iSecurity Command

User Guide
Version 17.31

www.razlee.com

Contents

About this Manual

This user guide is intended for system administrators and security administrators responsible for the implementation and management of security on IBM i systems. However, any user with basic knowledge of IBM i operations will be able to make full use of this product after reading this book.

Raz-Lee takes customer satisfaction seriously. Our products are designed for ease of use by personnel at all skill levels, especially those with minimal IBM i experience. The documentation package includes a variety of materials to get you familiar with this software quickly and effectively.

This user guide, together with the iSecurity Installation Guide, is the only printed documentation necessary for understanding this product. It is available in HTML form as well as in user-friendly PDF format, which may be displayed or printed using Adobe Acrobat Reader version 6.0 or higher. If you do not have Acrobat Reader, you can download it from the Adobe website: http://www.adobe.com/. You can also read and print pages from the manual using any modern web browser.

This manual contains concise explanations of the various product features as well as step-by-step instructions for using and configuring the product.

Raz-Lee's iSecurity is an integrated, state-of-the-art security solution for all System i servers, providing cutting-edge tools for managing all aspects of network access, data, and audit security. Its individual components work together transparently, providing comprehensive "out-of-the- box" security. To learn more about the iSecurity Suite, visit our website at http://www.razlee.com/.

Intended Audience

The Command User Guide document was developed for users, system administrators and security administrators responsible for the implementation and management of security on IBM® AS/400 systems. However, any user with a basic knowledge of System i operations is able to make full use of this document following study of this User Guide.

NOTE: Deviations from IBM® standards are employed in certain circumstances in order to enhance clarity or when standard IBM® terminology conflicts with generally accepted industry conventions.

This document may also serve for new versions' upgrade approval by management.

Native IBM i (OS/400) User Interface

Command is designed to be a user-friendly product for auditors, managers, security personnel and system administrators. The user interface follows standard IBM i CUA conventions. All product features are available via the menus, so you are never required to memorize arcane commands.

Many features are also accessible via the command line, for the convenience of experienced users.

Conventions Used in the Document

Menu options, field names, and function key names are written in **Courier New Bold**.

Links (internal or external) are emphasized with underline and blue color as follows: "About this Manual" on the previous page.

Commands and system messages of IBM i® (OS/400®), are written in ***Bold Italic***.

Key combinations are in Bold and separated by a dash, for example: **Enter**, **Shift-Tab**.

Emphasis is written in **Bold.**

A sequence of operations entered via the keyboard is marked as

STRAOD **> 81 > 32**

meaning: Syslog definitions activated by typing ***STRAOD***and selecting option: **81** then option: **32**.

Menus

Product menus allow easy access to all features with a minimum of keystrokes. Menu option numbering and terminology is consistent throughout this product and with other Raz-Lee products. *To* select a menu option, simply type the option number and press **Enter**. The command line is

available from nearly all product menus. If the command line does not appear (and your user profile allows use of the command line), press **F10** to display it.

Data Entry Screens

Data entry screens include many convenient features such as:

- Pop-up selection windows
- Convenient option prompts
- Easy-to-read descriptions and explanatory text for all parameters and options
- Search and filtering with generic text support

The following describes the different data entry screens.

- To enter data in a field, type the desired text and then press Enter or Field Exit
- To move from one field to another without changing the contents press Tab
- To view options for a data field together with an explanation, press F4
- To accept the data displayed on the screen and continue, press Enter

The following function keys may appear on data entry screens.

- **F1**: **Help** Display context-sensitive help
- **F3**: **Exit** End the current task and return to the screen or menu from which the task was initiated
- **F4**: **Prompt** Display a list of valid options for the current field or command. For certain data items, a pop-up selection window appears
- **F6**: **Add New** Create a new record or data item
- **F8**: **Print** Print the current report or data item
- **F9**: **Retrieve** Retrieve the previously-entered command
- **F12**: **Cancel** Return to the previous screen or menu without updating

Legal Notice

applicable laws. If you do not agree with these terms, please do not access or use the remainder of this document.

This document contains highly confidential information, which is proprietary to Raz-Lee Security Ltd. and/or its affiliates (hereafter, "Raz-Lee"). No part of this document's contents may be used, copied, disclosed or conveyed to any third party in any manner whatsoever without prior written permission from Raz-Lee. The information included in this document is intended for your knowledge and for negotiation purposes only. Raz-Lee makes no implicit representations or warranties with respect to such information. The information included in this document is subject to change without notice. Any decision to rely on the information contained herein shall be at your sole responsibility, and Raz-Lee will not accept any liability for your decision to use any information or for any damages resulting therefrom. Certain laws do not allow limitations on implied warranties or the exclusion or limitation of certain damages. If these laws apply to you, some or all of the above disclaimers, exclusions, or limitations may not apply to you.

Contacts

Raz-Lee Security Inc. www.razlee.com
Marketing: marketing@razlee.com 1-888-RAZLEE-4 (1-888-7295334)
Support: support@razlee.com 1-888-RAZLEE-2 (1-888-7295332)

Chapter 1: Introducing Command

Raz-Lee Security's Command, part of the iSecurity suite, provides total control over CL commands, command parameters, their qualifiers and elements, as well as the users who are permitted to issue specific commands and change parameters.

Command filters the use of specific commands–both IBM supplied and user-defined– by specific users. It also includes a variety of industry-unique parameter selection criteria which enable adding, replacing or removing qualifiers, elements and lists of values used as command parameters.

As Command is totally integrated into the infrastructure of products in the iSecurity suite, it can send real-time alerts as event-specific e-mails or SMS, Syslog, Twitter and other forms of messages. In addition, Command can execute corrective CL command scripts in response to specific command-related situations. Command's iSecurity-based "look and feel" relates to print command log options as well.

To start the Command program, type **STRCMD** on any command line.

If a system password is requested, type **QSECOFR**

The main screen is displayed which provides access to the different features of the product. The various feature groups are described in the following chapters:

- Command Security
- Definitions
- Analysis
- Maintenance

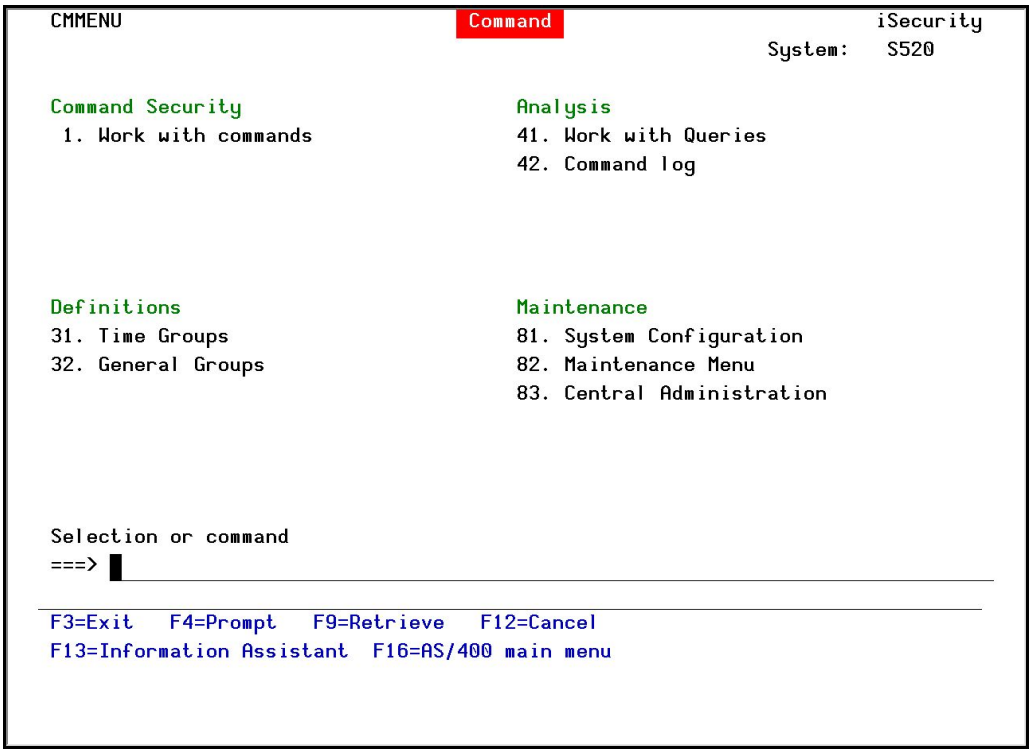

Figure 1: Command Main Screen

The Need for Command

The IBM i (AS/400) has traditionally been used as an “application server”, accessed by users via menu-driven interfaces. Such an interface reduces the risk of users entering potentially damaging commands; however these facilities are not “air-tight” and can easily be bypassed.

As the need for full compliance with industry and “best practice” regulations has become the norm, companies worldwide demand greater control of command-line access. At the same time, companies and their auditors must be able to log and monitor command-line usage more effectively in order to ensure its proper business use.

Indeed, all regulations–SOX, HIPAA, PCI, BASEL II, and auditor-mandated regulations–require auditing and traceability of commands issued by users, whether they be system or database administrators, help desk or application users.

Feature Overview

- Designed and implemented based upon specific customer requests for a “total” solution to command-line control and monitoring
- Incorporates easy-to-define rules for controlling both command and parameter usage.
- Includes advanced features, such as displaying the programs in the command stack which generated the command and displaying the program library from which the command was entered.
- Displays and enables replacing or changing qualified parameters, element parameters and parameters which contain a list of values.
- Log File
- Protects commands from all sources:
    - Command line
    - CL Programs
    - QSH
    - SSH
    - SQL
    - REXEC
    - FTP

Benefits

- Easy to use and even easier to set up!
- Totally protects and monitors command usage
- Flexible and dynamic support of command parameters
- Wide variety of parameter selection criteria
- Indicates Qualified & Element parameters as well as a “list of values” parameter
- Enables replacing Based on a popular signature file used in the Open Source (Linux) environment

System Requirements

- Disk space: 110 MB
- PASE (Portable Application Solutions Environment), a special Linux-like environment installation: required
  For further details, see: http://en.wikipedia.org/wiki/IBM_System_i
- Operating System: V5R3 or higher.

Native OS/400 Text Based User Interface

Command is designed to be a user-friendly product. The user interface follows standard System i CUA (Common User Access) conventions. All product features are available via the menus, so users are never required to memorize arcane commands. Many features are also accessible via the command line, for the convenience of experienced users.

