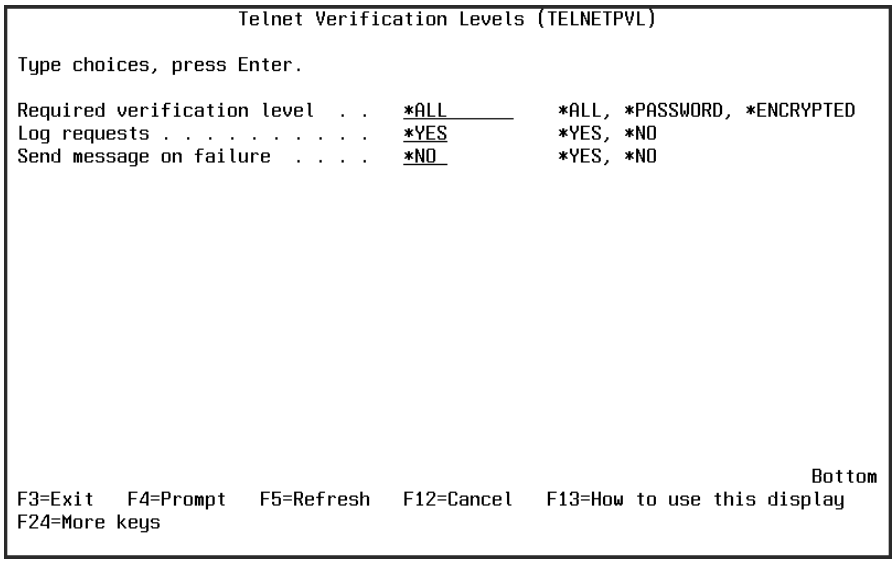
IBM provides three levels of password validation:

- No validation
- Clear text password validation
- Encrypted password validation

The TELNETPVL command lets you customize Exit Point Manager, which, if enabled, requires password verification on TELNET. To use the validation feature, users must use the 5250E protocol that allows the user ID to pass as part of the sign-on request.

To set up validation, enter the following command on a command line to display the Telnet Verification Levels panel:

TELNETPVL



Telnet Verification Levels Fields

You can enter the following on the Telnet Verification Levels panel:

Required verification level

Specify the verification level necessary to accept a Telnet request. Possible values are:

*ALL	Accept Telnet initialization requests when a client's password was not validated, or no password was received. If set to *ALL, any password verification level is allowed.
*PASSWORD	Accept Telnet initialization requests when a client's clear text password was validated, or an encrypted password was validated. Any Telnet requests where a client's password was not validated, or no password was received, are rejected by Exit Point Manager. If set to *PASSWORD, the settings passed by the Telnet exit point are checked to see if the password has been validated. If it hasn't, the connection is rejected.

*ENCRYPTED	Accept Telnet initialization requests when a client's encrypted password was validated. Any Telnet requests received where the password is not validated as encrypted are rejected by Exit Point Manager. If set to *ENCRYPTED, the settings passed by the Telnet exit point are checked to see if the encrypted password has been verified. If not, the connection is rejected. When you specify *ENCRYPTED, the connection must be a secured socket connection.

Log requests

Specifies if Exit Point Manager should log rejected password verification attempts. A password verification is rejected when either of the following occurs:

- Verification level *PASSWORD is specified, but the password was not verified.
- Verification level *ENCRYPTED is specified, but password was verified as a clear text password, or password verification did not occur.

Possible values are:

*YES	Log rejected password verification attempts.
*NO	Do not log rejected password verification attempts.

Send message on failure

Specifies if Exit Point Manager is to send a message to the message queue defined in the system values when a password verification failure has occurred. Possible values are:

*NO	Do not send a message when a failed password verification occurs.
*YES	Send a message when a failed password verification occurs.

Appendix F: Servers and Applications

The following tables list servers and their applications according to client function and server used. Because this information is subject to change by IBM, you should check the IBM Web site for current information.