Menus

Product menus allow for easy access to all features with a minimum of keystrokes. Menu option numbering and terminology are consistent throughout this product as well as other Raz-Lee products. To select a menu option, simply type the option number and press **Enter**. The command line is available from nearly all product menus. If the command line does not appear (and your user profile allows use of the command line), press **F10** to display it.

Data Entry Screens

Data entry screens include many convenient features such as:

- Pop-up selection windows
- Convenient option prompts
- Easy-to-read descriptions and explanatory text for all parameters and options
- Search and filtering with generic text support.

The following describes the different data entry screens.

- To enter data in a field, type the desired text and then press **Enter** or **Field Exit**
- To move from one field to another without changing the contents press **Tab**
- To view options for a data field together with an explanation, press **F4**
- To accept the data displayed on the screen and continue, press **Enter.**

These function keys may appear on data entry screens.

Function Key	Description
F1 - Help	Display context-sensitive help
F3 - Exit	End the current task and return to the screen or menu from which the task was initiated
F4 - Prompt	Display a list of valid options for the current field or command. For certain data items, a pop-up selection window appears
F6 - Add New	Create a new record or data item
F8 - Print	Print the current report or data item
F9 - Retrieve	Retrieve the previously-entered command
F12 - Cancel	Return to the previous screen or menu without updating

Chapter 2: Getting Started

A Summary of the explanation in this section is described as follows:

- Use Command for the first time, **STRCMD > 81 > 31**, set **Secure (Check commands)** to **Y**.
- Build a warning message rule.
- Add a filter condition (double check the filter logic Vs the rule itself).
- Test command.
- Activate Action, Send email and a message to QSYSOPR.
- Display the Command usage log.
- Build rules that allows injecting values into the command at run time, such as, **WRKSYSSTS** to ***PRINT**.

How to Begin Working with Command

1. To access the **Command** menu, type the command **STRCMD**.
2. In the **Command** menu, select **81 > 31. Command.: Definitions**. The **Command General Definitions** screen appears (see Work with Restricted Commands).

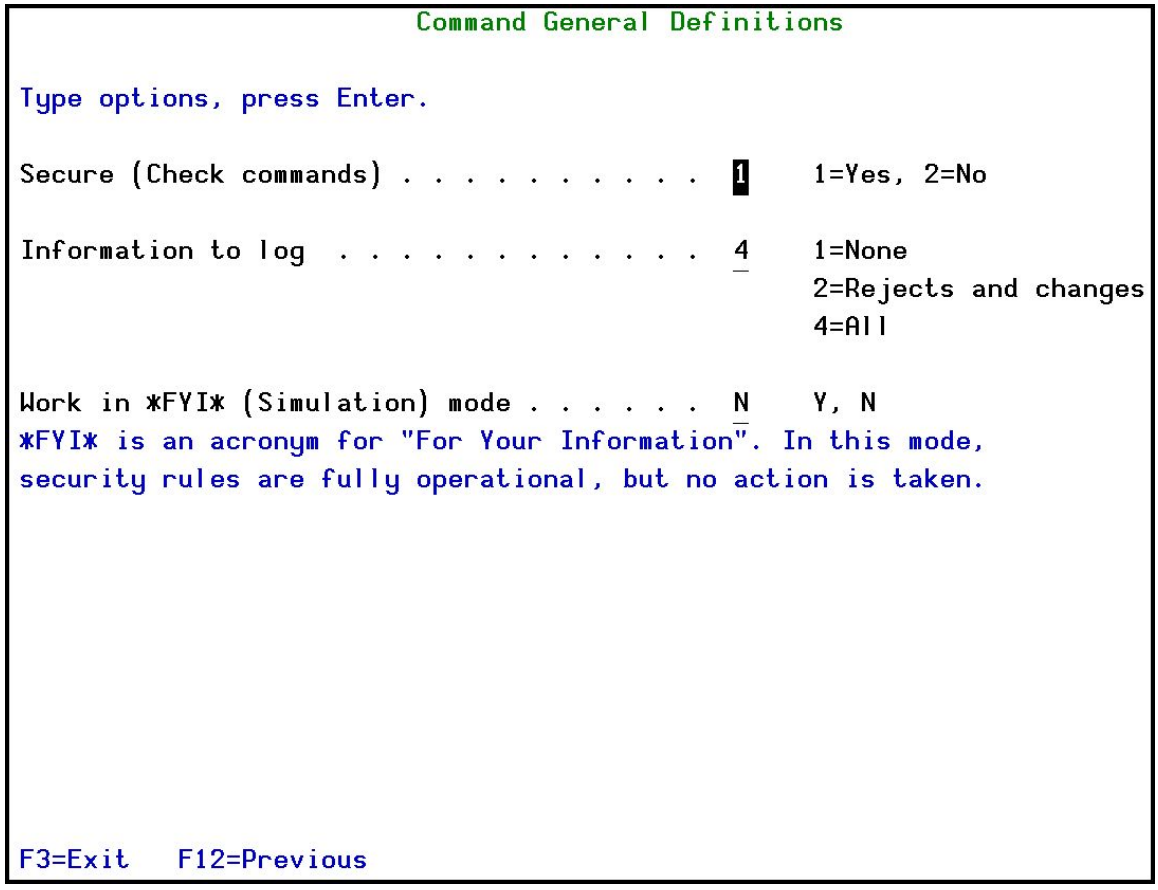

Figure 2: Command General Definitions

3. In the **Command General Definitions** screen, set **Secure (Check commands)** to **1=Y**, select **Enter**.
4. In the **Command** menu, select **1=Select**. The **Work with Restricted Commands** screen appears (see Work with Restricted Commands).

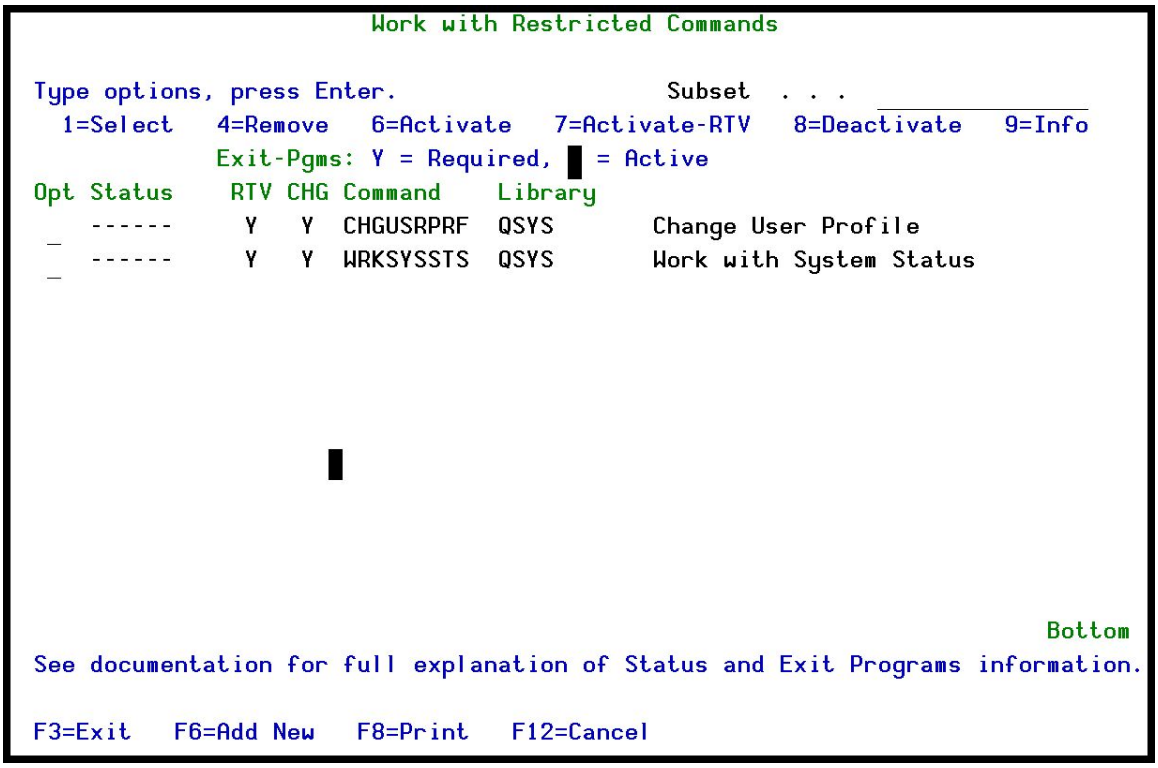

Figure 3: Work with Restricted Commands

5. Select **1=Select**. The **Work with Command Rules** screen appears (see Working with Command Rules).

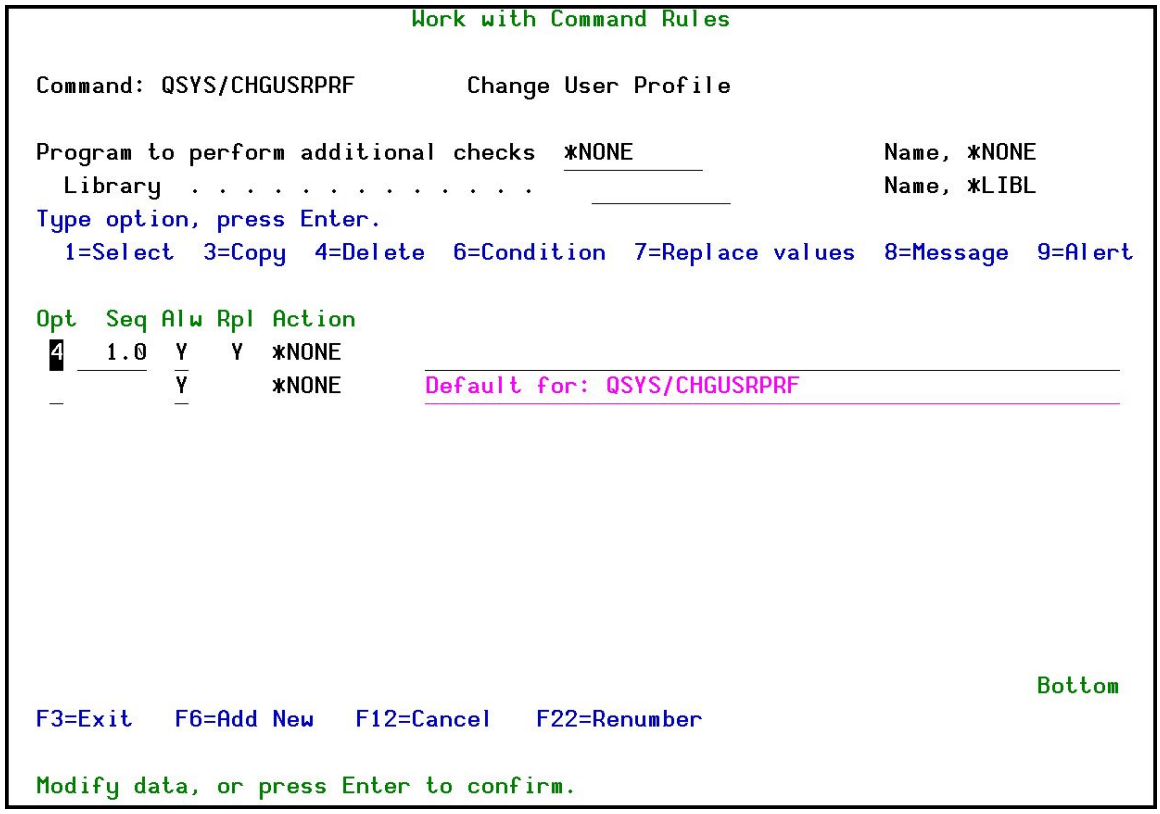

Figure 4: Work with Commands Rules

6. Select **1=Select**, and Enter. The Work with a Command Rule screen appears.

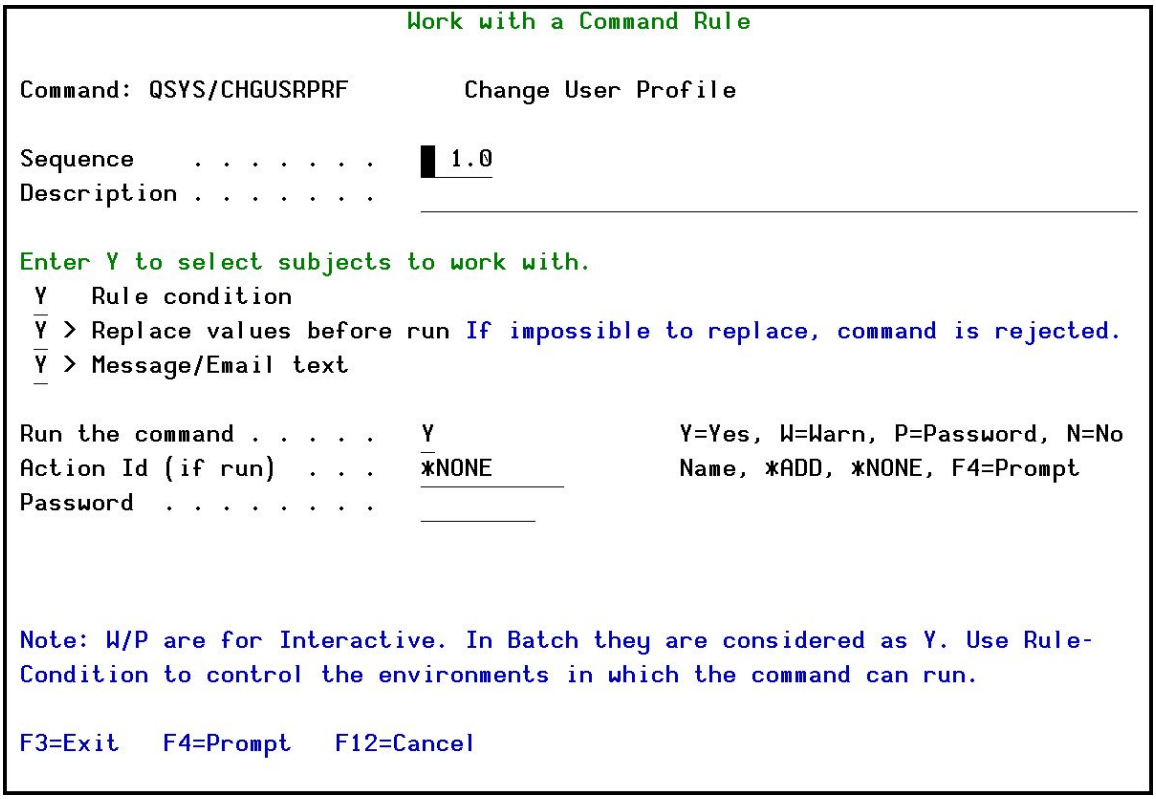

Figure 5: Work with a Commands Rule

7. Select **Enter**. The **Filter Conditions** screen appears (see Filter Conditions).

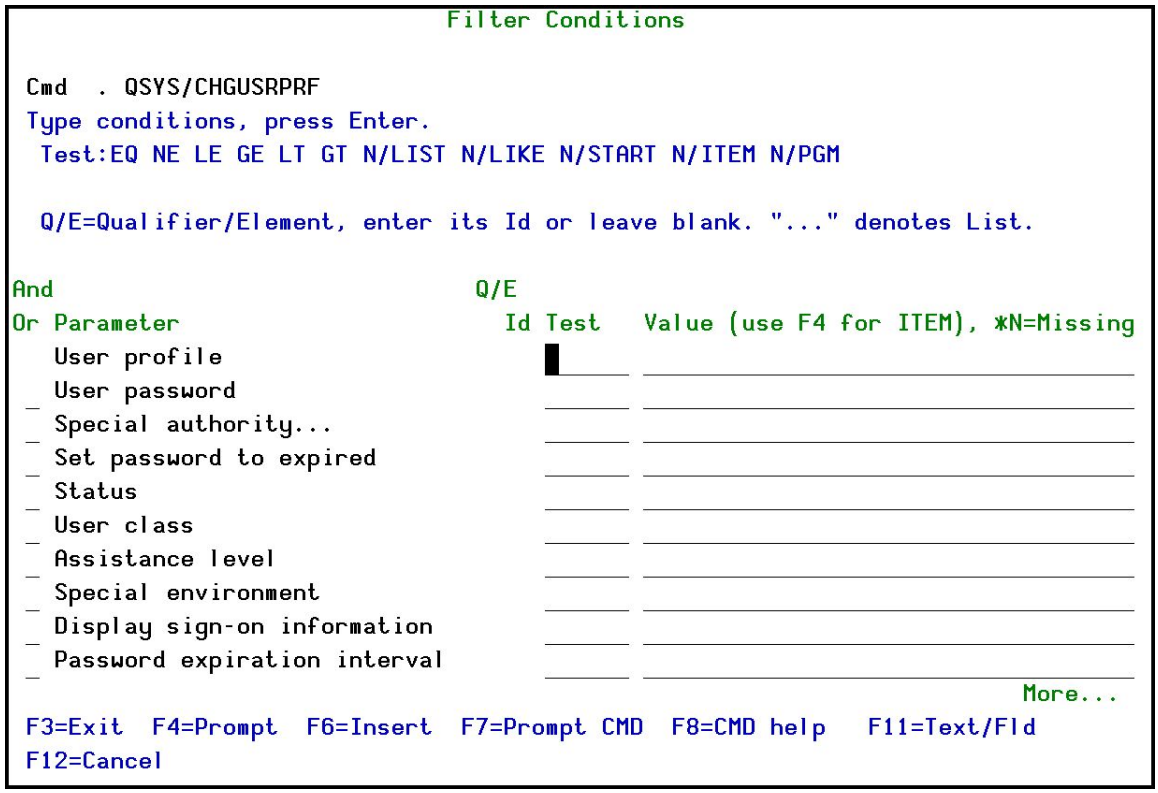

Figure 6: Filter Conditions

8. In the **Filter Conditions** screen, add **`Filter Condition`** (double check the filter logic versus the rule itself). Type conditions to test **Command**.
9. In the **Work with Command Rules** screen, select **`8=Message`** to activate **Action**, Send email and a message to QSYSOPR. In the **Work with Command Rules** screen, select **9=Alert** to add a unique alert message to the screen.
10. In the **Command** menu, select **`42. Work with Queries`** to display the **Command** usage log.
11. Build rules that allow injecting values into the command at run-time **WRKSYSSTS** using **`F8=Print`**.

Chapter 3: Command Security

This chapter describes the various features that are central to **Command** security.

Work with Restricted Commands

Restricted commands are the basis for the rules that one creates and associates with specific libraries to control user activity on the system.

To work with restricted commands, select **1. Work with commands** from the main menu. The **Work with Restricted Commands** screen appears. It displays each command rule that has been entered into the system, the associated library in which it resides, if it has a rule and its description. If **Command** is currently tracking a specific command, its status is marked as **`Active`**.