Client Function	Server Used
.NET Data Provider	Database Server Signon server Central server QXDAEDRSQL server

Client Function	Server Used
IBM Toolbox for Java	Signon server Central server File server Database Server DRDA(R) and DDM server Data queue server Remote command and distributed program call server Network print server
Data Transfer	Signon server Central server Database server
ODBC driver	Signon server Database server
Access integrated file system from iSeries Navigator	File server
Data queue APIs OLE DB provider	Data queue server Data queue server Database server Remote command and distributed program call server Signon server
Extended Dynamic Remote SQL server (QXDAEDRSQL)	Signon server Central server QXDAEDRSQL server (no exit point provided)
License management Done when an application that requires a license is started (Data Transfer and 5250 emulation)	Central server
Retrieve conversion map Done only on initial connection if the client does not contain the required conversion maps	Central server
Remote command functions	Remote command and distributed program call server

Client Function	Server Used
Distributed program call	Remote command and distributed program call server
Send password for validation and change expired password (TCP/IP)	Signon server
Network Print	Network print server

GUI and Programming Interfaces

File Server Objects:

Program Name	Library	Object Type	Description
QPWFSERVSO	QSYS	*PGM	Server program
QPWFSERVS2	QSYS	*PGM	Server program
QPWFSERVSD	QSYS	*PGM	Daemon program
QPWFSERV	QSYS	*JOBD	Job description used for server jobs
QPWFSERVER	QSYS	*CLS	Class used for all file server and database server jobs
QPWFSERVSS	QSYS	*PGM	SSL server program

Database Server Programs:

Program Name	Library	Description
QZDASOINIT	QSYS	Server program
QZDASON2	QSYS	Sockets setup program
QZDASRVSD	QSYS	Daemon program
QZDASSINIT	QSYS	SSL server program
Note: The QZDANDB and QZDACRTP *PGM objects along with the *SRVPGM object QZDASRV are used by the database server.		

Data queue server program provided for use with sockets support:

Program Name	Library	Description
QZHQSSRV	QSYS	Server program
QZHQSRVD	QSYS	Daemon program

Network Print Server:

Program Name	Library	Description
QNPSERVS	QSYS	Server program
QNPSERVD	QSYS	Daemon program

Central Server Programs:

Program Name	Library	Description
QZSCSRVS	QSYS	Server program
QZSCSRVSD	QSYS	Daemon program

Remote command and distributed program call server programs:

Program Name	Library	Description
QZRCSRVS	QSYS	Server program
QZRCSRVSD	QSYS	Daemon program

Signon Server Programs:

Program Name	Library	Description
QZSOSIGN	QSYS	Server program
QZSOSGND	QSYS	Daemon program

Server Port Mapper:

Program Name	Library	Description
QZSOSMAPD	QSYS	Server port mapper program

QXDAEDRSQL Server Programs:

Program Name	Library	Description
QXDARECVR	QSYS	Server program
QXDALISTEN	QSYS	Daemon program
Note: The QXDAEVT and QXDAIASP *SRVPGM objects are used by the QXDAEDRSQL server.		

DRDA/DDM Server Programs:

Program Name	Library	Description
QRWTSRVR	QSYS	Server program

Program Name	Library	Description
QRWTLSTN	QSYS	Listener program

Appendix G: Exit Point Manager and IPv6

Internet Protocol Version 6 (IPv6) is the next-generation protocol designed to replace IPv4. The primary difference between IPv6 and IPv4 is that IPv6 supports a greater number of IP addresses and is designed to meet the demand from Internet-capable devices in the future. Unlike IPv4, which uses 32-bit addressing, IPv6 addresses are 128-bits to handle the increased demand for IP addresses.

Exit Point Manager 6.0 is IPv6-tolerant. That means that Exit Point Manager can "tolerate" IPv6 addresses in every exit point managed by Exit Point Manager 6.0.

Exit Point Manager and IPv6 tolerance

A system can have both IPv6 and IPv4 address types active. However, when Exit Point Manager detects an IPv6 client address, the IPv6 address will be "tolerated" by converting it to an IPv4 address. Whenever possible, the IPv4 address will be the address associated with the client.

If no IPv4 address can be determined, but a valid IPv6 address is supplied, Exit Point Manager uses a default address (for example, 192.168.255.0). The default IP address is generated so you can make a decision on how to set rules.

If no valid address can be determined, Exit Point Manager uses second default address (for example, 1.0.0.0).

> **NOTE:** IPv6 "tolerance" differs from actual support of IPv6. Actual support of IPv6 will be included in a later release of Exit Point Manager, as determined by need.

Appendix H: Securing the *SQL vs. *SQLSRV Server

When securing these servers, note the *SQLSRV functions are only available if the *SQL server is available. (The *SQL server is like the front door to a house, and the *SQLSRV functions are like the various drawers and closets within that house.) You can block all *SQLSRV functions by blocking the *SQL server. When the *SQL server is available, rules can be used to control access to all the *SQL server functions individually.