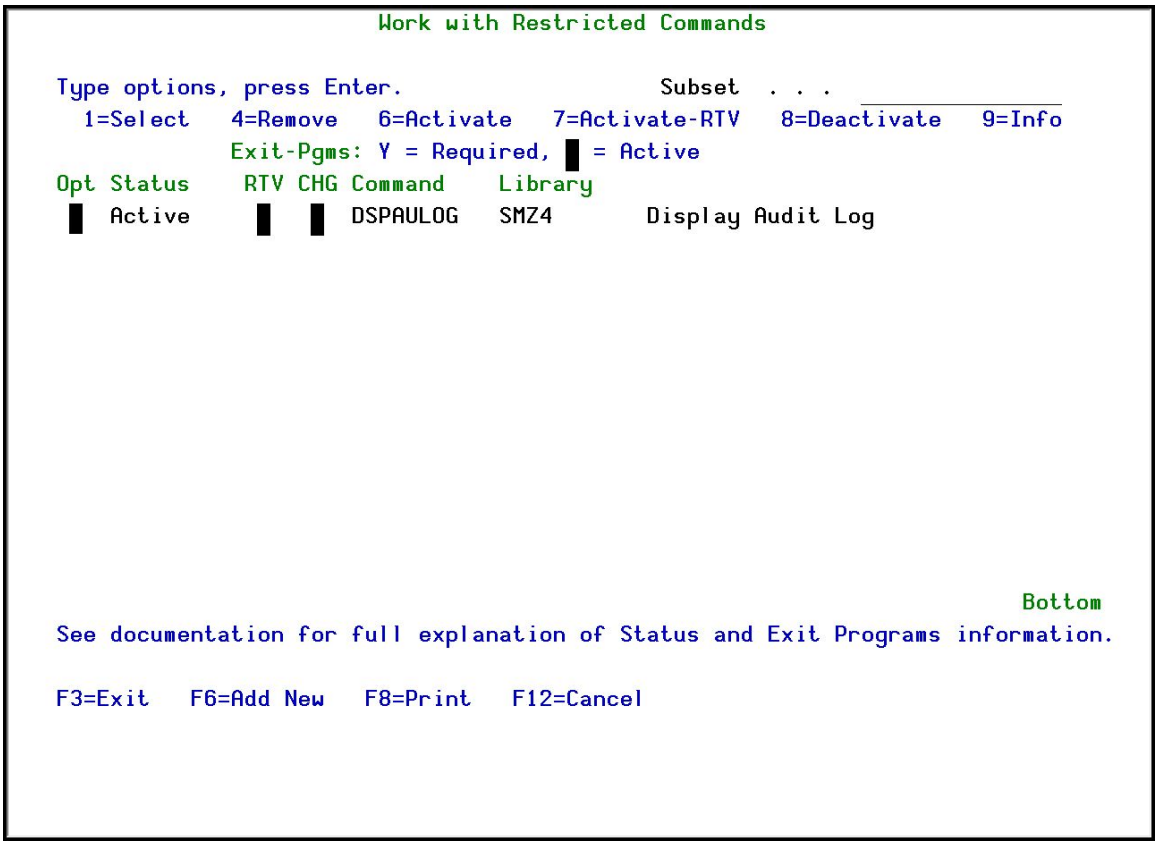

Figure 7: Work with Restricted Commands Screen

Parameter	Description
1=Select	Edit the selected command rule
4=Remove	Remove the selected command rule
6=Activate	Activate the selected command rule when the command is changed
7=Activate-RTV	Activate-RTV the selected command rule when the command is retrieved
8=Activate	Deactivate the selected command
9=Info	Display information about the selected command
F6	Opens the Add Restricted Command screen

Adding a New Command Restriction

To create a new command restriction, select **F6** from the **Work with Restricted Commands** screen. The **Add Restricted Command** screen is displayed.

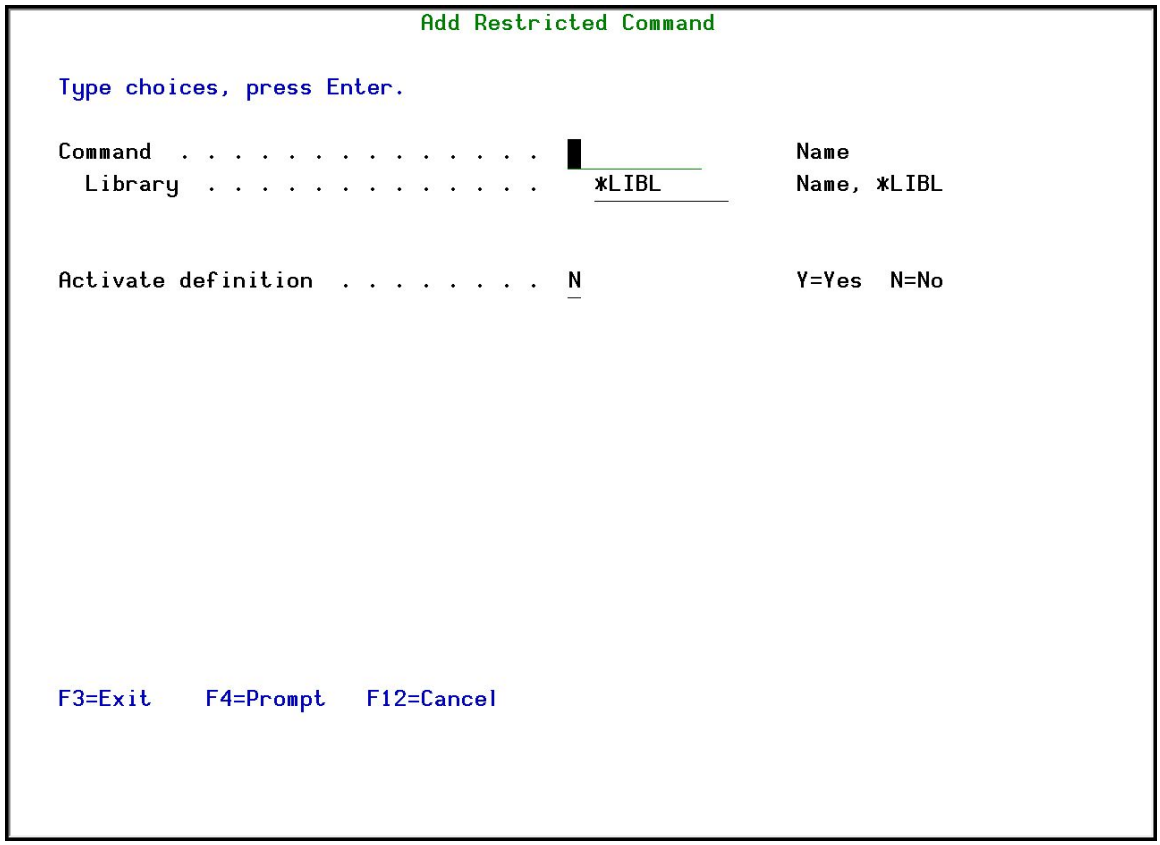

Figure 8: Add Restricted Command Screen

After completing the various fields described below, press **Enter** to continue. The new command restriction is added to the list on the **Work with Restricted Commands** screen.

Parameter	Description
Command	Enter the name of the command to restrict. If a specific library has already been defined, press F4 to display a prompt with the existing commands available to choose from in the library.
Library	Enter the name of the specific library where the command will run. If entering a command when *LIBL is displayed, Portable Application Solutions Environment will automatically insert the first library from the Library List that includes this command.
Activate Definition	Y =Yes N =No

Working with Command Rules

A command rule triggers an action and/or sends a message to a defined list of recipients. It appears as a single row above the actual command in the **Work with a Command Rule** screen.

Information

1. In the **Command** menu select, **1 > 9=Info**. The **Information** screen appears.

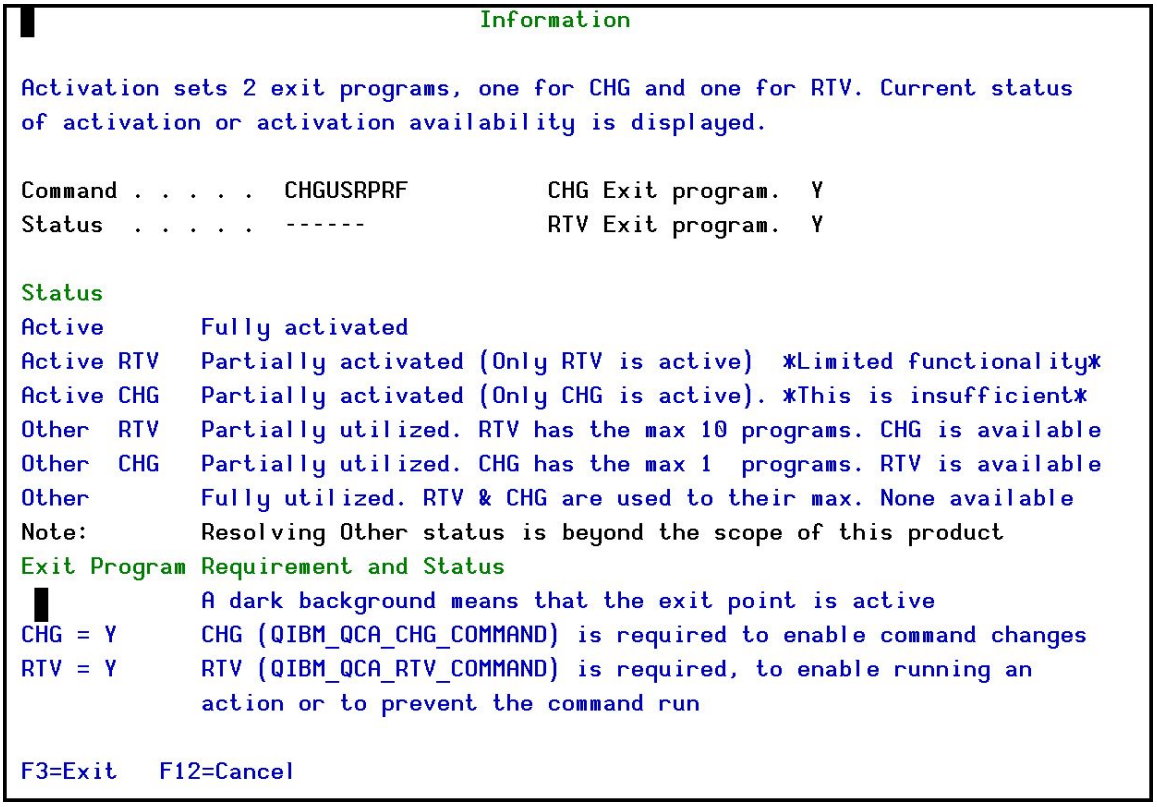

Figure 9: Information

2. For the filter to work, make sure the filter logic matches the full rule path by setting the property to **Y**.

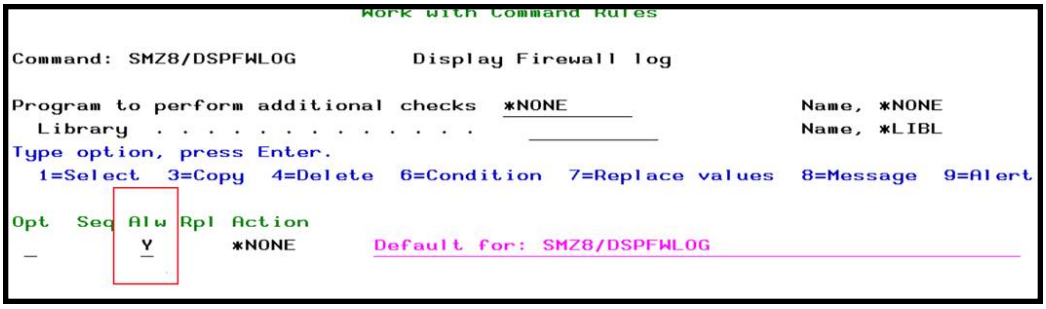

Figure 10: Work with Command Rules - Filter Logic Matches Full Path

Parameter	Description
Command	Command name and description (not editable)
Sequence Id	The number of this rule in the complete sequence of rules
Description	An editable description for the command rule. If the Run the command parameter is W, this is the message that is displayed to the user.
Program to perform additional checks	Name= Name of program with checks to perform *NONE= No program checks to perform
Library	The file library to perform the checks
Options	1=Select ; select the line 3=Copy; copy the line 4=Delete ; delete the line 6=Condition ; @@@ 7=Replace Values ;when Y=Yes (or empty) When updating the rule, if Yes is selected (a replacement value exists), displays the Replace Values screen when cycling through the different rule screens. Note: If the values cannot be replaced, the command will be rejected. 8=Message ; Y=Yes (or empty) When updating the rule, if Yes is selected (a message text exists), displays the Message to Send screen when cycling through the different rule screens. 9=Alert ; Y=Yes (with/out changes) W=Warn (when the command is run, displays the text in the Description field as a warning message) P=Password (when the command is run, the user will be asked to enter a password. Define the password in the Password field below) N=No (reject it) W and P are only relevant for interactive commands. If the command is used in batch mode, the parameter is assumed to be Y.

3. Check if **Command** mode is active in real or simulation mode.

Command Rules

1. In the **Work with Restricted Commands** screen, select 1=Select. The **Work with Command Rules** screen is displayed with each rule numbered according to the sequence in which it runs.

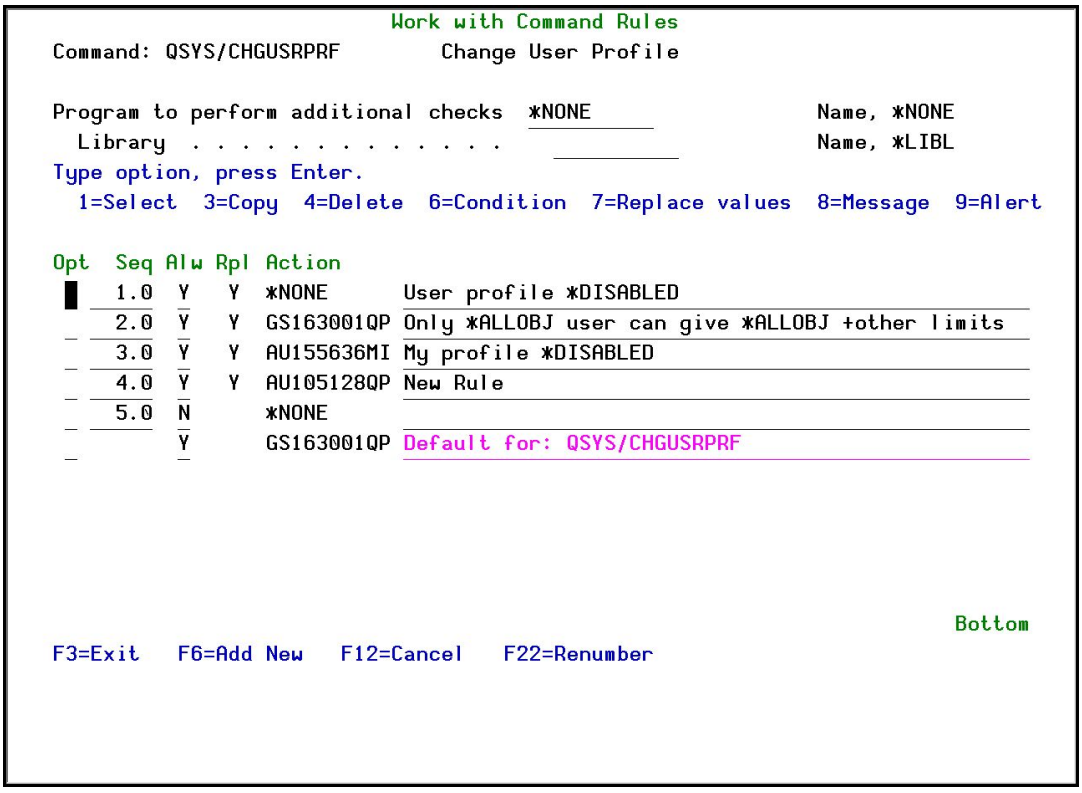

Figure 11: Work with Command Rules – Select

Parameter	Description
Library/Command	The specific library where the command will run and the name of the command.
Sequence	The order in which the command rule will run
Run	If the command rule will run (Yes/No)
Action	Action that will run and a description of the Action.
F6	Opens a new Add Command Rule screen (see the Work with a Command Rule screen)
F22	To change the order that command rules run, change the Sequence number and press Enter. The rows are re-ordered according to the correct sequence, but may not begin at 1 or increment uniformly (for example, 2, 4, 5). Select F22= Renumber to reset the first command rule in the sequence to 1, incrementing by +1 for each new row.

2. To edit a specific command rule, choose **1. Select**. The **Work with a Command Rule** screen appears.

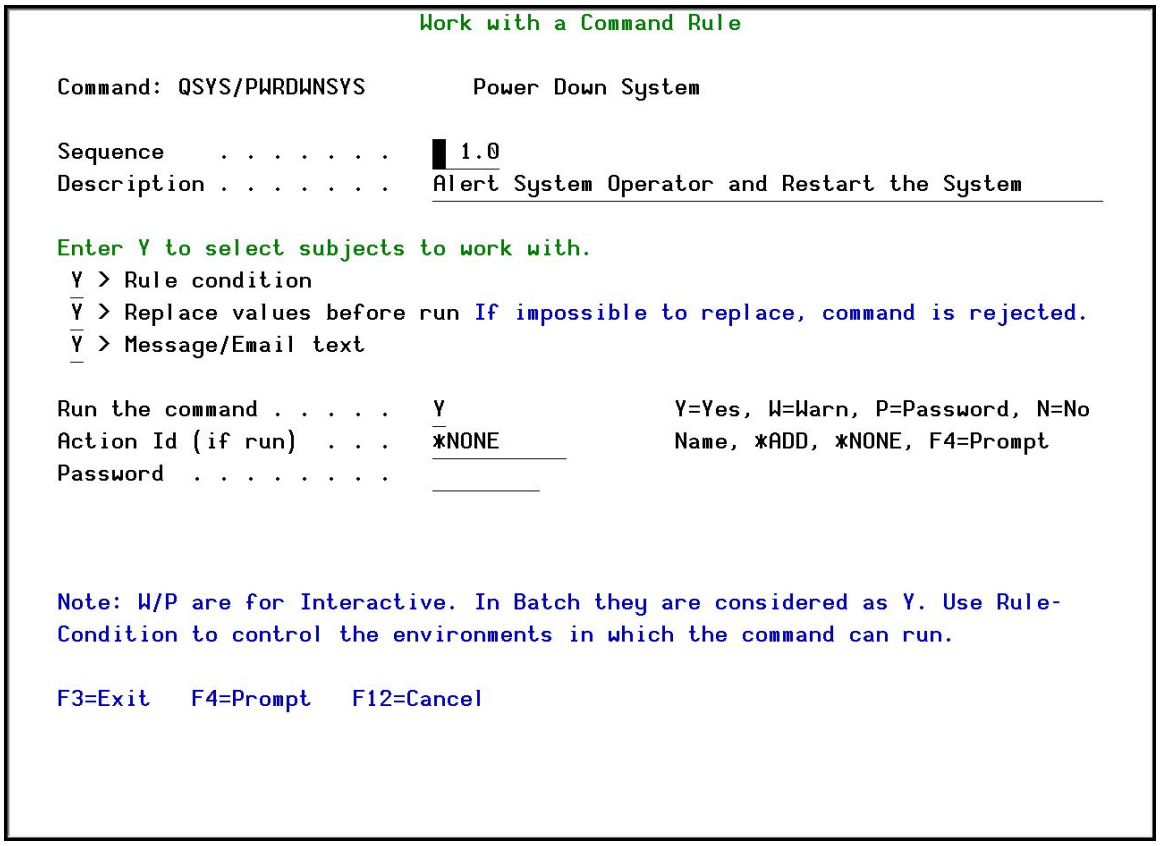

Figure 12: Work with a Command Rule – Edit

Parameter	Description
Command	Command name and description (not editable)
Sequence Id	The number of this rule in the complete sequence of rules
Description	An editable description for the command rule. If the Run the command parameter is W, this is the message that is displayed to the user.
Rule condition	Y=Yes (or empty) When updating the rule, if Yes is selected (a rule condition exists), displays the Filter Condition screen when cycling through the different rule screens. Note: For the actual command (the final command rule row), this option is called Default and is empty.
Replace values before run	Y=Yes (or empty) When updating the rule, if Yes is selected (a replacement value exists), displays the Replace Values screen when cycling through the different rule screens. Note: If the values cannot be replaced, the command will be rejected.
Message/Email text	Y=Yes (or empty) When updating the rule, if Yes is selected (a message text exists), displays the Message to Send screen when cycling through the different rule screens.
Run the command	Y=Yes (with/out changes) W=Warn (when the command is run, displays the text in the Description field as a warning message) P=Password (when the command is run, the user will be asked to enter a password. Define the password in the Password field below) N=No (reject it) W and P are only relevant for interactive commands. If the command is used in batch mode, the parameter is assumed to be Y.
Action ID (if run)	When updating the rule, displays the Add/Modify Alert screen when cycling through the different rule screens. If the option *NONE is selected, the Add/Modify Alert will not be displayed Name = Name of an action *ADD (default) = Define a new action for this rule

Parameter	Description
	*NONE = no action is defined F4 = Prompt to display a list of pre-defined messages. Pre-defined messages are stored in a special message file and are identified by their unique message ID.
Password	If the Run the command parameter is P, type the password that allows access to the command.
>	This symbol appears if a definition already exists

To update the position of a rule in the sequence, give it a new number and press **Return**. The rules are resorted according to their numbers, but the actual numbers in the sequence are not updated. To update the numbers, press **F22**. The final item in the sequence cannot be moved and runs only when all items higher in the sequence are completed successfully.