Appendix I: Order of Evaluation

Exit Point Manager follows a hierarchy when performing rule checking to validate the user's request. The following tables list the basic hierarchy for location, user, and object rule evaluation. For a complete description of the rule hierarchy, including Pre-filters, see Appendix K: Rules Hierarchy.

Exit Point Manager always evaluates rules in sequence from the most specific to the least specific.

Location Rules-Order of Evaluation

If a more specific rule exists, it is evaluated first. Once a rule is selected, further checking stops. The following table shows the order of evaluation for location rules.

Evaluation Sequence	Function Name	Location
1	Function being requested	Location request came from
2	*ALL	Location request came from
3	*ALL	*ALL
4	*	Check next higher level

NOTE: For new installations only, all Location rules default to the rule *USER. For existing users, if there is no location rule, Exit Point Manager looks at the Server level for the appropriate action to take.

User Rules-Order of Evaluation

The following table shows the order of evaluation for user rules.

Search Sequence	Function Name	User
1	Function being requested	User making request
2	*ALL	User making request
3	Function being requested	Primary group profile of user making request
4	*ALL	Primary group profile of user making request
5	Function being requested	Supplemental group profiles of user making request

Search Sequence	Function Name	User
6	*ALL	Supplemental group profiles of user making request
7	Function being requested	*PUBLIC
8	*ALL	*PUBLIC

Object Rules-Order of Evaluation

When evaluating object rules, the order also depends on whether the initiating *MEMOBJ rule was a user rule or a location rule. For object rules, most specific is an exact match; after that, the length of the string, up to any wildcard characters, determines the order of evaluation. The following table shows the order of evaluation for object rules.

Search Sequence	Object Rule
***MEMOBJ User Rule**	
1	Memorized transaction
2	Object rule for the user profile
3	Object rule for each supplemental group profile (if any), starting with the group profile
4	Object rule for user profile value *PUBLIC
5	Object rule for the location
6	Object rule for the location group of the location (if any)
7	Object rule for the location value *ALL
***MEMOBJ Location Rule**	
1	Memorized transaction
2	Object rule for the location
3	Object rule for the location group of the location (if any)
4	Object rule for the location value *ALL
5	Object rule for the user profile

Search Sequence	Object Rule
6	Object rule for each supplemental group profile (if any), starting with the group profile
7	Object rule for the user profile value *PUBLIC

Appendix J: Parameters and Default Values

Location Rules

All default location rules include the same parameters and are set with the same default values.

Parameter	Default Value
Location	*ALL
Function	*ALL
Authority	*OS400
Aud	*
Msg	*
Cap	*
Switch Profile	*SRVFCN

User Rules

All default location rules include the same parameters and are set with the same default values.

Parameter	Default Value
User	*PUBLIC
Function	*ALL
Authority	*OS400
Aud	*
Msg	*
Cap	*
Switch Profile	*NONE

Appendix K: Rules Hierarchy

The order/hierarchy of the Exit Point Manager Version 6 rules are:

1. **Pre-filters**
2. **Location Rules**
3. **User Rules**

Below is an explanation of each category of rules with the order/sequence of the specific rules in each group.

1) Pre-filters

In version R06M10, Exit Point Manager implemented an enhancement for Pre-filters.

Pre-filters allow you to establish a one-to-one relationship between a specific IP address (location) and a user. The order of the Pre-filters are based on server, function, location and user.

> **NOTE:** Pre-filters only have two valid actions, either (1) allow or (2) reject the transaction. If the Pre-filter allows the transaction, it continues onto the Location rules. If the Pre-filter rejects the transaction, no more checks are done for the transaction.

1-1) Exact Server, Exact Function, Exact Location, and User

The user is searched in the following order:

1-1-1) Specific individual user

1-1-2) Group profile

1-1-3) Supplemental group

1-1-4) All users or *PUBLIC

1-2) Exact Server, Exact Function, Location Group, and User

The user is searched in the following order:

1-2-1) Specific individual user

1-2-2) Group profile

1-2-3) Supplemental group

1-2-4) All users or *PUBLIC

1-3) Exact Server, Exact Function, Location (*ALL), and User

The user is searched in the following order:

1-3-1) Specific individual user

1-3-2) Group profile

1-3-3) Supplemental group

1-3-4) All users or *PUBLIC

1-4) Exact Server, Function (*ALL), Exact Location, and User

The user is searched in the following order:

1-4-1) Specific individual user

1-4-2) Group profile

1-4-3) Supplemental group

1-4-4) All users or *PUBLIC

1-5) Exact Server, Function (*ALL), Location Group, and User

The user is searched in the following order:

1-5-1) Specific individual user

1-5-2) Group profile

1-5-3) Supplemental group

1-5-4) All users or *PUBLIC

1-6) Exact Server, Function (*ALL), Location (*ALL), and User

The user is searched in the following order:

1-6-1) Specific individual user

1-6-2) Group profile

1-6-3) Supplemental group

1-6-4) All users or *PUBLIC

1-7) Server (*ALL), Function (*ALL), Location (*ALL), and User

The user is searched in the following order:

1-7-1) Specific individual user

1-7-2) Group profile

1-7-3) Supplemental group

1-7-4) All users or *PUBLIC

2) Location Rules

Location rules, like the Pre-filters, are sequenced from the most specific to the least specific.

Once a rule is selected, further checking stops unless the rule is a *MEMOBJ rule and neither a memorized transaction or an object rules exists for this transaction. The *MEMOBJ rule is ignored and processing will continue down the sequential order to the next rule.

2-1) Specific location (name or IP address) and specific function

2-2) Specific location (name or IP address) and all functions (*ALL)

2-3) Generic location (name or IP address) and specific function

2-4) Generic location (name or IP address) and all functions (*ALL)

2-5) All locations (*ALL) and all functions (*ALL)

The evaluation for location rules are based on location, function, and authority.

If the Authority column is *USER, Exit Point Manager proceeds to check the User Rules.

If the authority for the location rule has *MEMxxx, Exit Point Manager checks for a memorized transaction or an Object Rule. If no match is found, it will continue down the sequence and perform the action from the Authority column of the next location rule.

***MEMOS400** – Checks for a matched memorized transaction; if none are found, the transaction is allowed.

***MEMREJECT** – Checks for a matched memorized transaction; if none are found, the transaction is rejected.

***MEMSWITCH** – Checks for a matched memorized transaction; if none are found, the authority of the switch profile defined on the rule is used.

***MEMUSR** – Checks for a matched memorized transaction; if none found, the user rule for this transaction is searched.

***MEMOBJ** – Checks for a matched memorized transaction; if none found, the Object Rule for this transaction is searched.

2-6) *MEMOBJ Location Rule

Object Rules (*MEMOBJ) are associated either as a location or a user rule.

Object rules, like the other rules, are sequenced from the most specific to the least specific depending on whether the transaction was a memorized user or location rule. The most specific is an exact match, followed by the length of the string and/or the wildcard characters. The order depends on whether the initiating *MEMOBJ rule was a user rule or a location rule.

2-6-1) Can be a memorized transaction for the location

2-6-2) Object rule for the specific location

2-6-3) Object rule for the location group of the location

2-6-4) Object rule for all locations (*ALL)

2-6-5) Object rule for the specific user profile

2-6-6) Object rule for the group profile

2-6-7) Object rule for each supplemental group profile

2-6-8) Object rule for all users (*PUBLIC)

3) User Rules

User Rules, like the other rules, are sequenced from the most specific to the least specific.

Once a rule is selected, further checking stops unless the rule is a *MEMOBJ rule and neither a memorized transaction or an object rules exists for this transaction. The *MEMOBJ rule is ignored and processing will continue down the sequential order to the next rule.

3-1) Specific User and specific function

3-2) Specific User and all functions

3-3) Group Profile and specific function

3-4) Group Profile and all functions

3-5) Supplemental Group and specific function

3-6) Supplemental Group and all functions

3-7) All users (*PUBLIC) and specific function

3-8) All users (*PUBLIC) and all functions

The evaluation for user rules are based on location, function, and authority.

If the authority for the user rule has *MEMxxx, Exit Point Manager will check for a memorized transaction or an Object Rule. If no match is found, it will proceed down the sequence and perform the action from the Authority column of the next user rule.

***MEMOS400** – Checks for a matched memorized transaction; if none are found, the transaction is allowed.

***MEMREJECT** – Checks for a matched memorized transaction; if none are found, the transaction is rejected.

***MEMSWITCH** – Checks for a matched memorized transaction; if none are found, the authority of the switch profile defined on the rule is used.

***MEMOBJ** – Checks for a matched memorized transaction; if none found, the Object Rule for this transaction is searched.

3 -9) *MEMOBJ User Rule

Object Rules (*MEMOBJ) are associated either as a location or a user rule.