To create a new command rule, press **F6**.

NOTE: Each time **Enter** is pressed, the next screen in the **Command Rule** cycle is displayed if it was previously enabled (Default=**Yes**) in the **Work with a Command Rule** screen.

To access each of these screens directly from the **Work with a Command Rule** screen, select its option number (**6, 7, 8, 9**) in the **Work with Command Rules** screen.

Filter Conditions

Filter conditions are the criteria that must be matched when a command is entered by a user in order to trigger the command's alerts, messages and changes. Each filter condition consists of a comparison test applied against one of the fields in the journal record, such as a parameter, originator (job, user, IP) or context (from which program, environment).

The **Filter Conditions** screen appears immediately after completing the **Work with a Command Rule** screen. To open it directly, choose a rule and select **6. Condition** in the **Work with Command Rules** screen.

NOTE: Filter conditions are optional. If no filter condition is defined, the command rule will permit all attempts to run the specified command.

Press **Enter** to complete and save this screen.

```
                              Filter Conditions

 Cmd  . QSYS/CHGUSRPRF
 Type conditions, press Enter.
  Test:EQ NE LE GE LT GT N/LIST N/LIKE N/START N/ITEM N/PGM

  Q/E=Qualifier/Element, enter its Id or leave blank. "..." denotes List.

And                                Q/E
Or Parameter                         Id Test   Value (use F4 for ITEM), *N=Missing
   Initial program to call           Q 2 LIST   PGMLIB TESTLIB QGPL *N
_  Job description                   Q   EQ     QGPL/QBATCH
_  EIM association                   E 2 EQ     *ADMIN
_  User Profile (Current)                ITEM   *SPCAUT/*JOBCTL
_  Programs in stack                     LIKE   %MNUUSR%
_  Job type INT/BCH                      EQ     INT
_  From program name                     EQ     QCMDEXC
_  Initial program to call           Q   EQ     SSS
_  User profile
_  User password
                                                                        More...
 F3=Exit  F4=Prompt  F6=Insert  F7=Prompt CMD  F8=CMD help   F11=Text/Fld
 F12=Cancel
```

Figure 13: Filter Conditions Screen

Parameter	Description
And/Or	A or Blank = AndO = OrCombine multiple filter conditions in one rule using Boolean AND/OR operators to create complex rules that produce precise results. When using 'Or' operators in filter conditions, the order in which each condition appears in the list of conditions is critical. The 'Or' operator allows grouping of several conditions together because it includes all 'And' conditions that follow it until the next 'Or' operator, or until the end of the list. 'And' condition groups the 'Or' condition which was defined before it. **Example:** This rule will apply to all events meeting **either** the conditions listed in Group 1 **or** the conditions listed in Group 2. Group 2 includes the 'Or' condition and all of the 'And' conditions that follow it.
Parameter	Parameters "…" denotes a list of additional values **Pink** fields are part of the generic header common to all journal types **Green** fields represent data specific to this journal type
Q/E	Qualifier/Element of the parameter – enter its ID or leave it blank. **Example 1:** Reference to a specific qualifier or element enables one to differentiate between "PAYROLL" as part of the file name or the library name itself. **Example 2:** Some of the Change User Profile (CHGUSRPRF) parameters are: • Qualifier, such as INLPGM(library / program) • Composed of elements, such as EIMASSOC(admin *ADMIN *REPLACE) • Include a list of values, such as SUPGRPPRF(grpprf1 grpprf2 gprpprf3)
Test	Comparison test type (see table below for details)
Value	Comparison value text. **Note:** This filed is case sensitive.
F4	Displays explanatory information and/or options applicable to the data field on the line where the cursor is located
F6	Select another comparison test from a pop-up window and insert it at the current cursor position
F7	Prompt CMD – to display the command parameters
F8	Change Caps Lock from lower to upper case. An indicator appears on the screen.

Comparison Test Operators

Comparison test operators help pinpoint specific conditions and users, for example ensuring the existence of a specific user in an external table and verifying that the user has special authority.

Several different types of comparison test operators are available:

Test	Description	Value Field Data
EQ,NE	Equal to, Not equal to	Value
LT, LE	Less than, Less than or equal to	Value
GT, GE	Greater than, Greater than or equal to	Value
LIST, NLIST	Included in list, Not included in list	Values separated by a space
LIKE, NLIKE	Substring search	Value preceded and/or followed by **%**
ITEM/NITEM	Item in a group checks if the value is among the groups' members. The General group is an external value list that can be extended by creating new types.	*USER – Check that the value is a user in a %GROUP of users ***GRPPRF – Check that the value is a user in an OS/400 Group Profile** *USRGRP – USER and all user profiles which are members of same user groups as USER ***ALL – For both *GRPPRF and *USRGRP cases** If the TYPE is missing, *USER or *****USRGRP is assumed based on the appearance of % sign as the first character in the GROUP. *SPCAUT – Check that the value is in the users Special-Authority
START	Starts with, Does not start with	Starting characters of string
PGM, NPGM	Calls a specific user program to conduct a comparison which replies with True or False	The user program name (library/program)

Message to Send

When a command rule is matched, a message can be generated to alert different users. Enter the text of the message in this screen.

To automatically insert a system parameter within the body of the text, select **F7. Replacement Fields**. The Select Parameter screen opens. Move to the parameter you want to insert and choose **1. Select**. The screen closes and the parameter appears within the message.

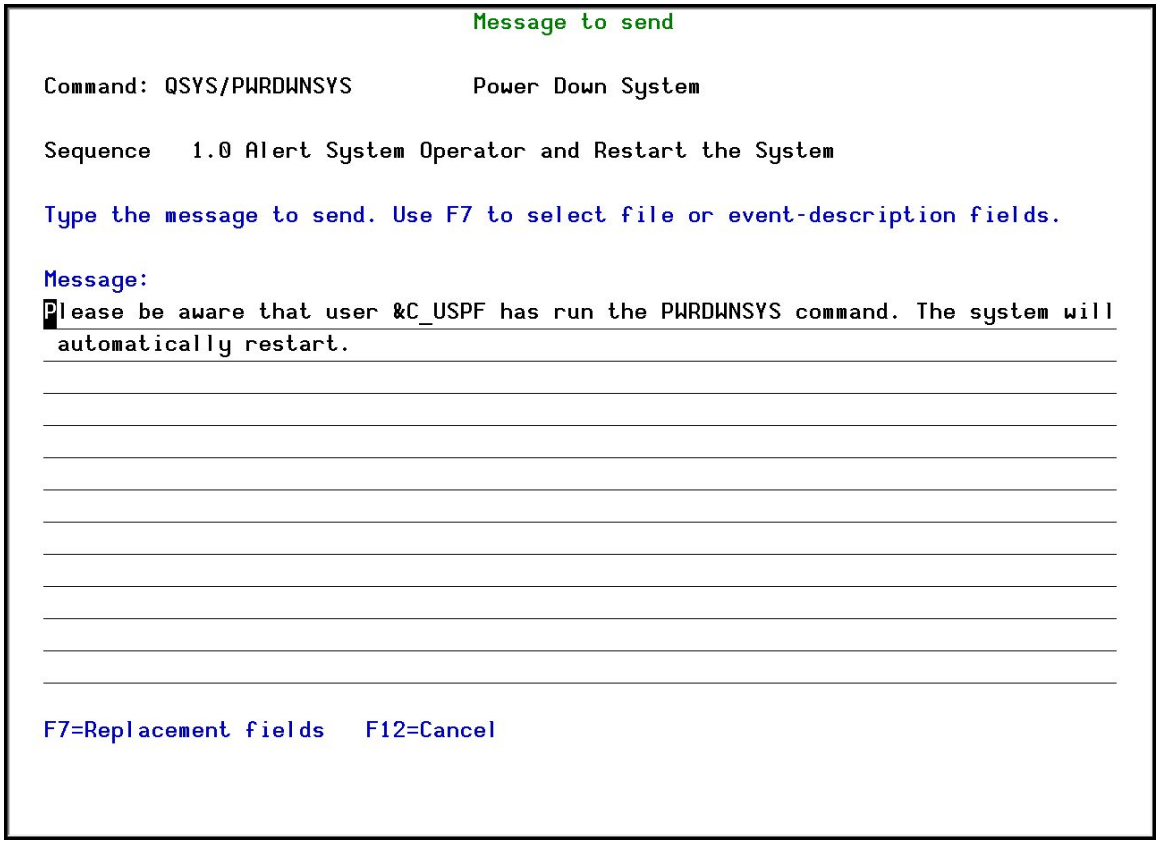

Figure 14: Message to Send Screen

Adding a Command Alert

The **Modify Alert** screen enables users to define how to send a command rule message that is already defined in the **Message to Send** screen and the recipients of the message.

To define alerts and alert recipients, choose the command rule in the **Work with Command Rules** screen and select **9. Alert**. The **Modify Alert** screen appears. This screen also appears after completing the **Work with a Command Rule** screen.

To specify a specific alert, enter its number in the **Type** column, and then define its recipient address types and formats as described in the table below.

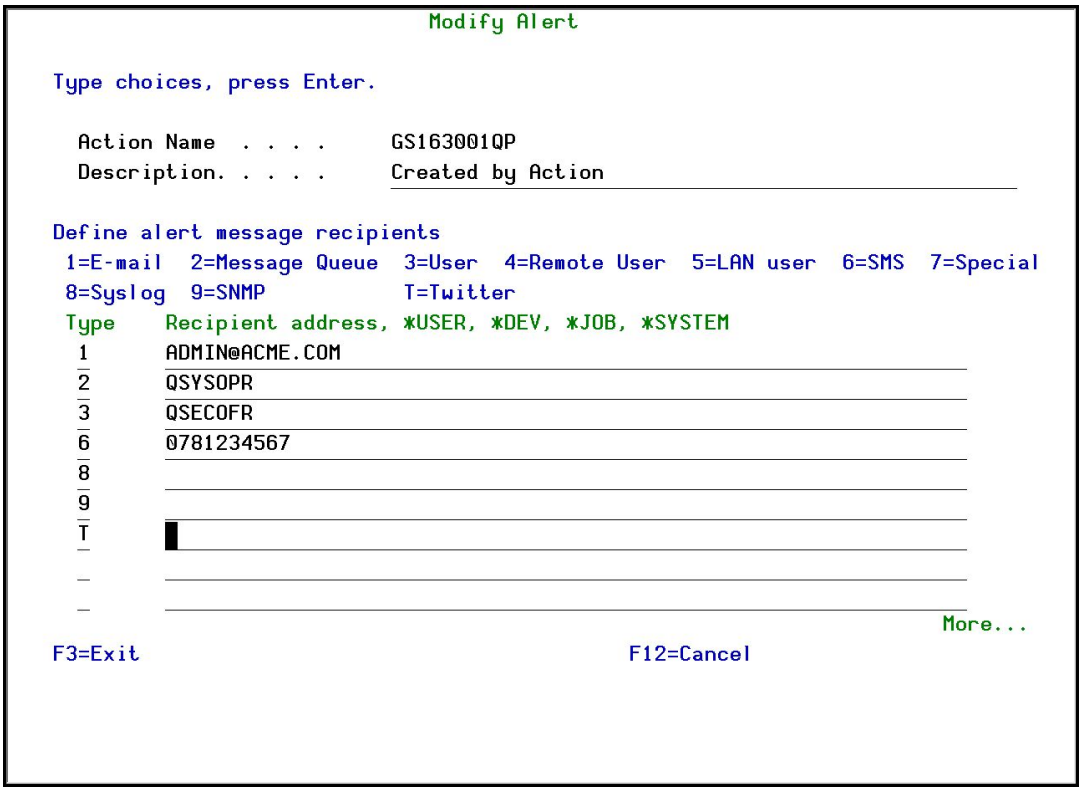

Figure 15: Add Alert Screen

Parameter	Description
Action Name	ID of the alert message
Description	Description of the alert
E-mail	E-mail address in standard format (user@company.com)
Message Queue	Fully qualified name of the message queue or *SYSOPR. For further details, see Audit User Manual, Working with Message Queues section.
User	User profile or AS/400 group profile
Remote User	Remote system user (SNDNETMSG)
LAN User	Valid network user name or *DOMAIN for all users on your domain
SMS	Phone number including country code and area code as necessary
Special	Phone number and access codes for the pager service
Syslog	As defined in 81 > 71. Syslog
SNMP	As defined in 81 > 81. iSecurity/Base > 32. SNMP
Twitter	As defined in 81 > 81 > 33. Twitter

Edit Action Script

Once an alert is completed, the **Edit Action Script** screen appears. Use this screen to define one or more command scripts to run whenever the command rule's conditions are met.

Commands execute sequentially according to a user-defined order. They may include replacement variables that extract data from the history log record and insert it as command parameters. **Command** also supports conditional branching in the event that an error occurs during script execution.

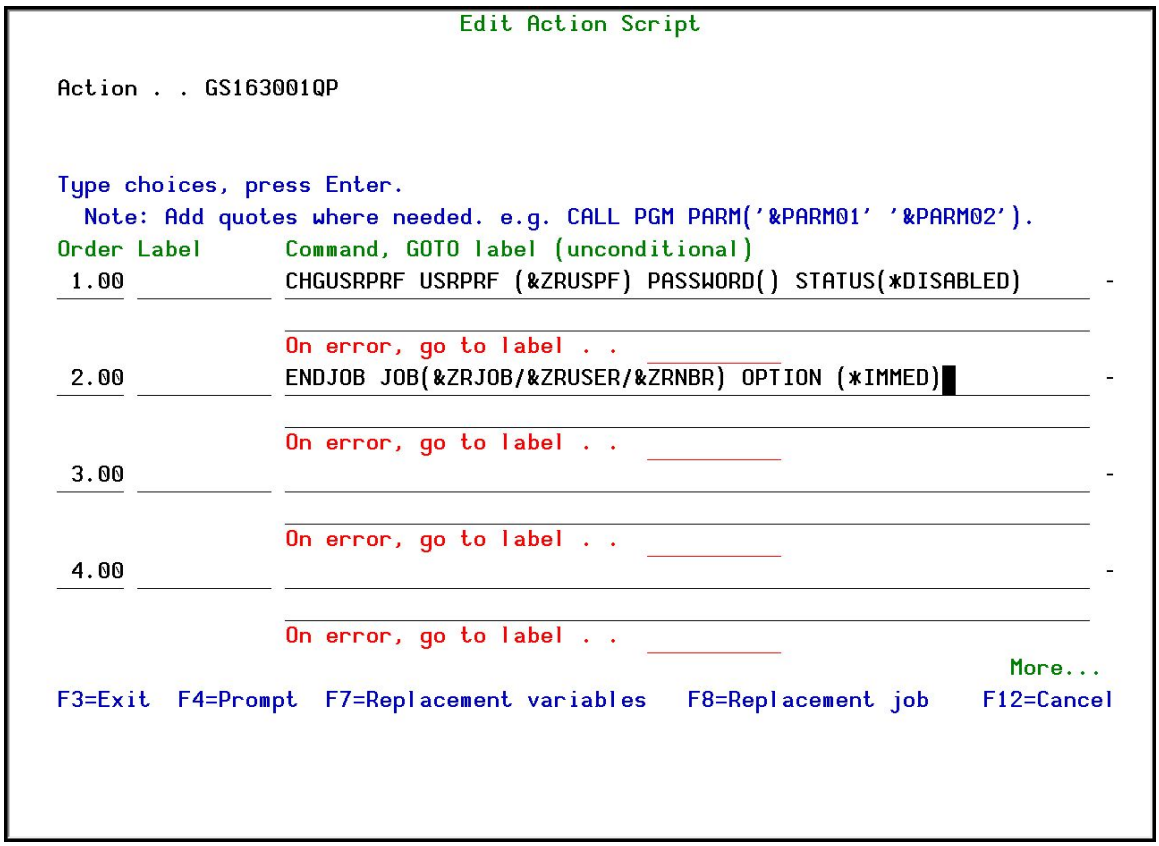

Figure 16: Edit Action Script Screen

Parameters / Options	Description
Order	Order in which the commands are executed
Label	Optional alphanumeric label for the current line. Used for the On Error Go To Feature.
Command	Command text including all parameters
On Error, Go to Label	Conditional branch to the line indicated by the label in the event a script error results from the command on the current line
F4	Open prompt window for command parameters and options
F7	Select a variable from pop-up window and insert it at the current cursor position. Variables insert contents of journal entry data fields as command parameters.
F8	Inserts the 3 job variables (User, Job and Number) that are to be replaced when the command runs

Replacement Variables

Replacement variables allow users to extract data from the history log record and insert it into command scripts as parameters. For example, in a command script intended to terminate a suspicious job, the **Job Name**, **Job User** and **Job Number** information would be extracted from the journal entry and inserted into the appropriate parameter fields for the *ENDJOB* command. The command with replacement values would appear as follows:

*ENDJOB JOB(&ZRJOB/&ZRUSER/&ZRNBR) OPTION(*IMMED)*

NOTE: Replacement variables are always preceded by the '**&**' character. When selecting the data field from a list using **F7**, this character is inserted automatically.

To insert a replacement parameter:

1. Move the cursor to the appropriate location in the command script within the **Edit Action Script** window.
2. Press **F7** to display the **Select Parameter** screen.
3. Select the desired parameter from which to extract data, and press **Enter**.

Conditional Branching

Action command scripts support conditional branching in the event of a script error. The **Label** field identifies a command line for branching purposes. The **On Error Go To Label** field instructs the script to branch to the line indicated by the label in the event that an error is generated by the command.

To end script processing in the event of a script error, insert a label on a blank line following the last command. Enter that label in the **On Error Go To Label** field on each active command line.

Replace Values

The **Replace Value** screen enables users to define what to replace, prior to execution of a command, any element, qualifier, an entire parameter or the *CL* command itself.

To define replacement values, choose the command rule in the **Work with Command Rules** screen and select **`7. Replace Values`**. The **Replace Values** screen appears. This screen also appears when cycling though the screens after the **Work with Command Rule** screen.

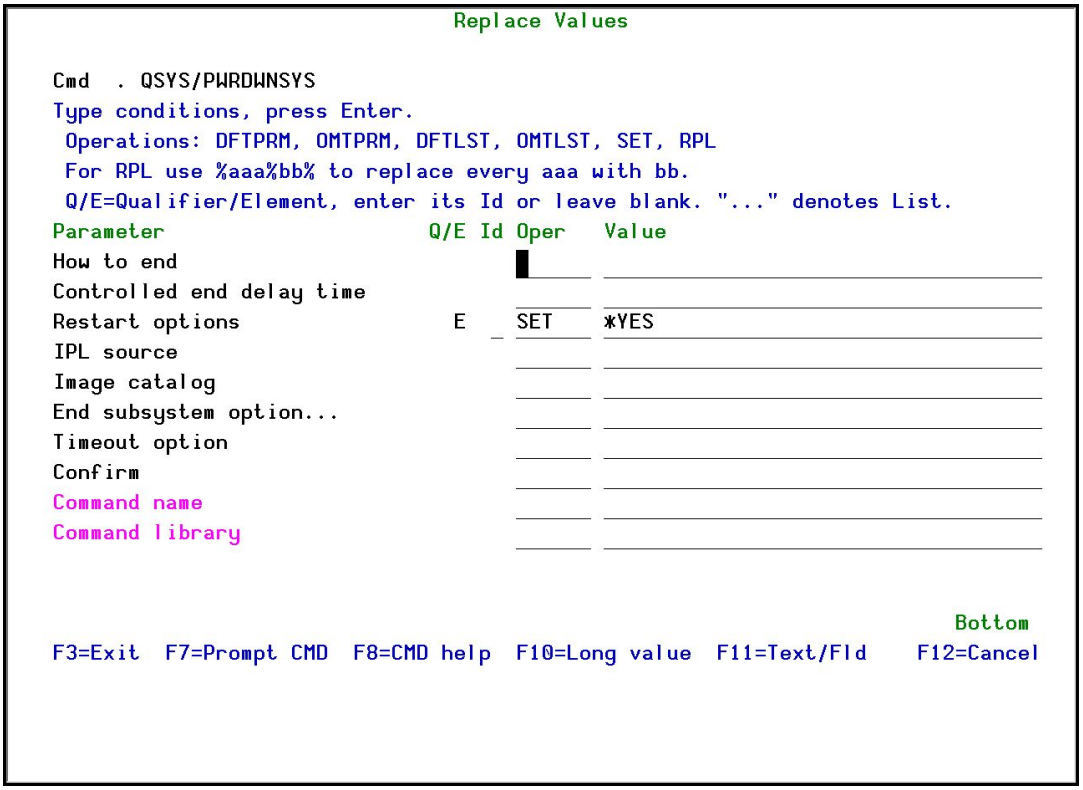

Figure 17: Replace Values Screen

Parameters / Options	Description
Operations	Cmd . QSYS/PWRDWNSYS DFTPRM – Default Parameter OMTPRM – Omit Parameter DFTLST –Default List OMTLST – Omit List SET – Set Parameter RPL – Replace Parameter **Note:** For RPL use %aaa%bb% to replace every aaa with bb.
Parameter	Parameters associated with the current command rule:
Q/E=Qualifier/Element	Qualifier or Element to replace
Id	ID of the Qualifier or Element
Oper	Status of the operation
Value	Replacement value
F7	Prompt CMD– to display the command parameters
F8	CMD help
F10	Long Value
F11	Toggles the parameter's descriptive name and field name

Copying a Command Rule

To make a copy of a command rule, choose the rule in the **Work with Command Rules** screen and select **3. Copy**. The **Copy a Command Rule** screen appears.