Object rules, like the other rules, are sequenced from the most specific to the least specific depending whether the transaction was a memorized user or location rule. The most specific is an exact match, followed by the length of the string and/or the wildcard characters. The order depends on whether the initiating *MEMOBJ rule was a user rule or a location rule.

3-9-1) Can be a memorized transaction for the user

3-9-2) Object rule for the specific user profile

3-9-3) Object rule for the group profile

3-9-4) Object rule for each supplemental group profile

3-9-5) Object rule for all user profiles (*PUBLIC)

3-9-6) Object rule for the specific location

3-9-7) Object rule for the location group for the location

3-9-8) Object rule for all locations

Removing Default Rules

This section describes the effects on, and functionality of, audit rules when removing default server rules for each of the rules tables. The path or hierarchical order of rule checking is presented at each rule table test. (No testing results are available for the individual profile and group profile ordering.)

The normal hierarchy of transaction rule processing takes the following path until an applicable rule is applied:

Pre-filter => Location (sub Mem&OBJTrans) **=> User** (sub Mem&OBJTrans) **=> Global rule**

The *Global Rule*, comprised of the settings in the Work with System Values panel, is the final collection of settings for a transaction if no prior rule can be applied to the request. Only in one situation does the path diverge from the above path. (See Location rules below.)

Global Rule

The global rule facility contains the final setting for any transaction if no other rules are applied to a transaction request. It's not possible to remove the global rule. The authority must contain a valid setting (*OS400, *REJECT, or *SWITCH) and cannot be altered or saved without selecting one. The shipped default value is *OS400.

User Rules

Removing User rules, such as the default *ALL or *PUBLIC, and named user rules, defers the decision to the Global Rule. If a transaction request cannot find any rule that would apply to an incoming transaction, the Global Rule for the authority setting and audit flags will be applied. If location rules are completely removed, and no *USER rule is found, the user rules will be skipped completely. Without User rules, settings are inherited from the expected path:

Pre-filter=>Location=>Global Rule

Location Rules

Removing Location rules (Default and IP address) defers the audit trail to the Global Rule. If a transaction cannot find any rule that would apply to a transaction, the audit flags in the Global Rule will be applied. An interesting item noted here is the transaction event trail, if all location rules are removed, the trail is not steered to the User table. The test sequence does not pass from **Location => User** but skips directly to the Global rule. With Location Rules removed the expected path is:

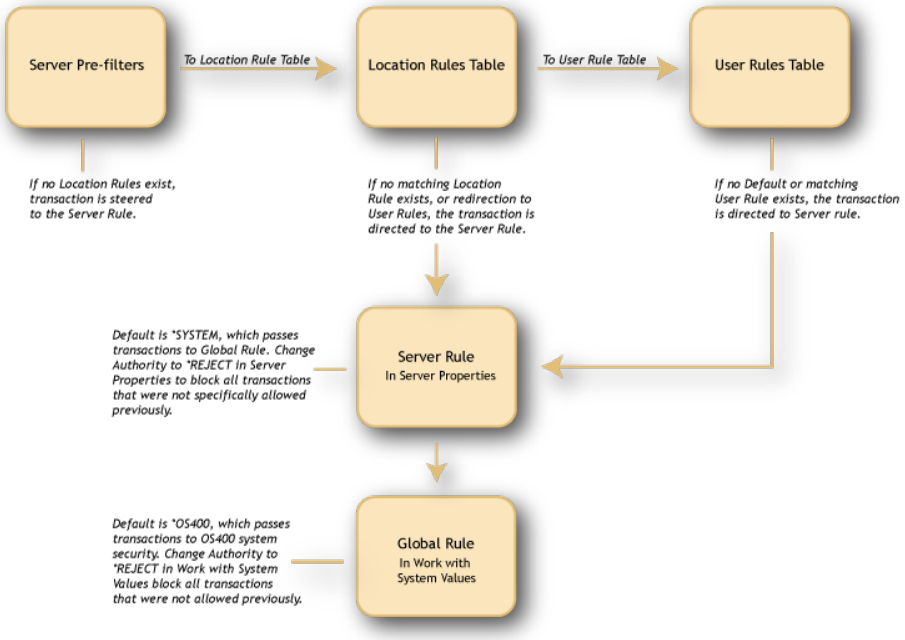
Pre-filter => Global Rule

Pre-filter Rules

It is not possible to remove the Server Pre-filters rules. You may remove the Location+User Pre-filters. Transaction requests are checked normally against location rules in the normal path.