Update the changes as described in the table below and press **Enter.** The command rule is displayed with the new rule added in the sequence defined.

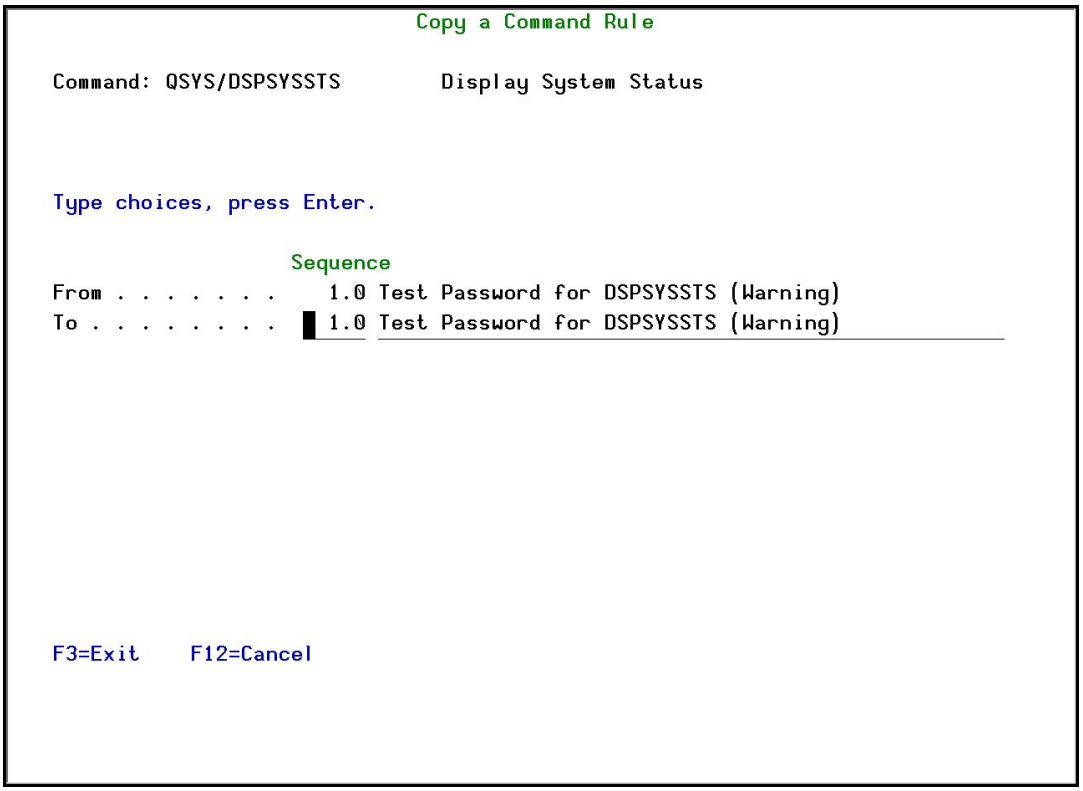

Figure 18: Copy a Command Rule Screen

Parameter	Description
From	Filter = Sequence ID of the current rule ID = Description of the rule
To	Filter = Enter a new sequence number for the new rule ID = Change the description of the rule

Removing a Restricted Command

To remove a command, choose it and select **4. Remove**. The **Remove Restricted Command** screen appears. Press **Enter** to confirm its removal.

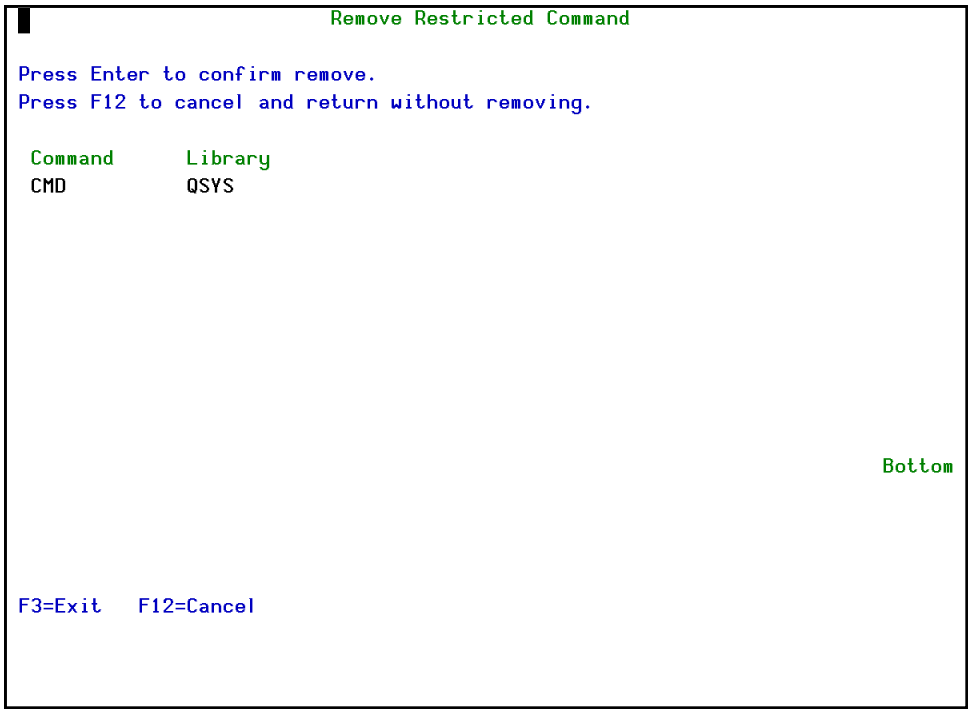

Figure 19: Remove Restricted Command Screen

Chapter 4: Definitions, Analysis and Maintenance

In addition to the unique features of **Command**, there are powerful functions included from the **Audit**, **Firewall** and **Password** products. During the initial setup, **Command** also installs the required libraries from these external products. For inherited Definitions, Analysis and Maintenance screens that appear within **Command** and require a pre-set product type, **Command** is the default.

For a full explanation of the inherited functionality, please see the latest version of the documentation.

Functionality	Reference
Definitions	
31. Time Groups	Audit User Manual
32. General Groups	Audit User Manual
Analysis	
41. Work with Queries	Audit User Manual
42. Command log	Audit User Manual
Maintenance	
81. System Configuration	Firewall User Manual
	21. Password Dictionaries – see Password User Manual
	31. General Definitions – see Command General Definitions on page 51
	81. iSecurity/Base – see Audit User Manual
82. Maintenance Menu	Firewall User Manual
83. Central Administration	Audit User Manual
83. Base Support	Audit User Manual

Command General Definitions

Command General Definitions is a unique Maintenance screen that enables users to disable the product completely, determine which mode to run it in and what data to log.

To open the **Command General Definitions** screen, select **81. System Configuration** from the main screen, then **31. General Definitions**.

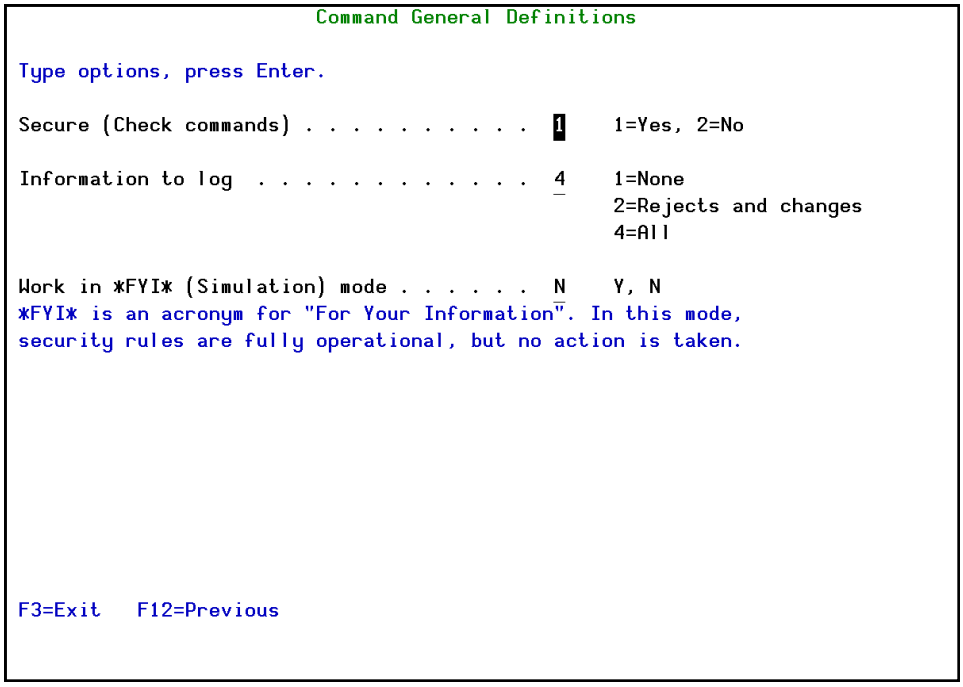

Figure 20: Command General Definitions Screen

Parameter	Description
Secure (Check commands)	1 = Yes – enables Command 2 = No – disables Command
Information to log	1 = None 2 = Rejects and changes 4 = All