Memorized and Object Rules

MEM[trans] Location and User Rules (e.g. MemOS400 or MEMOBJ) will test the memorized transaction and Object Rule table respectively. If no rule match exists that can be applied, the transaction is directed to the rest of the applicable rules inside that Table (Location or User). If a match is not found, the transaction test will follow the path **Location=>User=>Global Rules** until a rule is found, or until it reaches the Global rule settings.



Appendix L: Other Help

For help with the other components of HelpSystems Insite, see these user guides:

HelpSystems Insite User Guide

Access Authenticator Reference Manual

Automate Ops Console User Guide

Password Self Help for Insite User Guide

Deployment Manager for Insite User Guide

Robot Network for Insite User Guide

Robot Schedule for Insite User Guide

Webdocs for Insite User Guide

Appendix M: Interface Changes in Version 7.08

Several changes were made to the green screen interface as part of the Exit Point Manager 7.08 update.

Work with Security by Server

- The **F23** key has been removed.
- **CT=Captured Transactions** has been removed in favor of **F8=Captured Transactions**.
- **MT=Memorized Transactions** has been removed in favor of **F9=Memorized Transactions**.

- **F17=Top** and **F18=Bottom** have been removed.
- **UA=Edit User Authority** now opens Work with Security by User instead of Work with Server User Authorities (functionality the same)
- **LA=Edit Location Authority** now opens Work with Security by Location instead of Work with Server Location Authorities (functionality the same)
- **SP=Server Properties** now opens Change Server Function Rule instead of the Server Properties Window (functionality the same).

Work with Server Functions - Renamed "Work with Security by Server/Function"

See Work with Security by Server/Function.

- The **F23** key has been removed.
- **CT=Captured Transactions** has been removed in favor of **F8=Captured Transactions**.
- **MT=Memorized Transactions** has been removed in favor of **F9=Memorized Transactions**.
- **F17=Top** and **F18=Bottom** have been removed.
- **UA=Edit User Authority** now opens Work with Security by User instead of Work with Server User Authorities (functionality the same)
- **LA=Edit Location Authority** now opens Work with Security by Location instead of Work with Server Location Authorities (functionality the same)
- **SP=Server Properties** now opens Change Server Function Rule instead of the Server Properties Window (functionality the same).

Work with Server User Authorities - Renamed "Work with Security by User"

See Work with Security by User.

- Options **2=Change, 3=Copy, 4=Delete, and 5=Display** added.
- **F6=Create** added. Opens Create User Rule panel. (Replaces adding to blank line method.)
- **Typ** field has been added. U=User, G=User Group.
- **F21=User Groups** added. Opens Work with User Groups panel.
- **F16=Sort/Subset** added.
- **Subset by User** changed to **Position to User**.
- **F2=Global Rule Facility** panel changed to Add/Change User Rule panel.
- **F19=Properties detail** removed in favor of **5=Display**. See User Rule Derivation panel.

Work with Server Location Authorities - Renamed "Work with Security by Location"

See Work with Security by Location.

- Options **2=Change, 3=Copy, 4=Delete, and 5=Display** added.
- **F6=Create** added. Opens Create User Rule panel. (Replaces adding to blank line method.)
- **F16=Sort/Subset** added.
- **Subset by Location** changed to **Position to Location**.
- **F2=Global Rule Facility** panel changed to Add/Change Location Rule panel.
- **F19=Properties detail** removed in favor of **5=Display**. See Location Rule Derivation panel.

Server Properties Window - Renamed "Change Server Function Rule"

See Change Server Function Rule.

Loc+User Pre-filters - Renamed "Work with Loc+User Pre-filters"

See Work with Loc+User Pre-filters.

- **Typ** field has been added. U=User, G=User Group.
- **F21=User Groups** opens Work with User Groups panel.

Work with Captured Transactions

See Work with Captured Transactions.

- **F19** and **F20** command keys only allowed on View 3 (two F11's) (same as the Work with Memorized Transactions panel).
- **5** (display) shows starting position of displayed transaction and length of transaction.

Work with Memorized Transactions

See Work with Memorized Transactions.

- Labels for **F17 (Top)** and **F18 (Bottom)** have been added.
- U/G **Typ** flag for User Groups has been added.
- **F21=User Groups** opens Work with User Groups panel.
- **5** (display) shows starting position of displayed transaction and length of transaction.

Reports

See Reports Menu.

- Panels that allow selection of user now have a **User Type** flag (U or G) to specify User or User Group.
- Option **15**, 'Print User Groups" has been added.

If you are not redirected automatically, follow this link to the Insite Other Help topic.